

106 年度委託研究報告

建置基站資安檢測環境計畫(第 2 期)
委託研究案期末報告

計畫委託機關：國家通訊傳播委員會

中華民國 107 年 5 月

106 年度委託研究報告

PG106-06-0006

建置基站資安檢測環境計畫(第 2 期)

委託研究案期末報告

受委託單位

財團法人電信技術中心

計畫主持人

蔡志明

協同主持人

江亮均、范俊逸、黃士原

研究人員

蔡明德、陳志宇、莊惠婷

研究期程：中華民國 106 年 6 月至 107 年 5 月

研究經費：新臺幣 2,413 萬元

本報告不必然代表國家通訊傳播委員會意見

中華民國 107 年 5 月

目 次

表 次.....	VI
圖 次.....	VIII
提 要.....	XVII
Abstract	XXII
第一章、緒論	1
第一節 研究緣起.....	1
第二節 研究背景.....	3
第三節 研究目的.....	34
第二章、研究方法與進度說明	36
第一節 研究方法.....	36
第二節 研究進度說明	46
第三章、前瞻性資安技術研究	55
第一節 資安防護技術與服務之最新趨勢研究	55
第二節 資安檢測標準與檢測流程之最新趨勢研究.....	171
第三節 小結	221
第四章、國際行動寬頻框架研究	223
第一節 美國	223
第二節 加拿大	236
第三節 歐盟	259
第四節 英國	275
第五節 日本	295
第六節 行動寬頻資安政策芻議.....	313
第七節 小結	320

第五章、行動寬頻資安技術研究	324
第一節 空中介面資安技術研究.....	324
第二節 基站資安檢測技術研究.....	374
第三節 核心網路-MME 資安檢測技術研究	555
第四節 建置基站弱點資料庫	592
第五節 小結	604
第六章、建構行動寬頻基站資安檢測平臺	607
第一節 研析行動寬頻基站資安檢測平臺架構	608
第二節 驗證行動寬頻基站資安檢測平臺	668
第三節 小結	684
第七章、行動寬頻基站資安檢測規範草案建議	686
第一節 適用範圍.....	687
第二節 檢測環境建議.....	689
第三節 用語釋義.....	692
第四節 檢測項目與要求.....	693
第五節 小結	732
第八章、行動寬頻資安座談會及研討會辦理成果	733
第一節 行動寬頻基站資安檢測規範草案座談會.....	733
第二節 行動寬頻基站資安研討會.....	737
第三節 小結	743
第九章、研究發現與建議事項	744
第一節 研究發現.....	744
第二節 後續建議事項.....	752
參考書目	757
附錄一 出國參訪報告	
附錄二 3GPP TS33.216 V15.0.0 中譯版	
附錄三 NIST SP 800-187 Guide to LTE Security 中譯版	

附錄四 ETSI TR 103 456 版本 1.1.1 中譯版

附錄五 座談會紀錄及意見回覆

附錄六 研討會簡報

附錄七 期末審查簡報及審查意見回覆

表 次

表 1- 1 家用基站(HeNB)安全威脅	25
表 2- 1 期中報告交付之工作項目說明	46
表 2- 2 研究進度甘特圖	51
表 3- 1 近年行動寬頻網路資安事件整理	56
表 3- 2 信令安全防護措施	78
表 3- 3 檢測特徵值	79
表 3- 4 4G、5G 效能比較表	81
表 3- 5 5G 網路安全威脅及安全建議	96
表 3- 6 傳統網路架構與 SDN 架構的比較表	118
表 3- 7 SDN 實作架構比較	127
表 3- 8 SDN 攻擊及防護技術	135
表 3- 9 Category 比較表	145
表 3- 10 eMTC、EC-GSM 和 NB-IoT 比較表	146
表 3- 11 NB-IoT 頻段	153
表 3- 12 可用於 NB-IoT In-Band 模式中的 LTE PRB 索引	155
表 3- 13 物聯網安全需求	159
表 3- 14 3GPP 基站安全相關 33 系列標準	172
表 3- 15 3GPP 文件常用之英文縮寫	173
表 3- 16 3GPP TS 33.401 規範更新整理	174
表 3- 17 3GPP TS 33.117 檢測項目	177
表 3- 18 3GPP TS 33.117 規範更新整理	180
表 3- 19 3GPP TR 33.926 規範更新整理	183
表 3- 20 3GPP TS 33.216 特定於 eNB 之安全要求檢測項目	186
表 3- 21 NESAS 定義之生命週期	193
表 3- 22 產品生命週期之安全要求	194
表 3- 23 評估保證等級說明	216
表 3- 24 EAL4 之評估項目	218
表 3- 25 國際通信設備與 CC 保證等級認證概況	220
表 4- 1 美國關鍵基礎設施列表	230
表 4- 2 加拿大聯邦政府各機構於網路安全中之主責內容	240
表 4- 3 加拿大網路安全策略行動方案	243
表 4- 4 加拿大網路安全策略行動方案：政府資訊系統安全防護項目	244
表 4- 5 加拿大網路安全策略行動方案：政府外部之網路安全防護	247
表 4- 6 加拿大網路安全策略行動方案：提升加拿大公民的網路安全防護	252
表 4- 7 加拿大 2016 年網路安全月各週主題	254

表 4- 8 歐盟安全法律框架的合併	263
表 4- 9 英國關鍵基礎設施	286
表 4- 10 日本網路安全基本法輪廓	299
表 4- 11 第四次行動計畫措施	307
表 4- 12 資訊共享體制的各有關單位的職責	311
表 4- 13 各國資安體系與任務比較	322
表 5- 1 偽基站參數一覽表	333
表 5- 2 偽基站進行設備與身份追蹤參數一覽表	336
表 5- 3 Circuit Switched 及 Packet Switched Network 的比較	352
表 5- 4 VoLTE 之資安威脅及防護建議	361
表 5- 5 基站介面一覽表	382
表 5- 6 基站安全威脅一覽表	383
表 5- 7 基站自發性連外行為分析	501
表 5- 8 家用基站(HeNB)之資安威脅	512
表 5- 9 家用基站(HeNB)檢測項目研究	515
表 5- 10 程序監控功能	549
表 5- 11 檔案監控功能	550
表 5- 12 與 3GPP 所提的安全裝置比較	553
表 5- 13 MME 註冊程序相關規範	586
表 5- 14 MME 安全模式相關規範	587
表 5- 15 MME 換手行為與緊急通道相關規範	590
表 6- 1 建構基站資安檢測平臺執行步驟	610
表 7- 1 檢測範圍	688
表 7- 2 網路單元與檢測設備一覽表	691
表 7- 3 檢測項目及參考來源一覽表	694
表 8- 1 電信業者意見摘要及本計畫團隊之回應	733
表 8- 2 設備商意見摘要及本計畫團隊之回應	736
表 8- 3 行動寬頻基站資安研討會議程	738

圖 次

圖 1-1 行動寬頻網路(4G LTE)整體風險.....	4
圖 1-2 UE 初始基站選擇流程	7
圖 1-3 偽基站欺騙 UE 實驗架設	9
圖 1-4 SDN 架構圖	13
圖 1-5 IoT 架構圖	14
圖 1-6 系統開發生命週期	16
圖 1-7 安全觀念與關係	18
圖 1-8 LTE/SAE 安全架構	20
圖 1-9 SECAM 安全檢測流程(以 MME 為例).....	21
圖 1-10 3GPP SECAM & GSMA NESAG 認證之角色	23
圖 1-11 5G 安全架構構想	31
圖 1-12 SDN 各面向攻擊手法示意圖	32
圖 2-1 研究架構圖	36
圖 2-2 本計畫施行方式與執行步驟.....	39
圖 2-3 建構基站資安檢測平臺執行步驟	43
圖 2-4 各章節研究主題及關聯性.....	45
圖 3-1 SS7 之節點與連結 link 之關係圖.....	65
圖 3-2 SS7 協定堆疊對應 OSI 架構圖	68
圖 3-3 SS7 攻擊示意圖.....	71
圖 3-4 SS7 防禦方式.....	74
圖 3-5 組件流程圖	79
圖 3-6 IMT-2020 5G 標準訂定時刻表.....	84
圖 3-7 5G 生態系統示意圖.....	86
圖 3-8 三大服務示意圖	87
圖 3-9 網路切片(Network Slicing)示意圖	89
圖 3-10 SDN 與邊緣雲及核心雲關係示意圖.....	91
圖 3-11 頻譜應用示意圖	93
圖 3-12 2013~2018 年全球行動網路終端數量曲線圖	94
圖 3-13 蜂巢式基地台與 C-RAN 架構示意圖	95
圖 3-14 5G 基本安全需求	101
圖 3-15 高層級安全願景的基本要素	102
圖 3-16 5G eMBB 異構接入網路統一認證機制	105
圖 3-17 端到端用戶數據安全協議設計	107
圖 3-18 開放身分管理可促進 5G 生態環境的發展	109
圖 3-19 mMTC 去中心化身分與密鑰管理.....	111

圖 3- 20 IBC 去中心化的身份管理及認證.....	112
圖 3- 21 5G URLLC 4 大安全面向	113
圖 3- 22 傳統網路架構與 SDN 架構比較圖	117
圖 3- 23 SDN 架構示意圖	121
圖 3- 24 Open Network Operating System 架構示意圖.....	122
圖 3- 25 OpenDayLight 架構示意圖	124
圖 3- 26 VMware NSX 基於 SDN 的架構示意圖.....	126
圖 3- 27 DDoS 示意圖	131
圖 3- 28 SDN 網路架構攻擊途徑圖	134
圖 3- 29 NICE 執行過程.....	139
圖 3- 30 IoT 概念圖	143
圖 3- 31 IoT 架構圖	149
圖 3- 32 NB-IoT 網路架構圖.....	151
圖 3- 33 網路架構的空中介面.....	152
圖 3- 34 NB-IoT 佈建方式.....	155
圖 3- 35 NB-IoT slot 架構.....	156
圖 3- 36 NB-IoT frame 架構	156
圖 3- 37 金鑰管理機制示意圖.....	161
圖 3- 38 Mirai 攻擊流程	168
圖 3- 39 IPcam 攻擊流程	170
圖 3- 40 3GPP TS 33.401、TS 33.117、TR 33.926 與 TS 33.216 關係圖.....	185
圖 3- 41 NESAS 之架構概述.....	190
圖 3- 42 NESAS 檢測實驗室之認證流程.....	192
圖 3- 43 服務生態系統圖例	203
圖 3- 44 各層級的服務生態系統範例	204
圖 3- 45 常見的物聯網端點配置.....	205
圖 3- 46 私人網路配置範例	210
圖 3- 47 用於 M2M 設備管理的 ETSI 高階架構.....	215
圖 4- 1 美國 DHS 內之資安主責組織架構	228
圖 4- 2 加拿大聯邦政府各機構於網路安全議題之權責區分.....	239
圖 4- 3 加拿大網路安全通報架構.....	257
圖 4- 4 加拿大網路安全架構與各級單位標準作業程序關係.....	257
圖 4- 5 歐盟關鍵基礎設施保護行動綱要	267
圖 4- 6 影響關鍵基礎設施保護(CIIP)成效之因素.....	269
圖 4- 7 英國通訊法第 105A 相關標準	281
圖 4- 8 基礎設施應變恢復力的組成部分	285
圖 4- 9 網路安全 10 步驟	291

圖 4- 10 日本網路安全政策沿革	298
圖 4- 11 日本網路安全政策推展體制	301
圖 4- 12 資訊安全緊急支援小組架構	304
圖 4- 13 政府民間合作之關鍵基礎設施防護推展架構	306
圖 4- 14 關鍵基礎設施與政府機關各措施關聯圖	309
圖 4- 15 資訊共享體制	310
圖 5- 1 初始細胞選擇程序	326
圖 5- 2 檢測系統架構	327
圖 5- 3 認證同步失敗攻擊程序	328
圖 5- 4 認證中間人攻擊程序	328
圖 5- 5 追蹤攻擊程序	329
圖 5- 6 鏈接性攻擊程序	331
圖 5- 7 斷線/降等攻擊程序	331
圖 5- 8 偽基站測試平台架構	333
圖 5- 9 行動網路模擬器偽基站設定上下行鏈路	334
圖 5- 10 行動網路模擬器偽基站設定 MCC、MNC 與 TAC	334
圖 5- 11 手機收到 Attach Reject 信令	334
圖 5- 12 手機收到 Attach Reject 信令內容 PLMN not allowed	335
圖 5- 13 手機收到 Attach Reject 信令內容 Illegal UE	335
圖 5- 14 設備與身份追蹤設定上下行鏈路	337
圖 5- 15 設備與身份追蹤設定 MCC、MNC 與 TAC	337
圖 5- 16 偽基站收到手機 IMSI	338
圖 5- 17 偽基站收到手機 GUTI	338
圖 5- 18 USRP B210	339
圖 5- 19 OAI 架構	340
圖 5- 20 TAU Reject 訊息	341
圖 5- 21 TAU 程序測試-UE 端畫面	341
圖 5- 22 OAI 操作畫面	342
圖 5- 23 UE 端個人識別碼	343
圖 5- 24 UE 端被捕捉之程序	344
圖 5- 25 偽基站端捕捉畫面	344
圖 5- 26 LTE 安全解決方案	346
圖 5- 27 用戶端設備偵測示意圖	348
圖 5- 28 偽基站偵測示意圖	349
圖 5- 29 VoLTE 整體架構圖	352
圖 5- 30 LTE 網路架構示意圖	353
圖 5- 31 LTE Control plane 層之架構圖	354

圖 5- 32 IMS 架構示意圖	357
圖 5- 33 VoLTE 註冊流程	358
圖 5- 34 VoLTE 簡易 call setup	363
圖 5- 35 SIP-200 OK Response	365
圖 5- 36 SIP-INVITE 信號.....	365
圖 5- 37 QoS 優先乘載配置	367
圖 5- 38 200 OK 內含運營商相關訊息	369
圖 5- 39 200 OK 內含 IP 位址	369
圖 5- 40 P-Asserted-Identity	371
圖 5- 41 會話控制表	372
圖 5- 42 183 Session Progress.....	373
圖 5- 43 LTE 基本系統架構圖.....	378
圖 5- 44 E-UTRAN 與 EPC 功能說明	380
圖 5- 45 E-UTRAN 多重架構圖	382
圖 5- 46 E-UTRAN 網路安全階層示意圖	385
圖 5- 47 LTE 基站安全信令	386
圖 5- 48 一般性檢測項目測試架構.....	387
圖 5- 49 Initial RRC Connection Setup and Reconfiguration 信令截圖	389
圖 5- 50 UE Initial Attach Uu 介面信令截圖	391
圖 5- 51 S1AP Initial UE Message 信令截圖	393
圖 5- 52 S1AP UE Context Release Request 信令截圖.....	395
圖 5- 53 Tracking Area Update Accept 信令截圖	397
圖 5- 54 S1AP Initial Context Setup Request 信令截圖	400
圖 5- 55 X2 Setup Response 信令截圖	402
圖 5- 56 Downlink NAS Transport 信令截圖	404
圖 5- 57 Uplink NAS Transport 信令截圖.....	406
圖 5- 58 IPsec Connection 信令截圖	408
圖 5- 59 進階資安檢測架構	410
圖 5- 60 C 廠牌基站系統過載狀態時處理機制	412
圖 5- 61 C 廠牌基站 Flow Control Parameter	412
圖 5- 62 C 廠牌基站 CPU/DSP Usage Monitoring	413
圖 5- 63 C 廠牌基站之密碼雜湊函數	414
圖 5- 64 C 廠牌基站系統過載處理的機制.....	416
圖 5- 65 A 廠牌事件記錄.....	417
圖 5- 66 B 廠牌基站之 administrativeState 設定	417
圖 5- 67 B 廠牌基站之事件記錄	418
圖 5- 68 C 廠牌基站之事件紀錄詳細資訊.....	419

圖 5- 69 C 廠牌基站之總事件紀錄一覽表.....	419
圖 5- 70 C 廠牌基站之 Ping 異常事件紀錄	420
圖 5- 71 A 廠牌基站網站伺服器日誌內容.....	421
圖 5- 72 A 廠牌基站網站伺服器日誌內容摘錄	421
圖 5- 73 C 廠牌基站網站伺服器日誌內容摘錄	422
圖 5- 74 A 廠牌基站網站伺服器弱點掃描結果	423
圖 5- 75 C 廠牌基站網站伺服器弱點掃描結果	424
圖 5- 76 C 廠牌基站關閉 ARP Proxy 功能.....	430
圖 5- 77 C 廠牌基站之 SHA-256 完整性驗證.....	431
圖 5- 78 C 廠牌基站之軟體驗證與載入成功畫面	431
圖 5- 79 Windows Task Manager	432
圖 5- 80 A 廠牌基站 TRACK 與 TRACE 檢測	433
圖 5- 81 C 廠牌基站 TRACK 與 TRACE 檢測	433
圖 5- 82 C 未存有不使用之附加元件驗證.....	434
圖 5- 83 A 與 C 廠牌基站之網站目錄存取限制檢測.....	437
圖 5- 84 C 廠牌基站網站伺服器設定問題： Unprotected File	440
圖 5- 85 C 廠牌基站網站伺服器.gz 檔案一覽	440
圖 5- 86 A 與 C 基站 Directory Traversal 掃描結果	441
圖 5- 87 A 基站網站存有 CWE-79 弱點	443
圖 5- 88 A 基站網站存有 Server Error Message 問題	445
圖 5- 89 A 基站廠商之 User & Control Plane	449
圖 5- 90 C 廠牌基站之 User Date 設定	449
圖 5- 91 B 廠牌基站之 User Date 設定	451
圖 5- 92 A 廠牌基站之 TLS 加密	453
圖 5- 93 C 廠牌基站之 TLS 加密	454
圖 5- 94 A 廠牌基站之服務開啟結果	455
圖 5- 95 B 廠牌基站之服務開啟結果	456
圖 5- 96 C 廠牌基站之服務開啟結果	456
圖 5- 97 C 廠牌基站 VLAN 與 User Plane	458
圖 5- 98 C 廠牌基站 VLAN 與 Control Plane.....	458
圖 5- 99 C 廠牌基站 VLAN 與 Management Plane	458
圖 5- 100 A 廠牌基站已安裝軟體清單	460
圖 5- 101 B 廠牌基站已安裝軟體清單	460
圖 5- 102 C 廠牌基站已安裝軟體清單	461
圖 5- 103 A 廠牌基站之服務開啟結果	464
圖 5- 104 B 廠牌基站之服務開啟結果	465
圖 5- 105 C 廠牌基站之服務開啟結果	466

圖 5- 106 C 廠牌基站 IP Forwarding Enabled.....	467
圖 5- 107 C 廠牌基站 SSL 2.0/SSL 3.0.....	468
圖 5- 108 C 廠牌基站建立帳號組數	471
圖 5- 109 C 廠牌基站內建預設帳號停用	473
圖 5- 110 A 廠牌基站密碼複雜性設定.....	475
圖 5- 111 C 廠牌基站密碼複雜性設定.....	476
圖 5- 112 C 廠牌基站密碼可重複使用次數設定	477
圖 5- 113 A 廠牌基站登入輸入錯誤限制.....	479
圖 5- 114 A 廠牌基站 SSH 暴力破解測試	479
圖 5- 115 C 廠牌基站登入輸入錯誤限制.....	480
圖 5- 116 C 廠牌基站登入輸入錯誤次數限制設定	480
圖 5- 117 C 廠牌基站帳號權限控管	481
圖 5- 118 C 廠牌基站帳號登出功能	482
圖 5- 119 C 廠牌基站帳號操作逾時功能.....	484
圖 5- 120 A 廠牌基站主要操作介面	491
圖 5- 121 B 廠牌基站主要操作介面	491
圖 5- 122 C 廠牌基站主要操作介面	492
圖 5- 123 A 廠牌基站敏感性資料	493
圖 5- 124 B 廠牌基站敏感性資料	494
圖 5- 125 A 廠牌基站日誌紀錄資訊	495
圖 5- 126 B 廠牌基站日誌紀錄資訊	495
圖 5- 127 C 廠牌基站日誌紀錄資訊	496
圖 5- 128 A 廠牌基站軟體雜湊驗算資訊.....	497
圖 5- 129 B 廠牌基站軟體雜湊驗算資訊.....	497
圖 5- 130 C 廠牌基站軟體雜湊驗算資訊.....	498
圖 5- 131 A 廠牌基站 OAM 設定.....	499
圖 5- 132 B 廠牌基站 OAM 設定.....	500
圖 5- 133 已知威脅分析結果.....	502
圖 5- 134 未知威脅分析結果.....	502
圖 5- 135 A 廠牌基站之藍芽模糊測試	504
圖 5- 136 A 廠牌基站之 TLS 模糊測試	505
圖 5- 137 C 廠牌基站韌體分析結果一覽.....	506
圖 5- 138 A 廠牌基站韌體分析結果一覽.....	507
圖 5- 139 3GPP 之 HeNB 架構圖	509
圖 5- 140 3GPP 之 HeNB 安全架構	510
圖 5- 141 存取控制清單截圖.....	517
圖 5- 142 4G 設定檔截圖	518

圖 5- 143 系統日誌檔截圖	520
圖 5- 144 密碼資料截圖	521
圖 5- 145 後端鏈路傳輸通道截圖	523
圖 5- 146 遠端管理登入介面截圖	525
圖 5- 147 憑證唯一性截圖	526
圖 5- 148 系統更新截圖	528
圖 5- 149 韌體拆解過程截圖	530
圖 5- 150 韌體拆解後所顯示出之檔案系統截圖	531
圖 5- 151 後端鏈路之封包側錄截圖	533
圖 5- 152 首次連上核網之封包側錄截圖	534
圖 5- 153 弱點掃描結果截圖	536
圖 5- 154 開機程序竄改截圖	538
圖 5- 155 XSS 跨站腳本攻擊風險截圖	539
圖 5- 156 憑證強度不足風險截圖	540
圖 5- 157 日誌資料截圖	541
圖 5- 158 修改日誌檔存取權限截圖	543
圖 5- 159 日誌資料截圖	543
圖 5- 160 HeNB 外觀截圖-未使用防拆螺絲	545
圖 5- 161 HeNB 外觀截圖-SIM 卡插槽	546
圖 5- 162 系統呼叫執行流程	548
圖 5- 163 本防護機制之軟體架構圖	551
圖 5- 164 日誌檔實驗結果	552
圖 5- 165 防護測試實驗結果	553
圖 5- 166 EPC 架構圖	555
圖 5- 167 MME 漫遊架構圖	561
圖 5- 168 MME 介面架構圖	563
圖 5- 169 EPS 產生過程	571
圖 5- 170 UE 驗證程序圖	571
圖 5- 171 KASME 產生圖	572
圖 5- 172 安全模式程序圖	574
圖 5- 173 重新同步訊息交換流程圖	581
圖 5- 174 同核網的 MME 換手	582
圖 5- 175 CVE-2017-15326 漏洞	596
圖 5- 176 C 廠牌基站韌體檔案分析結果	596
圖 5- 177 A 廠牌基站韌體檔案分析結果	597
圖 5- 178 C 廠牌基站韌體檔案內之第三方開源軟體元件	597
圖 5- 179 A 廠牌基站韌體檔案內之第三方開源軟體元件	598

圖 5- 180 C 廠牌基站韌體檔案已存在之攻擊工具	598
圖 5- 181 A 廠牌基站韌體檔案已存在之攻擊工具	599
圖 5- 182 eNodeB VULDB 登入首頁畫面.....	601
圖 5- 183 eNodeB VULDB 快速篩選功能.....	601
圖 5- 184 eNodeB VULDB 根據 CVE 嚴重等級呈現不同數量.....	602
圖 5- 185 eNodeB VULDB Exploit-Tools 篩選功能	602
圖 5- 186 eNodeB VULDB 報表內容	603
圖 5- 187 eNodeB VULDB 之 CVE 漏洞一覽.....	604
圖 6- 1 建構基站資安檢測平臺執行步驟	608
圖 6- 2 基站資安檢測平臺各功能模組單元對應關係概念圖.....	610
圖 6- 3 第四代行動通訊網路層通訊功能模組關係概念圖	612
圖 6- 4 E-UTRAN 通訊堆疊圖	613
圖 6- 5 各種基站佈署情境比較.....	615
圖 6- 6 S1 通訊介面連接概念圖.....	616
圖 6- 7 不同世代基地台的演化與擔負之任務.....	617
圖 6- 8 X2 介面換手流程示意圖	618
圖 6- 9 基站資安檢測平臺-可應用之基站設備檢測類別圖說	619
圖 6- 10 基站資安檢測平臺-可應用之用戶端設備類別圖說	620
圖 6- 11 對用戶端設備進行 LTE 服務阻斷行為	622
圖 6- 12 對用戶端設備進行所有服務阻斷行為(進入緊急模式).....	622
圖 6- 13 大量用戶端裝置之信令堆疊關係圖.....	623
圖 6- 14 換手(Handover)程序的金鑰交換流程	625
圖 6- 15 核心網架構與基礎元件示意圖	626
圖 6- 16 核心網架構與基礎元件並內納入 IP 多媒體子系統之示意圖.....	627
圖 6- 17 核心網路與 VoLTE 結合的完整服務架構.....	628
圖 6- 18 IP 多媒體子系統使用 VoIP/LTE 之示意圖	629
圖 6- 19 基站資安檢測平臺-可應用之基本核心網路組套類別圖說.....	630
圖 6- 20 LTE 核心網路模擬器架構圖	631
圖 6- 21 策略與計費控制架構.....	634
圖 6- 22 實體核心網路設備、元件與架構對應示意圖	636
圖 6- 23 4G+網路接取與應用測試實驗室	637
圖 6- 24 以 Intel 通用型伺服器平臺構建之電信基礎環境.....	640
圖 6- 25 傳統核心網路設備與 NFV 架構的比較.....	641
圖 6- 26 ETSI 提出之新式 vEPC 概念框架.....	642
圖 6- 27 基站資安檢測平臺-主動式常見與潛在弱點檢測組套圖說.....	647
圖 6- 28 傳統的風險評估的估算方式	648
圖 6- 29 共通弱點探測與評估工具---以 OpenVAS 為例	652

圖 6-30 共通弱點探測與評估結果報表---以 OpenVAS 為例	653
圖 6-31 共通弱點滲透測試工具開放原始碼框架-以 Metasploit 為例	654
圖 6-32 共通弱點探測、評估與滲透測試整合-以 Nexpose 搭配 Metasploit 為例	656
圖 6-33 獨立式惡意軟體與行為分析架構	659
圖 6-34 整合式惡意軟體與行為分析概念架構	660
圖 6-35 基站資安檢測平臺-被動式連線與滲透行為分析組套圖說	661
圖 6-36 特徵與異常行為比對概念圖	663
圖 6-37 特徵與異常行為比對流程圖	664
圖 6-38 進階持續性威脅運作流程圖	666
圖 6-39 沙箱技術與整合式威脅管理共構運作流程圖	668
圖 6-40 行動寬頻基站資安檢測平臺配置概念圖	669
圖 6-41 一般性檢測實作基本架構圖	670
圖 6-42 工程手機檢測畫面範例	671
圖 6-43 UE 模擬器大量使用者連線畫面範例	672
圖 6-44 核心網路信令交握畫面範例	673
圖 6-45 LTE 資訊安全威脅與管理的切入點	674
圖 6-46 基站韌體/軟體掃描畫面範例	675
圖 6-47 基站服務掃描畫面範例	676
圖 6-48 網路服務弱點檢測畫面範例	678
圖 6-49 動態惡意行為與傳遞路徑描述畫面範例	679
圖 6-50 已知惡意之行為與軟體偵測機制示意圖	679
圖 6-51 已知惡意之行為與軟體偵測警示資訊	681
圖 6-52 進階持續性滲透攻擊行為偵測機制示意圖	682
圖 6-53 混合式進階持續性滲透攻擊分析畫面範例	683
圖 6-54 惡意行為偵知紀錄畫面範例	683
圖 6-55 待測基站連外行為檢測與分析畫面範例	684
圖 7-1 檢測規範草案擬定流程	686
圖 7-2 基站資安檢測規範草案架構	687
圖 7-3 檢測環境示意圖	690
圖 8-1 主持人致詞-TTC 林炫佑副執行長	739
圖 8-2 貴賓致詞-NCC 吳銘仁簡任技正	739
圖 8-3 建置基站資安檢測環境計畫介紹-計畫主持人蔡志明主任	740
圖 8-4 研討會講者簡報剪影	741
圖 8-5 基站檢測平臺展示及交流	742
圖 8-6 研討會貴賓及講者合影	742
圖 8-7 研討會 Q&A	743
圖 9-1 行動寬頻基站資安檢測流程	747
圖 9-2 行動寬頻基站資安檢測平臺	750

提 要

關鍵詞：行動寬頻網路、行動寬頻資訊安全、基站、網路攻擊、基站安全

一、研究緣起

行動寬頻網路已成為國內主流之寬頻上網服務，更是經濟資訊流通及交易重要通道。但在行動寬頻扁平式全 IP 網路架構下，用戶端連接至基站後即可直通核心網路，在 IP 傳輸環境下之基站系統與核心網路，若無強制性資安防護措施，未來可能成為各種不法攻擊的目標與途徑，使得行動寬頻基站系統的資安管理更具其重要性。

有鑑於國內需要積極建構行動寬頻友善的環境，以帶動豐富 4G 內容服務與創新應用服務發展，行政院於 103 年特別規劃「加速行動寬頻服務及產業發展方案」，該計畫之消費者權益保障推動項目中，即希望從行動寬頻基站管理及檢測著手，加強行動寬頻網路之安全，使民眾能安心使用 4G 服務。

因此本計畫係執行 NCC 源自行政院上述發展方案中之委託研究案，105 年已完成「建置基站資安檢測環境計畫第 1 期」研究，完成行動寬頻網路風險分析，研析行動寬頻網路資安之檢測工具及方法，規劃出行動寬頻資安檢測平臺並產出行動寬頻基站管理方針芻議。本計畫「建置基站資安檢測環境計畫第 2 期」委託專業服務工作項目，擬整合 NCC 採購之 LTE 基站及資安檢測工具，透過租賃之 LTE 核心網路，建置一行動寬頻基站資安檢測示範性平臺，研擬基站資安檢測項目，並執行實測，就實測結果與國際文獻研析，提出適合國內環境之行動寬頻基站資安檢測規範草案，協助國內電信業者加強行動寬頻網路安全，以保障消費者權益。

二、研究方法及過程

第 2 期計畫將延續第 1 期之研究結果，透過文獻分析與比較分析持續針對前瞻性資安技術、國際行動寬頻資安框架進行研究外，主要重點為以仿真 LTE 之檢測環境規劃行動寬頻基站(包含 eNodeB 及家用基站(HeNB))資安檢測項目、建構基站資安示範性檢測平臺並執行實測驗證，依實測結果並參考國際標準，規劃出適合國內環境之基站資安檢測規範草案與檢測流程，最終將本計畫之弱點檢測結果同時參考國際性之弱點資料庫，建置一基站弱點資料庫供產官學界參考。

上述研究將配合國外參訪與「行動寬頻基站資安座談會及研討會」之舉辦，促進相關領域主管機關、學界及業界彼此分享觀摩及交換意見與建議，藉此提升我國整體

行動寬頻網路安全。

三、重要發現

透過文獻研析、國際經驗之蒐集及基站之實測驗證，本研究之重要發現摘要如下：

(一) 資安防護技術及與服務最新趨勢

本團隊已針對近年國際最關注的 SS7 攻擊，以及國內電信業者已在積極發展的 5G、SDN 及 IoT 之資安攻擊與防護技術進行深入研析，綜整歸納出上述四大主題之最新安全防護技術。

(二) 資安檢測標準與檢測流程之最新趨勢

1. 國際標準組織已訂定基站安全保證規範

本團隊在研析 3GPP 與行動寬頻基站相關之 33 安全系列標準文件時，發現 3GPP 於 2017 年 9 月最新發表了 TS33.216 eNB 安全保證規範，本團隊於基站資安檢測規範規劃上即以此規範為主要參考依據，另分析與此文件有密切關聯的 TS 33.117(網通產品安全)、TR 33.926(網通產品之安全威脅)與 TS 33.401(EPS 架構)三份文件內容，綜整出 3GPP 對基站安全及檢測之最新規範。

2. GSMA 訂定安全認證流程，預計 2018 年試行

在 GSMA 產品與製程安全性的認證流程-安全保證方法方面，該流程從供應商之生命週期安全認證出發，且訂定第三方檢測實驗室之認證標準，於訪談 Ericsson 的過程中，該公司人員表示 GSMA 已通過兩家檢測實驗室之認證，預計今年將與設備製造商合作，透過認可的檢測實驗室依 3GPP 訂定之安全保證規範(SCAS)執行設備商產品之驗證測試。

(三) 基站資安實測結果發現

1. 商用基站現存之漏洞威脅

本研究實測發現，家用商用基站之身分認證、網站管理介面、敏感資訊及實體層存在風險；而在基站設備上也發現主要安全問題為韌體檔案內金鑰未加密、網站存在安全弱點及內建預設密碼於初次登入無要求強制變更等風險。本團隊在檢測過程中發現之商用設備安全漏洞，在第一時間也通知並輔導廠商進行相關修正及更新，並協助

重新檢測以確保其設備之安全性。

2. 基站設備之安全需源自產品設計

本研究實測發現，很多測試項目的需求必須由基站製造廠商提供更進一步的安全資訊才可完成測試，這些高階或專利授權功能掌握於設備商的技術與開發人員手上，採購使用的電信業者不全然有權限執行或了解這些設定與配置，印證了 3GPP 安全保證規範與 GSMA 合作建立的安全認證方法(NESAS)，要求流程認證必須從供應商之產品生命週期安全性驗證開始，以確保其產品商用化後之安全性。

3. 基站資安檢測流程

本團隊在經過實測 3 家廠牌基站與 2 家廠牌家用基站的實測過程及經驗中，建立了一套完整的基站資安檢測流程與方法，此流程除可供本中心檢測人員檢測操作之依據外，同時可做為輔導廠商設備檢測，提供廠商參考之 SOP，以節省受測者執行檢測研究之時間，提高檢測效率。

(四) 基站資安檢測規範草案執行時需考量重點

1. 版本適用性之考量

本檢測規範草案係引用 3GPP TS33.216 R15 版本為主的檢測項目，目前國內電信業者所採用之 4G 基站等通訊相關設備仍以 3GPP 版本 R12 與 R13 為主，雖本團隊於測試過程中大多已篩選 R12 版本可測試之項目，但為使本規範更具適用性，於試行前除與設備商及電信業者，再次逐條檢視其適用性，並訂定日出條款。

2. 安全功能實現差異性

標準規範僅定義應具備的安全功能，並不會限定設計方式，因此設備商在設計、開發產品時均無制式形式，造成機密性、完整性、可用性方面的安全功能實現上存在差異性，故建議可透過廠商自我宣告進行說明，指出基站、核網或加值系統功能與對應規範草案的安全功能，提供檢測單位作為判定是否符合檢測規範草案之要求。

3. 由第三方檢測實驗室協助執行

依 GSMANESAS 的安全認證方法上，其強調由第三方認證實驗室來執行相關檢測，檢測規範由第三方檢測實驗室推動之方法，為國際安全認證方法之所認可，使得檢測上具有可信度及公正性，且可減少業者額外投資之最佳方式。

(五) 國際行動寬頻資安框架研究

1. 國際經驗上並無對基站資安有強制性之檢測要求

本研究於國際資安框架研析及國外參訪中所蒐集資訊，目前國際對行動寬頻網路安全皆採自律性方式管理，並無實施強制性之檢測要求，僅提供資安聯防框架及安全指引建議，針對行動寬頻網路元件之安全，業者皆依循國際標準組 3GPP 之標準。

2. 政府訂定資安聯防框架，國際標準訂定各元件安全保證標準

由本團隊研究國際資安框架發現，政府角色主要在訂定資安聯防框架，在行動寬頻網路安全上，皆採業者自主要求及管理。針對至各網路元件之安全保證規範，設備製造商皆依循國際標準組 3GPP 所訂定之規範，設計其產品之安全性，GSMA 更設計了安全保證方法流程，希望業者可透過認證之第三方實驗室，來取得各元件之安全認證，此方法可做為未來國內業者採購設備時，對安全性的認定標準。

3. 關注及參與國際標準組織之重要性

GSMA 提供其會員，國際最新資安攻擊資訊及 SS7 完整防護建議，本次國外參訪之安全專家也強烈建議，國內應積極加入國際組織之討論，才可獲取最新資安攻擊與防護的最新資訊。

四、主要建議事項

本團隊將主要建議事項分為立即可行建議與中長期建議及作法整理如下：

(一) 立即可行之建議

建議項目	作法	理由	主辦/協辦
持續關注新興技術發展之資安議題	持續研究 SDN、IoT 及 SS7 防護，納入 107 年資安旗艦計畫研析資安技術標準、規範或指引之基礎內容中。	因電信網路新興技術及應用之安全規範及技術仍不斷在發展中，非常值得國內關注。	TTC
善用基站資安檢測平臺之檢測技術及工具	輔導廠商進行檢測。	為使 NCC 採購之檢測工具更有效運用，及建立更多的測試樣本。	TTC/廠商
平臺與場域之開放	將本計畫檢測平臺與各元件，模組化建構與重	提供國產設備試驗及其相應之系統資安驗	TTC/廠商

建議項目	作法	理由	主辦/協辦
	組，延伸為 4G 網路安全檢測平臺-電信網路開放場域。	證之試驗場域。	
輔導廠商檢測，使本計畫草擬之基站資安檢測規範更為完整	延伸至 108 年資安旗艦計畫 2.2 建構通傳事業資通設備之資安檢測機制，進行 HeNB 廠商試行。	經過試行後，可研訂為正式公告之 HeNB 資安檢測技術規範。	TTC/設備商

(二) 中長期性建議

建議項目	作法	理由	主辦/協辦
持續關注並積極參與國際標準組織之安全議題討論	- 鼓勵國內業者或法人加入 GSMA，以取得國際標準於資安攻擊之最新資訊。 - 持續關注 GSMA NESAS 推展進度。	使國內之資安防護措施可與國際接軌。	NCC/委託辦理單位
國內 SS7 資安事件分享機制	建立國內業者與政府間之 SS7 資安事件分享平臺。	使國內主管機關及電信業者更能掌握國內 SS7 資安事件，並可進行預先之防護措施。	NCC/電信業者
主管機關與產業合作建立自願性檢測機制	建議可提供此指引規範，鼓勵業者採取自律性之管理方式。	國際並無基站資安檢測的強制性的檢測規範。	NCC /電信業者
於基站資安檢測規範草案中，可納入通報及定期主動抽檢機制	利用本計畫檢測平臺，在行動用戶通報的疑慮設備加以檢測，或不針對特定業者及特定類型設備進行抽檢。	可定期、主動針對市面設備進行檢測，藉由公開機制向社會展現主管機關為資安議題把關之態度。	NCC/TTC

Abstract

Keyword : 4G, LTE, eNodeB, HeNB, Mobile Broadband Security

Mobile broadband network has become the mainstream broadband internet service in Taiwan, and the important channel for economic information circulation and trading. However, under the flat all-IP network architecture of 4G LTE, users can have direct access to the core network after being connected to the base station (eNodeB/ HeNB). If there is no mandatory data security measure, the base station system and core network in the IP transmission environment could become the target and path of various illegal attacks. Thus the data security management of mobile broadband base station system has become an even more important issue.

The primary objective of this project is to help domestic mobile broadband service telecommunication operators with improvement over the domestic overall mobile broadband security technology and detection capability in order to protect the rights and interests of consumers.

We have planned and completed the demonstrative mobile broadband base station security testing platform in accordance with the research result and the incorporation of international experience. And then the draft of mobile broadband base station security testing specification has be developed via actual tests of (H)eNB and study of mobile broadband base station security and testing technologies in advanced countries.

The primary discoveries of this project are as summarized below:

1. The International Organization for Standardization has established the Security Assurance Specification (SCAS) for eNodeB; the research and analysis process of this project can be traced to the security assurance specification for eNodeB released by 3GPP in September 2017, and the Network Equipment Security Assurance Scheme (NESAS) jointly defined by 3GPP and GSMA. Telecommunication operators and equipment vendors will follow the specifications of 3GPP and the GSMA guidelines, thus we are included as the main reference for the draft of data security testing specification of this project.

2. Discoveries in the results of actual tests of (H)eNB data security:

(1) Existing vulnerabilities in existing commercial (H)eNBs: the actual tests in this study reveals that there are risks in the identity authentication, network management interface, sensitive information, and physical layers of HeNB; and major security issues have been found in eNodeB, such as the unencrypted key in firmware file, security weakness in the website, and the built-in default password is not required to be changed during initial login.

(2) The security of base station equipment must be based on product design: the actual tests in this study reveal that many test items can only be completed when the base station manufacturer provides further security information. These high-end or patent authorization functions are in the hands of technical and development personnel of equipment vendors. The telecommunication operators purchasing the equipment do not have full authorization to perform or understand these settings and configurations. This has justified the requirement of 3GPP SCAS and the NESAS jointly defined with GSMA that the process certification must start with supplier' s product lifecycle security verification in order to ensure the security of product after commercialization.

3. The key points for the implementation of the draft of mobile broadband base station security testing specification: according to the results of actual tests of our team, it is recommended that the formulation and implementation of the draft of mobile broadband base station security testing specification should take into consideration the applicability of 3GPP release version, the difference in implementation approaches of security functions of various brands of equipment, and the importance of having a third party testing laboratory to assist in the implementation.

4. There is no mandatory testing requirement of mobile broadband base station security in international experience: in this study the information collected during overseas visits has been analyzed in the international data security framework. Currently the international mobile broadband network security is managed in a self-discipline manner, and there is no mandatory testing requirement. There are only suggestions for data security protection framework and security guidelines. As for the security of mobile broadband network devices,

all service providers and equipment vendors are in compliance with the International Organization for Standardization's 3GPP standard.

5. The importance of focus on and participation in International Organization for Standardization: GSMA provides its members with latest international data security attack information and SS7 complete protection recommendation. The security experts participating in this overseas visit also strongly recommended that our country should actively participate in discussion with international organization in order to obtain the latest information of data security attack and protection.

The follow-up suggestions proposed in this project are as summarized below:

1. Immediate and feasible suggestions:

(1) Continuous focus on data security issue in development of emerging technology: the continuous development of security specification and technology of emerging telecommunication technology is worthy of attention for our country. It is suggested that we should continue the research on SDN, IoT and SS7 protection to be included in the basic content of data security standard, specification, or guideline of 2018 Digital Convergence/IoT Cyber Threats Defense and Security Lab Project.

(2) Making good use of testing technology and tool of data security testing platform: for more effective utilization of testing tool purchased by NCC, the goal is to help service provider or equipment vendor with carrying out the test in order to enhance the effectiveness of use of technology and tool of mobile broadband base station security testing platform. Eventually we hope to drive the information communication security test to maximize the value and marginal benefits of the platform.

(3) Opening of platform and field: the testing platform and various devices of this project will be subject to modularized construction and restructuring in order to be extended to the 4G network security testing platform – telecommunication network open field. It can be provided as the test field for domestically produced equipment and the corresponding data security verification.

(4) Helping service providers or equipment vendors with the tests such that the mobile

broadband base station security testing specification drafted in this project can be more complete: it can be extended to the data security testing mechanism of 2.2 Construction of Information Communication Equipment of Communication Industry in 2019 Digital Convergence/IoT Cyber Threats Defense and Security Lab Project in order to carry out the trial operation by HeNB service provider. After trial operation, we can help NCC formulate the official HeNB security testing technology specification.

2. Mid-to-long term suggestion:

(1) Continuous focus on and active participation in the discussion of security issue of International Organization for Standardization: in order to ensure that domestic data security protection measures can be in line with the international standards, it is suggested to continuously focus on the progress of promotion of GSMA NESAS or to encourage domestic companies or corporate to join GSMA in order to obtain the latest information of International Organization for Standardization with respect to data security attack.

(2) Sharing mechanism of domestic SS7 data security incidents: the SS7 data security incident sharing platform between domestic service providers and government should be established such that domestic competent authority and telecommunication operators can have better control over domestic SS7 data security incidents in order to carry out advance protective measures.

(3) The competent authority should work with the industry to establish voluntary testing mechanism: it is suggested that the competent authority can provide this Mobile Broadband Base Station Security Testing Specification to encourage service providers to adopt self-discipline management.

(4) The reporting and periodic active sampling mechanism can be included in the mobile broadband base station security testing specification: the testing platform of this project can be used to test the equipment of concern reported by mobile users, or for sampling tests not targeting specific service provider nor specific type of equipment.

第一章、緒論

第一節 研究緣起

伴隨著網際網路全球普及化與無線通訊科技蓬勃發展，無線通訊因應科技革新而結合多媒體創造出多元化應用服務，諸如網頁瀏覽服務、互動影音服務及語音通訊服務等，用以滿足人類於行動裝置上對於數據、運算與多媒體服務的不同需求。有鑑於解決行動裝置應用需求增加及多媒體服務應用多樣性，LTE（Long Term Evolution，長期演進）已被第三代合作夥伴計畫（3rd Generation Partnership Project，簡稱 3GPP）組織指定為新一代無線數據通訊技術標準。

LTE 時代的來臨，已為各界帶來不同層次的衝擊。就產業界而言，創新無線通訊應用技術的湧現，促使我國通訊傳播產業須調整原有的服務系統架構、提升行動寬頻網路的速度與提升通訊服務的穩定度。業者必須透過多方面的改造策略，以確保提供消費者兼具穩定及品質的行動寬頻服務，並且在符合行動寬頻業務法規要求下，結合自身通訊傳播產業實力，掌握 LTE 技術所帶來的產業分工商機。

就政府而言，在面對各項資通訊技術的不斷創新演進時，更是以穩健的腳步推展各項策略，從電信自由化政策到數位匯流的推展與行動寬頻業務頻譜的釋出，皆是不可或缺的重要推手。

國家通訊傳播委員會（以下簡稱 NCC）於民國 102 年 5 月公布「行動寬頻業務管理規則」，並於同年 10 月 30 日完成行動寬頻業務第一次頻譜釋出作業，由中華電信、遠傳電信、台灣大哥大、亞太電信、國基電子和台灣之星六家電信業者得標，並自 103 年 5 月起陸續開台營運，我國從此正式邁入行動寬頻時代。

國內行動寬頻業務於民國 103 年 5 月正式商用化開始至 105 年 5 月，行動寬頻業務用戶數已超越第三代行動通信業務用戶；106 年 1 月止行動寬頻業務用戶數已超越 1,800 萬戶。行動寬頻通訊技術(4G LTE)已成為目前行動寬頻網路通訊之主流技術，加上數位匯流與物聯網之趨勢興起，行動寬頻網路將躍升為經濟資訊流通及交易的重要通道，行動數據流量預期將大幅成長。當網路與無線技術結合時，使用者不必被侷限在固定空間就能上網，帶來之方便性也更勝以往。

然而，當眾人沉醉於行動寬頻網路的迷人之處時，卻很容易忽略潛藏的安全危機。有線網路的有形傳輸線路較易防範外來的破壞，即使如此，有線網路仍遭受許多安全威脅，更遑論無線網路以空氣為介質傳輸訊號，有心人士將不著痕跡蒐集空中傳遞的封包資料，造成行動寬頻網路在安全上有更多不可忽視的危機。同時，基於行動寬頻網路設計架構，基站系統與核心網路之間若無完善安全控管與保護，未來可能成為各種不法攻擊的途徑，造成通訊上的安全疑慮，這種情況突顯了行動寬頻基站系統資訊安全管理的重要性。

有鑑於此，行政院科技會報辦公室於 103 年 5 月公告「加速行動寬頻服務及產業發展方案」之三年計畫，用以建構優良的行動寬頻發展環境，讓所有民眾早日享受品質優質與價格合理之高速行動寬頻服務外，同時著重於行動寬頻資訊安全之維護。因此，該方案訂定之「消費者權益保障」推動主軸中，擬定「資安檢測及認證」為推動策略之一，希望達成加強行動寬頻網路安全，建立電信設備（包括基站）的資安檢測機制，並透過輔導軟硬體產品業者技術、增加資訊安全監測、警示、與緊急處理能力，藉此完善行動寬頻系統與設施，以積極強化對民眾的通訊隱私與個人資料保護，減少行動寬頻網路被惡意攻擊、侵害之可能，確保消費者能安全、安心的使用行動寬頻應用服務之目標。

本團隊於 105 年已完成「建置基站資安檢測環境計畫第 1 期」研究，研究團隊以文獻研究、國際經驗蒐集方式，及實地考察行動寬頻網路資安管理先進之國家，就行動寬頻網路元件既有資安防護措施進行分析，完成行動寬頻網路風險評估，研析行動寬頻網路之檢測工具及方法，規劃出行動寬頻資安檢測平臺，並透過國內環境分析及國際標準研究，深度訪談國內電信業者，產出行動寬頻基站管理方針芻議供主管機關及電信業者參考。

本團隊將延續「建置基站資安檢測環境計畫第 1 期」研究成果，就「建置基站資安檢測環境計畫第 2 期」委託專業服務工作項目，整合 NCC 採購之 LTE 基站及資安檢測工具，透過租賃之 LTE 核心網路，建置一行動寬頻基站資安檢測示範性平臺，研擬基站資安檢測項目，並執行實測，就實測結果與國際文獻研析，提出適合國內環境之行動寬頻基站資安檢測規範草案，協助國內電信業者加強行動寬頻網路安全，以保障消費者權益。

第二節 研究背景

一、 行動寬頻網路風險分析

行動網路(2G)原本以簡訊與通話服務為主要功能。到了 3G 時代，上網服務需求逐漸增加，並隨各種行動裝置應用之普及化，消費者對更高之上網速率及效能需求增加，因此促使了行動寬頻網路(4G LTE)之發展。

行動寬頻網路(4G LTE)改變以往 2G/3G 複雜之網路架構，簡化為行動終端裝置透過基站(eNodeB)即可直接連結至核心網路之扁平化架構，其核心網路係採核心分組網演進(Evolved Packet Core，簡稱 EPC)，以封包交換(Packet Switch)取代了傳統電路交換(Circuit Switch)，將行動通訊全面 IP 化，優化上網效率。

但在全面 IP 化的網路架構下，對於行動寬頻網路(4G LTE)之安全也產生了疑慮，行動寬頻網路(4G LTE)架構上也為保障用戶安全，設計了許多安全機制，包含雙向認證、識別機密性(即使用許多暫時性的識別碼代表使用者)、特定的通訊協定、加密及完整性驗證等。但行動寬頻網路(4G LTE)內部與外接網路都是 IP 封包的情況下，致使傳統網路攻擊者可能直接套用現有的網路攻擊來癱瘓行動寬頻網路或是攻擊特定受害者。再加上因其利用基站(eNodeB)取代了部分無線電網路控制台(Radio Network Controller，簡稱 RNC)功能，讓基站能直接控制無線電資源，扮演聯繫用戶裝置與核心網路間的角色，因此相較於佈署在電信業者內部嚴格管控的核心網路，對於佈署在外部的基站可能遭受的攻擊機率較高。

(一) 行動寬頻網路威脅

建置基站檢測環境計畫(第 1 期)報告中，已根據 3GPP TS 33.805、3GPP TR33.820、McAfee 技術報告及 NIST 報告，歸納整理行動寬頻網路(4G LTE)整體風險層面(如圖 1-1)，共分類為以下六大項威脅①外來網路訊務量威脅;②無線訊號威脅;③行動裝置間的威脅;④系統、軟體漏洞威脅;⑤核心網路內部通訊介面威脅;⑥干擾網路服務。

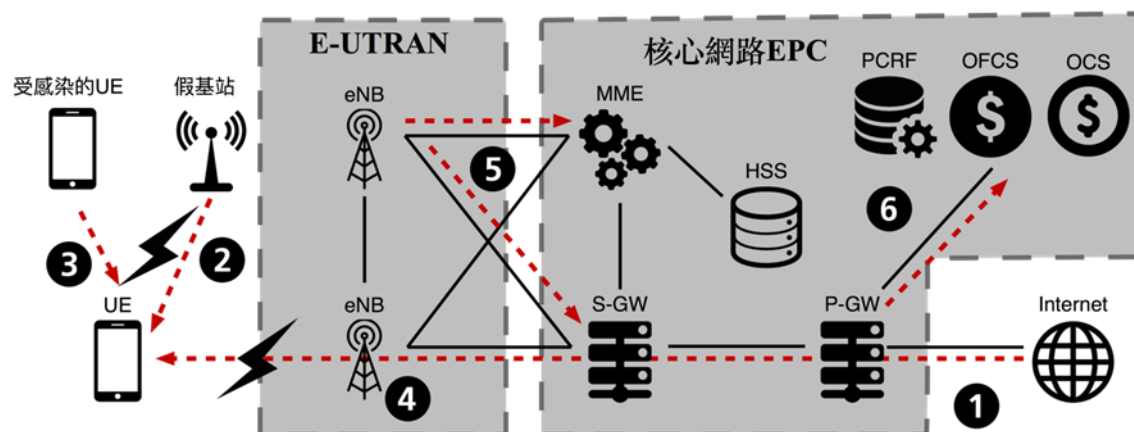


圖 1-1 行動寬頻網路(4G LTE)整體風險

資料來源：建置基站資安檢測環境計畫(第 1 期)

❶ 外來網路訊務量威脅：主要來自於網際網路的攻擊威脅，可分為整體網路架構之攻擊及使用者行動裝置之攻擊。

❷ 無線訊號威脅：無線網路是一個有範圍性的網路，透過無線訊號的發送與偽造，來達到攻擊的效果。手機訊號是以無線的方式傳遞，在行動寬頻基站與手機之間的系統稱之為演進的通用無線網路(E-UTRAN)。由於是以無線的方式傳遞，所以在訊號範圍內的所有接收者，都可以聆聽到相同的訊息。同樣的，在相同訊號範圍內的裝置，可以發送干擾訊號來造成通訊的中斷。無線訊號威脅(即空中介面攻擊)可略分為主動及被動兩種。被動無線訊號攻擊是指不介入通訊的攻擊手法，通常為竊聽攻擊；主動無線攻擊則會發送偽造的訊息，來破壞原有的資料。

❸ 行動裝置間的威脅：行動裝置間的威脅係利用行動寬頻內 IP 封包來進行行動裝置間的網路攻擊。在 3G 網路每次手機連接到網際網路時才會分配一個 IP 位置，但在行動寬頻網路中，手機一旦連接到電信業者的網路之後，將會配置一個 IP 位址，該位址一直到斷線以後才會被回收。使得行動裝置間可能藉由著 IP 網路的攻擊方式，在服務網路內部進行攻擊，或是探索內部的網路拓撲。行動裝置間的攻擊可能是起因於受感染的行動裝置，使用者可能受到誘騙或是系統漏洞，安裝了惡意程式，該惡意程式為了增加攻擊的能力，往往會具備有擴散及感染的能力。

❹ 系統、軟體漏洞威脅：系統漏洞或是軟體漏洞是指藉由精心設計的輸入，來達成控制系統或是軟體運行的目的。最常見的方式是緩衝區溢位，藉由著修改返回位址

來控制運行中的程序，雖然行動寬頻網路不會處理外來 IP 網路的封包，不會將資料讀入到重要的系統軟體之中，但網路設備系統軟體也可能因軟體漏洞的存在，而造成網路設備被植入惡意程式並將敏感性資料傳至特定主機之安全威脅，核心網路內的系統仍有可能遭受到漏洞攻擊進而影響整體 LTE 網路的安全性。

⑤ 核心網路內部通訊介面威脅：在電信業者實際建置的環境中，核心網路的元件是實體隔離的，不會讓一般人靠近，但核心網路仍然有可能遭受到攻擊，像是遭受到已感染的系統元件攻擊，或是內部攻擊(Insider)，造成其他受信任的元件暴露在被攻擊的威脅底下。

⑥ 干擾網路服務：在行動寬頻網路服務中，語音服務需要即時的品質管控。由於行動寬頻網路為全 IP 的網路架構，導致語音訊務量與資料訊務量可能共享同一個網路頻寬。在電信網路中，語音服務是最基本的服務，如果有攻擊能夠影響語音通訊，將可能影響語音可用性及計費方式，對使用者來說是很大的威脅。

(二) 行動寬頻網路安全威脅實例

近年網際網路重大資安事件已有許多是發生在行動寬頻網路中，或利用行動寬頻網路的漏洞進行攻擊行為的案例。如 VoLTE 之網路安全漏洞、偽基站之安全威脅及家用基站(HeNB)之資安威脅案例等。

1. VoLTE 網路安全漏洞

2015 年 10 月美國電腦安全應急回應組(CERT)發布了一個消息：美國兩大電信業者 Verizon 和 AT&T 其 Android 手機用戶在使用 VoLTE 服務時存在嚴重的網路安全漏洞，會導致使用者遭受點對點的攻擊，具體威脅包含：①通話內容遭到竊聽；②手機被植入的惡意軟體，經過手機的 SIP 接口撥打電話；③網路訪問遭到控制，被用作 DDoS 攻擊；④以上三點的費用均由用戶買單¹。

2. 偽基站之安全威脅

¹ Phil Goldstein, “Android phones on Verizon, AT&T face LTE security vulnerability, researchers say” in FierceWireless, 2015/10/19.

2015 年 BlackHat 歐洲研究人員們展示最新發現，4G 行動網路中的安全性漏洞可能導致使用者隱私洩露以及電話服務異常。這些安全性漏洞有可能允許攻擊者確定目標行動用戶的物理位置，並阻止行動用戶利用自己的行動設備撥打或者接聽語音通話，相關的展示主要是以設置偽基站方式執行²。

在中國自 2013 年開始，偽基站的大量發送垃圾簡訊和詐騙簡訊的攻擊方式泛濫。攻擊者將偽基站放入車中，在人群密集的地區搜索周圍手機訊息，冒充 95588、95533、95555 等銀行客服群發送詐騙簡訊，誘騙受害者以獲取帳戶積分獎金為由，使受害者訪問虛設網路銀行，輸入信用卡資訊，盜刷其銀行帳戶資金³。

央視甚至於 2016 年 5 月製作專題節目「偽基站：手機上的“黑陷阱”」，報導偽基站已是目前中國大陸詐騙集團普遍使用的詐騙工具。

詐騙集團即是利用行動寬頻網路「手機會連接到所搜尋到訊號最強的基站」特性，利用偽基站進行阻斷式攻擊，發送詐騙簡訊及網址，騙取用戶轉帳，且嫌犯表示網路上即可購置偽基站設備⁴。

2017 年 3 月提供網路安全設備產品及解決方案的公司 Check Point Software 報導指出，中國大陸發生了第一起利用偽基站設備，假冒電信業者(如中國移動及中國聯通)名義發送簡訊，傳播惡意程式"Swearing Trojan"的案例，該惡意程式為 Android 之惡意木馬程式。

Swearing 木馬程式可以從受感染的設備收集用戶個人資訊及相關認證資訊，甚至攔截簡訊(SMS)訊息，截取銀行機構使用的雙向認證或其它一次性代碼等。該 Android 木馬程式開始於中國行動寬頻網路，目前已開始蔓延全球，根據統計，全球至少有 1,000 萬用戶被感染，中國和印度的 Android 手機被感染的最多。Check Point 認為，透過偽基站傳送 SMS 訊息是很容易欺騙用戶的一種方式，利用 Swearing 惡意程式的攻擊活動若是透過偽基站方式誘騙用戶，將可能進一步推動此惡意程式的蔓延⁵。

在 3GPP 標準規範中，為了防止用戶端(UE)透過選擇其他遠方的基站，所產生上

² BlackHat EU, "LTE and IMSI catcher myths", 2015.

³ 中國新聞網, "电信诈骗高发伪基站泛滥难监管, 建议多部门打组合拳", 2016/1/8.

⁴ 新浪財經, "央视揭密伪基站冒充银行诈骗案件: 三条短信骗走五千块", 2016/5/13.

⁵ The Hacker News, "Hackers Using Fake Cellphone Towers to Spread Android Banking Trojan", 2017/3/22.

行鏈路訊號干擾影響，用戶端(UE)僅需搜索訊號最強的基站。假設一個偽基站在其功率發射，被顯示為在用戶端(UE)選擇頻率通道的最強基站，則用戶端(UE)將嘗試駐留到這樣的偽基站與不能夠選擇在該通道任何其他 LTE 基站，這可能會拒絕 LTE 網路存取導致服務中斷。其通訊信令如下圖所示。

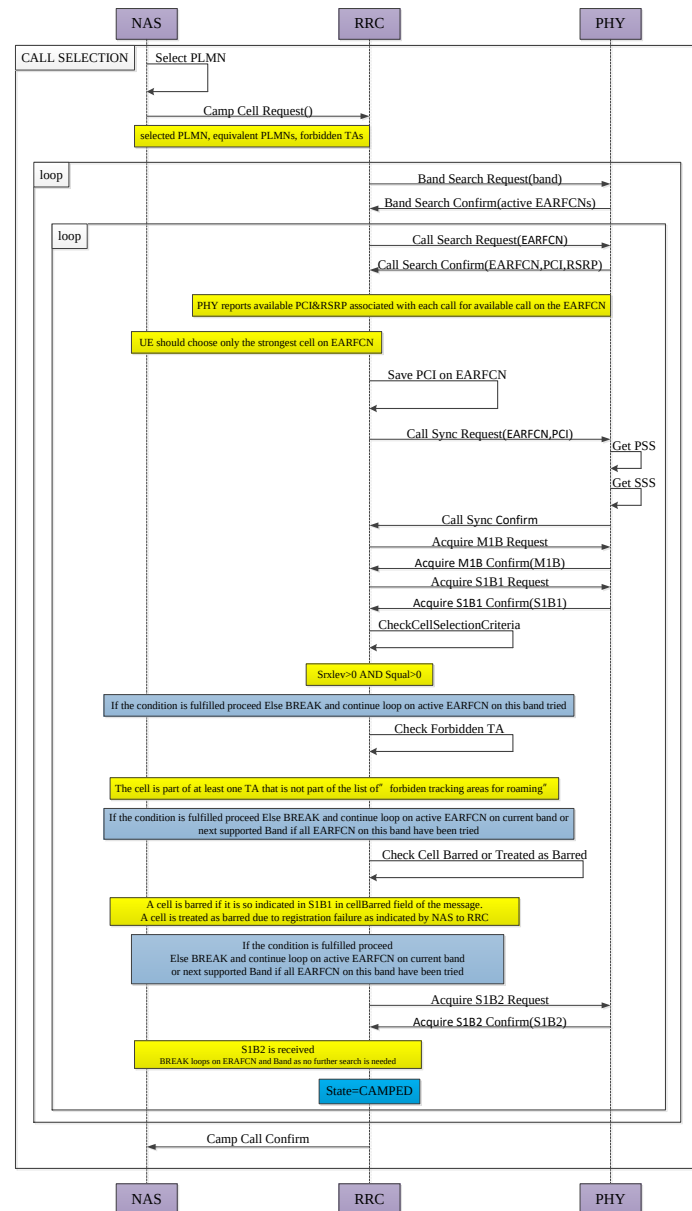


圖 1- 2 UE 初始基站選擇流程

資料來源：本團隊整理

上圖表示 UE 試圖找到一個基站並駐留，公眾行動電話網路(Public Land Mobile

Network，簡稱 PLMN)應首先由 NAS 選中。在 NAS 層然後請求 RRC 層來選擇所選擇的 PLMN。在基站選擇處理中，UE 循序掃描它所支援的頻段。該頻段掃描使 UE 能夠找到關於支援 LTE 頻段的來源 RF 訊號，如果接收的訊號強度指示(Received Signal Strength Indication，簡稱 RSSI)超過某個門檻值 RF 訊號被認為是可被接通，一旦支援頻段被選擇時，再對物理層(Physical Layer，簡稱 PHY 層)搜索，選擇訊號最強的基站，並且獲取時序與頻率(主要同步 PSS 和輔助同步 SSS 信號)的幫助。

2015 年 IEEE 通訊與網路標準研討會(Conference on Standards for Communications and Networking，簡稱 CSCN)中，發表了一篇利用偽基站欺騙用戶終端設備(UE)，妨礙用戶終端設備連接到真實基站的案例⁶，其實驗架設如下圖 1-3 所示。使用 LTE 接收的 USB 網卡模擬 UE 端，利用 Ettus USRP 的軟體無線電裝置，搭配開源碼的 Open LTE 模擬偽基站，以及 R&S CMW500 的設備模擬真實的基站(可讓 UE 完成 PLMN 登錄)。上述三者的空中介面，都在一個無線電遮罩金屬盒內，確保與外在因素隔離下進行實驗。

⁶ 2015 IEEE CSCN Conference：Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing.

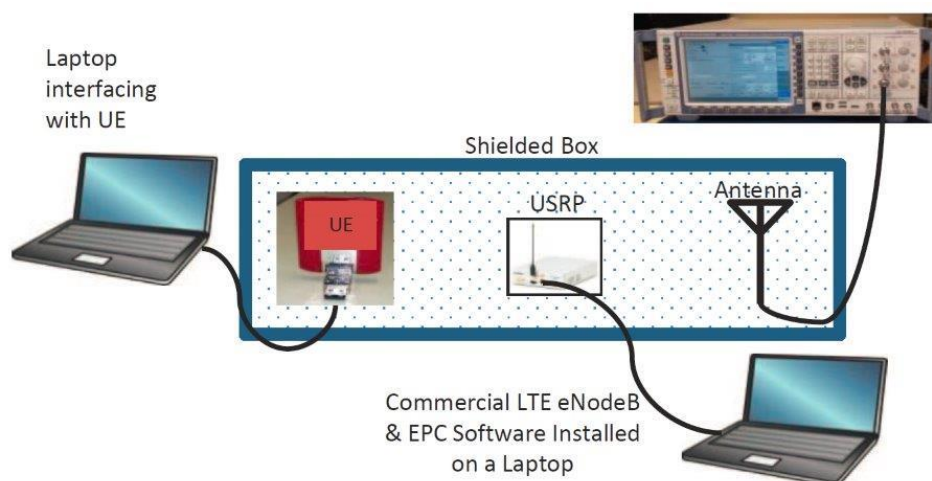


圖 1-3 偽基站欺騙 UE 實驗架設

資料來源：2015 IEEE CSCN

該實驗證實若一個偽基站在 UE 端顯示為訊號最強的基站，則 UE 將嘗試駐留到這個偽基站，然而在金鑰認證失敗後，偽基站沒有提供其它基站存在的列表資訊，則此時 UE 將導致行動寬頻網路(4G LTE)的阻斷服務。這種攻擊即便偽基站關閉訊號後，UE 被阻斷服務的狀態仍會持續，一直到重新開機或重新設定。

3. 家用基站(HeNB)之資安威脅

在行動寬頻網路技術的快速演進與智慧行動裝置的普及，帶動多樣化的行動應用服務快速發展，行動寬頻網路流量呈現指數型的成長。在此趨勢下，為解決連線擁塞與提升連線品質，國內外已有許多電信業者在行動寬頻網路下利用家用基站(Home eNodeB，簡稱 HeNB)作資料分流及增加室內覆蓋率，除可降低架設成本，也成為電信業者擴展頻寬與連線分流的最佳解決方案。

家用基站為家用的微型基站(Femto Cell)，具備低功率、低成本，且覆蓋距離不超過 10 公尺之特性，該設計主要為家中或小型企業所使用，以增加覆蓋率。雖然家用基站(HeNB)具有購買及架設成本低廉之優勢，但其廠牌眾多，使用的材質與元件等級較低，不同於大型基站，而且是座落在一般用戶端，使得家用基站(HeNB)比起大型基站更易遭受入侵威脅。另外，電信業者可選擇的製造商設備多，可要求製造商提供客製化管理介面(Application Programming Interface，簡稱 API)，而這些遠端管控之介面

API 將可能成為入侵管道。再加上家用基站(HeNB)可採用非封閉性之後置迴路(Backhaul)，被入侵的風險又提高許多。

2015 年阿里移動安全團隊與中國泰爾實驗室無線技術部對中國電信業者某型號之微型基站(Femto Cell)進行了安全分析，發現許多重大漏洞，可導致用戶的簡訊、通話、數據流量被竊聽。攻擊者可以將微型基站(Femto Cell)設備改造成偽基站簡訊群發器和流量偵測器，影響公眾的通訊安全。

二、 行動寬頻技術演進與資安風險

(一) 第五代行動通信(5G)的發展

雖國內目前行動寬頻網路以 4G LTE 技術服務為主，全球 4G 建設還在進行中，但包括電信業者、智慧型手機晶片製造商以及網路設備公司都已在研發 5G 網路科技，為 5G 技術發展作準備。2006 年全球領先的行動網路業者共同發起成立了新世代行動網路聯盟(Next Generation Mobile Networks Alliance，簡稱 NGMN)，其宗旨為確保新一代行動網路基礎設施、服務平臺和設備效能，能夠符合業者的要求，及滿足一般使用者的需求和期望。

2014 年 NGMN 董事會成員(含括全球超過 20 家的行動業者)決議 NGMN 開始專注於定義 5G 的需求及規格，為國際具規模之新世代通訊技術研究與推動組織。其主旨為研究、評估及推行可滿足 2020 年及其後商用通訊網路需求之新興技術。NGMN 由全球超過 100 位專家組成的團隊討論及貢獻相關建議，彙整行動業者及消費者的需求後於 2015 年 2 月完成了 5G 白皮書，其中包含 5G 須達到的規格：以每秒數十兆 bit(Mbps)的速率數據傳輸、覆蓋率比 4G 要來的高、延遲比 LTE 低等。其內容也訂定了 5G 技術架構設計原則。⁷

目前為止，國際上對於 5G 的標準始終沒有定義出一個完整的規範，因此國際電信聯盟(ITU)於 2015 年公布了 5G 技術標準化時間表。根據會議提出的 IMT-2020 計畫，5G 標準制定將於 2020 年完成，5G 系統也正式命名為 IMT-2020⁸。IMT-2020 的

⁷ NGMN, “NGMN 5G WHITE PAPER V1.0”, 2015/2/17.

⁸ Futuristic mobile technologies foresee, ITU towards “IMT for 2020 and beyond”.

推進組(PG)也於 2015 年 2 月 11 日發布了白皮書《Whitepaper on 5G Concept》，為國際上少數幾份針對 5G 標準所進行定義之白皮書，具有相當的參考價值。

雖 NGMN 及 ITU 皆預估於 2020 年 5G 將開始商用化，現階段 5G 規格與技術發展也尚未成熟，但幾個行動寬頻發展較為先進之國家如日本、韓國、美國、歐洲等已開始研發並建構適合該國的 5G 架構。南韓電信業者韓國電信(Korea Telecom，簡稱 KT)，於 2016 組織 KT PyeongChang 5G Special Interest Group(簡稱 KT 5G-SIG⁹)，此組織成員主要為電信設備供應商所組成，在 2016 年間已開始制訂 5G 相關通用規範，預計在 2019 年達到 5G 商用化，並規劃在 2018 年平昌冬季奧運上使用 5G 技術，提供多視角觀賞賽事，實現 5G 商業化的發展。日本最大電信業者 NTT DOCOMO 也為了發展 5G，採取了一些新的措施，如：採用頻率更高的頻帶以利擴大頻寬、局部的小型蜂窩採用高頻帶等等，希望能容納高膨脹及爆炸式的流量¹⁰。

NGMN 的 5G 白皮書中特別針對 5G 的安全需求進行說明。未來 5G 將支應更廣泛的應用和環境，包含從人的通信到機器的通信，它須處理大量的敏感數據，在 5G 網路中如何防止未經授權的訪問、使用、中斷、修改、檢查、攻擊等，為一非常重要的議題。因此，5G 的網路架構應提供超越節點到節點和端到端安全性的更多選項，以保護用戶的數據，創造新的商業機會並防止或減輕任何可能的網路安全攻擊。

另外由歐盟發起的 5G-PPP (5G Infrastructure Public Private Partnership)，會員包含歐盟委員會、電信製造商，電信業者，服務提供業者、中小企業和研究人員所組成，該協會之宗旨為新世代通信基礎設施提供解決方案、技術、標準及架構，2016 年 11 月 3 日 5G-PPP 發表了《5G-PPP security enablers open specifications》¹¹，此研究報告書主要針對 5G 值得關切的安全方向進行討論。可見國際上在制定 5G 技術標準的同時，其安全性已是發展網路架構時需同時考量的重要議題。

(二) 新興的網路架構-SDN¹²

軟體定義網路(Software-defined networking，簡稱 SDN)與網路功能虛擬化(Network

⁹ 韓國電信官網,KT 5G-SIG.

¹⁰ 商周,“台灣人還在癡癡等 4G...日本 5G 都快上路了!”, 2013/10/14.

¹¹ 5G-ENSURE, “5G-ENSURE publishes its 5GPPP security enabler open specifications V1”.

¹² 張景皓,“新一代網路架構 SDN 顛覆傳統網路的控制模式”, 2012/11/19.

Function Virtualization，簡稱 NFV)為 5G 電信網路服務架構的主要關鍵技術，主要目的為因應未來多變的使用情境。隨著資訊世代的進步，大量行動裝置的產生，雲端運算成為現代科技的一大要點，但是大量的數據流量對於傳統網路的可延展性、維護安全的能力、以及動態性都是一大挑戰，因此為了因應大量數據流量的需求與趨勢，SDN 為近幾年快速興起的網路架構及討論議題，甚至 5G 的網路架構中，也結合了 SDN 之概念。

SDN 架構早在 2009 年，由美國史丹佛大學 Nick McKeown 教授研究於 IEEE INFOCOM 的研討會中首度發表。2012 年 Nick McKeown 教授與 Scott Shenker 教授等人創辦 SDN 先驅公司 Nicira 發展網路虛擬化技術，被美國 AT&T、日本 NTT 與 Google 等大廠所採用，Google 甚至充分運用 SDN 架構佈建其全球之 IDC 網路，使頻寬使用率大為提升，因此近幾年 SDN 架構一直為內容服務業者及電信業者納入研究並考慮的網路架構。

在傳統的網路架構中，封包的傳遞工作，包括判斷網路訊息傳向目的地的路徑，都是以網路裝置的管理單位各自為政採用自我學習的方式決定網路訊息的流向路徑，但這樣即產生管理者無法確切掌握封包流向，導致不利於管理者對於網路的管理。管理者若要更改對於各種網路狀況的事件回應，必須一一對不同的網路設備更改設定，非常耗時耗力。

因此研究學者提出如果將控制層從資料層隔離出來，使網路設備只剩網路封包傳遞的工作，再以一個外部控制者作為首腦去統帥多數網路設備的控制層，統一只要從外部控制者發布命令，旗下的所有網路設備即可成功更改設定，這就是所謂 SDN 的核心概念。

SDN 共分為三層架構(如下圖 1-4)，分別為：應用層(Application Layer)、控制層(Control Layer)及基礎層(Infrastructure Layer)，其中 SDN 的控制核心在於控制層(Control Layer)。

SDN 擁有一個不同於傳統網路架構的最大特點，即「可程式化」管理，使用者可以設計管理網路的程式，控制 Control Layer，大幅度簡化網路控制的複雜度，這些程式將放置於 Application Layer，再由 API 連接傳遞訊息給 Control Layer。第二層 Control Layer 即為網路設備的中央控制處，使用者只要在 Control Layer 中的 SDN

Controller 下達命令，SDN Controller 就會傳遞命令給於 Infrastructure Layer 的各個網路設備，在途中負責傳送訊息的工作的主要協定為 Openflow。

SDN 的集中控制提升網路管理的效率及網路效能，但同時也帶來了新的風險，除了在於下達命令需要更加嚴謹之外，Controller 將成為新的攻擊對象，如果攻擊者成功攻佔 Controller，即會使其之下的所有網路設備陷入危險之中，因此對於 Controller 的安全將會成為 SDN 資安研究的重要課題。

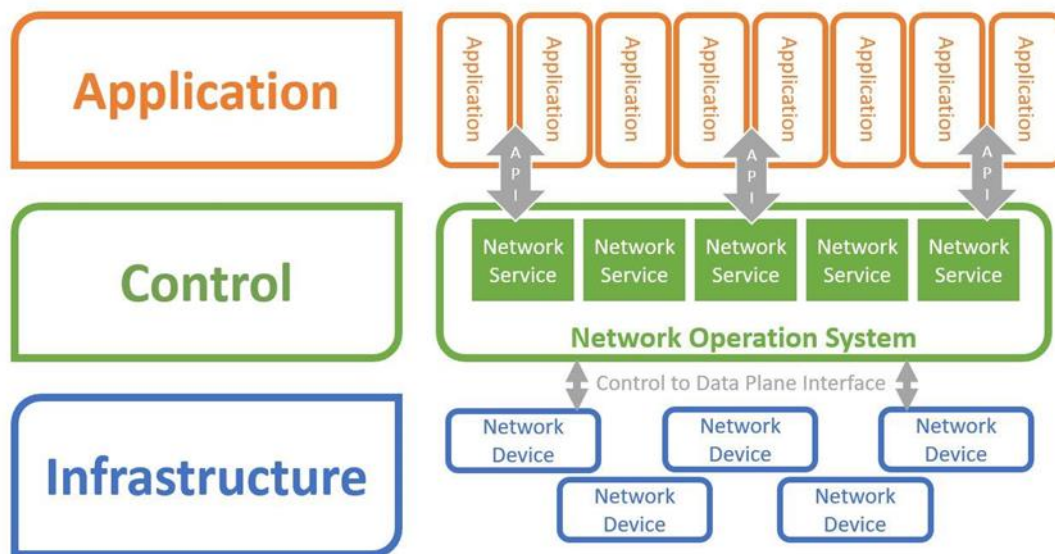


圖 1- 4 SDN 架構圖

資料來源：整理自 ONF White Paper¹³

(三) 物聯網(IoT)的發展¹⁴

物聯網(Internet of Thing，簡稱 IoT)，是一種網路的承載體，最早是由 Kevin Ashton 在 1999 年為 P&G 引入 RFID 時提出，以此用來實現物品在網路之間的互聯，整個物聯網的架構總共分三層，由上到下分別為應用層、網路層及感知層(如圖 1-5)，對於無線網路中的物聯網在每個人的周圍通常有一千到五千個物體，所以整個物聯網可能會包含五百兆至一千兆個物體，每個物體都可以利用上面連網的工具來找到他們正確的

¹³ ONF White Paper, "Software-Defined Networking: The New Norm for Networks", 2012/4/13.

¹⁴ Zanella Andrea; Bui Nicola; Castellani Angelo; Vangelista Lorenzo & Zorzi Michele, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, VOL. 1, NO. 1, 2014/2.

位置，進而達到對於物品的管理及控制，或是防止物品被竊盜。

物聯網中將產生巨量的資料，利用這些巨量資料來達成物聯網的應用，例如：找尋不見的車鑰匙、對道路車流量進行分析重新設計道路以減少路上車禍、流行病的控制等。物聯網將物與物之間的資訊結合在一起，可以讓現實的資訊不再那麼分散，也將傳統手寫的資訊數位化，應用範圍十分廣泛，主要可以應用在醫療、運輸、智慧家庭、智慧辦公等等，未來的市場及應用發展還非常廣闊。



圖 1- 5 IoT 架構圖

資料來源： 整理自北美智權報¹⁵

2016 年 9 月發生一個鎖定物聯網裝置的殭屍病毒 Mirai，利用數位錄影機及網路路由器進行了分散式阻斷服務攻擊(Distributed Denial-of-Service Attacks，簡稱 DDoS)，這隻程式讓物聯網的資安問題浮上檯面，因為物聯網的物體太多，如果每個物體都被控制了，對生活將造成非常大的衝擊，所以物聯網的資訊安全造成的影響將不容小覷¹⁶。

美國電信業者 Verizon 在 2017 年在即將發表的「資料安全報告」中揭露，美國當地某間校園網路攻擊事件，其攻擊手法是透過校園中隨處可見的照明系統以及自動販賣機，入侵並植入惡意軟體，進而被殭屍網路控制。攻擊者入侵高達 5,000 多個裝置，

¹⁵ 謝錦星，“IoT 晶片設計的商機與挑戰”，北美智權報第 119 期。

¹⁶ 陳曉莉，“Dyn 遭大規模 DDoS 攻擊，Mirai 殭屍網路脫不了關係”，2016/10/25。

植入惡意程式進行遠程操控，統一對校園網路進行龐大的 DDoS 攻擊，造成其網路速度大幅地降低，但幸運地，攻擊手法並非難以突破，並未造成無法挽回的傷害。雖然此次事件平安落幕，但由近年許多真實攻擊案例看來，物聯網可帶來生活極大的便利，同時也潛藏了極大的風險¹⁷。

三、 國際行動寬頻資安檢測標準現況

早在行動網路資訊安全普及之前，國際間已有許多組織針對電腦網路提出各種不同的網路安全測試機制、流程與細節，例如美國 NIST 的網路安全檢測指導原則 (Guideline on Network Security Testing, 簡稱 GNST)，即 NIST SP 800-42¹⁸；以及作為供應商生產電腦相關設備一致性標準的共通準則(Common Criteria, 簡稱 CC)。而行動寬頻之網路架構及安全規範，則是依國際標準組織 3GPP 訂定之標準規範為主，相關內容整理如下：

(一) GNST

NIST 的 GNST 主要目的為提供網路安全測試指引，文件中定義了如何在有限資源內定義網路安全測試需求的優先順序，提供網路安全檢測標準方法及指引，其設計了一個彈性且不同等級的網路安全測試標準，讓企業可依其預算、組織任務及安全目標而選擇不同的檢測標準及方法。

GNST 文件定義了一般網路系統之安全測試，從系統開發之生命周期(如圖 1-6)，訂定不同階段之安全檢測及評估標準供企業選擇。該文件定義的一般網路系統產品包含如下：

- 防火牆
- 路由器及交換器
- 網路周邊安全系統，如入侵偵測系統
- 網路伺服器、郵件伺服器及其他應用伺服器等
- 其他伺服器如 DNS(Domain Name Service)、Directory Servers 或檔案伺服器 (CIFS/SMB, NFS, FTP, etc.)

¹⁷ iThome, “美國大學遭到 DDoS 攻擊，「凶手」竟然是校內的自動販賣機、路燈”，2017/2/14.

¹⁸ NIST, “Guideline on Network Security Testing.”, 2003/10.

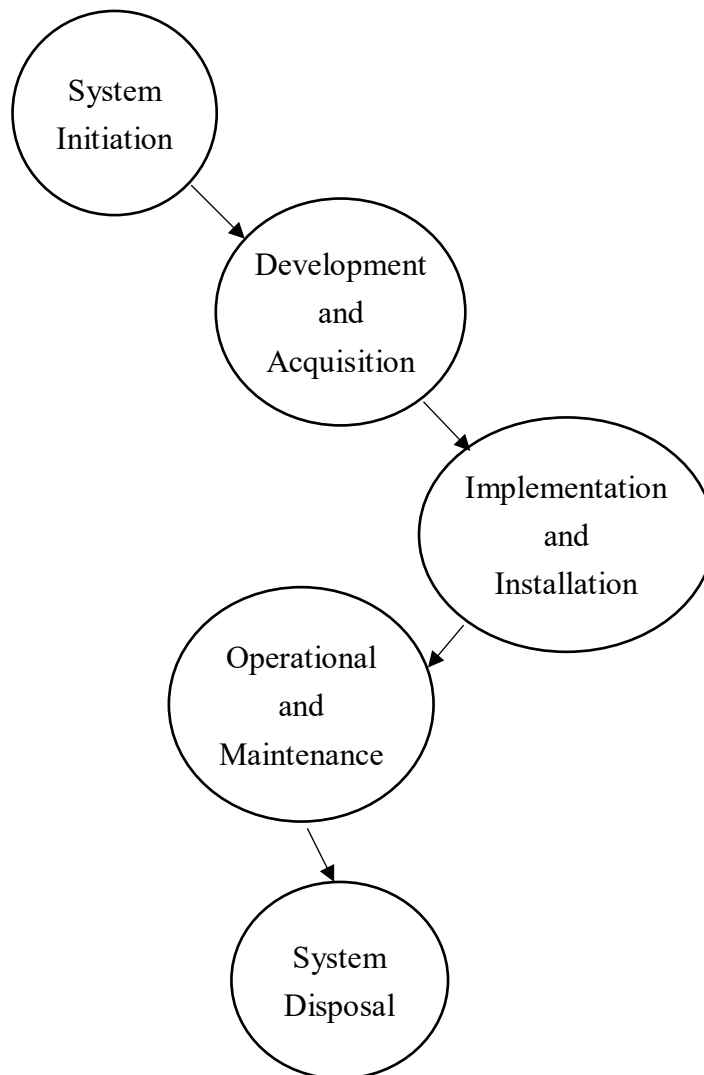


圖 1-6 系統開發生命週期

資料來源：NIST

(二) CC

共通準則(Common Criteria，簡稱 CC)，於 1999 年 8 月正式成為 ISO 國際標準 (ISO/IEC 15408)，為目前世界各國資通安全產品評估及驗證時所遵循之共同標準，截至目前為止的版本為 version 3.1 revision 4。

CC 的目標是建立一個國際通用的 IT 產品評估框架，量化資訊安全等級的評估工作，使評估結果更有意義；此外，透過共同準則進一步提升 IT 產品的安全度信心、降低取得驗證產品的難度、減少不同準則重複評估造成的負擔、改善與統一驗證流程以

增進總體效益。共通準則目前正逐步取代各區域性的安全評估準則，並且全球的許多國家已將共同準則視為 IT 產品最高層級的安全性認證，南韓政府並規定國家網路使用之資訊設備一定要經過 CC 認證才可採用。

CC 為資通訊產品之安全認證與驗證規範，提供測試實驗室針對資通產品進行安全性與安全等級之評估與測試驗證，其安全產品驗證適用範圍包括資通訊相關的軟體、硬體與韌體或是三者任一組合之安全功能與強度評估。資通訊產品之認證等級依據其高低不同而有評估檢測深度與廣度區分，程度係以評估保證等級(Evaluation Assurance Level，簡稱 EAL)為基準。

基於國際共通準則承認協議(Common Criteria Recognition Arrangement，簡稱 CCRA)，各國相互承認 EAL 1 至 4 安全等級的產品，而 EAL 5 等級以上(包含 EAL5)的產品，通常屬於各國國防與軍事安全認證的需求範圍，彼此標準規範並不互通。多數商用產品等級最高為 EAL4，亦可採增項方式加入 EAL5 以上的部分保證組件功能，即為 EAL4+。

為了確保資訊技術軟、硬體產品在安全性驗證上，有一定的公信力，目前國際間已有不少資通軟、硬體產品大廠以通過 CC 國際標準的認證做為產品發表目標，證明其產品有足夠的安全性。

CC 在資通訊產品的安全觀念與關係說明了安全與資產的保護有關，資產的擁有者依資產的價值，可能要求任何資訊的「可用性」、「傳播」與「修改」嚴格地控制以及資產的威脅受到因應對策的保護(如圖 1-7)。

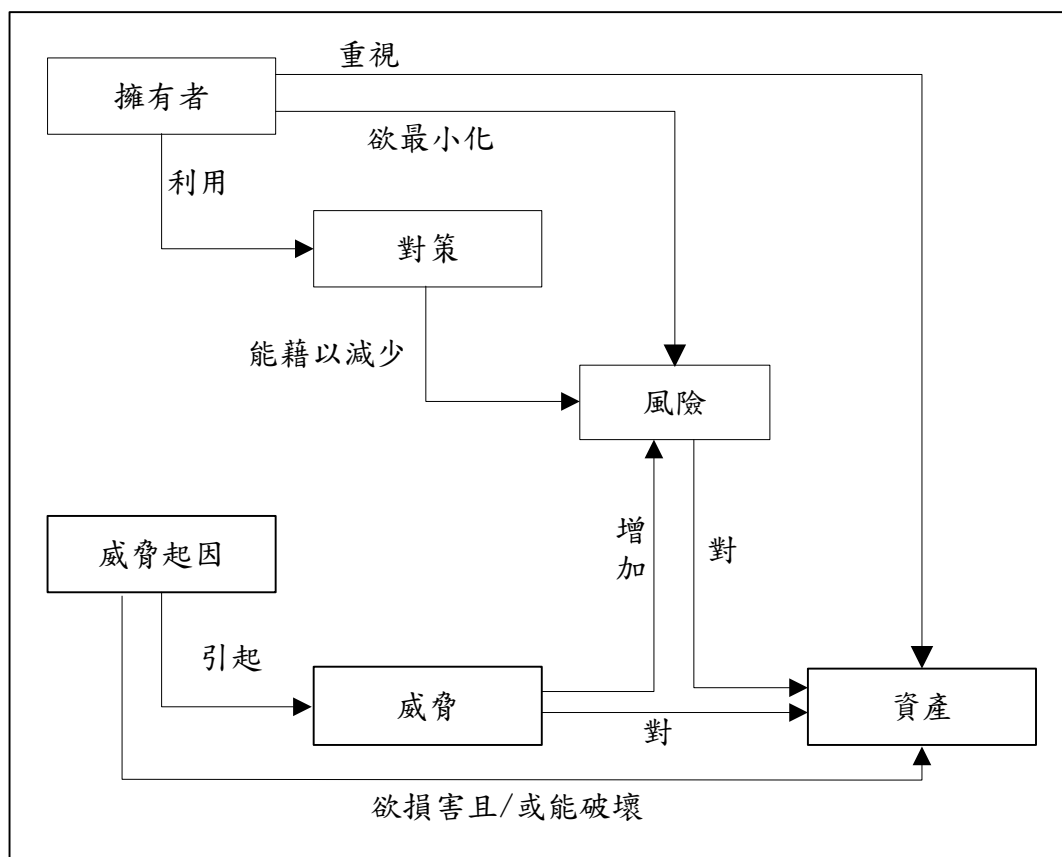


圖 1-7 安全觀念與關係

資料來源：國家通訊傳播委員會¹⁹

(三) 3GPP

上述國際間普遍使用之檢測標準係以網路系統及資通訊產品為主，而在行動寬頻網路標準部分，主要係遵循第三代合作夥伴計畫(3GPP)制定的全球通用標準，相關文件定義了行動寬頻網路(4G LTE)系統架構及資訊安全(33 系列)，包含行動寬頻網路(4G LTE)應具備之安全技術規範(Technical Specifications，簡稱 TS)與技術報告(Technical Reports，簡稱 TR)，其中詳列了威脅與元件群組的安全需求，可作為檢視行動寬頻網路(4G LTE)基本安全之主要依據。

¹⁹ 國家通訊傳播委員會，“共通準則：資訊技術安全評估共同準則第 1 部：導論與通用模型第 3.1 版”，2008/10。

在 3GPP TS33.401 中，制定了 LTE/SAE (SAE: System Architecture Evolution) 系統框架演進網路架構，包含整體網路架構的安全功能要求，內容中以五個介面(如圖 1-8)闡述行動寬頻網路應具備之安全機制²⁰，分別為：

- (I) 網路接取安全：為用戶提供安全接取服務，特別是防止無線接取連結攻擊。
- (II) 網路領域安全：節點能夠安全交換接取網路與服務網路間，以及接取網路內部的信令數據、用戶數據，防止有線網路攻擊。
- (III) 用戶領域安全：安全接取行動裝置。
- (IV) 應用領域安全：在用戶領域與業者領域安全地交換信息。
- (V) 安全服務的可視性和可配置性：通知用戶安全功能是否運行，是否依據安全功能使用與提供服務。

²⁰ 3GPP TS 33.401, “3GPP System Architecture Evolution (SAE); Security architecture (Release 13)”.

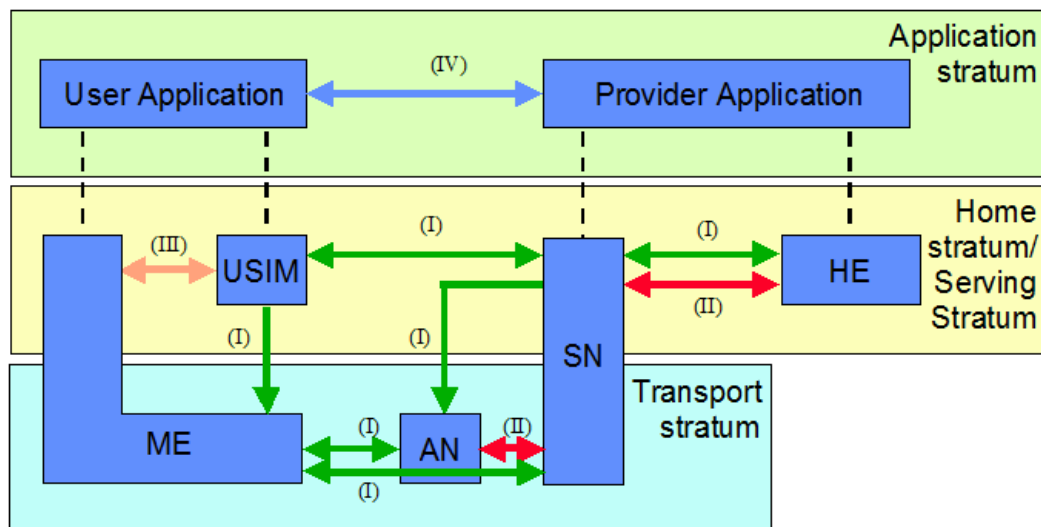


圖 1- 8 LTE/SAE 安全架構

資料來源：3GPP

有鑒於行動寬頻網路逐漸成為生活中重要且主要的關鍵基礎設施，3GPP 負責討論及制定行動網路架構及服務可用性及安全性的工作小組(SA WG3)，於 2015 年完成了網路設備資安確保與檢測框架(Security Assurance Methodology，簡稱 SECAM)，制定網路設備在上線前的資安檢測與評估機制(如圖 1-9)。

SECAM 已經完成研究階段，其研究成果為 3GPP 的 TR 33.805 報告²¹。目前 3GPP 開始發展正式的 SECAM 方法，已在 TR 33.916 技術報告中闡述相關內容²²。3GPP SECAM 定義了網路產品資安檢測的相關角色與流程及安全保證規範(Security Assurance Specifications，簡稱 SCASs)的制定方法²³。定義的認證安全範疇要求涵蓋：(1)供應商產品開發暨生命週期管理流程確認、(2)產品合規檢測、(3)基本弱點檢測、(4)進階弱點分析。

SECAM 與其他方法最大的差別在於設備安全認可的範圍涵蓋了設備開發商的產

²¹ 3GPP TR 33.805, “Study on security assurance methodology for 3GPP network products (Release 12)”.

²² 3GPP TR 33.916, “Security Assurance Methodology for 3GPP network products (Release 13)”.

²³ 3GPP TR 33.926, “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (Release 13)”.

品開發生命週期。也就是設備商在產品設計開發階段就要引入安全的概念。在此方法下，網路設備商的開發流程必須通過認證單位的認可，且須通過認證單位(目前為 GSMA)認證通過的檢測單位，所提供的設備檢測報告作為採購的決策依據。檢測單位可以是設備商本身或第三方的檢測單位。

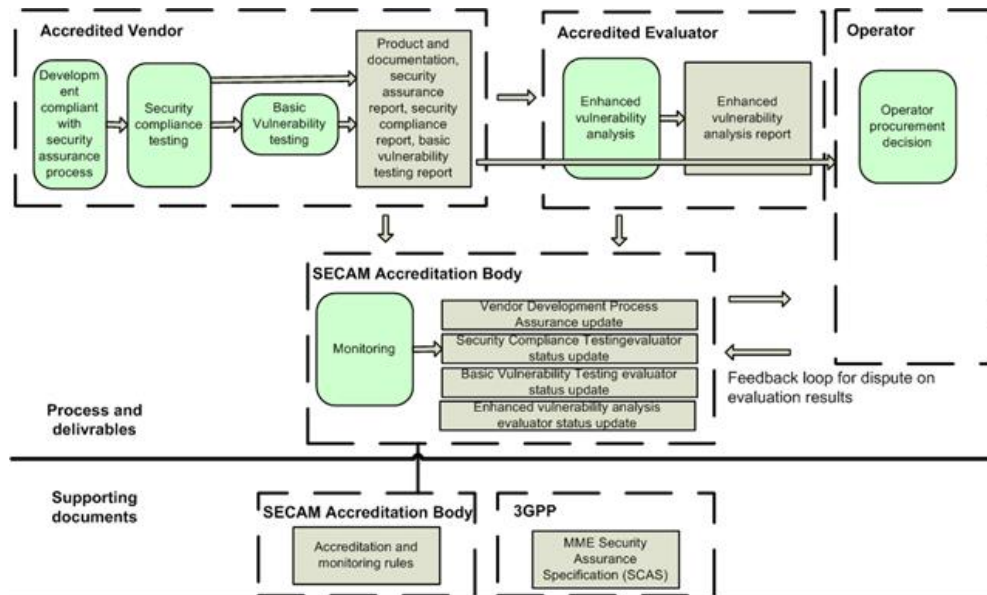


圖 1- 9 SECAM 安全檢測流程(以 MME 為例)

資料來源：3GPP

其中 3GPP 協助訂定不同設備之安全保證規範(SCASs)，SCASs 定義了該項產品之建議檢測項目(Test Case)，檢測項目內容包含檢測目的、檢測環境要求、執行步驟及預期結果；SCASs 的制定需遵行以下流程：(1)描述產品-定義產品的類型與重要資產；(2)定義產品安全問題-依此產品的重要資產產品定義可能遭受的安全威脅與安全目標；(3)找出產品的安全需求與測試案例-從產品的安全問題導出產品的安全需求。

目前 SCAS 已經完成所有設備共通的安全需求規範(3GPP TS 33.116)²⁴並完成核心網路-行動寬頻實體(Mobility Management Entity，簡稱 MME)設備特定的安全需求規範(3GPP TS 33.117)²⁵。2016 也開始著手討論基站(eNodeB)的 SCAS 制定工作。

²⁴ 3GPP TS 33.116, “Security Assurance Specification for the MME network product class (Release 13)”.

²⁵ 3GPP TS 33.117, “Catalogue of General Security Assurance Requirements (Release 14)”.

(四) GSMA

全球行動通訊協會(Groupe Speciale Mobile Association, 簡稱 GSMA)為 1995 年所成立,最初成立之主要原因是為了奠定與推廣 GSM 行動電話之共通標準的協會,演進至今,其主要工作為協助會員推動新興行動技術之商用化、互通性及研擬相關監理政策,此協會會員主要為電信業者、電信相關之設備商及網路業者等,主要目的為活絡電信產業之商業發展。而在 5G 的工作項目上,GSMA 也將協助電信業者擬定策略、監理框架及研究相關商用之應用發展,以利能輔助新世代通訊網路技術的推動。

在 3GPP SECAM 的安全檢測流程中,GSMA 扮演了檢測實驗室的認證單位,GSMA 成立了 Network Equipment Security Assurance Group (簡稱 NESAG)部門(如圖 1-10),主要為進行設備製造商及檢測實驗室資格審查,確保其可充分進行安全檢測,及確保其檢測之結果為國際性認可之安全規範。

近來,GSMA 為了因應逐漸高漲的行動網路安全意識,其 FASG (Fraud and Security Group)也開始制定相關的檢測項目與標準流程,包括:檢測及防止詐騙入侵行動服務中、探討行動服務條款的濫用情形、快速辨識交遞(Handover)漫遊期間的欺詐行為、雲端服務風險與控制、LTE 網路的安全性配置、LTE 漫遊安全、基礎設施架構的安全性和測試、SS7 安全、檢測惡意行動應用或軟體、IP 連線的安全性、VoLTE 服務的安全性分析等²⁶。

²⁶ GSMA 官網, Fraud and Security Group.

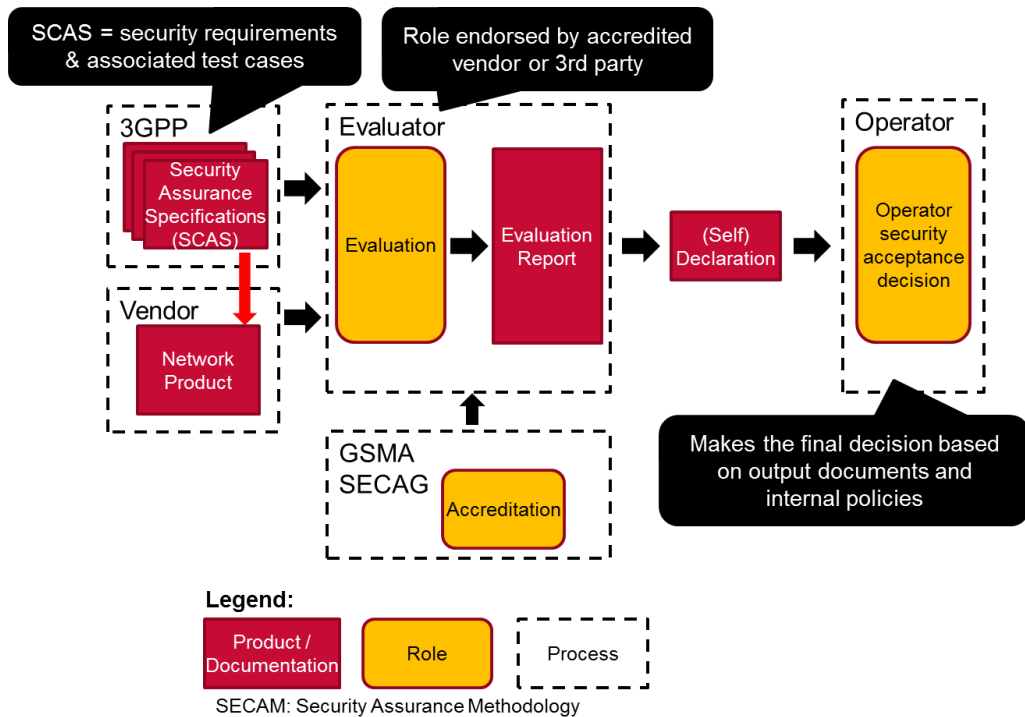


圖 1- 10 3GPP SECAM & GSMA NESAG 認證之角色

資料來源：3GPP

四、 問題陳述與初步看法

(一) 行動寬頻網路安全疑慮

1. 基站(eNodeB)安全威脅

由於行動寬頻基站(eNodeB)部署在非受控之暴露環境，同時也是行動寬頻核心網路(EPC)的主要入口，因此很容易成為安全上的威脅目標。在本企劃書背景分析之行動寬頻網路風險分析中，已列出行動寬頻網路(4GLTE)整體風險分析之六大威脅(請參見圖 1-1)，該威脅層面亦為基站本身易造成之安全風險。

基站可能的威脅面向包括通訊鏈路破壞，以及基站(eNodeB)裝置本身遭受的攻擊威脅，以下從行動寬頻網路風險分析中，歸納出三種基站之安全層面，說明基站所遭受之資安威脅：

1.1 用戶安全層面：

來自終端威脅(如圖 1-1 之威脅①、③)，例如惡意或受損的 LTE 使用者終端裝置 (User Equipment，簡稱 UE)可被用於向 eNodeB/MME 啟動 DoS 攻擊，偵測核心網路的拓撲，或進行任何其它類型的攻擊，或是某個使用者終端裝置設定不當，防護措施不足，則有可能啟動閘道上的安全防護機制，以致閘道被阻絕，而無法提供其他 UE 正常的網路存取服務。

1.2 管理安全層面：

- (1) OAM 的威脅(如圖 1-1 之威脅④、⑥)：心懷不滿的員工可能會透過遠程管理應用程式或物理介面來攻擊 eNodeB。
- (2) 來自網際網路或其他連接封包數據網路(PDN)的威脅(如圖 1 之威脅①、④)：如企業/合作夥伴的 IP 網路。這些來自 PDN 的攻擊，可能會侵犯網路邊緣的安全保護(如防火牆)，以及被植入病毒、蠕蟲、木馬程式進入核心網路等其他類型的攻擊。

1.3 控制/信令安全層面：

- (1) 空中介面和通訊路徑的威脅(如圖 1 之威脅②、③)：攻擊者可以啟動空中介面攻擊，例如竊聽、修改和偽造信令或用戶數據。
- (2) 接取網路設備實體接取威脅(如圖 1 之威脅④)：例如非法接取基站網路產品類別中的控制台介面。
- (3) 傳輸網路的威脅(如圖 1 之威脅⑤)：若為缺乏實體保護且暴露在外的後置迴路 (Backhaul)，攻擊者可以接取後置迴路(Backhaul)進行竊聽或修改傳輸的訊息。
- (4) 其他外部互連網路(如 GRX / IPX、其他 PLMN 等)與針對 MME / S-GW / P-GW 的威脅(如圖 1 之威脅①)：例如業者 A 為了提供漫遊服務給用戶，必須與外部行動業者網路連接，因此業者 A 的 MME / S-GW / P-GW 必須被外部行動業者的網路產品接取，若外部行動業者的網路產品遭受攻擊破壞，業者 A 的網路也可能受到攻擊。

2. 家用基站(HeNB)安全威脅

如之前背景分析所述，家用基站(HeNB)具備強化網路訊號覆蓋率與提供網路分流的功能。家用基站(HeNB)安裝在一般用戶家中或辦公室內，經由後置迴路(Backhaul)

連結其它基站(eNodeB)或連回核心網路，因此讓網路系統更容易受到惡意攻擊。在建置基站資安檢測環境計畫第 1 期研究中，參考了 3GPP 規範 TR33.820²⁷、TS 33.320，已列出家用基站(HeNB)設備的重要資產與相關的資安威脅，這些資產含括硬體、使用者帳號資料密碼與個人憑證、認證資料、組態資料、主控台介面、遠端介面、內建韌體與軟體及網路傳輸介面。

藉由分析上述這些重要資產可能遭受的攻擊方式包括憑證破解、中間人攻擊、重送攻擊、阻斷服務攻擊(Denial-of-Service Attacks，簡稱 DoS Attacks)、竊聽及偽裝攻擊等，整理出 14 項家用基站(HeNB)可能面對的資安威脅。這些威脅可以區分為下列幾大類別²⁸，請參見表 1-1。

表 1- 1 家用基站(HeNB)安全威脅

安全威脅	說明
2.1 身分驗證安全威脅	(1) 攻擊者取得合法家用基站(HeNB)的相關註冊資訊之後，即可偽冒合法的家用基站(HeNB)身分，與核心網路註冊，以開啟雙方後續之通訊。 (2) 家用基站雖然對核心網路啟用身分認證的功能，但倘若演算法強度不足可能會被攻擊者破解。 (3) 身分認證所用的憑證保存不當，攻擊者可透過網路入侵複製。另外若是使用插拔式的硬體式憑證，也有可能遭竊取。這些身分驗證的安全威脅將可能衍生偽冒攻擊，惡意攻擊者可以偽裝合法的設備竊取使用者裝置的機敏資料或進行竊聽。
2.2 機敏資料的傳輸安全威脅	(1) 家用基站(HeNB)與核心網路之間的資料傳輸若沒有加密處理，尤其後端接取鏈路(Backhaul link)這段是傳統之 IP 網路，攻擊者可透過中間人攻擊方式竊取機敏資料。 (2) 家用基站(HeNB)在初次連線上網時，會提供公眾行動電話網路(Public Land Mobile Network，簡稱 PLMN)、HeNB ID 等設備

²⁷ 3GPP TR33.820, “Security of H(e)NB”.

²⁸ 3GPP TS33.320, “Security of Home Node B (HNB) / Home evolved Node B (HeNB)”.

安全威脅	說明
	資訊與核心網路之 MME 進行註冊，若惡意使用者獲取設備相關資訊，可進一步以偽造家用基站(HeNB)的方式欺騙使用者連線而造成更大的危害。
2.3 系統設定的資安威脅	家用基站(HeNB)一般提供網頁管理、telnet 或 SSH (Secure SHell protocol)登入設定等設定模式，若惡意使用者獲取設備帳號相關資訊，依據帳號權限的高低可造成不同等級的危害。例如可以登入家用基站(HeNB)後改變存取控制表 (Access Control List，簡稱 ACL)或射頻功率，來影響用戶端設備使用其服務。甚至可以改變家用基站(HeNB)座標參數來混淆核心網路，以致於來自核心網路的服務遭到停止。
2.4 系統軟體更新的安全威脅	(1) 家用基站(HeNB)若遭攻擊者透過實體接觸植入非原廠的軟體，額外引起的資安漏洞，可能會造成家用基站的服務阻斷、或是遭受到控制。 (2) 家用基站(HeNB)可能經由未經官方認可的來源進行軟體及軟體更新，導致更新後的軟體潛藏著資安漏洞。
2.5 網路設定安全威脅	(1) 家用基站(HeNB)之系統設定若沒有正確的權限控管，使用者可能會誤改或蓄意修改設定檔的資料，如：與核心網路連線的 IP 位置、SeGW 的位置等，因而造成服務中斷之問題。或是將連線設定修改連接至惡意 IP 位置，造成 UE 連線後的資訊洩漏。 (2) 若家用基站(HeNB)的系統時間未與其他家用基站(HeNB)及 MME 正確同步，會無法正常提供服務。 (3) 若電信業者啟用家用基站管理系統(HeMS)來對家用基站(HeNB)進行資安方面的管控，可能導致攻擊者將攻擊目標改為 HeMS，藉由 HeMS 可能潛藏的網路管理介面漏洞，進行滲透。
2.6 無線通訊的安全威脅	惡意攻擊者可以透過無線側錄器等相關工具竊

安全威脅	說明
	聽、側錄甚至竄改無線通訊內容。此外攻擊者可設定偽造的家用基站(HeNB)的電信商代碼，會造成使用端設備誤連接到偽造的家用基站(HeNB)，造成使用者的國際行動用戶識別碼(International Mobile Subscriber Identity，簡稱IMSI)外洩。
2.7 存取控制之管理威脅	惡意 UE 可能透過修改自身之封閉型用戶群組(Closed Subscriber Group，簡稱 CSG)列表，與無適當存取控制表(Access Control List，簡稱 ACL)設定之家用基站(HeNB)連接，享用不屬於用戶自身之網路服務。

資料來源：本團隊整理

3. 偽基站的安全威脅

偽基站是目前行動寬頻網路(4G LTE)本身安全性漏洞最常被討論的議題，在無意的抗干擾研究，已經獲得廣泛的探討²⁹，但有意的攻擊由 LTE 控制通道的欺騙，所造成阻斷服務的攻擊行為已被證實，2015 IEEE 通訊與網路標準研討會(CSCN)中，已發表一篇利用偽基站發送 LTE 訊號，藉以欺騙用戶端(UE)連接，妨礙用戶終端設備連接到真實的基站案例。其方法是建立假的基站(NodeB 或 eNodeB)，發送一些 LTE 物理層的控制訊號與較高階層的訊息，但不具備認證金鑰，藉由控制通道達到欺騙的目標，造成手機阻斷服務。

而在國際上特別是中國大陸，已有多起利用偽基站發送之詐騙簡訊，騙取及盜刷民眾之信用卡帳號，因次如何防範偽基站所造成的干擾及惡意欺騙，已是基站安全及行動寬頻網路安全之重要議題。

4. VoLTE 安全威脅

VoLTE (Voice-over-LTE)是一個為行動寬頻(4G LTE)網路所設計的 IP 語音服務技術，此新技術的產生主要是因為行動網路將逐步捨棄舊有支援語音的電路交換(Circuit-switched)架構，進而採用全 IP 網路的封包交換(Packet-switched)。VoLTE 是根

²⁹ J. Acharya, L. Gao, and S. Gaur, "Heterogeneous Networks in LTEAdvanced, 1st ed.", 2014/5.

據網際網路的 Voice-over-IP (VoIP) 原理所設計，語音數據改由 IP 封包傳送，取代舊有的專用電路。藉由 IP 封包的傳送形式，VoLTE 不但可以經由高保真度的編碼提供高品質的語音服務，亦可輕易地擴充而支援影像通話和會議通話。然而，VoLTE 並未經過完整且系統化的安全檢驗，使得行動寬頻網路架構因 VoLTE 而產生多種危險性，使駭客得以利用漏洞成功攻擊系統。

傳統的 3G 架構中，手機若要撥打電話必須透過溝通處理晶片 (Communication processor)，而此該晶片的實作細節只被少部分的晶片製造商所掌握。相反地，透過 VoLTE 撥打電話的裝置則是透過應用處理器 (Application processor)，透過 IP 封包來傳遞語音，而攻擊者正可利用此特性來對手機網路進行攻擊。

VoLTE 的運作包含了控制層 (Control plane) 和數據層 (Data plane)，兩層皆由 IP 封包所傳送。在控制層上，VoLTE 採用 SIP (Session Initiation Protocol) 協定傳送語音服務通話的控制訊息，而語音數據則由 RTP (Real-time Transport Protocol) 協定於數據層上傳送。為了達到電信等級 (carrier-grade) 的語音服務品質，VoLTE 採用 LTE 網路所支援的高優先級承載 (High-priority Bearers) 來傳送控制訊息和語音數據。

當新技術 VoLTE 被整合至現有的 LTE 網路中，將造成 LTE 網路系統上不小幅度的改變，包括手機硬體和軟體的升級，以及在核心網路裡，原有數據封包閘道器 (Packet Data Network Gateway) 的配置升級，和新 IP 多媒體子系統 (IP Multimedia Subsystem) 的設置。這些改變都有可能導致 LTE 網路的安全性漏洞，原因有可能是 VoLTE 本身存在的安全性問題，或是 VoLTE 與 LTE 網路系統之間運作的不協調所致。

當 VoLTE 的控制和語音數據，依賴於與 LTE 數據服務相同的 IP 封包交換，且經由相同的數據封包閘道器轉送時，若 VoLTE 的網路安全沒有經過嚴謹地規畫與設計，它的服務通道有可能遭受攻擊，譬如：LTE 的數據服務可以經由 VoLTE 的通道傳送。尤其是 VoLTE 將原由手機硬體 (數據機) 所負責的電路交換語音服務，改由手機軟體 (作業系統和行動應用程式) 以封包交換的方式提供語音服務。

相較於硬體的安全性，基於 IP 封包而設計的 VoLTE 軟體更容易遭受攻擊，攻擊者可以偽造 IP 封包攻擊 VoLTE 在手機上的用戶端軟體，或是取得行動作業系統的管理者權限 (如安卓作業系統經由 Root 過後的 Superuser 權限) 後，製造惡意的 IP 封包，經由 VoLTE 服務通道攻擊核心網路和新 IP 多媒體子系統。

且 VoLTE 在與基站和核心網路溝通的過程中，只有到基站的內容是會加密的，而基站到核心網路則是沒有加密，所以可能會產生安全風險，例如在 VoLTE 封包裡可能會有暴露核心網路資訊的風險、惡意的使用者朝核心網路發送大量的信息使之資源耗竭、語音遭到中斷、電話號碼遭盜用等，隨著新技術慢慢的演變，攻擊手法也將更多元化，因此 VoLTE 的網路安全也是近年行動寬頻網路應用關注焦點之一³⁰。

(二) 行動寬頻技術演進之資安風險疑慮

1. 5G 的安全疑慮

對於第五代行動通信(5G)系統中，速度的追求雖為一大特性，但在安全與隱私上面也是有不可忽略的重要性。在 2015 年 6 月 24 日，Ericsson 公司發表了一篇有關 5G 安全的白皮書「5G SECURITY: SCENARIOS AND SOLUTIONS」，提到 5G 安全環境的構想，點出有關 5G 的一些安全問題，如身分管理問題、5G 無線網路安全問題、雲端運算安全平臺等。

在身分管理問題方面，現階段 4G LTE 定義了由用戶身分識別模組(Universal Subscriber Identity Module，簡稱 USIM)導入行動通訊網路的架構，此方式具有高安全性，因此在 5G 時代有希望延用此系統，但對於竊取國際行動用戶識別碼(International Mobile Subscriber Identity，簡稱 IMSI)的威脅雖然已經在制定 3G 及 4G 通訊系統時已討論過，但業界中各家電信業者卻未設計相關的保護機制，因此在 5G 系統中對於 IMSI 保護機制是否需要增強，是值得討論的議題。

另外在無線網路安全問題上，目前 4G LTE 網路已對無線網路設計相關的保護方案，如偵測竊聽，但 5G 在無線網路安全上，卻沒有針對新註冊用戶或修改帳號時的保護。在 5G 無線通訊中如工業自動化，是否需新增額外的保護也需要加以探討。

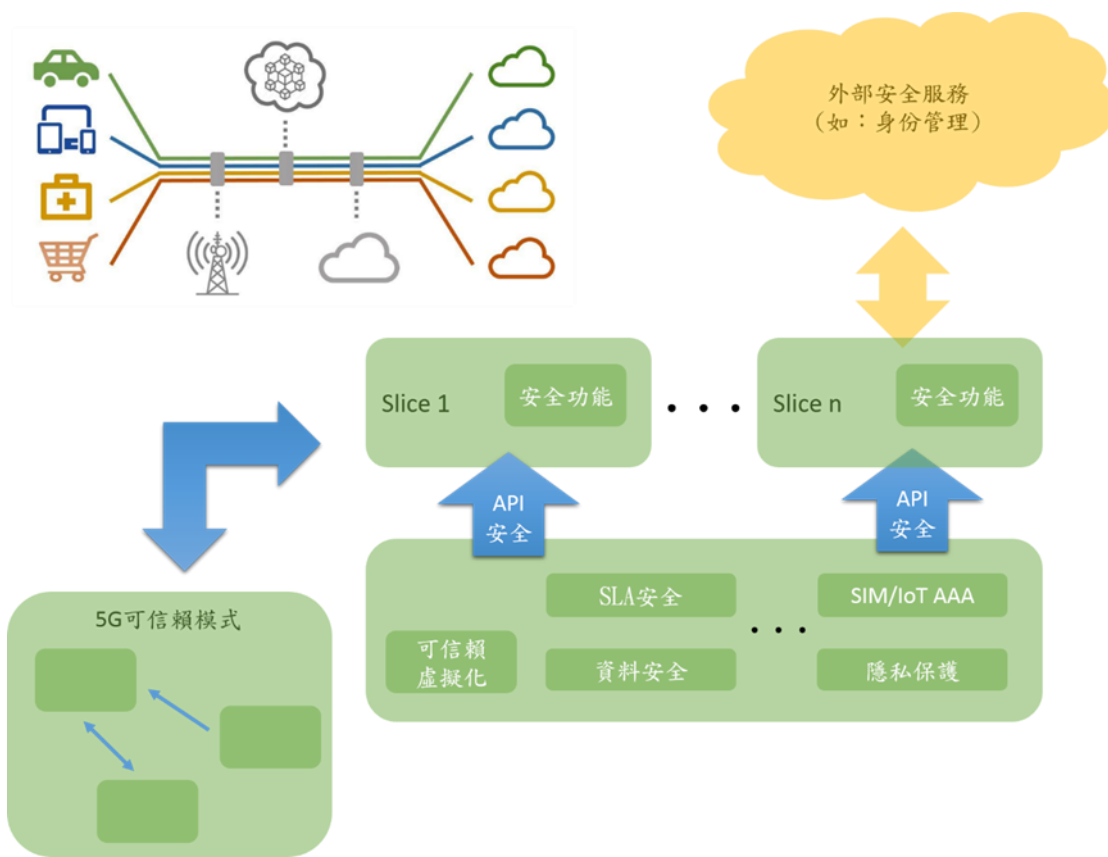
SDN 與 NFV 為 5G 電信網路服務架構的主要關鍵技術，以因應未來多變的使用情境。主要概念係以虛擬化統整硬體資源，以軟體管理及分配虛擬化資源，該架構將可能在雲端運算環境中實現。因此雲端運算安全問題也成為 5G 安全之重要討論議題

³⁰ Seongmin Park, Sekwon Kim, Kyungho Son and Hwankuk Kim, "Security Threats and Countermeasure Frame Using a Session Control Mechanism on VoLTE", 2015/11.

之一，為 5G 系統中所需考量的層面，因此 Ericsson 的 5G 白皮書提出雲端運算之安全要求，如開發具高度安全保障的管理程序及網路虛擬化技術、從現有遠端認證可信的運算工具及概念，架構有用的安全系統及架構、如提供雲友好(cloud-friendly)加密的有效解決方案，以及開發可信賴且易於使用的雲端系統等。

在 5G 行動網路通訊下，許多物聯網應用上的安全可能須仰賴 5G 網路的安全，如自動駕駛或醫療方面，這也就意味著 5G 網路產品將會有大量的成本投資在安全檢測方面，因此 Ericsson 白皮書提出了 5G 安全架構構想圖(如圖 1-11)。其網路構想係以網路切片(Network Slicing)的概念，可以處理多樣化且不同的應用與用戶要求，其可透過虛擬層將保密機制和安全統整起來³¹。

³¹ Ericsson White paper,“5G security”, 2015/6.



資料來源：Ericsson

SDN 是一種新的網路架構，網路專業人員能以透過中央控制的方式，利用程式重新規劃網路，即可以有效控制網路的流量。因此其安全性也是業者是否採用的重點之一，Global Technology Resources 公司的技術長 Scott Hogg 曾提出 SDN 架構下的安全威脅及安全強化方法，簡單描畫出 SDN 可能被攻擊的各個管道(如圖 1-12)，其中主要可以分為三層：

³² 劉榮太,“夯技術 SDN 的資安課題”,2014/1/27.

第二層控制層-Control Layer，其架構元件之 Controller，為 SDN 網路管理的控制核心，因此 Controller 想當然爾成為攻擊者炙手可熱的目標，除了發送大量訊息給於 Controller 造成網路崩潰，最糟糕的情況是攻擊者成功模擬出一個新的 Controller，偽裝成真正的大腦發布指令。

第三層 Infrastructure Layer 中，攻擊者除了能針對網路節點攻擊之外，還可能試圖攔截 Southbound API 傳送過來的信息，進行中間人攻擊，傳送錯誤的信息給網路設備。

SDN 除了上述所提到的外部攻擊疑慮之外，篩選管理者發布的命令是否會產生「策略衝突」也是不可忽視的要點。所謂的「策略衝突」即為發布錯誤命令給下層的網路設備，造成網路混亂影響整個系統運作，因此如何維護 SDN 網路能夠穩定且安全的執行將是業界是否採用 SDN 網路架構之主要重點之一。

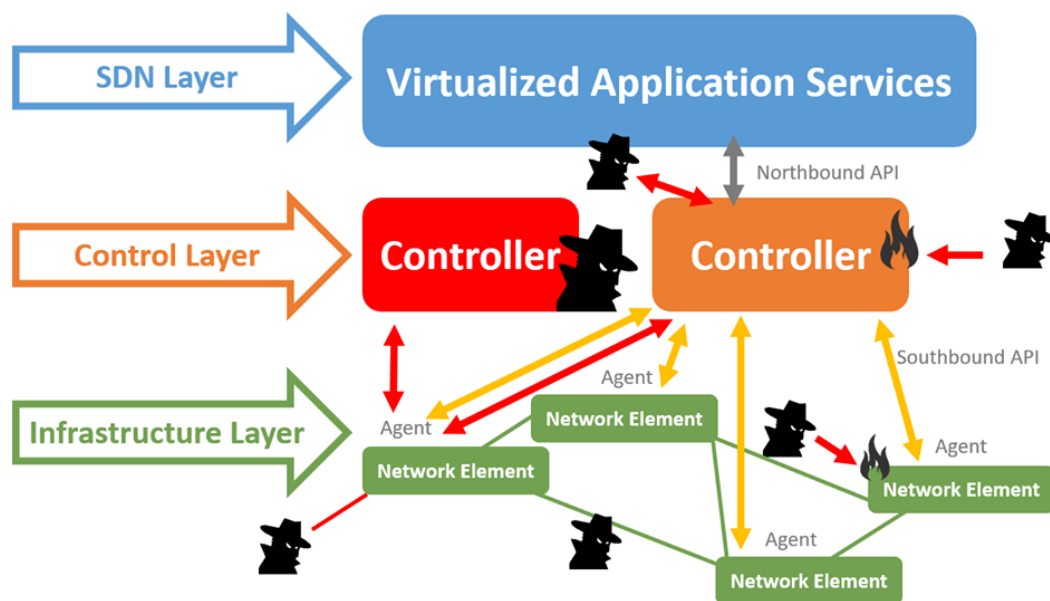


圖 1- 12 SDN 各面向攻擊手法示意圖

資料來源：整理自 NETWORKWORLD³³

³³ Scott Hogg, "SDN Security Attack Vectors and SDN Hardening", 2014/10/28.

3. IoT 的安全疑慮³⁴

物聯網的迅速崛起，提升了許多生活上的便利性，像是交通、商業和醫療等。然而，傳統的 IT 產品在設計時並非以物聯網裝置為考量所設計的，因此存在著許多資訊安全的疑慮。一旦裝置連上網際網路，駭客即有機會透過竊聽、金鑰淪陷及中間人攻擊等方式攔截物聯網設備所蒐集及傳輸的使用者資訊，除了帶來資料與隱私權保護的問題外，還可能影響人身及居家的安全，如駭客可以透過嬰兒監視器監視使用者屋內狀況、駭入居家的保安系統或電力線來癱瘓防盜設備等。

近年來已發生許多 IoT 的攻擊案例，例如在美國，有位用戶為了監視嬰幼兒因此採購監視器，該監視器具有錄影及播放音效的功能，可以透過遠端方式結合語音通話嚇阻犯案，結果某天在家時卻發現監視器有不明男子在說話，才發現原來他們的監視器已經被竊聽攻擊。

不只竊聽攻擊，智慧電表也有被攻擊的機會，如果家裡電表遭受攻擊了，攻擊者可以分析家裡用電情形乃至於知道家裡甚麼時候有人，這些都是可能會造成人財的損失，因此物聯網的攻擊並不可小覷。

(三) 應建立國內環境適用之行動寬頻基站資安檢測規範

電信網路已成為各國資訊化的重要基礎設施，行動寬頻網路扮演電信網路中的重要基礎設施，隨著行動寬頻網路持續演進、用戶與訊務量不斷增長，安全威脅日益成為行動寬頻網路的重要課題，欲解決這些安全威脅，國際間已有不同電信與資訊安全組織持續推動行動寬頻資安標準，考量通訊環境不斷變化與演進需求，各組織依據設備製造、業者環境、使用者等面向，設計周嚴、合宜的行動寬頻資安標準，以促進行動寬頻服務發展，並同時兼顧資訊安全。

在觀察行動寬頻資安檢測標準的發展，3GPP 已定義行動寬頻網路基本的安全功能要求，將安全功能在 LTE/SAE 研究項目中持續擴展與強化，涵蓋 LTE 整體安全性，其中也將基站安全機制納入 3GPP TS 33.401 標準文件中，將 LTE/SAE 網路安全區分網路接取安全、網路領域安全、用戶領域安全、應用領域安全、安全服務配置五個領

³⁴ 趨勢科技,“威脅情報資源-萬物聯網(IoE)”。

域。並另外在 TS 33.320 定義了家用基站(HeNB)的資安需求。

有鑒於行動寬頻網路安全之重要性，3GPP 於 2015 年制定了網路設備資安確保與檢測框架(SECAM)，制定網路設備在上線前的資安檢測與評估機制，其中的安全保證規範(SCAS)，將定義不同產品一般性的檢測項目與規範，3GPP 已於 2016 年完成 MME 產品之安全保證規範(SCAS)，也開始著手訂定基站(eNodeB)設備之安全保證規範(SCAS)中。

因此建議應參考國際標準及資安檢測技術之研究，研擬適合國內環境之基站安全檢測內容與檢測項目，並進行實測，以 3GPP 訂定之標準文件為基礎，提出適合我國環境之基站資安檢測規範草案。

(四) 提供行動寬頻基站資安檢測指引

一般資通訊網路設備之檢測作業程序已有 NIST GNST、CC 及 3GPP SECAM 可參考，建議應參考目前最新之國際資安檢測流程及框架，並追蹤 3GPP 對基站資安與檢測最新之會議結論與規範，結合本計畫實測結果，設計一套適合國內環境之基站資安檢測作業流程與指引提供主管機關、檢測實驗室及電信業者參考，可節省檢測單位及受測者所需耗費之時間及成本。

第三節 研究目的

本計畫主要目的期能協助國內行動寬頻服務電信業者，提升國內整體行動寬頻網路安全技術及檢測能量，以保障消費者權益。

透過蒐集及研析先進國家之行動寬頻基站資安及檢測技術，以發展適合國內環境之基站管理及檢測方針；並依據研究結果及導入國際經驗，規劃及完成建置示範性行動寬頻基站資安檢測平臺，本計畫目標如下。

- 一、結合學界、研究機構及產業專家組成專業行動寬頻資安研究團隊，研析行動寬頻基站資安相關檢測規範及技術。
- 二、整合國內既有檢測環境及本會採購之檢測工具，建構一示範性之行動寬頻基站資安檢測平臺。

三、參考國際行動寬頻資安檢測技術、檢測規範，及本計畫檢測平臺相關實測結果，發展一套適用於國內之行動寬頻基站資安檢測標準供電信業者自律性檢測之參考。

四、協助電信業者及廠商，提升國內行動寬頻網路之服務安全。

第二章、研究方法與進度說明

第一節 研究方法

一、研究架構

建置基站資安檢測環境第1期計畫，已完成行動寬頻網路風險與檢測工具之研究，並規劃出行動寬頻基站資安檢測平臺，產出行動寬頻基站資安管理草案；第2期計畫將延續第1期之研究結果，除持續針對前瞻性資安技術、國際行動寬頻資安框架進行研究外，主要重點為規劃行動寬頻基站(包含 eNodeB 及家用基站(HeNB))資安檢測項目、建構基站資安示範性檢測平臺並執行實測驗證，依實測結果與國際標準，規劃出適合國內環境之基站資安檢測規範草案與檢測流程，最終將本計畫之弱點檢測結果同時參考國際性之弱點資料庫，建置一基站弱點資料庫供產官學界參考。

上述研究將配合國外參訪與「行動寬頻基站資安座談會及研討會」之舉辦，促進相關領域主管機關、學界及業界彼此分享觀摩及交換意見與建議，藉此提升我國整體行動寬頻網路安全，整體計畫架構如下圖所示。



圖 2-1 研究架構圖

資料來源：本團隊整理

二、 研究方法

本計畫依據計畫架構擬定出各研究分項需要釐清的議題，採用適當的研究方法進行，再串連這些工作項目的成果產出各項研究報告，分述如下：

● 文獻分析法

此方法將用於前瞻性資安技術研究、國際行動寬頻資安框架研究、行動寬頻資安技術研究與基站資安檢測項目規劃及基站資安檢測規範與檢測流程之研究，蒐集國外行動通訊網路前瞻技術的發展趨勢，檢視因應科技變化趨勢，針對當前國家、社會所面臨重要資安議題，重新提出電信資安的架構及發展定位，以促進行動寬頻網路的服務安全。

● 比較分析法

針對與行動寬頻資安技術研究與國際行動寬頻資安框架研究之成功或代表性個案，進行研究分析；並針對這些個案，進行比較分析，找出個案之間的相似與差異之處，以及其背後的原因，以個案研究與比較分析法探討國際組織與先進國家資安技術與相關規範，以作為我國在相關議題規劃上之借鏡。

● 深度訪談法

此方法將應用於本計畫對國際經驗之蒐集與分析。透過國外參訪電信業者、檢測實驗室、專業人士或利益相關團體，蒐集行動寬頻資安技術與檢測之意見。

在國際經驗發展上，規劃訪談基站供應商如 NSN (Nokia Siemens Networks) Security Center，了解供應商之行動寬頻檢測平臺、檢測工具及檢測方法；以及行動寬頻發展較為先進國家之電信業者，認識其行動寬頻網路安全保護措施及新世代網路之發展。

● 座談會/研討會

以電信與資安管理機關、學界、專家及業者代表為對象，與各界進行雙向交流，舉辦座談會與研討會，適時提出本計畫之規劃方向或研究成果，了解利益相關團體對行動寬頻基站資安檢測規範草案及檢測流程之意見。

● 模擬法（模型方法）

模擬法是先依照原型的主要特徵，創設一個相似的模型，然後通過模型來間接研

究原型的一種方法。在概念性驗證（Proof of Concept，簡稱 PoC）的階段中，將結合 LTE 核心網路模擬器，架構 LTE 網路模擬仿真環境，設計相關基站檢測之測試項目 (Test Cases)，先行驗證檢測項之可行性。

● 實驗研究法

實驗研究法是指研究者在控制足以影響實驗結果的無關干擾變項下，操弄實驗變項，觀察實驗變項(即獨立變項，Independent Variables)對依變項(Dependent Variables)所產生的影響。這個研究法的設計主要目的是在探究獨立變項與依變項之間的因果關係，其作法是操縱獨立變項，然後檢討其對依變項的影響。

● 經驗總結法

經驗總結法是通過對實踐活動中的具體情況，進行歸納與分析，使之系統化、理論化，上升為經驗的一種方法。透過經驗總結法，將本計畫相關文獻、國際經驗及國際標準之研究，歸納綜整產出前瞻性資安技術、行動寬頻資安檢測技術、國際行動寬頻框架研究結果及行動寬頻基站資安檢測規範草案。

三、 施行方式與執行步驟

本計畫係配合 NCC「建置基站資安檢測環境計畫(第 2 期)」委託研究計畫書之業務需求，研擬規劃本計畫之施行方式與執行步驟(如圖 2-2)，詳細說明如下：

配合計畫核心焦點「加速行動寬頻服務及產業發展—建置基站資安檢測環境」，依其研究議題分為資安技術研究：包含「前瞻性資安技術研究」及「行動寬頻資安技術研究」；實測驗證：包含「建構行動寬頻基站資安檢測平臺」，執行「行動寬頻基站資安檢測」，建置「基站弱點資料庫」；與政策規範研究：包含「國際行動寬頻資安框架研究」及「行動寬頻資安檢測規範研究」。

本計畫將針對上述研究議題進行研討及執行實測驗證，各主題將採取適切七大研究方法包含文獻分析法、比較分析法、深度訪談法、座談會/研討會、模擬法（模型方法）、實驗研究法、經驗總結法予以進行，藉由各研究方法以獲得本計畫預期產出研究成果，包含「蒐集最新之資安技術與國際資安政策規範」、「完成基站及家用基站(HeNB)資安檢測項目與檢測方法規劃」、「建構一行動寬頻基站資安檢測示範性平臺」、「完成

基站及家用基站(HeNB)資安檢測驗證，產出檢測報告」、「建置基站弱點資料庫」、完成「行動寬頻基站資安檢測規範草案」與「行動寬頻基站資安檢測流程與指引」規劃。

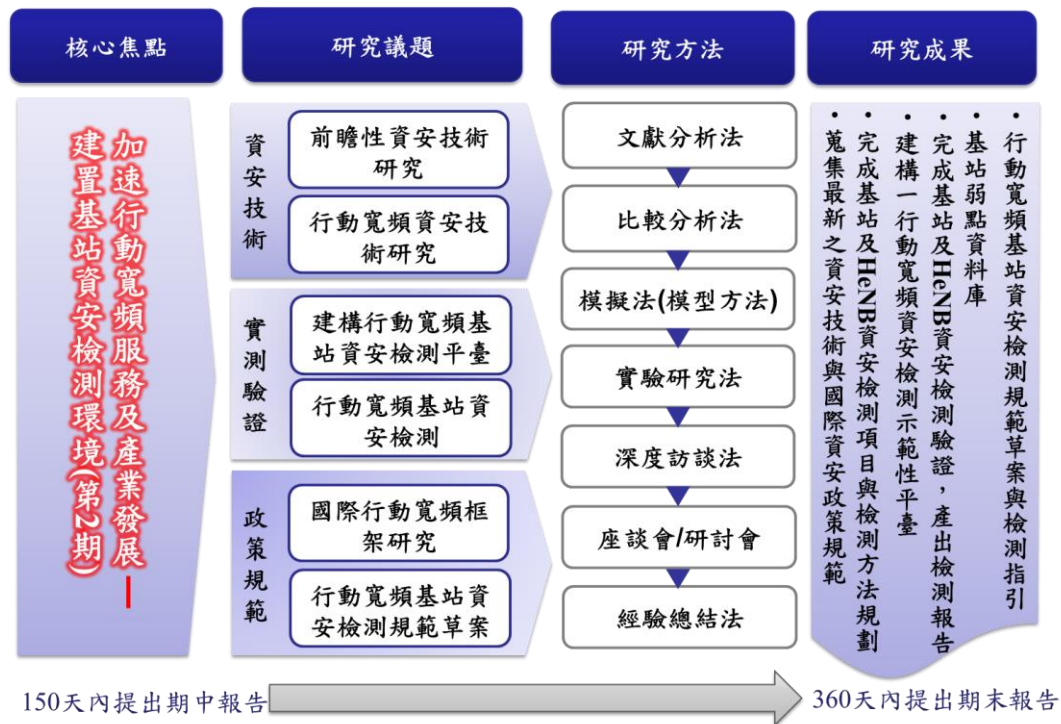


圖 2-2 本計畫施行方式與執行步驟

資料來源：本團隊整理

(一) 前瞻性資安技術研究

第1期委託研究案的前瞻性研究中，為了瞭解最新的網路資安議題及最新攻擊與防禦趨勢，本團隊參訪了國外行動寬頻網路發展先進國家之電信主管機關與研究中心。此外，蒐集近兩年的重大資安事件做分析與探討，尋找其中的缺失與可改進之處。搭配相關文獻的研究與實務經驗總結了資安攻擊技術最新趨勢研究。除此之外，也深入了解並參考國際間對於共通準則與美國聯邦資訊處理標準之檢驗流程概念，以及研究與閱讀 3GPP 與行動寬頻網路(4G LTE)相關的標準，綜整資安檢測標準與檢測流程之最新趨勢。

本計畫之委託研究將延續第1期之研究成果，針對新興的行動寬頻網路環境所面臨到不同的安全需求進行探討，包含全世界已開始制定與發展的 5G 標準與技術架構、

與 5G 網路架構與雲端運用密切相關之關鍵網路技術-SDN 的安全，以及隨 5G 發展將帶動的物聯網(IoT)應用，在萬物皆可聯網的時代來臨，行動寬頻網路技術與 IoT 的整合與安全是備受重視的議題。

本工作項目將透過文獻探討及參訪國外行動寬頻發展較為先進國家之行動寬頻資安檢測實驗室及電信業者，蒐集及交流行動寬頻基站資安檢測技術及新興行動寬頻技術之最新發展。

另在國際資安檢測標準與檢測流程最新趨勢研究上，本團隊將針對 3GPP、CC 與 GSMA 與基站資安相關之標準與檢測流程進行深入探討，本團隊將蒐集、閱讀、整理、綜整最新之文獻與技術報告，並針對與行動寬頻資安相關的議題做深入的討論，並將相關研究結果作為研擬本計畫基站資安檢測規範及檢測流程之參考。

(二) 國際行動寬頻資安框架研究

本工作項目將以行動寬頻網路發展先進之國家，包含英國、美國、歐盟、加拿大、日本等 5 個國家地區，首先蒐集研析其國家整體網路安全策略，包含政策、法規與權責機關，有鑑於行動寬頻網路之安全亦為其國家網路安全政策之一環，且為重要之基礎建設，由國家整體資安政策架構出發，可瞭解先進國家建構網路安全之策略，並針對行動寬頻網路之資安議題有初步定位。

在瞭解整體架構及權責機關的基礎下，將進一步針對行動寬頻網路之管制機關與資通訊網路安全負責機關之角色進行研析，並檢視其可能的分工或法規政策重點。由背景分析可知，各國關於通訊產業之管制機關與資通訊網路安全之權責機關並不必然為同一，初步推論原因在於通訊主管機關主掌產業管制，其組織可能為獨立機關，其管制對象為私部門企業；但資安議題橫跨公私部門，單純之產業管制機關未必在資安議題上擔任主要角色。

最後則針對通訊產業主管機關對於行動寬頻網路業者可能的資安權利義務要求之議題進行研析，搜研相關技術規範、準則、最佳實踐等文件，以具體瞭解各國針對行動寬頻之資安規範趨勢，並借鏡其作法與經驗，提供我國主管機關規劃政策之參考。

（三） 行動寬頻資安技術研究

建置基站資安檢測環境計畫第 1 期中，在行動寬頻資安技術研究上已提出行動寬頻網路之資安威脅、現有安全機制與漏洞及相關之資安檢測技術研究結果，第 2 期之委託研究案將延續第 1 期之研究，深入與基站(eNodeB/HeNB)系統本身及其密切相關之空中介面與核心網路-MME 資安技術進行研究，並研擬基站資安檢測項目，作為本計畫基站檢測之參考。

1. 空中介面資安技術研究

在行動寬頻網路運作過程中最基礎的空中介面資安技術研究中，將深入探討空中介面相關之新興資安議題，透過文獻分析及實驗方法，探討偽基站造成用戶端(UE)隱私之可能資安議題，提出可能之解決方案。並研析新一代的語音通信技術 VoLTE 對 LTE 網路所產生的新安全漏洞。

2. 核心網路-MME 資安技術研究

在核心網路-MME 資安技術研究上，因 MME 為核心網路的管理者，主要負責處理 Control-plane 訊息，如移動性、身分認證及安全性等的管理；因此，對於行動寬頻網路的環境，MME 扮演了一個極為重要的角色，倘若其安全性受到影響，將造成核心網路(EPC)整體網路控制訊息遭受破壞，且易危及到整體核心網路(EPC)環境。且 3GPP TS33.116 及 TS33.117 已對 MME 設備之 SCAS 完成相關檢測項目及檢測技術之規範，因此，在基站資安檢測項目之相關規劃中，將納入核心網路-MME 資安檢測技術研究作為規劃之參考。

3. 基站資安檢測技術研究

由於行動網路日益複雜與多元，各設備商所提供的服務與商品也不盡相同，因此基站資安檢測技術研究擬藉由 3GPP 標準規範 TS 33.320、TS 33.401、TS 36.413³⁵、TR 33.805、TR 33.820 等所提出的基站相關安全內容與行動寬頻網路安全內容，綜整及規

³⁵ 3GPP TS 36.413, “Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)”.

劃適合國內電信環境之基站資安檢測項目，本計畫將依複雜程度產出三大類型之檢測項目：一般性、進階性與家用基站(HeNB)之資安檢測技術及項目，並規劃如何透過檢測平臺現有設備及工具執行實測。所有檢測項目之規劃將包含檢測環境要求、檢測說明、檢測目的、檢測工具與方法、合格判定標準及參考資料。

- 檢測環境：環境的說明與起始狀態及初始條件。
- 檢測說明：說明檢測內容以及相關的安全需求或是威脅。
- 檢測目的：檢測案例的目標。
- 檢測方法：符合檢測需求之方法及步驟。
- 合格判定標準：判定檢測成功與否之標準，或是輸出的內容或格式
- 參考資料：參照的文件或是對應的威脅種類與細項。

(四) 建構行動寬頻基站資安檢測平臺

為了能防範常見攻擊威脅，通訊裝置的製造商，往往需要在裝置出廠前或上線前完成基本檢測，以瞭解這些裝置的抵禦能力。然而隨著使用者意識抬頭及因行動寬頻網路的全面 IP 化導致網路攻擊的影響層面更為廣泛，進而促使國際間開始著手發展安全檢測規範，以確保各網路元件及節點之安全防護能力。

考量本計畫擬定之檢測規範的適用性，本工作項目將完成符合我國使用環境之行動寬頻基站資安檢測示範性平臺建構，其建置之目的在檢測行動寬頻基站於我國使用可能存在之資訊安全風險，建議經由本第三方公正平臺的檢測並觀察待測基站抵擋攻擊的能力，並參考最終之檢測報告以瞭解其可能存在的弱點以及可能遭遇的最新資安威脅，提前規劃因應未來上線後需要採取的防禦策略。

而為能更進一步檢測行動寬頻網路中基站可能遭遇的資安威脅，參考建置基站資安檢測環境計畫第 1 期之研究結果及概念性驗證結果所規劃之行動寬頻資安檢測平臺架構，及本計畫前述研究所彙整之國際最新資安檢測標準與流程趨勢與行動寬頻資安技術，並進一步考量行動寬頻網路服務、通訊交握操作及攻擊切入點等特性，作為建構平臺細節之基礎。此外將依據建置基站資安檢測環境計畫第 1 期行動寬頻基站資安檢測平臺規劃，進行相關需求元件、功能及環境要求等評估，以完成本計畫基站資安檢測平臺建構之目標，相關執行步驟說明如下圖所示。

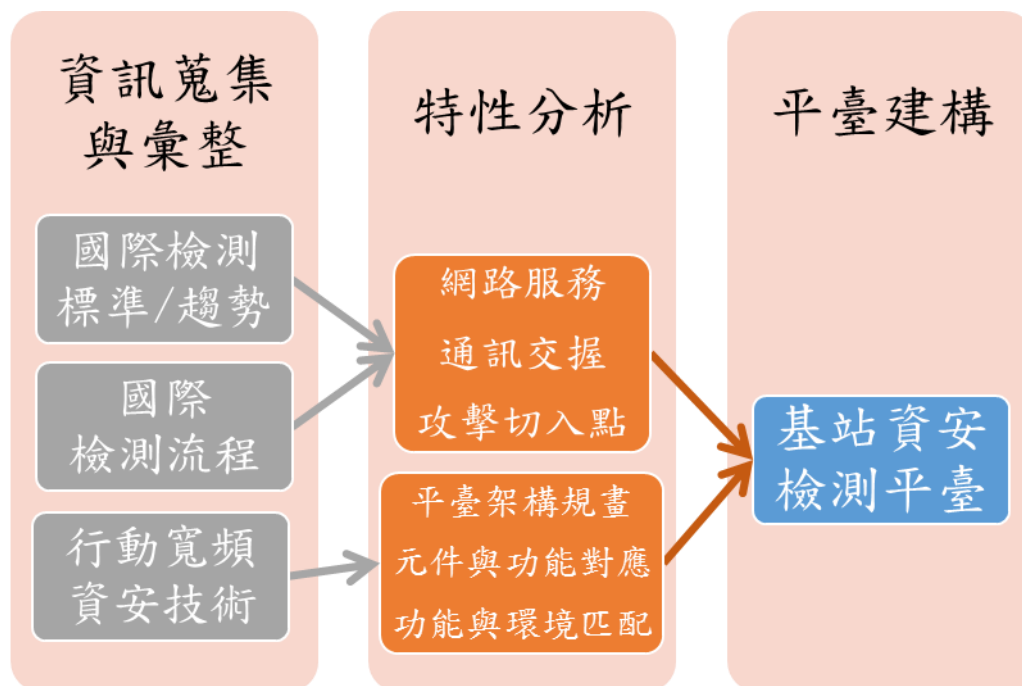


圖 2-3 建構基站資安檢測平臺執行步驟

資料來源：本團隊整理

依前述規劃所建構之行動寬頻基站資安檢測平臺，其將統整「建置基站資安檢測環境計畫」第 1 期所規劃之檢測平臺架構，與 NCC 所採購之檢測工具與本計畫租賃之行動寬頻實驗場域(包含使用者裝置、核心網路等)，依 3GPP 規範，架構行動寬頻(4G LTE)網路，完成設備介接及整合性功能驗證測試，確認平臺可正常運行，並能有效配合執行本計畫之基站資安檢測，提供檢測平臺相關驗證紀錄，以作為後續進行實際基站資安檢測、研擬基站資安檢測規範與作業程序之參考，最終產出一適用於國內行動寬頻環境之基站弱點檢測資料庫。

(五) 行動寬頻基站資安檢測

依基站資安檢測技術研究規劃之檢測項目，於本計畫建構之行動寬頻基站資安檢測平臺執行檢測，並產出檢測結果。依複雜程度將檢測項目分為三大類型：一般性資安檢測、進階資安檢測和家用基站(HeNB)資安檢測。檢測之目的為驗證設備是否符合相關規範及標準，並做為擬定本計畫行動寬頻基站資安檢測規範草案之參考，其相關弱點項目、弱點評估機制及檢測結果將蒐集並儲存，建置之基站弱點資料庫。

1. 一般性資安檢測：包含基本的通訊協定測試及相關安全信令測試，及開啟與關閉 IPSec 之安全性測試。
2. 進階資安檢測：包含系統配置安全、通訊協定檢測、存取控制、滲透測試、弱點分析、機敏資訊保護及基站自發性連外異常行為分析。
3. 家用基站(HeNB)資安檢測：根據在行動寬頻基站資安檢測技術研究所設計之家用基站(HeNB)檢測項目，以六大面向執行檢測，包括身分認證安全檢測、實體層安全檢測、系統安全檢測、通訊協定安全檢測、敏感性資料保護檢測、內建軟/韌體安全檢測。
4. 建置基站弱點資料庫。

本研究將針對行動寬頻(4G LTE)基站(eNodeB)與延伸室內通訊涵蓋範圍的家用基站(HeNB)之弱點評估結果，建置一弱點資料庫進行儲存。基站一般都部署在非受控之暴露環境，同時基站也是行動寬頻(4G LTE)網路核心網路系統的主要入口，因此從風險的角度來看確實很容易成為安全上的威脅目標。此外，駭客攻擊的手法日新月異，軟硬體在設計與實作過程中都可能會出現一些非預期的錯誤，一般稱之為弱點(Vulnerability)，這些弱點有時並非可即時發現，且在正常使用下這些問題並不會影響到軟硬體的使用，但是這些弱點一旦在日後被發現，很可能會被駭客利用來影響軟硬體的運作，造成不同層級的影響，而事後補救工作或追查事件發生的原因往往要付出不少沈重的代價。

因此本工作項目將蒐集國際資安研究機構弱點資料庫(如 CVE (Common Vulnerabilities and Exposures)³⁶、NVD(National Vulnerability Database)³⁷)所發表與基站軟硬體有關之弱點資料，設備廠商對於產品安全管控上設計不良所引發的弱點問題，並參考國際安全機構所發布之安全測試指南與標準，再搭配弱點掃描與滲透測試工具對基站進行不同探測，交互比對關聯、彙整和歸納出弱點資訊至基站弱點資料庫。建置一基站弱點資料庫，內容包含可能遭受的攻擊探測資料，已經既定存在國際安全機構發布之弱點攻擊，研究文獻上提出之可能威脅、地下駭客網站提供之 Exploit code 等，以作為對不同的基站進行基本的弱點評估，及建議改善的方向。

³⁶ Common Vulnerabilities and Exposures, “CVE-2013-7395”.

³⁷ NIST 官網, National Vulnerability Database (NVD).

（六）行動寬頻基站資安檢測規範草案

為強化國內行動寬頻網路資安管理能力，參考國內外行動通信相關基站資安管理經驗及國際標準，整合本計畫之實測結果，研擬適合我國環境之檢測規範，包含檢測環境建議、檢測項目要求、檢測結果及判定標準與檢測作業程序建議，以做為未來執行基站資安檢測時之參考。

下圖說明本計畫依研究目的，說明各章節研究主題及關聯性，與產出行動寬頻基站資安檢測規範草案及未來推動建議之過程。

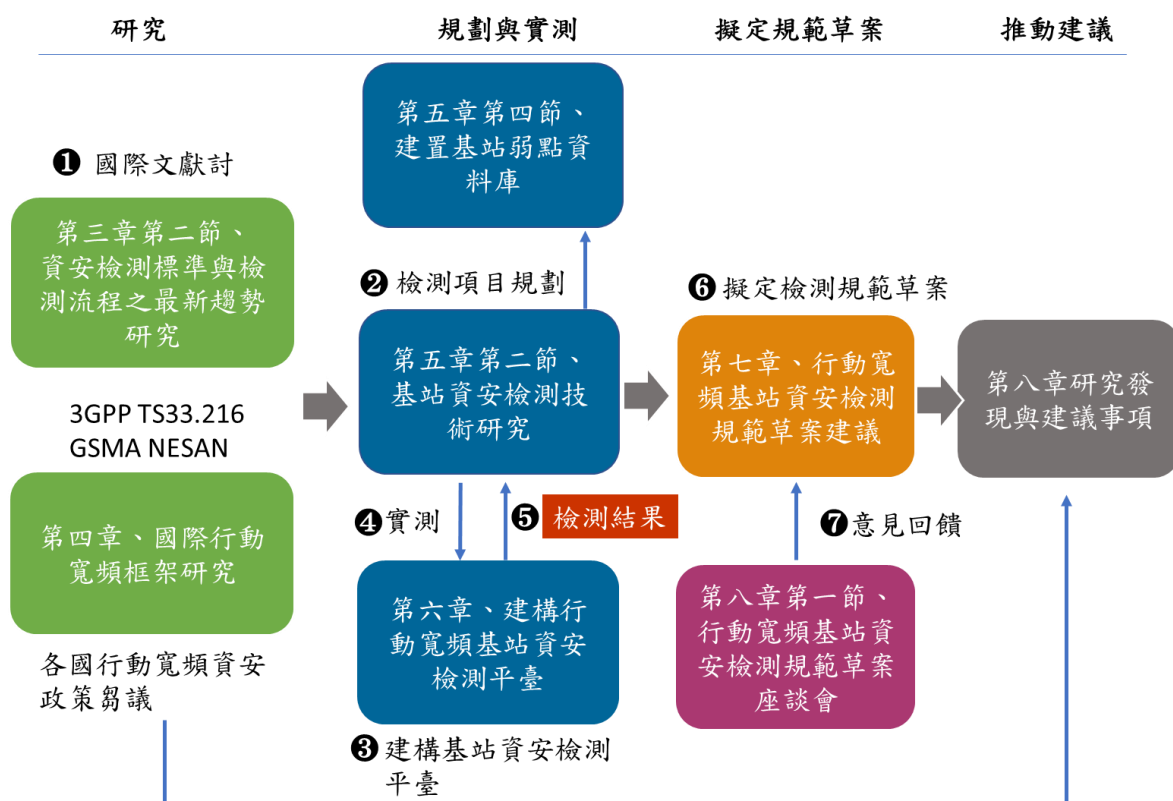


圖 2-4 各章節研究主題及關聯性

資料來源：本團隊整理

第二節 研究進度說明

一、 工作項目

本計畫透過國內外文獻研究，於期中報告提出國內外現況之前瞻性技術、國際行動寬頻資安框架、行動寬頻資安技術研究報告與建構行動寬頻基站資安檢測平臺；本團隊並於每月辦理工作進度會報，向委辦單位說明最新工作進度及研究結果。期中報告依委託研究案要求，已如期如質完成下表 2-1 之工作交付項目。

表 2-1 期中報告交付之工作項目說明

期末交付之工作項目			執行說明	章節
☑	一、前 瞻 性 資 安 技 術 研 究	(一) 國外參訪或研討	挑選國外行動寬頻網路發展較為先進之國家-芬蘭，參訪其檢測實驗室及研究中心。	附錄一：考察芬蘭行動寬頻資安檢測技術、資安最新趨勢與新興電信網路最新發展
		(二) 資安防護技術與服務之最新趨勢研究	研究最新行動寬頻網路最新資安議題與近年新興之前瞻資安議題與資安防護技術進行探討。 1.行動寬頻網路資安最新趨勢 2.資安防護技術與服務最新趨勢：主題包含SS7、5G、SDN 及 IoT	第三章第一節
		(三) 資安檢測標準與檢測流程之最新趨勢研究	深入探討與基站資安相關之國際檢測標準及檢測流程之最新趨	第三章第二節

期末交付之工作項目			執行說明	章節
			勢發展，包含 1. 3GPP 33 系列最新趨勢發展 2. GSMA 物聯網安全規範及網通設備安全認證方法 3. CC-最新通過 CC 認證之行動寬頻網路設備文件說明	
☑	二、國際行動寬頻資安框架研究	(一) 各國網路安全總體戰略、政策、法規、權責機關與任務分配。 (二) 各國推動資通安全之技術規範、參考指引與最佳實務。	介紹各國網路保全策略，與相關權責機關架構等二層面之發展狀況，以及國際間行動寬頻資安政策發展現況，作為我國規劃網路安全政策之參考基礎。 1. 美國 2. 加拿大 3. 英國 4. 歐盟 5. 日本 6. 行動寬頻資安政策芻議	第四章第一節 ~第七節
☑	三、行動寬頻資安技術研究	(一) 空中介面資安技術研究 1. 偽基站資安技術探討 2. VoLTE 資安技術探討研究	已完成偽基站資安議題研究、實驗平臺與實驗項目規劃，並於期末完成實測驗證，提出相關防護建議；另完成 VoLTE 造成基站 (eNodeB) 與核心網路 (EPC) 之可能資安威脅	第五章第一節

期末交付之工作項目			執行說明	章節
			研析，並提出建議之解決方案，及 UE 端之資安威脅及建議之解決方案。	
		(二) 基站資安檢測技術研究 1. 基站資安檢測技術及項目研究 (1) 一般性資安檢測項目研究 (2) 進階資安檢測項目研究 2. HeNB 資安檢測技術及項目研究 (1) HeNB 資安檢測項目研究 (2) HeNB 資安監測技術研究	已完成 eNodeB 及 HeNB 基站資安檢測項目規劃，所有檢測項目包含測試案例名稱、參考資料、測試目的、資訊安全需求(CIA)、測試環境暨初始條件、測試方法及合格判定標準。	第五章第二節
		(三) 核心網路-MME 資安檢測技術研究	已完成 MME 元件架構及功能研究、介面安全性研究、相關介面弱點分析及安全威脅分析。	第五章第三節
☑	四、建構行動寬頻基站資安檢測平臺	(一) 研析行動寬頻基站資安檢測平臺架構 (二) 驗證行動寬頻基站資安檢測平臺	已依所規劃之檢測平臺完成架設，並完成整合驗證測試，確認本計畫所建構之行動寬頻基站資安檢測平臺可穩定運行，且所採購之檢測工具亦可進行基站資安檢測。	第六章第一節~第三節
☑	五、行動寬頻基站資安檢測結果	(一) 一般性檢測 (二) 進階資安檢測 (三) HeNB 資安檢測	已完成第五章第二節規劃之基站資安檢測項目實測驗證，並將每一測項之檢測結果與	第五章第二節

期末交付之工作項目			執行說明	章節
	報告		檢測畫面進行詳細說明，整併於第五第二節之基站資安檢測技術及項目研究每一測項之下。	
		(四) 建置基站弱點資料庫	已依本團隊檢測之基站樣本結果，及參考NVD 國際弱點資料庫，完成基站弱點資料庫之建置。	第五章第四節
☑	六、行動寬頻基站資安檢測規範草案建議	(一) 檢測環境建議 (二) 檢測項目要求 (三) 檢測結果及判定標準建議 (四) 檢測作業程序	參照國際標準 3GPP TS33.216、TS33.320 及 TR33.820，與本計畫團隊檢測結果及座談會之訪談建議，完成行動寬頻基站資安檢測規範草案建議。	第七章第一節~第五節
☑	七、行動寬頻資安座談會及研討會辦理成果	(一) 舉辦行動寬頻基站資安檢測規範與作業程序建議座談。 (二) 舉辦行動寬頻基站資安檢測環境推動研討會	(一) 已完成 5 場電信業者，及 2 家設備製造商之座談會舉辦，並將辦理成果之會議紀錄及意見已整理至期末報告中。 (二) 已完成 1 場行動寬頻基站資安研討會之舉辦，研討會之相關簡報、紀錄及意見已整理至期末報告中。	第八章第一節~第三節

資料來源：本團隊整理

二、 研究進度

為配合前述研究議題與研究方法之落實推動，依據委託契約之要求，本計畫於契約生效次工作日起 150 日內(106 年 10 月 27 日)提出期中報告，契約生效次工作日起 360 日內(107 年 5 月 25 日)提出期末報告，本研究完整進度甘特圖如表 2-2。

本團隊依據原規劃之研究進度，在前瞻性資安技術研究，已完成資安防護技術與服務最新趨勢研究，蒐集資安最新攻擊及防護趨勢，期末深入資安檢測標準與檢測流程趨勢進行研究，蒐集與研析 3GPP 行動寬頻資安規範基站相關之 33 安全系列最新發展、GSMA 之物聯網安全推範及網通產品之安全保證方法、與共通準則(Common Criteria，簡稱 CC)與行動寬頻網路產品之最新資訊安全基本文件。國外參訪業於 106 年 9 月底完成芬蘭國家技術研究中心(VTT)、電信設備製造商 Nokia Security Center 及行動寬頻資安檢測軟體開發商 Synopsys R&D Center 參訪行程，參訪所得資訊及經驗已歸納並撰寫至期末報告中。

針對行動寬頻資安技術研究，期中完成空中介面之偽基站實驗項目設計、VoLTE 之初步研究，期末完成空中介面之偽基站實驗，產出资安威脅研析與解決方案，與 VoLTE 造成用戶端之資安威脅和現有解決方法；在基站資安檢測技術及項目研究中，參考 3GPP 於 106 年 9 月最新之 TS33.216 規範，重新調整本計畫基站資安檢測項目之規劃，提出 37 項之基站資安檢測項目及 41 項之 HeNB 資安檢測項目，並於期中建構之行動寬頻基站資安檢測平臺完成實測，產出檢測結果報告與基站弱點資料庫。

最後透過國外參訪蒐集國際經驗，及座談會蒐集國內電信業者及基站設備製造商之意見，提出適用於國內之行動寬頻資安檢測規範草案與檢測作業流程。本團隊也以研討會方式推廣本計畫建議之行動寬頻檢測規範與流程，並分享與展示行動寬頻基站資安檢測環境，於研討會中也得到熱烈的迴響與交流。

表 2-2 研究進度甘特圖

( 完成進度)

工作項目	第一月	第二月	第三月	第四月	第五月	第六月	第七月	第八月	第九月	第十月	第十一月	第十二月
1. 前瞻性資安技術研究												
1.1. 資安防護技術與服務最新趨勢研究												
1.2. 資安檢測標準與檢測流程最新趨勢研究												
1.3. 國外參訪及研討												
2. 國際行動寬頻資安框架研究												
2.1. 各國網路安全總體戰略、政策、法規、權責機關與任務分配												
2.2. 各國推動資通安全之技術規範、參考指引與最佳實務												
3. 行動寬頻資安技術研究												
3.1. 空中介面資安技術研究												
3.1.1. 偽基站資安技術探討												
3.1.2. VoLTE 資安技術探討												

工作項目	第一 月	第二 月	第三 月	第四 月	第五 月	第六 月	第七 月	第八 月	第九 月	第十 月	第十一 月	第十二 月
3.2. 基站資安檢測技術研究												
3.2.1. 基站資安檢測技術及項目研究												
3.2.2. 家用基站(HeNB)資安檢測技術及項目研究												
3.3. 核心網路-MME 資安檢測技術研究												
4. 建構行動寬頻基站資安檢測平臺												
4.1. 研析行動寬頻基站資安檢測平臺架構												
4.2. 建構行動寬頻基站資安檢測平臺												
5. 行動寬頻基站資安檢測												
5.1. 一般性檢測項目												
5.2. 進階資安檢測項目												
5.3. 家用基站(HeNB)資安檢測項目												
5.4. 建置基站弱點資料庫												
6. 行動寬頻基站資安檢測規範草案												

工作項目	第一月	第二月	第三月	第四月	第五月	第六月	第七月	第八月	第九月	第十月	第十一月	第十二月
6.1. 檢測環境建議												
6.2. 檢測項目要求												
6.3. 檢測結果及判定標準建議												
6.4. 檢測作業程序												
7.辦理行動寬頻資安座談會及研討會												
7.1. 舉辦行動寬頻基站資安檢測作業程序座談會												
7.2. 舉辦行動寬頻基站資安檢測環境推動研討會												
工作進度估計百分比 (累積數)	5	10	15	25	35	40	50	60	70	80	90	100
預定查核點	1. 於契約生效次工作日起150日內提出期中報告。 2. 於契約生效次工作日起360日內提出期末報告(完整研究報告初稿)。 3. 期末審查完成後，依通傳會指定期限內提出完整期末報告。											

工作項目	第一 月	第二 月	第三 月	第四 月	第五 月	第六 月	第七 月	第八 月	第九 月	第十 月	第十一 月	第十二 月
預定交付項目	1. 期中報告 ➤ 前瞻性資安技術期中研究結果 ➤ 國際行動寬頻資安框架研究結果 ➤ 行動寬頻資安技術期中研究結果 ➤ 建構行動寬頻基站資安檢測平臺 2. 期末報告(包含期中報告完成之工作項目) ➤ 前瞻性資安技術研究結果 ➤ 國際行動寬頻資安框架研究 ➤ 行動寬頻資安技術研究結果 ➤ 建構行動寬頻基站資安檢測平臺 ➤ 行動寬頻基站資安檢測結果與說明 ➤ 建置基站弱點資料庫 ➤ 行動寬頻基站資安檢測規範草案 ➤ 行動寬頻資安座談會及研討會辦理成果											
說明： 1. 完成進度以粗線表示其起訖日期。 2. 團隊每月辦理工作進度會報，向委辦單位說明最新工作進度及研究結果。												

第三章、 前瞻性資安技術研究

當前資訊社會行動寬頻網路已普及，且為了滿足使用者對於網路的更高需求，未來第五代行動通訊技術的演進，將實現更高速及便利的新興網路時代，其所帶來的網路架構變化及物聯網應用的普遍也將影響所有人的生活及安全。

然而建立新興網路環境前需釐清其環境及其技術內部架構、奠定各方標準以及基本的安全措施，以保障消費者之資訊安全，因此本計畫前瞻行資安技術研析將針對近年炙手可熱的行動寬頻網路資安事件、新興行動寬頻網路演進及物聯網應用之相關資安防護技術與服務之最新趨勢。

第一節 資安防護技術與服務之最新趨勢研究

本團隊蒐集近兩年主要之行動寬頻網路資安事件發現，近年國際上行動寬頻網路之資安事件多發生在物聯網(Internet of Things，簡稱 IoT)及 SS7 通訊協定漏洞上，因此本團隊於本節將先介紹近年行動寬頻網路最新資安議題，再深入近年新興之前瞻資安議題與資安防護技術進行探討，主要包括以下四大主題：1. SS7 Link 通訊協定漏洞；2. 第五代行動通訊系統(5th Generation Mobile Network，簡稱 5G)；3. 軟體定義網路(Software-defined networking，簡稱 SDN)；4. 物聯網(Internet of Things，簡稱 IoT)。

由於新世代的形成是奠基於以往的網路環境，在前瞻性資安技術研究之資安防護技術與服務最新趨勢研究中，本團隊首先統整近年重大電信資安事件，再深入研析上述每一主題之架構，彙整各項攻擊趨勢及其防護技術。

一、 行動寬頻網路資安最新趨勢

本團隊整理近兩年行動寬頻網路資安事件(如表 3-1)中發現，近年主要攻擊目標有三大類，包含 SS7 通訊協定、偽基站及物聯網設備，其中物聯網設備之攻擊已是近年發生最為頻繁的攻擊目標，在攻擊方式上，SS7 及物聯網之攻擊係利用相關漏洞進行攻擊及惡意程式入侵，而偽基站則是利用 3GPP 在 LTE 網路選擇較強訊號基站的標準，架設偽基站，攔截或傳送簡訊給用戶。

表 3-1 近年行動寬頻網路資安事件整理

來源/時間	事件	描述
cryptocoinsnews ³⁸ , 2017/9/22	Stealing Bitcoin with a Name and a Phone Number	Positive Technologies 研究人員展示透過一個姓名及電話號碼，駭客就能取得某用戶的 Google 帳號，且進而取得該用戶個人的比特幣帳號或銀行帳號。駭客即利用全球漫遊網路中 SS7 的漏洞，來竊取比特幣帳號，此漏洞將造成比特幣用戶非常大的威脅。
iThome ³⁹ , 2017/07/27	黑帽駭客大會： 3G/4G 網路協定漏洞可能洩露用戶行蹤，目前無解	於 2017 年 7 月中所舉辦的黑帽駭客大會(Black Hat Conference)中，參與人員提出目前的 3G/4G LTE 網路，在基地台證明手機用戶端的驗證過程中，會依憑電信系統中的計數器完成，但由於電信系統中的加密協定存在漏洞，導致計數器資訊暴露於眾人之下，且可利用國際移動用戶識別碼擷取器(IMS I catcher)，成功騙取用戶的使用手機軌跡資訊以及目前行蹤。
蘋果日報 ⁴⁰ , 2017/6	物聯網資安攻擊加劇，常見 IP CAM 成資安漏洞	日前美國聯邦貿易委員會(FTC)指控廠商廣告不實，我國知名廠商的無線路由器和攝影機存在嚴重安全瑕疵，駭客攻擊已不再只是等民眾上鉤，舉凡能夠連網的產品，都可能是資安攻擊目標，企業必須加速落實智慧聯網(IoT)隱私與安全保護。駭客攻擊模式與時俱進，隨著物聯網時代來臨，相

³⁸ cryptocoinsnews, “Stealing Bitcoin with a Name and a Phone Number”, 2017/9/22.

³⁹ 林妍臻, “黑帽駭客大會：3G/4G 網路協定漏洞可能洩露用戶行蹤，目前無解”, 2017/7/27.

⁴⁰ 蘋果日報, “物聯網資安攻擊加劇,常見 IP CAM 成資安漏洞”, 2017/6/8.

來源/時間	事件	描述
		關應用潛藏的資安危機，資安專家指出，9 成漏洞的弱點來自軟體開發，企業將如何自保防範，實是刻不容緩議題。
iThome ⁴¹ , 2017/5/13	勒索軟體 WannaCry 於 2017 年 5 月大規模感染全球	WannaCry 勒索蠕蟲第二代才大肆侵入各國，受感染的用戶會被要脅於一定時間內必須付出 300 比特幣，否則將付出加倍金額才有可能解密檔案。此種攻擊主要是針對為大眾最常使用的作業系統 Windows，其中的安全漏洞侵入電腦，目前統計至少有 150 國家受到感染，超過 30 萬台電腦受感染，其中影響最大的國家分別為俄羅斯、烏克蘭及台灣。
SC MEDIA, 2016/05/13 ⁴²	SS7 vulnerability defeats WhatsApp encryption, researchers claim	安全公司 Positive Technologies 的電信網路專家模擬利用 SS7 漏洞冒充用戶接收訊息。使用了一台運行 Linux 的筆記型電腦和一個能與 SS7 協議交互的 SDK。新的攻擊方法不是破解而是繞過了如 WhatsApp 和 Telegram 等應用的加密。新的攻擊對 Telegram 的影響更大，因為 Telegram 不使用點對點加密，而是明文儲存了用戶接收和發送的所有歷史訊息，因此攻擊者可以立即看到這些訊息。相比之下，WhatsApp 使用點對點加密，攻擊者無法存取到歷史訊息。

⁴¹ iThome, "WannaCry 進化為蠕蟲，勒索軟體殺傷力大增", 2017/5/22.

⁴² SC MEDIA, "SS7 vulnerability defeats WhatsApp encryption, researchers claim.", 2016/5/13.

來源/時間	事件	描述
iThome, 2017/5/5 ⁴³	駭客利用電信業者 SS7 協定漏洞破解雙因素認證，手機用戶的銀行帳戶遭盜領一空	德國媒體報導一駭客先以銀行木馬感染被害者的電腦，取得其銀行帳戶的密碼，再以遠端電腦登入帳戶後，利用 SS7 的漏洞攔截了銀行傳給手機用戶的行動交易認證碼（mobile transaction authentication number，簡稱 mTAN），將帳戶的金額轉出，該事件已有許多西班牙電信用戶受害，採用雙因子認證之電子銀行皆會受到此種攻擊的威脅。
The Hacker News, 2017/3/22.	Hackers Using Fake Cellphone Towers to Spread Android Banking Trojan	Check Point Software 報導指出，中國大陸發生第一起利用偽基站設備，假冒電信業者(如中國移動及中國聯通)名義發送簡訊，傳播惡意程式"Swearing Trojan"的案例，該惡意程式為 Android 之惡意木馬程式。 Swearing 木馬程式可從受感染的設備收集用戶個人資訊及相關認證資訊，甚至攔截簡訊(SMS)訊息，截取銀行機構使用的雙向認證或其它一次性代碼等。Check Point 認為，透過偽基站傳送 SMS 訊息是很容易欺騙用戶的一種方式，利用 Swearing 惡意程式的攻擊活動若是透過偽基站方式誘騙用戶，將可能進一步推動此惡意程式的蔓延。

⁴³ iThome, “駭客利用電信業者 SS7 協定漏洞破解雙因素認證，手機用戶的銀行帳戶遭盜領一空”，2017/5/5.

來源/時間	事件	描述
iThome ⁴⁴ , 2017/2	為甚麼學校的印表機會被入侵	今年 2 月，台灣校園收到駭客勒索的詐騙信，當時媒體公布有 46 間學校受害，這是因為學校通常都將列印設備暴露在外部 IP 之下，只要有心人士有辦法搜尋到這台印表機的 IP 位置，然後將印表機的語言包裝成網路封包，透過 9100 的埠傳送到印表機，因此印出的內容都是文字編碼。
theguardian ⁴⁵ , 2016/10	DDoS 攻擊中斷互聯網(Mirai)	Dyn 是 DNS 提供商之一。2016 年 10 月 21 日，Dyn 公司於受管 DNS 服務器上遭受 DDoS 攻擊，從 100,000 個啟用網路的 IoT 設備（如印表機、IP 攝影機、住宅 gateway 和嬰兒監視器），通過 port 53 生成 TCP 和 UDP 流量，據一些專家介紹，攻擊強度達到了 1.2Tbps，但並沒有得到 Dyn 的確認。
Freebuf ⁴⁶ , 2016/10/2	Uber 身分安全漏洞被發現，個人密碼存在風險	義大利安全專家 Vincenzo C. Aka 發現 Uber 身分安全漏洞，該漏洞為只須擁有一個合法 Uber 帳戶的電子郵件位址即可任意存取該帳戶。專家發現，只要傳送重設密碼請求，會收到一個 inAuthSessionID"session token，而此 token 可以更改任何帳戶的密碼。Uber 於 2016/10/6 以將此漏洞修復，並與此義大利專家合作，希望能夠發現更多 Uber 平台上的漏洞。

⁴⁴ iThome, “【IoT 攻擊無所不在】為什麼學校印表機會被入侵？”, 2017/5/27.

⁴⁵ theguardian, “DDoS attack that disrupted internet was largest of its kind in history, experts say”, 2016/10.

⁴⁶ Da Feed, "A critical Improper Authentication vulnerability in Uber allowed password reset for any account", 2017/5/18.

來源/時間	事件	描述
KrebsOnSecurity ⁴⁷ , 2016/9/21	KrebsOnSecurity 網站遭受 DDoS 攻 擊事件(Mirai)	2016 年 9 月 30 日，安全研究員 Brain Krebs 的部落格遭受來自大量 IoT 設備 623Gbps 的 DDoS 攻擊，這個攻擊事件被認為是來自一群駭客們針對 Krebs 的文章中揭露了以色列的 DDoS 攻擊服務商 vDOS 的創辦人遭受逮捕的報復行動。Krebs 是 CDN 電信業者 Akamai 的免費客戶，負責提供 DDoS 攻擊保護。由於 DDoS 舒緩工作開始對 Akamai 的付費客戶造成問題，Akamai 終止了與 Krebs 的無償合約。
iThome ⁴⁸ , 2016/7/25	一銀 ATM 遭駭客 入侵，自動從 ATM 吐鈔	第一銀行台北和台中發生總計 22 家分行 41 台提款機的所有內存款項遭人清空，被盜領的總金額高達 8,327 萬 7,600 元，駭客透過植入木馬及散播惡意程式方式，以一臺第一銀行倫敦分行內鎖在鐵櫃中的電話錄音伺服器主機，遠端遙控 ATM 吐鈔。
The Hacker News, 2016	Mirai 惡意程式入 侵物聯網(IoT)裝 置	DDoS 攻擊為 2016 年較常出現的攻擊手法，而導致此攻擊的元凶為 Mirai 惡意程式。此程式讓使用者裝置成為殭屍裝置進而發起 DDoS 攻擊，因此許多物聯網裝置受害，如監視攝影機、家庭網路設備及路由器等被攻擊的實際案例。
Trend Micro ⁴⁹ ,	發現高達 12 萬台	2016 年趨勢科技發現全球的高達 1,000

⁴⁷ KrebsOnSecurity, “KrebsOnSecurity Hit With Record DDoS”, 2016/9/21.

⁴⁸ iThome, “【詳細圖解】駭客入侵一銀 ATM 流程追追追”, 2016/7/25.

⁴⁹ TREND LABS 趨勢科技全球技術支援與研發中心, “< IOT 物聯網 >多達 1,000 多種型號,12 萬臺網

來源/時間	事件	描述
2016	網路攝影機，遭受 Persirai 殭屍病毒侵入攻擊	種型號的網路攝影機遭到 Persirai 殭屍病毒侵入感染。攻擊者藉由惡意軟體 Mirai 作為媒介，入侵 CCTV 攝影機和數位錄影機(DVR)，將其作為踏板進行分散式阻斷服務攻擊(DDoS)。
數位時代 ⁵⁰ , 2016	Gogoro 三大資安風險揭密，小心所有物聯網產品！	2016 年在 Hitcon 發表了有關 gogoro 的資安風險，發表者表示，gogoro 本身的安全機制沒有問題，但是手機很不可靠，比晶片鑰匙還不安全，所以需要更慎重設計機制來保護軟體通訊安全，並且提出三點關於 gogoro 的 APP 的一些資安弱點：APP 中的金鑰被存在不安全的目錄下、APP 到雲端的 SSL 加密有檢查的問題、每一次重新配對不會換新的金鑰，這些都說明了在物聯網中關於資安的重要性。
科技新報 ⁵¹ , 2015/12/23	烏克蘭電廠遭駭客入侵，為世界首例因駭客入侵而造成大規模停電的案例	烏克蘭電力網路遭到駭客入侵，造成數十萬戶沒電可用。事後調查，此攻擊主要透過網路釣魚方式，取得登入權限，透過遠端操控軟體登入，切斷電力接著將密碼改掉，造成合法員工無法登入，因此無法及時找出停電主要的原因。

資料來源：本團隊整理

路攝影機,恐受殭屍病毒 Persirai 感染”, 2017/5/11.

⁵⁰ 數位時代,“Gogoro 三大資安風險揭密，小心所有物聯網產品！”, 2016/7/25.

⁵¹ 科技新報,“烏克蘭電力系統遭駭原因是網路釣魚，如何加強資安防護引討論“, 2016/4/26.

二、資安防護技術與服務最新趨勢

(一) 第七號信令系統(SS7)

1. 架構說明

第七號信令系統（Signaling System 7，簡稱 SS7）為一套網路的信令協定，屬於 CCS⁵²（Common Channel Signaling）此種透過 out-of-band signaling protocol⁵³提供網絡節點通訊服務的訊號系統，及使用彈性極高的網路拓樸（Network Topology）來建設網路。許多通訊系統之核心網路，如較早期的 AMPS（Advanced Mobile Phone System，類比式行動電話系統）、GSM（Global System for Mobile Communication，全球行動通訊系統）等等無論是 PSTN⁵⁴（Public Switched Telephone Network）或者 PCS⁵⁵（Personal Communications Services）均會採用 SS7 的運作模式。

SS7 是一種局間信令系統，不負責用戶終端和局端之間用戶線上面信令的傳輸和處理，只負責局交換機之間、局交換機和其他電信設備之間的信令傳輸和處理。和其他信令系統一樣，SS7 不負責進行具體語音訊號的傳輸，但是它負責協調各種電信設備，使各種電信設備能夠準確地建立語音鏈路，為用戶提供服務。

SS7 所建構的通信漫遊網路，早被廣泛運用在 2G、3G 網路漫遊通訊中，但多數使用 SS7 均未考量各局端相互之間的認證、傳輸過程加密與資訊完整性檢測，在沒有任何防禦機制的保護下，可能遭受許多的攻擊，例如有竊聽、位置追蹤、詐騙、服務阻斷、信譽損失、資料通訊劫持、網路帳號/密碼竊取(部分網路服務是透過簡訊傳遞驗證訊息，如:高鐵購票刷卡驗證碼)等。

因此近年有許多資安事件的案例，係發生在利用 SS7 存在的協議漏洞使得駭客繞過特定身分驗證過程，獲得更多權限進行惡意的攻擊，然而此協定被運用在全球漫遊之信息交換、跨電信業者之計費等功能，根據 2016 年之統計，全球約有 800 多各電

⁵² Dialogic, “Common Channel Signaling (CCS)”.

⁵³ Malathi Veeraraghavan, Haobo Wang, “A Comparison of In-Band and Out-of-Band Transport Options for Signaling”, IEEE, 2005/4/18.

⁵⁴ Lifewire, “PSTN (Public Switched Telephone Network)”, 2017/3/14.

⁵⁵ TechTarget, “PCS (personal communications service)”.

信業者正在使用 SS7 協定來提供漫遊服務⁵⁶。

因各國國內電信業者與國外的電信業者 SS7 信令網路是各自獨立的，且其信令節點的編碼(signaling point codes，簡稱 SPCs)格式也不同，所以不同電信業者必須使用 SS7 信令系統中的 STPs (Signaling Transfer Points) 進行連接及轉送訊息。

而在討論這些攻擊及如何防範之前，必須先清楚了解 SS7 之架構，在 SS7 信令系統中，為了處理 SS7 之信號並傳遞，形成了名為「SS7 network」的網路架構，其中主要由三個部分所組成，分別為：

- **SSPs (Service/Signal Switching Points)**

從網路中的語音線路中收集相關控制信號，並將其轉換為 SS7 信令訊息。而這些數據包會傳送到 SS7 network 中，進而送到各個目的元件以供處理。除此之外，SSP 也扮演著交換機的角色，通話建立及終止甚至費用之計算資料收集均由 SSP 負責。

- **STPs (Signaling Transfer Points)**

採用 Packet Switching，透過 SS7 中訊息包含的位址資訊，扮演路由器的角色，專門確認信號單元之目的地以及對應之 link，進一步轉送 message，且主要形式為成對出現。

- **SCPs (Service/Signal Control Points)**

會接收到 SSP 所傳來的訊息，再指派對應之處理方式給 SSP，可視為一個資料庫，提供類似 0800 免付費電話或者與 VLR (Visiting Location Register 及 HLR (Home Location Register) 有關之功能，且亦為成對出現。

SS7 network 還包含了連接上面三個 points 的主要 links，而這些 links 又分為六種：A-link、B-link、C-link…F-link，且這些 links 均採用 56-kbps 或 64-kpbs，主要不同之處在於他們連接節點的不同，三大節點與連結 link 間的關係圖如圖 3-1)。

(1) A-link (Access Link)

-連接：STP-SCP/SSP

⁵⁶ The Hacker News, “How to Hack Someone’s Facebook Account Just by Knowing their Phone Numbers”, 2016/6/15.

-SSP 及 SCP 均至少會有一條連接成對的 STP (STP pair) 以用來傳送訊息。

(2) B-link (Bridge Link)

-連接：STP-STP

-與兩個不同 STP pair 中的 STP 相連。

(3) C-link (Cross Link)

-連接：STP-STP

-與 B-link 不同之處在於，此為連接同個 STP pair 中的兩個 STP，為加強 SS7 network 的可靠性(reliability)，以防有 links 發生問題，平時主要傳送 status message。

(4) D-link (Diagonal Link)

-連接：STP-STP

-與 B-link 不同之處在於，此為連接不同網路供應商 (vendor) 之間的 STP pair，PSTN 及 PCS 均屬於此類。

(5) E-link (Extended Link)

-連接：STP-SSP

-當通話流量增多時，除了 A-link 連接的 SSP，亦可使用這條來增加網路的可靠性(reliability)。

(6) F-link (Full-associated Link)

-連接：SSP-SSP

-兩相異設備不需經由 STP 即可相連。

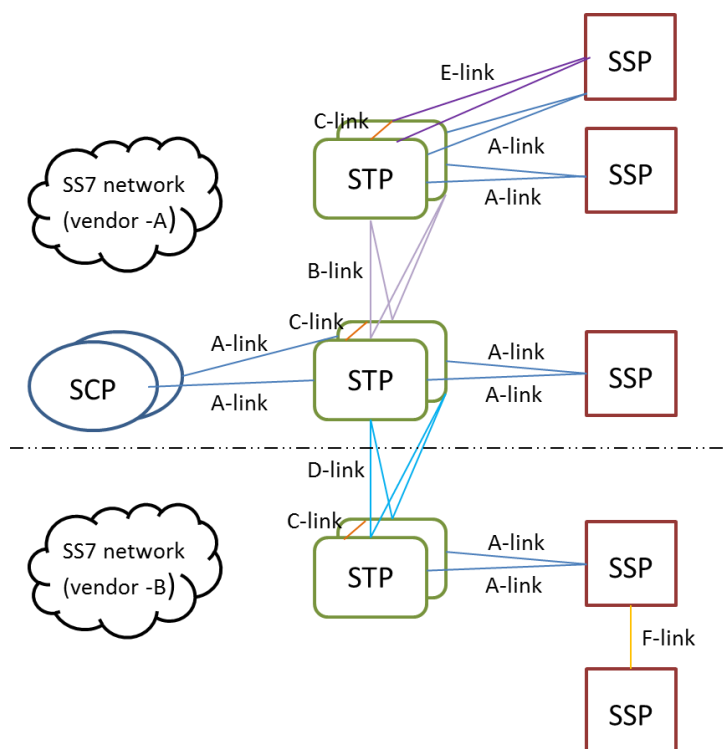


圖 3- 1 SS7 之節點與連結 link 之關係圖

資料來源：Rahnema, Moe. "Overview of the GSM system and protocol architecture."

IEEE Communications magazine 31.4 (1993): 92-100.

SS7 信令系統採用多個協定的堆疊模式，每個 layer 的相關協定所對應之開放式系統互聯通訊參考模型（Open System Interconnection Reference Model，簡稱 OSI）中七層的層次對應之架構圖如圖 3-2，各協定之說明如下。

● MTP（Message Transfer Part）

SS7 中最底層的階級，如名稱所示，主要負責將 SS7 message 順利地從來源端傳送到目的地，並細分成三個 level，MTP-Level1~MTP-Level3。

(1) MTP-Level1

提供信號連線中兩端節點（signaling terminal）link 及傳送信號的 bear 實體設定。

(2) MTP-Level2

經由 MTP-Level1 所提供的實體設定，建立相鄰元件的連結，並定義 signaling link 的功能特性，其中包含信號單元校驗(alignment)、信號單元誤碼更正(error correction)、流量控制（flow control）等等，而 MTP-Level2 會處理特定之信號單元，並將其餘轉

傳至 MTP-Level3 做下一步的處理。

(3) MTP-Level3

除了確保訊息可以經由 STPs 順利傳送到目的地，也負責監控管理 SS7 network 是否正常運作，當有 link 損壞時，必須做 load sharing，使訊息能夠從別條 link 重新傳送(rerouting)，並且發送特定指令，例如 MTP-Transfer request、MTP-Transfer indication、MTP-Status indication 等，與上層其他協定進行訊息狀況或者目的地等的確認，若訊息有誤，會查出對應之 signaling link，進一步轉傳至適當元件。

● SCCP (Signaling Connection Control Part)

為了完善路由工作之處理，主要提供兩個功能，如下：

兩個不同網路間進行實體訊息來往之功能：有別於 MTP 只允許在同個營運網路下進行資訊的交換，SCCP 能夠在無法識別對方信令位址⁵⁷ (point code) 的狀況下，透過 GTT⁵⁸ (Global Title Translation) 此種特殊定址方式，接收手機的相關資訊，從資料庫找出對應的目的地位址 (point code)，進而達成兩個不同網路間進行實體訊息來往之功能。

轉傳不必經由骨幹網路(trunk)進一步控制的電路無關之信令⁵⁹ (non-circuit-related signaling)，以及查詢用戶端資料或者網路控管等其他服務的信令，進一步提升效能。

(1) ISUP (ISDN User Part)

其中訊息會在交換機之間互相傳送，主要提供建立通話線路 (call- setup) 及通話結束 (teardown) 等基本載送服務，而通訊系統中，通話的建立速度極其被重視，所以此協定中的訊號對於時間掌控上的要求會相較其餘協定更為強烈。此外，雖然是為了服務 ISDN (Integrated Services Digital Network) 此種透過現有之通話線路高速傳送訊息的技術而衍伸出來，但在 ISDN 或 non-ISDN 的通話上都是可以被使用的。

(2) TCAP (Transaction Capability Application Part)

管理兩個節點間上層的 OMAP 及 MAP 中交易與操作的流程，包含 0800 免付費

⁵⁷ aculab, "What are point codes in SS7?"

⁵⁸ Tekelec, "Database Administration Manual - Global Title Translation", 2012/1

⁵⁹ IEEE Digital Library, "Non-Circuit-Related Signalling".

電話、大數據資料傳送等等，再透過這些交易去進行服務，使他們可以要求對方給予回應並且提供操作。

(3) OMAP (Operation Maintenance Administration Part)

協助網路管理，可以驗證網路路由表並且診斷 link 故障時之問題所在。

(4) MAP (Mobile Application Part)

處理與行動通訊有關之應用服務，GSM MAP 即為此層之應用。

(5) TUP (Telephone User Part)

提供 PSTN 此種傳統公共電話網路服務，相較 ISUP 更為簡易，然而因為沒有服務 ISDN，已漸漸被 ISUP 所取代。

SS7 network 的基本架構除了上面所提及的基本元件及連結 link，另外還包含在此網路中所傳送的訊息封包，稱為信號單元 (Signal Units，簡稱 SUs)，並分為三種：

(1) LSSUs (Link Status Signal Units)

在 SS7 信令堆疊的 MTP-Level2 中所負責處理之信號單元，主要負責網路控管，並且傳送相鄰節點鏈結的狀況資訊。

(2) FISUs (Fill-In Signal Units)

與 LSSUs 相同位於 MTP-Level2 之網管處理的信號單元，而如同它的命名般，當信號節點沒有 LSSUs 要傳送時，便會傳送 FISUs，讓兩邊連線持續保持忙碌(fill in link)，此外，他也會測試傳送之訊息是否有被對方準確依序的接收到。

(3) MSUs (Message Signal Units)

傳送至 MTP-Level3 所處理之信號單元，相較於 LSSUs 及 FISUs 多一個彈性空間可以封裝別層所傳來之通訊協定相關資料，並且主要透過 STP 轉送。

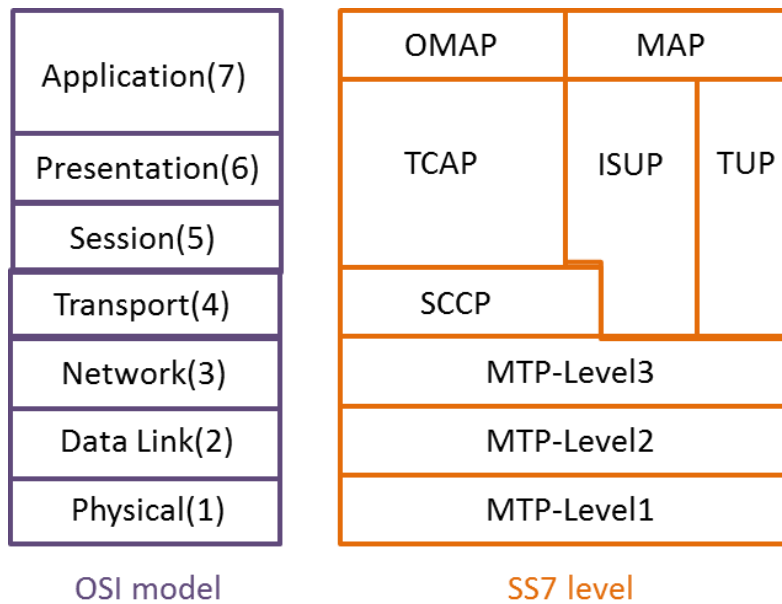


圖 3- 2 SS7 協定堆疊對應 OSI 架構圖

資料來源：Rahnema, Moe. "Overview of the GSM system and protocol architecture." IEEE Communications magazine 31.4 (1993): 92-100.

2. 攻擊流程

SS7 所建構的通信漫遊網路，早被廣泛運用在 2G、3G 網路漫遊通訊中，但多數使用 SS7 均未考量各局端相互之間的認證、傳輸過程加密與資訊完整性檢測，在沒有任何防禦機制的保護下，SS7 協定漏洞所造成的威脅，包含有竊聽、位置追蹤、詐騙、服務阻斷、信譽損失、資料通訊劫持、網路帳號/密碼竊取(部分網路服務是透過簡訊傳遞驗證訊息，如網路銀行轉帳交易、線上刷卡)等。SS7 主要的網路漏洞，與一般網路安全問題相似，其威脅會隨著元件數量及複雜度升高，此外，進階的服務通常都會有一些固有的漏洞，例如：攻擊者可以利用修改 SCP 來轉發目的地，進而攻擊轉接服務。以下從 SS7 三個節點 SSPs、STPs、SCPs 的四種型態的攻擊修改、竊聽、阻斷、偽造(如圖 3-3)，分別進行詳細說明如下。

(1) SSP 攻擊

SSPs 是生成 SS7 網路的參數也是遭受攻擊的開道，大部分的攻擊都是利用 SS7 比較弱的認證環節進行攻擊，例如：ISDN 是設計來連接 SS7 節點到用戶端，是可以讓用戶端連接到 SS7 網路之中，惡意的 ISDN 使用者可以修改或是偽造 ISUP 的訊息，

的確，ISDN 的連結看起來像是合法單位設計的，但其成本非常之低，所以很多惡意用戶端都可以取得。

所以有 SS7 的網路元件都容易受到網路探測的影響，然而 SSP 是一個網路探測的主要目標，因為每個用戶端的流量都會經過相對應的 SSP，攻擊者可以竊聽並且將自己的目的地加到訊息中的原始目的地，來攔截用戶的訊息，做法與 ARP 攻擊相似。

SSP 就像是所有網路的元件一樣，都有最大的服務負荷量，如果超過了 SSP 與 STP 之間連結的負荷量之後，就可以阻斷了 SSP 服務，進而拒絕用戶的請求，攻擊者也可以中斷所有的數據流以及對於目標用戶修改要求連接的 SSP，簡而言之就是 DDoS 攻擊，而此種攻擊對於越來越容易的網路探測技術中，將變得更難以防護。

(2) STP 攻擊

STP 主要扮演中間轉傳的角色，幾乎所有訊息都會經過 STP，所以其資訊安全是非常重要的地方。

SSP 的訊息會直接通過 STP，此外，攻擊者將可以通過探測 SSP 來知道所有經過 STP 的流量，更複雜的遠端攻擊入侵到了 STP，攻擊者會偽造假的 STP 來代替原本的 STP 轉傳以及過濾流量，或是修改 SCCP(end-to-end)訊息原本的目的地來允許對應的電話呼叫(或是資料庫存取)，所以攻擊者可以鎖定交談並且竊聽。

自從 OSS(Operations support system,業務支撐系統)連接上 STP 之後，就可以藉由取得 OSS 的控制權，來進行計費欺騙，GT(Global title)數字是由呼叫者提供受話者地址給網路端，就算 SCCP 將 GT 轉換成適當的點代碼，這些數字也不會提供點代碼或是子系統編號，SCCP 裡面包含著 GT 的訊息一定會經由 STP 轉發，也會被轉換成真正的點代碼再傳到 SCP，GT 轉換的點代碼是一個非常敏感的資訊，為了保護裡面的訊息，GT 要求來源的訊息只能提供通用的訊息，再利用 STP 來轉換成特別的點代碼，如果 STP 遭到入侵，那就會藉由存取相對應的 SCP 來取得內部網路節點的點代碼，另一種攻擊可以去修改保存在 STP 裡面的 GT 資料庫。

STP 和 SCP 負責維護本地號碼可攜性(local number portability,簡稱 LNP)的資料庫，資料庫裡面存的是一些路由器的呼叫，LNP 資料庫在查詢上是需要耗費很大的資源，因此，LNP 如果過載是一個很大的威脅，攻擊者會產生大量的資料庫查詢，讓 STP 跟 SCP 癱瘓，此外，在 LNP 資料庫中的電話號碼也有可能被修改或刪除。

SS7 中 MTP 的第三層的協定提供了一個複雜的資料流向管理，消息信令單元 (Message signaling units, 簡稱 MSUs) 如果發現了一個已經失效的點，此單元會通知此節點附近的其他節點，並且會重新發送到其他新的節點並且重新給出一個路徑，偽造的 MSUs 可以使一班正常運作的節點無效化，導致網路壅塞進而癱瘓網路。

(3) SCP 攻擊

SCP 的資料庫儲存很多敏感訊息，是非常脆弱，舉例來說，call management services databases (CMSDB) 就是處理免費電話的資料庫，免費電話不代表實際的電話被撥打了，反而應該是免費電話對應到一個實際的電話號碼，而計費是另外計算，CMSDBs 儲存了電話跟帳單之間的對應關係，攻擊者透過改變目標的電話號碼成其他電話號碼，因此便能將目的地端的費用消除，相同地，免費電話的擁有者也可以改變帳單資訊，來規避費用。

相同的修改方式，也可以利用在其他跟計費有關的資料庫中，例如 line information databases (LIDBs) 等資料庫，LIDB 維護的是使用者的資訊，包含了帳單、電話卡服務、驗證及 PIN 碼，惡意的用戶端如果存取這個資料庫，便可以進行個資竊取到收費詐騙，例如：攻擊者可能修改帳單數量、竊聽甚至修改 PIN 碼。

許多 SCP 攻擊是使用 TCAP 的訊息來存取及修改 SCP 的資料庫，例如：攻擊者可以在 TCAP 的訊息裡修改用戶端的帳號來規避費用，同樣的，用戶端的 PIN 碼也可以被特定的 TCAP 的要求訊息所獲得。

聲音郵件的資料庫也有類似的弱點，攻擊者可以寄 TCAP 查詢訊息來獲得用戶端密碼，來取得郵箱的存取權。

SCP 的資料庫也容易遭受的阻斷式服務攻擊，一個被入侵的 SCP 很容易被刪除掉資料庫裡面的內容擊破壞掉所有進階的服務，此外，此種動作可以破壞掉競爭對手的免費電話，甚至非法電話 (例如：色情公司電話)，一個攻擊者可以在資料庫中，修改掉所有的目的電話號碼 (例如：119)，使此電話崩潰。

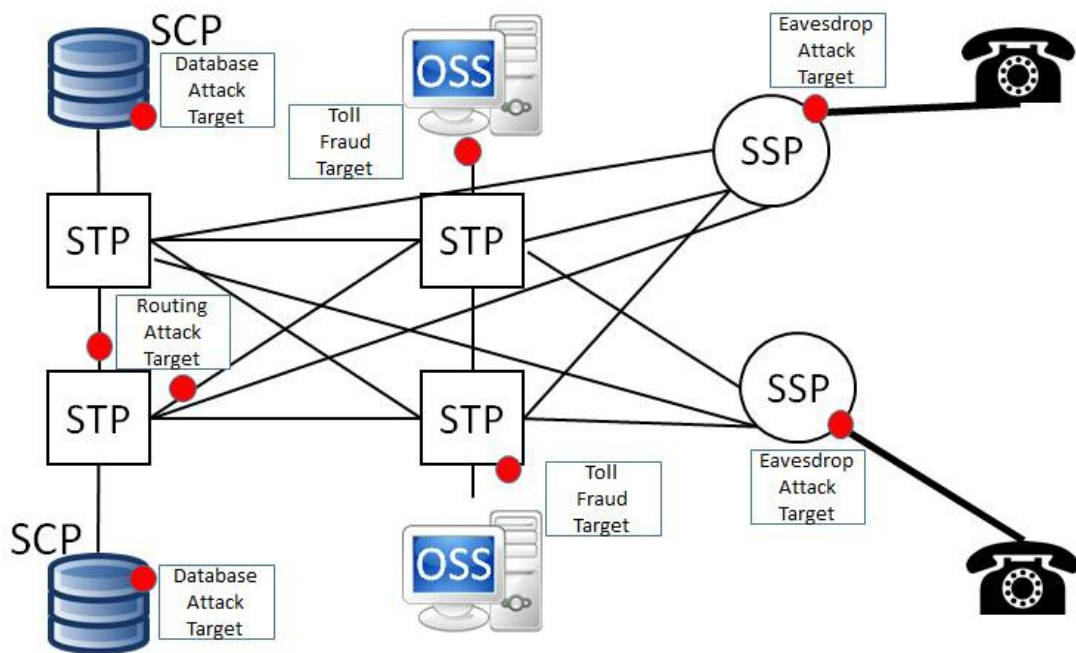


圖 3- 3 SS7 攻擊示意圖

資料來源：Moore, T., et al. "Signaling system 7 (SS7) network security." Circuits and Systems, 2002. MWSCAS-2002. The 2002 45th Midwest Symposium on. Vol. 3. IEEE, 2002.

(4) 三種位置追蹤的攻擊方式

Silke Holtmanns 博士在 User Location Tracking Attacks for LTE Networks Using the Interworking Functionality 這篇論文以及 SANS Institute Reading Room site 演示出了利用了 SS7 的漏洞來追蹤用戶的地理位置，而此種潛在的攻擊目前還沒有有效的防護辦法。在 SS7 位置追蹤的攻擊中主要分為三種攻擊

- (A) 第一種是利用 MAP anytimeInterrogation(ATI) 的訊息發送給 HLR 時，會觸發 provideSubscriberInfo(PSI) 的消息，並且會發送 cell Identifier(Cell-ID)給用戶所連接位置的 VLR/MSC，裡面包含許多用戶的私密資訊，攻擊者可以使用此消息來獲取 Cell-ID，並且可以將訊息位置對應到實際的位置直到街道級別。雖然 ATI 並沒有正常的情況來洩漏給外部網路，但應該還是需要在網路邊界上進行過濾。
- (B) 第二種為如果 ATI 消息已經被過濾，攻擊者仍可將 PSI 消息發送給用戶所在的 VLR/MSC，攻擊者首先需要使用 Global Title 回傳給 MSC 的訊

息，諸如 sendRoutingInfoForSM 之類的訊息來找出 MSC 的 IMSI 和地址，在正常情況下，不應該由營運商自己用戶的外部網路中接收到 PSI 訊息，然而。PSI 訊息還是可以在外部營運商自己的用戶漫遊在自己營運商網路中接收到。

(C) 第三種為 ProvideSubscriberLocation(PSL)由 Gateway Mobile Location Center (GMLC)合法使用，以提供用戶的位置。MSC 沒有能力驗證 GMLC 服務器，但可以驗證其發送者 GT 地址。不幸的是，攻擊者仍然可以欺騙 GMLC 地址並使用它發送 PSL 消息。

3. 防護建議

近年來國際間由於利用 SS7 漏洞發生的資安事件頻傳，已受到各國政府及國際標準機構的重視，GSMA 於 2016 年於 IR.82 已定義 SS7 之威脅及建議防護方式，該機構網站也會對其會員公佈最新的 SS7 威脅資訊做為防護；美國 FCC 於 2016 年 6 月特別成立一個新的工作小組 -CSRIC (Communications Security, Reliability and Interoperability Council)，該工作小組也於 2017 年 3 月完成一份完整的建議報告⁶⁰；北歐通信監管機構於 2016 年 12 月也經發布了第一個關於改善移動網絡安全的聯合建議⁶¹，該建議的目的為提高 SS7 信令系統技術的安全性，其中芬蘭通信監管機關 (Finnish Communications Regulatory Authority，簡稱 FICORA)則是發起並提供相關建議的關鍵角色。歐盟負責網路安全小組，也在 2018 年 3 月發表一篇 Signalling Security in Telecom SS7/Diameter/5G⁶²，透過文獻研析及問卷調查歐洲 39 個電信電信業者目前面臨的安全威脅及在上述協定的防護方式，同時也深度訪談國際監理機關及專家，綜整出此份報告，在報告中也提供對各不同角色單位之建議。透過年本計畫團隊此行參訪芬蘭 Nokia Security Center 時，也針對此議題及芬蘭政府之建議內容進行交流。

為提出一套完整之 SS7 防護建議方案，本團隊綜整相關文獻⁶³、國際標準機構及

⁶⁰ FCC, "The Communications Security, Reliability and Interoperability Council V Final Reports", 2017/3

⁶¹ FICORA, "FICORA calls for a single information security level for mobile network in the Nordic countries", 2016/12/1.

⁶² ENISA, "Signalling Security in Telecom SS7/Diameter/5G", 2018/3.

⁶³ Holtmanns, Silke, Siddharth Prakash Rao, and Ian Oliver. "User location tracking attacks for LTE networks using the interworking functionality." IFIP Networking Conference (IFIP Networking) and Workshops, 2016. IEEE, 2016.

政府單位與相關文獻針對 SS7 之防護建議方案，同時納入本次參訪芬蘭 Nokia Security Center 所交流之國際最新趨勢發展與相關解決方案，以下列出 FCC 公布的 SS7 防護建議、歐盟 ENISA 最新的研究報告及 Nokia 專家之建議，供主管機關及國內電信業者參考。

FCC 公布的 SS7 防護建議主要有以下 9 點建議：

1. 互聯的監控及過濾

GSM SS7 的防火牆規則，最為廣泛應用的檔案為 FS.11 和 IR.82，最被推薦為擔任過濾的節點為 STP 或 STP 附近的節點，因為其經過的封包為最多的，所以也需要最大的保護，歸屬位置暫存器(Home Location Register, 簡稱 HLR)最容易被當成目標，所以也需要有相同的保護，而網路元件也需要保證用戶的資料不會外洩或被修改。

在 SS7 的攻擊中有三種攻擊為主要攻擊手段，分別為追蹤、阻斷、計費欺騙，而主要有四種防禦手段，分別為 STP、HLR、SS7 防火牆功能及過濾和監控，本團隊參考 FCC 發表的 SS7 防護建議報告整理出四種防禦方式(如下圖 3-4)，分別為攔阻、路徑重組、根源追溯及位置檢查。

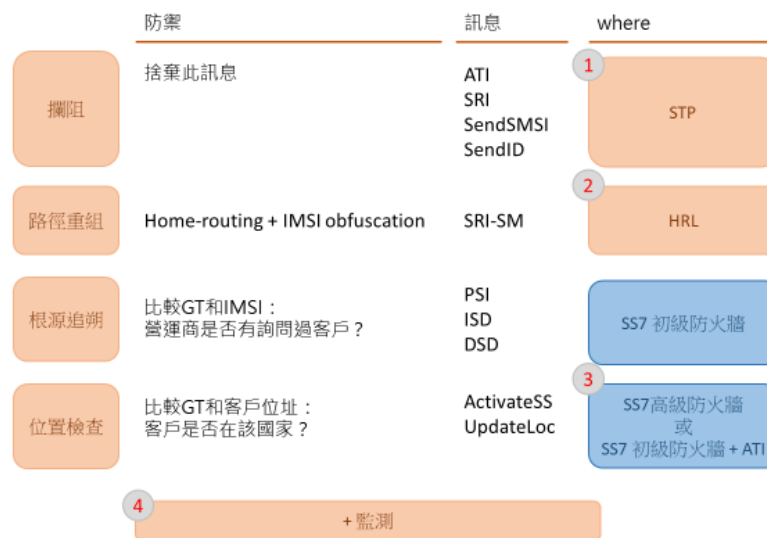


圖 3- 4 SS7 防禦方式

資料來源：FCC

歐盟 Signalling Security in Telecom SS7/Diameter/5G 的調查報告中，超過 84% 的受訪者表示，對於 SS7 的流量，有利用不同的分析技術，以檢測異常活動，超過 50% 的受訪者表示在流量檢查時係針對 STP 及 HLR 兩個層面完成的。歐盟此份調查報告對此也表示認同，認為對 STP 進行檢查可以對整個 SS7 進行全局的觀察，為一種核心措施，且檢查 HLR 也可以確保偵測到對於家庭用戶的攻擊，但並未提及這些檢查是在多複雜的情況下進行的，所以這些措施仍屬於基本保護級別並且還有改善空間。

本計畫於此次訪問 Nokia Security Center，Nokia 即是設計 SS7 防火牆的產品，提供 Monitoring 及 Protect Mode 配置模式，該產品也是依據 GSMA 定義的防護建議所設計，其功能即是主要是透過識別並過濾發話來源端與收話目的端號碼做為控制基礎，一旦非允許的收發雙方與建立連線，則可能會發出警告或直接阻斷該訊務，其主要透過使用 Rapid deployment of the analysis solution，據稱是一種入侵檢測系統（Intrusion-detection system，簡稱 IDS），能夠分析來自 SS7 的主動式威脅。

2. IPSec

在 GSM MAP 協定中，已經開始考慮使用 IPSec 來保護兩邊的通訊安全，但 Nokia

專家指出，此防護方式有可能不能完全相容於既有的系統，例如某些 SS7 系統或老舊的電信網路、電信業者之間相互接界的考量以及部份老舊節點不易升級等。且在升級後的 SS7 以及 MAP 協定中，如果使用 IPSec 來進行保護的話，兩邊都會需要有強大的運算能力而且並不是每個電信業者都受同一個政府機關監督，所以在這個時間點利用此種保護方式所帶來的效益較低。

3. 網路節點防止駭客攻擊

3GPP 有規定系統架構、網路元件及介面的安全需求(TS 33.401)來支援行動裝置的管理，這些要求解決了許多主要的攻擊，包括系統完整性、資料的安全以及存取核心網路之保護。

4. 信令聚合

聚合器為所有類型和規模的電信業者提供大量 SS7 互連的功能，作為一個樞紐，他們對於來自國內或國際的信令訊號有著更廣闊的傳輸視野，這個視野可以對整個流量進行更嚴格的監視及過濾，由主要的聚合器回覆，個別電信業者使用多個訊息串流的基本訊息來過濾及分析來辨識惡意或是可疑的流量，駭客利用電信業者來作為攻擊的媒介可能仍是一個問題，但是藉由擴展不同的互連點來控制安全可以降低其風險。

5. 資訊共享

在歐盟的報告中，有超過 90%的受訪者表示能夠利用不同的技術來應對惡意的流量，有些電信業者能夠引導定向流量，而其他電信業者已經將會發出惡意流量的 SCCP Global Titles 設置為黑名單。

GSMA 近年來一直在探討電信業者共享重點電信安全漏洞之可能性，以電信為中心的一些形式的資料共享，可以幫助電信業者開發或投資通訊安全的解決方案，GSMA 並為了事件回報建立了一組模板，該模板已有電信業者使用，並且至少已有一家營運商向 GSMA 的詐欺以及安全小組(Fraud and Security Group，簡稱 FASG)回報了安全漏洞(簡訊擷取)。

電信產業已經存在一個共享事件的框架，GSMA FASG 也積極的向其成員共享詐欺情報，並與通信詐欺協會(Communication Fraud Control Association，簡稱 CFCA)合

作共享詐欺訊息。此外，CSRIC 第五工作報告中概述了現有的威脅訊息共享資源，因為他與美國國土安全部(Department of Homeland Security，簡稱 DHS)、美國國家通訊協調中心(National Coordinating Center for Communications，簡稱 NCC)以及通訊訊息共享與分析中心(Communications Information Sharing and Analysis Center，簡稱 ISAC)來合作執法，隨著 2015 年 12 月美國網路安全訊息共享法案(Cybersecurity Information Sharing Act，簡稱 CISA)的通過，電信業者已承諾對於電信自動化安全訊息共享案例進行試做，包括 SS7 的安全訊息。

6. 互相信任

3GPP 正在研究電信業者之間群體信任的概念，包括擴展用戶的設備、3GPP 和非 3GPP 的接口以及核心網路和第三方服務的認證框架，如果盡可能的在上游和下游接口之間形成信任團隊是非常有益的，但期待不同類型的營運商以及第三方服務提供商有完全的信任是不現實的，其中有許多問題需要評估，例如：網路如何保護避免受到攻擊、節點是否安全、是否進行風險評估，出租業務等等…，雖然完全的信任在互連模式中是可以受益的，但這需要從小步驟開始按部就班地來隨著環境的變化而擴大。

7. 信令基礎建設之安全評估

信令基礎架構為信令協議、網路架構和支持營運基礎架構提供強大的安全性，必須要定期評估 SS7 的基礎設施安全性，以確定風險然後修復控制框架這應該由內部或是具有此專業技能之第三方進行，安全風險評估可能涉及不同的方面，例如：

- (1) 必須涵蓋到所有國內國外互連點的 SS7 協定的元件
- (2) 評估以通訊安全為重點之人員、流程及技術
- (3) 確定任何內部或外部的弱點
- (4) 須根據安全配置涵蓋到所有控制及管理平面
- (5) 模糊測試以評估協議過濾和數據分析的穩定性
- (6) 評估支持操作流程監控互連點，並回報惡意和可疑的流量
- (7) 隨時更新產品的安全補釘並對其生命周期作出管理

8. 關鍵基礎設施保護

關鍵基礎設施(Critical Infrastructure，簡稱 CI)，包括提供物品不同類型的系統，以支持基本的社會及政府運作，CI 也包含了通訊的部分，所以 CI 可能面臨不同類型的 SS7 以及 Diameter 攻擊，包括位置追蹤、呼叫攔截、詐欺、阻斷式服務，由於 CI 提供了社會的基本功能，所以必須有效的解決 SS7 和 Diameter 的漏洞，以確保 CI 保持彈性及群體連環故障，而為了維持這些基本功能，則需要持續監控、過濾和資訊安全的訊息共享。

9. 支援用戶加密

在 2016 年 12 月，CSRIC 進行的風險評估報告中所發布的 SS7 漏洞裡面提出會有效的原因主要是因為攻擊範圍很小，即使在最複雜的網路中，也可以輕易檢測到使用 SS7 對通話進行大規模竊聽或大規模的位置追蹤，這些攻擊是為了特定的用戶而設計的並與任何良好的防禦手段一樣，分層的方法可提供最好的防護，用戶能夠採用點對點加密的方法來保護訊息和語音通訊的內容。

點對點加密最初在中國、伊朗和中東等地區開始流行，因為這些地區的用戶可能擔心遭到政府的監控，隨著用戶對隱私問題的意識增強，點對點加密的應用程式已漸漸成為主流，這可能是用戶保護通訊內容隱私的一種方式，還有其他更複雜的工具可用於保護用戶，例如：通過安全的 IP 連接使用洋蔥網路。

對於商業客戶或重要的政府官員來說，使用能夠點對點加密的商業應用程式為防止潛在的訊息洩漏，也防止由 SS7 造成的訊息洩漏。隨著這些應用程式的可用性不斷提高，服務質量也隨之提升，雖然這些商業級加密並不被批准用於傳輸任何美國政府的安全機密訊息，然而，他們是一種便利的工具，可以保護敏感但非機密的資訊，所以也是潛在的竊聽目標。

在歐盟 ENISA 最新的研究報告中指出，電信業者通常沒有很多關於訊號的專家，並且大多數並不是 SOC(Security Operation Center)團隊，IT 安全團隊或是安全/欺詐的部門需要在這部分需要有更深層的了解以及努力。隨著攻擊者的技術提升，駭客也會開發出更有效率的攻擊場景，想必 SS7 的攻擊未來將會更為複雜，基本的保護能夠涵蓋住大部分的攻擊，但是卻會對於社會、經濟或政治層面上真正造成損害及針對性的攻擊留出空間，下表為此報告對信令安全防護措施的建議。

表 3-2 信令安全防護措施

防禦分類	防禦方式
核心措施：檢測攻擊和妥協措施的最低限度措施	監控所有互連流量 監視核心網路的元件 監控傳出的流量 加強網路節點
中級措施：為核心措施增加安全保證	定期執行外部網路安全評估和滲透測試 確保對惡意流量的回應及合法的分析互連的訊息 建議營運商在其互連產品中採用安全選項
高級措施：可以識別和減輕未知的攻擊	檢測高級攻擊 檢測即將發生的攻擊 深度信令消息

資料來源：ENISA

歐盟 ENISA 的報告中，對電信業者提出的建議是，雖然電信業者已進行基本的防護，可涵蓋大部分的攻擊，但是在某些情況下，對於基本的防護已經不夠，攻擊者還是能夠使用複雜的攻擊情境和手段，造成有損失的攻擊，所以必須更加強化 SS7 的基礎安全設施，不斷提升安全級別以因應各種不同的攻擊。

IEEE 的一篇論文研究⁶⁴，則是利用機器學習來保護 SS7 的安全，這篇論文主要是利用偵測 SS7 裡面關於位置描述的 Header 來訓練出攻擊的特徵值，並且利用這個特徵值來區分出正常的使用者及不正常使用者，而保護的內容主要是因為訊息因合理需要而對外曝光，如下列的 Header：updateLocation(UL) – sendAuthenticationInfo (SAI) – registerSS – eraseSS – processUnstructuredSS (PSU) – cancelLocation(CL) – sendRoutingInformation(SRI-SM, SRI-LCS)，而適用的營運商必須要達到：

1. 能夠蒐集整個 SS7 傳送到核心網路的流量；
2. 能夠分辨這個 SS7 的訊息的出處；
3. 能夠有一個區分出網路不同位置的度量。

下表 3-3 為檢測異常用戶使用的特徵，其中變量屬性大致上可分為兩種，分別是數量(continuous)屬性及名義(nominal)屬性，數量屬性為量化的數字，名義屬性為等級

⁶⁴ Jensen, Kristoffer, et al. "Better Protection of SS7 Networks With Machine Learning." *IT Convergence and Security (ICITCS)*, 2016 6th International Conference on. IEEE, 2016.

的區分。他們所使用的是異常檢測演算法(The Seasonal Hybrid ESD algorithm)，而 ESD 演算法主要是利用尋找離數據平均集最遠的點來檢測群裡單一的異常值， $G = \frac{|Y_i| - \bar{Y}}{s}$ ， $|Y_i|$ 為每個點的值， $\bar{Y}$ 則是數據集合的平均， s 則是標準差，以及利用 G 來訓練門檻值。下圖 3-5 為實施在網路異常使用檢測系統(Components of the implemented anomaly-based network abuse detection system)的組件流程圖，在這篇論文的實驗結果中，實驗數據為 59,682 組，並能在用戶行進時對於攻擊可達到 100%的準確預測，但是大約會有 4.7%的錯誤預報。在這樣高的檢測率上，或許在我們尚未拿到 GSMA 所訂定的標準之前，將可考慮發展為防禦 SS7 攻擊的方式之一。

表 3-3 檢測特徵值

描述	變量屬性
離上次更新位置的時間	數量屬性
離上次更新位置的距離	數量屬性
上次更新距離位置的 Byte 數	數量屬性
更新位置的頻率	數量屬性
網路訊息來源	名義屬性

資料來源：IEEE

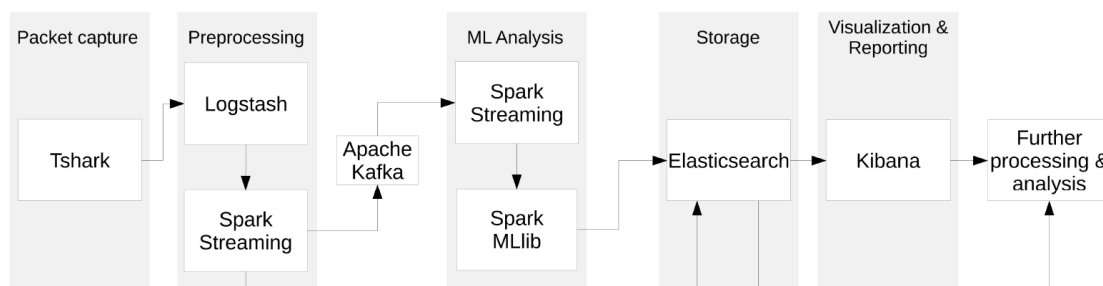


圖 3-5 組件流程圖

資料來源：IEEE

芬蘭政府建議採用 GSMA 的防護建議外，同時從消費者端著手，提供消費者自我通訊保護的指引⁶⁵，也是值得國內參考。以上述 FCC、歐盟、國際文獻及此次訪談 Nokia Security Center 專家之建議，在 SS7 的防禦上，綜整出以下四點的防護建議。

⁶⁵ FICORA, “Guidelines for protecting communications”,

1. 防禦攻擊-監控網路流量

監控異常之網路流量，已為目前電信業者網路普遍之功能，此為目前最基本之防禦攻擊措施。

2. 緩解攻擊-過濾訊息

過濾發話來源端與收話目的端號碼做為控制基礎，一旦非允許的收發雙方與建立連線，則可能會發出警告或直接阻斷該訊務。

3. 合作及訊息分享

GSMA 提供其會員公告全球最新攻擊資訊，因國內並無 GSMA 會員，目前研究團隊亦無法取得 GSM ASS7 相關完整防護建議文件及攻擊資訊，實為國內政府與電信業者可考量的重點；但國內亦可於業者間建立 SS7 攻擊訊息分享平臺，提升國內電信業者防禦攻擊之能量。

4. 加強網路節點安全

透過國際標準組織公布之內容，時時檢視電信網路弱節點，進行節點安全及流程之加強，以防禦不同的攻擊。

(二) 第五代行動通訊系統(5G)^{66、67}

基於大眾對行動數據的需求年年倍增，不只追求更高的傳輸速率，更要求提供多樣化的服務，因此需要第五代行動通訊技術(5th Generation Mobile Network，簡稱 5G)來滿足日益增加的需求。為了達成全新智慧生活網的願景，5G 的目標為無論通訊、交通以及各式各樣的人或物皆可連上網路，打造一個無縫連結的社會環境。因此相較於前一代行動通訊標準 4G 各方面性能而言，5G 通訊服務更可達到 0.1-1Gbps 的用戶體驗速率、支援 1 百萬/km² 的連線數、毫秒等級的端對端往復延遲、數十 Tbps/km² 的流量密度、高達 500km/hr 以上移動性和數十 Gbps 的峰值速率；此外，5G 頻譜效率也比 4G 提升 5-15 倍，效能和成本效率可望提升百倍以上。表 3-4 為第四代行動通訊技術(The fourth generation of mobile phone mobile communication technology standards,

⁶⁶ NGMN “NGMN 5G WHITE PAPER”, 2015/2/17.

⁶⁷ 5G-PPP, “View on 5G Architecture”, 2016/6.

簡稱 4G)與 5G 效能之比較，由表可知 5G 不僅僅在速度上大幅優於 4G，也可從表中了解 5G 服務的項目不再如 4G 單一，因此延伸出新的概念(如 Device to Device)，增加網路資料傳輸的靈活度。

表 3- 4 4G、5G 效能比較表

5G性能	5G目標與應用	4G目標與應用
用戶體驗速率	0.1-1Gbps，廣域覆蓋下設備傳輸速率之最低要求	定點或低速移動通訊達 1 Gbit/s
連線設備數量	1百萬/km ² 連線數量，適用於大規模集會活動	無特別說明
D2D延遲	低於毫秒等級，適用於快速道路系統、遠端操作	無D2D概念，Latency： Control-plane：100ms、 User-plane：10ms
流量密度	支援數十Tbps/km ² ，適用於辦公室等地方的網路流量	2.25 bit/s/Hz/cell，適用於室內環境
移動性	500km/hr，適用於高速鐵路行進中	於高速的環境下達到約100 Mbit/s移動性速率
峰值速率	數十Gbps，單一用戶可達最高傳輸速率	3GPP Release 8發布單通道峰值下載速率為300Mbps； 上行速率為75Mbps；

資料來源：IMT-2020⁶⁸、IMT-Advanced⁶⁹

現階段 5G 的標準尚未被制訂完成，國際間仍有許多重要的組織對於 5G 網路通訊環境的標準制定及推動不遺餘力，以下為 5G 標準制定與推動的重要國際組織簡介：

1. 國際電信聯盟無線電通信部門 (International Telecommunication Union Radiocommunication Sector，簡稱 ITU-R)：

為負責於無線電通訊的部門，隸屬於聯合國 ITU 之下，在 5G 中擔任制定行動通訊標準的重要推手。

2. 第三代合作夥伴計畫(3rd Generation Partnership Project，簡稱 3GPP)

⁶⁸ IMT-2020 (5G) 推進組, “《5G 願景與需求白皮書》”, 2014/5/28.

⁶⁹ ITU, “《Requirements related to technical performance for IMT-Advanced radio interface(s) 》”, 2008.

由日本 ARIB、北美 ATIS、中國 CCSA、歐洲 ETSI、印度 TSDSI、韓國 TTA 以及日本 TTC 所組成的國際標準化機構，負責行動通訊系統（Universal Mobile Telecommunications System，簡稱 UMTS）（為 3G 最廣泛採用的行動技術）、長期演進技術（Long Term Evolution，簡稱 LTE）/進階長期演進技術（LTE-Advanced，簡稱 LTE-A）等 3G 及 4G 標準的制定，並且也在 5G 中擔任制定行動通訊標準的重要推手。

3. 下世代行動網路聯盟 (Next Generation Mobile Network Alliance，簡稱 NGMN)：

其成員包含美國 AT&T、中國移動通信(China Mobile Communications Corp)、台灣中華電信(Chunghwa Telecom)、韓國通訊(Korea Telecom，簡稱 KT)、日本 DOCOMO(Do Communication over the Mobile network)等全球各大知名逾 80 個電信業者，在 5G 標準中並非扮演著標準制定的角色，NGMN 負責研究及推行標準制定組織所制定的標準，並且將成員的需求反應至 ITU-R 及 3GPP，做為標準組織制定標準的參考方向。目前 NGMN 所發行的白皮書皆可於官網中下載⁷⁰。

4. 5G 基礎設施協會(5G Infrastructure Public Private Partnership，簡稱 5G-PPP)：

歐盟委員會(European Commission，簡稱 EC) 於 2013 年 12 月正式宣佈成立 5G-PPP，其成員包含：瑞典 Ericsson、法國 Alcatel-Lucent、芬蘭 Nokia Solutions and Networks、德國 Deutsche Telekom、義大利 Telecom Italia、中國華為(Huawei)、美國 Intel、韓國 Samsung 等除了歐盟以外的國際重要電信設備製造商，在 5G 網路標準中與 NGMN 的角色相似，負責 5G 的推動及研究。目前 5G-PPP 所發行的白皮書皆可於官網中下載⁷¹。

國際電信聯盟(International Telecommunication Union，簡稱 ITU)於 2015 年 6 月發布了 5G 標準化時刻表(圖 3-6)，預定 5G 標準將於 2020 年制定完成，並且將 5G 系統命名為 IMT-2020⁷²，藉此達到整合的效果。ITU 除了頒布 5G 標準制定時刻表外，也指出 5G 行動通訊技術發展考量需包含系統平均吞吐量、可擴展性、非語音服務(如

⁷⁰ NGMN 官網。

⁷¹ 5G-PPP 官網。

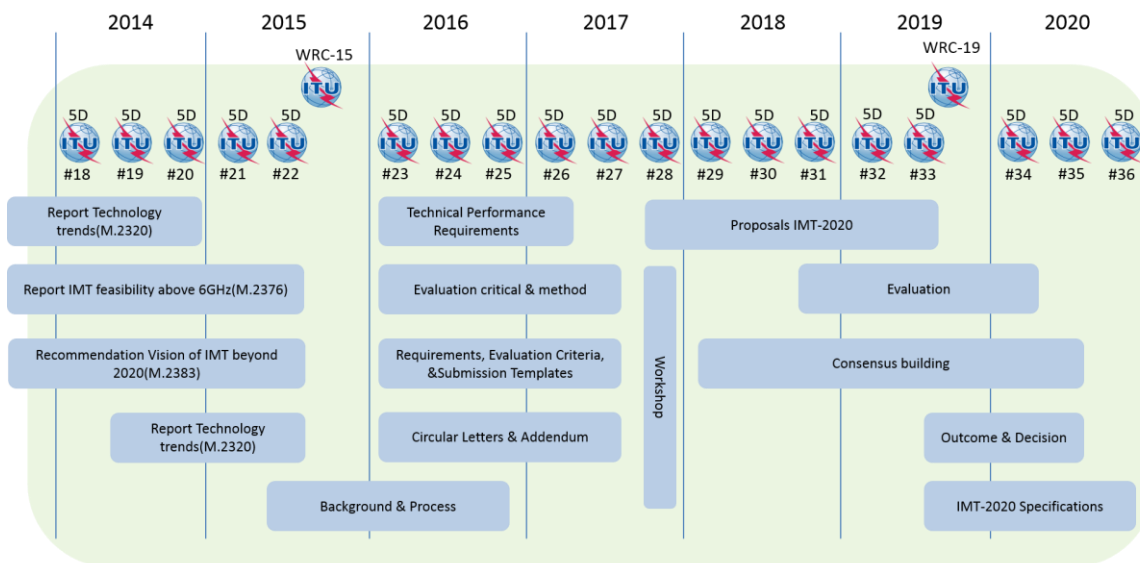
⁷² ITU, “Workplan, timeline, process and deliverables for the future development of IMT”, 2015.

IoT、高畫質影音服務等)、頻譜使用效益、時間延遲⁷³。ITU 認為 5G 行動通訊將協助產業、商業、數據、人與物互通連結，支持未來廣泛使用場景之需求。根據 ITU 規劃，第三代合作夥伴計畫(3GPP)啟動 5G 技術標準化前期研究，如全方位 MIMO 技術、終端對終端(Device to Device，簡稱 D2D)通訊、免執照頻譜分配使用等⁷⁴，並於 2017 年開始進行 5G 國際標準徵集、效能規格評估與無線介面技術，預期正式規格於 2019 年或 2020 年出爐。5G 行動網路提供的服務主要可劃分為三類；增強移動寬頻(Enhanced Mobile Broadband，簡稱 eMBB)、大規模物聯網(Massive Machine Type Communications，簡稱 mMTC)、低時延高可靠度連接(Ultra-reliable and Low-latency Communications，簡稱 URLLC)。

日前在全球最大規模 CES 消費電子大展上，瑞典電信設備業者 Ericsson 公開展示遠距操作挖土機技術，正是 5G 網路串流傳輸高畫質影像及低時延反應能力的一項應用展現，目前各國也都致力於 5G 商用運作，如南韓電信業者計畫於 2018 年平昌冬季奧運上展現 5G 連線能力；日本則是宣布預計在 2017 年下半年試行 5G 系統，爭取趕在 2020 年東京奧運前普及全日本；而中國的通訊企業華為更爭取到 5G eMBB 編碼技術標準。5G 創建高速且穩定可靠的行動網路，使得原本受限於前代行動網路而發展不夠迅速的應用服務隨著 5G 的普及得以加快腳步實現。

⁷³ ITU-R, "IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond", 2015/9.

⁷⁴ Balazs Bertenyi, "3GPP system standards heading into the 5G era", 3GPP, 2014.



註：世界無線電通訊大會（WRC-15），於2015/11/2 ~ 27在瑞士日內瓦舉行

世界無線電通訊大會（WRC-19），預計於2019/10/28 ~ 11/22舉行

圖 3- 6 IMT-2020 5G 標準訂定時刻表

資料來源：ITU, Emerging Trends in 5G/IMT2020

1. 5G 架構

因應物聯網時代的來臨，5G 所提供的服務不再單一，5G 通訊並不能僅單單滿足於語音以及數據傳輸的目的，因此 5G 網路除承襲 4G 網路架構外，必須提供更高彈性的網路環境，以供應 5G 通訊網路世代的整合。根據歐盟 5G PPP 在 2016 年 7 月所發表的「View on 5G Architecture」，描述 5G 通訊網路應達到高速率的數據傳輸、高密度的基站佈建、較低的延遲時間以及降低硬體成本等等，為了達成上述的目的，規劃了 5G 整體的架構應該要通過高成本效益的方式實施網路切片、支持原生網路的軟體化、整合通訊以及計算和整合異質網路(包括固網、接入網、3G、4G 以及 Wifi 等)，才可滿足 5G 多樣化的應用需求，因此 5G PPP 白皮書將 5G 大生態環境分為五層，如圖 3-7 所示，分別是：Business Service Layer(業務層)、Business Function Layer(業務功能層)、Orchestrator Layer(編排層)、Network Function Layer(網路功能層)以及 Infrastructure Layer(基礎設施層)，希望透過層層間的良好佈署以及鏈結，將 5G 的生態環境與現代生活做緊密的連接。本團隊將上述五層歸類整理為應用服務、網路服務

及物理服務簡介如下：

(1) 應用服務：包含 Business Service Layer(業務層)、Business Function Layer(業務功能層)

負責提供合適的功能給相對應的應用環境，在業務功能層存有功能庫可供業務層使用。3GPP 定義的三大場景便是於此實現。

(2) 網路服務：包含 Orchestrator Layer(編排層)、Network Function Layer(網路功能層)

為 5G 生態環境重要的兩層，網路功能層提供網路的功能給編排層，編排層將網路功能虛擬化並以軟體定義網路將以串聯，也就是 5G 網路的核心技術 — 網路切片 (Network Slicing)。

(3) 物理服務：即 Infrastructure Layer(基礎設施層)

5G 環境相關的硬體設施，無論接入網或核心網的佈署，或因為 5G 環境需求基地台的相關建設，皆定義在基礎設施層中。

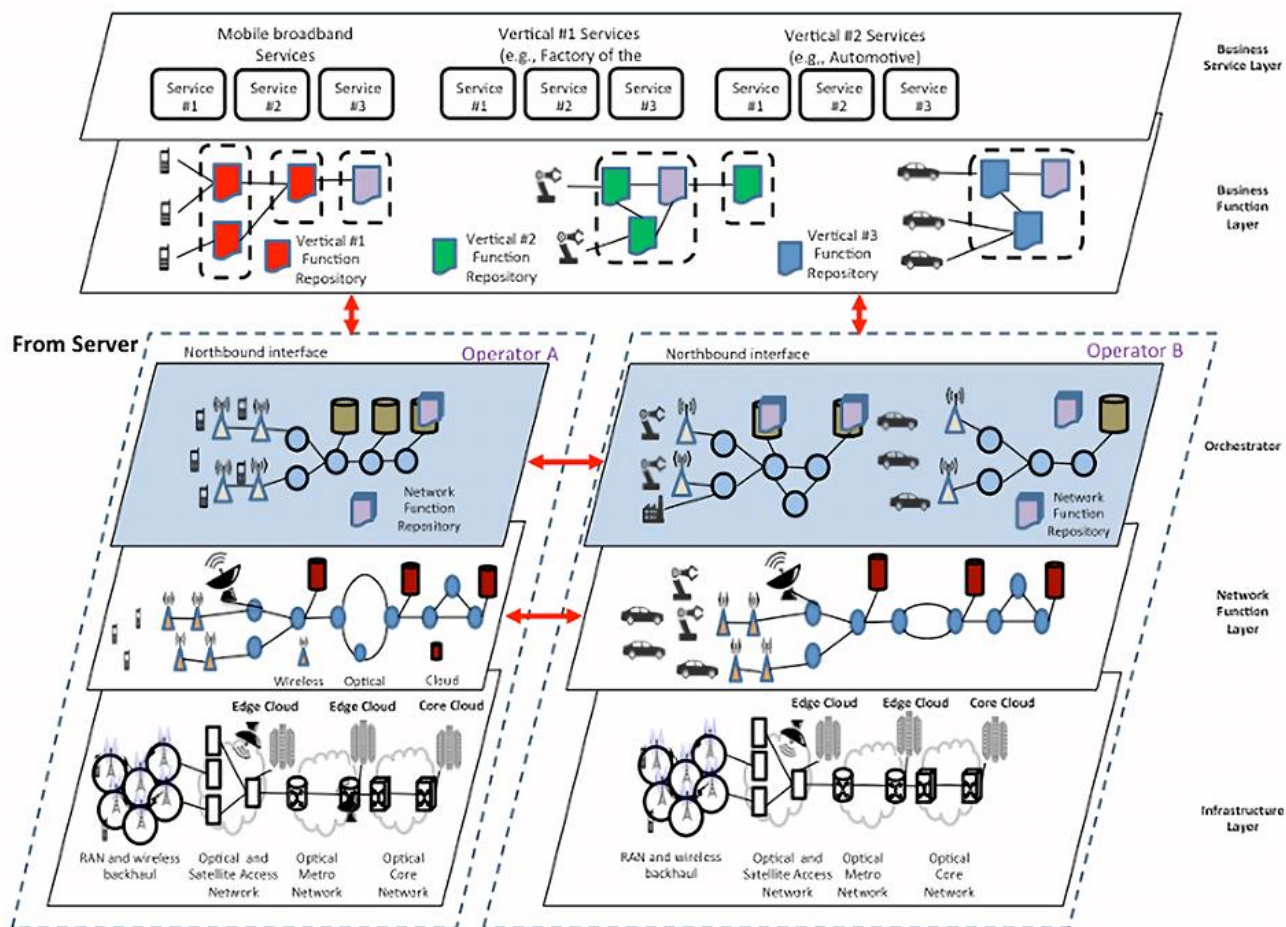


圖 3- 7 5G 生態系統示意圖

資料來源：5GPPP, View on 5G Architecture

在 5G PPP 白皮書中將 5G 的架構分成 5 層，其中業務層以及業務功能層統稱為最高層，負責提供應用等相關功能。3GPP 在其所發布的 TR 38.913「Study on scenarios and requirements for next generation access technologies」⁷⁵中則定義了 5G 的三大服務應用如下：

(1) eMBB(Enhanced Mobile Boardband)：

能提供更高頻寬，利用在高清影片(如監視器)以及虛擬實境(VR)等應用。

(2) mMTC(Massive Machine Type Communication)：

⁷⁵ 3GPP, "Study on scenarios and requirements for next generation access technologies", 2016/6.

為大規模物聯網所設計的應用，如：醫療、農業、商業等物聯網所使用。

(3) URLLC(Ultra-reliable and Low-latency Communication)：

提供高可靠度，必須應付各種即時通訊需求，作用於遠端控制以及無人駕駛等需要可靠度高且低時間延遲的應用。

圖 3-8 為各個實際應用所對應到的三大服務範圍。3GPP 除了定義出了三大服務，也對三大服務所要求的資料傳輸速率、控制延遲時間、覆蓋率等等皆詳述在「3GPP RAN progress on “5G”⁷⁶」文件中。

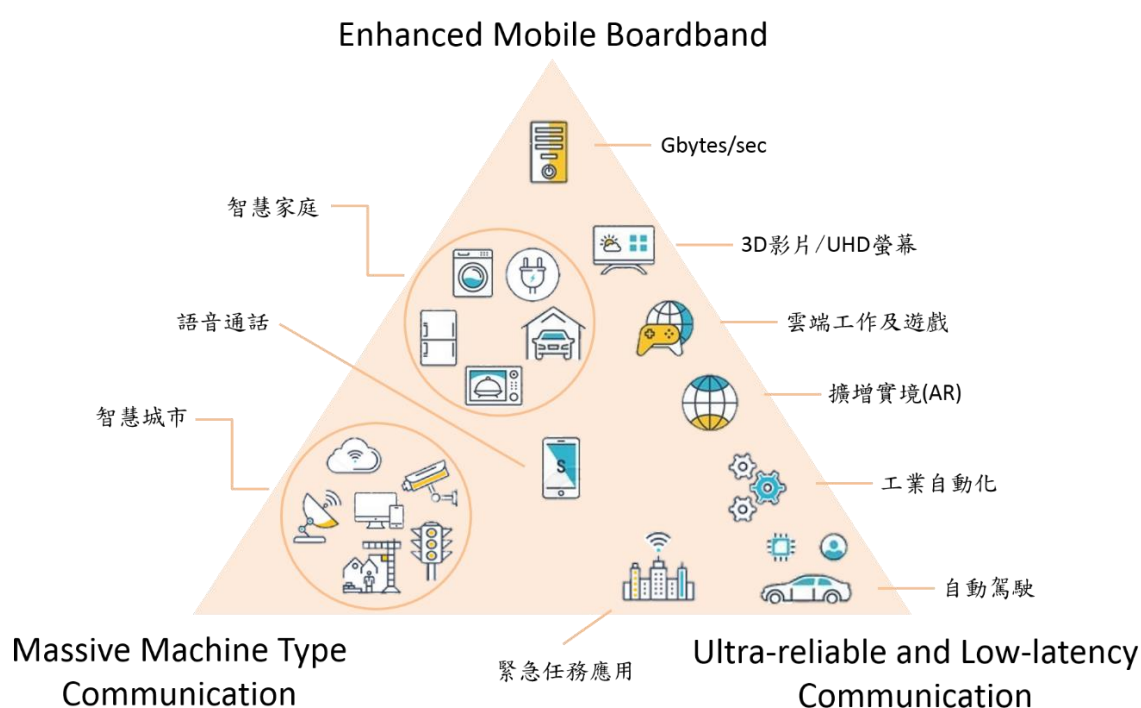


圖 3-8 三大服務示意圖

資料來源：ITU, Emerging Trends in 5G/IMT2020

在 2016 年 11 月 7 日於美國召開的 3GPP RAN1 #87⁷⁷中投票表決出以中國華為所支持的 Polar 極化碼做為 5G eMBB 短碼控制頻道的編碼方案，美國高通(Qualcomm)所支持的 LDPC 碼則為短碼數據頻道的編碼方案，長碼的編碼方案在 2016 年 10 月 14

⁷⁶ 3GPP, “3GPP RAN progress on “5G””, 2016.

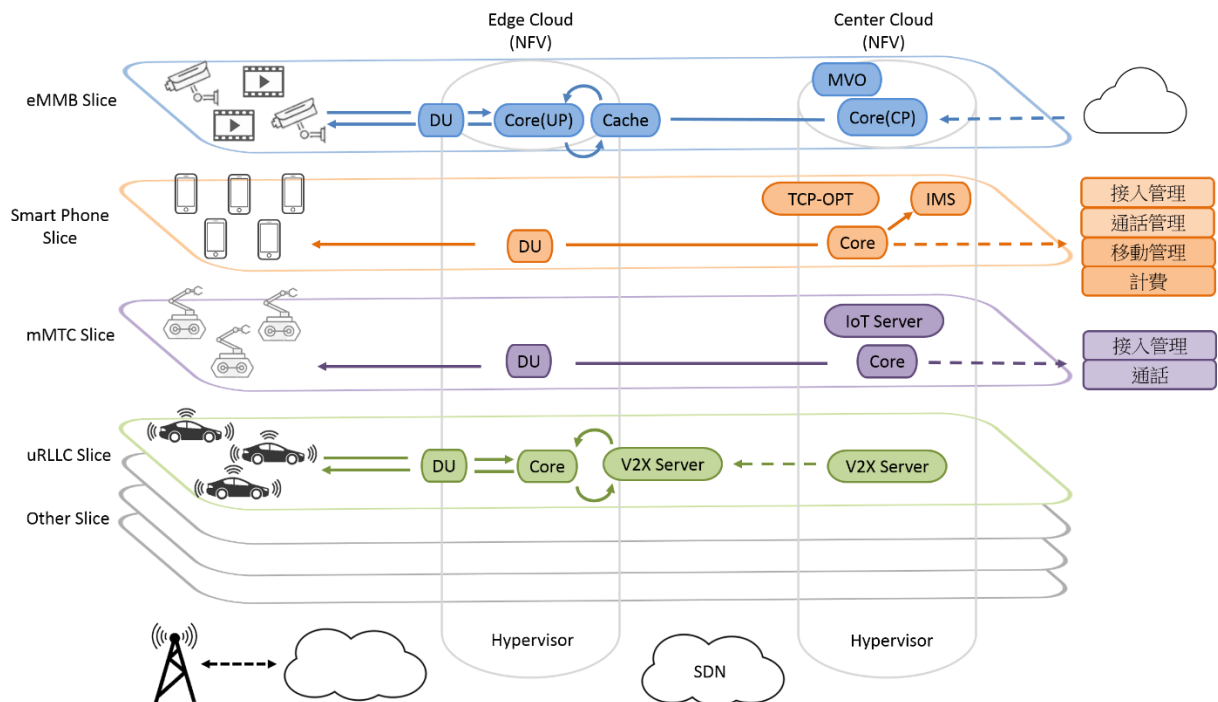
⁷⁷ 工研院資通所, “3GPP RAN1 #87 會議報告”, 2016/12/30.

日於葡萄牙舉行 3GPP RAN1 #86bis⁷⁸的會議上，由 LDPC 碼做為此編碼方案。在過去的通訊時代中，Turbo 碼與 LDPC 碼因接近編碼通道容量極限而曾被提出做為 3G、4G 及 Wifi 的編碼，但因應 5G 業務量龐大且可靠性必須更高，因此 Turbo 碼與 LDPC 碼並無法完全達成 5G 的服務需求。2008 年土耳其 Bilkent University 的 Erdal Arıkan 教授首次提出極化碼(Polar Code)，是目前唯一被證明以對稱式二進制輸入(Symmetric Binary-Input)的方式且在無記憶性通道中(Memoryless Channels)能達到香農極限(Shannon Limit)的編碼方式⁷⁹。目前各個組織訂定的標準比較偏向於 eMBB，mMTC 與 URLLC 則會於往後的時間訂定的更完整。

根據上段所述，5G 世代為了滿足大量的網路需求以及提供多樣化的服務，各個參與 5G 標準訂定的組織將技術重心放在網路切片(Network Slicing)上(如圖 3-9)。在 5G 之前的通訊世代，無論核心網路(Core Network，簡稱 CN)或者是接入網(Radio Access Network，簡稱 RAN)皆有專屬硬體設備提供服務，一套設備只對應到單一項服務，容易造成任何細微的調整極可能造成整體服務暫停運作、低效率以及硬體成本龐大等缺點；由於 5G 通訊時代有大量的網路接入，因此採用網路切片的概念為將物理網路劃分為多個虛擬網路，每一個虛擬網路靈活對應不同服務，有了網路切片的概念，佈建時不再需要將每個服務對應到服務專屬的網路環境，大大降低了網路硬體成本的支出，也可根據用戶端的需求隨時的進行調整而不需要暫停整體服務的運作。

⁷⁸ 工研院資通所, "3GPP RAN1 #86bis 會議報告", 2016/11/30.

⁷⁹ Arıkan, Erdal. "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels." *IEEE Transactions on Information Theory* 55.7 (2009): 3051-3073.



資料來源：NGMN white paper、Korea Communication Review Q4 2015

為了更容易執行網路切片，5G 採用網路功能虛擬化 NFV(Network Functions Virtualization)以及軟體定義網路 SDN(Software Defined Network)實現網路切片。

(1) 網路功能虛擬化 NFV(Network Functions Virtualization) :

NFV 將傳統網路須搭配專屬硬體功能虛擬化，作用在成本較低、規格大眾化的商用伺服器上的虛擬主機(Virtual Machines，簡稱 VMs)中，並搭配雲端計算(Cloud Computing)，每台虛擬主機遷移或備份將比起傳統硬體要來的簡單多，如此一來除了可以降低硬體成本，對於維修以及佈建將會有更高的彈性。將硬體虛擬化後，原本核心網路的大部分可統稱為核心雲(Center Cloud)，接入網以及小部分的核心網可統稱為邊緣雲(Edge Cloud)，以軟體定義網路(Software Defined Network，簡稱 SDN)作為邊緣雲以及核心雲之間的連接。

(2) 軟體定義網路 SDN(Software Defined Network) :

SDN 主要做為邊緣雲以及核心雲中間的連接橋梁，如圖 3-10 所示，核心雲以及邊緣雲中皆有虛擬機監視器(Hypervisor)，內含有虛擬路由器(Virtual Router)以及虛擬交換器(Virtual Switch)，IP 封包可藉由雲端伺服器中間的閘道器(DC G/W)經過 SDN 通道的將封包傳送到正確的位址，透過 NFV 將硬體虛擬化以及 SDN 將邊緣雲及核心雲之間的連結，網路切片的目的即可達成。⁸⁰

在傳統通訊網路中，使用者裝置與接入網做連接再由接入網連結核心網，但這樣的方式會造成不必要的資料回傳速度延遲。為了解決這個缺點以及因應 5G 多樣化的服務，核心網以及接入網的部分延伸出核心雲以及邊緣雲的概念，邊緣雲為接入網和小部分核心網的統稱，並架設在基站附近與基站連接，對於低延遲需求的服務將原本部分核心網的功能移至邊緣雲，在需要部分核心雲的計算及儲存等功能時，只需連接到位於基站附近的邊緣雲即可。

如此一來，可以大幅降低回傳速度的延遲，提供需高速運作的使用案例。如圖 3-10 所示，eMBB 服務對於頻寬有極大的需求，因此可將快取記憶體(Cache)以及核心網路的用戶面(User Plane，簡稱 UP)置放於離用戶較近的邊緣雲中，可增加使用者對於此服務的好感度。針對自動駕駛、遠程管理所設計的 URLLC 服務，對於回傳資料的時間延遲較為要求，因此將核心網路以及相對應的服務器(如 V2X Server)移至邊緣雲，降低資料傳輸的延遲時間。藉由 NFV 與 SDN 的互相配合以及雲端計算的相輔相成，5G 通訊網路世代將具有相當高彈性的網路環境，傳統的垂直網路環境允許被分為許多片狀結構，每片獨立且互相不干擾，營運商可依據客戶端的需求制定滿足客戶的虛擬網路服務。

⁸⁰ Netmanias, “Korea Communication Review Q4 2015”, 2015.

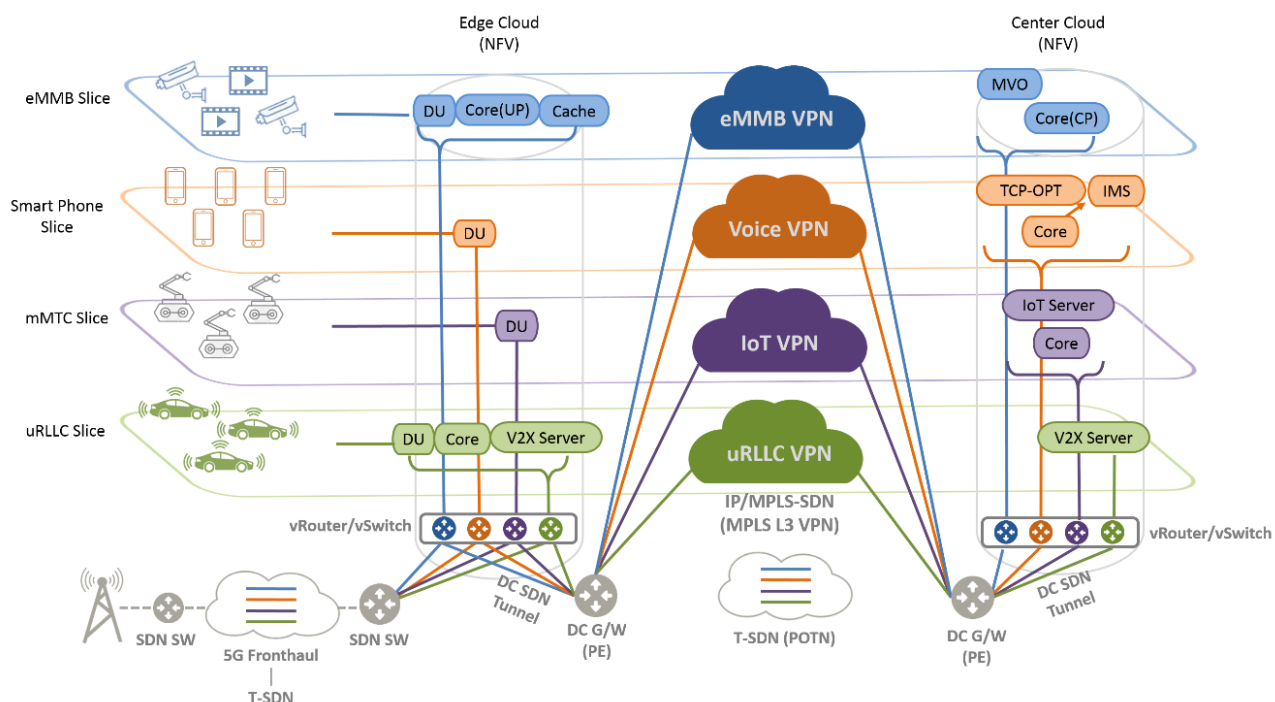


圖 3- 10 SDN 與邊緣雲及核心雲關係示意圖

資料來源：NGMN white paper、Korea Communication Review Q4 2015

在無線行動通訊中，實體設施提供網路功能運作的平台，然而傳統的實體架構難以滿足 5G 的需求，如上述，為了因應 5G 多樣化的場景需求及提供使用者更好的網路體驗，5G 網路環境需要提供更密集的網路覆蓋率及更快速的回應速度，這使得基站數量及頻譜使用需求大量增長。因此，網路的實體架構，包含接入網、基站的部署和邊緣雲等設備都需要革新來因應 5G 的行動網路時代。在 5G PPP 白皮書中針對小基站與異質網路(Small Cells and Heterogeneous Network)、毫米波(Millimeter Wave, 簡稱 mmWave)以及雲端無線接入網(Cloud Radio Access Network, 簡稱 C-RAN)等因應網路環境改變而衍伸出的硬體結構介紹如下。

(1) 小基站 (Small Cells)

為了因應 5G 網路場景的驟增，基站數量需求大幅增加，由於傳統大型基地台 (Macrocell) 包含所有無線網路連線所需的硬體設備，不僅成本高，且還有選址的問題，部署不靈活，因此 5G 將小基站的概念導入，此概念將會是 5G 基站部署很重要的一環。小基站是小型的基地台，網路覆蓋範圍較小，但擁有較低的部署成本及較少的發射功率。未來 5G 基站在佈建時，除了期望能夠保存現有的基站外，並且導入小基站

的概念做融合，提高訊號的覆蓋率以達成 5G 網路所定義的速率以及傳輸率

(2) 毫米波(Millimeter Wave，簡稱 mmWave)⁸¹

由於 5G 對於速度的要求為 4G 的十倍以上，但現存的 4G 頻譜機制已接近理論的極限，5G 世代尋找適合的頻譜在所難免(如圖 3-11)，因此毫米波成為 5G 頻譜的熱門選擇。波長為 1~10 毫米的電波統稱為毫米波，頻率約在 30G~300GHz 頻率範圍。5G 無線的頻譜資源需求在大量增加，且要求傳輸速度快，在這樣的趨勢下，啟用新的頻率波段類型(如毫米波)，可較容易達到 5G 所定義的速度要求，根據香農公式(Shannon Equation)⁸²的定義：

$$C = B \log_2(1 + \frac{S}{N})$$

- C ：頻道可能的最大傳輸速率
- B ：頻寬
- $\frac{S}{N}$ ：訊號雜訊比

由下圖 3-11 可知，目前國內頻率較小的範圍幾乎已被使用，毫米波的頻率範圍落在 30G~300GHz，特性除了波長短、頻率高外，毫米波能夠提供較大的頻寬，由上述公式可知， B (頻寬)與 C (傳輸速率)成正比，因此毫米波就比現存的波段來的速度較快，可有效增加無線傳輸速率的最大值，所以在 5G-PPP 《View on 5G Architecture》中提到 5G 網路將毫米波提出來做為未來訊號傳輸的波段，且運用毫米波可降低基站間的干擾，使基站部署更加密集。

⁸¹ 工業技術研究院, “5G 毫米波接取技術與挑戰”, 2015/8/14.

⁸² Shannon, Claude E. "A mathematical theory of communication." ACM SIGMOBILE Mobile Computing and Communications Review 5.1 (2001): 3-55.

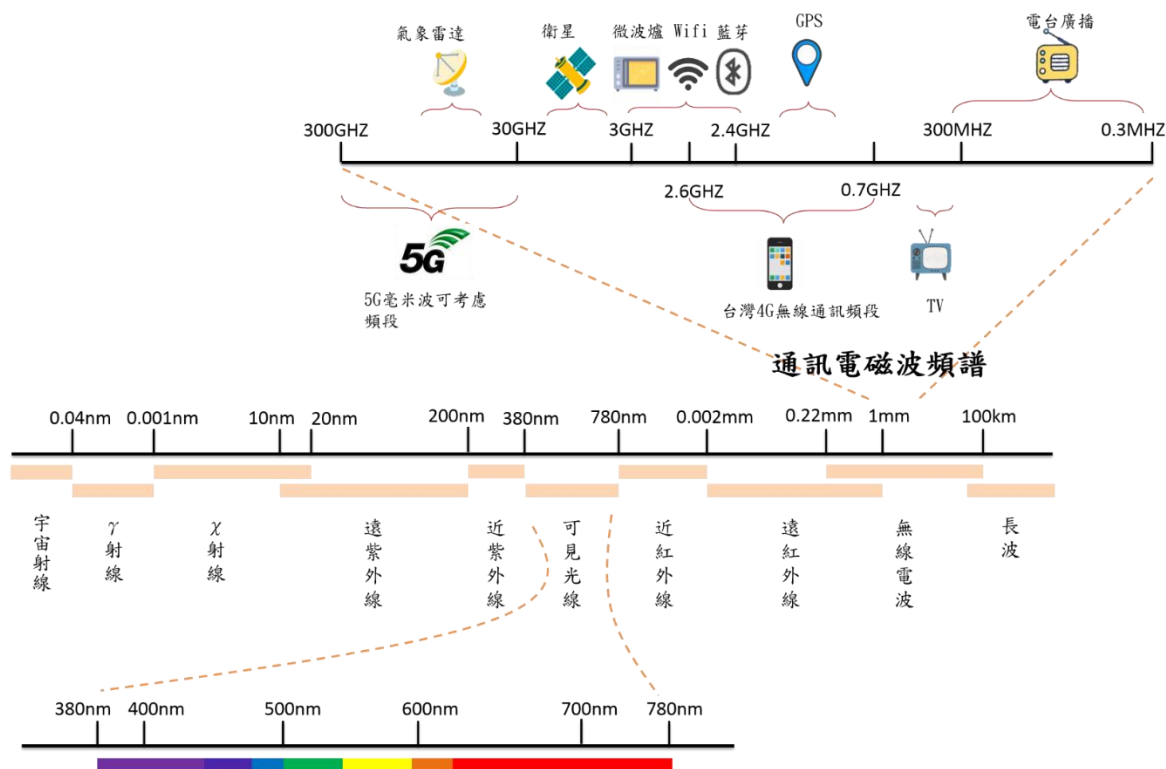


圖 3- 11 頻譜應用示意圖

資料來源：本團隊整理

(3) 雲端無線接入網(Cloud Radio Access Network，簡稱 C-RAN)

中國移動研究所最早提出 C-RAN 的概念，接下來如中國移動、日本 DOCOMO 以及一些設備大廠，如：中國華為、芬蘭 Nokia 等皆有發表 C-RAN 的解決方案。C-RAN 被提出來討論主要是為了解決 4G 時代的基地台數將會快速成長。根據資策會產業情報研究所(MIC)所發布的《新世代行動網路接取架構發展分析：Cloud RAN》⁸³，該報告分析從 2013 年至 2018 年(預估)的 2G、3G 以及 4G 的終端服務量(如圖 3-12)，得知 4G 網路成長快速，若以傳統基地台佈建方式，將會造成成本以及能源耗損龐大等相關議題。傳統基地台內部零件包括天線(Antenna)、射頻設備(RF equipment)、數位處理器(Digital Processor)及基頻單元裝置(Base Band Unit，簡稱 BBU)。

傳統基地台便是將上述四個零件設置在一個站點中，在往後的通訊世代對於基地

⁸³ 資策會產業情報研究所(MIC),“新世代行動網路接取架構發展分析：Cloud RAN”, 2014/5/28.

台的需求量越來越大，若是不改變基地台設置方式，不僅硬體成本增加快速，通訊的效益也會造成一定的增加，因此 C-RAN 的概念變日趨重要。

C-RAN 的概念為虛擬化複雜的基頻處理功能，打斷傳統 BBH 與多頻段遠端無線電站(Remote Radio Head，簡稱 RRH)之間的連結，改變留下化簡後的 RRH、天線，且以通用公共射頻介面(Common Public Radio Interface，簡稱 CPRI)與 BBU 連結，並將 BBU 集中管理，因此可更有效率的將基頻功能處理妥當(如圖 3-13)。

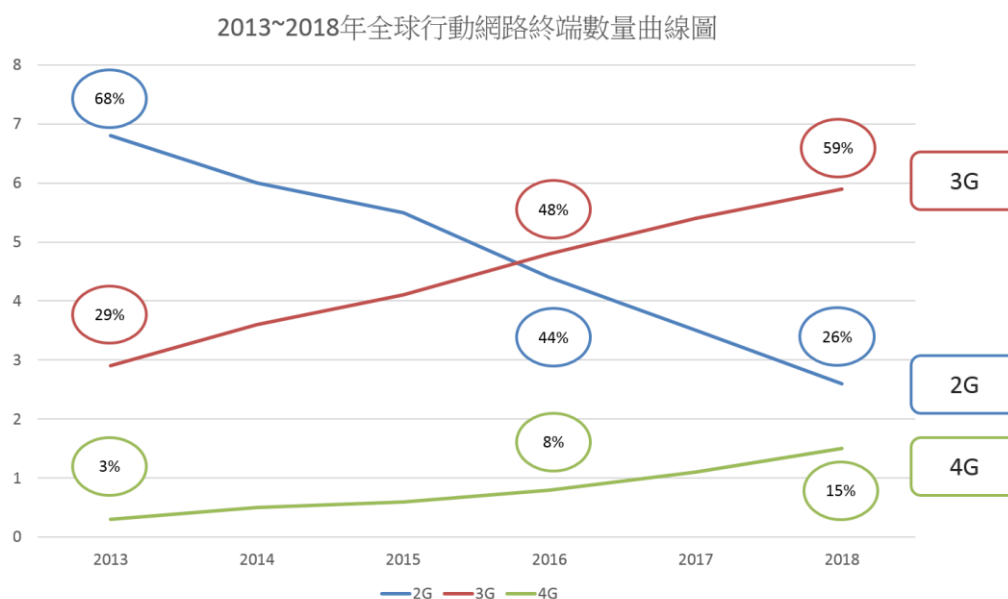


圖 3- 12 2013~2018 年全球行動網路終端數量曲線圖

資料來源：Cisco VNI Mobile，MIC 整理，2014 年 5 月

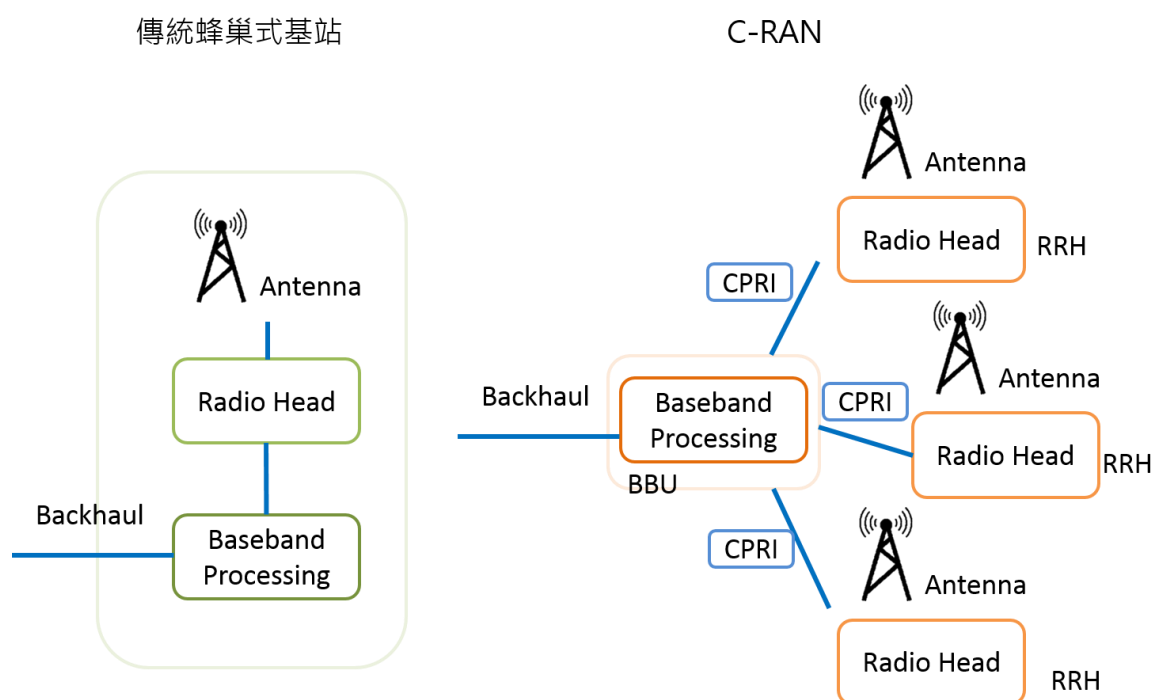


圖 3-13 蜂巢式基地台與 C-RAN 架構示意圖

資料來源：MIC 整理，2016 年 2 月

由於 ITU 發佈的《5G 願景與需求》中明確的提出 5G 必須所提供的峰值速度、延遲速率以及用戶體驗速率等(詳細數據請參見表 3-4)，因此在此高標準的定義中，BBU 與 RRH 中傳輸的流量上升快速，但根據資策會產業情報研究所(MIC)所發布的《營運商 5G C-RAN 發展動向分析⁸⁴》所述，目前 CPRI 只能夠負荷 10Gbps 的流量，因此無法滿足 5G 的流量速率需求，因此如何突破這個困境仍是 C-RAN 主要探討的目標。

綜合以上所述，5G 網路通訊時代與傳統網路相比最大的差異為傳統網路不需要面對多樣化的場景，主要為手機、平板等提供較單一服務；5G 網路不僅僅要應付多樣化的場景，各個場景所需的需求也不盡相同。基於此出發點，5G 網路環境相對於傳統網路將有革命性的改變，除了有網路切片概念產生，基站佈建及硬體結構方面更是與以往不同。

2. 5G 攻擊趨勢

⁸⁴ 資策會產業情報研究所(MIC),“營運商 5G C-RAN 發展動向分析”, 2016/2/26.

5G 與過去幾代無線行動網路區別主要是提供更高速的網路、更高密度的數據流量、更大量的設備連接數目，因此未來將部署數量眾多的基站，過去的系統並未考量到這種密集佈建節點的網路場景可能會造成的安全威脅，因此 5G 在制定規格之際也必須將各種服務的安全需求納入考量以避免安全威脅，根據 5G-PPP 的安全白皮書「Phase 1 Security Landscape」⁸⁵中提及了 5G 的安全威脅及安全建議如表 3-5。

表 3- 5 5G 網路安全威脅及安全建議

安全威脅	安全威脅內容	安全建議
(1) 無線接入網路威脅	主要威脅之一是阻斷服務攻擊(DoS)，5G 設備廠商另外還提到了幾項問題，例如無線電波密鑰傳輸問題、用戶資料完整性保護問題。	強化元件基礎層的連網安全，採用適當的存取控制機制對使用者授權、識別，並可讓網路管理員及時檢閱既有帳戶有效性避免遭受惡意或未經授權的存取。
(2) 網路設備	① SDN 威脅 • 應用層:包含訊息洩漏、通訊挾持、API 濫用等威脅。 • 控制層:網路操縱威脅會影響對網路集中管理的策略。 • 用戶數據保護:主要威脅包含 DoS 攻擊和通訊挾持。	為 SDN 建造一個檢測系統，系統內容包含封包資訊檢測、IP 位址防護、高速流量檢測、最大門檻值檢測、速率限制、自動化辨別攻擊模式等防護技術整合。
	• 惡意程式攻擊 SDN 基礎設施：惡意攻擊 SDN 管理控制器會導致拒絕服	典型 SDN 系統採用的是 x86 處理器和 TLS 加強控

⁸⁵ 5G-PPP, “Phase 1 Security Landscape”, 2017.

安全威脅	安全威脅內容	安全建議
	務攻擊、開啟網路訪問權限或者淪為殭屍網路。	制層安全，但長期而言可能使控制層易於受攻擊，建議將協議控制數據與主要傳輸訊息分流，透過讓控制數據通過其他網路安全檢測措施，防止惡意程式取的基礎設施控制權限。 ⁸⁶
	② NFV 包括中斷網路切片與該切片網路組成單元間的訊號與管理、針對網路切片管理模擬攻擊、DoS 攻擊以及訊息洩漏等威脅。	可透過虛擬主級的防火牆對流經虛擬機器的封包做檢測、網路流量偵測，強化虛擬機器的安全性。 ⁸⁷
	③ 基站 低成本的硬體與硬體軟體化之間的成本平衡可能對 5G 網路造成重大威脅。	標準訂定機構必須為 5G 訂定良好的安全架構，讓設備製造商及電信業者於布建實有標準依據。
	④ 網路安全威脅-5G 安全 架構單一節點被攻擊之威脅。	強化各節點間互相認證機制、將安全需求納入 5G 訂定標準時的考量條件，如此一來可減少應注意而未

⁸⁶ 壹讀,“如何確保 SDN 基礎設施的安全?”, 2015/3/18.

⁸⁷ 台灣岱凱,“虛擬化環境的安全防護”, 2008/12.

安全威脅	安全威脅內容	安全建議
		注意的安全漏洞。
	⑤ 惡意軟體攻擊 與 5G 安全架構漏洞相比用戶設備感染惡意軟體相對容易，該點強調使智慧型手機或大量 IoT 設備感染惡意程式進而發動 DDoS 攻擊。	偵測連網的合理 IP 數量，在未被攻擊前先預設一個門檻值為單一 IP 合理同時連線數，當遭遇攻擊時大量降低該門檻值，只要網路頻寬足夠可提供服務給真正需要的連網者。 ⁸⁸
(3) 認證機制基礎架構的惡意程式攻擊 ⁸⁹	AAA(Authentication, Authorization and Accounting)指的是驗證、授權、帳號管理，如果 5G 採用了 AAA 基礎架構，在安全方面至少可以保護無線電頻率和通信數據，為 5G 提供網路服務。若有惡意程式針對 AAA 基礎架構進行攻擊，這將會危害認證機制、金鑰傳送。	評估網路設備轉發而來的用戶安全資訊，為這些用戶的要求設置安全存取伺服器為認證、授權、稽核等安全資訊作集中管理，並且與應用伺服器共同協調提供更深層憑證或安全連線。

資料來源：5G-PPP，「Phase 1 Security Landscape」

由於第五代行動通訊規格尚未標準化也還未進入商用階段，目前仍有許多國際組

⁸⁸ 網管人,“淺談 DDoS 攻擊之手法與防禦”, 2009/6/25.

⁸⁹ Cisco 思科,“思科自我防禦網路與網路存取控制”, 2005/9.

織與電信廠商研議商討中，預期在 2019 或 2020 年發表正式規格，因此在最新攻擊趨勢方面尚未有重大傳聞及危害；另外，承襲 4G LTE 的部分也尚未明訂，因此對於 5G 行動網路的防範手法目前只能提出概略性探討。

3. 5G 防護技術⁹⁰

3.1 Nokia 的 5G 安全需求

5G 提供多樣化且新穎的服務，例如自動駕駛、遠端操控機器、虛擬實境等等，正因 5G 支持了如此豐富的服務生態，因此也為網路帶來許多安全挑戰，例如兼容舊有技術存在的漏洞、確保訊號不受惡意干擾完成低時間延遲高可靠度服務以及經由大規模物聯網發起的惡意流量攻擊。目前而言，5G 面臨的最大挑戰是滿足多種應用需求的服務，為了實現這一點 5G 網路必須制定協調且一致性的安全架構，另外還須提高該架構的安全彈性以因應未來快速變遷的應用。根據 NOKIA 在 2017 年發布的安全白皮書「Security challenges and opportunities for 5G mobile networks」⁹¹以及 5G-PPP 安全工作組在 2017 年推出的安全白皮書「Phase 1 Security Landscape」提出 5G 的安全需求如下。

(1) 基本安全需求

NGMN 聯盟白皮書中強調幾項 5G 安全需求，例如：增進網路安全彈性抵抗網路攻擊、提高系統對無線電干擾攻擊的防禦能力以及改進 5G 小型蜂巢式基地台的安全性，在提出這些安全需求後 NGMN 推動 5G 的安全工作小組提交了 5G 安全建議，下圖 3-14 為該工作小組提出的基本安全需求，內容為 5G 必須包含大量物聯網以及新型應用、兼容 LTE 的保護措施以及新的網路規範，如 SDN 以及 NFV。在 LTE 的保護措施中，3GPP TR 33.821 "Rationale and track of security decisions in Long Term Evolved (LTE) RAN/3GPP System Architecture Evolution (SAE)" 中有提到 LTE 的保護措施，例如：

- 國際移動用戶識別(International Mobile Subscriber Identity，簡稱 IMSI)的捕捉保護

⁹⁰ Huawei, "5G Scenarios and Security Design", 2016/11.

⁹¹ NOKIA, "Security challenges and opportunities for 5G mobile networks", 2017.

- 用戶平面資料的完整性保護
- 服務請求不可否認性。

再者考慮到網路切片安全需求，可分為橫向安全需求與縱向安全需求：

- 網路切片橫向安全需求

將網路切片功能隔離以限制單一網路切片的潛在網路攻擊，或是單個切片網路需要符合用戶個人的安全要求。

- 網路切片縱向安全需求

必須支援垂直的網路接入認證，系統必須提供用戶 ID、憑證、身分驗證的全面靈活性。

最後列出其他綜合的安全需求：

- 防止主動捕捉 IMSI
- 減少因安全所產生的傳輸訊號負荷
- 將憑證資源設置於設備內
- 改善各類型接入網路認證與授權機制
- 群組認證
- 端到端用戶數據完整性保護

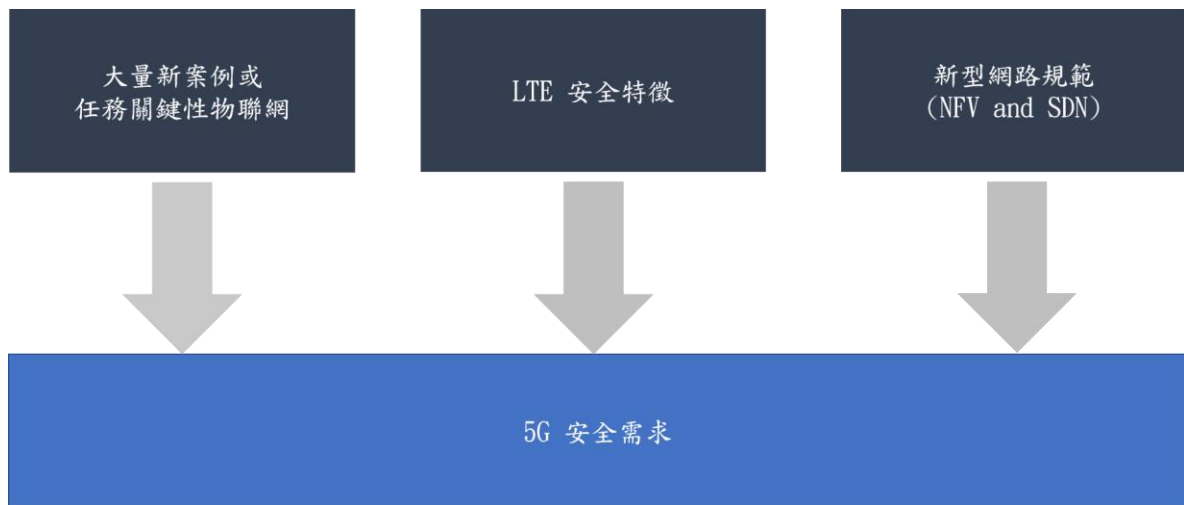


圖 3- 14 5G 基本安全需求

資料來源：NOKIA

(2) 高層級的安全願景(High-level 5G security vision)

除了上述基本安全需求外，5G 尚被賦予更高度的安全願景，包含安全內置議題、靈活安全機制、安全自動化偵測管理，圖 3-15 呈現了安全願景構成的基本要素。

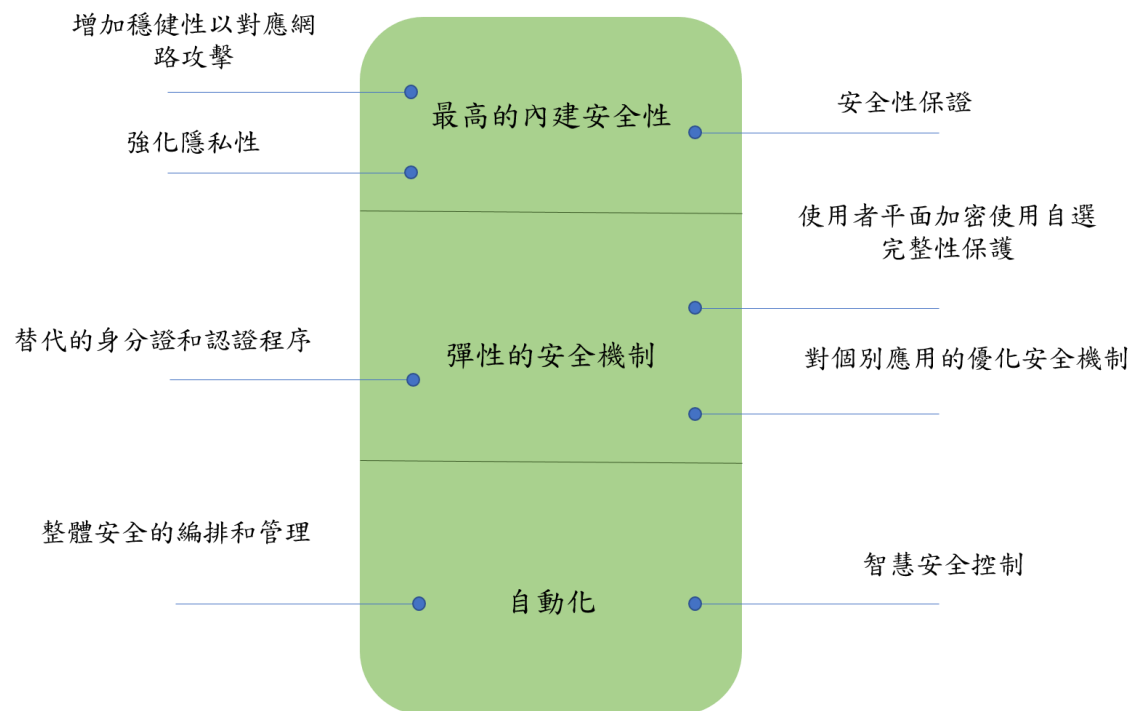


圖 3- 15 高層級安全願景的基本要素

資料來源：整理自 NOKIA

- 高度整合安全架構

5G 網路必須支撐用戶與流量非常高的安全性和隱私，同時也必須可抵禦各種網路攻擊，為解決這雙重的安全挑戰，不能僅僅將安全問題視為額外附加，安全性必須被視為整體架構的一部分。

- 靈活安全機制

針對每個不同的應用程式使用不同的安全性機制，意味著個人虛擬網路與網路切片會因應不同的應用程式給予不同的安全保護。這種靈活的安全機制包含識別及認證移動裝置/註冊資料，或確定通道上的安全機制。

- 自動化安全機制

自動化安全機制包括自動安全佈局與管理、以及智慧安全控制與偵測，前者需要正確部屬使機制有效率地持續解決多數獨立網域的安全問題，以及確定

與分配每個網域的安全策略並在動態網路中維持一致性的設定；後者需要偵測並減輕網路上未知的威脅，並且需要適應未來已知威脅的變種與進化。

3.2 Ericsson 的 5G 安全白皮書

對於第五代通信移動系統中，速度的追求雖為一大特性，但在安全與隱私上面也是有不可忽略的重要性。在 2015 年 6 月 24 日，Ericsson 公司發表了一篇有關 5G 安全的白皮書：5G SECURITY: SCENARIOS AND SOLUTIONS⁹²，提到 5G 安全環境的構想，及點出了有關 5G 的一些安全問題，如身份管理問題、5G 無線網路安全問題、雲端運算安全平臺等。

在身份管理問題方面，現階段 4G LTE 定義了由用戶身分識別模組(Subscriber Identity Module，簡稱 USIM)導入行動通訊網路的架構，此方式具有高安全性，因此在 5G 時代有希望延用此系統，但對於竊取國際行動用戶識別碼(International Mobile Subscriber Identity，簡稱 IMSI)的威脅雖然已經在制定 3G 及 4G 通訊系統時已討論過，但業界中各家電信業者卻未設計相關的保護機制，因此在 5G 系統中對於 IMSI 保護機制是否需要增強，是值得討論的議題。

另外在無線網路安全問題上，目前 4G LTE 網路已對無線網路設計相關的保護方案，如偵測竊聽，但 5G 在無線網路安全上，卻沒有針對新註冊用戶或修改帳號時的保護。在 5G 無線通訊中如工業自動化，是否需新增額外的保護也需要加以探討。

SDN 與 NFV 為 5G 電信網路服務架構的主要關鍵技術，以因應未來多變的使用情境。主要概念係以虛擬化統整硬體資源，以軟體管理及分配虛擬資源，該架構將可能在雲端運算環境中實現。因此雲端運算安全問題也成為 5G 安全之重要討論議題之一，為 5G 系統中所需考量的層面，因此 Ericsson 的 5G 白皮書提出雲端運算之安全要求，如開發具高度安全保障的管理程序及網路虛擬化技術、從現有遠端認證可信任的運算工具及概念，架構有用的安全系統及架構、如提供雲友好(cloud-friendly)加密的有效解決方案，以及開發可信賴且易於使用的雲端系統等。

⁹² Ericsson, "5G SECURITY SCENARIOS AND SOLUTIONS", 2015/6.

3.3 華為的 5G 網路安全設計

5G 行動通訊網路除了傳統的語音通訊與數據連線等常規服務，更結合了物聯網、工業互聯網、車聯網等新型服務，豐富的業務生態將支撐起完整的智慧生活網，又因為 5G 是一個真正融合社會環境中各種服務的網路系統，比起前幾代行動通訊網路，5G 在人類生活中扮演著更重要的角色，因此 5G 的安全保障也必須提升到新的高度。上述提及的安全課題其實不只針對各別服務提出，而是必須落實在 5G 的各大服務中，華為在 2016 年提出 5G 的安全需求及安全設計分為 5G eMBB、mMTC、URLLC 三大服務以及物理防護技術四大面向，說明如下。

(1) 增強移動寬頻(Enhanced Mobile Broadband，簡稱 eMBB)

為了滿足 5G eMBB 所提供的服務，例如高畫質影片傳輸，因此需要不同的安全需求以及支援高傳輸速率，5G 安全設計應考量 eMBB 服務下的核心安全功能，包括：端到端安全保護、統一認證、開放安全能力以及用戶隱私保護。如圖 3-16 所示，描述了 eMBB 服務的安全架構，透過這個模式，達成一個安全的防護平台。

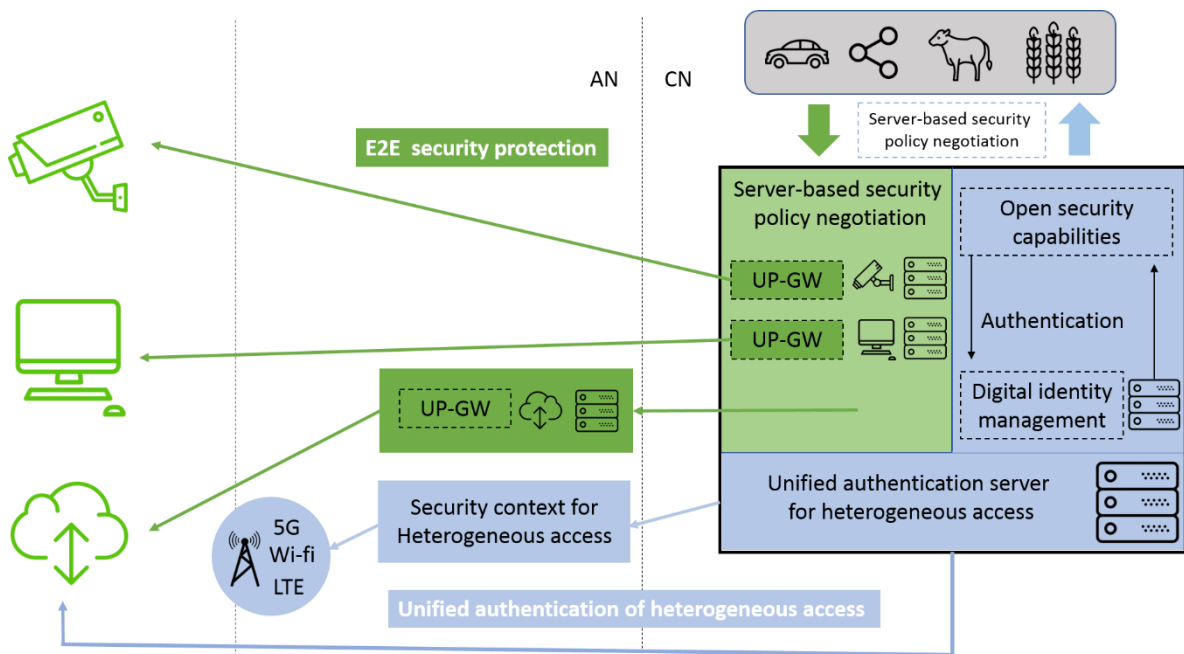


圖 3- 16 5G eMBB 異構接入網路統一認證機制

資料來源：Huawei⁹³

下列介紹 5G eMBB 服務安全設計機制：

A. 服務導向的端到端(End to End，簡稱 E2E)安全保護

在用戶設備(User Equipment，簡稱 UE)與服務終端之間設計既安全又有效率的數據保護方式。可分為以下四點概略介紹：

- 用戶終端與服務終端的 E2E 保護

E2E 的用戶數據保護起始於 UE 結束於出口閘道(egress gateway)，通常出口閘道設置於核心網路中，但在一些要求低時間延遲的服務(如 URLLC 服務)中，出口閘道則設置於邊緣網路，而無論數據傳輸至核心網路或離用戶較近的邊緣網路，都必須實行於可靠的高度安全性管道中以確保數據可安全地傳輸及儲存。

- 基於對話(session)的 E2E 傳輸數據保護

⁹³ Huawei, “5G Scenarios and Security Design”, 2016/11.

相同的 UE 使用不同應用時會傳輸不同類型的對話數據(session data)，因此 5G eMBB 安全設計應對不同應用採取差異化的數據保護，對不同對話數據採用不同保護方式也有助於增加安全保護的彈性。

- 靈活的安全策略協商(Flexible Security Policy Negotiations)

指 5G E2E 安全保護機制應具有彈性且高效率的協商且針對各種安全策略進行維護。首先 5G 網路向伺服器發出安全請求，接著伺服器會依照不同服務、網路、設備的安全能力決定採取何種保護策略，例如加密演算法、金鑰長度等等。

- E2E 用戶數據安全協議設計

上述提及不同的應用會以不同的 session 作為傳輸的協議數據單元(protocol data units，簡稱 PDUs)，如下圖 3-17 所示，E2E 數據保護會根據不同的 PDU 傳輸協定加密會話，但不會加密標頭(headers)以確保網路節點可正確判定路由資訊。

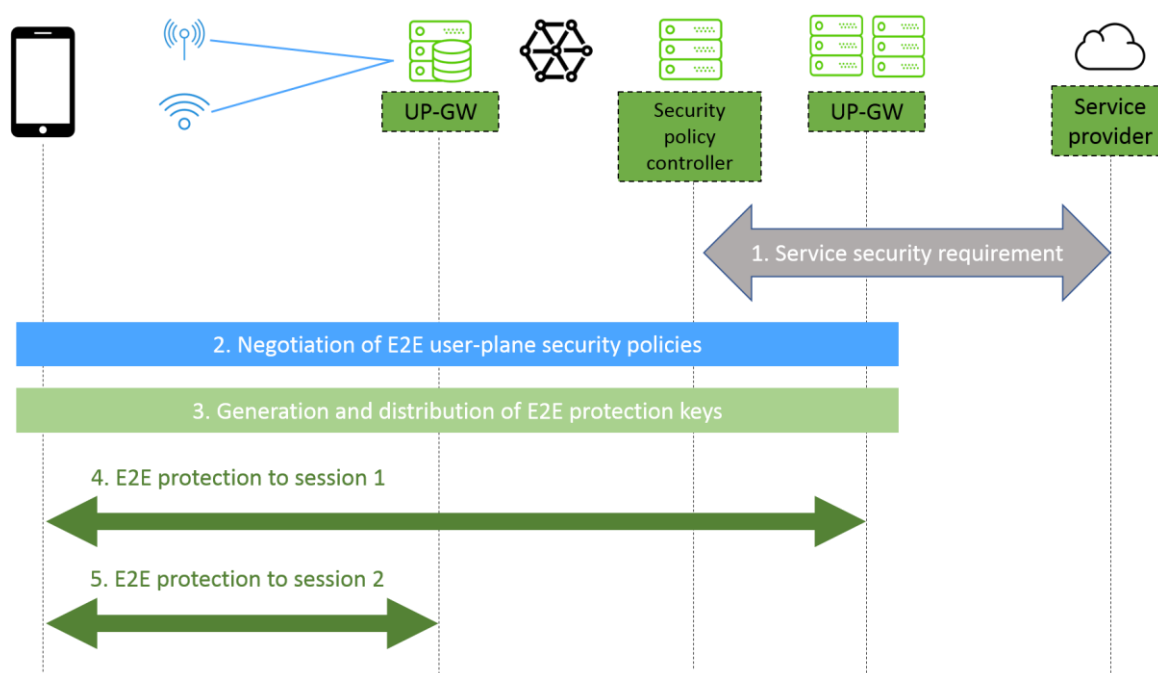


圖 3- 17 端到端用戶數據安全協議設計

資料來源：Huawei

B. 支援不同類型的接入網路和統一開放的認證框架

5G 異質接入網中包含 5G 新無線接入技術(5G New Radio，簡稱 5G NR)、LTE、Wi-Fi、3G、2G、固網等多種接入技術，傳統上不同接入方式就有不同認證框架與安全管理機制；相同設備在切換不同的接入網路時必須重新認證，這種多重認證機制並存的環境不只增加安全管理困難，頻繁切換認證也將造成額外時間延遲。5G 異質接入網路的認證與安全管理稍作介紹：

● 統一的認證框架及安全管理

為了因應 5G eMBB 服務，須建立起可支援多種接入技術與認證協定的框架進行統一的認證和安全管理，如此一來不只可降低安全管理複雜度，還能在切換不同接入網路時不需至後端重新做認證以降低時間延遲。擴展認證協議(Extensible Access Protocol，簡稱 EAP)經過多年演進可支援多種認證協定，例如 EAP 認證及密鑰協議(EAP Authentication and Key Agreement，簡稱 EAP-AKA)、EAP 傳輸層安全(EAP Transport Layer Security，簡稱 EAP-TLS)等；目前華為推薦 5G eMBB 認證框架為基於 EAP 的認證機制。

- 接入網路快速切換認證

5G eMBB 若採用 EAP 認證框架，切換不同接入網時可直接實現網路接入快速認證，不再需要像現行的認證機制必須先向終端伺服器認證用戶資料再發送認證請求，經過認證伺服器同意並發送憑證後再一路回傳至用戶終端，將會產生大量的時間延遲，5G eMBB 一改先前的認證機制，將有效的克服認證時所造成不必要的時間延遲。

C. 開放身分管理可促進 5G 生態環境的發展

電信業者採取基於用戶身分 USIMs/SIMs 建立對應的數位身分系統，該系統為全球最為廣泛使用之身份管理系統，並且得到用戶與第三方業務的高度信任；例如：許多要求高度安全性的業務會以手機簡訊發送驗證碼作為身分認證，提高第三方業務識別用戶身分的可靠度。為了因應多樣化服務融合的環境，5G 行動網路服務業者應開放基於 USIMs/SIMs 各種類別資料給予第三方業務使用，並且引進更多的認證方式增強認證安全。如下圖 3-18 所示，5G 行動網路業者可透過 API 開放身分管理與認證能力給第三方業務進入 5G 平台，一方面有利於電信業者建構以自身為核心的服務生態，增強客戶忠誠度；另一方面對於第三方業務供應商則可透過數位身份管理能力擴大自身業務範圍。

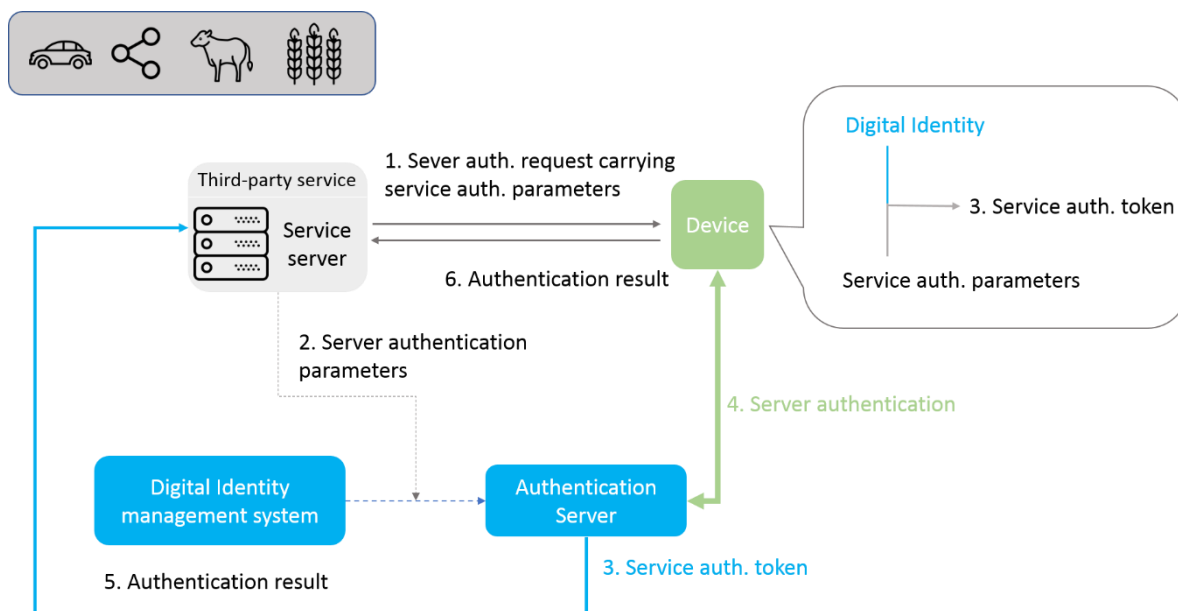


圖 3-18 開放身分管理可促進 5G 生態環境的發展

資料來源：Huawei

D. 加強用戶隱私保護

5G 網路將與更多行業與用戶接軌，用戶隱私保護也越來越備受重視，在開放式的環境中用戶 ID 需要被加強保護。其中一種方式是將用戶永久 ID 取代成隨機 ID 減少永久 ID 在空中介面傳輸被攔截或追蹤的可能，另一種方式則是利用非對稱式加密傳輸 ID。另外，由於 LTE 網路也屬於 5G 異構接入網路的一部分，因此國際移動用戶身分識別碼(international mobile subscriber identities，簡稱 IMSIs)的保護需要兼容 LTE 的認證機制，否則駭客可能利用 LTE 訊號發起降級攻擊⁹⁴，使系統放棄原本高安全性的連線(例如加密連線)反而使用老式的傳輸方法(例如明文傳輸)不法獲取用戶隱私。

(2) 大規模物聯網(Massive Machine Type Communications，簡稱 mMTC)

5G mMTC 的安全設計著重於降低身份管理的成本以及大量物聯網設備連接，過去基於 SIM/USIM 的身分認證機制成本較為高昂，若適用於 mMTC 服務將造成過大

⁹⁴ Google, "This POODLE Bites: Exploiting The SSL 3.0 Fallback Security Advisory", 2014/9.

的成本負擔，因此考慮採用去中心化方式管理 5G 物聯網中設備的接入認證與身份管理，相較於傳統的認證方式，去中心化機制可避免單一節點瞬間受到大量流量攻擊，降低遭受分散式阻斷服務攻擊(DDoS Attacks)風險。以下三點說明去中心化模式下身分管理與認證的安全機制設計：

A. 分層身分管理降低管理複雜度

網路與業務的分層身分管理有助於區別電信業者以及與電信商合作之產業的管理職責，並可為客戶量身打造專屬身份管理策略，對 5G 電信業者而言有很多種實現網路與業務分層身分管理的方法，例如：網路與第三方的信賴憑證可單純經由電信業者生成，或是電信業者與客戶端共同產生。

B. 去中心化認證機制有助於改善安全管理效率

5G mMTC 認證節點應以去中心化作為設置要點，例如將認證節點下放邊緣網路，如此一來在設備與網路之間的交互認證將不再需要連接核心網路中的用戶資料庫。如下圖 3-19 所示，非對稱式密鑰管理系統基於去中心化概念，網路不需要儲存設備的密鑰或者設置一個永久連線的身分管理中心節點。

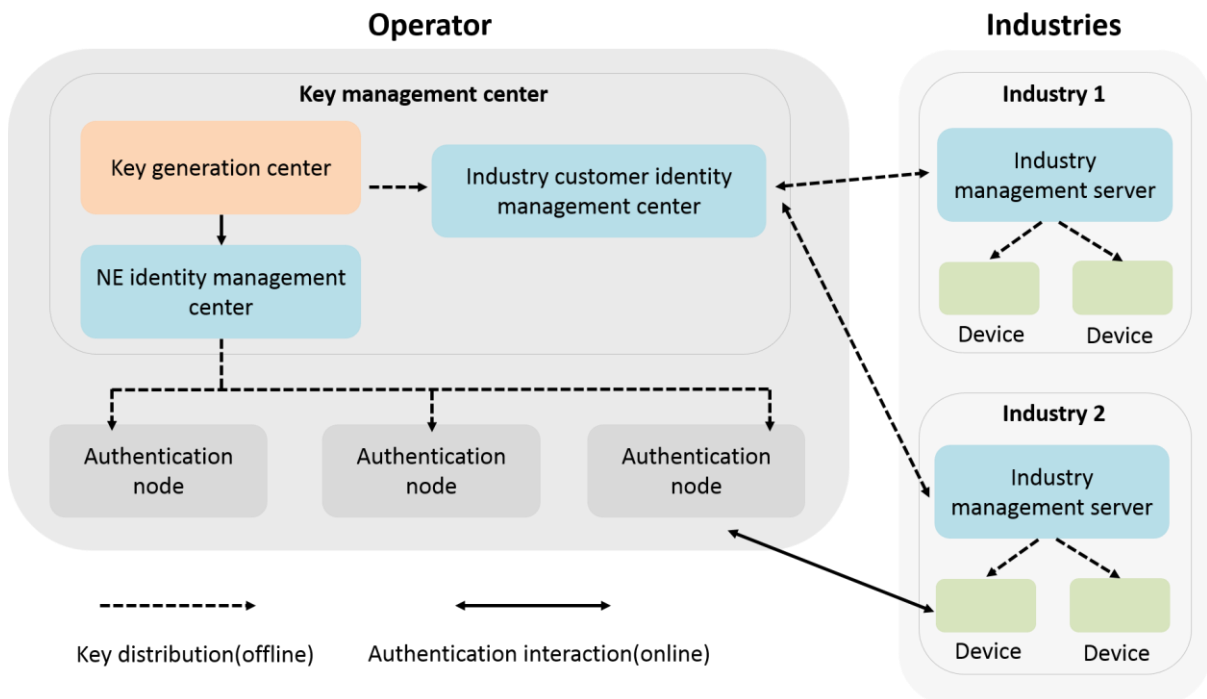


圖 3- 19 mMTC 去中心化身分與密鑰管理

資料來源：Huawei

C. Identity-Based Cryptography(簡稱 IBC)去中心化的身份管理認證

有別於一般認證管理，為了改善傳輸效率，IBC 身份管理用 ID 當作公鑰，進行認證時就不需要發送憑證。IBC 身份管理易於連結網路與其他應用的 ID，對於修改或制定身分管理策略具有相當大的彈性空間。如圖 3-20 所示，在車聯網中車輛頻繁地廣播訊息，為了過濾車輛系統間非法訊息交換，因此所有廣播訊息皆需攜帶著身分訊息進行認證，為了節省空中傳輸介面資源，5G 的安全設計將限制車聯網廣播訊息的長度，避免訊息太長或認證回合數太過頻繁增長時間延遲，因此在車聯網中的車輛都具備一個 IBC 的身分及密鑰，在進行廣播過程中直接使用 ID 即可完成驗證。採取 IBC 認證機制可減少認證訊息長度與認證回合數，符合 5G mMTC 服務安全高效率的要求。

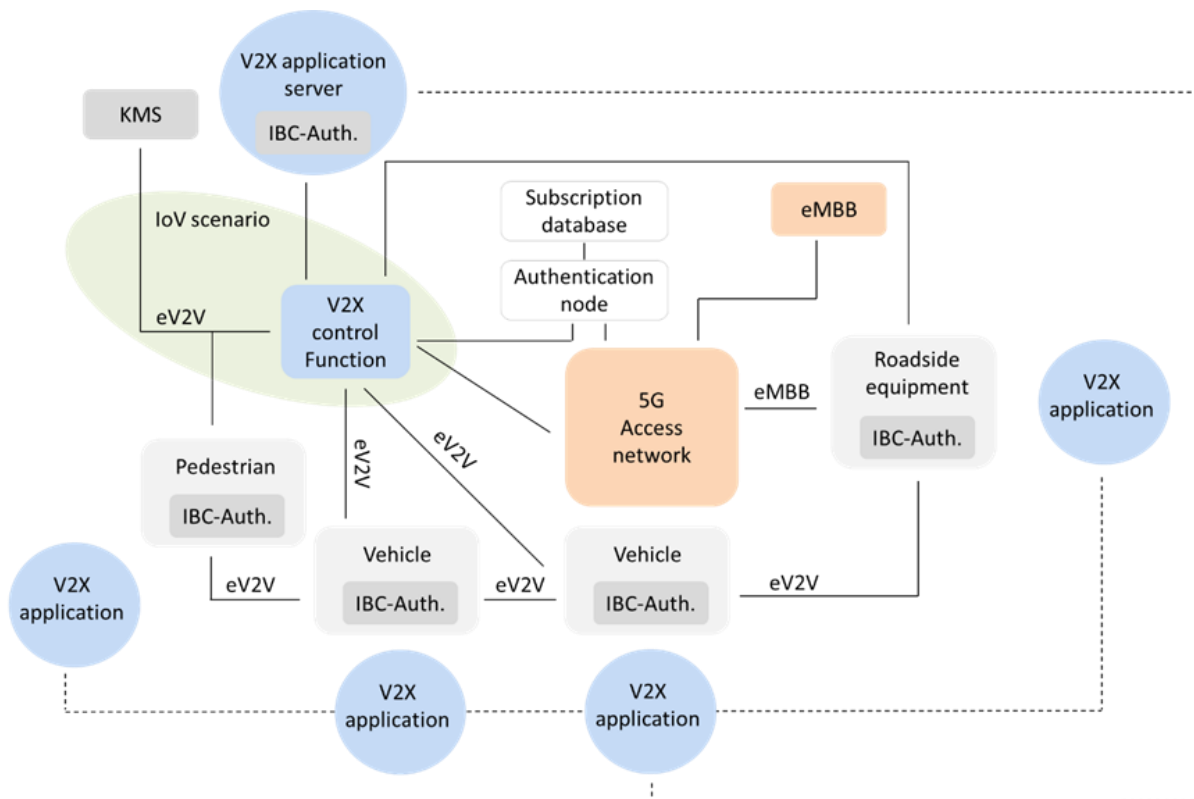


圖 3- 20 IBC 去中心化的身份管理及認證

資料來源：Huawei

(3) 低時延高可靠度連接(Ultra-reliable and Low-latency Communications，簡稱 URLLC)

5G URLLC 服務的安全需求包含超低時間延遲的接入認證、傳輸數據保護以及認證快速切換，端到端時間延遲以及各種異質網路節點時間延遲的累加，為達到毫秒等級的時間延遲服務，5G 數據傳輸時各環節皆須進行時間複雜度優化，採用下列五項措施將能迎合 5G URLLC 的安全需求：

- 改進空中介面的傳輸效率
- 制訂完善 5G 網路架構
- 減少數據傳輸必經的節點數目
- 改善網路傳輸協議
- 提高編碼與解碼效率

以下針對 5G 4 大安全面向包含接入認證的時間延遲、切換時重建認證的時間延遲、傳輸時數據保護的時間延遲以及靠近用戶端加解密的時間延遲對應的安全設計機制說明如下(如下圖 3-21)。

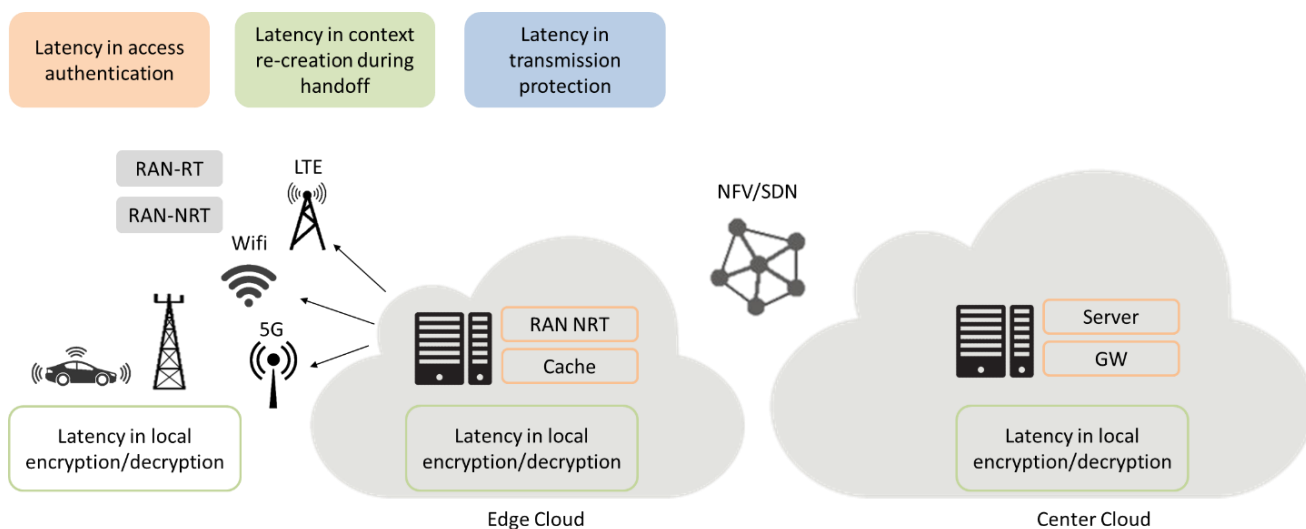


圖 3- 21 5G URLLC 4 大安全面向

資料來源：Huawei

A. 減少身分認證所產生的時間延遲

要降低設備終端與網路之間認證的時間延遲可透過以下方式達成：

- 減少設備終端與認證伺服器間的物理距離

採用分散式認證將認證伺服器從核心節點中下放至設備終端附近，如此一來縮短認證鏈可使認證訊息傳輸更快速。

- 降低認證協議的複雜度

建立更有效率的認證協議機制，例如：減少參數數量、訊息長度以降低雙向認證訊息處理時間和本地計算量。

B. 減少由數據傳輸安全保護所產生的時間延遲

傳統的數據傳輸安全機制中訊息的長度較長，額外的負載(payload)也是增加傳輸負荷的主因之一，有時在資料長度較短的傳輸服務中安全負載甚至超過訊息本身長度；

因此考慮研發新的演算法，包含減少加密、完整性保護等等所造成的額外開銷；另外，應提供數據具備從設備終端到服務出口開道 E2E 的加密保護，如此將避免數據經傳輸節點時反覆加解密造成的安全保護時間延遲。

C. 減少認證切換所產生的時間延遲

高速行驶的車輛或高鐵中設備需要進行快速的網路切換，在 4G 的安全機制中，要完成網路切換前基站需要計算、發送並接收安全密鑰；但是在 5G 行動網路架構中，基站將以超高密度部署，因此不同的接入系統、不同的接入技術、不同基站之間彼此協議將是普遍現象，這將是 URLLC 服務要求超低延遲的一大難題。而解決上述問題可採取的措施包含：異構多層接入網路的統一認證、高效率的認證演算法推導以及減少認證傳輸必經的節點數目等。

D. 減少網路節點中反覆的加解密

密碼演算法常採用複雜的邏輯運算，為了減少複雜的邏輯運算，過去傳統通訊系統大多以硬體加速方法，例如採用專門計算密碼演算法的晶片來操作加解密。5G URLLC 為了使本地加解密更快速，可採取的措施包含：引進更有效率的加密演算法、利用虛擬化網路或雲端網路中的計算資源、實施硬體加速以及採用可進行平行運算的加解密演算法等。

(4) 物理安全⁹⁵

由於 5G 的網路環境和以前的網路世代比較起來大相逕庭，在硬體層面除了基站結構改變外，對於伺服器的管理也從原本的單一功能對應單一硬體改變成以 NFV 虛擬化。在安全方面除了承襲之前世代的佈署，5G 網路生態系統必須有創新的安全機制，如此一來才可以提供電信業者或者使用者更全面的保護。

對於無線電傳輸期望達到的目標為在良好的通訊環境下，傳輸的訊息能不受竊聽或者中間人攻擊等惡意攻擊，因此在傳統的無線電傳輸安全機制中，通常以兩種機制做為安全的防護：

- 訊息加密

⁹⁵ 黃開枝，金梁，趙華，“5G 安全威脅及防護技術研究”，2015/6.

於訊息傳送時將明文加密，雖然可防止攻擊者得到密文卻無法立即得到原始訊息，但也衍伸出密碼管理、密鑰管理以及密鑰在傳輸通道中傳遞可能會發生的威脅等。

● 超寬頻傳輸

超寬頻為一種無載波的通訊技術，優點為速度快、傳輸量大，由於超寬頻的特性因此具有良好的保密性，可以提高訊息在通道傳遞中的隱蔽性，不過一旦攻擊者將訊號解調就會失去安全防護作用。

基於上述兩點，5G 必須尋找更多安全機制去支持網路生態的運作，包含利用高密度的基站佈建、雲端伺服器配置不同以及異構接入等 5G 特殊的網路環境物理特性，可研究訊息的安全傳輸、加密演算法、密鑰生成機制、端到端隧道協定機制、加強雙向認證以及異構接入認證等安全防護機制。以下兩點為針對物理層安全技術做簡介：

A. 端到端(End to End，簡稱 E2E)隧道密閉防護機制

在現存的 2G、3G 甚至是 4G 的網路傳輸中，身份訊息等較為私密的訊息往往是不經過加密直接在頻道中做傳輸，才能通過後端的身份驗證。但其實傳輸頻道中並不一定是安全的環境，因此在 5G 增加大量業務的情況下，須將用戶的私人資料於傳輸時做安全的保護並且不影響後續的身份驗證，才能減少訊息在頻道中傳輸時的安全疑慮。

B. 加強雙向認證

在 2G 時代，由於沒有做好基站與電信業者或使用者之間的雙向認證，導致偽基站猖獗。在 4G 時代雖然已有雙向認證的機制運行在基站與電信業者或使用者間，但在 2016/9/6 駭客 Seeker 於 KCon 上提出了偽基站高級利用技術——徹底攻破短信驗證碼⁹⁶，代表著 4G 基站的雙向認證也不是這麼安全。除了與基站間的雙向認證，5G 引入了邊緣雲以及核心雲的概念，因此要如何讓雙方之間做一個安全的雙向驗證，也是 5G 安全值得探討的議題。

⁹⁶ Seeker on Hacker@KCon, “偽基站高級利用技術——徹底攻破短信驗證碼”, 2016/9/6.

(三) 軟體定義網路(Software-defined networking, 簡稱 SDN)

傳統的網路架構中，封包行進的方向由各個獨立的路由器藉著自我學習的方式，決定此訊息最終的傳遞路徑，而眾多的獨立個體導致封包流向不易掌握，或是當網路出現問題或系統維護、更新時，網路管理員必須檢查所有的路由器得以除錯及調整，使得管理極為不易。

軟體定義網路(Software-Defined Networking, 簡稱 SDN)為近年興起的新型網路架構。而 SDN 網路概念的提出，無疑是傳統網路架構的一場新革命，而 SDN 的起源最早可追溯至 2006 年，美國 Stanford 大學 Nick McKeown 教授引領的學生 Martin Casado 於網路安全與管理的科研項目中研發出的網路模型—Ethane，此項目可說是衍生出 SDN 架構的墊腳石，藉此項目的深入研討⁹⁷，Nick McKeown 教授及學生 Martin Casado 研發出 Openflow 協議，並且於 2008 年正式於 ACM SIGCOMM 發表《OpenFlow: Enable Innovations in Campus Network》，此論文中敘寫了 OpenFlow 的核心概念及應用⁹⁸，緊接著於 2009 年 Nick McKeown 教授於 IEEE INFOCOM 2009 Keynote Talks 發表 SDN 架構概念，正式將此新興網路架構嶄露於大眾眼前⁹⁹。

SDN 相較於傳統架構，如下圖 3-22 所示，思路上最大的差別在於將路由器中控制封包傳送目標的決策權分離並匯集成一個中央處理系統(路由器只需負責封包的傳遞)，讓網路的管理更為集中。因 SDN 具有可程式化的特性，網路管理員只需要利用軟體實作，即能在不改動硬體的情形下直接控制路由器的行為或是修改通訊協定，達成網路自動化，使其更靈活、更快速地做出及時回應、可照當下需求而縮放網路規模，除了大幅降低管理難度，提升網路效能，更能節省支出。對於 SDN 及傳統網路架構各方面的差異，本團隊整理表格 3-5 以更加清楚表示兩者之區別。

引用 SDN 的首當其衝為著名企業 Google¹⁰⁰，於 2012 年已利用兩年的時間將 OpenFlow 傳輸協定為主要基底的 SDN 架構取代原先資料中心的傳統網路架構，原先只達三成的頻寬使用率，最後竟達到了將近 95%的使用率，成功改善無法善用所有頻

⁹⁷ Martin Casado, Michael J. Freedman, Justin Pettit, Jianying Luo,

, Nick McKeown and Scott Shenker, "Ethane: taking control of the enterprise", 2007/8.

⁹⁸ Nick McKeown et al., "OpenFlow: enabling innovation in campus networks", 2008/4.

⁹⁹ IEEE INFOCOM 2009, "INFOCOM 2009 Keynote Talks", 2009/4.

¹⁰⁰ Amit Agarwal, "SDN@Google", 2012/7/17.

寬資源的問題，隨後近年眾多網路服務者、電信業者皆逐一踏入 SDN 架構的研究，如 2016 年間美國與英國皆有 SDN 研究成果，美國通信服務供應商 AT&T 打造出 SDN 全新框架 ECOMP，並發表「ECOMP Architecture White Paper」¹⁰¹，AT&T 表示此文件期望能成為以 SDN 及 NFV 為基底建置電信網路的指導方針，且能達到高彈性的網路資源使用；英國電信 BT 推出建構在 SD-WAN 技術的新功能—BT Connect Intelligence IWAN¹⁰²，所謂的 SD-WAN 即為將 SDN 延伸運至廣域網路(WAN)的新興技術，而此功能主要功用可幫助網路流量的預測，並且改善與提高軟體性能。近幾年，各國最受討論的通信網路議題即為下一世代通訊網路—第五世代移動通訊系統 5G，且於國際間發表的各版 5G 白皮書中皆表示描述，如：5G-PPP、NGMN，SDN 必為搭建 5G 網路不可或缺的零件，藉由 5G 議題的推動，導致 SDN 的議論度又再度提至高峰。

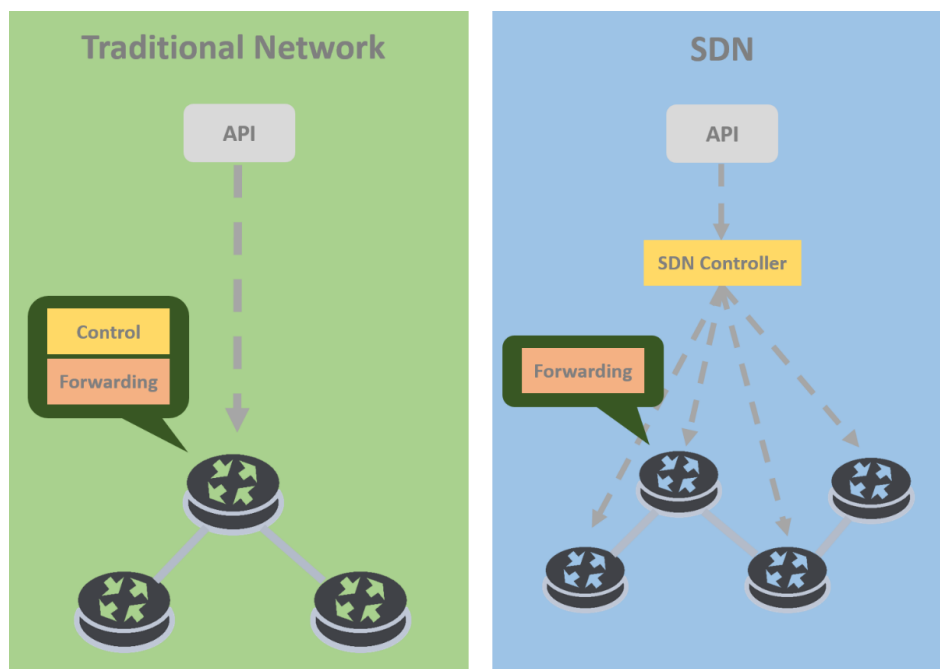


圖 3-22 傳統網路架構與 SDN 架構比較圖

資料來源：整理自「Open Networking Foundation」¹⁰³及「SDN architecture」，2014/6

¹⁰¹ AT&T, “ECOMP Architecture White Paper”, 2016.

¹⁰² Nav Chander, Courtney Munroe, Melanie Posey, “BT’s Connect Intelligence IWAN SD-WAN Solution — New Communication Choices for the Cloud-Connected Enterprise”, 2016/1/28.

¹⁰³ Open Networking Foundation, “SDN architecture”, 2014/6.

表 3- 6 傳統網路架構與 SDN 架構的比較表

	傳統網路架構	軟體定義網路
調整設備配置之媒介	設備商提供之應用程式、控制指令集	企業可基於控制器提供之 API，根據本身需求設計出控制應用程式
調整設備配置之單次調整數目	一台設備	管轄下所有設備
網路封包轉送方式	單一設備封閉決策。 設備具有控制兼轉送功能，且透過自身計算出最短路徑再進行發送。	中央集權控制決策。 設備只具有轉送功能，並且控制器根據使用者需求而設置的最佳路徑。
部署設備相容度	基於各設備商的設備各家設備研發時依附的作業系統不同，設備設定的控制指令集相異，導致企業如選購多家廠牌的設備容易產生管理困難的問題，因此具有相容性低的問題	由於設備配置管理是經由控制器集中管理，因此選購設備要求只需設備支援與控制器間的通訊協定即可

資料來源：整理自 Open Networking Foundation 及 SDN architecture

1. SDN 架構

SDN 之架構將分為兩部分進行介紹，第一部分為最起始開放網路基金會(Open Networking Foundation，簡稱 ONF)所提出的 SDN 架構，於此本團隊大致介紹各層功用以及運作方式，第二部分為現今最為推崇之三種 SDN 延伸成果，三種皆實現 SDN 主要概念，但於內涵卻大相逕庭。

1.1 原生架構

自 SDN 網路框架提出，OpenFlow 概念為 2008 年美國 Stanford 大學由 McKeown 教授帶領的 Clean Slate 小組所提出，以此概念為鋪墊，2008 年其團隊隨後便發表 OpenFlow 技術¹⁰⁴，2011 年開放網路基金會(ONF)成立，主力推動 SDN 之應用、推崇 OpenFlow 南向協議，並且提出一套 SDN 基礎架構，且受到科技界的廣為認同，而此架構便是作為世人沿用的 SDN 基礎架構。

¹⁰⁴Nick Feamster, Jennifer Rexford, Ellen Zegura, “The Road to SDN: An Intellectual History of Programmable Networks”, 2014/4.

SDN 藉由變更傳統的網路架構以達到中央集權控制的目的，改變硬體封閉性的自我控制管理，將資料層中的網路設備之決策控制權分離出來成一層控制層，而網路管理者只要對控制層中的控制中樞發送命令，控制中樞即會根據命令內容一一傳送至設備更改設定，此時架構就會呈現成起初定義 SDN 基礎架構如圖 3-23，由上至下分別為：應用層、控制層、基礎設施層¹⁰⁵。

(1) 應用層 (Application Layer)

網路管理者透過操作軟體，隨時監視底層設備運行情況以及管控底層設備，而這些相關軟體皆是屬於應用層。現今網路需求迅速膨脹，管理網路設備種類也同樣迅速上升，SDN 控管軟體並非侷限於一般交換器 Flow 流向控制，同時也隨著 SDN 的嶄露頭角，發展出多樣應用程式，如負載平衡、安全(防火牆)、監控、效能控管等等。

於應用層的北向接口(Northbound Interface)係來自應用層的網路管理者傳遞下來的控制命令以及底層監控狀態的訊息必須回報於網路管理者，北向接口(Northbound Interface)即作為應用層與控制層交換訊息的重要橋樑。

現今尚未出現一套全球公認的標準來奠定北向接口及南向接口。相對於南向接口面對的是行為較單一的網路設備，北向接口必須因應上層應用層的各種業務需求，須應付的情況較為多樣化，導致制定北向接口的標準較為困難許多。

但是成功制定北向接口標準，將可帶來極大的利益，因此多間資訊研發企業皆提出各種策略應對此場北向接口標準的戰爭。傳統設備商提供 API 作為北向接口給使用者直接管理設備層，為傳統設備管控上增添了靈活性；許多研發 SDN Controller 廠商推出的產品中，增添了北向接口，以便未來使用者可自行開發應用。除了上述直接著手產品的廠商以外，Linux 基金會為了研發出一套不偏袒任一廠商的共同標準，推出了一個開源社區為 OpenDayLight(ODL)，此社區聚集眾多擁有豐富專業知識的專家，共同探討、分享專業知識及研究發現，期許能研發出大眾公認的北向接口標準。

(2) 控制層 (Control Layer)

控制層中的 SDN Controller 為 SDN 核心大腦，其中附有各種控制模組以因應各種網路管理需求。SDN Controller 會接受至上層應用層給予的命令，經由解讀並決定

¹⁰⁵ 張衛峰, “深度解析 SDN：利益、戰略、技術、實踐”, 2014/6/6.

採取之策略後，便往下傳遞控制信息控制網路設備，同樣也會從底層設備層接收到詢問資料傳輸路徑，如不知名的封包，底層設備即會詢問 Controller 該封包路由決策，抑或網路拓樸的運行狀況，再往上層告知網路管理者目前網路情況。

現今時代網路蓬勃發展，網路類型多不勝數，因此為因應這些情況，目前 SDN Controller 已研究發展出多種不同的類型，得以滿足各種需求，如：NOX、Maestro、Beacon、Floodlight¹⁰⁶等。一個小型網路也許可只使用單一的 SDN Controller，但是控制的對象換成大型網路，一個 SDN Controller 是無法吸收那麼龐大的數據流，因此控制層中所放置的 SDN Controller 是可以為複數的，其中 Controller 之間的關係，不管是平等的，還是上對下的，皆能以網路管理者的需求來設計，但是對於 SDN Controller 之間溝通的東西向接口尚未有標準訂定。

在控制層的南向接口(Southbound Interface)，是 SDN 實現底層網路設備控制，不論是基本設備透過南向接口上報網路拓樸的監控狀態，抑或當 Controller 將路由政策制定或路由更新透過南向接口往下傳遞，皆必須透過南向接口作為溝通橋樑。南向接口與北向接口相同，尚未有統一的標準，因此存在各式各樣的南向接口 API 及 protocol，如 OpenFlow、OVB-DB、NETCONF、PCEP..等等，而其中 OpenFlow 是最為影響力的 protocol，也是最早出現的始祖，藉於 OpenFlow 的普及率，多數 Controller、網路設備都是依循 OpenFlow 協議設計。

(3) 基礎設施層 (Infrastructure Layer)

SDN 的起因雖是由交換器開始，但基礎設施層能存在的設備不只是交換器，也有可能會是防火牆、路由器、無線產品等，再者 SDN 基礎設施並未只拘泥於實體網路設備，目前虛擬網路設備同樣也可以實現 SDN。建立 SDN 的網路架構，此層網路設備必須是要能符合南向接口所適用的 protocol，Controller 才得以順利集中管控以下所有網路設備。

¹⁰⁶ 林傳筆,盧皓威,陳堃維,王永祥,“軟體定義網路(Software-defined Network)之實作”, 2014.

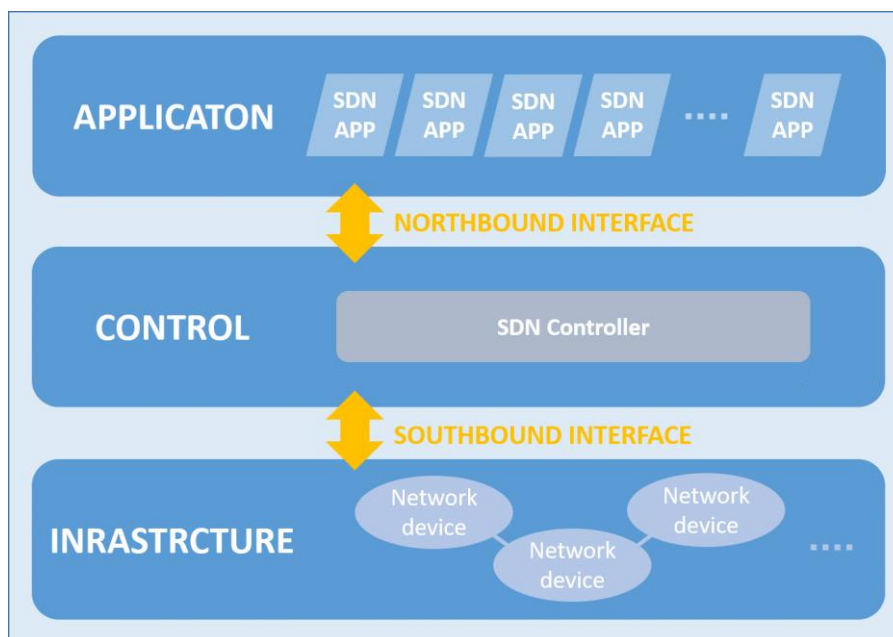


圖 3- 23 SDN 架構示意圖

資料來源：Open Networking Foundation, “SDN architecture”, 2014/6

1.2 實作架構¹⁰⁷：Open Network Operating System(ONOS)、OpenDayLight(ODL)、VMware NSX

藉於 SDN 此種新興網路架構，對於上至與網路息息相關之企業，下至生產網路底層設備之廠商皆有一定程度的衝擊，自 OpenFlow 概念提出，陸續有許多 SDN 產品推出，而其中最為廠商所青睞的即為 SDN Controller，但多種的 SDN Controller 皆未能符合商品的資格，缺少可擴展性、可靠性，難以在企業普及化，但於近年，Linux 基金會的 OpenDayLight(ODL)專案及 ON.Lab 的 Open Network Operating System(ONOS)帶來一線曙光，兩者皆克服過往 SDN Controller 的缺點，並受到各大企業的認同。除了以上兩種可運用於虛擬設備及硬體設備的產品，虛擬著名廠牌 VMware 推出 VMware NSX，此產品異於前兩者，此屬於建立虛擬網路。

(1) Open Network Operating System(ONOS)^{108、109}

¹⁰⁷ 高娟,“既生瑜何生亮？解讀 ODL 和 ONOS 之爭”, 2016/4/27.

¹⁰⁸ 王韋程,“獲電信業及網路設備商支持 ONOS 躍居 SDN 控制器主流”, 2017/1.

¹⁰⁹ 王韋程,黃秉鈞,“軟體定義網路中邊界閘道協議之實作”, 2016/10/4.

ONOS 為 2014 年 12 月 5 日為非營利組織 ON.Lab(Open Networking Laboratory)所發佈，此系統開發角度主要以電信服務供應商出發，因此較傾向於控制層與基礎設施層的分離，不須被網路硬體綁手綁腳，可以在網路控制的部分站穩腳步。異於前兩年發表的多樣 SDN Controller，此系統具有高擴展性、高可靠性及高性能，在存在千萬個用戶的網路環境下，仍然能夠高穩定運行及控管。

ONOS 區別於以往 SDN 架構實現主要的特色分為兩大特點分散式核心結構、北南向介面抽象層，這兩大特點導致架構與 SDN 基本架構產生了些許的偏差，其架構圖如下。

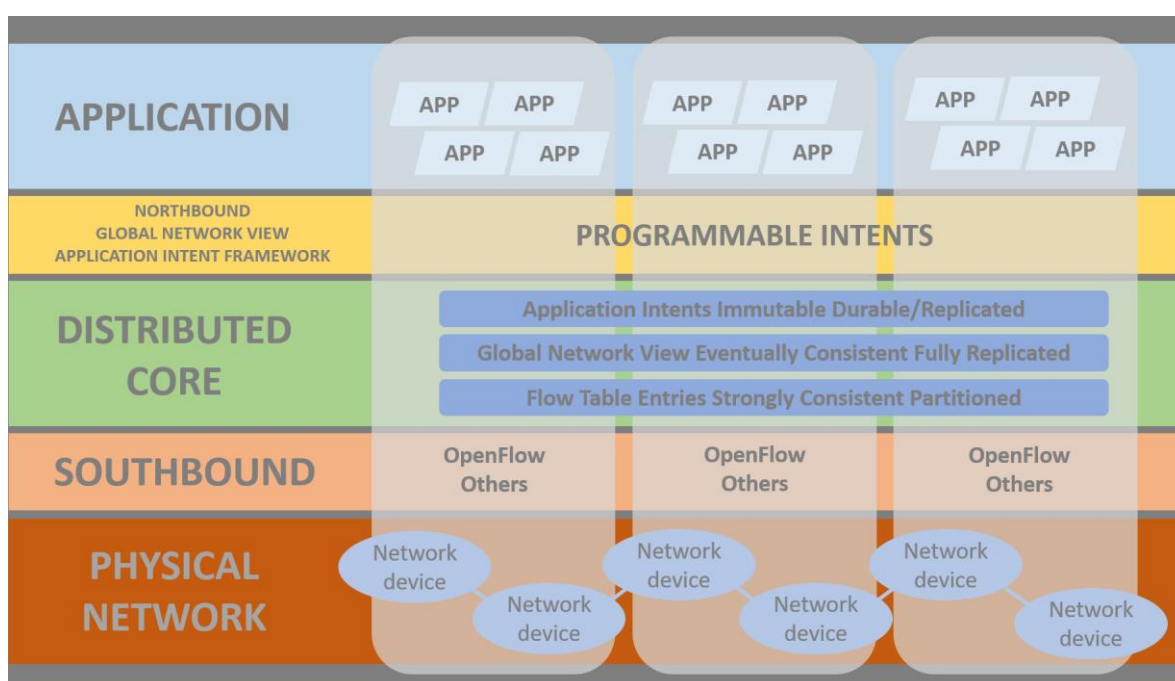


圖 3- 24 Open Network Operating System 架構示意圖

資料來源：ON.Lab, "ONOS Architectural Progress"¹¹⁰, 2014

ONOS 為一個分散式的叢集(Cluster)，此架構以分散式的 ONOS 系統聚集而成，叢集中所有 ONOS 利用 Raft 同步技術使得所有系統內部訊息一致，而此系統數量隨使用者意願動態增長或刪減以達到可擴張性，並於任一系統內部發生問題或者損壞時，可在服務、監控不中斷的情況下，迅速以運作正常的系統替換，以達到高可靠性，再

¹¹⁰ ON.Lab, "ONOS Architectural Progress", 2014.

者透過分散式運算的方式可達到高效能性。

北向介面抽象層擁有兩個核心功能，分別為：意圖框架(Application Intent Framework)、全局網路視圖(Global Network View)，意圖框架的設計使得使用者可以不需充分理解 Controller 內部運作的情況下，只需透過應用層將自身的「意圖」傳導下去，ONOS Controller 便會解析其意圖，並擬定最佳策略並且執行，此特點於電信服務供應商可謂最大的吸引力，不須了解內部運作，只需專注於應用開發即可滿足需求。全局網路視圖則是為使用者提供網路中各節點的狀態參數，並且使用者可直接對視圖上的各節點做調整，於使用者來說管理的複雜性驟降。

ONOS 為應付目前多個南向接口協議的情況，在南向介面抽象層中以「多插孔」的形式，網路部屬者可因應自身所運用的網路設備類型，而決定該使用何種協議，Controller 透過南向介面抽象層即可將底下設備視為同種網路設備控管。

如今 ONOS 部屬的主要客群分為學術網路與科學研究網路，並且絕大部分其選擇用 ONOS 即是因為 ONOS 其中具有 SDN-IP 的應用，其應用可讓使用者建立的 SDN 網路可透過邊界閘道器協定（Border Gateway Protocol，簡稱 BGP）連接至外部的網路。目前部屬完成之單位如下：美國 Internet2(I2)、韓國 KREONET、台灣 NCTU 交通大學、銜接 5 個拉丁美洲學術網路的 AmLight 網路。

除了直接採用 ONOS 的案例之外，於歐洲的 GEANT 及澳大利亞的 AARNet 研究於 ONOS 架構，並自行研發出符合自我需求的產品並引用。而中國大陸的中國天津聯通作為全球首一以 ONOS 建構出 SDN IP-RAN 企業專線服務。¹¹¹

(2) OpenDayLight(ODL)¹¹²

ODL 為 Linux 基金會發布的開源社區，在 SDN 三層式架構下誕生的新實作方法，目的在於創造中立的開放環境，其優點為對於硬體的高相容性，能支援多種協定以及虛擬機器，且不要求控制平面與設備分離，只將部分邏輯轉到控制器上，因此能以專用接口套用到現有的網路設備，保留現有架構；缺點則是網路管理者需要熟悉各個設備，因為同一組設定可能無法同時套用在它們身上。

¹¹¹ Huawei, “ONOS 總覽”。

¹¹² OpenDayLight, “OpenDayLight: Platform Overview”。

圖 3-25 為 ODL 發表的 SDN 架構圖，ODL 和原本 SDN 三層式架構最大的差別在於 ODL 在南向接口部分並沒有定義標準，且將南向接口拉出變成四層式的結構，強調能支援包含 OpenFlow 在內，如 LSIP、BGP、SNMP 等多種協定，基礎層也支援虛擬設備；相對的，ODL 提出北向接口的開放式標準，開發者能利用 REST API 介面或 OSGi 框架和控制器溝通，當定址空間與控制器相同時使用 OSGi，不同時則使用 REST。

另外，ONOS 與 ODL 架構都能提供叢集(Clustering)功能提高運算效能及管理效率，而兩者叢集運作的模式有些許不同：ONOS 中各控制器不互為 master/slave，並成為各個設備的 master 或是 slave，當設備與 master 連線中斷時再從其它 slave 中選出一個作為新 master；ODL 的叢集較為集中，控制器中只有一台 master，其餘皆為 slave，整體成為 master-slave-elements 的拓模架構。¹¹³

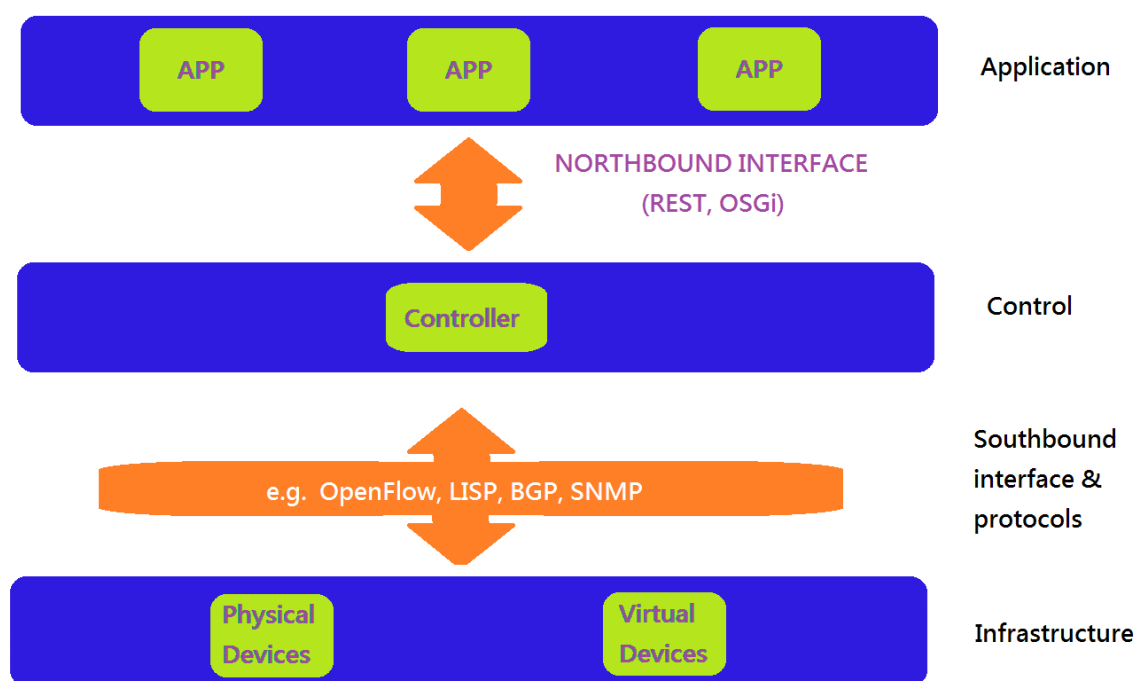


圖 3- 25 OpenDayLight 架構示意圖

資料來源：OpenDayLight, "Carbon-Fertile Ground for New Use Cases"¹¹⁴, 2017

¹¹³ 王浩丞 林盈達, "SDN 兩大控制器之比較：ONOS vs OpenDayLight", 2016/9/23.

¹¹⁴ OpenDayLight, "Carbon-Fertile Ground for New Use Cases", 2017.

現今眾多透過 ODL 成功部屬 SDN 網路的案例，如(1)韓國通訊(KT)為了提高其韓國境內的網路效率且同時可以有效降低成本而提出的 T-SDN 方案，即是透過 ODL 的控制器當作控制核心建構新型網路¹¹⁵；(2)Extreme Networks 的 OneController 是基於 ODL 的架構所開發的，目前已成功被部署於英國的恩菲爾德鎮(Enfield)以及瑪麗山大學(Mount Mary University)。現今成功使用 ODL 的案例眾多，以上例子只是於眾多案例中的其中小部分，但從上述可知，ODL 於 SDN 的市場中，確實有受到重視。¹¹⁶

(3) VMware NSX

網路虛擬化的宗旨即是要將網路從硬體的禁錮逃脫，當企業需要額外的網路資源時，不再需要特意去購買昂貴的網路設備，只要擁有穩定且高速的實體網路環境，透過基於 VXLAN、NVGRE、STT 等隧道技術¹¹⁷等虛擬網路軟體即可搭建虛擬網路，企業擁有網路需求時即能動態調動網路資源，但在於 SDN 概念發展之前，雖然已存在虛擬網路這項科技，卻礙於在需要將設備套用新的政策，人工一對一的對虛擬網路設備進行調整而導致耗費龐大人力，因此阻礙了網路虛擬化的發展。

但由於 SDN 概念的出現，SDN 突破傳統網路最大特點—網路設備集中管理，間接掙開了阻礙網路虛擬化發展的桎梏，突破了以往傳統設定方法帶來的難關，帶起了網路虛擬化之發展，多間企業積極研發相關虛擬網路產品，眾多產品中 VMware NSX 為相當著名搭建虛擬網路且可聯合 SDN 概念的產品，此產品只需搭建穩定且高速的實體網路，即可迅速部屬虛擬網路，且此網路建置具有高彈性、安全性的特色。VMware NSX 的架構圖如圖 3-26。

¹¹⁵ OpenDayLight, “KT Corporation Uses OpenDayLight to Deploy Transport-SDN WAN Network”.

¹¹⁶ digital spotlight-NETWORK WORLD, “SDN:AN EMERGING REALITY”, 2015/6.

¹¹⁷ 曾惠敏 胡仁維 劉德隆,“使用隧道技術實現網路虛擬化”, 2013.

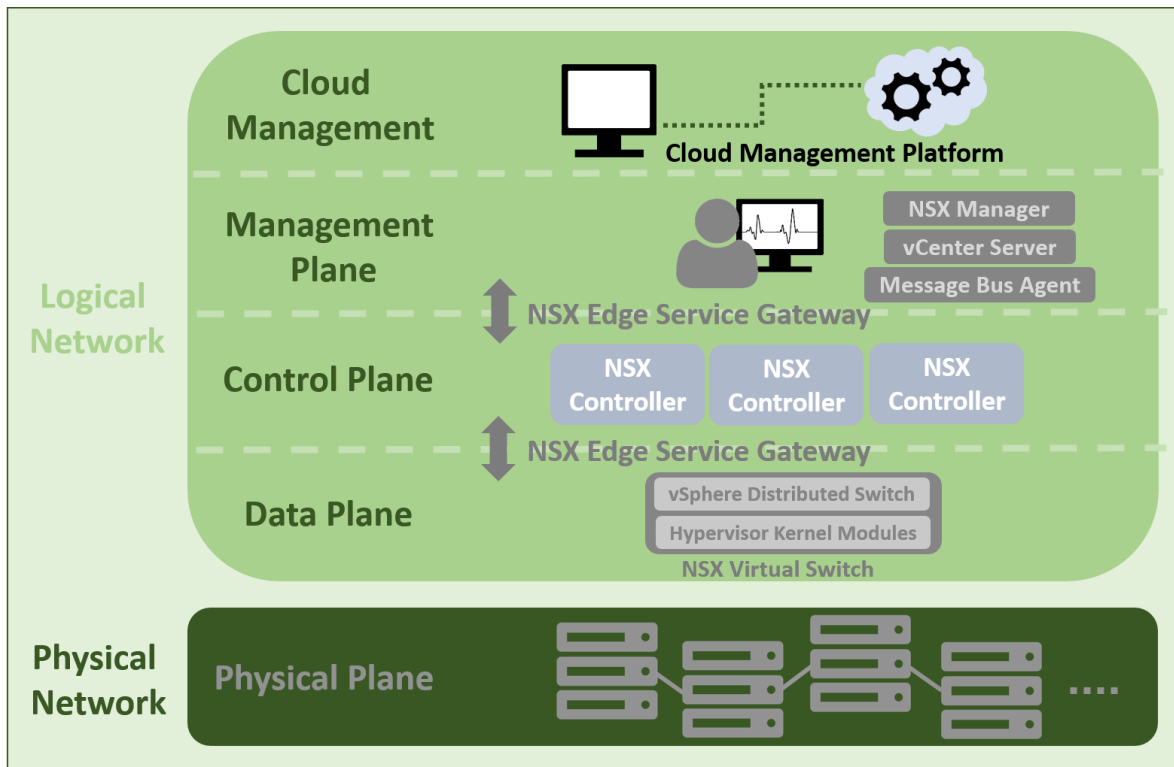


圖 3- 26 VMware NSX 基於 SDN 的架構示意圖

資料來源：VMware¹¹⁸

由圖 3-27 可看出 VMware NSX 確實可以實現 SDN 的概念，Cloud Management 中使用者可利用雲端管理平台及 NSX Manager 部屬及設定虛擬網路；Management Plane 中使用者能夠透過 NSX Manager 設定網路，並整合 vCenter Server 同步對虛擬網路及虛擬機進行管理，因此可將 Cloud Management 及 Management Plane 視為 SDN 的應用層。Control Plane 中的 NSX Controller 解讀從上層傳遞下來的命令，此層為 SDN 的控制層，NSX Controller 分析命令並且向下控管 Data Plane 的各項虛擬網路設備，而這個虛擬網路建置於實體網路之上，因此可將虛擬網路層的 Data Plane 及 Physical Plane 視為基礎建設層。最為重要的銜接橋梁北向及南向接口則是透過 NSX Edge Service Gateway。¹¹⁹

如今 VMWare NSX 於全球使用的狀況，統計有超過 1,400 家企業使用，其中 25%

¹¹⁸ VMware, “Reference Design:VMware® NSX for vSphere (NSX)Network VirtualizationDesign Guide”, 2014.

¹¹⁹ 饒康立, “軟體網路虛擬化安全平台 VMware NSX 功能架構簡述”, 2016/5/5.

的企業完整利用 NSX 部屬其企業網路。NSX 的 Micro-Segmentation 將安全防護細分為每一台虛擬機為單位，達到高安全性以保護公司最高機密，而此安全機制吸引了超過 700 個企業使用 NSX¹²⁰。

以下針對三種實作架構的特點整理如下表 3-7。

表 3-7 SDN 實作架構比較

	ONOS	ODL	VMware NSX
研發單位	ON.Lab	OpenDayLight	VMware
開發理念	提供具有高擴展性、高可靠性及高性能，趨向可管理大型的網路	部屬 SDN 網路，仍可以沿用傳統網路設備，支援現有多項南向通訊協定	基於隧道協議 VXLAN 於實體網路之上建立虛擬網路
目標市場	電信業者、大型網路管理需求之企業	傾向不更動現有底層網路設備的使用者	底層為穩定且高速的實體網路，但底層網路設備廠牌的多樣導致管理不易，期望簡化管理方式的客戶
特點”	(1)分散式核心架構 (2)北向介面抽象層：意圖框架、全局網路視圖 (3)南向介面抽象層：支援多種南向通訊協定，並且統	(1)北向接口支援 REST API、OSGi (2)南向接口支援多種，使得具有硬體高相容性 (3)實體、虛擬網路設備皆可使用	(1)專攻於網路虛擬化 (2)VMware NSX 為一體成型的產品，內容包含本身研發的管理程式、接口通訊協議、虛擬交換器等
成功部屬案例	主要集中於學術網路及科學研究網路，其中較為有名的案例為：美國	ODL 部屬成功的案例眾多，較為代表性為韓國通訊(KT)的 T-SDN 方案、Extreme Network 的	全球超過 1400 成功部屬 VMware NSX，其中較為耳熟能詳為 IBM 全球資訊科技服

¹²⁰ 王立恒, “VMware NSX 兩大未來戰略剖析”, 2016/5.

	ONOS	ODL	VMware NSX
	Internet2、韓國 KREONET、台灣 NCTU 交通大學、AmLight 拉丁美洲學術網路	OneController、英國的恩菲爾德鎮(Enfield)以及瑪麗山大學(Mount Mary University)的學術網路	務部、Heartland Payment Systems、Fulton County Schools、巴帝電信(Bharti Airtel)等 ¹²¹

資料來源：本團隊整理^{122、123、124、125、126、127}

2. SDN 攻擊趨勢

SDN 的攻擊趨勢主要分為兩個部分說明，分別為攻擊手法以及惡意攻擊對 SDN 各層的影響。

2.1 SDN 的攻擊手法

SDN 是利用軟體去定義底層網路運行的各種行為，可編程化、集中管理及開放性的特點，雖然改變了傳統網路難以管理、靈活性低、設備難以升級的種種缺點，且可以運用集中管理的特性應對各種網路攻擊時更加具有靈活化且智慧化，但在於另一個面向，卻是為此種新興網路帶來新的安全議題。

針對 SDN 的攻擊手法，主要可歸類為四種，分別為電子欺騙攻擊(Spoofing Attacks)、入侵式攻擊(Intrusion Attacks)、異常式攻擊(Anomaly Attacks)以及阻斷服務攻擊(DoS Attacks)與分散式阻斷服務攻擊(DDoS Attacks)，以下將介紹如何利用這些方法攻擊 SDN。

(1) 電子欺騙攻擊(Spoofing Attacks)

此種模式的攻擊目標集中在基礎層以及南向接口部分，因為控制器下方缺乏中間

¹²¹ VMware, “VMware 客戶成功案例”。

¹²² 高娟, “既生瑜何生亮？解讀 ODL 和 ONOS 之爭”, 2016/4/27.

¹²³ 王韋程, “獲電信業及網路設備商支持 ONOS 躍居 SDN 控制器主流”, 2017/1.

¹²⁴ 王韋程, “黃秉鈞,”軟體定義網路中邊界閘道協議之實作”, 2016/10/4.

¹²⁵ digital spotlight-NETWORK WORLD, “SDN:AN EMERGING REALITY”, 2015/6.

¹²⁶ VMware, “Reference Design:VMware® NSX for vSphere (NSX)Network VirtualizationDesign Guide”, 2014.

¹²⁷ 饒康立, “軟體網路虛擬化安全平台 VMware NSX 功能架構簡述”, 2016/5/5.

盒(middle box)的架構(如防火牆、網路位址交換、代理伺服器)，並且 SDN 拓樸內的高度信任關係，駭客只要竊取任一個內部的合法 IP 位址後將其自身的機器冒充 SDN 內部的機器，即可繞過防火牆，不需經過身分認證就能侵入目標，可竊取資料、監聽並竄改封包、植入惡意的應用程式等。另外 OpenFlow 拓樸中存在負責網路虛擬化的交換器，由於此種交換器需與 SDN 控制器直接連結，所以也容易成為被攻擊的目標。

(2) 入侵式攻擊(Intrusion Attacks)

只要是未經認證強行進入系統的手段皆可稱為入侵式攻擊，因此這種攻擊的方法非常多樣化，SDN 各層皆有可能受到影響。一般網路系統中會架設中間盒(middlebox)來抵擋來自外部的攻擊，因為 SDN 使用了「解耦」(decoupling)結構(可減少控制平面與數據平面間交互作用產生的額外影響)並將一切決策權交給控制器，若在控制器中結合了額外的模塊，會增加整個 SDN 網路的負載量，且駭客傳送的惡意封包或程式也有可能因此而被控制器誤認為正常的消耗，導致 SDN 中了入侵式攻擊，所以中間盒難以和 SDN 整合。

(3) 異常式攻擊(Anomaly Attacks)

對於使用者來說，異常式攻擊即是造成網路運行時，發生超出預期的行為，甚至導致網路癱瘓，但網路管理者卻難以推測攻擊者為何者、在何地。此類攻擊的攻擊源頭可能來自於任何一層：

- 應用層中的應用程式，攻擊者可以藉由植入惡意程式抑或本身程式具有系統漏洞，皆會導致在運行程式的途中，網路出現異常狀況甚至是癱瘓。
- 控制器作為 SDN 網路的控制核心，當攻擊者入侵或者仿冒為合法控制器，藉此發送錯誤政策及竊取網路機密資料等危害網路系統的攻擊，導致整個網路失去控制，甚至成為殭屍網路，成為攻擊他人的跳板。
- 設備層透過入侵式攻擊或是電子欺騙攻擊將主機做為跳板，進而發送合法惡意封包，傳遞錯誤訊息至控制器。

(4) 阻斷服務攻擊(DoS Attack)與分散式阻斷服務攻擊(DDoS Attack)

阻斷服務攻擊為攻擊者藉由某種手法(如傳送大量訊息)將攻擊目標的主機或是網路資源耗盡，導致正常服務對象無法使用其服務，造成停止服務的假象，是一種常見的攻擊方式。DDoS Attacks 可視為 DoS Attacks 的延伸攻擊，差別在於前者為多台機

器同時發動攻擊，後者為單一機器，DDoS Attacks 以「殭屍網路」(Botnet)作為攻擊跳板，而所謂的殭屍網路即攻擊者將專門設計為可遠端控制電腦的惡意程式，一一植入分散各地的機器，使得所有受到感染的機器可聽從攻擊者遠端下達的命令，因此只要攻擊者下達命令使得分散各處受感染的「殭屍」，對攻擊目標展開 DoS Attacks，即可使目標網路或主機資源耗盡，導致服務停擺，如下圖所示。

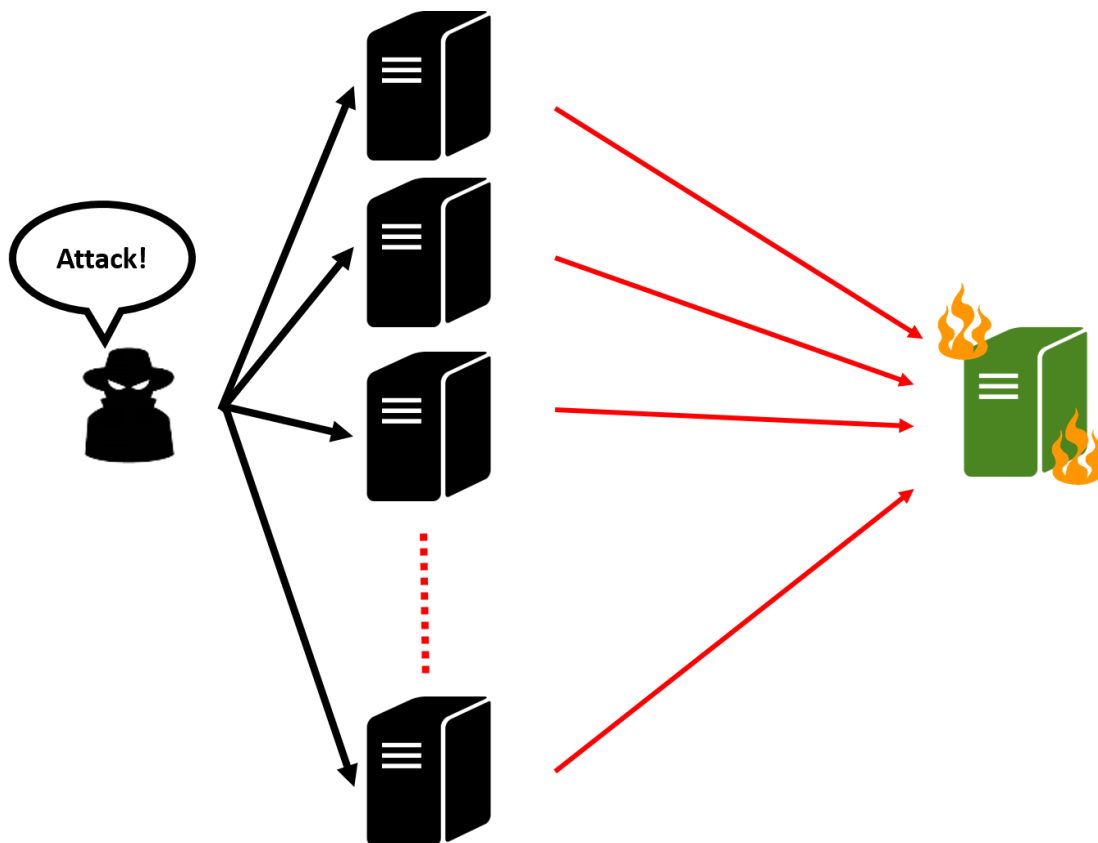


圖 3- 27 DDoS 示意圖

資料來源： Software Defined Networking Architecture, Security and Energy Efficiency: A Survey¹²⁸及本團隊整理

在 SDN 網路架構中，SDN Controller 作為控制底層網路的核心角色，因此當攻擊者意圖透過 DoS/DDoS Attacks 使目標網路癱瘓，SDN Controller 必為首要攻擊目標，此外設備作為網路建構的基底，設備的健康狀況同樣也是網路管理者關注名單之一，因此當攻擊者計畫癱瘓網路時，除了控制器，設備必是其次要攻擊目標，因此可統整出 DoS/DDoS Attacks 主要是鎖定 SDN 的控制層以及基礎建設層。

檢測 SDN 網路是否遭到 DoS/DDoS Attacks 的方法，藉於 DoS/DDoS Attacks 中的攻擊手法內涵相同，同樣是以大量消耗資源為目的，因此傳統網路的檢測技術仍可以延伸利用於 SDN 網路，但由於 SDN 架構與傳統架構的不同，防範技術便無法同樣套

¹²⁸ Danda B. Rawat, Swetha R. Reddy, “Software Defined Networking Architecture, Security and Energy Efficiency: A Survey”, 2016/10.

用在 SDN 架構網路之上。

2.2 惡意攻擊統整及對 SDN 各層的影響

以下說明 SDN 各層可能會遭遇到的攻擊及影響¹²⁹，本團隊將各層的攻擊途徑整理如圖 3-28

(1) 基礎設備層

基礎設備層中的交換器在 SDN 網路中擁有不可取代的地位，儘管在 SDN 網路中只需要轉送封包，但卻作為主要推動網路運作的角色，其安全議題同樣不可忽視。對於與設備相關的攻擊管道，分為下列兩種：

其一為攻擊者侵入網路中的主機使其成為傀儡，抑或者試圖竊取合法 IP 將攻擊者主機偽裝為合法主機，同時可隱藏非法主機的實際位置，減少被偵測出的機率，接著藉由主機發送惡意流量，此處含有電子欺騙攻(Spoofing Attacks)以及入侵式攻擊(Intrusion Attacks)。

其二為單面向某台交換器攻擊，如針對某一台交換器發動 DoS Attack，塞滿其有限額度的路由表，使交換器不能如預期地轉送封包，且當某台交換器服務癱瘓時，由於 SDN 網路各個交換器路由表皆由控制器設定，因此如某台交換器發生問題時，部分網路將會停止運作。

(2) 控制層

控制層中的控制器做為 SDN 的控制核心大腦，已經為攻擊者的首要目標，攻擊者成功奪取控制器的掌控權，即代表整個 SDN 網路已成攻擊者的囊中之物，因此控制器的安全措施備為看重。攻擊者會影響至控制器分為兩個攻擊路線：

其一針對控制器的向外通訊窗口，通訊窗口分為兩種，一種是面對網路管理者的北向接口，網路管理者藉由應用程式傳遞指令於控制器，另一種則是與設備通訊的南向接口，設備負責隨時通報網路設備狀態、警訊以及詢問決策等要務，因此與控制器銜接的北、南接口中流動控制訊息及資料訊息可經由攻擊者的竄改、攔截及偽造，使得內容不正確造成控制器的發下錯誤政策或內容被更改為控制器無法處理之格式，導

¹²⁹ 戴彬，王航远，徐冠，杨军，“SDN 安全探讨：机遇与威胁并存”，2014/8.

致控制器無法辨識或執行動作與原先指令相背，網路脫離使用者的控制，此處屬於 Anomaly Attacks。

其二為直接鎖定控制器為目標，分為兩種，第一種為目標擊潰控制器，如攻擊者透過觀察目標網路中，何種類型封包交換器會上交至控制器處理，攻擊者即可利用此類封包的性質，大量且密集的發送此類封包，對控制器發動 DoS/DDoS Attack，消耗控制器的資源，導致處理速率大幅下降，甚至服務癱瘓；第二種則是觀察控制器的系統漏洞，利用獲取控制器之控制權限，進行入侵式攻擊(Intrusion Attacks)。

(3) 應用層

應用層中的攻擊與 SDN 應用程式息息相關，現實中管理者主要的管理介面即為應用層中的應用程式，因此當應用程式受到濫用時，即會造成難以想像的損失，以下整理出兩個應用程式的攻擊管道：

其一為網路管理者使用惡意程式或程式本身具有系統漏洞，導致程式運行時，間接使得在應用程式的控制下，網路運行出現異常，甚至造成政策衝突，網路的安全性急轉直下，而此種可列為 Anomaly Attack。

其二為藉由入侵獲取 SDN 應用程式控制的身分，攻擊者即可藉由應用程式蒐集網路的資訊及作為跳板掌控底下網路，甚至經由刻意調控，以致於發下的政策與其他 SDN 應用程式所訂下的安全政策造成衝突，導致安全政策失效，使網路暴露於危險之中，此種攻擊屬於入侵式攻擊(Intrusion Attacks)。

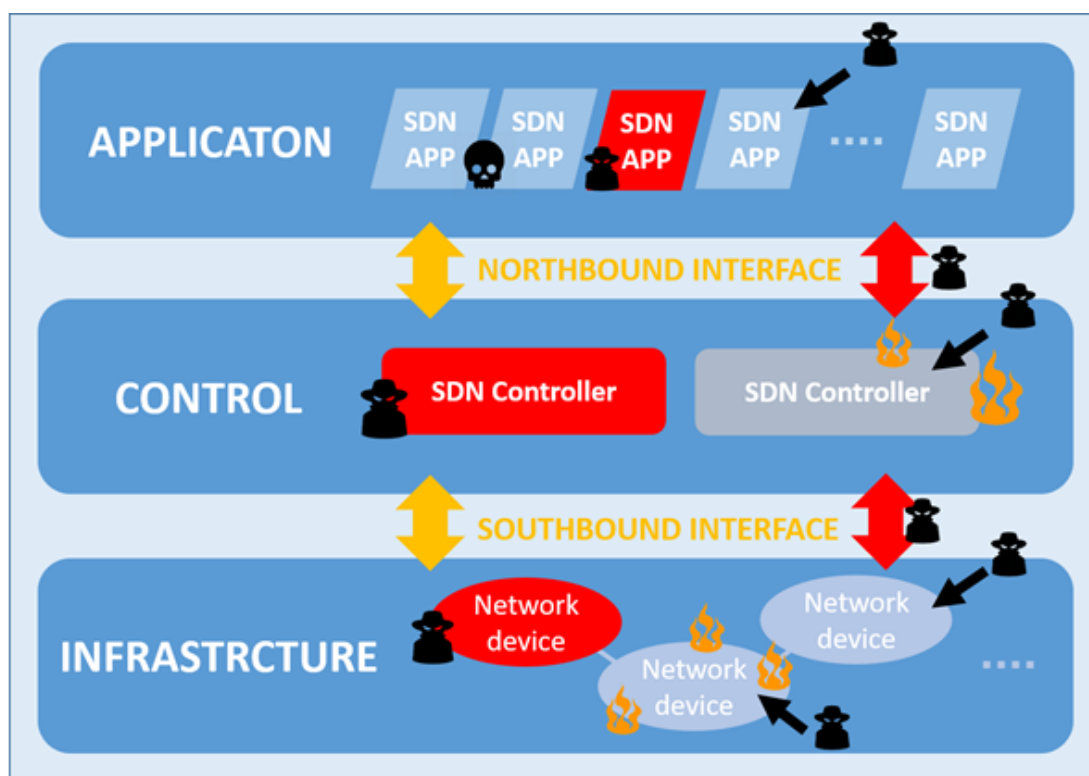


圖 3- 28 SDN 網路架構攻擊途徑圖

資料來源： Software Defined Networking Architecture, Security and Energy Efficiency: A Survey¹³⁰

3. SDN 防護技術

本團隊將針對電子欺騙攻擊(Spoofing Attacks)、入侵式攻擊(Intrusion Attacks)、異常式攻擊(Anomaly Attacks)以及阻斷服務攻擊(DoS Attack)與分散式阻斷服務攻擊(DDoS Attack)列出多項檢測及防範之技術，期望協助未來企業及電信業者部屬 SDN 的安全防範技術之時，能有具體的研究方向提高網路運行的安全性，下表 3-8 為 SDN 各式攻擊手法以及相對應的防範與檢測方法。

¹³⁰ Danda B. Rawat, Swetha R. Reddy, “Software Defined Networking Architecture, Security and Energy Efficiency: A Survey”, 2016/10.

表 3- 8 SDN 攻擊及防護技術

防護技術 攻擊方法	防範與檢測方法
電子欺騙攻擊	● 封包檢測 ● IP 位址防護
入侵式攻擊	● FlowGuard ● FlowTag ● NIMBLE
異常式攻擊	● TRW-CB (Threshold Random Walk with Credit Based Rate Limiting) ● Rate-Limiting ● NICE (No bugs In the Controller Execution) ● FRESCO
阻斷服務攻擊及分散式阻斷服務攻擊	● 辨別攻擊模式 ● 高速流量檢測系統(High Speed Flow-level Detection System, HiFIND) ● 輕量級的 DDoS 攻擊檢測 ● 基於 Entropy 的檢測 ● Avant guard

資料來源：本團隊整理¹³¹

3.1 電子欺騙攻擊(Spoofing Attacks)

對於電子欺騙的防護技術，現已有多種方法來防範此種攻擊，盡早的發現這些受到惡意使用的交換器能減少此種攻擊帶來的影響，而最直觀的防禦手段就是檢查所有進入這個拓樸系統的封包。

¹³¹ Danda B. Rawat, Swetha R. Reddy, “Software Defined Networking Architecture, Security and Energy Efficiency: A Survey”, 2016/10.

(1) 封包檢測^{132、133}

現在已有許多封包檢測的方法：SPHINX 為基於 OpenFlow 協定的偵測技術，利用 OpenFlow 中現有的內部指令來檢測南向接口部分的任何可疑資料；另一種方式則是事先紀錄 SDN 拓樸中每台交換器流量的門檻值，當某個交換器的流量超過門檻值時，這個位址便有可能已經被偽造，控制器將會深入調查並把此交換器從拓樸中分離，而沒被控制器偵測到的部分則是藉由此網路的所有使用者觀察，提供具有被偽造跡象的交換器名單給第三方伺服器，而第三方伺服器會定期傳送這份名單至控制器，提醒控制器檢驗名單中的交換器。

(2) IP 位址防護¹³⁴

另外一種面向的防禦手段為保護內部的 IP 位址，駭客若無法取得合法的 IP 位址，此種攻擊自然無法進行。例如可在 SDN 架構中做出了 OpenFlow 主機隨機突變 (Random Host Mutation) 機制，管理系統隨著時間推移不斷得隨機分配虛擬 IP 位址來隱藏真實 IP，使駭客難以破解。

3.2 入侵式攻擊(Intrusion Attacks)

防止入侵式攻擊的首要目標便是在不影響 SDN 網路性能的前提下做出檢測系統，現今也已經有提出了多種方法：

- (1) FlowGuard¹³⁵：是專門為 SDN 設計的防火牆，此研發仍屬於 SDN 資安學術研究階段，其可監視整個內部網路以檢測惡意封包及違法的規則修改，而為了能套用在 SDN 系統，其結構比起一般網路用的防火牆更為複雜。
- (2) FlowTag¹³⁶：該技術可擴展中間盒的結構，在所有經過中間盒的封包加上標籤，

¹³² M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, in Proc. Netw. Distrib. Syst. Security (NDSS) Symp., San Diego, CA, USA, “SPHINX: Detecting security attacks in software-defined networks,” pp. 1–15, 2015.

¹³³ X. Du, M.-Z. Wang, X. Zhang, and L. Zhu, “Int. J. Security Appl., vol. 8, no. 5,” pp. 119–130, 2014.

¹³⁴ J. H. Jafarian, E. Al-Shaer, and Q. Duan, in Proc. 1st Workshop Hot Topics Softw. Defined Netw., Helsinki, Finland, “OpenFlow random host mutation: Transparent moving target defense using software defined networking,” pp. 127–132, 2012.

¹³⁵ H. Hu, W. Han, G.-J. Ahn, and Z. Zhao, in Proc. 3rd Workshop Hot Topics Softw. Defined Netw., Chicago, IL, USA, “FLOWGUARD: Building robust firewalls for software-defined networks,” pp. 97–102, 2014.

¹³⁶ S. K. Fayazbakhsh, V. Sekar, M. Yu, and J., “FlowTags: Enforcing network-wide policies in the presence of dynamic middlebox actions,” pp. 19–24.

可使得追蹤遺失、惡意封包更為容易，並將這些標籤變成資料的一部分，以便控制器能正確的運行。

- (3) NIMBLE¹³⁷：可嘗試在不修改中間盒、使用 OpenFlow 協定及現行 SDN 拓樸中的交換器的條件下運行，NIMBLE 會依據網路管理員所下的指令並考慮流量、實體架構、中間盒等因素後彙整成轉送規則(forwarding rule)，所以網路營運者只需要定出方針而不需要擔心內部會如何處理。

3.3 異常攻擊(Anomaly Attacks)

對於異常式攻擊的防護以下分別對各層的安全措施進行個別介紹，其中 TRW-CB 及速率限制¹³⁸為設備層防護技術，藉由設備上報之所有資訊判斷設備是否出現異常行為，進而展開後續的處理動作；FRESCO 為控制層防護技術，將敘述可提高控制器安全性的安全框架；NICE 則是應用層防護技術，將說明應用程式正確性的檢測方法。

(1) TRW-CB (Threshold Random Walk with Credit Based Rate Limiting)

正常主機與受感染主機最主要的區別在於，正常主機對於別的主機進行 TCP 握手協議連接成功次數會遠高於受感染用戶，此特點即為 TRW-CB 的啟發。TRW-CB 會設立一個感染的門檻值，如果在偵測主機的過程中，將此主機的連接失敗次數與總連接數通過 TRW-CB 計算出的概率大於門檻值，即可將此台主機列入受感染主機列表。

此方法運用在 SDN 檢測上，當交換器接收到未設定路由的封包時，即會向上詢問控制器，而控制器中的 TRW-CB 會在無設定任何路由的情況下，直接將接收的封包透過交換器傳送至目的地，假使目的地確實有回傳回應，然而設定還未回傳至發源地交換器的路由，所以交換器仍會向上詢問控制器，此時 TRW-CB 得知目的地可成功連結，即在目的地及源發地的交換器設置兩地的傳送路由，反之如果目的地交換器無回應則無處理動作。透過以上的行為，控制器中的 TRW-CB 可統計各處主機連接的總詢問次數及連接失敗次數，以供辨認是否為感染用戶。

(3) 速率限制(Rate-Limiting)

¹³⁷ Z. Qazi et al., in Proc. Open Netw. Summit, Santa Clara, CA, USA, “Practical and incremental convergence between SDN and middleboxes,” pp. 1–15, 2013.

¹³⁸ Syed Akbar Mehdi, Junaid Khalid, Syed Ali Khayam, “Revisiting traffic anomaly detection using software defined networking”, 2011.

此方法是從受感染者會在短時間向大量且密集的不同主機連接的角度出發，各主機皆擁有一個工作集(Working set)的名單，上面會列出近期頻繁連接的主機，當主機要連接外界時，如目的地是工作集之中的一員，即視為正常行為，但如果不在名單之中，其目標主機會列入延遲序列(delay queue)，而此序列每隔 d 秒即會釋出固定數目，此 d 秒會根據網路環境的不同，而設定不同的數值，此方法會持續觀察其延遲序列長度，當延遲序列大於此方法預設長度的門檻值時，即會將此主機列為高危險用戶。

若將此方法套用於 SDN 架構中，當主機收到新的 TCP 連線要求時，會確認發出請求的主機是否存在於工作集，如果存在控制器即會立即下發路由至接收端主機及發送端主機的路由表，倘若並不在工作集內，便將發送端主機列入延遲序列，並且在於 d 秒內觀察延遲序列是否有高過於門檻值，通過 d 秒的觀察期，控制器會在不設立路由的情況下，對發送端送出請求，如果控制器成功收到回應，控制器即會於接收端及發送端的路由表設定互相連接之路由。

(4) FRESCO^{139、140}

由 Shin 及 Porras 等人提出的 FRESCO 為一種提升 NOX 控制器安全性框架，此安全框架包含於 FRESCO 應用層以及 FRESCO 安全核心組成，其框架的應用層中包含多種安全組合模組，除此之外 FRESCO 還提供多種 API，網路管理者可自行設計所需的安全模組，自由遞增及刪減應用層中的模組，並且模組間具有相容性，可互相合作處理工作，進而可設計出更複雜的安全應用，另一方面，FRESCO 可協同部分傳統的安全檢測工具，如做為檢測流量變化的 BotHunter，一同抵禦針對控制器的安全威脅。

(5) NICE (No bugs In the Controller Execution)¹⁴¹

此工具是由於 SDN 的進步發展，越來越多元化的 SDN 應用程式產生，而 NICE 的衍生即是為了去檢驗該 SDN 應用程式的正確性，以確認當 SDN 應用程式在運行當中，控制器在應用程式的控制下並不會出現影響網路正常營運的缺失。

¹³⁹ 王蒙蒙, 刘建伟, 陈杰, 毛剑, 毛可飞, "软件定义网络:安全模型、机制及研究进展", 2016.

¹⁴⁰ Seugwon Shin, Phillip Porras, Vinod Yegneswaran, Martin Fong, Guofei Gu, Mabry Tyson, "FRESCO: Modular Composable Security Services for Software-Defined Networks", 2013/4.

¹⁴¹ Marco Canini, Daniele Venzano, Peter Perešini, Dejan Kostić, Jennifer Rexford, "A NICE way to test openflow applications", 2012/4.

NICE 結合兩個核心技術，分別是「模型檢測」(Model Checking，簡稱 MC)及「符號執行」(Symbolic Execution，簡稱 SE)，MC 的技術為 NICE 搜索出整個系統會產生所有的狀態，利用檢驗的過程，觀察系統是否滿足該有的性質，而系統包含控制器、交換器、終端的主機。SE 的技術在於不執行程式的情況下，能協助分析出控制器程式有多少種不同的執行路徑，其組成每一條路徑的稱為代碼路徑(Code Path)。透過 MC 及 SE 兩個技術，即可達到檢驗應用程式是否存在危險的漏洞。

運行 NICE 之前除了基本的系統資訊之外，還需定義測試正確性的屬性，其屬性如：無黑洞(Blackholes)、無轉發循環(forwarding loops)。NICE 執行方法如下圖 3-29，輸入要求的資訊，分別為控制器之程序、網路拓樸及正確性屬性，輸入完透過 NICE 的執行，透過 MC 及 SE 所蒐集到的狀態空間及代碼路徑測試是否符合其預設的正確性屬性，如果搜索出異常，即會輸出 Trace 的文件，內容列出此系統會有哪些缺失導致不符合其正確性屬性。

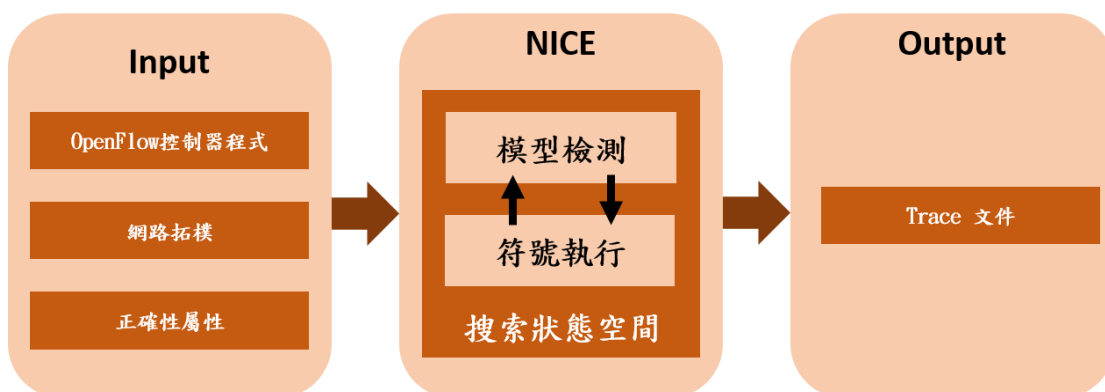


圖 3- 29 NICE 執行過程

資料來源： A NICE way to test openflow applications¹⁴²

3.4 阻斷服務攻擊(DoS Attack)及分散式阻斷服務攻擊(DDoS Attack)

本團隊統整多篇已發表 SDN 安全相關論文發現，以下為可有效運用於 SDN 架構上的檢驗 DoS/DDoS Attack 的措施及防護方法。

¹⁴² Peter Perešini, Dejan Kostić, Jennifer Rexford, Marco Canini, Daniele Venzano, " A NICE way to test openflow applications", 2012/4.

(1) 辨別攻擊模式¹⁴³

此篇論文為傳統中利用蒐集以往受到的網路攻擊，且詳細記錄其攻擊發生日期、持續的時間、攻擊的性質及受到攻擊的影響並作為統計資料，以利系統可從中觀察紀錄進行對比，協助判斷當前攻擊為何種網路攻擊模式，而如此判別攻擊模式的方法同樣也可用於 SDN 網路架構中，藉由控制器自交換器獲得的封包訊息統計各種攻擊模式的性質，藉而做為未來可依據的特徵資料，檢測出目前是否有遭到任何攻擊。

高速流量檢測系統(High Speed Flow-level Detection System, 簡稱 HiFIND):¹⁴⁴

此系統的研發針對 DDoS Attacks 的高密集封包攻擊，給予易受害 DDoS Attacks 的服務供應商相當程度的保護，但對於非高密集性的封包攻擊就未有太大的適用性。

(2) 輕量級的 DDoS 攻擊檢測¹⁴⁵

此輕量級的檢測方法是基於 SOM(Self Organizing Maps)模型所研發出來的檢測方法，SOM 為 T. Kohonen 所提出，此模型可經由輸入巨量資料，並且根據資料的性質映射成 2 維圖形，而圖形上即顯示分類的結果，此方法經由 SOM 模型持續的訓練及分類流量，基於 DDoS Attacks 流量都具有相似的特徵，如流量平均含有的封包數量、流量平均持續傳送至主機的時間等性質，可有效將其分為一類，因此藉由此方法可分類出目前所接收到的流量是否可能為 DDoS Attacks。

其檢測方法分為三個階段，分為流量收集、特徵提取及分類，首先交換器收集流量訊息，並擷取當中的訊息特徵，最後特徵經由訓練過後的 SOM 模型分類判斷是否為合法用戶。

(3) 基於 Entropy 的檢測¹⁴⁶

此篇發表論文是基於 Entropy 延伸出的，所謂的 Entropy 來自於熱力學第二定律的一個狀態，用來表示一個混亂程度的數值，再來於此著作所提到，其會擁有 Entropy

¹⁴³ Myung-Sup Kim, Hun-Jeong Kong, Seong-Cheol Hong, "A flow-based method for abnormal network traffic detection", 2004/4.

¹⁴⁴ Zhichun Li, Yan Gao, Yan Chen, "HiFIND: A high-speed flow-level intrusion detection approach with DoS resiliency", 2009/10.

¹⁴⁵ Rodrigo Braga, Edjard Mota, Alexandre Passito, "Lightweight DDoS flooding attack detection using NOX/OpenFlow", 2010/10.

¹⁴⁶ Seyed Mohammad Mousavi, Marc St-Hilaire, "Early detection of DDos attacks against SDN controllers", 2015/3.

值是做為一個衡量封包是否異常的門檻，因此在這個網路中，假使封包集中於一個主機發送，那麼此狀態可計算出一個高 Entropy 值，反之當封包是發散四處，即可運算出較低的 Entropy 值。此方法提出於每五十個封包傳入 SDN 網路的控制器時，控制器會計算當下五十個封包的 Entropy 值，比較其當初預設為可列入異常行為的門檻值，如高於門檻，即表示這些可列為可疑行為名單，此作法可有效排除其可疑封包進入 controller，導致其 controller 免於遭受 DDoS Attacks。

(4) Avant guard¹⁴⁷

Avant guard 為檢測 TCP 型 DDoS Attacks 的安全框架，其中建構兩組工具專門針對過濾惡意封包，分別為 connection migration 及 actuating trigger。接收到的封包的 IP 如果不存在於交換器的路由表內，此封包會在傳送至控制器前由 connection migration 攔截，並且進行封包分析、紀錄 TCP 連接資訊，如封包 IP 是否連接成功、連接速率等訊息機率等並對發送端發送 TCP 請求，取得發送端回應之後即會啟動 actuating trigger。actuating trigger 內存有控制器所發下的各式封包策略，而封包即依據發送端的回應結果以及 TCP 連接紀錄等資訊，對應策略的條件得出封包後續的處置。

此種方式可以成功阻攔 DDoS Attacks 帶來大量的封包而導致 Controller 服務癱瘓，並且同時能達到不需另外增加硬體，就可以達到清洗中心的功能。

(四) 物聯網 (Internet of Things, 簡稱 IoT)

早在 1985 年 Peter T. Lewis 發表演說時就曾提及物聯網概念¹⁴⁸，隨後比爾蓋茲於 1995 年《未來之路》一書中提及 IoT 的概念，但由於受限當時的網路、硬體及感測設備的發展，而未受到重視¹⁴⁹。但隨著技術不斷進步，一直到 2005 年國際電信聯盟 ITU 發布《The Internet of Things》後宣布了物聯網時代正式來臨¹⁵⁰，隨著行動裝置普及與無線網路快速的發展，IoT 讓設備與設備間透過無線通訊協定彼此串聯互相交流，其中不需要人類直接操縱判斷，真正達到現實世界數位化。而目前物聯網尚未有統一

¹⁴⁷ Seungwon Shin, Vinod Yegneswaran, Phillip porras, Guofei Gu, "AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks", 2013/11.

¹⁴⁸ Sadler, M., Prelicean, D., Sowinski, M., & Cucu, V., "Magic or Mischief: A look into Disney's adaptation of IoT", 2016/11/27.

¹⁴⁹ Gates, B., Myhrvold, N., Rinearson, P., & Domonkos, D., "The road ahead", 1995

¹⁵⁰ ITU, "The Internet of Things", 2005/11.

標準，目前制定物聯網標準主要有四大聯盟: AllSeen、OIC、Thread Group 以及蘋果主導的 HomeKit。AllSeen 與 OIC 目標在於建立互通性的框架，使得不同品牌、平台、作業系統的設備可互相通信，兩大聯盟於 2016 年合併並致力於建立強大且開放的物聯網解決方案¹⁵¹。Thread Group 則是訂定新的物聯網標準: Thread，基於原有的 ZigBee 技術並加以改造的一種衍生協定，與其他標準相比更接近底層¹⁵²。HomeKit 則是結合 Apple 原有的各項軟硬體，打造智慧家庭平台¹⁵³。

物聯網(IoT) 是指植入各種微型感應晶片或感測器在物體上使其智能化，並通過射頻識別(RFID)、環境感測器、紅外線感應、全球定位系統、雷射掃描器等訊息感測設備¹⁵⁴，之後再藉助無線網路連結上網，使物體的資訊得以透過網路分享。從圖 3-30 的概念圖可看出，透過將蒐集到的資訊傳送至雲端平台，智慧裝置能與其他裝置、物件、環境及基礎設施互相交流，產生大量資料，並將資料轉換分析應用，使生活更加的輕鬆便捷¹⁵⁵，實現「人與物」、「人與人」及「物與物」之間的資訊分享，使生活中的各項物體更具有智慧、能藉由回報自身狀態，被使用者聰明的所使用，達到物品的最大效益¹⁵⁶。

¹⁵¹ Rick Merritt, "IoT Consumer Groups Merge", EETimes, 2016/10/10.

¹⁵² Stackowiak, R., Licht, A., Mantha, V., & Nagode, L., "Big Data and the Internet of Things (pp. 185-190)", 2015.

¹⁵³ Hong, J., Shin, J., & Lee, D., "Strategic management of next-generation connected life: Focusing on smart key and car-home connectivity". *Technological Forecasting and Social Change*, 103, 11-20., 2016.

¹⁵⁴ 吕廷杰, "物联网的由来与发展趋势", *信息技术*, 4(2), 4-8., 2010.

¹⁵⁵ 廖國男, 楊雪芳, 李炫昇, "以物聯網 (IoT) 概念運用行動載具 (iPAD) 於提升住院病人會診時效" *醫務管理期刊*, 16(4), 345-358., 2015

¹⁵⁶ 張書瑋, "物聯網來了! 會計大數據的挑戰", *會計研究月刊*, (357), 76-81., 2015.

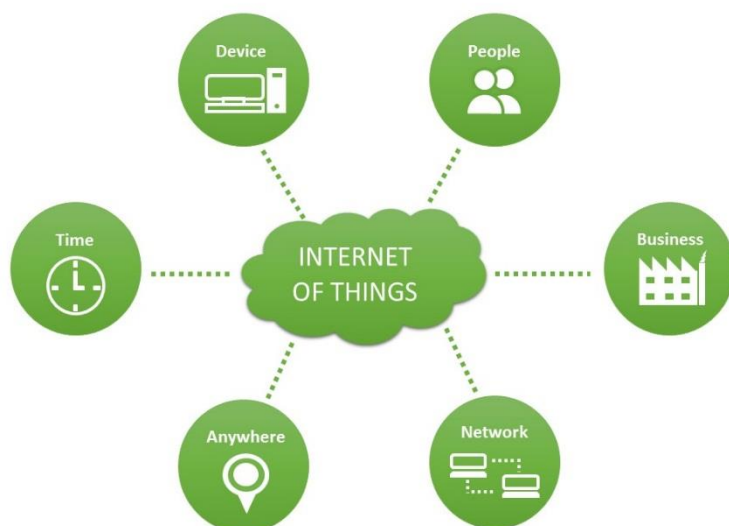


圖 3- 30 IoT 概念圖

資料來源：IoT, D. O. (2014). Internet of Things.

物聯網應用相當廣泛遍及消費、商業與工業市場，應用範圍包括家居設備遠端追蹤及控制、穿戴型醫療設備即時監控與紀錄、交通運輸流量管理系統、改變過往能源基礎設備生產與分配模式、自動化監測工業生產設備來提高產率和彈性，以及環境污染監測與防災預警等¹⁵⁷，在物聯網持續活絡發展之下，拉近了原本分散的資訊，自動化的網絡交流為人類建立智慧生活的第一步。物聯網大多數應用要求使用無線通訊協議進行資料傳輸，因此如 Wi-Fi、藍芽、NFC、Zigbee 等之無線通訊協定成為促成物聯網成長的關鍵技術。

目前物聯網產業仍持續迅速發展中，「Encore Media Group」2017 年將舉行「IoT Tech Expo Global 2017」、「IoT Tech Expo Europe 2017」與「IoT Tech Expo North America 2017」三場 IoT 年度盛會¹⁵⁸，展覽議程重點在於討論智慧城市的發展趨勢、萬物聯網環境下數據傳輸的安全性探討和物聯網創新技術的研究等。今日，全球已有超過 84 億數量的數位電子設備互連運作中，美國信息研究公司 Gartner 估計 2020 年全球使用的連網物件將達到 204 億個¹⁵⁹，可見物聯網系統蘊含巨大成長前景，偌大規模的前景將

¹⁵⁷ Beecham Research, "M2M World of Connected Services: The Internet of Things", 2015/11/4.

¹⁵⁸ Encore Media Group, "IoT TECH EXPO", 2017.

¹⁵⁹ Gartner, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", 2017/1.

趨使企業機構相繼投入發展，同時配合 5G 行動通訊標準明朗化，創建完整智能城市、智慧生活的目標即在咫尺。

在 2016 年中，由國際標準組織 3GPP 在 Release-13 中所引入並且定義的一種低功耗廣域網的(Low-Power Wide-Area Network，簡稱 LPWAN)技術標準，其目的在於能夠為物聯網提供低成本、低功耗、覆蓋廣以及連接多為趨勢的廣域蜂窩連接，此稱為窄頻物聯網 (Narrow Band Internet of Things，簡稱 NB-IoT)。

現今機器通訊類別(Machine-Type Communications，簡稱 MTC)的應用正逐漸被廣泛使用並迅速發展，使得整個物聯網的規模不斷擴大中，因此透過廣域的無線網路連接技術在未來會成為物聯網體系中極為重要的一部分。根據調查，在 2016 年底，使用蜂窩網路的物聯網設備估計約達到了 4 億個，而在 2022 年時，這個數目預計將增加到 15 億個，相當於 IoT 設備的複合年增長率達到 21%¹⁶⁰。從不斷增加的龐大設備數量可看出，該如何對於低數據傳輸速率、覆蓋需求廣闊、連接設備眾多等未來物聯網應用趨勢的場景提供更好的解決手段，並且最終希望能夠結合全球覆蓋的電信業者網路開拓更大的市場，實現智慧抄表、環境監測等廣域物聯網之目標，正是如今窄頻物聯網技術興起的如此迅速且被積極地研究開發的主要原因。

物聯網實現的基礎在於機器與機器彼此之間數據的溝通，而對於不同的物聯網應用來說，數據的傳輸速率能力以及性質也相對的有著差異性，也因此而出現了許多行動物聯網的技術標準。在 3GPP 中主要有三種關於 CIoT(Cellular IoT)的技術標準，分別是 LTE-M、EC-GSM 和 NB-IoT：

A. LTE-M

LTE-Machine-to-Machine(簡稱 LTE-M)，乃是一種基於現有的 LTE 技術而演進的 IoT 技術。在 3GPP 的 Release-12 中被稱為 Low-Cost MTC，在 Release-13 中則稱為 LTE enhanced MTC(簡稱 eMTC)，主要的目的為能夠在現今的 LTE 技術標準中來滿足物聯網的應用需求。為了適應物聯網應用以及迎合發展，在 Release-12 中所定義的 LTE Cat.0(Category)通訊技術為每秒只有 1Mbit/s 的資料傳輸率。如下表 3-9 所示，可看出到了 Release-13 中，資料傳輸率的標準甚至降低到了大約為 200kbps。

¹⁶⁰ Ericsson Mobility Report, “Internet of Things outlook”, 2016/6.

表 3- 9 Category 比較表

	Release-8 Cat-4	Release-8 Cat-1	Release-12 Cat-0	Release-13
Downlink peak rate	150Mbps	10Mbps	1Mbps	~200kbps
uplink peak rate	50Mbps	5Mbps	1Mbps	~200kbps
Max number of downlink spatial layers	2	1	1	1
Number of UE RF receiver chains	2	2	1	1
Duplex mode	Full duplex	Full duplex	Half duplex	Half duplex
UE receive bandwidth	20MHz	20MHz	20MHz	1.4MHz
Max.UE transmit power	23dBm	23dBm	23dBm	~20dBm
Modern complexity relative to Cat-1	125%	100%	50%	25%

資料來源：3GPP Specification number 36.306

B. EC-GSM

擴展覆蓋的全球行動通訊系統技術(Extended Coverage - Global System for Mobile Communications, 簡稱 EC-GSM), 由於現在的無線技術正朝向長距離通信的方面邁進, 因此許多 LPWAN(Low-Power Wide-Area Network)技術出現, 例如採用非授權頻譜的 Sigfox、LoRa、Weightless、HaLow、RPMA 等, 而本篇介紹的 NB-IoT 則是採用了所謂的授權頻譜, 這麼多的技術興起更加凸顯出了將傳統 GPRS 應用於物聯網的劣勢。在 2014 年時, 3GPP GERAN (GSM EDGE Radio Access Network) 在會議的研究項目¹⁶¹裡提出了將窄帶技術的應用到 GSM 上, 比傳統 GPRS 的覆蓋範圍更高以及消耗更低, 最後因此定義了 EC-GSM-IoT 技術標準。

C. NB-IoT

由於 NB-IoT 的技術類似於嶄新的開始而並不是建構於現有的 GSM 技術上, 因此 3GPP 內部中主要分成了兩種研究方向: 一種是 3GPP GERAN 繼續研究 EC-GSM,

¹⁶¹ 3GPP GERAN #62 會議, “Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things”.

另一種 NB-IoT 的研發工作則轉移給 3GPP RAN 組。3GPP RAN (Radio Access Network) 在 2015 年時開始研發新的窄頻無線空中接口技術，又稱之為 Clean-Slate CIoT，“Clean-Slate”的意思指的是設計一種全新技術。NB-CIoT 的出現，不僅能夠滿足降低複雜性 (Reduced complexity)、改進了大約 20 dB 的室內覆蓋率(Improve indoor coverage by 20 dB)、支援 IoT 中的大量設備(Support of massive number of devices)、提升能量的效率並降低消耗(Improved power efficiency)以及對於異常事件的報告具有 10 秒之內的延遲時間(Exception report latency of 10 seconds or less)等五大目標，它的通信模組成本也低於 GSM 和 NB-LTE，最後在經過 3GPP 2015 年 9 月的 RAN #69 會議的討論協商過後 162，NB-IoT 可以被當作是 NB-LTE 以及 NB-CIoT 的結合體。表 3-10 為 eMTC、EC-GSM 和 NB-IoT 間之比較。

表 3- 10 eMTC、EC-GSM 和 NB-IoT 比較表

	LoRa	GSM (Release-8)	EC-GSM-IoT (Release-13)	LTE (Release-8)	eMTC (Release-13)	NB-IoT (Release-13)
LTE user equipment category	N/A	N/A	N/A	Cat.1	Cat.M1	Cat.NB1
Max.coupling loss	155dB	144dB	164dB	144dB	156dB	164dB
Spectrum	Unlicensed < 1GHz	Licensed • GSM Bands	Licensed • GSM Bands	Licensed LTE • Bands In-band	Licensed LTE • Bands In-band	Licensed LTE • In-band • Guard-band • Stand-alone
Bandwidth	< 500kHz	200kHz	200kHz	LTE-carrier bandwidth (1.04 ~ 20MHz)	1.08MHz (1.04MHz carrier bandwidth)	180kHz (200kHz carrier bandwidth)
Max.data rate	<50kbps (DL/UL)	<500kbps (DL/UL)	<140kbps (DL/UL)	<10Mbps(DL) <5Mbps(UL)	<1Mbps (DL/UL)	<170kbps(DL) <250kbps(UL)

資料來源：Nokia, “LTE evolution for IoT connectivity”¹⁶³

窄頻物聯網的主旨在於能夠實現結合 GSM 以及 LTE 技術，並且提供更為優秀的共存性能，主要技術概念為建構於現有的蜂窩網路和現有 LTE 功能的一套新的改進系

¹⁶² 3GPP RAN #69 會議報告, 2015/10/15.

¹⁶³ Nokia, ”LTE evolution for IoT connectivity”, 2017.

統，因此能夠減少 NB-IoT 開發產品所需要消耗的時間。在 3GPP 的 Release-13 版本中，NB-IoT 具有下述五項的引入性能目標¹⁶⁴：

- 降低複雜性：目標是能夠提供超低複雜度的應用設備來支援 IoT，能夠藉由減少設備的傳輸塊大小(transport block size)、只用半雙工的操作方式、以及單一接收天線等方式來實現。
- 改進室內覆蓋率：比傳統的 GPRS 設備多 20 dB 覆蓋擴展，以及對應於需要達到 164 dB 最大耦合損耗(maximum coupling loss，簡稱 MCL)的目標，並且在這個 MCL 的目標當中，對於上行鏈路(uplink)以及下行鏈路(downlink)的速率要求至少須達 160 bps 的應用層數據速率。
- 支援 IoT 大量的設備：依據倫敦的情況來做為家庭密度的參考¹⁶⁵（每平方公里具有 1517 戶的家庭密度以及 1732 米的間隔距離），目標在蜂窩扇區(cell site sector)內至少支持 52,547 個設備。
- 提升能量的效率並降低消耗：目標為對於電池容量為 5 Wh 以及 164 dB MCL 的電池功率能夠提供十年的使用壽命。
- 對於異常事件的報告具有 10 秒之內的延遲時間。

1. IoT 架構

物聯網強調所有物品的聯網，而且這些設備須具備感測與運算能力，並透過資訊通訊技術(ICT)對資料進行蒐集、監控、傳送、分析，再回饋到機器本身，促成機器的深度學習。根據歐洲電信標準協會(European Telecommunications Standards Institute，簡稱 ETSI)之定義，IoT 可依照不同的功能劃分為感知層、網路層及應用層¹⁶⁶(如下圖 3-31 所示)。

(1) 感知層 (Perception layer)

就此層而言，重點在於將各種物體中嵌入具有感測或辨識能力的元件，使其更具

¹⁶⁴ Ratasuk, Rapeepat, et al. "Overview of narrowband IoT in LTE Rel-13.", 2016 IEEE Conference on Standards for Communications and Networking (CSCN), 2016.

¹⁶⁵ 3GPP TR 36.888, "Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE, v.12.0.0", 2013/6.

¹⁶⁶ ETSI TS 102 690 v2.1.1, "Machine-to-Machine communications(M2M): Functional architecture", 2013

智能，並且利用這些感知功能，取得有關於設備運作情形的資訊，並將這些資訊轉換成可利用的數據，以便進行對設備的遠端監控。其中，常被用來嵌入物體的感測元件，包括紅外線、溫溼度、超聲波、亮度、壓力、室內定位系統等感測器，使物件具有感應環境變化的能力¹⁶⁷。感知層已普遍運用在許多日常生活中的應用技術，例如：安裝在汽車上的超音波感測器，倒車時即時告知車主與後方障礙物之間的距離，避免車輛與物體發生碰撞；震動感測器可監測地表震動情形，因此能提早得知地震發生區域及地震級數，並即時發出告警訊息。裝置在火車上的紅外線感應器，可用來判斷是否有乘客經過並自動開啟車門。

(2) 網路層 (Network layer)

網路層也可以稱為傳輸層，連接感知層以及應用層，作為兩層之間溝通的橋樑，負責訊息的可靠傳輸，經過初步的處理和分類感知層所蒐集的資訊後，將資料安全的傳送到資料處理系統。為了達到訊息傳送的目的，會在傳感設備中，加入具有聯網能力的元件，以便能隨時將資訊傳送至應用層進行資料讀儲存、處理、分析，以服務的方式表現給使用者，讓使用者能掌握即時資訊。訊息藉由有線或無線網路傳送，例如：互聯網、移動網路、衛星網路以及無線網路，而取決於不同傳感設備，使用技術主要有 3G、UMTS、Wifi、Bluetooth、紅外線以及 ZigBee 等等，因此，網路的基礎架構和通訊協議對於設備之間的資料交換非常重要^{168、169}。

(3) 應用層 (Application layer)

物聯網中的應用層主要是將「感知層」以及「網路層」的技術融合再一起，讓人們不受到地點的限制，藉由透過「聯網」的形式來享受各種不同設備間所串接起的應用服務，甚至能夠利用這些設備所收集到的資料來進行分析，以及和其他系統整合，以便於因應企業或社會上各種不同的需求。例如：現今蓬勃發展的大數據分析，就十分適合拿來對物聯網所收集到的大量數據做出許多的分析和應用，並從數據的分析結果中進行設備的最佳化(optimization)與自動化(automation)，讓設備的效率及效能提升。

¹⁶⁷ Yun, Miao, and Bu Yuxin. "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid.", IEEE, 2010/8/26.

¹⁶⁸ Khan, R., Khan, S. U., Zaheer, R., & Khan, S., "Future internet: the internet of things architecture, possible applications and key challenges", (pp. 257-260), IEEE, 2012/12.

¹⁶⁹ Suo, H., Wan, J., Zou, C., & Liu, J., "Security in the internet of Things: A Review", 2012 international conference on (Vol. 3, pp. 648-651), IEEE, 2012/3.

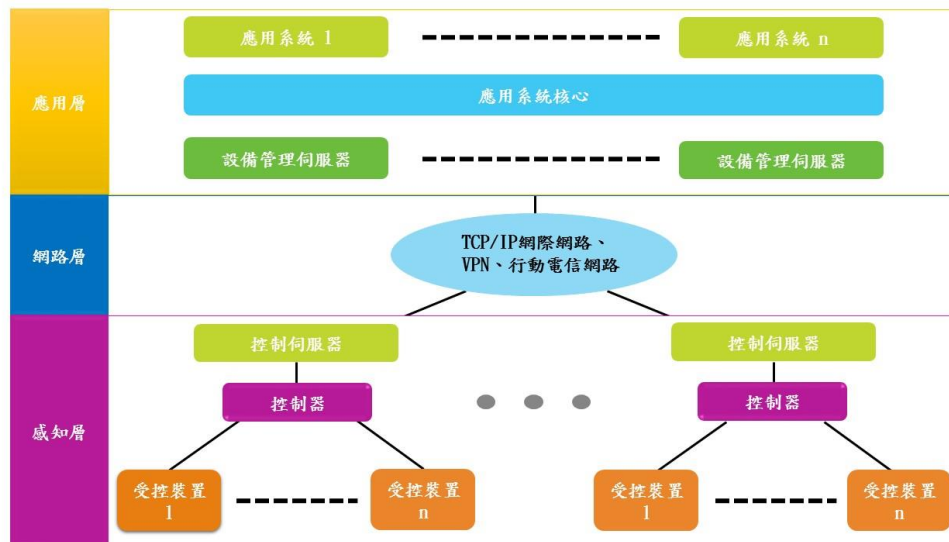


圖 3- 31 IoT 架構圖

資料來源：中華電信，2011 年 12 月

雲端運算的各種技術能夠讓物聯網更加擴大規模，他們之間融合後所產生的優勢是能夠被預期的¹⁷⁰。一方面，雲端能夠從儲存、運算能力、耗能等幾個優勢方面來補足物聯網其餘技術上的限制，相對來說，雲端可藉由物聯網來擴展範圍，用較為分散和動態的方式去處理現實生活的事情，進而能夠在這些場景中得到新的服務應用，因此當雲端和物聯網相互整合後，他們之間各種的互補特徵能夠解決兩種技術所存在的問題，並且能夠擴大優勢面，進一步影響未來的各種應用開發。

另外一項物聯網的重要應用是智慧城市的發展，由於物聯網能夠促進許多應用的開發，並且產生數量龐大以及多樣的數據，為公司和公共行政部門提供新的服務，因此將物聯網應用於城市環境是特別有意義的，它響應了許多國家政府正強力推動採用資訊及通訊技術(Information and Communication Technology，簡稱 ICT)解決管理公共事務，從而實現了所謂的智慧城市概念。雖然目前還沒有一個被正式廣泛接受的“智慧城市”的定義，但最終的目標是能夠更好地利用公共資源，提供公民更佳的服務質量，同時降低公共行政部門的營運成本¹⁷¹。

¹⁷⁰ Botta, Alessio, et al. "On the integration of cloud computing and internet of things", 2014 International Conference on. IEEE, 2014.

¹⁷¹ Zanella, Andrea, et al. "Internet of things for smart cities", IEEE Internet of Things journal 1.1 (2014): 22-32.

物聯網在健康與醫療產業上的應用也越來越明顯，目前穿戴式的醫療裝置可分為兩大產品類別，一種為專業的醫療裝置，需得到醫療之相關認證；另一種則是消費性的電子產品，而此種則不需要取得認證。其中發展出的特點為持續監控以及將醫療帶進家庭。在科技發展下，能將多種感測器裝置在衣物上，隨時監控使用者的健康資訊，讓醫療朝著行動化邁進。而醫療機械也開始往貼近使用者的方向發展，注重基本功能的穩定性和簡單的操作，讓高齡人口也能輕易的使用，在長照體系上補足醫護人員無法隨時到府的缺憾¹⁷²。而在遠端醫療監控以及臨床照護也都是物聯網運用的方向之一，在物聯網技術發展下，能節省醫療上的成本，以及降低人為上的失誤率。

2. NB-IoT 基礎架構

除一般物聯網架構外，在 3GPP Release-13 中特別提出了 NB-IoT 基礎架構，NB-IoT 旨在實現與傳統 GSM，通用分組無線業務(GPRS)和 LTE 技術的極佳共存性能，NB-IoT 下行鏈路和上行鏈路頻寬分別只佔了 180 kHz，相當於 LTE 傳輸中的一個資源塊(Resource Block)，遠低於 LTE 中 1.4-20 MHz 的頻寬。這代表資料的傳輸率將會因而下降，而優點則在於和寬頻相同的功率下較能夠抗干擾，傳輸距離也能夠延伸，更代表了它具有更加靈活的佈建方式。例如：GSM 電信業者可以用 NB-IoT 代替一個 GSM 載波（200 kHz）；電信業者可以通過將 180kHz 的物理資源塊（physical Resource Block，簡稱 PRB）中的一個分配給 NB-IoT 在 LTE 載波內部署；電信業者還可以在 LTE 載波的保護帶中部署 NB-IoT。

NB-IoT 廣泛使用了 LTE 原有的技術，包括下行鏈路正交頻分多重存取 (OFDMA)，上行單載波頻分多重存取 (SC-FDMA)，頻道編碼等等，顯著減少開發完整規格所需的時間。並且，基於現有 LTE 設備和軟件供應商，預計開發 NB-IoT 產品所需的時間將會大大的降低。以下分別就網路及實體層進行說明^{173、174}：

2.1. 網路架構

NB-IoT 是基於 LTE 的 EPC 網路架構並結合其特點對 LTE 進行優化，NB-IoT 網

¹⁷² 张晨光, 刘岩, 许伟, “智能医疗器械信息安全问题研究与对策. 中国药物警戒, 12(6)”, 363-365, 2015.

¹⁷³ Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper”, 2016.

¹⁷⁴ 张万春, 陆婷, 高音, “NB-IoT 系统现状与发展”, *ZTE TECHNOLOGY JOURNAL*, 2017.

路架構如下圖 3-32，主要分為無線接入部分(Evolved Universal Terrestrial Radio Access Network，簡稱 E-UTRAN)以及核心網(Evolved Packet Core，簡稱 EPC)，用戶端為下圖的使用者設備(User Equipment，簡稱 UE)，基地台為下圖中 E-UTRAN NodeB (eNodeB，簡稱 eNB)^{175、176}。

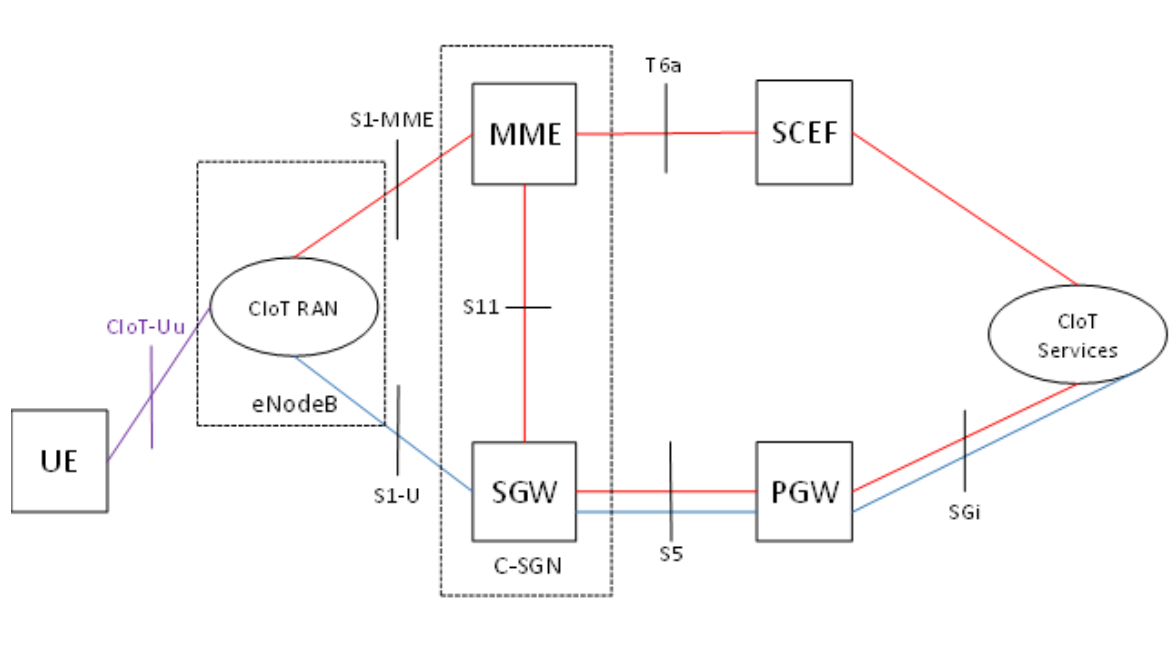


圖 3- 32 NB-IoT 網路架構圖

資料來源：Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper¹⁷⁷”, 2016

(1) 核心網路(Core Network)

為了向應用程式傳送數據，對演進封包系統 (Evolved Packet System，簡稱 EPS) 中的蜂窩移動網路(CIoT)定義了控制平面(Control-plane)與用戶平面(User-plane)，分別用來傳送認證訊息或傳送使用者訊息，在 NB-IoT 中則是對這兩個平面進行優化，如上圖 3-32，紅色顯示控制平面 ClIoT EPS 優化，藍色顯示用戶平面 ClIoT EPS 優化。

在控制平面 EPS 優化中，上行鏈路資料從 eNodeB(CIoT RAN)傳送給核心網路的管理者，MME (Mobility Management Entity)，從這裡，可以選擇通過 SGW (Serving

¹⁷⁵ 麥毅廷, 陳振庸, 楊峻權, 張朝欽, “在 3G 與 LTE 的異質網路下多重無線存取技術整合之評估”, *Journal of Computer Science and Educational Technology*, 2(1), 61-78, 2012.

¹⁷⁶ 郭昱賢, & 林盈達, “LTE 架構, 協定與效能”, 2011.

¹⁷⁷ Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper”, 2016.

Gateway) 傳送到 PGW (Packet Data Network Gateway), 或是到 SCEF (Service Capability Exposure Function), 後者只能用於非 IP(non-IP)資料傳送。經由這些節點, 最終被轉發到應用伺服器 (CIoT Services), 下行鏈路數據沿相反方向通過相同的路徑發送。在該方案中, 沒有建立數據無線電承載(data radio bearer), 而是在信令無線電承載(signaling radio bearer)上發送數據分組, 因此, 該方案最適合傳輸不頻繁和較小的資料封包。SCEF 是為 NB-IoT 設計的新節點, 用於通過 control plane 傳送非 IP 數據, 並為網路服務(認證、授權、發現和訪問網路功能)提供抽象接口。通過用戶平面(User-plane)EPS 優化, 與傳統資料流量相同的方式傳送資料, 通過 radio bearer 傳送資料, 通過 SGW 和 PGW 傳輸到應用服務器, 雖然在建立連接時產生一些開銷, 但是它有助於發送封包的序列。此路徑同時支持 IP 和非 IP 數據傳輸。

(2) 接取網路(Access Network)

在整體接入網架構上與 LTE 沒有任何區別。如下圖 3-33, eNodeB 使用 S1 介面連接到 MME 和 S-GW, 具有攜帶 NB-IoT 消息和數據分組的差異。即使沒有定義換手(Handoff)機制, 在兩個 eNodeB 之間仍然有一個 X2 接口, 這使得在 UE 進入空閒狀態後能夠快速重建連線。

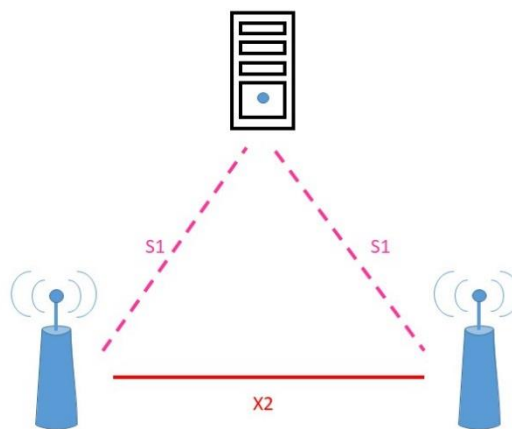


圖 3-33 網路架構的空中介面

資料來源：Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper”, 2016

(3) 頻段(Frequency Bands)

對於頻段, 使用與 LTE 中相同的頻率數, 並將部分 LTE 的頻譜分配給 NB-IoT。

在 Release-13 中定義了 NB-IoT 所使用的頻段，如下表 3-11 所示。

表 3- 11 NB-IoT 頻段

Band Number	Uplink frequency (range/MHz)	Downlink frequency (range/MHz)
1	1920-1980	2110-2170
2	1850-1910	1930-1990
3	1710-1785	1805-1880
5	824-849	869-894
8	880-915	925-960
12	699-716	729-746
13	777-787	746-756
17	704-716	734-746
18	815-830	860-875
19	830-845	875-890
20	832-862	791-821
26	814-849	859-894
28	703-748	758-803
66	1710-1780	2110-2200

資料來源：Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper” 2016

2.2. 實體層

NB-IoT 使用實體層訪問網路服務¹⁷⁸，並針對非常低的功耗和低成本進行了優化，以下為實體層的特性¹⁷⁹：

¹⁷⁸ Zayas, A. D., & Merino, P. (2017, May). The 3GPP NB-IoT system architecture for the Internet of Things. In Communications Workshops (ICC Workshops), 2017 IEEE International Conference on (pp. 277-282). IEEE.

¹⁷⁹ Wang, Y. P. E., Lin, X., Adhikary, A., Grövlén, A., Sui, Y., Blankenship, Y., ... & Razaghi, H. S. (2016). A

(1) 下行傳輸方案

NB-IoT 的下行鏈路基於與 LTE 相同的 15kHz 子載波間隔的 OFDMA。slot，subframe 和 frame 的持續時間分別為 0.5ms，1ms 和 10ms，與 LTE 相同。此外，在循環前綴（cyclic prefix）持續時間的 slot 格式和每 slot 的 OFDM 符號數量方面的也與 LTE 中的相同。實質上，NB-IoT 載波在頻域中使用一個 LTE 物理資源塊，即總共 180kHz 的十二個 15kHz 的子載波。重複使用與 LTE 相同的 OFDM 參數配置(OFDM numerology)，確保下行鏈路中與 LTE 的共存性能。例如，當 NB-IoT 部署在 LTE 載波內時，在下行鏈路中保留 NB-IoT 物理資源塊與所有其他 LTE 物理資源塊之間的正交性。

(2) 上行傳輸方案

NB-IoT 的上行鏈路支持多頻和單頻傳輸。多頻傳輸基於具有與 LTE 相同的 15kHz 子載波間隔，0.5ms slot 和 1ms subframe 的 SC-FDMA。單頻傳輸則是支持兩種參數，15 kHz 和 3.75 kHz。15 kHz 參數與 LTE 相同，從而在上行鏈路中實現與 LTE 的最佳共存性能。3.75 kHz 單頻參數配置使用 2ms slot。與下行鏈路相同，上行鏈路 NB-IoT 載波使用 180kHz 的系統頻寬。

(3) 操作模式

NB-IoT 可以獨立部署於超過 180 kHz 的任何可用頻譜。也可以部署在 LTE 載波內或在 LTE 載波保護頻帶內部署，共有 3 種佈建方式(如圖 3-34)，一為單獨佈建（Standalone），二是運用保護頻段（Guard Band）來佈建，三是在現行運作頻段內佈建（In Band），為了達到高覆蓋性，一般也建議使用較低的頻段來實現 NB-IoT，如 700MHz、800MHz、900MHz 等低於 1GHz 的頻段。此外，覆蓋不僅牽涉距離，也牽涉穿透能力，此方面業界強調 NB-IoT 比過往 2G GSM 有更好的穿透性，信號強度多 20dB，即便在室內用也能獲得高通信品質。

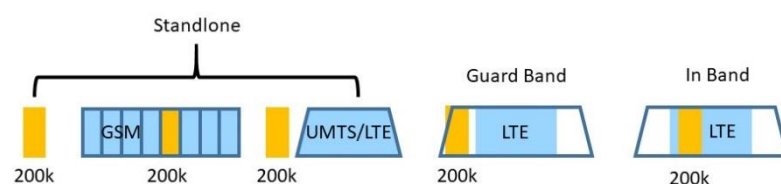


圖 3- 34 NB-IoT 佈建方式

資料來源：Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper” 2016

- **In-Band：**佈建在 LTE 頻段內，利用 LTE 載波(carrier)內的 resource blocks 來傳輸，在 In-Band 操作中，LTE 和 NB-IoT 之間的資源分配不是固定的。不是所有頻率都可使用，例如 LTE 載波內的資源塊，被允許用於連接，但僅限以下值，如表 3-12 中所示，不支持帶寬為 1.4 MHz 的 LTE 頻帶內操作。

表 3- 12 可用於 NB-IoT In-Band 模式中的 LTE PRB 索引

LTE system bandwidth	3 MHz	5 MHz	10 MHz	15 MHz	20 MHz
LTE PRB indices for NB-IoT synchronization	2,12	2,7,17,22	4,9,14,19,30,35,40,45	2,7,12,17,22,27,32,42,47,52,57,62,67,72	4,9,14,19,24,29,34,39,44,55,60,65,70,75,80,85,90,95

資料來源：Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper”, 2016

- **Guard Band：**佈建在 LTE 保護頻段上，利用 LTE 載波中未使用的 resource blocks 來傳輸。
- **Stand-alone：**使用其他獨立的蜂窩式系統專用頻帶來進行資料傳輸，例如：採用當前使用的 GSM 頻段，其帶寬為 200 kHz，在頻譜兩側仍然保留 10 kHz 的保護間隔。

(4) Frame 和 Slot 架構

在下行鏈路中，OFDM 使用具有標準循環前綴（CP）間隔的 15kHz 子載波。每個 OFDM symbol 由 12 個子載波組成，佔用 180kHz 的頻寬。一個 slot 中包含七個 OFDMA symbol。resource element 被定義為一個 OFDMA symbol 中的一個子載波，如下圖 3-35(NB-IoT slot 架構)中的一個方格。

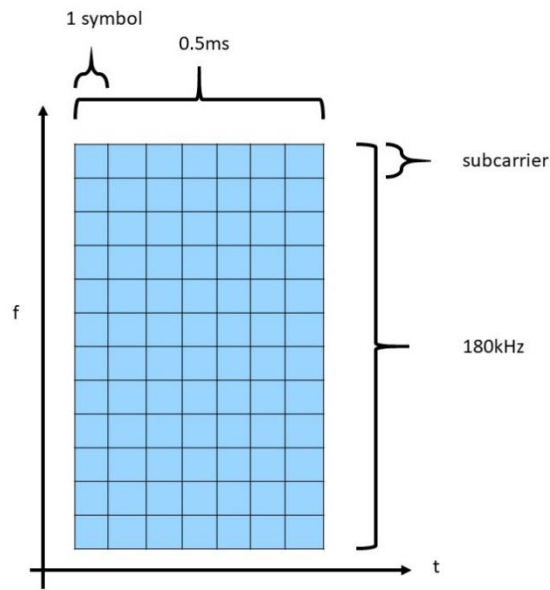


圖 3- 35 NB-IoT slot 架構

資料來源：Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper” 2016

這些 slot 以 LTE 相同的方式組成為 subframe 和 radio frame，一個 radio frame 持續 10ms，並分割成 10 個 subframe，一個 subframe 由兩個 slot 組成，如圖 3-36(NB-IoT frame 架構)所示。

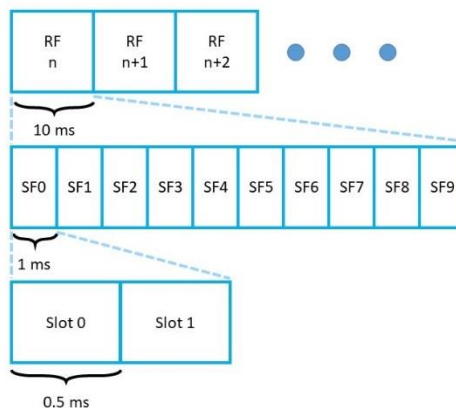


圖 3- 36 NB-IoT frame 架構

資料來源：Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper” 2016

NB-IoT 藉由現有 GSM 以及 LTE 的基礎上進行改進，不但可以減少開發時間還

可以減少建造基礎設施的龐大成本，並且針對低功耗的改進，大大延長設備的使用年限，這對於未來在廣大區域中大量佈建終端裝置有極大的幫助，也能更進一步實現智慧生活。

3. IoT 防護技術

物聯網藉由部署在環境中的感知設備取得資訊，透過網路將資料進行上傳，結合各種產業產生具有更高價值的服務，提高資料及設備的附加價值，產生如智慧醫療、智慧城市以及車聯網等等的智慧應用，為了取得更廣泛更即時的資訊，大量的設備將會連接到網路上，蒐集涵蓋個人、交通、土地、天氣、軍事等等，有些甚至與國家安全息息相關，在資料傳輸及應用過程中，資料的安全與否將會影響使用者對於物聯網的信賴。

此外，物聯網將從傳統網路拓展至移動網路以及傳感網路，並且這些物品將會互相溝通傳遞訊息，在安全上，物聯往將面對嚴峻的挑戰，安全及隱私問題的風險提升。在訊息和網路上的安全應具有識別、保密性和完整性等特性。不同於互聯網，物聯網將被應用在國家經濟相關的領域，例如智能交通、醫療服務、健康照護等，因此物聯網需要更高的可用性。綜上所述，除了物聯網帶來的智慧生活，在安全上也帶來不容忽視的威脅，如同表 3-13 所呈現出各階層所會遇到的安全需求以及機制，為了享用物聯網帶來的便利，建立一個安全的物聯網環境將是首要目標。首先，必須達到下列幾項原則¹⁸⁰：

(1) 保密性(Confidentiality)

確保資料的安全性和唯一性，並只允許已授權的用戶使用是非常重要的，所以在資料的管理上，必須確認良好的機制、管理的過程以及管理人員。

(2) 完整性(Integrity)

物聯網基於大量裝置間的資料交換，所以必須確認資料的精準度、是否是正確的傳送者，以及資料的傳送的過程中是否遭受惡意的篡改。

¹⁸⁰ Mahmoud, Rwan, et al, "Internet of things (iot) security: Current status, challenges and prospective measures." Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for. IEEE, 2015.

(3) 可用性(Availability)

物聯網連接大量的裝置，而這些裝置、所蒐集到的資料、服務能即時的提供有需求的使用者。

(4) 認證(Authentication)

在物聯網中的每個物件需要能識別和認證其他物件。然而，這個過程在物聯網中是一大挑戰，因為物聯網中包含大量不同的個體(裝置、人、服務等等)，而這之中的很多個體與其他的對象都是第一次相互溝通，所以物件彼此之間在每一次溝通時必須互相認證。

(5) 輕量級的解決方法(Lightweight Solutions)

輕量級解決方法是針對於物聯網中物件計算能力與電力限制的獨特安全功能。這本身不是一個目標，而是在設計加密或認證物聯網中裝置及資料時所需考量到的限制，因為必須能在物聯網中的裝置上運行，所以必須要有與裝置相容的能力。

(6) 異質性(Heterogeneity)

物聯網連接不同能力、複雜度的個體和不同的供應商，這些裝置甚至是不同的版本或使用不同的技術介面，且用於不同的功能上，因此設計的協議必須設計可以在不同裝置以及不同情況下使用。物聯網的目的是連接裝置與裝置、人與裝置以及人與人之間，因此可以提供不同性質物品與網路之間的連結。而物聯網中的一大挑戰是隨時變動的環境，一個裝置在同一時間可能連結到完全不同的設備群中，所以必須確認具有金鑰管理與安全協議的最佳安全加密系統。

(7) 政策(Policies)

必須制訂政策及標準確保資料的保護、管理以及傳送，更重要的是能執行這些政策的機制，以確保每個個體都能遵守這些標準。每項服務中都必須清楚的訂定服務層級協議(Service Level Agreements，簡稱 SLAs)，由於物聯網的異質性和變動的性質，現階段的政策用於電腦和網路安全的政策可能不適用，政策的制訂將會增加使用者對於物聯網的信任並為其增長及擴大規模。

(8) 金鑰管理系統(Key Management Systems)

在物聯網中的裝置必須交換加密資料確保資料的機密性，因此，需要可用於所有

框架的輕量級金鑰管理系統與能消耗裝置最少的運算能力去傳送金鑰，使得不同物品間可互相信任。

表 3- 13 物聯網安全需求

物聯網安全	安全需求	安全機制
感知層	- 機密性 - 節點行為偵測(信譽評估) - 密鑰協商	- 輕量化加密技術 - 入侵偵測系統 - 安全路由 - 金鑰管理機制
網路層	- 網路入侵偵測 - 資料保密性與完整性	- 節點認證 - 存取控制 - 防火牆技術
應用層	- 資料隱私防護 - 惡意行為偵測 - 資料庫存取權限 - 智慧財產權維護	- 統一身份認證 - 集中授權管理 - 資料庫存取控制 - 有效的電腦取證技術和資訊洩露追蹤機制 - 安全的電腦資料存儲和銷毀技術 - 惡意指令分析和預防

資料來源：ITSA 物聯網安全¹⁸¹

以下以物聯網的三個架構階層說明其安全需求^{182、183、184}：

(1) 感知層安全

感知層中具有各式各樣的節點，但都具有相似的共通性如構造較為簡單、電量有限、缺少如電腦的電量以及儲存空間，因此無法提供跳頻通訊以及公開金鑰加密演算法安全的保護，設置安全保護系統也非常困難，設備本身的防護能力非常低落，而由這些設備所組成的傳感網路必須建立因應的防護措施抵擋來自外部網路的攻擊，另一方面，感知設備所蒐集資料的隱私安全也是一大重點。為了保護節點間的訊息傳送的機密性，資料加密是絕對必要的，在資料進行加密之前，金鑰協商是非常重要的過程，

¹⁸¹ ITSA 學習資源服務平臺，“物聯網安全”。

¹⁸² 聂元铭, 张红军, & 韩惠良, “物联网的安全层级防护策略研究. 信息安全, (6), 0-0”, 2011.

¹⁸³ 武传坤, “物联网安全关键技术与挑战. 密码学报”, 2(1), 40-53, 2015.

¹⁸⁴ 刘宴兵, 胡文平, 杜江, “基于物联网的网络信息安全体系”, ZTE TECHNOLOGY JOURNAL 23, 2011.

使用越強的安全措施，耗費的資源相對更多，為了解決這個問題，輕量加密技術變的非常重要，包括輕量加密演算法以及輕量加密協定。目前主要應用在感知層中的防護技術為加密技術、金鑰管理機制、入侵檢測以及安全路由。加密技術方式例如：輕量認證協議；而侵入檢測的技術則包含入侵檢測系統(Intrusion-detection system，簡稱IDS)。

A. 輕量認證協議

RFID 是在物聯網中常見的感知設備，在應用上可同時辨識多個標籤，雖然較為便利使用，但卻存在著存取問題，攻擊者可以透過合法的裝置去竊取設備中的資訊或是對資料進行惡意篡改，目前可以透過結合物理以及加密機制進行安全防範，但在感知層中的設備為了大量部署以及貼近生活，在構造上都較為簡單，電力也較為短少，無法負荷大量的運算，因此，傳統的加密機制在物聯網中無法發揮最大的效益，這也產生了另一個安全議題:適合在有限資源的情況下的加密演算法，而輕量化加密協定就是為了該情況而被提出以增加感知設備的安全性。

B. 金鑰管理機制

在物聯網中，存在非常大量的資料，為了保護這些資料不被攻擊者所竊取，必須進行加密以保證安全，而金鑰就變成了攻擊者的攻擊對象之一，如下圖 3-37 所示。在資料傳輸前，必須確認發送者與接收者的身分認證，其中一個方法就是金鑰管理方案，這個方案包含了整個加密金鑰的生命週期，包含金鑰生成、建立、儲存、使用、更新以及破壞¹⁸⁵。

¹⁸⁵ Shah, P. G., & Ambareen, J., “A Survey of Security Challenges in Internet of Things (IoT) Integration with WSN”, AUSJOURNAL, 2014.

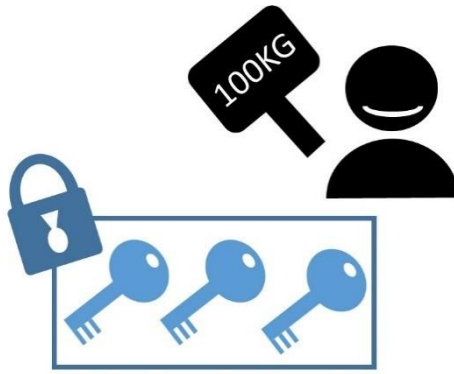


圖 3- 37 金鑰管理機制示意圖

資料來源：本團隊整理

C. 入侵檢測系統(Intrusion-detection system，簡稱 IDS)

入侵偵測系統(IDS)，在 1980 年時由 Anderson 提出的概念¹⁸⁶，目的是幫助系統如何處理攻擊，透過從電腦和網路不同來源所取得的資訊，包含網路所產生的流量以及封包，將這些訊息與先前存在的模式進行比較區別，確定是否存在攻擊或弱點，在受到攻擊之前，就進行預先偵測，並在判斷受到入侵時通知管理員，讓管理員能即時做出相應的對策或是判斷是否為誤判的情形。入侵檢測功能包括監控和分析使用者和系統活動、分析系統配置和漏洞、評估系統和檔案完整性、能夠判斷攻擊的特徵、異常活動模式分析。目前的入侵偵測系統，可分為特徵偵測(Signature-based)與異常偵測(Anomaly-based)兩種類型。

● 特徵偵測

對於已存在的攻擊非常有效，在系統建立之前，藉由觀察過去所受過攻擊的情形，分析攻擊的行為特徵，建立資料庫，並定時更新該特徵資料庫，對攻擊行為進行比對，判斷是否遭受攻擊，這個方法可以較為準確的判斷攻擊行為，有較低的誤判率，但在資料庫的建立上，需要長時間蒐集資料以及耗費人力進行分析、整理攻擊行為的特徵，並且對於新型態的攻擊手法，因為建立特徵行為，而導致無法及時的做出因應，目前較常見到的特徵偵測系統為 Snort。

¹⁸⁶ J.P Anderson, “Computer Security Threat Monitoring and Surveillance”, 1980/4.

● 異常偵測

則是先建立一套正確的範本，並在運行時透過規則判斷是否異常，不同於特徵偵測系統，異常偵測系統可以檢測出未知的攻擊，但同時也有著較高的誤判率，容易將正常行為誤認成惡意攻擊，因而造成系統的效益低落^{187、188}。

D. 安全路由

在感知層中會由各種不同的設備組成無線感測網路(Wireless Sensor Network，簡稱WSN)，路由和資料傳送是達成感知網路通訊的重要關鍵，但現今的路由協議存在著許多安全漏洞，導致資料在節點之間進行通訊時可能會遭受欺騙、改變、模仿以及重送等攻擊，或是遭到攻擊者注入惡意路由訊息，導致路由不一致，而安全路由就是確保資料在節點與節點間是安全的，主要使用的機制有資料保密、資料完整性、驗證或是新鮮度檢測^{189、190}。

(2) 網路層安全

網路層的功能是透過有線以及無線網路在感知層及應用層間進行資料的傳遞，雖然核心網路具有比較完善的安全防護能力，但是仍在存在中間人攻擊以及偽造攻擊等等，此外，垃圾信件、電腦病毒以及大量資料發送造成的壅塞也不容忽視。而在無線網路方面，相比有線網路具有更多的接口，惡意程式具有更多的入侵的路徑，因此在有線網路或是無線網路所存在的安全問題都是網路層所需要面對的問題，例如未授權的節點訪問或惡意攻擊，在這個階層中，現有的通訊安全機制(如存取控制、節點認證等)很難實際上的完全阻擋住有心人士的網路惡意攻擊。

分佈式阻斷服務攻擊(DDoS)是網路中一種常見的攻擊方式，在物聯網中則是更加嚴重，如何防止節點遭受DDoS攻擊也是一大課題。目前主要在網路層中使用到防護技術有存取控制、節點認證以及防火牆等。

¹⁸⁷ Ashoor, A. S., & Gore, S., "Importance of intrusion detection system (IDS)", International Journal of Scientific and Engineering Research, 2(1), 1-4., 2011

¹⁸⁸ 蔡秉任, "針對未知攻擊辨識之混合式入侵偵測系統(碩士論文)", 2014.

¹⁸⁹ Al Ameen, M., Liu, J., & Kwak, K., "Security and privacy issues in wireless sensor networks for healthcare applications.", Journal of medical systems, 36(1), 93-101., 2012

¹⁹⁰ Padmavathi, D. G., & Shanmugapriya, M., "A survey of attacks, security mechanisms and challenges in wireless sensor networks", 2009.

A. 存取控制(Access control)

在資料的傳輸過程中，資料的保密性是安全中的一環，確保資料的安全並只允許已授權的用戶使用。存取控制就是確保資源僅給予被授權的用戶，對於存取控制的資訊，設置對於目標的存取權並保護資源避免被未授權的存取，確保系統資源的機密性和完整性是基本的安全服務之一¹⁹¹。

B. 節點認證

物聯網在許多設備之間交換資訊，在這過程中，必須確保資料的完整性，首先需要確定就是資料是來自正確的發送者。節點認證讓互相溝通的個體間可以確認彼此身分並交換金鑰，在傳感網路中，使用者和終端節點必須互相認證以確保網路是安全的，終端節點間也需要互相認證以避免惡意節點的攻擊，並且防止未授權的用戶訪問物聯網節點。

C. 防火牆

防火牆是基於預設好的安全策略來檢查以及管理接收和離開的網路流量，通常在安全可信任的內部和外部網路間建立障礙，以下將防火牆分為兩個種類¹⁹²。

● 個人防火牆

個人防火牆是用於保護連接單一網路的電腦避免受到入侵者攻擊，能控制進出的網路流量與基於安全策略允許或拒絕通信，通常作為應用層的防火牆。

● 網路伺服器防火牆

網路伺服器防火牆是介於網路應用程式與客戶端的安全策略實施點，可在軟體或硬體中實現，像是在設備中運行或是在一個運行作業系統的伺服器上實現。

(3) 應用層安全

¹⁹¹ Ye, N., Zhu, Y., Wang, R. C., & Lin, Q. M., “An efficient authentication and access control scheme for perception layer of internet of things”, 2014.

¹⁹² Mlelwa, K. L., & Yonah, E. D. Z. O., “CHALLENGES THAT RESTRICT THE EFFICIENCIES OF SECURITY FRAMEWORKS IN E-COMMERCE: A REVIEW”, 2017/3.

在應用層中會處理大規模的資料以及對網路行為進行智能決策，而智能處理會受限於惡意資訊，因此必須建立一套規則對資料進行過濾，判斷資料是否是有用或是不是惡意訊息。而應用層最大的特點就是資料的應用，對於處理分析後的資訊，會依照不同需求結合不同的領域以及行業形成服務提供用戶進行使用，因此，在不同服務中所需要的安全需求就不盡相同，在資訊進行處理的過程中，系統本身所存在的漏洞就是一大問題，攻擊者藉由系統本身所存在的漏洞或是缺陷，植入病毒、遠端遙控來達到竊取資訊或是破壞系統的目的，而這影響的範圍不單只是系統本身，甚是擴及客戶、伺服器、防火牆等等。

在此階層中，資訊的分享是一大特徵，這也產生了如資料隱私、使用者權限控管以及訊息洩露等問題。針對於這個階層的安全問題，需要由兩個方向進行，一個是對於跨異質網路的認證以及金鑰協商，另一個則是用戶的隱私保護。在物聯網的應用層中，其安全挑戰及安全需求如下¹⁹³：

A. 依據不同使用層級權限來對同一資料庫的資料進行篩選

由於在 IoT 的應用當中，經常需要分配各種不同的使用權限給使用者，或是根據不同的情況進行資料庫中數據的篩選。例如進行城市規劃時，需要拿到各個道路交通堵塞的大概路況，此種數據的應用不需要很高的影像分辨率即可；當用於即時的交通管制時，需要的是較為詳細的資料，以利於即時的發現交通事故現場以及判斷當下的情況，像是發生事故的正確位置等資訊；當警方用於偵查時，期望從資料庫中拿到的資料是極為清晰的圖像資料，像是汽車牌照等此種清楚的訊息，如何根據不同的使用情形讓使用者拿到所需要的篩選資料，這種資料庫的訊息處理技術以及篩選將是應用中的一項挑戰。

B. 保護用戶隱私訊息的同時能夠正確進行認證

隨著訊息的網路化，越來越多的個人資訊以及商業機密在傳送同時，所需要顧慮到的是隱私保護的問題，以下說明幾種應用時之用戶隱私訊息保護。

- 正在移動中的使用者需要取得其位置資訊，同時不希望本身的位置資訊被不法取得。

¹⁹³武传坤,“物联网安全架构初探”,中国科学院院刊第 25 卷第 4 期, 2010/5/17.

- 使用者執行業務時，其業務之合法性需要被證明，同時間不希望他人所熟悉自己執行業務的相關資訊。
- 即時取得隱密的訊息，並確保此訊息不會被洩漏。例如：病人在急救時，醫護人員需即時取得病患的病歷等資料，但同時這些訊息屬於高度個人隱私機密的資訊，必須確保不被非法取得，甚至包含病歷資料庫的管理員亦不能窺探其病患的資料，因此，隱私保護技術需要讓病歷內容與病患身份之間不具備關聯性。
- 當匿名性的業務需要進行用戶資訊的認證，或是對隱私的資料進行加密傳輸同時，能夠正確驗證其身分的正確性。

C. 解決訊息洩漏追蹤的問題

對於網路高度依存的現今社會來說，面對每天各種網站的瀏覽或是隱私的保密級別不夠高，一個不小心就會造成個人資訊的洩漏。由於訊息洩漏的根本原因具有許多種，因此除了本身做好資料的隱密性之外，以技術層面來說使用者希望能夠追蹤這些已被流露出去的資訊，如此能夠了解自身的資訊是否被使用在不法的用途上，進一步的去追究洩漏訊息的根本原因，防範使用物聯網應用技術所造成可能的安全漏洞。

D. 從遭受惡意攻擊的硬體中進行取證

惡意行為的攻擊從來都是網路商業活動不可避免的意外，尤其在物聯網的環境中，由於其應用範圍十分廣泛，因此造成有心人士更加容易針對系統上的疏失來進行攻擊。若是能夠從被攻擊的系統當中去取得犯罪的有效證據，並且給予這些犯罪者相對應的懲罰，就可以達到威嚇的效果來減少惡意行為的發生。其中所衍伸出來的就是取證技術，從物聯網所串連的眾多平台當中去找尋蛛絲馬跡，甚至模擬駭客如何侵入物聯網中的設備，將能夠幫助使用者們更好的去防範惡意攻擊，減少利益的損失。

E. 如何銷毀因為加密而產生的臨時參數

和證據的取得對應的是數據的銷毀，任何重要的數據及資料在物聯網傳輸過程中必定會經過加密這道安全程序，有些加密技術的演算法在過程中會產生臨時參數，駭客透過挖掘出這些數值之後可能使他成功攻擊的機率提升。因此，就提升安全層面來說，這些臨時參數需要透過安全的技術及時地被移除，但就某方面而言，攻擊者也可能透過銷毀技術來確保犯罪的證據不被調查者蒐集到，進而提升取證的難度。因此以結論來說，如何以安全的技術手法來刪除對惡意攻擊者有利的數據將是可以被探討地

一個防護目標。

F. 保護電子產品和軟體的智慧財產權

物聯網融合商業上的應用將是實用上期望達成的目標之一，由於商業活動目的在於營利，但是盜版猖狂將會帶給企業利潤的損失，光是透過專利申請不見得能夠帶給產品的保護，因此對於企業來說該如何以技術層面來有效保護公司的電子產品以及軟體技術等產品，將是未來可以發展的防護技術。

除了在上述技術以及環境上的防護，在物聯網中，終端設備的使用者本身也非常的重要，物聯網的安全性不僅僅取決於採取的安全措施，使用者的使用方式也非常的重要，具有良好的使用習慣，可降低設備的安全風險。以下列出幾項在安全上需要注意的地方：

- 不連接不明的免費 Wi-Fi，經由 Wi-Fi 傳送的訊息，有可能被攻擊者所擷取。
- 將預設密碼修改為強密碼，預設或是太簡單的密碼很容易就能被暴力破解。
- 從聲譽良好且提供產品韌體更新的設備商購買設備，更新設備才能修補已被發現的漏洞。
- 定期更新由設備商提供的產品 Patch，避免網路上下載來路不明的更新軟體使得設備中被安裝不明軟體¹⁹⁴。

4. IoT 攻擊趨勢及防護建議

近年攻擊實際案例多以 IoT 攻擊為主，從本章一開始所整理的近年行動寬頻網路資安事件整理(如表 3-1)，即彙整了許多 2016 年至 2017 年最新之 IoT 攻擊事件。其中可發現 IoT 最常見之攻擊趨勢主要有兩種：❶惡意程式入侵及❷殭屍病毒侵入攻擊，本團隊已深入上述兩種資安威脅之攻擊流程進行研析並提出建議之防護措施。

4.1 惡意程式入侵-以 Mirai 為例

¹⁹⁴ Angrishi, K., “Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets”, 2017/2/13.

近年來已有許多 IoT 的攻擊事件，是遭受 Mirai 惡意軟體的攻擊，Mirai 通過不斷傳播到容易受攻擊的 IoT 設備，對目標服務器造成 DDoS 攻擊¹⁹⁵，Mirai 的攻擊流程及防護技術說明如下。

(1) 攻擊流程

Mirai 惡意軟體主要由四個部分組成：

- bot：是感染設備的惡意軟體。其雙重目標是傳播感染到配置不正確的設備，並在收到控制 bot 或 botmaster 的人員的相應命令後立即攻擊目標服務器。
- 命令和控制（C&C）服務器：為 botmaster 提供一個集中的管理介面，以檢查殭屍網絡的狀況並組織新的 DDoS 攻擊。
- Tor：平常則是透過匿名 Tor 網路與基礎架構的其他部分進行通信。
- Loader：通過與新的受害者直接溝通，促進針對不同平台（包括 ARM，MIPS 和 x86 共 18 個）的可執行文件的傳播。報表伺服器維護一個含殭屍網路中所有設備詳細信息的資料庫。新感染的裝置通常直接與之溝通。

其操作與通訊過程，最初，Mirai 通過 TCP port 23 或 2323 掃描隨機的公開 IP 地址。包括美國郵政局、國防部、網路號碼分配機構、通用電氣公司和惠普在內的一些 IP 地址被排除在外，可能是為了避免吸引政府關注，圖 3-38 為 Mirai 殭屍網絡運行和通信的關鍵步驟，詳細說明如下。

- 步驟一：進行暴力攻擊以發現弱配置的 IoT 設備的預設密碼。Mirai 有 62 個可能的用戶名稱和密碼。
- 步驟二：在發現正確的密碼並獲取 shell（command-line 或使用者圖形化介面）後，bot 會通過不同的 port 向報表伺服器發送各種設備特性。
- 步驟三：botmaster 經常經由 Tor 網路，透過 C&C 伺服器，與報表伺服器通訊來檢查新的潛在目標受害者以及殭屍網絡的當前狀態。
- 步驟四：在確定哪些易受攻擊的設備感染後，botmaster 會在 Loader 中發出感染命令，其中包含所有必要的詳細信息，例如 IP 地址和硬體架構。
- 步驟五：Loader 登錄到目標設備，並指示通過 GNU Wget 或小型文件傳輸協議（Trivial File Transfer Protocol，簡稱 TFTP）下載並執行相應版本的惡意軟體。此時，新增加的 bot 可以與 C&C 伺服器進行通訊，以接收攻擊命令。它通過解析執行文件中的域名，而不是靜態 IP 地址。因此，botmaster 可以隨著時間的推移而改變他的 IP 地址，而不需要修改 binary 文件，不需要額外的通訊。

¹⁹⁵ Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J., “DDoS in the IoT: Mirai and Other Botnets”. IEEE, 2017/7/7.

- 步驟六：botmaster 通過 C&C 伺服器發出簡單命令指示所有 bot 來對目標伺服器發起攻擊，並使用相應的參數，如攻擊的類型和持續時間以及 bot 和目標伺服器的 IP 地址。
- 步驟七:bot 將使用 10 種可用的攻擊之一開始攻擊目標伺服器，例如通用路由封裝（GRE）、TCP 或 HTTP 洪氾攻擊。

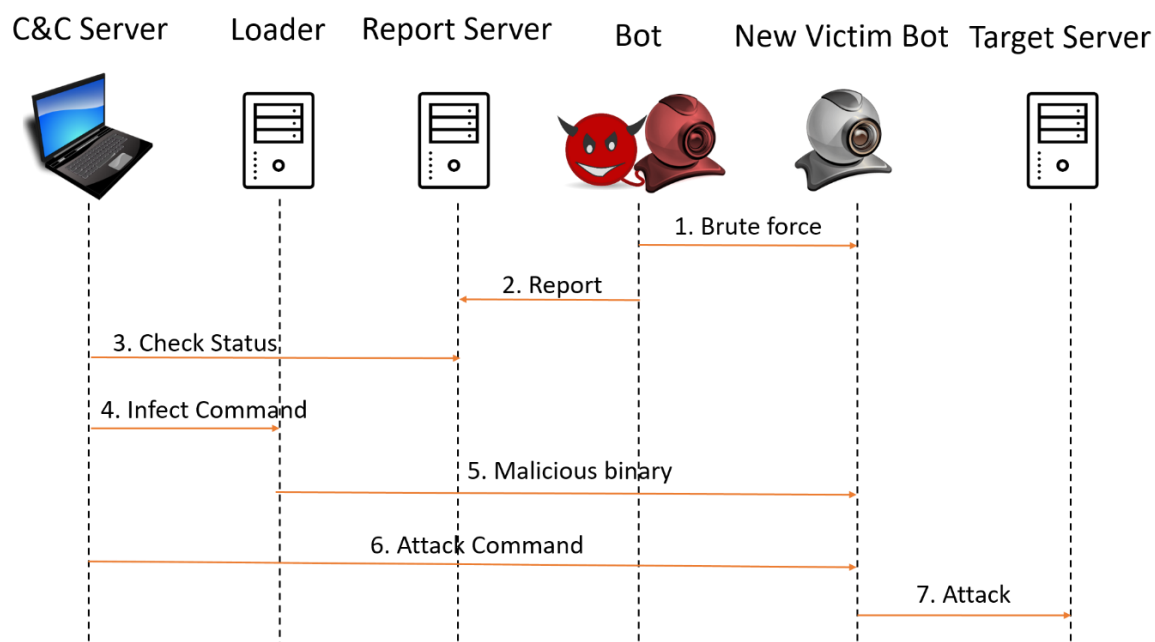


圖 3- 38 Mirai 攻擊流程

資料來源：DDoS in the IoT: Mirai and Other Botnets. Computer

(2) 防護流程

由上文的 Mirai 的攻擊流程可看出在進行攻擊之前會先經由 port 去掃描裝置，因此，建議關閉 IoT 設備上的 port 23 或 port 2323，或是在購買裝置後修改裝置的預設密碼並改為強密碼，避免被惡意程式暴力破解取得控制權。

4.2 殭屍病毒入侵-以 Persirai 為例

於 2016 年趨勢科技發現全球高達 1,000 種型號，約 12 萬台的網路攝影機遭到 Persirai 殭屍病毒所入侵感染，其攻擊流程及防護技術說明如下。

(1) 攻擊技術

於 2016 年的時候，趨勢科技發現全球高達 1,000 種型號的網路攝影機總計約 12

萬台遭到 Persirai 殭屍病毒侵入感染¹⁹⁶。而這一切的攻擊和病毒入侵的始作俑者是由於開放的原始碼 Mirai，攻擊者藉由惡意軟體 Mirai 作為媒介，入侵 CCTV 攝影機和數位錄影機(DVR)，將其作為踏板進行分散式阻斷服務攻擊(DDoS)。

主要攻擊流程入下圖 3-39。網路攝影機中通常會使用到的一種名為隨插即用(UPnP)的網路協定，由於其作用是讓設備將路由器上的端口開啟而當成伺服器的網路協定，但也因為如此變成惡意軟體眼中顯著的攻擊目標。而駭客登入這個有漏洞的缺口後便可以將命令注入，其作法是讓網路攝影機連上某一個下載網站，而該網站會回應一些命令，這些命令則導致其自網域下載惡意軟體的腳本並且執行。之後會先封鎖零時差攻擊，以避免其他惡意程式的入侵，受到攻擊影響的網路攝影機會向命令和控制(C&C)服務器發出報告並且接收 C&C 服務器的命令，接著再使用公布的零時差漏洞來攻擊其他裝置，其他使用這些網路攝影機的買家並不知道自己所購買的產品已經成為了駭客擴大攻擊範圍的幫兇。

儘管這些網路攝影機都是由不同的工廠製造生產，但都同時具備五個零時差漏洞，包含(CVE-2017-8224、CVE-2017-8222、CVE-2017-8225、CVE-2017-8223 和 CVE-2017-8221)¹⁹⁷。而駭客則可以藉由這些漏洞來入侵裝置更可以竊取出使用者的帳號密碼等資料，甚至可以攔截受害者在遭到攻擊後要傳回主機的資料。

¹⁹⁶ 大紀元, “鎖定陸製網路攝影機 恐 12 萬台染病毒”, 2017/05/12

¹⁹⁷ iThome, “全球 12 萬臺中國製網路攝影機，恐受殭屍病毒 Persirai 感染”, 2017/5/11

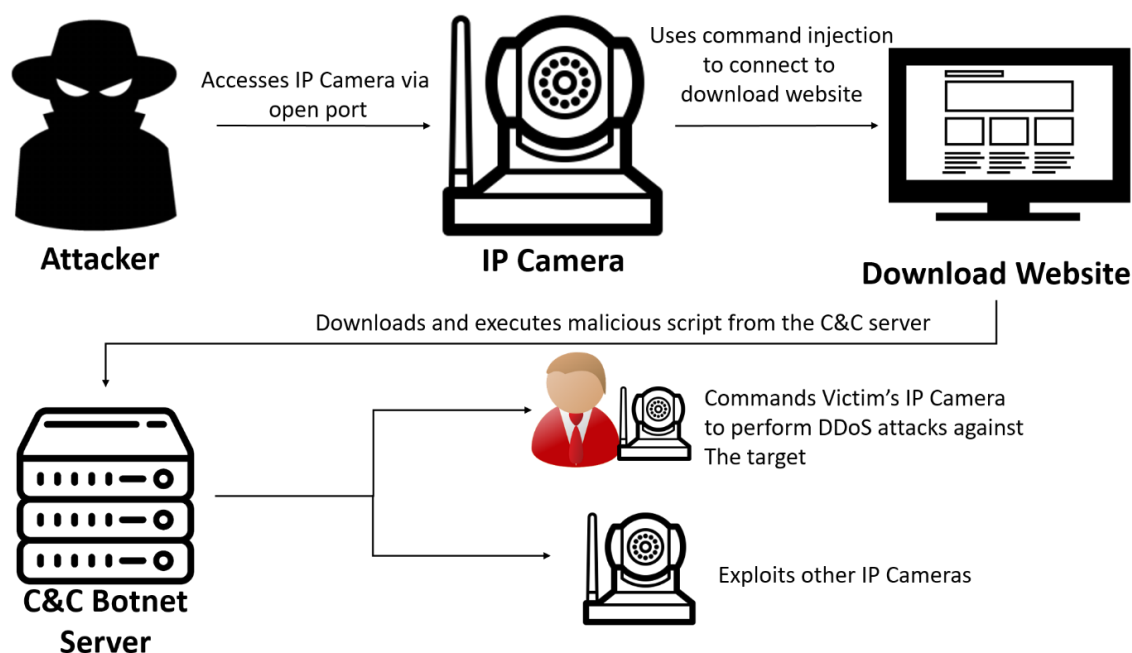


圖 3- 39 IPcam 攻擊流程

資料來源：The State Of Security,” Persirai IoT botnet threatens to hijack over 120,000 IP cameras”¹⁹⁸

(2) 防護措施

儘管網路攝影機藉由物聯網的幫助便利了人類的常生活也提供極大的貢獻，但其中存在的資訊安全漏洞卻成了最大威脅的存在，遭到入侵的裝置可以在使用者渾然不知的方式一步步探查該身邊資訊甚至所有生活作息，如沒有做好徹底完善的防護措施和資安防護，這將間接威脅到所有使用者的人身安全及隱私。以下提供幾個可以讓使用者避免此攻擊的防護措施¹⁹⁹：

- 變更密碼：由於許多的攻擊漏洞是因為使用者在設備界面中持續地使用默認密碼所造成的。因此，建議使用者應盡快地變更密碼，並且進一步的使用高強度的密碼來防範，使攻擊者無法輕易的達到攻擊的目的。
- 使用者禁用 UPnP：網路攝影的使用者建議在其路由器上禁用 UPnP，來防止網路的設備可以略過任何警告訊息並將端口連到外部網路。
- 最新版本更新：使用者應時時刻刻確保設備始終保持在最新版本，並且留意供

¹⁹⁸ Graham Cluley, “Persirai IoT botnet threatens to hijack over 120,000 IP cameras”, 2017/5/11.

¹⁹⁹ Trend Micro, “Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras”, 2017/5/9.

應商方面技術人員所發布的產品漏洞消息，以便可以減少攻擊者利用漏洞來攻擊的機會。

第二節 資安檢測標準與檢測流程之最新趨勢研究

在資安檢測標準與檢測流程最新趨勢研究上，本團隊深入 3GPP 與行動寬頻基站相關之 33 安全系列標準文件進行探討，關注其最新脈動，並針對 3GPP 2017 年 9 月最新發表之 TS33.216 eNodeB 安全保證規範進行研析，以做為本計畫第五章基站資安檢測項目規劃及第七章基站資安檢測規範草案之主要參考文獻；另也針對 GSMA 在產品與製程安全性的認證流程-安全保證方法及物聯網安全規範進行探討；並對現今全球認可的資安檢測標準 CC，在近年通過認證的行動寬頻網路產品安全文本進行研析，以做為本計畫研究之參考。期望藉由相關最新規範的研究，了解目前國際已制訂的檢測標準與流程，以作為本計畫基站資安檢測檢測規範草案制訂的參考及依據。

一、 第三代合作夥伴計畫(3GPP)

3GPP 組織創立於 1998 年 12 月²⁰⁰，自成立以來，致力於制定與推廣 2G、3G、4G、LTE 等行動網路的標準，並依環境與網路的演進及需求，在每次 Release 中持續發佈新的標準文件，全球電信業者與網通設備製造商皆會參考與依循 3GPP 制定之電信技術標準。3GPP 標準文件以不同主題及適用範圍分成許多系列，並且在每個系列中，對於各個面向提出了許多包含技術規範(Technical Specifications，簡稱 TS)與技術報告(Technical Reports，簡稱 TR)的文件。

因本計畫研究主軸為「基站」的「安全性」，本團隊延續一期的研究成果，持續追蹤與行動寬頻基站相關的 33 系列安全規範。在第一期的研究報告中已詳細說明及剖析與基站安全相關的 TS 33.401、TR 33.820(超微型(小型)基站安全技術報告)與 TS 33.320(超微型(小型)基站安全技術規範)這三份文件，本期將針對 3GPP 2017 年底最新釋出的 TS 33.216 文件作為介紹主軸，並深入研析與其相關的三份安全文件：包含 TS 33.117、TR 33.926 及已於第一期介紹過的 TS 33.401，這三份文件於近兩年的更新

²⁰⁰ 3GPP 官網, [Online]. Available: <http://www.3gpp.org/about-3gpp/about-3gpp>

動態與關注焦點。下表整理本工作項目將介紹之 3GPP 安全標準規範及 3GPP 文件常用之英文縮寫說明。

表 3- 14 3GPP 基站安全相關 33 系列標準

文件編號	文件名稱	規範內容	發布日期	備註
TS 33.401	3GPP System Architecture Evolution (SAE); Security architecture	3GPP 網路系統演進架構(SAE)及安全架構	Release8 2008/3	
TS 33.117	Catalogue of general security assurance requirement	網通產品之通用安全保證要求	Release14 2015/9	訂定 70 項網通產品通用之安全檢測項目
TR 33.926	Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes	3GPP 網通設備之安全保證規範的威脅與關鍵資產	Release13 2016/9	定義一般網通產品之關鍵資產與安全威脅，附錄特別針對 MME、PGW 及 eNB 定義其關鍵資產與安全威脅
TS 33.216	Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class	特定於演進式基站節點(eNB)之安全目標、安全要求及安全檢測項目	Release15 2017/9	訂定 12 項 eNB 基本安全功能需求檢測項目及延用 TS33.117 之 70 項檢測

資料來源：本團隊整理

表 3- 15 3GPP 文件常用之英文縮寫

英文縮寫	英文全名	中文翻譯
CIoT	Cellular IoT	蜂巢式物聯網
EPC	Evolved Packet Core	演進數據分組核心網路
EPS	Evolved Packet System	演進數據封包系統
GPRS	General Packet Radio Service	通用封包無線服務
HSS	Home Subscribe Server	歸屬用戶伺服器
ICMP	Internet Control Message Protocol	網際網路控制訊息協定
MME	Mobile Management Entity	移動管理實體
NAS	Non-Access Stratum	非存取層
PDN	Packet Data Network	封包數據網路
PGW	PDN Gateway	封包資料網路閘道
RAN	Radio Access Network	無線接取網路
RRC	Radio Resource Control	無線資源控制
SRVCC	Single Radio Voice Call Continuity	單一無線語音電話之連續性
UE	User Equipment	用戶終端裝置
E-UTRAN	Evolved Universal Terrestrial Radio Access Network	演進統一陸地無線接取網路
WLAN	Wireless Local Area Network	無線區域網路

資料來源：整理自 3GPP

(一) 3GPP TS 33.401-3GPP System Architecture Evolution (SAE); Security architecture

SAE 為 3GPP 提出對 LTE 網路演進核心網路架構安全的標準，為現今 LTE 網路架構的安全準則。TS 33.401 中詳細說明了 SAE 的安全架構，包含定義各元件與階層架構(第四章)、提出內部各個節點的安全要求(第五章)、UE 與 EPC 核心網間的元素(第六章)、金鑰的生成與銷毀(第七章)、經由 MME 的 NAS 資料與訊號安全技術(第八

章)、E-UTRAN 和 UTRAN(3G)間切換的安全機制(第九章)、E-UTRAN 和 GREAN(2G)間切換的安全機制(第十章)、網域控制平面的防護(第十一章)、後置迴路連結用戶層的防護(第十二章)、S1(eNB-EPC)介面防護(第十三章)、使用 SRVCC 完成 E-UTRAN 和 2G、3G 的切換(第十四章)和 IMS 安全機制(第十五章)。

在本計畫第 1 期研究中已對本份文件做過詳盡的介紹，於本期研究內容中，主要針對近年更新之重點進行研析，下表 3-16 為 Release15 中 2018 年 1 月 4 日發布的 15.2.0 版與 Release13 中 2015 年 12 月 18 日發布的 13.1.0 版的差異進行比較。由 3GPP TS33.401 更新的重點可看出，主要焦點為核心網路及基站(eNodeB)安全的加強，另針對 3GPP 所制定且全球許多電信業者已在試行的 LTE-WLAN 聚合(aggregation)安全架構進行定義。

1. 核心網安全性之加強：NAS 和其雜湊的方法、HSS 的防護措施。
2. eNodeB 安全性之加強：RRC 連線/中斷的處理、RRC 再連線程序應用於 CIoT 核心系統控制平面的最佳化、主要與次要 eNodeB 間的雙向連線。
3. LWA 之安全架構：金鑰的生成、LWA 聚合之安全並使用 IPSec 達成此目的。

表 3- 16 3GPP TS 33.401 規範更新整理

新增/改動的項目	新增/改動部分的說明
參考資料	新增[36]~[42]:TS 33.210、TS.33.310、TS 33.402、TS 36.463、TS 38.413、IETF RFC 7296、IEEE 802.11
7.2.4.4 NAS 安全模式指令程式	對 NAS 說明的補充並增加了 $HASH_{UE}$ 、 $HASH_{MME}$ ：NAS 為網路層的協定，負責管理維護 UE 與 MME 之間的連結； $HASH_{UE}$ 、 $HASH_{MME}$ 分別是 UE 和 MME 各自計算的雜湊值，提供 UE 作安全性的比對。
7.2.11 RRC 連線中斷與恢復	RRC 是存在於 UE 和 eNodeB 之間的網路層協定，主要功能為廣播 NAS 發出的訊息。
7.4.4 RRC 再連線程序應用	提出在此條件下的再連線方法。

新增/改動的項目	新增/改動部分的說明
於 CIoT 核心系統控制平面的最佳化	
附件 A 金鑰生成函式之 A.16~A.19	補足 EPS 內部的金鑰生成方式。
附件 E.3 主要與次要 eNB 間的雙向連線	UE 與主要、次要 eNodeB 間的金鑰生成及溝通。
附件 F.4 對 HSS 的妥協 (Compromise) 攻擊緩解與當 HSS 被妥協時的應對處理	HSS 為 EPC 內的資料庫，儲存了用戶的相關資料，主要用於提供系統作用戶的驗證。
附件 G LTE-WLAN 聚合 (aggregation) (簡稱 LWA) 的安全	LWA 定義為：當一台行動裝置同時開啟 Wi-Fi 與 LTE 服務時，可同時使用這兩種方式傳輸資料，也能進行無縫切換。
附件 H 使用 IPsec 協定完成 LTE-WLAN RAN 層整合	RAN 負責控制與優化 UE 和核心網間的連結，而附件 H 提供了藉由 IPsec 達成其安全性的方法。
附件 I 雜湊函式	定義 HASH _{UE} 和 HASH _{MME} 的雜湊方法。

資料來源：本團隊整理

(二) 3GPP TS 33.117- Catalogue of general security assurance requirements

3GPPTS 33.117 為網通產品之安全性要求的「目錄」，提出了適用於一般網路設備類別的檢測案例(包含存取認證、資料完整性、資料防護等)、檢測方法及目標，因為不少設備在常規環境下的安全要求大多相同，於是彙整成此份集大成的安全保證要求文件，作為檢測產品安全的基礎參考資料。另外，為了因應個別產品特性、環境要求的特殊測試案例，3GPP 也訂定個別設備的安全保證要求規範，將其分別收錄在 33 系列的其他文件內，目前包括 TS 33.116- MME 設備的安全保證要求規範，該規範內容

除依循 TS33.117 之檢測項目外，加入 MME 設備基本安全要求的檢測項目；及 TS33.216-eNodeB 的安全保證規範，同樣依循 TS33.117 之檢測項目外，加入 eNodeB 設備基本安全要求的檢測項目。

3GPP TS33.117 於第 4.1 節先訂定做檢測前網路設備應完成的事前準備：安裝完畢、開啟、標準化介面與營運管理維護介面的連結建立，以及建議檢測的工具：已實際投入案例檢測的商用產品、開源軟體，該文件建議若使用上述兩種之外的工具，則應提出此工具的品質保證以獲得公信力。

第 4.2 節定義安全功能要求及對應之檢測案例，主要內容有來自 3GPP 規範安全功能要求(4.2.2 節)，4.2.3 節以後則是羅列了 3GPP 規範中未涉及的要求但對於達到通用安全標準也是很重要的檢測項目，包含了網路設備通用的基本檢測項目(4.2.3 節)、作業系統相關(4.2.4 節)、網頁伺服器相關(4.2.5 節)、網路裝置相關(4.2.6 節)，保證網通產品基本的安全性。

第 4.3 節提出減少來自攻擊面的安全要求和檢測案例，包含了基本檢測項目(4.3.2 節)、作業系統相關(4.3.3 節)、網頁伺服器相關(4.3.4 節)、網路裝置相關(4.3.5 節)，透過通過這些測試項目以減少缺陷。

最後第 4.4 節為基本的漏洞檢測要求，利用商用產品或是開源軟體掃描包括連接埠(4.4.2 節)、漏洞(4.4.3 節)和進行強健性與模糊測試(4.4.4 節)來找出網通產品的缺陷。表 3-17 整理了 TS 33.117 的檢測項目。

表 3- 17 3GPP TS 33.117 檢測項目

4.2.3 基本檢測項目	
檢測項目	檢測子項目
4.2.3.2 資料保護	4.2.3.2.1 保護敏感數據的適當安全措施
	4.2.3.2.2 防止敏感性資料外洩
	4.2.3.2.3.敏感性資料的儲存保護
	4.2.3.2.4 敏感性資料的傳輸保護
	4.2.3.2.5 log 不能洩漏個人資料
4.2.3.3 系統可用性 及完整性保護	4.2.3.3.1 系統處理過度承載狀況
	4.2.3.3.2 開機不可透過外部儲存媒體從內建裝置啟動檢測
	4.2.3.3.3 系統過載情況的處理策略
	4.2.3.3.4 堅實性測試
	4.2.3.3.5 韌體更新應要求完整性驗證
4.2.3.4 認證與授權	4.2.3.4.1 認證策略
	4.2.3.4.1.1 系統功能的使用須先經過身分鑑別
	4.2.3.4.1.2 使用者帳號必須可以識別
	4.2.3.4.2 認證屬性
	4.2.3.4.2.1 每一個帳號至少要有一個身分鑑別因子方可鑑別成功
	4.2.3.4.2.2 預設帳號應要能移除或註銷
	4.2.3.4.3 密碼準則
	4.2.3.4.3.1 通行碼強度
	4.2.3.4.3.2 通行碼變更機制
	4.2.3.4.3.3 暴力及字典攻擊的防護
	4.2.3.4.3.4 通行碼顯示遮罩

	4.2.3.4.4 特別授權檢測案例											
	4.2.3.4.5 通行碼連續輸入錯誤處理											
	4.2.3.4.6 授權與存取控制											
	4.2.3.4.6.1 授權策略											
	4.2.3.4.6.2 角色型存取控制											
4.2.3.5 Sessions 防護	4.2.3.5.1 登出功能是否有效											
	4.2.3.5.2 授權具有閒置時間限制											
4.2.3.6 日誌檔	4.2.3.6.1 安全事件日誌檔											
	4.2.3.6.2 Log 傳輸應經過加密保護											
	4.2.3.6.3 安全事件日誌檔的存取控制											
4.2.4 作業系統												
<table border="1"> <thead> <tr> <th>檢測項目</th><th>檢測子項目</th></tr> </thead> <tbody> <tr> <td rowspan="6">4.2.4.1 一般性作業系統需求及相關檢測案例</td><td>4.2.4.1.1 可用性及完整性</td></tr> <tr> <td>4.2.4.1.1.1 系統容量不足的處理</td></tr> <tr> <td>4.2.4.1.1.2 ICMP 處理策略</td></tr> <tr> <td>4.2.4.1.1.3 標頭的處理策略</td></tr> <tr> <td>4.2.4.1.2 認證與授權檢測</td></tr> <tr> <td>4.2.4.1.2.1 確保高權限的系統功能必須經過身分鑑別</td></tr> <tr> <td>4.2.4.2 UNIX 作業系統需求及相關檢測案例</td><td>4.2.4.2.2 系統帳號必須能識別</td></tr> </tbody> </table>		檢測項目	檢測子項目	4.2.4.1 一般性作業系統需求及相關檢測案例	4.2.4.1.1 可用性及完整性	4.2.4.1.1.1 系統容量不足的處理	4.2.4.1.1.2 ICMP 處理策略	4.2.4.1.1.3 標頭的處理策略	4.2.4.1.2 認證與授權檢測	4.2.4.1.2.1 確保高權限的系統功能必須經過身分鑑別	4.2.4.2 UNIX 作業系統需求及相關檢測案例	4.2.4.2.2 系統帳號必須能識別
檢測項目	檢測子項目											
4.2.4.1 一般性作業系統需求及相關檢測案例	4.2.4.1.1 可用性及完整性											
	4.2.4.1.1.1 系統容量不足的處理											
	4.2.4.1.1.2 ICMP 處理策略											
	4.2.4.1.1.3 標頭的處理策略											
	4.2.4.1.2 認證與授權檢測											
	4.2.4.1.2.1 確保高權限的系統功能必須經過身分鑑別											
4.2.4.2 UNIX 作業系統需求及相關檢測案例	4.2.4.2.2 系統帳號必須能識別											
4.2.5 網頁伺服器												
<table border="1"> <thead> <tr> <th>檢測項目</th><th>檢測子項目</th></tr> </thead> <tbody> <tr> <td>4.2.5.1 HTTPS</td><td>網頁管理介面須支援安全通道傳輸</td></tr> <tr> <td>4.2.5.2 日誌檔</td><td>網頁管理介面須具備登入紀錄</td></tr> <tr> <td>4.2.5.3 User</td><td>HTTP User sessions 的控制與管理</td></tr> </tbody> </table>		檢測項目	檢測子項目	4.2.5.1 HTTPS	網頁管理介面須支援安全通道傳輸	4.2.5.2 日誌檔	網頁管理介面須具備登入紀錄	4.2.5.3 User	HTTP User sessions 的控制與管理			
檢測項目	檢測子項目											
4.2.5.1 HTTPS	網頁管理介面須支援安全通道傳輸											
4.2.5.2 日誌檔	網頁管理介面須具備登入紀錄											
4.2.5.3 User	HTTP User sessions 的控制與管理											

sessions 的管控	
4.2.5.4 網頁輸入控制	確保網頁輸入指令不會導致隱碼攻擊或是跨站腳本攻擊，應能對用戶的輸入進行驗證、過濾及轉換
4.2.6 網路裝置	
檢測項目	檢測子項目
4.2.6.1 資料保護	檢測同 4.2.3.2
4.2.6.2 可用性及完整性保護	4.2.6.2.1 IP 封包過濾策略 4.2.6.2.2 網路介面強健性要求 4.2.6.2.3 須支援傳入之 GTP-C 封包過濾功能 4.2.6.2.3 須支援傳入之 GTP-U 封包過濾功能
4.3 強化安全需求相關之檢測項目	
檢測項目	檢測子項目
4.3.2 基本檢測項目	4.3.2.1 不應存在不安全之網路服務 4.3.2.2 限制網路介面之網路服務 4.3.2.3 不應存在未使用軟體 4.3.2.4 軟硬體之除錯功能應關閉 4.3.2.5 不再支援的軟硬體應移除 4.3.2.6 遠端登入之權限控管 4.3.2.7 檔案系統存取權限控管
4.3.3 作業系統	4.3.3.1.1 須支援詐騙防止(anti-spoofing)功能 4.3.3.1.2 關閉 gratuitous ARP 4.3.3.1.3 可卸除儲存媒體禁止啟用自動播放功能 4.3.3.1.4 SYN Flood 防護 4.3.3.1.5 緩衝區溢位防護 4.3.3.1.6 外部檔案系統掛載限制
4.4 基本漏洞檢測要求	

檢測項目	檢測子項目
4.4.2 連接埠掃描	網路介面中只有被記錄的埠才能回應系統外部的要求
4.4.3 漏洞掃描	確認作業系統和安裝的應用程式不存在已知的漏洞
4.4.4 強健性與模糊測試	確認系統收到不可預期的輸入時仍保有強健性

資料來源：整理自 3GPP TS33.117

因 3GPP TS33.117 為 2016 年所發布的安全保證規範，追蹤近兩年的更新，主要為加強部分測試案例的說明或測試方法完整性的補強。其中值得關注和基站相關的更動是新增了 GTP-U 的測試案例。GTP 全名為 GPRS Tunneling Protocol(GPRS 通道傳輸協定)，此協定存在於網路層，起初作為 2G 系統的擴充協定，現在也應用在 LTE 網路，傳輸用戶的數據資料。在 GTP 協定包含以下三個部分：

- GTP-Control(GTP-C)：負責建立、管理與維持通道，3GPP TS33.117 (Release13)中已有提出 GTP-C 的檢測案例。
- GTP- User data tunneling(GTP-U)：用在 UE 和 PGW 間用戶資料的傳輸，能相容 IPv4、IPv6 等封包格式，檢測案例於 3GPP TS33.117 更新版本中新增，目的在於避免攻擊者透過此通道傳送惡意資料，因此系統應要有能力檢查此封包。
- GTP' (GTP prime)：用於傳輸計費相關的數據，目前尚未有測試案例。

表 3-18 整理了 3GPP TS33.117 近兩年檢測案例之更新內容，表中係以 Release14 中於 2017 年 6 月 14 日發布的 14.2.0 版，與 Release13 中於 2016 年 5 月 23 日發布的 1.3.0 版的所做差異比較。

表 3- 18 3GPP TS 33.117 規範更新整理

新增/改動的項目	新增/改動部分的說明
參考資料	移除了對 IETF3871 及 TR33.806 的參考
定義	將可辨識人員的定義從個人資料中獨立出來(舊版說明中也有提到但歸類在個人資料條目中)。
4.2.3.4.1.1 系統功能	測試方法：新增測試者需依靠自身經驗判斷製造商所

新增/改動的項目	新增/改動部分的說明
的使用須先經過身分鑑別	提供的系統運作相關功能的清單是否充足。
4.2.3.4.3.3 暴力及字典攻擊的防護	測試目標： 新增應建立預設的黑名單去阻擋用戶設定易受攻擊的密碼及相關測試的要求
4.2.6.2.3 GTP-U 封包過濾	新增此 測試項目 。對於所有基於 GTP-U 協定的訊息，系統應有能力檢查此訊息的發送者是否合法。
4.3.2.1 不應存在不安全之網路服務	測試方法&結果： 新增測試者須重啟一次網路產品並在未改變配置的情況下再重複測試一次，而重啟前/後應要有相同的行為及效能。
4.3.2.3 不應存在未使用軟體	測試方法&結果： 新增測試者應檢查系統內的預設範例檔案且不應在內部發現有更多的預設範例檔案。
4.3.1.1.2 關閉 gratuitous ARP	測試環境暨初始條件： 新增不適用於此測試的產品定義：此網路產品可能為了達到滿足特定部屬而在無聲明的情況下發送 gratuitous ARP(此 ARP request 目的為取得本機 IP 位址對應的 MAC 位址)。
4.3.3.1.4 SYN flood 防護	測試環境暨初始條件： 新增主機須連線到這個有能力執行 SYN flood 攻擊(利用 TCP 三向交握時傳送大量的 SYN 訊息達到 DoS 攻擊)的網路產品(例如：nmap 或 hping)
4.3.3.1.5 緩衝區溢位防護	測試說明： 新增注記：Solaris®, Linux® and Windows® 為常用的商業產品，此資訊是為了方便此文件檔的用戶們提供的，並不代表 3GPP 已認可這些產品。

資料來源：整理自 3GPP TS33.117

(三) 3GPP TR 33.926- Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes

TR33.926 文件定義了網通設備類別、安全威脅及其關鍵資產，並整理出 3GPP 目前已發現的安全威脅，此規範適用於 3GPP 定義的各類別網通設備，該文件附件部分則是針對單一類別產品的安全威脅及關鍵資產進行詳細定義及說明。

本文件在第四章描述了 3GPP 通用網通設備(Generic Network Product，簡稱 GNP)內容，並於 4.3 節定義了 GNP 的模型，包括 3GPP 定義功能、其他功能、作業系統、硬體和界面，4.4 節則訂出了這些項目的涵蓋範圍。

第五章部分列出了 GNP 須被保護的關鍵資產(5.2 節)，包含：

- 用戶資料和憑證(密碼)
- Log 資料
- 組態資料(GNP 的 IP 位址、連結埠、VPN ID、管理對象等)
- 作業系統
- GNP 應用程式
- 足夠的運算能力(處理能力不會接近臨界點)
- 硬體(大型電腦、電路板、電源供應器等)
- 欲保護之 GNP 介面

並根據上述關鍵資產進行威脅分析(5.3 節)，目前 3GPP 已識別的威脅有以下七大類，包含：

- 3GPP 定義介面之威脅(5.3.2 節)
- 身分欺騙(5.3.3 節)：使用他人身分進行非法存取
- 資料竄改(5.3.4 節)：入侵資料庫竄改資料或是攔截封包做中間人攻擊
- 抵賴(5.3.5 節)：用戶執行某項指令時拒絕此動作與其有關聯
- 資訊揭露(5.3.6 節)：將訊息暴露給不應該知道的使用者
- DoS(5.3.7 節)：使目標服務癱瘓
- 提升權限(5.3.8 節)：攻擊者獲得管理員權限以妥協或破壞系統

該文件附錄部分為單一設備類別的關鍵資產與安全威脅，目前以三個附錄定義三個設備個別的關鍵資產與安全威脅：附錄 A 是 MME，須保護的資產(A.2.1 節)有行動數據的管理、路由路徑的選擇與 MME 介面，威脅部分有認證與共同金鑰協定(Authentication and Key Agreement；簡稱 AKA)相關(A.2.2 節)、安全模式指令程序相關

(A.2.3 節)、行動無線接取內部安全相關(A.2.4 節)、行動無線接取間安全相關(A.2.5 節)和釋放非緊急之承載(A.2.6 節)；附錄 B 是 PGW，須保護的資產(B.2.1 節)UE 資料、PGW 介面、PGW 軟體；附錄 C 是 eNodeB，須保護的資產(C.2.1 節)有行動數據的管理、SCAS 範疇內的 eNodeB 介面、eNodeB 軟體，其中附錄 B、C 為近期新增的威脅，這兩種類別的威脅項目將於下表一併呈現。

近兩年 3GPP TR 33.926 主要新增 PGW 與 eNodeB 方面的安全描述，而這兩項設備為構成 3GPP 對於 LTE 無線通訊標準所提出的 SAE 架構中的兩個重要元件，該兩項元件之功能說明如下。

- PGW 主要能讓 UE 從外部連線到系統，並可在閘道中執行 LTE 和非 LTE 系統之間的相容切換；此外也能支援計費系統，導致此閘道可能成為攻擊者攻擊計費系統的標的，因而特別將此項目獨立出來。
- eNB 為連接用戶與行動網路之間的硬體設備(即為基站)。附件 C 內的數種威脅皆為假設若沒有在無線通用網路與核心網之間、或是基站與基站之間做防護時會發生的情況。eNodeB 的相關檢測案例可參考 TS 33.216 文件。

由此可看出 3GPP 對 TR 33.926 文件目前的更新方向著重在 SAE 架構的安全威脅。表 3-19 整理 3GPP TR 33.926 近年更新的內容，表中為 Release15 於 2017 年 9 月 21 日發布的 15.1.0 版與 Release13 於 2016 年 9 月 30 日發布的 13.1.0 版的差異比較。

表 3- 19 3GPP TR 33.926 規範更新整理

新增的威脅	新增威脅的說明
5.3.4.7 竄改用戶 Session	若生成 Session 的方法不夠隨機，攻擊者可藉由預測、猜測破解此 Session 後進行資料竄改。
附件 B：網路設備類別的 PGW 相關方面	威脅說明如下列三欄
B.2.2.1 IP 位址之連續使用	當某個 UE 使用到其它 UE 剛釋出的 IP 位址，網路端可能會因此而誤以為先前使用此 IP 位址的 UE 仍在使用中，導致部分的網路功能異常(例如誤傳私人資料到新的 UE)。

新增的威脅	新增威脅的說明
B.2.3.1 傳送未認證的資料到其它 UE	當互傳訊息的兩個 UE 在同一個 PGW 內時，封包將不會進入 PGW 而是直傳到目標。攻擊者可用此種特性繞過網路上的防護機制而直接攻擊其他 UE。
B.2.4.1 無作用的緊急 PDN 連接版本	當設定過期時，PGW 必須釋放出占用的資源，否則會導致伺服器的資源被耗盡。
附件 C：網路設備類別的 eNB 相關方面	威脅說明如下列四欄
C.2.2.1 控制平面的資料保密防護	攻擊者能藉由攻擊基站以偽造傳送到 MME 的封包而成為合法 UE，或是直接竊取他人的隱私資料。
C.2.2.2 控制平面的資料完整性防護	攻擊者可操控封包，對 UE 做 DoS 攻擊。
C.2.2.3 用戶在 eNB 中做的加解密	攻擊者能在無線通用網路的平面間做 DoS 或是中間人攻擊。
C.2.2.4 用戶明文資料的完整性防護	攻擊者能控制、修改用戶在無線通用網路與核心網之間的資料並做 DoS 攻擊。

資料來源：整理自 3GPP TR 33.926

(四) 3GPP TS 33.216²⁰¹- Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class)

因應 5G 技術的發展，3GPP 組織於 2017 年 9 月發表 3GPP TS 33.216 基站(eNodeB)的安全保證規範，本團隊並將該規範全文翻譯為中文版本請參閱附錄二。3GPP TS 33.216 主要參考 3GPP TS33.401、TS33.117 及 TR33.926 三分規範文件，圖 3-40 即說

²⁰¹ 3GPP TS 33.216, “Security Assurance Specification (SCAS) for the evolved Node B (eNodeB) network product class (Release 15)”.

明 3GPP TS 33.216 參考其他文件之主要內容

3GPP TS33.216 規範的目標與 TS 33.117 相似，差別在於 TS 33.216 主要是針對 eNodeB 設備的安全技術要求和檢測案例。該規範的安全定義與要求、檢測內容幾乎為承自其它規範，擷取適用於 eNodeB 設備的部份，3GPP TS33.216 主要引用 TS33.401、TS33.117 及 TR33.926 三分規範文件的內容說明如下：

- 基於 TS 33.117 的規範內容，採用適合 eNodeB 的通用測試案例，增加部分 TS 33.117 內沒有的檢測內容，確立出 eNodeB 專用的檢測案例。
- 引用 TS 33.401 的 eNodeB 之基本安全功能要求。
- 引用收錄於 TR 33.926 附件 A 的 AKA(Authentication and Key Agreement，認證密鑰協商)相關威脅，為了去除這些威脅，設計出 eNodeB 於認證上之安全要求。

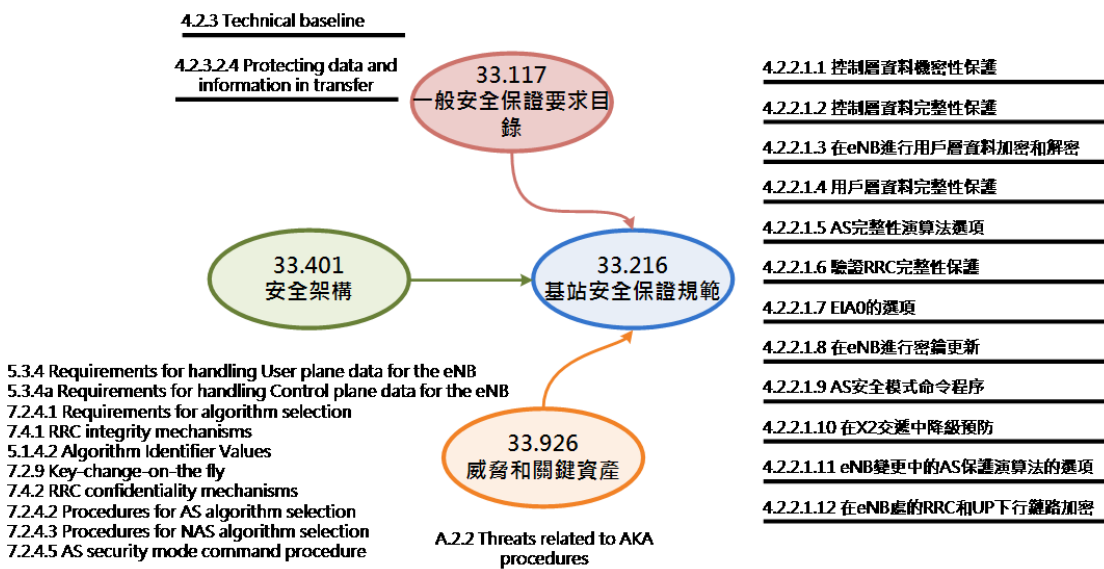


圖 3- 40 3GPP TS 33.401、TS 33.117、TR 33.926 與 TS 33.216 關係圖

資料來源：本團隊整理

3GPP TS 33.216 參照上述三份安全規範文件，構成完整的 eNodeB 檢測案例。內容包含 eNodeB 特定安全要求的具體檢測項目共 12 項(如表 3-20)，及 3GPP TS33.117 通用之檢測項目 70 項；在 12 項 eNodeB 特定安全要求的具體檢測項目中，前 4 項檢測項目係引用自 TS 33.117 的 4.2.3.2.4 節，另外 8 項檢測項目則是於本規範所定義；本規範 4.2.3 節之後的檢測項目則完全取自 TS 33.117 4.2.3 節。

表 3- 20 3GPP TS 33.216 特定於 eNB 之安全要求檢測項目

基於 TS 33.401 的 eNB 安全性功能要求	
檢測項目	要求說明
4.2.2.1.1 控制層資料機密性保護	S1(eNB-EPC)/X2(eNB-eNB)介面間控制層封包的保密保護
4.2.2.1.2 控制層資料完整性保護	S1/X2 介面間控制層封包的完整性保護
4.2.2.1.3 在 eNB 進行用戶層資料加密和解密	eNB 應負責 Uu(UE-eNB)介面、S1/X2 介面間用戶層封包的加解密。
4.2.2.1.4 用戶層資料完整性保護	eNB 應負責 S1/X2 介面間用戶層封包的加解密。
4.2.2.1.5 應用伺服器完整性演算法選項	應預先設定好可使用的加密演算法，排出優先順序
4.2.2.1.6 驗證無線資源管理訊息完整性保護	當完整性驗證失敗時應能做出應對，捨棄掉此訊息
4.2.2.1.7 EPS 完整性演算法零號選項	只有在無授權的緊急電話時才能選擇使用演進式封包系統完整性演算法零號
4.2.2.1.8 在 eNB 進行金鑰更新	當封包數據匯聚協定中的 COUNT 欄位將溢位歸零導致金鑰重複分配時，eNB 應觸發內部金鑰的更新
4.2.2.1.9 應用伺服器安全模式命令程序	安全模式指令應由最高順位的完整性演算法保護
4.2.2.1.10 在 X2 交遞中降級預防	在路徑變更的訊息中，目標 eNB 應將從來源 eNB 所發出的 UE EPS 安全功能列表轉送至 MME
4.2.2.1.11 eNB 變更中的應用伺服器保護演算法選項	目標 eNB 應根據收到的 UE EPS 安全功能列表選擇最高順位的演算法，若和來源

基於 TS 33.401 的 eNB 安全性功能要求	
檢測項目	要求說明
	eNB 的選擇不同時應藉由換手指令通知 UE
4.2.2.1.12 在 eNB 處的 RRC 和用戶層的下行連結加密	eNB 應在傳送應用伺服器安全模式指令訊息之後開始加密 RRC 與用戶層的下行資料

資料來源：整理自 3GPP TS33.216

二、 全球行動通訊協會(GSMA)

GSM 協會的起源可追溯至 1982 年由歐洲郵電行政大會(Confederation of European Posts and Telecommunications，簡稱 CEPT)建立的 EU GSM(Groupe Speciale Mobile)小組，目的在於建立出泛歐的行動技術，而隨著越來越多歐洲國家的認同及簽署合約，GSM 協會正式於 1995 於瑞士成立。協會成立初期主要致力於 GSM 行動電話系統的共通標準化與推動，和當時的 GSM 相比，協會推出的版本之最大差異在於語音訊號的數位化。隨著科技的演進，GSM 協會的文件也不斷地推陳出新，發表前瞻的網路相關文件。在 3GPP 推出安全保證規範(SCAS)的同時，也與 GSMA 合作訂定「網路設備安全保證方法」(Network Equipment Security Assurance Scheme，簡稱 NESAS)，訂定網通產品通過安全保證規範認證的流成；另外 GSMA 在協助電信業者推動物聯網服務的同時，近年也訂定了「物聯網安全」標準，因此本工作團隊特別將 GSMA 訂定「網路設備安全保證方法」(NESAS)及「物聯網安全」標準深入探討。

(一) 網路設備安全保證方法(NESAS)

NESAS (Network Equipment Security Assurance Scheme)網路設備安全認證方法為 GSM 協會和 3GPP 組織合作，主要搭配 3GPP 訂定之安全保證規範(SCAS)，共同定義的檢測方法，旨在增加安全性與降低商業風險及成本。提出一套可滿足網通設備之一系列安全性要求標準及認證流程，從業者在開發與產品生命週期的條件下即開始進行。儘管目前 NESAS 尚未發表正式版的文件，但整體認證流程的架構大致上已經完整，因此本團隊將說明 GSMA NESAS 所建議之認證流程，主要參考 GSMA 之四份文件：

- FS.13 NESAS 整體概述²⁰²(Network Equipment Security Assurance Scheme Overview)：介紹了 NESAS 整個體系的架構與驗證流程，並以引用連結的方式帶出後三份文件的主題與相關參考資料，這些文件會更詳細地描述 NESAS 不同面向的細節。(Ver 0.3)
- FS.14 NESAS 安全檢測實驗室之認證²⁰³(Network Equipment Security Assurance Scheme - Security Test Laboratory Accreditation)：定義安全檢測實驗室該如何依照 NESAS 進行認證，也提出了評估實驗室和授予其憑證的標準。(Ver 0.7)
- FS.15 供應商開發與產品之生命週期的要求及認證過程²⁰⁴(Network Equipment Security Assurance Scheme - Vendor Development and Product Lifecycle Requirements and Accreditation Process)：定義供應商開發和產品生命週期過程的要求，並且描述了產品認證的過程。(Ver 0.21)
- FS.16 NESAS 之爭議處理程序²⁰⁵(Network Equipment Security Assurance Scheme - Dispute Resolution Process)：定義爭議解決的流程。(Ver 0.3)

1. NESAS 整體概述

如引言所述，NESAS 為 3GPP 組織和 GSM 協會共同建立，3GPP 定義 3GPP 網路功能的安全要求與檢測案例，提出的安全保證規範(SCAS)(NESAS 認證所需通過的檢測項目即為 3GPP TS 33.117、TS 33.116、TS33.216 等規範)；GSM 協會則是負責定義且維護 NESAS 規範，範圍涵蓋了供應商開發和產品生命週期過程的認證流程，檢測實驗室的認證以及網路設備安全的評估，此外還定義了爭議解決流程並管理整個計畫，將這些元素結合後便是 NESAS 的全貌。

NESAS 期望藉由一套完整的驗證方法，使一項產品通過 NESAS 的認證，即可代表此產品擁有開箱即用的安全保證，並且能幫助供應商避免零散的監控管理與客戶要求。因為 NESAS 的最終目標是讓這些與 NESAS 計畫相關的利益關係廠商願意參與，一起制定共同標準，因此在提出有效的安全保證技術時，並非只考量技術層面，還須重視組織安全性的改進、網路設備安全層級的可檢視性、營運可行性與市場接受度，

²⁰² GSMA, “Network Equipment Security Assurance Scheme Overview (Version 0.3)”, 2016/5/11.

²⁰³ GSMA, “FS.14 Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation (Version 0.7)”, 2016/3.

²⁰⁴ GSMA, “Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process (Version v0.21)”, 2016/6.

²⁰⁵ GSMA, “FS.16 Network Equipment Security Assurance Scheme - Dispute Resolution Process (Version 0.3)”, 2016/3/16.

必須在這些因素之間取得最佳平衡，

現在各個國家的電信業者，透過各國制定的法律，必須為設備的可靠度負起責任，然而業者在經營中只能對設備進行安全控制，因此相當仰賴設備供應商當初設計此產品時的安全性，所以在購買之前，衡量網路設備的安全等級是十分重要的。目前業者主要的評估方法有兩種：

- (1) 對供應商的安全相關開發和產品生命週期過程進行認證：允許供應商各自定義自己的內部流程，並且描述如何將安全性嵌入至設計、開發、營運和維護裡面，再將此份報告書交給外部的審計委員來評估是否確實且具有可行性，供應商可藉此獲得合格的認證。這種方法的好處為供應商不需要向外界發表其產品設計的內部細節，只有審計委員知道，因此能保有自身產品的商業機密。
- (2) 交由具有標準化安全檢測的合格測試實驗室對網路設備進行安全評估：若該網路設備有一套已定義的一系列安全檢測，並且所有網路設備都依據這些檢測案例進行測試，則可以客觀的衡量產品的安全層級且具備了可檢視性。且若這些檢測是經由被認可的檢測實驗室進行，則更能確保檢測的一致性與此產品的品質，因此網路功能的標準化將有助於此種方法的可靠度。

以上方法皆能有效的給予電信業者選擇其供應商，而 NESAS 的認證流程亦是遵循這兩種方法，定義了以下步驟：

- 供應商定義了產品的安全設計、開發、經營和維護流程並進行應用
- 供應商向外部的審計委員展示這些流程
- 網路設備的安全層級經過測試和記錄
- 產品的測試交由合格的測試實驗室根據 3GPP SA3 定義的安全要求進行
- 測試結果的文件可隨同被購買的網路設備一同交給電信業者

圖 3-41 為 NESAS 認證的流程。當有一個網路設備申請認證時，GSMA 首先會任命一個審計小組來審核此設備的供應商並撰寫成審計報告，GSMA 依此報告決定是否給予認證。通過後供應商設計出此產品並將其送達 NESAS 認可之安全檢測實驗室(由 ISO 17025 認證之機構來進行認證)進行評估測試，檢測實驗室依據審計報告中提供驗證流程所需的訊息與相關 SCAS 來做評估，驗證產品的安全性，並撰寫出包含檢測結

果的評估報告，日後供應商便能將報告書連同此設備一併交給客戶。NESAS 提出的評估流程同時已被 3GPP 收錄於 TR 33.916 規範文件中。

總而言之，NESAS 採用以下方法來解決業界的需求及挑戰：

- 認證供應商的產品開發流程
- 認證供應商的產品生命週期過程
- NESAS 安全檢測實驗室使用 3GPP 定義的和標準化的安全檢測進行網路設備的評估

但為了在行動業者和利益關係人間取得雙方皆能接受的平衡，以下項目的驗證被 NESAS 排除在初始檢測範圍之外：

- 官方認可的網路設備不用進行認證
- 此技術無法辨明網路設備是否真的沒有某些功能(例如後門)
- 此技術不能取代現有業者或是國家的要求
- 此技術不包含網路設備之間介面的安全性
- 此技術不處理端到端的安全需求

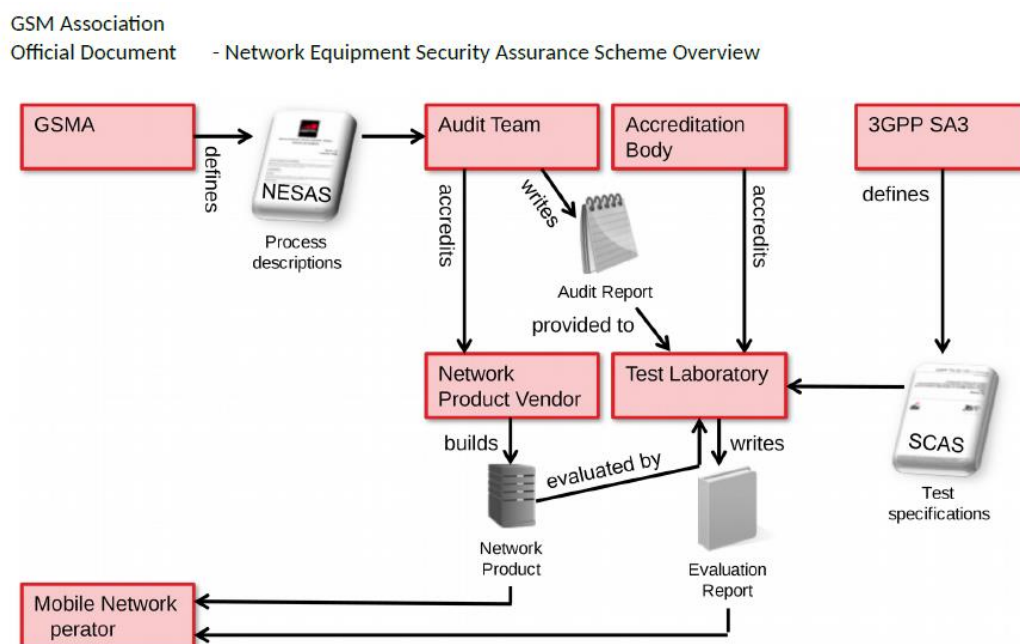


圖 3- 41 NESAS 之架構概述

資料來源：GSMA

2. NESAS 安全檢測實驗室之認證

為了能夠令安全檢測實驗室的建立與維護具有實際效益，使其能夠進行可理解、可重複並保持一致性的完整測試，因此 NESAS 的認證流程中，檢測實驗室本身必須被 GSMA 認證。安全檢測實驗室需要被保護的資產包含了：

- 實驗室的人事資源
- 實驗室的工作流程與準則
- 實驗室使用所需的設備及工具

以確保安全檢測實驗室以上資產的完整性，NESAS 選擇 ISO 17025 作為實驗室是否合格的認證標準。ISO 17025(General requirements for the competence of testing and calibration laboratories，實驗室品質與管理系統)是認證檢測實驗室的國際標準，且具有通用性，不論進行哪一種類的產品測試皆能進行鑑定，而實際上 ISO 17025 也是目前唯一做檢測實驗室認證的全球標準。

ISO 17025 為檢測實驗室的認證打下了良好且堅固的基礎，當一個實驗室申請欲成為 NESAS 認可的檢測實驗室時，首先需要聯繫 ILAC 的成員來進行 ISO 17025 的認證。ILAC (International Laboratory Accreditation Cooperation)全名為國際實驗室認證聯盟，ILAC 會員擁有認證檢測實驗室的能力，認證時遵循 ISO 17011(A Standard for Accreditation Bodies，認證機構之標準)標準，組成成員包含了檢測的認證機構與通過 ISO 17011 的實驗室。除了 ISO 17025 內規定的標準要求之外，NESAS 也會定義額外的檢測內容，目前已增加的項目是：必須保留網路設備相關的商業使用年限之紀錄或報告。通過驗證的安全檢測實驗室將通知 NESAS 認證委員會並提供 ISO 17025 證書之副本，NESAS 認證委員會便認可此實驗室且檢測報告可能會公開在網路上，最後頒發證書，正式予以承認。而實驗室進行 NESAS 的網路設備評估必須等到 GSMA 確認其 NESAS 證書後才能正式開啟流程。下圖為檢測實驗室的認證流程，在 GSMA 定義的 NESAS 認證流程中，其安全檢測實驗室可為第三方組織或是附屬於供應商本身，此外 NESAS 充分認可 ILAC 成員的安全檢測能力，因此所有的 ILAC 成員也被視為已通過 ISO 17025 和 NESAS 要求，預設為已取得 NESAS 認證的實驗室。

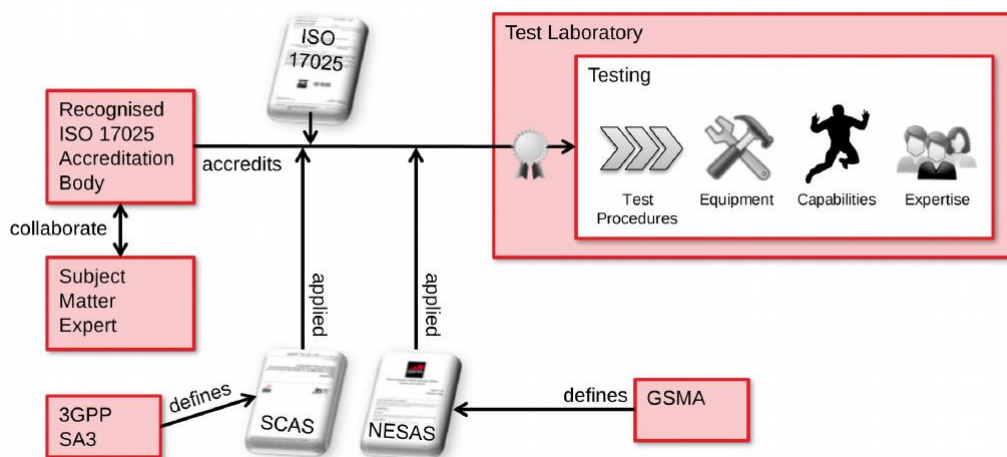


圖 3- 42 NESAS 檢測實驗室之認證流程

資料來源：GSMA

3. 供應商開發與產品生命週期的要求及認證過程

網路設備的生命週期由多個階段所組成，可簡單的區分成產品設計、開發、營運實行，直到產品使用壽命為止，供應商負責設計、開發，而電信業者負責設備的營運，並倚賴供應商提供的設備安全層級。因為網路設備的開發與產品生命週期的認證評估涵蓋了供應商的工作流程，而此流程不一定只用於單一網路設備的開發，這也意味著一份評估的結果可同時適用於多個產品。此外流程的憑證亦具有繼承性，當供應商合併或是被收購時，買家將持有原供應商擁有的開發和產品生命週期之認證。

供應商必須滿足不同國家的法規和電信業者的要求，為不同的市場客製化網路設備，導致產品設計與開發區複雜化，額外增加產品的成本，因此各方利益關係者必須合作以有效地解決新的需求，確保完善的網路安全，所以 NESAS 提供了一個解決方案，以滿足業界和其他利益關係者的需求。行動電信業者目前最需要的是：

- 網路設備的安全性
- 考量生命週期中各階段的安全
- 安全層級的客觀量化與測量
- 安全承諾的展示與可檢視性

(1) 產品生命週期

NESAS 定義的產品生命週期包含設計、開發、產品營運，各階段生命周期的階段

工作及定義整理如下表。

表 3- 21 NESAS 定義之生命週期

生命週期	階段	名稱	定義
設計、開發	1	計畫	若為新產品，規劃初版的需求；反之則是針對新功能和漏洞進行版本更新之規劃。
	2	設計	詳細規劃實行的需求。
	3	實行	照計畫需求實行。
	4	測試與驗證	驗證實行階段的履行程度，若失敗，通常為退回上一步驟，此階段也包含了安全性的驗證。
	5	釋出	做出釋出經過驗證的版本之決定。
	6	製造	將開發版本轉換成實際產品。
	7	配送	將產品投入市場。
產品營運	1	第一次商業介紹	產品開始其商業生命週期，以便在商業網路中使用。過去版本可能已於測試環境中進行過測試。
	2	更新	網路設備持續進行次要、主要的版本更新。
	2.1	次要版本	修復早期發現的漏洞或程式錯誤。
	2.2	主要版本	除了進行上欄的工作外，可能還會有主要功能的增強和結構的變化
	3	產品壽命結束	產品停止更新，也代表著生命週期的終結。

資料來源：GSMA

(2) 產品之安全資產

供應商開發產品的安全性，能讓電信業者的利益受到保護，正常情況下，電信業

者會希望其經營的網路能夠穩定且安全的運作。而 NESAS 定義了開發生命週期安全相關的資產，若這些資產受到侵害，將會對電信業者產生負面的衝擊。NESAS 目前定義的安全資產包含以下幾項：

- 原始碼(包含了軟體與寫在設備內的腳本語言)。
- 軟體包(通常由原始碼在開發或維護階段中產生，並且容易受到測試或驗證階段的決策影響，並可能用於製造階段)。
- 完成品。
- 安全性文件(用於指導產品設計和原始碼開發並於此階段提供出來)
- 產品經營。
- 產品開發支援系統(支援系統用於管理生命週期中的活動、產生出的原始碼和文件)。

(3) 產品生命週期之安全要求

除了保護安全資產之外，為了使電信業者能夠對供應商提供的網路設備有足夠的信賴，開發的生命週期必須滿足所有已定義的安全目標並且需要更高層級的保證，但在 NESAS 文件安全目標內容尚未定義完成，但已說明相關之安全要求，故本團隊先將此文件已納入的安全要求統整及介紹。具該文件指出，安全要求的篩選是根據其有效性來判斷，以實現安全目標並提供投資報酬。每項要求滿足了一至多項的安全目標，也有可能必須同時達成多項要求才能滿足一項安全目標。已納入 NESAS 安全要求之項目及內容整理如下表。

表 3- 22 產品生命週期之安全要求

要求名稱	要求內容
安全設計	產品應當在設計的同時一併考慮其安全性，因此在設計階段，應該對產品進行威脅分析，已辨別潛在威脅及對應的緩解手段。
版本控制系統	在整個商業相關的生命週期中，供應商應使用版本控制，確保原始碼的個人不可否認性。
變更追蹤	供應商應將程序定期建檔，確保產品在生命週期中出現的所有要求和設計變更(包含原始碼、開放資源、第三方軟體、文件、要求文件和設計文件)被妥善地管理與即時追蹤。
原始碼審查	供應商應在原始碼啟用前進行適當審查，除了人力直接地審查，

要求名稱	要求內容
	也應使用程式分析工具，以降低潛在風險及漏洞。
軟體安全性 檢測	在此檢測中應辨別出並且解決潛在漏洞的問題，安全測試包含手動及自動化的檢測，必須測試產品對未定義輸入的反應，以及產品是否存在不必要的行為。
職員教育	應提供網路產品設計、開發、實行和維護等相關人員的長期訓練，以確保對安全方面的知識和敏感度始終保持在高水平。
漏洞補救流程	供應商應建立一個流程來處理在營運中網路設備中發現或與其相關的漏洞，並在合約指定的時間內處理好漏洞並將修補程式/軟體更新分發給所有電信業者。
漏洞補救之 獨立性	供應商應有能力提供修補程式/軟體升級以便於部署，進而將漏洞排除，與修改網路設備功能無關的修補程式/軟體隔離。
資訊安全管理系統	供應商應採用資訊安全管理系統以避免碰到敏感資訊。
自動化建構 工具	供應商應利用自動化構建工具來編譯原始碼並儲存建構紀錄。
建構環境控制	編譯建構環境的所有資料應來自版本控制系統。
漏洞資訊管理	供應商本身應要有可靠的程序以確保其能警覺到於第三方元件最新發現的潛在漏洞，並評估此漏洞是否也會出現在自己的網路設備。
軟體完整性的防護	供應商應建立一套方法以確保產品的交付在受控的條件下進行，並提供適當的手段以確定收到的軟體包之完整性。
單一軟體版本 辨別	所有釋出的軟體包應具有唯一的版本編號。
安全修復通	流程應確保可和具有維護協定的業者在修復版本釋出時進行安全

要求名稱	要求內容
訊	修復資訊相關的通訊。
文件精確性	客戶文件應在安全相關方面保持著最新的版本，並反映產品、其軟體升級及將此文件發送給客戶時的當前功能
安全聯繫點	供應商應為安全問題提供聯繫點並將此聯繫點告知電信業者。當客戶提出安全問題時，應當能在供應商組織內部找到適合的解答人員或是部門。

資料來源：GSMA

(4) 產品生命週期認證步驟

前面幾個段落介紹了產品開發生命週期的定義，及其相關安全資產與安全需求，以下將介紹產品生命週期認證的步驟。

A. 認證申請建立

- 認證請求：當供應商欲認證其開發與產品之生命週期時，將通知 GSMA 進行審計，受審計方須確保此認證符合客戶、合約的要求。
- 確定審計日期：紀錄需求細節後，將訊息寄至審計小組，小組再聯絡受審計方約定審計日期。
- 合約：供應商將尋求與 GSMA 達成共同協定。審計前須先向 GSMA 支付審計費用，GSMA 再進行審計。
- 保密性：與審計小組之間的溝通資訊或是期間收集的其他相關資料歸受審計方所有。做為與 GSMA 合約的一部分，審計團隊將簽署保密合約，並可能和受審計方簽有另外的協定。
- 語言：審計過程中使用英語。
- 報告：內容包含了唯一的審計編號、審計的 NESAS 版本、審計摘要與整體評估(包含是否通過的建議)、須採取之操作、審計委員評論、滿足哪些安全要求等。
- 認可證書：內容包含供應商名稱、審計通過之聲明、唯一的審計編號、審計的 NESAS 版本、有關最終審計報告的 SHA-512 雜湊之 16 進位表示等。

- 有效性：當發生以下情形時，供應商需要更新其證書(重新認證)：NESAS 範圍內的開發和產品之生命週期產生變化，或是 NESAS 釋出新版本，且供應商有意願遵守新版本。NESAS 並不會要求強制重新認證，因此客戶必須進行監督。
- 時間表：盡可能地縮短審計流程花費的時間(流程最長期限為三個月)。

B. 審計準備

- 在確定審計日期之後，審計小組和被審計方將繼續聯繫，協商行程的安排並做好審核的預先準備。雙方的電子郵件往來建議使用帶有個人憑證的 S/MIME 標準。
- 雙方應明確陳述審計範圍，防止彼此間的認知有落差，包含：使用的 NESAS 版本、參與審計的團隊、要審計的流程、審計位置等。
- 臨時議程最慢於審核前一周談妥。審計過程中可能需要臨時修改流程，此時由審計小組和受審計方互相協調。

C. 審計程序

- 審計小組的介紹與相關文件：計開始前受審計方須向審計小組提供關於欲認證流程的書面文件及為何符合 NESAS 提出的安全要求。審計可選擇開線上或是線下會議。會議開始時，受審計方將提供所提交資訊的概要，審計小組也可利用此機會提出何處需要進一步澄清，受審計方應在約定的時間範圍內提交補足的文件。
- 審計小組之文件審核-第一輪：審計小組評估受審計方提交文件中描述的流程是否有滿足安全要求，並提出內容缺失或是未達到部分要求。
- 審計結果之中間會議：此次會議上，審計小組將告知受審計方哪些地方需要補充或未達到安全要求，中間審計報告將依主要、次要問題進行分類。雙方將協調補交期限，受審計方須將內容改進後交給審計小組，其時限為 28 日至 56 日。
- 審計小組之文件審核-第二輪：確認補交之文件是否有將問題修正，並提出仍未排除之問題。
- 現場審計(本項敘述的現場審計為通用認證、並不局限於網路設備)：在文件

確認沒問題後，審計小組將繼續在受審計之現場進行審核。現場審計期間，審計小組將評估：

- 此流程是否活躍地應用於日常業務中
- 受審計方是否具有 NESAS 文件定義的人員，技能，設備，運行實務和資源
- 員工是否有對此流程接受充足的培訓並且了解此流程

受審計方向須向審計小組提供證據，證明受審計方的工程部門和生產部門可有效地實行先前於文件中描述的流程；也須提供哪些員工屬於本次認證範圍，並確保審計小組能夠選定個人進行面試。審計小組可以斟酌決定如何進行現場審計，現場審計應持續一個工作日並不得超過兩個工作日。建議審計小組需親眼見證平時產品的開發及維護，並根據需求訪問相關技術人員。審計小組應將其活動限制在樣本上，並不需要進行全面性的審計。

- 提供結果：審計結束時，審計小組將審計結果告知受審計方的同時也建立出詳細的審計報告。審計報告之草案反映了審計意見和結果。在雙方互相同意此結果後，審計小組將向受審計方和指定的 GSM 協會工作人員最終審計報告。報告建議使用 PDF 檔案格式。

D. 認證授予

當指定的 GSMA 工作人員收到建議合格的最終審計報告後，將直接(不做任何評論)將報告轉交到 NESAS 認證委員會，最後由 NESAS 認證委員會依此報告決定是否授予認證。若同意即頒發證書並發送至受審計方，若受審計方也認可，則在 GSMA 網站上公開此副本。

4. NESAS 之爭議處理程序

網路設備安全保證方法(NESAS)爭議解決委員會(NESAS Dispute Resolution Committee，簡稱 NESAS DRC)為負責處理兩名或更多的 NESAS 參與者(電信業者、設備供應商、檢測實驗室、審計人員等)之間就 NESAS 程序、文件有重大的詮釋爭議時的仲裁機構，並依雙方提出之事項做出客觀的裁決。NESAS DRC 和 NESAS 之間

的關係如同我國司法院之於憲法，只負責單就文件內容的解釋。以下說明對所有 NESAS 參與者具有約束力的 NESAS 爭議解決流程。

NESAS DRC 是由 NESAS 認證機構成員所組成的常設委員會。身為 NESAS 程序和文件公正的解釋者，其解釋內容將成為雙方或多方之間分歧的主題，在牽扯到 NESAS DRC 之前，各爭議方應盡可能地利用所有的可用資源解決爭議，

只有在彼此仍然無法互相達成共識且無其他解決方案的條件下才能聯繫 NESAS DRC，啟動程序。各相關方應於會前確定爭議的議題，以便對其有共同的理解。各爭議方引用的措詞應達成一致，包含引起爭議的時間點。若有參與者發現 NESAS 文件的錯誤或說明不清楚的地方，該參與者必須以書面形式指出錯誤或含糊之處，並將其提交到 NESAS 認證機構進行決議。

NESAS DRC 必須依照本節描述的爭議處理程序進行並視會議需求提出額外的指導方針或是進一步地議程，並且盡快的解決爭端，通常於十日內通知召開。裁決的結果由所有 NESAS DRC 的成員做出決定並且採用多數決，此裁決對爭議各方皆有約束力，且極有可能做為將來的判例參考。如果其中一方或多方拒絕接受 NESAS DRC 之裁決，或是財務相關的問題，則必須透過適當的合法合約來解決爭議，此外，NESAS DRC 將不負責因裁決而導致的一切財物損失。

（二）物聯網安全指引

隨著物聯網得各種應用如雨後春筍般的出現，許多開發平台的業者也積極地加入、開發這一大片藍海。當然地，攻擊者也不會錯過這塊新興領域，近年來針對物聯網的攻擊與威脅種類不斷地增加，物聯網的安全性也備受考驗。因此，GSMA 於 2016 和多家行動業者合作，提出一套物聯網安全的指引，以物聯網安全評估技術為基礎，提供端到端的可靠驗證方法。文件內容包含了促進物聯網中各部分的安全、提供常見安全威脅緩解的建議、與包含開發設計、部署安全物聯網服務的最佳作法。GSMA 提出之物聯網安全指引共包含以下四份文件：

- CLP.11 物聯網安全指南概述文件²⁰⁶(IoT Security Guidelines Overview Documents)：介紹物聯網整體架構其安全相關議題，並帶出以下三份文件之架構主題。

²⁰⁶ GSMA, “IoT Security Guidelines Overview Document”, 2016/2.

- CLP.12 服務生態系統的物聯網安全指南²⁰⁷(IoT Security Guidelines for Services Ecosystems)：敘述服務生態系統的相關標準、使用設備、安全相關問題以及風險。
- CLP.13 端點生態系統的物聯網安全指南²⁰⁸(IoT Security Guidelines for Endpoint Ecosystems)：敘述端點生態系統的相關標準、使用設備、安全相關問題以及風險。
- CLP.14 電信業者的物聯網安全指南²⁰⁹(IoT Security Guidelines for Network Operators)：敘述物聯網營運商的相關標準、設備、安全相關問題以及風險。

1. 物聯網安全指引概述

由於物聯網的發展，使得在物聯網架構下包含用戶、服務生態系統、通訊網路、端點生態系統皆產生了許多對應的新型供應商，隨著各產業在物聯網上的應用，物聯網架構更趨向複雜端點，也就是端點模型可在長距離的通訊連結下運作，如蜂巢式、衛星或乙太網等的線路連接。

未來，GSM 協會期望在 4G 網路下能將低功耗廣域(Low Power Wide Area，簡稱 LPWA)無線技術匯集至蜂巢式通訊空間以滿足當今物聯網(即 NB-IoT)的需求，同時也要求各個電信業者將 LPWA 技術融合至其產品中。

身分管理的部分長久以來面臨了相當大的考驗，因此 GSM 協會提出了一項基於 SIM 卡的解決方案——嵌入式 SIM 遠程配置架構：目的為抵禦故障、旁道攻擊、被動數據攔截、實體干擾、身分盜用等攻擊，將信任密鑰帶入了物聯網格局，並結合電信業者安全規範，如 3GPP 通用引導架構(Generic Bootstrapping Architecture、簡稱 GBA)、OMA(開放移動聯盟)、oneM2M 等，使該領域的配備能有效更新，並且能夠管理其性能及認證，以達到雙重作用。

因應現代物聯網的應用，在安全性的設計上必須面臨的挑戰包含了可用性、認證、隱私與安全：

(1) 可用性

²⁰⁷ GSMA, “IoT Security Guidelines for Service Ecosystems”, 2016/2.

²⁰⁸ GSMA, “IoT Security Guidelines for Endpoint Ecosystems”, 2016/2.

²⁰⁹ GSMA, “IoT Security Guidelines for Network Operators”, 2016/2.

可用性為端點設備與端點使用者之間能持續與後端服務溝通，使得物聯網能如預期速度發展。而為了達到與現實符合之情況，需考慮以下幾點：

- 如何將 LPWAN(低功耗廣域網路)應用於現代蜂巢式系統的安全等級？
- 如何讓不同的行動業者與現代新型物聯網端點能在網路邊界移動後有相同的安全等級？
- 如何讓網路在閘道能保有信任直到最後毛細端點(capillary Endpoints)？
- 如何限制在安全通訊環境下輕量端點的功耗？

(2) 認證

此部分在物聯網技術中為重要且基礎的，在物聯網架構下的不同裝置，若要能順利互相溝通，則必須能安全的表明自身身分。認證部分需考慮以下幾點：

- 執行端點的用戶是否能與其身分做準確的連結性？
- 如何確認端點身分？
- 端點安全技術能否安全驗證其他端點及服務？
- 是否會有冒充授權服務的異常服務及端點？
- 如何確保各個設備之身分能被正確使用而不被他人操作或干涉？

(3) 隱私

除了各個設備的身分認證外，必須確保在物聯網服務下的活動及資料能不被洩漏、保有隱私，並且針對含有個人隱私資料如醫療資訊等等，能達到高度的隱私保護，降低洩漏的傷害。因此在設計上必須考量到以下幾點：

- 各端點身分是否洩漏至授權設備或使用者？
- 在物聯網服務中，是否能允許端點服務受到實際監測或追蹤？
- 在物聯網服務中，每個端點或服務所發出的資料是否正確表達其目前狀態？
- 對於機密資料是否有足夠的保護，並保持其完整性？
- 產品或服務如何儲存或保留特定用戶的個別識別資訊(Personally identifiable information，簡稱 PII)？
- 端點用戶在物聯網服務中是否能控制上述之 PII 訊息？

(4) 安全

現實世界中包含大量用戶及設備，在目前物聯網技術中最大的兩個部分：嵌入式系統及雲端服務中，即便在安全部分與過去有顯著的差異，實踐上仍有許多問題必須考量：

- 在產品設計時是否有考量安全問題？
- 產品生命週期是否包含安全生命週期？
- 在嵌入式系統中運作的服務與應用程式是否已包含應用安全程序？
- 端點及服務生態系統中是否執行可信賴計算機(Trusted computing base，簡稱 TCB)？
- TCB 在應用程式圖片及服務上如何進行自我驗證？
- 端點或物聯網服務能否偵測出配置設備及應用程式中之異常？
- 如何監控上述之異常？
- 如何讓身分認證與服務安全流程有相關性？
- 如何制定事件安全相關計畫以因應檢測遇到損害異常情形時的對策？
- 遭受損害異常後該如何修復？

2. 服務生態系統的物聯網安全指引

服務生態系統為整個物聯網系統不同核心內的功能及通訊連結樞紐，為物聯網產品及服務提供一個系統使得端點、合作夥伴與使用者具有價值、意義和實際功能，可替其他生態系統進行分級認證、連結用戶，達到可用性、管理與執行平常物聯網所需之相關關鍵任務。

(1) 系統之服務模型

根據不同產品和服務所提供的應用程式，由許多不同類型的服務和存取點組成的基礎設施可能非常龐大，也可能較為簡化。為了達成系統運作等功能，服務生態系統由許多層級組成，如資料庫叢集、應用程式伺服器、應用程式代理伺服器等基礎設備均屬於此層級。而現代物聯網的服務生態系統範例(如圖 3-43)包含：

- 基於雲基礎設施的解決方案
- 基於容器的應用程式部署
- 傳統資料中心伺服器環境
- 資料庫叢集
- Web 應用程式框架服務叢集

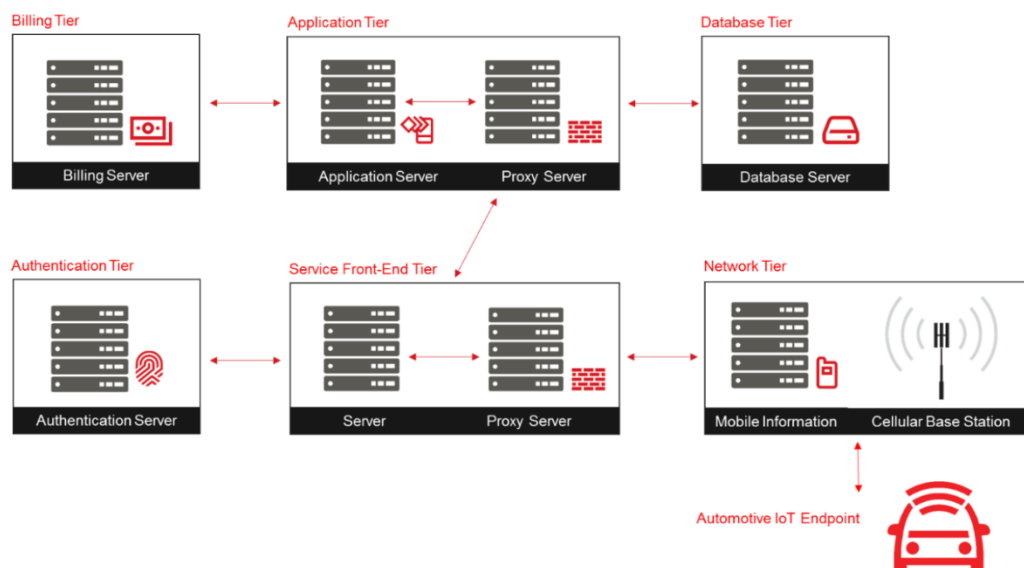


圖 3- 43 服務生態系統圖例

資料來源：GSMA

一般而言，即便環境的差異導致設計上大相逕庭，但訊息與應用程式之間的連接方式，均基於同一標準，而服務生態系統與現今的計算機系統皆必須具備以下條件：

- 服務存取點：一個用以進入各個應用程式之基礎設施的點。
- 內部子系統：為此應用程式建立的內容和環境必須能安全且可靠的處理網路中的資料。
- 資料存於某處後，將會再返回服務層，並回應授權指令，服務層將回應此指令、或者是將其發送至同一生態系統、其他生態系統及網路中的相關元件。
- 每層通常皆包含一個代理或防火牆系統用以管理伺服器。
- 計費層含有計費服務。
- 應用程式伺服器存在於特定的應用層級。
- 資料庫層負責管理資料庫服務。

(2) 系統之安全模型

通用的基礎設施和策略設計服務端點環境的安全性，在不同拓模或創新應用程式架構中皆可使用。服務生態系統中的各個元件皆必須單獨保護。如以通用元件共同建立簡易服務，可對應查詢，並在端點合作夥伴與使用者之間發送回應，此模型包含以下層級(如圖 3-44)，但不僅限於這些層級：

- Web 服務層
- 應用程式伺服器層

- 資料庫層
- 驗證層
- 網路層
- 第三方應用程式層，例如計費層

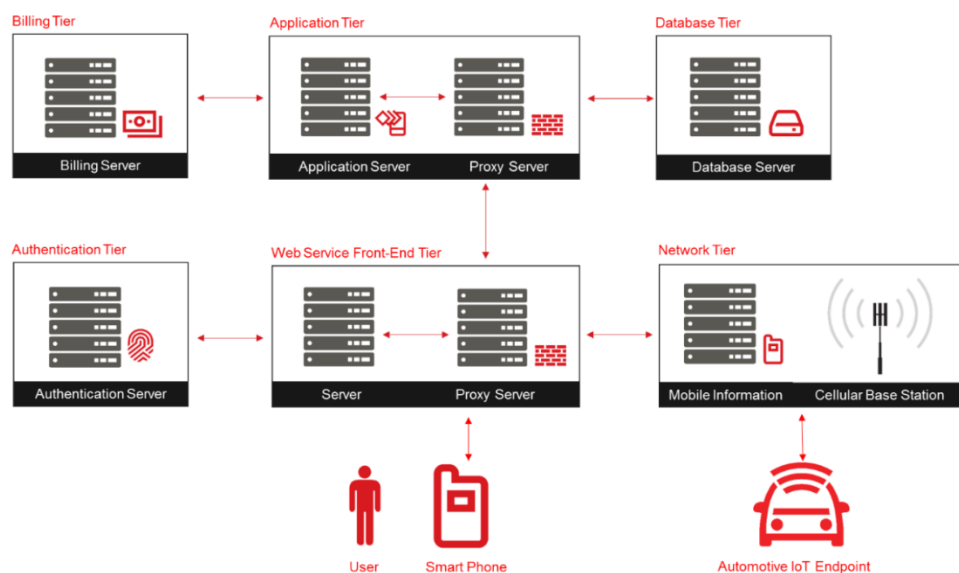


圖 3- 44 各層級的服務生態系統範例

資料來源：GSMA

儘管每個層級只有一台伺服器，若將每個邏輯概念分級至各層，能使執行更有效率。若 API 有充足的多樣化功能，便可在整個層級週期中進行擴展或調整，而在選擇 API 時可考慮以下規範：

- ETSI M2M TS 102 690(European Telecommunications Standards Institute，歐洲電信標準協會)
- ETSI M2M TS 102 921
- 3GPP TS 33.220

不論實際上控制的是硬體或軟體防火牆、安全性群組(Security Group)、存取控制清單或其他技術，都會有一個元件代表該層，負責管理進出。而對於可訪問之元件，如服務前端層，模組需要的是一個額外的安全元件，用途如下：

- DDoS 防護
- 負載平衡

- 冗餘(Redundancy)
- 選擇性 Web 應用程式防火牆功能

而在各個層級的安全運作定義伺服器的管理平台，則應考慮以下幾點：

- 登錄集中式日誌服務
- 管理驗證和授權
- 通訊安全實施
- 資料備份、恢復和複製
- 應用程式職責的分離
- 系統監控和完整性

3. 端點生態系統的物聯網安全指南

從物聯網的角度來看，端點為一種用來作為網路連結產品或是執行部分服務功能的物理計算設備。端點設備的安全挑戰在絕大多數的情形下皆和服務所使用的設備特徵有直接關聯，而主要特徵包含了以下幾項：低功耗、低成本、使用週期長(>10 年)以及可實際接觸。

(1) 端點設備之模型

隨著時間的發展，端點設備的模型(如圖 3-45)主要可分為以下三類：輕量端點、複雜端點與閘道（集線器）。

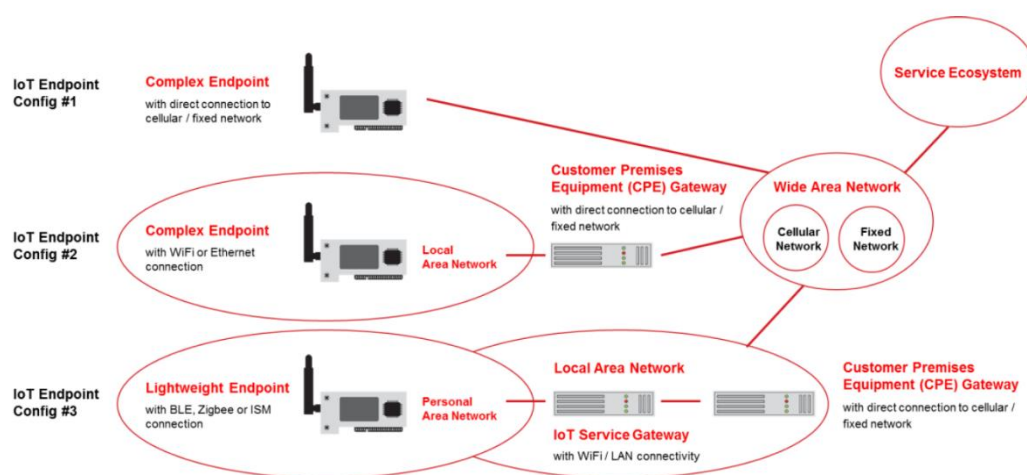


圖 3- 45 常見的物聯網端點配置

資料來源：GSMA

● 輕量端點

通常為感測器或是簡易物理設備，用於單一物理用途，為消費者或服務生態系統提供指標，常透過物聯網服務閘道和使用者設備閘道連接至服務生態系統。其多採用成本較低的處理單元(如八位元單晶片)，主要使用個人區域網路或毛細協定(capillary protocol)進行連接(如藍芽、Thread、Zigbee)，其儲存、計算能力與安全能力皆較複雜端點與閘道低。此端點功率往往較低，使用小型鋰聚合物電池或太陽能電源即可運作。因輕量端點成本較低，因此能使用的安全技術較少，安全技術需要考量大量電流消耗、成本與電路板空間，因此難以使用於這類系統，但仍可以使用小型信任錨點(trust anchor)來穩定安全框架。其設備包括可穿戴設備、家庭安全感測器端點、鄰近信標(Proximity beacons)、非蜂巢式毛細設備。

● 複雜端點

通常藉由蜂巢式等長距離通訊連結的方式、並且透過 Wi-Fi 或以太網經由用戶端點設備閘道持續連接至後端伺服器。其可能內建基本處理器，甚至是八位元單晶片，能運行更穩定的處理單元。而此類端點會連接交流電源與電池，可經常使用電池充電系統。有些複雜端點可通過毛細協定來通訊，並需要更多功率使本地應用程式的運行更加有效，如串流音訊設備。複雜端點可以支援更高的電流消耗，通常會採用更為強大的處理器，並且電路板上也有更多空間可供安全技術使用，也因此可以實現更多功能，可輕易的實施個人化預先共享密鑰或非對稱可信賴計算機模型。其設備包括連接物聯網的照明系統、冰箱或洗衣機等家用電器、工業控制系統(例如 SCADA(supervisory control and data acquisition, 簡稱 SCADA))、改造 OBD-II(On-Board Diagnostics, 第二代車上診斷系統)蜂巢式「互聯汽車」追蹤和監測設備等。

● 閘道（集線器）

通常連接專用電源，管理輕量端點與其所驅動的後端系統之間的通訊，主要用於管理長距離通訊連結，如蜂巢式、衛星、固定線路、光纖或以太網，接收服務生態系統中後端系統的命令，再將命令轉換為輕量端點可解析的消息。閘道與複雜端點一樣具有強大處理能力，支援更高的電流消耗，電路板上通常也有更多空間，使物聯網閘道可相對容易地實現複雜的可信賴計算機解決方案與 GBA 認證客戶端等技術，在本地生態系統中達到聚合的作用，使設備之間可互相通訊，

實現網路與服務生態系統間的通訊。雖然其主要功能為輕量端點傳輸訊息，但也能執行關鍵任務，例如：發現設備、部署網路驅動、功能管理、運行監控、GBA 或 TLS(Transport Layer Security，傳輸層安全協定)設置等身分驗證和安全功能。技術上而言，不一定由端點管理，可能由物聯網服務供應商或電信業者管理，且可被設計為複雜端點以便有效利用其連結分配至局部網路輕量端點的功能。

典型的開道類型有兩種：物聯網服務開道和 CPE 開道。物聯網服務開道通常由物聯網服務供應商提供，亦有可能為端點用戶擁有。通常用於將輕量端點連接至服務生態系統的集線器(通過固定/蜂巢式直接連接或通過用戶端設備(Customer Premises Equipmen，簡稱 CPE))，端點用戶從物聯網服務供應商購買管理服務。CPE 開道則由電信業者提供，常為通過蜂巢式或固定網路(fixed networks)連接至寬頻路由器，可用於住宅或企業環境。開道通常由電信業者管理和配置。

● 整體模型：

不論是哪種端點，都具備共同的子模型如下：

- CPU 必須執行應用程式碼
- CPU 必須能載入/儲存且傳送至/接收自永久儲存器的可執行程式碼
- CPU 必須在臨時儲存器內進行運算
- 必需使用可信賴計算機驗證環境
- 設備必須與其物聯網生態系統通訊

每個端點模型皆有一項主要任務：定義可靠、高品質、安全的平台來執行特定應用程序，工程團隊必須確保硬體提供應用程式一個可信任的平台，使高品質應用程式可與其對等的硬體做安全溝通，類似於智慧型手機、雲端伺服器、大型機器等更複雜的計算平台。物聯網端點會加入其他端點的網路，用以在執行操作時受到監督服務的影響或參與，可提高特定設備的可信度，減少由於安全性或可靠性漏洞導致的潛在不利因素。

(2) 端點設備之安全模型

端點生態系統的安全性即為設備元件的安全性，藉由前面所定義的整體模型，工程師便可較方便得評估端點設備，只需最少的專業知識、設備及成本便能模擬、建構出攻擊模型，快速地找出此端點存在的安全缺陷。必須考慮的威脅面向包括以下幾點：網路通訊、可訪問網路服務、控制台存取、本地端匯流排通訊與晶片存取。

4. 電信業者的物聯網安全指引

電信業者與物聯網服務供應商在物聯網架構安全需求上是類似的，須確保物聯網服務的資產並做到一定程度的保護，而個別實施的安全功能則取決於各個服務。因此物聯網服務商必須分別評估其風險及隱私影響評估的流程，以達到特殊的安全需求。在許多情況下，電信業者同時為物聯網服務供應商。通訊網路最基本的安全機制如下：

- 物聯網服務相關實體(如閘道、端點設備、家用網路、漫遊網路、服務平台)的識別和驗證。
- 建立物聯網服務需要連接的不同實體的存取控制。
- 保證網路所承載的物聯網服務資訊的安全性(保密性、完整性、可用性、真實性)與隱私所需的資料保護。
- 確保網路資源可用並防止其受到攻擊的流程與機制(例如部署合適的防火牆、入侵防禦和資料過濾技術)。

(1) 用戶、應用程序、端點設備、網路及服務平台之安全識別

在蜂巢式物聯網服務中，可用國際移動設備識別碼 (International Mobile Equipment Identity，簡稱 IMEI)與國際移動用戶識別碼(International Mobile Subscriber Identity，簡稱 IMSI)來辨別端點，EID(eUICC Identity)可用於識別帶有 eUICC 的設備。eUICC(Embedded Universal Integrated Circuit Card)為嵌入式通用積體電路卡，而 UICC 為 ETSI TS 102 221 規定的安全元件平台，可支援以密碼區分的安全域中多個標準網路或服務驗證應用程式。在物聯網中，必須保護發放和使用的身分(如 IMSI、IMEI 或 ICCID(積體電路卡識別碼))，須防止未經授權的修改、冒充或竊盜。

在識別端點設備上，電信業者建議可基於 UICC 的機制來安全地識別，而 UICC 提供的安全儲存功能可從電信業者擴展至物聯網服務供應商，UICC 上便能儲存其他物聯網服務的相關身分，且這項技術適用於蜂巢式和非蜂巢式端點設備。而電信業者在考慮跨越多個平台使用安全權衡和風險時，可提供「單點服務」，允許在端點設備之間多建立和證明身分一次，如此便可連接至多個物聯網服務平台。

A. 使用者、應用程式、端點設備、網路和服務平台的安全驗證

由 NIST(National Institute of Standards and Technology，美國國家標準研究局)的定義可知，「驗證」指的是驗證用戶、過程或端點設備的身份，在系統中允許訪問訊息的資源是必須的。而驗證中重要的屬性為不可否認性，在 NIST 中，不可否認性的定義為：保證訊息發送者提供送達證明，並且向接收者提供發送者的身分證明，這樣雙方將來都無法否認曾處理過此訊息。因此不可否認性將取決於交易與消息來源是否認定違反真實性。電信業者可藉由此驗證確保與物聯網服務相關的用戶、應用程式、端點設備、網路和服務平台。

B. 提供安全的頻道

安全頻道的目的為在於確保在未經資料主體知情和同意的情況下，不處理、使用或傳輸透過通道發送的資料。在廣域蜂巢式和固定網路中，電信業者必須提供「業界最高等級」的通訊完整性、保密性和真實性。加密技術可以確保保密性、真實性與機密性，達到安全數據傳輸的作用，而加密技術在設計上也必須考量到輕量端點設備、網路方面(如衛星回程限制(backhaul constraints))以及提供的服務，電信業者同時也可提供此加密服務以確保資訊完整性和網路恢復能力。在適當情況下，電信業者可利用虛擬私人網路和加密的互聯網連接提供並管理與企業網路之間的安全連結。

電信業者亦可為客戶提供私人網路，而私人網路可以以下方式建立：

- 使用例如第二層穿隧協定(Layer Two Tunneling Protocol)等穿隧協定並透過網際網路安全協定(IPsec)等協定進行保護。
- 配置一個帶有共用電台網的單獨核心網路實例，為物聯網服務建立一個私人網路，如下圖所示。

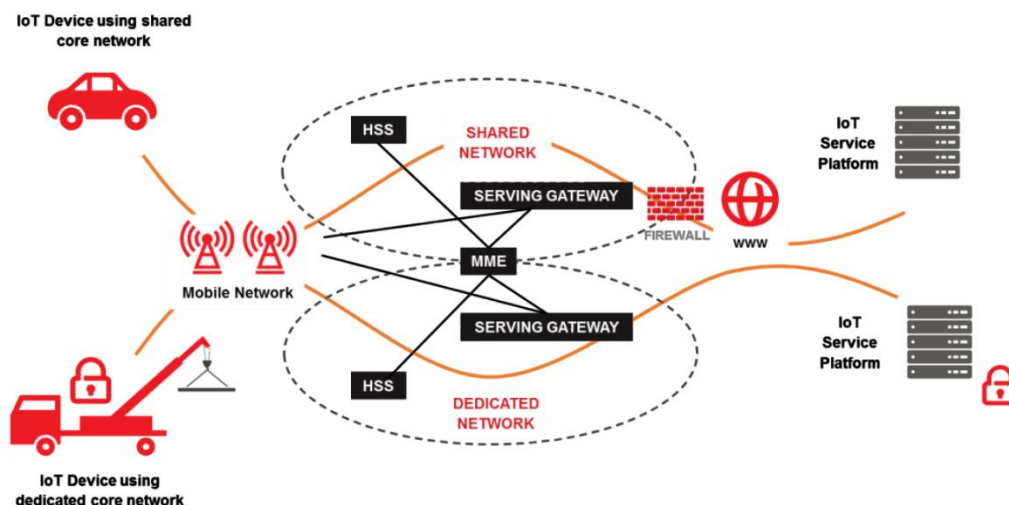


圖 3- 46 私人網路配置範例

資料來源：GSMA

C. 確保頻道的可用性

電信業者也必須確保頻道的可用性，而根據 NIST 定義，「可用性」為可以根據授權實體的要求需可進行訪問和使用。電信業者提供的網路可用性的基本機制如下：

- 使用授權頻譜：GSM 協會電信業者的成員會根據其所在國家監控管理機構所頒布的許可條款使用私人授權頻譜營運網路，此方法能確保網路可用性不受影響。使用授權頻譜可為電信業者提供用於經營網路的專用頻段，以確保網路涵蓋和產能規劃。
- 實施標準化與成熟的網路技術：GSM 協會的電信業者成員實施 3GPP 等標準機構規定的 GSM、UMTS 和 LTE 等標準網路技術。標準化技術除了可確保電信業者之間的互用性，也能在制定標準的期間經過最大限度的審查，確保技術的強韌性。
- 實施經過測試和認證的網路技術：電信業者會根據國際測試標準進行測試和認證。複雜端點、射頻存取網路(RAN)和 UICC 皆遵循 3GPP 測試規範且須通過電信業者驗收測試，而複雜端點還需要額外通過 GCF(Global Certification Forum，全球認證論壇)、PTCRB(PCS(Process Control System，程序控制系統) Type Certification Review Board，北美 PCS 型號認證委員會)測試。
- 彈性網路拓撲和配置：電信業者須根據地理環境建構彈性網路，以達到最大限度的可用性及其最短的延遲。

- 網路資源的即時監控和管理：可全天候管理網路性能以管理流量和排除故障。
- 威脅管理和訊息共享：GSM 協會的反詐騙安全小組(Fraud and Security Group)為電信業者提供開放、可接受、可信任的環境，能即時共享詐騙情報與事件的詳細內容。
- 漫遊服務：可為客戶提高網路涵蓋和可用性。
- 端點設備性能的監控和管理：電信業者可測試與其網路連接的端點設備，以隔離過量無線電的干擾或網路訊息流量異常的端點設備。

(2) 電信業者提供之服務

A. 安全訂閱管理程式

電信業者或物聯網服務供應商應對現今和將來提供物聯網服務(語音、資料、簡訊等)所需的服務進行評估。

- 電信業者應當根據此類評估結果，在操作中遵循「最小權限原則」，只為物聯網服務供應商的訂閱提供特定物聯網服務所需的服務。例如：
- 僅使用資料承載的物聯網服務不應提供語音和簡訊服務。
 - 如果端點設備僅連接至一個已知的物聯網服務平台，則設備相關訂閱只可允許其連接至白名單內的一個 IP 位址或網域。
 - 如果物聯網服務使用語音或簡訊，應考慮使用預設的固定撥號清單。
- 對於關鍵物聯網服務(例如關鍵醫療保健服務)相關的訂閱，電信業者應當實施安全訂閱管理流程，因為此類服務不可隨意斷開。
- 電信業者應區分用於物聯網服務的 UICC 與提供傳統服務的傳統 UICC，並根據物聯網服務供應商的要求對這些 UICC 進行適當地隔離。
 - 如果將用於物聯網服務的 UICC 和用於傳統手機的 UICC 進行隔離，可使電信業者能更安全、高效率地管理。例如，電信業者可能考慮對使用壽命較長且配置較好的端點設備採用單獨的 HLR(Home Location Register，歸屬位置暫存器)、HSS，以便為這些 UICC 提供長期(持續數年)的支援。

UICC 供應和管理：UICC OTA(Over-the-Air，空中)安全機制遵循最新的 ETSI 和 3GPP 規範，採用最新的安全層級。若物聯網的服務威脅模型已表明物聯網端點設備可能會被竄改，則電信業者需為其提供不可拆卸的 UICC。若物聯網服務需要將端點設備設置於遠方或是難以取得的位置，電信業者應提供不可拆卸 UICC(即 eUICC)的安全遠端系統管理。基於 UICC 的服務通常使用 JavaCard™開發，可在所有能相容此平台的 UICC 卡之間互相操作。UICC 亦可用於物聯網服務中敏感數據的防竄改儲存，

包括物聯網服務供應商控制的安全密鑰。ETSI TS 102 225 利用 GlobalPlatform 規範中的機密卡內容管理。

B. 網路驗證和加密算法

許多現有物聯網服務有使用 USSD(Unstructured Supplementary Service Data，非結構化補充資料服務)和簡訊，相對於 IP 封包的保護，其安全支援功能有限，這兩者的流量通常並非預設由電信業者和加密保護機制進行「端對端」的加密保護，以確保訊息沒有保密性和完整性。

- GSM/GPRS(2G)系統安全：在 GSM/GPRS 系統中，端點設備不會驗證網路，只有網路會驗證端點設備，因此使用時建議採用服務層端對端加密。而在系統中 GRX(GPRS Roaming exchange，GPRS 漫遊交換)網路上建立的 SGSN(Serving GPRS Support Node，GPRS 服務節點)和 GGSN(Gateway GPRS Support Node，GPRS 閘道節點)之間的 GTP 通道並未加密，電信業者須將 GRX 作為私人網路進行管理。而電信業者應注意以下事項：
 - 使用至少 128 位元的 A5/3 字串密碼以保護物聯網端點設備和基站之間的連結。電信業者應盡可能避免使用 A5/1 和 A5/2 或未加密連結。
 - 使用 MILENAGE 驗證演算法。電信業者應避免使用 COMP128-1 和 COMP128-2。電信業者應考慮支援 TUAK 驗證演算法。
 - 採用適當措施應對和緩解虛假基站攻擊。
- UMTS(3G)系統安全：提供 UMTS 電信業者應支援 MILENAGE 驗證和密鑰生成演算法。而電信業者應支援 Kasumi 保密性和完整性加密演算法，以及 TUAK 驗證算法。
- LTE(4G)系統安全：提供 LTE 網路的電信業者應當支援 MILENAGE 驗證演算法。電信業者應支援 LTE EEA1、EEA2 或 EEA3 加密演算法，且需支援 TUAK 驗證算法。
- 低功率廣域網路(LPWAN)安全：現有的幾種 LPWAN 技術大多為專有技術，通常不在公共區域使用，例如 LoRa、SigFox 和 Weightless。雖然 LPWAN 最初是作為獨立技術開發，但現在 3GPP 正考慮將多項此種類的技術納入其標準中。

C. 固定網路安全

對於電信業者或物聯網服務供應商控制的 Wi-Fi 網路，其預設配置的建議包括 EAP-SIM 或 EAP-AKA 驗證，並可能依賴於 ETSI TS 102 310 的 UICC EAP 框架。

D. 流量優先級別

電信業者可根據所提供的物聯網服務提供相對應的服務質量級別。

E. 後置迴路安全(Backhaul security)

3GPP 標準指明 GSM、UMTS 和 LTE 沒有強制使用加密 E.後置迴路連結，此外不同電信業者之間的 RAN 及回程共用可能會引入其他安全性漏洞。電信業者應替端點使用者資料和訊號平面資料的流量實施 GSM、UMTS 和 LTE 網路的後置迴路加密。

F. 漫遊

連接歸屬網路和漫遊網路的 SS7/Diameter 互通功能相對較為開放，因此漫遊網路容易出現安全性漏洞。電信業者須考慮如何保護 HLR 和 VLR(Visitor location register，拜訪位置暫存器)、防禦 DoS 攻擊(包括非蓄意的)、未授權來源的請求以及對漫遊定向(steering of roaming)服務的開發利用。漫遊是互聯網業者在主核心移動網路實體間交換的訊號協定所促成，漫遊所使用之協定如下：

- 被訪問漫遊網路的 VLR 或 SGSN 與歸屬網路的 HLR 之間：MAP(The Mobile Application Part，行動應用部分)協定
- LTE 漫遊網路的 MME 與歸屬 LTE 網路的 HSS 之間：Diameter 協定(存在某些變體，如 S6a)。
- 被訪問網路的 SGSN/S-GW 與歸屬網路的 GGSN/P-GW 之間：漫遊資料傳輸使用 GTP。

3GPP TS 23.122 定義了擴展存取限制(Extended Access Barring，簡稱 EAB)服務：除了通用和特定網域的存取控制機制外，電信業者還可限制為了 EAB 所配置端點設備的網路訪問。EAB 配置可以在 UICC 或端點設備中進行。網路安全閘道應配置為「容納(sinkhole)」DoS 攻擊

基於安全考量，電信業者可以執行的另一種方法為物聯網端點設備的漫遊引導(Steering of Roaming，簡稱 SoR)。若沒有使用延後計時器(back-off timer)，拒絕更新位置將導致端點設備進行重試，最後嘗試從另一個漫遊網路註冊。SoR 的另一種方法是經由 OTA，使用 UICC 的優先漫遊清單和儲存在 UICC 的其他參數。UICC 的 OTA 更新功能讓歸屬網路可以更新優先漫遊清單，該清單訂出了漫遊網路內選擇網路的優先

順序。歸屬網路還可以使用新清單刷新端點設備的記憶體，使其立即搜尋新的網路。

目前大多數的漫遊數據是從 SGSN(LTE 為 S-GW)路由至 GGSN(LTE 為 P-GW)，少部分會使用 LBO (Local Breakout，本地突破：數據從被訪問網路直接路由至互聯網)的方法。由於相關法規的影響，未來的情況可能有所改變：如歐盟法規從 2014 年 7 月起啟用 LBO 服務，LTE(特別是 VoLTE)，其漫遊網路中進行的語音通話可由國內的 P-GW 處理(如現在被訪問網路中進行的常規電路交換語音通話)。當歸屬 GGSN/P-GW 的新工作階段(session)提出氾濫(flood)請求時，可能會發生訊號風暴。GPRS 協定在端點設備和 GGSN 之間建立了安全通道，當發出新的工作階段(建立 PDP(Packet Data Protocol，封包資料協定)上下文)請求時便會建立此通道，並為端點設備分配一個 IP 地址。若端點設備沒有以個別化方式運作，可能會產生前述的訊號風暴。只需少量的端點設備便能發生 DoS 攻擊，同時建立多個新工作階段的請求。通道的頻寬有限，因此應盡量避免其受到這種風暴的攻擊。

G. 端點設備管理

電信業者可為物聯網服務供應商提供一些為了傳統行動裝置管理而開發的規則和技術。而對於使用 UICC 註冊並連接至蜂巢式網路的物聯網端點設備管理，可利用現有的連結管理平台、設備管理平台和 UICC 管理平台。下圖為一個典型的端點設備管理架構範例，來自 ETSI M2M 通訊原則。藍框為通常由電信業者現有的設備管理平台管理，紅框表示由物聯網服務平台管理的服務元件。電信業者可因應物聯網服務供應商要求，分擔部分紅框內的設備管理功能。

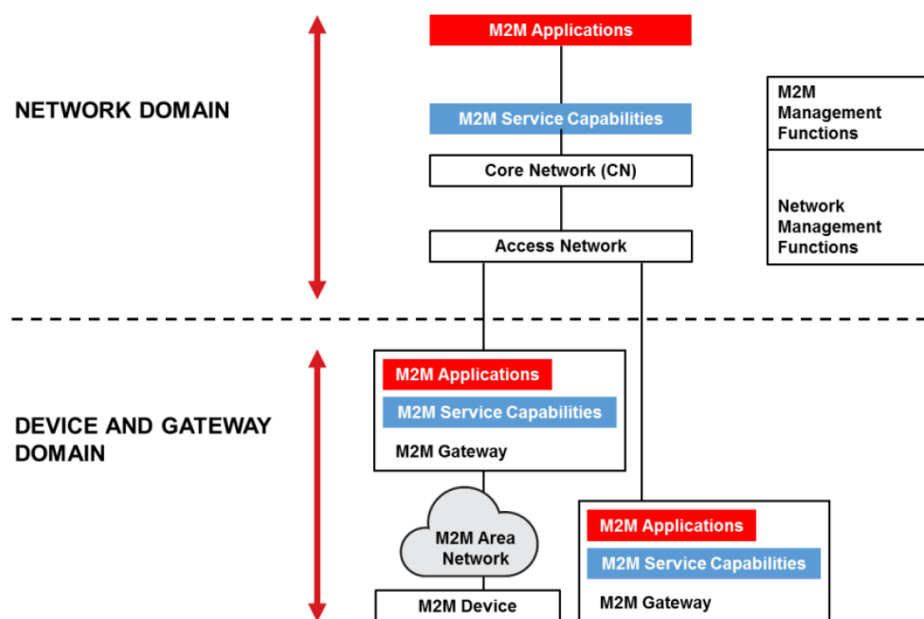


圖 3- 47 用於 M2M 設備管理的 ETSI 高階架構

資料來源：GSMA

H. 開道設備管理

電信業者可代表物聯網服務供應商提供和管理安全開道，使端點設備透過電信業者的廣域網路安全機制整合成最佳的安全連接。可用寬頻論壇 TR-069：用戶端設備廣域網路管理協定，對使用固定網路連結的開道進行遠端管理。而蜂巢式網路連結開道的遠端管理則能使用 OMA 設備管理和韌體更新管理物件(Firmware Update Management Object，簡稱 FUMO)協定。

三、 共同準則(Common Criteria，CC)

CC²¹⁰為目前世界各國評估、驗證資通安全產品時所採用的共同標準。CC 起源於以下三個不同安全標準的統一、整合：美國國防部的 TCSEC(Trusted Computer System Evaluation Criteria)、歐洲的 ITSEC(Information Technology Security Evaluation Criteria)

²¹⁰ CC 官網，[Online]. Available:<https://www.commoncriteriaportal.org/>

和加拿大的 CTCPE(Canadian Trusted Computer Product Evaluation Criteria)。制訂 CC 的目的為了讓政府只需要參照一套標準就能完整評估產品，且確保 IT 產品和保護剖繪(Protection Profile，產品的安全需求聲明文件)的高標準、一致性、與可用性，減少重覆評估的成本負擔，並提高評估、驗證程序的效率及效益。CC 的標準最早的是由加拿大、法國、德國、荷蘭、英國和美國政府共同制訂，並於 1999 年 8 月正式成為 ISO 國際標準(ISO/IEC 15408)，而現今使用 CC 評估的機構不僅限於政府，也已經成為業界對於資通安全產品安全性的共同標準。

CC 文件主要可分為三個部分，第一部分為導論及通用模型(Introduction and General Model)，主要除了提供 CC 的導論之外，也提出一個評估的通用模型，第二部分為安全功能要求(Security Functional Requirements)，主要為將其列出目錄並將進行類別與屬性的分類，第三部分為安全保證要求(Security Assurance Requirements)，依據上述的安全功能要求制訂出評估標準，並建立表達評估標的(Target of Evaluation，簡稱 TOE)之保證安全的評估標準模式，並將其量化成評估保證等級(Evaluation Assurance Level，簡稱 EAL)，表 3- 23 為各評估保證等級的說明。

表 3- 23 評估保證等級說明

評估保證等級	評估內容	評估說明
EAL1	功能性檢測(functionally tested)	檢驗產品及相關文件的符合性，並確認產品是否符合文件宣稱之用途
EAL2	結構性測試(structurally tested)	經過評估來測試產品的結構，包括產品的設計歷程和測試
EAL3	條理化測試和檢查(methodically tested and checked)	評估產品的設計階段，獨立驗證程式開發者的測試結果，也評估程式開發者的漏洞檢查程度、開發環境控制及產品的組態管理
EAL4	條理化設計、測試和審查(methodically designed, tested and reviewed)	更多設計描述、部分實作及更完善之機制或程序，以提供TOE在開發或運送過程中不被竄改之可信度

評估保證等級	評估內容	評估說明
EAL5	半正規化設計及測試 (semiformally designed and tested)	需要半正規化設計的描述方式、完整之實作、一個更組織化的架構及在發展期間確保TOE不受干預之改良機制和/或程序
EAL6	半正規化驗證設計與測試(semiformally verified design and tested)	需要更廣泛之分析、一個結構化實作之呈現、更多結構化架構、更廣泛之獨立脆弱性分析及改良之組態管理與開發之環境控制
EAL7	正規化驗證設計與測試(formally verified design and tested)	需要更廣泛且使用正規方式呈現與正規一致性之分析及廣泛測試

資料來源：國防部²¹¹

基於國際共同準則相互承認協定(Common Criteria Recognition Arrangement，簡稱CCRA)，EAL1 至 EAL4 的安全等級為各國互相承認的；而 EAL5 以上的安全性為國防等級的安全需求，基於軍事機密，各國 EAL5 以上的標準規範並不互通，因此大多數商業產品的安全等級最高採用到 EAL4，基站設備亦不例外。部分產品會在某些認證項目額外採用更高階的安全標準，此時會在其所通過的安全等級後方加上「+」號(如 EAL4+)。本團隊將延續第一期對安全等級的研究，介紹 CC 認證中商用最高等級 EAL4 所需通過之評估(介紹版本為 Ver3.1 Release 5)，評估內容如表 3-24(保證元件欄內小數點後數字為該元件評估第 X 階的標準，例如 ADV_TDS.3 為基本模組呈現的第三階級標準，ADV_TDS.1 和 ADV_TDS.2 為 EAL3 以下的要求)：

²¹¹ 吳專吉・謝宛真(Wan-Chen Hsieh)，”資通產品安全性共同準則評估檢測技術發展現況，國防部新季刊第四十一卷第四期”，2013/10

表 3- 24 EAL4 之評估項目

保證類別	保證元件	元件內容
ADV：發展	ADV_ARC	安全架構描述
	ADV_FSP	完整功能規格
	ADV_IMP	TOE安全功能之實作與呈現
	ADV_TDS	基本模組呈現
	ADV_SPM	安全政策模組化
	ADV_INT	TSF本質
AGD：指引文件	AGD_OPE	操作使用者之指南
	AGD_PRE	準備程序
ALC：生命週期支援	ALC_CMC	產品驗收程序和自動化的支援
	ALC_CMS	問題追蹤組態管理範圍
	ALC_DEL	交付程序
	ALC_DVS	安全測量之辨別
	ALC_FLR	缺陷報告過程
	ALC_LCD	開發者定義之生命週期模型
	ALC_TAT	明確定義的開發工具
ASE：安全標的評估	ASE_CCL	符合性聲明
	ASE_ECD	元件延伸定義
	ASE_INT	安全標的介紹
	ASE_OBJ	安全目標
	ASE_REQ	衍生安全要求
	ASE_SPD	安全問題定義
	ASE_TSS	評估標的彙整規格
ATE：檢測	ATE_COV	分析範圍
	ATE_DPT	基本設計
	ATE_FUN	功能測試
	ATE_IND	獨立測試-樣本
AVA：脆弱性評估	AVA_VAN	重點之弱點評估

資料來源：CC

CC 的認證已然成為目前多個國家資訊安全相關產品必要的認證，否則會因安全

考量可能無法進入市場之中，因此，本團隊根據目前市面上行動網路、基站相關之內容的產品，依照上述評估保證等級，分別進行產品簡介及所達到之保證等級分析。觀察近幾年通過 CC 認證的行動網路相關產品發現，主要為華為設備之軟體，該公司為能打入各國行動通訊網路市場，其產品積極以通過商業類產品最高安全等級(EAL4)前甚至 EAL4⁺來證明其產品之安全性，

透過下表可得知，目前商用的通信設備在 CC 保證等級，2014 年之後，無論在硬體或是軟體的認證，所有的產品幾乎都已有達到 EAL3 等級以上，甚至部分產品達到 EAL4 等級的認證，因此可得知廠商皆朝商業類產品之最高安全等級(EAL4)前進。以 Huawei 3900 Series LTE eNodeB Software 為例，該產品於 2012 年時達到 EAL3 評估保證等級，當時的等級已達到評估產品的設計階段，但在 2014 年及 2017 年時同一樣產品已經完成 EAL4 的評估保證等級，此等級說明包含將有提供更多的設計描述、部分實作以及更完善的機制或程序。其 Huawei 3900 Series LTE eNodeB Access Control Software 於 2014 年也通過 EAL4⁺的認證，證明該軟體有具備避免未授權實體裝置訪問 TOE 資源之功能。

然因 EAL 認證通常需要花費較長的時間，且隨著驗證等級提高，所需花費的時間就越久，以目前 EAL4 為例，一般來說至少也需花費 12 至 16 個月，甚至可能需要更長的時間，並隨著產品進行改版，新版的產品就必須再次進行驗證才能取得認證，也因為 CC 驗證花費時間過長，大多數廠商皆於產品剛推出時即先驗證 EAL2 或 EAL3⁺等級，往後若有版本更新時，在進一步驗證 EAL4。因此，本團隊所探討的項目中，目前除 Huawei 3900 Series LTE eNodeB Software 外，其他設備尚未有公開更新認證資料。

因此，目前國際間已有不少的通信軟、硬體產品廠商皆是以通過 CC 認證做為產品的目標，同時也不斷的提高認證等級，讓使用者相信其產品具有足夠的安全性。在 3GPP 安全保證規範(SCAS)起草時，其安全標準多參考 CC 規範，因此其保證安全的評估標準模式亦值得於規劃基站資安檢測技術規範草案時之參考。

表 3- 25 國際通信設備與 CC 保證等級認證概況

產品類別	產品名稱	版本編號	保證等級	認證日期	產品簡介
網路裝置與系統 (軟體)	Huawei 3900 Series LTE eNodeB Software	V100R011C10 SPC112T	EAL4, ALC_FLR.1	2017/07/07	TOE 是部署在 LTE eNodeB 基站中的軟體，它是 LTE/SAE 系統中的無線接入節點。TOE 可以廣泛用於支持家庭和企業用戶的寬帶無線接入。它也可以用於支持移動寬頻無線接入。TOE 支持 FE、GE、光纖、數位用戶迴路家族(xDSL)、被動式光纖網路(PON)、微波接入、衛星等多種接入方式。
		V100R008C01 SPC820B002	EAL4	2014/11/03	
		V100R004C00 SPC100	EAL3 +	2012/03/20	
網路裝置與系統 (軟體)	Huawei 3900 Series LTE eNodeB Access Control Software	V100R008C01 SPC820	EAL4 +, ALC_FLR.1	2015/03/06	TOE 是 Huawei 3900 系列 LTE eNodeB 的軟體組成元件，實現完整的接入控制和會話建立機制，避免未授權實體裝置訪問 TOE 資源，並同時提供審計功能。TOE 可廣泛用於支持家庭和企業用戶寬帶無線接入的產品的訪問控制和事件記錄，並支援移動寬頻無線接入。
網路裝置與系統 (軟體)	Huawei Carrier Grade Platform (CGP)	V1 Release 5	EAL3	2014/10/12	Huawei 的營運商用平台，特別為用戶提供核心網路設備運行管理維護(OAM)功能的軟體。實現 client 端/server 端的架構，服務器功能位於網路設備本身，而客戶端 GUI(通常稱為本地維護終端(LMT))可以

					在 PC 上運行，以便遠程管理設備。
網路裝置 與系統 (軟體)	Huawei iManager U2000	V200R016C50	EAL3, ALC_ CMC. 4,LC_ FLR.2	2015/ 03/06	Huawei 的設備管理系統，是對於未來網路管理的主要產品，具備強大的網路單元層、網路層管理功能。U2000 能夠對傳送設備、接入設備、IP 設備進行統一管理，可管理華為 MSTP、WDM、OTN、RTN、Router、Switch、ATN、PTN、MSAN、DSLAM、FTTx、Firewall 等設備。
網路裝置 與系統 (硬體)	Huawei USN9810 Unified Service Node	V900R012	EAL3 +, ALC_ CMC. 4	2014/ 03/07	Huawei USN9810 提供了服務 GPRS 支持節點 (SGSN) 和移動管理實體 (MME) 的功能，可以作為單獨的 SGSN，單獨的 MME 或組合的 SGSN/MME 使用。USN9810 也可以用作單一網路單元 (NE) 來管理其他 USN9810。

資料來源：本團隊整理

第三節 小結

本章節主要針對最新行動寬頻資安事件及資安防護技術與服務最新趨勢做為兩個主要討論項目。在行動寬頻資安最新事件中特別針對近年國際上資安事件頻傳的第七號信令系統(SS7)的資安事件、傳輸架構、攻擊方式進行研析，並提出目前國際間與電信設備製造商建議之防護方式。

除了行動寬頻資安議題最新趨勢外，本章節另針對最新行動寬頻技術與應用之資安防護技術與服務最新趨勢進行研析，包含第五代行動網路通訊系統(5G)、軟體定義網路(SDN)以及物聯網(IoT)做了完整的詳細介紹，包含定義、架構、防護以及最新的

資安威脅。由於此重點討論的東西較為前瞻，如 5G 還未商用化、SDN 有許多安全議題待解決、NB-IoT 於全球皆在發展階段。但相關研究及防護建議上皆可做為未來國內發展新技術及應用時之參考。

我國政府近年來對於資訊安全的重視日益增加，除了透過提倡資安的重要性外，由於行動寬頻網路已是國內民眾上網之主流媒介，更是未來物聯網發展之基礎建設，每時每刻接有大量的訊息往返，國內電信產業除了防護可能遭受的攻擊外，也可針對上述已被攻擊的實例做一個針對性的漏洞檢查，鞏固我國電信資安領域的安全，本計畫之基站資安檢測項目及技術研究中，也將參考前瞻性資安技術中資安威脅與防護技術之發展，研析相關檢測項目之規劃。

在資安檢測標準與檢測流程最新趨勢研究上，在 3GPP 與基站相關的 33 系列安全規範，以 2017 年正式發布的 TS 33.216 eNodeB 安全保證規範為主軸，分析與此文件有密切關聯的 TS 33.117(網通產品安全)、TR 33.926(網通產品之安全威脅)與 TS 33.401(EPS 架構)這三份文件，探討其近年的更新方向及意義。最後再回到 TS 33.216 文件，整理此文件和另外三份文件的關係，並且介紹 3GPP 已訂出的基站安全檢測項目，作為本計畫第五章檢測項目歸化之參考。

而在安全保證規範部分，3GPP 與 GSMA 合作訂定網路設備安全保證方法(NESAS)，訂立產品安全認證的流程，其範圍包含了產品、開發生命週期的審計流程、合格認證實驗室的認證方式，也提出了 NESAS 成員間爭議的解決程序，但因該規範尚未釋出正式版本，相關動態值得關注；另外 GSMA 也因應目前電信業者應用的發展，定義了 NB-IoT(窄頻物聯網)的安全，相關內容也值得國內業者布建物聯網的參考。

最後本團隊也持續對全世界已行之多年，各國評估、驗證資通安全產品時採用的共同標準(CC)，所通過之行動通訊網路產品及認證等級進行追蹤，CC 是全球較為嚴謹的安全評估準則之一，某些國家的通訊產品都必須得通過 CC 認證，方可進入如金融、通信及國防等特定市場，本團隊研析發現，許多行動通訊產品會通過 EAL3 以上認證，來代表該產品有一定的安全標準。

第四章、國際行動寬頻框架研究

行動寬頻網路的快速普及，已成為先進國家資通訊網路之主要基礎設施，隨著網路使用深入政府與民間各層面，各國紛紛提出保障網路安全之策略，透過政策與規範之推動，保障網路資訊安全。其範圍廣及固網、無線與行動網路。

隨著 4G 頻譜執照釋出以及我國積極推動行動寬頻普及政策，行動寬頻同樣為我國行動通訊服務之主流，在用戶及流量大幅成長的趨勢下，行動寬頻網路成為資訊流通及交易的重要媒介。以下將介紹各國網路保全策略，與相關權責機關架構等二層面之發展狀況，作為我國規劃網路安全政策之參考基礎。

第一節 美國

美國做為全球最先進國家，在國土安全（Homeland Security）層面上，面臨恐怖主義結合網路空間、跨境犯罪、緊急事態的安全威脅。這些威脅改變了傳統的來源途徑，不僅超越傳統疆界，亦多指涉其他類領域，與非軍事性的全球治理、政治價值觀、外交政策、經濟等議題相互複合。也因此，「網際空間（Cyberspace）」的安全，早已被認為與國防、水力、電力、能源等國家重要關鍵基礎建設之安全同等重要。

故在 2003 年，布希總統執政期間，即公布《確保網路空間的國家戰略》(The National Strategy to Secure Cyberspace)，這是第一次將「網際空間」設定為國家安全戰略一環，透過制定防護措施，保護資訊基礎設施免於遭受破壞、干擾，進而維護美國經濟發展，達成國家安全之目的。

而法制化及權責機構之建立，更是由 2001 年即已展開，透過國土安全部（DHS）的建立以及聯邦資訊安全管理法（FISMA）之制訂，奠定美國資通訊安全之核心基礎，透過政策執行、督導管理、技術標準制訂等三個層面，完善保護美國資通訊基礎建設之安全。

一、 美國網路安全政策規範與組織架構

(一) 美國網路安全政策與規範架構

1. 制定國土安全法，成立國土安全部

美國網路安全政策之發展時間非常早，尤其自 2001 年 10 月，因應 911 事件之發生，美國總統布希即發佈行政命令籌組國土安全局（Office of Homeland Security），正式展開國家網路安全政策之發展。而後於 2002 年 10 月，國會通過國土安全法（Homeland Security Act of 2002），成立國土安全部（Department of Homeland Security，DHS），其職責為負責執行分析安全漏洞，降低網路威脅，反應網路攻擊，即時通報、分享資安事件資訊等。

2. 制定聯邦資訊安全管理法，明訂機關權責任務

為完善保護聯邦政府資訊安全，於 2002 年 11 月，國會通過聯邦資訊安全管理法（Federal Information Security Management Act，下稱 2002 FISMA²¹²），要求聯邦政府機構使用之資通訊系統必須符合聯邦安全認證標準。（法律指定由國家標準技術研究所（NIST）主責）；聯邦政府機構並須制定和實施全機構資通訊安全計畫，並將相關資訊、安全措施等加以記錄。上述措施除聯邦機構外，包括其他協力機構、承包採購商或其他為聯邦機構提供服務之之機構。而監督並稽核聯邦機構是否達成法定任務要求，則由隸屬白宮之行政管理與預算局（Office of Management and Budget，簡稱 OMB）主責。

2002 FISMA 定義了一個管理聯邦政府資訊安全的架構，所有美國聯邦政府機構、立法機關、承包政府業務的機構或代表行使公權力的機構，其所使用之資訊系統均需遵循此一規範。該資訊安全架構由 NIST (National Institute of Standards and Technology) 負責開發相關的標準和準則²¹³，提供聯邦政府部門作為擬定其資訊安全保護計畫之基礎。

²¹² NIST FISMA, H.R. 2458 - E-Government Act of 2002.

²¹³ NIST, "RISK MANAGEMENT FRAMEWORK (RMF) OVERVIEW".

由於前述 DHS 之成立與 2002 FISMA 之制定日期相近，因此，在當時 2002 FISMA 並未考量納入 DHS 之角色，以致 DHS、OMB 與各聯邦政府機構在資訊安全事項產生權責爭議，因此於 2014 年通過聯邦資訊安全現代化法（Federal Information Security Modernization Act，下稱 2014 FISMA），進一步強化聯邦政府資訊安全措施。2014 FISMA 主要目標如下：

- 完善 DHS 執行不具國家安全性質（non-national security）之聯邦行政部門資訊安全政策，包括向聯邦部門提供技術援助或部署。（意指該聯邦政府部門之執掌並非屬於國家安全相關事務。）
- 修訂和釐清 OMB 對聯邦部門資訊安全政策實施的監督職責。
- 要求 OMB 簡化或消除無效率和浪費的行政程序與文書，提升行政效率。

3. 以總統行政命令強化聯邦部門間之合作

美國為總統制國家，總統領導聯邦政府內閣，為了強化聯邦機構間的合作與協調，2013 年 2 月歐巴馬總統發佈了「改善關鍵基礎設施網路安全」行政命令²¹⁴（Executive Order 13636 -- Improving Critical Infrastructure Cybersecurity），該行政命令指出，有鑑於關鍵基礎設施的網路威脅持續增長，成為嚴重的國家安全挑戰之一，為有效防止重要基礎設施網路入侵，需改進網路安全，維護關鍵基礎設施的可靠運作。由政策面提高國家關鍵基礎設施的安全性和彈性，並維護一個鼓勵效率、創新和經濟繁榮的網路環境，以促進安全、保密、隱私和公民自由。

行政命令同時要求公私部門必須進行網路安全資訊共享，並要求 NIST 應制定網路安全架構，以減少關鍵基礎設施的網路風險。網路安全架構應包括一套標準、方法、程序和流程，並應盡可能納入自願協商一致的標準和行業最佳作法。

網路安全架構應提供具有靈活性、可重複性、基於績效和成本效益的方法，包括資訊安全與控制措施和控制，以幫助關鍵基礎設施的所有者和電信業者評估和管理網路風險。網路安全架構應著重確定適用於關鍵基礎設施的跨部門安全標準和準則。NIST 於 2014 年 2 月發佈「強化關鍵基礎設施網路安全架構（Framework for Improving

²¹⁴ WhiteHouse, “Executive Order -- Improving Critical Infrastructure Cybersecurity”, 2013/2/12.

Critical Infrastructure Cybersecurity)」，作為各部門制定自身網路安全計畫之參考。最後，行政命令要求 DHS 與聯邦各部門協調，推動自願性的關鍵基礎設施網路安全計畫，以支持關鍵基礎設施和任何其他有關利害關係人採用 NIST 制定之網路安全架構（Cyber Security Framework，以下稱 NIST CSF）²¹⁵。NIST, “Framework for Improving Critical Infrastructure Cybersecurity”即為後續介紹之網路安全架構，此後均以 NIST CSF 稱之。

此外，歐巴馬總統同時發佈了總統政策指令「維護關鍵基礎設施安全與彈性 Presidential Policy Directive (PPD-21) -- Critical Infrastructure Security and Resilience」²¹⁶，要求 DHS 應與聯邦部門合作，共同加強國家關鍵基礎設施的安全性和彈性，該指令同時指定了關鍵基礎設施部門和對應之主管部門，共 16 個關鍵基礎設施部門，並指定 DHS 部長應定期評估關鍵基礎設施部門的需求和情況。最後則是 DHS 部長與科技政策辦公室（OSTP）等聯邦部門和機構協調聯邦資助的研究與開發（R&D），以加強國家關鍵基礎設施的安全性和彈性。例如促進安全網路技術之研發，強化關鍵基礎設施的安全；提供誘因促進網路安全投資和採用新的安全技術，加強安全和恢復能力。

新總統川普就任後，於 2017 年 5 月發佈「加強聯邦網絡和關鍵基礎設施網絡安全的總統行政命令 Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure」²¹⁷，其中，要求各聯邦機構應使用 NIST CSF 安全架構或任何後續文件，來管理該機構的網路安全風險。每個機構負責人應在本命令之日起 90 天內向 DHS 部長和 OMB 局長提供風險管理報告。

此外，除再度重申前述 PPD-21 之政策指令外，也針對網路安全人才培育與國際合作等事項做出政策指示。

整體而言，美國針對網路資訊安全之多數要求均為自願性質，僅針對聯邦政府重要國家安全系統採行強制性安全要求，包含國防、情報、外交事務之系統。然而，雖

²¹⁵ NIST, “Cybersecurity Framework”.

²¹⁶ WhiteHouse, “Presidential Policy Directive -- Critical Infrastructure Security and Resilience”, PRESIDENTIAL POLICY DIRECTIVE/PPD-21.

²¹⁷ WhiteHouse, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”.

然為自願性質之規範，一旦發生資安事件，仍會依據其他法律進行處置，產業廠商若不積極遵守相關規範，一旦發生事件，則後果仍是相當嚴重。

（二）主責機構

依據前述美國國家資通安全的政策架構介紹，我們可歸納出美國的資安架構大致分為三個部分，分別為 1.政策執行 2.政策制定與稽核 3.技術與標準發展，以下分述之。

1. 政策執行：以國土安全部（DHS）為核心

國土安全部（DHS）係依據國土安全法於 2002 年成立，將 22 個與國家安全相關之不同的聯邦部門和機構合併成一個統一的綜合性內閣機構，負責維護美國國家安全。美國很早便將網路安全視為國家安全之一環，因此與網路空間之安全維護相關之機構如聯邦電腦事件反應中心（Federal Computer Incident Response Center, FedCIRC）加入 DHS 之後，更名為美國電腦緊急反應小組（Computer emergency response teams, CERT），國防部國家通訊系統（National Communications System）等部門整合進入 DHS。

DHS 內部由網路安全與通訊辦公室（CS&C）負責提高國家網路和通訊基礎設施的安全、彈性和可靠，防止或減少關鍵資訊基礎設施的破壞，以保護公眾，經濟和政府服務。其隸屬於國家保護與計畫局（NPPD）。CS&C 下設網路安全與通訊整合中心（NCCIC）、網路安全部（NSD）、電腦應變小組（US-CERT/ICS-CERT）等單位。

NSD 負責設計、開發、部署和維護國家網路安全保護系統（NCPS），該系統提供入侵檢測、高級分析、資訊共享和入侵防禦功能，以打擊和減輕聯邦行政部門的網路威脅。NSD 還負責管理「持續診斷和緩解（Continuous Diagnostics and Mitigation, CDM）」計畫，該計畫為聯邦部門提供了分析、識別網路安全風險的能力和工具，並根據潛在風險進行優先排序，以分配資源解決問題。

NCCIC 的目標是降低可能嚴重影響國家重要資訊技術和通信網路安全性的風險及嚴重性。NCCIC 結合 US-CERT/ICS-CERT，負責整合、分析與回應網路威脅資訊，降低國家網路資安風險。US-CERT 以先進的網路和數位媒體分析技術，針對美國國家網路的惡意活攻擊動，制定及時和可行的資訊，分發通知聯邦部門和機構、州和地方政府、私部門組織和國際合作夥伴，此外，US-CERT 還負責維護 NCPS，為聯邦部門和機構提供入侵檢測和預防功能。

工業控制系統網路緊急應變小組 (ICS-CERT) 則通過與執法機構和情報界的合作，協調聯邦、州、地方政府以及控制系統的工作，降低關鍵基礎設施部門內部以及外部之，包含擁有者、電信業者和供應商。ICS-CERT 的網路安全和基礎設施保護專家分析緊急事件和後續服務恢復之狀況，分析相關攻擊事件對關鍵基礎設施的潛在影響，為關鍵系統的所有者和電信業者提供協助控制未發生的風險(請參閱圖 4-1)。

至此，美國國家整體網路安全主責，即以 DHS 為核心，協調其他有關部門進行資安維護。

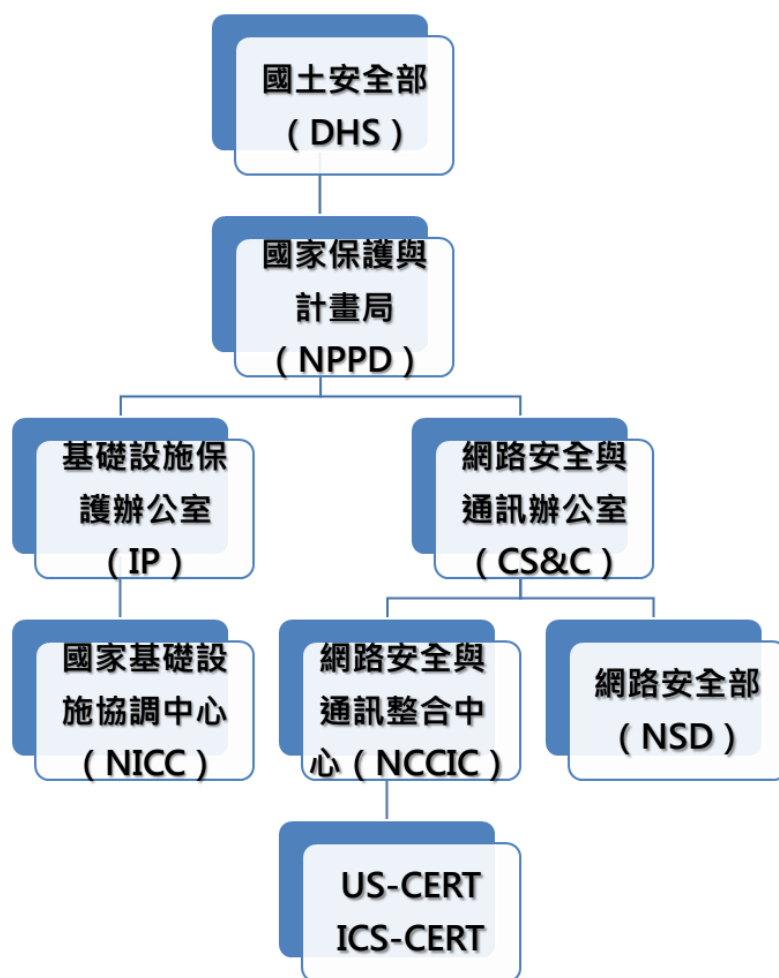


圖 4-1 美國 DHS 內之資安主責組織架構

資料來源：本團隊整理

2. 政策制定與稽核：白宮行政管理與預算局 (OMB)

美國為總統制國家，白宮為最高行政單位領導內閣部會，OMB 隸屬於白宮，負責

預算與行政管理事項，負責監督行政部門實施其願景。具體來說，OMB 的使命是協助總統履行其政策，預算，管理和監管目標，並履行機構的法定責任。依據聯邦資訊安全管理法（FISMA），負責管理、督導聯邦機構資訊安全事項之落實。OMB 負責預算之開發與執行管理，包括機構績效監督、人力資本、聯邦採購、財務管理和資訊技術。OMB 在監管政策之職責，包括協調和審查執行機構所有重要的聯邦法規。

聯邦機構必須遵守 OMB 之要求。OMB 亦針對聯邦機構之資訊安全事項發佈相關備忘錄，例如 2015 年 10 月，OMB 推動網路安全策略與實施計畫（M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government），CSIP 全面審查聯邦政府網路安全，確定和解決嚴重的網路安全漏洞和新出現的優先事項，並提出具體建議解決這些差距和優先事項。包含前述 DHS 下的 CDM 計畫與 NIST 技術之更新等事項，皆由 OMB 加以監督。

3. 技術標準制訂：國家標準技術研究所（NIST）

NIST 前身為國家標準局（NBS），是一家測量標準實驗室。NIST 隸屬於美國商務部（DOC），屬於非主管機構，並不管理任何產業。NIST 之主要任務是促進美國的創新和產業競爭力，推進度量衡學、標準、技術以提高經濟安全。NIST 也是美國資通安全技术標準的制訂者，依據 FISMA 之規定，負責聯邦資通安全標準之制訂，如密碼相關的 FIPS 系列標準，安全相關的 SP-800 系列標準等。針對管件基礎設施之網路安全，NIST 依據總統政策指令發佈網路安全架構（即 NIST CSF），以提供整體資安規劃藍圖架構予尚未建立網路安全架構的組織參考，並協助公、私部門改善資通訊科技和工業控制系統風險管理的能力。因此，NIST 在美國資安技術標準扮演關鍵的角色。

4. 通訊產業主管機關：聯邦通訊委員會（FCC）

依據 1934 年通訊法，美國有關州際及國際之有線、無線廣電媒體、有線及無線通訊、衛星、無線電頻率之管制由聯邦通訊委員會（FCC）管轄，在美國行政體制為總統制之基礎下，FCC 之性質為非內閣部會之獨立委員會，向國會負責。依據先後修訂之 1934 年通訊法及 1996 年電信法，FCC 負責非政府使用之通訊及媒體產業之管理，包含執照發放、通訊傳播產業之市場競爭監理。

FCC 在通訊傳播產業中，就媒體方面，負責管理廣播、有線電視與衛星電視業務；就無線通訊部分，行動通訊、衛星通訊以及商用無線頻率之分配、頻譜拍賣、租賃、

次級交易與執照管理；固網通訊部分，則負責州際及國際通訊服務之管制；FCC 負責通訊安全與穩定性、公共安全、緊急服務通訊之運作與互連。

因此，就國家網路安全而言，FCC 由於屬於獨立機關，故需依據總統政策指令 PPD-21 與 DHS 合作，確認通訊基礎設施之資安優先性、確認通訊部門的脆弱性，並與業界或其他單位合作解決，並與產業、外國、國際組織合作，以促進通訊領域內的關鍵基礎設施安全性和靈活性。同時，FCC 也依據 NIST CSF 架構向通訊業者建議自願性質之資安風險管理機制。

二、 美國關鍵基礎設施保護

關鍵基礎設施提供了支撐美國社會的基本服務。必須採取積極和協調的努力，加強和維護對公眾信心和國家安全、繁榮和福祉至關重要的安全、有效和有彈性的關鍵基礎設施，包括資產、網路和系統。關鍵基礎設施是多樣化和複雜的，包含不同類型的網路、組織結構和營運模式，也因此物理空間和網路空間的功能和系統是相互依賴的。關鍵基礎設施必須是安全的，能夠承受並迅速從資安危險中恢復。

目前美國關鍵基礎設施的範圍，係由前述總統政策指令 PPD-21 所指定，一共包括 16 個重要基礎設施²¹⁸，其範圍與主責單位如下表所示。

表 4-1 美國關鍵基礎設施列表

重要基礎設施範圍	主責單位
化學部門 Chemical	國土安全部
商業設施 Commercial Facilities	國土安全部
通訊部門 Communications	國土安全部
關鍵製造業 Critical Manufacturing	國土安全部
水壩部門 Dams	國土安全部

²¹⁸ DHS, “Critical Infrastructure Sectors”.

重要基礎設施範圍	主責單位
國防工業基礎 Defense Industrial Base	國防部
緊急服務 Emergency Services	國土安全部
能源部門 Energy	能源部
金融服務業 Financial Services	財政部
糧食和農業部門 Food and Agriculture	農業部 衛生部
政府設施 Government Facilities	國土安全部 總務局（General Services Administration）
醫療與公衛 Healthcare and Public Health	衛生部
資訊技術部門 Information Technology	國土安全部
核能部門 Nuclear Reactors, Materials, and Waste	國土安全部
交通運輸系統 Transportation Systems	國土安全部 交通運輸部
水利與污水系統 Water and Wastewater Systems	環保局

資料來源：美國國土安全部（DHS）

針對關鍵基礎設施之保護，PPD-21 提出 3 個主要目標：

- 優化和釐清聯邦政府各部門的職能關係，推動國家團結合作，加強關鍵的基

礎設施安全和彈性；

- 確認、識別聯邦政府的基準資訊（baseline data）和系統需求，實現有效率的資訊交換，所有聯邦部門和機構負責人必須確定優先順序，並評估補救和安全性之需求；
- 實施整合與分析功能，為關鍵基礎設施的規劃和營運決策提供資訊，包括事件、威脅和新興風險的運營和戰略分析。。

由上表可知，國土安全部（DHS）在關鍵基礎設施保護中扮演核心的角色。DHS 應提供戰略指導，協調聯邦各機構一起努力，提升關鍵基礎設施的安全性和彈性。依據 2002 年國土安全法規定，DHS 也負責評估國家在保護關鍵基礎設施方面的能力、機遇和挑戰；分析所有危害關鍵基礎設施的潛在威脅與脆弱性；並確定與所有關鍵基礎設施部門有效的公私協力合作，達成必需的安全和恢復力；DHS 需制定國家計畫和指標，與各部門主責單位和其他關鍵基礎設施合作夥伴協調；整合和協調聯邦跨部門的安全活動；確定和分析關鍵基礎設施部門之間的關鍵相互依賴關係等。

DHS 有關關鍵基礎設施保護之其他任務和職責包括與其他部門主責單位和其他聯邦部門機構協調，確定關鍵基礎設施並考慮物理和網路威脅、漏洞的優先級；分析可能的威脅和影響關鍵基礎設施的事件狀況；向關鍵基礎設施之擁有者或電信業者提供技術援助與情報交換、全面評估國家關鍵基礎設施的脆弱性；處理關鍵基礎設施的重大網路事件，並支援執法單位之調查；按照法規要求，每年報告國家重點基礎設施建設情況。

在 DHS 內部機關組織上，關鍵基礎設施之保護分別由網路安全與通訊辦公室（CS&C）下的網路安全與通訊整合中心（NCCIC）與基礎設施保護辦公室（IP）下的國家基礎設施協調中心（NICC）所負責。

NCCIC 屬於全天候的網路事件反應與管理中心，在公私部門之間分享資訊，同時 NCCIC 也透過工業控制系統網路緊急應變小組（ICS-CERT），協調聯邦、州、地方政府以及控制系統的工作，降低所有關鍵基礎設施部門的風險，協助關鍵系統的擁有者與電信業者應對資安事件並進行恢復。

NICC 屬於全天候協調和資訊共享之營運中心，管理 DHS 與各關鍵基礎設施之間的協調。主要任務在針對與關鍵基礎設施之安全威脅相關資訊的收集、整合、評估、

協調與傳遞，透過收集、維護基礎設施威脅的資訊，並加以協調和評估這些資訊的準確性、重要性和影響性，並整合傳遞給關鍵基礎設施夥伴，並作為 DHS 決策之參考。

國土安全部並於 2014 年 2 月推動「關鍵基礎設施網路社群自願計畫（Critical Infrastructure Cyber Community Voluntary Program, C³VP）²¹⁹」，C³VP 為自願性計畫，由國土安全部使用 NIST CSF 架構(Supra note 215)，協助關鍵基礎設施部門和企業組織，了解 NIST CSF 架構和其他網路風險管理工作的使用情況，並依據 NIST CSF 架構制定與實施具體指導，提升其安全性，降低網路安全風險。

C³VP 第一年的重點在關鍵基礎設施，計畫後期階段將擴大該計畫的範圍，讓有興趣使用 NIST CSF 的所有關鍵基礎設施和其他有關企業均能參與。C³VP 計畫還與前述 16 個關鍵基礎設施部門合作，根據各部門需求，以 NIST CSF 為基礎製定適用該部門的指導原則。

C³VP 鼓勵所有使用之組織或機構就使用該計畫資源的經驗提供反饋，以進行架構的改進，提升協助品質，相關經驗也將與 NIST 分享，以幫助指導下一個版本的 NIST CSF 架構的開發與改進工作。

三、 美國網路安全推動策略

資訊共享對於保護關鍵基礎設施和促進國家網路安全至關重要。作為聯邦主要保護關鍵基礎設施和推動網路安全部門，國土安全部（DHS）制定並實施了大量的資訊共享計畫。通過這些計畫，DHS 開發合作夥伴關係，並與公、私部門共享實質性資訊，在美國，私部門擁有並經營全國大部分關鍵基礎設施。DHS 還與地方政府與國際合作夥伴共享資訊，因為網路安全威脅不受地理邊界的限制。

（一） 增強的網路安全服務（ECS）計畫

ECS 計畫是一種入侵防禦功能，可幫助美國公司保護其電腦系統，防止未經授權的訪問、開發和數據洩露。ECS 之運作，係由 DHS 與經認可的商業服務業者（CSP）共享敏感和分類的網路威脅資訊，CSP 可使用這些威脅資訊來阻止某些類型的惡意流

²¹⁹ DHS, “Critical Infrastructure Cyber Community C³ Voluntary Program”.

量進入客戶網路。

ECS 計畫目前提供三種服務：

- 防止惡意域名服務：阻止訪問指定的惡意域名；
- 電子郵件（SMTP）過濾，阻止具有指定惡意條件的電子郵件進入網路；
- Netflow Analysis 使用被動檢測來識別威脅。

所有美國公私部門都有資格參加 ECS，計畫參與是自願性質，目前有 3 個經認可的 CSP 被認可提供 ECS，包括：AT&T、CenturyLink、Verizon。

（二） 資訊共享組織：ISAC 與 ISAOs

DHS 內部設立之資訊共享和分析中心（Information Sharing and Analysis Centers，簡稱 ISAC）是由各主責部門(Supra Note 218)、關鍵基礎設施擁有者和電信業者組成，以分享政府和特定關鍵行業之間的網路安全資訊。由 NCCIC 與所有的 ISAC 協調，以提高資訊安全防範、應變和恢復的能力。

2015 年歐巴馬總統發布了「促進私部門網路安全資訊共享 (Executive Order 13691 Promoting Private Sector Cybersecurity Information Sharing)²²⁰」，指示國土安全部(DHS)鼓勵發展資訊共享和分析組織（Information Sharing and Analysis Organizations，簡稱 ISAOs）。由 NCCIC 與 ISAOs 進行持續性的合作與協調，促進聯邦政府和私部門合作夥伴之間的網路安全資訊共享與分析。

ISAOs 與前述之 ISAC 功能相似，但組成不同，ISAC 屬於 DHS 內部單位，而 ISAOs 則為外部單位。其主要的方式，透過公開評選的流程，選擇一個非政府組織作為 ISAOs 標準組織，由該獲選組織確定一套關於建立和運作 ISAO 的自願標準或準則。2015 年 5 月 ISAO 標準組織由德州聖安東尼奧大學（UTSA）物流管理研究所（LMI）和零售網路智能共享中心（R-CISC）獲選，UTSA 團隊必須與既有資訊共享組織、關鍵基礎設施的擁有者和電信業者，及其他公私部門利益相關者合作，建立和運作 ISAOs 的自願性準則。

²²⁰ WhiteHouse, Executive Order -- Promoting Private Sector Cybersecurity Information Sharing.

通過公開的活動，ISAO 標準組織將製定符合所有行業團體需求的最佳實踐 (Best Practice)。雖然制定和運作標準仍然必須通過標準化組織開展的公開招標來製定，但 ISAO 屬於自願參與、非強制性的，並透過透明與包容的過程，形成資訊共享的準則，讓所有參與者皆能獲得適合的資訊。

(三) 網路資訊共享與協同計畫 (Cyber Information Sharing and Collaboration Program，簡稱 CISCP) ²²¹

此一計畫由 NCCIC 發動並擔任資訊共享活動的中心，透過和參與公司分享有關網路威脅、事件和漏洞的資訊，使參與者能妥善的保護自身網路。CISCP 提供了一個協作環境，分析師相互學習，以更好地了解新興的網路安全風險和有效的防禦。CISCP 的運作類似於社群，所有參與者都通過強大的資訊共享和協作來獲得互利。由於涉及各方參與者之敏感資訊，要加入 CISCP，參與者必須簽署合作研究和開發協議 (CRADA)，通過審核者有資格獲得許可以查看 NCCIC 監控、分析與分類的威脅資訊。

CISCP 運作流程由合作伙伴提供觀察到的網路威脅指標、網路事件的資訊，並確定網路漏洞之後提高給 DHS，DHS 以其匿名的方式與其他 CISCP 合作夥伴共享。CISCP 分析人員在收到資訊後，會對涉及安全之資訊或產品進行準確、及時和可行的分析，並以各種形式通知合作伙伴。例如：

指標公告 (Indicator Bulletins，簡稱 IB)：關於新的威脅和漏洞的簡短及時的公告。這些公告每週以機器可讀格式發送幾次。這些格式可以更快地進行解析和分析，從而可以採取更快的措施來阻止攻擊並修復漏洞。

分析報告 (Analysis Report，簡稱 AR)：更深入的分析產品，將相關的威脅和入侵者活動聯繫起來，並提出如何檢測、防禦措施和補救建議。

優先警報 (Priority Alert，簡稱 PA)：對預期會產生重大和深遠影響的單一威脅或漏洞提供預警。

推薦作法 (Recommended Practices，簡稱 RP)：產品提供了協同定義和記錄一系

²²¹ DHS, “Cyber Information Sharing and Collaboration Program (CISCP)”.

列最佳實踐（Best Practice）建議或策略的方法。

作為 CISC 的一部分，DHS 促進與政府和行業合作夥伴的協作活動，促成共享網路威脅資訊的信任環境。這些交流是未分類的，專注於即時的威脅或最近的活動。此外，該小組負責分析師與分析師之間的技術威脅交流和分析師培訓活動，以便進行分類和未分類的報告。

第二節 加拿大

加拿大擁有完善的網際網路基礎設施，其所引發的資訊安全問題也使得加拿大成為全球最早倡導保障網際網路安全的國家之一。加拿大政府不但在國家政策與法律層面強化網路安全的防護，更提倡政府跨部會的資安合作，以及網際網路業者的資安自律管理。另一方面，關鍵基礎設施的安全防護也是加拿大政府的施政重點，藉由所制訂的關鍵基礎設施國家策略（National Strategy for Critical Infrastructure）與關鍵基礎設施行動計畫（Action Plan for Critical Infrastructure），加拿大目標建設一個更安全、穩定和彈性的基礎設施環境。

一、 加拿大網路安全政策規範與組織架構

加拿大公共安全部（Public Safety Canada，簡稱PSC）於2010年公布加拿大網路安全策略（Cyber Security Strategy），其中有三項工作重點，分別包括：

（一） 確保政府公部門系統安全

加拿大國民信任其個人與企業資訊於政府中的運作，同時也信任政府提供的服務，並相信政府會採取相關行動確保加拿大的網路主權，並保護、提升國家安全與經濟利益。加拿大政府將建立必要的架構、工具以及人員配置，以履行其維護網路安全之義務。

（二） 協同確保聯邦政府以外系統的安全

加拿大的經濟繁榮和國民安全取決於政府以外系統的順利運作。加拿大政府將與區域省、縣市地方政府和民間企業合作，透過相關支援並採取必要的措施以強化加拿

大的網路延伸，包括其關鍵基礎設施。

（三）協助保障加拿大國民線上安全

加拿大政府將協助加拿大國民獲得保護自己及其家人線上安全的必要資訊，並強化執法機關打擊網路犯罪的能力。

針對確保政府系統網路安全項目，加拿大公共安全部更進一步細分為以下工作：

- 建立明確的聯邦機構角色與權利
- 強化聯邦網路系統的安全
- 提升政府網路安全意識

至於與聯邦系統以外之機構協同處理網路安全議題，加拿大公共安全部細分如下：

- 與省政府與縣市政府的協同合作

強化與各級政府間的伙伴關係，是為加拿大和加拿大國民提供全面性網路安全策略的重要元件。加拿大省份與縣市政府提供民眾一系列的基礎服務，會需要其網路系統的安全和可靠運作。例如，各級政府在電子資料庫中所持有的敏感性個人資料，包括健康紀錄、婚姻狀態、駕照以及省級納稅申報資訊等。各省和縣市政府對於提升加拿大國民網路安全意識上扮演重要角色，尤其是年輕一輩的加拿大國民，透過其教育體系，使民眾最初接觸虛擬世界時，能夠具備安全意識。只有各級政府協同合作，才能確保加拿大國民的隱私資訊，並且信賴所獲得之服務。

- 與民間企業和關鍵基礎設施的協同合作

加拿大網路安全策略具備以下特點：

- 反應加拿大的價值觀，如法治、公共責任與隱私；
- 允許不斷改進以應對新浮現的威脅；
- 整合加拿大政府相關活動；
- 強調與加拿大國民、省、縣市政府、企業與學術界的夥伴關係；

- 建立於與盟友的密切合作關係之上。

2011 年 2 月加拿大政府公布 2010 年至 2015 年之網路安全策略行動方案 (Action Plan 2010-2015 for Canada's Cyber Security)，概述加拿大政府如何實踐策略之相關計畫，以保障加拿大公民網路安全與經濟利益。

加拿大政府於 2011 年明定加拿大通信安全機構 (Communications Security Establishment Canada，簡稱 CSES) 與加拿大網路事件應變中心 (Canada Cyber Incident Response Centre，簡稱 CCIRC) 的角色與任務，提高加拿大識別、預防與減輕網路安全威脅的能力。加拿大網路事件應變中心 (CCIRC) 主責網路安全議題，整合公部門與民間企業，強化網路系統安全以確保國家安全。同時，加拿大公共安全部響應美國國土安全部 (Department of Homeland Security) 與國家標準與技術研究所 (National Institute for Standard and Technology，簡稱 NIST) 開發的 NIST 架構，認同此一架構可適用於加拿大的背景環境。²²²

CCIRC 扮演國家級協調中心的角色，負責減少加拿大關鍵系統與服務面臨的網路風險，關鍵系統則包括銀行或通訊服務供應商，該類系統會被歸類為關鍵基礎設施。CCIRC 為加拿大公共安全部下轄之部門，其合作對象包括聯邦政府、省政府與縣市政府、加拿大關鍵基礎設施服務業者、學術機構、網際網路服務供應商與網路安全專家社群等。同時，CCIRC 也和國際相關組織密切合作，處理網路安全威脅與共享保護關鍵設施之相關資訊，例如美國電腦緊急整備小組 (United States Computer Emergency Readiness Team，簡稱 US-CERT)、英國國家網路安全中心 (National Cyber Security Centre，簡稱 NCSC)、澳洲電腦緊急整備小組 (CERT Australia) 與紐西蘭政府通訊安全局 (Government Communications Security Bureau，簡稱 GCSB)。

2012 年，加拿大簽署網路安全行動計畫 (Cyber Security Action Plan)，該跨國行動方案將與美國共同提升網路安全能力。

目前加拿大聯邦政府中，處理網路安全事件的單位包括公共安全部、加拿大安全情報局 (Canadian Security Intelligence Service，簡稱 CSIS)、加拿大通信安全機構 (CSES) 與加拿大皇家騎警 (Royal Canadian Mounted Police，簡稱 RCMP) 等。加拿大聯邦政

²²² Public Security Canada, "Fundamentals of cyber security for Canada's Critical Infrastructure Community", p.5, 2016.

府正努力改善各單位間之溝通協調，目前主責協調單位為 CCIRC。加拿大政府中各單位擁有不同的負責內容(如圖 4-2)。

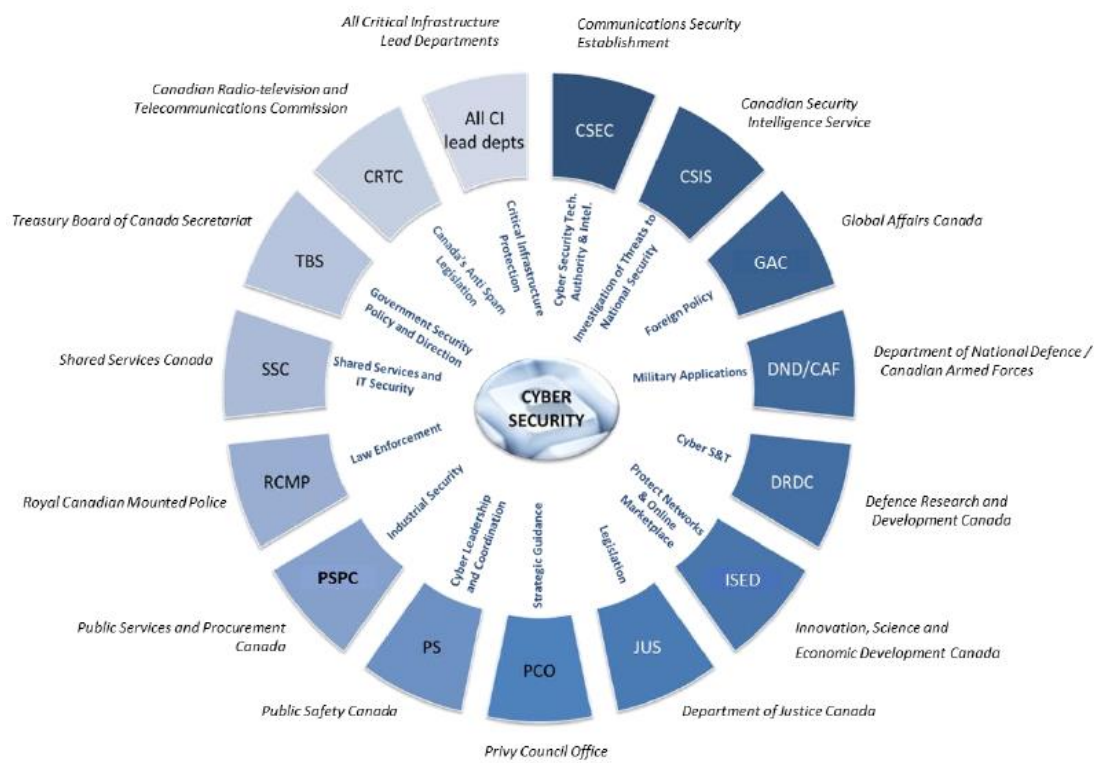


圖 4-2 加拿大聯邦政府各機構於網路安全議題之權責區分²²³

資料來源：加拿大公共安全部

加拿大聯邦政府各機構於網路安全中之責任義務如下表 4-2。

²²³ Public Safety Canada, “Fundamentals of cyber security for Canada’s Critical Infrastructure Community”, 2016.

表 4-2 加拿大聯邦政府各機構於網路安全中之主責內容

單位名稱	主責內容
加拿大通訊安全機構 (Communications Security Establishment, CSE)	加拿大通訊安全機構 (CSE) 是加拿大政府的安全部門，負責蒐集網路外國情報，並扮演加拿大聯繫國際密碼學社群的對口單位。CSEC 負責網路安全的研究和開發。CSEC 監測與防禦加拿大的網路，透過偵測、發現並回應可能對政府造成的網路威脅，並提供緩減和恢復之建議措施給政府部門，幫助相關單位從網路意外事件中恢復。
加拿大安全情報局 (Canadian Security Intelligence Service, CSIS)	加拿大安全情報局 (CSIS) 處理國家安全調查，提供報告與諮詢建議給加拿大政府關於網路安全威脅的相關活動。CSIS 提供分析建議給加拿大政府，協助了解網路威脅，以及可能在加拿大境內造成威脅的境內行為人或海外行為人的意圖和能力。相關情報有助於加拿大政府改善其整體運作意識、強化識別網路漏洞、防止網路間諜活動或其他網路威脅，並採取相關作為保護關鍵基礎設施。
加拿大全球事務部 (Global Affairs Canada, GAC)	加拿大全球事務部支持國際組織減輕網路安全威脅，並協助外國政府提高其網路安全能力；另外也透過外交參與方式，形成網路安全的多邊監管，讓加拿大政府在國際上有更好的位置，捍衛與促進其外交政策和與網路安全利益相關的事務。
加拿大國防部 (Department of National Defense/ Canadian Armed Forces, DND/CAF)	加拿大國防部負責提供國防情報給加拿大政府的威脅與風險評估流程。國防部對於加拿大政府資訊技術事件管理計畫提供貢獻，包括監測、分析、減輕與回應階段。透過提供有關軍事來源的網路安全資訊、監督與提報技術性資訊威脅，以及提供潛在的軍事回應。
加拿大創新、科學與經	負責頻譜管理和建立安全可靠的電信系統，發展政策以確

單位名稱	主責內容
濟發展部 (Innovation, Science and Economic Development Canada, ISED)	保的網際網路環境，同時確保緊急狀態下的電信服務持續性。
加拿大司法部 (Department of Justice Canada)	針對網路政策與法規提供相關法律建議，協助部門與機關。針對與刑事犯罪法律政策和資訊共享議題，以司法部扮演主要領導角色。
樞密院辦公室 (Privy Council Office)	向總理與國家安全顧問提供協助，協調加拿大安全情報成員之活動，促進國家安全的協同與整合。
公共安全部(PSC)	公共安全部保障加拿大國民擁有免受自然災害、犯罪和恐怖主義等相關風險的安全保護。該部門將使政府運作中心得作為國家緊急應變系統 (National Emergency Response System, NERS) 的樞紐。公共安全部於網路安全領域中扮演重要且獨特角色，負責協調、實施網路安全策略，包括與關鍵基礎設施之溝通協調、提高對網路威脅的認知、識別安全漏洞與制訂解決策略。 加拿大網路事件應變中心(CCIRC)位於公共安全部旗下，扮演加拿大電腦安全及時應變小組，負責監督和提供網路威脅的解決策略，將國家重要的網路事件升級到政府運作中心進行處理，幫忙協調國內網路威脅緊急事務之應變，以保護國內關鍵基礎設施。
加拿大公共服務與採購部	扮演共享與共同服務的提供者。作為產業安全計畫活動的一部分，確保政府單位簽署契約的安全性。同時，確保加拿大民間企業保護外國政府與北約組織的機密資訊。產業安全部門將維繫與盟國的關係，並推動簽署產業安全事宜

單位名稱	主責內容
	(包括網路安全) 協議備忘錄。
加拿大皇家騎警 (RCMP)	加拿大皇家騎警(RCMP)負責對可能的網路犯罪事件進行刑事調查,例如未經許可使用電腦或損毀數據。RCMP主導對國家網路安全的犯罪調查,並協助提供關於網路犯罪威脅的建議與指導方針給國內和國外合作機關。
加拿大共享服務 (Shared Services Canada)	負責協助簡化與整合電子郵件、數據中心和網路的資通訊技術
加拿大政府秘書處財政 委員會(Treasury Board of Canada Secretariat)	加拿大政府秘書處財政委員會負責提供相關政策建議給總理辦公室,例如政府資訊安全政策或方針等。
加拿大廣播與電信委員 會(Canadian Radio- television and Telecommunications Commission)	加拿大廣播與電信委員會負責確保加拿大人民能接取世界級的通訊系統,保護加拿大人民不會遭受未經授權的通訊,並提供消費者與企業更安全的網際網路環境。

資料來源：加拿大公共安全部

2014 年 2 月時,加拿大政府宣布網路安全協同專案(Cyber Security Cooperation Program,簡稱CSCP),以五年期專案時間投入 150 萬加幣支持加拿大的網路安全策略。該項專案將用以改善加拿大重要網路系統的安全,提供補助或捐款給系統持有者、運作者、產業界與貿易協會、學術單位與研究機構所提出的合格研究專案。

二、 加拿大關鍵基礎設施保護

針對公部門網路安全與關鍵基礎設施之保護,2009 年加拿大公共安全部與省/地

區政府合作推出關鍵基礎設施國家型策略 (National Strategy for Critical Infrastructure) 與行動方案 (Action Plan for Critical Infrastructure)，相關內容整理相關計畫，確保加拿大的關鍵基礎設施能夠及時回應各種網路意外事件，並能即時於網路中斷後回復。

根據該策略內容，將關鍵基礎設施定義為和加拿大公民之人身健康安全與政府有關之必要流程、系統、設施、科技、網路、資產和服務。加拿大網路安全策略擬訂之行動方案整理如下表 4-3。

表 4-3 加拿大網路安全策略行動方案

行動方案	時間表	工作項目	主導單位
主導並於政府部門間溝通協調，聚焦網路安全計畫與相關資源	2010 年開始	導入與實施加拿大網路安全策略	公共安全部
完善發展政府內部的網路安全	2010 年開始	建立與支持網路安全跨部門管理機制	公共安全部
	2011 年開始	建立與支持加拿大政府的安全管理架構，該架構由主責單位安全指導委員會與各工作小組組成	財政委員會秘書處
改善聯邦法律部門於網路安全之合作	2011 年開始	建立與維運網路安全執法實務小組	司法部
提供政府當局績效評估相關指標，以評量加拿大網路安全策略的執行成果	2012 年開始	制定績效評估策略，並從 2015 年開始評估	公共安全部

資料來源：加拿大公共安全部

加拿大政府透過網站與電子資訊系統提供相關服務給個人或企業，或傳送高度機密資訊給軍方，須保護其電子資料庫中儲存之個人與商業資訊。網路事件牽涉大範圍的電腦網路，包含政府系統，網路事件的負責人員會定期探討系統漏洞，有效確保該系統以及儲存於系統中的數據得以安全，其重要性與國家安全相當。

保障加拿大公民於網路上的個人資料，以及政府資訊基礎建設之安全性，是加拿大政府的重要目標，因此，加拿大政府會提供更多服務，對加拿大公民的網路安全採取相關措施，並鞏固資通訊基礎設施，以提高安全防護程度。

加拿大政府正在努力強化其偵測、制止與防範網路事件的能力，佈建資訊安全技術來推動加拿大的經濟與國家安全利益(如表 4-4)。

表 4-4 加拿大網路安全策略行動方案：政府資訊系統安全防護項目

行動方案	時間表	工作項目	主導單位
強化政府的資訊安全架構，以改善政府網路的安全性	2011 年開始	建立加拿大共享服務，強化政府的數位骨幹網路	加拿大公共工程與政府服務部
		制定與實施新的安全標準，適用於政府採購之資訊技術產品與服務	加拿大共享服務、公共工程與政府服務部門以及加拿大通訊安全機構
建立對於政府網路安全事件的預防與處理機制	2011 年開始	於加拿大通訊安全機構中建立網路威脅評估中心 (Cyber Threat Evaluation Centre)	加拿大通訊安全機構
增加對政府網路安全的投資	2011 年開始，持續至 2016 年第四季	預計於四年間投入 1.55 億加幣以雇用專業人士以及購買新設備	分屬不同部門
	2012 年開始	發展企業級資通訊安全架構，確保政府資通訊	財政委員會秘書處、加拿大共享服

行動方案	時間表	工作項目	主導單位
		基礎設施更新時具備基礎資訊安全能力。	務與加拿大通訊安全機構共同合作
	2012 年開始	提供新的政府資通訊安全事件回復能力，確保及時回應與妥善處理	財政委員會秘書處、加拿大共享服務與加拿大通訊安全機構
	2012 年開始	增加資訊收集與分析能力	加拿大通訊安全機構
	2012 年開始	改善網路威脅的偵測與防禦能力	加拿大通訊安全機構
加強軍方的網路安全能力	2010 年開始	強化防衛加拿大國防部與軍方網路的能力	加拿大國防部/軍方
		建立加拿大軍方網路任務編組與總網路部門	加拿大國防部/軍方
		建立加拿大軍方關於網路安全實務的資訊交流	加拿大國防部/軍方
改善政府計畫，有效回應重大網路事件	2009 年開始	修訂政府資通訊事件管理計畫	財政委員會秘書處
提高政府的安全培訓與意識	2010 年開始	主導與促進各種政府安全相關活動、論壇與培訓課程等相關措施	財政委員會秘書處

資料來源：加拿大公共安全部

2016 年加拿大公共安全部發布加拿大關鍵基礎設施網路安全基礎報告 (Fundamentals of Cyber Security for Canada's Critical Infrastructure Community)，針對網路安全的基礎，建立以下關鍵目標，包括：

- 提升網路安全意識

加拿大公共安全部認為，即使是最先進的網路安全技術，如果人民未正確使用時，則該技術也無法發揮效益。駭客社群誘導員工非法取得公司資產的狀況日趨嚴重，因此，建立強大的網路安全意識計畫，是因應不斷變化的網路安全戰場的關鍵。從對於人員的基礎培訓，逐漸擴大到提供駭客如何詐騙員工的最新資訊。安全意識計畫可能包括定期檢視、升級現有防護措施，或根據需求採取新的防護措施。

- 定義角色與責任；

加拿大公共安全部認為，網路安全雖然是每個人的責任，但有必要從組織的最上層開始建立各機構之角色與責任。組織高層扮演關鍵的角色與責任，應促進安全意識與預防的文化，確保已評估相關弱點，建立網路安全計畫與問責機制。

每一個組織都應該要有至少一位網路安全聯絡人，負責以下事務，包括學習威脅、趨勢與安全方案；規劃、取得以及實施網路安全防護；協助其他人理解網路安全最佳實務與政策；在管理架構的協助下實施最佳的網路方案與政策；維護與升級現有的網路安全防護能力。

組織管理者應該將網路安全視為其責任的一部分，並為員工提供網路安全應視為日常運作中重要一部分的指導，包括網路安全責任的相關政策；同時，支持和監督網路安全專案；並且諮詢法律顧問等專家，提供與省級或聯邦法令的外部規範。

- 發展相關政策與標準；

網路安全政策用來說明員工在網路安全議題上，可從事或不可從事的行為，例如是否允許員工透過公司網路接取社群媒體或網際網路。網路安全政策有助於幫助員工了解自己的角色與責任。

- 建立網路安全計畫；

每家公司都應該發展自己的網路安全計畫，網路安全計畫可識別出最基礎的網路安全控制底線，同時針對需要額外防護的資產，增加對威脅、風險以及實

施安全策略之相關細節。加拿大網路事件應變中心(CCIRC)擁有相關資源可協助各組織規劃其網路安全政策。網路安全計畫應包含對於敏感資訊的標記、處理、儲存、傳輸與銷毀等相關安全規範。

- 編列網路安全預算。

網路安全控制應於組織發展初期即將相關措施納入考量，並且長期存在於組織的生命週期之中。組織應將網路安全編列為整體預算中的一部分，組織編列年度計畫與預算時，均應考量網路安全相關活動。有些政策或內部文件可於組織內部成本支應，但有部份額外的安全措施須向外部購買，並可能牽涉每年年度費用，例如一次性費用、防毒軟體的每年年費等。對於組織的資源分配，可能會分布在安全工具的固定成本、網路安全資源的年度更新費、諮詢與訓練成本、稽核或驗證費以及偶發成本等。

三、 加拿大網路安全推動策略

為有效確保政府外部單位與加拿大公民的網路安全，故加拿大政府公布之 2010-2015 網路安全策略行動方案中(請參見表 4-5 及 4-6)，建立相關推動策略，包括建立新的重大網路事件協調處理流程、吸引關鍵基礎設施服務商採用由國家網路安全策略建立的安全機制、吸引各級政府跟進網路安全議題並積極參與改善其網路安全、協助政府外部的重要系統制定網路安全夥伴專案，提供實際支持等。

同時，加拿大政府亦持續改善 CCIRC 的能力，支持政府外部系統；另外，加拿大也持續提升研發能力、積極參與國際社群。

表 4-5 加拿大網路安全策略行動方案：政府外部之網路安全防護

行動方案	時間表	工作項目	主導單位
建立新的重大網路事件協調處理流程	2012 年開始	建立網路事件管理架構	加拿大公共安全部
吸引加拿大關鍵基礎設施的擁有者與	2010 年開始	提供網路安全說明給所有的網路	加拿大公共安全部

行動方案	時間表	工作項目	主導單位
運作者採用由國家網路安全策略和行動方案所建立的安全機制	2013 年開始	發展和實施相關策略，吸引高階經理人採用	加拿大公共安全部
吸引省級與縣市政府跟進網路安全議題，讓各級政府積極參與改善其管轄下系統之網路安全	2011 年開始	建立聯邦、省級與各縣市助理副首長之網路安全委員會	加拿大公共安全部
		取得安全許可，並提供簡報給國家資訊長資訊保護分組委員會以及各省、縣市政府代表	加拿大公共安全部
		建立與實施資訊共享規劃與協定	加拿大公共安全部
	2001 年開始	在資深官員網路犯罪工作小組委員會下運作聯邦、省與各縣市政府之溝通協調	加拿大司法部
為政府外部的重要系統制定網路安全夥伴專案，以提供實際支持給該系統擁有者或經營者	2010 年開始	於全國各地舉辦研討會，提高產業系統對潛在威脅之認識與了解	加拿大公共安全部與加拿大皇家騎警
		建立工業控制系統的實驗室專案與測試環境：國家能源基礎設施測試中心（National Energy Infrastructure Test Center）	加拿大公共安全部、加拿大自然资源部、加拿大皇家騎警與加拿大國防研究機構

行動方案	時間表	工作項目	主導單位
		運作工業控制系統的實驗室專案與測試環境	加拿大公共安全部、加拿大自然資源部、加拿大皇家騎警與加拿大國防研發機構
		發展與實施捐助計畫	加拿大公共安全部
		與重要系統的擁有者與電信業者協商，設計與實施其他專案	加拿大公共安全部
改善加拿大網路事件應變中心(CCIRC)的能力，以支持加拿大政府以外之外部系統			
增進 CCIRC 的能力	2012 年開始	增加 CCIRC 運作時間達每周七天、每日 15 小時	加拿大公共安全部
	2011 年開始	投資 CCIRC 的技術能力，包括培訓、分析系統、處理程序、自動化與技術等。	加拿大公共安全部
改善 CCIRC 能力，協助重要系統的擁有者與經營者改善其網路安全態勢	2011 年開始	優化與更新 CCIRC 的授權，聚焦於向政府以外的重要系統提供產品和服務	加拿大公共安全部
		更新 CCIRC 的標準程序相關政策，提供高等級的協助給用戶，包括擴大其運作業務。	加拿大公共安全部

行動方案	時間表	工作項目	主導單位
		在關鍵基礎設施的閘道器內啟動 CCIRC 的社群入口網站	加拿大公共安全部
		運作 CCIRC 的社群入口網站	加拿大公共安全部
		建立 CCIRC 與加拿大通訊安全機構間的人員交流	加拿大公共安全部與加拿大通訊安全機構
		提供重要的測試設施，以提高 CCIRC 的能力，進行技術研究與分析	加拿大公共安全部
確認與評估加拿大網路安全政策在政策面與實務面的落差	2011 年開始	提供相關建議給加拿大政府	加拿大公共安全部
提升研發能力			
支持網路安全研究與發展，以提升技術能量、改善網路安全	2011 年開始	提供資金於創新系統（包含學術界），發展新的網路安全技術解決方案	加拿大國防研發機構
建立網路安全的學術參與計畫，提升網路安全在社會科學領域上的力量與凝聚力。	2012 年開始	舉辦關鍵基礎設施和網路安全議題的學術研討會	加拿大公共安全部
		委託網路安全相關研究	加拿大公共安全部
參與國際社群			

行動方案	時間表	工作項目	主導單位
發展加拿大與美國的網路安全行動計畫，提升加拿大網路安全能力，並改善雙方共享基礎設施的網路安全	2012 年開始	在跨國行動方案下，發展加拿大-美國的網路安全行動方案	加拿大公共安全部
	2010 年開始	實施加拿大-美國的網路安全行動方案	加拿大公共安全部
與關係密切的盟邦與夥伴共同合作，提升加拿大在網路空間的利益，促進開放、可互通性、安全與信賴度。	2010 年開始	長期指派外交人員於聯合國日內瓦辦事處，專門處理網路安全議題	外交與國際貿易部
		將加拿大定位為聯合國內為聯合國秘書長整備重要研究工作的 15 個國家之一。	加拿大公共安全部、外交與國際貿易部及加拿大國防部/軍方
		在國際協同範圍內採取定期政策與業務作業	加拿大公共安全部、外交與國際貿易部及加拿大國防部/軍方
與國際組織和外國政府共同合作，改善其網路安全能量，藉以提升加拿大保障共享基礎設施安全	2012 年開始	與安全理事會在內的區域合作夥伴合作，包括歐洲組織、東南亞區域論壇和美洲國家組織等。	加拿大公共安全部及外交與國際貿易部

行動方案	時間表	工作項目	主導單位
的能力。		主辦美洲國家組織的研討會，與相關國家共享各國網路安全策略的實務與發展	加拿大公共安全部
建立架構以確保網路空間的相關活動，符合外交政策、國際貿易與安全之目標	2012 年開始	建立網路安全外交政策	外交與國際貿易部
改善政府在國際網路議題上的溝通協調	2011 年開始	建立與維護對國際網路議題的國際事務工作小組	由外交與國際貿易部、加拿大公共安全部、加拿大司法部與加拿大工業部輪流擔任輪值主席
參與聯合國網路犯罪相關國際研析	2010 年開始	參與聯合國對於網路犯罪的研究	加拿大司法部及外交與國際貿易部

資料來源：加拿大公共安全部

表 4-6 加拿大網路安全策略行動方案：提升加拿大公民的網路安全防護

行動方案	時間表	工作項目	主導單位
協助確保加拿大公民的網路安全	2011 年開始	建立與行銷廣告、合作推廣、網站、社交媒體、民意參與、展覽與特別活動、內部溝通之相關策略	加拿大公共安全部

行動方案	時間表	工作項目	主導單位
		實施通訊策略	加拿大公共安全部
	2011 年 開始	進行公眾輿論研究，評估加拿大公民的網路安全意識、態度與行為	加拿大公共安全部
	2011 年 開始	建立全國性的公眾宣傳活動，透過網站、社交媒體與媒體活動，建立公眾意識。	加拿大公共安全部
	2011 年 開始	建立與其他聯邦組織的夥伴關係，包括國內與國際利害相關人等，增加觸及率、頻率以及對目標受眾的影響	加拿大公共安全部
	2011 年 開始	與相關部門、非營利以及政府組織，例如國土安全部等，建立夥伴關係	加拿大公共安全部
	2012 年 開始	進行對網路安全環境威脅的次級資料分析，以提供公眾意識	加拿大公共安全部
網路犯罪措施			
建立網路犯罪防制中心，提升對網路犯罪趨勢的分析與意識，包含新的評估方式來衡量和統計分析	2011 年 開始	建立網路犯罪防制中心	加拿大皇家騎警
		發展及時回應機制，透過分析網路犯罪威脅與方法	加拿大皇家騎警

行動方案	時間表	工作項目	主導單位
提出加拿大網路犯罪策略草案	2012 年 開始	發展網路犯罪策略草案，處理包括網路犯罪、詐欺、組織犯罪和識別威脅等。	加拿大皇家騎警
改善法案工具，提升加拿大公民在網路空間的保護度	2010 年 開始	建立加拿大反垃圾郵件草案	加拿大工業部
	2011 年 開始	建立加拿大個人資訊保護法案	加拿大工業部

資料來源：加拿大公共安全部

從 2011 年開始，加拿大政府開始推動網路安全宣導活動，公共安全部每年 10 月會配合國際活動，舉辦「網路安全意識月」(Cyber Security Awareness Month)，以提升所有加拿大國民的網路安全意識。2016 年網路安全月的主題依照各週區分如下表 4-7。

表 4-7 加拿大 2016 年網路安全月各週主題

週次	日期	主題
第 1 週	10/3-7	網路安全意識月相關活動啟動
第 2 週	10/10-14	中小企業網路安全
第 3 週	10/17-21	網路犯罪
第 4 週	10/24-29	物聯網與連網社會
第 5 週	10/31	虛擬與關鍵基礎設施

資料來源：加拿大公共安全部

加拿大網路安全的緊急應變機制與通報機制主要由加拿大網路事件應變中心 (CCIRC) 負責，當關鍵基礎設施服務供應商、企業、各級政府發現關於網路安全威脅或事件的相關資訊時，應盡速通報 CCIRC，CCIRC 也會針對潛在、有可能發生或

真實已發生的網路安全威脅、漏洞或可能影響關鍵基礎設施的事件，向相關成員發出警報與建議。CCIRC 於公共安全部的網頁建立通報機制²²⁴，機制中針對網路安全議題區分如下：

- 垃圾郵件 (Spam)：由垃圾郵件通報中心 (Spam Reporting Centre，簡稱 SRC) 主責；
- 詐欺類：由加拿大反詐欺中心 (Canadian Anti-Fraud Centre，簡稱 CAFC) 主責；
- 網路犯罪：由加拿大皇家騎警處理；
- 剝削兒少：由加拿大兒少保護中心處理；
- 對關鍵基礎設施、企業與各級政府之威脅：由 CCIRC 主責。

加拿大政府於 2013 年 8 月發布加拿大網路事件管理架構 (Cyber Incident Management Framework for Canada，簡稱 CIMF)。網路空間提供許多優點給加拿大國民，但是對網路技術的依賴，導致更可能受到那些攻擊數位基礎設施人士的傷害，破壞國家安全、經濟繁榮與公共安全。加拿大政府於 2007 年建立緊急管理架構 (Emergency Management Framework，簡稱 EMF)，確保各省級政府、地方政府都有一致的緊急管理計畫，同時明訂各級政府均具備處理緊急管理與公共安全議題之責。國家緊急應變系統 (National Emergency Response System，簡稱 NERS) 負責實施 EMF 相關規範，協調聯邦、省與區域縣市政府的緊急應變事宜，並促進各層級政府、民間企業、非政府部門與國際利害相關人間的協調合作。

與常見的自然災害、交通事故、公共衛生突發事件與關鍵基礎設施不同，網路安全事件更為複雜性，因為網路空間獨立於地理邊界與實體邊界之外。現有網路空間由各級政府與民間企業設計、監管、維護、運作、擁有與保障。EMF 與 NERS 主要提供整體框架的指導，以處理重大網路安全事件，而 CIMF 架構則專門針對網路事件設定管理架構，以補充現有緊急管理政策之不足。

CIMF 架構涉及各省、縣市政府、關鍵基礎設施擁有者與電信業者及其他公部門

²²⁴ Public Safety Canada, “Report a Cyber Security Incident”.

與民間企業合作夥伴之指導方針，CIMF 設計來補充與配合既有聯邦、省級與縣市政府緊急應變管理計畫與架構，同時也適用於關鍵基礎設施擁有者與電信業者的緊急應變計畫。²²⁵

加拿大公共安全部透過協同合作之方法發展 CIMF，政策制定過程中徵求加拿大網路安全界的意見，並運用既有聯邦、省級與縣市地方政府等各級政府與產業界的結構，希望藉以打造出能因應需求而不斷調整、修改的管理架構。CIMF 並無強制性，採志願加入性質，參考國際上最佳實務作法，所有利害相關人均被鼓勵採用 CIMF 架構來管理網路安全事件，並共享資訊。

參與 CIMF 的組織都必須要負責維護其內部網路安全，相關組織必須要具備強而有效的網路安全能力，該能力必須要與當下產業的最佳實務標準相符。目前許多產業正依照自身需求建立相關資料保護、操作規範與安全標準。對於網路安全適合的相關措施，尚包含事件的緊急回應計畫、軟硬體的安全標準、網路設備的安全標準、對網路日誌（log）的安全稽核監督與分析、災後復原計畫、進階管理的升級程序以及和聯邦政府、各省級、縣市地區政府緊急事件管理機構的聯繫與通訊事務計畫。加拿大網路安全通報架構如下圖 4-3。

²²⁵ Government of Canada, “Cyber Incident Management Framework for Canada”, 2013.

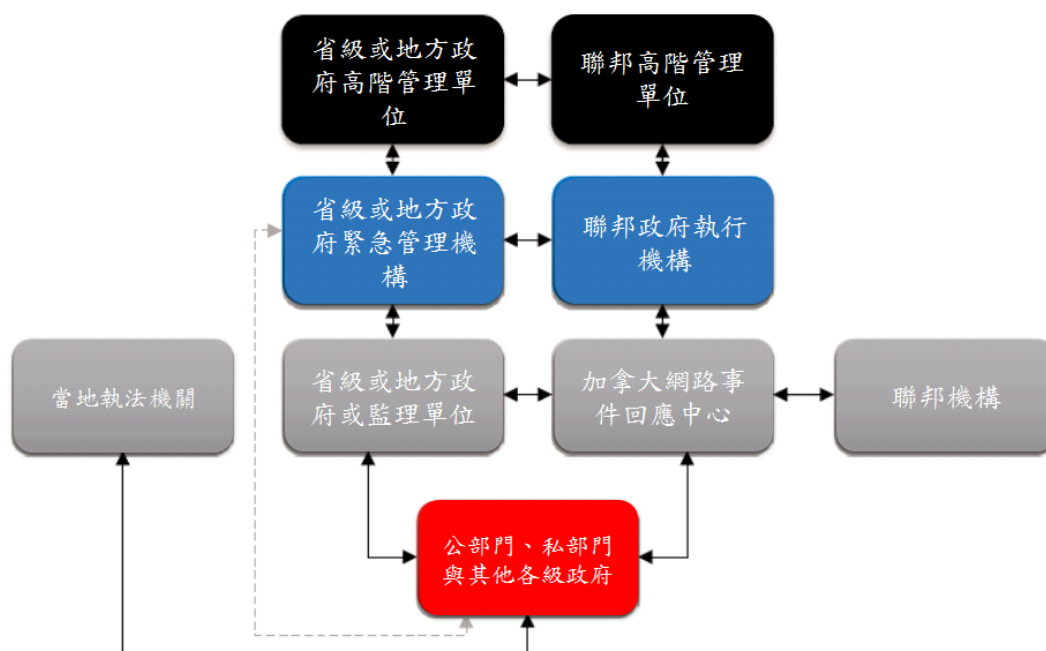


圖 4-3 加拿大網路安全通報架構

資料來源：加拿大公共安全部

CIMF 與聯邦、省級與縣市政府間標準作業程序之關係如下圖 4-4。

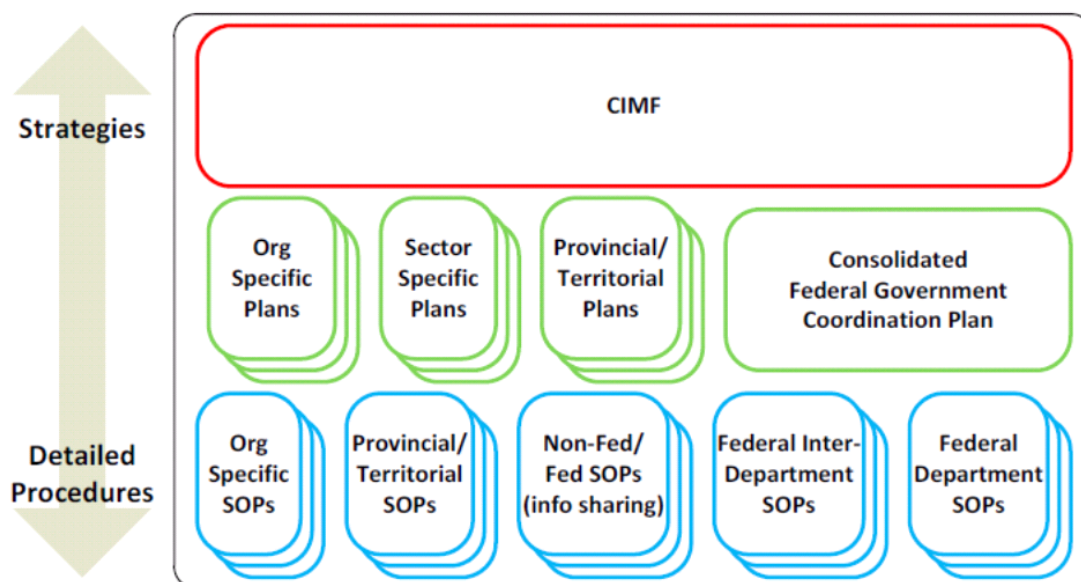


圖 4-4 加拿大網路安全架構與各級單位標準作業程序關係

資料來源：加拿大公共安全部

根據 CIMF 的要求，每個參與其中的組織都必須要擁有能夠預防、減輕、整備與回覆因應網路事件的相關計畫。各級政府與關鍵基礎設施部門也應該根據相關計畫，確保有效的溝通協調。聯邦政府則持續努力讓其內部協調機制更有效率。同時，各參與組織也需要詳細的標準作業程序（Standard operational procedures，簡稱 SOPs），包括紀錄技術人員的每日活動，例如通報機制、資訊共享與其他操作相關議題。確保參與者間能達到資訊共享。

CCIRC 則針對影響程度高低，制訂不同等級之影響指標。當網路安全事件發生時，所有參與 CIMF 的組織都必須向 CCIRC 報告，藉由通報機制與資訊共享，才能夠確保主管機關通盤了解影響狀態。CCIRC 則必須要確保通報單位的匿名性，消除可能識別出特定對象的特徵。

主責加拿大網路安全政策的 CCIRC 認為，當網路安全事件發生時，最好的預防方式是確保內部已具備精密且準備充分的相關功能。同時，由於加拿大政府組織架構包含聯邦政府、省政府以及各地方政府，因此從聯邦層級的 CCIRC 主責工作觀察，當網路安全事件發生時，CCIRC 著重於政府整體與外部單位的溝通、協調，做為網路安全政策的專責單位。

加拿大網路安全策略之工作重點從確保公部門系統安全、確保聯邦政府以外系統安全到保障國民線上安全等三大項目。在確保公部門系統網路安全的角度，則重視權責區分，明確訂定各部門應負責之項目，同時也投資研發技術能量，確保聯邦層級的網路安全防護能力與時俱進。另外，加拿大的網路安全策略亦重視網路安全意識之提升，透過舉辦網路安全月的方式，提高所有加拿大國民的網路安全意識。

除了提升對公部門的網路安全能量外，加拿大亦注重於確保關鍵基礎設施的安全性，公共安全部與 CCIRC 重視保障關鍵基礎設施，透過跨部會的方式，由公共安全部主導，確保政府各部門之溝通協調順利，並聚焦於整備政府整體網路安全計畫，完善政府內部的網路安全。同時，公共安全部會定期評量政府網路安全專案的執行成果，確保儲存於政府系統中的個資與數據獲得完善保護。

加拿大亦持續增加對政府網路安全的投資，從 2011 年開始持續至 2016 年底投入 1.55 億加幣雇用專業人士以及購買網路安全設備，另外也透過強化資訊安全架構、建立政府網路安全預防與處理機制、加強軍方網路安全能力與政府相關部門網路安全培

訓與宣導等措施，提升加拿大網路安全防護能量。

另外，加拿大定期諮詢網路安全專業社群對網路安全相關議題之看法，同時積極投入國際社群之參與，與美國等盟邦發展網路安全計畫，透過資訊共享、國際間的溝通協調與研析跨國網路犯罪等方式，提升加拿大網路安全能力，也確保加拿大得以持續掌握網路安全議題的最新發展。

為了促進加拿大各級政府與政府外部機構間的網路安全通報機制的順暢，加拿大建立網路安全事件管理架構（CIMF），讓所有參與者都能夠在一致的架構下管理網路安全資訊，並共享相關資訊。所有參與者也必須要負責維護其內部網路安全，並依照標準作業程序通報 CCIRC。同時，參與者也必須要按照 CIMF 的規範，建立相關資料保護、資訊安全標準計畫、災後復原計畫、升級程序以及和相關單位的溝通聯絡計畫等。

第三節 歐盟

根據歐盟統計局（Eurostat）所公布的網路安全報告指出，截至 2014 年 10 月，有至少 25% 的歐盟民眾曾經出現電腦病毒感染、個人資料遭駭、財務損失或兒童登錄不當網站等網路安全問題。同時，歐盟民眾對網路資訊安全存有極大的疑慮，約有 19% 的歐洲人不願意透過網路來購物；有 18% 的民眾拒絕使用網路銀行或相關網路金融服務；有 13% 的民眾除了自家裡的網路外，會避免在戶外或其他地方使用手機上網或是利用其他無線網路²²⁶。由於網路安全問題往往與資通訊設備的安全性有極大的關連。儘管歐盟的會員國本身有優良的資訊安全服務、技術與設備製造商，但大部分的歐洲企業及政府機關仍會考量成本因素，使用非歐盟國企業所生產製造的網路及資通訊設備。因此歐盟執行委員會(European Commission)期望以網路安全策略來約束會員國盡量使用歐盟業者的網路及資通訊設備，並針對非歐盟地區的資通訊設備業者，訂出一套監督與治理規則。

一、 歐盟網路安全政策規範與組織架構

²²⁶ EU, “Special Eurobarometer 423 CYBER SECURITY REPORT”, 2014/10.

(一) 歐盟網路安全策略及國家網路安全計畫

近年歐盟網路安全建設透過多項決議、指令、建議、規則、報告等方式，不斷完善網路安全法律體系。2010 年歐盟通過《內部安全策略(Internal Security Strategy)》²²⁷來提高網路安全水平，該策略除規定在 2013 年前需設立歐盟網路犯罪中心(EU cybercrime centre)外，並要求各會員國和歐盟應有一運作良好的電腦應急小組(Computer Emergency Response Team，簡稱 CERT)，另鑒於網路犯罪事件的通報是至關重要的，建議開發設置「歐洲資訊和預警系統(European Information and Alert System，簡稱 EISAS)」，作為告警平台和網路聯絡點。同時，該策略也促進了在歐盟層面上對網路事件回應的演練。歐盟於 2010 年 5 月在「Europe 2020 策略(Europe 2020 Strategy)」²²⁸旗艦計畫下，發布「歐洲數字議程(2010 Digital Agenda for Europe)」，強調數位社會中對於信任和安全的需求，進而促使歐盟擴大 CERT 網路，承諾為歐盟機關設立電腦應急小組(CERT)，作為加強歐盟高水平網路和資訊安全政策。

2013 年歐盟有鑒於網路威脅所帶來的負面效應，為進一步保護網路與資訊系統以確保網路經濟的運行與繁榮，歐盟執行委員會與歐盟外交暨安全政策高級代表(High Representative of the Union for Foreign Affairs and Security Policy)，於 2013 年 2 月 7 日共同發布「歐盟網路安全策略(Cybersecurity Strategy of the European Union)」²²⁹。新的歐盟網路安全策略，以「開放、安全與可靠網路空間 (An Open, Safe and Secure Cyberspace)」為主軸，對應所面臨的網路安全威脅，並提出五項重要策略，包括：

1. 實現網路韌性(Achieving cyber resilience)

此策略重點在於推動政府與私有企業建立資安防禦機制與有效互助合作。包含建立最低網路安全要求準則，建置整體網路安全預防、偵測、處理及回應機制，建置各界網路安全資訊分享與互助合作方式，提升整體網路安全認知能量。

2. 徹底減少網路犯罪(Drastically reducing cybercrime)

此策略重點在於如何讓日益猖獗的網路犯罪大幅降溫。建立有效及重罰法則為第

²²⁷ EU, "Internal security strategy for the European Union Towards a European security model", 2010/3.

²²⁸ EU, "Europe 2020 strategy", 2010/5.

²²⁹ EU, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", 2013/2.

一要務；其次在於提升執法單位針對網路犯罪的辦案能量，包含裝備與人員能力的提升；最後則是精進歐盟整體的執法協調合作機制。

3. 針對一般安全暨防禦政策，發展網絡防禦政策和能力(Developing cyber defence policy and capabilities)

網路威脅通常為多面向，影響的層面及對象可能非常廣泛，但各層面及對象所遵循的安全法規及準則各有不同，如何避免資源重複浪費，在各種不同之安全政策中，整合出一套各方皆可適用的網路安全政策為此策略的重點。歐盟初步計畫先與「北大西洋公約組織(North Atlantic Treaty Organization, NATO)」進行討論如何整合雙方的安全政策及資安防禦機制，朝一致化目標前進。

4. 針對網路安全發展產業和技術性資源(Developing the industrial and technological resources for cyber security)

歐盟自身有極好的資安業者、技術及設備製造商，但大部分的歐洲企業及政府機關仍使用歐洲以外地區企業所生產的網路及資安設備。此策略的重點在歐盟希望能儘量使用歐盟國家所生產的網路及資安設備，針對其他地區的資安與設備業者，也能訂出一套監督與治理規則。另外，投入資源加速歐盟相關業者研發網路安全設備、資安服務與技術，希望在網路安全方面能逐步做到自給自足，不再需要自歐盟以外地區採買網路安全相關設備與服務。

5. 為歐盟建立一個完整的國際網絡空間政策與促進歐盟核心價值(Establishing a coherent international cyberspace policy for the EU and promoting core EU values)

此策略的重點在如何跟國際資安組織、相關合作夥伴、政府機關與私人企業進行溝通及建立共識，以利建置及推動網路安全政策及更緊密的策略合作。

為了達成歐盟網路安全策略所形塑的優先事項及策略目標，歐盟執委會於 2013 年 2 月提出一項網路及資訊安全指令的提案，即為《網路安全指令(Cyber Security Directive)》或稱《NIS 指令(Directive on Network and Information Security, NIS Directive)》²³⁰。該提案歷經兩年協議，歐洲議會(Parliament)與歐盟理事會(Council)在 2015 年 12

²³⁰ EU, “DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6
261

月 7 日達成共識，並於 2016 年 7 月 6 日由歐洲議會正式通過，各會員國須在 2018 年 5 月將該指令轉入國內法令，NIS 指令也將成為歐盟所有會員國都必須遵守的第一個網路資訊安全法令。NIS 指令旨在確保歐盟境內網路和資訊安全高度的共同水平，指令主要內容包括：

1. 會員國必須制定一個國家層級的網路及資訊安全(NIS)策略和合作計畫。其中，國家相關的措施應涵蓋：提高國家對風險和應對措施的意識、公民營部門合作機制，以及向經濟體發出安全預警機制等。例如，英國即在 2010 年發布「國家網路安全策略(National Cyber Security Strategy)」和建立「網路安全資訊共享夥伴關係(Cyber Security Information Sharing Partnership, CiSP)」來因應指令的要求。
2. 會員國必須指定國家層級的「主管機關和單一窗口」，作為監測指令轉入國家措施的適用情況並接收事件通知，並評估與執行相關合規性要求。
3. 會員國必須指定一個或多個電腦機應急小組 (Computer Emergency Response Teams, CERT)，其中包括：
 - 監測國家層級的事件；
 - 向經濟體提供有關風險和事件的預警(early warnings)；
 - 提高公眾意識；
 - 規範相關作法、風險處理和分類方案。
4. 歐盟將組建一個由國家主管機關、CERT 和其他機構等構成的合作網路(cooperation network)，執行包括：
 - 傳遞關於風險和事件的早期警告；
 - 制定協調一致回應；
 - 與執法機關合作。
5. 公家行政機關和市場經營者應對網路安全採取適當的技術和組織措施，並對營運的控制和使用之網路和資訊系統安全性進行管理。這些當事方應事先向主管機關通報嚴重事件，違規事件揭露不可拖延。
6. 主管部門有權對公家行政機關和市場經營者執行法律，包括要求他們進行安全審核(security audits)。
7. 會員國將要求推動安全的標準和規範。
8. 如果公家行政機關和市場經營者未能達到適當的安全水平，將實行制裁(Sanctions)。

另外，對於某些重大基礎設施領域的市場經營者(金融服務、交通、能源或醫療)、

資訊社會服務的參與者(APP 商店電子商務平台、線上支付、雲端運算、搜尋引擎、社群網路)和公家行政機關必須在其核心服務上，進行風險管理及通報重大網路安全事故並做成報告。同時，配合 NIS 指令的實施歐盟已著手展開各種涉及網路安全指令相關主題的法律改革行動，其中包括：

1. 一般資料保護規則 (General Data Protection Regulation，簡稱 GDPR)。

GDPR 將取代《1995 年資料保護指令(Data Protection Directive 1995)》。同時 GDPR 修改法律對資料控制者(data controllers)和資料處理者(data processors)進行處理個人資料安全的方法，並納入與《網路安全指令》(採取適當的技術和組織安全措施)所載之資料安全性的相同責任，以及對違反披露和監理審計提出相關要求。

2. 支付服務 2 指令 (Payment Services 2 Directive，簡稱 PSD2)。

PSD2 指令也映對網路安全指令的框架在管理、違反披露(breach disclosure)和監理審核方面的責任條款。

現行歐盟安全相關法律和未來發展，如表 4-8 所示。

表 4-8 歐盟安全法律框架的合併

規範	一般資料保護 (General data protection)	特定資料保護 (電子隱私) Specialised data protection (e-privacy)	網路安全(Cyber security)	支付服務和信託服務 (Payment services and trust services)
重點	關注重點： 處理個人資料的安全	關注重點： 透過電子通信傳送的個人資料的安全	關注重點： 網路和資訊系統的安全	關注重點： 支付服務、信託服務和電子身分認證的安全
現行	法律： 資料保護指令 1995 (Data Protection Directive 1995)	法律： 2002 年隱私和電子通信指令 (2009 年修訂) (Privacy and Electronic Communications Directive 2002 (as amended in 2009))	法律： 電子通信框架指令 (2009 年修訂) (Electronic Communications Framework Directive (as amended in 2009))	法律： 2007 年付款服務指令 (PSD) (Payment Services Directive 2007 (PSD)) ; 1999 年電子

未來				簽名指令 (ESD) Electronic Signatures Directive 1999 (ESD)
	監理： 資料控制者 (Data controllers)	監理： 電信公司和 ISP 業 者 (Telecommunications companies and Internet Service Providers)	監理： 電信公司和 ISP 業 者 (Telecommunications companies and Internet Service Providers)	監理： PSD：支付服 務提供商 (Payment Service Providers); ESD：驗證 服務提供商 (Certification Service Providers)
	要求： 對安全採取適當的 技術和組織措施。	要求： 對安全採取適當的 技術和組織措施， 違反披露和監管審 核。	要求： 對安全採取適當的 技術和組織措施， 違反披露和監管審 核。	要求： PSD：防止對 個人安全功能 支付工具的非 法接取; ESD：使用適 當的技術和程 序手段來保護 簽名設備。
	法律： 擬議的一般資料保 護規則(GDPR) (General Data Protection Regulation)	法律： 無變更	法律： 擬議的網路安全指 令(NIS) (Cyber Security Directive)	法律： 擬議的支付服 務指令 2 (PSD2)；擬 議的電子識別 和信託服務規 則 (EID & TSR)
	監理： 資料控制者和資料 處理者	監理： 無變更	監理： 關鍵基礎設施和服 務，包括支付服務 提供商和公有機關	監理： PSD2：支付 服務提供商; EID & TSR： 信託服務提供 商
	要求： 對安全採取適當的 技術和組織措施，	要求： 無變更	要求： 對安全採取適當的 技術和組織措施，	要求： PSD2：防止 非法接取付款

	違反披露和監管審核。		違反披露和監管審核。	工具的個人化安全功能、違規披露、提供年度風險報告，強化客戶認證。 EID & TSR： 對安全採取適當的技術和組織措施，違規披露和提供審計證據予監理機關。
--	------------	--	------------	---

資料來源：THOMSON REUTERS 2017

（二） 歐盟網路資訊安全防护應變主責機關

通訊網路及資訊系統已成為歐盟經濟與社會發展的基礎，兩者的安全性與可用性，愈來愈受到社會關注。受惠於歐洲寬頻市場的高度競爭，消費者已將寬頻網路視為日常生活要素，因此資安議題更顯重要。由於過去歐盟會員國對於網路和資訊安全問題上的合作是在自願的基礎上，沒有機制來保證歐盟能有效的資訊共享。特別是各會員國在網路和資訊安全的能力差異很大。因此，歐盟委員會除透過網路和資訊安全高層次的指令來解決這個問題外，並在 2004 年 3 月成立「歐洲網路及資訊安全局（European Network and Information Security Agency，簡稱 ENISA）」，以確保區域內的網路及資訊安全，並發展一個有利於民眾、消費者、企業及公部門組織的資安文化，從而促進歐盟市場順利運作。ENISA 的主要任務，包括：第一，與會員國及私部門緊密合作，提供軟、硬體產品資訊安全之諮詢與解決方案；第二，收集並分析歐洲資安事件與潛在風險之情資，提高風險評估與解決資安風險的能力，並強化處理資訊安全威脅的技術能量；第三，提高對其他資訊安全領域的監控，特別是提升開發中國家的國營企業或私人公司之資訊安全意識。

ENISA 在 NIS 指令的執行中亦扮演重要的角色，任務包括支援歐盟機構、會員國與產業界，快速對網路威脅與資訊安全問題做出反應。也被要求在執行任務中協助各國間成立的合作小組。此外，更透過指令要求 ENISA 協助成員國與執委會，提供他的專業意見和建議等。ENISA 策略主要有五個面向：

1. 提供關鍵網路設施和資訊安全問題之資訊和專業知識。
2. 制定和執行歐盟網路政策。
3. 建立歐盟間跨國支援能力。
4. 培育網路與資訊安全社群的網路演習、協調與支援。
5. 促進各國間的合作關係。

由於 ENISA 在建立之後網路發展情勢有顯著的演變，其任務和目標應該因應新發展做出調整，故歐盟執委會也在 2017 年 9 月開始重新審視其設立之法律依據以應對新情勢發展。

二、 歐盟關鍵基礎設施保護

由於關鍵基礎設施是維護社會功能重要的資產或系統，歐盟認為對於關鍵基礎設施的破壞，無論來自天然災害、恐怖主義、犯罪活動或惡意行為的破壞，可能對歐盟的安全和公民的福祉產生重大的負面影響。為此，歐盟自 2004 年起陸續推動會員國之「關鍵資訊基礎設施保護(Critical Information Infrastructure Protection, CIIP)」²³¹。2005 年歐盟正式發布「歐盟關鍵基礎設施保護計畫 (European Programme for Critical Infrastructure Protection, EPCIP)」²³¹綠皮書，設定改善歐洲關鍵基礎設施保護的整體框架，並在 2008 年 12 月 8 日立法通過「理事會指令 2008/114 / EC (Council Directive 2008/114/EC)」²³²，建立一個識別和指定「歐洲關鍵基礎設施 (European Critical Infrastructures, ECI)」的程序，以及評估改善其保護需求的通用方法。

同時，為建立關鍵基礎設施資訊交流平台，2008 年 10 月歐盟發布一項理事會決議的「關鍵基礎設施預警資訊網路(Critical Infrastructure Warning Information Network, 簡稱 CIWIN)」提案²³³，旨在協助會員國和歐盟委員會交流分享關於威脅、脆弱性和適當措施及策略的資訊，以減輕支持關鍵基礎設施保護 (Critical Infrastructure Protection, CIP) 的風險。CIWIN 網路已發展成歐盟委員會用來保護公眾網路資訊和通信的系統平台，為歐盟 CIP 成員提供交流和討論 CIP 相關資訊的機會，以及為所有歐

²³¹ EU, “Green Paper on a European programme for critical infrastructure protection”, 2005/11.

²³² EU, “COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”, 2008/12.

²³³ European Commission 官網.

盟會員國和相關產業部門的經濟活動研究交流最佳的實務作法。

為強化重要的資訊和通信技術基礎設施 (ICT) 之安全性和應變力，2009 年 3 月 30 日歐盟委員會通過「通信關鍵資訊基礎設施保護 (Communication on Critical Information Infrastructure Protection)」計畫²³⁴，制定 CIIP 行動計畫 (CIIP action plan)，以保護歐洲免受大規模的網路攻擊和網路破壞，激勵和支持會員國和歐洲層面具有高度的準備、安全和應變能力。歐盟並在 2011 年 3 月 31 日啟動新一代的關鍵資訊基礎設施保護計畫²³⁵，將計畫焦點集中在全球化的挑戰，著重在歐盟成員國與全球其他國家的合作，與相互之間的合作關係。同時，為了達成這個目標，歐盟執委會訂定行動綱要，如圖 4-5 所示。



圖 4-5 歐盟關鍵基礎設施保護行動綱要

資料來源：本計畫整理

歐盟關鍵資訊基礎設施保護行動綱要內容，包括：

1. 準備和預防(Preparedness and prevention)：利用會員國論壇(European Forum for Member States, EFMS)分享資訊及政策。

²³⁴ EU, “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, 2009/3.

²³⁵ EU, “Achievements and next steps: towards global cyber-security”, 2011/3.

2. 偵測和回應(Detection and response)：發展資訊分享及警示系統，建置民眾、中小型企业與政府部門之間的資訊分享、警示系統。
3. 緩和及復原(Mitigation and recovery)：發展會員國間緊急應變計畫，組織反應大規模網路安全事件，強化各國電腦緊急反應團隊的合作。
4. 國際與歐盟的合作(International cooperation)：根據歐盟會員國論壇所制訂的，歐洲網際網路信賴穩定指導原則和方針，進行全球大規模網路安全事故的演習。
5. 制訂資訊通信技術的標準(Criteria for European Critical Infrastructures in the ICT sector)：針對關鍵資訊基礎設施制訂技術標準。

2016 年 1 月歐洲網路與資訊安全局 (ENISA) 也發布「會員國對於實施關鍵基礎設施保護的盤點、分析與建議(Stocktaking, Analysis and Recommendations on the Protection of CIIs)²³⁶」，指出要建構有效的國家 CIIP 制度，可依各國情境出發，並從下列不同領域之交互影響來評估其 CIIP 成效，如下圖 4-6 所示，包括：

1. 政府政策及策略發展(Policy)：包括策略優先性、目標、措施、公私利害關係人協作夥伴(Public-Private Partnership, PPP)之角色與責任(Roles and Responsibilities)定義。
2. 治理架構(Governance structure)：建立明確角色與責任，包括發展 CIIP 責任之公共機構或延伸現行機構之責任。也包括建立溝通通道、與企業合作機制。
3. 法律與規範(Legislation)：包括公私部門須遵循之安全標準，如法定式的安全標準、事件報告、安全作業規範等。
4. 風險管理及消除措施(Risk management and mitigation measures)：執行國家層級、部門層級之資安風險評鑑、因應措施及安全稽核作業。
5. 緊急準備度(Emergency preparedness)：資安事件處理程序，包括例行演練、緊急事件處理程序、CERT 危機處理中心機制、對 CII 提供者之資安專家建議與諮詢。演練可包括特定部門(sector-specific)、跨部門(Cross-sectional)、跨國(International)演練。
6. 威脅知識及資訊分享(Threat intelligence and information sharing)：威脅監測與資訊分享、散播(Information Sharing and Analysis Centers, ISAC)公私部門合作機制。

²³⁶ EU ENISA, “Stocktaking, Analysis and Recommendations on the Protection of CIIs”, 2016/1.



圖 4-6 影響關鍵基礎設施保護(CIIP)成效之因素

資料來源：ENISA

ENISA 報告亦建議 CIIP 良好之實務準則，至少應包括：強化利害關係人公私協作夥伴關係、強化資訊分享機制、強化電腦安全事件處理小組（CSIRT）社群合作機制、強化風險評鑑、強化網路危機管理機制、適切之一般性法律架構等，且負責 CIIP 的國家機構之主要任務通常至少應建立包括：事件報告之聯絡點（Point of Contact）、組織及進行 CIIP 相關演練及訓練、CII 提供者之諮詢顧問服務、事件處理（incident response）、政策或策略研議、國家 CII 安全監測、提出規範或立法建議、國家 CSIRT 監督等措施。

三、 歐盟網路安全推動策略

(一) 建立歐盟網路安全法律責任與通報義務

歐盟自 2013 年開始推動網路安全的綜合性立法，最終在 2016 年 7 月 6 日正式通過「確保歐盟統一、高水準網路與資訊系統安全之相關措施」的網路安全指令(Network and Information Security Directive，簡稱 NIS)。NIS 指令是歐盟網路安全立法政策的基石。指令涵蓋產業包括：能源、運輸、銀行、金融市場基礎設施、衛生、水源供給和配送、數位基礎設施和數位服務提供商等。NIS 指令除要求會員國：採取一個國家網路安全策略；指定具授權的國家主管機關，來評估和執行合規性(compliance)；指定電腦安全事件回應小組（CSIRT）監測威脅；參與新的合作小組，以支援會員國之間的策略合作和資訊交流。並對公家行政機關和市場電信業者建立網路安全的法律責任，要求他們採取適當的技術和組織措施進行網路安全，重大安全事件須向主管機關通報(notify)。當確認需要通報時，須考慮，包括：受影響的用戶數量、事件持續時間、地理範圍、破壞程度以及潛在的經濟和社會影響。如果主管機關認為通知公眾能有助於防止或限制事件的影響，則有權酌情決定。

由於 NIS 指令將重要資訊系統營運者區分為「基本服務營運者(operators of essential services)（基本服務由各會員國認定）」和「數位服務提供者(digital service providers)」。其中，基本服務營運者有義務通報「對其所提供基本服務的連續性產生重大影響的事件」；而數位服務提供者也有義務通報「在歐盟內提供服務的重大影響事件」，其範圍也包括非歐盟數位服務提供商。如果非歐盟的數位服務提供者提供基於歐盟(EU-based)的服務，公司必須指定一代表在歐盟範圍內代理其行事。

此外，歐盟也針對銀行在內的支付服務提供商（Payment Service Providers, PSP）要求其依據《支付服務 2 指令（PSD2）》進行網路安全義務。對於受影響的組織將有義務向監理機關報告安全事件(security incidents)。如果安全事件可能影響客戶的財務利益，那麼這些客戶也必須被通知。

(二) 擴大資料保護範圍及管理力度

隨著科技進步和全球化的發展，資料蒐集、接取、使用的方式已經發生深刻變化，

快速的科技發展為個人資料保護帶來了全新的挑戰，為擴大資料保護的範圍及加強資料保護管理的力度，歐洲對於現行資料保護法進行了重大的改革。2016 年 4 月 27 日歐盟通過《一般資料保護規則 (General Data Protection Regulation, GDPR)》取代原《資料保護指令(Data Protection Directive 1995)》。GDPR 將於 2018 年 5 月生效並直接適用於各會員國，成為歐盟境內個人資料保護的單一規則。GDPR 規則主要是對個人資料的資料控制者(Data Controllers)和處理者(Data Processors)直接施加安全義務(security obligations)，並強制性要求對個人資料洩漏通報的義務。GDPR 也將「個人資料」擴大解釋為涵蓋可直接或間接過濾出特定對象資訊之資料類型，例如：網路瀏覽器 Cookies、網路 IP 位址或足以辨識特定個人身分或性別之基因、生物特徵或醫療資料等。

同時，GDPR 也增加對歐盟境內及境外業者之符合性要求和資料保護的責任。對歐盟內之資料主體(data subjects)提供商品服務或監測個人行為的非歐盟公司，亦受 GDPR 的規管。各會員國的國家資料保護監理機關(National Data Protection Authorities, NDPAs)能向違規業者施加其全球年營收 4%的巨額罰款或是 2000 萬歐元的罰款，並以數額較大者為準。另 GDPR 也要求業者：

7. 具有“適當”的技術和組織措施，以防止未經授權或非法處理個人資料，防止意外遺失或破壞或損害個人資料。
8. 公司在意識到違規行為的 72 小時內，須將任何個人資料違規事件通報到有關的各國資料保護監理機關(NDPA)。
9. 任何專案一開始或在設立資料處理系統時，就需考慮隱私和安全問題。
10. 並就可能對資料主體(data subjects)產生高風險的任何資料處理，進行隱私影響評估 (Privacy Impact Assessments，簡稱 PIA)。

(三) 推動打擊網路犯罪措施

雖然許多網路威脅超出執法的範圍，但歐盟已試圖推動一系列措施因應網路犯罪：

1. 推動成立網路犯罪公約(Convention on Cybercrime)

2004 年 7 月 1 日正式生效的《網路犯罪公約(Convention on Cybercrime)》是全球第一份處理網路犯罪的指導文件。該公約係由歐洲理事會 26 個會員國與 4 個非會員國(美國、加拿大、日本及南非)在 2001 年 11 月 23 日於布達佩斯簽署通過，包含

三個主旨：

- 提供簽約國實質之法律修正方向與依據。
- 提供執法機構調查與處理犯罪行為之程序規定與依據。
- 建立快速有效的國際合作關係。

網路犯罪公約主要的目標是追求一個共同的刑事政策(common criminal policy)，並透過適當立法和促進國際合作。由於網路攻擊容易跨界，執法機構難以在引渡條件有限的司法管轄區(jurisdictions with limited extradition arrangements)採取行動。因此，透過網路犯罪公約的國際協定，簽署方同意將相關活動（例如蓄意干擾電腦系統）定為刑事犯罪，藉以保護歐盟資訊社會免受網路犯罪。

2. 立法解決對資訊系統的攻擊

2013 年歐盟基於《歐盟運作條約(Treaty on the Functioning of the European Union, TFEU)》第 83 條通過一項《2013/40 / EU 指令》²³⁷，藉以取代 2005 年有關攻擊資訊系統的《理事會框架決議(2005 Council Framework Decision)》。該指令旨在建立對資訊系統攻擊之刑事犯罪和裁罰定義的最低限度規則。指令中定義的主要犯罪行為，包括：非法的接取資訊系統、非法的系統干擾、非法的資料干擾和非法攔截等。此外，針對關鍵資訊基礎設施(CIIP)造成嚴重損害，包括使用殭屍網路(botnets)及犯罪行為，在犯罪組織框架下也將面臨最嚴厲的處罰。

3. 成立歐洲網路犯罪中心(European Cybercrime Centre)

由歐洲刑警組織(Europol)主辦的「歐洲網路犯罪中心(European Cybercrime Centre, EC3)」於 2013 年 1 月成立。EC3 是歐盟打擊網路犯罪的焦點，其作用是支援各會員國之間的業務合作，包括進行聯合網路犯罪調查和分析歐盟的網路威脅。EC3 主要執行網路犯罪任務的範圍，包括：

²³⁷EU, “Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision”, 2013/12/8.

- 組織犯罪集團的犯罪行為
- 對受害者造成的嚴重傷害，例如對兒童的性剝削（Sexual Exploitation）。
- 影響歐盟的關鍵基礎設施和資訊系統。

歐洲網路犯罪中心的成立，將提高歐盟打擊網路犯罪的能力，進而維護一個自由、開放和安全的網際網路，以保護歐洲民眾和企業不受網路犯罪的威脅。

（四）舉辦歐洲「網路安全月」活動，提高網路安全意識

歐盟為提高民眾網路安全意識，保護歐洲數位經濟繁榮發展，根據網路安全策略和「安全網路計畫（EU Safer Internet Program）（2014—2018）」的要求，於每年10月舉行「歐洲網路安全月（European Cyber Security Month）」通識教育活動。歐洲網路安全月旨在提升公眾網路安全意識，改變公眾對網路威脅的理解，同時通過教育和共用最佳實踐等方式為公眾提供最新的安全資訊。歐洲網路安全月的目標包括：作為《歐盟網路安全策略》的優先任務之一，形成對網路安全的總體認識；為落實《網路與資訊安全指令》提出的要求，形成對網路與資訊安全的具體認識；推動所有用戶更安全地使用網際網路；通過歐洲網路安全月，建立意識提升情況的追蹤記錄；吸納有關利益相關者的參與；通過歐洲和歐洲網路安全月的全球維度拓展，提高各國媒體的關注；通過政治領域與媒體方面的協作，增強對資訊安全相關議題的關注與重視。

歐洲網路安全月主要是由歐洲網路與資訊安全局（ENISA）和歐洲委員會共同籌備，結合歐洲刑警組織（Europol）、歐洲經濟和社會委員會（EESC）、歐盟委員會（EC）相關部門、資訊系統安全協會（ISSA）以及工業界的40多個公共和私營等組織的積極參與，宣傳活動範圍覆蓋全歐洲。2013年歐洲網路安全月活動正式啟動，並以「線上安全需要你的參與（Online security requires your participation）」為主題，吸引歐盟27個會員國及民營部門和企業界的共同參與。2014年歐洲網路安全月活動在ENISA展開「十年來，確保歐洲網路安全（EU Cybersecurity Cooperation: ENISA - 10 years of securing Europe's cyber future）」活動的基礎上，開展了形式多樣的宣傳教育活動，對目標對象的細分更加具體，包括：針對專業技術人員進行網路安全演練、針對在校學生舉行程式編寫等主題活動、針對公共和私營組織進行員工訓練、針對所有網路用戶展開電腦和行動保護以及隱私保護的宣傳。自2013年以來，歐洲網路安全月每年都會

舉辦 50 多場網路安全的相關宣傳活動，活動形式主要包括舉辦會議、論壇和演講，通過電臺和電視節目、線上遊戲和線上交易等管道進行宣傳等，藉以提高歐洲民眾網路安全的意識。

歐盟最初認為網路安全屬於 ICT 日益增長相依的次要問題。但隨著美國和歐盟的重大恐怖襲擊事件後，提升了對網路資訊安全的重視。目前歐盟對於網路安全領域的主要是朝向兩條軸線發展：一方面是採取行動來提高網路抵禦潛在攻擊和事件回應能力，相關措施涉及網路和資訊安全（NIS）、關鍵基礎設施保護（CIP）和關鍵資訊基礎設施保護（CIIP）等。另一方面，歐盟從執法的角度來看待網路犯罪和網路恐怖主義。

在採取行動方面，歐盟於 2004 年成立歐洲網路資訊安全局（ENISA），專責歐洲的資安事務運作，並在 2013 年針對網路資訊安全範疇頒佈新的網路安全指令(NIS Directive)，以落實網路安全策略之項目。同時配合新指令的實施，著手展開各種涉及“網路安全指令”相關主題的修法動作，改革方面圍繞三個關鍵支柱：

- 安全照顧的責任，要求組織需為網路安全實施適當的技術和組織措施。
- 必須向監理機關和受影響的人員公開透露(disclosed)嚴重的安全違規行為。
- 監理機構將有權進行安全稽核和/或要求揭露稽核證據。

歐盟也擴大資料保護範圍及管理力度，並對個人資料的資料控制者(Data Controllers)和處理者(Data Processors)直接施加安全義務(security obligations)，強制性要求對個人資料洩漏通報的義務。另外，為提高民眾網路安全意識，每年 10 月舉行「歐洲網路安全月」教育活動，增進公眾對網路威脅的理解，及提供最新的安全資訊，藉以保護歐洲數位經濟繁榮發展。

在打擊網路犯罪方面，歐盟推動一系列措施因應網路犯罪：推動全球第一部針對網路行為規範之網路犯罪公約，藉以保護歐盟資訊社會免受網路犯罪。並通過《2013/40/EU 指令》建立對資訊系統攻擊之刑事犯罪和裁罰定義，若對關鍵資訊基礎設施(CIIP)造成嚴重損害，將面臨嚴厲的處罰。同時，成立歐洲網路犯罪中心，提高歐盟打擊網路犯罪的能力，確保自由、開放和安全的網際網路，以保護歐洲民眾和企業不受網路犯罪的威脅。

2017 年 5 月歐盟發布的數位單一市場（Digital Single Market, DSM）策略中期報

告(Mid-Term Review)²³⁸指出，歐盟將在 2017 年 9 月審查「2013 年網路安全策略(2013 EU Cybersecurity Strategy)」和網路與資訊安全局(ENISA)的工作，使其與歐盟範圍內新的網路安全框架保持一致。歐盟也將提出物聯網在內的網路安全標準、驗證和標籤措施，以加強連接設備的安全性。

第四節 英國

英國政府高度重視網路資訊的安全保障，並將其視為國家政策發展之重點，全力建設國家層級的資訊安全與保障體系，另一方面，英國政府也鼓勵民間商業機構提升自我資安防護來對抗網路犯罪。2016 年 5 月英國文化媒體暨體育部(Department for Culture, Media and Sport, 簡稱 DCMS)發布的有關大型英國企業之資安狀況報導中指出，有 2/3 的大型企業在 2015 年飽受網路攻擊之苦。為了制衡日新月異的網路攻擊，並確保英國公民與商業機構在安全的網路環境下進行資訊交流，英國政府將於未來五年投入 1.9 億英鎊處理網路攻擊問題，為大型商業機構提供「資安防護 10 步驟(10 Steps To Cyber Security)」建議，協助大型商業機構提升網路自我防護；此外亦為各類商業機構推動網路必備防護計畫(Cyber Essentials Scheme)，鼓勵企業採納基本網路安全實踐(Cyber Security Practice)，並取得資安認證；最後是建立國家網路安全中心(National Cyber Security Centre)，協助業界提升網路安全，

一、 英國網路安全政策規範與組織架構

早在 1990 年，英國政府即頒布《計算機濫用法(Computer Misuse Act)》，將非法佔用、修改、破壞電腦資料或程式認定為違法。2000 年則頒布了《通信監控權法(Interception of Communications Act)》，允許動用警察對網路進行監控及執法，從法律層面允許國家機器依法截收或強制公開某些資訊。2000 年並頒布《調查權管理法(Regulation of Investigatory Powers Act)》規定，所有的網路服務商均要通過軍情五處(Military Intelligence Security Service, MI5)負責運營的政府技術協助中心發送資料。2008 年，英國內政部提出「監聽現代化計畫(Interception Modernisation Programme,

²³⁸ EU, “The Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All”, 2017/10.

IMP)」，監聽並保留英國網路上所有人的通信資料，如電子郵件和網頁流覽時間、地址等資訊。

（一）英國網路安全策略及國家網路安全計畫

隨著英國對於整個網路空間安全所受到的危險意識程度提高，英國政府遂全面推行網路安全策略，加強行業自律。英國政府於 2009 年 6 月正式發布「英國網路安全策略(Cyber Security Strategy of the United Kingdom)」²³⁹，同時為保護政府機關及民眾免於網路安全威脅的考量下，設置了網路安全辦公室(Office of Cyber Security，簡稱 OCS)及網路安全營運中心(Cyber Security Operations Centre，簡稱 CSOC)兩個新的網路安全機關來維護國家網路安全，並在 2010 年 3 月正式運作。

在英國政府的規劃下，OCS 設在內閣辦公室下，負責提供政府跨部會的資訊安全策略，並整合協調政府部門間網路安全之工作；CSOC 則是設置於英國政府通信總部下(Government's Communications Headquarters，簡稱 GCHQ)，負責有效的監測網路空間之健全性並針對緊急事件提出應變措施、瞭解攻擊英國政府及使用者之技巧、提供對於企業及大眾有關網路安全風險應變之忠告與建議。由於英國政府意識到網路空間對於政府在安全防護上的挑戰，因此內閣辦公室強調網路安全防護策略之整合是重要的，其將透過企業，國際合作伙伴及民眾的力量，藉由專業知識及能力的提升、以及更為完善的策略，降低安全風險及發掘安全防護機會，發揮英國在網路安全防範之優勢²⁴⁰。

此外，OCS 也與內政部(Home Office)及警察協會(Association of Chief Police Officers，簡稱 ACPO)合作，制訂有關防範網路犯罪之相關策略。而後，為了因應網路攻擊所造成之高風險，英國政府於 2010 年 11 月斥資 6.5 億英鎊執行四年期「國家網路安全計畫 (National Cyber Security Programme)」，由內政部主導將其他國家針對英國網路空間的敵對攻擊和大規模網路犯罪列為國家面對的主要威脅之一。同時，網路安全辦公室(Office of Cyber Security，簡稱 OCS)亦於 2010 年更名為「網路安全和資訊保安辦公室 (Office of Cyber Security and Information Assurance，簡稱 OCSIA)」續在

²³⁹ UK Cabinet Office, "UK Cyber Security Strategy of the United Kingdom", 2009/06.

²⁴⁰ 資策會科法所，英國政府將設置兩個新的網路安全機關以維護國家網路安全，葉亭巖，2009/7。

「國家網路安全計畫」下負責策略指導和監督協調的工作。

然隨著網路恐怖主義活動的日益增加，英國在 2010 年的國家安全戰略報告中指出，網路攻擊與恐怖主義、國家間軍事危機、重大事故和自然災害被定為英國國家安全面臨的四大主要威脅。對此，英國政府在 2011 年 11 月再度頒布新的「國家網路安全策略(UK Cyber Security Strategy)」，闡述英國如何通過構建更為信賴、更加彈性的數位環境以促進經濟繁榮與保護國家安全，並提出四大目標的戰略藍圖：

1. 有效對抗網路犯罪，使英國成為全球網路空間發展商務最安全的地方；
2. 更有效抵禦網路空間威脅，保護網路空間的國家利益；
3. 致力於形成一個開放、穩定的網路空間，使公眾能夠安全使用並維持一個開放的社會；
4. 具備維持所有網路安全目標的跨領域知識、技術和能力。

新的「網路安全策略」延續在高度重視網路安全的基礎上，進一步提出實際可行的計畫和方案，包括：

1. 成立 CERT-UK：CERT-UK(UK's Computer Emergency Response Team, CERT-UK) 是英國國家電腦網路危機處理中心，負責處理國家網路安全事件，並向關鍵基礎設施和服務提供商提供支援。CERT-UK 協調整個經濟體系與行為的情報意識，並為英國與國外其他 CERT 關係的單一聯繫點。
2. 建立 CiSP 機制：「網路安全資訊共享夥伴關係 (Cyber-Security Information Sharing Partnership, CiSP)」是一個在公共部門和私營部門之間分享威脅、風險和資訊回應的機制。大多數公司可以申請加入 CiSP。CiSP 也是 CERT-UK 的一部分。
3. 國家網路犯罪組 (National Cyber Crime Unit, NCCU)：NCCU 是「國家犯罪局 (National Crime Agency)」的一部分，NCCU 為執法部門提供專業資源，並為企業提供一專門通報網路犯罪的辦公室。
4. 網路安全指導 10 步驟 (10 Steps to Cyber Security guidance)：指導說明組織為提高網路安全而採取的實際步驟。
5. 網路街智慧運動(Cyber Street Wise campaign)：這個措施為民眾和企業提供一個關於如何改善他們形勢的實用建議。商業領袖可能會發現一些素材對於內部提高意識活動是有用的。
6. 英國網路安全挑戰(Cyber Security Challenge UK)：由政府 and 產業資金支持舉辦的全國性挑戰大賽，尋找英國的「網路安全冠軍」，藉以幫助填補經濟體中的技能差距。
7. 網路安全基礎計畫(Cyber Security Essentials Scheme)：是網路安全的組織標準，為

最佳實踐提供基礎，它是建立在 10 個步驟網路安全指導基礎上。該計畫允許組織自行驗證(self-certify)符合其組織標準，自我驗證(self-certifications)由確校機構(validation agency)進行檢查。或者尋求其它認證(accreditation)。目前對於要成為英國政府的供應商(government supplier)，遵守該計畫是強制性的。

新的網路安全策略除得到原「國家網路安全計畫」6.5 億英鎊之挹注外，2013 年英國政府肯定該計畫取得之成就，另追加編列 2.1 億英鎊用於網路安全領域，進而使得在 2016 年前政府對網路安全的持續投資達到 8.6 億英鎊。使英國能夠更加靈活地應對網路攻擊，幫助政府與私營行業建立夥伴關係，發展網路安全知識、技能和能力。

繼 2011-2016 年英國網路安全策略通過利用市場力量，加強安全網路空間建設，使網路安全環境得到顯著改善後，但隨著網路科技普及和物聯網的快速發展，網路犯罪規模日益擴大，一旦這些系統受到攻擊，對整個英國社會影響層面會非常廣泛，可能造成用戶資料外洩、鉅額財務損失，以及關鍵服務中斷等，實際威脅國家基礎措施的安全。在此背景下，英國於 2016 年 11 月發布「2016 - 2021 年國家網路安全策略 (National Cyber Security Strategy 2016-2021)」，未來 5 年將投資 19 億英鎊來捍衛其網路系統和基礎設施，阻止敵人的攻擊，並發展出一個泛社會的網路安全能力 (a whole-society capacity)，從最基本的個人網路使用好習慣 (cyber hygiene) 到最複雜的威懾 (deterrence)，設計一套全面性的反應措施，透過更強大的防禦和更好的網路技術，提高對英國任何人進行網路攻擊的成本。

該策略並提出英國網路安全的願景：「到 2021 年，英國力爭建立起一個安全而富有彈性、繁榮而可靠的數位社會，具備所需的知識和能力，能夠有效應對網路威脅，最大程度把握機會和管控風險，進而確保全球網路空間優勢地位」。為實現上述願景，英國應努力實現以下目標：

- 防禦(Defend)：有能力捍衛英國免受各種演變的網路威脅；有效因應突發事件，以確保英國網路、資料和系統受到保護並能迅速恢復。個人、企業和政府部門擁有自我保護的知識和能力。
- 嚇阻(Deter)：有能力探測、了解、調查和阻擾對英國採取的敵對行動，並追究和起訴犯罪者，必要時還能在網路空間採取進攻行動。
- 發展(Develop)：擁有不斷創新發展的網路安全產業，形成研發能力全球領先、技術創新能力強、產業規模不斷壯大的網路安全體系。大力培養滿足公

共和私營部門需要、擁有分析和專業能力的人才，使英國有能力應對未來的各種威脅和挑戰。

基於這些目標，英國將透過投資於合作夥伴關係來追求國際行動，並發揮影響力。這些夥伴關係將以促進英國更廣泛的經濟和安全利益的方式，影響全球網路空間的發展。英國除將加強與最親近國際夥伴的現有聯繫，加強彼此的集體安全外，還將與新合作夥伴建立關係，以建立其網路安全級別，並保護英國在海外的利益。透過雙邊和多邊合作（包括歐盟，北約和聯合國），英國將向在網路空間威脅損害英國利益或英國盟友利益的敵人，發出其將導致後果的明確訊息。為了在未來五年內達到這些成果，英國政府打算更積極地干預，並使用增加的投資提高英國境內網路安全標準，同時藉其能力和產業的力量，開發和應用網路防禦措施，以顯著地提高網路安全水準。

這些措施包括：極小化最常見的網路釣魚攻擊形式，過濾已知的不良 IP 網址，以及主動阻止惡意線上活動。這些基本網路安全的改進，將提高英國面對最常見的網路威脅時的恢復能力。同時英國政府也設立「國家網路安全中心(National Cyber Security Centre, NCSC)」，成為英國網路安全的主管機構，分享知識，解決系統脆弱問題，和引領國家網路安全關鍵議題的討論。並確保英國軍方(Armed Forces)具有強大的網路防禦能力，足以防禦他們的網路和操作平台；在網路威脅下，還能繼續運作和保持全球自由調度的能力。英國軍方的「網路安全管理中心（Cyber Security Operations Centre, CSOC）」也與「國家網路安全中心(NCSC)」密切合作，確保軍方可以協助處理重大的國家網路攻擊事件。此外，英國政府也將透過權力和影響力來資助相關計畫，來解決從學校到整個勞動市場網路安全技能短缺的問題。同時也辦理「英國網路安全挑戰賽(UK Cyber Security Challenge)」，由英國政府、會計顧問公司(PwC)、政府通訊總部(GCHQ)和英格蘭銀行(Bank of England)共同運作管理，為英國最佳人才提供一個機會。

針對通訊傳播產業，歐盟委員會為強化對網路和服務之安全性和可靠性的監理，2009 年 11 月，歐盟電子通信產業的《框架指令(EU Framework Directive)》被《2009 年更好監理指令(Better Regulation Directive 2009)》修訂，為產業引進有關網路安全的立法。修訂的框架指令，首次將網路和服務之安全性和完整性要求正式納入監理條款，並擴大會員國、國家監管機關和產業在網路和服務安全的義務。這些新義務被引入到框架指令第 13(a)和第 13(b)條款。

由於歐盟會員國被要求執行第 13a 和第 13b 條於國家法律中，因此英國即修改其《2003 年通訊法 (Communications Act 2003，簡稱 CA2003)》，將第 13 (a) 條和第 13 (b) 條規定增訂在第 105A 至 105D 條款中，並於 2011 年 5 月 26 日生效。英國通訊法(CA2003)第 105A~D 條分別規定電子通訊網路及電子通訊服務之資通安全要求，包含基本風險管理、終端用戶保護、網路互連與網路可靠性的維護，並規範資安事件通報與違反法律之裁罰，以保障通訊傳播服務使用者之資訊安全。具體規範內容，主要包括：

- 網路和服務提供商必須對安全性，採取適當措施來管理風險，特別是盡量減少對終端用戶和互連的網路影響；
- 網路提供商必須採取一切適當措施，盡可能保護網路可用性；
- 當網路或服務產生重大影響時，網路和服務提供商必須向 Ofcom 通報安全漏洞或服務供應削減情形。
- 如果合適 Ofcom 必須通知其他會員國監理機關、歐洲網路和資訊安全局 (ENISA) 和公眾接受任何的報告；
- Ofcom 必須向歐盟委員會和 ENISA 發送相關的年度摘要報告；
- Ofcom 可能要求網路或服務提供商，提交並支付採新要求的審核；
- Ofcom 可使用法案中的資訊收集和執行規定，以對要求的任何侵權行為進行調查、矯正和處罰。

英國通訊法第 105A 條指導的主要內容²⁴¹，如下圖 4-7 所示。

²⁴¹ Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003, 2014-08.

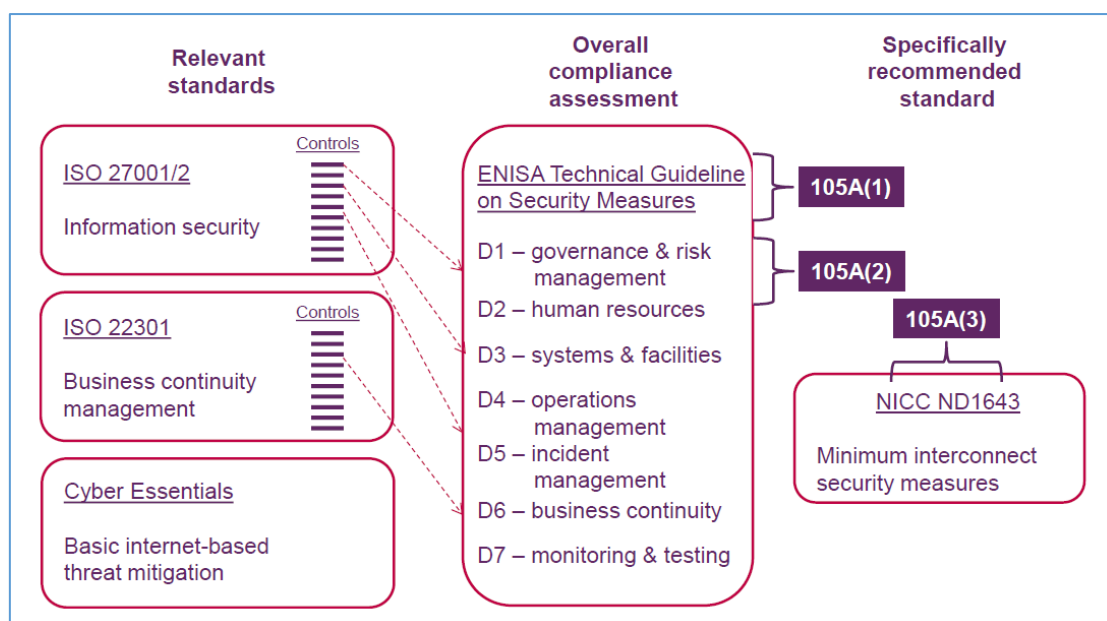


圖 4-7 英國通訊法第 105A 相關標準

資料來源：Ofcom

Ofcom 認為 ENISA 的「安全措施技術指南(Technical Guideline on Security Measures)」設定之最佳作法能確保符合第 105A (1) 條的需求。由於 ISO 27001 是資訊安全管理系統 (ISMS) 的國際標準，也是大多數國家及產業作法的來源，因此根據 ISO 27001 標準適當範圍的認證，可涵蓋 ENISA 指南文件中列出的許多考慮因素。唯一不屬於 ISO 27001 領域解決的服務連續性(business continuity)，也可引用最為密切關係的 ISO 22301 作為標準。同時，Ofcom 也注意到其他安全標準的相關性，包括政府的「網路基礎計畫(Cyber Essentials scheme)」。Ofcom 強烈鼓勵通信業者在供應鏈中採用這一計畫，以彰顯對網路安全的承諾。

(二) 英國網路資訊安全防護組織架構

1. 內閣辦公室：網路安全暨資訊保障辦公室(OCSIA)

為了保護英國網路資訊安全，內閣辦公室 (Cabinet Office) 成立「網路安全暨資訊保安辦公室 (Office of Cyber Security and Information Assurance, 簡稱 OCSIA)」以英國網路安全策略 (The UK Cyber Security Strategy) 為指導原則，協調政府各部會，包含內政部、國防部、外交暨聯邦事務部、政府通訊總局、電子通訊安全機構、國家

基礎設施保護中心等多個政府部門和機構，協同實施國家網路安全計畫（National Cyber Security Programme）。

OCSIA 為內閣辦公室之幕僚單位，負責協助內閣辦公室與國家安全委員會（National Security Council）進行有關網路資訊安全政策執行之優先順序安排，支援有關網路資安策略之擬定，提供政策方向，並協調政府各機關執行網路安全計畫，增強英國的網路安全與資訊保障。OCSIA 以跨部會的方式，與政府各部會機關針對網路資訊安全一起合作，並執行一系列之合作事務，其包括：英國網路安全與資訊保障的戰略方向（含網路犯罪議題）；支援資安教育、宣傳與培訓事宜，如確保上網安全（Get Safe Online）和網路安全挑戰賽（Cyber Security Challenge）；與民間私部門之合作夥伴進行資訊交流並推廣實踐之典範；確保英國網路資訊安全的技術能力及維運架構能有效地維護並精進；與政府資深資訊風險主管辦公室（Office of the Government Senior Information Risk Owner, OGSIRO，隸屬內閣辦公室）共同保障政府資通訊技術之基礎設施的韌性與安全性，並與國際夥伴合作增進網路空間與資訊之安全性。

2. 內閣部會：政府通訊總局（GCHQ）

政府通訊總局（Government Communications Headquarters, GCHQ）是英國最大的情報與安全機構，由外交暨聯邦事務大臣負責領導（但不隸屬於外交暨聯邦事務部）。GCHQ 在實現國家安全策略的過程中也扮演重要的角色，其致力於運用專門知識和經驗，特別是藉由情報研析可能發生的網路攻擊，提供事前預警與防護，以達到維護國家安全與資通訊安全，實現網路空間與基礎設施安全之目的。

具體而言，GCHQ 與工業界及學術界建立夥伴關係，收集分析來自國家基礎設施保護中心（Centre for the Protection of National Infrastructure, CPNI），安全情報局（軍情五處，Military Intelligence, Section 5, MI5）和秘密情報局（軍情六處，Military Intelligence, Section 6, MI6）等單位對安全威脅的研判成果，提供政府對於現有或未來欲新建之 IT 系統一套量身定制的安全風險建議，並提供防範安全風險的思路和方案。

另一方面，GCHQ 下設電子通訊安全小組（CESG）為英國國家資訊安全防護以及緊急事件應變的技術單位。CESG 與工業界合作建立資安標準，並透過審驗及認證程序，確保政府部門使用適當的 ICT 產品、服務和人員。CESG 對資安專業人員提供考核與認證，以建立世界級的資訊保障和網路安全專業人才庫，同時對現有系統運行

提供支援。此外，CESG 為網路諮詢顧問機構 (Certified Cyber Consultancy) 提供認可，以提供正確的資安諮詢服務予政府機關，如對特定的威脅和漏洞進行警告、提供應急回應以及保護資料的技術解決方案，如使用加密金鑰保護最敏感的資訊等。後 2016 年 10 月英國政府啟用「國家網路安全中心 (National Cyber Security Centre, NCSC)」，作為「政府通信總部 (Government Communications Headquarters, GCHQ)」的一部分。NCSC 融合並取代了 CESG (前 GCHQ 的資訊安全部門)、網路評估中心 (Centre for Cyber Assessment, CCA)、英國計算機緊急回應小組 (CERT UK) 以及國家基礎設施保護中心 (CPNI) 的網路相關責任。NCSC 是英國主要帶領網路安全技術的機構，並對英國政府發布之所有網路安全建議的技術內容負全責。

3. 國家基礎設施保護：國家基礎設施保護中心 (CPNI)

國家基礎設施保護中心 (Centre for the Protection of National Infrastructure, CPNI) 成立於 2007 年 2 月。CPNI 是向國家基礎設施提供保護性安全建議的政府機構，並為保護國家安全提供有關物理安全、人員安全、網路安全和資訊安全保障等有關建議，例如安全的放置、安全的建築設計、安全措施或協議，以阻止和檢測威脅或將攻擊後果最小化。

英國將國家基礎設施視為國家運作和日常生活所必需的設施、系統、場所、資訊、人員、網路和過程，並區分為：化學、民用核能、通信、國防、緊急服務、能源、金融、食品、政府、衛生、太空、交通運輸和水等 13 大類。有些類別更細分出次項類別，例如通信產業可再細分為：廣播、電信、網際網路及郵政等。因此每項關鍵基礎設施 (CNI) 產業都有一個對應的政府指導部門，負責識別 CNI 及評估其應變能力，並與電信業者和其他機構合作，提高必要的應變力。CPNI 資助各種保護英國網路空間國家利益、防範來自國家層面、犯罪分子和恐怖主義襲擊等安全威脅的廣泛計畫，同時協助減少國家基礎設施對恐怖主義和其他威脅的脆弱性 (vulnerability) 以保護國家安全。

4. 通訊傳播產業：通訊辦公室 (Ofcom)

為因應數位匯流跨媒體管制之需，英國制訂 Ofcom 組織法 (Office of Communications Act 2002)，整合既有之通訊傳播管制機關，成立單一管制機關「通訊辦公室 (Ofcom)」，並依據 2003 年通訊法 (Communications Act 2003) 賦予 Ofcom 監管英國無線通訊、電信、電視與廣播等通訊傳播領域之產業與服務之權責，包含無線

電頻率及執照之管理，電信產業、商業廣播電視之監理與媒體內容之監督。在資安事務部分，依據 2003 年通訊法第 105 條 A~D 之規範，Ofcom 亦針對電子通訊網路及電子通訊服務業者，發佈資安要求之指導文書，以協助業者符合法律要求。

二、 英國關鍵基礎設施保護

英國政府自第一次世界大戰後擁有廣泛權力，來確保公共安全和捍衛領土。戰後，該緊急權力法得到保留，使得政府能在事件發生或受到威脅下宣布緊急狀態。根據英國 1920 年的《緊急權力法(Emergency Powers Act)》第 1(1) 條、第 2(1) 條的規定：當食物、水、燃料或光源等供應受到干擾的情形，政府可以不經國會的授權，公布實施緊急規則以維護社會必要物質的正常供應²⁴²。同時隨著《2004 年民事應急法(Civil Contingencies Act 2004)》和實施條例，英國將繼續保持和維護關鍵國家基礎設施（Critical National Infrastructure，簡稱 CNI）的基本目標。

英國政府將關鍵國家基礎設施(CNI)定義為資產、設施、系統、網路或流程，如果遺失或中斷，將影響國家安全或基本服務的交付，導致嚴重的經濟或社會後果或生命損失²⁴³。為此，2007 年 2 月英國政府大幅整併「國家基礎設施安全協調中心」(National Infrastructure Security Co-ordination Centre，簡稱 NISCC)、「軍情五處」(Security Service, MI5)及「國家安全諮詢中心」(National Security Advice Centre，簡稱 NSAC)等單位相關人員，成立國家基礎設施保護中心(Centre for the Protection of National Infrastructure，簡稱 CPNI)，提供有關人身安全、人員安全和網路安全/資訊保證的建議。前 NISCC 主要是對運作國家關鍵基礎設施的公司提供建議，而 NASC 則為軍情五處(Security Service, MI5)的內部單位，主要是向政府及其他部門提供安全建議。CPNI 主要對 MI5 安全局長(Director General of the Security Service)負責，並依 1989 年《安全服務法(Security Service Act)》運作。

由於英國關鍵國家基礎設施(CNI)多為民營業者所擁有，因此每個 CNI 產業都有一個對應的政府指導部門，負責識別 CNI 及評估其應變能力，並與電信業者和其他機

²⁴² UK Emergency Power Act 1920, ss. 1(1), 2(1).

²⁴³ POSTNOTE, Cyber Security of UK Infrastructure, The Parliamentary Office of Science and Technology, Number 554., 2017/5.

構合作，提高必要的應變力。因此，2010 年 3 月英國內閣辦公室(Cabinet Office)發布「關鍵基礎設施之部門適變機制規劃(Sector Resilience Plan for Critical Infrastructure 2010)」，該計畫闡述由「國家風險評估(National Risk Assessment)」確定的英國最重要基礎設施之相關風險與其應變能力。政府部門(Government departments)主要負責確保各產業部門(Sector)採取適當措施，以提升安全保護，同時「國家基礎設施中心(Centre for the Protection of National Infrastructure，簡稱 CPNI)」和產業組織協商，進行產業關鍵基礎設施的確認。

英國對於關鍵基礎設施強調重點為安全(Security)與應變恢復力(Resilience)，其中關鍵基礎設施的應變恢復力係指：資產和網路的預備(anticipate)、承受(absorb)、適應(adapt)和從破壞中恢復(recover)的能力，並由四個面向的組合：抵抗力(Resistance)、可靠性(Reliability)、回應及恢復(Response and Recovery)、備援(Redundancy)得以保障，如下圖 4-8 所示。



圖 4-8 基礎設施應變恢復力的組成部分²⁴⁴

資料來源：UK Cabinet Office

英國目前將關鍵基礎設施分為 13 大類，如表 4-9 所示，並將關鍵等級依照失效影響程度分為五級，藉以區分關鍵國家基礎設施以及一般國家基礎設施，以進一步進行風險管理。在風險管理方面則強調在預防以及主動打擊等階段以降低威脅為目的，在保護以及準備階段則以降低脆弱性為目的，進而達成降低風險的目標。

²⁴⁴ UK Cabinet Office, 2016 Sector Security and Resilience Plans.

表 4-9 英國關鍵基礎設施

產業類別	次項產業類別	應變主責機關
化學		「商業、能源及產業策略部」(Department for Business, Energy and Industrial Strategy, 簡稱 BEIS*)
民用核能		「商業、能源及產業策略部」(BEIS)
通信	廣播	文化媒體暨體育部 (Department for Culture, Media and Sport, DCMS)
	電信	
	網際網路	
	郵政	「商業、能源及產業策略部」(BEIS)
國防		國防部 (Ministry of Defence, MOD)
緊急服務	救護	衛生部 (Department of Health, DH)
	海岸巡防	運輸部 (Department for Transport, DfT)
	消防與救援	內政部 (Home Office, HO)
	警察	內政部 (Home Office, HO)
能源	電力	「商業、能源及產業策略部」(BEIS)
	瓦斯	
	石油	
財政金融		財政部 (HM Treasury, HMT)
食品		環境、食品及農村事務部 (Department for the Environment, Food & Rural Affairs, Defra)
健康衛生		衛生部 (Department of Health, DH)

產業類別	次項產業類別	應變主責機關
太空		「商業、能源及產業策略部」(BEIS)
交通運輸	航空	運輸部 (Department for Transport, DfT)
	港口	
	鐵路	
	公路	
水資源		環境、食品和農村事務部 (Department for the Environment, Food & Rural Affairs, Defra)

資料來源: UK Cabinet Office

* 「商業、創新及技能部」(Department for Business, Innovation & Skills, 簡稱 BIS) 和 「能源與氣候變遷部」(Department for Energy and Climate Change) 於 2016 年 7 月合併, 重新改組為 「商業、能源及產業策略部」(Department for Business, Energy and Industrial Strategy, 簡稱 BEIS)

由於英國大多數的關鍵基礎設施(CNI)是民營業者, CNI 網路風險管理的責任在於電信業者, 但政府仍將監控和確保 CNI 網路安全, 並通過各種管道與民營業者合作。因此英國政府與 CNI 有關的工作, 主要採取非強制性指導和最佳實務倡議的形式, 透過「國家基礎設施中心(CPNI)」和「國家網絡安全中心(NCSC)」與產業合作。由於關鍵基礎設施的網路安全被英國政府列為優先事項, 關鍵系統(critical systems)必須被確認和保護, 如果發生攻擊產業部門必須具有能力來應對。若營運業者網路風險管理不善, 政府可以為了國家安全利益進行干預。

三、 英國網路安全推動策略

(一) 制定資料保護的法律框架

由於商業網路安全義務之關鍵起點, 是管理資料保護的法律框架, 為此英國在 1998 年發布《1998 年資料保護法(Data Protection Act 1998, 簡稱 DPA 1998)》, 要求組織應採取適當的技術和措施, 保護個人資料遭受到破壞、遺失或被盜用。根據 1998 年

資料保護法，個人資料被定義為“可以從這些資料中確定(a)與個人生活相關的資訊，或(b)這些數據和其他資訊，很有可能為資料控制者(Data Controllers)所占有(possession)”。該法《資料保護原則(Data Protection Principle)》第七項(1998 DPA 附表 1)，組織必須擁有“適當(appropriate)”的技術和措施，以防止未經授權或非法處理個人資料，並防止意外遺失或破壞或損害個人資料。適當的措施應採取適合該被保護的資料性質以及由於資料安全漏洞而導致個人可能發生的危害，資料保護所涉技術的可用性和相關成本亦應考慮。

同時《資料保護法(DPA 1998)》的安全規定已被「英國資訊委員會辦公室(Information Commissioner's Office, ICO)」解釋為包括網路空間和遏止網路安全責任、保護個人資料免受網路安全漏洞的影響。ICO 並運用在《2003 年隱私和電子通信(EC 指令)規則(Privacy and Electronic Communications (EC Directive) Regulations 2003)》賦予的權力來稽核英國公眾電子通信網路和服務提供商的安全性。當 ICO 進行監理調查(investigation)或監理稽核(audit)時，將尋找證據表明資料控制者(data controller)是否已建立一個控制範圍內的安全框架。對於未能防止安全漏洞以保護個人資料的事件，根據《資料保護法(s55A DPA 1998)》規定可處以高達 50 萬英鎊的裁罰。例如，2013 年 ICO 對 Sony 其 PlayStation 網路遭到駭客攻擊後罰款 25 萬英鎊，普遍認為 Sony 是因網路安全疏忽(failure)而引起英國有史以來的首宗監理處罰。

(二) 設置資訊共享機制

為因應歐盟網路安全指令要求建立公民警部門合作機制，英國在 2010 年發布「國家網路安全策略」中，即提出「網路安全資訊共享夥伴關係(CiSP)」來解決這些要求。CiSP 是 CERT-UK 於 2013 年 3 月成立的一個產業與政府的資安合作夥伴關係。CiSP 除允許英國各領域的組織，在一個安全的環境中，即時且安全的交換資訊，CiSP 也結合產業與政府的資安分析團隊，成立一個資訊融合小組(Fusion Cell)。該小組會廣泛收集各種來源的資安資訊，在分析整理後以警示(alerts)與公告(advisory)的方式提供給會員。會員亦可收到 CERT-UK 提供的網路監看報告(Network Monitoring Report)。為了要接收這份報告，CiSP 會員必須提供其連接網際網路的資訊架構細節，CiSP 會將其收集到的網路惡意行為資訊與會員提供的資訊進行比對，一旦比對出有對會員發動的網路惡意行為，CiSP 會在 60 秒內以電子郵件通知會員，也會在每週彙整一份完整的

報告提供給會員。報告內容包括：

- 受惡意程式感染的主機。
- 由惡意程式分析產生的指標。
- 殭屍電腦網路架構(例如 C&C)。
- 被入侵且提供惡意程式下載的電腦主機。
- 遭網頁置換的 Web 伺服器資訊。
- 發動網路攻擊的 IP。
- 發送垃圾與釣魚信件的來源。
- 可能存在弱點的網路設備。

要加入 CiSP 會員必須是在英國登記的公司，或是負責管理英國境內通訊網路的個人。申請加入時必須獲得英國政府機關、現有的 CiSP 會員或是商業貿易協會的背書，方有可能被核准加入。截至 2016 年 5 月，已有 2,225 多家機構參與計畫，包括 Virgin Media、BAE Systems 和英國電信等²⁴⁵。

(三) 通報機制

英國對於網路安全事件的法律，目前還沒有強制性要求通報，除非是受「2003 年隱私和電子通信規則(Privacy and Electronic Communications (EC Directive) Regulations 2003)」規定的通信服務提供商(communications service providers，簡稱 CSP)。該規則主要係執行歐盟電子隱私指令(e-privacy Directive) 2002/58 / EC，要求服務提供商須依歐盟《第 611/2013 號規定(Regulation 611/2013) (通報規則(Notification Regulation))》，在 24 小時內通報客戶網路安全漏洞及個人資料洩漏事件通報「資訊委員辦公室(Information Commissioner Office, ICO)」。在《通報規則(Notification Regulation)》引入了「技術實施措施(technical implementing measures)」，旨在澄清供應商應如何履行這些義務。如果違規行為(breach)對個人造成不利影響，服務供應者也必須毫不遲延(without undue delay)地通知這些人。

²⁴⁵ National Cyber Security Centre 官網, “Cyber Security Information Sharing Partnership (CiSP)”.

由於英國對於受管制的實體，監理機關可能要求網路安全事件通報，特別是因系統和控制中斷，或者提供服務或客戶的實際或潛在的風險。例如，英國《2003 年通信法(Communications Act 2003, CA 2003)》在第 105A~D 部分也規範「通信供應商 (Communications Providers, CP)」的網路安全法律義務，要求對於公眾電子通信網路 (ECN)或服務(ECS)的運作或可用性產生重大影響的安全漏洞，供應商也有向 Ofcom 通報的義務。同時，網路和服務供應商也必須採取技術和組織措施來管理公眾電子通信網路和服務安全的風險。Ofcom 可能會向公眾或其他監理機關，包括向歐盟網路與資訊安全局 (ENISA) 提出警示通報(alert)。

(四) 設立單一通報窗口

對於民眾網路通報窗口，英國的「詐騙與網路犯罪通報中心(Action Fraud)」是民眾舉報任何詐騙行為及網路犯罪的前哨站。Action Fraud 是由「國家詐騙調查局 (National Fraud Authority, NFA)」負責運作。NFA 管理所有組織和機構，並負責調查和起訴詐騙犯罪。英國反詐騙機構網路和 17 個不同的組織可起訴的詐欺行為超過 60 種詐騙類型。而 NFA 是協調反詐騙和制定政策的主要政府機構²⁴⁶。另國家網路犯罪單位 (National Cyber Crime Unit, NCCU) 是英國國家犯罪局(National Crime Agency)的一部分，NCCU 為執法部門提供專業資源，並為企業提供一專門通報網路犯罪的辦公室。

(五) 提出網路安全 10 步驟

為提高企業網路安全，英國為大型組織提出「網路安全 10 步驟(10 Steps To Cyber Security)」建議，以幫助大型組織在網路空間中的資安防護，如下圖 4-9 所示。

²⁴⁶ National Fraud & Cyber Crime Reporting Centre 網站.



圖 4-9 網路安全 10 步驟

資料來源：UK CESSG

這些建議包括：

- 家庭和行動工作(Home and mobile working)：制定行動工作政策，並教育員工遵守。將安全基準建構在應用的所有設備。不論是在轉移或靜置狀態下資料都應進行保護。
- 用戶教育和認知(User education and awareness)：制定組織系統可接受且安全使用的用戶安全策略。建立員工培訓計畫。保持用戶對網路風險的意識。
- 事件管理(Incident management)：建立事件應變和損害復原能力。建立及維護事件處理計畫，並對事件應變小組團隊提供專業訓練。舉報犯罪事件予執法機關。
- 資訊風險管理制度(Information risk management regime)：建立有效的治理結構並確定風險容忍程度。保持董事會對網路風險的參與。制定配套資訊風險管理政策。
- 管理用戶者權限(Managing user privileges)：建立帳戶管理流程並限制特權帳戶的數量。限制用戶權限並監測用戶活動。掌握對活動和審核日誌(audit logs)的

接取控制。

- 可移動媒體的管控(Removable media controls)：制定監測策略及相關配套政策。持續監控所有 ICT 系統和網路。分析可能指示攻擊的異常活動日誌。
- 監測(Monitoring)：建立監測策略與支援政策。持續監控所有 ICT 系統和網路。分析可能指示攻擊的異常活動日誌。
- 安全配置(Secure configuration)：制定更新及應用安全修補，確保維護所有 ICT 系統的安全配置。建立維護系統軟硬體庫存清單，並為所有 ICT 系統定義安全基準。
- 惡意軟體的防範(Malware protection)：制定相關政策，建立適用於所有業務領域反惡意軟體的防範措施。全面偵測整個組織中的惡意軟體。
- 網路安全(Network security)：保護組織網路免受外部和內部的攻擊。管理網路周邊。過濾未經授權的接取和惡意內容。監控和進行安全控管測試。

(六) 推動公共領域之網路安全基礎計畫(Cyber Security Essentials Scheme)

2014 年 6 月英國政府正式啟動網路基礎計畫(Cyber Essentials scheme)，旨在針對所有組織制定基本技術控制措施，以減輕常見的基於網路的威脅，並提供了一個保障框架(assurance framework)。網路基礎計畫是屬網路安全的組織標準，建立在 10 個步驟網路安全指導基礎上。該計畫允許組織自行驗證(self-certify)符合其組織標準，自我驗證(self-certifications)可由確校機構(validation agency)進行檢查驗證，或者尋求其它認證(accreditation)。對於要成為英國政府的供應商(government supplier)，遵守該計畫是強制性的。例如，英國國防部即要求其所有供應商須符合「Cyber Essentials」安全標準。

(七) 發展網路進攻能力(Offensive Cyber Capabilities)

英國為有效應對網路攻擊，在 2011 年公布的《網路安全策略》提出了自衛的概念，指出英國將開發及整合網路防禦能力，採取一種更積極的方法來瓦解英國受到的網路安全方面的威脅以及阻止潛在的攻擊。

（八）推廣宣導資安教育，提高公民意識

英國政府希望鼓勵更多人使用數位服務，但必須同時努力向個人和企業宣傳資料洩露的風險。因此在國家網路安全計畫（National Cyber Security Programme）對宣傳教育非常重視，同時也將網路安全學科納入英國學術教育體系中，從國中電腦科學課程到博士學位研究均有相關內容。2015 年英國內閣日前公布一系列鼓勵年輕人加入網路安全事業的措施。依英國國家網路安全計畫，英國政府與多方組織合作提供一定數量的學徒培訓機會，並增加公務員隊伍中網路專家的數量，同時也在終身教育和高等教育中設置網路安全培訓課程。除英國電腦協會（British Computer Society，簡稱 BCS）將安全方面的課程列為獲取電腦領域學位的必要學科外，2016 年英國工程技術學會（Institution of Engineering and Technology，簡稱 IET）亦將網路安全列為學士學位課程的必要組成部分。2017 年 2 月英國政府更進一步出資 2000 萬英鎊為青少年提供網路安全培訓，大力引導青少年積累自身網路安全技能。此項計畫為國家網路安全計畫的一部分由英國文化、媒體與體育部（DCMS）負責管理，目標是到 2021 年至少培訓 5700 名青少年完成相關課程，並尋找、培養及快速追蹤未來的網路安全專業人才。

隨著網路科技的快速發展，網路犯罪規模日益擴大，英國重要基礎設施網路攻擊事件的數量不斷增加。根據英國國家打擊犯罪調查局（National Crime Agency，簡稱 NCA）估計，網路犯罪對英國經濟成本影響每年高達數 10 億英鎊，並且還不斷增長²⁴⁷。國家網路安全中心（NCSC）報告也顯示，英國每個月約有 60 次高層次（high-level）的網路攻擊，其中許多威脅到國家安全²⁴⁸。因此，英國政府將網路（Cyber）視為對國家安全的一級（Tier）威脅。網路安全也提升至英國政府議程的首位。英國第一份網路安全策略（UK Cyber Security Strategy）於 2009 年公布，陸續投入 8.6 億英鎊支援網路安全計畫（Cyber Security Programme），成立英國電腦緊急應變中心（CERT-UK）、建立網路安全資訊共享夥伴關係（CiSP）機制及設置國家網路犯罪組（NCCU），分享網路威脅最新資訊、提供企業專用通報網路犯罪窗口，提高英國產業總體安全；推出網路安全指導 10 步驟，指導產業提高網路安全的實務作法；並辦理網路街智慧運動、網路安全挑戰，提高全民網路安全意識與技能；推動網路安全基礎計畫（Cyber Security Essentials

²⁴⁷ NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016, 2016/7.

²⁴⁸ NSCS, The cyber threat to UK business 2016/2017 Report, 2017.

Scheme)，強制性要求政府供應商(government supplier)遵守計畫以降低網路威脅。

繼 2009 年網路安全策略取得一定重要成果後，英國政府進一步推出 2021 年願景是：建立一個安全而富有彈性、繁榮而可靠的數位社會，並能具備知識與能力因應網路威脅，把握機會和管控風險，進而確保全球網路空間優勢地位。因此，2016 年 11 月英國發布第二個為期五年的「2016-2021 年國家網路安全策略(National Cyber Security Strategy 2016-2021)」，將投資 19 億英鎊打造世界最安全經商之地。新策略核心目標是：防禦(Defend)網路攻擊、遏制(Deter)潛在的攻擊者以及發展(Develop)英國的網路安全產業。同時為統整政府網路安全資源與簡化職責分工，在政府通信總部(GCHQ)下成立國家網路安全中心(NCSC)，提供政府有關網路安全領域創新與技術的政策建議。

由於英國將關鍵國家基礎設施(CNI)定義為資產、設施、系統、網路或流程，如果遺失或中斷，將影響國家安全或基本服務的交付，導致嚴重的經濟或社會後果或生命損失。為此，2010 年 3 月英國內閣辦公室(Cabinet Office)發布關鍵基礎設施之產業部門適變機制規劃(Sector Resilience Plan for Critical Infrastructure 2010)，藉由四個面向組合：抵抗力(Resistance)、可靠性(Reliability)、回應及恢復(Response and Recovery)、備援(Redundancy)，確保關鍵基礎設施的安全與應變能力，同時也成立國家基礎設施保護中心(CPNI)，對國家關鍵基礎設施提供有關人身安全、人員安全和網路安全/資訊保證的建議。另新策略也將關鍵國家基礎設施(CNI)網路安全列為優先事項，關鍵系統(critical systems)必須被確認和保護，一旦發生網路威脅時產業必須具有能力來應對，若營運者網路風險管理不善，政府可以為了國家安全利益進行干預。

針對通訊傳播產業，英國目前的《2003 年通信法(Communications Act 2003, CA 2003)》第 105A~D 部分是唯一規定網路安全的法律義務，該法規定電子通訊網路及電子通訊服務之資通安全要求，包含基本風險管理、終端用戶保護、網路互連與網路可靠性的維護，並規範資安事件通報與違反法律之裁罰，以保障通訊傳播服務使用者之資訊安全。同時，Ofcom 強烈鼓勵通信業者在供應鏈中採用網路基礎計畫(Cyber Essentials scheme)，以彰顯業者對網路安全的承諾。由於英國政府意識數位領域對於國家發展的重要性，未來 5 年的國家網路安全策略，也將以防禦、嚇阻和發展等三個面向鞏固網路安全的領先地位：

- 在防禦的層面上，將加強國家重要基礎設施部門的防禦，而且與相關網路安

全產業合作，發展可以降低網路攻擊影響的技術，同時推動公部門和私部門的網路安全標準，確保大部份敏感性的資訊和網路，可以受到安全的保護。另英國政府未來會採取更積極的網路防禦方式，支持業界使用自動防禦技術，可以在發生網路威脅和網路攻擊之前，阻斷惡意行動的發生。

- 從嚇阻的層面上，英國政府未來將阻止那些從網路空間裡面，試圖竊取、威脅或以其他方式損害國家利益的網路犯罪者。政府未來將會提高成本，投資網路偵測、追蹤和還擊的能力，加強政府在網路上的執法能力，降低網路犯罪的數量，並且確保有能力可以執行追蹤、逮捕和起訴網路罪犯。此外，由於目前有少數國外的網路攻擊者已發展和部署具有進攻性的網路能力，可能會威脅到英國關鍵的基礎設施和工業控制系統的安全性。因此，英國的「國家網路進攻計畫(UK's National Offensive Cyber Programme)」也將開發這種能力，以有效回擊阻止潛在的攻擊。
- 在發展層面上，英國政府正在與各個英國大學共同建立最新的網路安全研究所，確保未來有一些擁有網路安全技能的學生，可以在國家或企業裡面提供網路安全的專業能力。同時也將構建完整的網路安全技術的教育體系，未來能夠發展網路安全方面的專業領域和事業。

此外，值得注意的是歐盟新版《網路安全指令(Directive on Network and Information Security, NIS Directive)》²⁴⁹及《一般資料保護規則 (General Data Protection Regulation, GDPR)》將在英國脫歐(Brexit)前生效(2018 年 5 月執行)，目前英國政府計畫維持現有的歐盟法律，無論 Brexit 如何，政府都將實施 NIS 指令²⁵⁰。同時，由於任何希望在歐盟進行交易的企業都需要遵守 GDPR。因此，英國的科技、媒體和電信公司也將必須遵守 GDPR 而不受 Brexit 影響。

第五節 日本

日本自 2000 年起逐步建立網路安全的相關政策，包含主管機關、法律架構以及

²⁴⁹ EU, DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016/7.

²⁵⁰ Out-Law.com, "Network and Information Security Directive will be implemented in the UK despite Brexit vote, government confirms", 2017/1/4.

推動的策略，其中亦對於關鍵基礎設施的保護有相關的措施。以下則以政策架構、關鍵基礎設施與推動策略來進一步申述。

一、 日本網路安全政策規範與組織架構

（一） 政策沿革

日本政府以 2000 年作為網路安全政策的起始點。在 2000 年之前（Try and error 時期），日本各部會（省廳）的資訊安全政策是自己制定與負責的，各省對於關鍵基礎設施、企業、個人的措施皆碎片化，沒有整體的戰略。約在 2000 年 1 月起，日本政府官方網頁懷疑遭到中國網軍的第一次大規模攻擊²⁵¹，因而展開網路防恐對策，以及對於政府機關的資訊安全對策進行強化，2 月設置「內閣官房資訊安全對策推進室」、7 月擬定「安全政策指引」，針對關鍵基礎設施擬定「網路防恐特別行動計畫」，不過整體戰略並未持續。²⁵²

2003-2005 年間，各種資通訊災害陸續出現，對於社會的威脅逐漸增大，也對於國民生活與經濟活動產生直接的打擊，再次表現出政府機關的資訊安全政策並不充分，因此於 2005 年制定「政府機關資訊安全對策統一基準」、「關鍵基礎設施資訊安全對策有關之行動計畫」，並基於「對於資訊安全問題處理，往政府的職務、功能調整方向邁進」（2004 年 12 月 7 日 IT 戰略本部議決），日本政府強化與發展了資訊安全對策推進室，在內閣官房中設置了「資訊安全中心（NISC）」與「資訊安全政策會議」。2006 年制定「第一次資訊安全基本計畫」，並啟動每年的年度計畫「Secure Japan」，2010 年改名為「資訊安全計畫」（Jouhou Plan，簡稱 JS），2013 年起改名為網路安全計畫（Cyber Security，簡稱 CS）。

2013 年日本在資通訊成長戰略上提出「世界最先進 IT 國家創造宣言」，目標是來實現「世界最高水準的 IT 活化利用之社會」。在網路高度使用的情況下，圍繞在網路空間的風險愈來愈加深，而且基於網路空間日後更加擴展與變化，透過實現「世界最

²⁵¹ 木暮仁，“中央官庁 Web ページ集中改ざん事件（2000 年）”。

²⁵² 內閣官房情報セキュリティセンター，“情報セキュリティ戦略元年— わが国の情報セキュリティ政策の現状 —”，2007。

高水準的 IT 活化利用之社會」的成長戰略與確保國家安全保障與危機管理的目的下，日本在網路空間構成資訊系統與資通訊網路的處理資訊與現實空間關鍵基礎設施等資訊系統、資通訊網路一體化、融合相關的機密性、完全性、可用性所確保的狀態，以強化「網路安全」為主體的推展體制的機能。

同年，「網路安全戰略」（2013 年 6 月 10 日資訊安全政策會議議決）實施，擬檢討推動日本體制之強化，成為目前日本政府之網路安全重要政策（並會依據當時社會環境做修訂）。另外「世界第一安全的日本」創造戰略（2013 年 12 月 10 日閣議議決）、「國家安全保障戰略」、「日本再興戰略改訂 2014」皆是網路安全戰略後的重要附帶政策。「世界第一安全的日本」創造戰略，意旨是建構世界最高水準的安全網路空間；「國家安全保障戰略」（2013 年 12 月 17 日閣議議決）是為了日本國內全體的網路保護、對應能力的更加強化所推展組織強化；「日本再興戰略改訂 2014」（2014 年 6 月 24 日閣議議決），是在資訊自由流通的確保之目的下，為了 IT 的使用安全性與確保信賴性，確保穩固成長戰略，關於網路安全之政府機能、日本自身要加強發揮領導能力的推展體制，深化法制之檢討。除此之外，2020 年預定舉辦的東京奧運，屆時 IT 技術的活化利用考慮到會有更加跳躍突破性的進展，可能會有新形態從未出現過的網路攻擊之發生。有鑑於 2012 年夏天舉辦的倫敦奧運，就有針對官方網站有 2 億次以上之網路攻擊發生，因此網路安全的保護是日本推展體制的機能強化所持續精進的目標方向²⁵³。

2014 年 11 月 6 日，日本更進一步制定「網路安全基本法」，真正將過往的網路安全設置機構與處理方式提升至法律層次。日本網路安全政策自 2000 年迄今的沿革歷程請參閱圖 4-10。以下將針對日本 2014 年制定的「網路安全基本法」進行說明。

²⁵³ 情報セキュリティ政策会議，“我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針”，2014。

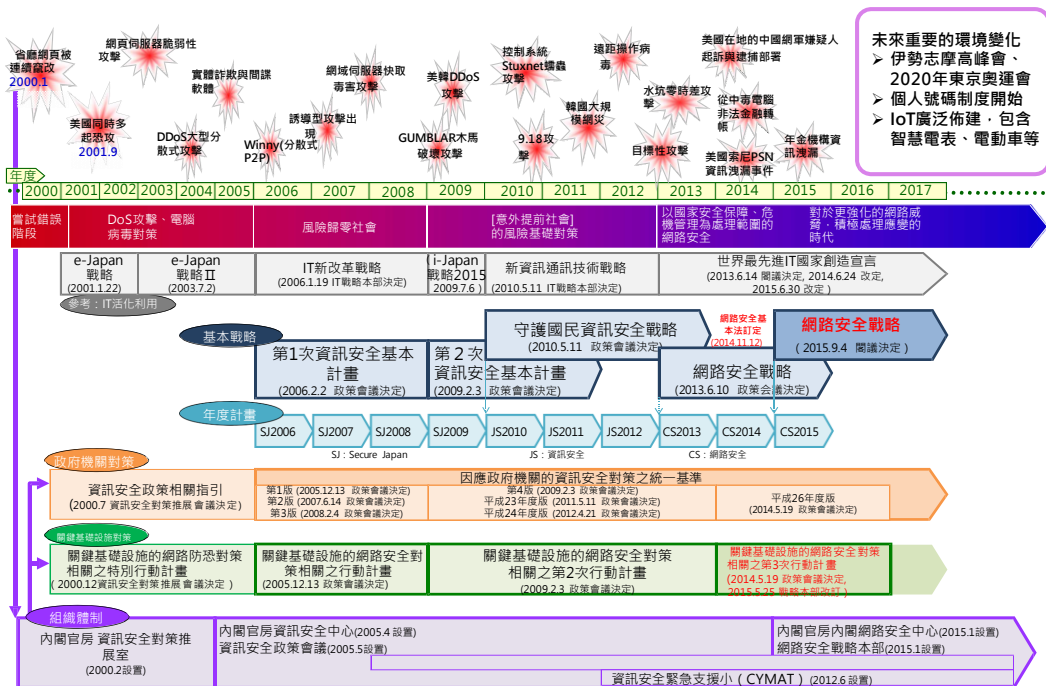


圖 4-10 日本網路安全政策沿革

資料來源：內閣官房資訊安全中心

(二) 法制規範

2014 年 11 月 6 日，日本第 187 次國會臨時會中，通過強化網路安全推展體制的「網路安全基本法」（請參見表 4-10）。基本法的概念包含：在國家安全保障、危機管理方面，試圖對於網路空間的防護；根據國家為主導來分配任務(如「網路安全基本法」第 13 條~第 23 條)、政府與人民的關係（包含國家、地方公共團體的關鍵基礎設施事業者、企業、教育、研究機關與一般使用者）在各式各樣於社會立場上相對應發揮角色；有必要在國際合作與公私合作為首的相互合作與協助。並且，以資通訊網路社會的形成為目的，最後由民間為主導角色之基本理念所制定的高度資訊網路社會形成基本法（2000 年法律第 144 號），日後會持續維持這樣的基本架構。

表 4-10 日本網路安全基本法輪廓

章節	內容	
第一章 總則	目的(§1)、定義(§2)*、基本理念(§3)*、關係單位的責任義務(§4-9)、法制上措施(§10)、行政組織整備(§11)	定義(§2)：本法所謂的「網路安全」是指以電子、電磁的方式，基於一般人知覺無法察覺之方式來防止記錄、發信、傳送接收資訊的洩漏、滅證、毀損之資訊安全管理的必要措施；以及為了資訊系統與資訊通訊網路的安全性與信賴性的確保措施（包含為了基於違法活動損害防止之必要措施，以資通訊網路或電磁方式所做成透過電子計算機的記錄有關之媒體）在這樣情形下所適當維持的管理方式。 基本理念(§3)：網路安全有關措施推展的基本理念，規定如下： 1.基於公私合作來積極對應，確保資訊自由流通。 2.國民每人要加深認識，自發對應促進，建構堅強的體制。 3.高度資訊通訊網路的整備與根據 IT 活化利用建構有活力的經濟社會。 4.為了國際秩序的形成擔任先期導入的角色，在國際協調之下實施。 5.關心與實施 IT 基本法的基本理念。 6.留意不可以不當侵害國民權利。
第二章 網路安全戰略	網路安全戰略(§12)	關於網路安全戰略的內容規定事項如下： 1.網路安全有關措施的基本方針

章節	內容
	2.確保國家行政機關的網路安全 3.確保促進關鍵基礎設施事業者的網路安全 4.其他必要事項
第三章 基本措施	確保國家行政機關的網路安全（§13）、確保促進關鍵基礎設施事業者的網路安全（§14）、促進民間事業者與教育研究機關的自發性作為（§15）、多樣的主體合作（§16）、犯罪取締與防止被害擴大（§17）、達到我國安全中重大影響對應的可能事項（§18）、產業振興與強化國際競爭力（§19）、推展研究開發（§20）、確保人才（§21）、教育與學習振興、普及啟發（§22）、國際協力的推展（§23）
第四章 網路安全戰略本部	設置（§24）、掌管事務（§25）、組織（§26）、首長權責（§27）、副首長權責（§28）、部員配置（§29）、事務委託（§30）、資料提供（§31）、其他單位資料提出的協助（§32）、地方公共團體的協助（§33）、其他（§§34-37）等
附則	施行日期（§1）、在法制必要整備下，讓內閣官房能適切處理本部相關事務（§2）、檢討（§3）、IT 基本法的部分修正（§4）

資料來源：本計畫整理

（三）重要執行組織

日本網路安全政策推展體制架構如圖 4-11，各單位職掌範圍說明如下。

網路安全戰略本部最核心的幕僚運作單位為「內閣官房資訊安全中心」(NISC)。前身是 2000 年 2 月內閣官房設置之「資訊安全對策推展室」與 2005 年改組之「資訊安全中心」。

NISC 實質上在網路安全有關政策與事件對應上為發揮權責的司令塔，進行戰略本部有關事務的處理，其在內閣官房組織令上已明確化此一常設組織(如網路安全基本法附則第 2 條第 1 項)；此外，NISC 為了在政府全體的網路安全強化綜合推展為目標上，進行必要的制度檢討工作。其相關事務如下：

- (1) 進行政府機關資訊系統的資通訊網路非法活動之監視與分析業務。
- (2) 行政機關發生的網路安全重大事件原因探討之調查相關事務。
- (3) 確保有關行政機關網路安全之必要監察與建議，以及其他資訊提供援助之相關事務。
- (4) 確保綜合調整有關網路安全計畫與立案之相關事務。

NISC 首長也就是所謂的「內閣網路安全長」，其為了要確保從平常事態處理、危機管理到安全保障可以持續對應之體制得負責擔任事態處理、危機管理等職務，另外，國家安全保障局次長被指派為內閣官房助理安全長。

NISC，特為了 2020 年東京奧運進行了以下必要措施之檢討，以及快速得出可行結論：

- (1) 政府機關、資訊安全橫向監視、即時調整小組 (GSOC) 功能的強化：對於政府機關資訊系統的資通訊網路，GSOC 除了進行政府機關資訊系統的資通訊網路非法活動之監視與分析業務，從 2017 年度起，針對新系統的運用，從體制強化觀點來擬定、推展必要體制、機材與設施有關的具體計畫。
- (2) 綜合分析機能的強化：強化國外政策、網路威脅情勢、網路攻擊使用技術綜合分析功能，並且確保能活用有高度專門知識與真知灼見之專家及提升人才資質。
- (3) 國內外資訊彙整功能的強化：往政府機關、獨立行政法人、關鍵基礎設施事業者的事件資訊匯集功能與建議功能強化，並強化政府與民間合作，以及提升 NISC 內的體制、系統整備能力。

(4) 國際合作的強化：強化國際合作、國際協力團隊的體制整備，以及網路安全有關之緊急對應關係機關與構建國際夥伴關係的窗口功能。

(5) 人才育成與錄用：通過以返回原單位、預約任期與推展人事交流等基礎，積極從各省廳募集有見識、經驗的人到中心，確保完備有技能之人才。

此外，各府省廳為了要提高資訊安全水準，2005 年擬定了政府機關的資訊安全對策統一基準，經過了 5 次的更新，試圖讓各府省廳資訊安全水準能同時提升。此外，政府機關 GSOC 在 2008 年開始正式運作，監控政府機關的網路攻擊。

另一方面，運用複雜、巧妙的手法來進行在特定標的的組織進行攻擊，這對於個別組織來說應對上的困難；對於隨機性的事件，整備政府機關內的電腦資安事件應變團隊(CSIRT)，以及有必要建立其他府省的 CSIRT 成員的支援體制。爰此，2012 年在 NISC 之中，設置一超越府省廳壁壘的合作機動性支援體制—資訊安全緊急支援小組 (CYMAT) ²⁵⁴(請參見圖 4-12)。其任務如下：

- (1) 支援對象機關：政府機關、CISO 等聯絡會議。觀察員知參加機關、獨立行政法人等
- (2) 支援對象與發生事項：基於網路攻擊的支援對象機關之資訊系統災害發生或可能發生之場合，政府作為共同對應所必要之資訊安全相關事項。

CYMAT 的組織架構為從各府省廳派出員額，現階段有 26 人，常態約 40 名左右的員額數。內閣官房資訊安全中心長 (CISO) 作為 CYMAT 的統合責任者。平時小組成員以研修訓練等相關事宜提升同仁之安全部署能力。

²⁵⁴ 內閣官房情報セキュリティセンター, “情報セキュリティ緊急支援チーム (CYMAT) 設置について”, 2012.

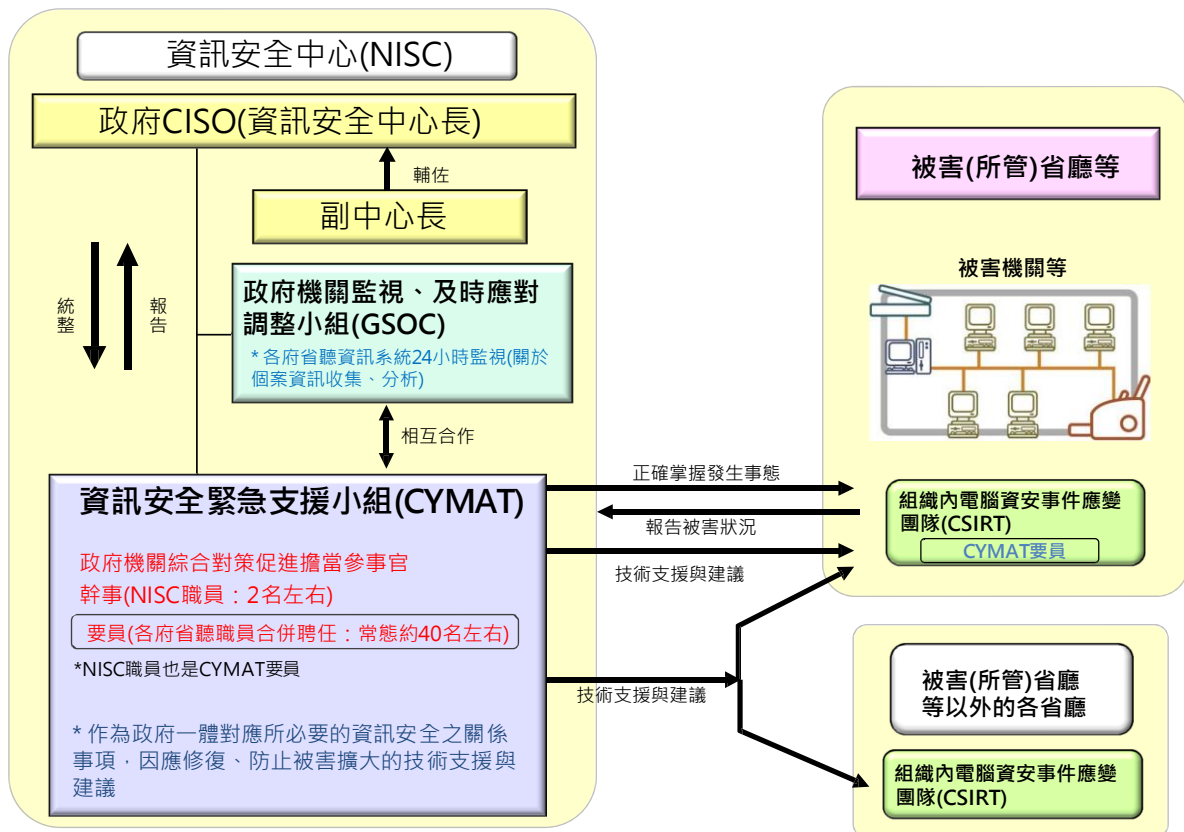


圖 4-12 資訊安全緊急支援小組架構

資料來源：內閣官房資訊安全中心

3. 資訊安全政策會議

資訊安全政策會議原先是根據 IT 綜合戰略本部首長決議，由 2005 年 5 月在 IT 綜合戰略本部下設置之。目前會議根據網路安全基本法由本部設置，在法律的權限賦予之下成為官方與民間統一、橫向的資訊安全對策推展之重要功能。

會議由內閣官房長官為議長，其他參與人員為 IT 政策擔當大臣、國家公安委員會委員長、總務大臣、外務大臣、經濟產業大臣、防衛大臣與 IT 綜合戰略本部長及民間智庫學者構成，必要時其他大臣亦可參與其中。會議經過三年左右的基本戰略經驗中累積形成，目前基於「網路安全戰略」，透過會議事務局 NISC，展開各種措施。

二、 日本關鍵基礎設施保護

對於關鍵基礎設施的防護之法源，主要規定於網路安全基本法中的對象為「重要的社會基礎設施事業者」條文中²⁵⁵。NISC 施行關鍵基礎設施計畫通稱為「關鍵基礎設施資訊安全對策行動計畫」，肇始為 2000 年的「關鍵基礎設施的網路恐攻對策有關之特別行動計畫」（2000 年 12 月資訊安全對策推動會議議決），經過 311 震災發生時的資訊系統災害，數據消失的解決方案，以及隨時因應社會、技術環境產生的各種複雜的網路攻擊，繼而調整更新計畫，最近一次計畫更新為 2017 年 4 月的「關鍵基礎設施資訊安全對策之第四次行動計畫」，其推展架構如圖 4-13。

第四次行動計畫基於 2014 年「網路安全基本法」的基本理念，以及根據第三次行動計畫後的評估、2015 年的「網路安全戰略」，擬定維持在第三次行動計畫下的五項主要措施。第二，關鍵基礎設施成為網路攻擊目標，以及社會技術環境變化已是非常明顯之事，除此之外，資通訊在社會經濟環境中已融合控制系統，而且成為網路攻擊目標的物聯網系統逐漸普遍化。第三，2020 年東京奧運會的舉辦讓後續關鍵基礎設施之風險增加，因而針對這些狀況來強化、改善各項措施之作法。²⁵⁶

²⁵⁵ 網路安全基本法第 6 條、第 14 條。內閣サイバーセキュリティセンター, “重要インフラ等に係るサイバーセキュリティ政策の概要”, 2016.

²⁵⁶ サイバーセキュリティ戦略本部, “重要インフラの情報セキュリティ対策に係る第 4 次行動計画”, 2017.



圖 4-13 政府民間合作之關鍵基礎設施防護推展架構

資料來源：網路安全戰略本部

第四次行動計畫的五項措施分別為「安全基準的整備與滲透」、「資訊共享體制的強化」、「災害對應體制的強化」、「風險管理與處理狀況的整備」、「基礎設施防護的強化」，相關內容如下表 4-11。

表 4-11 第四次行動計畫措施

第四次行動計畫的措施	與第三次行動計畫的措施對應	從第三次行動計畫中主要補強改善的方向
安全基準的整備與滲透	繼承「安全基準的整備與滲透」之原則	經營層期待擬定包含認識、行動、意外事故計畫的對應整備，以及充實指引
資訊共享體制的強化	繼承「資訊共享體制的強化」之原則	資訊共享的進一步推動 1. 聯繫方式的多樣化 2. 促進服務災害的判斷基準為基礎的資訊共享更有效率與有效的事件對應 3. 建立熱線與基於可能的資訊共享系統的整備，在 24 小時、365 天的體制中迅速與有效實現網路攻擊有關的資訊共享 4. 資訊聯絡、資訊提供的範圍，包含關於運作技術（OT）、智慧聯網（IoT）的範圍明確化有關單位的認識共享
災害對應體制的強化	繼承「災害對應體制的強化」之原則	● 持續改善關鍵基礎建設事業者的實用性跨部門演習與資料分析中心訓練 ● 從跨部門橫向演習中得到的知識與 Know How，滲透到各關鍵基礎建設事業者，並藉由提供一個環境模擬演習，來促進基於各關鍵基礎建設業者自主演習的實施
風險管理與處理狀況的整備	繼承在「風險管理」的基本原則上，重新命名	● 擴大措施範疇，從功能保證的觀點，基於風險管理結果的處理狀況額外

第四次行動計畫的措施	與第三次行動計畫的措施對應	從第三次行動計畫中主要補強改善的方向
	並發展「風險管理與處理狀況的整備」	加上整備支援相關作為(包含針對奧運的措施) ● 藉由保證功能能運作的觀點,推動重要的「風險溝通與協議」與「監控與分析」相關作法
基礎設施防護的強化	繼承「基礎設施防護的強化」之原則	● 持續進行關鍵基礎設施領域內外的資訊共享範圍評估 ● 積極提供給有關單位國際會議中的資訊 ● Security by Design 的推展 ● 對於關鍵基礎建設業者的經營層的影響 ● 人才育成的支援(推動具體人才育成有關的產官學合作)

資料來源：內閣官房資訊安全中心

三、 日本網路安全推動策略

在網路資安通報與運作上，日本藉由「關鍵基礎設施資訊安全對策行動計畫」中所制定的 PDCA 流程 (Plan、Do、Check、Act)，作為各單位實施之參考 (如下圖)。

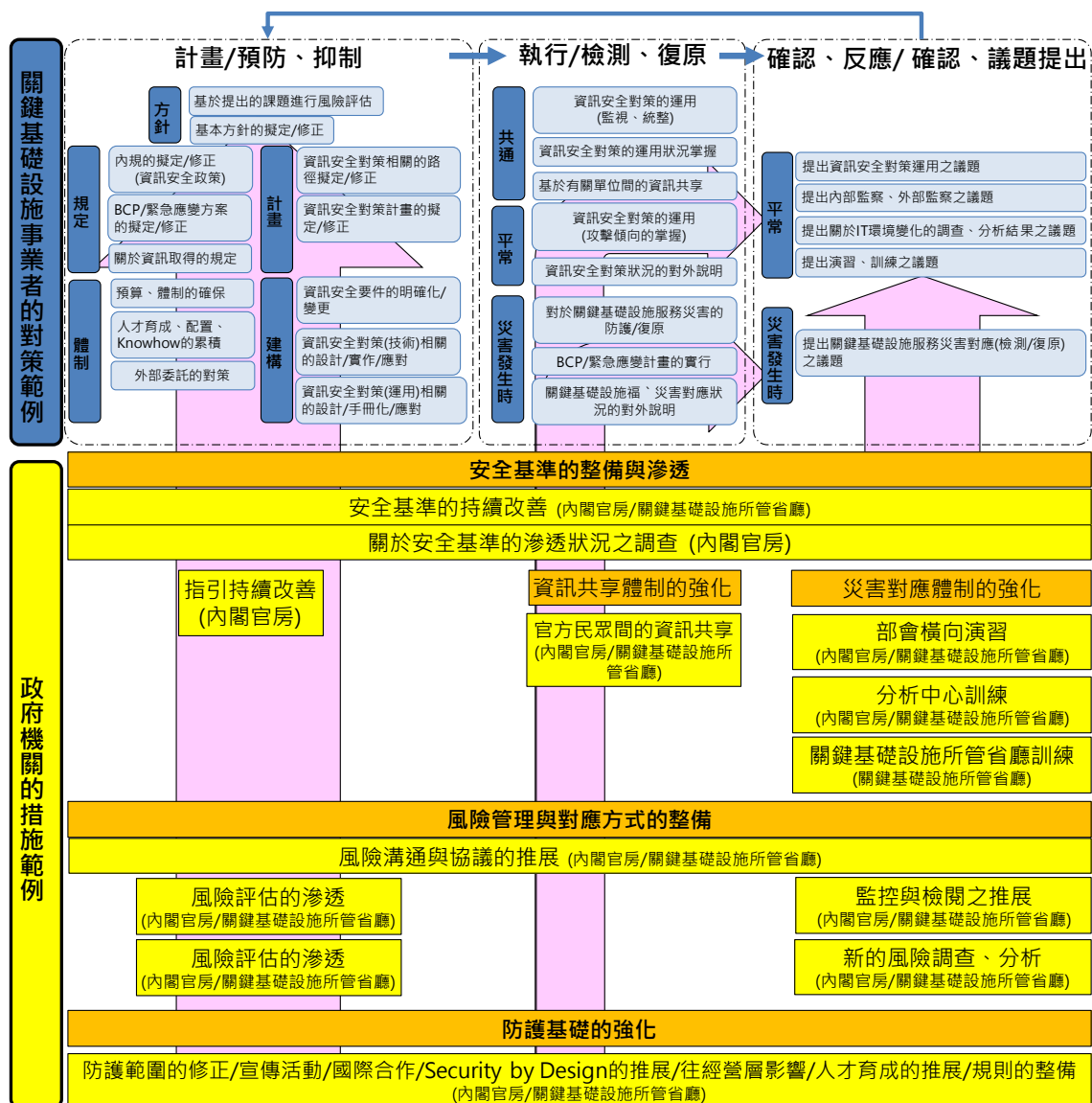


圖 4-14 關鍵基礎設施與政府機關各措施關聯圖

資料來源：網路安全戰略本部

此外，在過往的經驗發現各單位在緊急狀況發生時，資訊的統整經常產生許多問題，因此「關鍵基礎設施資訊安全對策之第四次行動計畫」特別強調「資訊共享體制的強化」(如圖 4-15)，作為本行動計畫的重點項目。

- 各產業部門資料分享中心之間、之內，將資訊共享進一步完善。
- 採取較先進作法的資安資訊分享與分析中心（ISAC）展開活動。

表 4-12 資訊共享體制的各有關單位的職責

有關單位	平時各單位的職責	大規模關鍵基礎設施災害對 應時各單位職責
內閣官房（事件 對策處理、危機 管理負責人）	關於關鍵基礎設施有關之事件 資訊，與 NISC 進行資訊的共享	除了平時擔任的角色外，與 NISC 整合，匯集從事件對應 省廳與防災關係府省廳所提 供之災害資訊、對應狀況資 訊，與 NISC 進行彼此資訊的 共享
內閣官房 （NISC）	與關鍵基礎設施所管省廳、資訊 安全關係省廳、事件處理省廳、 防災關係府省、資訊安全關係機 關與網路空間關聯事業者，共享 彼此系統漏洞相關資訊	與內閣官房（事件對策處理、 危機管理負責）整合，與關鍵 基礎設施所管省廳、資訊安 全關係省廳、事件處理省廳、 防災關係府省、資訊安全關 係機關與網路空間關聯事業 者，共享彼此系統漏洞相關 資訊
關鍵基礎設施所 管省廳	從各管轄之關鍵基礎設施事業 者取得系統漏洞等相關資訊，聯 繫 NISC 與對應之資料分享中心 （CEPTOAR）；從 NISC 取得系 統漏洞等相關資訊，提供給 CEPTOAR	除了平時擔任的角色外，必 須在大規模關鍵基礎設施服 務發生障礙時協助體制因應
各產業部門資料 分享會議	資料共享各產業部門資料分享 會議是一獨立會議形式，並非隸	除了平時擔任的角色外，必 須在大規模關鍵基礎設施服

有關單位	平時各單位的職責	大規模關鍵基礎設施災害對 應時各單位職責
(CEPTOAR Council)	屬在政府機關的下級單位，其是各資料分享中心基於專業判斷的合作會議。 基於各中心的判斷，各中心積極參與計畫，進行關鍵基礎設施事業者的服務維持、復原等廣泛的資訊共享活動。	務發生障礙時建構體制，且與作為產業資料分享中心間為首的關係機構試圖進行合作
各產業部門資料 分享中心事務局	與關鍵基礎設施所管省廳、事件對應省廳、防災關係府省、資訊安全關係機關、資料共享各產業部門資料分享會議、關鍵基礎設施事業者合作，共享彼此系統漏洞相關資訊	除了平時擔任的角色外，必須在大規模關鍵基礎設施服務發生障礙時建構體制，且與作為內閣官房為首的關係機構試圖進行合作
關鍵基礎設施事業者	有關系統漏洞的相關資訊，除了有必要因應所屬資料分享中心內共享外，要以「附件：關於資訊聯絡、資訊提供」為基礎進行關鍵基礎設施所管省廳的聯繫。 另外，一旦有犯罪被害時，要自主判斷進行事件對應的省廳通報	除了平時擔任的角色外，必須在大規模關鍵基礎設施服務發生障礙時建構體制，且與作為內閣官房為首的關係機構試圖進行合作

資料來源：內閣官房資訊安全中心

第六節 行動寬頻資安政策芻議

本章前 5 節針對各國資安政策之分析可知，電信事業在資安政策中扮演非常關鍵之角色，也是各國重要關鍵基礎設施，其重要性甚至高過其他設施。原因在於電信事業所提供之通訊服務除了提供一般民眾相互通信之外，也是政府部門與其他關鍵基礎設施的通訊服務，各種基礎設施都必須透過通訊服務加以連結，倘若通訊服務受到資安影響，其他所有的關鍵基礎設施都將受到影響。各國雖未特別針對行動寬頻服務提出直接的政策或規範，但由各國對電信事業資安之重視，加諸行動寬頻已成為通訊服務之主力，實質上可由電信事業之規範觀察行動寬頻資安之發展。

一、英國通訊法對行動寬頻業者之規範

由前 5 節各國之發展觀察，其中英國在通訊法中針對電信事業的資安責任進行規範。在 2003 年通訊法 105A 中要求業者必須維護網路之安全與穩定，並結合相關技術標準。此一規範同樣適用於行動寬頻業者。同時，Ofcom 與政府部門推動之安全標準相連結，包括英國政府推動「網路基礎計畫(Cyber Essentials scheme)」旨在幫助組織保護自己免受網際網路上之威脅。大多數網路攻擊利用了軟體和 IT 系統的弱點，Ofcom 強烈鼓勵電信業者在供應鏈中採用這一計畫，以彰顯對網路安全的承諾。

此外，Ofcom 在 2017 年 6 月針對 2014 年發佈之資安準則（Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003）進行修訂諮詢²⁵⁸，對於通訊法 105A 之要求進行補充，為了強化網路安全風險管理，Ofcom 認為通過網路安全漏洞測試（Cyber vulnerability testing），對於安全措施的有效性能夠更好的評估，也比單純的資安認證更為實際。

Ofcom 提到英格蘭銀行（Bank of England，即為英國中央銀行）於 2013 年推動資安漏洞測試架構²⁵⁹（CBEST Vulnerability Testing Framework，下稱 CBEST），為英國金融體系及其基礎設施的核心制定一項資安工作計畫，以提高和測試網路攻擊的抵禦能力。為了協助金融公司和基礎設施供應商以及監管機構，提高他們對破壞英國金融穩

²⁵⁸ Ofcom, Review of Security Guidance.

²⁵⁹ CBEST, Bank of England.

定的網路攻擊類型的了解，以及英國金融部門容易遭受網路攻擊的程度，由英國央行聯合其他部門聯合設計資安測試架構。

參酌 CBEST 之發展，英國數位文化媒體體育部（DCMS）聯合 Ofcom、NCSC 和電信業者代表，為電信事業制定類似的政策。將收集關於電信業者面臨威脅的情報，並依據情報設計出各種滲透測試的基礎，評估電信業者網路的防禦程度，這樣的測試也將顯示有多少威脅能夠被檢測、以及是否能夠成功回應。初步看來，未來將會成為電信業者自願進行資安檢測之機制。

二、 美國行動寬頻資安之消費者保護規範

在美國資安政策發展上，針對電信事業之資安需求，國土安全部（DHS）與通訊委員會（FCC）依據國家標準技術研究所（NIST）之資安架構，擬定自願性及建議性之資安評估文件，包含衛星、固網、行動寬頻、有線/無線廣電業者，協助業者針對其網路架構中各項組件之資安需求進行評估極強化。

另一方面，除了 DHS 與 FCC 外，聯邦貿易委員會（FTC）也扮演相當重要的監督角色。FTC 的主要職責在保護消費者權益，因此對於市售所有商品有造成消費者損害之情形，FTC 均能依法進行處罰。例如聯想²⁶⁰、宏達電與華碩均曾因為販售之設備（筆電軟體、手機或路由器），因網路安全漏洞有損害消費者權益之可能性，而遭到 FTC 之處罰。FTC 原則上針對違法之業者進行罰款處分，業者可選擇與 FTC 進行和解，在數個與資通訊設備資安相關之案例中，FTC 的和解條件是要求業者必須建立一個全面性的安全計畫（comprehensive security program），並且需經 FTC 多年期的資安稽核。安全計畫的內容從產品設計到生產上市的流程，都必須包含足夠的資安監督機制，以確保上市產品不會造成消費者受損。

綜合美國資安政策與法制分析，業者在提供設備與服務時，主管機關僅會鼓勵業者自願性參與相關資安測試的機制。然而，在設備上市或服務進入市場之後，可能發生以下狀況：

1. 設備或服務實際上造成消費者損害；

²⁶⁰ FTC, “Cases and Precedings: Lenovo, Inc.”, 2017/9.

2. 雖未造成消費者損害，但被舉報有安全漏洞；
3. 業者宣稱設備或服務符合資安標準、或有採用某些防護機制，但實際上沒有做到。

FTC 針對以上情況均可能以「欺瞞消費者」為由，對業者進行處罰。相對而言，若業者確實的做好資安防護，或是確實參與了自願性機制，卻仍然發生損害事件，此時即使造成消費者損害，亦可以減輕相關賠償責任，或是僅需負責將漏洞加以修補。

三、 美國 NIST 發布之 LTE 安全準則²⁶¹

NIST 依據聯邦資訊安全現代化法 (FISMA) 之規定，針對 LTE 網路安全提出 LTE 安全準則 (Guide to LTE Security NIST SP 800-187)，這一份文件描述了資訊科技實驗室 (ITL) 在 LTE 資訊系統安全方面的研究與指導方針，也包括業界、政府和學術機構的合作活動。此文件的目的是，係因蜂巢技術 (cellular) 已經成為大數民眾的主要網路服務技術，在社會中扮演著越來越重要的角色，行動寬頻的普及也與第四代 (4G) 行動通訊技術 LTE 的部署有關。故 NIST 發布本文件作為 LTE 網路運行和探索 LTE 安全架構的基礎指南，並分析 LTE 網路遭受到的威脅與證實的緩解措施。

特別說明的是，LTE 係由 3GPP 提出之行動通訊網路標準，其技術標準除包含 LTE 網路運作所採用之無線電介面、基站架構、核心網路、身分認證等一整系列的標準之外，也包含了安全標準 (即 3GPP 技術規範 TS 33 系列)，因此 NIST SP 800-187 文件的目的並非在於取代 3GPP 本身所制定之技術標準，而是藉由針對 LTE 網路架構以及 3GPP 技術標準的分析，說明業者運行 LTE 網路所需注意的安全威脅以及解決方案，本研究團隊認為此文件為美國推展行動寬頻網路安全之最佳實務參考，故已將此文件完整翻譯請參閱附錄三，以下為該文件內容重點之摘要。

承上所述，本文件主要內容在分析由行動寬頻業者經營之系統安全，但亦包含為行動裝置與行動基站之系統晶片編寫軟體的組織，所以包含行動網路業者 (mobile network operators, MNOs)、LTE 空中介面、後置迴路 (backhaul)、核心網路及使用者行動裝置的通用積體電路卡 (Universal Integrated Circuit Card, UICC) 與用戶全球識別卡 (Universal Subscriber Identity Module, USIM) 的應用軟體等，均在本文件的討論範

²⁶¹ NIST SP 800-187, "Guide to LTE Security", 2017/12.

圍內。

在本文件第一章的概述後，第二章首先針對 LTE 網路整體架構進行介紹，包含使用者裝置 (UE) 與 UICC、IMEI、IMSI 的組合，次接入 eNodeB、小型基地台 (Small Cell) 組成之 E-UTRAN 連接，再接取核心網路 (EPC) 的架構。另外，對於 LTE 使用者設備 (UE) 與 eNodeB 間、與 eNodeB 與行動管理實體(MME)間的信令通訊也都有詳細介紹。

第三章開始針對 LTE 網路安全架構進行介紹，包括 LTE 提供之認證、加密保護機制、硬體保密機制與網路保護機制。在本文件提到，3GPP 對於 LTE 網路使用者裝置接取 eNodeB、再接取至核心網路 EPC 之間均有相對的安全性規範 (TS 33 系列標準)，然而由於 LTE 網路全 IP 化的關係，核心網路 EPC 的安全準則並不完整，必須借重傳統 IP 網路安全性的原則。

3GPP 將為行動管理實體 (MME) 建立安全保證規範 (SCAS)，之後，3GPP SA3 工作小組 (定義 LTE 安全標準的團隊) 將繼續進行其他網路產品等級適用的安全保證規範 (SCAS)。另外，3GPP 正與 GSMA 的網路設備安全保證團隊 (NESAC) 合作建立一套認證程序與解決方案，以根據安全保證規範 (SCAS) 的要求進行評估產品。3GPP 標準沒有針對核心網路安全的強制安全規範或要求，因此，安全保證規範(SCAS) 的未來發展尚須加以關注。

第四章則介紹 LTE 網路威脅，概列如下：

- 一般網路安全性威脅：包含對使用者設備(UE)的惡意軟體攻擊、影響無線存取網路(RAN)基礎建設的惡意軟體攻擊、影響核心基礎建設的惡意軟體攻擊以及未經授權存取運算與存取管理(OAM)網路等。
- 偽基站安全性威脅：包含可對使用者進行不當的裝置與身份追蹤、利用降級攻擊讓使用者無法連至高速基站、阻止撥打緊急電話以及發出未認證的拒絕訊息，阻斷使用者連上正常基站的可能性。
- 竊聽空中介面。
- 通過綁架小型或微型基站發動攻擊。
- 無線電干擾攻擊：包含干擾使用者設備 (UE) 的無線電介面以及干擾 eNodeB 的無線電介面。

- 竊聽回送網路和核心。
- 對網路基礎建設發動實體攻擊。
- 攻擊加密金鑰 K。
- 盜用使用者的通訊服務。

第五章則針對第四章的 LTE 網路威脅提出緩解方案，本文件首先提出這些威脅緩解措施主要需由行動通訊業者（MNO）或是行動裝置作業系統開發者及硬體製造商等來加以實現；其次是這些業者應與網路安全業者進行合作，採用足夠的安全防禦措施。

另一個重點是落實 3GPP 的網路安全標準，包括對於空中介面的加密、確保核心網路介面的安全性等，這些措施可以確保通訊過程間的安全。再者，對於基站的實體安全以及對於偽基站的偵測也非常重要，如此才可防止使用者裝置被入侵；最後則是針對 IP 網路的運作，在 OTT 服務上進行加密可以提供使用者數據強大的認證、完整性和機密性保護，使用者能利用在一般行動裝置作業系統上運行的應用程序，提供影像、聲音或其他某些通訊服務。此外，OTT 通訊防護亦可作為深層的防禦手段，選擇不只是依賴其行動網路業務提供機密性保護。

最後，本文件認為 LTE 僅利用 IP 技術，攻擊者可能借助既有工具來利用以 IP 為基礎的網路，攻擊在行動網路業者（MNO）網路中的 LTE 核心和其他相關基礎設施。相對的，這也可讓 LTE 網路可以應用以 IP 為基礎的既有防禦技術提高系統安全性。

本文件討論在 LTE 及其安全架構的基本原則，但仍有許多概念尚未納入，包含多媒體子系統（IMS）的安全分析、LTE 語音（VoLTE）安全分析或是網路功能虛擬化（Network Function Virtualization，簡稱 NFV）的安全性等，均需未來更進一步的研究。

四、 歐盟 ETSI 發布有關 NIS 指令之技術報告²⁶²

歐盟標準組織 ETSI 於 2017 年 10 月發布了有關 NIS 指令實施之技術報告文件（ETSI TR 103 456），該文件就目前可用的全球主要網路安全社群正在開發的技術規範提供準則，旨在滿足與實施 NIS 指令相關的法律措施和技術要求，包括資訊分享、

²⁶² ETSI TR 103 456, “CYBER; Implementation of the Network and Information Security (NIS) Directive”, 2017/10.

基於網路之風險和事件、與必要的防禦措施，主要包含事件通知之考量點與網路安全風險管理的最佳實踐。

2016 年 7 月 6 日歐盟議會和理事會通過歐盟網路和資訊系統的高階共同安全措施的 NIS 指令 (EU 2016/1148)，NIS 指令要求歐盟會員國間在資訊安全事務上彼此合作，以支援和促進會員國之間的戰略合作與資訊交換，並改進特定網路安全事件之自願合作以及分享風險相關資訊。此外，並要求歐盟會員國內之關鍵服務業者以及特定數位服務提供者，需實施適當安全措施，及於服務受嚴重事件顯著影響時，應通知國家主管機關的必要義務。上述 NIS 指令的要求帶來一系列通用的網路安全技術需求，因此 ETSI 發布此指導文件，提供會員國將 NIS 指令轉換為國家立法或制定相關資訊安全準則之參考。本研究團隊認為此文件為歐盟推展行動寬頻網路安全之最佳實務參考，故已將此文件完整翻譯並於附錄四中供讀者參考，以下為該文件內容重點之摘要。

該文件於第二部分列出參考文件，包含 ETSI 其他資安領域的技術報告與技術標準，也包含其他國家的資安政策文件，如美國 NIST 以及德國內政部，其他尚包含如「資訊技術安全評估之共同標準 (Common Criteria，簡稱 CC)」等。第三部分為相關名詞參考。第四部分概略介紹 NIS 指令針對網路安全之考量與風險分析、資訊分享等事項之討論與規範說明。

第五部分開始針對「網路威脅資訊分享」之要求進行說明。首先，該文件說明實行資安事件通報規定時，為了能讓主管機關或電腦安全資安事件小組 (CSIRT) 採取行動以減少重大資安事件的影響，同時亦不會使該主管機關或資安事件小組負擔過重或造成額外系統風險，遵循以下的原則是很重要的：

- 設定適當的通報範圍：各國在規範關鍵服務業者和數位服務提供者必須通報的資安事件時，其通報範圍應侷限在適當的範圍內，以避免與歐盟其他法律和法規重疊或導致通報規定重覆；
- 制定通報的門檻：若規定應通報時，應考量不同風險與重要性，以及不同服務支援技術架構的多樣性來制定通報門檻；
- 規範一致性：資安事件通報門檻的架構與規範需要充分協調一致，以便讓受資安事件影響的單位能儘速由資安事件中恢復，而非遵守零散或過度的規定。同時，該文件亦同時將可參考的產業規範以及交換威脅情報及防禦資訊的相

關資訊提供指導。

NIS 指令主要針對關鍵服務業者以及數位服務提供者需負擔資安威脅分享的義務，因此該文件也提出結構化的威脅情報分享平台（Structured Threat Intelligence eXchange Platform，簡稱 STIX）相關資訊做為參考。例如 NATO CDXI 與 NCIRC，係指位於荷蘭海牙的北大西洋公約組織（NATO）的資通訊網路防禦及資訊分享單位；網路防禦資料交換與協力基礎建設（Cyber Defence Data Exchange and Collaboration Infrastructure，簡稱 CDIX）隸屬 NATO 的電腦資安事件應變小組（NCIRC），協助 NATO 會員國間有關網路防禦資料交換與網路安全情報交換。

第六部分陳述風險分析所扮演的角色，網路安全風險管理是一種有關評估組織環境風險、了解對組織至關重要的資產、資源及程序，並採取確保組織持續改善其保護、偵測威脅與應變與其資產、資源及程序相關資安事件的辦法。網路安全風險管理與安全措施相關，由於組織資源有限，若能經由風險分析瞭解組織當前面對的可能風險，便能優先分配資源加以進行風險管理。

在概念及方法的部分，該文件提到 ETSI TR 103 305 及相關實施準則，提供了可廣泛利用的有效、可實施的控制方法。此外，許多國家或跨國家組織的資通安全政策及計畫其實早已包含許多廣泛可操作的網路防禦機制，可提供網路風險分析參考。例如由加拿大、法國、德國、荷蘭、英國及美國共同制定之資訊技術安全評估的共同準則（CC）為統一化安全評估標準，以共同評估進入國際市場的資通訊產品的安全性。在本研究前章節介紹英國國家網路安全中心（UK National Cyber Security Centre，簡稱 NCSC）下之基礎建設保護中心（CPNI），也設有網路防禦計畫。另外本研究前章節介紹美國 NIST 的網路安全架構也屬於可用的概念及方法之一。

最後，該文件也針對新興科技所帶來的風險提出了觀察與建議，簡述如下：

- 網路功能虛擬化（NFV）與軟體定義網路（SDN）：網路功能虛擬化（Network Function Virtualization，簡稱 NFV）與軟體定義網路（Software Defined Networking，簡稱 SDN）提供創新的雲端技術與彈性的網路資源管理技術，使網路服務業者可更有效率的運用網路資源提供服務。但 NFV 與 SDN 同時也帶來了新的網路威脅風險，高度軟體化及虛擬化的網路管理提高了系統受到資安侵害的風險，故需實施需要一系列新的和改變後的網路威脅資訊分享

及網路防禦方法。

- 5G 行動網路、行動邊緣運算（Mobile Edge Computing，簡稱 MEC）與物聯網（IoT）。在 5G 中，網路架構有了重大變化，除利用 NFV 與 SDN 技術支援高動態網路管理，且利用網路切片技術（Network Slicing）支援多種類型的網路使用者。行動邊緣運算（MEC）在行動網路的邊緣地帶（edge）提供強大的處理和儲存功能以預先處理大量資訊，因此位於網路邊緣的系統其資訊安全防禦能力不若核心網路完備，較為脆弱易受攻擊。
- 網路服務（Over the Top，簡稱 OTT）與「全面加密」措施。今日出現的重大網路安全挑戰是 OTT 服務與「全面加密」措施的相互結合，提升了通訊的保密性，但這些做法可能帶來不利影響，例如妨礙惡意軟體的偵測及其他網路安全威脅。

由於前述網路新技術帶來的威脅也多樣化，因此含有新標準基礎規範的網路開道網路防禦相關活動有顯著增加，未來將可能利用提升網路邊緣的「middleboxes」安全性以加強網路防禦功能。歐盟希望透過 NIS 指令的實施，強化會員國之間的資安合作，提升網路防禦能力，也因此 ETSI 此一文件可提供各會員國建構完善資安防禦架構所需支各項資安資源之參考。

第七節 小結

觀察美國、加拿大、歐盟、英國、日本等國之主要資安防護體系，依據其政府體制不同而略有差異，但整體來說是大同小異(請參閱表 4-13)。相同的部分是，資安主責單位在其組成或屬性上即具有跨組織協調之特性，或被賦予跨部門協調之權力義務。例如美國國土安全部（DHS）即由原本散佈在聯邦各政府部門的數個單位所組成；日本的網路安全戰略本部為一部跨門組成之機構，由內閣官房之網路安全中心負責日常維運；英國的國家網路安全中心（NCSC）所附屬之政府通訊總部（GCHQ），為政府情報與安全核心；加拿大公共安全部（PS）屬於國家安全機構，本即具有協調聯邦政府所有機構緊急管理、執法、懲戒、預防犯罪和邊界安全的任務。

各國差異之部分，則在於資安事務主責單位屬於事權集中或是分散。美國 DHS、英國 NCSC、加拿大 PS 均屬於事權集中的型態，這幾個國家的主責範圍也不僅只網

路資訊安全，基本上均廣及整體國家安全之維護；而日本及我國則並未設立事權集中之單位，而由跨部會組成之任務編組協調各部會進行。

我國資通安全防護體系之架構²⁶³，於行政院設立國家資通安全會報，幕僚作業由行政院資通安全處辦理，其下設「網際防護體系」及「網際犯罪偵防體系」。網際防護體系由資通安全處主辦，負責整合資安防護資源，推動資安相關政策；網際犯罪偵防體系由內政部及法務部共同主辦，負責防範網路犯罪、維護民眾隱私、促進資通訊環境及網際內容安全等工作。另為積極研議國家資安政策及推動策略，強化產官學研資安技術、情資及經驗之交流及分享，另設資通安全諮詢會作為諮詢單位。

在關鍵基礎設施防護之部分，由於各國關鍵基礎設施有相當大比例為民間私部門所經營，因此非常重視公私協力夥伴（Public-Private Partnership，簡稱 PPP）之角色與責任之確立，在治理部分，建立明確角色與責任，多數以自願性機制推動公私協力關係之建立，這也與後續之資通訊安全資訊分享以及應變通報機制有極大之關連性。

在法律與規範部分，公私部門遵循之安全標準、事件報告、安全作業規範等，均由明確的法制為基礎，並延伸出各種標準規範與管理規範。例如美國於其聯邦資安管理法（FISMA）中即明定由美國標準研究所（NIST）為其資安技術標準之主責單位，多年來，NIST 在資安標準（如 SP 系列）、加密技術（FIPS 系列）等方面，均制定出非常多的標準文件，並進一步成為全球通用的標準，獲得如 ISO 等國際組織之採納；英國標準協會（BSI）亦扮演類似的角色。其他國家如加拿大，雖然在技術標準部分並未指定發展，但於政策說明中已闡述，加拿大將以美國 NIST 或英國 BSI 等機構推出之技術標準為主，著重於國際合作。

而我國目前亦正進行「資安管理法」草案之制定，由於資安事件之複雜與跨機關之特性，故資安管理法提升至行政院層級，由資安處統籌。草案中將政府部門、關鍵基礎設施以及政府捐助成立之財團法人納入管理，主要要求各納管機關應制定資安防護計畫，並有資訊共享集資安事件之通報義務。相較於外國立法例，我國資安管理法重點在於各公務機關與非公務機關之資安責任執行，對於技術標準、公私協力等規範較為不足。同時由於我國資安管理法起步較晚，其他對應之關鍵基礎設施規範以及財

²⁶³ 行政院國家資通安全會報，「行政院國家資通安全會報組織架構圖」，2016/8/1。

團法人規範需仰賴其他配套法制之完善，恐有立法不完整之虞。

我國關鍵基礎設施之規範，於 2014 年 12 月行政院通過《國家關鍵基礎設施安全防護指導綱要²⁶⁴》，由行政院國土安全辦公室（下稱國土辦）負責國家關鍵基礎設施防護之監督、統合，以及跨部門基礎設施防護之協調，並藉由舉辦演練來驗證防護策略及佈署是否到位，進而提升關鍵基礎設施的持續營運韌力及深化國家關鍵基礎設施之防護能量。該綱要中指出，我國關鍵基礎設施（CI）分類採三層架構。第一層為主部門（Sector），分為能源、水資源、通訊傳播、交通、銀行與金融、緊急救援與醫院、中央與地方政府機關、高科技園區等 8 類。

我國之關鍵基礎設施保護規範相較於其他國家差異不大，然而，由於資安管理法尚未完成制定，因此關鍵基礎設施之資安維護規範不足，但我國已成立行政院資安會報並設置行政院資安處，可與國土辦相互協調合作。

最後，國外針對資通訊設備之資安檢驗，多仍採取自願參與，政府部門除與國家安全有關之系統外，並未強制業者必須將設備通過檢驗。本計畫建立行動寬頻基站資安檢測機制，未來亦應思考與政府採購等機制結合，鼓勵業者將設備送測，進一步維護資通訊系統之安全。

表 4-13 各國資安體系與任務比較

國家 比較項目	美國	英國	日本	加拿大	我國
主要執行機關	國土安全部 (DHS) 網路安全與 通訊辦公室 (CS&C)	政府通訊 總局 (GCHQ) 國家網路 安全中心 (NCSC)	網路安全戰 略本部(跨部 會) 內閣官房 網路安全中 心	公共安全部 (Public Safety)	行政院 資通安全 處

²⁶⁴ 交通部，“國家關鍵基礎設施安全防護指導綱要”，2014/12/29。

國家 比較項目	美國	英國	日本	加拿大	我國
通訊傳播部門 主責	DHS (FCC 協助)	NCSC (Ofcom 協 助)	總務省	創新部 (ISED) 電訊安全諮 詢委員會 (CSTAC)	通傳會
技術標準	商務部 (DoC) 國家標準技 術研究所 (NIST)	創新部 (BIS) 英國標準 協會(BSI)	經產省 JIS 標準	公共安全部 發展網路事 件管理架 (CIMF)	參考國外
政策監督	白宮 預算辦公室 (OMB)	內閣辦公 室	內閣官房	總理辦公室	總統府國 安會、 行政院資 通安全會 報
防護重點	聯邦重要安 全系統	關鍵基礎 設施	政府機關及 關鍵基礎設 施	關鍵基礎設 施	關鍵基礎 設施
產業資安政策	自律	自律	自律	自律	自律
立法	聯邦資訊管 理法 (FISMA) 國土安全法 (HSA)	2003 通訊 法賦予 Ofcom 監 督電信業 者資料保 護之責任	網路安全基 本法		資通安全 管理法(草 案)

資料來源：本團隊整理

第五章、行動寬頻資安技術研究

第一節 空中介面資安技術研究

本工作項目將從行動寬頻網路運作過程中最基礎的空中介面資安技術，透過文獻分析及實驗方法，探討空中介面相關之資安議題，包含探討偽基站造成用戶端(UE)隱私之可能資安議題，提出可能之解決方案。另透過文獻分析，研析新一代的語音通信技術 VoLTE 對 LTE 網路所產生的安全漏洞與防禦技術。

於期中報告工作項目之空中介面資安技術研究，首先針對近年資安事件頻傳之偽基站造成之資安議題進行研究，並設計偽基站之實驗平臺及實驗項目，期末將以實測方式進行偽基站之資安技術探討，提出可能的資安威脅與解決方案；另外在 VoLTE 資安技術探討上，期中已完成 VoLTE 造成基站(eNodeB)與核心網路(EPC)之可能資安威脅進行研析，並提出建議之解決方法，期末將針對用戶端可能遭受之資安威脅進行研析，並提出相關解決方法。

一、偽基站資安技術探討

2018 年 3 月 5 日 YAHOO 新聞報導『4G 網路存在 8 種漏洞，用戶手機安全及私隱無保障²⁶⁴』就在近期大學研究人員使用了一種名為 LTEInspector 的測試方法來進行實驗，檢測網路是否存在漏洞，實驗結果表明在美國四大營運商網路發現並以確認了 8 種 4G LTE 網路安全漏洞。而安全漏洞的產生是因為協議信息中缺乏適當的認證，加密和傳送保護，未能保護到用戶的隱私問題。這些攻擊利用常見的研究設備和開源 4G LTE 協議軟體發起，以冒充他人手機登錄網路及追蹤用戶的位置。

大學研究人員還由此發現了一系列利用 4G LTE 網路協議中存在的漏洞進行攻擊，會監視用戶的通話、信息、設備離線、跟踪用戶位置並發送虛假警報等 10 種攻擊，對用戶的隱私以及安全問題影響極大。

²⁶⁴ Yahoo 新聞, “4G 網路存在 8 種漏洞，用戶手機安全及私隱無保障”, 2018/3/5

2017 年 3 月提供網路安全設備產品及解決方案的公司 Check Point Software 報導指出，中國大陸發生利用偽基站設備，假冒電信業者(如中國移動及中國聯通)名義發送簡訊，傳播惡意程式"Swearing Trojan"的案例，該惡意程式為 Android 之惡意木馬程式。

Swearing 木馬程式可以從受感染的設備收集用戶個人資訊及相關認證資訊，甚至攔截簡訊(SMS)訊息，截取銀行機構使用的雙向認證或其它一次性代碼等。該 Android 木馬程式開始於中國行動寬頻網路，目前已開始蔓延全球，根據統計，全球至少有 1,000 萬用戶被感染，中國和印度的 Android 手機被感染的最多。資安業者 Check Point 認為，透過偽基站傳送 SMS 訊息是很容易欺騙用戶的一種方式，利用 Swearing 惡意程式的攻擊活動若是透過偽基站方式誘騙用戶，將可能進一步推動此惡意程式的蔓延²⁶⁵。

由上述近年的新聞報導可看出，偽基站問題已受到全球的重視。在 3GPP LTE 標準規範中，為防止用戶端(UE)選擇其他遠方的基站，所產生上行鏈路訊號干擾影響，用戶端(UE)僅需搜索訊號最強之基站。假設一個偽基站在其功率發射，顯示在用戶端(UE)選擇頻率通道的最強基站，則用戶端(UE)將嘗試駐留到偽基站並不能夠選擇該通道其他任何 LTE 基站，這可能會造成 LTE 網路拒絕存取導致服務中斷。其通訊信令如圖 5-1 所示。

表示 UE 選擇細胞之過程，第一階段 NAS 選中公眾行動電話網路(Public Land Mobile Network，簡稱 PLMN)後提供給 RRC 層，RRC 層透過 PHY 層掃描 UE 支援的頻段，依據接受到的訊號強度指示(Received Signal Strength Indication，簡稱 RSSI)，判定是否有超過 RSSI 門檻值，若有超過 RSSI 門檻值，則代表該 RF 訊號被認為是可接通的，再來會進行細胞的搜尋。

第二階段 UE 端在選擇細胞時，先透過主要同步訊號 (Primary Synchronization Signal，簡稱 PSS) 與輔助同步訊號 (Secondary Synchronization Signal，簡稱 SSS) 進行同步，確定同步才能在正確的訊框位置抓取到主系統訊息(Master Information Block，

²⁶⁵ The Hacker News, "Hackers Using Fake Cellphone Towers to Spread Android Banking Trojan", 2017/3/22.

簡稱 MIB)，透過 PSS、SSS 以及 MIB 可以獲得 System Information Block type 1 (SIB 1) 訊息，訊息內容有 PLMN 以及追蹤區域碼 (Tracking Area Code，簡稱 TAC)、行動裝置國家代碼 (Mobile Country Code，簡稱 MCC) 以及行動裝置網路代碼 (Mobile Network Code，簡稱 MNC)，供 UE 端做為選擇細胞的依據，而 UE 根據收到的 SIB 1 裡提供的細胞選擇資訊以及訊號品質判定該細胞是否能夠接取。

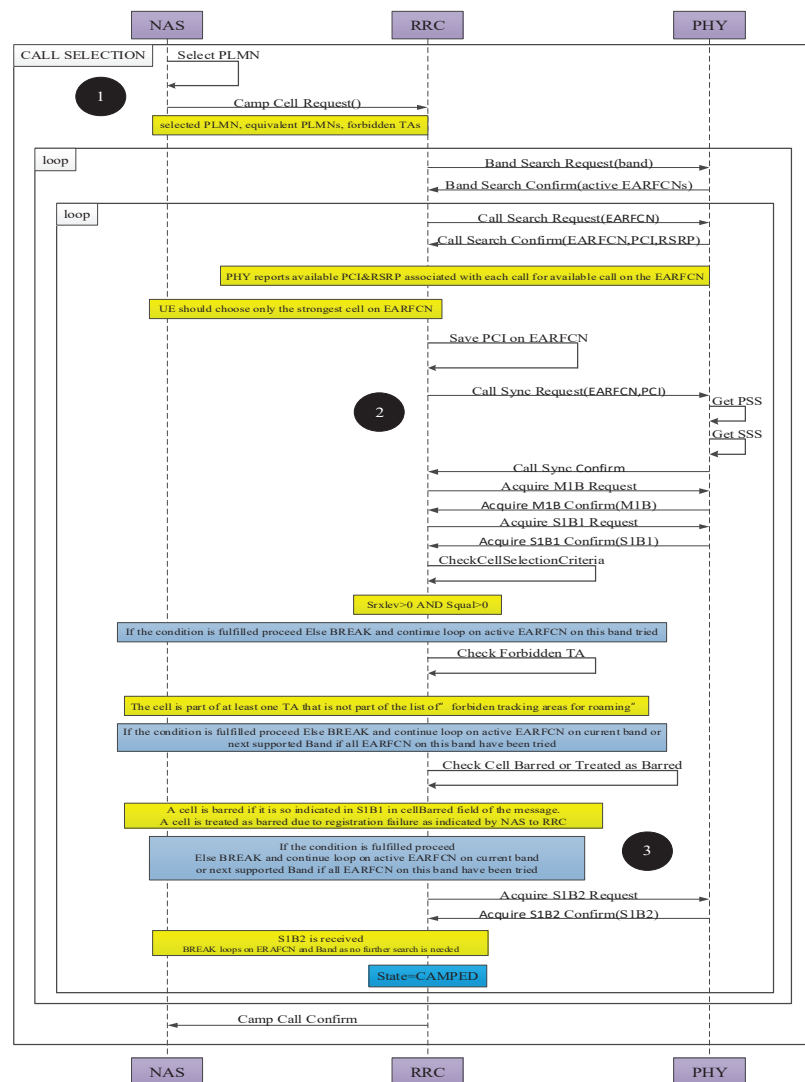


圖 5-1 初始細胞選擇程序

資料來源：本團隊整理

如果一個或多個選擇細胞的條件無法符合，PHY 層繼續掃描其它支援的頻段，直到適合的細胞出現。一旦 UE 在一個細胞上駐留時，UE 將會進行與網路接取過程。接取過程有隨機接取過程、認證以及 RRC 的重新配置等。認證成功，則 UE 將紀錄

新的追蹤區域(TA)，如果 UE 與網路之間的相互認證失敗，則 UE 將對細胞做處理，例如：UE 將排除禁止的細胞，在三百秒內認為該細胞是非首選擇。

(一) 偽基站造成之資安議題

在 LTEInspector 研究文獻²⁶⁶，作者提出一個檢測系統如圖 5-2 所示，利用此檢測系統將協定分析方式以系統化進行，檢測在 UE 端每個階段狀態下，收到不同的信令而有所反應，進而利用偽基站觸發 UE 出現錯誤行為。

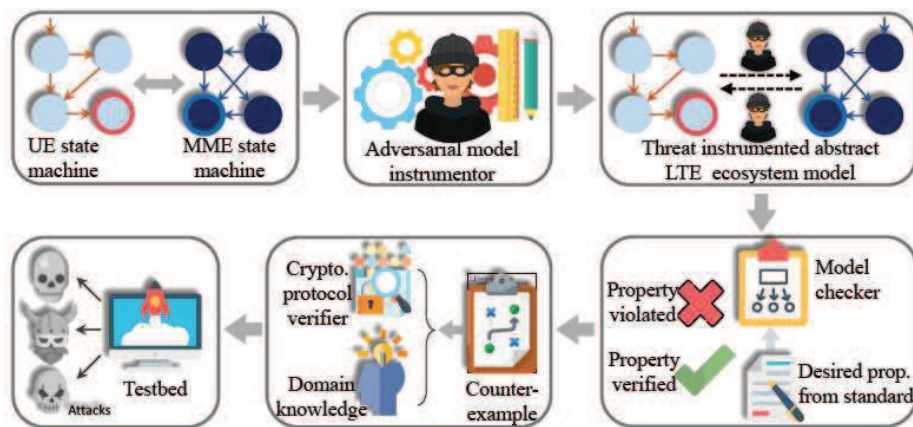


圖 5-2 檢測系統架構

資料來源：LTEInspector

本團隊參考 LTEInspector 系統整理偽基站可能造成之資安議題及說明如下：

1. A-1. Authentication Synchronization Failure Attack(認證同步失敗攻擊)

在 Authentication and Key Agreement(AKA，Attach 程序的一環)中，UE 端會檢測 sequence number 的健全性(即 $XSQN - SQN \leq Range$)，此項攻擊方式利用這點，惡意裝置 UE 偽造受害者 UE 發起 Attach(帶有受害者 IMSI)，打亂 sequence number 的健全性($m > range$)，導致認證失敗。結果：受害者 UE 無法連線至核心網路，失去網路服務。

²⁶⁶ Hussain, S. R., Chowdhury, O., Mehnaz, S., & Bertino, E. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE.

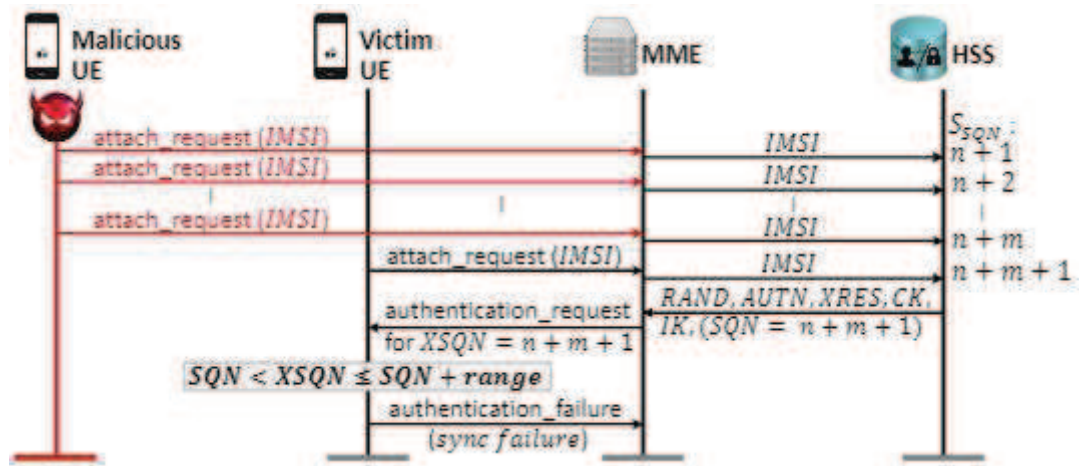


圖 5-3 認證同步失敗攻擊程序

資料來源：LTEInspector

2. A-4. Authentication Relay Attack(認證中間人攻擊)

攻擊者同時扮演惡意裝置 UE 與偽基站的角色，受害 UE 向偽基站發起 Attach 程序，偽基站將訊息傳給惡意裝置 UE，向合法基站發起 Attach 程序，透過中間人的方式將整個 Attach 程序完成。

結果：若電信業者未執行加密演算法（即在 security mode command 採取 EEA0），會造成之後所有傳送的資訊洩漏。

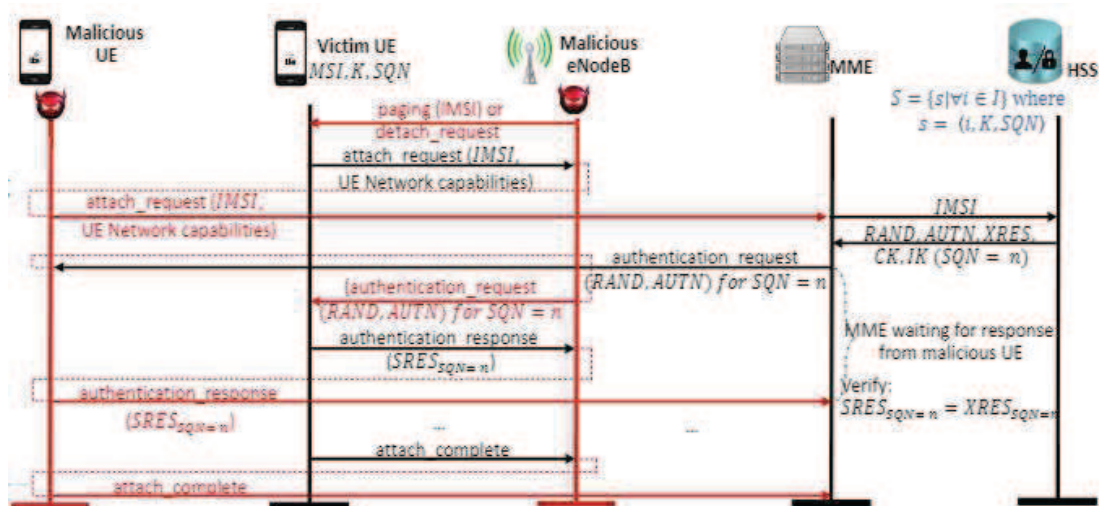


圖 5-4 認證中間人攻擊程序

資料來源：LTEInspector

3. A-2. Traceability Attack(追蹤攻擊)

在正常狀態下，UE 收到 security mode command 時，UE 會透過驗證 MAC 來確認訊息的完整性，若完整性無誤，即回應 security_mode_complete，攻擊者利用這點，捕捉到特定受害 UE 的 security_mode_command，透過偽基站傳送，只會有對應的受害 UE 回應 complete，其餘皆會回應 reject，以此確認特定的受害 UE 有沒有出現在偽基站所屬區域內。結果：能判斷特定用戶是否出現在該區域。

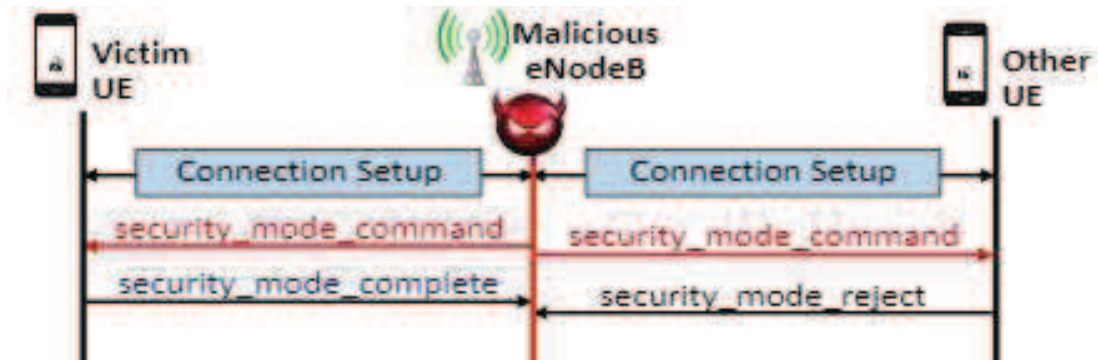


圖 5-5 追蹤攻擊程序

資料來源：LTEInspector

4. A-3. Numb Attack

以偽基站的形式傳送 Authentication Reject，因認證拒絕使 UE 失去服務。因為 UE 不會自行重新連結網路或是降至 2G/3G，需重新開機才能解決問題，故作者命名為 Numb Attack。結果：受害者 UE 無法連線至核心網路，失去網路服務。

5. P-1. Paging Channel Hijacking(尋呼通道劫持)

為了省電考量，UE 不會長時間與核心網路保持連接，而是會在一段時間內去接收 Paging 訊號，以 Paging 訊號內容判斷需不需要重新連接核心網路（例：有來電訊息），攻擊者透過偽基站與合法基站相同的 paging channel，發送 empty paging message，讓受害 UE 認為不需要重新連接網路。結果：讓受害 UE 漏接通話與訊息等。

6. P-2. Stealthy kicking-off Attack

與 P1 概念類似，一樣使用與合法基站相同 paging channel，不同的是，此次的

paging 訊號內容帶著受害 UE 之 IMSI 進行呼叫，受害 UE 會與原先核心網路斷開，並重啟 attach 程序，作者提到可以搭配 A4 進行後續攻擊。結果：受害 UE 轉 attach 至偽基站。

7. P-3. Panic Attack(假緊急警報攻擊)

在這個攻擊中，攻擊者想要向大量的 UE 注入假的緊急尋呼訊息(emergency paging messages)，偽基站發送具有假的緊急警告的尋呼訊息，為了確保這種假的尋呼消息大量的送達 UE，偽基站持續廣播該消息用於合法 eNodeB 的所有可能的尋呼時機。

結果：發送假警報，其威脅的影響，造成大眾誤信緊急訊息之內容，例如：人為的恐怖活動。

8. P-4. Energy Depletion Attack(電力消耗攻擊)

這個攻擊的想法是讓受害者 UE 執行耗電的加密操作，實現此目的的一種方法是強制 UE 透過在連續兩個 Attach 過程之間發送具有 IMSI 的尋呼消息來一次又一次地繼續執行耗電的 Attach 過程，在偽基站知道受害者 GUTI 的情況下，它可以發送具有 GUTI 的尋呼消息，UE 用加密服務請求消息進行響應，透過 P-2，迫使受害 UE 不斷進行 Attach。結果：電力耗損，造成用戶無法使用裝置。

9. P-5. Link ability Attack(鏈接性攻擊)

此攻擊上未被作者實作，Broek 等人相信這攻擊能被實現，在 4G LTE 的情況下，攻擊者可以 paging 訊息去證實受害 UE 是否有在覆蓋範圍內，造成地理位置資訊洩漏。結果：在與受害者 UE 的 IMSI 廣播尋呼之後，如果攻擊者觀察到具有相同 IMSI 的 Attach 請求，則攻擊者可以確認受害者 UE 的存在。

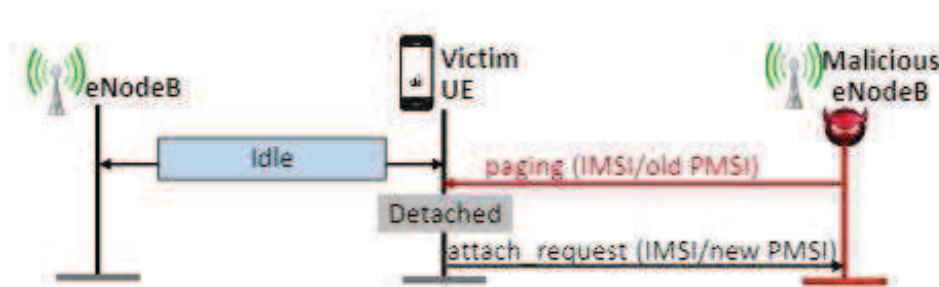


圖 5-6 鏈接性攻擊程序

資料來源：LTEInspector

10. D-1. Detach / Downgrade Attack(斷線/降等攻擊)

這個攻擊中，當受害 UE Attach 至偽基站時，攻擊者發起 detach_request，而 UE 端會接受這個請求，失去服務或是降等，中斷受害者 UE 的網路服務。結果：阻斷服務。

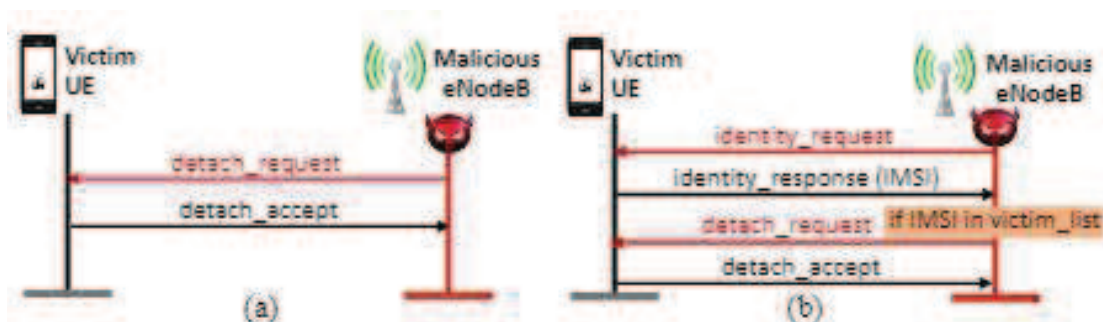


圖 5-7 斷線/降等攻擊程序

資料來源：LTEInspector

經由上述整理，發現研究人員利用 LTEInspector 模擬 UE 與 MME 之間的協定，分析完協定錯誤後再用偽基站(SDR + OpenSource eNodeB)去驗證攻擊，偽基站為系統架構中最後的 Testbed 測試平臺，其論文發表的 10 種攻擊，A1、A4 需偽 UE，其餘僅需偽基站，彙整說明如下：

- 資訊洩漏：A-4 項目是因為電信商設定不當的安全命令模式 EEA0(不加密)，造成資訊洩漏，故能監視 4G 通訊內容及訊息；
- 用戶位置跟蹤：A-2 及 P-5 這 2 項，透過用戶回傳信令內容，可追蹤用戶位置資訊。

- DoS 服務阻斷攻擊(含 2G 降等)：共 5 項為 A-1, A-3, P-1, P-2, D-1，阻斷用戶連結正常行動網路之可用性；
- 消耗用電力：P-4 項目為不斷透過偽基站尋呼程序(paging)，進而消耗用戶手機電力。
- 假警報告警：P-3 項目為使用尋呼程序傳送假警報(emerge message)。

(二) 偽基站檢測項目實測

透過上述程序說明，攻擊者可架設一個功率較為強大的偽基站，透過模擬核心網路與基站之行為，廣播偽基站的訊息偽裝成一個合法的電信業者網路，讓 UE 端在進行細胞選擇的過程認為偽基站為最佳選擇，誘使 UE 駐留。

1. 以行動網路模擬器架設偽基站實驗

在本團隊規劃的測試環境下，以 R&S CMW-500²⁶⁷ 行動網路模擬器，建置實驗測試平台，以模擬偽基站之行為，如圖 5-8 所示。

1.1. 偽基站阻斷式攻擊 (Denial of Service，簡稱 DoS)

本研究進一步根據電信業者參數設定，驗證偽基站在 LTE 控制通道欺騙的效果，如圖 5-9 及圖 5-10 所示。偽基站的設定須依據商用行動網路環境的參數設定，以使 UE 啟動與偽基站的接取程序，而這些參數的取得一般由手機的工程模式即可取得對應的營運業者的網路資訊，如表 5-1 所示，對國內某家電信業者之用戶測試，以證明攻擊的真實性。

²⁶⁷ C. Gessner and A. Roessler, "LTE technology and LTE test; a deskside chat," Rohde & Schwarz, 2009.

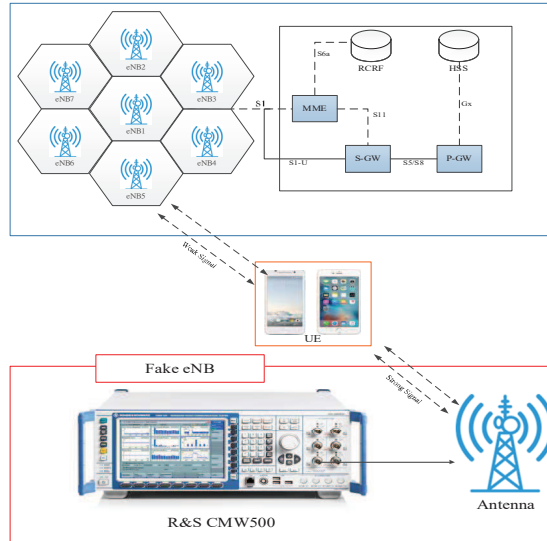


圖 5-8 偽基站測試平台架構

資料來源：本團隊繪製

表 5-1 偽基站參數一覽表

參數	名稱	描述
Current Time	因為 UE 通電時連接傳遞時間	秒
PS State	UE 狀態	連接或未連接
LTE Band	LTE 頻段	Band3
LTE BW	LTE 頻寬	10MHz
Tx Channel	EARFCN 下行鏈路	1857.5MHz
Rx Channel	EARFCN 上行鏈路	1762.5MHz
Cell ID	UE 選擇 eNodeB 的 ID	可以從智慧型手機使用 API 呼叫顯示
MCC	行動裝置國家代碼	466
MNC	行動裝置網路代碼	92
TAC	追蹤區域代碼	60222
TAI	Tracking Area Identity(TAI)全球性的編號	MCC +MNC+TAC 所組成
IMSI	移動用戶識別碼	IMSI 來自 SIM 卡

資料來源：本團隊整理

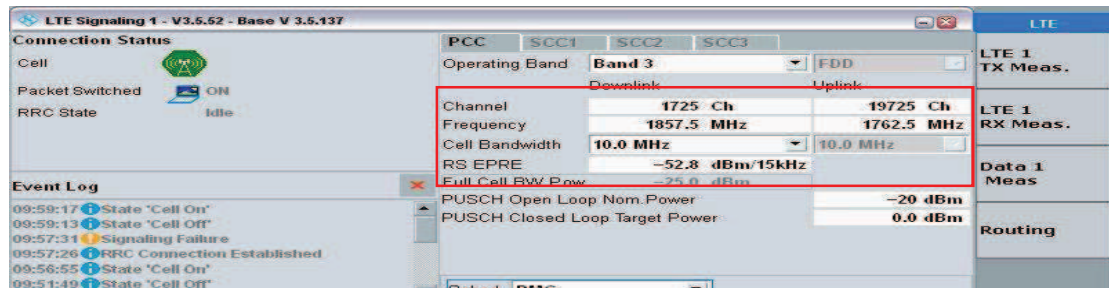


圖 5-9 行動網路模擬器偽基站設定上下行鏈路

資料來源：本團隊製作

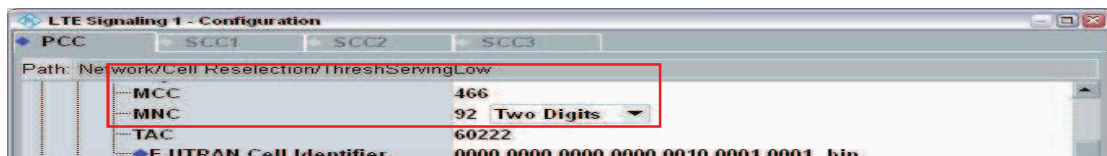


圖 5-10 行動網路模擬器偽基站設定 MCC、MNC 與 TAC

資料來源：本團隊製作

在通訊過程中，手機將嘗試連接偽基站，但 AKA 協商失敗，手機收到 Attach Reject 信令，如圖 5-11 所示，信令內容為 PLMN not allowed，如圖 5-12 所示，當關閉偽基站後手機大約 300 秒後手機連回電信營運商。



圖 5-11 手機收到 Attach Reject 信令

資料來源：本團隊製作

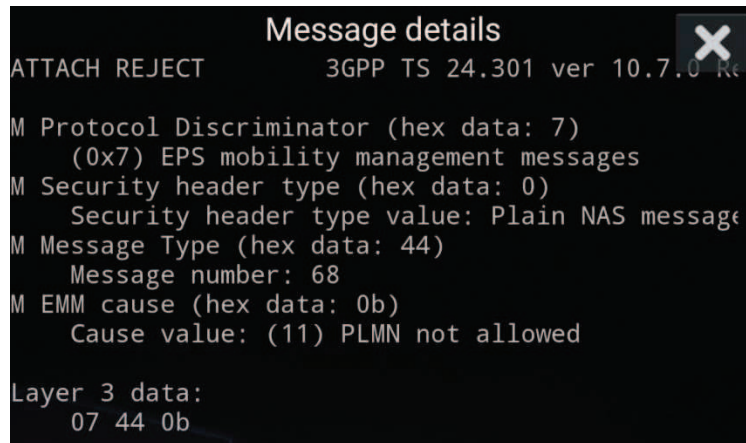


圖 5-12 手機收到 Attach Reject 信令內容 PLMN not allowed

資料來源：本團隊製作

手機將偽基站作為新的細胞選擇，PHY 層將報告最強的細胞，UE 將嘗試連接偽基站，但 AKA 協商失敗，UE 收到 Attach Reject 為 Illegal UE，如圖 5-13 所示，當關閉偽基站，手機仍然無法連回電信營運商，除非開啟飛航模式或重新開機。

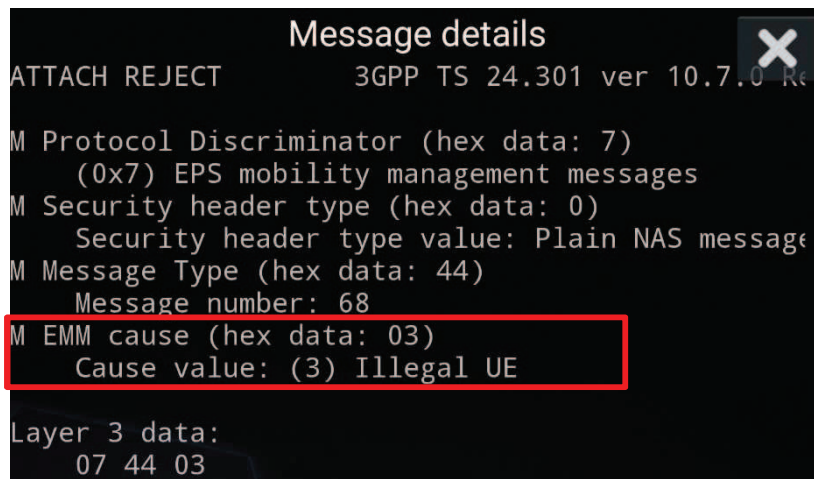


圖 5-13 手機收到 Attach Reject 信令內容 Illegal UE

資料來源：本團隊製作

1.2. 偽基站進行設備與身份追蹤

IMSI 與 IMEI 作為 SIM 卡與手機硬體唯一的標識符號，這兩個標識符號可以辨識是否出現在細胞的覆蓋範圍內。在 Attach 尚未完成前，EPC 端與 UE 端尚未完成認證與加密等相關程序，UE 端會向 EPC 端進行註冊的動作，發起的 Attach Request 為明文傳輸且帶著個人識別碼 IMSI，當 UE 端與 EPC 端完成註冊時，EPC 端將派發臨時碼給使用者，並將此臨時碼與 IMSI 在 EPC 內部建立關聯性，而臨時碼用於往後無

線介面傳輸之識別用。

當 UE 端依附至偽基站時，手機發起的 Attach Request 可讓偽基站捕捉到 IMSI 碼，透過此 IMSI 碼，可以判斷受害者是否出現在偽基站訊號覆蓋範圍內。實驗參數如表 5-2 所示。

表 5-2 偽基站進行設備與身份追蹤參數一覽表

參數	名稱	描述
Current Time	因為 UE 通電時連接傳遞時間	秒
PS State	UE 狀態	連接或未連接
LTE Band	LTE 頻段	Band8
LTE BW	LTE 頻寬	10MHz
Tx Channel	EARFCN 下行鏈路	935MHz
Rx Channel	EARFCN 上行鏈路	897.5MHz
Cell ID	UE 選擇 eNodeB 的 ID	可以從智慧型手機使用 API 呼叫顯示
MCC	行動裝置國家代碼	466
MNC	行動裝置網路代碼	89
TAC	追蹤區域代碼	60222
TAI	Tracking Area Identity(TAI)全球性的編號	MCC +MNC+TAC 所組成
IMSI	移動用戶識別碼	不設定

資料來源：本團隊整理

R&S CMW500 參數設定如圖 5-14 與圖 5-15 所示。

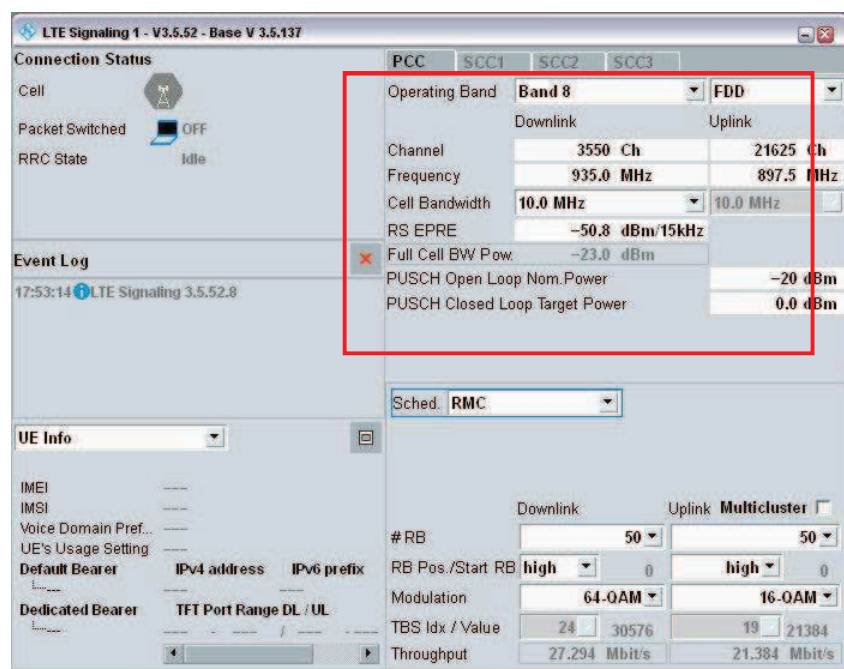


圖 5-14 設備與身份追蹤設定上下行鏈路

資料來源：本團隊製作

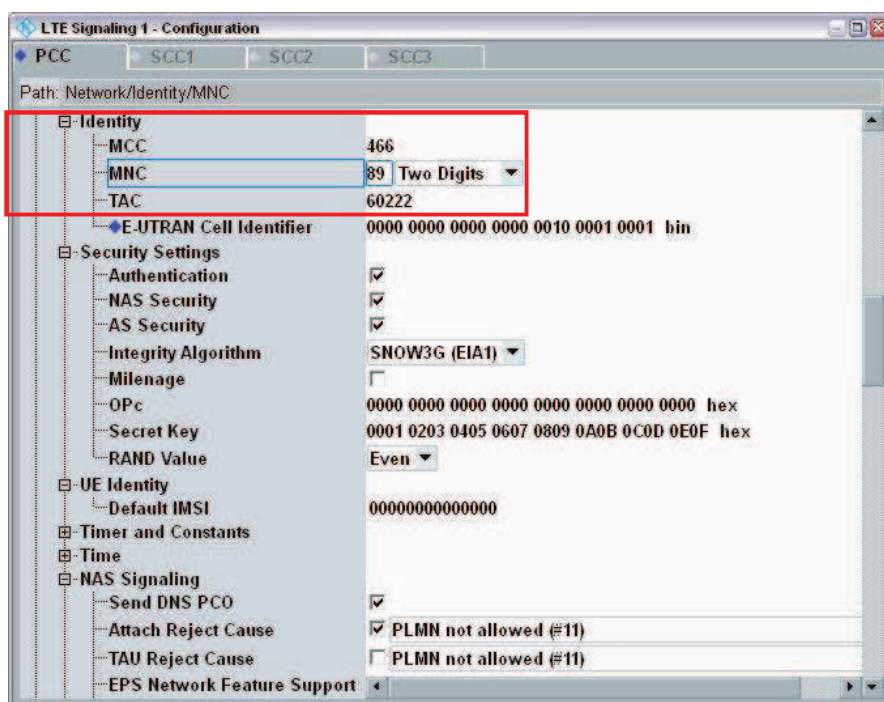


圖 5-15 設備與身份追蹤設定 MCC、MNC 與 TAC

資料來源：本團隊製作

Bit			
ID=301 TS=2016-06-22 11:17:32.574 RFN=0			
Byte	Bitstream	Identifier	Value
40		Choice	
40		Identity Digits	
40		Mobile Identity digits	
40	0100----	IdDigit	0x4 4
41	----0110	IdDigit	0x6 6
41	0110----	IdDigit	0x6 6
42	----1000	IdDigit	0x8 8
42	1001----	IdDigit	0x9 9
43	----0001	IdDigit	0x1 1
43	0000----	IdDigit	0x0 0
44	----0000	IdDigit	0x0 0
44	0000----	IdDigit	0x0 0
45	----0111	IdDigit	0x7 7
45	0011----	IdDigit	0x3 3
46	----1001	IdDigit	0x9 9
46	0100----	IdDigit	0x4 4
47	----0000	IdDigit	0x0 0
47	1001----	IdDigit	0x9 9
48		EndMarkDigit	

圖 5-16 偽基站收到手機 IMSI

資料來源：本團隊製作

Bit				
ID=290 TS=2016-06-22 11:17:32.527 RFN=0				
Byte	Bitstream	Identifier	Value	Interpretation
39		Mobile Identity - (LV)		
39	00001011	Length	0x0B 11	
40	-----110	Identity type	0x6 6	GUTI
40	-----0---	number of digits in ID (odd even (also when GUTI is used)	0x0 0	
40		Mobile Identity (GUTI)/IMSI		
40		GutiValue		
40	1111----	PadDigit	0xF 15	
41		MCC/MNC digits		
41	----0100	MCC[1]	0x4 4	
41	0110----	MCC[2]	0x6 6	
42	----0110	MCC[3]	0x6 6	
42	1111----	MNC[3]	0xF 15	
43	----1000	MNC[1]	0x8 8	
43	1001----	MNC[2]	0x9 9	
44	10000000	MME Group ID	0x8002 32770	
45	00000010			
46	01110010	MME Code	0x72 114	
47	11100000	M-TMSI - (V)[0]	0xE0 224 'à'	
48	10000110	M-TMSI - (V)[1]	0x86 134 '?'	
49	11111011	M-TMSI - (V)[2]	0xFB 251 'ó'	
50	11111000	M-TMSI - (V)[3]	0xF8 248 'ø'	

圖 5-17 偽基站收到手機 GUTI

資料來源：本團隊製作

實驗結果驗證偽基站無法 Attach，手機將嘗試連接假 eNodeB，但 AKA 協商失敗，當關閉偽基站後手機連回電信營運商網路，但是偽基站取得手機的 IMSI，如圖 5-16 所示，GUTI 如圖 5-17 所示，能夠識別特定手機是否存在(或不)在特定的位置。

1.3. 軟體定義無線電與 Open Source

在本團隊研究中，除了利用 R&S 通訊協定模擬器 CMW-500 架設成偽基站外，軟體無線電（Software Defined Radio，以下簡稱 SDR）搭配 Open Source 軟體也能成為一個偽基站，SDR 的概念是希望在既有的基礎元件上，以軟體定義接收端或傳輸端的通訊協定架構，再接下來的實驗使用 USRP B210 作為訊號的發送與接收端，如圖 5-18 所示，其硬體 RF 頻率支援 70MHz~6GHz、全雙工以及 MIMO 等特性，足夠支援 LTE 的架設。

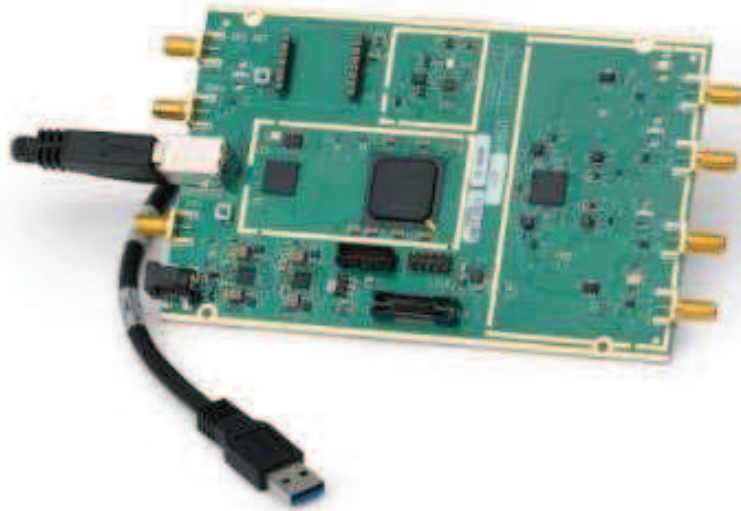


圖 5- 18 USRP B210

資料來源：Ettus Research²⁶⁸

目前有幾種 Open Source 軟體能夠搭配 USRP B210 建置成為完整 LTE 行動網路系統，例如：OpenLTE²⁶⁹、srsLTE²⁷⁰與 OpenAirInterface²⁷¹。目前最常被使用於架設偽基站的 Open Source 軟體當屬 OpenAirInterface（以下簡稱 OAI），而團隊也架設 OAI，進行偽基站實驗，目的是驗證 Open Source 軟體是否可以進行偽基站攻擊，未來有心人士是否能以低成本設備架設偽基站。

²⁶⁸ Ettus Research, [Online]. Available: <https://www.ettus.com/product/details/UB210-KIT>

²⁶⁹ Open LTE, [Online]. Available: <http://openlte.sourceforge.net/>

²⁷⁰ srsLTE, [Online]. Available: <https://github.com/srsLTE/srsLTE>

²⁷¹ OpenAirInterface, [Online]. Available: <http://www.openairinterface.org/>

OAI 是由 EURECOM 組織所發起的 Open Source SDR 項目，分別實現了 LTE 系統中核心網路 EPC 與無線存取網路 EUTRAN 兩大主軸的通訊協定，如圖 5-19 所示，核心網路中的 HSS、MME、S-GW 及 PDN-GW 由電腦內部虛擬連接，再經由實體線路連結至另一台電腦，該電腦及 USRP B210 模擬成 EUTRAN 無線存取網路基地台部分。

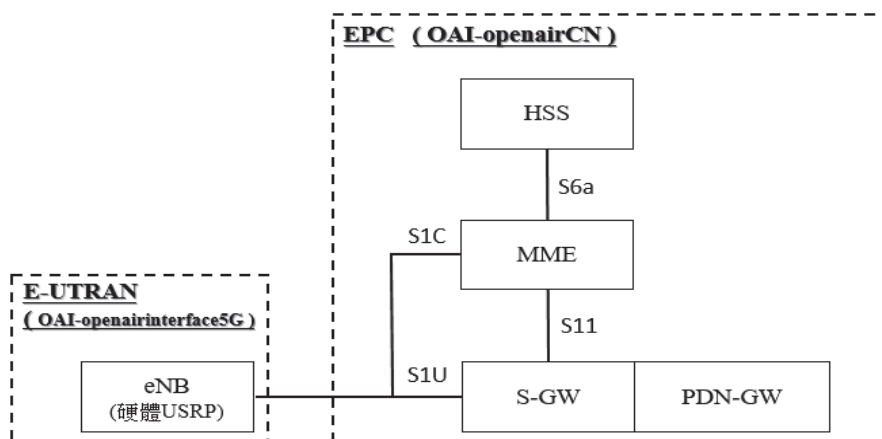


圖 5-19 OAI 架構

資料來源：本團隊製作

1.4. TAU 程序測試

在 TAU 程序測試中，本團隊將 TAC 設置為 60222，讓手機端接受到，誤認為進入到新的區域後，手機端將會執行 TAU 程序，偽基站在收到 TAU 的 Request 之後隨即回覆 TAU Reject 訊息給手機端，其中 TAU Reject 訊息包含的 Cause Code 為 EPS services and non-EPS services not allowed。

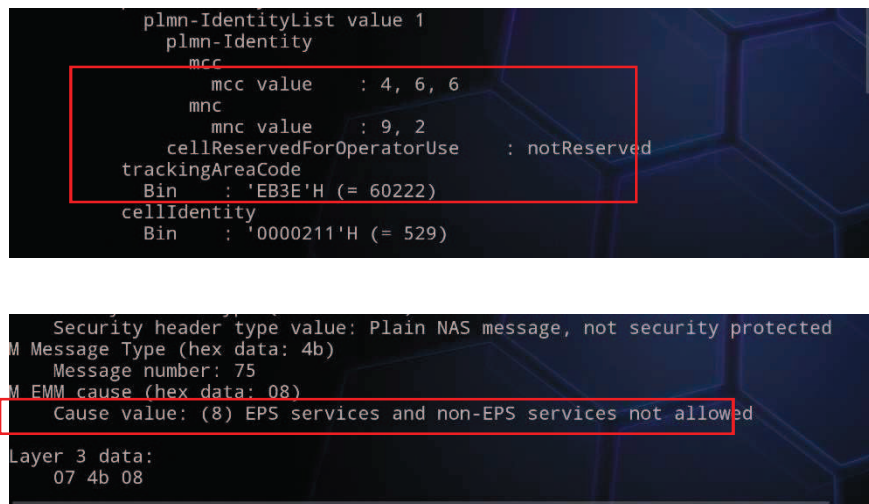


圖 5-20 TAU Reject 訊息

資料來源：本團隊製作

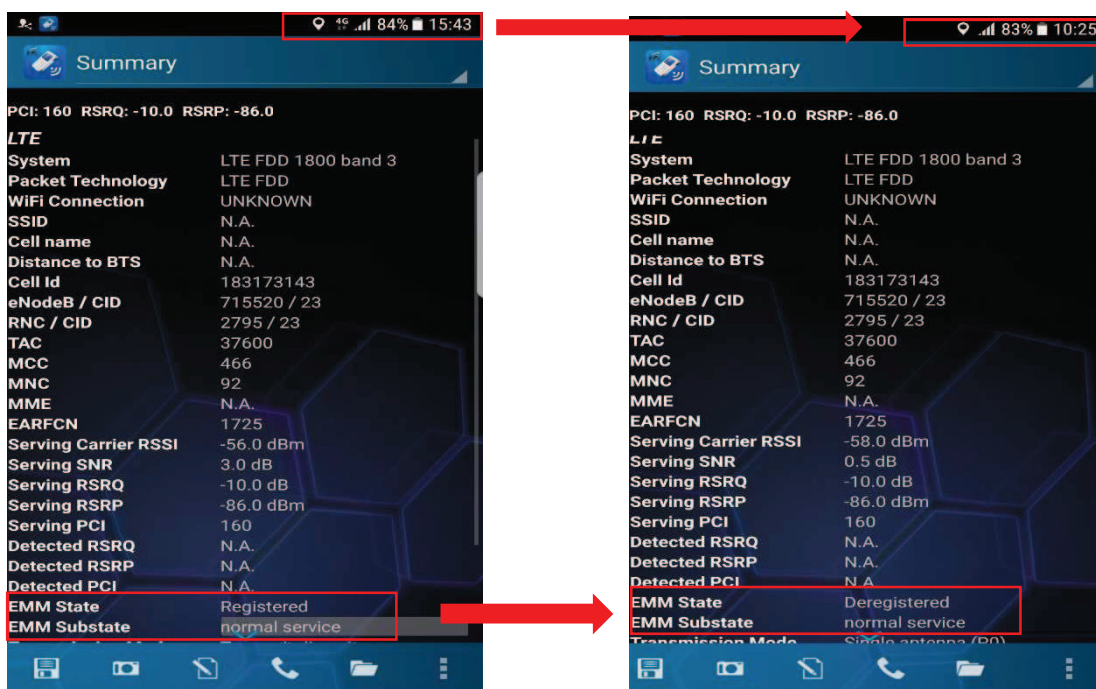


圖 5-21 TAU 程序測試-UE 端畫面

資料來源：本團隊製作

如圖 5-20 所示，手機端會接收到本團隊偽基站所發出的訊息，在依附該為基站後，根據 TAC 為 60222 與原先 37600 不同，判斷需進行 TAU 程序，而隨後收到的

TAUReject 訊息，UE 端解讀其 Cause Code，認定自身無法使用 EPS 與非 EPS 網路，導致讓 UE 端的 EMM state 為 Registered 轉變為 Deregistered 進而使手機端失去通訊能力，達成阻斷式攻擊之結果，如圖 5-21 所示。

1.5. 個人識別碼捕捉

如圖 5-22 所示，本階段實驗使用 OAI 建置偽基站，OAI 可以搭配 Wireshark 觀察 LTE 訊令的傳遞。本團隊將此偽基站頻段設置在 Band 3 中下行頻率為 1857.5MHz、上行頻率為 1762.5MHz、MCC 為 466、MNC 為 92 以及 TAC 為 1，將廣播訊號傳播出去，創造假新區，等待手機依附。

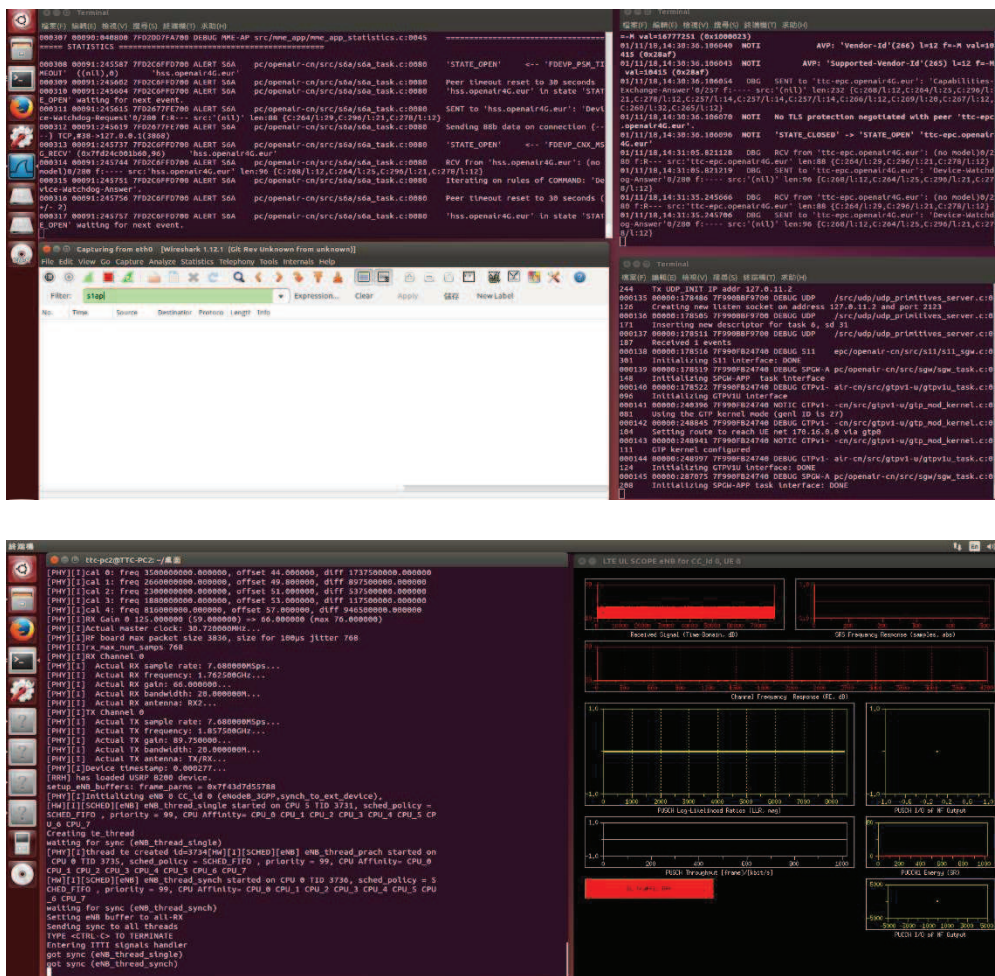


圖 5-22 OAI 操作畫面

資料來源：本團隊製作

如圖 5-23 所示，此用戶之個人識別碼為 466924250XXXXXX，本團隊將偽基站開啟，等待手機端接受到偽基站的訊號時，



圖 5-23 UE 端個人識別碼

資料來源：本團隊製作

手機端會進行 TAU 程序，如圖 5-24 所示，偽基站回應的 TAU Reject 訊息中的 Cause Code 為 UE Identity cannot be derived by the network，這會使 UE 端在接收到 Reject 訊號後，會重新發起 Attach，內容會將自己的個人識別碼一併發送出去，此時就能被偽基站端捕捉到，如圖 5-25 所示。

以上實驗證明使用 Open Source 軟體，也可以架設偽基站進行 TAU 程序測試、個人識別碼捕捉等實驗，有心人士能以軟體無線電（Software Defined Radio，以下簡稱 SDR）輕易架設偽基站進行攻擊，甚至可以進行降階攻擊的手法，讓手機降階至尋找 2G 服務，而攻擊者可透過 OpenBTS 架設 2G 偽基站，誘使手機進行註冊，當註冊成功時 2G 偽基站發送一封包含下載惡意軟體網址簡訊給手機，當使用者下載並安裝惡意軟體，此時有心人士就可對手機進行攻擊。

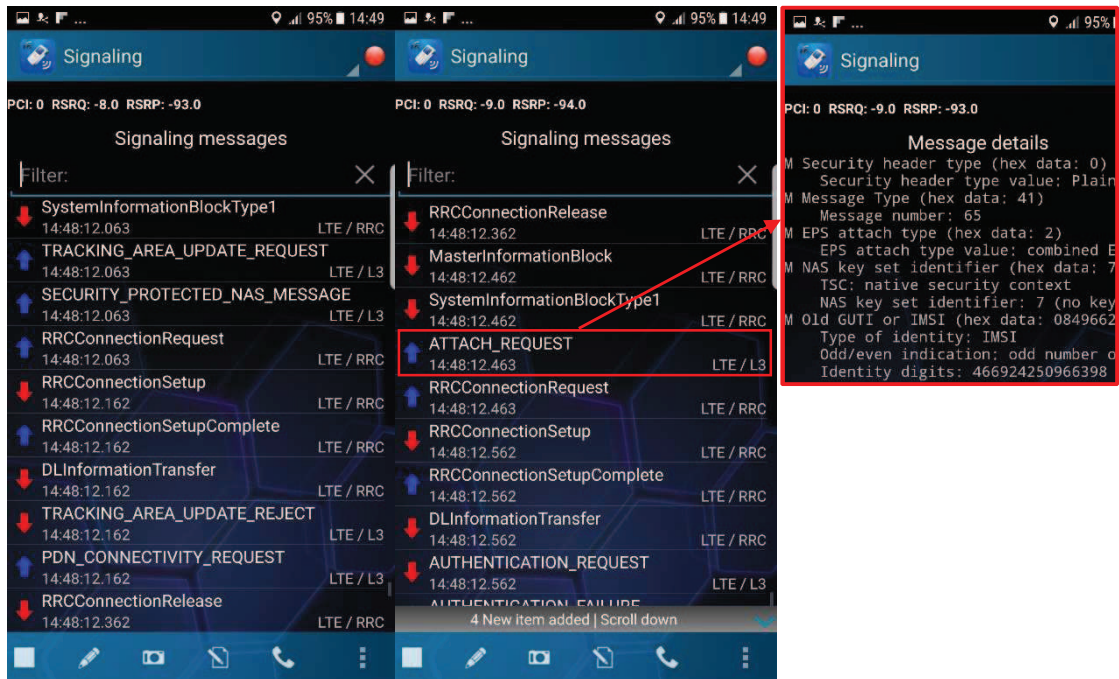


圖 5-24 UE 端被捕捉之程序

資料來源：本團隊製作

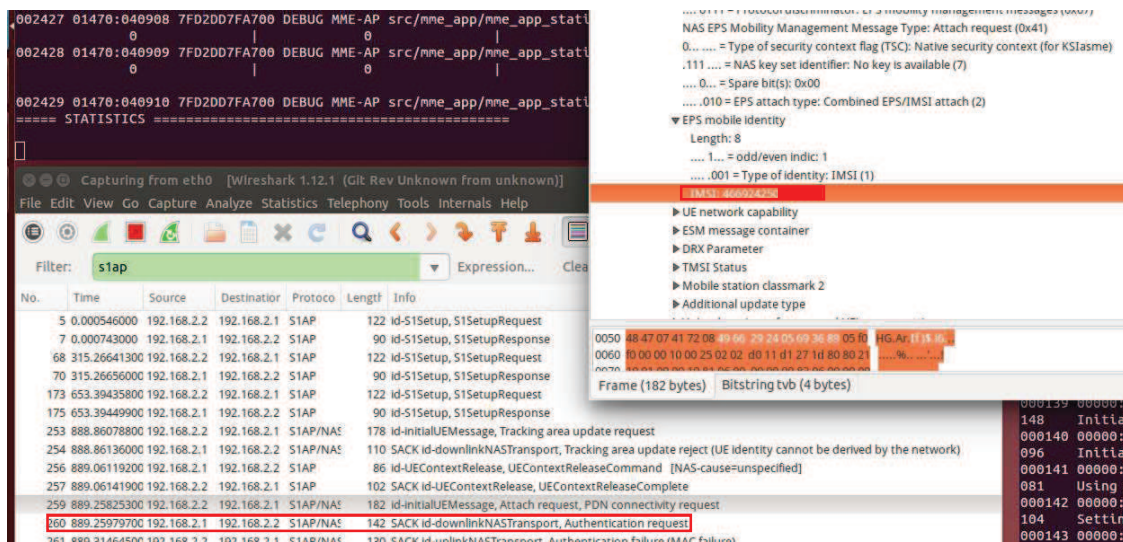


圖 5-25 偽基站端捕捉畫面

資料來源：本團隊製作

(三) 偽基站防護方案建議

目前所看到偽基站造成通訊服務無法正常使用，只能影響小型區域，危害少數用

戶。目前有效的解決方案無法即時發現，為了保障大眾手機安全及隱私保障，電信服務供應商應主動啟用加密演算法。對於偽基站防護建議，本團隊參考諸多文獻、專利與報導，大致上可以分為以下幾個層面：

- LTE 基站部署憑證進行認證。
- 設計終端設備導入基站的識別。
- 提出對 LTE 細胞選擇過程的系統性修改。
- 電信服務供應商減緩偽基站所帶來的影響。

以下綜整各個文獻建議之防護解決方案：

1. 安全閘道器與憑證認證中心

在 D. Herceg 的文獻中²⁷²，指出 NSN (Nokia Siemens Networks) 提出的 LTE 傳輸安全解決方案，包括兩個主要元件：安全閘道器與憑證認證中心，以數據機密性、完整性與可用性為主，計畫在成千上萬個 LTE 基站部署，預先分發共享金鑰，如圖 5-26 所示。

- 安全閘道器 (Security Gateway, 簡稱 SecGW) 過濾與防火牆的連接，並通過使用 IPSec 加密流量來保護數據流。
- 憑證認證中心 (Certificate Authority, 簡稱 CA) 對 eNodeB 與安全閘道器進行基於證書的身份驗證，以防止對數據通訊或網路設備未經授權訪問，並為流量加密提供金鑰。

IPSec(Internet Protocol Security)是多個 LTE 接口上的 3GPP 標準化安全解決方案，主要是部署於 S1-MME 與 X2 控制平面(Control Plane)及 S1 和 X2 用戶平面(User Plane)。NSN 進一步建議在管理平面(Management Plane)的安全性納入使用 IPSec 或傳輸安全性，其方式是在 NSN eNodeB 中，內置的 IPSec 支援安全閘道器提供憑證的 VPN 連接，結合在 eNodeB 與安全網關上使用憑證，IPsec 的啟動使任何未經授權的人員都難以獲得對核心網路的訪問，也不會竊聽 eNodeB 與核心網路之間的流量，這樣可以保證任何數據的完整性。

在電信業者網路的 eNodeB 首次初始化期間，利用憑證頒發，只應用於硬體驗證，以認證 eNodeB 與安全閘道器後，產生 IPSec 憑證，後續建立 IPSec 通道，以防止未

²⁷² D. Herceg, "LTE transport security", *Proc. 34th Int. Conv. MIPRO*, pp. 1464-1467, May 2011.

經授權的網路元素與使用 eNodeB，且憑證具有有效期間，須在屆期之前進行更新及確認。

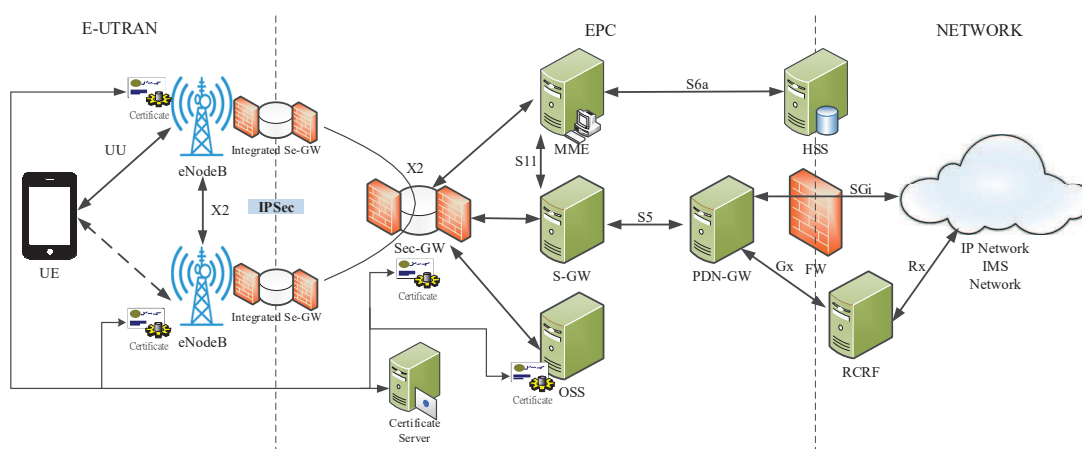


圖 5-26 LTE 安全解決方案

資料來源：LTE transport security

2. 對細胞選擇程序進行簡單的修改

在 IEEE 發表的一篇文獻²⁷³測試結果顯示，LTE 可用性的主要威脅是欺騙 LTE 控制通道。其建議對細胞選擇程序進行簡單的修改，以有效地降低 LTE 控制通道欺騙的影響，說明如下：

²⁷³ M. Labib, V. Marojevic, J. Reed, "Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing", *IEEE Conf Standards for Commun. and Net. Proc.*, pp. 160-65, 2015-Oct.

- PHY 層應該向 RRC 層報告在相同頻率上可用的所有細胞的列表及其相對應的 PCI 及其 RSRP 級別，並且 RRC 層應當保存該列表。
- RRC 層應創建兩個單獨的標籤，一個用於在 SIB1 訊息中接收的禁止細胞，另一個用於被禁止的細胞。這是為了確保 UE 將以不同的方式處理這兩種情況，在 UE 與網路之間的相互認證過程失敗時，該細胞應被視為禁止。
- RRC 層應該首先檢查該細胞是否被禁止，然後檢查該細胞是否被禁止。
- 當細胞被禁止時，應允許 UE 選擇同一頻率下的次強的細胞。
- 如果 cellBarred 標籤為”True”，則 RRC 層應檢查同一頻率內是否有重複的 PCI。如果 RRC 發現 SIB1 訊息中的 cellBarred 為”True”，並且該細胞的 PCI 在該頻率的所有可用 PCI 的列表中被複製，則 RRC 層應當將該細胞標記為被禁止。

3GPP 規範要求 UE 僅選擇訊號最強的細胞，原因是當與遠處的細胞進行通信時，UE 不會向其他 UE 產生過多的上行鏈路干擾。細胞被設定為 cellBarred 禁止時，UE 便不能連接到它。因此，如果 UE 選擇訊號強度下一順位的細胞，則 UE 不會產生任何上行鏈路干擾。因此修改建議允許選擇訊號強度下一順位的細胞，在訊號最強的細胞被禁止時。

因此如果偽造的 eNodeB 在 SIB1 訊息中被廣播為禁止，建議 UE 應該檢查在這個頻率接收到的 PCI 列表中是否重複這個 PCI。在這種情況下，UE 將能夠以相同的頻率駐紮在合法的相鄰 eNodeB 上，能夠透過交遞過程使該 UE 連接到附近合法的 eNodeB。

這些修改建議將共同成為 LTE 控制通道欺騙的有效緩解方法，為了保持與當前 LTE 設備的向下兼容性，所提出的改變不會造成任何過多的上行鏈路干擾，所以當前的 LTE 網路將不會有性能下降的問題。

3. 在細胞選擇的過程加入偵測

UE 端偽基站防護的方向，設計終端設備時導入偽基站的識別²⁷⁴，在細胞選擇的過程加入偵測，方法程序(如圖 5-27)為：

- (1) 從基站收到的系統訊息，做第一次評估，檢測基站，若疑似偽基站將其判定為偽基站候選。

²⁷⁴ 偽基站識別方法及裝置，專利公開號：CN 106572450 A

- (2) 若判定為偽基站候選，進行駐留後強制進行鑑權。
- (3) 鑑權失敗，判定其是否為偽基站。

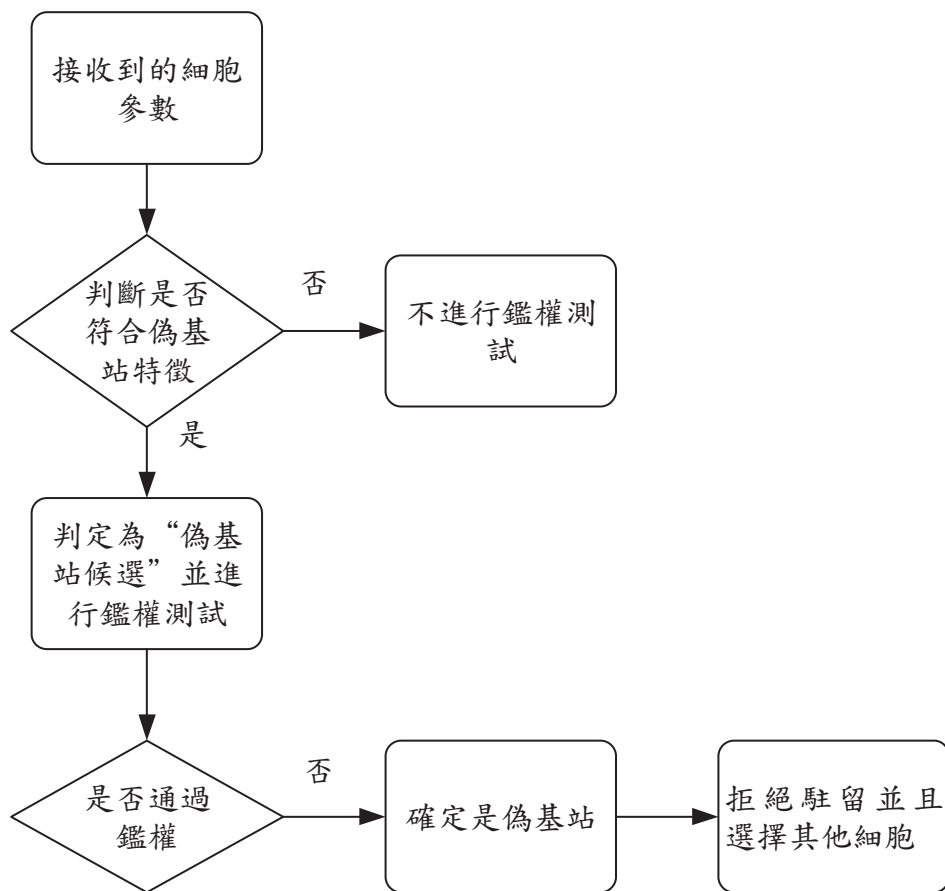


圖 5-27 用戶端設備偵測示意圖

資料來源：本團隊製作

從電信業者的角度，能透過偽基站的偵測，減緩偽基站所帶來的影響，傳統偵測方式是基於客訴所回饋的訊息，但無法因應現在偽基站流動性及偶發性等特性，因此提出了一個偽基站的偵測方式，其程序(如圖 5-28)如下²⁷⁵：

- (1) 按照指定時間區間獲取信令數據。
- (2) 基於規則模型庫進行處理。
- (3) 處理結果滿足預設條件，進行告警，並將處理結果導入分析平台。
- (4) 數據分析，基於用戶、事件、時間、空間等，生成偽基站干擾圖。

²⁷⁵ 一種偽基站定位方法及系統，專利公開號：CN 106162688 A

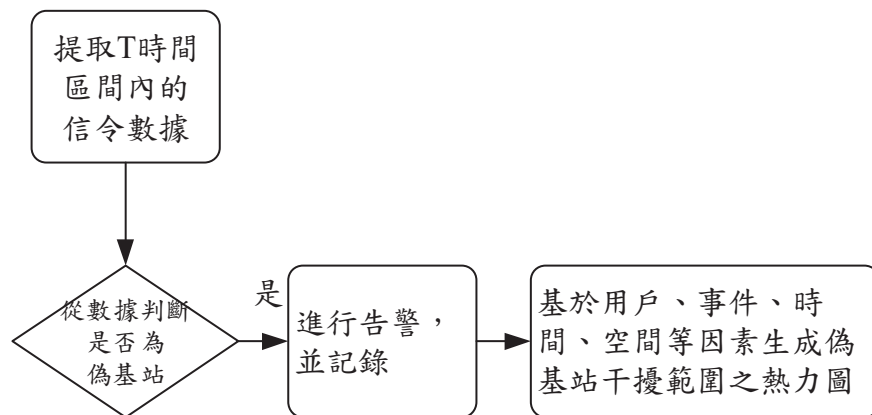


圖 5- 28 偽基站偵測示意圖

資料來源：本團隊製作

經由上述研究發現：偽基站攻擊在台灣確實會使用戶無法連接至電信網路，導致服務無法正常使用，但目前能影響圍屬小型區域。此問題屬於偽基站涵蓋範圍內的 Attach 與 Paging 程序觸發所致，是 4G 協定上設計問題，短時間內無法有效的解決，只能從偽基站的偵測與排除著手，但偵測的方式也同屬困難問題，需電信營運商定時監控無線訊號品質與干擾情況進行判定，或是由單一基站有用戶大量離線情況來判斷是否有偽基站存在，但針對小規模的偽基站或移動式的偽基站，就無法透過此方式有效排除。

建議用戶若發現手機中斷服務或無法發受話的情況一直沒有改善，即可能遭受偽基站之攻擊，只要用戶在不同的地點或位置移動超過 200 公尺，再透過重新開機能解決此情況，若中斷服務的情況持續發生請向 NCC 或電信業者進行回報。營運商應開啟加密演算法，避免使用者通話、訊息等隱私遭受洩漏威脅。主管機關在管制作為上，建議可列管 Open LTE 射頻元件的採購及使用，限制於研究與開發的用途，不得影響正常網路服務，以防止濫用成為偽基站設備，進一步杜絕偽基站在國內發生機會，影響用戶權益。

二、 VoLTE 資安技術探討

隨著上網服務需求的增加，以及行動電信產業的進步，人們對於上網速率及效能的提升都有更高的期待，因此語音傳輸的技術便跟著演進，從原本提供數據服務業務且只能滿足簡單的通訊、簡訊、上網單一功能的 2G，到了有較多媒體形式可處理的 3G 網路，而為了滿足用戶們對於無線服務及更高速語音通話的需求，行動寬頻網路（4G LTE）因應而生，也進一步研究出擁有更大頻寬的語音技術，能夠將語音轉換為數據，直接透過 LTE 網路去傳輸更清晰更快速的語音，也就是本團隊這次討論的主題-VoLTE(Voice over LTE)。

VoLTE 的網路架構相較 2G、3G 較為簡單，而其最大的差別在於傳輸方式原本是以 Circuit Switched Network(電路交換式網路)，會分成語音及多媒體訊息協定，但可能產生「佔線」問題，等到兩端通話結束，連線專用路徑才能提供給下一個使用，使得效益不彰²⁷⁶，因此演變出現在使用的 Packet Switched Network(封包交換式網路)，將資料切割成多個封包，每個封包都有自己的位址，再透過路由器逐一處理，讓收發方式以 IP 為基礎，當有需要時才會收發資料，且有許多不同的網路路徑可傳送，資料傳輸率遠遠超過 2G、3G 的量且更加精確，可實現更高速的語音編碼方式，而有更清晰的視頻語音通話。

下表 5-3 簡要說說明 Circuit Switched 及 Packet Switched Network 的比較。4G LTE 發展初期電信業者使用 CSFB(Circuit Switched Fallback)，提供用戶語音通話服務，通話時會從 4G 降回至 3G、2G，結束通話才切換至 4G，造成通話的延遲時間較長，且無法於通話時同時進行高速上網，而 VoLTE 則能透過封包交換讓建立呼叫的時間更短，並保持著同時能夠 4G 上網的特性。

VoLTE 係建立在 IMS (IP Multimedia Subsystem) 核心網上，IMS 的部署以及 4G 網路的覆蓋性必須夠完整，否則可能直接斷訊，為了解決這個問題，3GPP 提出

²⁷⁶ Shiimoto, Kohei, and Naoaki Yamanaka. "Circuit-switched network." U.S. Patent No. 6,731,628. 2004/5/4.

SRVCC²⁷⁷(Single Radio Voice Call Continuity) 單模式語音呼叫連續性方案，當用戶不處於網路涵蓋範圍時，可以透過 IMS 的 CSCF(Call Session Control Function)發起會話傳送請求，在能夠不影響通話服務品質 (QoS)，流暢地將 4G LTE 切換至傳統網路彌補 4G 網路覆蓋性不足的問題。因此 VoLTE 除了能夠提供高品質的音訊，建立通話時間也相較快速，甚至可以同時進行清晰通話及高速上網。

早在幾年前，GSMA 所提出的 VoLTE 次世代語音計畫即獲得許多世界領先的電信業者及手機製造商一路支持。全球的 VoLTE 營運部署節奏正在加快，亞太以及北美地區²⁷⁸都擁有了大量的客戶群，近年來，除了首先推出 VoLTE 業者間互連及漫遊服務的韓國，美國與日本也隨之跟進漫遊服務，但他們的 VoLTE 服務尚未能於不同電信業者間互通，相互連結的規格細節還有待商榷，不過用戶都有急遽成長，尤其近期中國為了改變原本 CDMA (Code Division Multiple Access) 此種非主流的通訊系統，開始建構大規模的 4G 基站，並結合 SRVCC 切換技術，由中國移動帶頭並影響其餘電信全國大範圍的推行 VoLTE，網路涵蓋範圍可謂全球第一²⁷⁹。

反觀國內五大電信業者，中華電信雖已經過 VoLTE 測試，但仍在等待整體產業生態時機成熟，因而尚未推出，其餘四大電信之 VoLTE 則均已通過國家通訊傳播委員會之審核，並且開放用戶申請，而最大的差別在於台灣大哥大結合了上述提及的 SRVCC 技術，因此可以無縫轉換 3G、4G，表示其他電信業者只要離開 4G 環境就會斷線，但台灣之星說明由於 4G 涵蓋率已達 98%，經過實測不會有太大的斷訊問題，然而因語音營收是電信業者主要的獲利來源之一，VoLTE 費率如何收取，及業者間互連費率、技術等問題皆尚未解決，在台灣被普及化之速度也較為緩慢。

²⁷⁷ Radio-Electronics.com, “SRVCC Single Radio Voice Call Continuity”.

²⁷⁸ AT&T, “AT&T’s Voice Over LTE Network Reaches More than 27 Million Subscribers”, 2015/12/29.

²⁷⁹ 郝勇志, “全球 VoLTE 市場前景看好 中國移動完成部署”, 2016/7/21.

表 5- 3 Circuit Switched 及 Packet Switched Network 的比較

	3G 通話 (Circuit Switched)	VoLTE (Packet Switched Network)
1.	兩通訊端傳輸前須建立專屬路徑	不需預先設立專用通訊路徑
2.	頻寬被單一訊息佔用直到通訊結束	多個訊息可共享頻寬
3.	因有通訊專屬路徑，延遲時間較短	通訊量越大，延遲時間越長
4.	按發送順序傳送訊息，所以不須編號	每個封包必須編號以免失序
5.	以通訊時間長短計費	以數據傳輸量來計費

資料來源：本團隊整理

(一) VoLTE 架構說明

VoLTE 的基本架構包括 LTE(Long-Term Evolution)無線網及 IMS(IP Multimedia Subsystem)核心網，主要傳輸協定為 SIP(Session Initiation Protocol)，VoLTE 架構圖如圖 5-29。

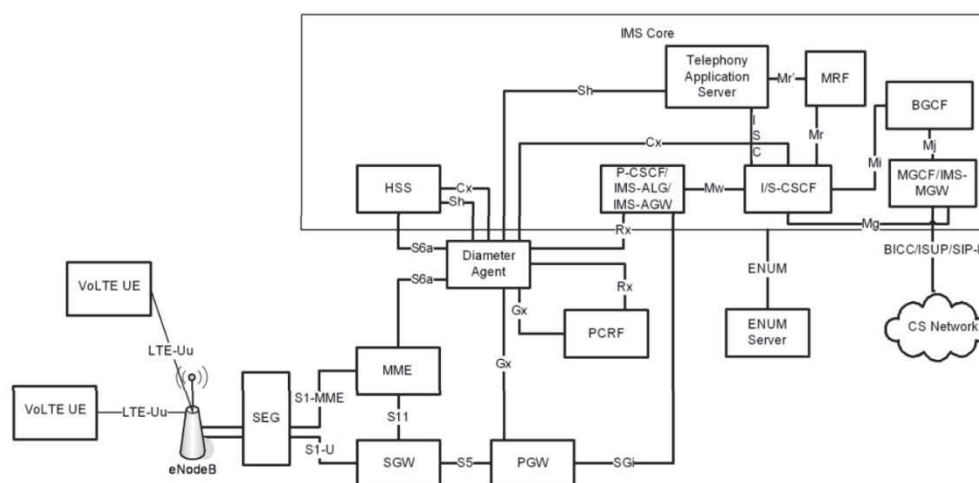


圖 5- 29 VoLTE 整體架構圖

資料來源：GSMA VoLTE Service Description and Implementation Guidelines Version 2.0

1. LTE 無線網架構²⁸⁰

LTE 無線網架構(如圖 5-30)是基於增強 3G 現有的網路架構，主要分為無線部分 E-UTRAN (Evolved Universal Terrestrial Radio Access Network)與核心網路部分 EPC (Evolved Packet Core)。訊息傳輸方面則分為 Control-plane 與 User-plane 來區分出用戶為控制封包或是實際傳輸的資料封包，此作法將可以更有效率的管理系統，已能依照個別進行設計與改良，也更靈活了佈署方式。

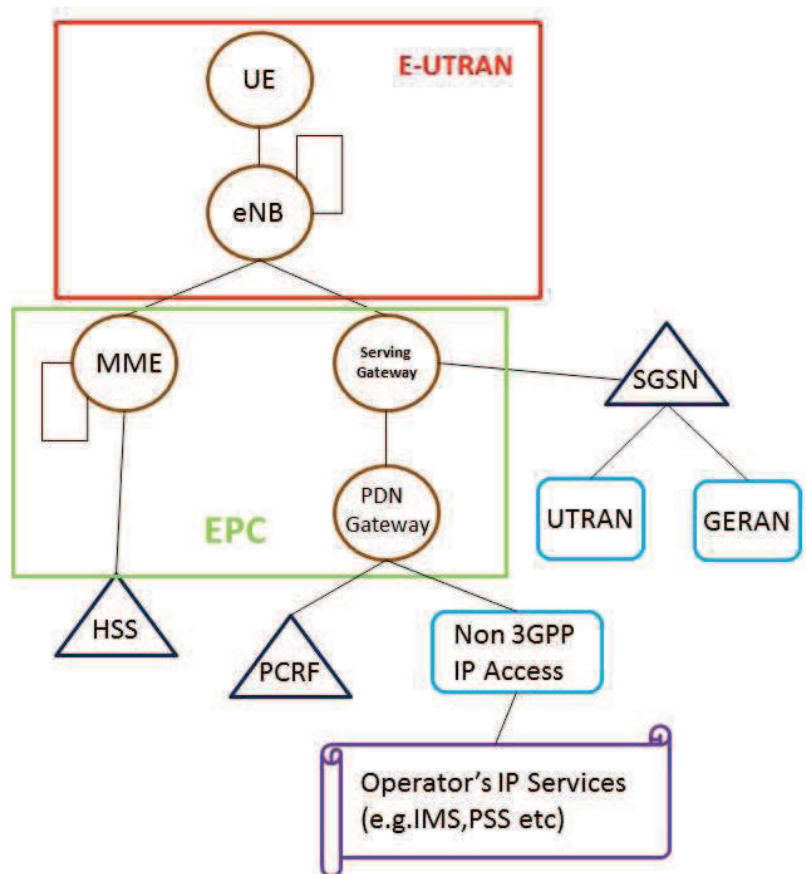


圖 5-30 LTE 網路架構示意圖

資料來源：GSMA

(1) E-UTRAN²⁸¹：主要是 LTE 無線通訊的架構，包含了用戶端(UE)以及基站 eNB(Evolved Node B)，透過無線介面 LTE-Uu 進行通訊，LTE-Uu 分為三層：

- 第三層屬於 User-plane 的 NAS (Non-Access Stratum)及 RRC (Radio

²⁸⁰ 郭昱賢 林盈達, "LTE 架構、協定與效能", 2011/9/30.

²⁸¹ Chew, Mutale. "VoLTE by IP Multimedia Subsystem.", 2015.

Resource Control)，NAS 主要是移動性的管理以及用戶的身分認證，RRC 主要是在負責資源之分配。

- 第二層屬於 Control-plane(如下圖 5-31 所示)，包含 PDCP (Packet Data Convergence Protocol)主要是處理壓縮及加密，以及 RLC (Radio Link Control)和 MAC (Medium Access Control)。RLC 負責配合各個 frame 來進行封包的分割與重組，MAC 負責 QoS(Quality of Service)的優先順序排程，QoS 是一種控制的機制，將會針對不同的客戶、資料或是目的將封包進行優先順序的排程，以此為例就是將 VoLTE 的 SIP 封包擁有較高的優先權。
- 第一層 PHY (Physical)為負責實體訊號的接收與發送，其中也包含了 OFDMA(Orthogonal Frequency Division Multiple Access)與 MIMO(Multi-input Multi-output)等技術。

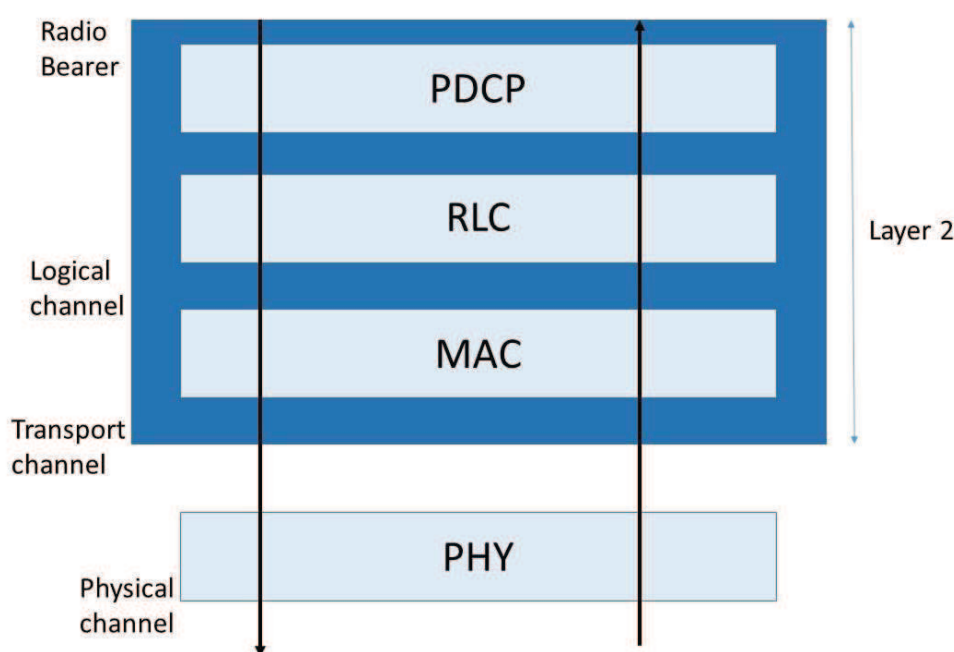


圖 5- 31 LTE Control plane 層之架構圖

資料來源：新通訊原件雜誌

- (2) EPC²⁸²: 為了因應未來網路趨勢及降低網路複雜度，設計上改採 All-IP 的架構，捨去原有的 Circuit Switch 電話交換線路，僅保留 Packet Switch 封包交換網路，主要由三個部分組成：

²⁸² GSMA : VoLTE Service Description and Implementation Guidelines Version 2.0.

- MME (Mobility Management Entity)：用來管理核心網路中 Control-plane 裡包括安全性等等的管理。
- S-GW (Serving Gateway)：處理 User-plane 裡面的訊息，包括資料封包等等，以及各個 eNodeB 之間的轉換，和 LTE 與 3GPP 之間相容性的切換。
- PDN-GW(Packet Data Network Gateway)：主要處理 User-plane 對外連線的部分，和 LTE 與 WLAN 等非 3GPP 之間相容性的切換。

E-UTRAN 中的 eNodeB 會經由 S1 Interface 與 EPC 的 S-GW 和 MME 分別進行通訊，如上圖 5-31 所示，連接 S-GW 的部分為 User-plane 的 S1-U 介面，至於連接 MME 的部分則為 S1 Interface 於 Control-plane 中的 S1-MME 介面，且此在傳輸層採用 SCTP(Stream Control Transmission Protocol)此種綜合 TCP 及 UDP 特性的通訊協定，能達到較高的可靠性。此外，會透過 S11 Interface 支持 S-GW 及 MME 之間的通道乘載管理。

2. IMS(IP Multimedia Subsystem)核心網²⁸³

IMS 核心網(如圖 5-32)，是能夠實現 VoLTE 主要的核心，主要是由封包資料網路閘道(Packet Data Network Gateway)、歸屬用戶伺服器(Home Subscriber Server，簡稱 HSS)、呼叫會話控制功能(Call Session Control Function，簡稱 CSCF)、策略與計費功能(Policy Charging and Rules Function，簡稱 PCRF)以及應用伺服器(Application Server，簡稱 AS)所組成。

- (1) PGW 是在封包交換的網路中在 EPC 裡面的通訊通道，包含了兩種通訊通道，一種是負責傳送手機的信令交換，另一個是負責傳送媒體(影像、聲音)的封包。此外，PGW 經由 S5 Interface 實行與 S-GW 之間的通道管理，以及透過 Gx Interface 允許 PCRF 可以直接控制 PGW 的策略執行相關功能。
- (2) HSS 主要包含了 HLR (Home Location Register) 和 AuC (Authentication Center)，HLR 主要為管理及儲存用戶資料庫及提供用戶 IP 位址等相關訊息，對所有實際通話提供支持及管理，AuC 利用之前就已經分享好的金鑰進行用戶的認證及授權，兩把金鑰分別儲存在 AuC 的網路層以及用戶的 SIM 卡上，並透過 S6a

²⁸³ Ventuzelo, Patrick, Olivier Le Moal, and Thomas Coudray. "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone", 2017.

Interface 來驗證與 MME 之間授權用戶的訪問，以及經由 Cx Interface 完成 IMS 核心網的註冊，進一步將數據資料傳送給 S-CSCF。

(3) CSCF(Call State Control Function)主要是在 IMS 系統中處理 SIP 信號數據包，分為代理-CSCF(P-CSCF)、服務-CSCF(S-CSCF)以及詢問-CSCF(I-CSCF)。

- P-CSCF 主要是在用戶以及 IMS 之間做代理的服務，是用戶要發出 VOLTE 請求的原始出發點，也必須要在用戶以及 IMS 溝通的期間做好安全的管理，除此之外，藉由 Rx Interface 允許應用功能替每個會話請求適合的策略應用，並透過 SGi Interface 於 PGW 間傳送相關參考點資料。
- S-CSCF 是負責所有的會話管理，像是會話開始、結束或是控制等等，也是負責為用戶在 IMS 網路裡面進行註冊。
- I-CSCF 主要是遇到尚未註冊的使用者，必須要發送初始化的 SIP 要求去尋找適合的 S-CSCF，讓 S-CSCF 去負責用戶的註冊。

(4) AS 負責與 S-CSCF 之間發起 SIP 協定，並且在 SIP 應用伺服器中負責以及提供服務，是聲音及影像通話中主要使用的 Server，也可以稱做 TAS(Tephony Application Server)或是 MMTel(Multimedia Telephony)，並會透過 Sh Interface 與 HSS 連接，將服務和訂閱戶的相關資訊傳遞至 AS 或者儲存在 HHS 當中。

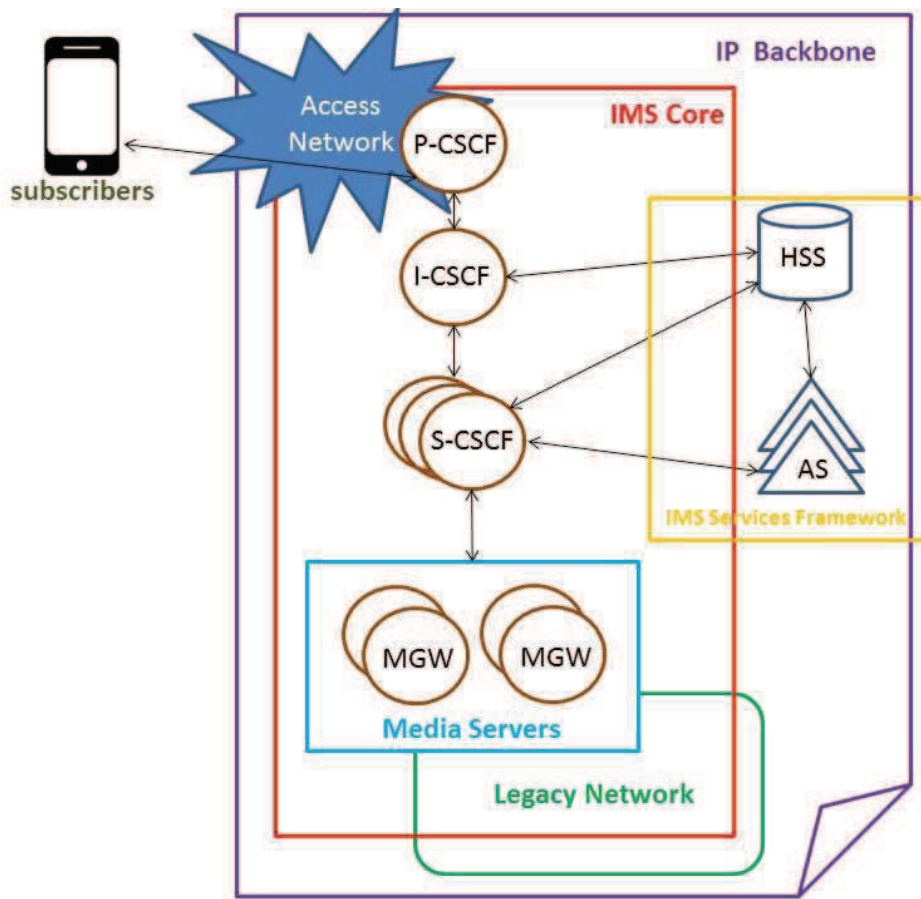


圖 5- 32 IMS 架構示意圖

資料來源：GSMA

用戶端(User equipment，簡稱 UE)傳 SIP Registration 的要求，經由 LTE 無線網傳輸到 IMS 核心網進行註冊及通話之處理(如下圖 5-33 所示)。LTE 無線網負責 IP 連接及通道的設置，為用戶提供滿足 QoS(Quality of Service)要求的 IP 通道，IMS 核心網負責用戶的呼叫及業務控制。如果一個用戶端(UE)傳入 SIP 要求進來，封包將會經由 E-UTRAN(Evolved Universal Terrestrial Radio Access Network)先傳到 MME(Mobility Management Entity)裡面，MME 會再到 IMS 核心網中的 HSS 查詢用戶端資料，如果未註冊過的用戶就會藉由 P-CSCF(Proxy Call Session Control Function)來尋找 I-CSCF(Interrogating Call State Control Function)來幫用戶進行註冊，如果為已註冊過的用戶，就會利用 S-CSCF(Serving Call State Control Function)來進行會話的開始與結束等，最後所有封包都會傳到 AS(Application Server)來做通話的處理，再傳給被撥打電話的用戶。註冊流程舉例說明如下：

用戶 Alice 將會傳送一個初始化的 REGISTER 要求，包含了參數 username 裡面有私人 ID alice_private@atlanta.com 等等，全部包含在 Authorization 封包的 header 裡面。

用戶 Alice 提供了電信商的名字以及基站的 ID 在 P-Access-Network-Info 這個 header 裡面。

在 Security-Client 這個 header 裡面提供了在 P-CSCF 溝通過程中，創建 IPsec 所需要用到的參數。並經由 Security Gateway 此種選擇性的網路節點來管理 eNodeB 和 EPC 之間的安全關聯，而因為 IPsec 由安全共享密鑰所建立，可以採用多種不同的格式，並根據通話雙方於通道設置期間所使用到的參數，強制實行流量加密，進而提供更完善的保護。

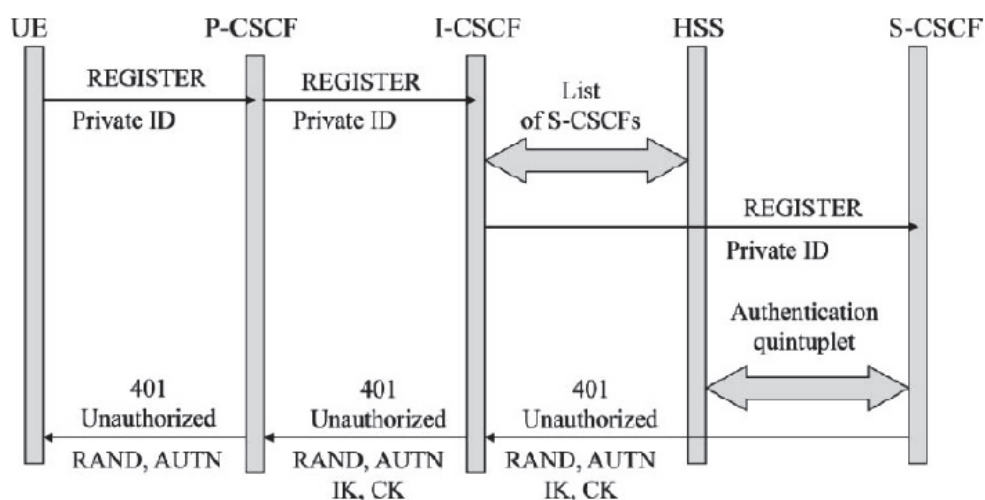


圖 5- 33 VoLTE 註冊流程

資料來源：GSMA VoLTE Service Description and Implementation Guidelines Version 2.0

（二） VoLTE 造成基站(eNodeB)與核心網路之可能資安威脅和現有解決方法。

1. VoLTE 造成基站(eNodeB)與核心網路之資安威脅

因用戶對高品質網路服務的期許，演變出了現今 VoLTE 語音技術，根據前面所提

及，相較於 2G/3G 網路，VoLTE 的架構簡化成只需經由 UE 連接到 eNodeB，再透過 LTE 無線網傳輸取得 IP 連接，連線至 IMS 核心網路進一步驗證並建立通話，然而在數據交換的過程中，由於 VoLTE 是在蜂巢式網路（cellular network）執行，並且需要透過 SIP（Session Initiation Protocol）此種基於 TCP/IP 協定上層運作的信號指令來幫助數據傳輸，我們發現這裡面的協議漏洞，以及原本蜂巢式網路所存在的問題都有可能造成 eNodeB 及 IMS 核心網路較大危害，本團隊在此列下幾出幾點並進行討論。

(1) Headers(標頭檔)洩露資訊

當 VoLTE 通話建立前，UE 會送出 INVITE 的 SIP 訊息請求，如果接收者連接上 IMS 並同意此次通話，UE 便會透過 SIP 所回傳之“200 OK”來表示訊號傳送請求已被許可，且用戶已被授權接收此訊號，然而因著某些 SIP“200 OK”的標頭檔會包含 IMS 核心網路中相關設備的 server 版本及類型之詳細設置資訊，導致攻擊者可經由這些隱密資訊得知設備之漏洞，進行精確的攻擊。

(2) 惡意訊息傳送導致網路癱瘓

當 SIP 呼叫要建立時，server 端都會收到 UE 的 INVITE 信息，並且產生個別獨立控管之 session 處理每條訊息的往返，就如同我們打電話，一次只能撥打一組號碼，反之攻擊者可以透過特殊發話模組，大量的傳送 INVITE 訊息，儘管對方沒有回應此通話，通訊承載通道（bearer）都已經被建立，然而無論啟動此通訊承載通道抑或釋放他，都會佔用無線介面 LTE-Uu 之 Control-plane 大量資源，造成封包資料閘道（P-GW）的負載量過大，進而癱瘓核心網路之服務。

(3) 計費欺騙

因為 VoLTE 是基於 SIP 協定的通話服務，在 IMS 中，HSS 將會提供用戶之間 IP 的配對以及在 SIP REGISTER 的過程中提供公共身分，然而，找到對方的 IP 位址並不難，在通話建置的階段，收話者的 IP 將會提供給發話者，這樣才可以建置數據通道，當發話者收到收話者的 IP 位置時，他可以傳送 CANCEL 指令到核心網路中，並且利用這些數據來建立自己的連線並且進行語音的溝通。

由於 VoLTE 計費方式較 3G 網路不同，是用使用者的數據流量來計費，所以計費欺騙攻擊可能會偽造持續通話的時間，並且可以在使用者之間進行任何類型的數據傳輸，但是核心網路將檢測不到這些數據的傳輸。

(4) 信令攻擊

信令攻擊是利用攻擊用戶與核心網路之間的信令傳輸，利用修改、竊聽達到想要的目的，例如中止或偽造 SIP 訊息。為了達成這樣的攻擊，攻擊者必須選定一個確切的對話參數，並且在用戶在傳送這些信令後，再從中竊聽，並且偽造出一個相對應的 SIP 訊息，送到核心網路中，從而達成目的。

A. SIP BYE 攻擊

攻擊者先竊聽到會話中所需要的參數，如會話 ID、使用者 IP 等等，攻擊者再利用這些訊息，插入 BYE 請求給核心網路，進而實現 BYE 攻擊。

B. SIP CANCEL 攻擊

一個 CANCEL 能夠用來取消一個 INVITE，所以，攻擊者會偽造 CANCEL 請求，來取消其他用戶的 SIP 連線請求，來中斷其他用戶的會話建立。

C. SIP-Update 攻擊

是利用修改 SIP 封包裡面的參數，包刮 QoS 或是端口號等等，來達成對於用戶端的攻擊，通常是在會話建立之後，從中間干擾會話的攻擊。

2. VoLTE 造成基站(eNodeB)與核心網路之資安威脅和現有解決方法

在前文本團隊提及了 VoLTE 技術是經過 SIP 指令來傳送，可能會造成基站及 IMS 核心網路哪些危害，同時，我們也將在底下篇幅中進一步探討，並提出對應之可行解決方法(如表 5-4)。

首先為 SIP 訊息中 Headers 可能洩漏資訊，造成攻擊者可得知設備相關資訊進而針對漏洞進行攻擊。我們知道 IMS²⁸⁴中有四個呼叫會話功能，其中一個為 P-CSCF(Proxy-CSCF)，是 IMS 連接網路的聯繫點²⁸⁵，所有 SIP 來往的 UE 指令都必須經過這裡，當 P-CSCF 要傳送 200(即 OK 的代碼)時，進一步審核，當發現有關隱密訊息的標頭檔便拒絕請求，同時回送錯誤訊息給 UE，抑或刪除這些包含在內的隱密訊息，

²⁸⁴ Cuevas, Antonio, et al. "The IMS service platform: a solution for next-generation network operators to be more than bit pipes." IEEE Communications Magazine 44.8: 75-81., 2006.

²⁸⁵ J.Rosenberg, H.Schulzrinne, G.Camarillo, A.Johnston, J.Peterson, R.Sparks, M.Handley, E.Schooler, "SIP: Session Initiation Protocol", 2002/6.

才能有效避免機密外漏導致駭客透過這些資訊對 DOS (Disk Operation System) 進行傷害。

前面我們知道攻擊者可以透過大量傳送 INVITE 訊息，而此種訊息可以啟動通話並且占用資源，當數量龐大時會導致負載量太大，進而癱瘓核心網路，為了避免遭受因著接收惡意訊息導致被拒絕服務之攻擊，電信業者必須嚴格限制每段時間內 UE 可發送之 SIP 訊息的最大量，而當偵測到信息量超過所制定之數值，電信業者應該馬上進行有效攔截，並確認此活動是否可能為攻擊者所發出。同時，SIP server 也要檢查此 UE 是不是通話中，是的話就攔截發出的其餘 INVITE 信息，透過 SIP server 及電信電信業者的同步監控下，進而有效預防駭客之攻擊。

除此之外，針對前面所提到 VoLTE 因著計費方式是採用數據流量，其中發現的漏洞即是可能隱藏免費通道，因此遭受到計費欺騙攻擊，這主要因著 VoLTE 是在 cellular network 中執行，然而 cellular network 卻沒有合理控管封包資料閘道 (P-GW) 中的用戶請求，而所建立之通話承載通道 (bearer) 主要目的僅是為了處理相關通話信令，因著如此，P-GW 應當先行過濾此封包是否為 SIP 信息，同時，電信業者應該嚴格監督數據包來往的發送路徑，先行攔截 UE 至 UE 直接發送之封包，僅開放 UE 透過 SIP 伺服器代理傳送封包，並且搭配深度封包檢測系統 (Deep Packet Inspection，簡稱 DPI) 進行流量的監控，進一步避免免費通道的數據傳輸。

在前文最後所提及的資安威脅中，我們談到了攻擊者可能透過掌握到連接通話前之特定參數進行竊聽，並且進一步偽造 SIP 訊息來終止或者竄改已建立之通話，而會造成此種攻擊主要是因為 IMS 核心網路裡信令對於安全方面之機密性 (Confidentiality) 保護不夠。在此可以透過採用各式加密法 (例如：對稱加密、Diffie – Hellman 密鑰交換等)，對需要傳送的資料進行加密，保障傳訊過程中無法遭到竊取，進而避免更大之攻擊傷害。

表 5-4 VoLTE 之資安威脅及防護建議

資安威脅	描述	防護建議
1. Headers(標頭檔)洩露資訊	利用攔截 SIP 的 INVITE 的請求訊息，來得知相關 Server 的相關訊息。	利用 P-CSCF 當作網路的聯繫點來進行審核，如果有發現隱密訊息的標頭檔，便拒絕請求。

2.惡意訊息傳送導致網路癱瘓	利用大量傳送 INVITE 訊息來建立通話通道，造成閘道負載過大，進而癱瘓核心網路。	可以利用限制用戶端每隔多就才能發出 INVITE，如果發出太多訊息就可以進行限制與監控。
3.計費欺騙	當發話者收到收話者的 IP 位置時，便可以繞過計費系統，建立屬於自己的通話連線。	電信業者僅開放透過 SIP 代理傳送封包，並且搭配封包檢測系統，進行監控。
4.信令攻擊	利用修改或是竊聽封包中的信令，來進行攻擊。	可以透過各式加密法來對於信令裡面的資料進行加密。

資料來源：本團隊整理

(三) VoLTE 造成用戶端(UE)可能遭受惡意軟件(Malware)之資安威脅和現有解決方法。

本團隊將結合前面所提及 VoLTE 可能帶來之資安威脅的影響，把這些攻擊受害者從基站與核心網路轉換為用戶端，更細部地描述出所有對用戶端可能的攻擊影響，並從兩個面向去做探討。首先為當使用者裝置無意間被植入惡意軟件時，會造成受害者行動裝置承受到什麼潛在的危害和損失，以及現今所對應之解決方法為何，並列舉幾點加以討論。

惡意軟件泛指一切可能對電腦或網路造成非預期的負面影響之軟體程式，例如占用系統的資源或者未經許可蒐集使用者之機密訊息等，而觸發這些惡意行為的包含特洛伊木馬或蠕蟲病毒等均歸於此類。VoLTE 主要採用 SIP (Session Initiation Protocol) 作為信號協定進行資料的傳輸，其中訊號建立及傳輸過程如圖 5-33，VoLTE 的數據傳輸方式已經由 Circuit Switched 演變成 Packet Switched，然而在這個傳送的过程當中，並沒有一個電信業者或者規範禁止 Packet 數據封包轉換成 VoLTE 的信號。

而在 VoLTE 的架構中，存在著一個控制平面(Control-plane)，其中包含了專門傳送信號的信令乘載通道(signaling bearer)，當 LTE 網路中獲得 IP 的連接位址，且有任何的呼叫請求之服務啟動時，SIP 訊息就可以開始經由這個信令乘載通道在通話裝置以及 IMS 核心網之間進行傳遞，而當此呼叫請求被允許時，即會觸發語音乘載通道(voice bearer)來傳送語音的數據流量，直到通話結束，再釋放此語音乘載通道。但在

控制平面上卻沒有一個存取權限能夠確保使用此通道的僅能是 VoLTE 的信號，進而防止非 VoLTE 的數據封包被嵌入此信令乘載通道，因此當使用者經由網路連線無意之中將惡意軟件，例如間諜病毒等，載入至行動裝置時，將會因為以上的漏洞，導致一些對於使用者潛在威脅的產生。

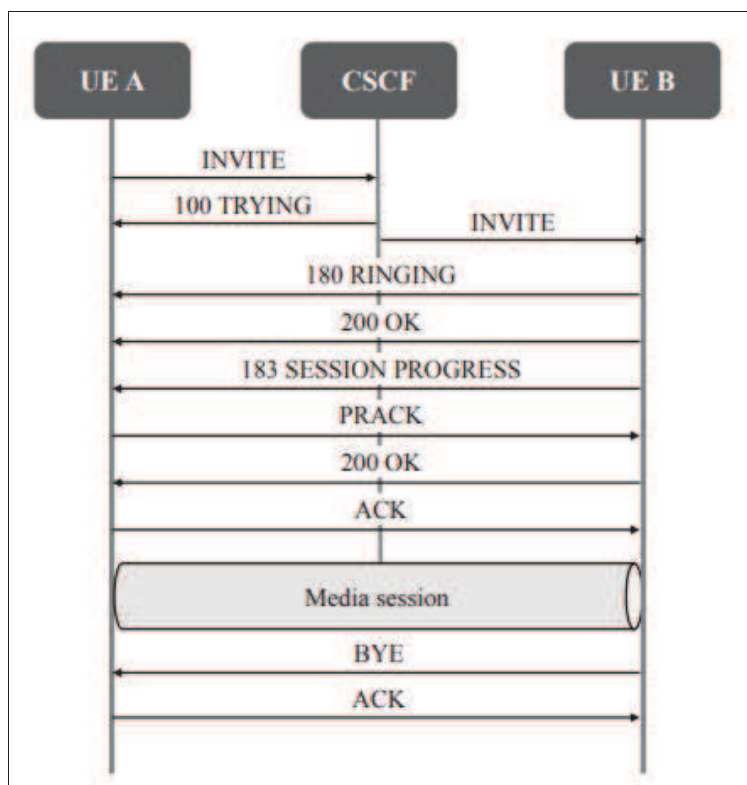


圖 5- 34 VoLTE 簡易 call setup

資料來源：Kim, Hongil, et al. "Breaking and fixing volte: Exploiting hidden data channels and mis-implementations." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.²⁸⁶

1. 免費數據通道

(1) 安全威脅

在 VoLTE 的架構中存在著專門接收信號的 VoLTE 接口(VoLTE interface)²⁸⁷，而此 VoLTE 接口由於暴露於行動裝置的網路接口當中，且目前在 VoLTE 接口中尚未提供

²⁸⁶ Ventuzelo, Patrick, Olivier Le Moal, and Thomas Coudray. "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone."

²⁸⁷ GSM Association. "VoLTE Service Description and Implementation Guidelines." 2014.

類似 WiFi 當中能夠有效阻隔非授權的存取權限，因此未經授權的惡意軟件可以從設備中輕易地獲得 VoLTE 接口的相關訊息，例如帶有特定規則的路由表中之信號伺服器之 IP 位址。因為 VoLTE 信令乘載通道在流量傳輸時並沒有額外驗證及過濾，即使沒有 root 權限，攻擊者甚至可以將 IMS 核心網路中並沒有被分派到 VoLTE 伺服器，與 VoLTE 無關之數據封包嵌入至 VoLTE 的信令乘載通道，並將此數據封包之目的地指定給其餘的 VoLTE 伺服器。

假使攻擊者獲得 root 權限，便可任意更改 VoLTE 接口所指向目的地之路由的規則，經由信令乘載通道達到將封包傳送至任意目標的最終目的。然而 VoLTE 僅收集數據平面(data plane)上的通話時間用做計費依據，傳送建立通話前所交換的信號，例如「INVITE」、「INVITE-ACK」等均是不收費的，任何經由信號乘載通道之數據資料均為免費傳輸，但電信運營商並未規定只有 VoLTE 信號才能通過信令乘載通道，導致無論此信號是否為 VoLTE 信號，且最終目的地是否為信號伺服器，都可成功避開合法計費機制，進而出現免費數據通道的威脅。

除了存取權限的不足所導致，SIP 協定中亦存在著此危害。SDP²⁸⁸ (Session Description Protocol)為涵蓋於 SIP 中的一種會話描述協定，主要用來協助 SIP 建立 VoLTE 通話所需的多媒體封包通道，並於「INVITE」信號的傳遞時交換雙方的通訊資料格式，由於此種協定是以文字為基礎，極其容易被偽造竄改，惡意軟件能夠繞過合法攔截 LI (Lawful Interception)，抑或不觸發 CDR(Call Detail Record)計費系統的情況下，將任意的字串插入至 SDP 封包的 header 中。而此種攻擊的成功與否取決於電信業者網路架構的安全性及成熟度以及儲存在 LI 網路中的數據是否完善。

因此一旦惡意軟件經由建置 VoLTE 通話的過程中獲取接收端的 IP 位址，攻擊者就能獲取到 IP，將封裝好的封包嵌入至「200 OK」信號 header(標頭檔)之任一處(如圖 5-35)，當 VoLTE 通話被建立時，使用者才會發送「200 OK」給 SIP server，甚至有些訊息在通訊建立前即會開始來往，如「INVITE」信號，因此竄改「INVITE」中的內容，直接於 Content 中加入訊息(如圖 5-36)，藉著 VoLTE 僅收集通訊建立成功後之數據時間長短的收費特徵，便能於通訊建立前創造出與用戶之間免費的通訊交換。

²⁸⁸ Johnston, Alan B. " SIP: understanding the session initiation protocol. " Artech House, 2015.


```

SIP/2.0 200 OK
To: <sip:bob@aboutsip.com>;tag=89uasdkfjoiu
From: <sip:alice@aboutsip.com>;tag=987lkajsdf89au
Call-ID: lkjasdf90989lkj
CSeq: 1 INVITE
Via: SIP/2.0/TCP 192.168.0.122:5060;branch=xxx;rport
...
Contact: <sip:192.168.0.22:3156;transport=TCP>
Record-Route: <sip:192.168.1.52:5060;transport=tcp;lr>
Content-Type: application/sdp
Content-Length: 451

```

圖 5- 35 SIP-200 OK Response

資料來源：Jonas Borjesson, “Sip-The Basics”

```

INVITE sip:dgen@aegean.gr SIP/2.0
To: Geneiataki Dimitri <dgen@aegean.gr>
From: Karopoulos Georgios
<sip:gkar@aegean.gr>;tag=76341
CSeq: 2 INVITE
Authorization: Digest username="gkar",
realm="195.251.164.23", algorithm="md5",
uri="SIP:195.251.164.23",
nonce="41352a56632c7b3d382b39e0179ca5f98b9fa03b",
response="a6466dce70e7b098d127880584cd57"
Contact: <SIP:195.251.166.73:9384>;>
Content-Type: application/sdp

```

SIP headers

```

v=0
o=Tesla 2890844526 IN IP4 lab.high-voltage.org
c=IN IP4 100.101.102.103
t=0 0
m=audio 49170 RTP/AVP 0
a=rtpmap:0 PCMU/8000

```

Session Description (body)

圖 5- 36 SIP-INVITE 信號

資料來源：IEEE²⁸⁹

(2) 現有解決方法

VoLTE 通訊是採用 RTP(Real Time Protocol)傳送聲音封包，因此電信運營商能夠透過 IMS 的呼叫會話功能 P-CSCF(Proxy-CSCF)中之封包檢測系統(Deep Packet Inspection,簡稱 DPI)，進一步監控 RTP 專屬的媒體承載通道(bearer)流量傳輸是否為合

²⁸⁹ Zhang, Shen, et al. "Automatic Detection of SIP-Aware Attacks on VoLTE Device." Vehicular Technology Conference (VTC-Fall), 2016 IEEE 84th. IEEE, 2016.

理用戶所使用，以及封包之目的地及來源是否異常，而系統應該接著傳送有關被阻止的封包之相關訊息，以便安全管理員可以驗證 DPI 檢測結果是否為真。

電信運營商亦可利用封包資料閘道（P-GW）嚴格過濾非 SIP 信息，並從 SDP header 中刪除惡意數據，配合電信運營商監控數據來往路徑是否經由 SIP 伺服器代理傳送封包，有效避免惡意軟件之漏洞利用。

此外，運營商應該停止信號免費的這個策略，更新計費系統並且收取任何與數據流量類似的信號傳輸費用，亦可替每個語音通話的 VoLTE 數據流量進行配額限制，當數值低於此配額時，便不會有額外的費用產生。

2. 阻斷服務(Denial of Service)攻擊

(1) 安全威脅

由於 VoLTE 數據交換之方式是採用 IP 為基礎的封包交換(Packet Switching)，因此也容易遭受到針對 IP 的常見攻擊，阻斷服務攻擊即為其中一項。在此攻擊中，受害者行動裝置上的惡意軟件首先檢測設備上的數據服務是否已經啟動，若已啟動，此惡意軟件便伺機發送訊息至攻擊者裝置，攻擊者便能接收到受害者所在的 IP 位址，而因為 VoLTE 採用全 IP 傳輸的 IMS 架構，攻擊者可傳送大量偽造 IP 來源的訊息封包，且每一次 SIP 呼叫要建立時，一個「INVITE」信號就會產生一次新的 SIP 對話，當伺服器端接收到 UE 的「INVITE」信號，儘管訊息接收者沒有答覆這個對話，依舊會建立個別的通訊乘載通道（bearer），在多個 bearer 生成的狀況下，便會佔用無線介面 LTE-Uu 之控制層面(Control-plane)的資源。

而 VoLTE 傳輸的其中一個特點為採取滿足 QoS 的策略，相較網路或者視頻流量等等，會優先傳送語音封包，使得 VoLTE 能夠保持良好的通話品質，降低中途斷訊的情況發生，其中，信令乘載擁有最高優先權(如圖 5-37)，然而這卻成為有心人士利用 VoLTE 的誘因。攻擊者可透過信令乘載通道，將普通數據包偽裝成信號封包，3GPP²⁹⁰的規範提及，QoS 語音數據流量參數是在「INVITE」信號中所制定，因此攻擊者若能改寫此參數，便能增加乘載通道的容納頻寬，加上利用 SIP 的高優先性，高速傳送大

²⁹⁰ 3GPP. ETSI TS 23.228. IP Multimedia Subsystem (IMS) Stage 2, 2011.

量垃圾訊息到受害者的裝置上，造成 IMS 核心網路因封包資料開道（P-GW）的負載量過大而資源耗竭，無法提供服務。此外，因為 IMS 會檢查 SIP 對話請求是否已呼叫過，若是，則會丟棄此則信號，所以攻擊者會隨機產生 SIP 信號裡的 Call-ID 及 tag 參數(如上圖 5-36 紅色框框處)避免重複請求的出現。而在這個攻擊的過程當中，若受害者並未申辦流量無限使用的服務，受害者將會因為接收到大量的數據包而必須向電信運營商支付巨額的費用。

除此之外，在前文 VoLTE 架構介紹到，CSCF 主要為建立及處理 SIP 的信號，其中，P-CSCF 為終端傳送 SIP 信號之第一站，而 P-CSCF 會藉由確認信息中是否有未經定義的欄位來過濾掉異常的 SIP 信號。然而服務器的容量有限，此舉將會導致 P-CSCF 的負擔量過大，使得實際上所能處理的信號數量受到大幅影響，因此當惡意使用者從多個終端機傳送大量的 SIP 信號時，無論此信號是否為異常，P-CSCF 都必須進行處理及過濾，造成所能提供的資源超過負荷，最終癱瘓 VoLTE 整體服務，因此亦會引發 DoS 攻擊的產生。

QCI	Priority	Bearer Type	Delay	Loss	Traffic Example
1	2	Guaranteed Bit Rate (GBR)	100 ms	10^{-2}	VoLTE calls video call
2	4		150 ms	10^{-3}	
...	...		...	...	
5	1	non-GBR	100ms	10^{-6}	VoLTE signaling Web, Email, etc.
9	9		300ms	10^{-6}	

圖 5- 37 QoS 優先乘載配置

資料來源：ACM²⁹¹

(2) 現有解決方法：

電信運營商應該提出新的機制，嚴格限制 SIP 中 Session 的數量，界定出信息量之最大閾值，超出此數值立即降低其 QoS 的優先配置，進行有效攔截。

除此之外，電信運營商亦可設計一個能夠收集和處理 VoLTE 數據封包的流量檢測系統。LTE 網路中有大量的 VoLTE 流量及數據流量，因此流量的分類及整理非常重

²⁹¹ Li, Chi-Yu, et al. "Insecurity of voice solution volte in LTE mobile networks." Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

要，可以使用 P-GW 和 S-GW 之間的 S5 interface²⁹²來收集流量，並結合機器學習之技術加上欺詐管理系統(Fraud Management Systems, 簡稱 FMS)高效識別出此行為模式是否異常，進而產生潛在欺詐警報，幫助運營商能夠及時阻斷攻擊，確保乘載通道裡的資源有被利用在真實的流量上。

3. 通訊設備收集機密資訊

(1) 安全威脅

當受害者行動裝置連上 VoLTE 網路後，其中之惡意軟件可以監控通訊流量的來往，並檢查受害者所收到之 SIP 訊息，然而由於 SIP 標頭檔(header)中存放著許多資訊，包含 IMS 核心網設備的所有相關資訊，當惡意軟件偵測到 SIP 所回傳之「200 OK」信號後，便能竊取標頭檔中包含有關通訊網路運營商服務器的類型、設備版本等機密資訊(如圖 5-37)，使得攻擊者進一步利用這些訊息來針對此運營商之特定漏洞進行有效攻擊。其中甚至可能包含 S-CSCF 此種負責會話控制及綁定用戶位址和 SIP 位址的服務所使用的相關 IP 位址，進而洩漏出 S-CSCF 中已註冊完畢的終端有哪些，而在 VoLTE 註冊的流程中，「INVITE」信號首要會先抵達 P-CSCF，然而當 P-CSCF 中不包含受害者之 S-CSCF 訊息，「INVITE」信號便無法被傳送到已註冊之 S-CSCF，整個通話建立過程便失敗，而一般來說，S-CSCF 位址的表示方法為一個由其 IP 位址所定義之 URI(Uniform Resource Identifier)，因此攻擊者便可經由所竊取到之「200 OK」信號標頭檔裡的 IP 得到 S-CSCF 之所在位址。

此外，由於整個 IMS 核心網使用相同範圍(range)的 IP 位址可能性極高，且終端之 IP 被惡意軟件鎖定住時，攻擊者可輕易透過此惡意軟件大量傳送 SIP 訊息的請求，並藉由特定 IP 所回傳之訊息，例如「400 Bad」信號，得到 S-CSCF 的 IP 位址，再將大量訊息的請求傳送至已知的 S-CSCF IP 位址，並監控 SIP 所回傳信號之 IP 位址，進而得到整個 IMS 核心網設備中用於提供 VoLTE 服務的 IP 列表(如圖 5-38)。

²⁹² CabelFree, “LTE S5/S8 Interface – Interfaces between the S-GW and P-GW”, [Online]. Available: <http://www.cablefree.net/wirelesstechnology/4glte/lte-s5-s8-interface-s-gw-p-gw/>

```

SIP/2.0 200 OK
...
P-com.siemens.maximum-chat-size:1300
P-com.siemens.maximum-IM-size:1300
P-com.siemens.chat:direct
...

```

圖 5- 38 200 OK 內含運營商相關訊息

資料來源：SSTIC²⁹³

The image shows a Wireshark packet capture of a SIP 200 OK response. The packet list on the left shows several packets, with packet 46 (SIP) selected. The packet details pane on the right shows the structure of the SIP message. Key fields are highlighted with red boxes and labels:

- VoLTE UE IP**: Points to the source IP address in the User Datagram Protocol (UDP) section.
- IMS Gateway IP Address**: Points to the destination IP address in the User Datagram Protocol (UDP) section.
- S-CSCF IP Address**: Points to the 'Service-Route' field in the Message Header section, which contains the IP address of the S-CSCF.

The packet details pane shows the following information:

- Frame 46: 507 bytes on wire (4056 bits), 507 bytes captured (4056 bits)
- Linux cooked capture
- Internet Protocol Version 4, Src: [redacted], Dst: [redacted]
- User Datagram Protocol, Src Port: sip (5060), Dst Port: sip (5060)
- Session Initiation Protocol (200)
 - Status-Line: SIP/2.0 200 OK
 - Status-Code: 200
 - [Resent Packet: False]
 - [Request Frame: 45]
 - [Response Time (ms): 109]
 - Message Header
 - P-Associated-Uri: <sip:01084795800@sktims.net>
 - Service-Route: <sip:orig@[redacted]> S-CSCF IP Address
 - To: <sip:01084795800@sktims.net>;tag=5bc0abe8e2e0f
 - From: <sip:01084795800@sktims.net>;tag=cf3c
 - Call-ID: 0002919076970
 - CSeq: 2 REGISTER
 - Via: SIP/2.0/UDP [redacted];branch=z9hG4bK0005179edc3e
 - Contact: <sip:01084795800@sktims.net>;video;+g.3gpp.icsi-ref="urn:3A3gpp-service.ims.icsi.mmtel";expires=8400

圖 5- 39 200 OK 內含 IP 位址

資料來源：IEEE²⁹⁴

(2) 現有解決方法：

當 P-CSCF 要傳送「200 OK」信號時，電信運營商必須將此標頭檔做嚴格審核，刪除內含任何與通訊設備相關隱密資訊的訊息，進而達到防範攻擊者有目的性的準確攻擊。

²⁹³ Ventuzelo, Patrick, Olivier Le Moal, and Thomas Coudray. "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone.", SSTIC Conference, 2017/6.

²⁹⁴ Park, Seongmin, et al. "Security threats and countermeasure frame using a session control mechanism on VoLTE." Broadband and Wireless Computing, Communication and Applications (BWCCA), 2015 10th International Conference on. IEEE, 2015.

(四) VoLTE 造成用戶端(UE)可能遭受惡意用戶端(Malicious UEs)之資安威脅和現有解決方法

瞭解 VoLTE 因為惡意軟件可能造成的重大危害有哪些之後，在底下篇幅本團隊將進一步探討另一個面向，亦即當攻擊者之角色變成惡意用戶端也就是我們俗稱的駭客時，例如有駭客對行動裝置進行非法的入侵或存取，或是假扮使用者所信任之人傳送病毒皆為此面向所可能造成之危害等等，因此本團隊列出現今常看到的 VoLTE 之間的漏洞若被惡意用戶端濫用將會造成什麼樣的威脅，以及現今技術可做到的相對應解決方法有哪些，陳列幾點如下。

1. MSISDN 欺騙

(1) 安全威脅

由於 SIP 訊息之架構均由文字所組成，因此要從中修改敏感資訊相對容易，惡意用戶端可以經由更改「INVITE」header(標頭檔)中的 From 或者 P-Asserted-Identity(在 IMS 核心網中負責會話控管的 S-CSCF 裡，若要回傳「INVITE」訊息給受害者時，會加在封包裡面的訊息)(如圖 5-40)，於適當的呼叫流程中產生或修改假的 MSISDN(Mobile Subscriber International ISDN number)，由於通訊封包只能經由 P-GW 傳送，只要通話發起人的消息格式正確，VoLTE 並不會在發話者與接收者之間有多一步的驗證，使其能以另一個身分進行通話，進而實現語音釣魚攻擊(voice phishing)，造成惡意用戶端冒充合法公司的電話號碼來詐騙博取受害者之信任，獲得受害者之相關隱私信息，甚至使得罪犯透過所仿冒之電話號碼躲避司法部門的監控，而在最終，通話費用將會累積在惡意用戶端偽造的電話號碼上。

```
INVITE sip:+14085551212@proxy.pstn.net SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;taq=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 69
P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
P-Asserted-Identity: tel:+14085264000
Privacy: id
```

圖 5- 40 P-Asserted-Identity

資料來源：RFC²⁹⁵

(2) 現有解決方法：

透過架構於 IMS 核心網路上的會話邊界控制器²⁹⁶(Session Border Controller,簡稱 SBC)檢查所接收到的「INVITE」憑據，將原 IP 與 header 之內容進行比較，且於註冊時先行確認 S-CSCF 所允許的 URI(Uniform Resource Identifier)為何，若為異常則拒絕請求，並回傳錯誤訊息。

此外，亦可經由電信運營商的控管阻擋用戶端之間封包直接性的互傳，僅許可封包能從用戶端傳遞至 SIP 伺服器進而間接傳送到接收者用戶端，此舉便可有效避免通訊封包缺少認證所造成之上述危害。

在資安威脅的對策上，也可透過 TEID(Tunnel Endpoint Identifier)²⁹⁷此種在 GTP(GPRS Tunneling Protocol)中所使用的辨識符號，在獨立的 LTE 網路中表示方法亦是唯一的，且每當終端連接上 LTE 網路時，TEID 就必須重新產生，可以藉由這個特

²⁹⁵ Jennings, Cullen, Jon Peterson, and Mark Watson. "Private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.", 2002.

²⁹⁶ Hautakorpi, Jani, et al. Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments. No. RFC 5853. 2010.

²⁹⁷ Said, Siwar Ben Hadj, et al. "New control plane in 3GPP LTE/EPC architecture for on-demand connectivity service." Cloud Networking (CloudNet), 2013 IEEE 2nd International Conference on. IEEE, 2013.

色使用 TEID 來設置加密的密鑰，並確認信號封包的完整性，當會話進行時，比對其中的 MSISDN 以及 IP 是否相同(如圖 5-41)，進而判斷此 SIP 訊號的真假。

1st Session Table		2nd Session Table		3rd Session Table	
Session Key	Value	Session Key	Value	Session Key	Value
Uplink Control TEID	Uplink Data TEID	Uplink Data TEID	UE IP	UE IP	MSISDN

圖 5-41 會話控制表

資料來源：SSTIC

2. 竊取 IMEI 信息

(1) 安全威脅

VoLTE 通話建立前，UE 會產生 INVITE 的 SIP 訊息請求，當送出「INVITE」之後，此通話發起者會收到另一個訊息的交換-183 Session Progress (如上圖 5-31)，然而透過可監控網路傳輸確認是否有異常活動的入侵檢測系統(Intrusion-detection System，簡稱 IDS²⁹⁸)發現，「183 Session Progress」回應訊息的 Contact 標頭檔會提供 SIP 中的 URI，以便之後與通話發起者的聯繫²⁹⁹，而惡意用戶端可在雙方尚未連接通話前獲取串接於「+sip.instance」之後的 IMEI (International Mobile Equipment Identity) (如圖 5-42 橘色註記處)，並在接收者不知情的狀況下立即結束通話，導致 IMEI 在神不知鬼不覺的狀況下被洩露，而此為行動裝置的識別碼，就相當於人們的身分證，一旦流出，攻擊者就能知道使用者手機的情報，甚至極有可能被犯罪集團鎖定。

²⁹⁸ Liao, Hung-Jen, et al. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36.1 (2013): 16-24.

²⁹⁹ Real Time Communication, [Online]. Available: "SIP Illustrated 2: SIP Message", <https://realtimecommunication.wordpress.com/2017/02/09/sip-illustrated-2-sip-message/>


```

SIP/2.0 183 Session Progress
Content-Length: 530
User-Agent: IM-client/OMA1.0 Samsung/SM-G920F-XXU2BQFJ Samsung-RCS
/5.0
P-Access-Network-Info: 3GPP-E-UTRAN-FDD;
    utran-cell-id-3gpp={UE_victim_cellid}
Allow: INVITE,BYE,REGISTER,ACK,OPTIONS,CANCEL,SUBSCRIBE,NOTIFY,PRACK
,INFO,REFER,UPDATE
Contact: <sip:{PCSCF_id}@[{PCSCF_ip}]:6000;x-afi=1;encoded-param=
    cGsgcmVnYXJkZXIgaY2UgZ2VucmUgZGUgZGV0YWlsPwo>;+g.3gpp.icsi-ref="
    urn:urn-7:3gpp-service.ims.icsi.mtel";
    *sip.instance="<urn:gsm:imei:{UE_victim_IMEI}>"
CSeq: 1 INVITE
Call-ID: 1920569543@{UE_attacker_ip}

```

圖 5- 42 183 Session Progress

資料來源：SSTIC

(2) 現有解決方法：

藉由電信營運商更嚴苛的安全審核動作，確認出現在「183 Session Progress」裡面對於 Contact 標頭檔欄位中有關 IMEI 的有效資訊是否適宜，於傳輸時過濾對於 UE 來說為非必要之訊息，進而防範攻擊。

3. 竊取詳細地理資訊

(1) 安全威脅

此攻擊危害與上述第二點「竊取 IMEI 信息」相似，同樣經由 IDS 入侵檢測系統監測發現，藉由惡意用戶端傳送 INVITE 指令而得到的 SIP 回傳訊息「183 Session Progress」，我們看到了其中的「P-Access-Network-Info」包含了「utran-cell-id-3gpp」³⁰⁰之值(如上圖 5-42 紅色標註處)，而此為行動裝置連接網路的唯一標識，當使用者被要求提供所在地的資訊時，例如撥打緊急電話時，這個標頭檔即為必須添加的。此由四個主要資訊所組成，分別為：MCC(Mobile Country Code)-行動裝置國家代碼、MNC(Mobile Network Code)-網路電信運營商代碼、LAC(Location Area Code)-為了優化訊號的基站集合區代碼、Cell ID-結合 RNC (Radio Network Controller) 的基站位址編號，如同 google map³⁰¹的應用，使得接收者的定位被準確抓取。進而竊取更多有關

³⁰⁰ Drage, Keith, Roland Jesske, and Christer Holmberg. "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP." (2014).

³⁰¹ Google Maps Geolocation API",Google,2017/6/4, [Online]. Available:

接收者的私人資訊。

(2) 現有解決方法：

與上述第二點「竊取 IMEI 信息」相似，藉由電信運營商更嚴苛的檢核來確保是否「P-Access-Network-Info」所提供的敏感訊息只在基礎設施中出現，並移除一般人民使用的行動裝置中 IMS 核心網路的「P-Access-Network-Info」標頭檔，進而防範有心人士之攻擊。

第二節 基站資安檢測技術研究

以往的電信網路比較封閉且行動裝置無法有強大的運算功能，電信設備技術集中在少數廠商，在安全防護方面可以用不公開的方式來保護內部的機密。然而，隨著標準化以及多樣性的設備，即便是網路設備廠商也能夠切入到電信領域之中，加上行動寬頻應用的興起及智慧型手機的普及，行動寬頻網路內不再只有語音訊務量，這樣的發展導致更快更多的網路服務，新的技術與應用可能因尚未成熟，不管是從無線網路、後置迴路(Backhaul)或核心網路，有機會流入攻擊的網路封包，大大地增加了受攻擊的風險，促使行動寬頻的資安保護趕不上整體架構的安全需求。

3GPP 積極的規劃行動寬頻 4G LTE 的標準，從 Release 8 一直到現在的 Release 15。規範裡面包含了許多系統架構、無線通訊、通訊安全的設計與實作，在第一章的研究背景中，已提到 TS 33.401 是行動寬頻系統架構的安全性規範，該文件規定安全架構，亦即演進分封系統與演進分封核心的安全特性與安全機制，以及包括在演進分封核心(EPC)與演進 UTRAN (E-UTRAN)的分封系統(EPS)內所執行的安全程序。與基站的安全性有密切的關係，可以說是行動寬頻網路的安全基礎架構(請參閱第一章圖 1-8)。

TS33.401 文件中，首先定義行動寬頻網路的整體架構，利用 5 項安全領域來規範應提供的安全機制及其所保護的目標：

(I) 網路接取安全：為用戶提供安全接取服務，特別是防止無線接取連結攻擊。

(II) 網路領域安全：節點能夠安全交換接取網路與服務網路間，以及接取網路內部的信令數據、用戶數據，防止有線網路攻擊。

(III) 用戶領域安全：安全接取行動裝置。

(IV) 應用領域安全：在用戶領域與業者領域安全地交換訊息。

(V) 安全服務的可視性和可配置性：通知用戶安全功能是否運行，是否依據安全功能使用與提供服務。

在其安全架構下，涵蓋的網路單元區分以下：

- HE（Home Environment）與 SN（Serving Network）間的雙向箭頭，表示增加服務網路認證。LTE/SAE 適當調整認證與金鑰協商協議，在 MME 發送 HSS 的認證資料請求消息中，增加了服務網路的身分資訊，並針對 MME 從 HSS 請求多個認證向量情況下的處理機制做了規定，進一步提高了認證與金鑰協商協議的安全性。
- ME（Mobile Equipment）與 SN（Serving Network）間的雙向箭頭表示 ME、SN 間具有非接取層安全機制。也就是增加 ME 對服務網路的認證，LTE/SAE 認證與金鑰協商協議在從 MME 到 HSS 的認證資料請求中，增加了服務網路身分標識（SNID），透過 HSS 驗證 SNID，HSS 可以確保 MME 的合法性，間接使 ME 對服務網路的身分進行認證，藉此防止偽裝基站的安全疑慮。
- AN（Access Network）與 SN（Serving Network）間的雙向箭頭表示 AN、SN 間的通訊具備安全保護機制。

LTE 採取扁平化架構後，基站 eNodeB 納入了更多的控制功能，上述接取網路 AN 單元內即為本計畫所關注的基站安全，在考量 eNodeB 安全要求時，除了 eNodeB 自身的安全性，eNodeB 間共用線路的資料傳輸也是重點之一，也就是後置迴路之安全機制，關於 eNodeB 方面，TS 33.401 內定義了五項安全要求，整理如下：

1. 設定與組態要求

eNodeB 應經過認證與授權，才能設定與進行組態配置，因此攻擊者無法透過本

地或遠端修改 eNodeB 設定與軟體組態。

- eNodeB 與 EPC 應建立雙向認證機制，同時具備保密性、完整性與重傳保護。
- eNodeB 與 eNodeB 應建立雙向認證機制，同時具備保密性、完整性與重傳保護。
- eNodeB 與 O&M 應建立雙向認證機制，同時具備保密性、完整性與重傳保護。
- eNodeB 應確保軟體與數據變更嘗試得到授權。
- eNodeB 應使用經授權的資料或軟體。
- 確保軟體傳送到 eNodeB 的保密性保護與完整性保護。

2. 內部金鑰管理要求

EPC 提供給 eNodeB 的用戶會話(session)金鑰，以及使用於身份認證與安全連結建立程序的長期金鑰，應保護所有存放在 eNodeB 中的金鑰。存放在 eNodeB 中的金鑰應不能離開 eNodeB 中的安全環境，除了有其它 3GPP 標準規定的情形。

3. eNodeB 用戶層資料要求

eNodeB 的任務包括 Uu 介面與 S1/X2 介面的用戶層(User Plane)封包加解密，以及處理 S1/X2 介面的用戶層封包完整性保護。

- 在相關金鑰存放的安全環境下，處理用戶層資料加解密與完整性保護。
- 確保 eNodeB 處理 S1-U 與 X2-U 用戶資料傳輸具備完整性、保密性與重傳保護，不受到未經授權方攻擊。如果需要透過加密方式實現，則可使用 IPsec ESP 技術。

4. eNodeB 控制層資料要求

eNodeB 的任務在於提供 S1/X2 介面的控制層(Control Plane)封包的機密性與完整性保護。

- 在相關金鑰存放的安全環境下，處理控制層資料加解密與完整性保護。
- 確保 eNodeB 處理 S1-MME 與 X2-C 的控制資料傳輸具備完整性、保密性與重傳保護，不會受到未經授權方攻擊。如果需要透過加密方式實現，則可使用 IPsec ESP 技術。

5. 安全環境要求

eNodeB 的安全環境為一種邏輯上的定義，安全環境可以透過相關功能或敏感性操作來實現。

- 安全環境應支援敏感資料的安全化儲存，例如對機密與重要組態資料加密。
- 安全環境應支援敏感功能執行，例如用戶資料的加解密與認證協定。
- 安全環境中的敏感資料不應暴露給外部實體。
- 應確保安全環境的完整性。
- 經授權才能使用或儲存安全環境中資料，或是執行其中的安全功能。

本研究之資安檢測範圍係以基站為主，透過相關資安檢測技術規範研究，規劃基站資安檢測技術及檢測項目，其安全要求適用於所有 eNodeB 類型，並延伸於家用型基站（Home eNodeB，簡稱 HeNB），對於這些特定類型的 eNodeB，3GPP 標準則有更嚴格要求，TR 33.820 安全要求是針對 HeNB 安全所做的評估，由於 HeNB 架設的環境更複雜，面臨的安全問題更多，所以針對 HeNB 的技術研究特別規劃於 TR 33.820 內，在 2009 年正式被納入 TS 33.320 標準規範，而持續更新至今 Release 14 的版本，以下將分別敘述基站與家用型基站的檢測項目規劃。

一、 基站資安檢測技術及項目研究及檢測結果

（一） LTE 架構概述

LTE 主要的系統架構是由核心網 EPC(Evolved Packet Core)與 E-UTRAN(Evolved Universal Terrestrial Radio Access Network)所構成，整體稱為 EPS(Evolved Packet

System)，圖 5-43 為 LTE 系統架構圖³⁰²。整個 EPS 系統由核心網(EPC)、基站(Evolved Node B，簡稱 eNodeB 或 eNB)和使用設備(UE) 3 個部分組成，UE 代表用戶終端設備，而 eNodeB 負責接取網路部分，也稱 E-UTRAN；在虛線右方為 EPC 負責核心網部分，EPC 的組成單元區分為信令處理部分稱 MME(Mobility Management Entity)移動性管理實體，資料處理部分稱為服務閘道 S-GW(Serving Gateway)組成，主要單元如下所述：

- MME 管理核心網路，主要處理 Control-plane 的訊息，如移動性、身分認證以及安全管理。S-GW 管理系統內 User-plane 的訊息，如資料封包的 Routing/Forwarding 以及 Mobility Anchor(eNodeB 間的換手)。
- P-GW(Packet Data Network Gateway)則是負責 User-plane 的外部連結(Internet)，P-GW 與 S-GW 透過 S5 介面來溝通。
- S-GW 則透過 S1 介面與 eNodeB 來溝通，S1 介面可以分為 Control-plane 的 S1-MME 介面(與 MME 做連結)和 User-plane 的 S1-U 介面(與 S-GW 做連結)。

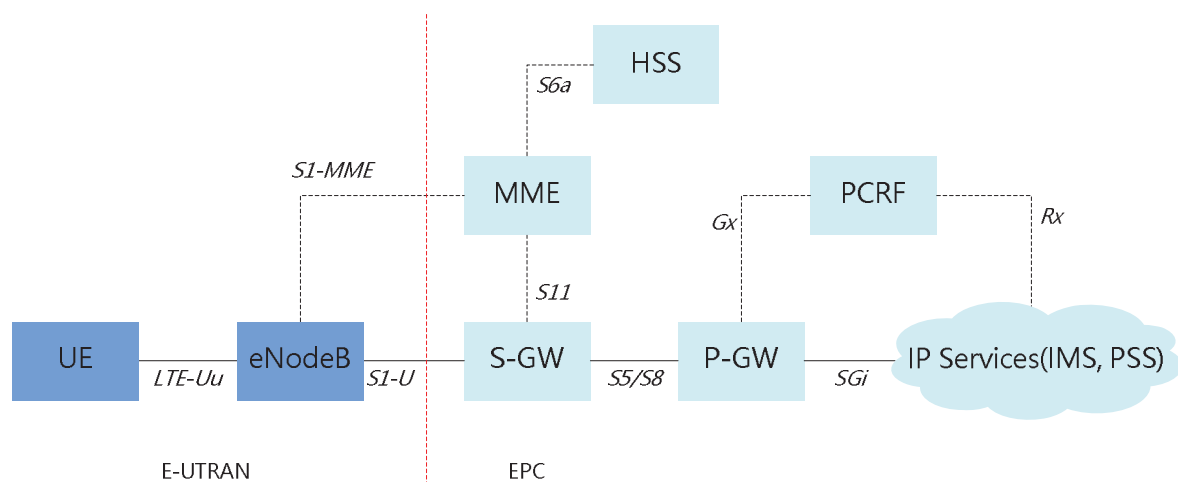


圖 5- 43 LTE 基本系統架構圖

資料來源：本團隊整理

³⁰² 3GPP, TS 36.300 Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Release 14, 2017/6

(二) LTE 基站及協定

在 E-UTRAN 的部分，主要單元為基站 (eNodeB)，及 eNodeB 之間的介面，包含傳輸介面 S1、X2 及無線介面 LTE-Uu 通訊，基站主要功能為：

- 無線資源管理功能：無線承載控制、無線准許控制，連接移動性控制，在上傳和下載的排程，動態資源分配給 UE；
- IP 表頭壓縮和用戶數據的串流加密；
- 當 UE 資訊無法提供 MME 的路由時，決定 MME 的路由選擇；
- 用戶層數據與服務開道的路由；
- 從 MME 發起的排程和呼叫訊息傳輸；
- 從 MME 或 O&M 的排程和廣播資訊傳輸；
- 量測與移動性和排程量測回報配置；
- 從 MME 發起的 PWS 災防告警系統(包括 ETWS 和 CMAS)資訊的排程和傳輸；
- 上傳鏈路的傳送層級分封標記。

上述的功能，如圖 5-44 所示，白色部分為對應的控制實體，藍色部分代無線協定層。

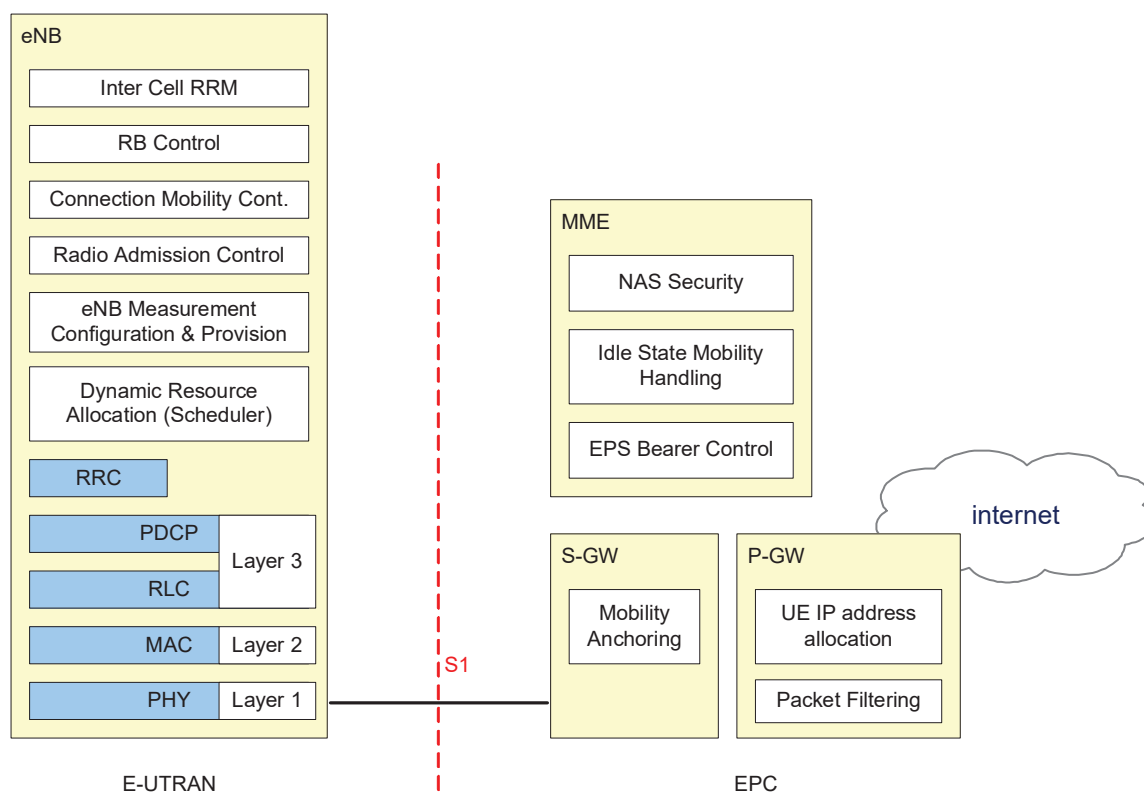


圖 5- 44 E-UTRAN 與 EPC 功能說明

資料來源：3GPP TS36.300 與本團隊整理

LTE 這些通訊協定堆疊（Protocol Stack），按照功能區分可略分為三層：

- 第一層是實體層（Physical Layer，簡稱 PHY），位於最下面的 PHY，用來傳遞無線電波訊號。主要負責承載訊號波段的技術，例如分工技術 Time Division Duplex（TDD）、Frequency Division Duplex（FDD），或是 LTE 採用的 Orthogonal Frequency Division Multiple Access（OFDMA），還有傳輸技術（Multi-input Multi-output，簡稱 MIMO）等。
- 第二層是媒體控制層（Media Access Control，簡稱 MAC），媒體存取控制協定技術位於 LTE 第二層的最下層，其負責主要功能為邏輯通道(Logical Channel)與傳輸通道(Transport Channel)的對應，將屬於單一或不同邏輯通道的 MAC，以服務資料單元(Service Data Unit，簡稱 SDU)多工組合成傳輸區塊(Transport Block)，再透過傳輸通道傳送到實體層。

- 第三層是增加了無線連接控制（Radio Link Control，簡稱 RLC）和封包資料匯聚通訊協定(Packet Data Convergence Protocol，簡稱 PDCP)兩層。RLC 主要是包含了傳輸的可靠性，用來判斷是否要重送訊息；而 PDCP 用來做更高層級的傳輸保護，可以加密資料或是做檔頭的壓縮。

最上層可以分作控制訊號（Control Plane）的無線資源控制（Radio Resource Control，簡稱 RRC）和 EPS 行動管理（EPS Mobility Management，簡稱 EMM），用戶資料的一般 IP 封包，透過無線資源傳遞使用者資料，用一般傳統的 IP 封包來當做傳遞資料的終端地址。然而在傳遞控制訊號時，RRC 用來做無線訊號的管理和設定，在 RRC 之上還有 EMM，用來實作行動寬頻網路中的控制功能，這一層也可以稱之為非存取層（Non-Access Stratum，簡稱 NAS），而 RRC 與 IP 這一段則稱之為存取層（Access Stratum，簡稱 AS）。

（三） LTE 基站介面及安全威脅

行動寬頻網路其服務品質的維持，必須仰賴大量的基站建設，方能提供良好的品質與頻寬，業者必須佈建綿密的基站網路，包含一般基站與家用型基站，而基站間除 S1 介面與核心網連結外，基站彼此間也可以透過 X2 介面直接交換資料如圖 5-45 所示，以提供交遞服務（Handover），或是服務網路內的通訊。

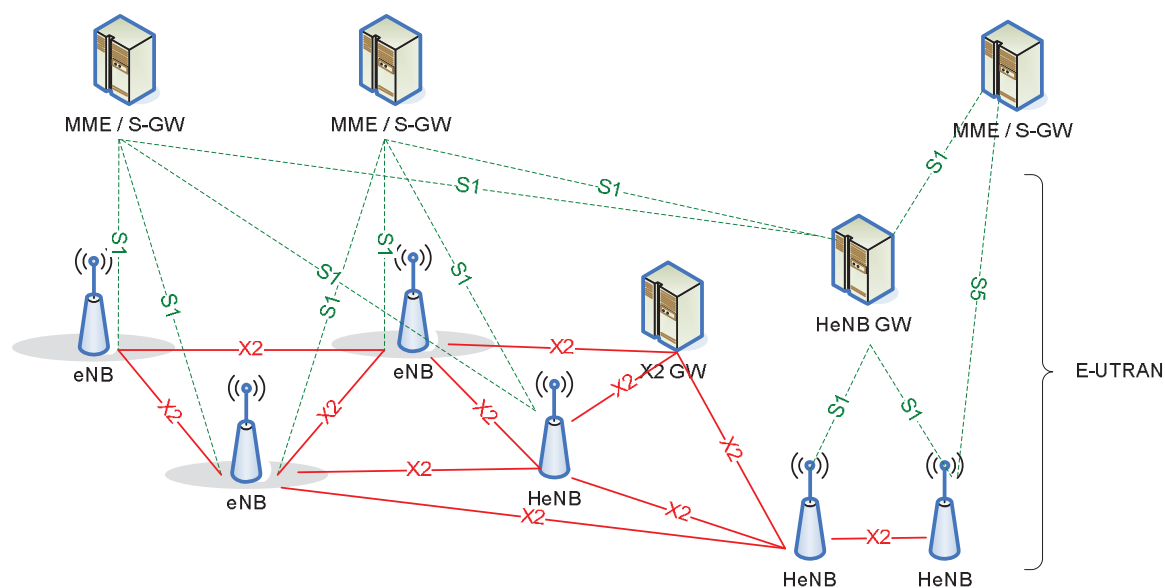


圖 5-45 E-UTRAN 多重架構圖

資料來源：3GPP TS36.300

TS 33.401 是以功能分解 (Functional Decomposition) 的方式，把整個 LTE 系統細分成數個子系統，再把接取網路 (AN) 往下細分成數個功能，分離出基站的五項安全要求，本團隊另由資料流程 (Data Flow) 的導向，考慮 LTE 訊務量流程，分析在基站 S1 與 X2 介面的主要流程，有各式資料及控制會流進或流出不同的處理程序，由基站的功能及流程兩種方式歸納出基站應具備安全保護機制，整理如表 5-5 所示。

表 5-5 基站介面一覽表

介面	範圍	說明
S1-U	S1 User data	與服務閘道(S-GW)的通訊。
S1-C	S1 Control plane	利用 S1-移動管理實體(S1-MME)傳輸介面與移動管理實體(MME)進行溝通。
X2-U	X2 User data	傳遞基站間用戶面資訊。
X2-C	X2 Control plane	支援 eNodeB 與 eNodeB 之間的換手機制。

介面	範圍	說明
OAM	Management	屬於後置迴路，提供不同網路單元訊務交換的管理機制。

資料來源：本團隊整理

根據 ITU-T X.805 協定的描述，電信系統的安全風險和攻擊主要有如下種類：

- 毀壞(Destruction)：資訊及/或其他資源的毀壞(可用性攻擊)。
- 竄改(Corruption/Modification)：資訊的損毀(完整性攻擊)。
- 刪除(Removal)：資訊的盜竊、刪除或遺失和/或其他資源(可用性攻擊)。
- 揭露(Disclosure/Interception)：資訊揭露(保密性攻擊)。
- 阻斷(Interruption)：服務阻斷(可用性攻擊)。

在 LTE 網路架構中有面臨了許多新的威脅，3GPP TR33.805 安全規範依據網路單元提出應對控制面、使用者面、維運管理面三個層面採取控制措施，本研究根據上述相關文獻，整理出 LTE 基站可能面臨的安全威脅，如表 5-6 說明。

表 5-6 基站安全威脅一覽表

安全面	安全威脅
Control Plane 控制面	1. 攻擊者經由無線接取網路(RAN)利用 DoS 方法重複向 MME 發送假訊號訊息，及利用受損的基站 (eNodeB 網路節點或模仿基站 (eNodeB) 自身裝置向 MME 發送假訊號訊息達到安全威脅目的。 2. 攔截移動管理的控制平面訊號流量以竊取用戶或電信電信業者敏感資料。 3. 重複攻擊 (Replay Attack) 修改未受保護的控制平面資料。 4. 攻擊者篡改移動管理的控制訊號訊息進而修改未受保護的控制平面資料，濫用已獲授權之存取權限，隨意更改控制平面流量路徑、入侵無線接取網路領域 (RAN)、由外部或內部網路進入核心網路系統 (EPC) 或任意進行重複攻擊。

安全面	安全威脅
	5. 入侵者偽裝成用戶通過實體網路進行網路存取服務。 6. 攻擊者使用阻斷式攻擊方法由外部網路攻擊基站 eNodeB 節點，利用控制訊號廣播作業影響多個基站 eNodeB 節點服務。
User Plane 用戶面	1. 竊聽未受保護的用戶層服務訊號訊息，攻擊者利用用戶設備（UE）與服務閘道（S-GW）之間的弱點竊聽未受保護的用戶層服務訊號，非法使用路由位址資訊造成用戶通信秘密洩漏。 2. 注入假的用戶層數據封包，攻擊者分別利用壅塞廣播及獲得內部人員權限，經由用戶設備（UE）與移動管理設備（MME）和服務閘道（S-GW）傳送注入假的用戶層數據封包到基站 eNB 節點，造成用戶訊務結算和計費訊號影響。 3. 修改用戶層數據封包，攻擊者入侵傳輸層中受損的基站 eNodeB 或交換器路由設備節點，修改用戶層數據封包然後再置入基站 eNodeB 節點或傳輸層中，造成用戶訊務服務重傳或執行阻斷式攻擊。 4. 濫用已獲授權之存取權影響網路服務或引發阻斷式（DoS）攻擊，隨意更改用戶服務流量路徑或由內/外部網路攻擊無線接取網路域（RAN）或核心網路系統域（EPC）造成用戶訊務服務重傳攻擊。
Management Plane 維運管理面	入侵基站 eNodeB 實體環境，利用近端管理終端 LMT 重設基站 eNodeB 運作參數並趁此漏洞攻擊其他 eNodeB 節點或 MME。

資料來源：本團隊整理

根據這些威脅情境，LTE 網路安全性機制須考慮資訊與服務的保密性、完整性以及可用性的安全威脅，以保護接取層 AS 和非接取階層 NAS 信令之間，及用戶平面的安全為目標，因此透過分層管制的作法展開 LTE 的安全防護，第一線的基站通信傳輸保護提供無線接取與核心網路單獨的加密密鑰，第二線核心系統具備分層安全保護

(Layered Security)，構成 LTE 的安全防護，如圖 5-46 所示。第一層是 E-UTRAN 網路（RRC 安全和用戶平面保護）和第二層是演進分組核心（EPC）網路（NAS 信令的安全性）³⁰³。

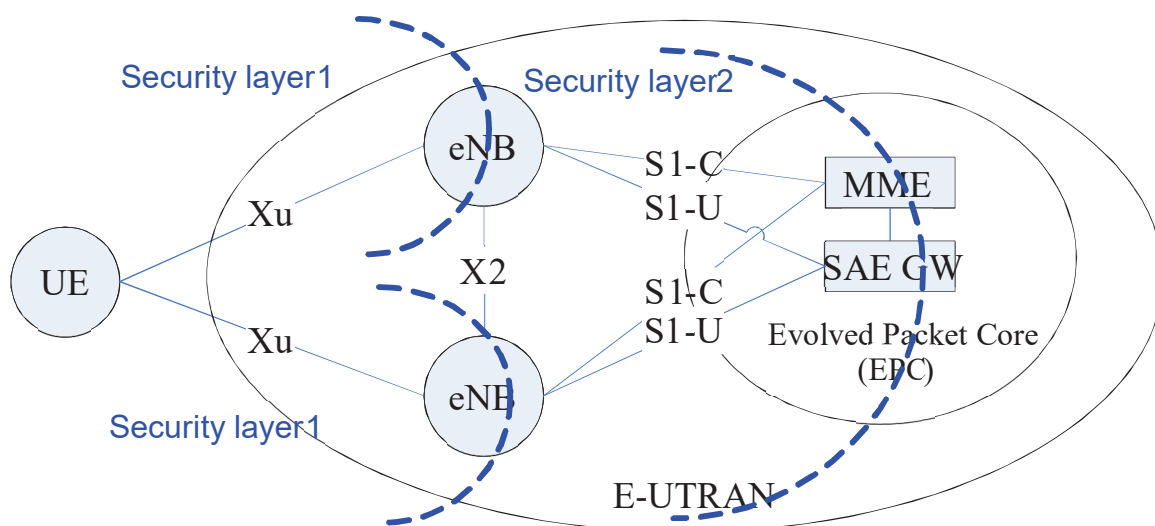


圖 5-46 E-UTRAN 網路安全階層示意圖

資料來源：3GPP 及本團隊整理

第一層是應用在 E-UTRAN 區域，在用戶設備（UE）與 eNodeB 之間，訊號傳送介面為 X_u(LTE-Uu)，該安全層提供保護以無線資源控制（RRC）信令。第二層是在用戶設備（UE）和核心（EPC）之間，訊號傳送介面包含 S1-C 和 S1-U，此層提供保護的 NAS 信令在 UE 和 MME 之間的訊息流量安全傳送。這種安全設計方法的優點為，如果安全性在第一層（E-UTRAN）被破壞，則還有第二層的保護可以隔離。

基於上述 LTE 的安全架構說明之後，以下介紹 LTE 如何設置安全配置，在控制平面中，為了使 UE 和 MME 之間安全地傳送 NAS 信令，使用由 K_{ASME} 密鑰產生的 NAS 安全密鑰，每次執行 EPS AKA 時都會生成新密鑰，在 NAS 安全設置完成之後，UE 和 MME 分別在傳輸之前共享 NAS 加密密鑰（K_{NASenc}）和 NAS 完整性保護密鑰（K_{NASint}）。而在 AS 存取層 AS 安全性的目的是使用 AS 安全密鑰在用戶平面中的控制平面中的 UE 和 eNodeB 之間安全地傳送 RRC 訊息。AS 安全密鑰來自於 K_{eNB}，每

³⁰³ 3GPP, TR 33.821 Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE), 2009/6

當建立新的無線電鏈路時(即當 RRC 狀態從空閒狀態移動到連接時)生成新的密鑰。在 AS 安全建立完成之後, UE 和 eNodeB 共享 RRC 完整性密鑰 (K_{RRCint}), RRC 加密密鑰 (K_{RRCenc}) 和用戶平面加密密鑰 (K_{UPenc})。使用這些密鑰的加密和完整性保護在 PDCP 層執行。 K_{RRCint} 和 K_{RRCenc} 用於在控制平面中安全地傳送 RRC 訊消息, K_{RRCint} 進行完整性保護, 並在發送之前使用 K_{RRCenc} 在 PDCP 層進行加密。 K_{UPenc} 用於在用戶平面中安全地傳遞 IP 資料, 發送之前, 資料在 PDCP 層使用 K_{UPenc} 進行加密, 如圖 5-47 所示。

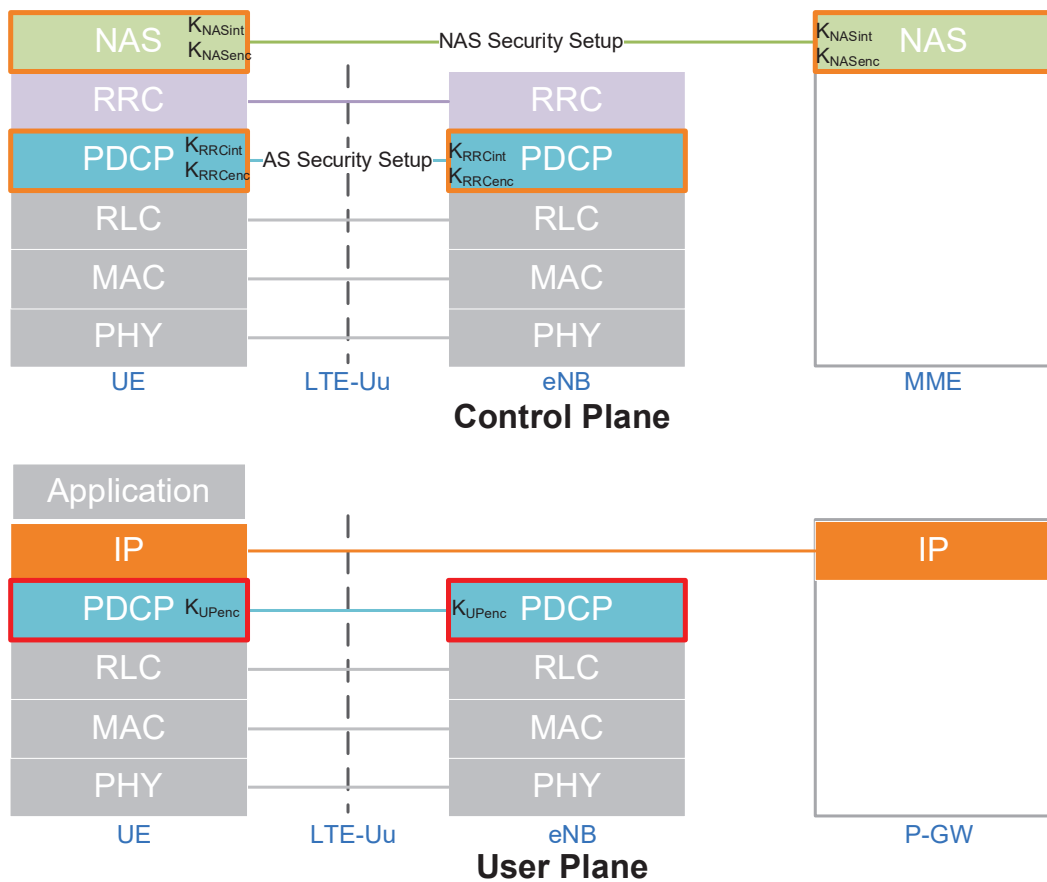


圖 5-47 LTE 基站安全信令

資料來源：本團隊整理

綜上所述, 面對行動網路複雜性, 本章節工作項目首先介紹整個 LTE 網路, 其次闡述電信與網路安全的要求及 LTE 分層的安全架構, 再進入本計畫研究主體基站, 分析基站通訊流程所涵蓋的 S1 介面、X2 介面或管理介面可能的威脅, 提出風險評估以避免攻擊的發生, 以見樹又見林的整體思考, 降低風險及提高安全為目標, 對應在控

制面、用戶面及管理面，可能遭受之資安風險，以規劃基站資安檢測技術及檢測項目。就基站本身及其相關介面資安漏洞，檢測規劃內容將細分為一般性資安檢測項目、HeNB 資安檢測項目及進階資安檢測項目。

（四）一般性資安檢測項目研究及測試結果

一般性檢測項目之目的在於檢測待測基站(eNodeB) 在 S1 傳輸介面負責定義 eNodeB 和移動管理實體/服務閘道器間控制訊息與資料封包的溝通傳遞，及 eNodeB 之間互相連接溝通的 X2 傳輸介面，所支援的通訊協定，包含 SCTP 與 GTP 通訊協定，除了利用 IP 封包來封裝使用者與控制層的訊息，上面還會疊加其他不同的通訊協定來當作路由、機密性保護、完整性保護的實作機制。為了要確認待測基站是否能與測試平臺相通，必須先通過基本的通訊協定測試及相關之信令測試。當基站後端傳輸網路(Backhaul)是利用非專線電路等非信賴網路(untrust network)，IPSec 保護機制則可提供安全通訊的能力與資料傳輸保護，因此本項目亦包含檢測開啟與關閉 IPSec 之安全性測試，一般性檢測項目的工作架構，如圖 5-48 所示。

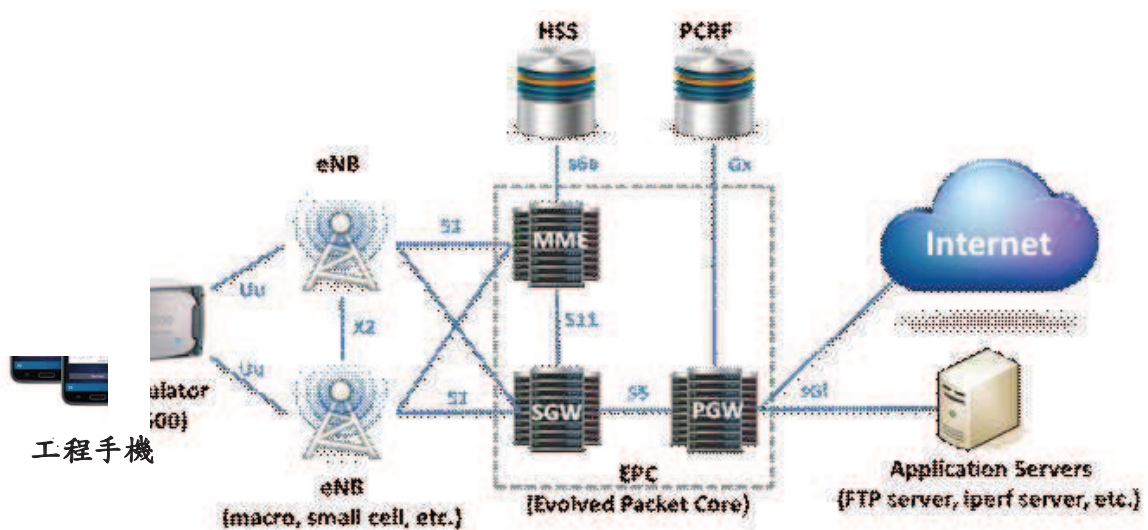


圖 5-48 一般性檢測項目測試架構

資料來源：本團隊整理

以下分別說明本計畫規劃之一般性資安檢測項目，每一項檢測項目包含測試案例、參考資料、測試目的、所符合之資訊安全需求、測試環境暨初始調建、測試方法及合格判定標準。

1. Initial RRC Connection Setup and Reconfiguration

測試案例	Initial RRC Connection Setup and Reconfiguration
參考資料	3GPP TS 36.331 Section 5.3.3
測試目的： 驗證終端找到合適的 cell 後，可成功執行 RRC connection establishment procedure 與基站建立連線進入 RRC_CONNECTED 狀態。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。 3. 終端處於飛航模式	
測試方法： 1. 終端離開飛航模式 2. 終端向基地台發起 RRC connection establishment procedure。 下圖為 RRC connection establishment procedure 的信令流程 <pre> sequenceDiagram participant UE as UE participant eNB as eNB Note over UE: 1 RRC Note over eNB: RRC UE->>eNB: RRC Connection Request (UE identity, establishment cause) Note over UE: 2 RRC Note over eNB: RRC eNB->>UE: RRC Connection Setup (air interface protocol configuration) Note over UE: 3 RRC Note over eNB: RRC UE->>eNB: RRC Connection Setup Complete (PLMN ID, last GUMMEI, embedded EMM message) </pre>	
合格判定標準： 1. 終端向基地台發起 RRC Connection Request，夾帶 UE identity (S-TMSI or random)與 establishment cause 資訊。 2. 基地台回覆 RRC Connection Setup 給終端，夾帶空口協議的配置資訊(PHY、MAC)。 3. 終端根據基地台要求，配置空口相關的協議後回覆 RRC Connection Setup Complete 給基地台，夾帶 PLMN、MME identity 與 EMM message(attach request)資訊。	
測試說明： 在終端上可看到 RRC connection establishment procedure 信令按照 3GPP 規範流程	

測試案例	Initial RRC Connection Setup and Reconfiguration
執行。	

測試結果：UE 終端向基地台發起 RRC Connection Request，夾帶 UE identity 與 establishment cause 資訊，基地台回覆 RRC Connection Setup 給 UE 終端，根據基地台要求，配置空口相關的協議後回覆 RRC Connection Setup Complete 給基地台。如圖 5-49 所示。

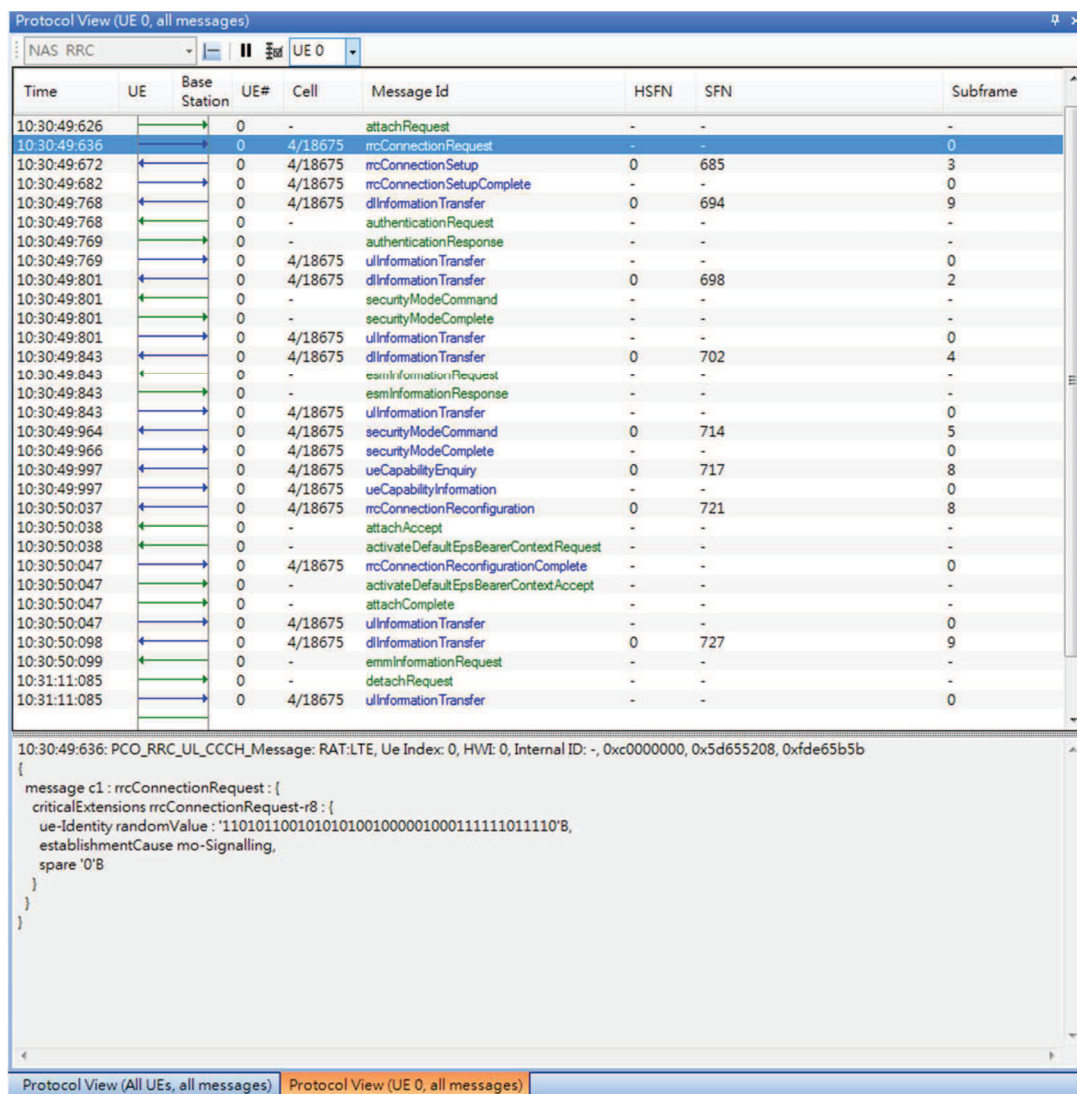


圖 5-49 Initial RRC Connection Setup and Reconfiguration 信令截圖

資料來源：本團隊整理

2. UE Initial Attach (Uu 介面)

測試案例	UE Initial Attach (Uu 介面)
參考資料	3GPP TS 23.401 Section 5.3.2
測試目的： 驗證終端與基地台建立連線進入 RRC_CONNECTED 後，藉由 RRC Connection Setup Complete 向基站發起 ESM PDN Connectivity Request 與 EMM Attach Request。 資訊安全需求： ☐機密性(Confidentiality) ☒完整性(Integrity) ☒可用性(Availability)	
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。 3. 終端處於飛航模式。	
測試方法： 1. 終端離開飛航模式。 2. 終端向基地台發起 RRC connection establishment procedure。 3. 終端向基地台發起 Attach Request。 下圖為終端向基地台發起 Attach Request 的信令流程 <pre> sequenceDiagram participant UE participant eNB participant NewMME as New MME Note over UE, eNB: Contention based random access RRC connection setup steps 1-2 Note over UE, eNB: 1. ESM EMM RRC PDN Connectivity Request Attach Request RRC Connection Setup Complete UE->>eNB: Note over eNB, NewMME: 2. ESM EMM S1-AP PDN Connectivity Request Attach Request Initial UE Message eNB->>NewMME: </pre>	
合格判定標準： 1. 終端向基地台發起 RRC Connection Setup Complete，夾帶 ESM message (PDN Connectivity Request)與 EMM message (Attach Request)。	
測試說明： 在終端上可看到 Attach Request 信令按照 3GPP 規範流程執行。	

測試結果：UE 終端向基地台發起 Attach Request，夾帶 PDN Connectivity Request，傳送 ESM 加密需求。如圖 5-50 所示。

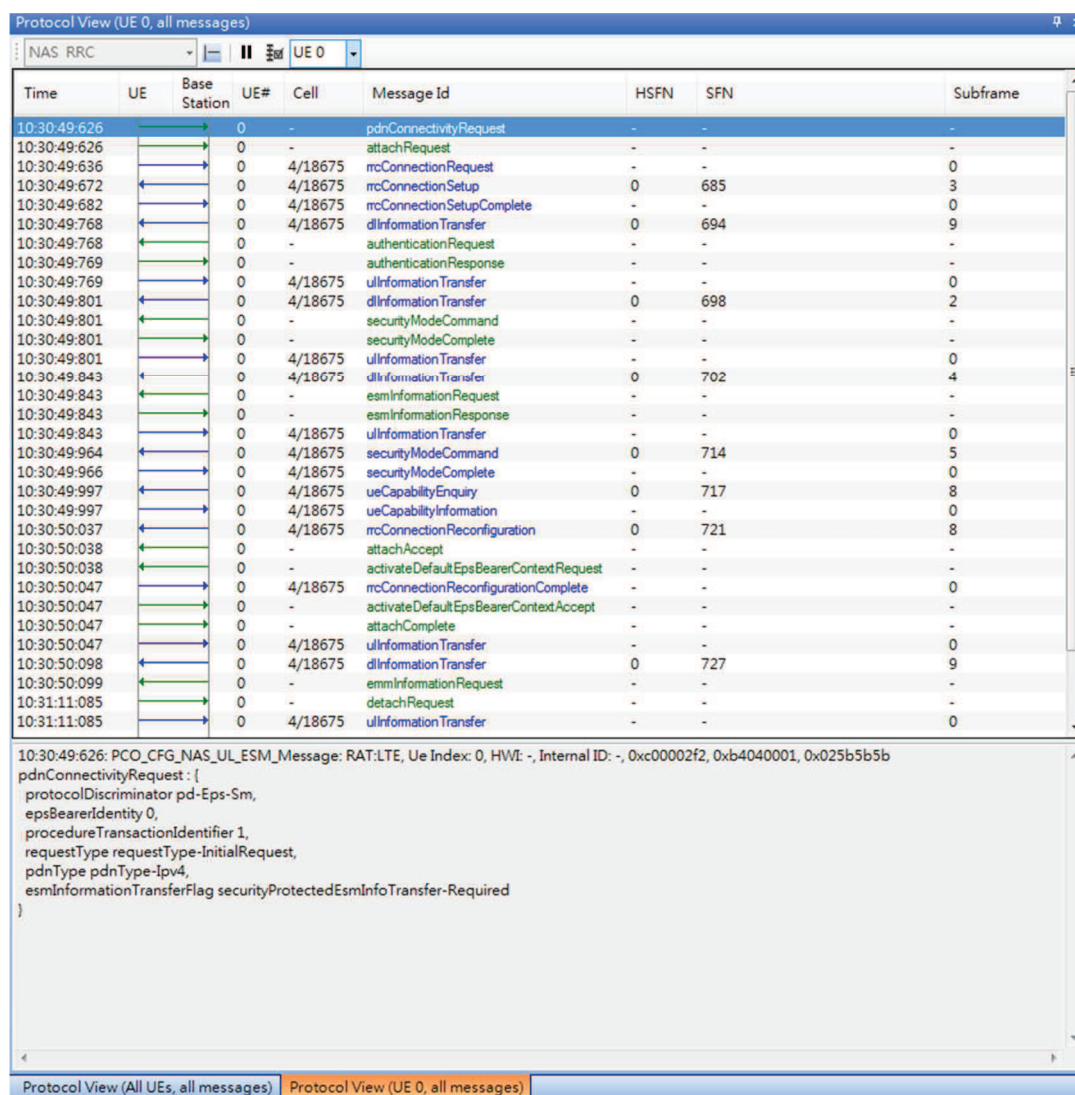
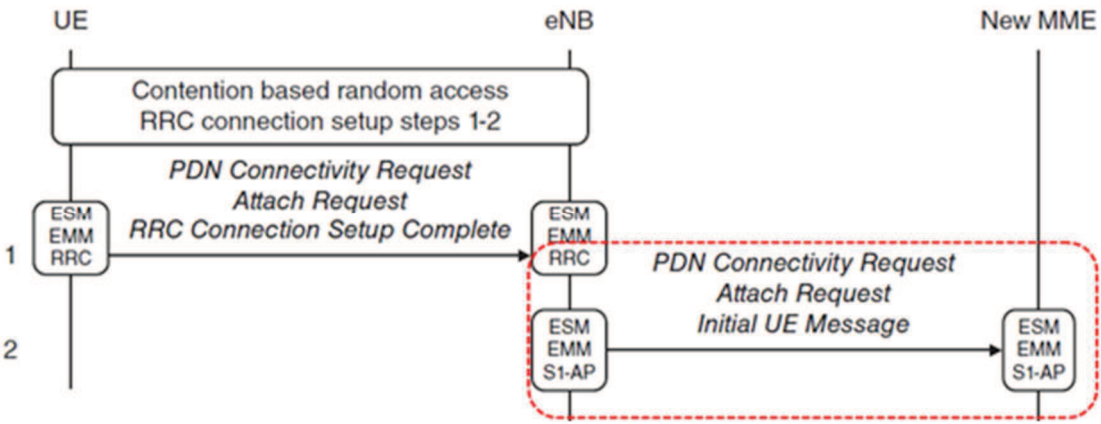


圖 5- 50 UE Initial Attach Uu 介面信令截圖

資料來源：本團隊整理

3. UE Initial Attach (S1 介面)

測試案例	UE Initial Attach (S1 介面)
參考資料	3GPP TS 23.401 Section 5.3.2
測試目的： 驗證基地台收到終端的 RRC Connection Setup 後，將 ESM PDN Connectivity Request 與 EMM Attach Request 截取出來包裝成 Initial UE message 轉傳給 MME。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☒ 可用性(Availability)	

測試案例	UE Initial Attach (S1 介面)
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。 3. 終端處於飛航模式。	
測試方法： 1. 終端離開飛航模式。 2. 終端向基地台發起 RRC connection establishment procedure。 3. 終端向基地台發起 Attach Request。 下圖為終端向基地台發起 Attach Request 的信令流程  <pre> sequenceDiagram participant UE participant eNB participant NewMME as New MME Note over UE,eNB: Contention based random access RRC connection setup steps 1-2 UE->>eNB: PDN Connectivity Request Attach Request RRC Connection Setup Complete Note over UE: 1 Note over UE: 2 Note over eNB: ESM EMM RRC eNB->>NewMME: PDN Connectivity Request Attach Request Initial UE Message Note over eNB: ESM EMM S1-AP Note over NewMME: ESM EMM S1-AP </pre>	
合格判定標準： 1. 終端向基地台發起 RRC Connection Setup Complete，夾帶 ESM message (PDN Connectivity Request)與 EMM message (Attach Request)。 2. 基地台將 ESM 與 EMM message 截取出來並包裝成 S1AP Initial UE Message 轉發給 MME。	
測試說明： 在 S1-MME 介面上可看到 Attach Request 信令按照 3GPP 規範流程執行。	

測試結果：確認 S1AP Initial UE Messag，即 procedureCode: id-initialUEMessage (12) 中有夾帶 NAS message，包含 NAS EPS session management messages: PDN connectivity request 與 NAS EPS Mobility Management Message Type: Attach request，如圖 5- 51 所示。

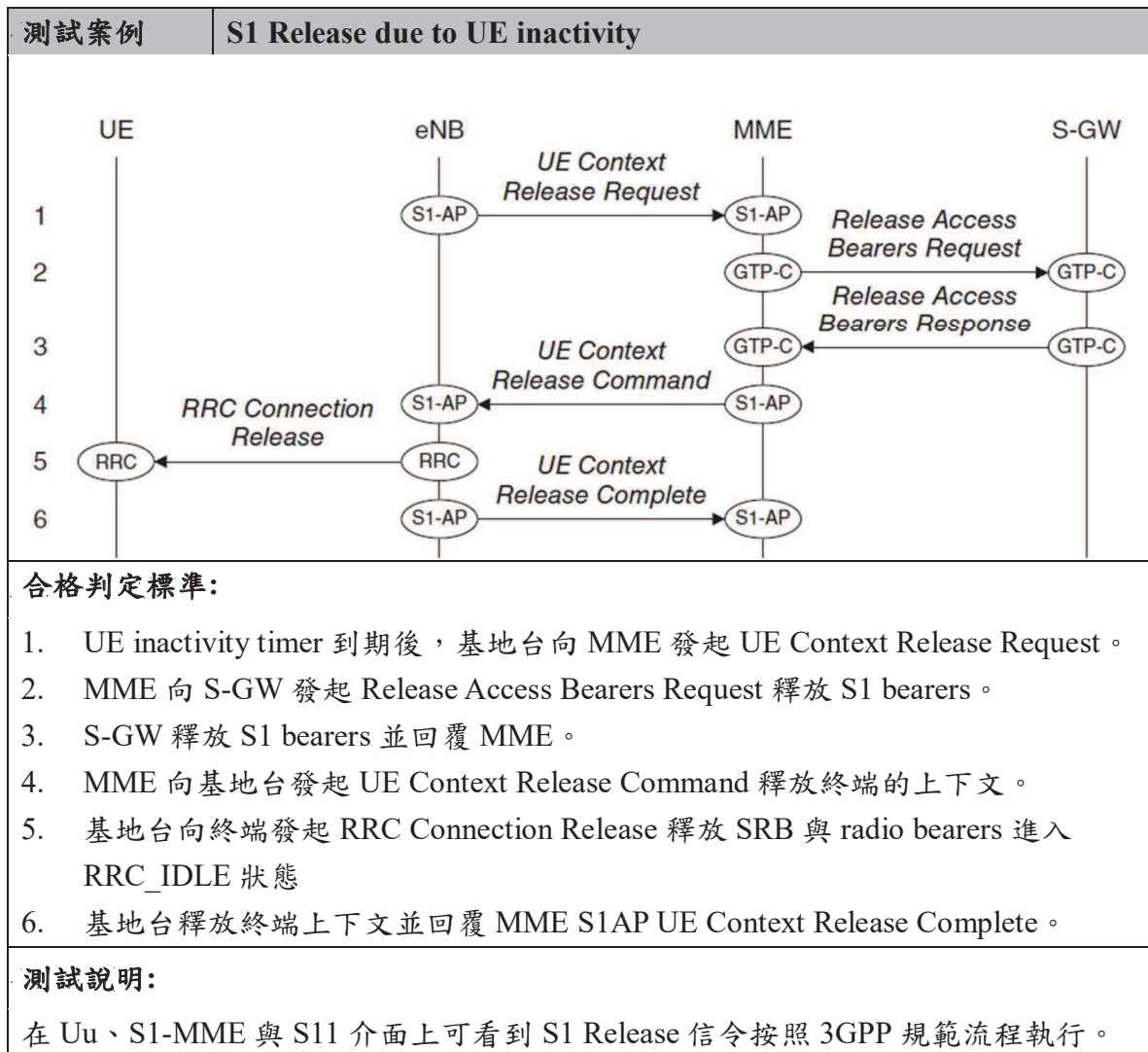
No.	Time	Source	Destination	Protocol	Length	Info
4894	87.041985	10.101.128.66	10.101.145.5	S1AP/NAS-EPS		InitialUEMessage, Attach request, PDN connectivity request
4898	87.091132	10.101.145.5	10.101.128.66	S1AP/NAS-EPS		DownlinkNASTransport, Authentication request
4901	87.113290	10.101.128.66	10.101.145.5	S1AP/NAS-EPS		UplinkNASTransport, Authentication response
▶ Frame 4894: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0 ▶ Ethernet II, Src: Ericsson_1e:6f:ad (ac:60:b6:1e:6f:ad), Dst: Routerbo_02:b6:66 (4c:5e:0c:02:b6:66) ▶ Internet Protocol Version 4, Src: 10.101.128.66, Dst: 10.101.145.5 ▶ Stream Control Transmission Protocol, Src Port: 36422 (36422), Dst Port: 36412 (36412) ▶ S1 Application Protocol ▶ S1AP-PDU: initiatingMessage (0) ▶ initiatingMessage procedureCode: id-initialUEMessage (12) criticality: ignore (1) ▶ value ▶ InitialUEMessage ▶ protocolIEs: 5 items ▶ Item 0: id-eNB-UE-S1AP-ID ▶ Item 1: id-NAS-PDU ▶ Item 2: id-TAI ▶ Item 3: id-EUTRAN-CGI ▶ Item 4: id-RRC-Establishment-Cause						

圖 5- 51 S1AP Initial UE Message 信令截圖

資料來源：本團隊整理

4. S1 Release due to UE inactivity

測試案例	S1 Release due to UE inactivity
參考資料	3GPP TS 23.401 Section 5.3.5
測試目的： 驗證終端進入 RRC_CONNECTED 後，經過一段時間無資料傳輸(UE inactivity timer)觸發 S1 release procedure，釋放 SRB、radio bearer 與 S1 bearer 進入 RRC_IDLE。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。 3. 終端處於飛航模式。 4. 配置 UE inactivity timer 為 30 秒。	
測試方法： 1. 終端離開飛航模式。 2. 終端向基地台發起 RRC connection establishment procedure。 3. 終端向基地台發起 Attach Request。 4. 終端 attach 上 LTE 網路並執行 FTP 上下行資料傳輸。 5. 停止資料傳輸 30 秒。 6. 基地台執行 S1 Release Procedure 釋放相關承載(bearer)，終端進入 RRC_IDLE 狀態。 下圖為基地台發起 S1 Release 的信令流程	



測試結果: 確認基地台向 MME 發起 S1AP UE Context Release Request，
 procedureCode: id-UEContextReleaseRequest (18)、UEContextReleaseRequest，最後，
 確認 MME 向基地台發起 S1AP UE Context Release Command 釋放終端的上下文，如
 圖 5- 52 所示。

No	Time	Source	Destination	Protocol	ENB-UE-S1AP-ID	MME-UE-S1AP-ID	Info
126329	17.920136	10.101.128.66	10.101.145.5	S1AP	262308	4760448	UEContextReleaseRequest [RadioNetwork-cause-user-inactivity]
126330	17.921378	10.101.145.6	10.101.145.4	GTPv2			Release Access Bearers Request
126331	17.921379	10.101.145.6	10.101.145.4	GTPv2			Release Access Bearers Request
126332	17.922827	10.101.145.4	10.101.145.6	GTPv2			Release Access Bearers Response
126333	17.922828	10.101.145.4	10.101.145.6	GTPv2			Release Access Bearers Response
126491	17.937914	10.101.145.5	10.101.128.66	S1AP			UEContextReleaseCommand [RadioNetwork-cause-release-due-to-eutran-generated-reason]
126738	17.980519	10.101.128.66	10.101.145.5	S1AP	262308	4760448	UEContextReleaseComplete

```

> Frame 126329: 94 bytes on wire (752 bits), 94 bytes captured (752 bits) on interface 0
> Ethernet II, Src: Routerbo_02:b6:66 (4c:5e:8c:02:b6:66), Dst: Ericsson_ec:20:d9 (a4:a1:c2:ec:20:d9)
> Internet Protocol Version 4, Src: 10.101.128.66, Dst: 10.101.145.5
> Stream Control Transmission Protocol, Src Port: 36422 (36422), Dst Port: 36412 (36412)
# S1 Application Protocol
# S1AP-PDU: InitiatingMessage (0)
# InitiatingMessage
# procedureCode: id-UEContextReleaseRequest (18)
# criticality: ignore (1)
# value
# UEContextReleaseRequest
# protocolIEs: 3 items
# Item 0: id-MME-UE-S1AP-ID
# ProtocolIE-Field
# id: id-MME-UE-S1AP-ID (0)
# criticality: reject (0)
# value
# MME-UE-S1AP-ID: 4760448
# Item 1: id-eNB-UE-S1AP-ID
# ProtocolIE-Field
# id: id-eNB-UE-S1AP-ID (8)
# criticality: reject (0)
# value
# eNB-UE-S1AP-ID: 262308
# Item 2: id-Cause
# ProtocolIE-Field
# id: id-Cause (2)
# criticality: ignore (1)
# value
# Cause: radioNetwork (0)

```

圖 5- 52 S1AP UE Context Release Request 信令截圖

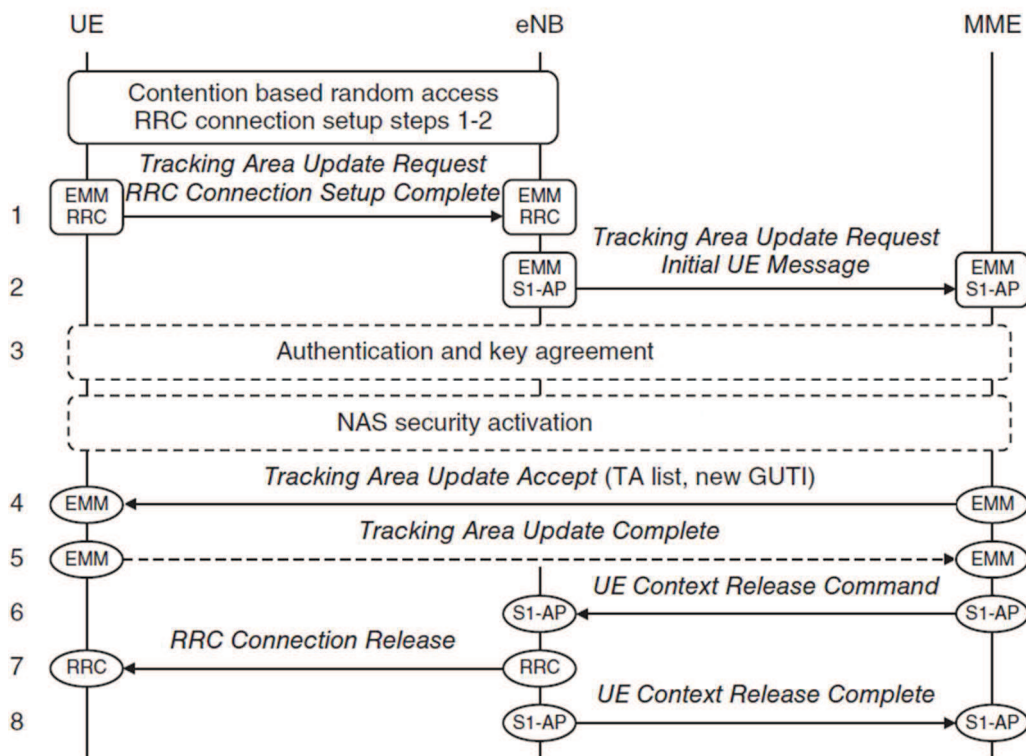
資料來源：本團隊整理

5. Tracking Area Update (追蹤細胞更新狀態)

測試案例	Tracking Area Update (追蹤細胞更新狀態)
參考資料	3GPP TS 23.401 Section 5.3.3
測試目的： 驗證終端週期性的 Tracking Area Update (TAU)告知 MME 其仍然存在 LTE 的覆蓋範圍下，即使 tracking area 沒有改變。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。 3. 終端處於 RRC_IDLE 狀態。 4. 終端處於相同的 MME pool area 與 S-GW service area (MME 與 S-GW 不變)。 5. 配置週期性 TAU 的 timer (T3412)為 60 秒。	
測試方法： 1. 終端 attach 上 LTE 網路並處於 RRC_IDLE 狀態。 2. T3412 到期後終端執行 Tracking Area Update Procedure。 下圖為終端發起 Tracking Area Update 的信令流程	

測試案例

Tracking Area Update (追蹤細胞更新狀態)



合格判定標準:

1. T3412 到期後，終端向基地台發起 RRC connection establishment procedure，並將 EMM message Tracking Area Update Request 包裝在 RRC Connection Setup Complete 中。
2. 基地台將 EMM message 截取出來包裝成 S1AP Initial UE Message 轉發給 MME。
3. (Optional) MME 對終端進行認證與 NAS security activation。
4. MME 向終端回覆 EMM message Tracking Area Update Accept 並夾帶終端所註冊的 tracking areas。
5. (Optional) 若步驟 4 MME 有提供新的 GUTI，終端會回覆 Tracking Area Update Complete。
6. TAU 完成後，上圖步驟 6~8 使終端回到 RRC_IDLE 狀態。

測試說明:

在 Uu 與 S1-MME 介面上可看到 Tracking Area Update 信令按照 3GPP 規範流程執行。

測試結果：確認 UE 終端向基地台發起 EMM message Tracking Area Update Request，基地台將 EMM message Tracking Area Update Request 截取出來包裝成

S1AP Initial UE Message，之後 MME 向終端回覆 EMM message Tracking Area Update Accept，並夾帶終端所註冊的 Tracking area code，如圖 5- 53 所示。

No.	Time	Source	Destination	Protocol	Info
9927	27.510767	10.101.128.39	10.101.145.5	S1AP	UEContextReleaseRequest [RadioNetwork-cause=user-inactivity]
9930	27.530430	10.101.145.5	10.101.128.39	S1AP	UEContextReleaseCommand [RadioNetwork-cause=release-due-to-eutran-generated-reason]
9944	27.550823	10.101.128.39	10.101.145.5	S1AP	UEContextReleaseComplete
19751	55.086830	10.101.145.5	10.101.128.39	S1AP	Paging
631055	1827.650258	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	InitialUEMessage, Tracking area update request
631064	1827.667668	10.101.145.5	10.101.128.39	S1AP	UEContextReleaseCommand [NAS-cause=normal-release]
631076	1827.689710	10.101.128.39	10.101.145.5	S1AP	UEContextReleaseComplete


```

# S1 Application Protocol
# S1AP-PDU: initiatingMessage (0)
# initiatingMessage
  procedureCode: id-initialUEMessage (12)
  criticality: ignore (1)
  # value
    # InitialUEMessage
      # protocolIEs: 6 items
      > Item 0: id-eNB-UE-S1AP-ID
      # Item 1: id-NAS-PDU
        # ProtocolIE-Field
          id: id-NAS-PDU (26)
          criticality: reject (0)
          # value
            NAS-PDU: 1752592952030748330bf664f666000100e0019b715264f6...
            # Non-Access-Stratum (NAS)PDU
              0001 .... = Security header type: Integrity protected (1)
              .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
              Message authentication code: 0x52592952
              Sequence number: 3
              0000 .... = Security header type: Plain NAS message, not security protected (0)
              .... 0111 = Protocol discriminator: EPS mobility management messages (0x7)
              NAS EPS Mobility Management Message Type: Tracking area update request (0x48)
              0... .... = Type of security context flag (TSC): Native security context (for KS-ASME)
              .011 .... = NAS key set identifier: (3) ASME
              .... 0... = Active flag: No bearer establishment requested
              .... .011 = EPS update type value: Periodic updating (3)
              > EPS mobile identity - Old GUTI
              > Tracking area identity - Last visited registered TAI
              > EPS bearer context status
              > Voice Domain Preference and UE's Usage Setting
              > GUTI type - Old GUTI type
              > MS network feature support
            > Item 2: id-TAI
            > Item 3: id-EUTRAN-CGI
            > Item 4: id-RR-Establishment-Cause
            > Item 5: id-S-TMSI

```

圖 5- 53 Tracking Area Update Accept 信令截圖

資料來源：本團隊整理

6. Service Request

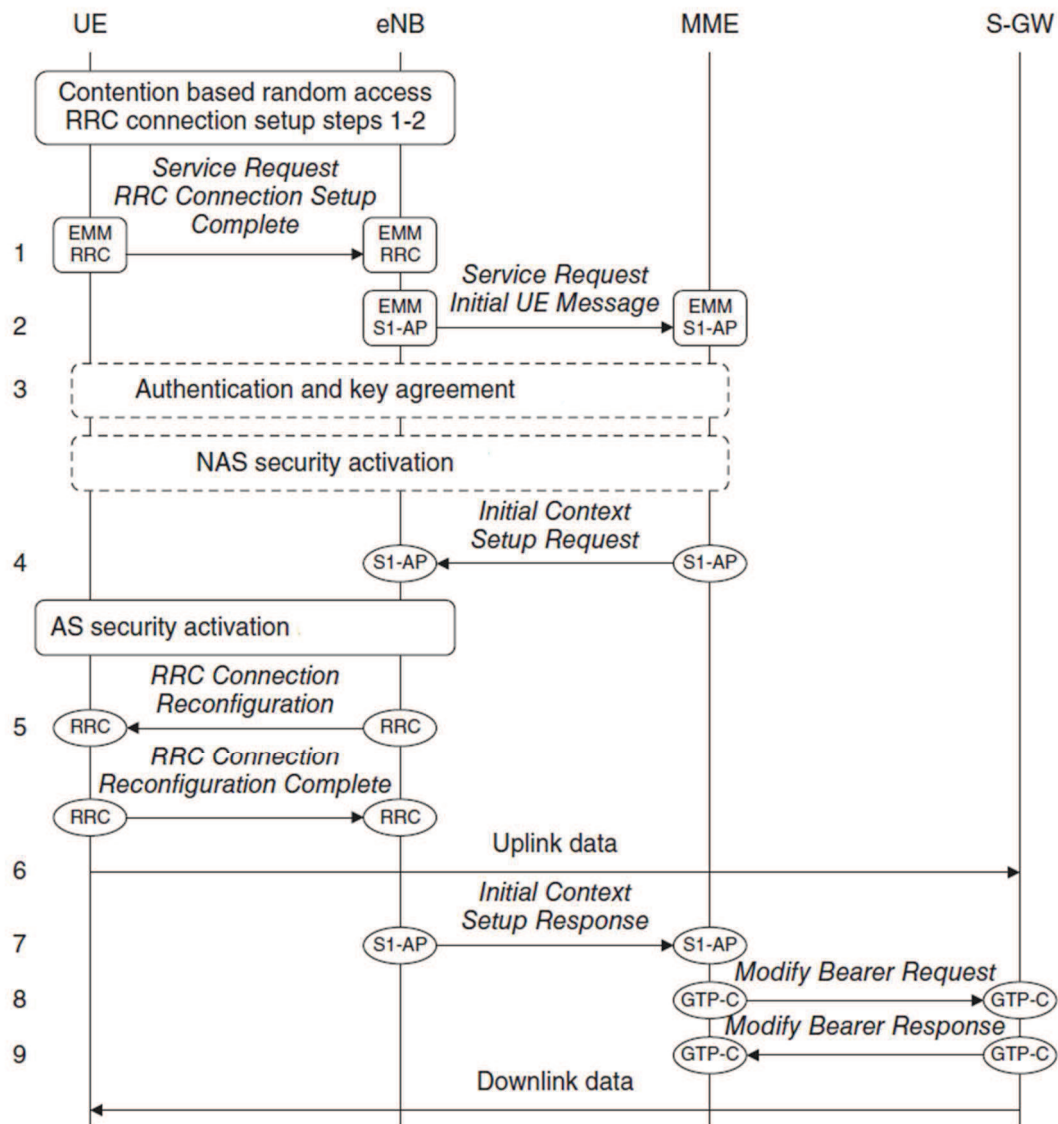
測試案例	Service Request
參考資料	3GPP TS 23.401 Section 5.3.4
測試目的： 驗證終端處於 RRC_IDLE 狀態但需要傳送(Mobile Originated)資料時，觸發 Service Request procedure 進入 RRC_CONNECTED，重建 SRB、radio bearer 與 S1 bearer。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。	

測試案例	Service Request
------	-----------------

測試方法：

1. 終端 attach 上 LTE 網路並處於 RRC_IDLE 狀態。
2. 終端執行 FTP 下行資料傳輸。
3. 終端發起 Service Request Procedure。

下圖為終端發起 Service Request 的信令流程



合格判定標準：

1. 終端與基地台建立 RRC connection 之後，將 EMM message Service Request 包裝在 RRC Connection Setup Complete 發送給基地台。
2. 基地台將 EMM message 截取出來包裝成 S1AP Initial UE Message 轉發給 MME。

測試案例	Service Request
	3. (Optional) MME 對終端進行認證與 NAS security activation。 4. MME 向基地台發起 S1AP Initial Context Setup Request 建立 S1 bearer 與 radio bearer。 5. 基地台向終端發起 RRC RRC Connection Reconfiguration 建立 SRB2 與 radio bearer。 6. 終端可執行上行資料傳輸。 7. 基地台發起 Initial Context Setup Response 回覆 MME，夾帶下行 TEID 資訊。 8. MME 將下行 TEID 藉由 GTP-C Modify Bearer Request 轉發給 S-GW。 9. S-GW 回覆 GTP-C Modify Bearer Response 給 MME。
測試說明： 在 Uu、S1-MME 與 S11 介面上可看到 Service Request 信令按照 3GPP 規範流程執行。	

測試結果：確認 UE 終端將 EMM message Service Request，即 serviceRequest 在 RRC Connection Setup Complete 訊息內發送給基地台，後續基地台將 S1AP Initial UE Message 轉發給 MME，MME 向基地台發起 S1AP Initial Context Setup Request，夾帶 Security Key，如圖 5- 54 所示

No.	Time	Source	Destination	Protocol	ENB-UE-S1AP-ID	MME-UE-S1AP-ID	Info
102048	38.571569	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	2698866		InitialUEMessage, Service request
102057	38.586202	10.101.145.5	10.101.128.39	S1AP	2698866	47583085	InitialContextSetupRequest, UECapabilityInformation
102077	38.610402	100.64.40.7	10.101.136.123	GTP <ICMP>			Echo (ping) request id=0x11b9, seq=0/0, ttl=255 (reply in 102151)


```

# S1 Application Protocol
# S1AP-PDU: initiatingMessage (0)
# initiatingMessage
  procedureCode: id-InitialContextSetup (9)
  criticality: reject (0)
  value
    # InitialContextSetupRequest
    # protocolIEs: 8 items
    > Item 0: id-MME-UE-S1AP-ID
    > Item 1: id-eNB-UE-S1AP-ID
    > Item 2: id-uEAggregateMaximumBitrate
    # Item 3: id-E-RABToBeSetupListCtxtSUReq
    # ProtocolIE-Field
    id: id-E-RABToBeSetupListCtxtSUReq (24)
    criticality: reject (0)
    value
      # E-RABToBeSetupListCtxtSUReq: 1 item
      # Item 0: id-E-RABToBeSetupItemCtxtSUReq
      # ProtocolIE-SingleContainer
      id: id-E-RABToBeSetupItemCtxtSUReq (52)
      criticality: reject (0)
      value
        # E-RABToBeSetupItemCtxtSUReq
        e-RAB-ID: 5
        # e-RABLevelQoSParameters
        qCI: 9
        # allocationRetentionPriority
        priorityLevel: Unknown (6)
        pre-emptionCapability: shall-not-trigger-pre-emption (0)
        pre-emptionVulnerability: pre-emptable (1)
        # transportLayerAddress: 0a659129 [bit length 32, 0000 1010 0110 0101 1001 0001 0010 1001 decimal value 174428457]
        transportLayerAddress(IPv4): 10.101.145.41
        gTP-TEID: 3bdfb11c
    > Item 4: id-UESecurityCapabilities
    # Item 5: id-SecurityKey
    # ProtocolIE-Field
    id: id-SecurityKey (73)
    criticality: reject (0)
    value
      SecurityKey: 6251f736bdd36f27fee91acb54b37e54f1c902951d818d5a... [bit length 256]
    > Item 6: id-HandoverRestrictionList

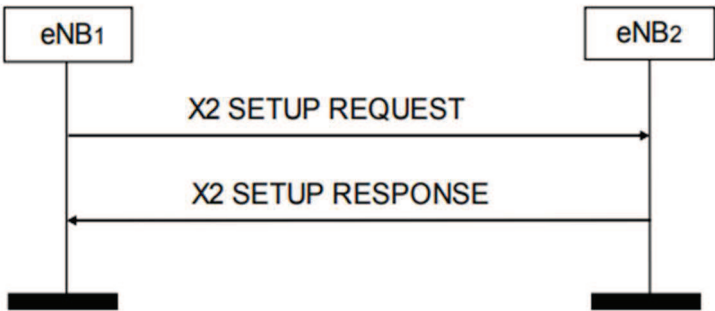
```

圖 5- 54 S1AP Initial Context Setup Request 信令截圖

資料來源：本團隊整理

7. X2 Setup

測試案例	X2 Setup
參考資料	3GPP TS 36.423 Section 8.3.3
測試目的： 驗證基地台與基地台之間可以透過 X2 介面建立連線。 資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： - eNB1、eNB2 與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 - 用戶資料存在 HSS 資料庫中。 - eNB1 與 eNB2 連接到相同的 MME 與 S/P-GW。 - MME 支援 eNB Config Transfer capability。 - eNB1 與 eNB2 之間存在 X2 介面(eNB1 與 eNB2 可以互相 ping 成功)。	

測試案例	X2 Setup
測試方法： 1. 配置 eNB2 為 eNB1 的鄰區，並觸發 X2 Setup procedure。 下圖為 X2 Setup 的信令流程  <pre> sequenceDiagram participant eNB1 participant eNB2 eNB1->>eNB2: X2 SETUP REQUEST eNB2-->>eNB1: X2 SETUP RESPONSE </pre> 合格判定標準： 1. eNB1 向 eNB2 發起 X2 Setup Request，夾帶 eNB1 的 serving cell ID 資訊。 2. eNB2 向 eNB1 回覆 X2 Setup Response，夾帶 eNB2 的 serving cell ID 資訊。 測試說明： 在 X2 介面上可看到 X2 Setup 信令按照 3GPP 規範流程執行。	

測試結果：確認 eNB1 向 eNB2 發起 X2 Setup Request，夾帶 eNB1 的 serving cell ID 資訊，X2 建立成功後，向 eNB1 回覆 X2 Setup Response，夾帶 eNB2 的 serving cell ID 資訊，如圖 5-55 所示。

No.	Time	Source	Destination	Protocol	Info
12102	32.023448	10.101.128.34	10.101.128.39	X2AP	X2SetupRequest
12108	32.024558	10.101.128.39	10.101.128.34	X2AP	X2SetupResponse
Default Message					
> Frame 12108: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0 > Ethernet II, Src: HuaweiTe_2b:1c:33 (e0:28:61:2b:1c:33), Dst: HuaweiTe_2b:14:67 (e0:28:61:2b:14:67) > Internet Protocol Version 4, Src: 10.101.128.39, Dst: 10.101.128.34 > Stream Control Transmission Protocol, Src Port: 2300 (2300), Dst Port: 2300 (2300) * EUTRAN X2 Application Protocol (X2AP) * X2AP-PDU: successfulOutcome (1) * successfulOutcome procedureCode: id-x2Setup (6) criticality: reject (0) * value * X2SetupResponse * protocolIEs: 3 items > Item 0: id-GlobalENB-ID * Item 1: id-ServedCells * ProtocolIE-Field id: id-ServedCells (20) criticality: reject (0) * value * ServedCells: 1 item * Item 0 * ServedCells item * servedCellInfo pCI: 1 * cellId * pLMN-Identity: 64f666 Mobile Country Code (MCC): Unassigned (466) Mobile Network Code (MNC): Unknown (66) eUTRANcellIdentifier: bf429010 [bit length 28, 4 LSB pad bits, 1011 1111 0100 0010 1001 0000 0001 decimal value 200550657] tAC: 2781 (0x0add) * broadcastPLMNs: 1 item > Item 0 * eUTRA-Mode-Info: fDD (0) * fDD uL-EARFCN: 19300 dL-EARFCN: 1300 uL-Transmission-Bandwidth: bw100 (5) dL-Transmission-Bandwidth: bw100 (5) * iE-Extensions: 2 items > Item 0: id-Number-of-Antennaports > Item 1: id-PRACH-Configuration * neighbour-Info: 1 item					

圖 5- 55 X2 Setup Response 信令截圖

資料來源：本團隊整理

8. Downlink NAS Transport 核心網路向用戶端裝置回應程序處理結果

測試案例	Downlink NAS Transport
參考資料	3GPP TS 24.301 Section 6.6.1.2
測試目的： 驗證下行 NAS 訊息(MME→終端)可正確的藉由 S1 介面(S1AP)與 Uu 介面(RRC)傳送。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。 3. 終端處於飛航模式。 4. 終端有配置 ESM information transfer flag。	

測試案例	Downlink NAS Transport
測試方法： 1. 終端離開飛航模式並 attach 上基地台。 下圖為 Downlink NAS Transport (ESM Information Request)的信令流程	
合格判定標準： 1. MME 向 UE 發起 ESM Information Request，並包裝成 S1AP Downlink NAS Transport 傳送給基地台。 2. 基地台將 ESM message 包裝成 DL Information Transfer 轉傳給 UE。	
測試說明： 在 S1-MME 與 Uu 介面上可看到 Downlink NAS Transport 信令按照 3GPP 規範流程執行。	

測試結果： MME 向 UE 發起 ESM Information Request 傳送給基地台，確認基地台將 ESM message 包裝成 DL Information Transfer 轉傳給 UE，如圖 5-56 所示。

No.	Time	Source	Destination	Protocol	Info
2506	6.769856	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	InitialUEMessage, Attach request, PDN connectivity request
2528	6.826115	10.101.145.5	10.101.128.39	S1AP/NAS-EPS	DownlinkNASTransport, Authentication request
2536	6.839315	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	UplinkNASTransport, Authentication response
2541	6.850849	10.101.145.5	10.101.128.39	S1AP/NAS-EPS	DownlinkNASTransport, Security mode command
2545	6.864328	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	UplinkNASTransport, Security mode complete
2550	6.875661	10.101.145.5	10.101.128.39	S1AP/NAS-EPS	DownlinkNASTransport, ESM information request
2556	6.889287	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	UplinkNASTransport, ESM information response

▶ Frame 2550: 118 bytes on wire (944 bits), 118 bytes captured (944 bits) on interface 0
 ▶ Ethernet II, Src: Routerbo_02:b6:66 (4c:5e:0c:02:b6:66), Dst: HuaweiTe_2b:1c:33 (e0:28:61:2b:1c:33)
 ▶ Internet Protocol Version 4, Src: 10.101.145.5, Dst: 10.101.128.39
 ▶ Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
 ▲ S1 Application Protocol
 ▲ S1AP-PDU: initiatingMessage (0)
 ▲ initiatingMessage
 procedureCode: id-downlinkNASTransport (11)
 criticality: ignore (1)
 ▲ value
 ▲ DownlinkNASTransport
 ▲ protocolIEs: 3 items
 ▶ Item 0: id-MME-UE-S1AP-ID
 ▶ Item 1: id-eNB-UE-S1AP-ID
 ▲ Item 2: id-NAS-PDU
 ▲ ProtocolIE-Field
 id: id-NAS-PDU (26)
 criticality: reject (0)
 ▲ value
 NAS-PDU: 2798a763eb010201d9
 ▲ Non-Access-Stratum (NAS)PDU
 0010 = Security header type: Integrity protected and ciphered (2)
 0111 = Protocol discriminator: EPS mobility management messages (0x7)
 Message authentication code: 0x98a763eb
 Sequence number: 1
 0000 = EPS bearer identity: No EPS bearer identity assigned (0)
 0010 = Protocol discriminator: EPS session management messages (0x2)
 Procedure transaction identity: 1
 NAS EPS session management messages: ESM information request (0xd9)

圖 5- 56 Downlink NAS Transport 信令截圖

資料來源：本團隊整理

9. Uplink NAS Transport 用戶端裝置向核心網路發送程序處理需求

測試案例	Uplink NAS Transport
參考資料	3GPP TS 24.301 Section 6.6.1.2
測試目的： 驗證上行 NAS 訊息(終端→MME)可正確的藉由 S1 介面(S1AP)與 Uu 介面(RRC)傳送。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 基地台與核心網成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。 2. 用戶資料存在 HSS 資料庫中。	

測試案例	Uplink NAS Transport
3. 終端處於飛航模式。 4. 終端有配置 ESM information transfer flag。	
測試方法： 1. 終端離開飛航模式並 attach 上基地台。 下圖為 Uplink NAS Transport (ESM Information Response)的信令流程	
合格判定標準： 1. 終端向 MME 回覆 ESM Information Response 夾帶 APN 資訊，並包裝成 RRC UL Information Transfer 傳送給基地台。 2. 基地台將 ESM message 包裝成 S1AP Uplink NAS Transport 轉傳給 MME。	
測試說明： 在 S1-MME 與 Uu 介面上可看到 Uplink NAS Transport 信令按照 3GPP 規範流程執行。	

測試結果：UE 終端向 MME 回覆 ESM Information Response 傳送給基地台，基地台將 ESM message 包裝成 UplinkNASTransport 訊息轉傳給 MME，夾帶完整性與機密性演算法資訊，如圖 5- 57 所示。

No.	Time	Source	Destination	Protocol	Info
2506	6.769856	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	InitialUEMessage, Attach request, PDN connectivity request
2528	6.826115	10.101.145.5	10.101.128.39	S1AP/NAS-EPS	DownlinkNASTransport, Authentication request
2536	6.839315	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	UplinkNASTransport, Authentication response
2541	6.850849	10.101.145.5	10.101.128.39	S1AP/NAS-EPS	DownlinkNASTransport, Security mode command
2545	6.864328	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	UplinkNASTransport, Security mode complete
2550	6.875661	10.101.145.5	10.101.128.39	S1AP/NAS-EPS	DownlinkNASTransport, ESM information request
2556	6.889287	10.101.128.39	10.101.145.5	S1AP/NAS-EPS	UplinkNASTransport, ESM information response

▶ Frame 2556: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
 ▶ Ethernet II, Src: HuaweiTe_2b:1c:33 (e0:28:61:2b:1c:33), Dst: Routerbo_02:b6:66 (4c:5e:0c:02:b6:66)
 ▶ Internet Protocol Version 4, Src: 10.101.128.39, Dst: 10.101.145.5
 ▶ Stream Control Transmission Protocol, Src Port: 36412 (36412), Dst Port: 36412 (36412)
 ▲ S1 Application Protocol
 ▲ S1AP-PDU: initiatingMessage (0)
 ▲ initiatingMessage
 procedureCode: id-uplinkNASTransport (13)
 criticality: ignore (1)
 ▲ value
 ▲ UplinkNASTransport
 ▲ protocolIEs: 5 items
 ▶ Item 0: id-MME-UE-S1AP-ID
 ▶ Item 1: id-eNB-UE-S1AP-ID
 ▲ Item 2: id-NAS-PDU
 ▲ ProtocolIE-Field
 id: id-NAS-PDU (26)
 criticality: reject (0)
 ▲ value
 NAS-PDU: 27b0ecba71010201da280908696e7465726e6574
 ▲ Non-Access-Stratum (NAS)PDU
 0010 = Security header type: Integrity protected and ciphered (2)
 0111 = Protocol discriminator: EPS mobility management messages (0x7)
 Message authentication code: 0xb0ecba71
 Sequence number: 1
 0000 = EPS bearer identity: No EPS bearer identity assigned (0)
 0010 = Protocol discriminator: EPS session management messages (0x2)
 Procedure transaction identity: 1
 NAS EPS session management messages: ESM information response (0xda)
 ▲ Access Point Name
 Element ID: 0x28
 Length: 9
 APN: internet
 ▶ Item 3: id-EUTRAN-CGI
 ▶ Item 4: id-TAI

圖 5- 57 Uplink NAS Transport 信令截圖

資料來源：本團隊整理

10. IPSec Connection 網際路安全協定傳輸保護機制

測試案例	IPSec Connection
參考資料	RFC 4303
測試目的： 驗證 S1 介面上，所有封包是否可透過 eNB 與 MME/SGW 之間的 IPSec 協定加密。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	

測試環境暨初始條件：

1. eNB 與 MME 成功建立 S1 連線(S1 setup)並正常發射 LTE 訊號。
2. eNB 與 MME/SGW 之間建立 IPSec 通道 (Tunnel)，基本相關參數如下：
 - 協定：ESP
 - 加密演算法：AES-128-CBC
 - 認證演算法：HMAC-SHA-1-96
3. 用戶資料存在 HSS 資料庫中。
4. 終端處於飛航模式。

測試方法：

1. 終端離開飛航模式並 attach 上基地台。
2. 終端瀏覽網頁或從 FTP 伺服器下載檔案。

合格判定標準：

eNB 與 MME/SGW 之間開啟 IPSec 協定之後將無法解析被保護的封包內容。

測試說明：

在 S1 介面上透過 wireshark 封包截取只會看到加密的 ESP 封包。

測試結果：MME/SGW 之間開啟 IPSec 協定後，可以觀察到 IPSec 初始化後，支援與 eNodeB 之間採用 IKE 預共享密鑰或證書認證機制，進一步加強設備之間的相互認證能力，提供封包的傳輸提供機密性和完整性保護，如圖 5- 58 所示。

No.	Time	Source	Destination	Protocol	Length	Info
16	6.281648	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
17	6.312831	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
18	9.000708	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
19	9.077490	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
20	9.313143	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
21	9.344398	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
22	12.063332	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
23	15.063407	192.168.127.77	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
24	34.348827	192.168.127.66	190.1.128.1	ISAKMP	346	IKE_SA_INIT MID=00 Initiator Request
25	36.349012	192.168.127.66	190.1.128.1	ISAKMP	346	IKE_SA_INIT MID=00 Initiator Request
26	39.352483	Private_02:02:03	WistronI_c6:89:21	ARP	60	Who has 192.168.127.77? Tell 192.168.127.66
27	39.352961	WistronI_c6:89:21	Private_02:02:03	ARP	42	192.168.127.77 is at 3c:97:0e:c6:89:21

>	Frame 30: 346 bytes on wire (2768 bits), 346 bytes captured (2768 bits) on interface 0
>	Ethernet II, Src: Private_02:02:03 (10:00:00:02:02:03), Dst: WistronI_c6:89:21 (3c:97:0e:c6:89:21)
>	Internet Protocol Version 4, Src: 192.168.127.66, Dst: 190.1.128.1
>	User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
>	Source Port: 500
>	Destination Port: 500
>	Length: 312
>	Checksum: 0xe0cd [validation disabled]
>	[Stream index: 3]
>	Internet Security Association and Key Management Protocol
>	Initiator SPI: 8e6da4683d348910
>	Responder SPI: 0000000000000000
>	Next payload: Security Association (33)
>	Version: 2.0
>	Exchange type: IKE_SA_INIT (34)
>	Flags: 0x08 (Initiator, No higher version, Request)
>	Message ID: 0x00000000
>	Length: 304
>	Type Payload: Security Association (33)
>	Type Payload: Key Exchange (34)
>	Type Payload: Nonce (40)
>	Type Payload: Notify (41) - NAT_DETECTION_SOURCE_IP
>	Type Payload: Notify (41) - NAT_DETECTION_DESTINATION_IP

0000	3c 97 0e c6 89 21 10 00 00 02 02 03 08 00 45 00	<...!..
0010	01 4c 00 00 40 00 40 11 bb b3 c0 a8 7f 42 be 01	.L..@..
0020	80 01 01 f4 01 f4 01 38 e0 cd 8e 6d a4 68 3d 34	8 ...m.h=4
0030	89 10 00 00 00 00 00 00 00 00 21 20 22 08 00 00	! "...
0040	00 00 00 00 01 30 22 00 00 30 00 00 00 2c 01 01	0". .0... ..
0050	00 04 03 00 00 0c 01 00 00 0c 80 0e 00 80 03 00	
0060	00 08 03 00 00 02 03 00 00 08 02 00 00 02 00 00	
0070	00 08 04 00 00 02 28 00 00 88 00 02 00 00 66 32	(.f2

圖 5- 58 IPSec Connection 信令截圖

資料來源：本團隊整理

(五) 進階資安檢測項目研究及測試結果

由於行動寬頻網路的核心網路元件狀態，包含 HSS、MME、S-GW、P-GW 等，這些具有特定功能的核心網路元件與 UE 和基站的運作正確性息息相關。行動寬頻網路設備供應商與監理機關在當前移動網路日益複雜化下的各種不同需求，衍生資安議題亦在交錯架構下稍有不慎可能導致攻擊事件的發生。

許多國家監管機構逐步要求電信業者必須安全的評估行動寬頻網路與設備的部署，並將視這些設備為國家重要的關鍵基礎設施之一，希望可保證這些網路的可靠性、強健性與安全性，但是電信業者只能在營運期間透過安全架構的設計與應用安全控制來達到整體行動寬頻網路運作的安全，且從一開始就只能倚賴電信製造供應商提供的設備。所以對電信業者而言，如何評量這些電信設備的安全水準相通重要³⁰⁴。

以印度為例，目前印度政府已經規定所有在印度販售或連接到行動通訊網絡之電信設備，必須取得印度電信工程中心(The Telecommunication Engineering Centre, 簡稱TEC)所核發之證書³⁰⁵，其中包含安全之要求須取得印度當地或國際資安標準，例如：IT 相關產品須通過 ISO 15408、資安管理面須取得 ISO 27001 標準、電信相關產品須通過 3GPP 資安標準，並預定將於 2018 年 10 月 1 日起強制生效³⁰⁶。

有鑒於此，本計畫除了一般性測試外，為了要確保基站在進行通訊以及接收控制訊號時與核心網路的安全性，需要測試進階的安全項目來確保基站能夠與測試平臺串接，安全測試項目規劃架構如下圖。

³⁰⁴ GSMA NESAS, [Online]. Available: https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf

³⁰⁵ Extension of time for telecom testing and security certification, [Online]. Available: <http://www.dot.gov.in/sites/default/files/2017%2003%2029%20Extension%20of%20Time%20for%20Telecom%20Testing%20and%20Security%20Certification.pdf>

³⁰⁶ Mandatory Testing and Certification of Telecom Equipments, [Online]. Available: <http://www.tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments/>

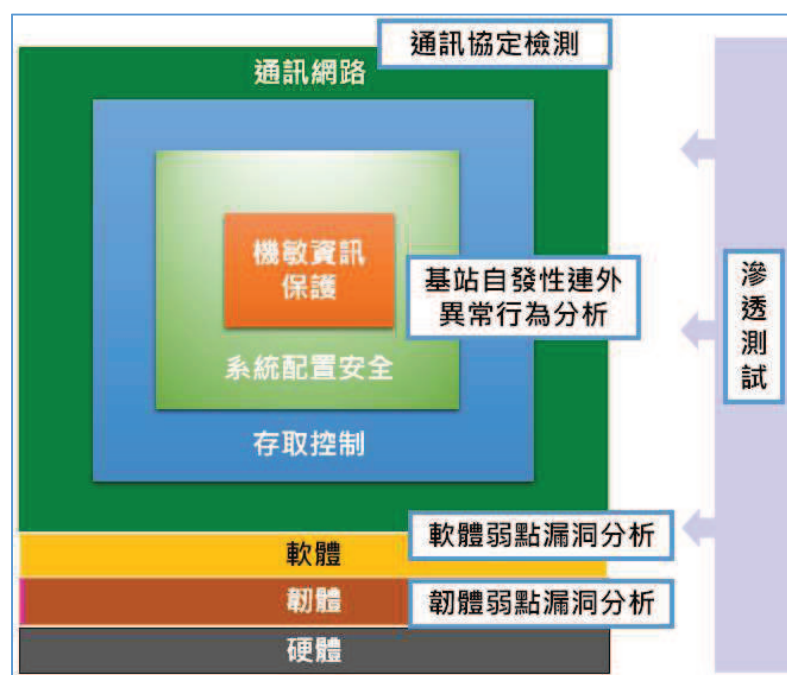


圖 5- 59 進階資安檢測架構

資料來源：本團隊整理

以下分別說明基於進階資安檢測架構圖之每一項檢測項目包含測試案例、參考資料、測試目的、所符合之資訊安全需求、測試環境暨初始調建、測試方法及合格判定標準。

1. 系統配置安全

基站通常為因應不同需求而有對應不同之系統設定配置，但不適合的配置可能引起安全威脅存在，例如：網站伺服器應盡可能採用最低許可權限、當程式處理出現例外應該安全的進行錯誤處理，避免將錯誤訊息外漏、正式上線後產品應移除不需使用之功能或程式檔案、目錄應做好權限設定控管，防止外部不正常的檢索探測等。

1-1. 系統過載狀態時處理機制

測試案例	系統過載狀態時處理機制
參考資料	3GPP TS 33.117 Section 4.2.3.3.1
測試目的：	

測試案例	系統過載狀態時處理機制
基站(eNodeB)應提供關於系統過載，例如：拒絕服務攻擊或者流量增加攻擊，應提供相關措施，避免影響系統運作。 資訊安全需求： ☐機密性(Confidentiality) ☒完整性(Integrity) ☒可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供技術文件說明系統發生過載時之處理機制。	
測試方法： 1. 測試人員檢視文件是否描述系統過載時之控制設計介紹。 2. 測試人員檢視系統是否存有過載控制之觸發門檻值機制。 3. 測試人員檢視文件是否描述遭受何種攻擊會造成系統過載與因應處理之辦法。 4. 測試人員檢視文件是否描述在過載時是否影響安全功能的運作。 5. 測試人員檢視文件是否描述系統在何種最極端過載狀態下會進行重新開機、執行調整動作等。	
合格判定標準： 1. 文件內包含描述系統過載機制資料，並確認已在系統有相對應功能與實作。 2. 文件內包含描述如何產生過載機制的條件，包含如果使用模擬器或腳本之細節說明。 3. 文件內描述系統遭受何種攻擊會造成系統過載與因應處理之辦法。 4. 文件內描述系統在何種最極端過載狀態下會進行重新開機、執行調整動作等	
測試說明： 本測試僅只有一台 C 廠牌基站在介面操作上具備部分需求，但是並無提供相關文件描述最大負載程下會進行重新開機或調整等運作，也並無提供如何產生觸發過載機制條件，建議的模擬器設定或程式腳本細節。	

測試結果：下圖為該基站可透過 eNodeB Flow Control Parameter 設定來控制基站的負載調整情況。

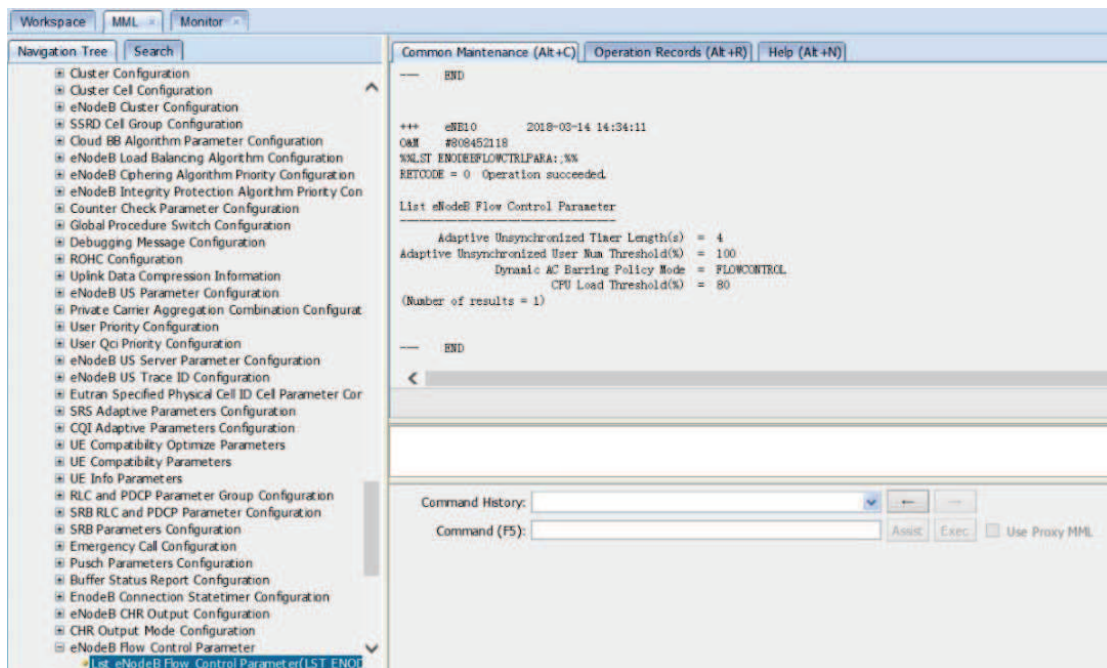


圖 5- 60 C 廠牌基站系統過載狀態時處理機制

資料來源：本團隊整理

下圖可看到 CPU Load Threshold 在測試狀態下設定為 80%，意為當 CPU 處理負荷達 80%會有告警與紀錄產生，以及 Dynamic AC Barring Policy Mode 設定為 FLOWCONTROL，啟用基於服務的動態存取控制用於 Cells 是否擁塞的策略設定，以因應拒絕服務攻擊或者流量增加攻擊。

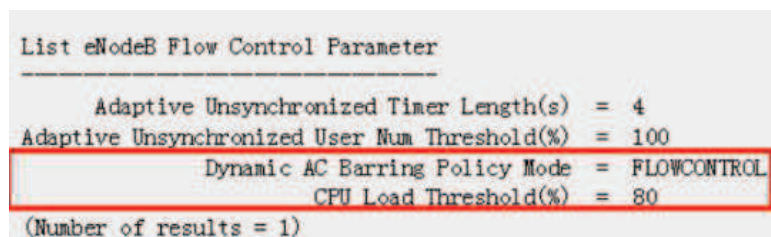


圖 5- 61 C 廠牌基站 Flow Control Parameter

資料來源：本團隊整理

透過上述的設定並搭配下圖的監控機制，以期達到過載預警的保護。

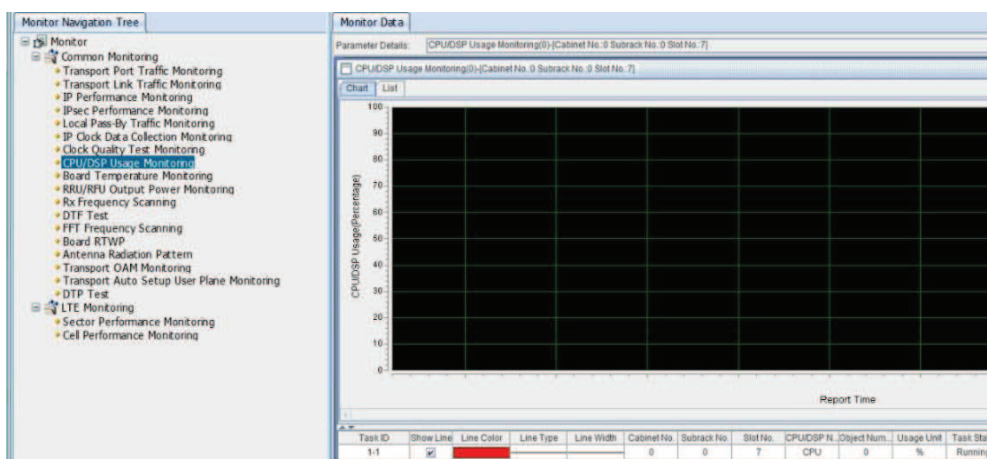


圖 5- 62 C 廠牌基站 CPU/DSP Usage Monitoring

資料來源：本團隊整理

另外 A 廠牌與 B 廠牌基站從測試場域的管理人員表示目前從文件與系統功能上並無相關功能與描述。但是有特別提到這兩組基站都內建有 RRC (Radio Resource Control) 連線功能，可達到部分系統面臨過載時的處理。RRC 係指一種無線資源控制機制，在 UMTS 與 LTE 的空中介面中使用，存在介於 UE 與 eNodeB 之間的 IP 層，主要包含有 RRC 連線管理過程(RRC CONNECTION MANAGEMENT PROCEDURES)、無線承載控制過程(RADIO BEARER CONTROL PROCEDURES)、RRC 連接移動性過程(RRC CONNECTION MOBILITY PROCEDURES) 以及測量過程 (MEASUREMENT PROCEDURES)。本團隊認為對於內建於基站 RRC 的設計與機制，區分不同基站型號系列等，而有不同可支援進階設定的功能，目前仍需要仰賴基站原廠提供更多的資訊才能進一步的掌握。另外，此測試項目整體看來比較偏向可用性的測試，但是電信業者對於基站可用性、效能等管理，必然從系統性的架構來做設計，單一基站若真過度負載無法提供服務，亦仍有區域範圍內其他基站可協同負擔用戶連線話務等處理。

1-2. 系統僅能由內部裝置啟動

測試案例	系統僅能由內部裝置啟動
參考資料	3GPP TS 33.117 Section 4.2.3.3.2
測試目的： 測試基站(eNodeB)內系統僅能由內部裝置啟動	

測試案例	系統僅能由內部裝置啟動
資訊安全需求：	
■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件：	
文件內記錄關於儲存裝置可以啟動系統韌體存取機制。	
測試方法：	
確認基站(eNodeB)是否僅由文件內規定之裝置進行系統啟動。	
合格判定標準：	
基站(eNodeB)不能藉由非韌體規定之裝置啟動系統	
測試說明：	
本項測試 A 廠牌與 B 廠牌基站在實體上並無提供可外部插入之介面，只能透過基站(eNodeB)內系統啟動與提供服務。另外 C 廠牌基站實體有 USB 介面，但是管理人員表示基站所有原廠提供的軟體都存有完整性驗證保護。	

測試結果：如下圖透過 SHA256 密碼雜湊函數技術，不管是更新或透過實體 USB 插入，基站都會進行完整性驗證，避免基站不慎誤植或載入其他來源不明軟體。



```

packcfg.sgn x
--iPSI SIGNFILE BEGIN--
ALGID - SHA256
--iPSI HASH SECTION BEGIN--
--D:/MBTS11.1/trunk/project/makepkg/output/mbts_LO/pkg/temp/SingleOM/Tool/MBTS/packcfg.xml--
a80ab75ba6030841854378e201ae22dae20731fba2022af8d015af7ff8b9822z
--iPSI HASH SECTION END--
--iPSI SIGNATURE BEGIN--
473d26599eeb432e98734ec8d73be294b952ac117984821d5b67a2adf345b562fb87dfe3aa7b6893985bbd09fef31c00e54ce7651a6
SIGN LENGTH - 128
--iPSI SIGNATURE END--
--iPSI SIGNFILE END--

```

圖 5- 63 C 廠牌基站之密碼雜湊函數

資料來源：本團隊整理

1-3. 系統過載處理

測試案例	系統過載處理
參考資料	3GPP TS 33.117 Section 4.2.3.3.3
測試目的：	
測試系統面臨過載狀態下，應可有相對應方式可進行控制。	

測試案例	系統過載處理
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供技術文件說明系統過載處理的機制、測試流程與測試環境。	
測試方法： 1. 測試人員檢視基站(eNodeB)技術文件具備描述系統過載處理的機制或功能，包含如下： (1) 文件包含描述基站(eNodeB)提供可設定系統過載機制之功能。 (2) 文件包含描述基站(eNodeB)當面臨過載時，如何處理調整資源，讓系統回歸至正常運作狀態。 (3) 文件包含描述基站(eNodeB)面臨過載時安全功能的運作。 (4) 文件包含描述基站(eNodeB)在怎樣最壞負載情況下會關機、執行剩餘運作程序等動作。 (5) 文件包含描述可產生觸發過載機制的相關模擬器或程式腳本。	
合格判定標準： 1. 基站(eNodeB)文件內詳細描述測試時過載條件。 2. 基站(eNodeB)文件內描述用於驗證過載控制機制之測試流程。 3. 基站(eNodeB)文件內描述已實作之過載控制機制的過程。 4. 基站(eNodeB)文件描述包含建立過載情境之測試環境。	
測試說明： 本測試僅只有一台 C 廠牌基站在介面操作上具備部分需求，另外 A 廠牌與 B 廠牌基站從測試場域的管理人員表示目前從文件與系功能上並無相關功能與描述，一樣提到透過內建之 RRC (Radio Resource Control)連線功能應可達到負載管控。	

測試結果：下圖為 C 廠牌基站系統過載處理時之測試結果，其可對於若上行同步 (uplink-synchronized) 的 UEs 數量超出設定值時，將會啟動 Adaptive Unsynchronized Timer Length(s)功能設定之參數期間讓部分 UE 短暫無法發送或接受傳輸數據，再透過 Physical Uplink Control Channel (PUCCH)釋放部分資源給其他 UE 使用，以達負載調節之作用。


```

List eNodeB Flow Control Parameter
-----
Adaptive Unsynchronized Timer Length(s) = 4
Adaptive Unsynchronized User Num Threshold(%) = 100
Dynamic AC Barring Policy Mode = FLOWCONTROL
CPU Load Threshold(%) = 80
(Number of results = 1)

```

圖 5- 64 C 廠牌基站系統過載處理的機制

資料來源：本團隊整理

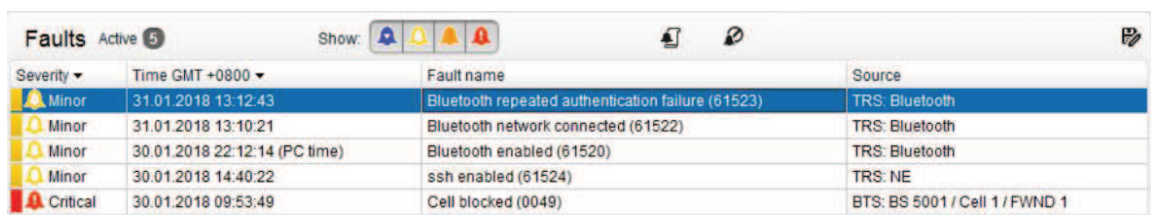
1-4. 安全事件記錄

測試案例	安全事件記錄
參考資料	3GPP TS 33.117 Section 4.2.3.6.1 Security event logging
測試目的： 測試系統提供不同事件類型之安全事件紀錄，例如：登入失敗、管理者存取、管理者操作行為、設定變更、重新開機、關機、當機、網路介面狀態改變。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供已紀錄的安全事件如何存取、安全事件功能如何啟用 2. 測試人員需有足夠的權限執行測試	
測試方法： 1. 測試人員依次觸發每個安全事件類型，並記錄如何觸發之過程。 2. 測試人員檢視安全事件與相關事件描述是否被正確的紀錄。	
合格判定標準： 記錄所有安全事件，包含基站(eNodeB)廠商也提供必要的安全事件說明文件。	
測試說明： 本測試 A、B 與 C 廠牌基站都有提供事件紀錄，但並無法完全滿足 3GPP 規範所有的安全事件類型。	

測試結果：

綜整 A、B、C 廠牌基站之測試結果，各廠牌基站皆尚未完全符合與 3GPP 建議之登入失敗、管理者存取、管理者操作行為、設定變更、重新開機、關機、當機、網路介面狀態改變。但是實質上有些廠牌基站定義的類型內容是與 3GPP 建議相接近，畢竟不同廠牌、型號與市場需求造就不同的設計，但至少都在 3GPP 制定框架下之結果，只是測試場域管理人員表示並無相關文件內容有描述到所有提供的事件類型，仍需原廠提供從設計規格或進階技術文件等才可以掌握清楚的資訊。

下圖為 A 廠牌基站測試結果，從圖上表格第一列可以看到在 Fault name 欄位顯示 Bluetooth repeated authentication failure (61523) 事件，並對應到 Source 欄位顯示 TRS:Bluetooth，此項事件是測試人員使用模糊測試工具刻意對 A 廠牌基站藍芽功能進行測試，致使因為不斷的連線異常觸發此事件紀錄產生。但是 A 廠牌基站從測試場域管理人員表示並無相關文件內容有描述到所有提供的事件類型，仍需原廠提供從設計規格或進階技術文件等才可以掌握清楚的資訊。



Severity	Time GMT+0800	Fault name	Source
Minor	31.01.2018 13:12:43	Bluetooth repeated authentication failure (61523)	TRS: Bluetooth
Minor	31.01.2018 13:10:21	Bluetooth network connected (61522)	TRS: Bluetooth
Minor	30.01.2018 22:12:14 (PC time)	Bluetooth enabled (61520)	TRS: Bluetooth
Minor	30.01.2018 14:40:22	ssh enabled (61524)	TRS: NE
Critical	30.01.2018 09:53:49	Cell blocked (0049)	BTS: BS 5001 / Cell 1 / FWND 1

圖 5- 65 A 廠牌事件記錄

資料來源：本團隊整理

下圖為 B 廠牌基站管理設定介面，測試人員刻意將 administrativeState 調整為 LOCKED 狀態，嘗試觸發一個介面上被關閉之事件，來確認是否該事件會記錄。

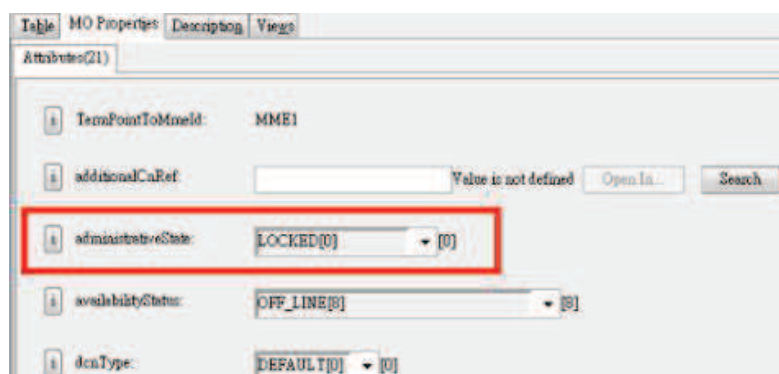


Table	MO Properties	Description	Views
Attributes(21)			
TermPointToMmeId	MME1		
additionalCnRef		Value is not defined	Open In... Search
administrativeState	LOCKED[0]	[0]	
availabilityStatus	OFF_LINE[0]	[0]	
denType	DEFAULT[0]	[0]	

圖 5- 66 B 廠牌基站之 administrativeState 設定

資料來源：本團隊整理

測試結果從下圖表格第五列可以看到 Event Type 欄位為 Communications alarm，而在 Probable Cause 欄位顯示 Unavailable，在最後 Additional Text 欄位更為詳細描述為 S1 Connection Failure for PLMN mcc:66 mnc:66 事件。(註：下圖為求版面清楚，將原圖切分為上下兩部份。)

Alarms: [12/12] Changed: 2018-02-01 16:01:14+08:00			
Severity ▲	Event Type	Time	MO Instance
MAJOR	Communications alarm	2018-01-29 14:19:38+08:00	...,TransportNetwork=1,Synchronization=1,PacketFrequencySyncRef=1
MAJOR	Communications alarm	2018-01-29 14:19:33+08:00	ManagedElement=1,IpSystem=1,IpAccessHostEt=2,IpSyncRef=1
MAJOR	Processing error alarm	2018-01-29 11:17:38+08:00	...ctions=1,Licensing=1,OptionalFeatureLicense=MixedModeRadioLte
MAJOR	Quality of service alarm	2018-01-29 11:17:23+08:00	ManagedElement=1,SystemFunctions=1,Licensing=1
MAJOR	Communications alarm	2018-02-01 16:00:57+08:00	ManagedElement=1,ENodeBFunction=1,EUtranCellFDD=200502236-C
MAJOR	Processing error alarm	2018-02-01 16:00:57+08:00	ManagedElement=1,ENodeBFunction=1,NbIotCell=200502236-c
MINOR	Equipment alarm	2018-01-29 11:19:16+08:00	ManagedElement=1,Equipment=1,RiLink=1
MINOR	Equipment alarm	2018-01-29 13:20:22+08:00	...ment=1,Equipment=1,AntennaUnitGroup=3,AntennaNearUnit=RET-3
MINOR	Equipment alarm	2018-01-29 11:19:16+08:00	ManagedElement=1,Equipment=1,RiLink=6
MINOR	Equipment alarm	2018-01-29 11:19:16+08:00	ManagedElement=1,Equipment=1,RiLink=5
MINOR	Equipment alarm	2018-01-29 11:19:16+08:00	ManagedElement=1,Equipment=1,RiLink=4
MINOR	Equipment alarm	2018-01-29 11:19:16+08:00	ManagedElement=1,Equipment=1,RiLink=2
Alarm summary: 0 6 6 0 0			
Probable Cause		Specific Problem	Additional Text
Unavailable		Packet Server Availability Fault	
Unavailable		NTP Server Reachability Fault	
Configuration or Customizing Error		License Key Missing	
Alarm Indication Signal (AIS)		Emergency Unlock of Software Licensing	Emergency Unlock has been activated and the alar...
Unavailable		PLMN Service Unavailable	S1 Connection Failure for PLMN mcc:466 mnc:66
Underlying Resource Unavailable		Service Unavailable	
Equipment Malfunction		Link Failure	No signal detected (link start time-out). ManagedEI...
Equipment Malfunction		No Connection	Timeout: Failed to get anuConnectIndication
Equipment Malfunction		Link Failure	No signal detected (link start time-out). ManagedEI...
Equipment Malfunction		Link Failure	No signal detected (link start time-out). ManagedEI...
Equipment Malfunction		Link Failure	No signal detected (link start time-out). ManagedEI...
Equipment Malfunction		Link Failure	No signal detected (link start time-out). ManagedEI...

圖 5- 67 B 廠牌基站之事件記錄

資料來源：本團隊整理

下圖為 C 廠牌基站事件紀錄顯示介面，測試人員以帳號登入基站，刻意製造多次登入失敗，來確認基站是否有該筆事件記錄。測試結果如下圖可看到 Detailed Information 小視窗內的 Name 說明有指出 Local User Consecutive Login Retries Failed 紀錄。

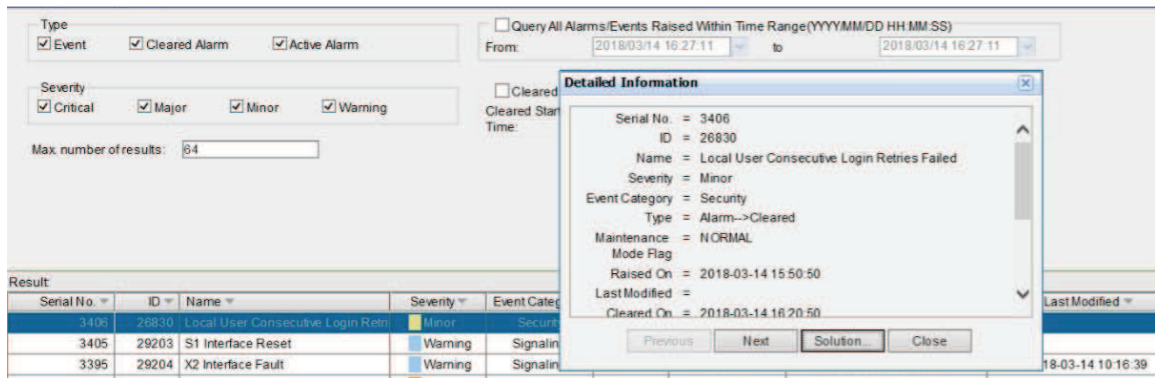


圖 5- 68 C 廠牌基站之事件紀錄詳細資訊

資料來源：本團隊整理

而完整的 C 廠牌基站如下圖，就以事件的角度來看，不同於 A 與 B 廠牌基站，除了 Severity 來表示此事件的嚴重程度外，更特別有區分是歸屬於 Alarm 需盡快處理由一系列事件所組成的警報，或僅是單一 Event 事件。註：下圖為求版面清楚，將原圖切分為上下兩部份。

Result							
Serial No.	ID	Name	Severity	Event Category	Type	Maintenance Mode	Raised On
2872	26261	External Clock Reference	Minor	Hardware	Alarm	TESTING	2018-03-14 16:40:22
2871	26213	NE Startup	Minor	Running	Event	TESTING	2018-03-14 16:39:52
2861	26200	System Clock Failure	Major	Hardware	Alarm->Cleared	TESTING	2018-03-12 19:18:18
2857	25801	Remote Maintenance Lin	Major	Trunk	Alarm->Cleared	TESTING	2018-03-12 19:15:15
2851	26261	External Clock Reference	Minor	Hardware	Alarm->Cleared	TESTING	2018-03-12 19:15:15
2870	28380	NE Shutdown	Major	Running	Event	TESTING	2018-03-14 16:36:06
2869	25881	MAC Excessive Frame Er	Minor	Trunk	Alarm->Cleared	TESTING	2018-03-14 15:04:28
2868	26257	NE Software Download S	Warning	Running	Event	TESTING	2018-03-14 15:02:34
2867	26256	NE Software Download S	Warning	Running	Event	TESTING	2018-03-14 15:00:16
2866	26257	NE Software Download E	Warning	Running	Event	TESTING	2018-03-14 14:57:12
			Critical 64	Major 707	Minor 147	Warning 82	
Last Modified		Cleared On		Common	Special Info	Location	
					RAT_INFO=L, AFFECTE	Res	
					RAT_INFO=L, AFFECTE	Cat	
					RAT_INFO=L, AFFECTE	Soft	
					RAT_INFO=L, AFFECTE	Soft	
					RAT_INFO=L, AFFECTE	Soft	

圖 5- 69 C 廠牌基站之總事件紀錄一覽表

資料來源：本團隊整理

此外，測試人員使用 ping 指令持續丟送封包給基站，基站也會自主將這樣的行為紀錄歸類在 Base Station Being Attacked 類型在事件日誌內，如下圖。

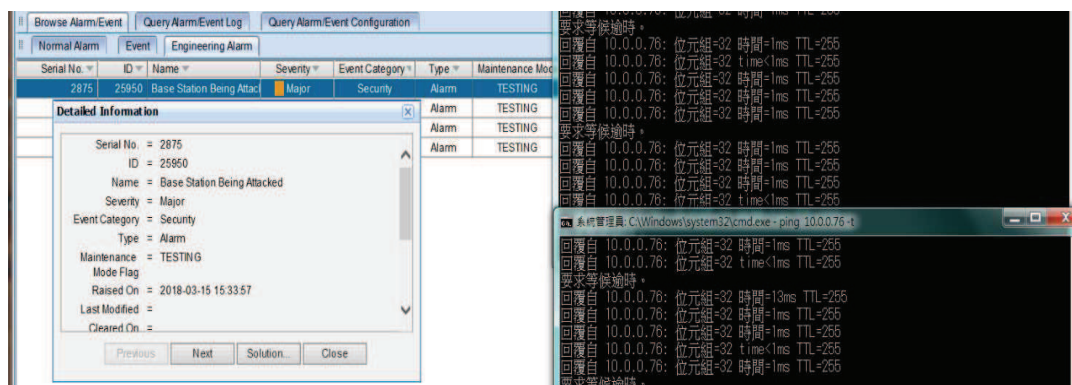


圖 5-70 C 廠牌基站之 Ping 異常事件紀錄

資料來源：本團隊整理

1-5. 網站伺服器日誌

測試案例	網站伺服器日誌
參考資料	3GPP TS 33.117 Section 4.2.5.2.1 Webserver logging
測試目的： 測試網站伺服器日誌有無包含存取的時間戳記、來源 IP 位址、嘗試登入不存在之帳號、網站伺服器回應的狀態代號。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供包含網站日誌存放位置與存取步驟與權限。	
測試方法： 測試人員利用正確與非正確的帳號嘗試登入到網站伺服器，進而檢視是否可符合測試目的之需求。	
合格判定標準： 測試人員可於網站伺服器內檢視測試目的所列之需求。	
測試說明： 本測試 A 與 C 廠牌基站都有提供事件紀錄，而 B 廠牌基站從場域測試管理人員討論中得知並無網站伺服器，很可能是當下這個系列規格未設計。	

測試結果：

綜合 A 與 C 廠牌基站測試，結果並無本項目測試目的提到之網站伺服器回應的狀態代號，而使用不存在帳號登入測試並無看到紀錄。

下圖是 A 廠牌基站之網站伺服器日誌資訊，設計上並無做額外的整理分類，循序式的呈現。

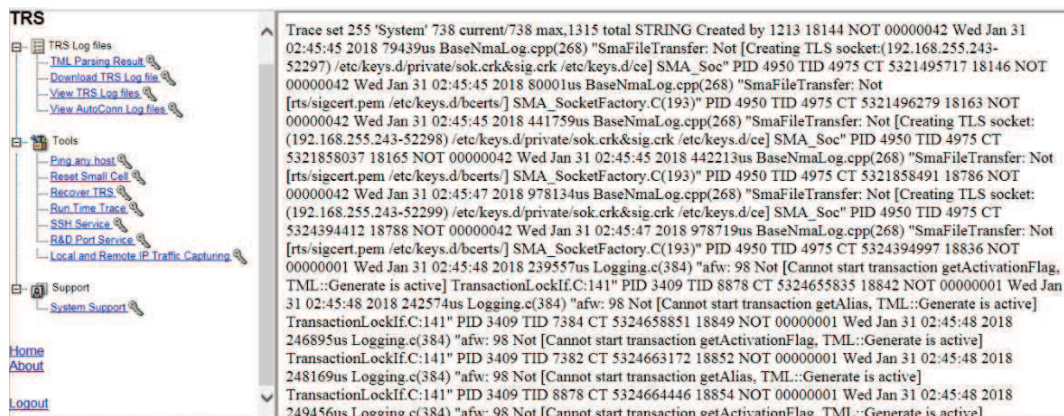


圖 5-71 A 廠牌基站網站伺服器日誌內容

資料來源：本團隊整理

測試人員設計登入基站，並刻意製造多次登入失敗，經查看如下圖描述到"Err [Authentication for user lostjack failed!] SMA_XOHRUIMForwarder.C(819)"的登入錯誤紀錄。

Wed Jan 31 02:55:29 2018 928240us BaseNmaLog.cpp(268) "Err [Authentication for user lostjack failed!] SMA_XOHRUIMForwarder.C(819)" PID 4894 TID 6423 CT

圖 5-72 A 廠牌基站網站伺服器日誌內容摘錄

資料來源：本團隊整理

下圖是 C 廠牌基站之網站伺服器之部份日誌資訊，介面上有以操作人員帳號為主的分類設計。不同於 A 廠牌基站設計，有特別針對所有具備管理者之帳號都需紀錄登入時間、來源 IP 位址、上次登入時間等資訊。

Common Maintenance (Alt+C) Operation Records (Alt+R) Help (Alt+N)									
Operator Name	Status	IP Address	Service	Login Time	Account Status	Use Default Pwd	Last Login IP	Last Login Time	
admin	Online	10.0.0.99	10.0.0.99—O&M System	2018-03-15 11:54:50	Enable	Yes	10.0.0.99	2018-03-15 11:54:50	
admin1	Offline	NULL	NULL	NULL	Enable	No	172.16.105.145	2017-03-20 15:58:58	
admin2	Offline	NULL	NULL	NULL	Enable	No	172.16.105.142	2017-03-17 15:15:13	
admin3	Offline	NULL	NULL	NULL	Enable	No	172.16.105.144	2017-03-21 10:51:55	
test	Offline	NULL	NULL	NULL	Enable	No	NULL	NULL	
scottwu	Offline	NULL	NULL	NULL	Enable	No	10.0.0.99	2018-03-14 15:36:06	
guest	Offline	NULL	NULL	NULL	Enable	No	10.0.0.99	2018-03-15 09:14:00	
(Number of results = 7)									

圖 5- 73 C 廠牌基站網站伺服器日誌內容摘錄

資料來源：本團隊整理

1-6. HTTP 使用者交談識別碼

測試案例	HTTP 使用者交談識別碼
參考資料	3GPP TS 33.117 Section 4.2.5.3 HTTP User sessions
測試目的： 測試使用者與基站(eNodeB)建立連線時，基站(eNodeB)應提供該連線之交談識別碼(Session ID)，做為連線期間之唯一識別碼，並須符合下列需求。 1. 交談識別碼之產生應該具有唯一性，不得重複使用。 2. 交談識別碼具備不可被預測性。 3. 交談識別碼不可以明文方式顯示敏感資訊 4. 交談識別碼應具有時效性，超過則應關閉刪除，使用者在網頁應用中亦須強制登出重新驗證，最大可允許有效時間為八小時。 5. 使用者每次登入網站都須重新產生交談識別碼。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供文件說明產生交談識別碼使用的演算法。 2. 基站(eNodeB)廠商提供文件說明交談識別碼的維護方式與儲存位置，及當超出有效時間時的處理。	
測試方法： 1. 測試人員使用不同使用者帳號重複登入，並連續多次使用相同的使用者帳號，收集交談識別碼。 測試人員驗證以下項目： (1) 測試人員驗證使用相同帳號，但每次登入後的交談識別碼都不同。	

測試案例	HTTP 使用者交談識別碼
(2) 測試人員根據經驗驗證交談識別碼是否隨機產生。	
合格判定標準： 1. 相同使用者帳號，每次登入後的交談識別碼都不同。 2. 交談識別碼隨機產生。 3. 保有交談識別碼最大有效時間為八小時。	
測試說明： 本測試 A 與 C 廠牌基站都有提供透過網頁方式登入。而 B 廠牌基站從場域測試管理人員討論中得知並無網站伺服器，很可能是當下這個系列規格未設計。本測試使用 HP WepInspect 工具來對 A 與 C 廠牌基站之交談識別碼(Session ID)相關機制進行弱點掃描，HP WebInspect 的弱點檢測主要已經包含常見(1)猜測 Session ID (Session Prediction)、(2)竊取 Session ID (Session Hijacking)、(3)固定 Session ID (Session Fixation)共三種攻擊手法。	

測試結果： 整體測試結果並無發現弱點，符合本項目測試需求。

下圖摘錄 A 廠牌基站掃描結果。(註：HP WebInspect 掃描之弱點項目很多，下圖僅特別針對 Session 相關進行摘要整理)。

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
11305	Session Fixation: OAuth	High	Yes	Pass	-
11303	Session Management: Insufficient Session ID Entropy	High	Yes	Pass	-
11289	Session Management: Insufficient Session ID Entropy	High	Yes	Pass	-
11288	Session Management: Insufficient Session ID Length	High	Yes	Pass	-
11201	Session Fixation	High	Yes	Pass	-
11304	Cookie Security: Overly Broad Session Cookie Domain	Medium	Yes	Pass	-
11291	Cache Management: Session Cookies	Medium	Yes	Pass	-

圖 5-74 A 廠牌基站網站伺服器弱點掃描結果

資料來源：本團隊整理

下圖摘錄 C 廠牌基站掃描結果。(註：HP WebInspect 掃描之弱點項目很多，下圖僅特別針對 Session 相關進行摘要整理)

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
11305	Session Fixation: OAuth	High	Yes	Pass	-
11303	Session Management: Insufficient Session ID Entropy	High	Yes	Pass	-
11289	Session Management: Insufficient Session ID Entropy	High	Yes	Pass	-
11288	Session Management: Insufficient Session ID Length	High	Yes	Pass	-
11201	Session Fixation	High	Yes	Pass	-
11291	Cache Management: Session Cookies	Medium	Yes	Pass	-
11304	Cookie Security: Overly Broad Session Cookie Domain	Medium	Yes	Pass	-

圖 5-75 C 廠牌基站網站伺服器弱點掃描結果

資料來源：本團隊整理

1-7. 封包過濾

測試案例	封包過濾
參考資料	3GPP TS 33.117 Section 4.2.6.2.1
測試目的： 測試基站(eNodeB)是否提供可過濾任何 IP 封包之功能 資訊安全需求： ☐機密性(Confidentiality) ☐完整性(Integrity) ☒可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)啟動封包過濾功能。 2. 基站(eNodeB)具備兩個不同邏輯或實體乙太網路介面，將其連結到測試主機。	
測試方法： 1. 測試人員將基站(eNodeB)封包過濾功能設定僅允許來自第一台測試主機的 ICMP 流量。 2. 測試人員從第一台測試主機發送 Ping 流量。 3. 測試人員從第二台測試主機發送 Ping 流量。	
合格判定標準： 第一台測試主機將會收到 Ping 回應，但第二台測試主機不會。	
測試說明： 本測試 A、B、C 廠牌基站在測試場域的管人員表示並無這種用於網通產品，例如：路由器、交換器等設備上具備的功能。	

1-8. 網路介面堅實性需求

測試案例	網路介面堅實性需求
參考資料	3GPP TS 33.117 Section 4.2.6.2.2
測試目的： 測試基站(eNodeB)在運作過程不受其他大量無效封包，並可進行丟棄與不影響基站(eNodeB)效能。包含有：SYN Flood 攻擊、Smurf 攻擊、Ping-of-death 攻擊。 資訊安全需求： ☐機密性(Confidentiality) ☐完整性(Integrity) ☒可用性(Availability)	
測試環境暨初始條件： 1. 測試人員有特殊權限存取登入基站(eNodeB)，包含日誌檔案存取權限。 2. 基站(eNodeB)廠商提供之文件應該至少包含使用到的通訊協定資訊。	
測試方法： 1. 測試人員使用有效的堅實性測試工具，且測試時間需合理可對基站(eNodeB)產生效用的時間為考量。 2. 測試人員檢視基站(eNodeB)是否正常運作且無當機情況。	
合格判定標準： 1. 基站(eNodeB)正常運作且無當機情況。 2. 紀錄使用的堅實性測試工具名稱、版本與設定資訊。 3. 檢視日誌檔案追蹤可能當機或相關錯誤訊息紀錄。	
測試說明： 基站在整個 LTE 網路的架構下原就屬於重要的終端設備，因此為滿足 LTE 行動通訊技術不管是對傳輸效能、頻譜使用效率等各方面，各家電信製造商都遵循 3GPP 所制定出的相關架構指引，在軟硬體規格上都相當嚴謹要求，以求可滿足 LTE 功能與協定一致性的要求，及更進一步追求穩定性與效能，以因應僅一個區域就可能高達成千上萬的用戶連線需求。 因此，本測試項目目前團隊暫缺乏可運用的工具可以對基站可產生有效用與效能上影響之堅實性或壓力測試，這樣的測試也一般用於路由器、交換機等網通設備上會有更實際的需求，在業者部署 LTE 網路服務的整體架構上，都有提供各個基站之間的負載平衡，同區域間單一基站停止服務，就會將負載轉至其他基站協助	

測試案例	網路介面堅實性需求
提供用戶服務，不至於讓該區域的通訊服務停擺。	

1-9. GTP-C 過濾

測試案例	GTP-C 過濾
參考資料	3GPP TS 33.117 Section 4.2.6.2.3
測試目的： 測試基站(eNodeB)是否具備 GTP-C 過濾功能。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供基站(eNodeB)文件描述設定 GTP-C 過濾功能。 2. 基站(eNodeB)內建網路流量分析功能。 3. 測試人員具備權限可於基站(eNodeB)上設定 GTC-C 過濾功能。	
測試方法： 1. 測試人員設定 Interface 1 只接受 GTP-C EchoRequest。 2. 測試人員設定捨棄 Interface 2 上所有 GTP-C 訊息。 3. 測試人員開啟 Interface 2 上之網路流量分析功能 4. 測試人員發送 Interface 2 EchoRequest 訊息，驗證基站(eNodeB)是否可在 Interface 2 收到 EchoRequest 訊息。 5. 測試人員發送 Interface 1 EchoRequest 訊息，驗證基站(eNodeB)是否可在 Interface 1 收到 EchoRequest 訊息。 6. 測試人員設定僅接受 IP 1 位址的 GTP-C EchoRequest，驗證當來源不是 IP 1，EchoRequest 是否被丟棄。	
合格判定標準： 1. 發送 Interface 2 EchoRequest 訊息，基站(eNodeB)可在 Interface 2 收到 EchoRequest 訊息。 2. 發送 Interface 1 EchoRequest 訊息，基站(eNodeB)可在 Interface 1 收到 EchoRequest 訊息	

測試案例	GTP-C 過濾
3. 設定僅接受 IP 1 位址的 GTP-C EchoRequest，來源不是 IP 1，EchoRequest 會被丟棄。	
測試說明： GTP (GPRS Tunneling Protocol, GTP)是一組基於 IP 的通訊協定標準，用於在 GSM、UMTS 和 LTE 網絡中承載 GPRS，而 GTP-C 是該標準中控制的部份。本測試項目相似於 3GPP TS 33.117 Section 4.2.6.2.2 的需求，這部分經在測試環境與 A、B、C 廠牌基站之管理人員討論後認為這些應屬於進階功能，目前基站操作介面上並無這些 GTP 相關的設定功能，對於維運人員而言也無法理解或方法可以知道如何操控這些 GTP 相關功能，只有設備製造商的內部研發測試單位才可以有這些資訊的掌握。然而，毫無疑問這些全球知名電信製造商都必然遵循 3GPP 制定的相關設計需求，只是本測試項目以製造基站的生命週期來看會偏在製造商之研發設計與測試階段，而非在產品上市後一般維運人員可接觸到的功能。	

1-10. GTP-U 過濾

測試案例	GTP-U 過濾
參考資料	3GPP TS 33.117 Section 4.2.6.3
測試目的： 測試基站(eNodeB)是否具備 GTP-U 過濾功能。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供基站(eNodeB)文件描述設定 GTP-U 過濾功能。 2. 基站(eNodeB)內建網路流量分析功能。 3. 測試人員具備權限可於基站(eNodeB)上設定 GTC-U 過濾功能。	
測試方法： 1. 測試人員設定 Interface 1 只接受 GTP-U EchoRequest。 2. 測試人員設定捨棄 Interface 2 上所有 GTP-U 訊息。 3. 測試人員開啟 Interface 2 上之網路流量分析功能	

測試案例	GTP-U 過濾
4. 測試人員發送 Interface 2 EchoRequest 訊息，驗證基站(eNodeB)是否可在 Interface 2 收到 EchoRequest 訊息。 5. 測試人員發送 Interface 1 EchoRequest 訊息，驗證基站(eNodeB)是否可在 Interface 1 收到 EchoRequest 訊息。 6. 測試人員設定僅接受 IP 1 位址的 GTP-U EchoRequest，驗證當來源不是 IP 1，EchoRequest 是否被丟棄。	
合格判定標準： 1. 發送 Interface 2 EchoRequest 訊息，基站(eNodeB)可在 Interface 2 收到 EchoRequest 訊息。 2. 發送 Interface 1 EchoRequest 訊息，基站(eNodeB)可在 Interface 1 收到 EchoRequest 訊息 3. 設定僅接受 IP 1 位址的 GTP-U EchoRequest，來源不是 IP 1，EchoRequest 會被丟棄。	
測試說明： 本測試項目相似於前一個測試內容 GTP-C，都是屬於 GTP (GPRS Tunneling Protocol, GTP)基於 IP 的通訊協定標準，而 GTP-U 是該標準用戶的部份。目前基站操作介面上並無這些 GTP-U 相關的設定功能，同樣認為只有設備製造商的內部研發測試單位才可以有這些資訊的掌握，而非在產品上市後一般維運人員可接觸到的功能。	

1-11. 網路核心功能最小化

測試案例	網路核心功能最小化
參考資料	3GPP TS 33.117 Section 4.3.3.1.2
測試目的： 網路核心功能應關閉不需要的網路元件功能，包含以下： - 關閉 IP 封包在不同介面的轉送，在 linux sysctl.conf 設定 net.ipv4.conf.all.forwarding=0 參數。 - 關閉 APR Proxy，在 linux sysctl.conf 設定 net.ipv4.conf.all.proxy_arp=0 參數。	

測試案例	網路核心功能最小化
3. 關閉直接 Broadcast，設定 net.inet.ip.directed-broadcast=0 參數。 4. IPv4 群播處理應預設丟棄 224.0.0.0 至 239.255.255.255 封包，及應關閉群播路由快取與轉送來避免 Smurf、Fraggle 攻擊。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)有至少兩個實體乙太網路介面。 2. 測試人員有特殊權限存取登入基站(eNodeB)，包含存取 linux sysctl.conf。	
測試方法： 1. 測試人員登入系統驗證 linux sysctl.conf 內設定之參數符合測試目的需求。 2. 測試人員透過流量分析工具，驗證基站(eNodeB)的 IP 封包是否會轉送至其他基站(eNodeB)設備。 3. 測試人員透過流量分析工具，驗證基站(eNodeB)是否會收到 ARP 封包但不回應 ARP 對應主機的 MAC 位址。 4. 測試人員透過流量分析工具，驗證基站(eNodeB)是否會廣播封包。 5. 測試人員透過流量分析工具，驗證基站(eNodeB)若為群播 IP 範圍 224.0.0.0 至 239.255.255.255 時是否會丟棄封包。	
合格判定標準： 1. linux sysctl.conf 內設定之參數符合測試目的需求。 2. 基站(eNodeB)的 IP 封包不會轉送至其他基站(eNodeB)設備。 3. 基站(eNodeB)收到 ARP 封包但不回應 ARP 對應主機的 MAC 位址。 4. 基站(eNodeB)不會廣播封包。 5. 基站(eNodeB)若為群播 IP 範圍 224.0.0.0 至 239.255.255.255 時丟棄封包。	
測試說明： 本測試 A 與 B 廠牌基站無此測試需求之功能，而 C 廠牌基站只支援部份，可能是目前測試環境使用的這些基站系列規格尚未支援與設計。	

測試結果：下圖為 C 廠牌基站可對 ARP Proxy 予以關閉之設定畫面。

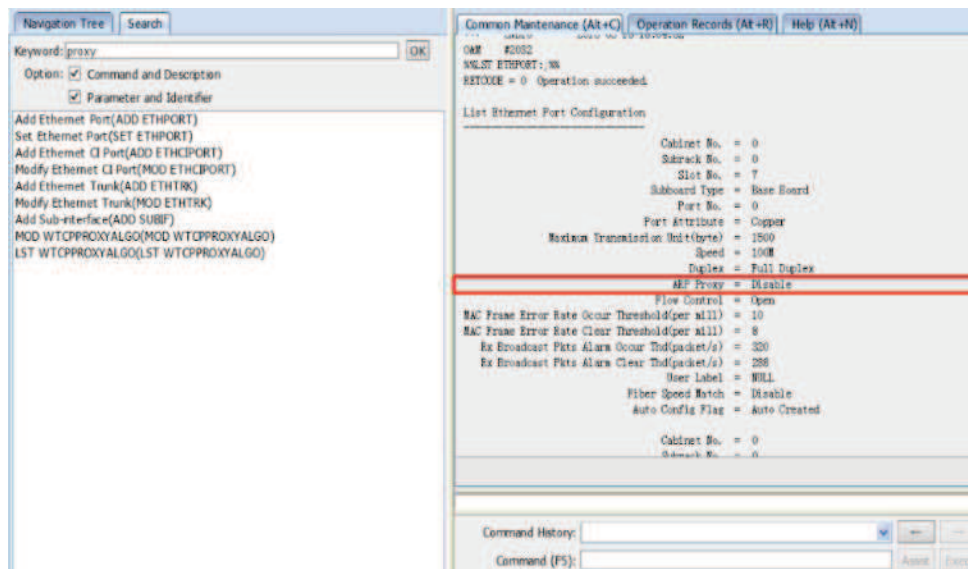


圖 5- 76 C 廠牌基站關閉 ARP Proxy 功能

資料來源：本團隊整理

1-12: 可移除裝置不可具備自動載入執行功能

測試案例	可移除裝置不可具備自動載入執行功能
參考資料	3GPP TS 33.117 Section 4.3.3.1.3
測試目的： 測試基站(eNodeB)不得在連接 CD、DVD 或者 USB-Storage 時，自動載入執行任何應用程式，在非特殊須用下應將其關閉。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)支援可移除式裝置(CD/DVD、USB 連接埠等)	
測試方法： 1. 測試人員登入基站(eNodeB)系統。 2. 測試人員在基站(eNodeB)上插入可移除式裝置。	
合格判定標準： 基站(eNodeB)不會從可移除裝置自動執行任何應用程式。	
測試說明：	

測試案例	可移除裝置不可具備自動載入執行功能
本測試 A 與 B 廠牌基站無外接介面，而 C 廠牌基站有提供 USB 介面。	

測試結果：

經在測試環境與 C 廠牌基站管理人員討論後表示雖有 USB 介面，但是插入基站後無法自動載入執行，因為所有要安裝進入到基站前都須經過完整性驗證，如下圖。

```
packcfg.sgn x
--iPSI SIGNFILE BEGIN--
ALGID - SHA256
--iPSI HASH SECTION BEGIN--
-D:/MBTS11.1/trunk/project/makepkg/output/mbts_LO/pkg/temp/SingleOM/Tool/MBTS/packcfg.xml--
a80ab75ba6030841854378e201ae22dae20731fba2022af8d015af7ff8b9822z
--iPSI HASH SECTION END--
--iPSI SIGNATURE BEGIN--
473d26599eeb432e98734ec8d73be294b952ac117984821d5b67a2adf345b562fb87dfe3aa7b6899985bbd09fef31c00e54ce7651a68
SIGN LENGTH - 128
--iPSI SIGNATURE END--
--iPSI SIGNFILE END--
```

圖 5- 77 C 廠牌基站之 SHA-256 完整性驗證

資料來源：本團隊整理

基站完成驗證後才會更新或載入軟體，並於下圖畫面上呈現狀態為 Success，確保基站的安全。

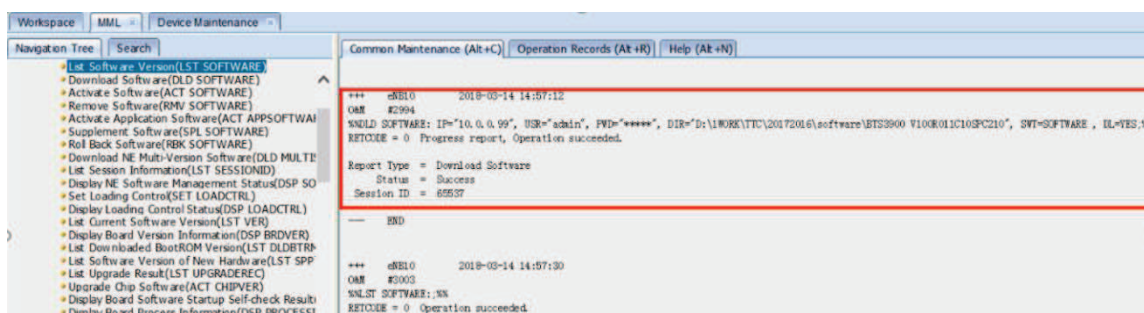


圖 5- 78 C 廠牌基站之軟體驗證與載入成功畫面

資料來源：本團隊整理

1-13. 網站伺服器非以系統權限執行

測試案例	網站伺服器非以系統權限執行
參考資料	3GPP TS 33.117 Section 4.3.4.2
測試目的： 測試網站伺服器的程序(processes)不應以系統權限執行，應為最低的一般權限執	

測試案例	網站伺服器非以系統權限執行
行。	
資訊安全需求：	
☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨測試環境暨初始條件：	
1. 測試人員取得需要的管理權限。 2. 基站(eNodeB)網站伺服器在運作的狀態下。	
測試方法：	
檢測網站伺服器的程序是否以系統權限執行。	
合格判定標準：	
檢測網站伺服器的程序未以系統權限執行。	
測試說明：	
本測試項目以製造基站的生命週期來看會偏在製造商之研發設計與測試階段，而非在產品上市後一般維運人員可接觸到的功能。	

測試結果：

以下圖 Windows Task Manager 舉例，在使用者名稱欄位代表這一個程序是以哪一種作業系統權限角色下去執行，例如：svchost.exe 這與核心相關則是由 SYSTEM(Local System)屬於系統權限執行。

名稱	PID	狀態	使用者名稱	CPU	記憶體 (私...)	描述
系統閒置處理程序	0	執行中	SYSTEM	90	8 K	處理器的閒置時間百分比
Taskmgr.exe	3560	執行中	ttc	04	30,852 K	工作管理員
dwm.exe	2308	執行中	DWM-7	02	80,956 K	桌面視窗管理員
explorer.exe	1344	執行中	ttc	02	68,048 K	Windows 檔案總管
系統掛鐘	-	執行中	SYSTEM	01	0 K	延遲程序呼叫與掛鐘服務常式
ctfmon.exe	5308	執行中	ttc	01	4,200 K	CTF 載入程式
chrome.exe	10920	執行中	ttc	00	12,636 K	Google Chrome
WINWORD.EXE	7556	執行中	ttc	00	325,716 K	Microsoft Word
csrss.exe	9992	執行中	SYSTEM	00	1,592 K	用戶端伺服器執行階段處理程序
System	4	執行中	SYSTEM	00	20 K	NT Kernel & System
vmware-authd.exe	4932	執行中	SYSTEM	00	3,128 K	VMware Authorization Service
atieclxx.exe	12144	執行中	SYSTEM	00	1,952 K	AMD External Events Client Module
svchost.exe	2556	執行中	SYSTEM	00	4,580 K	Windows Services 的主機處理程序
fontdrvhost.exe	4488	執行中	UMFD-7	00	4,748 K	Usermode Font Driver Host

圖 5- 79 Windows Task Manager

資料來源：本團隊整理

1-14. 未使用之 HTTP 功能應關閉

測試案例	未使用之 HTTP 功能應關閉
參考資料	3GPP TS 33.117 Section 4.3.4.3
測試目的： 一般標準網站伺服器需要 GET、HEAD、POST 功能。若仍有其他功能須增加，不建議將有漏洞的 TRACK 與 TRACE 納入。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)	
測試環境暨測試環境暨初始條件： 1. 測試人員擁有管理權限。 2. 網站伺服器在運作狀態。	
測試方法： 測試人員使用自動評估工具連線至基站(eNodeB)網站伺服器進行掃描。	
合格判定標準： 網站伺服器正確的完成設定，無未使用而開啟或開啟 TRACK 與 TRACE 功能。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，使用 HP WEBINSPECT 測試都為通過。	

測試結果：以下為 A 與 C 廠牌基站網站伺服器，使用 HP WEBINSPECT 測試都為通過。

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
10071	HTTP TRACK Method Cross-Site Scripting	Low	Yes	Pass	-
10069	HTTP TRACE Method Cross-Site Scripting	Low	Yes	Pass	-

圖 5- 80 A 廠牌基站 TRACK 與 TRACE 檢測

資料來源：本團隊整理

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
10071	HTTP TRACK Method Cross-Site Scripting	Low	Yes	Pass	-
10069	HTTP TRACE Method Cross-Site Scripting	Low	Yes	Pass	-

圖 5- 81 C 廠牌基站 TRACK 與 TRACE 檢測

資料來源：本團隊整理

1-15. 未存有不使用之附加元件

測試案例	未存有不使用之附加元件
參考資料	3GPP TS 33.117 Section 4.3.4.4
測試目的： 所有可用附加元件若不需要時應關閉，例如：WebDAV 或其他腳本元件。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨測試環境暨初始條件： 1. 基站(eNodeB)廠商提供系統運作所需的附加功能或者腳本工具一覽表。 2. 測試人員擁有特殊執行權限。 3. 網站伺服器在運作狀態。	
測試方法： 1. 測試人員透過檢測工具確認網站伺服器運作僅監聽特定需要之連接埠(80/443 port)，其餘元件已關閉不使用。 2. 檢測相關的系統設定符合需求。	
合格判定標準： 所有網站元件中不需要的附加元件或腳本已關閉和正確的完成設定。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，使用 HP WEBINSPECT 測試。	

測試結果：測試結果都為通過，並無相關未使用元件。

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
10823	Flash Misconfiguration: Policy Restrictions Bypass	Critical	Yes	Pass	-
10755	Flash Misconfiguration: ENABLEDEBUGGER Tag	High	Yes	Pass	-
10241	Flash Misconfiguration: Overly Permissive Cross-Domain Policy	Medium	Yes	Pass	-
10275	Web Server Misconfiguration: Open Proxy Access	Critical	Yes	Pass	-
10050	Web Server Misconfiguration: Account Information	Critical	Yes	Pass	-

圖 5- 82 C 未存有不使用之附加元件驗證

資料來源：本團隊整理

1-16. 無編譯器、直譯器或 shell 可使用

測試案例	無編譯器、直譯器或 shell 可使用
參考資料	3GPP TS 33.117 Section 4.3.4.5
測試目的： 如網站伺服器使用 CGI(Common Gateway Interface)或其他腳本功能，則 CGI 與相關目錄不能包含編譯器或直譯器，例如： PERL 程式語言直譯器、PHP 程式語言直譯器/編譯器、TCL 直譯器/編譯器或作業系統中介於核心(Kernel)與使用者操作介面之間的 Shell。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)	
測試環境暨測試環境暨初始條件： 1. 測試人員具有特殊權限。 2. 網站伺服器為運作狀態。	
測試方法： 測試人員檢測網站伺服器目錄中是否使用 CGI 或其他腳本工具(如 PERL、PHP 或者其他)的編譯器或直譯器(例如：PERL 直譯器、PHP 直譯器/編譯器、TCL 直譯器/編譯器或作業系統 shell)	
合格判定標準： 在網站伺服器中找到適當的系統設置和配置，確保所有不需要的附加腳本工具的編譯器/直譯器與 Shell 都未使用或已停用。	
測試說明： 本測試項目無法從基站找到可進行對 CGI 或其他腳本工具配置功能，以製造基站的生命週期來看會偏在製造商之研發設計與測試階段才可使用到的設定，例如有些基站使用 Linux 相關作業系統下，則可在 OS 模式下找到上述設定進行參數上的調整，但是產品開發完成後就僅會提供 Web 或應用程式介面的方式提供基站電信服務功能讓一般維運或管理人員操作使用。	

1-17. 不允許可利用 CGI 或其他腳本程式用以上傳資料

測試案例	不允許可利用 CGI 或其他腳本程式用以上傳資料
參考資料	3GPP TS 33.117 Section 4.3.4.6
測試目的： 網站伺服器不允許可利用 CGI 或其他腳本程式用以上傳資料。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)	
測試環境暨測試環境暨初始條件： 網站伺服器使用 CGI 或其他腳本程式語言工具。	
測試方法： 測試人員檢測網站伺服器上傳目錄是否與存放 CGI 或其他腳本程式之目錄分開，並且有寫入權限的控管。	
合格判定標準： 網站伺服器上傳目錄與存放 CGI 或其他腳本程式之目錄分開，並且有寫入權限的控管。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，使用 HP WEBINSPECT 測試。	

測試結果：下圖為 A 與 C 廠牌基站網站伺服器測試，使用 HP WEBINSPECT 測試都為通過，並無相關目錄可寫入之權限。

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
5362	Web Server Misconfiguration: Unprotected Directory	High	Yes	Pass	-
5290	Web Server Misconfiguration: Directory Listing	High	Yes	Pass	-
4909	Reget Directory Traversal	High	Yes	Pass	-
4818	NetCam Directory Traversal	High	Yes	Pass	-
4462	Directory Traversal	High	Yes	Pass	-
4271	Directory Traversal Web Server Access	High	Yes	Pass	-
3835	Sybase Power Dynamo Directory Traversal	High	Yes	Pass	-

圖 5- 83 A 與 C 廠牌基站之網站目錄存取限制檢測

資料來源：本團隊整理

1-18. 網站伺服器內嵌腳本語言不得可執行系統指令

測試案例	網站伺服器內嵌腳本語言不得可執行系統指令
參考資料	3GPP TS 33.117 Section 4.3.4.7
測試目的： 當網站伺服器內嵌腳本語言(Server Side Includes)是啟動，則要確保不得可執行系統指令。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨測試環境暨初始條件： 網站伺服器內嵌腳本語言(Server Side Includes)是啟動	
測試方法： 測試人員將網頁伺服器設定內之執行系統指令的功能關閉。	
合格判定標準： 測試人員檢視在設定檔中出現 Includes NOEXEC(APACHE)或者 ssiExecDisable(IIS)被設定之訊息。	
測試說明： 本測試項目無法從基站找到可檢視在設定檔中出現 Includes NOEXEC(APACHE)或者 ssiExecDisable(IIS)被設定之訊息，這應為基站研發設計與測試階段才可使用到的設定，例如有些基站使用 Linux 相關作業系統下，則可在 OS 模式下找到上述設	

測試案例	網站伺服器內嵌腳本語言不得可執行系統指令
定進行參數上的調整，但是產品開發完成後就僅會提供 Web 或應用程式介面的方式提供基站電信服務功能讓一般維運或管理人員操作使用。	

1-19. 網站伺服器存取權限

測試案例	網站伺服器存取權限
參考資料	3GPP TS 33.117 Section 4.3.4.8
測試目的： 網站伺服器設定檔之存取權限應僅限於 Web 伺服器的特定程序或具備系統特殊權限的使用者才能存取。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 測試人員具備特殊權限。 2. 網站伺服器正常運作。	
測試方法： 1. 測試人員檢視網站伺服器設定檔權限情況。 2. 測試人員檢視相關系統參數設定是否可符合測試目的要求。	
合格判定標準： 網站伺服器之系統設定檔存取權限已被正確的設定	
測試說明： 本測試項目無法從基站找網站伺服器之系統設定檔，亦也無法找到對應的功能可設定其存取權限。這應為基站研發設計與測試階段才可使用到的設定，例如有些基站使用 Linux 相關作業系統下，則可在 OS 模式下找到上述設定進行參數上的調整，但是產品開發完成後就僅會提供 Web 或應用程式介面的方式提供基站電信服務功能讓一般維運或管理人員操作使用。	

1-20. 不得存有網站伺服器相關預設文件檔

測試案例	不得存有網站伺服器相關預設文件檔
參考資料	3GPP TS 33.117 Section 4.3.4.9
測試目的： 網站伺服器安裝設定完成後，可能存有 Help 檔案、說明檔等預設檔案，而這些檔案應該移除，減少網站資訊暴露。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨測試環境暨初始條件： 1. 測試人員具備特殊權限。 2. 網站伺服器正常運作。	
測試方法： 測試人員移除所有在安裝時所產生的預設文件(範例、help 檔案、文件等)。	
合格判定標準： 測試人員檢視所有在安裝時所產生的預設文件(範例、help 檔案、文件等)已移除。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，其中 C 廠牌基站透過 WebInspect 檢測出存有可被挖掘出.gz 副檔名文件。	

測試結果：

如下圖這一般是 Web 備份檔案，如果遭受存取下載可能會被揭露網站伺服器相關設定參數、版本等，造成容易被攻擊的風險。

High

Web Server Misconfiguration: Unprotected File

Summary:

Webinspect has detected an archive file with the .gz extension on the target server. The severity of the threats posed by the web-accessible backup files depends on the sensitivity of the information stored in original document. Based on that information, an attacker can gain sensitive information about the site architecture, database and network access credential details, encryption keys, and so forth from these files. The attacker can use information obtained to craft precise targeted attacks, which may not otherwise be feasible, against the application.

Execution:

Browse to <https://10.0.0.86:443/jse/core/dom.js.gz> and inspect the content. Response should be a return with HTTP status code 200 and should not match target site's file not found response.

Report Date: 3/19/2018

FORTIFY

圖 5- 84 C 廠牌基站網站伺服器設定問題： Unprotected File

資料來源：本團隊整理

下圖是被挖掘出的.gz 檔案一覽。

- File Names:
- <https://10.0.0.86:443/jse/core/dom.js.gz>
 - <https://10.0.0.86:443/jse/xui/xui.js.gz>
 - <https://10.0.0.86:443/platform/lmtlib/lmtutil.js.gz>
 - <https://10.0.0.86:443/login.html.gz>
 - <https://10.0.0.86:443/jse/binaryproperty.js.gz>
 - <https://10.0.0.86:443/jse/core/container.js.gz>
 - <https://10.0.0.86:443/jse/base/util.js.gz>
 - <https://10.0.0.86:443/jse/jse.js.gz>
 - <https://10.0.0.86:443/jse/base/xpath.js.gz>
 - <https://10.0.0.86:443/config/config.js.gz>
 - <https://10.0.0.86:443/jse/base/eventqueue.js.gz>
 - <https://10.0.0.86:443/jse/conf.js.gz>
 - <https://10.0.0.86:443/jse/base/ajax.js.gz>

圖 5- 85 C 廠牌基站網站伺服器.gz 檔案一覽

資料來源：本團隊整理

1-21. 不得瀏覽目錄資料夾列表

測試案例	不得瀏覽目錄資料夾列表
參考資料	3GPP TS 33.117 Section 4.3.4.10
測試目的： 網站伺服器應關閉目錄列表或目錄瀏覽的功能。	
資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☐可用性(Availability)	

測試案例	不得瀏覽目錄資料夾列表
測試環境暨測試環境暨初始條件： 1. 測試人員具有管理者特殊權限。 2. 網站伺服器正常運作。	
測試方法： 測試人員使用檢測工具搜尋網站伺服器是否存有可被目錄列表或目錄瀏覽。	
合格判定標準： 網站伺服器已關閉目錄列表或目錄瀏覽的功能。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試。	

測試結果：如下圖測試結果網站伺服器已關閉目錄列表或目錄瀏覽的功能。

Vuln ID	Check Name	Severity	Enabled	Passed	Vuln Urls
5352	SD Server Directory Traversal	Critical	Yes	Pass	-
5188	Directory Traversal	Critical	Yes	Pass	-
4909	Reget Directory Traversal	High	Yes	Pass	-
4818	NetCam Directory Traversal	High	Yes	Pass	-
4781	SAP DB Web-Tools Directory Traversal	High	Yes	Pass	-
4271	Directory Traversal Web Server Access	High	Yes	Pass	-
3868	Path Manipulation: Absolute Path Traversal	High	Yes	Pass	-
3835	Sybase Power Dynamo Directory Traversal	High	Yes	Pass	-
3468	Northern Solutions WebMan Webserver Directory Traversal File Access	High	Yes	Pass	-
3323	PCI Netsupport Manager Directory Traversal File Access	High	Yes	Pass	-
1960	Path Manipulation: Absolute Path Traversal	High	Yes	Pass	-
3840	Enceladus Directory Traversal File Access	Medium	Yes	Pass	-

圖 5- 86 A 與 C 基站 Directory Traversal 掃描結果

資料來源：本團隊整理

1-22. HTTP 表頭不得揭露出網站伺服器資訊

測試案例	HTTP 表頭不得揭露出網站伺服器資訊
參考資料	3GPP TS 33.117 Section 4.3.4.11
測試目的： HTTP 表頭(Header)內之網站伺服器資訊應該最簡化設計。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☐可用性(Availability)	
測試環境暨測試環境暨初始條件： 1. 測試人員具有管理者特殊權限。 2. 網站伺服器正常運作。	
測試方法： 檢測 HTTP 表頭內不應包含關於網站伺服器或附加功能相關資訊。	
合格判定標準： 1. 檢測 HTTP 表頭內未包含關於網站伺服器或附加功能相關資訊。 2. 測試畫面截圖。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，試結果顯示 A 廠牌基站網站伺服器存有 CWE-79 弱點。 在 SANS TOP 25 稱為 XSS, (Cross-site Scripting)攻擊，該網站伺服器於回應時揭露 Content-type：image/jpeg，攻擊者可能可以建立惡意 Flash (SWF) 檔案，將附檔名更換為 JPG 並上傳至網站伺服器，或者使用網路上例如：FakeImageExploiter 將圖檔³⁰⁷內嵌入可執行檔，這時網站伺服器已經成為一個具有資安漏洞的網站，進而等候當企業內部網路有操作人員瀏覽到特定網頁時後將會被植入惡意程式，並將相關資訊回傳給攻擊者。	

測試結果：下圖測試結果顯示 A 廠牌基站網站伺服器存有 CWE-79 弱點，C 廠牌基站並沒有

³⁰⁷ FakeImageExploiter, [Online]. Available: <https://github.com/r00t-3xp10it/FakeImageExploiter>

CWE: 79

Kingdom: Environment

Page: https://192.168.170.42:443/images/nsn_logo.jpg

Request:

```
GET /images/nsn_logo.jpg HTTP/1.1
Accept: */*
Referer: https://192.168.170.42/protected/index.cgi
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; Trident/4.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E)
Host: 192.168.170.42
Connection: Keep-Alive
Pragma: no-cache
Cookie: CustomCookie=WebInspect130381ZXC2D6926C48034330B4F2888C462D1CA0Y840B
```

Response:

```
HTTP/1.1 200 OK
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Frame-Options: sameorigin
Cache-Control: no-cache
Pragma: no-store
Content-Type: image/jpeg
Accept-Ranges: bytes
ETag: "658190923"
Last-Modi...TRUNCATED...
```

圖 5- 87 A 基站網站存有 CWE-79 弱點

資料來源：本團隊整理

1-23. 錯誤頁面包含網頁伺服器資訊

測試案例	錯誤頁面包含網頁伺服器資訊
參考資料	3GPP TS 33.117 Section 4.3.4.12
測試目的： 網站伺服器的錯誤訊息不應直接顯露出內部資訊，例如：內部伺服器名稱、錯誤代號等，應改轉導往由廠商自行設計開發的錯誤頁面取代。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 測試人員具有管理者特殊權限。 2. 網站伺服器正常運作。	
測試方法： 測試人員檢測錯誤訊息與頁面不應出現網站伺服器的資訊。	

測試案例	錯誤頁面包含網頁伺服器資訊
合格判定標準：	
1. 測錯誤訊息與頁面未出現網站伺服器的資訊 2. 測試畫面截圖。	
測試說明：	
本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試。	

測試結果：

下圖測試結果顯示 A 廠牌基站網站伺服器存有 Poor Error Handling：Server Error Message 問題，C 廠牌基站並沒有 500 以上顯示之伺服器錯誤，係指伺服器在處理某個正確請求時發生錯誤，回應錯誤訊息本身不危險，但需要留意的是可能會讓攻擊者掌握應用程式如何處理這些錯誤條件的設計概念，進而修改開發可以透過遠端攻擊的工具對網站伺服器造成影響。從資安的角度上，應用程式開發與管理人員都應該盡可能減少，應該設計統一的錯誤頁面做為顯示，減少攻擊者對相關資訊的蒐集管道。

Poor Error Handling: Server Error Message (10932)

View Description

CWE: 388,497,200

Kingdom: Environment,Errors

Page: https://192.168.170.42:443/<script>alert('TRACK');</script>

Request:

TRACK /<script>alert('TRACK');</script> HTTP/1.1

Referer: https://192.168.170.42/protected/

Accept: */*

Pragma: no-cache

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0

Host: 192.168.170.42

Connection: Keep-Alive

X-WIPP: AscVersion=10.30.507.10

X-Scan-Memo: Category="Audit.Attack";

SID="08685BF536D896003343FE2401946ABD";

PSID="E0A13761BB4BC3BD9C389CF0F0390E4A"; SessionType="AuditAttack";

CrawlType="None"; AttackType="Search"; OriginatingEngineID="65cee7d3-561f-40dc-b5eb-c0b8c2383fcb"; AttackSequence="0"; AttackParamDesc="";

AttackParamIndex="0"; AttackParamSubIndex="0"; CheckId="5152";

Engine="Request+Modify"; Retry="False"; SmartMode="NonServerSpecificOnly";

ThreadId="121"; ThreadType="Task";

X-RequestManager-Memo: StateID="45"; sc="1"; ID="6425f525-fef5-4177-bf6c-8febb04c555d";

X-Request-Memo: ID="1754580b-6048-4426-bca8-1a549144f476"; sc="1";

ThreadId="128";

Cookie: CustomCookie=WebInspect130381ZXC2D6926C48034330B4F2888C462D1CA0Y840B

Response:

HTTP/1.0 501 Not Implemented

Content-Type: text/html

Content...TRUNCATED...

圖 5- 88 A 基站網站存有 Server Error Message 問題

資料來源：本團隊整理

1-24. 最小化檔案關聯

測試案例	最小化檔案關聯
參考資料	3GPP TS 33.117 Section 4.3.4.13
測試目的： 網站伺服器未使用之檔案或腳本關聯應被刪除，如：php、phhtml、js、sh、csh、bin、exe、pl、vbe 或 vbs。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☐可用性(Availability)	

445

測試案例	最小化檔案關聯
測試環境暨初始條件： 1. 測試人員具有管理者特殊權限。 2. 網站伺服器正常運作。	
測試方法： 測試人員檢測所有用不到的檔案或腳本關聯。	
合格判定標準： 1. 檢測所有用不到的檔案或腳本關聯。 2. 測試畫面截圖。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，但在現有的操作介面上無法檢測檔案或腳本關聯之功能，這需要進入到作業系統層級的操作環境才可以進行檢測上述設定與關聯。	

1-25. 限制檔案存取

測試案例	限制檔案存取
參考資料	3GPP TS 33.117 Section 4.3.4.14
測試目的： 應於網站伺服器目錄中，限制直接或間接存取檔案(如：透過連結或虛擬目錄)，避免網站伺服器存取所有檔案	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供文件設定網站伺服器。	
測試方法： 1. 測試人員驗證網站伺服器，其目錄或檔案存取權限是否可被網站伺服器以外之使用者帳號寫入。 2. 測試人員執行網站測試時使用非特殊權限帳號身分。	

測試案例	限制檔案存取
3. 如作業系統有 chrooted 環境下，測試人員在 chrooted 環境下執行測試。	
合格判定標準： 1. 未有特殊權限執行網站伺服器時無法直接或間接存取檔案。 2. 若有 chrooted 環境則顯示設定內容與截圖。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，但在現有的操作介面上無法檢測是否運行 chrooted 環境，且這需要進入到作業系統層級的操作環境才可以進行檢測。	

1-26. CGI 或腳本語言應限定於特定目錄有執行權限

測試案例	CGI 或腳本語言應限定於特定目錄有執行權限
參考資料	3GPP TS 33.117 Section 4.3.4.15
測試目的： 若 CGI 或者其他腳本運作中，應限定於特定目錄有執行權限，其他目錄應不能被執行。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 網站伺服器啟用 CGI 或腳本工具。	
測試方法： 測試人員檢測是否網頁伺服器僅擁有 CGI 或腳本工具目錄下的執行權限。	
合格判定標準： 1. 在部分設定檔案或螢幕截圖，顯示 CGI 或腳本語言可執行權限的目錄 2. 在部分設定檔案或螢幕截圖，顯示非 CGI 或腳本語言不可執行權限的目錄	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試，但在現有的操作介面上無法檢測 CGI 或腳本工具目錄的執行權限，且這需要進入到作業系統層級的操作	

測試案例	CGI 或腳本語言應限定於特定目錄有執行權限
環境才可以進行檢測。	

1-27. 流量分配

測試案例	流量分配
參考資料	3GPP TS 33.117 Section 4.3.5.1
測試目的： 基站(eNodeB)應支援實體或邏輯上可針對 O&M 與 control plane 流量分配。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 如果基站(eNodeB)用於處理 O&M 與 control plane，則適用此測試。 2. 網路基站(eNodeB)至少有一網路介面，提供 O&M 另一網路介面提供 control plane。	
測試方法： 測試人員操作基站(eNodeB)網路配置介面，設定用於處理 O&M 與 control plane 之介面。	
合格判定標準： 基站(eNodeB)可支援設定用於處理 O&M 與 control plane 之介面。	
測試說明： 檢測 A 廠牌及 C 廠牌的流量分配功能。	

測試結果：

下圖是 A 廠牌基站可透過 VLAN 技術將 User Plane 與 Control Plance 分別設定於不同介面上來達到流量分開。

圖 5- 89 A 基站廠商之 User & Control Plane

資料來源：本團隊整理

下圖是 C 廠牌基站一樣透過 VLAN 技術將 User Data 獨立分切出來。

圖 5- 90 C 廠牌基站之 User Data 設定

資料來源：本團隊整理

1-28: 動態內容不斷增長之處理機制

測試案例	動態內容不斷增長之處理機制
參考資料	3GPP TS 33.117 Section 4.2.4.1.1.1
測試目的： 基站(eNodeB)應具備對於擴增或動態內容，例如：日誌檔案或上傳檔案等，當達到最大可允許容量空間時，仍不會影響系統功能，並提供相關措施可進行監控與設定等。 資訊安全需求： ☐機密性(Confidentiality) ☐完整性(Integrity) ☒可用性(Availability)	

測試案例	動態內容不斷增長之處理機制
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供日誌檔案或上傳檔案的儲存路徑文件。 2. 基站(eNodeB)廠商提供當儲存容量不足之對應措施文件。	
測試方法： 1. 測試人員啟用監控系統功能。 2. 測試人員增加日誌檔案數量，並監控系統，持續直到日誌檔案超出系統可儲存空間容量。 3. 如果基站(eNodeB)允許檔案上傳，例如：使用 SFTP，測試人員上傳檔案直到超出系統可儲存空間容量。	
合格判定標準： 當日誌檔案或上傳檔案超出系統可儲存之空間，系統具備相關主動式提醒訊息，或者可透過監控介面掌握系統儲存空間現況。	
測試說明： 根據測試環境之管理人員表示 A、B、C 廠牌基站對當儲存空間不足時會於操作介面的日誌顯示區域上主動提醒，但並無相關技術文件可瞭解使用空間容量多大。 另外這三種廠牌基站都支援將日誌檔案傳輸至其他管理設備集中保存，可避免影響系統持續性的紀錄警報與事件。	

2. 通訊協定檢測

針對基站通訊傳輸的安全進行檢測。

2-1. 資料與資訊的傳輸防護

測試案例	資料與資訊的傳輸防護
參考資料	3GPP TS 33.117 Section 4.2.3.2.4
測試目的： 基站(eNodeB)與外部設備之網路傳輸須加密保護，且不應使用被公開認定之弱加密技術。	
資訊安全需求：	

測試案例	資料與資訊的傳輸防護
☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商應在所提供之文件中包含 OAM 協定相關資訊。	
測試方法： 在 OAM 伺服器間建立安全通道，並檢視安全協定與加密方式是否符合安全要求，螢幕截圖記錄。	
合格判定標準： 連線的過程是受保護的，且未使用不安全的連線模式。	
測試說明： OAM 伺服器一般是基站的網管系統，本次測試場域環境管理人員表示僅有 B 廠牌基站有購買網管系統，但是與 OAM 之間的傳輸並未使用加密技術。	

測試結果：如下圖。

129 6.631752	192.168.170.65	10.101.136.83	TCP	66 80 → 56777 [SYN, ACK] Seq=0 Ack=1 Win=32768 Len=0 MS
130 6.631824	10.101.136.83	192.168.170.65	TCP	54 56777 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0
131 6.632159	10.101.136.83	192.168.170.65	HTTP	225 GET /em/rbsemconfig.xml HTTP/1.1
132 6.646213	192.168.170.65	10.101.136.83	TCP	260 80 → 56777 [PSH, ACK] Seq=1 Ack=172 Win=33580 Len=26
133 6.646214	192.168.170.65	10.101.136.83	TCP	1294 80 → 56777 [ACK] Seq=207 Ack=172 Win=33580 Len=1248

User-Agent: Java/1.6.0_25\r\n	
Host: 192.168.170.65\r\n	
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2\r\n	
Connection: keep-alive\r\n	
\r\n	
[Full request URI: http://192.168.170.65/em/rbsemconfig.xml]	
[HTTP request 1/1]	

0000	02 20 c5 40 d2 c4 34 02	86 7c b9 6a 08 00 45 00	c .@..4. .].j..f.
0010	00 d3 54 93 40 00 80 06	a7 ef 0a 65 88 53 c0 a0	..T.β... ..e.S..
0020	aa 41 dd c9 00 50 04 b4	03 e5 64 ef cd a3 50 18	.A...P... ..d...P.
0030	40 29 b1 cf 00 00 47 45	54 20 2f 65 6d 2f 72 62	@)....GE T /em/rb
0040	73 65 6d 63 6f 6e 66 69	67 2e 78 6d 6c 20 48 54	semconfig.xml HT
0050	54 50 2f 31 2e 31 0d 0a	55 73 65 72 2d 41 67 65	IP/1.1.. User-Age
0060	6e 74 3a 20 4a 61 76 61	2f 31 2e 36 2e 30 5f 32	nt: Java /1.6.0.2
0070	35 0d 0a 48 6f 73 74 3a	20 31 39 32 2e 31 36 38	s..Host: 192.168
0080	2e 31 37 30 2e 36 35 0d	0a 41 63 63 65 70 74 3a	.170.65..Accept:
0090	20 74 65 78 74 2f 68 74	6d 6c 2c 20 69 6d 61 67	.text/html, imag
00a0	65 2f 67 69 66 2c 20 69	6d 61 67 65 2f 6a 70 65	e/gif, i mage/jpe

圖 5- 91 B 廠牌基站之 User Date 設定

資料來源：本團隊整理

2-2. ICMP 封包處理

測試案例	ICMP 封包處理
參考資料	3GPP TS 33.117 Section 4.2.4.1.1.2

測試案例	ICMP 封包處理
測試目的： 基站(eNodeB)不需處理 ICMPv4 和 ICMPv6 封包，因 ICMP4 和 ICMPv6 在大多數網路中可以不須使用，但可能存有風險。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)有支援 IPv4、IPv6。 2. 測試人員須具備必要的權限，用於確認 ICMP 訊息是否在傳送過程被基站(eNodeB)過濾排除。	
測試方法： 1. 測試人員架設可發送 ICMP 封包訊息之設備，用來測試基站(eNodeB)是否具備可過濾排除 ICMP 封包之功能。 2. 測試人員確認基站(eNodeB)本身具備例如：防火牆規則等功能，用以過濾排除 ICMP 封包訊息。 3. 測試人員確認當基站(eNodeB)進行過濾排除 ICMP 封包時，不影響系統本身設定。	
合格判定標準： 基站(eNodeB)對於 ICMP 封包訊息不予回應，確實進行過濾排除。	
測試說明： 本測試 A、B、C 廠牌基站在測試場域的管人員表示並無這種用於網通產品，例如：路由器、交換器等設備上具備的功能。	

2-3. HTTPS

測試案例	HTTPS
參考資料	3GPP TS 33.117 Section 4.2.5.1
測試目的： 用戶端與網站伺服器之間的通訊應使用 TLS 進行。	
資訊安全需求：	

測試案例	HTTPS
☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商應在所提供之文件中包含 TLS 協定相關資訊。	
測試方法： 檢視 TLS 安全協定與加密方式是否符合安全要求，螢幕截圖記錄。	
合格判定標準： 連線的過程是受保護的，且未使用不安全的連線模式。	
測試說明： 本測試項目僅有 A 與 C 廠牌基站具有網站伺服器可測試。	

測試結果：

下圖為 A 廠牌基站的測試確認連線的過程使用 TLS 1.2 技術保護。

No.	Time	Source	Destination	Protocol	Length	Info
331	14.999639	10.101.136.83	192.168.170.42	TLSv1.2	246	Client Hello
336	15.019030	192.168.170.42	10.101.136.83	TLSv1.2	83	Server Hello, Certificate, Server Key Exchange, Server Hello Done
338	15.028529	10.101.136.83	192.168.170.42	TLSv1.2	244	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
339	15.029807	192.168.170.42	10.101.136.83	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
341	15.032730	10.101.136.83	192.168.170.42	TLSv1.2	596	Application Data
361	16.403842	192.168.170.42	10.101.136.83	TLSv1.2	512	Application Data, Encrypted Alert

> Frame 336: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0
 > Ethernet II, Src: MS-WLB-PhysServer-32_c5:40:d2:c4 (02:20:c5:40:d2:c4), Dst: IntelCor_7c:b9:6a (34:02:86:7c:b9:6a)
 > Internet Protocol Version 4, Src: 192.168.170.42, Dst: 10.101.136.83
 > Transmission Control Protocol, Src Port: 443, Dst Port: 55600, Seq: 2701, Ack: 193, Len: 29
 > [4 Reassembled TCP Segments (2729 bytes): #333(1240), #334(220), #335(1240), #336(29)]
 v Secure Sockets Layer
 v TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 2724
 v Handshake Protocol: Server Hello

圖 5- 92 A 廠牌基站之 TLS 加密

資料來源：本團隊整理

下圖為 C 廠牌基站的測試確認連線的過程同樣使用 TLS 1.2 技術保護。

No.	Time	Source	Destination	Protocol	Length	Info
49	9.387495	10.0.0.76	10.0.0.99	TLSv1.2	231	Server Hello, Change Cipher Spec, Encrypted Handshake Message
50	9.387605	10.0.0.99	10.0.0.76	TCP	54	63960 → 443 [ACK] Seq=197 Ack=178 Win=64063 Len=0
51	9.387889	10.0.0.99	10.0.0.76	TLSv1.2	145	Change Cipher Spec, Encrypted Handshake Message
52	9.389855	10.0.0.99	10.0.0.76	TLSv1.2	715	Application Data
53	9.427150	10.0.0.99	10.0.0.76	TLSv1.2	379	Application Data
54	9.427248	10.0.0.99	10.0.0.76	TCP	54	63960 → 443 [ACK] Seq=949 Ack=503 Win=63738 Len=0
55	9.447017	10.0.0.76	10.0.0.99	TCP	1514	443 → 63960 [ACK] Seq=503 Ack=949 Win=8192 Len=1460 [TCP segment of a reassembled PDU]

> Frame 49: 231 bytes on wire (1848 bits), 231 bytes captured (1848 bits) on interface 0
 > Ethernet II, Src: HuaweiTe_ae:93:31 (4c:f9:5d:ae:93:31), Dst: HewlettP_84:33:61 (fc:3f:db:84:33:61)
 > Internet Protocol Version 4, Src: 10.0.0.76, Dst: 10.0.0.99
 > Transmission Control Protocol, Src Port: 443, Dst Port: 63960, Seq: 1, Ack: 197, Len: 177

▼ Secure Sockets Layer

▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 81

▼ Handshake Protocol: Server Hello
 Handshake Type: Server Hello (2)
 Length: 77
 Version: TLS 1.2 (0x0303)
 > Random: 5aa92fc30b7c0f76becd36f1d93015a899cd87956f1eb087...
 Session ID Length: 32
 Session ID: 7fbac45b9699d23b556953c35168f1c51d1810184a914482...
 Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
 Compression Method: null (0)
 Extensions Length: 5
 > Extension: renegotiation_info (len=1)

▼ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec
 Content Type: Change Cipher Spec (20)
 Version: TLS 1.2 (0x0303)
 Length: 1

圖 5- 93 C 廠牌基站之 TLS 加密

資料來源：本團隊整理

3. 弱點分析

針對基站啟用協定與服務、弱點漏洞等與軟體相關之檢測。

3-1. 系統使用之協定或服務安全

測試案例	系統使用之協定或服務安全
參考資料	3GPP TS 33.117 Section 4.3.2.1
測試目的： 基站(eNodeB)在預設條件下，僅能執行需要的協定或服務，業者維運時因實際任務需求，可將原本未啟用協定或服務予以暫時性啟用與適當管理。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☐可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商應提供系統預設已啟用協定與服務用途。	
測試方法： 1. 測試人員檢視文件所描述已使用之協定與服務用途。 2. 測試人員使用檢測工具對基站(eNodeB)進行掃描，逐一檢視掃描結果與文件描述是否有一致。	

測試案例	系統使用之協定或服務安全
合格判定標準：	
檢測工具掃描結果與基站(eNodeB)廠商提供之說明文件一致。	
測試說明：	
確認原本未啟用協定或服務予以暫時性啟用與適當管理。	

測試結果：

下圖為 A 廠牌基站測試結果，測試環境管理人員表示並無相關文件描述啟用那些協定與服務。

```
Starting Nmap 7.31 ( https://nmap.org ) at 2018-02-01 20:13 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try u
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.33% done; ETC: 20:14 (0:00:43 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.83% done; ETC: 20:15 (0:00:40 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.13% done; ETC: 20:15 (0:00:40 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 66.60% done; ETC: 20:15 (0:00:37 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.00% done; ETC: 20:15 (0:00:36 remaining)
Nmap scan report for 192.168.170.41
Host is up (0.0026s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
3300/tcp   open  ceph
6000/tcp   open  X11
6001/tcp   open  X11:1
12000/tcp  open  cce4x
MAC Address: 60:A8:FE:F9:8E:71
Nmap done: 1 IP address (1 host up) scanned in 273.72 seconds
```

圖 5- 94 A 廠牌基站之服務開啟結果

資料來源：本團隊整理

下圖為 B 廠牌基站測試結果，主要比較不合理的存有 Telenet 明文傳輸，以往許多物聯網產品資安事件都是透過暴力破解 Telnet 帳號密碼後再植入惡意程式，所以此服務建議應該關閉。另外使用在電子郵件相關之 SMTP、POP3、IMAP 則應非基站服務的內容，同樣應該關閉。


```

root@kali:~# nmap 192.168.170.66

Starting Nmap 7.31 ( https://nmap.org ) at 2018-01-31 22:24 EST
mass dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.170.66
Host is up (0.0024s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
990/tcp   open  ftps
993/tcp   open  imaps
995/tcp   open  pop3s
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8008/tcp  open  http
8010/tcp  open  xmpp
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 82.93 seconds

```

圖 5- 95 B 廠牌基站之服務開啟結果

資料來源：本團隊整理

下圖為 C 廠牌基站測試結果，初步觀察並無開啟特殊服務。

```

root@kali: ~
File Edit View Search Terminal Help

root@kali:~# nmap 10.0.0.86

Starting Nmap 7.31 ( https://nmap.org ) at 2018-03-19 03:23 EDT
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.44% done; ETC: 03:23 (0:00:09 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.64% done; ETC: 03:23 (0:00:09 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.68% done; ETC: 03:23 (0:00:09 remaining)
Nmap scan report for 10.0.0.86
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
6000/tcp   open  X11
6006/tcp   open  X11:6
6007/tcp   open  X11:7
MAC Address: 4C:F9:5D:AE:90:F9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 136.95 seconds
root@kali:~#

```

圖 5- 96 C 廠牌基站之服務開啟結果

資料來源：本團隊整理

3-2. 限制可使用之服務

測試案例	限制可使用之服務
參考資料	3GPP TS 33.117 Section 4.3.2.2
測試目的： 基站(eNodeB)應限制服務的可用性，使其只能使用在需要的介面上。 資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商應提供如何設定限制服務功能於特定需要介面上。 2. 基站(eNodeB)廠商應提供文件描述以開啟之服務與用途。 3. 測試人員具有管理權限。 4. 測試設備具有網路連接埠掃描功能。	
測試方法： 1. 測試人員設定特定服務於需要介面上。 2. 測試人員使用網路連接埠掃描工具對基站(eNodeB)進行掃描，確認該服務是否在所設定之特定介面上開啟與運作中。	
合格判定標準： 1. 測試人員確認該服務僅在所設定之特定介面上開啟運作中。 2. 螢幕截圖紀錄。	
測試說明： 本項目僅有 A 廠牌基站可測試。	

測試結果：

下圖是 A 廠牌基站可透過 VLAN 技術將 User Plane 設定於特別之介面。

圖 5- 97 A 廠牌基站 VLAN 與 User Plane

資料來源：本團隊整理

下圖是 A 廠牌基站可透過 VLAN 技術將 Control Plane 設定於特別之介面。

圖 5- 98 A 廠牌基站 VLAN 與 Control Plane

資料來源：本團隊整理

下圖是 A 廠牌基站可透過 VLAN 技術將 Management Plane 設定於特別之介面。

圖 5- 99 A 廠牌基站 VLAN 與 Management Plane

資料來源：本團隊整理

3-3. 未使用的軟體應予移除

測試案例	未使用的軟體應予移除
參考資料	3GPP TS 33.117 Section 4.3.2.3
測試目的： 基站(eNodeB)未使用的軟體元件或部分軟體，不得安裝或在安裝後應刪除。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☐可用性(Availability)	

測試案例	未使用的軟體應予移除
測試環境暨初始條件： 基站(eNodeB)廠商應提供已安裝的軟體、附加元件與相關元件的列表，包含以下資訊：軟體/附加元件名稱、軟體/附加元件安裝版本、相關的軟體與版本的列表、任何附加元件和功能、授權資訊、簡述其功用。	
測試方法： 1. 測試人員檢查系統中安裝軟體的名稱與版本資訊。 2. 測試人員根據基站(eNodeB)廠商提供已安裝軟體清單與檢測結果比對是否一致。	
合格判定標準： 1. 測試人員列印輸出檢查到之軟體清單，或者螢幕截圖方式記錄。 2. 測試人員檢查確認與基站(eNodeB)廠商提供已安裝軟體清單與檢測結果比對一致。	
測試說明： 本項測試三家基站廠牌都無法提供已安裝軟體清單。	

測試結果：

下圖為 A 基站廠商軟體清單部份摘錄。

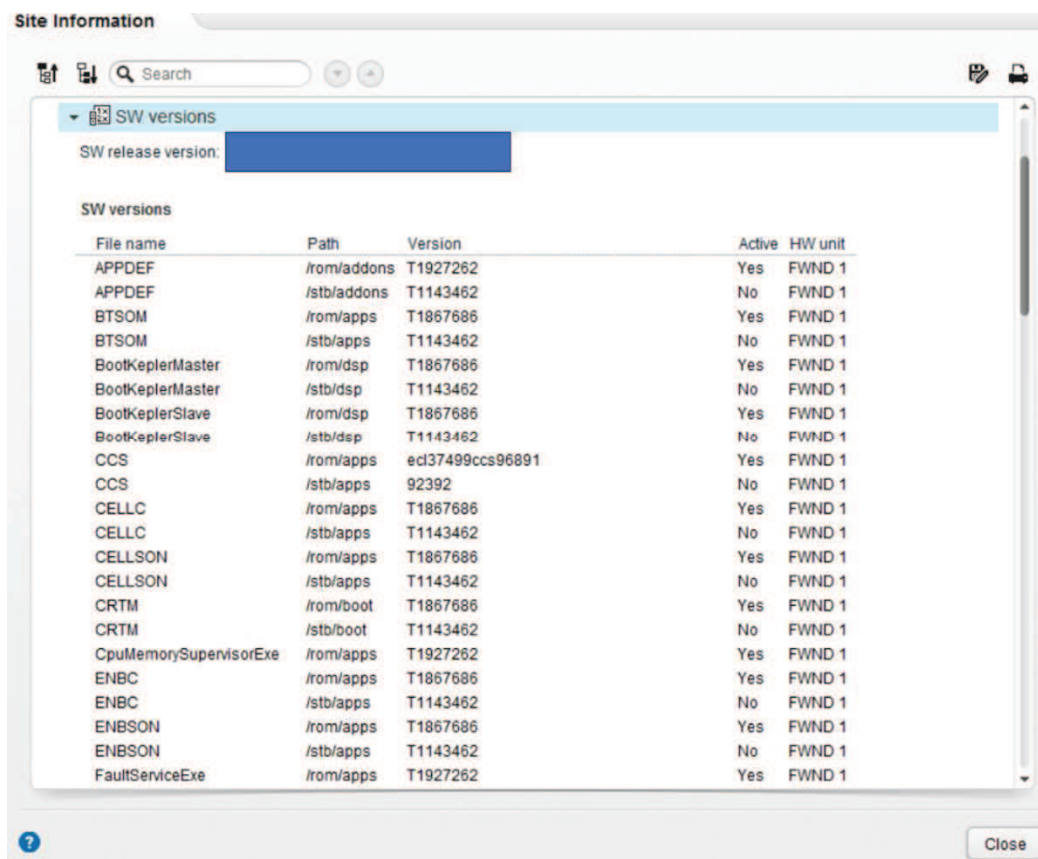


圖 5- 100 A 廠牌基站已安裝軟體清單

資料來源：本團隊整理

下圖為 B 基站廠商軟體版本相關內容摘錄，並無軟體清單，不同廠牌呈現的設計皆有不同。

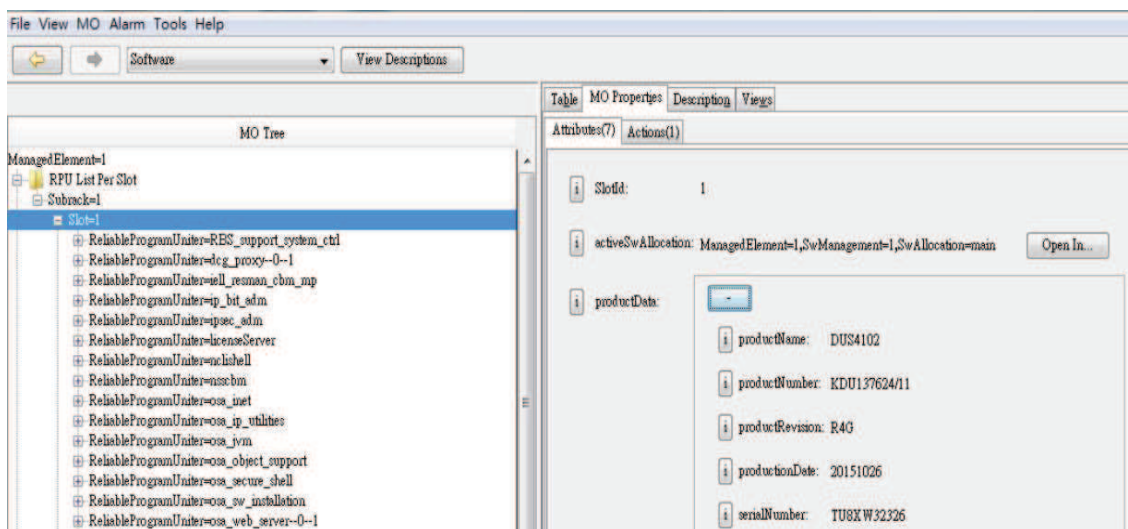


圖 5- 101 B 廠牌基站已安裝軟體清單

資料來源：本團隊整理

下圖為 C 基站廠商軟體版本相關內容摘錄，並無軟體清單。

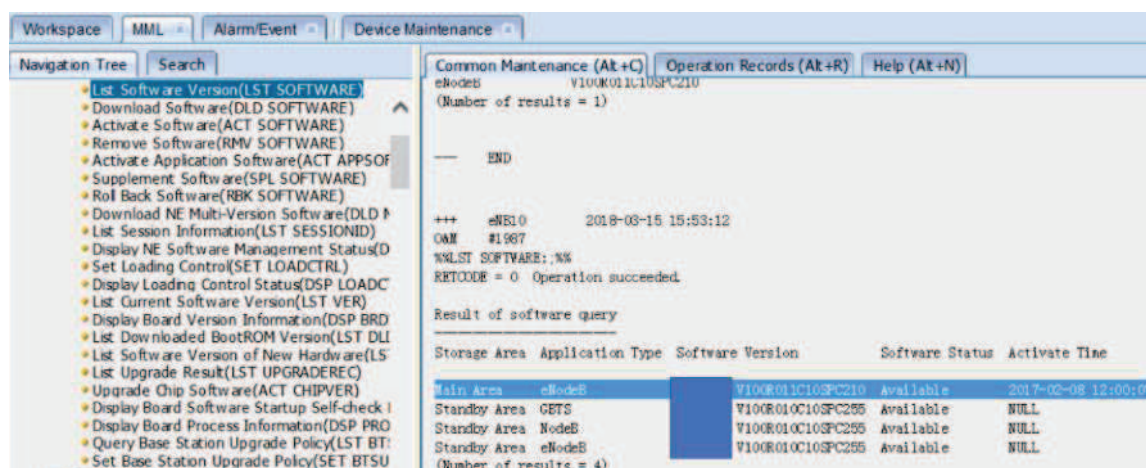


圖 5-102 C 廠牌基站已安裝軟體清單

資料來源：本團隊整理

3-4. 未使用之功能應予以關閉

測試案例	未使用之功能應予以關閉
參考資料	3GPP TS 33.117 Section 4.3.2.4
測試目的： 基站(eNodeB)正式上線使用前，如果未使用的軟體或硬體介面連接埠應進行刪除或停用該功能，並確保基站(eNodeB)重新啟動後仍維持停用的狀態。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商應提供已安裝使用之軟體名稱、版本、所有附加元件與功能、任何硬體介面連接埠、授權資訊之文件說明，及如何查閱上述這些軟硬體資訊之操作步驟。	
測試方法： 1. 測試人員根據文件操作指引識別已安裝在基站(eNodeB)上之軟體與硬體，確認那些已經被停用。 2. 測試人員根據基站(eNodeB)廠商提供之軟硬體文件清單，確認與檢測結果是否一致。	

測試案例	未使用之功能應予以關閉
合格判定標準： 基站(eNodeB)廠商提供之軟硬體文件清單與檢測結果一致。	
測試說明： 本項目測試三台廠牌基站之管理人員無法提供文件操作指引，與已安裝軟體清單協助檢測比對。	

3-5. 未安裝已不受支援之軟硬體元件

測試案例	未安裝已不受支援之軟硬體元件
參考資料	3GPP TS 33.117 Section 4.3.2.5
測試目的： 基站(eNodeB)不可安裝已不被供應商支援的軟體或硬體元件。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供已安裝所有軟硬體元件資訊，包含名稱、版本、任何附加的元件與功能說明、特殊的硬體或除錯連接埠、授權資訊，並提供支援說明。	
測試方法： 1. 測試人員審閱基站(eNodeB)廠商提供之關於硬體、軟體元件、版本資訊以及軟體提供的支援的說明。 2. 測試人員確認基站(eNodeB)廠商提供已安裝之硬體或軟體清單中，是否都在可支援的範圍。	
合格判定標準： 確認基站(eNodeB)廠商提供已安裝之硬體或軟體清單中，都在可支援的範圍。	
測試說明： 本項目測試三台廠牌基站之管理人員無法提供已安裝軟體支援說明，只是本測試項目以製造基站的生命週期來看會偏在製造商之研發設計與測試階段就應該確認使用的軟硬體元件是否供應商仍在支援的狀態下，而非在產品上市後一般維運人員可掌握的訊息。	

3-6. 緩衝區溢位防護

測試案例	緩衝區溢位防護
參考資料	3GPP TS 33.117 Section 4.3.3.1.5
測試目的： 基站(eNodeB)系統支援防止緩衝區溢位，基站(eNodeB)文件中應提供相關機制以及如何檢測其是否啟用。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☒可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供系統具支援緩衝區溢位防護機制，文件中應提供相關機制以及如何檢測其是否啟用。	
測試方法： 測試人員審查基站(eNodeB)廠商提供之文件，確認緩衝區溢位防護機制已經被實作在系統內，並詳細說明是否其機制已預設在系統中或者需要額外的執行其他動作(例如：手動腳本或指令)。	
合格判定標準： 測試人員呈現已經實作於基站(eNodeB)之緩衝區溢位防護機制。	
測試說明： 本項目測試三台廠牌基站之管理人員無法提供緩衝區溢位防護機制支援說明，本測試項目以製造基站的生命週期來看會偏在製造商之研發設計與測試階段就應該納入，目前在這三台廠牌基站的的操作介面僅針對 LTE 網路維運相關功能，並無這緩衝區溢位防護等設定性功能。	

3-7. 連接埠掃描

測試案例	連接埠掃描
參考資料	3GPP TS 33.117 Section 4.4.2
測試目的： 測試僅只有基站(eNodeB)廠商提供網路連接埠列表文件內所載之連接埠才可開啟與外部系統相連接。	

測試案例	連接埠掃描
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供網路連接埠列文件，並說明其功能與用途。	
測試方法： 1. 測試人員檢核網路連接埠列文件，並確認文件內所有項目與功能之合理性。 2. 測試人員使用掃描工具對基站(eNodeB)進行掃描，並確認結果是否與網路連接埠列文件一致。	
合格判定標準： 掃描工具結果與網路連接埠列文件一致。	
測試說明： 確認 A、B、C 廠牌設備是否達以上標準。	

測試結果：

下圖為 A 廠牌基站測試結果，測試環境管理人員表示並無相關文件描述啟用那些協定與服務。

```
Starting Nmap 7.31 ( https://nmap.org ) at 2018-02-01 20:13 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try u
Stats: 0:00:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 46.33% done; ETC: 20:14 (0:00:43 remaining)
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 56.83% done; ETC: 20:15 (0:00:40 remaining)
Stats: 0:00:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 57.13% done; ETC: 20:15 (0:00:40 remaining)
Stats: 0:01:14 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 66.60% done; ETC: 20:15 (0:00:37 remaining)
Stats: 0:01:15 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 67.00% done; ETC: 20:15 (0:00:36 remaining)
Nmap scan report for 192.168.170.41
Host is up (0.0026s latency).
Not shown: 994 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp    open  https
3300/tcp   open  ceph
6000/tcp   open  X11
6001/tcp   open  X11:1
12000/tcp  open  cce4x
MAC Address: 60:A8:FE:F9:8E:71
Nmap done: 1 IP address (1 host up) scanned in 273.72 seconds
```

圖 5- 103 A 廠牌基站之服務開啟結果

資料來源：本團隊整理

下圖為 B 廠牌基站測試結果，主要比較不合理的存有 Telenet 明文傳輸，以往許多物聯網產品資安事件都是透過暴力破解 Telnet 帳號密碼後再植入惡意程式，所以此服務建議應該關閉。另外使用在電子郵件相關之 SMTP、POP3、IMAP 則應非基站服務的內容，同樣應該關閉。

```
root@kali:~# nmap 192.168.170.66

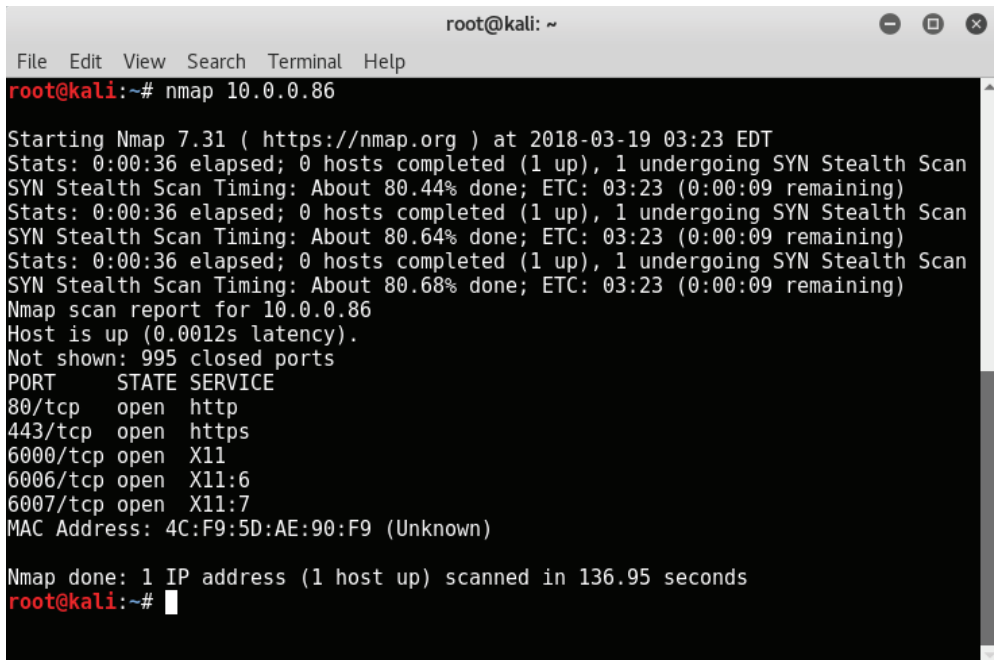
Starting Nmap 7.31 ( https://nmap.org ) at 2018-01-31 22:24 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.170.66
Host is up (0.0024s latency).
Not shown: 981 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
135/tcp   open  msrpc
143/tcp   open  imap
443/tcp   open  https
465/tcp   open  smtps
990/tcp   open  ftps
993/tcp   open  imaps
995/tcp   open  pop3s
2000/tcp  open  cisco-sccp
5060/tcp  open  sip
8008/tcp  open  http
8010/tcp  open  xmpp
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 82.93 seconds
```

圖 5- 104 B 廠牌基站之服務開啟結果

資料來源：本團隊整理

下圖為 C 廠牌基站測試結果，初步觀察並無開啟特殊服務。



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# nmap 10.0.0.86

Starting Nmap 7.31 ( https://nmap.org ) at 2018-03-19 03:23 EDT
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.44% done; ETC: 03:23 (0:00:09 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.64% done; ETC: 03:23 (0:00:09 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 80.68% done; ETC: 03:23 (0:00:09 remaining)
Nmap scan report for 10.0.0.86
Host is up (0.0012s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp    open  https
6000/tcp   open  X11
6006/tcp   open  X11:6
6007/tcp   open  X11:7
MAC Address: 4C:F9:5D:AE:90:F9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 136.95 seconds
root@kali:~#
```

圖 5-105 C 廠牌基站之服務開啟結果

資料來源：本團隊整理

3-8. 漏洞掃描

測試案例	漏洞掃描
參考資料	3GPP TS 33.117 Section 4.4.3
測試目的：	
基站(eNodeB)系統本身不應存在重大風險已知弱點漏洞。	
資訊安全需求：	
☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件：	
1. 提供 IP-based 協定。	
2. 測試人員具有特殊權限登入基站(eNodeB)，與存取基站(eNodeB)相關資源。	

測試案例	漏洞掃描
測試方法： 1. 測試人員使用漏洞掃描工具對基站(eNodeB)進行掃描。 2. 評估掃描結果的嚴重性，是否存在 CVSS v3 評分為 7 分以上之資安漏洞。	
合格判定標準： 掃描結果不存在 CVSS v3 評分為 7 分以上之資安漏洞。	
測試說明： 本項目測試僅有 C 廠牌基站掃描的結果存有中等風險之威脅。	

測試結果：

下圖測試結果表示不該啟動 IP Forwarding 功能，可能導入攻擊者 bypass 防火牆等安全設備。

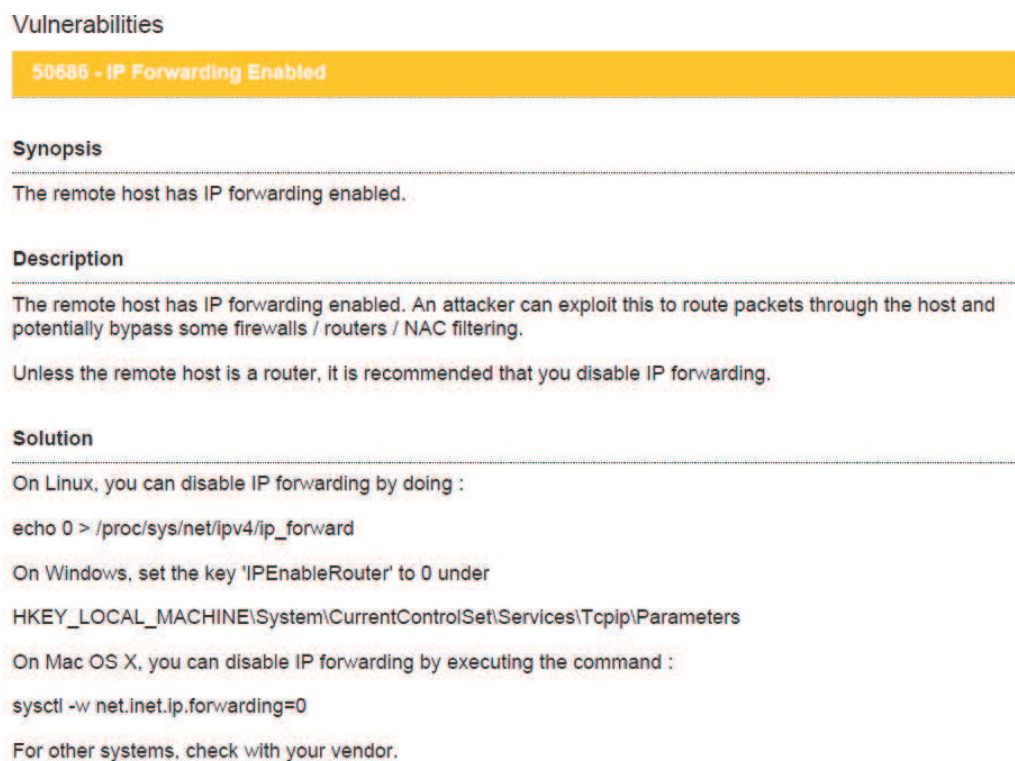


圖 5- 106 C 廠牌基站 IP Forwarding Enabled

資料來源：本團隊整理

下圖測試結果表示不該使用已存有弱點威脅的加密技術，以 SSL 2.0 而言因為 SSLv2 設計不當，導致存在安全威脅，包含：同一密鑰(Secret Key)用於訊息身分驗證

與加密、認證密文(Cipher)支援不安全的 MD5 雜湊值、可被利用修改 ClientHello 與 ServerHello 封包，導致中間人(Man In the Middle, 簡稱 MITM)攻擊。目前網頁伺服器(HTTPS)已不建議使用 SSLv2 協定³⁰⁸，避免遭破解金鑰交換加密演算法，以取得加密金鑰，進而還原加密封包，解析通訊內容。

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

圖 5- 107 C 廠牌基站 SSL 2.0/SSL 3.0

資料來源：本團隊整理

4. 存取控制

檢測基站的安全控制措施，帳號管控、授權管理、鑑別因子要求等安全控制功能。

4-1. 系統功能應該已驗證和授權下才得以使用

測試案例	系統功能應該已驗證和授權下才得以使用
參考資料	3GPP TS 33.117 Section 4.2.3.4.1.1

³⁰⁸ Transport Layer Protection Cheat Sheet, [Online]. Available:
https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet

測試案例	系統功能應該已驗證和授權下才得以使用
測試目的： 基站(eNodeB)系統之功能應在完成身分鑑別後才得以使用。系統功能包含網路服務(例如：SSH、SFTP)或透過管理介面使用本機端的存取等。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供系統性功能清單，包含網路服務、作業系統或應用程式之本機端存取。 2. 基站(eNodeB)廠商提供可存取系統功能的所有登入方式。	
測試方法： 1. 測試人員根據經驗評估基站(eNodeB)廠商提供之系統功能清單是否足夠完整。 2. 測試人員根據基站(eNodeB)廠商提供之可登入方式，比較在完成與未完成登入系統與驗證，測試兩種方式對存取系統功能的差異。	
合格判定標準： 未完成登入與驗證，測試人員無法存取系統功能。	
測試說明： 本項目測試三台廠牌基站都需經過網頁或應用程式登入方式完成驗證，才得以存取基站系統相關功能。	

4-2. 帳號必須可以識別

測試案例	帳號必須可以識別
參考資料	3GPP TS 33.117 Section 4.2.3.4.1.2
測試目的： 基站(eNodeB)中的帳號應明確有對應至每一位使用者使用者，避免帳號共用之情形。基站(eNodeB)提供之資料庫應至少能夠支援大量帳號建立。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	

測試案例	帳號必須可以識別
測試環境暨初始條件： 1. 基站(eNodeB)廠商須提供文件描述基站(eNodeB)可支援帳號與使用者身份的對應設計。 2. 所有預先設定於基站(eNodeB)內之帳號必須詳列於文件內。 3. 基站(eNodeB)文件需描述如何建立與維護帳號或群組的管理方式。	
測試方法： 1. 測試人員根據基站(eNodeB)文件指引建立大量帳號進行測試。 2. 測試人員檢視基站(eNodeB)是否支援帳號與使用者身份的對應設計。	
合格判定標準： 1. 基站(eNodeB)支援多個帳號建立。 2. 基站(eNodeB)支援使用者身分與帳號的對應設計。	
測試說明： 本項目測試 A 廠牌基站無法新建帳號，只能更改帳號名稱，而 B 廠牌基站則已經將帳號密碼綁定於應用程式內，登入系統後也無法新建立帳號。上述兩款的帳號管理主要都透過需額外購買的網管中心即可以完整這項需求。	

測試結果：下圖是 C 廠牌基站的測試畫面，最多單一基站可建立 10 組帳號。

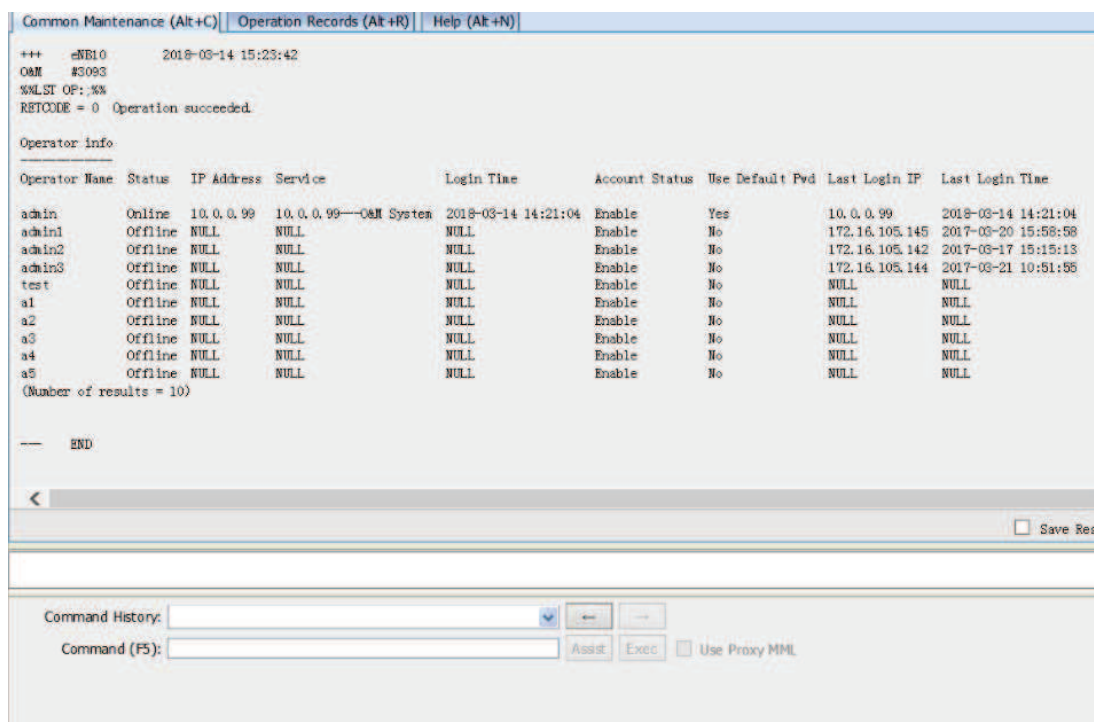


圖 5- 108 C 廠牌基站建立帳號組數

資料來源：本團隊整理

4-3. 每個帳號都需要至少一個身分鑑別因子

測試案例	每個帳號都需要至少一個身分鑑別因子
參考資料	3GPP TS 33.117 Section 4.2.3.4.1
測試目的： 基站(eNodeB)系統使用者身分鑑別的帳號至少須具備一項身分鑑別因子，例如加密金鑰(Cryptographic keys)、Token 或通行碼。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability) 測試環境暨初始條件： 1. 所有已經預先定義於基站(eNodeB)之帳號都需詳列於基站(eNodeB)文件。 2. 基站(eNodeB)廠商須提供如何建立新帳號之文件說明。 3. 測試人員有可建立帳號之特殊權限。 測試方法： 1. 測試人員使用預先定義在基站(eNodeB)的帳號登入系統，並不輸入其他身分鑑別因子，截圖記錄。	

測試案例	每個帳號都需要至少一個身分鑑別因子
2. 測試人員使用特殊權限登入，並建立新帳號。 3. 測試人員使用新帳號登入系統，並不輸入其他身分鑑別因子，截圖記錄。	
合格判定標準： 使用帳號登入系統階段，都需輸入其他正確的身分鑑別因子後才得以登入。	
測試說明： 本項目測試 A 與 C 廠牌基站登入都需帳號與密碼搭配下才得以登入網站伺服器系統。	

4-4. 預先定義之帳號與通行碼應刪除或停用

測試案例	預先定義之帳號與通行碼應刪除或停用
參考資料	3GPP TS 33.117 Section 4.2.3.4.2.2
測試目的： 基站(eNodeB)系統所有預定義或預設帳號都應於初始化設定完成後應予移除或停用。否則應設定預防遠端登入或設定複雜性較高之通行碼。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)提供系統出廠預定義之帳號與通行碼資料。 2. 提供帳號管理設定之操作文件。	
測試方法： 測試人員依據帳號管理設定之操作文件，確認是否可將預定義帳號刪除或停用	
合格判定標準： 可將預定義帳號刪除或停用	
測試說明： 本項目測試 A 廠牌基站無法移除內建之預設帳號，僅能透過更改名稱來變換。而 B 廠牌基站無法確定是否內建預設帳號，C 廠牌基站可在新建一個最高權限帳號後，可對原內建預設帳號予以停用。	

測試結果：如下圖可看到 admin, STATUS=DISABLE。

Common Maintenance (Alt+C) Operation Records (Alt+R) Help (Alt+N)									
Operator Name	Status	IP Address	Service	Login Time	Account Status	Use Default Pwd	Last Login IP	Last Login Time	
scottwu	Online	10.0.0.99	10.0.0.99---OAM System	2018-03-14 15:33:32	Enable	No	10.0.0.99	2018-03-14 15:33:32	
admin	Offline	NULL	NULL	NULL	Enable	Yes	10.0.0.99	2018-03-14 15:27:20	
admin1	Offline	NULL	NULL	NULL	Enable	No	172.16.105.145	2017-03-20 15:58:58	
admin2	Offline	NULL	NULL	NULL	Enable	No	172.16.105.142	2017-03-17 15:15:13	
admin3	Offline	NULL	NULL	NULL	Enable	No	172.16.105.144	2017-03-21 10:51:55	
test	Offline	NULL	NULL	NULL	Enable	No	NULL	NULL	
(Number of results = 6)									
--- END									
+++ eNE10 2018-03-14 15:34:49									
OAM #3153									
%%MOD_OP: OP='admin', STATUS=DISABLE, %									
RETURN = 0 operation succeeded									

圖 5-109 C 廠牌基站內建預設帳號停用

資料來源：本團隊整理

4-5. 通行碼複雜性

測試案例	通行碼複雜性
參考資料	3GPP TS 33.117 Section 4.2.3.4.2
測試目的： 基站(eNodeB)系統應支援與設定不同組合之通行碼複雜性規格，規則如下： (1) 通行碼長度不得低於最小長度 8 字元 (2) 至少包含一大寫字母(A-Z)、一小寫字母(a-z) 、一個數字(0-9) 、一特殊字元(@#\$%&*)。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商須提供通行碼修改操作文件。	
測試方法： 測試人員使用特定帳號登入系統，並修改通行碼，確認是否具符合要求之通行碼複雜性規格。	
合格判定標準： 基站(eNodeB)支援可設定不同組合之通行碼複雜性規格。	
測試說明： 本項目測試 A 與 C 廠牌基站都具有密碼複雜性設計。	

測試結果：下圖為 A 廠牌基站測試結果。

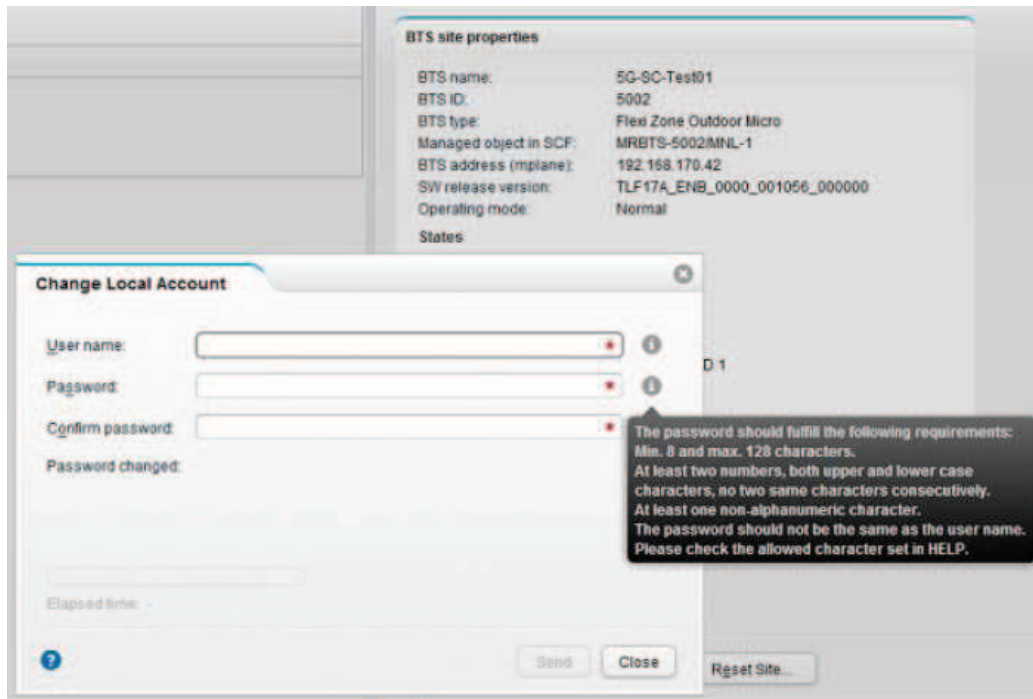


圖 5- 110 A 廠牌基站密碼複雜性設定

資料來源：本團隊整理

下圖為 C 廠牌基站測試結果，有密碼強度政策的要求。

The screenshot shows a web-based configuration interface for a network device. At the top, there are tabs for 'Common Maintenance (Alt+C)', 'Operation Records (Alt+R)', and 'Help (Alt+N)'. Below the tabs, the 'List of Password Policy' is displayed with the following settings:

- Password Minimal Length = 6
- Password Complicacy = Lowercase
- Digit = 3
- Password Max Miss Times = 3
- Auto Unlock Time(min) = 30
- Reset Interval of Account Lock(min) = 5
- New Password Repeat Limit = 5
- Password Validity(day) = 0
- Minimum Password Duration(min) = 1440
- Password Expiration Reminder(day) = 10
- Must Modify Password When First Login Switch = OFF
- Max Repeat Char Times = 2
- Weak Dictionary Check Switch = OFF
- Maximum Consecutive Characters from User Name = 0

Below the list, it states '(Number of results = 1)'. Underneath, there is a command execution section with the command 'ADD OP: UG=GUEST, DATE=NOLIMIT, TIME=NOLIMIT, WEEK=NOLIMIT;'. Below this, there is a 'Command History' dropdown and a 'Command (F5): ADD OP' input field. To the right of the command field are 'Assist' and 'Exec' buttons, and a checkbox for 'Use Proxy MML'. Below the command field, there are several input fields for 'Operator Name', 'Operator Password', 'Operator Description', 'Confirm Password', 'User Group' (set to GUEST(Guest)), 'Date Limit' (set to NOLIMIT(No Limit)), 'Time Limit' (set to NOLIMIT(No Limit)), 'Week Limit' (set to NOLIMIT(No Limit)), and 'Account Status' (set to ENABLE(Enable)).

圖 5- 111 C 廠牌基站密碼複雜性設定

資料來源：本團隊整理

4-6. 通行碼更改

測試案例	通行碼更改
參考資料	3GPP TS 33.117 Section 4.2.3.4.3.2
測試目的： 基站(eNodeB)系統應支援可隨時更改密碼之功能，且系統預設密碼應於初次登入階段強制要求變更，同時支援密碼變更不得超過重複使用次數的功能。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability) 測試環境暨初始條件： 基站(eNodeB)廠商須提供通行碼修改操作文件。	

測試案例	通行碼更改
測試方法： 1. 測試人員使用系統預設之密碼登入，觀察系統是否要求初次登入強制變更系統預設密碼。 2. 測試人員使用管理員帳號登入系統，選擇特定帳號，並測試密碼變更機制是否符合不得超過特定重複使用次數之要求，螢幕截圖記錄。	
合格判定標準： 1. 基站(eNodeB)系統有強制要求初次登入變更系統預設密碼。 2. 基站(eNodeB)系統符合不得超過特定重複使用次數之要求。	
測試說明： 本項目測試 A 與 C 廠牌基站未強制要求初次登入變更系統預設密碼。而密碼不得重複之要求僅只有 C 廠牌基站可以設定次數。	

測試結果：密碼不得重複之要求僅只有 C 廠牌基站可以設定次數，如下圖

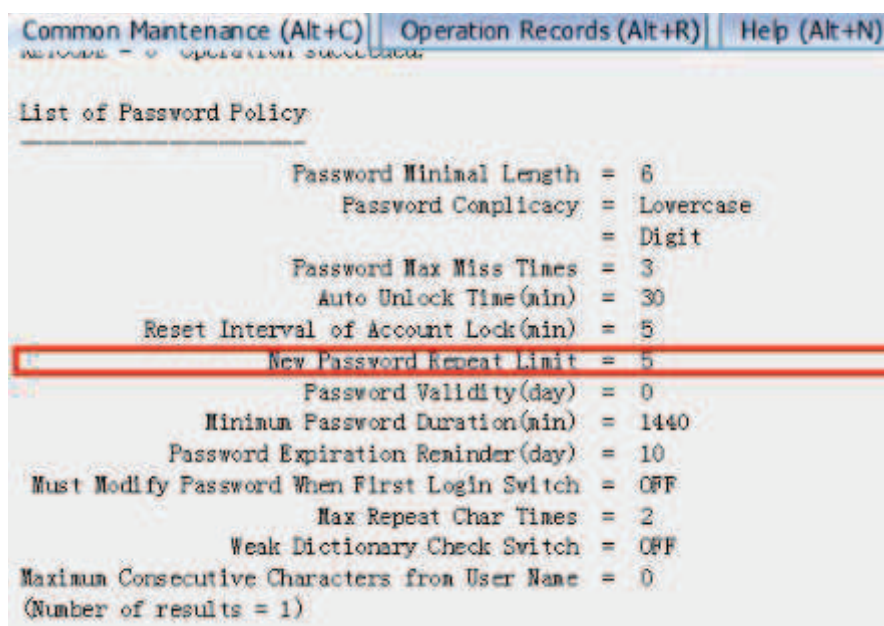


圖 5- 112 C 廠牌基站密碼可重複使用次數設定

資料來源：本團隊整理

4-7. 暴力及字典攻擊防護

測試案例	暴力及字典攻擊防護
參考資料	3GPP TS 33.117 Section 4.2.3.4.3.3
測試目的： 基站(eNodeB)系統應具備暴力及字典攻擊的防護措施，包含網頁介面設置CAPTCHA 功能、嘗試登入失敗次數限制與鎖定帳號時間。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供文件描述對於暴力與字典攻擊之防護措施與功能說明。	
測試方法： 1. 測試人員輸入不正確的密碼，確認系統是否於超出輸入錯誤限制次數後鎖定帳號，螢幕截圖記錄。 2. 使用測試工具進行暴力破解，確認是否可被進行暴力破解，螢幕截圖記錄。	
合格判定標準： 1. 基站(eNodeB)系統具備超出輸入錯誤限制次數後鎖定帳號之機制。 2. 基站(eNodeB)系統具防護機制，不可被進行暴力及字典攻擊。	
測試說明： 針對 A 廠牌及 C 廠牌登入功能進行測試。	

測試結果：

本項測試 A 廠牌基站具輸入錯誤限制次數後鎖定帳號之機制。



圖 5- 113 A 廠牌基站登入輸入錯誤限制

資料來源：本團隊整理

A 廠牌基站當開啟與透過 SSH 服務登入系統，可被攻擊工具進行暴力破解動作，如下圖，應該可搭配其他例如：限制來源 IP 與錯誤登入次數限制等機制來預防。

```
root@kali:~# hydra -l root -P passlist_revise.txt 192.168.170.41 ssh
Hydra v8.1 (c) 2014 by van Hauser/THC - Please do not use in military or secret services.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-01-31 21:14:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to use -x parameter.
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting it use -R parameter.
...

[DATA] max 16 tasks per 1 server, overall 64 tasks, 1190968 login tries (l:1/p:1190968)
[DATA] attacking service ssh on port 22

[STATUS] 139.00 tries/min, 139 tries in 00:01h, 1190829 todo in 142:48h, 16 active
[STATUS] 180.00 tries/min, 540 tries in 00:03h, 1190428 todo in 110:14h, 16 active
```

圖 5- 114 A 廠牌基站 SSH 暴力破解測試

資料來源：本團隊整理

C 廠牌基站除了帳號密碼管控外，並增加 Verification code 來提高安全性與避免遭受暴力破解攻擊，當超過登入限制則會顯示” The user is locked” ，如下圖。



圖 5- 115 C 廠牌基站登入輸入錯誤限制

資料來源：本團隊整理

此外，C 廠牌基站額外支援可自行設定限制時間與次數，如下圖。

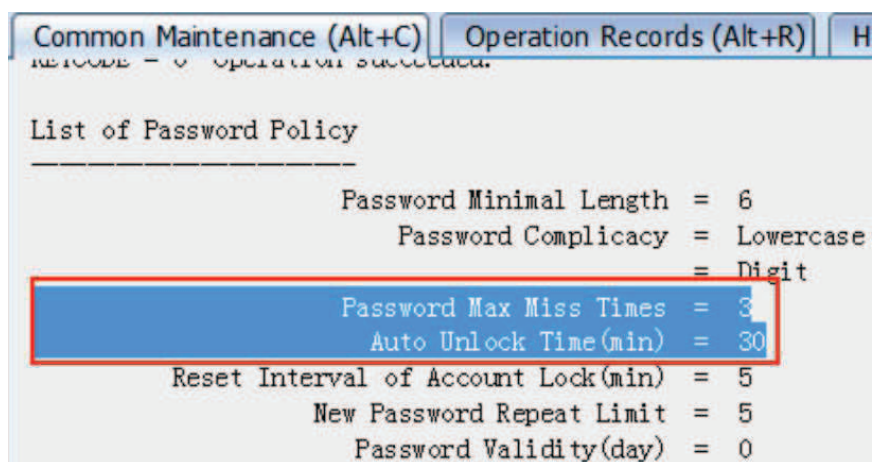


圖 5- 116 C 廠牌基站登入輸入錯誤次數限制設定

資料來源：本團隊整理

4-8. 存取控制

測試類型	存取控制
測試案例	授權策略、角色存取控制
參考資料	3GPP TS 33.117 Section 4.2.3.4.6.1, 3GPP TS 33.117 Section 4.2.3.4.6.2
測試目的： 基站(eNodeB)系統應具備依不同帳號不同授權之設定機制。	
資訊安全需求：	

測試類型	存取控制
測試案例	授權策略、角色存取控制
■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供文件描述如何依不同帳號設定不同授權。	
測試方法： 測試人員根據基站(eNodeB)廠商提供之文件檢視是否具備不同帳號設定不同授權之功能。	
合格判定標準： 基站(eNodeB)確實具備可對不同帳號設定不同授權之功能。	
測試說明： 本項目測試 A 廠牌基站只能有一個帳號且是最高權限，帳號的管理在原廠的設計上都在後端的網管中心控制。測試 C 廠牌可將帳號設定有權限之分。	

測試結果：如下圖為 C 廠牌不同權限帳號如要存取特定介面，系統則會顯示 RETCPDE 939720711 No Permission。

```

Common Maintenance (Alt+C) | Operation Records (Alt+R) | Help (Alt+N)

+++ eNB10 2018-03-14 16:09:29
O&M #3252
%%LST DEVIP:;%
RETCODE = 0 Operation succeeded.

List Device IP Configuration Data

Cabinet No. Subrack No. Slot No. Subboard Type Port Type Port No. VRF Index IP Address Mask User Label
0 0 7 Base Board Ethernet Port 0 0 10.0.0.76 255.255.255.0 NULL
0 0 7 Base Board Ethernet Port 0 0 190.1.128.2 255.255.255.0 NULL
0 0 7 Base Board Ethernet Port 0 0 191.1.128.2 255.255.255.0 NULL
0 0 7 Base Board Ethernet Port 0 0 192.168.127.76 255.255.255.0 NULL
(Number of results = 4)

--- END

+++ eNB10 2018-03-14 16:10:13
O&M #3254
%%ADD DEVIP: SN=0, SRT-ETH OVERBOARD, PT=ETH, PN=0, IP="1.1.1.1", MASK="255.255.255.0", USERLABEL="test", %
RETCODE = 939720711 No permission.
  
```

圖 5- 117 C 廠牌基站帳號權限控管

資料來源：本團隊整理

4-9. 登出功能

測試案例	登出功能
參考資料	3GPP TS 33.117 Section 4.2.3.5.1
測試目的： 基站(eNodeB)系統應支援帳號隨時登出功能，並於登出階段提供是否登出系統之提醒畫面。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)	
測試環境暨初始條件： 無	
測試方法： 測試人員使用特定帳號登入系統後，進行登出行為，確認系統是否顯示提示畫面，並完成系統登出，螢幕截圖記錄。	
合格判定標準： 基站(eNodeB)系統支援登出功能，並有顯示提示畫面。	
測試說明： 本項測試僅有 C 廠牌基站在登出階段會有提示確認畫面。	

測試結果：如下圖。

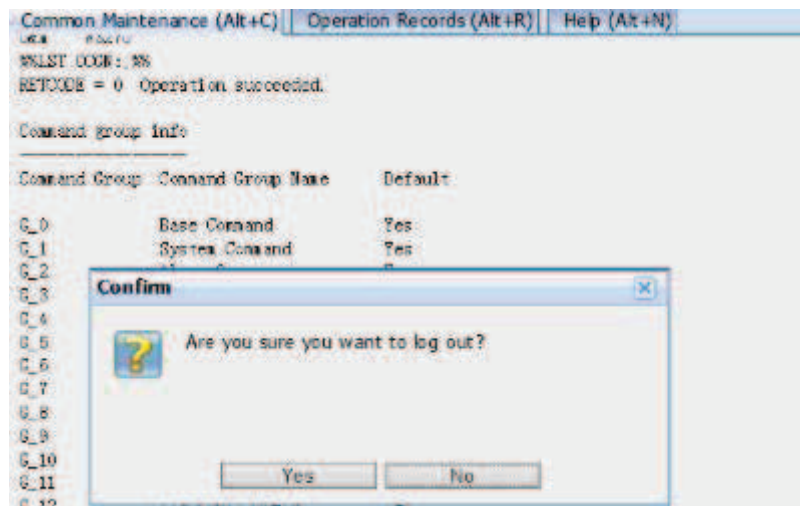


圖 5- 118 C 廠牌基站帳號登出功能

資料來源：本團隊整理

4-10. 操作逾時功能

測試案例	操作逾時功能
參考資料	3GPP TS 33.117 Section 4.2.3.5.2
測試目的： 基站(eNodeB)系統應具備帳戶操作逾時時間的設定功能，超出設定時間，系統應強制登出。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☒可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供文件描述逾時登出機制。 2. 基站(eNodeB)廠商提供設定逾時功能操作說明。	
測試方法： 1. 測試人員使用建立帳號登入系統，設定逾時登出時間。 2. 使用建立帳號登入系統，依所設定逾時登出時間進行操作閒置，確認系統是否依逾時設定對帳號進行強制登出。 3. 若系統沒有逾時設定功能，使用建立帳號登入系統，依逾時登出時間說明文件，進行操作閒置，確認系統是否依逾時設定對帳號進行強制登出。	
合格判定標準： 1. 基站(eNodeB)系統確認依逾時設定對帳號進行強制登出。 2. 若無逾時功能設定，系統於閒置時間後自行進行帳號強制登出。	
測試說明： 本項測試僅有 C 廠牌基站在有逾時管理機制，但非強制登出系統，而是要求重新輸入密碼再做一次驗證。	

測試結果：如下圖。

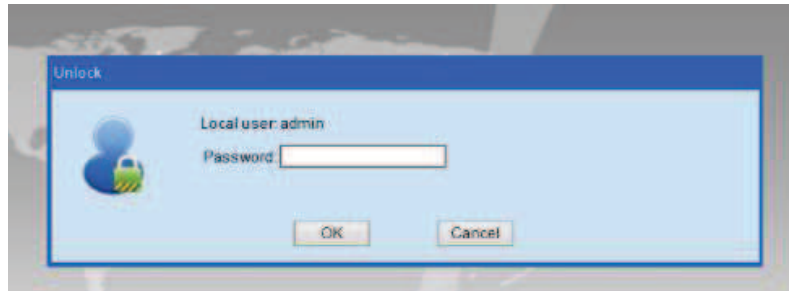


圖 5- 119 C 廠牌基站帳號操作逾時功能

資料來源：本團隊整理

4-11. 高權限系統功能之存取控制

測試案例	高權限系統功能之存取控制
參考資料	3GPP TS 33.117 Section 4.2.4.1.2.1
測試目的： 驗證擁有特殊權限的系統功能是否經過認證與授權方可使用。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☒可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供一清單 A，說明哪些系統函數可以取得高權限與其組態設定規則。例如： sudo command and its configuration file /etc/sudoers. 2. 提供一清單 B，包括系統指令、GUI 功能及檔案，這些即使較高權限只能執行特定的有限任務，在低特權用戶使用的情況下也是一樣。此列表須包含： • 設定這些指令和 GUI 功能。 • 文件的擁有者和權限設定。 • 這些指令、GUI 功能及檔案的合理性 例如： root-owned files with SUID and SGID permissions 3. 提供使用者取得系統管理者權限的方法。	
測試方法： 1. 測試人員判斷清單 A 中內容的合理性外，並驗證是否使用都要經過身分認證。 2. 測試人員判斷清單 B 中內容描述的正确性及合理性外，並驗證是否使用都要經過身分認證。 3. 測試人員確認列表“B”中的文件項目對擁有者之外的其他任何人都沒有寫入權	

測試案例	高權限系統功能之存取控制
限。	
合格判定標準：	
基站(eNodeB)不允許使用者透過另一個使用者帳戶，在沒有重新認證的情況下	
測試說明：	
本測試項目各廠牌基站無法提供說明哪些系統函數可以取得高權限與其組態設定規則，這些操作需求應該屬於在 OS 模式下才可以找到設定進行參數上的檢查與調整，但是產品開發完成後就僅會提供 Web 或應用程式介面的方式提供基站電信服務功能讓一般維運或管理人員操作使用。	

4-12. 系統帳號識別

測試案例	系統帳號識別
參考資料	3GPP TS 33.117 Section 4.2.4.2.2
測試目的：	
UNIX 中每個系統帳號都具有唯一的 UID。	
資訊安全需求：	
☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件：	
MME 作業系統為 UNIX。	
測試方法：	
1. 測試人員建立 UNIX 帳號。 2. 測試人員檢視帳號的 UID 是否都不同。	
合格判定標準：	
每個帳號都具有唯一的 UID。	
測試說明：	
本項目測試與 UNIX 及 UID 相關，基站產品開發完成後就僅只會提供 Web 或應用程式介面的方式提供基站電信服務功能讓一般維運或管理人員操作使用，目前並無在 OS 層級下可查看 UID 識別編號等資訊。	

4-13. 遠端登入控管

測試案例	遠端登入控管
參考資料	3GPP TS 33.117 Section 4.3.2.6
測試目的： 基站(eNodeB)系統最高管理權限帳號應不得從遠端登入，降低被攻擊的風險。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供如何遠端登入系統與限制最高管理權限帳號遠端登入之說明文件	
測試方法： 測試人員使用 root 或者最高權限的帳號進行遠端登入系統測試。	
合格判定標準： 基站(eNodeB)不允許最高權限的帳號可從遠端登入至系統。	
測試說明： 這項測試以基站的角色而言，除了安裝建置開機初始化設定以外，其餘時段登入基站通常目的是處理重要的相關設定，所以一般登入的帳號已具高權限身分，這是 IT 與 OT 維運需求上與環境角色不同之間的差異點。目前所測試之三種廠牌基站登入後即為最高權限，也有業者如果在非廠商私有線路下登入的才符合此項目要求，後續這部分需更業者有更多討論實際運作情況的溝通。	

4-14. 檔案系統存取權限控管

測試案例	檔案系統存取權限控管
參考資料	3GPP TS 33.117 Section 4.3.2.7
測試目的： 基站(eNodeB)系統應具備檔案系統存取權限控管機制，僅授權帳戶可修改作業系統層級之檔案、資料或系統檔案等。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☒ 可用性(Availability)	

測試案例	檔案系統存取權限控管
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供系統登入作業系統層級之操作介面與最高管理者帳號密碼。 2. 基站(eNodeB)廠商提供文件描述如何進行檔案系統存取權限控管機制之功能操作。	
測試方法： 1. 測試人員使用最高權限帳號登入作業系統層級之操作介面。 2. 測試人員依據書面資料對特定帳號行檔案系統存取權限設定，並重新登入再測試是否可對有授權管控之檔案系統進行存取。	
合格判定標準： 測試帳號無法對有授權管控之檔案系統進行存取。	
測試說明： 基站產品開發完成後就僅只會提供 Web 或應用程式介面的方式提供基站電信服務功能讓一般維運或管理人員操作使用，目前並無法登入 OS 層級下可查看特定帳號資訊。	

4-15. 阻絕不明來源 IP 位址

測試案例	阻絕不明來源 IP 位址
參考資料	3GPP TS 33.117 Section 4.3.3.1.1
測試目的： 基站(eNodeB)系統應可處理不明來源 IP 位址封包，應具備內建實作逆向過濾功能 (Reverse Path Filter)。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	

測試案例	阻絕不明來源 IP 位址
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供文件描述基站(eNodeB)如何設定過濾不明來源 IP 位址。 2. 基站(eNodeB)廠商提供文件說明如何調閱封包被丟棄的紀錄。 3. 基站(eNodeB)廠商提供文件說明如何啟用或外接基站(eNodeB)之網路流量分析功能 4. 測試人員擁有特殊管理權限。	
測試方法： 1. 測試人員使用測試設備啟動封包流量產生工具對目的端設備，其過程中經過基站(eNodeB)進行轉送。 2. 測試人員啟用基站(eNodeB)過濾來源 IP 位址功能與網路流量分析功能。 3. 測試人員觀察啟用過濾來源 IP 位址，並從網路流量分析上看到封包流量明顯被遞減，確認是否有被過濾掉。	
合格判定標準： 基站(eNodeB)可有效的過濾特定的 IP 位址。	
測試說明： 本測試 A、B、C 廠牌基站在測試場域的管人員表示並無這種用於網通產品，例如：路由器、交換器等設備上具備的功能。	

4-16. 防止 SYN Flood 攻擊

測試案例	防止 SYN Flood 攻擊
參考資料	3GPP TS 33.117 Section 4.3.3.1.4
測試目的： 基站(eNodeB)應具備 SYN Flood 攻擊處理能力。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 基站(eNodeB)廠商提供文件描述基站(eNodeB)處理 SYN Flood 攻擊。 2. 基站(eNodeB)廠商提供文件說明如何啟用或外接基站(eNodeB)之網路流量分析	

測試案例	防止 SYN Flood 攻擊
功能 3. 測試人員擁有特殊管理權限。	
測試方法： 1. 測試人員在基站(eNodeB)上開啟一個 TCP Port 做流量監聽。 2. 測試人員啟動網路流量分析功能或外接其他流量分析工具。 3. 測試人員使用具備 SYN Flood 攻擊工具與基站(eNodeB)相連接。	
合格判定標準： 基站(eNodeB)在經 SYN Flood 攻擊測試下，仍可正常運作，不發生當機狀態，基站(eNodeB)仍在可操控範圍內。	
測試說明： 本測試 A、B、C 廠牌基站在測試場域的管人員表示並無這種用於網通產品，例如：路由器、交換器等設備上具備的功能。	

4-17. 外部檔案系統掛載限制

測試案例	外部檔案系統掛載限制
參考資料	3GPP TS 33.117 Section 4.3.3.1.6
測試目的： 基站(eNodeB)之 OS 層級應可對外部檔案系統掛載做控制，防止從連接的檔案系統中被取得最高權限或更多的存取權限。 資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 測試人員具有特殊管理權限可設定外部檔案系統掛載控制。 2. 測試人員另有一般使用者帳號，此帳號能具有特殊權限連接外部檔案系統。	
測試方法： 1. 測試人員驗證 OS 層級設定，例如：在 Linux 系統，應設定選項 nodev 與 nosuid 在/etc/fstab 對於所有檔案系統，設定為「一般使用者」選項。 2. 測試人員連接外部檔案系統，確認是否可取得特殊權限。	

測試案例	外部檔案系統掛載限制
合格判定標準： 基站(eNodeB)在 OS 層級的限制設定下，可防止從外部檔案系統取得特殊權限與存取權限的提升。	
測試說明： 基站產品開發完成後就僅只會提供 Web 或應用程式介面的方式提供基站電信服務功能讓一般維運或管理人員操作使用，目前並無法登入 OS 層級下可設定相關系統掛載參數。	

5. 機敏資訊保護

檢測基站對機敏性資訊是否提供適當保護。

5-1. 防止敏感性資料外洩

測試案例	防止敏感性資料外洩
參考資料	3GPP TS 33.117 Section 4.2.3.2.2
測試目的： 確認基站(eNodeB)系統功能不會洩露一般僅在維護模式狀態下顯示之敏感性資料。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 基站(eNodeB)廠商提供文件描述系統如何處理敏感性資料。	
測試方法： 1. 測試人員審閱基站(eNodeB)廠商提供之文件對於敏感資料處理的描述。 2. 測試人員檢視文件中，例如：日誌訊息、警報、錯誤訊息、匯出設定檔等，並與基站(eNodeB)系統實際做操作對應看是否以明文顯示敏感性資料。	
合格判定標準： 基站(eNodeB)系統各功能的操作上並無以明文顯示敏感性資料。	
測試說明： 本測試項目三種廠牌基站在各功能操作上並無以明文顯示敏感性資料。	

測試結果：

下圖為 A 廠牌基站主要操作介面。

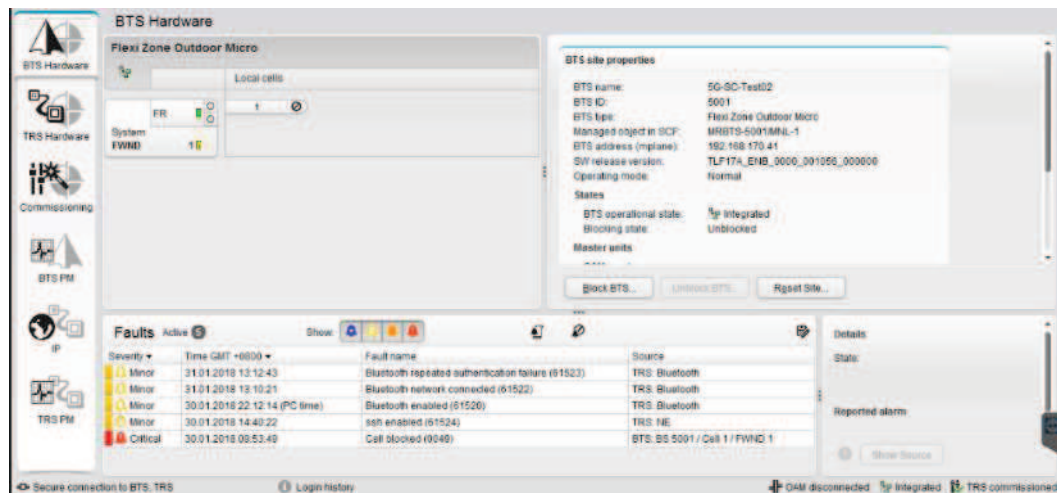


圖 5- 120 A 廠牌基站主要操作介面

資料來源：本團隊整理

下圖為 B 廠牌基站主要操作介面。

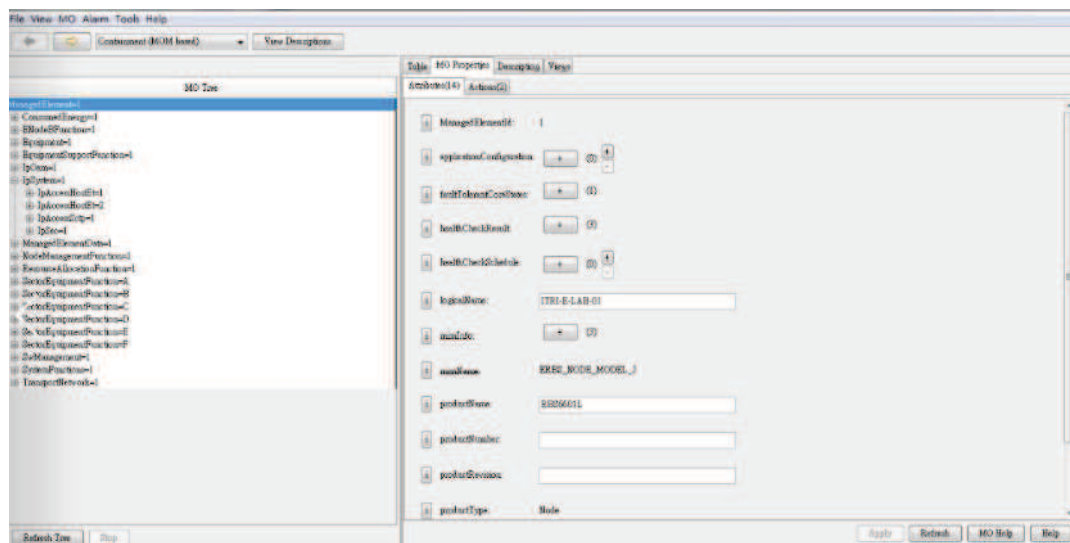


圖 5- 121 B 廠牌基站主要操作介面

資料來源：本團隊整理

下圖為 C 廠牌基站主要操作介面。

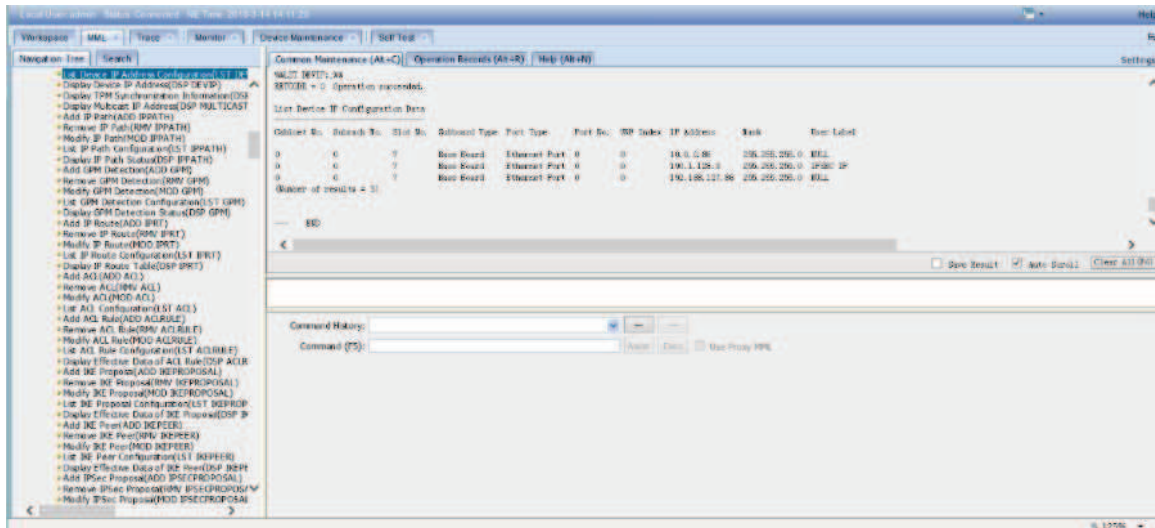


圖 5- 122 C 廠牌基站主要操作介面

資料來源：本團隊整理

5-2. 敏感性資料儲存保護

測試案例	敏感性資料儲存保護
參考資料	3GPP TS 33.117 Section 4.2.3.2.3
測試目的：	基站(eNodeB)對敏感性資料應採用適當且有效之加密技術，使資料不會以原來的形式呈現，達到保密的目的，並確保避免遭操作修改。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)
測試環境暨初始條件：	提供系統敏感性資料儲存區域與存取操作書面資料。
測試方法：	1. 測試人員依照基站(eNodeB)廠商書面文件檢視敏感性資料。 2. 檢視敏感性資料是否明文顯示。
合格判定標準：	敏感性資料以非明文(Plain-Text)方式顯示。
測試說明：	本項測試僅有 A 與 B 廠牌基站可另外登入至指令模式。

測試結果：

下圖為 A 廠牌基站透過 SSH 方式登入的指令模式，而用戶帳號的密碼被加密儲存在/etc 資料夾下。

```

daemon*:17452:0:99999:7:::
bin*:17452:0:99999:7:::
sys*:17452:0:99999:7:::
sync*:17452:0:99999:7:::
games*:17452:0:99999:7:::
man*:17452:0:99999:7:::
lp*:17452:0:99999:7:::
mail*:17452:0:99999:7:::
news*:17452:0:99999:7:::
uucp*:17452:0:99999:7:::
proxy*:17452:0:99999:7:::
www-data*:17452:0:99999:7:::
backup*:17452:0:99999:7:::
list*:17452:0:99999:7:::
irc*:17452:0:99999:7:::
gnats*:17452:0:99999:7:::
nobody*:17452:0:99999:7:::
ftp!:17452:!::::
dhcpcd!:17452:!::::
sshd!:17452:!::::
rpc!:17452:!::::
ntp!:17452:!::::
toor4nsn:$5$hcMw0/UpyQI/wP$PKeatbbX6PU62ElY4Y9XzD01u..1RusIW7aKwfK9O6:17452:0:99999:7:::
btssw!:17452:0:99999:7:::
messagebus!:17452:!::::
rpcuser!:17452:!::::
systemd-journal-gateway!:17452:!::::
systemd-timesync!:17452:!::::
systemd-bus-proxy!:17452:!::::
systemd-network!:17452:!::::
smafilettransfer!:12418:0:99999:7:::
smacertmgr!:12418:0:99999:7:::
smaruim!:12418:0:99999:7:::
smaasn1!:12418:0:99999:7:::
smachoh!:12418:0:99999:7:::
smactacmgr!:12418:0:99999:7:::
smaruem!:12418:0:99999:7:::
nma!:12418:0:99999:7:::
nmapagent!:12418:0:99999:7:::
bfd!:12418:0:99999:7:::
quagga!:12418:0:99999:7:::
lighttpd!:12418:0:99999:7:::

```

圖 5-123 A 廠牌基站敏感性資料

資料來源：本團隊整理

下圖為 B 廠牌基站透過 SSH 方式登入該廠牌基站專有的 ncli 指令模式，但經與測試環境該基站的管理人員討論，這應該是經過額外客製化僅保留部分指令，並無找到相關敏感性資料。


```

login as: rbs
rbs@192.168.170.65's password:
Server refused to allocate pty
Welcome to OSE Shell OSE5.8.
$

$ ncli
ncli

[ManagedElement=1]>

[ManagedElement=1]> help
help
Command                Description
!                        Execute command from history
action                  Execute an action on a Managed Object
alarms                  Print active alarm list
alarmsev                Change alarm severity configuration
cd                      alias for jump
create                  Create Managed Object
delete                  Delete Managed Object
diff                    Compare Managed Objects
exit                    Terminates an NCLI session
get                     Get attributes and children of a particular Managed Object
group                    Manage group of Managed Objects
help                    alias for man
history                 Display command history
info                    Print information from the Managed Object Model (MOM)
jump                    Change working Managed Object
ls                      alias for get
man                     Display manual pages
pwd                     alias for pwldn
pwldn                   Print working Managed Object
rm                      alias for delete
search                  Search for Managed Objects
set                     Set Managed Object attribute values
tx                      Transaction management

```

圖 5- 124 B 廠牌基站敏感性資料

資料來源：本團隊整理

5-3. 日誌檔不可洩露個人資料

測試案例	日誌檔不可洩露個人資料
參考資料	3GPP TS 33.117 Section 4.2.3.2.5
測試目的： 基站(eNodeB)系統日誌檔如有個人資料不應以明文顯。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 提供系統日誌檔存取操作書面資料。	
測試方法： 1. 測試人員依照基站(eNodeB)廠商書面文件檢視日誌檔。 2. 檢視日誌檔是否存有敏感性資料且以明文顯示。	

測試案例	日誌檔不可洩露個人資料
合格判定標準： 日誌檔內之敏感性資料不得以明文顯示。	
測試說明： 本項測試僅有 A、B 與 C 廠牌基站的日誌檔都僅有系統運作相關的日誌紀錄。	

測試結果：

下圖為 A 廠牌基站日誌紀錄資訊。



圖 5-125 A 廠牌基站日誌紀錄資訊

資料來源：本團隊整理

下圖為 B 廠牌基站日誌紀錄資訊。

Total [175] Changel: 2019-02-01 11:23:00-00:00							
Severity	Event Type	Time	360 Instance	Possible Cause	Specific Problem	Additional Text	
MAJOR	Communication alarm	2017-11-11 01:51:40:00	...SystemFunction=1,TimeCritical=1	Clock synchronization problem	NTP System Time Sync Fault	NTP error alarm	
MAJOR	Communication alarm	2017-11-11 08:32:10:00:00	...net_EIPPortCellID=2005022236-C	Unavailable	PLMN Service Unavailable	S1 Connection Failure for PLMN net...	
MAJOR	Communication alarm	2017-11-11 08:32:10:00:00	...net_EIPPortCellID=2005022236-C	Unavailable	PLMN Service Unavailable	S1 Connection Failure for PLMN net...	
MAJOR	Processing error alarm	2017-11-11 08:32:46:00:00	...net_EIPPortCellID=2005022236-C	Duplicating Resource Unavailable	Service Unavailable		
MAJOR	Processing error alarm	2017-11-11 08:32:46:00:00	...net_EIPPortCellID=2005022236-C	Duplicating Resource Unavailable	Service Unavailable		
MAJOR	Quality of service alarm	2017-11-15 08:53:29:00:00	...net_SystemFunction=1,Access=1	Alarm Indication Signal (AIS)	Emergency Unlock of Software License	Emergency Unlock has been activated	
MAJOR	Communication alarm	2017-11-15 08:53:30:00:00	...net_EIPPortCellID=2005022236-C	Unavailable	Packet Service Availability Fault		
MAJOR	Communication alarm	2017-11-15 08:53:30:00:00	...net_EIPPortCellID=2005022236-C	Unavailable	NTP Service Reachability Fault		
MAJOR	Processing error alarm	2017-11-15 08:53:43:00:00	...net_EIPPortCellID=2005022236-C	Duplicating Resource Unavailable	Service Unavailable		
MAJOR	Processing error alarm	2017-11-15 08:53:46:00:00	...net_EIPPortCellID=2005022236-C	Duplicating Resource Unavailable	Service Unavailable		
MAJOR	Processing error alarm	2017-11-15 08:53:46:00:00	...net_EIPPortCellID=2005022236-C	Duplicating Resource Unavailable	Service Unavailable		
MAJOR	Processing error alarm	2017-11-15 08:53:46:00:00	...net_EIPPortCellID=2005022236-C	Duplicating Resource Unavailable	Service Unavailable		
MAJOR	Quality of service alarm	2017-11-15 14:06:37:00:00	...net_SystemFunction=1,Access=1	Alarm Indication Signal (AIS)	Emergency Unlock of Software License	Emergency Unlock has been activated	
MAJOR	Communication alarm	2017-11-15 14:06:38:00:00	...net_EIPPortCellID=2005022236-C	Unavailable	Packet Service Availability Fault		
MAJOR	Communication alarm	2017-11-15 14:06:38:00:00	...net_EIPPortCellID=2005022236-C	Unavailable	NTP Service Reachability Fault		
MAJOR	Processing error alarm	2017-11-15 14:06:38:00:00	...net_EIPPortCellID=2005022236-C	Duplicating Resource Unavailable	Service Unavailable		

圖 5-126 B 廠牌基站日誌紀錄資訊

資料來源：本團隊整理

下圖為 C 廠牌基站日誌紀錄資訊。

Navigation Tree		Common Maintenance (Alt+C)		Operation Records (Alt+R)		Help (Alt+N)	
MML Commands		Operation Command Information: MOD EUEPSEC: IntAlgo=EIA1-04EIA2-0;					
System Management		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 11:47:22	Success	0 MAJOR 2018-03-14 11:47:22
Version Management		Operation Command Information: LST EUEPSEC;					
Time Management		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 11:51:23	Success	0 MAJOR 2018-03-14 11:51:23
Configuration Management		Operation Command Information: MOD EUEPSEC: IntAlgo=EIA1-04EIA2-1;					
License Management		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 11:51:28	Success	0 MAJOR 2018-03-14 11:51:28
Application Management		Operation Command Information: LST EUEPSEC;					
File Management		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 11:54:53	Success	0 MAJOR 2018-03-14 11:54:53
CB Management		Operation Command Information: LST PDPCPROCPARA;					
Configuration Rights Management		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 11:56:54	Success	0 MAJOR 2018-03-14 11:56:54
Batch Command Processing		Operation Command Information: CmdCode=0x00000101 CmdName="Create trace task" TaskID=2162694 TraceType=0x00000066 ReportMethod=0 Res					
Log Management		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 12:11:40	Success	0 MAJOR 2018-03-14 12:11:40
Lst Operation Log(LST OPTLOG)		Operation Command Information: LST ENOGERALGOSWITCH;					
Lst Security Log(LST SEQLOG)		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 12:13:57	Success	0 MAJOR 2018-03-14 12:13:57
Lst Log File(LST LOGFILE)		Operation Command Information: LST SRELLTDCPCFG;					
Upload Log File(ULD LOG)		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 12:14:20	Success	0 MAJOR 2018-03-14 12:14:20
Set Log File Automatically Upload		Operation Command Information: LST ELFCPCPPARAGROOF;					
Lst Automatically Upload Informa		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 12:14:36	Success	0 MAJOR 2018-03-14 12:14:36
Security Management		Operation Command Information: LST UEINFO;					
Security Query		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 14:19:30	Success	0 MAJOR 2018-03-14 14:19:30
Routine Test		Operation Command Information: LST RE;					
Equipment Management		LNT	admin Local 10.0.0.99	MAINTENANCE	2018-03-14 14:21:05	Success	0 MAJOR 2018-03-14 14:21:05
Alarm Management		Operation Command Information: LST RE;					
Transmission Management		(Number of Results = 19)					

圖 5- 127 C 廠牌基站日誌紀錄資訊

資料來源：本團隊整理

5-4. 軟體完整性

測試案例	軟體完整性
參考資料	3GPP TS 33.117 Section 4.2.3.3.5
測試目的： 基站(eNodeB)系統應具備出廠預載軟體安裝時完整性檢測，驗證軟體是否已遭受修改。 資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) □可用性(Availability)	
測試環境暨初始條件： 1. 測試人員具備特殊管理權限。 2. 基站(eNodeB)廠商提供軟體完整性機制相關文件描述與實際系統畫面。	
測試方法： 測試人員根據書面資料操作，從專業上判斷是否達到軟體完整性的保護。	
合格判定標準： 基站(eNodeB)所安裝之軟體有透過安全技術確保其完整性。	
測試說明： 檢測 A、B、C 廠牌設備軟體完整性的保護。	

測試結果：

本項目測試，A 廠牌基站所有安裝軟體都會將過雜湊驗算來確保完整性，但在操作介面上並無額外顯示軟體已經過驗證等資訊，如下圖。

```
1 addons/APPDEF_T1927262.tgz F2M sha256 d2df7c06dc0ca735d369a0689dc96ce820d97f031f53208573df6e907e66afc1
2 addons/ant/APPDEF_T1927262.tgz F2M sha256 f063899fbf0f268c637b2b3006bbd0c969b5e67d6300e919c31ac6f459389129
3 AdaptationVersions_T1927262.xml F2M sha256 41fad51c3ff902829599c1bd1e04f3a24d62a0ede1f6413310c225a4fde07e44
4 AntBD_TLA17A_ENB_0000_001056_000000.tgz F2M sha256 f64db13c32ec4ce2b2fe06a5c2e5a89cdfecf0c9b5ef8bda369063995255d31
5 apps/BTSOM_T1867686.tgz F2M sha256 2339afda4b42281907b6db79fcd677ea396630db793cf33e4389f9bdd0dd5016
6 dsp/BootKeplerMaster_T1867686.out F2M sha256 98722a5fa58d89a02b6800165640716af1a235c4382509247e259d89c9c72d1f
7 dsp/BootKeplerSlave_T1867686.out F2M sha256 a15817a43390db96c2b4fab2abf2d5c248afae125a95f5dd5b6dfb02bb704b7
8 apps/CCS_ec137499ccs96891.tgz F2M sha256 6f18d8f9f2769a4f5909a358b25e7c66e2be49735322ebae4c41487386e9f47d
9 uplane0/CCS_102995.tgz F2M sha256 b9f30a5d2f298a0f3ad8bf4d4242f29dcd855dd3f632bde8e65f55b5a7c3933
10 apps/CELLC_T1867686.txz F2M sha256 c53118ed7340395274485d3a25ee335d146d5bae093222c285385566084ca7d
11 apps/CELLSON_T1867686.txz F2M sha256 ccbfbc1cb0c7072983036f2bee44bf7483cbb9c9a8ab9212454bd76f45db36c
12 boot/CRTM_T1867686 F2M sha256 030e104a36bc95306e3876233cc0d6475cc117fbc08994d8f8fa698df41a70a6
13 apps/CpuMemorySupervisorExe_T1927262.txz F2M sha256 98c42b9927dcd6971b852bbef5c19a615cf66c98428ba6517f03eacd3c9f3398
14 apps/ENBC_T1867686.txz F2M sha256 5296c0276548c271e2f8b13bb86fe2d8fa08dde47cb2d643c223e9c2120ea3a6
15 apps/ENBSON_T1867686.txz F2M sha256 d280b4be6db048a1f93ae60922d563bcded175132b10a73db7f42d92ebac50b5
16 trs/FTM_FLI7A_TLA17A_2017.10.28_0254.xml F2M sha256 d5a112afe407e44c2b5d0a8c3ae59425e1efe5db65e442df930f06c4b68f6875
17 apps/FaultServiceExe_T1927262.txz F2M sha256 b9edf5a2deb29e5094b0cc963b9955975486c44016b7f1c2bb1ab6d8f55b999
18 FlexiSiteEM_T1867686.xml F2M sha256 19bd040d71d715c7810b651cd94e0b466b4f2a2631fca22db33b560d7d35eebc
```

圖 5-128 A 廠牌基站軟體雜湊驗算資訊

資料來源：本團隊整理

下圖為 B 廠牌基站所有安裝軟體在系統內部都有完整驗證，並會將資訊呈現於 Description for - ignatureValidationService 介面上。

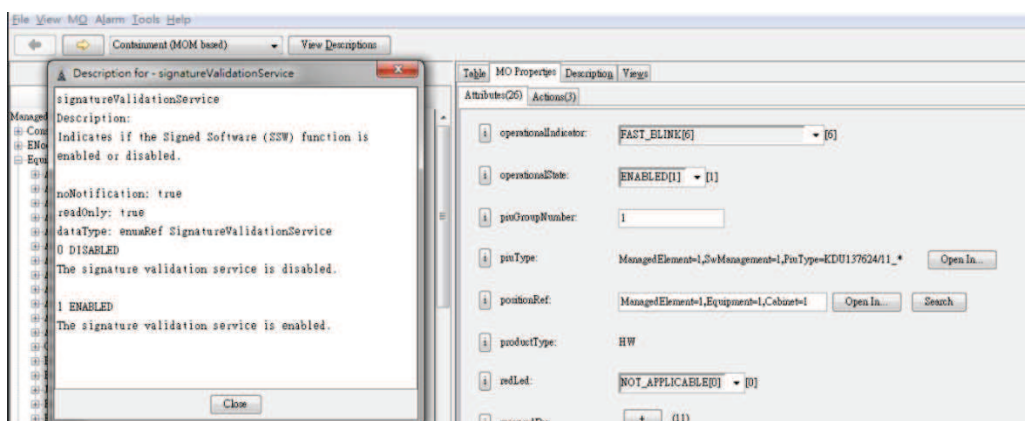


圖 5-129 B 廠牌基站軟體雜湊驗算資訊

資料來源：本團隊整理

下圖為 C 廠牌基站所有安裝軟體在系統內部都有完整驗證，並會將資訊呈現於 Software Status 介面上，如果顯示 Available 則表示驗證完整正常運作。

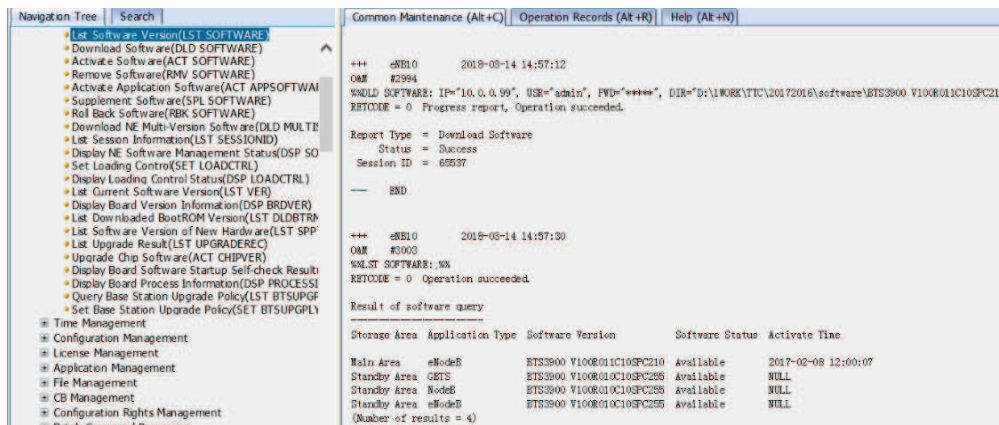


圖 5- 130 C 廠牌基站軟體雜湊驗算資訊

資料來源：本團隊整理

5-5. 日誌轉移至集中式管理

測試案例	日誌轉移至集中式管理
參考資料	3GPP TS 33.117 Section 4.2.3.6.2
測試目的： 基站(eNodeB)系統應提供可將安全事件記錄功能傳輸備存至集中管理設備或其他外部系統設備，並於傳輸過程使用加密技術保護。 資訊安全需求： ☒機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)	
測試環境暨初始條件： 1. 提供安全事件紀錄傳輸至外部系統使用之標準協定文件。 2. 提供基站系統可支援傳輸安全事件紀錄之外部設備，提供整合設定操作文件。 3. 提供如何觸發每一個安全事件之操作文件。	
測試方法： 1. 測試人員觸發安全事件紀錄，將事件日誌傳送到外部系統，螢幕截圖記錄。 2. 測試人員側錄與保存網路傳輸過程間之通訊封包。 3. 測試人員檢視集中式管理設備或外部系統是否儲存相關安全事件日誌	
合格判定標準： 具備安全事件記錄功能傳輸至集中管理設備或其他外部系統設備，並於傳輸過程使用加密技術保護。	

測試案例	日誌轉移至集中式管理
測試說明： 檢測 A、B、C 廠牌設備安全事件記錄功能是否傳輸至集中管理設備或其他外部系統設備，並於傳輸過程使用加密技術保護。	

測試結果：

本項目測試，A 廠牌基站可設定 Primary OAM system，相關的日誌資訊就會由網管中心發起回傳至後端集中管理設備，如下圖。

圖 5- 131 A 廠牌基站 OAM 設定

資料來源：本團隊整理

B 廠牌基站透過設定 IPHostLink，將外部網管系統設定，並可於 availabilityStatus 欄位做好啟用設定與後端連接。

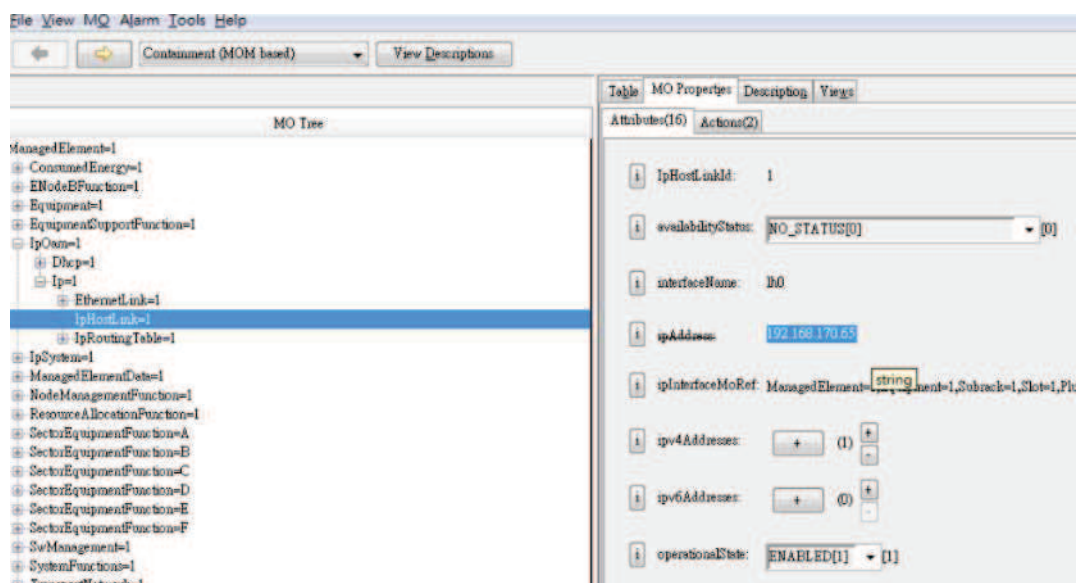


圖 5- 132 B 廠牌基站 OAM 設定

資料來源：本團隊整理

C 廠牌基站管理人員表示在基站端不須額外設定，主要由後端網管中心直接找到做設定即可收取來自基站端的日誌事件。

5-6. 安全事件日誌防護

測試案例	安全事件日誌防護
參考資料	3GPP TS 33.117 Section 4.2.3.6.3
測試目的： 基站(eNodeB)之安全事件紀錄應有存取控制限制。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 提供安全事件紀錄儲存位置、如何存取之說明文件。 2. 測試人員具有特殊權限。	
測試方法： 1. 測試人員使用具安全事件存取權限之帳號登入系統，確認是否可以存取安全事件日誌文件檔。 2. 測試人員使用無安全事件存取權限之帳號登入系統，確認是否可以存取安全事	

測試案例	安全事件日誌防護
件日誌文件檔。	
合格判定標準： 基站(eNodeB)之安全事件紀錄只限定具有權限才可存取。	
測試說明： 由於基站使用之帳號登入已具高權限身分，所以可以存取安全事件紀錄，這是 IT 與 OT 維運需求上與環境角色不同之間的差異點。目前只有 C 廠牌基站可以額外設定其他低權限帳號即可以限制存取安全事件紀錄。	

6. 基站自發性連外異常行為分析

針對測試過程中，判斷基站是否主動發出異常連線進行分析。在本次於測試環境為期四天的紀錄，並無發現有異常結果，統整如下表。

表 5-7 基站自發性連外行為分析

被動式檢測		基站廠牌	A 廠牌	B 廠牌	C 廠牌
已知威脅分析	一般性資安檢測觸發期間主動連接非預期之目的主機		未檢出	未檢出	未檢出
	進階資安檢測觸發期間主動連接非預期之目的主機		未檢出	未檢出	未檢出
	一般性資安檢測觸發期間之異常通訊行為		未檢出	未檢出	未檢出
	進階資安檢測觸發期間之異常通訊行為		未檢出	未檢出	未檢出
	惡意軟體之傳送或下載行為		未檢出	未檢出	未檢出
	已知類型之惡意行為		未檢出	未檢出	未檢出
	Handover 過程之異常通訊行為		未檢出	未檢出	未檢出
未知威脅分析	進階持續性滲透攻擊之行為		未檢出	未檢出	未檢出

資料來源：本團隊整理

另外根據兩套資安檢測工具的紀錄，整體威脅分析結果都為正常，如下圖。

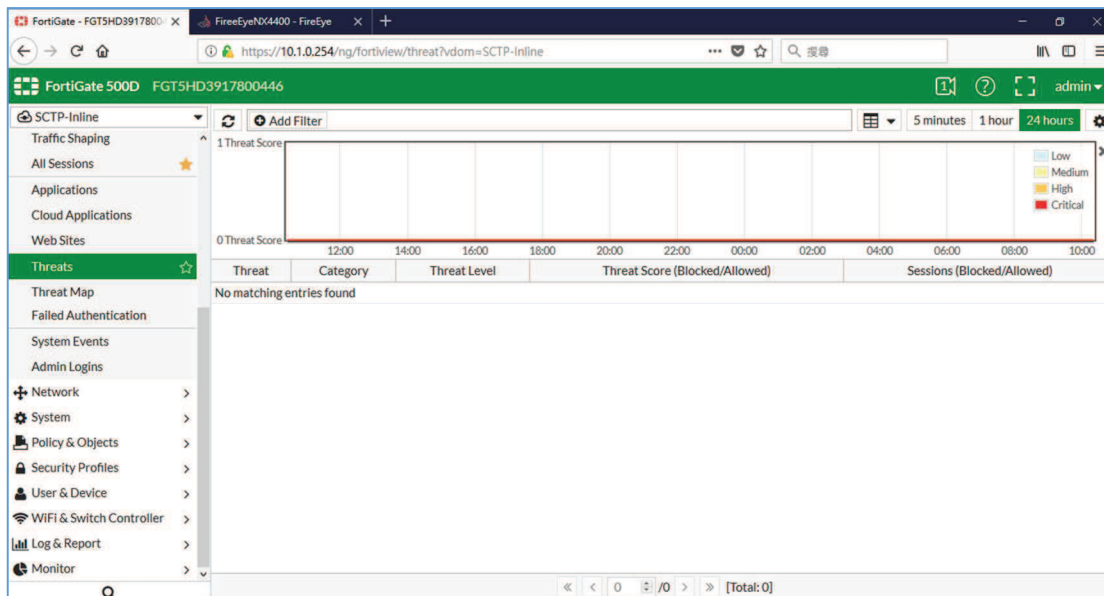


圖 5- 133 已知威脅分析結果

資料來源：本團隊整理

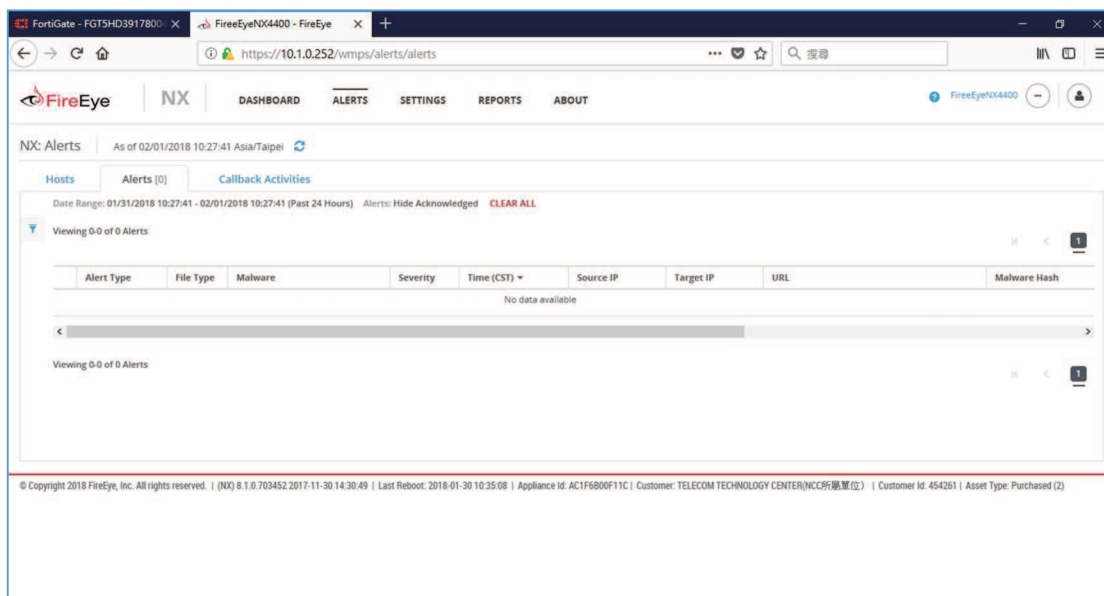


圖 5- 134 未知威脅分析結果

資料來源：本團隊整理

7. 滲透測試

主要針對通訊協定進行異常資料傳送，驗證安全強度。並對基站可蒐集到之軟體進行安全檢測。

7-1: 堅實性與模糊測試

測試案例	堅實性與模糊測試
參考資料	3GPP TS 33.117 Section 4.4.4
測試目的： 測試基站(eNodeB)遇到輸入超出範圍或異常資料的穩定性，是否存有程式設計缺陷。 資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 測試人員有特殊權限存取登入基站(eNodeB)，包含日誌檔案存取權限。 2. 基站(eNodeB)廠商提供之文件應該至少包含使用到的通訊協定資訊。	
測試方法： 1. 測試人員使用有效的模糊測試工具，且測試時間需合理可對基站(eNodeB)產生效用的時間為考量。 2. 測試人員檢視基站(eNodeB)是否正常運作且無當機情況。 3. 測試人員檢視模糊測試工具結果是否存有程式設計缺陷。	
合格判定標準： 1. 模糊測試過程中無當機情況。 2. 模糊測試結果並無 SANS/CWE Top 25 所列前 25 大常見之程式設計缺陷。	
測試說明： 本測試項目對 A 廠牌基站進行藍芽模糊測試	

測試結果：

測試結果如下圖。主要是 CWE-189 對於整數的處理有問題。

Failure summary:

Test #	Test suite	Test group	Anomaly description	CWE(s)
1	L2CAP Test Suite	l2cap.connect-disconnect.connection-request.ACLData.Code.connection_request	Integer value 128 (int-8bit)	Integer, CWE-189
1	L2CAP Test Suite	l2cap.connect-disconnect.connection-request.ACLData.Code.connection_request	Integer value 255 (int-8bit)	Integer, CWE-189
1	L2CAP Test Suite	l2cap.connect-disconnect.connection-request.ACLData.Code.connection_request	Integer value 33 (int-8bit)	Integer, CWE-189
1	L2CAP Test Suite	l2cap.connect-disconnect.connection-request.ACLData.Code.connection_request	Integer value 129 (int-8bit)	Integer, CWE-189
1	L2CAP Test Suite	l2cap.connect-disconnect.connection-request.ACLData.Code.connection_request	Integer value 192 (int-8bit)	Integer, CWE-189
1	L2CAP Test Suite	l2cap.connect-disconnect.connection-request.ACLData.Code.connection_request	Integer value 204 (int-8bit)	Integer, CWE-189

圖 5- 135 A 廠牌基站之藍芽模糊測試

資料來源：本團隊整理

此外，TLS 1.2 的模糊測試結果也出現有錯誤情形，主要為 CWE-189、CWE-166、CWE-399 與 overflow 的程式缺陷問題，如下圖。

1	TLS 1.2 Server Test Suite	TLS.TLS12.Basic.RSA-Groups.TLS_RSA_WITH_AES_256_CBC_SHA.Client-Hello.ClientHelloBody.Extensions.Opaque-16bit.SignatureAndHashAlgorithm.ExtensionData.Opaque-16bit.AlgorithmExtension.element	Omitted int-16bit	CWE-189, CWE-166
1	TLS 1.2 Server Test Suite	TLS.TLS12.Basic.RSA-Groups.TLS_RSA_WITH_AES_256_CBC_SHA.Client-Hello.ClientHelloBody.Extensions.Opaque-16bit.SignatureAndHashAlgorithm.ExtensionData.Opaque-16bit.AlgorithmExtension.element	Omitted int-16bit	CWE-189, CWE-166
1	TLS 1.2 Server Test Suite	TLS.TLS12.Basic.RSA-Groups.TLS_RSA_WITH_AES_256_CBC_SHA.Client-Hello.ClientHelloBody.Extensions.Opaque-16bit.SignatureAndHashAlgorithm.ExtensionData.Opaque-16bit.AlgorithmExtension.element	1-byte extra in heading	CWE-189
1	TLS 1.2 Server Test Suite	TLS.TLS12.Basic.RSA-Groups.TLS_RSA_WITH_AES_256_CBC_SHA.Client-Hello-SSL2.element	Repeat of 8 octets	Overflow
1	TLS 1.2 Server Test Suite	TLS.TLS12.Basic.RSA-Groups.TLS_RSA_WITH_AES_256_CBC_SHA.Client-Hello.ClientHelloBody.Extensions.Opaque-16bit.AppLayerProtocolNegot.app-layer-protocol-negotiation-extension.ExtensionData.Opaque-16bit.protocol-name-list.Opaque-8bit.app-protocol	Invalid regular expression with empty OR	CWE-399

圖 5-136 A 廠牌基站之 TLS 模糊測試

資料來源：本團隊整理

7-2: 韌體分析

測試案例	韌體分析
參考資料	UL 2900-1, Software Cybersecurity for Network-Connectable Products, Part 1 : General Requirements
測試目的： 測試基站(eNodeB)之韌體檔案是否存有 CVE 漏洞。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 測試人員需有未經加密基站韌體檔案。	
測試方法： 測試人員使用韌體分析工具進行分析，從檢測結果評估是否存有 CVE 漏洞。	

測試案例	韌體分析
合格判定標準： 須考量基站所處環境、提供之服務與設定功能，進而判斷這些 CVE 漏洞是否會影響基站的商用服務。	
測試說明： 測試 C 廠牌基站韌體，從檢測結果評估是否存有 CVE 漏洞。	

測試結果：

本項目測試 C 廠牌基站韌體分析結果如下圖，共有 1002 筆 CVE 弱點，Critical 有 269 筆、Major 有 546 筆、Minor 有 187 筆。(註：基於敏感性資料與安全考量，本研究未列出所有 CVE 編號清單)

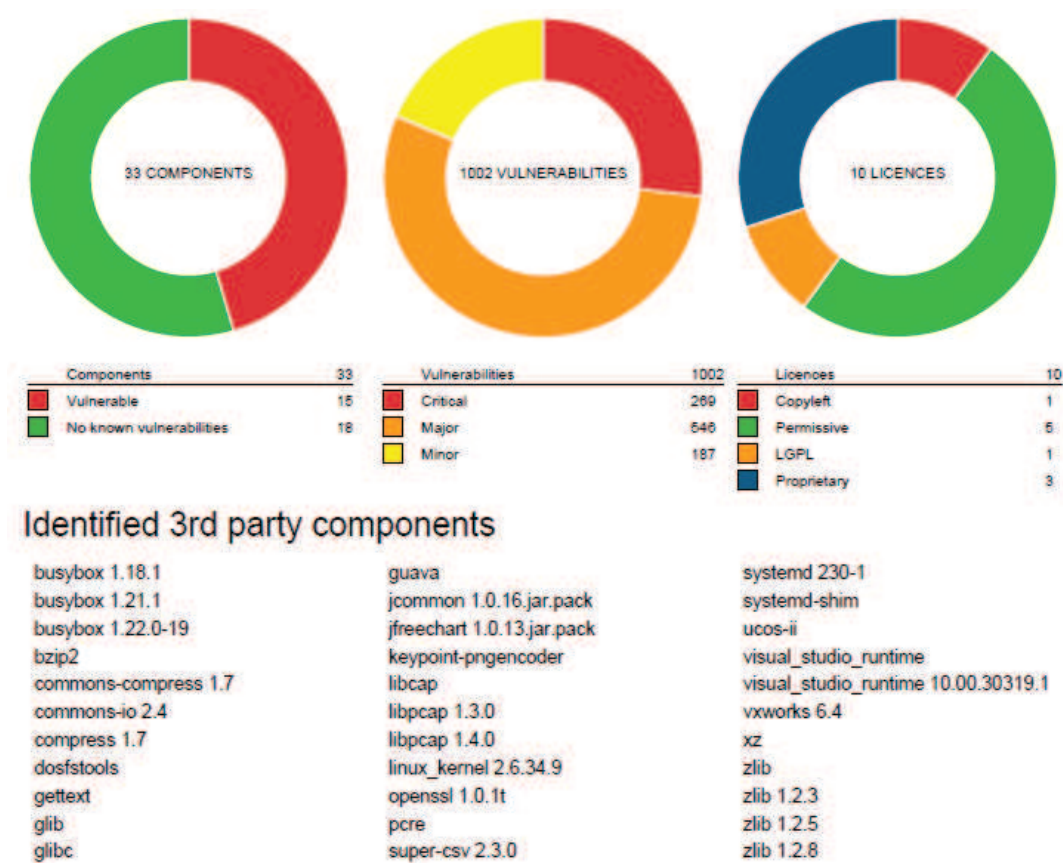


圖 5- 137 C 廠牌基站韌體分析結果一覽

資料來源：本團隊整理

下圖為廠牌 A 基站韌體分析結果如下圖，共有 778 筆 CVE 弱點，Critical 有 297

筆、Major 有 394 筆、Minor 有 87 筆。(註：基於敏感性資料與安全考量，本研究未列出所有 CVE 編號清單)

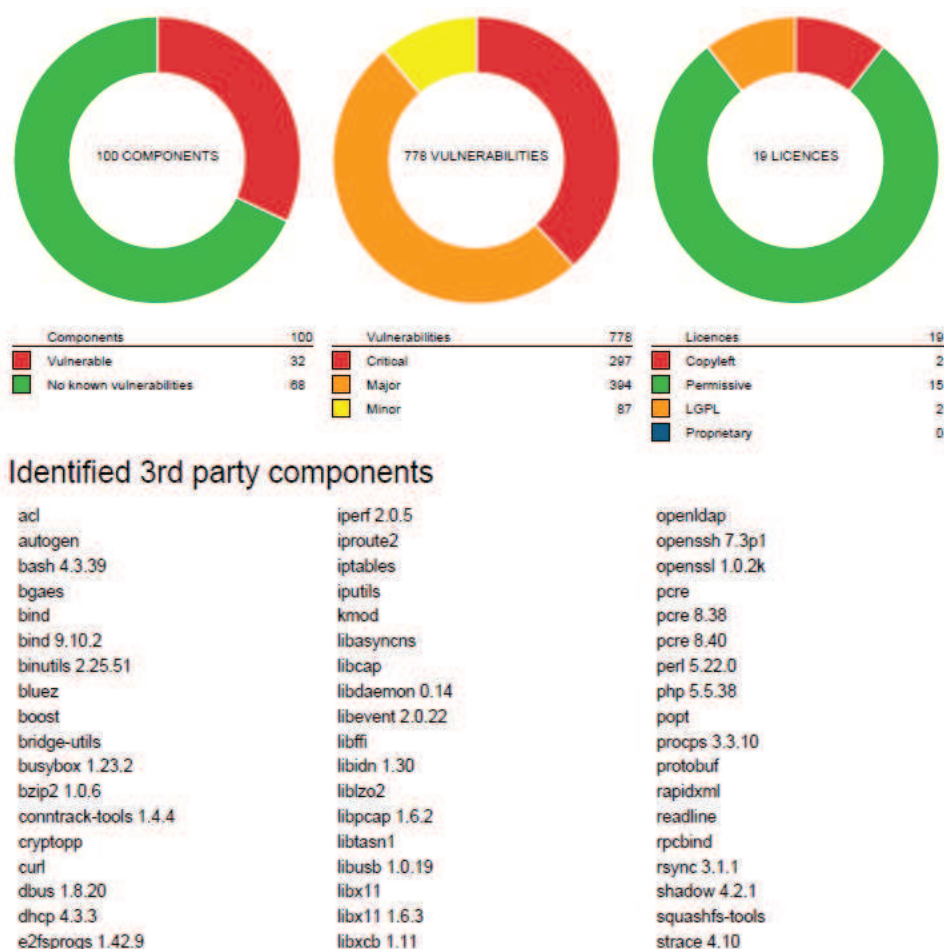


圖 5-138 A 廠牌基站軟體分析結果一覽

資料來源：本團隊整理

嵌入於硬體裝置中的軟體稱為韌體(Firmware)，是作為與電子裝置溝通的控制程式。韌體相同於一般的軟體，同樣存有資安弱點漏洞的威脅，多數類型的軟體缺陷(Defects)在程式碼的實作過程中產生，致使這些缺陷可能遭受駭客利用。

在現今，許多企業為加速產品上市速度，透過委外方式大量使用來自合作廠商的程式，而這些合作廠商又將軟體轉移到多個開發者手中，並大量套用第三方開放原始碼程式與套件，且越來越依賴合作廠商軟體或應用程式。然而，雖然企業本身確實存有安全的軟體開發流程，但是許多的軟體安全品質仍難以控管與評估，企業內軟體開發組織的管理結構將對軟體品質產生直接重要的影響。舉例在單一應用程式中就可能使用到數百個來自委外合作廠商與自由開源軟體程式與套件，多數類型的軟體安全缺

陷是在程式碼的實作過程中產生，這樣龐大的程式碼可能難以獲得相同級別之品質要求、安全檢查與測試要求。

LTE 基站功能日趨複雜，軟體內部的邏輯也變得異常複雜，軟體測試所耗費的資源甚至超過開發，但仍然無法確保排除所有安全漏洞。當前許多企業的軟體開發模式缺乏足夠的安全意識、安全設計與測試，從美國國家弱點資料庫(National Vulnerability Database, NVD)歷年來層出不窮的 CVE(Common Vulnerabilities and Exposures)漏洞與軟體開發商所發布的安全修補程式即是最好的證明。

本次測試之兩款廠牌基站軟體檔雖 CVE 漏洞數量甚高，但資安的考量不是只有單點，必須系統性的評估，包含與營運商、基站製造商，共同討論基站所處環境、提供之服務與設定功能，進而判斷這些 CVE 漏洞是否會影響基站的商用服務。

二、 家用基站(HeNB)資安檢測技術及項目研究

本節對於家用基站(Home Evolved Node B，簡稱 HeNB)提出資安檢試項目的規劃及檢測技術的研究，於檢測項目的規劃上，針對家用基站所面臨的資安威脅，從各個面向制定資安檢測項目，包括：敏感性資料保護檢測、身分認證安全檢測、軟體更新安全檢測、通訊協定安全檢測、實體層安全檢測，以確認家用基站是否潛藏資安漏洞。在檢測技術研究方面，透過對於家用基站的核心系統搭配系統監控模組，藉由分析監控模組的事件日誌，回饋作為資安檢測項目制定的依據及檢測技術的精進，同時可提供家用基站的動態行為監測與保護能力。

(一) HeNB 架構概述

家用基站(HeNB)於 LTE 中之系統架構同大基站，由核心網、家用基站(HeNB)和使用設備 3 個部分組成 EPS 系統，與核心網路之間也是透過 MME 接入(請參閱圖 5-139)，不僅如此，家用基站相關之通訊介面及通訊協定也完全與大基站一致，詳細的介紹詳見上一節基站資安檢測技術及項目研究。

無論是家用基站(HeNB)或大基站(eNodeB)，與後端核心網之間皆是透過網際網路和 IP 協定傳輸資料，然而家用基站在應用上是為了延伸室內傳輸範圍而建置於用戶家中，換句話說，這個透過網際網路傳送 LTE 訊息至核心網的過程，是透過用戶端

之數位用戶迴路(DSL)或光纖等寬頻連線，這介於家用基站與核心網路之間的環境，是無法令人信賴的。

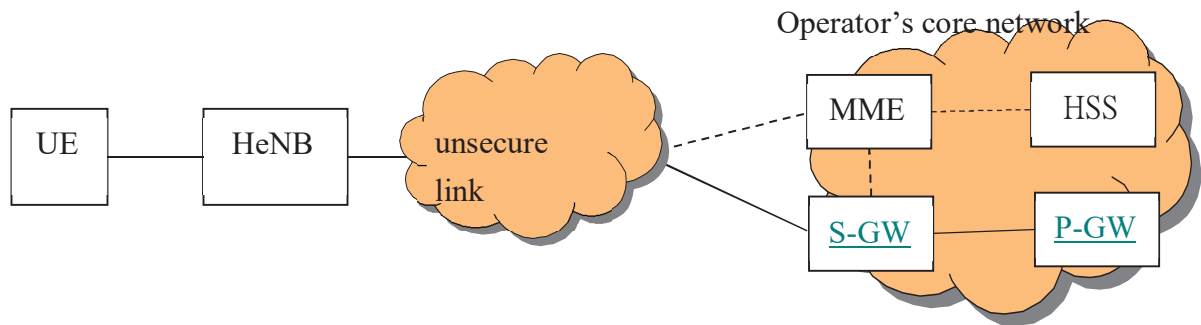


圖 5- 139 3GPP 之 HeNB 架構圖

資料來源：本團隊整理

(二) HeNB 資安威脅

4G LTE 透過 HeNB 來延伸室內通訊範圍，但也導致新的資安威脅發生，像是國際行動用戶辨識碼(IMEI)竊聽、蓋台、簡訊攔截、手機定位以及偽基站攻擊等，更影響了電信商的使用信心，本研究提出一個家用基站的自我防護機制，以防止駭客入侵控制家用基站，來達到防範偽冒合法基站攻擊，文中最後與現有 3GPP 的解決方案比較，並展示本機制對於 HeNB 防護的必要性。

電信網路(Telecommunication)一直是透過基站提供終端設備行動上網服務，然而基站的布建有其限制，像是土地成本、設備成本等，因此在延伸傳輸範圍的需求下，小基站(small cell)孕育而生，而小基站當中傳輸範圍最小且只為延伸室內傳輸範圍的 femtocell，在 LTE 世代正名為 Home eNB(HeNB)。HeNB 是設計為室內使用的小功率基地站，其發射功率為 10mW~100mW 與 WiFi 類似，主要透過 DSL、Cable 或光纖寬頻接入電信電信業者的網路。HeNB 可建置在一些收訊不佳的家中或辦公環境中，以改善室內通話品質及增進多媒體傳輸率，因此被視為能降低 4G LTE 佈建成本及改善 4G LTE 覆蓋率的重要解決方式。HeNB 有別於大型基地台，具備體積小、功耗少、成本低、建置便利性等先天優勢，勢必扮演 4G 服務的重要角色，然而也相對帶來新的資安威脅。

由於家用基站是為延伸住家的 LTE 訊號覆蓋範圍，換句話說，該機器是置於一般用戶家中，這說明家用基站的實體入侵風險是相當高的，後端與 EPC 介接的後置迴路(backhaul link)同樣是用戶家中的網路，這使得家用基站曝露在充斥著資安威脅的情境下(見圖 5-140)，這對於電信網路來說是個嚴重的威脅，偽造 (H)eNB 的問題也層出不窮。

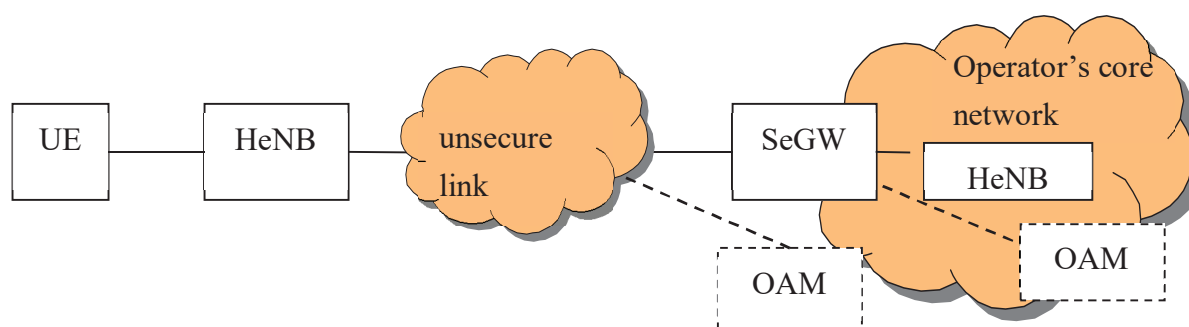


圖 5-140 3GPP 之 HeNB 安全架構

資料來源：3GPP TS 33.320

圖 5-27 顯示家用基站在 3GPP 的框架下，需倚靠安全閘道(SeGW)建立與後端核網的安全通道，與 HeNB 之間建議 IPsec VPN，為封包的傳輸提供隱密性和完整性保護並且支持 PKI 系統，接著再透過家用基站管理系統(HeMS)，對 HeNB 的身分識別及內建軟體的更新嚴格控管，降低家用基站所須面對的資安風險，HeMS 可同時控管多台基站，並透過 TR069 的協定進行相關認證、憑證發送、軟體更新…等。然而駭客還是有可能透過 HeNB 本身的漏洞(例如:管理介面、軟體設計等)入侵以達到控制的目的，因此本篇提出一個用於可即時察覺並阻止駭客植入 HeNB 的惡意程序發動攻擊，由於零時差攻擊使得 HeNB 隨時存在可能被入侵的風險，HeNB 需要能自我抵禦來自外部的攻擊，而不只是仰賴核心網路的保護。

3GPP TR 33.820³⁰⁹將家用基站所面臨的資安問題一一指出，本篇將該文件指出的

³⁰⁹ 3GPP. Technical Specification Group Services and System Aspects; Security of H(e)NB; Release 8, TR 33.820.

資安威脅整理出 7 個面向，說明如下：

- (1) HeNB 實體攻擊：是指攻擊者透過修改或替換 HeNB 組件的一種攻擊方式，這種方式對終端用戶和網路都可能造成影響，在無線網路端，一個天線組件被修改過的家用基站會對周圍區域的小型機站服務範圍造成干擾，這部分需要利用可信任的模組區塊保護 HeNB 啟動的過程。
- (2) HeNB 憑證攻擊：是指攻擊者獲取 HeNB 的憑證並進行惡意利用，在此類攻擊中，攻擊者從目標家用基站獲取一份授權憑證副本，並對終端用戶和核心網路發起假冒的攻擊，家用基站的授權憑證應該儲存在一個受保護的信任區域。
- (3) HeNB 配置攻擊：是對家用基站的 CSG 列表進行錯誤的修改，攻擊者會先進入 CSG 列表並修改，讓非法使用者連進相關網路設備，另外，攻擊者還可以修改 CSG 列表禁止合法用戶接入網路，造成合法用戶被阻斷服務，非法用戶可以使用。因此保障 CSG 列表的建立、維護、儲存是非常重要的。
- (5) HeNB 協定攻擊：包含了第一次 S1AP 註冊時的攻擊，可能會對用戶產生非常有害的影響。當家用基站沒有擁有唯一的資格認證時，是非常難以抵擋此類攻擊。此時，當目標家用基站首次與核網建立連接時，網管中心無法辨識家用基站是否遭受攻擊。如此，來自網路上的攻擊者可以竊聽來自家用基站所有的流量獲取敏感訊息，並且進一步利用。
- (6) 核心網路攻擊：是透過已被攻擊的 HeNB 產生惡意流量繼續向核心網路發起 DoS 攻擊。兩種直接向核網發起的 DoS 攻擊包括：IKEv2 攻擊和家用基站的位置攻擊。IKEv2 攻擊，如：IKE_SA_INIT 攻擊和 IKE_AUTH 攻擊，可以攻擊 HeNB 和安全開道之間 IKEv2 通道的初始建立過程。家用基站的位置攻擊，改變家用基站的位置但是不回報給核網，攻擊者可以重新設定家用基站的位置，使之前已經提供的位置資料失效。
- (7) 用戶資料和身分隱私攻擊：是藉由竊聽其他 E-UTRAN 用戶的資料對用戶產生嚴重威脅的攻擊。攻擊者可以自己建立一個家用基站，並設置成開放的模式讓用戶都能連線，這樣會造成目標用戶在不知情的狀況下通過該惡意家用基站連接到核心網路。如此一來攻擊者可以竊聽用戶對網路連接的所有訊息。
- (8) 無線資源管理攻擊：是當 HeNB 提供錯誤的無線資源訊號，干擾其他裝置。為

了攻擊無線資源管理，惡意的攻擊者可以接入家用基站並對其天線參數部分進行修改，能修改家用基站的功率控制部分。

上述有 1/4 的資安威脅都將衍生偽基站攻擊，主要起因是家用基站內的 4G 相關認證資料(如:Authentication token、eNB ID 等)外洩所引發的，而對於 HeNB 而言外洩之管道無所不在，backhaul link 竊聽、遠端入侵及 physical intrusion 等都有可能取得。而且如假冒的軟體更新、防火牆的錯誤設置甚至 HeNB 本身的錯誤設定檔設置都會對 HeNB 的服務造成阻斷，這些威脅應該要有方式去預防。

此外，3GPP TS33.320 中提出 HeNB 子系統的安全架構，說明整個子系統應具備的安全設備(如:SeGW、HeMS 等)及安全功能(如:IPsec、EAP-AKA 等)，然而由於電信網路相當仰賴通訊效能，實際上電信商多半不願意為了犧牲效能以換取安全性。因此 Lai³¹⁰ 提出家用基站與核網之間的重認證協定，此認證協定不但可以降低傳輸資源消耗(communication cost)、功率資源消耗(energy cost)、計算資源消耗(computation cost)，使現行的安全解決方案更加實際可用於電信網路。此外，Han³¹¹ 發現雖然 3GPP 在後端鏈路有強健的認證機制，但在 UE 與 HeNB 之間卻是有機可乘，因此提出介於 UE 與 HeNB 之間強化版的認證機制，以防止偽造 HeNB 的攻擊。

本團隊也將上述攻擊面向歸類為以下家用基站(HeNB)所面臨的六大資安威脅面向(如表 5-8)，包括：敏感性資料外洩、身分認證安全檢測、軟體更新安全檢測、通訊協定安全檢測、系統安全檢測、實體層安全檢測，作為後續檢測項目制定之依據。

表 5-8 家用基站(HeNB)之資安威脅

威脅面向	安全威脅
敏感性資料	1. 用戶清單包括存取控制清單(ACL)及 CSG ID，在 LTE 時代，多半的家用基站已經不包含 ACL，而 CSG ID 可被利用在偽基站的攻擊上，導致 UE 在家用基站進行換手時連上偽基站。 2. 4G 設定檔若被拿去使用，同樣會可以利用在偽基站攻擊，

³¹⁰ Chengzhe Lai, Hui Li, Yueyu Zhang, Jin Cao, "Simple and low-cost re-authentication protocol for HeNB," China Communications, Vol.10, No.1, pp.105-115, 2013.

³¹¹ Chan-Kyu Han, Hyoun-Kee Choi, In-Hwan Kim, Building femtocell more secure with improved proxy signature. In: Global Telecommunications Conference, pp. 1-6 (2009) 8.

威脅面向	安全威脅
	可能會發生蓋台、或是 UE 在不知情的狀況下誤連，攻擊者就可以竊聽到所有來自 UE 端的資料流量。 3. 本機的系統日誌是紀錄系統相關變化的檔案，可以用來分析系統是否有異常的行為發生，如果遭到竄改會無法察覺異常情況的發生。 4. 設備的帳號密碼檔案，如果是明文儲存，可能會導致整個設備的控制權將會被攻擊者使用。
身分認證機制	1. 在各種偽基站攻擊中，有種攻擊方式是側錄合法基站和核網註冊過程時的封包，之後將這段封包進行重送攻擊，導致偽基站成功被核網所接受。 2. 家用基站的管理介面在應使用支援安全認證的方式，如未使用安全的認證方式可能會在登入時被截取到帳號密碼。 3. 家用基站和核網認證時使用的憑證，如果不具唯一性會有被攻擊者使用其複製的憑證向核網註冊的風險。
韌體更新	1. 家用基站更新之後，相關安全參數被錯誤設置，造成服務無法正常提供之外，還可能會因為這段空窗期造成控制權或是資料的外洩。 2. 韌體更新檔的簽章是能夠辨識該更新檔是否合法，以避免安裝到含有惡意程式碼的更新檔，造成家用基站曝露在高風險之下。 3. 受測物的更新檔案必須是加密狀態，以避免被攻擊者得到檔案進行反組譯，從中解析家用基站韌體進而找出漏洞。
通訊協定	1. 家用基站的後端鏈路如果是明文傳輸的話，將會對用戶端所傳送的資料造成風險，攻擊者可以透過中間人攻擊或是竊聽的方式取得封包。 2. 許多設備首次連網時，會有明文傳輸的現象，這將造成認證資訊在這個階段外洩，這是常見的認證機制漏洞。
系統安全	1. 設備的系統和所開啟的網路服務埠，如果存在已知的資安漏洞，很可能被駭客透過已經公開的攻擊手法或攻擊程式，造成傷害。 2. 設備的開機程序需要保護，避免開機過程中，執行含有惡意原始碼之程序被執行。

威脅面向	安全威脅
	3. 網頁管理介面是駭客常用來入侵的介面，常存在高風險漏洞，導致設備的資料庫會比其他敏感資料外洩。 4. 日誌資料是分析異常行為的重要依據，若其可用性無法確保，將無法提早預防傷害或者是防止更嚴重的傷害發生。
實體層	1. 家用基站與大型基站不同，實體破壞而導致的實體入侵在所難免，導致駭客透過實體入侵拿到裝置的系統管理者權限。 2. 家用基站的實體憑證，若可以被任意插拔，將會被惡意使用者作為偽基站攻擊之用。

資料來源：本團隊整理

（三）HeNB 資安檢測項目研究及測試結果

透過上述家用基站(HeNB)所面臨之資安威脅分析，本節將根據資安威脅所設計之測試項目如下表 5-9。

表 5-9 家用基站(HeNB)檢測項目研究

檢測項目	編號	檢測案例	CIA
1. 敏感性資料保護	1-1	用戶清單的存取控管	完整性
	1-2	4G 設定檔的存取控管	完整性
	1-3	系統日誌的存取控管	完整性
	1-4	密碼的儲存保護	機密性
2. 身分認證安全	2-1	認證方式需要足夠強度	完整性
	2-2	遠端管理介面的認證安全	機密性
	2-3	憑證具唯一性	完整性
3. 韌體更新安全	3-1	更新後安全參數的設置錯誤	可用性
	3-2	韌體簽章驗證功能	完整性
	3-3	韌體更新檔案的加密	機密性
4. 通訊安全	4-1	後端接取鏈路的傳輸保護	機密性
	4-2	首次連結核網的傳輸保護	機密性
5. 作業系統安全	5-1	作業系統及網路服務安全	機密性、完整性、可用性
	5-2	系統開機程序於應用層的保護	完整性
	5-3	網頁管理介面的安全	機密性、完整性、可用性
	5-4	日誌檔保存期限	可用性
	5-5	日誌檔無法儲存的警示機制	可用性
6. 實體層安全	6-1	家用基站的整機保護	完整性
	6-2	硬體憑證的設計	完整性

資料來源：本團隊整理

1. 敏感性資料保護

資料保護安全測試是為確認產品設計上，是否確保敏感性資料無論是在傳輸或儲存時，都具有外洩防堵的能力，包括敏感性資料存取控管、加解密演算法等，通過此節的資安測試，可確保產品具備防止敏感性資料外洩能力。

1-1. 用戶清單的存取控管

測試案例	用戶清單的存取控管
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 用戶清單的機敏資訊需妥善控管。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將檢測用筆電接上受測物。 2. 檢測受測物內對於用戶清單的機敏資訊是否有被權限控管。	
合格判定標準： 用戶清單的機敏資訊不可被未授權使用者存取。	
測試說明： 檢測受測物的敏感資訊檔案，受測物必須具備二種以上不同權限之角色，測試時以不同權限之角色存取用戶清單，該用戶清單不可被未授權使用者存取，實測時另須搭配廠商自我宣告各角色之權限，方可判斷用戶清單是否有存取控制功能。	

測試結果：

下圖顯示 HeNB 之用戶清單，必須透過系統管理者權限於作業系統層級檢視儲存於家用基站(HeNB)之用戶清單(如: CSG)，確實用戶清單中設有啟動 CSG ID 之設定，配合 UE 端對可接受 CSG ID 的存取達到存取控制的目的。

```

configure cell pwr u16phichpoweramp 0 2667
configure cell pwr u16pbchpoweramp 0 2667
configure cell pwr u16pdcchpoweramp 0 2667
configure cell edlrschblock 0 4
configure cell phich ephichduration 0 0
configure cell phich ephichresource 0 1
configure cell access u16trackingareacode 0 10000
configure cell access u32ce/ tracjng
llidentity 0 25600
configure cell access ecellbarred 0 1
configure cell access eintrafregrselection 0 1
configure cell access bcsqindication 0 0
configure cell access u32csgidentity 0 0
configure cell access ecellreservd 0 1
configure cell selection s8qrxlevmin 0 -65
configure cell selection bqrxlevminoffset 0 0
configure cell selection u8qrxlevminoffset 0 2
configure cell bpmax 0 0
configure cell s8pmax 0 23
configure cell u8freqbandindicator 0 3
configure cell u8numsi 0 1
configure cell sched esipericodicity 0 0 0
configure cell sched u8numsi bmappinginfo 0 0 0
- startup.cfg 65/916 7%

```

圖 5- 141 存取控制清單截圖

資料來源：本團隊整理

1-2. 4G 設定檔的存取控管

測試案例	4G 設定檔的存取控管
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 4G 設定檔需妥善控管。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將檢測用筆電接上受測物。 2. 檢測受測物內對於 4G 設定檔的機敏資訊是否有被權限控管。	
合格判定標準：	

測試案例	4G 設定檔的存取控管
4G 設定檔的機敏資訊不可被未授權使用者存取。	
測試說明： 檢測受測物的敏感資訊檔案是否有控管其存取權限，受測物必須具備二種以上不同權限之角色，測試時以不同權限之角色存取 4G 設定檔，該 4G 設定檔不可被未授權使用者存取，實測時另須搭配廠商自我宣告各角色之權限，方可判斷用戶清單是否有存取控制功能。使用低權限使用者存取受測物的 4G 設定檔，結果應不可存取。	

測試結果：

下圖之測試結果表示受測物之 4G 設定檔資料為可讀，且由於此受測物只有一種權限角色(系統管理權限)之使用者，故只要能登入受測物之作業系統層，即可存取受測物之 4G 設定檔。

```

configure eqt gen u32enbid 25600
configure eqt gen u8enbnamelength 20
configure eqt gen szenbname Cavium LTE Femto eNB
configure eqt gen eantenna 1
configure eqt gen u8numplmnidentity 1
configure eqt gen plmnidentity mcc 0 3 4 4 0
configure eqt gen plmnidentity mnc 0 2 2 0
configure eqt gen bpmcontract 0
configure eqt board eadminstate 0 1
configure eqt board eadminstate 1 1
configure eqt board eadminstate 2 1
configure eqt board eadminstate 3 1
configure eqt board eadminstate 4 1
configure eqt board eadminstate 5 1
configure eqt board eadminstate 6 1
configure eqt board eadminstate 7 1
configure eqt board eadminstate 8 1
configure eqt board eadminstate 9 1
configure net net u32enbipaddress 192.168.7.44
configure net net u32enbsubnetmask 255.255.255.0
configure net net u32enbgwipaddress 255.255.255.0
configure net u8nummeinterface 1
configure net mme u32mmeipaddress 0 192.168.7.77
configure net mme u16mmesctpportnumber 0 36412

```

4G設定檔含PLMN
本機IP、核網IP

圖 5- 142 4G 設定檔截圖

資料來源：本團隊整理

1-3. 系統日誌的存取控管

測試案例	系統日誌的存取控管
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 本機系統的日誌不可被未授權使用者存取。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將檢測用筆電接上受測物。 2. 檢測受測物內對於系統日誌檔是否有被權限控管。	
合格判定標準： 本機系統的日誌不可被未授權使用者存取。	
測試說明： 檢測受測物的敏感資訊檔案，受測物必須具備二種以上不同權限之角色，測試時以不同權限之角色存取系統日誌，該系統日誌不可被未授權使用者存取，實測時另須搭配廠商自我宣告各角色之權限，且廠商須提供相關日誌的存取，檢測未授權使用者是否可以存取，未授權使用者存取的結果應為失敗。	

測試結果：

下圖為受測物之日誌檔的權限，由於此受測物只有一種權限角色(系統管理權限)之使用者，故只要能登入受測物之作業系統層，即可存取受測物之所有系統日誌。


```

/var/log # date
Fri Jan 2 00:02:51 PST 1970
/var/log # ls -l
-rw-r--r-- 1 root root 43828 Jan 2 00:02 core0
-rw-r--r-- 1 root root 97522 Jan 2 00:00 core2
-rw-r--r-- 1 root root 545 Jan 2 00:02 messages
-rw-r--r-- 1 root root 0 Jan 2 00:00 mini_httpd.log
/var/log # █

```

圖 5-143 系統日誌檔截圖

資料來源：本團隊整理

1-4. 密碼的儲存保護

測試案例	密碼的儲存保護
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 本機系統的密碼不可被未授權使用者存取，且不可明文儲存。	
資訊安全需求： ☒ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將檢測用筆電接上受測物。 2. 檢測受測物內對於密碼檔是否有被權限控管。 3. 開啟密碼檔案，檢視密碼資料是否經由 one-way hash 處理過。	
合格判定標準： 本機系統的密碼檔不可被未授權使用者存取且經由 one-way hash 處理過。	
測試說明： 此測項受測廠商須提供測試人員系統管理者權限，並提供系統密碼檔存放位置，檢測人員瀏覽本機系統密碼檔案時，瀏覽其密碼部份是否為明文儲存。	

測試結果：

如下圖密碼經過單向雜湊函數處理，其結果為非明文儲存，然而雜湊函數也並非全然安全，例如: MD5 已經遭到破解，建議參照 FIPS 140-2 Annex A 所建議的安全演算法來要求。

```
root:$1$vED/gSpA$n021mKUS4d94qQA/bT0U20:10933:0:99999:7:::
bin:*:10933:0:99999:7:::
daemon:*:10933:0:99999:7:::
adm:*:10933:0:99999:7:::
lp:*:10933:0:99999:7:::
sync:*:10933:0:99999:7:::
shutdown:*:10933:0:99999:7:::
halt:*:10933:0:99999:7:::
uucp:*:10933:0:99999:7:::
operator:*:10933:0:99999:7:::
ftp:*:10933:0:99999:7:::
nobody:*:10933:0:99999:7:::
default::10933:0:99999:7:::
```

圖 5- 144 密碼資料截圖

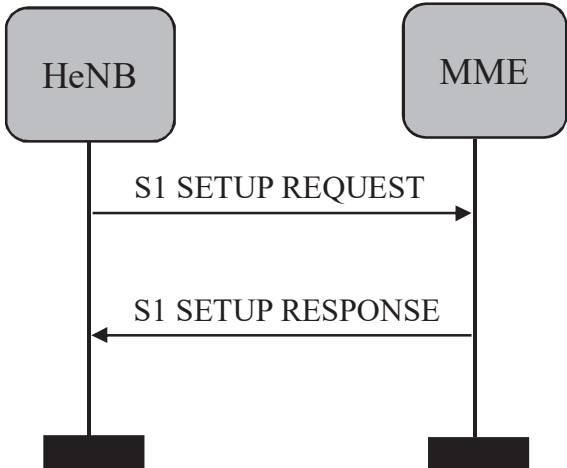
資料來源：本團隊整理

2. 身分認證安全檢測

身分鑑別與授權資安測試是為確認產品設計上，身分鑑別與授權機制之強度，包括權限控管、通行碼機制複雜度、身分鑑別機制強度等，通過此節的資安測試，可確保產品具備堅實之身分鑑別與授權機制。

2-1. 認證強度要求

測試案例	認證強度要求
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物與核網之間的認證要避免重送攻擊。 資訊安全需求：	

測試案例	認證強度要求
☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 受測 HeNB 與 MME 建立 S1 介面之連線。 2. 測試筆電開啟 sniffer 監聽 S1 介面上之封包。  <pre> sequenceDiagram participant HeNB participant MME HeNB->>MME: S1 SETUP REQUEST MME-->>HeNB: S1 SETUP RESPONSE </pre>	
測試方法： 1. 將受測物連上網路集線器 2. 確認受測物是否可以連上後端網路 3. 筆電連上網路集線器，並測錄受測物封包。 4. 使用工具對核網進行重送攻擊。	
合格判定標準： 受測物須能抵禦重送攻擊。	
測試說明： 受測物與核網之間因為認證用之因子為固定，且核網與受測物之間資料的傳送是經由網際網路，可能遭受重送攻擊的威脅，因此有些電信商透過專線來保護這段經由網際網路的傳輸，然而無法佈建專線的電信商則必須依靠受測物的安全功	

測試案例	認證強度要求
能，例如 3GPP 所規定的 IPsec 安全通道；由於 IPsec 有防止重送攻擊的能力，且又是必備之功能，因此本測項驗測重點應該要測試受測物的 IPsec 功能是否正常啟動。	

測試結果：

下圖為受測產品試測後，確認 S1 介面的 IPsec 功能有正常啟動。

No.	Time	Source	Destination	Protocol	Length	Info
1398	183.812553000	103.231.48.193	192.168.30.15	ISAKMP	378	IKE_SA_INIT MID=00 Initiator Request
1399	183.822372000	192.168.30.15	103.231.48.193	ISAKMP	359	IKE_SA_INIT MID=00 Responder Response
1400	183.900007000	103.231.48.193	192.168.30.15	ISAKMP	1466	IKE_AUTH MID=01 Initiator Request
1401	183.984509000	192.168.30.15	103.231.48.193	ISAKMP	1342	IKE_AUTH MID=01 Responder Response
1402	184.499944000	fe80::b252:16ff:fe2...	ff02::2	ICMPv6	70	Router Solicitation from b0:52:16:20:77:c2
1403	184.668109000	103.231.48.193	192.168.30.15	ESP	158	ESP (SPI=0x0500aa30)
1404	184.673706000	192.168.30.15	103.231.48.193	ESP	162	ESP (SPI=0xcb727e0c)
1405	184.868464000	103.231.48.193	192.168.30.15	ESP	158	ESP (SPI=0x0500aa30)

0... = Critical Bit: Not Critical
Payload length: 12
Transform Type: Encryption Algorithm (ENCR) (1)
Transform ID (ENCR): ENCR_AES_CBC (12)
▼ Transform IKE2 Attribute Type (t=14,l=2) Key-Length : 128
1... = Transform IKE2 Format: Type/Value (TV)
Transform IKE2 Attribute Type: Key-Length (14)
Value: 0000
Key Length: 128

圖 5-145 後端鏈路傳輸通道截圖

資料來源：本團隊整理

2-2. 遠端管理介面的認證安全

測試案例	遠端管理介面的認證安全
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物的管理介面需支援安全的認證方式。 資訊安全需求： ☒機密性(Confidentiality) ☐完整性(Integrity) ☐可用性(Availability)	

測試案例	遠端管理介面的認證安全
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將受測物連上網路集線器。 2. 確認受測物是否可以連上後端網路。 3. 筆電連上網路集線器。 4. 檢視受測物的管理介面是否有支援安全的認證方式。	
合格判定標準： 遠端存取受測物之身分認證機制，必須使用安全通道(secure tunnel)。	
測試說明： 執行本測項時受測廠商須提供遠端管理的登入方式，根據該方式執行遠端登入並側錄封包，驗證此段網路傳輸是否為明文。	

測試結果：

下圖是使用 telnet 協定進行遠端管理登入，因透過此協定所傳輸的資料皆為明文，包括帳號與密碼，是相當不安全的重大缺失。

```

root@kali:~/Desktop# telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.68.7.MAC Address:
Escape character is '^]'.
femto login: root
root@kali:~#
[root@femto ~]#

```

圖 5-146 遠端管理登入介面截圖

資料來源：本團隊整理

2-3. 憑證具唯一性

測試案例	憑證具唯一性
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物與核網認證時的憑證需要具有唯一性。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。 2. 受測 HeNB 與 MME 建立 S1 介面之連線。 3. 測試筆電開啟 sniffer 監聽 S1 介面上之封包。	
測試方法： 1. 將受測物連上網路集線器 2. 確認受測物是否可以連上後端網路 3. 筆電連上網路集線器，側錄封包。	

測試案例	憑證具唯一性
4. 檢測受測物除了憑證之外，是否有其他因素可以讓核網辨識。	
合格判定標準： 受測物與核網認證時的憑證需要具有唯一性。	
測試說明： 監聽 S1 介面並擷取受測物之憑證，或者是要求受測廠商提供系統管理者權限之帳號並宣告存放位置，以提取憑證，抽測任兩台待測物憑證的 fingerprint 比較，只要 fingerprint 是相異，那麼憑證必定相異，此測項需要廠商配合送驗 2 台相同設備。	

測試結果：

下圖顯示，透過 openssl 所提供的指令，擷取憑證的 fingerprint，結果說明任二個相異憑證的 fingerprint 是相異的。

```

root@kali:/home/ahwan# openssl x509 -noout -fingerprint -sha256 -inform pem -in rootCA.pem
SHA256 Fingerprint=EB:F2:A9:6D:C9:60:53:24:F5:17:8B:CC:86:FE:89:2C:5D:64:6E:FB:DB:85:EE:D2:25:41:AF:FF:8C:59:E9:35
root@kali:/home/ahwan# openssl x509 -noout -fingerprint -sha256 -inform pem -in HNB.pem
SHA256 Fingerprint=71:1E:FE:1B:0C:D2:6E:60:B5:D5:08:E4:FB:B0:B1:26:38:B7:3F:C3:3E:D1:33:50:43:0D:EC:3E:48:F8:F1:74

```

圖 5- 147 憑證唯一性截圖

資料來源：本團隊整理

3. 韌體更新安全檢測

確認 HeNB 在內建軟/韌體的更新上，無論是在更新階段抑或韌體檔案本身是否有足夠的安全保護機制，及是否存在敏感性資料外洩之疑慮。

3-1. 更新後安全參數的設置錯誤

測試案例	更新後安全參數的設置錯誤
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 更新後的受測物安全參數設置需與更新前相同。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將受測物連上網路集線器。 2. 將受測物連上核網，並確定功能正常。 3. 對受測物進行更新，並等待更新完畢。 4. 更新完成後檢測受測物的參數是否正常。	
合格判定標準： 受測物更新後，安全參數需與更新前相同，且能正常運行。	
測試說明： 此測項需要廠商配合觸發更新，並由受測廠商告知相關安全參數(例如：逾時限制)存放位置，檢視更新前後相關安全參數是否相同，更新後與後端核網是否能正常建立連線並正常運作。	

測試結果:

下圖顯示之測試結果，說明試測時無法順利觸發更新，因此此測項需要受測廠商協助觸發更新。

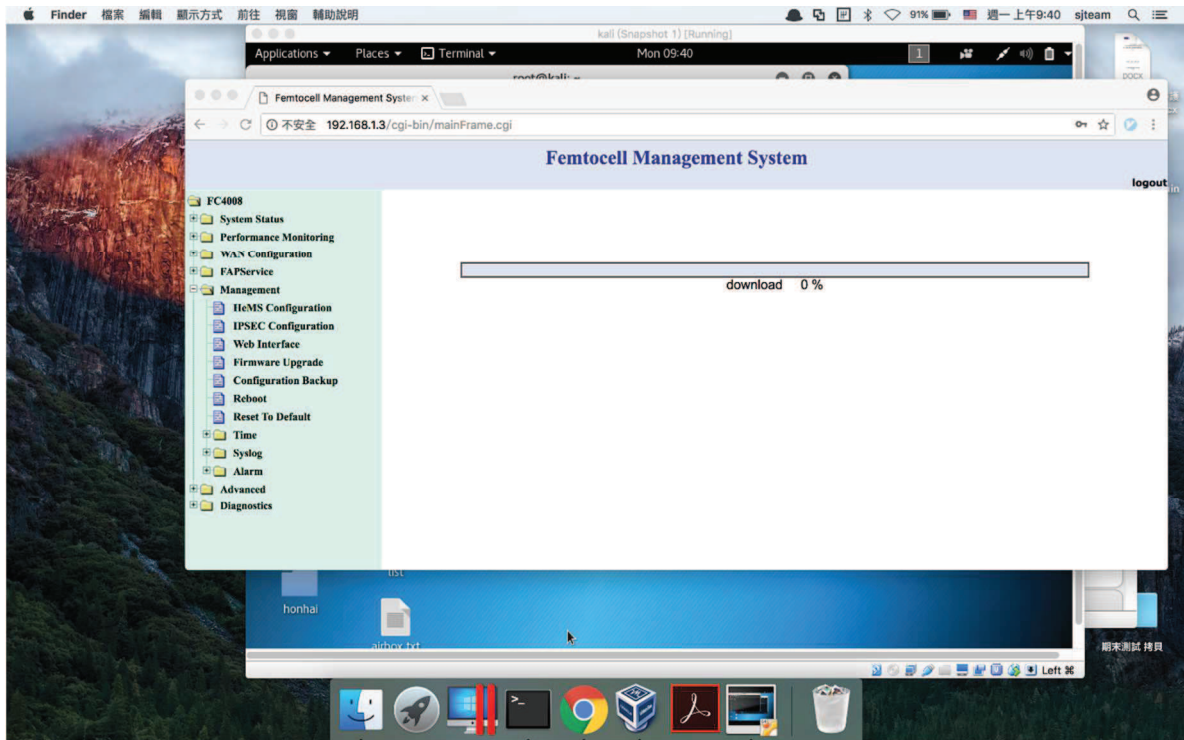


圖 5- 148 系統更新截圖

資料來源：本團隊整理

3-2. 韌體簽章驗證功能

測試案例	韌體簽章驗證功能
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 產品必須具備驗證韌體的正确性及完整性之功能。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將已簽章之二位元韌體檔案竄改。	

測試案例	韌體簽章驗證功能
2. 開啟韌體更新頁面。 3. 測試竄改過後的韌體檔案可否被成功更新。 4. 將已簽章之韌體檔案再簽章一次。 5. 測試再簽章的韌體檔案可否被成功更新。	
合格判定標準： 經過竄改之簽章韌體檔案無法被成功更新，則本測試項目結果為通過。 經過再次簽章之韌體檔案無法被成功更新，則本測試項目結果為通過。	
測試說明： 受測廠商需提供韌體檔案，測試人員對韌體檔案進行簽章，此簽章無論是使用自簽還是經由可信根憑證機構所發佈的憑證，在經由測試人員自行簽章後的韌體檔案不可被成功更新。	

測試結果：

由上圖 5-148 結果可看出，重新簽章後更新無法成功，更新進度永遠停留在 0 的位置。

3-3. 韌體更新檔案的加密

測試案例	韌體更新檔案的加密
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物的韌體更新檔必須是加密的狀態。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法：	

測試案例	韌體更新檔案的加密
1. 將檢測用筆電連上受測物。 2. 檢測受測物的更新檔案是否加密。	
合格判定標準： 受測物的韌體更新檔必須是加密的狀態。	
測試說明： 此測項需要廠商提供韌體檔案，並使用具韌體拆解功能之檢測工具進行解包，若韌體經可靠之演算法加密處理後，其結果應不能被解包成功。	

測試結果：

下圖即是韌體未加密被成功拆解之結果，可看到韌體拆解的執行過程，以及拆解後檔案系統都被解析出來。

```
root@kali:~/Desktop/bts_sw# binwalk -e TLF-K2-L1ExL2DSP_1867686.BIN
DECIMAL      TL17A_  HEXADECIMAL      DESCRIPTION      TLF17A_...  TLF17A_E...  T1927262...
-----
152064      0x25200      Zlib compressed data, best compression
175616      0x2AE00      Zlib compressed data, best compression
212992      TLF-  0x34000      TLF-K2-  Zlib compressed data, best compression
310784      L1ExL2  0x4BE00      L2DSP_  Zlib compressed data, best compression
349184      _18676  0x55400      867686.  Zlib compressed data, best compression
353280      BIN  0x56400      BIN.  Zlib compressed data, best compression
353792      0x56600      Zlib compressed data, best compression
1031680      extracted  0xFBE00      extracted  Zlib compressed data, best compression
1085952      0x109200      Zlib compressed data, best compression
1086464      0x109400      Zlib compressed data, best compression
1139712      0x116400      Zlib compressed data, best compression
1141248      0x116A00      Zlib compressed data, best compression
1492992      0x16C800      Zlib compressed data, best compression
1497600      0x16DA00      Zlib compressed data, best compression
1536000      0x177000      Zlib compressed data, best compression
1718272      0x1A2000      Zlib compressed data, best compression
```

圖 5- 149 韌體拆解過程截圖

資料來源：本團隊整理

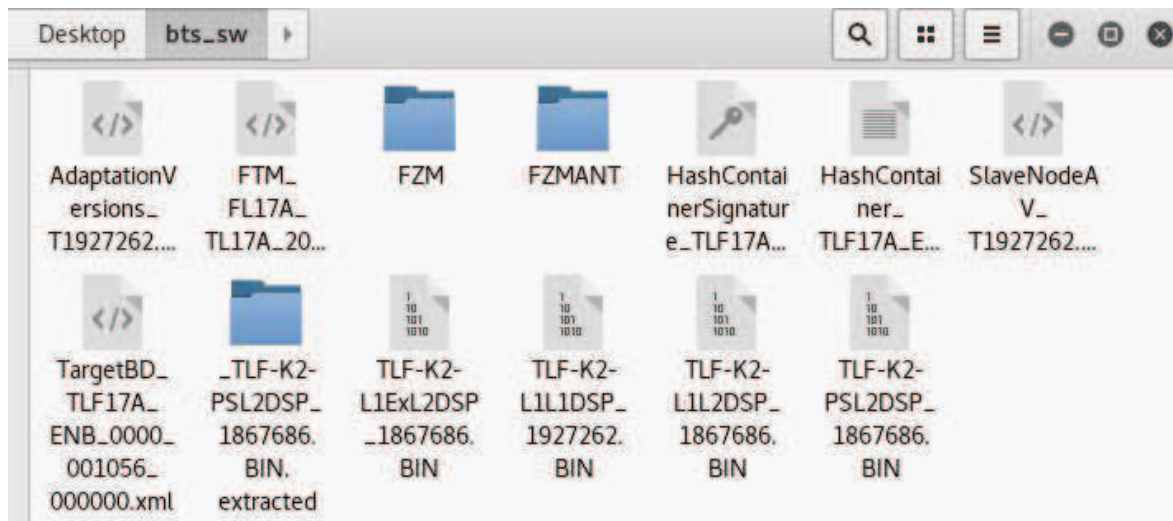


圖 5- 150 韌體拆解後所顯示出之檔案系統截圖

資料來源：本團隊整理

4. 通訊安全

通訊安全測試是為確認產品設計上，是否符合通訊傳輸介面的安全要求，包括網路服務啟用限制、空中介面通訊安全、傳輸加密技術要求等，通過此節的資安測試，可確保產品具備可靠之通訊傳輸功能。

4-1. 後端接取鏈路的傳輸保護

測試案例	後端接取鏈路的傳輸保護
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物與後端接取鏈路之間所傳送的資料，不可為明文傳輸、或透過中間人攻擊取得。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 受測 HeNB 與 MME 建立 S1 介面之連線。	

測試案例	後端接取鏈路的傳輸保護
2. 測試筆電開啟 sniffer 監聽 S1 介面上之封包。	
測試方法： 1.將受測物連接上核心網路。 2.側錄受測物於後端接取鏈路上傳送的封包，可利用 wireshark 等封包側錄軟體執行。 3.檢測所側錄的封包資訊。	
合格判定標準： 受測物與核心網路的 S1 介面，支援安全通道傳輸。	
測試說明： 後端鏈路即是指家用基站與核網之間的 S1 介面是否有提供傳輸通道的安全保護，側錄受測物的網路傳輸過程，並確認其使用的加密演算法、安全協定名稱與版本。實際上，受測物在互通性(interoperability)測試時即必須驗證 IPSec 功能，IPSec 對於傳輸在後端鏈路上的資料所提供的機密性強度是相當足夠的，因此只要符合互通性測試之家用基站，此測項相對也會是通過的。	

測試結果：

下圖顯示後端鏈路是具有 IPSec 通道加密的，因此通道中所有封包都被 ESP 封裝，不被顯示出來。

1398	183.812553000	192.168.30.15	103.231.48.193	ISAKMP	378 IKE_SA_INIT MID=00 Initiator Request
1399	183.822372000	103.231.48.193	192.168.30.15	ISAKMP	359 IKE_SA_INIT MID=00 Responder Response
1400	183.900007000	192.168.30.15	103.231.48.193	ISAKMP	1466 IKE_AUTH MID=01 Initiator Request
1401	183.984509000	103.231.48.193	192.168.30.15	ISAKMP	1342 IKE_AUTH MID=01 Responder Response
1402	184.499944000	fe80::b252:16ff:fe2...	ff02::2	ICMPv6	70 Router Solicitation from b0:52:16:20:77:c2
1403	184.668109000	192.168.30.15	103.231.48.193	ESP	158 ESP (SPI=0x0500aa30)
1404	184.673706000	103.231.48.193	192.168.30.15	ESP	162 ESP (SPI=0xcb727e0c)
1405	184.868464000	192.168.30.15	103.231.48.193	ESP	158 ESP (SPI=0x0500aa30)

0...		= Critical Bit: Not Critical
Payload length: 12		
Transform Type: Encryption Algorithm (ENCR) (1)		
Transform ID (ENCR): ENCR_AES_CBC (12)		
▼ Transform IKE2 Attribute Type (t=14,l=2) Key-Length : 128		
1...		= Transform IKE2 Format: Type/Value (TV)
Transform IKE2 Attribute Type: Key-Length (14)		
Value: 0000		
Key Length: 128		

圖 5- 151 後端鏈路之封包側錄截圖

資料來源：本團隊整理

4-2. 首次連上核網之認證安全

測試案例	首次連上核網之認證安全
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 首次連結上核網於 S1 介面所傳送的認證因子應加密保護。	
資訊安全需求： ☒ 機密性(Confidentiality) ☐ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 1. 受測 HeNB 與 MME 建立 S1 介面之連線。 2. 測試筆電開啟 sniffer 監聽 S1 介面上之封包。	
測試方法： 1.將受測物連接上核心網路。 2.側錄受測物於首次連上核網時傳送的訊息(S1 SETUP REQUEST)，可利用 wireshark 等封包側錄軟體執行。	

測試案例	首次連上核網之認證安全
3.檢測所側錄的封包資訊	
合格判定標準：	
受測物與核心網路於 S1 訊息交握前，即必須啟動安全通道。	
測試說明：	
此測項是為驗證受測物所啟用之安全通道時機，除上一測項是為確認受測物是否支援 IPSec 安全通道，此一測項是為了確保安全通道從連線建立後，搶在認證之前即率先建立，因此實測方式採用側錄受測物的網路傳輸過程，是否會洩露認證資料。	

測試結果：

下圖可看到從 HeNB 連上核網後，沒側錄到任何一個 S1 封包，即表示此 HeNB 從一連上核網後即率先建立了安全通道。

1398	183.812553000	192.168.30.15	103.231.48.193	ISAKMP	378	IKE_SA_INIT MID=00 Initiator Request
1399	183.822372000	103.231.48.193	192.168.30.15	ISAKMP	359	IKE_SA_INIT MID=00 Responder Response
1400	183.900007000	192.168.30.15	103.231.48.193	ISAKMP	1466	IKE_AUTH MID=01 Initiator Request
1401	183.984509000	103.231.48.193	192.168.30.15	ISAKMP	1342	IKE_AUTH MID=01 Responder Response
1402	184.499944000	fe80::b252:16ff:fe2...	ff02::2	ICMPv6	70	Router Solicitation from b0:52:16:20:77:c2
1403	184.668109000	192.168.30.15	103.231.48.193	ESP	158	ESP (SPI=0x0500aa30)
1404	184.673706000	103.231.48.193	192.168.30.15	ESP	162	ESP (SPI=0xcb727e0c)
1405	184.868464000	192.168.30.15	103.231.48.193	ESP	158	ESP (SPI=0x0500aa30)

0...		= Critical Bit: Not Critical
Payload length:	12	
Transform Type:	Encryption Algorithm (ENCR) (1)	
Transform ID (ENCR):	ENCR_AES_CBC (12)	
Transform IKE2 Attribute Type (t=14,l=2)	Key-Length : 128	
1...		= Transform IKE2 Format: Type/Value (TV)
Transform IKE2 Attribute Type:	Key-Length (14)	
Value:	0080	
Key Length:	128	

圖 5- 152. 首次連上核網之封包側錄截圖

資料來源：本團隊整理

5. 作業系統安全

作業系統資安測試是為確認產品設計上，於產品之作業系統上增加資安防護能力，與已知資安漏洞的修補程度，包括日誌檔的管控、已知漏洞掃描、敏感性資料洩露等，通過此節的資安測試，可確保產品具備系統層資安防護功能。

5-1. 作業系統及網路服務安全

測試案例	作業系統及網路服務安全
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物的作業系統和網路服務 CVSS Base Score 7.0 以上的資安漏洞。 資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1.使用檢測用筆電接上受測物，使用檢測工具如：NESSUS 進行作業系統的弱點掃描。 2.檢驗測試報告中的 CVSS Base Score。	
合格判定標準： 不可存在 CVSS Base Score 7.0 以上的資安漏洞。	
測試說明： 需要廠商提供進入至作業系統層方法與測試帳號密碼，使用檢測工具對受測物進行檢測，對產出的報告進行審視，不可存在 CVSS Base Score 7.0 以上的漏洞。	

測試結果：

下圖是透過弱點掃描軟體檢測出 CVSS Base Score 達到 10 分的漏洞。

22/tcp
93650 - Dropbear SSH Server < 2016.72 Multiple Vulnerabilities
Synopsis
The SSH service running on the remote host is affected by multiple vulnerabilities.
Description
According to its self-reported version in its banner, Dropbear SSH running on the remote host is prior to 2016.74. It is, therefore, affected by the following vulnerabilities : - A format string flaw exists due to improper handling of string format specifiers (e.g., %s and %x) in usernames and host arguments. An unauthenticated, remote attacker can exploit this to execute arbitrary code with root privileges. (CVE-2016-7406) - A flaw exists in dropbearconvert due to improper handling of specially crafted OpenSSH key files. An unauthenticated, remote attacker can exploit this to execute arbitrary code. (CVE-2016-7407) - A flaw exists in dbclient when handling the -m or -c arguments in scripts. An unauthenticated, remote attacker can exploit this, via a specially crafted script, to execute arbitrary code. (CVE-2016-7408) - A flaw exists in dbclient or dropbear server if they are compiled with the DEBUG_TRACE option and then run using the -v switch. A local attacker can exploit this to disclose process memory. (CVE-2016-7409)
See Also
https://matt.ucc.asn.au/dropbear/CHANGES
Solution
Upgrade to Dropbear SSH version 2016.74 or later.
Risk Factor
Critical
CVSS v3.0 Base Score
10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
CVSS Base Score
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:A/D:)

圖 5- 153 弱點掃描結果截圖

資料來源：本團隊整理

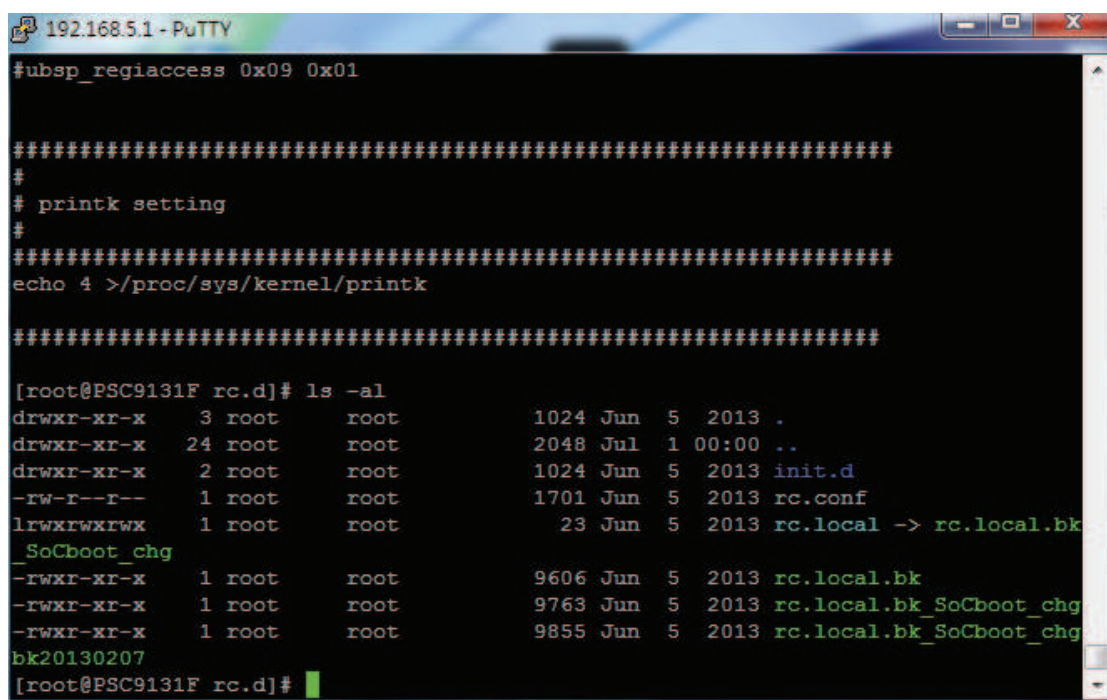
5-2. 系統開機程序於應用層的保護

測試案例	系統開機程序於應用層的保護
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物的作業系統和網路服務 CVSS Base Score 7.0 以上的資安漏洞。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	

測試案例	系統開機程序於應用層的保護
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將受測物接上檢測用筆電。 2. 檢測受測物中的開機程序設定檔如：rc.local 檔案是否能被修改。 3. 修改過程中，會寫入測試程序並加入 rc.local 檔案中，並重啟受測物檢視是否會被執行。	
合格判定標準： 步驟 3 中，若重啟後測試程序被執行，即判定不合格。	
測試說明： 受測廠商應聲明進入作業系統的方法，並提供系統管理者權限供測試用，測試人員修改開機程序設定檔（如：rc.d），加入其他測試程序，並在重開機後觀察是否可被執行，如不可被執行即表示受測產品有具備保護系統開機程序之功能。	

測試結果：

下圖為測試人員修改開機時所呼叫的程式清單，將其置入自行編譯之程式，於下次開機時，執行自行編譯之程式。



```

#ubsp_regiaccess 0x09 0x01

#####
#
# printk setting
#
#####
echo 4 >/proc/sys/kernel/printk

#####

[root@PSC9131F rc.d]# ls -al
drwxr-xr-x  3 root    root      1024 Jun  5  2013 .
drwxr-xr-x 24 root    root      2048 Jul  1 00:00 ..
drwxr-xr-x  2 root    root      1024 Jun  5  2013 init.d
-rw-r--r--  1 root    root      1701 Jun  5  2013 rc.conf
lrwxrwxrwx  1 root    root         23 Jun  5  2013 rc.local -> rc.local.bk
_SoCboot_chg
-rwxr-xr-x  1 root    root      9606 Jun  5  2013 rc.local.bk
-rwxr-xr-x  1 root    root      9763 Jun  5  2013 rc.local.bk_SoCboot_chg
-rwxr-xr-x  1 root    root      9855 Jun  5  2013 rc.local.bk_SoCboot_chg
bk20130207
[root@PSC9131F rc.d]#

```

圖 5-154 開機程序竄改截圖

資料來源：本團隊整理

5-3. 網頁管理介面的安全

測試案例	網頁管理介面的安全
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物的網頁管理介面不可有高風險的漏洞存在。	
資訊安全需求： ■機密性(Confidentiality) ■完整性(Integrity) ■可用性(Availability)	
測試環境暨初始條件： 1. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將受測物接上檢測用筆電。	

測試案例	網頁管理介面的安全
2.開啟檢測用筆電上的檢測軟體如:NESSUS、Acunetix，對受測物的網頁管理介面進行軟點掃描。 3.檢測報告中的 CVSS Base Score。	
合格判定標準： 受測物的網頁管理介面不可存在 CVSS Base Score 7.0 以上的資安漏洞。	
測試說明： 受測廠商須提供登入網頁伺服器之最高權限帳號，使用具網站弱點掃描之檢測工具對受測物的網頁伺服器進行檢測，從產生的報告內容中可以比對受測物是否符合測項。	

測試結果：

下圖是受測物經過網頁弱點掃描軟體所呈現之結果，結果顯示存在 OWASP top10 中跨站腳本攻擊風險以及 SSL 憑證版本強度不足風險。



圖 5- 155 XSS 跨站腳本攻擊風險截圖

資料來源：本團隊整理

The DROWN attack (SSLv2 supported)	
Classification	
CVSS	Base Score: 2.6
	- Access Vector: Network - Access Complexity: High - Authentication: None - Confidentiality Impact: Partial - Integrity Impact: None - Availability Impact: None
CVSS3	Base Score: 9.1
	- Attack Vector: Network - Attack Complexity: Low - Privileges Required: None - User Interaction: None - Scope: Unchanged - Confidentiality Impact: High - Integrity Impact: High - Availability Impact: None
CWE	CWE-310
CVE	CVE-2016-0800
Affected Items	
	Server

圖 5-156 憑證強度不足風險截圖

資料來源：本團隊整理

5-4. 日誌檔保存期限

測試案例	日誌檔保存期限
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 日誌的保存需要有期限的限制。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 受測 HeNB 與 MME 建立 S1 介面之連線。 2. 檢測用筆電與 HeNB 透過 RJ45 介面對連，並且可遠端登入 HeNB。	
測試方法： 1. 將檢測用筆電連上受測物。	

測試案例	日誌檔保存期限
2. 檢測受測物內的系統日誌是否有保存期限的限制。	
合格判定標準： 日誌的保存需要有期限的限制，至少要3個月以上。	
測試說明： 受測廠商應聲明進入作業系統的方法，並提供系統管理者權限供測試用，根據廠商所宣告的日誌檔存取路徑，檢視是否該日誌檔有存放超過1年；然而實際檢測時，必須搭配文件審查，由廠商宣告日誌存放期限，交由測試單位來判讀，這是因為受測產品日誌中所存在的過舊資料，在儲存空間不夠時，會是優先刪除的。	

測試結果：

下方測試結果顯示僅有當下開機後的日誌有記錄，且一開始時間會是錯的，會回到系統的 epoch time，這是在 HeNB 上普遍常見的現象，一般作法是會將本機の日誌檔回傳至 log server 集中管理，因此本測項必須廠商提供後端伺服器的日誌資料供查驗。

```

root@kali: ~
File Edit View Search Terminal Help
ocalIp:1
< 6>1970-01-01T00:03:32.650Z 1522: [STCL-IPSEC] Send READY_REQ to ipsec broker
kernel
<id 6>1970-01-01T00:03:32.650Z 1523: [IPSec] Process MSG_READY_REQ from 127.0
.0.1:55200
< 6>1970-01-01T00:03:32.740Z 1524: [OAM] Send READY_REQ to OAM
< 6>1970-01-01T00:03:32.830Z 1525: [SIAP] foxSlap_sctpInit: SIAP wait for i
psec:0, ls-init:1, freq-sync:0, sniffer:0, provision: 1, Lte_AdminState:1
< 6>1970-01-01T00:03:33.150Z 1526: [IPSec] NTP not synced yet, start IPsec
module later
< 3>1970 01 01T00:03:33.300Z 1527: [FailSafe] Fail to connect to NTP server
< 6>1970-01-01T00:03:33.300Z 1528: [Alarm] Alarm Set Event: 50201
< 6>1970-01-01T00:03:33.470Z 1529: [PM] pmLoop wait CWMP ready uptime=214,
currentUTC=213
< 6>1970-01-01T00:03:33.470Z 1530: [PM] Get next upload time is [1119]
< 6>1970-01-01T00:03:33.470Z 1531: [PM] pmGetNextSampleTime() current uptim
e:219 utc:219
< 6>1970-01-01T00:03:33.480Z 1532: [SCTP] X2 SCTP Server wait for ipsec:0 l
ocalIp:1
< 6>1970-01-01T00:03:33.650Z 1533: [STCL-IPSEC] Send READY_REQ to ipsec bro
ker
< 6>1970-01-01T00:03:33.650Z 1534: [IPSec] Process MSG_READY_REQ from 127.0
.0.1:55200
[root@femto log]#
  
```

圖 5- 157. 日誌資料截圖

資料來源：本團隊整理

5-5. 日誌檔無法儲存的警示機制

測試案例	日誌檔無法儲存的警示機制
參考資料	3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) 3GPP TR 33.820 Security of H(e)NB
測試目的： 受測物的日誌無法提供正常服務時，應主動告知裝置管理者。	
資訊安全需求： ☐ 機密性(Confidentiality) ☐ 完整性(Integrity) ☒ 可用性(Availability)	
測試環境暨初始條件： 1. 受測 HeNB 與 MME 建立 S1 介面之連線。	
測試方法： 1. 將產品儲存空間填滿。 2. 反覆登入登出直到日誌檔無法儲存。 3. 檢視產品是否依照使用說明達到告警效果。	
合格判定標準： 日誌紀錄檔無法正常儲存時，須發出警示。	
測試說明： 受測廠商應聲明進入作業系統的方法，並提供系統管理者權限供測試用，測試人員藉由修改日誌檔的存取權限，再執行觸發系統日誌寫入的行為，檢視受測物在無法儲存時是否有告警機制。	

測試結果：

下圖試測結果顯示，受測物在無法儲存日誌時僅有日誌記錄此異常，並未提供告警機制。

```
[root@femto log]# df
Filesystem                Size      Used Available Use% Mounted on
/dev/root                  36.0M    36.0M      0 100% /
tmpfs                     4.0M    132.0K      3.9M   3% /tmp
tmpfs                     12.0M      0     12.0M   0% /tmp2
tmpfs                     2.0M      2.0M      0 100% /var/log
tmpfs                    256.0K    16.0K    240.0K   6% /var/run
tmpfs                    32.0K      8.0K    24.0K  25% /var/tmp
ubi0:maincfg              18.7M    436.0K    17.3M   2% /cfg/main
ubi1:bakcfg               18.7M      1.6M    16.1M   9% /cfg/bak
ubi2:manu                  2.1M     28.0K     2.0M   1% /manu
ubi3:info                  5.8M     28.0K     5.5M   0% /info
[root@femto log]# ls
httpd-2.4.29.tar.bz2  test3*  test6
test                  test4
test2                 test5
```

圖 5- 158 修改日誌檔存取權限截圖

資料來源：本團隊整理

3	0001-01-01T00:09:59	58C232F40B052162077C2_168	NewAlarm	Syslog	Communications	1603	160301	WARNING
4	0001-01-01T00:03:13	58C232F40B052162077C2_169	NewAlarm	FailSafe	Communications	502	50201	WARNING
5	0001-01-01T00:10:03	58C232F40B052162077C2_170	NewAlarm	Syslog	Communications	1603	160301	WARNING
6	0001-01-01T00:03:14	58C232F40B052162077C2_171	NewAlarm	FailSafe	Communications	502	50201	WARNING
7	0001-01-01T00:09:58	58C232F40B052162077C2_172	NewAlarm	Syslog	Communications	1603	160301	WARNING
8	0001-01-01T00:03:29	58C232F40B052162077C2_173	NewAlarm	FailSafe	Communications	502	50201	WARNING
9	0001-01-01T00:03:25	58C232F40B052162077C2_174	NewAlarm	FailSafe	Communications	502	50201	WARNING
10	0001-01-01T00:01:26	58C232F40B052162077C2_175	NewAlarm	FailSafe	Communications	501	50101	CRITICAL
11	0001-01-01T00:01:50	58C232F40B052162077C2_176	NewAlarm	Ethernet	Communications	301	30101	CRITICAL
12	0001-01-01T00:01:58	58C232F40B052162077C2_176	ClearedAlarm	Ethernet	Communications	301	30101	CRITICAL
13	0001-01-01T00:02:11	58C232F40B052162077C2_175	ClearedAlarm	FailSafe	Communications	501	50101	CRITICAL
14	0001-01-01T00:02:17	58C232F40B052162077C2_177	NewAlarm	FailSafe	Communications	501	50101	CRITICAL
15	0001-01-01T00:03:19	58C232F40B052162077C2_178	NewAlarm	FailSafe	Communications	502	50201	WARNING

圖 5- 159 日誌資料截圖

資料來源：本團隊整理

6. 實體防護

實體防護測試是為確認產品設計上，有無阻礙駭客實體入侵之能力，包括增加產品外殼拆除難度、實體介面之存取控制等，通過此節的資安測試，可確保產品具備實體資安防護功能，由於僅家用基站是布建於終端使用者環境中，因此本節僅家用基站

適用。

6-1. 家用基站的整機保護

測試案例	家用基站的整機保護
參考資料	• 3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) • 3GPP TR 33.820 Security of H(e)NB
測試目的： 檢測微型基站的實體安全，機殼不能被輕易拆解。 資訊安全需求： ☐機密性(Confidentiality) ☒完整性(Integrity) ☐可用性(Availability)	
測試環境暨初始條件： 無	
測試方法： 檢測受測物的外殼是否有防盜螺絲保護。	
合格判定標準： 受測物之外殼不能被輕易拆除。	
測試說明： 目視受測物的機殼，是否有防拆螺絲或是一體成形。	

測試結果：

下圖為本測項之測試結果顯示，受測物未使用防拆螺絲，面臨可透過硬體介面入侵作業系統的風險。



圖 5- 160 HeNB 外觀截圖-未使用防拆螺絲

資料來源：本團隊整理

6-2. 硬體憑證的設計

測試案例	硬體憑證的設計
參考資料	• 3GPP TS 33.320 Security of Home Node B (HNB) / Home evolved Node B (HeNB) • 3GPP TR 33.820 Security of H(e)NB
測試目的： 檢測微型基站的實體安全，硬體憑證(token)的設計不能被任意插拔使用。	
資訊安全需求： ☐ 機密性(Confidentiality) ☒ 完整性(Integrity) ☐ 可用性(Availability)	
測試環境暨初始條件： 無	
測試方法： 檢測受測物的外殼是否有防盜螺絲保護。	
合格判定標準：	

測試案例	硬體憑證的設計
受測物不可存在外接式硬體憑證(token)。	
測試說明： 此測項需目視受測物外殼是否有外接式的硬體憑證，若無則拆解外殼，假使拆解不須經由防拆螺絲，即可以見到 SIM 卡插槽，則面臨硬體 token 被卸除的風險。	

測試結果：

下圖即是此 HeNB 的 SIM 卡插槽輕易即可碰觸到。



圖 5- 161 HeNB 外觀截圖-SIM 卡插槽

資料來源：本團隊整理

(四) HeNB 資安監測技術研究

檢測技術研究是建立在駭客攻擊手法的基礎之上，欲達成此目的，本篇藉由研究可與既有之家用基站的系統整合之 4G HeNB 系統安全監測技術，提供家用基站的動態行為監測與保護能力，利用應用程式白名單核心技術達成下列目標：(1) HeNB 應用服務行為的監控與異常日誌的記錄，提供資安檢測人員進行後續分析；(2) 建立敏感資料的新增/修改/移除記錄；(3) 抵擋駭客入侵控制 HeNB。因此本團隊參考 3GPP TS 33.320 和 3GPP TR 33.820 所提到需要妥善保存且須進行權限控管之敏感資料，包括

用戶清單、4G 設定檔、系統日誌和密碼檔，執行監控和分析。

透過此研究研發作業系統平台之動態監測技術，運用於威脅偵測、應用服務異常行為監控以及異常事件分析等，作為資安檢測技術研發與改進之依據，監控應用服務行為可以觀看哪些程序被抵擋以及關鍵檔案被存取過的日誌紀錄，改善檢測人員解析攻擊途徑的效率。而受測廠商往往在檢測過後，需要有效之資安解決方案，可藉由此系統監控核心技術抵擋惡意入侵程式，例如：檢測在韌體更新後的安全參數設置以及系統開機程序的保護，可以提供抵擋和通報的協助。

1. HeNB 監測技術功能規劃

本文所提出的 HeNB 即時防護機制，主要是透過 hook HeNB 作業系統(i.e., Linux kernel)之 system call，並做出 Access Deny、Execute-Proof 及異常行為記錄等相應的處理，來限縮駭客的入侵行為，因此首要工作即是釐清應該要監控的 system call，像是監控應用程式的執行對應到的是 sys_execve，監控檔案的讀取是透過 sys_read，也可利用 hook sys_open 來提高駭客入侵時的應對效率。

在 Linux 中，使用者程式要執行某項功能時(例如：檔案讀寫)，基於系統管理(例如存取硬體)或是系統安全性(有些操作需要較高的權限)的原因，作業系統會提供一組介面來幫忙做事情，這組介面就稱為系統呼叫，就連執行程式本身也必須透過系統呼叫(execve)，系統呼叫流程如下圖所示：

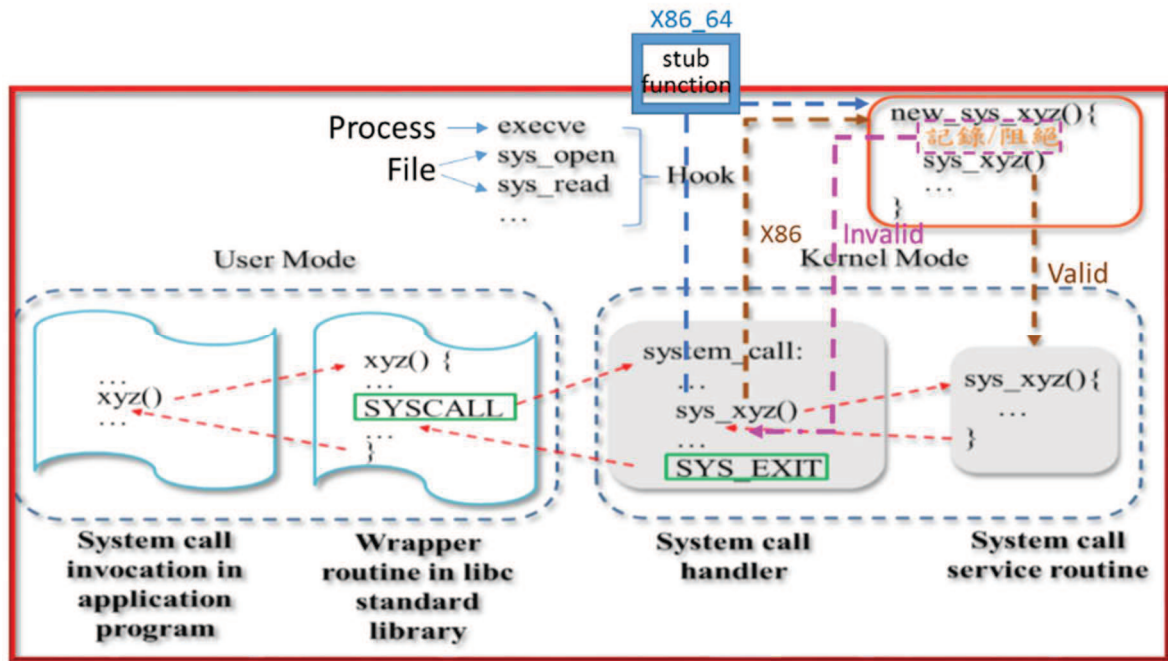


圖 5-162 系統呼叫執行流程

資料來源：本團隊整理

由上圖可以看到，使用者執行程式，當執行到 SYSENTER 的時候，執行流程就會轉移到 Kernel 位置空間中負責處理系統呼叫的程式區塊，找到對應的系統呼叫 (sys_xyz) 後執行，執行完畢則透過 SYSEXIT 回到使用者位置空間。

目前的 Linux 系統呼叫分為三種：

- int 0x80 (iret to exit)
- sysenter (sysexit to exit)
- syscall (sysret to exit)

此三種系統呼叫的方法差異在於進入 kernel 位置空間的方法不一樣，除了傳統的 int 0x80 之外，sysenter 和 syscall 相較於傳統 int 0x80 能提供較快的進入方法，主要是透過把系統呼叫處理區塊的進入點存進 MSR(Model-Specific Register) 中，當程式流程執行到 sysenter 或是 syscall 時，就會依據 MSR 來進入 kernel 空間做處理。當執行完對應的系統呼叫後會執行到各自的離開方法(iret, sysexit, sysret)。

透過劫持原系統 system call 之呼叫，將其導引至具備本防護機制功能(見表 5-10、表 5-11)的程式，並對 HeNB 的存取行為進行監控或阻絕。

表 5- 10 程序監控功能

功能名稱	功能說明
程序異常行為偵測及阻絕	提供程序監控、阻絕等功能，阻擋未授權程序及遭竄改/替換的合法程序啟動。
程序監控白名單機制	透過編輯白名單來定義欲授權之程序，以控管未授權檔案的執行，功能包括： ◆ 建立出廠預設程序白名單。 ◆ 新增/刪除「程序白名單」中之程序
防竄改程序啟動	察覺已遭竄改的程序，並阻止其啟動。
程序異常紀錄日誌檔	當發生未經授權或被竄改程序之啟動事件時，將自動記錄此異常事件至日誌檔中。 ◆ 日誌檔中的每一筆異常紀錄包含： ◆ 發生日期/時間 ◆ 程序名稱 ◆ 處置理由（如:未授權/遭竄改）。

資料來源：本團隊整理

表 5- 11 檔案監控功能

功能名稱	功能說明
檔案監控	提供檔案監控、記錄等功能，能有效得知欲監控檔案的存取行為，預防惡意行為的發生
檔案監控名單機制	透過編輯監控名單來定義欲監控之檔案，條列於此名單中的檔案將會被監控其存取行為，功能包括： 1. 新增欲監控之檔案至檔案監控名單 2. 移除已監控之檔案從檔案監控名單
檔案存取監控日誌檔	當監控的檔案發生讀寫事件時，將自動記錄此行為監控事件至日誌檔中，日誌檔中的每一筆檔案存取紀錄包含： 1. 事件發生之日期/時間 2. 檔案名稱 3. 行為（讀/寫/刪除/改名）

資料來源：本團隊整理

本防護機制在 kernel space 會建立一個白名單過濾機制，白名單中記錄著所有合法授權的 process 名單，一旦有駭客藉由 HeNB 漏洞來植入惡意程式，將會因為該惡意程式不在白名單內而被視為未授權執行，此攻擊將會被擋下。此外，本白名單還記錄合法授權 process 的 digest，只要在 process 啟動時比對 digest，即可防止駭客竄改或偽裝成原合法授權 process。此外駭客還可能藉由讀取 4G 組態設定檔來達到偽冒合法基站之攻擊，或者竄改白名單及系統日誌檔來規避被本防護機制察覺，因此本防護機制還需要進行對上述等關鍵檔案進行存取控制，此關鍵檔案的防護需考慮到駭客可能提權成為超級使用者的可能性，為避免因為此一情況而造成本防護機制失效，在關鍵檔案的防護上，另外還增加了密碼認證的保護，換句話說，只有認證成功的超級使用者可以存取關鍵檔案，圖 5-163 顯示本防護機制之軟體架構，從架構中可看出，在運行本防護機制之前需先產生白名單，之後在核心模組啟動時才會載入進白名單，而主要的功能如：程序偵防、關鍵檔案監控等功能都是建置於核心網路中。

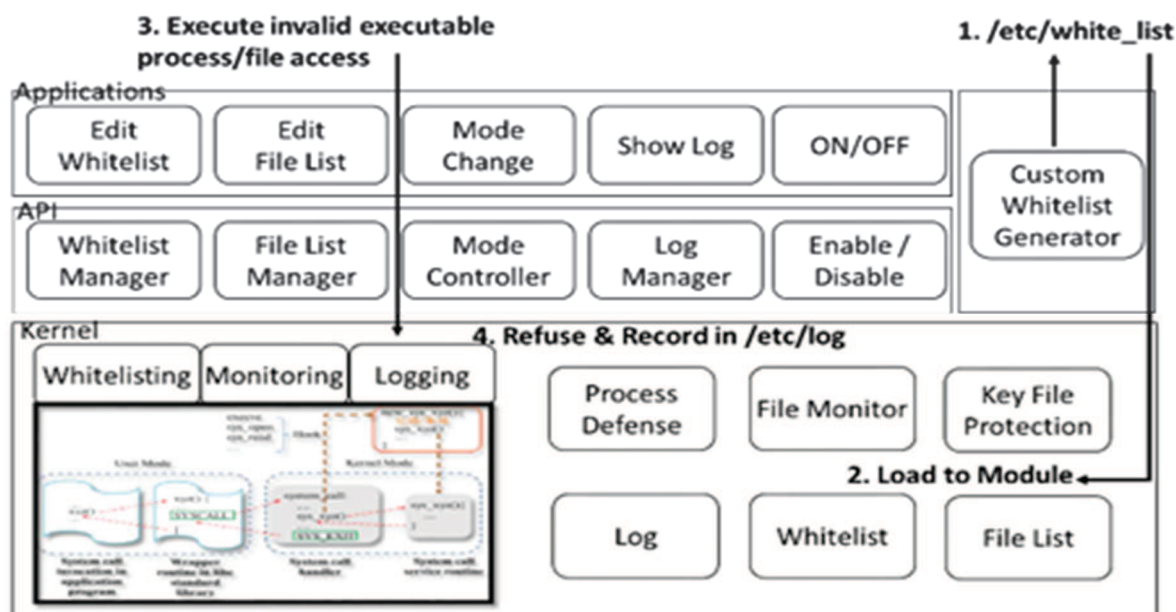
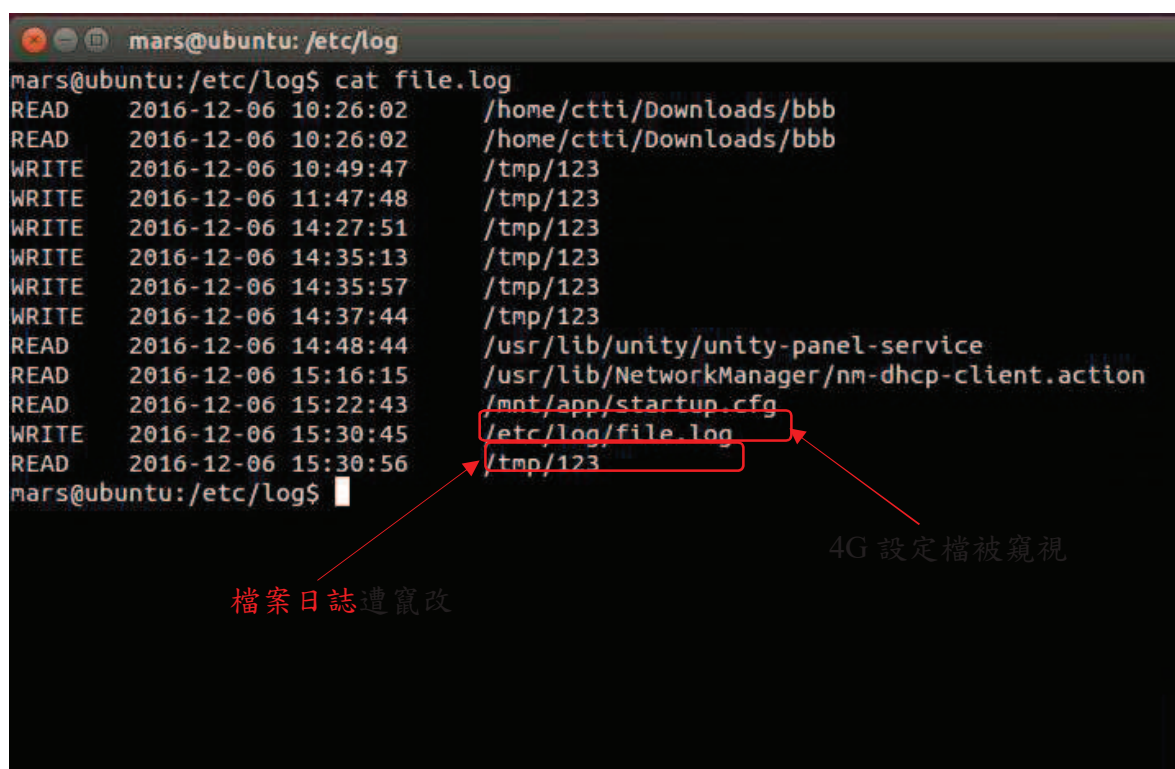


圖 5-163 本防護機制之軟體架構圖

資料來源：本團隊整理

2. 實驗結果

下圖 5-164 為本技術所監控之系統異常事件日誌檔內容，根據 3GPP TR 33.820 去選擇一定範圍的關鍵檔案，再根據日誌檔所顯示之異常行為紀錄，進一步修正檢測手法，例如：監控存有 4G 組態設定之檔案，發覺該檔案內容時常被讀取，這說明某些惡意的攻擊可能只要透過 4G 設定檔內容的窺視即可達成，再比對 3GPP 所條列之資安威脅，確定設定檔應該要加密或者是某些關鍵欄位要遮罩，避免相關敏感性資料的外洩，因此回饋到檢測項目，應該要包含 4G 設定檔的權限管控。



```
mars@ubuntu: /etc/log
mars@ubuntu:/etc/log$ cat file.log
READ    2016-12-06 10:26:02    /home/ctti/Downloads/bbb
READ    2016-12-06 10:26:02    /home/ctti/Downloads/bbb
WRITE   2016-12-06 10:49:47    /tmp/123
WRITE   2016-12-06 11:47:48    /tmp/123
WRITE   2016-12-06 14:27:51    /tmp/123
WRITE   2016-12-06 14:35:13    /tmp/123
WRITE   2016-12-06 14:35:57    /tmp/123
WRITE   2016-12-06 14:37:44    /tmp/123
READ    2016-12-06 14:48:44    /usr/lib/unity/unity-panel-service
READ    2016-12-06 15:16:15    /usr/lib/NetworkManager/nm-dhcp-client.action
READ    2016-12-06 15:22:43    /mnt/app/startup.cfg
WRITE   2016-12-06 15:30:45    /etc/log/file.log
READ    2016-12-06 15:30:56    /tmp/123
mars@ubuntu:/etc/log$
```

檔案日誌遭竄改

4G 設定檔被窺視

圖 5-164 日誌檔實驗結果

資料來源：本團隊整理

此外，我們模擬駭客透過 HeNB 中的軟體程式漏洞入侵 HeNB 以驗證本防護機制的實驗結果，圖 5-31 顯示的攻擊流程如下，首先透過軟體程式漏洞植入惡意程式(vul)，由於未被授權而被防護機制擋下，駭客轉而替換原合法程序(ls)，但是遭偽造的合法程序又再次被阻擋，後續駭客可能成功提權為 super user，以解讀 4G 設定檔的內容，以進一步執行偽基站攻擊，從圖中的 kernel message 截圖，明顯看出本文所提之防護機制一層層抵擋駭客的攻擊。本章節我們模擬駭客透過 HeNB 中的軟體程式漏洞入侵 HeNB 以驗證本防護機制的實驗結果，圖 5-165 顯示的攻擊流程如下，首先透過軟體程式漏洞植入惡意程式(vul)，由於未被授權而被防護機制擋下，駭客轉而替換原合法程序(ls)，但是遭偽造的合法程序又再次被阻擋，後續駭客可能成功提權為 super user，以解讀 4G 設定檔的內容，以進一步執行偽基站攻擊，從圖中的 kernel message 截圖，明顯看出本文所提之防護機制一層層抵擋駭客的攻擊。

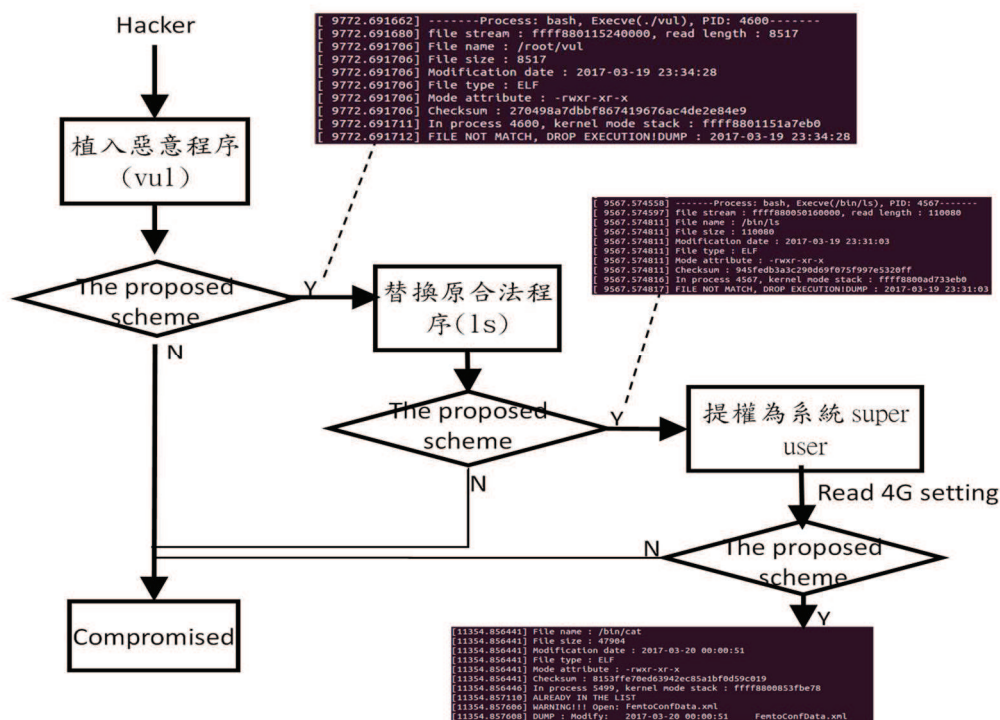


圖 5- 165 防護測試實驗結果

資料來源：本團隊整理

由上圖實驗結果發現，(1)駭客欲植入惡意程序或偽冒合法程序的執行是不可行的；(2)駭客即使提權成為 super user 也無法執行偽基站攻擊；(3)關鍵檔案可透過本模組取得完整保護，綜合上述 3 點，像是 User cloning the H(e)NB authentication Token 及 Mis-configuration of H(e)NB 等會引發偽基站攻擊的威脅將會被抵擋。下表將 the proposed scheme、SeGW 及 HeMS 比較其所能抵禦的資安威脅。

表 5- 12 與 3GPP 所提的安全裝置比較

威脅編號	資安威脅	SeGW	HeMS	本防護機制
Threat 2)	Compromise of H(e)NB authentication token by local physical intrusion	●		
Threat 4)	User cloning the H(e)NB authentication Token.			●
Threat 5)	Man-in-the-middle attacks on H(e)NB first network access.	●		
Threat 7)	Fraudulent software update / configuration		●	●

威脅編號	資安威脅	SeGW	HeMS	本防護機制
	changes.			
Threat 9)	Eavesdropping of the other user's UTRAN or E-UTRAN user data.			●
Threat 11)	Changing of the H(e)NB location without reporting.	●		
Threat 12)	Software simulation of H(e)NB.	●		
Threat 14)	Misconfiguration of the firewall in the modem/router.			●
Threat 17)	Compromise of an H(e)NB by exploiting weaknesses of active network services			●
Threat 19)	Mis-configuration of H(e)NB			●
Threat 20)	Mis-configuration of access control list (ACL) or compromise of the access control list			●
Threat 22)	Masquerade as a valid H(e)NB			●
Threat 26)	Environmental/side channel attacks against H(e)NB	●		
Threat 27)	Attack on OAM and its traffic		●	
Threat 28)	Threat of H(e)NB connectivity to network access	●		

資料來源：本團隊整理

上個章節表 5-6 中所條列出的威脅編號，可直接對應到 3GPP TR 33.820 中的威脅編號，而表格顯示出 SeGW、HeMS 及本防護機制各有擅長的防護項目，由上表明顯可以看出本防護機制填補 SeGW 所無法提供的安全防護，更說明本防護機制對於降低 HeNB 資安威脅的必要性。

家用基站不像傳統基站般難以觸及，無論是來自實體或網路的威脅都令電信商難以防範，而且 zero day 的漏洞更是令人防不甚防，今天能保證駭客無法入侵，幾年後可能無法確定，因此直接侷限系統的存取控制權限，才是無效化駭客入侵的攻擊手段，透過本篇的防護機制，大部份家用基站的攻擊發起契機被隔離，使得家用基站除了仰賴核網的保護外，本身亦有自我保護的能力，大幅提升家用基站的安全可信度。

第三節 核心網路-MME 資安檢測技術研究

行動網路 LTE 的環境中，核心網路 EPC(Evolved Packet Core)在設計上改採 All-IP 的架構，並設計成多重網路存取架構，可相容既存的通訊系統(如 2G、3G 等)及 IP 網路系統(如 WLAN、WiMAX 等)。

EPC 內包含多個網路元件(如下圖)：❶S-GW、❷P-GW、❸MME、❹HSS、❺SGSN。訊息分成控制面(Control-Plane)與用戶面(User-Plane)，控制面訊息為網路控制與存取、移動性、身分認證及安全性、封包路由、無線訊號等的管理。用戶面訊息是處理用戶網路服務的封包，這些網路元件包含：MME(Mobility Management Entity)幫助 EPC 驗證 UE 的身分與 UE 移動性管理、HSS(Home Subscriber Server)是管理用戶歸屬伺服器、S-GW(Serving Gateway)為處理 User Plane 的連線、eNodeB 管理 UE 的無線訊號。

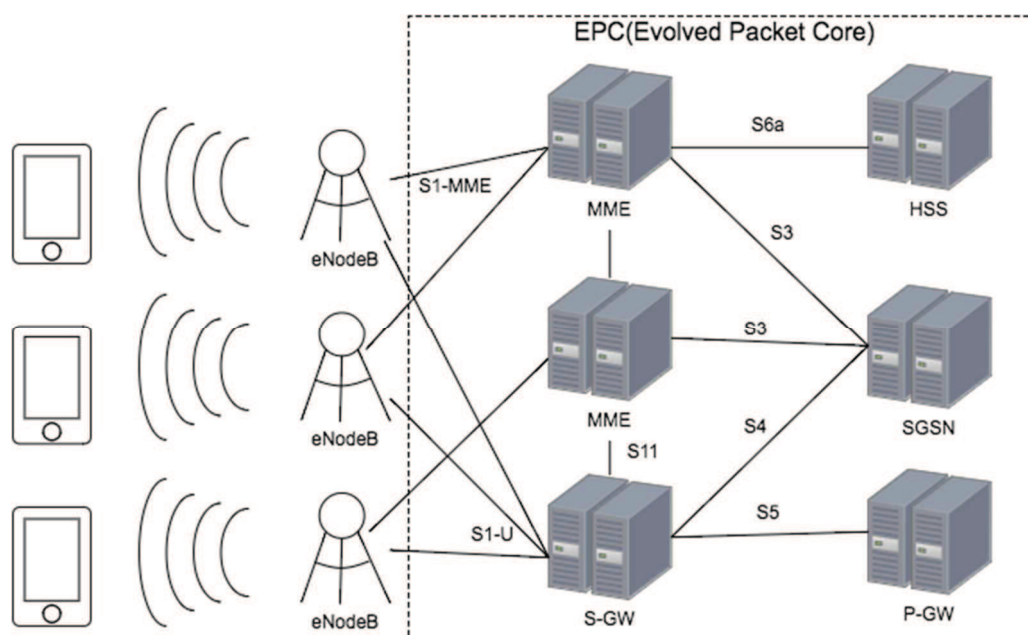


圖 5- 166 EPC 架構圖

資料來源：本團隊整理

透過 EPC 的網路元件，核心網路取得終端的資訊，並管理終端設備在連接時的

驗證與授權，大致上歸類出以下八項功能³¹²：

(I) 網路存取控制(Network Access Control)：管理 UE 的授權與認證，讓 UE 取得 IP 以連結網際網路。

(II) 無線訊號管理(Radio Resource Management)：定義 UE 連線能力，包括在網路服務的封包速率與無線訊號的資源。

(III) 移動性管理(Mobility Management)：在 eNodeB 的服務範圍有限下，又因為 UE 不斷在移動，為了使得網路服務不中斷，必須要與其他 eNodeB 交換訊息來繼續服務 UE，協調 UE 的資訊轉移到不同的 eNodeB，此工作由 MME 來協調 (Coordination)，另外一種情況為 UE 離開 MME 的追蹤範圍(Track Area)，也就是所謂的追蹤服務更新(Track Area Update)程序，就需要將 UE 的資訊轉移到新的 MME。

(IV) 漫遊管理(Roaming Management)：管理 UE 在跨 PLMN 之間的協調 (Coordination)。

(V) UE 可取得性(Reachability)：分成主動通知與被動接收 UE 的行為記錄，主動通知為通知服務 UE 的 MME，提出要求並在 UE 下個行為發生時給予回覆，被動通知為 UE 行為產生時就會從 MME 接收行為記錄。

(VI) 追蹤範圍管理(Tracking Area Management)：提供 UE 可以在訊號範圍內，連接 eNodeB 服務清單

(VII) 合法監聽(Lawful Intercept)：讓電信業者可以合法的存取私人通話與封包擷取，此服務依當地的法律依據為主。

(VIII) 閘道間負載平衡(Load Balancing Between Gateways)：幫助 UE 選擇較適合的閘道進行服務，防止單一閘道服務數目過多

EPC 在眾多介面上執行了不同流程，這些流程是環環相扣的，E-UTRAN 與 EPC 之間的橋樑是 MME，且 MME 主要負責了移動性管理功能，該元件對 LTE 網路扮演極為重要的角色，其安全性也受到 3GPP 的重視，該元件之安全保證規範早於 eNodeB

³¹² RCR Wireless News , “LTE MMEA Core Connector for LTE”, 2014/5/9. [Online]. Available: <http://www.rcrwireless.com/20140509/diameter-signaling-controller-dsc/lte-mme-epc>

一年公佈，故本章節特別針對 MME 之安全性進行探討。

以下將從 MME 功能研究介紹 MME 的管理流程，包含位置訊息管理、通道管理、錯誤處理、驗證管理、安全性訊息加密等流程。並進一步針對 MME 與其他網路元件之間的溝通進行說明，因為 MME 需要針對 UE 的資訊進行管理與監控，MME 就會需要與不同介面交換訊息來完成管理 UE 的資訊。最後將從 MME 介面安全性及攻擊行為分析，分析 MME 之弱點及安全威脅。

在介面安全研究發現，MME 的介面：S1、S3、S6a、S10、S11，有著許多的程序在執行，這些程序必定需要傳輸 UE 的資訊，因此 UE 的資訊會需要曝露在無線訊號中，過往的研究許多的無線訊號擷取³¹³，讓 UE 的資訊不安全，可能讓駭客有機可趁可以取的 UE 的資訊並攻擊，所以在 3GPP TS 33.401 規範了許多 UE 的安全性議題，需要在執行程序時需要注意及遵守的規則。

MME 中包括了與 UE 的 NAS 信令與 UE 的身分驗證，這個部分包括了 S1、S6a 在 UE、MME 與 HSS 之間傳輸著 UE 的驗證資料，從建立通道、安全模式、產生金鑰、換手程序，MME 必須要在這之間進行驗證，在建立通道時 MME 要先確認 UE 的安全模式，依照 UE 支援的安全模式，UE 驗證安全模式訊息內的金鑰與加密方式成立後，就會產生金鑰並進行訊息內容的加密。

在 LTE 中 UE 的行動管理，MME 管理 UE 在移動時，需要將金鑰與 UE 的資訊進行換手，而換手方面分成了 eNodeB 換手、MME 換手、3G 之間的換手(S3 與 SGSN 之間的訊息交換程序)，在 UE 資訊傳遞中，MME 為了確保 eNodeB 換手後 UE 的安全模式還是相同，必須要在換手程序中驗證 UE 與前 eNodeB 的安全模式相同，否則將執行額外程序。在 MME 換手階段，MME 會先確認是否 UE 能夠支援相同於原 MME 的安全模式，若沒有的話就要與 UE 確認驗證資料與安全模式。在 3G 之間換手時，MME 就需要產生對應的金鑰，讓 3G 模式下的 UE 能夠進行加密，並且在 SGSN 的 S3 介面進行 UE 的身分驗證。另外，在 UE 沒有辦法進行驗證或者緊急時，MME 會有緊急通道建立，此通道會在未經驗證的狀態下，讓加密方式為零號演算法，也就是不進行加密，因此在這個部分，MME 需要避免駭客從此狀態下的程

³¹³ Meyer, U., & Wetzel, S. (2004, October). A man-in-the-middle attack on UMTS. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 90-97). ACM.

序，從 UE 的資訊中獲得其他 MME 的資源，這部分提及了包括用戶層資料傳輸的 S11 介面，其功能在管理 S1-U 的 UE 與 S-GW 交換的用戶層資料。

在 MME 攻擊行為上，參考 3GPP TS 33.926 的威脅與 TS23.401 的程序呼應，檢視相關訊息傳輸的程序步驟，從 MME 訊息交換的內容到訊息的傳遞路徑、駭客修改 UE 與 MME 安全模式、傳遞冗餘的訊息給其他核網元件、非法使用已驗證的服務等，MME 雖然不牽涉在產生 UE 的驗證資料與 EPS 安全性文本，但是卻負責在傳遞這些資訊，因此 MME 的安全性應該被重視與規範。

透過 3GPP TS 33.116 的 MME 安全保證規範，針對 MME 的檢測規範，在 MME 相關的程序中，應該對 UE、eNodeB、HSS、S-GW 與 SGSN 之間訊息交換的內容，先初步的進行篩選，以條件的方式處理不同的例外情況，避免 MME 消耗過多的資源，例如 MME 收到訊息時，先檢查訊息的完整性，再來檢查訊息中是否為 4G 應該出現的訊息等，這些規範都能加強 MME 在受到駭客攻擊時，造成更深入影響的規範。

一、 MME 功能研究

MME 在 EPC 與 E-UTRAN 之間，負責交換訊息包括驗證與移動性信令等功能，我們在此項目主要參考 3GPP TS 23.002³¹⁴中規範的 MME 功能，並從 3GPP TS 23.401³¹⁵研析其個別的功能與說明。

（一） NAS 信令及安全性

NAS(non-access stratum)為控制面在 UE 與 MME 之間的訊號介面，用於 UE 的移動性管理、UE 與 S-GW 的通道(IP 連線管理及維護)，並為用戶提供"隨時可用"的 IP 連線和"永遠開啟"特性。在 UE 與 MME 之間的流程，NAS 訊息都是透過 EPS 安全性文本，訊息進行加密與完整性的保護，在 EPS 安全性文本內，包括驗證、完整性與加密的密鑰。

³¹⁴ 3GPP TS 23.002 V14.1.0, 2017/3.

³¹⁵ 3GPP TS 23.401 V15.1.0, 2017/9.

在安全性被啟用前，UE 與 MME 會先建立 EPS 安全性文本，透過在 AKA 流程產生 UP(User Plane)、RRC(Radio Resource Control)、NAS 的加密密鑰以及 NAS 與 RRC 的完整性密鑰，在流程一開始 MME 傳送訊息給 USIM，USIM 會透過 UE 收到訊息，訊息內包含一隨機值 RAND 與 AUTN，AUTN 為驗證 UE 的參數，UE 收到訊息後會檢查 AUTN 是否正確。

許多的 EPS 安全性文本需要被持續的維護，因此需要注意在完成驗證後，在轉移狀態、結束服務、轉換加密演算法時，MME 應刪除不該存在的 EPS 安全性文本。

(二) 在 EPC 的網路元件間傳遞移動性信令

在 EMM(EPS 移動性管理)，有兩種狀態：EMM-DEREGISTERED 與 EMM-REGISTERED，來管理 UE 的註冊與追蹤範圍更新程序。在 EMM-DEREGISTERED 狀態下，MME 中的 EPS 安全性文本不儲存 UE 的位置或路由資訊。在 EMM-REGISTERED 狀態下，UE 可以接收 EPC 中註冊時需要的信令，且 UE 應至少有一個啟用的 P-GW 與啟用 EPS 安全性文本。

移動性信令分為三種程序：跨 eNodeB、跨 MME、切換至 2G 或 3G；跨 eNodeB 是使用 X2(eNodeB 之間)介面，將 UE 從原 eNodeB 轉移到新 eNodeB，當 UE 到達新 eNodeB 時，可以發送原 eNodeB 轉送訊息給新 eNodeB。

跨 MME 在 X2 的轉換不能執行時，即執行 S1-MME 的轉換程序，原 eNodeB 從 S1-MME 發送轉換要求的訊息，在 UE 離開 MME 的服務範圍，原 eNodeB 通過在 S1-MME 上發送轉移要求訊息來發起轉移，原 MME 選擇新 MME。

在轉移過程中，原 MME 將拒絕自從轉移過程開始以來接收到的任何 P-GW 發起的 UE 通道要求，並且應包括由於轉移過程正在進行，暫時拒絕轉送給 P-GW，並回覆該要求已被暫時拒絕。

(三) 在 ECM-IDLE 狀態下，UE 的可靠度

在 UE 已經註冊的狀態下，UE 與 MME 之間的 NAS 信令通道不存在時稱為 ECM-IDLE 狀態。UE 在 ECM-IDLE 狀態時，UE 的位置可以從網路的追蹤範圍列表取得，而追蹤範圍所在的 eNodeB 會記錄呼叫的次數，因為 UE 會註冊於多個追蹤範圍，包

含 UE 註冊過的所有追蹤範圍都會由服務的 MME 記錄下來。

MME 會計算 UE 的計數器，一旦 UE 進入 ECM-IDLE，如果計數器結束了，MME 就會推斷 UE 已經結束服務。

(四) 追蹤範圍列表管理

追蹤範圍列表用在 E-UTRAN 範圍內，為 UE 分配追蹤範圍列表，當 UE 註冊網路服務時，MME 會分配追蹤範圍給 UE，並且在 UE 註冊過的追蹤範圍，MME 也會追蹤該區域，而列表產生的依據由 UE 現在位置為中心來計算，這樣能減少追蹤範圍更新的機會。

(五) 選擇 P-GW 與 S-GW

提供 LTE 的 UE 連線與分配 P-GW/S-GW，由 HSS 的用戶資訊與連線能力，以及 P-GWs/S-GWs 的負載平衡，避免多個 P-GW/S-GW 服務多個 UE，假如提供 P-GW/S-GW 權重，除了負載平衡外也要計算權重。在 HSS 提供的資訊內也包含 UE 文本，內容包含 P-GW/S-GW 與連線能力的對應，HSS 分配的 P-GW/S-GW 是否允許外部 PLMN 或所屬的 PLMN 有已指定的 P-GW/S-GW。

當 UE 可以選擇多個 P-GWs/S-GWs 建立連線時，UE 會提供 HSS 的要求去選擇 P-GW/S-GW，UE 就必須根據 HSS 要求，以 P-GW /S-GW 動態建立新的連線，同樣在 HSS 如果提供指定分配的 P-GW/S-GW，或 P-GW/S-GW 提供動態分配的功能下，提出換手的要求的訊息，就會直接指定 P-GW/S-GW。當 P-GW 與 S-GW 的組合已被指定為 UE 服務，就會直接使用該 P-GW 與 S-GW 使用網路服務。

(六) 在 MME 換手時，決定新的 MME

原 MME 應選擇 UE 在移動時，較接近原追蹤區域的新 MME，這樣能減少 MME 再次換手的機會並增加 UE 的網路訊號穩定性。

(七) 在換手到 2G 或 3GPP 存取網路的 SGSN 選擇

以網路拓撲選擇 SGSN，如：所選擇的 SGSN 應指定重疊位置較多，這樣能減少

SGSN 改變的機會，當 SGSN 選擇的 SGSN 主要透過負載平衡的規則。在針對網路配置為低優先存取的 UE 群中，SGSN 的選擇通常被限制為相同的 SGSN。

（八）漫遊

在 ECM-CONNECTED 狀態期間應用於移動性的訊息，漫遊中可能不支援某些機敏相關服務或功能，或者在要求中通知 MME 僅用戶服務與功能，則 HSS 通過設定來限制該 MME 中的 UE 服務並發送訊息促使替換服務，如可用服務，MME 漫遊架構如下圖。

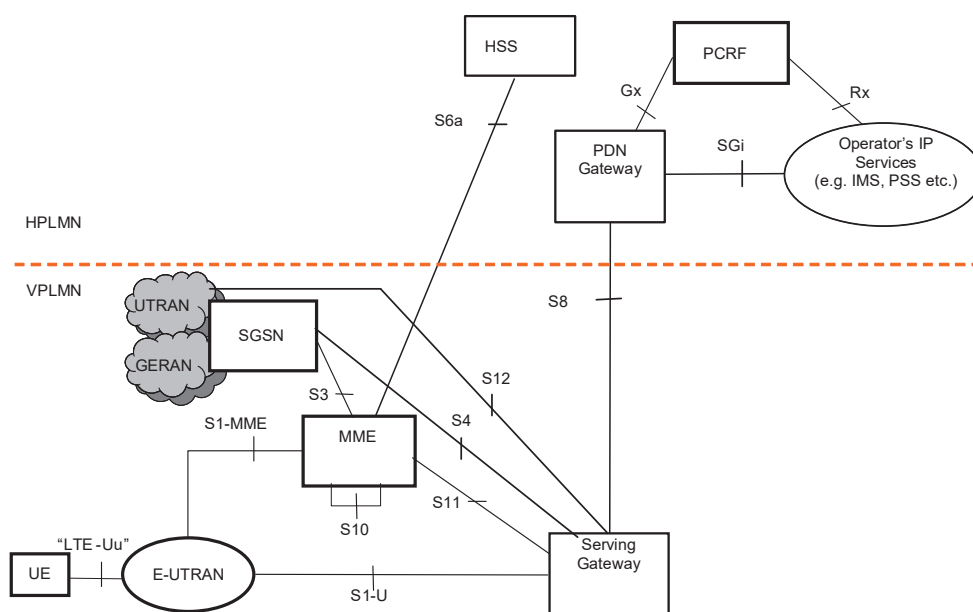


圖 5- 167 MME 漫遊架構圖

資料來源：3GPP TS 23.401

（九）驗證

在 AKA 流程適用於 E-UTRAN，流程一開始 MME 傳送訊息給 UE，UE 收到包含一隨機值 RAND 與 AUTN 的訊息，AUTN 為驗證 UE 的參數，UE 收到訊息後會檢查 AUTN 是否正確，如果正確，UE 會計算回覆的 RES 以及計算 RES 為回覆 MME 的訊息。

此流程讓 MME 傳送驗證資料的要求後取得 UE 文本，要求中包含 IMSI、所服務的電信業者，此流程同樣地網路類型僅適用於 E-UTRAN，最後就可以從 HSS 取得驗

證參數(RAND、AUTN、XRES)給 MME，其中 XRES 與 RES 這兩個參數是讓 MME 去驗證 UE，為了讓 UE 的參數不在 HSS 與 UE 之間直接的曝露出來，因此會加密成 XRES 從 HSS 送出，RES 從 UE 計算出來，最後再從 MME 進行驗證。

(十) 通道管理功能包括專用通道建立

EPC 透過 P-GW 連線服務提供 UE 通道以 S5/S8 的 GTP 協定，如果提供 IP 服務，EPS 通道是串連 S-GW 與 P-GW，在用戶資料(MME 設定初始值基於 HSS 所提供的相關)，在非漫遊情況下，MME 提供的連線能力，PCEF(Policy and Charging Enforcement Function)可以與 PCRF (Policy and Charging Rules Function)交換中進行改變。

在漫遊情況下，根據電信業者配置，MME 會降低連線能力的對應，這些從 HSS 取得的值將會設定在 MME 中，PCEF 與 PCRF 的交換訊息後，會改變 MME 提供的連線能力，但 PCEF 可拒絕通道的建立。

當 eNodeB 收到信令初始化高優先存取，eNodeB 處理 RRC 連線優先要求。當 MME 接收與驗證初始信令的建立階段，MME 建立 S1 優先權通道，MME 可以從要求上處理 UE 優先。

(十一) 合法信令流量監聽

這個功能是依照電信業者所依照當地的規定與提供執法單位進行監聽。

(十二) UE 可取得性程序

有兩種方式來確認 UE 在 EPC 的可取得性，UE 可取得與通知要求程序、UE 行為通知程序：

1. UE 可取得與通知要求程序是當 HSS 收到其他網路元件的要求 UE 可取得性，HSS 就會發送 URRP(UE Reachability Request Parameter)的參數給 MME 並設定可取得性為啟用，如果 MME 擁有 UE 資訊，可取得性參數就會回覆給 HSS。
2. UE 行為通知程序是在 MME 收到關於 UE 可取得性訊息時，像是 UE 啟用要求或 S-GW 切換到 2G/3G。如果 MME 包含 UE 資訊與可取得

性被設定為 UE 可取得，MME 應傳送 UE 行為通知訊息給 HSS 並清除 UE 的可取得性。當 HSS 收到 UE 行為通知訊息或更新位置訊息時，HSS 也會清除 UE 的可取得性。

二、 MME 元件架構

在 4G LTE，UE 與 eNodeB 之間的無線訊號部分為 E-UTRAN，而 MME 在 E-UTRAN 與核心網路之間扮演著橋樑，為 E-UTRAN 與核心網路之間所傳遞的控制面訊息進行管理，為不斷移動下使用網路服務，MME 就需要管理 UE 的移動，因為在核心網路中每個網路元件都受限於服務範圍，不管是無線訊號的服務範圍(如：eNodeB)、EPC 的服務範圍(如：2G/3G 與 4G 之間的切換)、連線數量上的限制(如：S-GW、MME)，以上都需要有訊息交換的流程，協助 UE 獲得更好的資源，如圖 5-168 中五個介面使用到的訊息交換程序圖。

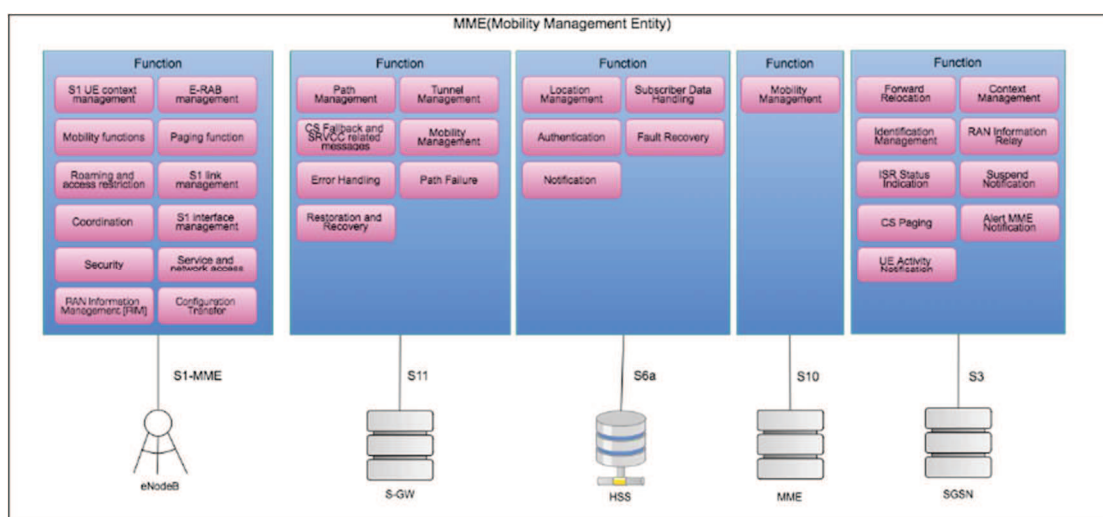


圖 5- 168 MME 介面架構圖

資料來源：本團隊整理

EPC 中包含許多的網路元件，功能包括負責 UE 初始化階段的驗證與呼叫的部分，在 UE 使用中或者移動中記錄 UE 的位置，並幫助 UE 在移動時讓網路服務不中斷，因此 MME 需要透過介面在網路元件之間進行溝通，而這些介面各自負責不同的訊息交換流程，如下：

(一) S1：MME-eNB

S1-MME：是與 eNodeB 之間溝通介面並提供功能³¹⁶，第一種是呼叫(Paging)UE，在 UE 省電模式下，UE 會進入 ECM-IDLE 模式，透過週期性地詢問是否收到呼叫，若在收到呼叫後就喚醒手機並執行服務，第二種是 UE 離開 eNodeB 服務範圍時，需要換手(Handover)到另外一個 eNodeB，這時候就會開始這個流程，第三種是 UE 在開機時要進行註冊，確認 UE 是否有權使用網路，並使用 EPS 安全性文本來進行身份驗證。

此介面使用在驗證 UE 身份、UE 的移動上進行管理與 UE 訊息的安全性，再將其功能細分到以下十二個功能進行探討³¹⁷：

1. EPS 安全性文本管理是眾多 UE 在 LTE_ACTIVE 的狀態下，MME 管理 UE 文本，在初始化階段交換所需要的文本並讓 UE 從 idle-to-active 的狀態轉換，就像導遊要擁有遊客的名單，在旅遊的都市或者城市中需要確認每個人的資料時，都能很快瞭解哪一位遊客的身份。
2. E-RAB(Evolved Radio Access Bearer)管理是 eNodeB 收到某一 RRC 安全性文本後，MME 會建立、調整、修改與釋出 E-UTRAN 的資源，讓使用者傳輸資料與提供相對應的連線能力給 eNodeB。
3. S1 連結管理是管理 E-UTRAN 與 EPC 之間提供可靠的傳輸，在 MME 發送要求之後相關的通道建立與釋放。
4. 移動性管理是協調 UE 在移動時，管理 EPS 安全性文本的傳遞，分成三種情況：跨 eNodeB、跨 MME、切換至 2G 或 3G，針對不同的情況啟動不同傳遞 EPS 安全性文本的程序。
5. 呼叫 UE 是指 MME 送出要求到特定追蹤範圍，從追蹤範圍下 eNodeBs 找到 UE 並呼叫該 UE，因為在 UE 閒置模式下，UE 會進入睡眠模式，透過週期性地詢問是否收到呼叫 UE，若在收到呼叫 UE 後就喚醒並執行服務。
6. 漫遊與存取限制是指在漫遊服務的過程中，為了保護用戶的安全性且限

³¹⁶ Olsson, M., & Mulligan, C. (2012). *EPC and 4G packet networks: driving the mobile broadband revolution*. Academic Press

³¹⁷ 3GPP TS 36.410 V14.0.0 (2017-03)

制於漫遊的費用上，就會有存取上的限制以及服務上的不同。

7. S1 介面管理：用於 MME 之間 eNodeB 傳遞訊息時，處理邏輯或訊號上的錯誤，另一方面是失敗事件發生後，MME 與 eNodeB 進行重新連線所需要的流程。
8. 協調管理是包含①過載控制、②NAS 的 MME 選擇，①過載情況可能發生於 MME 服務的 eNodeB，MME 有太多的訊息需要同時處理，或者傳遞訊息到無效的 eNodeB 造成 MME 過載的情況，MME 就必須使用控制過載的功能；在② NAS 的 MME 選擇是 UE 在初始化過程中需要在眾多的 MME 中選擇一個 MME 來負責 UE 的溝通，在 eNodeB 分配 MME 的過程中，讓 MME 能夠承受 UE 的訊息處理數量，不至於讓 MME 癱瘓或者停止運作。
9. 安全性管理主要是資料加密，不管是 UE 在傳遞控制訊息或者用戶的網際網路服務，為了確保用戶的資訊安全性，提供了完整性與機密性加密方式，兩者皆有不同的安全性等級來使用加密演算法，這兩個的演算法依附複雜度目前分為四級(完整性：EIA0、EIA1、EIA2、EIA3，機密性：EEA0、EEA1、EEA2、EEA3)，通常會使用最複雜的加密演算法進行保護。
10. 服務與網路存取：記錄 UE 在 EPC 的行為與記錄 UE 的位置，主要為了在呼叫(Paging)時，能夠找到 UE 所服務的 eNodeB，如：地震、颱風等，關於用戶人身安全的突發性事件的訊息發送。
11. eNodeB 資訊管理(RAN Information Management)，當 UE 移動到 eNodeB 範圍之外時，就必須要將 UE 的資訊移交給另一個 eNodeB 來進行服務，讓 UE 能夠在不同的 eNodeB 下繼續使用網路。
12. 配置轉移是當另一 eNodeB 被啟動或者設定出現錯誤時，能夠快速的將 eNodeB 的參數設定交換至另一個 eNodeB，讓新的 eNodeB 能夠快速執行服務。

以上描述了 S1-MME 介面包含了關於 eNodeB 及 UE 方面的功能，主要影響著 UE 能否在移動中，不間斷地使用服務，與 UE 在資料傳輸中的安全性包含加密方式、金鑰的管理(如：EPS 安全性文本、MME 與 UE 之間的驗證資料)，如：跨 eNodeB 的訊息交換等，皆是透過 S1-MME 介面進行協調的部分。

(二) S11：MME-S-GW

是 MME 與 S-GW 之間通道的管理，網路服務封包路徑的選擇，在 S1 介面中 eNodeB 有兩個溝通介面：S1-MME 與 S1-U，S1-MME 主要是管理 UE 的行為與初始連線階段的驗證，而 S1-U 就是在與 S-GW 建立連線後，eNodeB 直接傳輸關於用戶面封包的遞送，MME 分配多個 S-GW 給 UE 使用來達成負載平衡(Load Balancing)，在 S11 介面中 MME 扮演著幫助 UE 選擇 S-GW 的角色。

S11 主要用在 UE 驗證完成身份後，要指定 S-GW 給 UE，讓 UE 不僅能夠使用網際網路服務，也讓 UE 不壅塞於同一個 S-GW 之下，我們參考 TS 29.274³¹⁸描述了七種功能，詳細介紹如下：

1. 路徑管理(Path Management)：在固定時間發出要求與取得回覆，從流程中的訊息交換確認 MME 與 S-GW 之間的介面正常運作。
2. 通道管理(Tunnel Management)：管理 UE 網路服務的通道，在 UE 完成驗證後，與 P-GW 建立通道，在移動性程序發生時，更動 UE 網路服務通道。
3. 移動性管理(Mobility Management)：用於管理 UE 註冊與離線、UE 的傳輸能力、eNodeB 換手時 S-GW 的更動，主要是在 UE 的初始化或者移動時的狀態，像是追蹤範圍更新程序伴隨 S-GW 更動發生時，就必須要重新 S-GW 的選擇，或者 S1、X2(eNodeB 之間)介面換手伴隨 S-GW 改變時，此流程會在 S11 介面進行訊息交換像是 UE 的資訊(如：IMSI、IMEI 與用戶位置資訊、IP 等)。
4. 電路交換切換等相關訊息交換程序(CS Fallback and SRVCC related messages)：從封包交換切換到電路交換時，MME 透過 S11 介面會通知 S-GW 給 P-GW，中斷 UE 網路服務的通道。在 UE 從電路交換切換至封包交換時，MME 再透過 S11 介面會恢復 UE 網路服務的通道並繼續使用網路服務。
5. 錯誤處理程序(Error Handling)用在 GTP 可能會因為封包內容錯誤或者某個位元的遺漏，這些訊息就應該進行重送或者錯誤回復等功能。

³¹⁸ 3GPP TS 29.274 V15.0.0 (2017-06)

6. 路徑錯誤(Path Failure)在固定時間發出的要求與回覆程序中，未在正確的時間內取得訊息，此程序就會為 MME 與 S-GW 連線發生錯誤時的處理，可能在 MME 讓太多 UEs 指向同個 S-GW 就會造成錯誤產生，例如 S-GW 需要同接受多個 UE 的封包，造成 S-GW 的過載情況並選擇丟棄或者無法在時間內回覆，最後造成錯誤的結果必須重新建立連線。
7. 回復與復原(Restoration and Recovery)是在 MME 與 S-GW 發生失敗的處理，如：S-GW 或 MME 在路徑管理時發生錯誤，該如何重新恢復連線。

(三) S3-MME&SGSN

此介面在 2G/3G 與 EPC 之間，進行用戶與通道的資訊交換。在 3GPP 規範中，SGSN 主要是用於網路服務切換至 2G 與 3G，因此在 LTE 切換至 2G 或 3G 時，MME 會交換 UE 的資訊給 SGSN，也在 SGSN 提供 UE 網路服務時給予 UE 的行為記錄，包含以下功能：

1. 轉送重新定位：當 UE 需要從 2G/3G 至 4G 或 4G 至 2G/3G，需要將 UE 定位從 MME 至 SGSN 或從 SGSN 至 MME。
2. 文本管理：在原 MME/SGSN 與新的 SGSN/MME 之間，執行 TAU(Track Area Update)或 RAU(Routing Area Update)程序來交換 UE 的移動性管理與 EPS 通道的文本。
3. 識別(Identification)管理：如果 UE 使用暫時識別或在改變 MME/SGSN 處於未註冊狀態，新 MME/SGSN 就會要求原 MME/SGSN 取得 IMSI 辨識 UE 身分。
4. eNodeB 中繼資訊：若存在中繼 eNodeB 資訊，在 MME 與 SGSN 之間切換時傳遞訊息，讓 SGSN 在提供 UE 網路服務時，SGSN 指定將封包傳遞至中繼 eNodeB。
5. ISR(Idle state Signalling Reduction) 狀態指示：為處理 UE 的 ISR 狀態，在 MME 與 SGSN 之間換手後，S-GW 錯誤發生時回復封包網路連線與 HSS 回復程序。
6. 中斷通知：為中斷的 UE 收到的封包，在 S3 介面上由 SGSN 發送到 MME，在 S11 介面上由 MME 發送到 S-GW，在 S5 / S8 介面上由 SGW

發送到 P-GW，P-GW 來控制接收的封包。

7. 電路交換的 UE 呼叫：在 ISR 狀態時，MME 會要求與服務 UE 的 SGSN 進行呼叫。
8. 警告 MME 通知：在 ISR 狀態下，MME 送出要求至 SGSN 並取得 UE 的行為紀錄。
9. UE 行為通知：在 ISR 狀態下，SGSN 送出要求至 MME 並取得 UE 的行為紀錄。

(四) S6a：MME-HSS

S6a 是 MME 與 HSS 之間的溝通介面，負責 HSS 與 MME 之間的訊息交換，HSS 是用戶能夠使用網路服務的開關，S6a 介面溝通的內容包含開啟用戶的連線與驗證用戶存取網路的資料，這些資料包括：用戶能夠存取的權限、網路品質以及用戶所屬的電信等。

HSS 儲存著用戶的資訊，此介面主要在註冊時提供驗證 UE 的身分，透過密鑰與公鑰的計算，雙向驗證 UE 與 EPC，通過驗證後在提供相對應的服務包含提供用戶的網路服務能力，HSS 主要管理用戶的資訊(如：位置、服務)與曾經連線過的 eNodeB 或者出現過的地區等，透過 MME 一直取得 UE 資訊回傳至 HSS，讓 HSS 能夠獲得 UE 的即時位置資訊，這些功能皆由 S6a 介面來完成訊息交換，該介面具備以下五種功能³¹⁹：

1. 位置管理程序(Location Management Procedures)用在管理 UE 的位置資訊，當 UE 在註冊之後就會開始更新，到 UE 離開 EPC 或者 UE 離線之後，就會停止更新。
2. 用戶資料處理程序(Subscriber Data Handling Procedures)在記錄與處理用戶的服務項目與用戶的行為，如：在電信業者或者管理者進行更動用戶服務項目時，UE 已在服務範圍內，就會即時更動其服務項目，在用戶服務期間 HSS 會持續要求 MME 來取得用戶的位置資訊，並且記錄用戶的使用網路服務的行為。

³¹⁹ 3GPP TS 29.272 V15.0.0, 2017/6.

3. 驗證程序(Authentication Procedures) 在 UE 註冊時 MME 與 UE 需要進行驗證，MME 需要透過 HSS 取得用戶資訊，再經由擷取用戶的 IMSI 與金鑰取得身分。
4. 錯誤回復程序(Fault Recovery Procedures)屬於錯誤處理的部分，當 S6a 介面發生中斷或者 MME 或 HSS 其一方發生連線問題，就要執行此流程，如：UE 位置更新失敗、用戶資料驗證失敗等。
5. 通知程序(Notification Procedures)用在 HSS 通知 MME 來獲取資訊、讓 HSS 改變 P-GW、在 MME 之間無法更新位置執行時，由 HSS 產生取消追蹤位置給 SGSN。

(五) S10：MME-MME

S10 是 MME 與 MME 之間的溝通介面³²⁰，主要在 MME 之間換手時的管理與訊息的傳遞，在 UE 移動時因為 eNodeB 服務範圍的關係，必須在範圍交界處進行換手，為了讓 UE 的服務不中斷，每個 MME 也會管理多個 eNodeB，當 UE 移動範圍超出 MME 的追蹤範圍，S10 介面就會進行訊息交換，UE 資訊就會藉由 S10 來換手到另一個 MME。

此部份參考 TS 33.401，歸類為以下流程：

1. 傳輸 IMSI、驗證資料於同網路服務區域(同核網)

此流程在新 MME 與原 MME 於相同網路服務區域時，原 MME 會提供驗證資料給新 MME，新的 MME 在一開始會收到原 MME 的追蹤區域資訊，去分辨 MME 是否是屬於同網路服務區域。原 MME 會資料庫搜尋用戶資料，原 MME 會回覆追蹤範圍更新訊息，如果有搜尋到用戶且 NAS 完整性加密檢查成功，原 MME 會回覆包含 IMSI、EPS 安全性文本。原 MME 即刪除已傳送的 EPS 安全性文本，如果用戶會被搜尋到或 NAS 完整性加密檢查失敗，原 MME 會回覆用戶無法被辨識。

2. 傳送 IMSI 於不同網路服務區域(跨核網)

一般來說，IMSI 與驗證資料是能夠在不同網路服務區域間傳輸，但特殊情形下，

³²⁰ LTE and Beyond, "Interfaces and their protocol stacks", 2012/1/8. [Online]. Available: <http://www.lteandbeyond.com/2012/01/interfaces-and-their-protocol-stacks.html>

EPS 安全性文本的傳輸有限制條件，當存在未使用的 EPS 安全性文本與使用中的 UE 文本時，應不能夠在不同的網路服務區域(PLMNs)間傳輸未使用的 EPS 安全性文本。

3. 傳輸 IMSI 與 3G 驗證參數於不同 MME 間或 MME 與 SGSN

此部分流程用在 3G 驗證資料傳輸於相同網路服務間，遵守 3G 驗證資料不應該在 MME 間傳送。若 MME 與 SGSN 於相同網路服務區域下，SGSN 能傳送未使用的 3G 驗證資料給 MME。儲存在 MME 的 3G 驗證資料，可以被傳送到相同網路服務區域的 SGSN。儲存在 MME 的 3G 驗證資料，不能被傳送到不同網路服務區域的 SGSN。

三、 介面安全性研究

本項目參考 3GPPTS 33.401，針對 MME 的安全性介面程序與步驟，整理 NAS 金鑰、UE 驗證資料的管理與在換手時分成同核心網路與跨核心網路，主要在安全性介面上於 S1、S3、S6a、S10、S11 有著不同功能，整理規範的安全性程序與規則。

(一) EPS 與 NAS 安全性文本

1. 金鑰產生

K 為主要存在 SIM 卡與 HSS 的金鑰，如圖 5-169 在驗證階段會產生 RAND 與 SQN，RAND 為隨機值用於加密 K 值後產生的 XRES、CK、IK，將 CK 與 IK 加密成 K_{ASME}，EPS 安全性文本就是 RAND、XRES、K_{ASME} 與 AUTN。

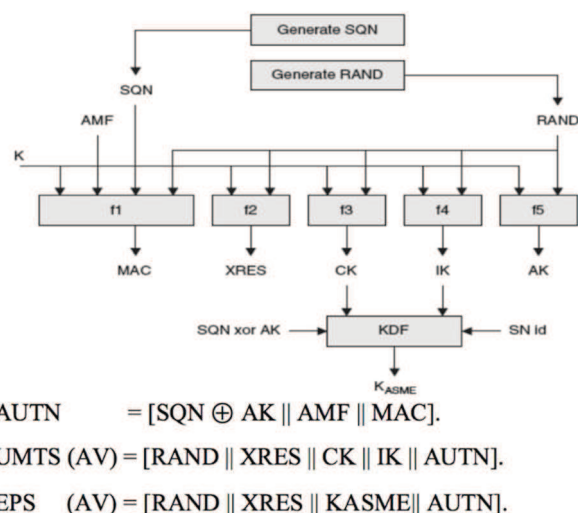


圖 5- 169 EPS 產生過程

資料來源：IEEE³²¹

2. 金鑰驗證

如圖 5-170，MME 會保留 XRES 與傳送其他參數到 UE，讓 UE 在運算過後回傳運算結果 RES 給 MME，而 XRES 就是用於驗證 UE 的身分，並確認從 HSS 收到的 XRES 等於 UE 回傳的 RES，就完成了身分驗證，接下來運用產生的金鑰計算出完整性金鑰與機密性金鑰，稱為 NAS(Non Access Stratum)安全性文本。

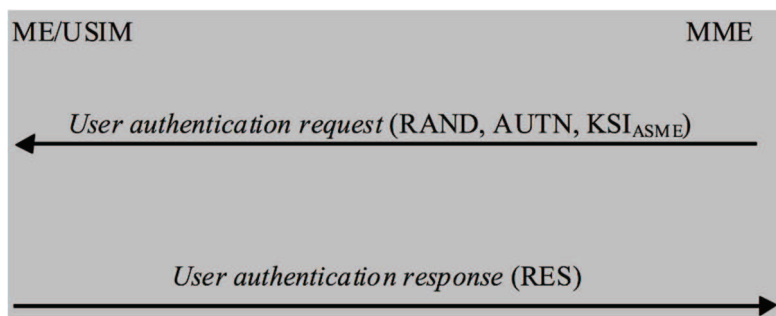


圖 5- 170 UE 驗證程序圖

資料來源：3GPP TS 33.401

3. 金鑰驗證的演變

³²¹ HASSAN, Zakaria Zakaria; ELGARF, Talaat A.; ZEKRY, Abdelhalim. Modifying authentication techniques in mobile communication systems. In: Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2014 Third International Conference on. IEEE, 2014. p. 38-44

在 2G³²²時，K 僅透過隨機產生的 RAND 加密產生 Kc 與 SRES，這樣單向驗證會導致金鑰容易被解開，因此在 3G(UMTS)³²³採用多重加密方式，從 HSS 先產生隨機的 RAND 與準備進行加密的 SQN，利用 AMF(Authentication Management Field)³²⁴的欄位檢查是否為 UMTS 或 LTE，接下來用 SQN 與 RAND 還有 K 產生 MAC(K、AMF、SQN、RAND 與 f_1 演算法)、XRES(K、RAND 與 f_2 演算法)、CK(K、RAND 與 f_3 演算法)、IK(K、RAND 與 f_4 演算法)、AK(K、RAND 與 f_5 演算法)，而 SQN 以 XOR 方式從 SQN 與 AK 來產生，產生出 UMTS 的驗證資料，將這些參數傳送到 UE 讓 UE 產生 SRES 來驗證(請參考圖 5-171)。

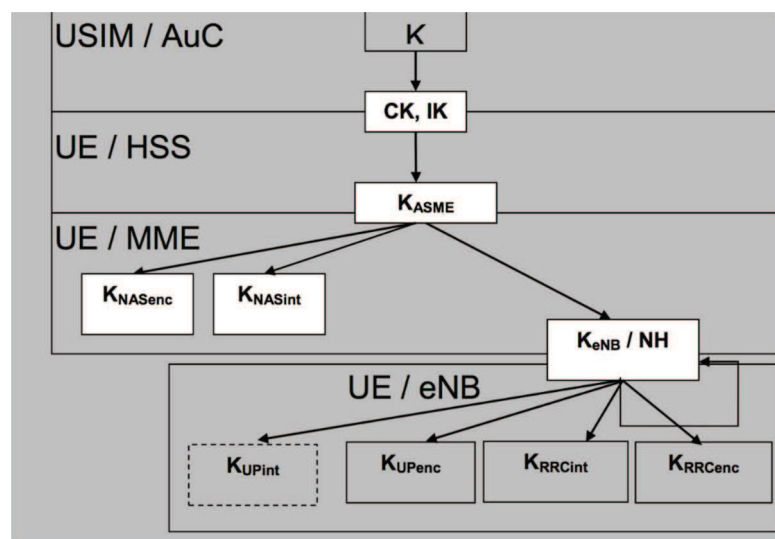


圖 5- 171 K_{ASME} 產生圖

資料來源：3GPP TS 33.401

4. NAS 信令金鑰與演算法

關於 NAS 信令的部份，K_{ASME} 是用在產生 NAS 信令的完整性加密與機密性加密的金鑰：完整性加密為檢查 NAS 訊息是否完整，而機密性加密為檢查 NAS 訊息是否

³²² Chang, C. C., Lee, J. S., & Chang, Y. F. (2005). Efficient authentication protocols of GSM. *Computer Communications*, 28(8), 921-928.

³²³ Choudhary, Anilmit, and Randhir Bhandari. "Analysis of UMTS (3G) Authentication and Key Agreement Protocol (AKA) for LTE (4G) Network." *International Journal on Recent and Innovation Trends in Computing and Communication* 3.4 (2015): 2146-2149.

³²⁴ 3GPP TS 33.102: "3G security; Security architecture"

進行加密，其演算法現行的方式包括³²⁵：

- (1) 完整性加密為 EIA0、機密性加密為 EEA0：使用 NULL 演算法。
- (2) 完整性加密為 EIA1、機密性加密為 EEA1：使用 SNOW 3G 演算法。
- (3) 完整性加密為 EIA2、機密性加密為 EEA2：使用 AES 加密演算法。
- (4) 完整性加密為 EIA3、機密性加密為 EEA3：使用 ZUC 加密演算法，在 EIA0、EIA1 與 EIA2 應該實作在 NAS 通道加密演算法中，EIA3 則是選擇性的實作選項。
- (5) 在 UE 開機時應檢查 SIM 卡是否被移除、SIM 卡運算的 EPS 安全性文本不相同與 SIM 卡不存在，以上情形應該刪除 UE 內的所有 EPS 安全性文本。
- (6) IMSI 與 IMEI 不應該在建立 NAS 通道前傳輸。
- (7) 其中在 AUTN 的 separation bit 檢查值是否為 1，若不是則是用在 2G SIM 或其應用程式上，在 4G 中 2G SIM 是不被允許存取網路的。
- (8) EIA0 或 EEA0 僅使用於 IMS 緊急通道。
- (9) EPS 安全性文本應該在開機時被清除。

(二) 安全模式指令

安全模式由 MME 與 UE 之間的交換訊息所成立(如圖 5-172)，目的在於安全的建立 NAS 安全性文本，防止在 UE 與 MME 之間有中間人攻擊，因為在註冊(Attach)與追蹤區域更新(TAU)時容易從之間的空中攔截訊息，而成功收到安全模式訊息前，所有的註冊與追蹤區域更新訊息都會被拒絕。

³²⁵ Orhanou, G., Hajji, S. E., Bentaleb, Y., & Laassiri, J. (2011). EPS confidentiality and integrity mechanisms algorithmic approach. *arXiv preprint arXiv:1102.5191*.

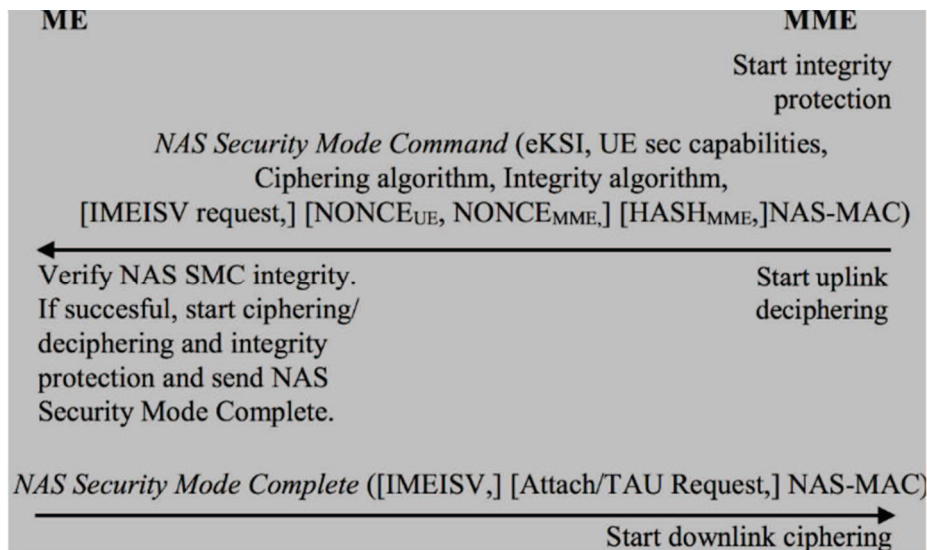


圖 5- 172 安全模式程序圖

資料來源：3GPP TS 33.401

在註冊或者追蹤區域更新的程序時，MME 與 UE 會交換安全模式指令的訊息，在 UE 接收到要求後，會開始驗證安全模式、SIM 卡內的金鑰檢查與完整性及機密性保護演算法是否支援，若檢查完成就會回覆 IMSI 與註冊或追蹤區域更新的要求，且對應在 MME 的要求中若包含 HASH 值就會跟著運算 HASH 回覆在註冊或追蹤區域更新訊息中。

安全模式指令訊息應包括重送 UE 的安全性能力，因此所選的 NAS 演算法會定義 UE 中參數 NONCE 與 MME 中參數 NONCE 來預防重送攻擊（NONCE 在三向交換中主要是用於預防重送攻擊所產生的參數）。在 NAS 信令未被完整性保護時，MME 會依照訊息內容產生 HASH 值，確保不會被駭客進行修改與完整性。

針對通過驗證的 UE 與核心網路之間的通訊應該確認以下需求：❶確實使用 NAS 機密性加密與完整性加密❷演算法的選擇應符合 UE 的安全模式與核心網路允許的安全模式。❸為了防止 UE 更動加密演算法，應確認 UE 的完整性保護的方式。

（三） EPS 安全性文本管理

1. EPS 移動管理(EMM, EPS Mobility Management)與 EPS 通道管理(ECM, EPS Connection Management)

EPS 移動管理(EPS Mobility Management)³²⁶是一種用在無線介面(LTE-Uu)的協定，EMM 有兩種狀態，EMM-DEREGISTERED 與 EMM-REGISTERED，在 EMM-DEREGISTERED 下代表 UE 位置未知且與沒有建立與 MME 的 NAS 通道，EMM-REGISTERED 則是已經建立 NAS 通道。

ECM³²⁷指的是在 NAS 通道的建立狀態，包括對用戶層資料的連線與無線訊號的資源，分為 ECM-IDLE 與 ECM-CONNECTED，ECM-IDLE 是指與 MME 之間沒有 NAS 通道存在，當然包括無線訊號與用戶層資料的連線，ECM-CONNECTED 則反之。

接下來分別介紹 EMM 狀態與 ECM 狀態下，UE 與 MME 之間 EPS 安全性文本與 NAS 安全性文本的管理，這兩樣狀態之間的轉換可能導致安全性文本內的金鑰遭竄改或進行模擬。

(1) EMM-DEREGISTERED

在 EMM-DEREGISTERED 狀態時，為維持 UE 與 MME 安全性文本的一致性，若有從 3G 對應的 EPS 安全性文本與先前完整的 EPS 安全性文本，將會維持在先前完整的 EPS 安全性文本，還需要將先前不完整的 EPS 安全性文本與從 3G 對應的 EPS 安全性文本刪除。

在註冊拒絕、離線與追蹤區域拒絕，以上三種情況處理 EPS 安全性文本：

- (I) 註冊拒絕：應刪除所有驗證時產生的 EPS 安全性文本。
- (II) 離線：UE 若為關機狀態，則刪除所有驗證時產生的安全性文本，若不為關機狀態則保持儲存。MME 應在 UE 無線訊號不佳與 MME 進行重新註冊時，皆為 EPS 安全性文本進行保存。若 HSS 的訊息為身分撤銷應將 UE 與 MME 內的 EPS 安全性文本進行刪除。
- (III) 追蹤區域拒絕：刪除先前未通過驗證的 EPS 安全性文本與從 3G 對應的 EPS 安全性文本。

(2) EMM-REGISTERED

當 UE 要從 EMM-DEREGISTERED 到 EMM-REGISTERED，若 EPS 安全性文本

³²⁶ 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3"

³²⁷ Karandikar, A., Akhtar, N., & Mehta, M. (2017). *Mobility Management in LTE Heterogeneous Networks*. Springer Singapore.

無法從 UE 取得，就需要從 SIM 卡內重新計算後取得，並且從新的 EPS 安全性文本產生 NAS 的安全性文本(完整性與機密性保護的金鑰)。

當 UE 內儲存著 EPS 安全性文本，NAS 訊息經過完整性與機密性保護，雖然與 MME 當前產生的 EPS 安全性文本無法對應，經過驗證後為正確的 EPS 安全性文本，MME 就需要將該 EPS 安全性文本與 UE 同步，並刪除 MME 當前產生的 EPS 安全性文本。

(3) ECM-CONNECTED

UE 傳送建立 NAS 通道的訊息，MME 應可以檢查是否驗證是必須的，加密保護無線通道建立與用戶層資料保護金鑰。建立 NAS 通道的訊息應使用 UE 的 EPS 安全性文本用於完整性保護，若無 EPS 安全性文本應於訊息中顯示”無可取得之金鑰”。

K_{ASME} 建立於 AKA 程序，依照換手或閒置模式的程序，其他 MME 產生的安全性文本，當 ECM-IDLE 時 MME 應保存 EPS 安全性文本，因為 eNodeB 就會在無線釋放後就會刪除金鑰。

(4) ECM-IDLE

MME 與 UE 應保有 EPS NAS 安全性文本，除了以下情況 K_{ASME} 應被刪除：

- (I) 當 UE 無線加密已建立、MME 也應建立安全模式完成產生新 K_{ASME} ，MME 應由舊的 K_{ASME} 來傳遞狀態轉換的訊息，直到 UE 文本修改的程序，並完成由新的 K_{ASME} 產生無線金鑰。
- (II) 在 UE 文本改變程序時，MME 就會在 S10 轉送定向訊息內包括新與舊的 K_{ASME} 。
- (III) 當(II)程序完成後，依然會執行 UE 文本改變程序來更動 K_{ASME} 。

2. 在 LTE 網路下換手

(1) X2 換手

在路徑轉換訊息，eNodeB 應傳送 UE 的安全模式並保持原有安全模式，MME 的角色是要去驗證 UE 安全模式是否等同於原本 eNodeB 時的安全模式，若兩者不為相

同時應紀錄與額外的功能如警告。

(2) S10 換手

在 MME 進行換手時，針對 UE 安全性文本與支援的演算法不同，需要從 K_{ASME} 產生新的 NAS 金鑰，所以在新的 MME 建立 NAS 安全模式程序訊息就需要包括完整性與機密性演算法與 UE 安全模式(為了避免駭客從中修改)給 UE，MME 應選擇 NAS 演算法中較優先的選項。

3. LTE 與 3G 之間換手

在閒置模式下的兩種狀態，從 LTE 轉移到 3G 的閒置模式與閒置模式信令減少 (ISR, Idle mode Signaling Reduction)，這兩個狀態下會需要產生 3G 所使用的金鑰³²⁸，而 MME 與 UE 就要從 K_{ASME} 產生 3G 的金鑰 CK 與 IK，稱之為 3G 的安全性文本。

反之，當閒置模式下從 3G 轉移到 LTE 時或閒置模式信令減少時，MME 將不會使用 SGSN(S3 介面)參考任何 UE 安全模式，當 SGSN 驗證完成的 UE，可以允許 UE 與 MME 依照 CK 與 IK 產生對應的 EPS 安全性文本。在 3G 中的 P-TMSI 用於在用戶層資料使用的暫時身分，若存在於 GUTI 中，就會產生對應的 EPS 安全性文本，若存在當前的 EPS 安全性文本，就應該有 GUTI 在 TAU 訊息中，若不存在 GUTI 時 MME 就應該當作 EPS 安全性文本不存在。

MME 若收到 UE 的 P-TMSI 的身分，MME 就需要跟 SGSN 要求 3G 安全性文本，這時若從 SGSN 收到 2G 的安全模式，MME 就應該拒絕此程序。

MME 保有 EPS 安全性文本，若追蹤區域訊息未經過完整性保護，MME 應該產生新的對應 EPS 安全性文本，MME 會產生 NONCE 與從 UE 接收到的 NONCE 從 P-TMSI 跟 3G 的安全性文本產生新的對應的 K_{ASME} 。

為避免 EPS 安全性文本與 UE 配對錯誤，因此 3GPP TS 33.401 有制定規則來遵守：

³²⁸ Choudhury, H., Roychoudhury, B., & Saikia, D. K. (2012, June). Enhancing user identity privacy in LTE. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 949-957). IEEE.

- (1) 當安全模式程序正在執行時，MME 不應建立 NAS 安全性文本或者 UE 文本修改程序，並且包含 UE 與 eNodeB 之間的 K_{eNB} 。
- (2) 若 NAS 安全性文本件建立階段或 UE 文本修改包括 K_{eNB} 時，MME 不應該執行安全模式程序。
- (3) 當 UE 已經有無線通道的加密保護，MME 也已經開始使用 NAS 安全模式並啟用新的金鑰，MME 應在換手訊息與路徑轉換訊息內使用舊的金鑰，直到新的金鑰已經完成 UE 文本修改程序。
- (4) 當為了 MME 換手或者與 3G 之間換手，MME 建立 NAS 安全模式並產生了新的 K_{ASME} ，MME 應等待完成 NAS 安全模式後再開始 MME 換手程序或者 3G 換手的程序。
- (5) 當為了 MME 換手而產生新的 K_{eNB} 的時候，MME 應等到 3G 到 LTE 的換手程序完成才能開始 UE 文本修改程序。
- (6) MME 在執行 NAS 安全模式程序並完成產生 K_{ASME} 時，應在 UE 文本修改程序中，同時加入新與舊的 K_{ASME} 再轉送重新定位訊息。
- (7) MME 在執行轉送重新定位程序時，MME 應使用新的 K_{ASME} 在 NAS 程序，但是在 AS 安全性文本中需要使用舊的 K_{ASME} 執行換手程序與路徑轉換程序，直到 UE 文本修改程序完成。
- (8) 當 MME 發送轉送重新定位程序到新的 MME 後，原 MME 不應再接收任何 NAS 訊息，除非換手的程序失敗。
- (9) K_{ASME} 不應被轉移到其他核心網路。

4. IMS(IP Multimedia Service)緊急通道

IMS 緊急通道是用在 IMS 的緊急通話上，過去 2G 與 3G 都是使用電路交換的方式去使用緊急通話，LTE 下支援以 IMS 進行通話，才出現 IMS 緊急服務，IMS 緊急通道是能夠在驗證與未驗證狀態下皆可執行，而 MME 的工作就是在審核 UE，主要依照電商的設定是否允許使用緊急通道的註冊訊息，而驗證的狀態也分成以下四種：

- 驗證過的 UEs：在 UE 不為限制服務模式，僅有完整的驗證 UE 並註冊位置，且在用戶層資料傳輸的連線，UE 才能夠建立 IMS 緊急通道。
- IMSI 驗證過的 UEs：UE 必須擁有合法的 IMSI，UE 雖已驗證，但是因

為 UE 的位置關係導致處於限制服務模式，除此之外未經驗證的 UE 都將被 MME 拒絕建立通道。

- 擁有 IMSI 但未驗證的 UEs：在 UE 擁有 IMSI 時，若 UE 驗證未通過，UE 將會被拒絕存取並記錄其行為，IMEI 將會被用來辨識 UE 的身分，但是若 UE 僅有 IMEI 的話通道也是無法建立。
- 所有 UEs 皆允許：除了以上三點的情況外，包括僅有 IMEI 的 UEs，IMEI 就會被用來記錄 UE 的身分。

(1) 已驗證的 IMS 緊急通道

UE 在非限制服務模式，當尚未註冊 EPS 緊急通道服務時，應已經註冊。當 IMS 緊急通道建立後，NAS 的完整性或機密性保護使用中，但是檢查完整性與機密性失敗，應視為正確的 EPS 通道。

註冊或者服務要求程序時，但 UE 驗證失敗，此時 UE 若想要建立緊急通道，應重新執行註冊程序。在未驗證的 IMS 緊急通道不允許時，MME 收到 UE 要求建立緊急通道且以 EPS 安全性文本進行完整性保護，若 UE 的驗證失敗，則應要求重新執行 UE 驗證程序。

當緊急通道的註冊程序執行中且驗證 UE 或者 MME 失敗，但完整性保護金鑰是正確的，此時緊急通道應執行其中之一的程序：

- (I) 當未驗證的緊急通道是允許的，UE 就不需要重新進行註冊程序，MME 應要求使用零號完整性與機密性保護，UE 與 MME 之間就不會共用 EPS 安全性文本。
- (II) 當未驗證的緊急通道是允許的，且 UE 也存在用戶層資料連線時，MME 可以繼續使用 EPS 安全性文本。

(2) 未驗證的 IMS 緊急通道

在 UE 已經註冊並通過驗證正常的 EPS 通道，才會使得 IMS 緊急通道註冊失敗，以及在限制服務模式下，UE 無法進行身分驗證或者應用完整性或機密性保護時，才能使用 IMS 緊急通道。

UE 在無法被 MME 驗證身分稱為限制服務模式，此時是能夠建立緊急通話與緊急註冊程序，透過緊急註冊程序與 MME 建立 NAS 通道，NAS 訊息就會使用零號機密性保護與完整性保護。無法進行完整性或機密性保護的前提，如以下情況：

- (I) 在沒有 SIM 卡的情況下。
- (II) 所使用的網路發生錯誤，無法取得驗證資料。
- (III) 因為 SIM 卡導致 UE 進入限制服務模式(可能是沒有漫遊的服務)。
- (IV) 在驗證 UE 的過程中，SIM 卡提供的資料無法成功驗證身分。

四、 攻擊行為分析

MME 在 UE 與核網之間搭起橋樑，進行 UE 的身分驗證、驗證 EPS 安全行文本、管理 NAS、RRC(無線訊號)、UP(S1-U 用戶層資料)的安全模式，讓 UE 的訊息都能夠進行加密，在前提下，MME 的運作必須是穩定的，若 MME 出現系統停滯或反應緩慢，將會直接影響 UE 的網路服務，因此我們將分析如何降低 UE 的安全模式、增加 MME 資源消耗、影響降低加密方式的複雜度，達成 MME 的運作受影響並且讓其他的 UE 服務不穩定，從攻擊行為來分析執行步驟，在第六章節整理 3GPP 規範內的檢測項目，檢視現有的組織已經將這些威脅訂定規範，達到 MME 安全性的提升。

(一) 註冊程序攻擊

1. 重新同步

在驗證資料訊息中，有兩種訊息結果回傳至 MME，一為 IMSI、電商號碼、網路種類，❶用於 UE 完成驗證後 MME 可以驗證 UE 的身分，一為同步錯誤訊息，此案例用於同步錯誤發生。

如圖 5-173，❷在 UE 送出同步錯誤訊息並包括 AUTS 後，MME 會發送同步錯誤訊息與參數 RAND、AUTS 給 HSS，HSS 會依照 AUTS 解密出來的 SQN 是否與 HSS 內 SQN 的數值對應，如果有對應就會依照 SQN 來產生新的 AUTN，若沒有的話就會檢查 AUTS 解密後的其他參數(K、RAND 與 AMF)，檢查完成後就將 HSS 內的 SQN 直接同步成 UE 的 SQN，接下來❸回傳 EPS 安全性文本給 UE 進行驗證。

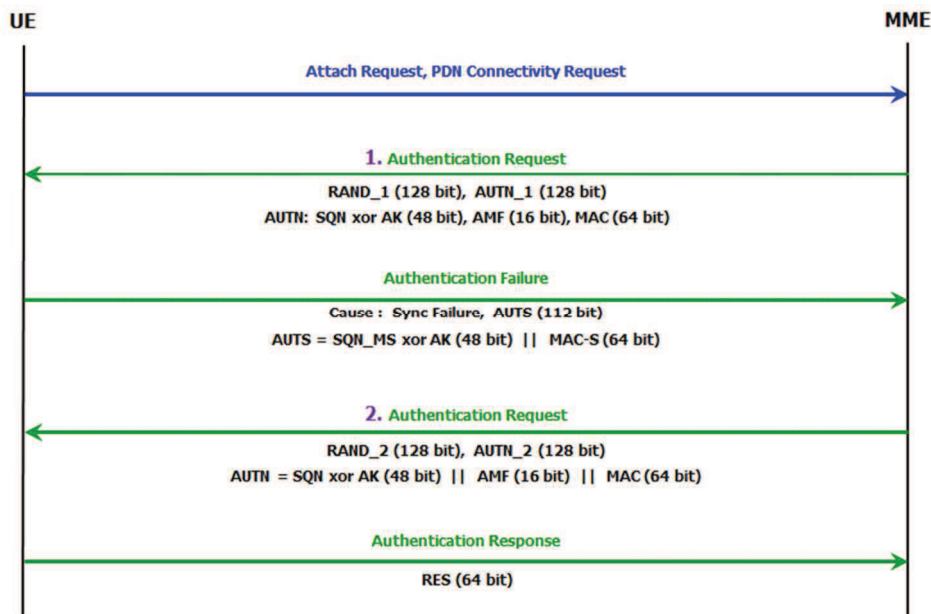


圖 5-173 重新同步訊息交換流程圖

資料來源：Forensics and IT-Security, LTE Re-Authentication after network caused SQN failure³²⁹

駭客攻擊的方式主要透過 UE 與 HSS 進行模擬，當 MME 收到驗證失敗，包含 RAND 以及 AUTS 時，MME 應該在收到 HSS 的驗證錯誤訊息時，從 UE 收到 AUTS，若無法收到 AUTS 情況下重複向 HSS 進行驗證，可能會導致 UE 永久的無法使用服務。

2. 完整性檢測

在同核網內的 MME 換手時(如下圖)，新的 MME 會先將追蹤區域更新訊息與舊的 GUTI 傳給原 MME，原 MME 就要檢查追蹤區域更新訊息的完整性，以及原 GUTI 去查詢用戶資料，在經過確認後原 MME 就會回傳 IMSI 與 EPS 安全性文本。

³²⁹ ng4T, [Online]. Available:<http://www.ng4t.com/forensics.html>

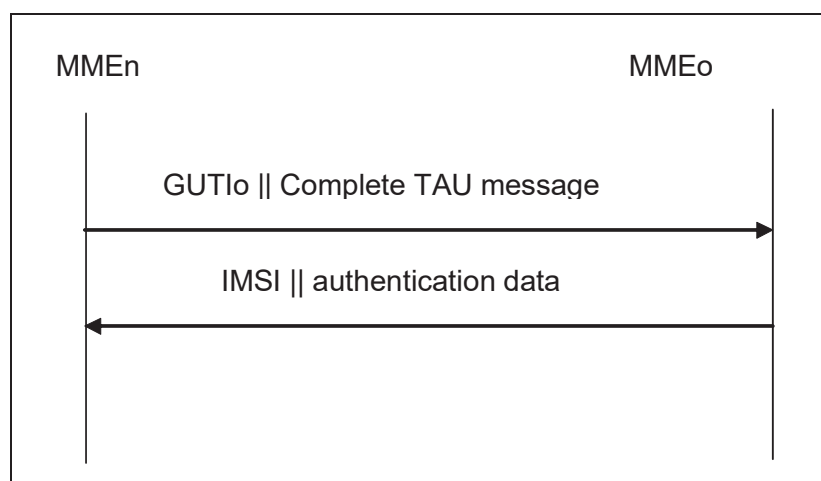


圖 5- 174 同核網的 MME 換手

資料來源：3GPP TS 33.401

這部分的風險在駭客可以在換手時模擬新的 MME，原 MME 在追蹤區域更新訊息的完整性，如果原 MME 不檢測完整性時，為了避免新 MME 取得 EPS 安全性文本，就會需要重新驗證 UE 的身分，原 MME 就消耗了資源在 S10 介面進行完整性驗證，如果重複出現此情況的問題，就會使得原 MME 的資源耗盡。

IMSI(International Mobile Subscriber Identity)可以辨識用戶身分，在 LTE 訊息交換時會將 IMSI 變成 GUTI(Globally Unique Temporary Identity)，讓 IMSI 不會一直曝露在訊息中，減少 IMSI 遭竊取的風險。

(二) 無用(Unused)的資料

1. 3G 之間換手

在 UE 的網路服務從 4G 切換到 3G 時³³⁰，UE 與 MME 應分別依照 EPS 安全性文本內的 K_{ASME} 產生 3G 技術下的金鑰，金鑰分別為機密性金鑰 CK 與完整性金鑰 IK，產生後 MME 會將 CK、IK 傳遞到 SGSN，UE 可以繼續在 3G 使用服務，並且維持 UE 與 SGSN 的安全性。

在 3G 換手之間的程序中，SGSN 發送身分驗證訊息到 MME 後，MME 會先驗證

³³⁰ Han, C. K., Choi, H. K., Baek, J. W., & Lee, H. W. (2009, October). Evaluation of authentication signaling loads in 3GPP LTE/SAE networks. In *Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on* (pp. 37-44). IEEE.

UE 的身分，確認後才會產生金鑰，但是在傳遞金鑰時，在系統面來說，為了方便可能會忽略 EPS 安全性文本並不需要傳遞到 SGSN，如果 EPS 安全性文本從 MME 被送到 SGSN，此行為將隱藏著浪費儲存 EPS 安全性文本的空間，也可能導致 SGSN 處理程序時錯誤使用。另外也可能在 SGSN 遭模擬的情況下，如果 EPS 安全性文本隨著身分要求訊息傳遞到 SGSN，會導致 EPS 安全性文本被駭客取得並能夠從 EPS 安全性文本與 CK、IK 取得破解 EPS 安全性文本的機會。

2. 跨核網

在同核網內，EPS 安全性文本可以透過相同的 HSS 運算 RAND、SQN，讓 EPS 安全性文本的解密一致，但是若 UE 在移動時執行追蹤區域更新程序，在跨核網與遇到完整性檢測失敗時，就需要重新產生 EPS 安全性文本，但是如果新 MME 使用原核網預先產生的 EPS 安全性文本進行驗證時，UE 就無法通過與電商號碼已改變。

當原 MME 收到從新 MME 發送的身分要求(Identification Request)時，如果新 MME 被模擬的情況，原 MME 傳送預先產生的 EPS 安全性文本到新 MME，可能會導致金鑰被破解，以及系統資源浪費在傳輸用不到³³¹的 EPS 安全性文本。

(三) 安全模式選擇

1. 完整性保護

完整性保護主要用在 NAS 信令上，為了確保訊息在沒有錯誤的傳輸過程中進行交換，MME 與 NAS 從 K_{ASME} 產生完整性保護金鑰與機密性保護金鑰，這些都是基於安全模式訊息交換後開始進行保護，而安全模式的選擇應該依照 MME 給予的安全模式選項中最嚴密的加密演算法，UE 接收 MME 的安全模式訊息後，依照加密演算法使用完整性金鑰與機密性金鑰，將訊息進行加密並回傳至 MME，MME 就會檢查 MAC(Message Authentication Code)，MAC 是伴隨著訊息一起傳遞到 MME，由 MME 以相同的完整性加密計算後，取得 XMAC 值來比較是否與 MAC 值相同，即完成完整

³³¹ Purkhiabani, M., & Salahi, A. (2012). Enhanced authentication and key agreement procedure of next generation 3GPP mobile networks. *International Journal of Information and Electronics Engineering*, 2(1), 69.

性檢查。

駭客是將 UE 進行模擬並依此流程進行攻擊，首先 MME 發送安全模式訊息，UE 回覆安全模式訊息時，NAS 不使用較嚴密的加密演算法(可能為零號)保護，駭客就可以在其中修改 NAS 信令與 EPS 安全性文本，顯露出漏洞與弱點在之後進行攻擊。

2. 機密性保護

與 1.程序相同，UE 在被駭客模擬時，MME 收到安全模式訊息，如果沒有機密性防護的情況下，MME 就會重複的執行安全模式的啟用，因此要不斷與 UE 交換訊息，導致資源浪費在一個程序，當其他 UE 要與 MME 進行訊息交換或程序執行時，就會影響 MME 的效能，當此情況的 UE 發生數量達到 MME 上限時，駭客就會達到拒絕服務攻擊的目的，讓其他 UE 的服務中斷並且可能影響核網的運作。

3. 降次³³²

在 UE 註冊流程時，UE 與 MME 的安全模式是根據 MME 給予的安全模式並選擇最嚴密的演算法，但是在安全模式建立的過程中，駭客可以運用重送(replayed)攻擊³³³安全模式的訊息。

在 UE 遭到模擬的時候，將會導致 MME 與 UE 的加密演算法更改，甚至使用比較不嚴謹的(零號)演算法或者不加密，這樣的方式導致 MME 與 UE 之間容易受到駭客攻擊。

(四) 換手問題

1. eNodeB 由 X2 介面³³⁴換手

在安全模式訊息中，MME 可以取得 UE 的安全模式，UE 在 eNodeB 的 X2 介面之間進行換手，當 MME 不進行 UE 的安全模式確認時，駭客能夠藉由模擬 eNodeB

³³² Banescu, S., & Posea, S. Security of 3G and LTE. *Faculty of Computer Science, Eindhoven University of Technology*.

³³³ HUSSAIN, Syed Rafiul, et al. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE.

³³⁴ Bikos, A. N., & Sklavos, N. (2013). LTE/SAE security issues on 4G wireless networks. *IEEE Security & Privacy*, 11(2), 55-62.

來更動在無線訊號上的加密方式，讓訊息或 NAS 信令被破解或其他弱點進行攻擊。

2. MME 由 S10 介面換手

在 S10 介面 MME 換手時，新的 MME 應該要能夠從 UE 接收加密後的訊息，且 UE 是以原 MME 相同的安全模式進行加密，此加密的方式應該以安全模式中的選項最嚴密的演算法，以設定的演算法進行原 MME 訊息的解密成功才算完成換手程序。

駭客利用 S10 介面 MME 換手程序，模擬原 MME 並選擇較弱的安全模式，接下來在 MME 換手程序的追蹤區域更新訊息進行較弱的演算法加密，在新 MME 為符合原 MME 的安全模式相同的演算法不斷的去嘗試解密，達到 UE 與 MME 之間 S1 介面安全性降低，也成功將新 MME 的資源消耗。

(五) 緊急通道

在 MME 介面安全性中，報告中有說明 4G 發展出 IMS 緊急通道，讓 UE 可以在緊急狀況下使用通話，而在允許使用 IMS 緊急通道的層級可以分成：僅有驗證的 UE、限制服務的合法 IMSI、未通過驗證 IMSI 的 UE、僅有 IMEI 的 UE，依照當地的電商或者法律，可以調整接受使用 IMS 緊急通道的 UE。

在此行為中構成攻擊的程序，駭客可以在合法 UE 建立非緊急的通道後，模擬同個 UE 的身分，因為驗證失敗而使用緊急通道，因為沒有釋放或中斷 UE 先前建立的非緊急通道，讓駭客能以不用付費的前提下取得非緊急通道資源與付費的通話，達成盜用受害 UE 付費資源的目的。

五、 MME 相關介面弱點及安全威脅分析研究

在此項目將探討現今 3GPP 的規範中，針對前章節的攻擊手法以及步驟，以 3GPP 針對 MME 提出的三個規範，以互相對應的方式整理出表格，依照表格說明目前國際規範已經重視 MME 的安全性問題，以下分別在 3GPP TR 33.926、TS 33.401、TS 33.116 中，而 TR 33.926 提出 MME 的隱藏威脅、TS 33.401 提出 MME 在 EPS 安全性文本、UE 安全模式、非緊急通道的防護、TS 33.116 提出 MME 的檢測項目。

(一) 註冊程序威脅分析

下表為 3GPP 對 MME 註冊程序之相關規範。

表 5- 13 MME 註冊程序相關規範

33.926 威脅項目	33.401 項目	33.116 檢測項目
A.2.2.2 重新同步❶	6.1.2 在核心網路中，HSS 傳遞驗證資料 “在同步錯誤的案例中，MME 也應該保有 RAND 與 AUTS”	4.2.2.2.2 重新同步 UE 與 HSS 遭模擬
A.2.2.3 追蹤區域更新時，註冊訊息完整性檢查失敗❷	6.1.4 在同一核心網路中，傳遞 IMSI 與驗證資料 當用戶身分無法被辨識或者完整性檢測失敗，MME 應該回覆”用戶身分無法取得”之訊息	4.2.2.2.3 註冊時，完整性 檢測服務 MME 遭模擬

資料來源：本團隊整理

1. 重新同步

相關弱點：

為達到拒絕服務的威脅，駭客在同步失敗時，在訊息不傳遞 RAND 與 AUTS，重新同步程序就不會正常運作，在同步錯誤時應回覆 RAND 與 AUTS，避免 MME 資源耗盡的風險。

檢測方式：

當 MME 收到驗證失敗訊息時，MME 應在傳遞給 HSS 驗證身分訊息中包括 EMM(EPS Mobility Management)的同步失敗以及重新同步的 AUTS，傳遞原有 RAND 與從 UE 收到的 AUTS，以此檢測方式來達到重新同步程序的正確運作。

2. 追蹤區域更新時，註冊訊息完整性檢查失敗

相關弱點：

UE 在執行追蹤區域更新程序時，在 S10 介面 MME 會包含完整性的金鑰，因此

當註冊訊息的完整性檢查失敗時，不僅使用者身分就無法被確認，也會讓系統因為花費時間在確認完整性，最後浪費 MME 的資源，當這樣的問題重複發生後可能還會導致拒絕合法使用者存取系統。

檢測方式：

在追蹤區域更新時 MME 應該檢測 UE 資訊(辨識 GUTI)前先確認訊息完整性保護，當完整性保護經過檢測失敗時，原 MME 就應該直接回覆 UE 身分無法辨識的訊息給新的 MME，讓原 MME 減少資源的浪費在辨識 UE 身分上，也降低在 S10 換手期間等待的時間。

(二) 安全模式威脅分析

下表為 3GPP 對 MME 安全模式之相關規範。

表 5- 14 MME 安全模式相關規範

33.926 威脅項目	33.401 項目	33.116 檢測項目
A.2.3.1 降次威脅①	7.2.4 安全模式指令程序與演算法選擇 安全模式 (SECURITY MODE)訊息應該包含 UE 的加密訊息能力	4.2.2.3.1 降次預防 UE 遭模擬
A.2.3.2 NAS 完整性加密的選擇與使用②	7.2.4.4 NAS 安全模式指令程序 MME 根據優先排序中，選擇最優先的完整性演算法防護安全模式 (SECURITY MODE)訊息	4.2.2.3.2 NAS 完整性演算法選擇與使用 UE 遭模擬
A.2.3.3 NAS NULL 完整性加密演算法③	5.1.4.1 完整性需求 EIA0 應只在未授權的緊急通話時使用	4.2.2.3.3 NAS NULL 完整性防護 UE 遭模擬
A.2.3.4 NAS 機密性加密演算法④	7.2.4.3.1 初始 NAS 安全性文本 UE 在傳送 NAS 安全性模式訊息給 MME 時，應啟用 NAS 完整性保護與	4.2.2.3.4 NAS 的可用性防護 UE 遭模擬

33.926 威脅項目	33.401 項目	33.116 檢測項目
	加密	
A.2.4.2 MME 換手時，NAS 完整性加密演算法的選擇⑤	7.2.4.3.2 MME 換手 MME 應根據排序中，選擇最高 NAS 完整性演算法	4.2.2.4.2 在 MME 改變時 NAS 完整性演算法的選擇 MME 遭模擬

資料來源：本團隊整理

1. 降次威脅

相關弱點：

在安全模式程序中，若訊息交換期間遭到重放(replayed)攻擊，UE 可能直接被降低安全模式並使用較弱的加密演算法甚至是關閉，導致系統容易受到攻擊。

檢測方式：

MME 必須在收到安全模式訊息時，檢測 UE 的安全模式是否與 MME 設定相同，且要設定與 UE 安全模式中最嚴密的演算法進行保護。

2. NAS 完整性加密的選擇與使用

相關弱點：

NAS 不使用較嚴密的完整性演算法保護，NAS 信令就會被修改，可能導致 UE 安全模式被關閉，讓 MME 與 UE 的問題容易被發現並受到攻擊。

檢測方式：

MME 發送安全模式訊息，且 UE 回覆安全模式訊息時，MME 應該檢查安全模式訊息中的 MAC，並選擇 UE 安全模式中最嚴密的演算法來防護。

3. NAS NULL 完整性加密演算法

相關弱點：

若 NAS NULL 完整性加密演算法(即 EIA0)未正確使用，在未進行驗證的前提下，

駭客就可以藉由 NAS 取得使用非緊急通話的方式，模擬正常 UE 的身分使用非緊急通話，導致 UE 的權益受到危害。

檢測方式：

在 UE 身分成功驗證後，MME 發送安全模式訊息所使用的完整性演算法需要不同於 NULL 完整性加密演算法。

4. NAS 機密性加密演算法

相關弱點：

NAS 不使用安全模式較嚴密機密性演算法保護，NAS 信令暴露可能導致需要浪費資源去重新進行安全模式程序，讓 MME 與 UE 的問題容易被發現並受到攻擊，拒絕其他 UE 使用服務。

檢測方式：

MME 在沒有機密性防護的情況下收到安全模式訊息，此時 MME 選擇不同於零號(EEA0)的機密性演算法，MME 就會拒絕該訊息，因為 MME 與 UE 的安全模式的選擇並不一致。

5. MME 換手時，NAS 完整性加密演算法的選擇

相關弱點：

當 MME 在換手時，若較高的 NAS 完整性加密演算法無法被正確選擇，使得新 MME 使用較弱的加密演算法，讓 UE 與 MME 處於較弱的安全模式下，NAS 信令容易被攻擊或破解。

檢測方式：

當 S10 介面執行換手時，新 MME 取得 UE 安全模式並檢查舊 MME 所使用之演算法不相同的情況下時，需要檢測新 MME 是否重新執行安全模式程序中，會包含所選擇的演算法與 UE 安全模式。

(三) 換手行為威脅分析

下表為 3GPP 對 MME 換手行為與緊急通道之相關規範。

表 5- 15 MME 換手行為與緊急通道相關規範

TR33.926 威脅項目	TS33.401 項目	TS33.116 檢測項目
A.2.4.1 X2 換手時，降次攻擊 ^①	7.2.4.2.2 由 X2 換手 eNB 時，MME 應驗證從 eNB 收到 UE 安全模式，是相同於 MME 內儲存的 UE 安全模式	4.2.2.4.1 X2 換手時防護能力降低 eNB 遭模擬
A.2.2.4 傳遞 EPS 驗證資料至 SGSN ^②	6.1.6 在 MME 與 SGSN 間，傳遞 IMSI 與 UMTS 驗證資料 EPS 驗證資料內若不包括 CK 與 IK，對於 SGSN 來說沒有幫助	4.2.2.2.4 不傳輸 EPS 授權資訊至 SGSN SGSN 遭模擬
A.2.2.5 傳遞未使用的驗證資料至不同核網 ^③	6.1.5 在不同核心網路間，傳遞 IMSI 與驗證資料 未使用的驗證資料或非服務的核心網路安全性文本不應該在之間互相傳遞	4.2.2.2.5 EPS 授權資訊不傳輸於不同核網 MME 遭模擬
A.2.6 非緊急通道的釋放 ^④	15 IMS 緊急通話 當 MME 或 UE 授權失敗時，MME 或 UE 應釋放非緊急通道(bearers)	4.2.2.6.1 釋放非緊急通道(bearers) UE 遭模擬

資料來源：本團隊整理

1. X2 換手時，降次攻擊

相關弱點：

若 MME 無法確認 UE 的安全模式與 eNodeB 相符，UE 可能會直接接受 eNodeB 使用較弱的加密演算法，導致容易被攻擊或破解。

檢測方式：

MME 收到 UE 安全模式時，如果 UE 與 eNodeB 的安全模式不同於 MME 收到的

安全模式，MME 應該視為事件並記錄下來。

2. 傳遞驗證資料至 SGSN

相關弱點：

當 UE 的位置僅能夠使用 3G 服務，MME 就需要產生 3G 需要的金鑰(CK、IK)，因此 MME 就依照 3G 的金鑰產生規則從 KASME 產生 CK、IK，而 SGSN 就不需要 EPS 的安全性文本，這時候如果 MME 在 S3 介面與 SGSN 交換 EPS 安全性文本，這訊息不僅浪費空間儲存使用不到的資訊，也可能導致這些資訊被錯誤使用，增加 SGSN 在執行時產生錯誤的風險。

檢測方式：

在 S3 介面交換金鑰到 SGSN 的時候，MME 應該只有傳輸 CK 與 IK，不應該在訊息內包括 EPS 安全性文本，讓 EPS 安全性文本留在 MME 內。

3. 傳遞未使用的 EPS 安全性文本至不同安全性區域

相關弱點：

當 UE 移動而執行追蹤區域更新時，如果需要到換手不同核網的 MME 時，在沒有正確處理跨核網的問題下，導致傳遞未使用的 EPS 安全性文本至不同核網，MME 資源將會被浪費，因為發生驗證問題時，還是需要 HSS 重新產生新的 EPS 安全性文本才能進行驗證。

檢測方式：

當原 MME 收到從新 MME 發送的身分要求(Identification Request)，應該檢測原 MME 回覆新 MME 不包含未使用的 EPS 安全性文本。

4. 非緊急通道的釋放

相關弱點：

UE 在建立 IMS 緊急通道且驗證身分失敗時，MME 如果不釋放 UE 的非緊急通道，則 UE 可以在未驗證的狀態下繼續接收通話、使用付費的核網資源

檢測方式：

應該在 UE 建立緊急通道時，如果 MME 驗證 UE 失敗，UE 應該釋放已建立的非緊急通道。MME 釋放所有 UE 的非緊急通道後，UE 的緊急通道才能夠建立。

第四節 建置基站弱點資料庫

一、 基站弱點評估

本計畫基站弱點的評估主要是參考 3GPP TS 33.117 - Catalogue of general security assurance requirements 安全標準的精神來進行，TS 33.117 也是 TS 33.216 - Security Assurance Specification (SCAS) for evolved Node B (eNB) network product class 標準內引用最多的。

以製造商的角度來看，每一個網路產品都是基於公司考量不同的商業價值與市場定位，甚至產品如果將使用在特定的產業領域，同時也需要滿足對應的標準規範要求，再進而琢磨不同的產品需求規格、功能與品質等條件下衍生出來的產物，因此不同產品系列可能在安全的設計要求上會有不同。

在廣義上來看，3GPP TS 33.117 整體的概念包含製造商產品文件、設計與使用文件，及對網路產品軟體與韌體之弱點暴露與探測攻擊和軟體缺陷(Software Weaknesses)，以及網路產品本身安全控制的功能，並且有些測試與觀測更涵蓋從網路產品整體生命週期，包含網路產品的設計與測試階段，及在商業市場上部署運作後如何持續更新安全上的考量等，歸納整理對基站弱點評估的面向如下：

(一) 產品操作性與說明文件

此項目是 3GPP TS 33.117 標準內許多地方要求產品製造商應該提供的內容，可區分為一般功能使用與管理者功能的描述與操作說明，但需求上又會比一般提供給電信維運人員的技術文件更多，有些需求是屬於在產品開發測試階段所使用的，例如：script 等。另外所有介面的說明與操作，例如：遠端登入介面、所有產品本身實體輸入/輸出介面、所有無線介面與支援通訊協定。

而在產品的組態設定則須提供包含網路安全與實體存取控制等安全層面，例如：

防火牆的埠與協定，產品本身介面組態設定選項等。許多 3GPP TS 33.117 標準的測試項目需要產品製造商提供詳細的過程，才可以進一步測試項目，例如：評估繞過或暴力破解等可能規避產品認證系統的可能性。

（二）存取控制、使用者認證與授權

在這個項目，3GPP TS 33.117 標準許多測試項目的要求同樣考慮到應將適當的存取控制程序納入至產品，並且需要能鑑別設備的存取行為，確保只有已授權、程序與經授權活動能使用產品系統，降低資訊或檔案等遭竊取的威脅。因此，任何可能影響或改變產品安全設定的操作都需要經過用戶認證，並確定只能執行授權下的操作行為。同時，需要預防永久授權的機制，應具備可設定超出特定閒置時間後須進行再認證之行為。

此外，遠端登入存取服務，仍應該要求進行使用者認證與授權鑑別。3GPP TS 33.117 標準指出除非該遠端服務不涉及傳送機敏資料或個人識別資料，單純只有輸出產品狀態或歷史傳輸資料，或許可以接受在未經認證的情況下存取服務，但仍必須基於風險評估的結果來認定。然而在使用帳號與密碼進行認證的安全機制，必須符合國際上可接受相關資安標準規範與技術方式來儲存密碼。

另外，所有系統相關的錯誤或警告訊息，都不應該揭露帳號名稱或系統內部、程式碼片段訊息，避免攻擊者可以在很短的時間內蒐集得到有幫助的資訊，進而整理製作出對基站有影響的攻擊工具。

除了身分認證機制的安全設計外，3GPP TS 33.117 標準也要求須設定於產品內每一個帳號角色對應的存取權限，同時應該保有一個管理者權限，例如：Administrator 或 System 的角色來管理產品，包含增加、修改或停用、刪除帳號。至於一般其他帳號角色則只要給予滿足所需的功能操作即可，以最小權限為考量。此外，當遠端登入至產品使用服務過程中遇到連線中斷，當連線恢復再次登入時務必要求重新認證。

（三）通訊傳輸

3GPP TS 33.117 在檢測上會要求要達到通訊過程之完整性(Integrity)與身份鑑別(Authenticity)。目的是預防中間人針對資料傳輸的情況下，竊取或竄改機敏資料。

（四）加密技術

加密是種用來將資料加以編碼的數學演算法，只有預期的對象可以加以讀取，確保提升安全防護的難度。在 3GPP TS 33.117 提及產品機敏資訊不得已明文顯示，例如：機敏資料與個人身分資料的機密性，使用階段與傳送過程都應該有安全機制做保護。

（五）軟體完整性

3GPP TS 33.117 標準內對於軟體安裝都會要求完整性，系統如何驗證完整性，是否相關介面呈現上述。主要要求利用雜湊演算法進行檔案驗證，確保安裝的軟體都是製造商提供的，可避免預防例如：攻擊人員利用降級韌體版本的方式，讓產品因韌體版本已降為舊版而導致漏洞暴露，進而遭受攻擊影響產品運作。

（六）弱點掃描

軟體缺陷弱點係指系統軟體或程式中存在任何影響正常功能運作的問題、錯誤或隱藏之功能缺陷等，這些缺陷可能被駭客利用作為竊取與破壞系統的機密與運作。當前有很高的比例利用緩衝區溢位的問題來達到遠端攻擊。基本上隨著更多元與自主化功能的需求，軟體的設計日趨複雜，也因此程式碼行數越來越多，進而相對的軟體缺陷也越多，雖然缺陷不等於攻擊，但卻是攻擊必須的要件。

在進行軟體安全評估測試時，主要包含以下項目：

1. 已知弱點漏洞

已知弱點掃描評估，可使用業界知名度較高資安軟體進行掃描評估是否存有 CVE 已知安全漏洞。例如：發現該產品有開啟未加密之 Telnet 服務，並建議改成 SSH 作為替代，或者偵測出該產品使用不夠長的金鑰來對 64 位元的資料區段進行加密，這常見於使用 OpenSSL 可能會讓遠端攻擊者取得機密性資訊，透過擷取 SSL/TLS 伺服器與用戶端之間的大量已加密資料流量，駭客可能會惡意探索此漏洞，以還原取得機密性資訊。另外尤其可能容易探測到 Private key 這樣重要的檔案卻無加密，很容易遭取出進行中間人攻擊。

或者進行靜態二進制檔案與位元組碼分析，包含有系統之韌體檔、可執行檔或已

編譯之原始碼，透過分解(Disassembly)和模式辨識(Pattern Recognition)等技術進行靜態二進位檔案安全檢測。

2. 異常輸入測試

異常輸入測試，也稱之為黑箱測試，係指將產品視為一個黑盒子，安全測試人員不知道產品內部如何運作，單純透過輸入去觀察系統的回應。這部份將採用模糊測試工具進行對該軟體傳送特定或異常的輸入，進而觀察與評估該軟體系統是否具足夠的強健性可以正常回應，及監控整個輸出過程中是否存有異常或通用弱點缺陷(Common Weakness Enumeration, CWE)等。

上述一般透過模糊測試的技術，產生隨機產生、調整變異測試和特定有演算法來產生出大量的弱點探測資料集，例如緩衝區溢位攻擊來對待測產品進行可能潛在漏洞探測或通用弱點缺陷列表(Common Weakness Enumeration, CWE)所載之缺陷。再從結果是否有產品重置、設定回到初始化配置、在測試完成特定時間後，處理程序當掉、產品出現未處理的異常、發生資料儲存異常、產品與資安測試工具之間的連線中斷或服務關閉。

異常輸入測試執行的速度，與產品的系統條件與回應速度有相當大的關係，不同產品對於異常輸入封包的回應速度都不一樣。

3. 滲透測試

利用評估出的已知可能 CVE 漏洞，搭配攻擊工具進行未經授權方式存取、阻斷式服務攻擊、中間人攻擊等可能造成產品當機、異常運作或入侵取得資料等手法。

LTE 基站是一個一般人員不容易接觸，且須具備許多電信領域專業知識與實務經驗的技術領域。目前也幾乎暫無文獻實際提到 LTE 基站相關的軟體漏洞，通常都會提到的都是可能的威脅。目前在 CVE 網站上與基站有相關僅有 CVE-2017-15326，該漏洞問題主要是基站支援不安全加密演算法，可能產生中間人攻擊破解加密數據，如下圖。

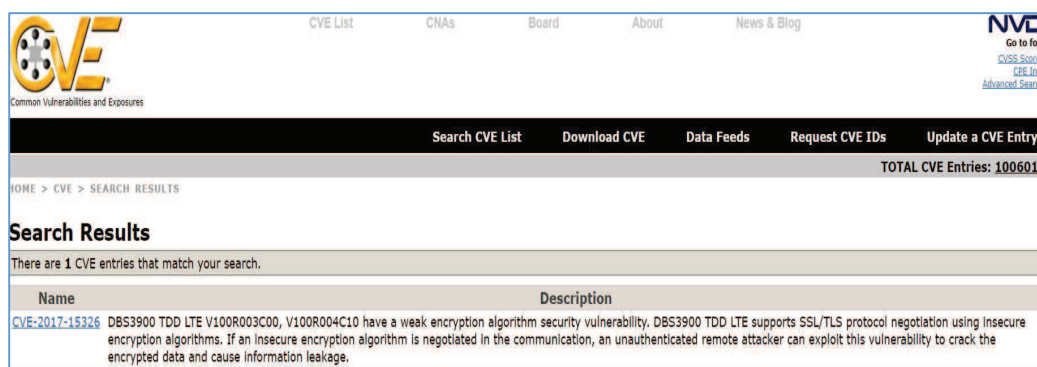


圖 5-175 CVE-2017-15326 漏洞

資料來源： CVE-2017-15326³³⁵

因此，本研究直接從嵌入於基站硬體裝置中的韌體，透過韌體分析工具來進行資安檢測。下圖 5-176 是 C 廠牌基站韌體檔案分析的結果一覽，其中檢測出共有 16 種軟體元件(Components)存有的 CVE 漏洞達 1,097 筆。

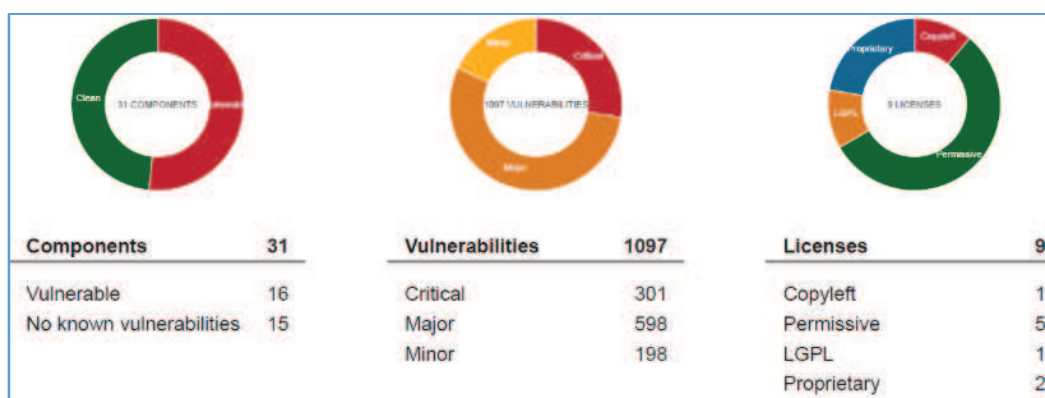


圖 5-176 C 廠牌基站韌體檔案分析結果

資料來源： 本團隊整理

下圖 5-177 是 A 廠牌基站韌體檔案分析的結果一覽，其中檢測出共有 42 種軟體元件(Components)存有的 CVE 漏洞達 874 筆。

³³⁵ CVE, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15326>

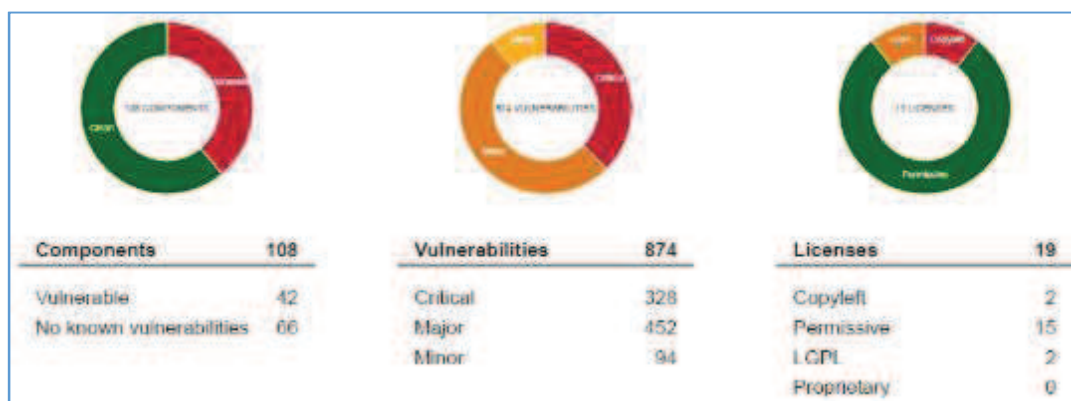


圖 5-177 A 廠牌基站韌體檔案分析結果

資料來源： 本團隊整理

下圖 5-178 為 C 廠牌基站韌體共有 31 種不同類型之第三方開源軟體元件，如下圖。

Identified 3rd party components		
busybox 1.18.1	guava	systemd 230-1
busybox 1.21.1	jcommon 1.0.16.jar.pack	systemd-shim
busybox 1.22.0-19	jfreechart 1.0.13.jar.pack	ucos-ii
bzip2	keypoint-pngencoder	vxworks 6.4
commons-compress 1.7	libcap	xz
commons-io 2.4	libpcap 1.3.0	zlib
compress 1.7	libpcap 1.4.0	zlib 1.2.3
dosfstools	linux_kernel 2.6.34.9	zlib 1.2.5
gettext	openssl 1.0.1t	zlib 1.2.8
glib	pcrc	
glibc 2.11.1	super-csv 2.3.0	

圖 5-178 C 廠牌基站韌體檔案內之第三方開源軟體元件

資料來源： 本團隊整理

下圖 5-179 為 A 廠牌基站韌體共有 108 種不同類型之第三方開源軟體元件。

Identified 3rd party components		
acl	iperf 2.0.5	netbsd-resolv
attr	iproute2	nettle 3.1.1
autogen	iptables	ntp 4.2.8p10
bash 4.3.39	iputils	openldap
bgaes	kmod	openssh 7.3p1
bind	libasyncns	openssl 1.0.2k
bind 9.10.2	libcap	pcre
binutils 2.25.51	libdaemon 0.14	pcre 8.38
bluez	libevent 2.0.22	pcre 8.40
boost	libffi	perl 5.22.0
bridge-utils	libidn 1.30	php 5.5.38
busybox 1.23.2	liblzo2	popt
bzip2 1.0.6	libmnl	procps 3.3.10
conntrack-tools 1.4.4	libnftnl	protobuf
cryptopp	libnftnl 1.0.1	rapidxml
cryptsetup 1.7.2	libpcap 1.6.2	readline
curl 7.55.1	libtasn1	rpcbind
dbus 1.8.20	libusb 1.0.19	rsync 3.1.1
dhcp 4.3.3	libx11	shadow 4.2.1
e2fsprogs 1.42.9	libx11 1.6.3	squashfs-tools
ebtables 2.0.10	libxcb 1.11	squashfs-tools 4.3
elfutils 0.163	libxml2 2.9.4	strace 4.10
ethtool 4.0	libzip	strongswan
expat 1.95.8	lighttpd 1.4.37	sudo 1.8.15
expat 2.2.2	linux-pam	systemd
expat 2.2.4	linux_kernel 3.10.107	systemd-shim
file	log4cplus	tcpdump 4.9.0
fuse 2.9.3	lvm2 2.02.166	tdb

圖 5-179 A 廠牌基站韌體檔案內之第三方開源軟體元件

資料來源：本團隊整理

本計畫從 C 廠牌基站韌體檔分析出的 CVE 漏洞 1,097 筆，再進一步搜尋比對 Exploit Database 網站上已經存在之攻擊程式碼或工具，可能容易被整合或修改對基站造成威脅，共有 8 筆，如下圖。

1	Component	Version	CVE	CYSS	CYSS3	Exploit Database
2	linux_kernel	2.6.34.9	CVE-2016-0728	7.2	7.8	Linux Kernel 4.4.1 - REFCOUNT Overflow Use-After-Free in Keyring Local Privilege Escalation
3	systemd	230-1	CVE-2016-10156	7.2	7.8	Systemd 228 (SUSE 12 SP2 / Ubuntu Touch 15.04) - Local Privilege Escalation
4	linux_kernel	2.6.34.9	CVE-2016-3672	4.6	7.8	Linux Kernel (x86) - Disable ASLR by Setting the RLIMIT_STACK Resource to Unlimited
5	linux_kernel	2.6.34.9	CVE-2016-4557	7.2	7.8	Linux Kernel 4.4 (Ubuntu 16.04) - BPF Local Privilege Escalation (Metasploit)
6	linux_kernel	2.6.34.9	CVE-2016-4997	7.2	7.8	Linux Kernel 4.6.3 (x86) - Netfilter Local Privilege Escalation (Metasploit)
7	linux_kernel	2.6.34.9	CVE-2016-8655	7.2	7.8	Linux Kernel 4.4.0 (Ubuntu 14.04/15.04 x86-64) - NET_PACKET Race Condition Privilege Escalation
8	linux_kernel	2.6.34.9	CVE-2017-6074	7.2	7.8	Linux Kernel 4.1.0 (Ubuntu) - LXCFS Double-Free (PoC)
9	linux_kernel	2.6.34.9	CVE-2017-7388	7.2	7.8	Linux Kernel 4.8.0-41-generic (Ubuntu) - Packet Socket Privilege Escalation

圖 5-180 C 廠牌基站韌體檔案已存在之攻擊工具

資料來源：本團隊整理

下圖 5-181 是從 A 廠牌基站韌體檔分析出的 CVE 漏洞 874 筆之中找出存在於 Exploit Database 網站上有公開的 9 筆攻擊程式碼與工具。

1	Component	Version	CVE	CVSS	CVSS3	Exploit Database
2	linux_kernel	2.6.34.9	CVE-2016-0728	7.2	7.8	Linux Kernel 4.4.1 - REFCOUNT Overflow Use-After-Free in Keyrings Local Privilege Escalation
3	linux_kernel	2.6.34.9	CVE-2016-5072	4.6	7.8	Linux Kernel (x86) - Disable ASLR by Setting the RLIMIT_STACK Resource to Unlimited
4	linux_kernel	2.6.34.9	CVE-2016-4557	7.2	7.8	Linux Kernel 4.4 (Ubuntu 16.04) - BPF Local Privilege Escalation (Metasploit)
5	linux_kernel	2.6.34.9	CVE-2016-4997	7.2	7.8	Linux Kernel 4.6.3 (x86) - 'Netfilter' Local Privilege Escalation (Metasploit)
6	linux_kernel	2.6.34.9	CVE-2016-8555	7.1	7.8	Linux Kernel 4.4.0 (Ubuntu 14.04-16.04 x86-64) - /AI_PACKET Race Condition Privilege Escalation
7	linux_kernel	2.6.34.9	CVE-2017-6074	7.2	7.8	Linux Kernel 4.4.0 (Ubuntu) - DCCP Double-Free (PoC)
8	linux_kernel	2.6.34.9	CVE-2017-7306	7.2	7.8	Linux Kernel 4.8.0-11-generic (Ubuntu) - Tacklet Socket Privilege Escalation
9	bind	9.10.2	CVE-2015-5177	7.8	NA	ISC BIND 9 - DKEY Remote Denial of Service (PoC)
10	bind	9.10.2	CVE-2016-2776	7.8	7.5	ISC BIND 9 - Denial of Service

圖 5- 181 A 廠牌基站韌體檔案已存在之攻擊工具

資料來源： 本團隊整理

二、 建置基站弱點資料庫

基站弱點資料庫應該是行動通訊網路安全防護體系中建置基礎的一環，其他國際網路安全組織亦因應不同需求而建立各樣所需之資料庫，包含有來自政府、民間組織與資安公司積極建立起弱點資料庫，並投入許多專業人員及資源進行維護的工作，將相關弱點資料以有系統的整理與收集、分析與發佈，比較知名且小有規模的弱點資料庫例如³³⁶：

1. IBM ISS X-Force：X-Force 是全球最完整威脅與漏洞的資料庫之一數據庫是其中之一。在 2010 年資料庫內存有 54,604 筆漏洞資料，涵蓋 12,562 不同廠商中 24,607 種軟體。主要提供弱點資訊、CVSS 嚴重分數、引導如何處理或緩解漏洞，對何種平台有衝擊與發現日期等。
2. National vulnerability database：NVD 隸屬於美國國家標準技術中心電腦安全部門的資訊技術實驗室，主要作為提供美國政府存放標準弱點資訊管理的資料庫。自 1999 年來總共紀錄至少 4,6176 筆漏洞資訊。主要提供漏洞資訊來源、CVSS 嚴重分數、參考資料、漏洞影響的軟體名稱與版本等資訊。
3. SecurityFocus vulnerability database：SecurityFocus 是一個自 2002 年來由賽門鐵克維護扮演中立角色的漏洞資料庫平台。至今至少超過 40,000 筆漏洞資訊，涵蓋影響 14,000 廠商與超過 105,000 種軟體弱點問題。主要

³³⁶ Anshu Tripathi, Umesh Kumar Singh, Taxonomic Analysis of Classification Schemes in Vulnerability Databases

提供 BugTrag ID, CVE-ID 編號、漏洞揭發日期、漏洞可被入侵的工具清單與參考資料。

4. Open Source Vulnerability Data Base：OSVDB 是自 2002 年起由一群 BlackHat 會議舉辦人員共同建立之開放原始碼資料庫，至今至少涵蓋 70,789 筆漏洞，長年來多達 4,735 位研究人員針對 32,272 種軟體進行評估，同樣提供提供 BugTrag ID, CVE-ID 編號、漏洞揭發日期、漏洞可被入侵的工具清單與參考資料。
5. Secunia：Secunia 是私人組織提供資安防護、弱點分析的顧問服務。在弱點資訊提供包含嚴重等級、衝擊影響、解決方案、CVSS 分數等資訊。
6. Common Vulnerabilities and Exposures：CVE 是一個與資訊安全有關的資料庫，蒐集各種弱點及漏洞，制定管理漏洞編號以便於查閱。此資料庫現由美國非營利組織 MITRE 所屬的 National Cybersecurity FFRDC 所營運維護。
7. P1 Vulnerability Knowledge Base (VKB)：P1 VKB 是私人組織提供電信領域資安防護、弱點分析的顧問服務。在弱點資料庫資訊提供包含嚴重等級、衝擊影響、解決方案、遠端檢測等服務與資訊³³⁷。

本計畫基站弱點資料庫建立之目的為考量電信產業屬於高敏感產業，從上述不同單位所建置之弱點資料庫僅有 P1 Security 公司提供與電信產業相關的弱點資料，但是內容仍比較偏向 3G 階段系統居多，LTE 弱點資料仍持續建置中，實質上 LTE 基站弱點資訊的來源與蒐集確實難度較高。

因此，計畫團隊針對基站韌體弱點分析這個面向切入，利用韌體分析工具來拆解與分析基站韌體的組成架構，包含哪些第三方開放原始碼組件名稱、版本、CVE 漏洞資訊等，這是直接從設備內部探測分析的方向來蒐集、整理與保存基站已知 CVE 漏洞，這也是與 P1 Security 公司從原始碼分析、電信通訊協分析、滲透測試等角度出發差異之處。

本計畫基站弱點資料庫名稱制定為 eNodeB VULDB，主要提供整合本團隊內部使用之 Protecode-SC 韌體分析平台將韌體分析的結果，由管理者上傳至 eNodeB VULDB

³³⁷ P1 Security, <http://www.p1sec.com/corp/>

進行處理與儲存，並可透過 CVE ID 自動化的啟動程式至網際網路上相關弱點資料網站抓取該 CVE ID 細節資訊，及快速篩選該 CVE ID 是否於現有 Exploit-DB 網路上已經存有攻擊工具或程式碼，用以可快速識別那些 CVE 漏洞的風險程度最高，下圖 5-182 是 eNodeB VULDB 登入首頁畫面截圖。

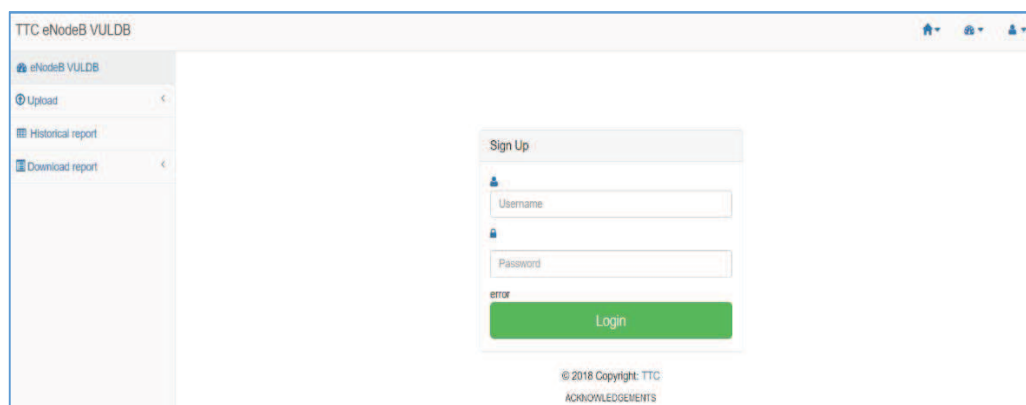


圖 5- 182 eNodeB VULDB 登入首頁畫面

資料來源： 本團隊整理

登入 eNodeB VULDB 後可精簡的透過一些過濾的選項，快速篩選結果(如圖 5-183)，例如：篩選出那些 CVE 在 Exploit Database 網站已存有攻擊工具或程式碼。

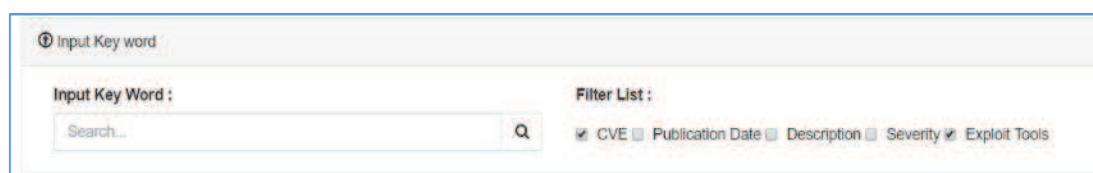


圖 5- 183 eNodeB VULDB 快速篩選功能

資料來源： 本團隊整理

在快速篩選的上方則是目前 CVE 從不同嚴重等級與相對應數量以長條圖顯示，如下圖。

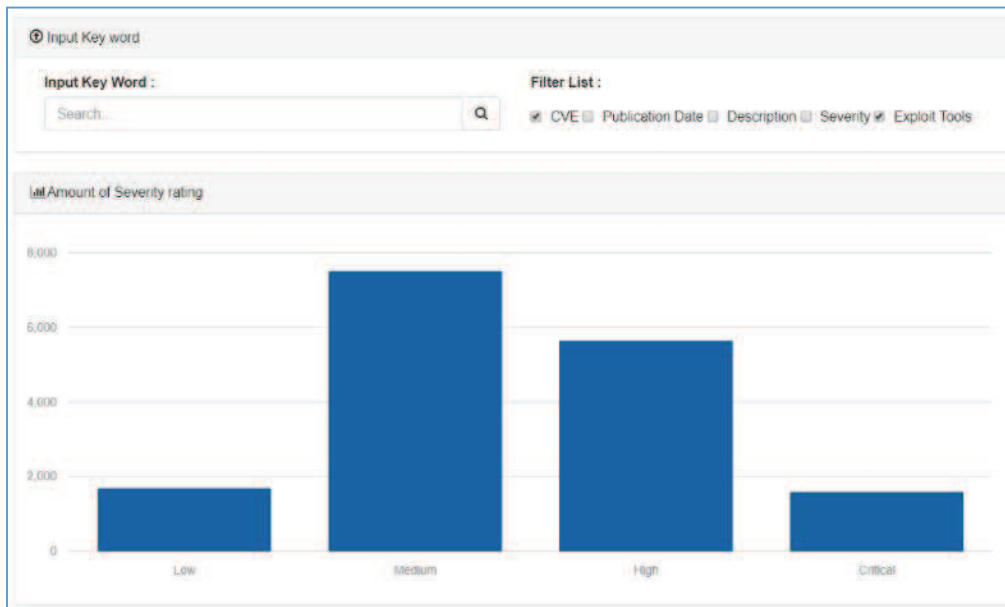


圖 5- 184 eNodeB VULDB 根據 CVE 嚴重等級呈現不同數量

資料來源： 本團隊整理

下圖為篩選出 CVE-2016-2776 漏洞在 Exploit Database 網站已存有攻擊工具或程式碼畫面。

Report					
CVE	Date Publication	Description	CVSS-Severity	Exploit-Tools	Download PDF
CVE-2016-2776	2016-09-28T10:59:00Z	buffer.c in named in ISC BIND 9 before 9.9.4-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc.....	High	EXPLOIT-DB:40453	Download pdf report

圖 5- 185 eNodeB VULDB Exploit-Tools 篩選功能

資料來源： 本團隊整理

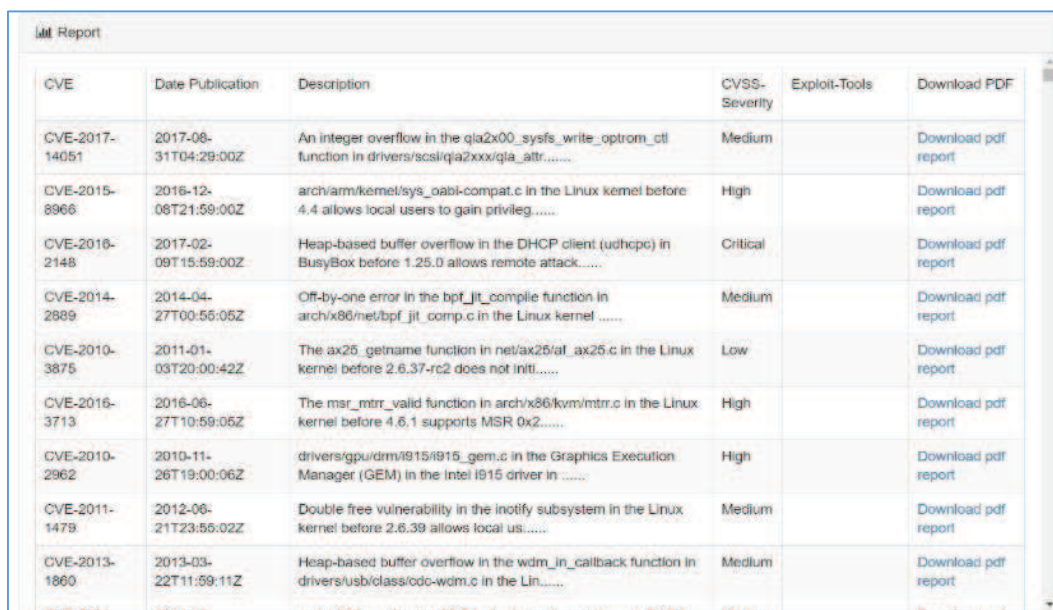
另外在介面上最後一欄則可選擇點選自動產出如下圖報表內容。

CVE	CVE-2016-2776
Publication Date	2016-09-28T10:59:00Z
CVE Description	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
CVE Severity	High
Exploit Tools	EXPLOIT-DB:40453
Exploit URL	https://www.exploit-db.com/exploits/40453/
Product ID	nokia
Recommendation	nokia
Technic Title	CWE-20: Improper Input Validation
Technic Description	The product does not validate or incorrectly validates input that can affect the control flow or data flow of a program.
Component	bind
Version	9.10.2
Latest Version	9.11.2
Match Type	Exact match
CVSS2	7.8
CVSS3	7.5

圖 5- 186 eNodeB VULDB 報表內容

資料來源： 本團隊整理

當清除掉篩選功能，系統畫面將顯示所有的 CVE 漏洞清單，如下圖摘要部分結果。



CVE	Date Publication	Description	CVSS-Severity	Exploit-Tools	Download PDF
CVE-2017-14051	2017-06-31T04:29:00Z	An integer overflow in the qia2x00_sysfs_write_optrom_ctl function in drivers/scsi/qia2xxx/qia_altr.....	Medium		Download pdf report
CVE-2015-8966	2016-12-06T21:59:00Z	arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privilege.....	High		Download pdf report
CVE-2016-2148	2017-02-09T15:59:00Z	Heap-based buffer overflow in the DHCP client (udhcpo) in BusyBox before 1.25.0 allows remote attack.....	Critical		Download pdf report
CVE-2014-2889	2014-04-27T00:55:05Z	Off-by-one error in the bpf_jit_compile function in arch/x86/net/bpf_jit_comp.c in the Linux kernel	Medium		Download pdf report
CVE-2010-3875	2011-01-03T20:00:42Z	The ax25_getname function in net/ax25/af_ax25.c in the Linux kernel before 2.6.37-rc2 does not initl.....	Low		Download pdf report
CVE-2016-3713	2016-06-27T10:59:05Z	The msr_mtrr_valid function in arch/x86/kvm/mtrr.c in the Linux kernel before 4.6.1 supports MSR 0x2.....	High		Download pdf report
CVE-2010-2962	2010-11-26T19:00:06Z	drivers/gpu/drm/i915/i915_gem.c in the Graphics Execution Manager (GEM) in the Intel i915 driver in	High		Download pdf report
CVE-2011-1479	2012-06-21T23:55:02Z	Double free vulnerability in the notify subsystem in the Linux kernel before 2.6.39 allows local us.....	Medium		Download pdf report
CVE-2013-1860	2013-03-22T11:59:11Z	Heap-based buffer overflow in the wdm_in_callback function in drivers/usb/class/usb-wdm.c in the Lin.....	Medium		Download pdf report

圖 5- 187 eNodeB VULDB 之 CVE 漏洞一覽

資料來源： 本團隊整理

第五節 小結

本章行動寬頻資安技術研究，從行動寬頻網路運作過程中最基礎的空中介面資安技術，透過文獻分析方法，探討偽基站造成用戶端(UE)隱私之可能資安議題，並規劃偽基站之概念性實驗平臺及實驗項目，研究發現目前有許多方式可以實現偽基站的架設，硬體的部分可以透過部分市售商品完成，而軟體的部分可透過開源軟體達成，例如：SRS LTE、OpenLTE 與 Openairinterface 等，而本團隊硬體與軟體規劃以 CMW500 完成實驗項目，期末以規劃之實驗平臺進行實測驗證，並提出建議之防護方向。

因為 VoLTE 需要使用 SIP 幫助資訊的傳輸，雖然 VoLTE 已成為各國通訊領域近年來的發展趨勢，但 SIP 協議裡面的漏洞所可能造成的嚴重危害，至今為止尚未被正視，並提出有效的解決方案，對於使用者來說，將會面臨非常大的威脅，因此，本團隊希望可以透過所提出的危害以及建議可能的有效防範方法，來做好萬全措施，防止這些問題將來可能造成更重大的資安漏洞。

另外在基站資安檢測技術研究上，首先從介紹了 LTE 系統架構分析基站安全威脅，行動寬頻網路內不再只有語音訊務，實現數據與語音業務在同一 IP 網路下，LTE

將全部業務承載於 4G 網路上，而基站又是行動寬頻網路僅次於 UE 終端設備，數量最多的網路單元，且位於網路管理邊緣，凸顯其資訊安全角色的重要性。

整理與分析 3GPP 在 LTE 所規劃的通訊協定及通訊安全設計與實作，但這些配置及規劃屬建議性質，並非強制規定。因此透過導入 ITU-T X.805 安全架構，進一步將基站功能分解，其通訊流程包含 S1 介面、X2 介面及管理介面，對應不同的安全平面：控制面、用戶面及管理面，分析 LTE 電信系統可能面對的安全風險。本團隊規劃檢測項目初步分為一般檢測項目及進階資安檢測項目，期中報告已完成一般性資安檢測項目規劃，其目的在於檢測待測基地台(eNodeB) 的功能性驗證，例如 Attach、S1 Release、X2 Setup 等功能，確認信令由終端 UE 到核網 EPC 之間的建立，其參數傳遞的可用性與完整性，經由加密演算法產生密鑰，以建立各網路單元從 UE、eNodeB、MME 到 HSS 的保密性、完整性與可用性。

我國目前行動網路服務以 LTE 技術為重心，成為有史以來成長最快的行動網路通訊技術，其中包含連結技術改變、通訊模式改變，以及資料取用模式等改變，進階資安檢測則以系統配置安全、通訊協定檢測、存取控制、滲透測試及弱點分析等項目，測試基站是否得以防禦常見之威脅，因為科技演進將帶來更多不同的市場發展趨勢變化，例如整合物聯網、巨量數據分析、更即時的雲端連結、人工智慧、工業應用改革或虛擬實境等成長趨勢，行動通訊的資訊安全是不可或缺的基本要素。

進階資安檢測項目主要基於 3GPP TS 33.117- Catalogue of general security assurance requirements 來作為進階資安檢測項目研究之基礎，並逐項進行評估與測試。在測試過程中發現 3GPP TS 33.117 許多測試項目內容要求，都必須從產品研發、設計、測試等階段去思考與理解，因為安全源自於設計，安全必須融入在製造產品的每一個階段，以至於 3GPP TS 33.117 很多測試項目的需求都必須由基站製造廠商提供更進一步的資訊才可以完成測試，而非購置設備的電信營運商的技術與維運人員可以掌握，製造商已經將許多細節包裝成簡易容易操作之介面，以因應行動通訊網路環境下面臨的各式各樣的突發狀況，讓維運人員可以快速操作使用與調整。

而在家用基站(HeNB)檢測項目研究中，本團隊主要參考 3GPP TR 33.820 和 3GPP TS 33.320，以及實際家用基站的試測，進而統整出了 6 個面向的測試項目，從實體層、本機的系統、家用基站的連網以及敏感性資料等方面撰寫測項，以檢驗家用基站是否

存在資安漏洞，為家用基站資安品質把關。透過實際檢測家用基站，發現許多設定皆需要原廠提供相關設定，家用基站拆解上較為容易，所以實體上的檢測較一般 HeNB 不同。而實測第三節的檢測項目，檢測到一些實際上可能遇到的威脅，比如資料保護的項目，拆解韌體可發現 IP 或是 Email 資料，應用程式的安全部分，網頁管理介面出現 OWASP top10 的威脅，通訊安全部分，相關網路連接埠不可使用公認明文傳輸的協定，而身分鑑別與授權的部分，身分鑑別與認證機制未確實，作業系統安全部分，可能會出現 CVSSv3 評分 7 分以上的威脅，最後硬體層的部分須嚴防可從 UART 到 JTAG 至除錯模式。透過上述實際檢測的結果，本文所提供的六大項目可提供家用基站更嚴密的防護。

同時根據家用基站所面臨之問題核心，研究家用基站資安監測技術，透過對系統內核的掛鉤配合白名單的機制可以對非法的程序進行監控和阻擋，監控結果用以反饋測試項目，同時在韌體更新後的安全參數設置以及系統開機程序的保護可以提供抵擋和通報的協助，至於在建立重要檔案的防護的部分，可以用來保護用戶清單、4G 設定檔、系統日誌和密碼檔的存取控管，在優化家用基站資安檢測技術研發的同時，提供反駁客入侵家用基站的防護。

在本章節的研究中，本團隊也納入 EPC 與 E-UTRAN 最重要的橋樑 MME 的安全與威脅探討，並深入 3GPP 安全規範研究，研析 MME 的隱藏威脅、MME 在 EPS 安全性文本、UE 安全模式、非緊急通道的防護及 MME 的檢測項目，以上說明目前國際組織已經重視 MME 的安全性問題並提出相應的解決辦法，起初認為 MME 應該能夠介入 UE 的認證邏輯，經研究後發現 MME 無法介入 UE 的邏輯檢測（如：異常位置註冊網路），這些檢測屬於其他核心網路元件來完成，但是 MME 在傳輸訊息的安全性卻極為重要。由整理 3GPP 規範 TS 33.926、TS 33.401、TS 33.116，在未來參考 MME 安全防護上，建議可以上述規範作為制定 MME 檢測項目之參考依據。

最後本團隊也將基站檢測結果，建立弱點資料庫，未來也希望能持續更新，以供各界參考。

第六章、建構行動寬頻基站資安檢測平臺

本章主要從建構行動寬頻資安檢測平臺的功能與元件加以說明，從資安即國安的戰略思維出發，以保護國家基礎建設安全為依歸，延續第一期研究的成果，將概念性平臺藉由實作加以延伸，以提供全方位基站資訊安全檢測為目標，考量行動網路之特性，以務實的態度發展出適合我國資訊安全環境需求，完整且全方位的行動寬頻基站資訊安全檢測方案(Scheme)。

基於適用性考量，本章將完成符合我國使用環境之行動寬頻資安檢測平臺建構，其建置之目的在檢測行動寬頻基站於我國使用可能存在之資訊安全風險，建議經由第三方公正平臺的檢測並觀察待測基站抵擋攻擊的能力，參考最終之檢測報告以瞭解其可能存在的弱點以及可能遭遇的最新資安威脅，提前規劃因應未來上線後需要採取的縱深防禦策略。

為確保檢測平臺的可用性、可控性與真實性，平臺中包含營運環境的仿真(Emulation)，藉由將基站上線於仿真環境以瞭解在標準、異常信令與兩者混和的運作狀況，一方面確認基站的穩定性、堅實性與可靠度及對於異常狀況的基礎因應能力，須能符合作為國家基礎建設營運使用的基本要求，另一方面也可避免模擬(Simulation)環境所可能造成不夠客觀的疑慮。

除了真實營運環境的評估外，另一個重點則是在面對來自網路上各類資訊安全威脅時，對基站可能的存在弱點所造成之影響，及對於惡意行為與攻擊之抵禦能力評估，在此一階段中，本平臺將透過相關的軟、硬體對待測基站進行評估與弱點識別，藉此瞭解基站抵禦威脅之能力。為能更進一步針對長程演進計畫(LTE)行動網路中基站可能遭遇的資安威脅加以檢測，考量 LTE 網路服務、通訊交握操作及攻擊切入點等特性，以作為建構平臺細節之基礎。此外依前期行動寬頻基站資安檢測平臺規劃，進行相關需求元件、功能及環境要求等評估，以完成本計畫目標之基站資安檢測平臺之建構，預期能完成配合本計畫基站資安檢測項目之執行，提供檢測平臺測相關驗證紀錄，以作為後續進行實際資安檢測、研擬並提出檢測方針與作業程序標準化建議作業內容，產出適用於行動寬頻環境之專屬弱點檢測資料庫。相關執行步驟說明如圖 6-1 所示。

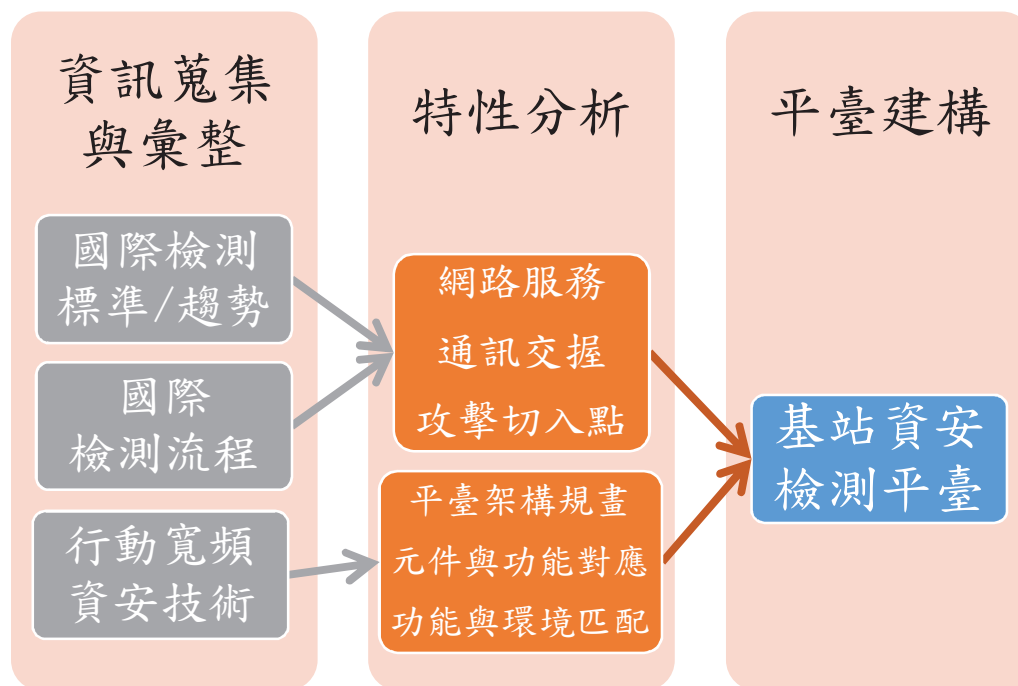


圖 6-1 建構基站資安檢測平臺執行步驟

資料來源：本團隊整理

此外，平臺以基站實際運作情境設計作為基礎測試，單一測試情境可包含多種不同的使用任務，而任務本身即根據電信業者實際上使用基站的狀況而設計。當使用情境越能反映出真實狀況，則平臺測試結果的可信賴度就更高，能夠精確的產出一個近似於實際使用狀況的測試結果。因此，能致使受測基站更加容易呈現在受到攻擊時的運作狀況。

以下的章節中，將先從平臺的架構與各元件分別進行解構與逐一說明和研析，之後透過一系列的方法對平臺及各元件的有效性進行驗證，並作出建議。

第一節 研析行動寬頻基站資安檢測平臺架構

本計畫之平臺架構係基於建置基站資安檢測環境計畫(第 1 期)的研究成果加以落實外，同時考慮到未來的延伸與檢測應用之需求，務求在技術上與時俱進，從更為全面的觀點出發，在架構上要更有彈性，藉由將平臺模組化以簡化佈署，透過框架(Framework)概念組合各模組元件，使基站能在近似完整的行動寬頻網路中被實驗與檢測，此外本團隊更進一步參考國際上針對 5G 及物聯網(Internet of Things)的檢測環境

設計考量^{338、339、340、341、342}，去蕪存菁後加以整合並納入架構之中，因應未來行動寬頻技術結構因應整體趨勢而升級時，平臺架構既有的彈性與擴充性能提供良好的因應策略，除了維持對既有設備的投資保障外，亦可兼顧使用者經驗的提升，以減少教育訓練、支援成本與維護費用，進而提升檢測品質。

相關的研究中 Andrea³³⁸ 等人使用較為先進的虛擬化核心網路架構測試網路，是針對應用服務提供相對完整的開發與測試環境；Almudena³³⁹ 等人嘗試使用基站模擬器，核心網路模擬器與軟體定義網路混搭出三種模式，進行通訊效能檢測，結果與商業實際核網的比較，仍是實際核網有較佳的表現；但這些都未將資訊安全納入考量。Aleksandr³⁴⁰ 等人使用實體核心網路進行裝置對裝置通訊(D2D)的測試架構，其強調透過中繼設備加強 UE 之間通訊應用之安全，並未將基站納入整體安全考量。George³⁴¹ 等人使用虛擬化平台展示了可擴展性與靈活性佈署應用於 2G/3G/4G 環境的可行性，並且驗證可用以進行訊息完整性檢查、UE 與 P-GW 之間通訊時的核心網路有關資訊洩漏檢測、及 UE 的 IP 可接受手動配置等問題，但仍缺少對基站的安全評估工作。Jill³⁴² 等人的研究則是透過大量的 UE 模擬，以產生分散式阻斷攻擊模型藉此提供電信業者檢測自家防禦機制是否奏效之評估。

本平臺各功能模組單元之規劃如圖 6-2 所示，主要由五大部分所構成，包含用戶端裝置單元、核心網路單元、主動式常見與潛在弱點檢測單元，以及被動式連線與滲透行為分析單元。其中，以實心線段連接表示各單元之間可能產生相互作用的對應關係，此外主動式常見與潛在弱點檢測單元的連接位置則用以表示可能的攻擊切入點。上述提及的相關規劃，將本平臺各單元之目的、功能與可運用及整合的設備之綜整概述如表 6-1 所示。

³³⁸ Andrea F. Cattoni et al., "An End-to-End Testing Ecosystem for 5G the TRIANGLE Testing House Test Bed", Journal of Green Engineering, 2016/12.

³³⁹ Aleksandr Ometov, Pavel Masek, Jani Urama, Jiri Hosek, Sergey Andreev, and Yevgeni Koucheryav, "Implementing Secure Network-Assisted D2D Framework in Live 3GPP LTE Deployment", 2016 IEEE International Conference on Communications Workshops (ICC), 2016/5.

³⁴⁰ Almudena D'íaz-Zayas(B), Cesar A. García-Pérez, 'Alvaro M. Recio-Pérez, and Pedro Merino-Gómez, "PerformLTE: A Testbed for LTE Testing in the Future Internet", 13th International Conference, WWIC 2015, Malaga, Spain, May 25-27, 2015.

³⁴¹ K. Jijo George, A. Sivabalan, T. Prabhu and Anand R. Prasad, "End-to-End Mobile Communication Security Testbed Using Open Source Applications in Virtual Environment", Journal of ICT Standardization, 2015/7.

³⁴² Jill Jermyn, Roger Piqueras Jover, Mikhail Istomin and Ilona Murynets, "Firecycle: A scalable test bed for large-scale LTE security research", 2014 IEEE International Conference on Communications (ICC), 2014/6.

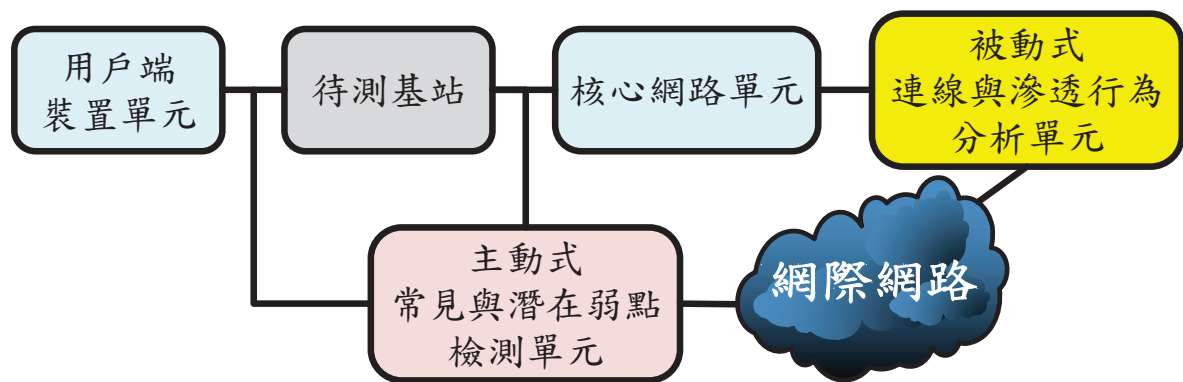


圖 6-2 基站資安檢測平臺各功能模組單元對應關係概念圖

資料來源：本團隊整理

表 6-1 建構基站資安檢測平臺執行步驟

對應功能 元件名稱	目的與功能說明	可運用及整合的設備
用戶端裝置單元	使用者行為仿真，以檢測基站之符合性與功能性為主，並進一步模擬大量負載與變因控制對基站進行檢測。	● 工程手機 ● 用戶端模擬器
待測基站	以介面、信令與通道特性為受測基礎之基站，由本平臺對其施行資安弱點檢測。	● 符合 LTE 通訊規範之基站
核心網路單元	核心網路行為仿真，作為基站與用戶端裝置之行動性、政策管理和安全性等功能之檢測使用。	● 核心網路模擬器 ● 實際核心網路 ● 虛擬化核心網路
主動式常見與潛在弱點檢測單元	惡意/攻擊行為仿真，針對待測基站進行各式弱點掃描與探測。	● 程式碼分析工具 ● 網頁弱點分析工具 ● 通用弱點分析工具 ● 滲透測試工具 ● 未知弱點檢測工具

對應功能 元件名稱	目的與功能說明	可運用及整合的設備
被動式連線與滲透行為分析單元	基站連線行為監測，評估待測基站在正常營運狀況下與遭遇攻擊時可能發生的行為。	● 集中式威脅管理系統 ● 防毒閘道 ● 入侵偵測/防禦系統 ● 防火牆 ● 行為分析沙箱系統

資料來源：本團隊整理

基於檢測平臺使用模組化建構，高彈性設計使每個模組單元可使用多種不同之元件，且高擴充性設計可使各個模組以及模組所使用之元件，均能依據不同的檢測任務及需求加以調整與置換，且能依據實際需求調整檢測規模，使檢測複雜度更能比擬真實的網路應用環境，從模擬(simulation)到仿真(Emulation)再到近似於真實(Near Real)的逐步提升，以期能為國家基礎建設的資通安全作適當而嚴謹的把關。以下內容將就各模組單元逐一列舉，並提供進一步的說明與研析。

一、待測基站 (Evolved Node B)

最初行動寬頻網路(4G LTE)網路主要的設計目標有：

1. 提高尖峰資料傳輸率(Peak Data Rate)，以提供與 xDSL 匹敵的資料傳輸速率。具體來說，其目標為在 20MHz 的頻寬中能夠提供下行 100Mbit/s、上行 50Mbit/s 的尖峰傳輸速率；
2. 提高網路覆蓋區域邊緣的傳輸性能，允許網際網路應用能夠被無縫整合，不受到載波技術的影響；
3. 降低系統延遲與連線設定時間。其具體目標為將無線存取網路區域的延遲減少至 10 毫秒，同時要讓使用者在 LTE 網路上要有「隨時連線」的即時感覺。其他設計目標則包括增進頻譜效率、支援可調式頻寬以及和現有系統及非 3GPP 系統的互通等。

為了實現上述要求，LTE 無線通訊系統須對 3G 系統的空中介面(Air Interface)技

術和網路結構提出改進與增強。由於牽涉到兩種行動通訊的主要元素，因此 3GPP 於 3GPP Release 8 標準規範中，將 LTE 與系統架構演進(System Architecture Evolution, SAE)技術規範區隔開來，後來兩者分別演進成 3GPP Release 8 標準中定義新型無線存取網路的演進統一陸地無線接取網路(Evolved Universal Terrestrial Radio Access Network, E-UTRAN)，與核心網路的演進數據分組核心網路(Evolved Packet Core, EPC)，其網路概念架構如圖 6-3 所示。

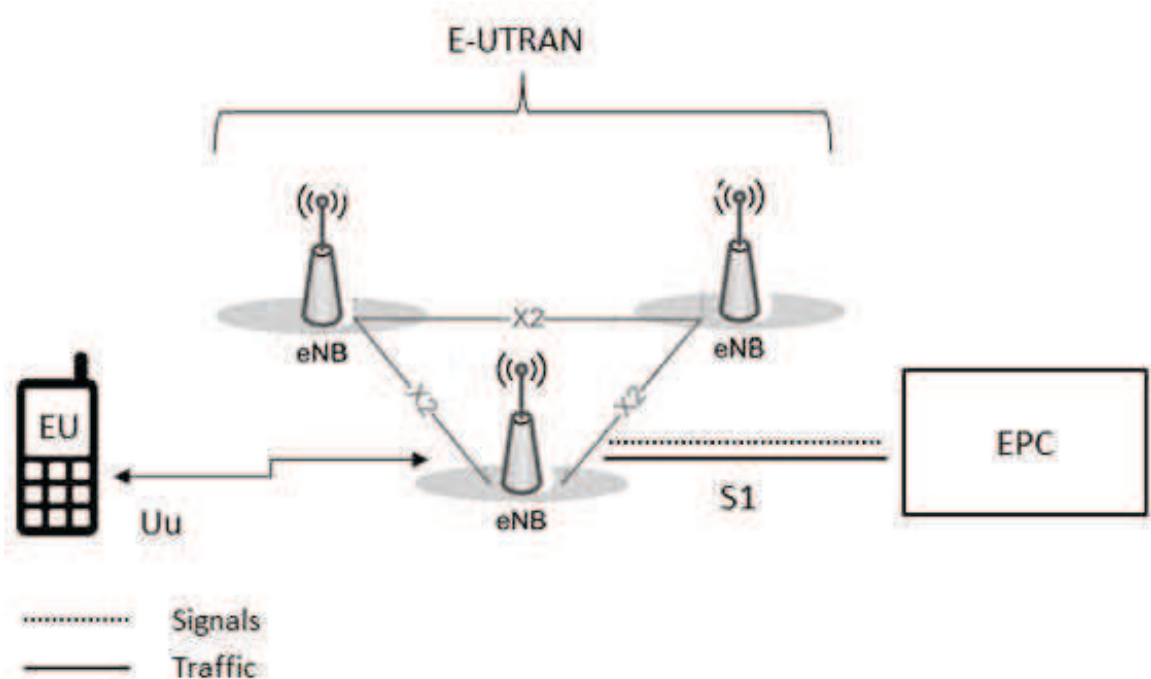


圖 6-3 第四代行動通訊網路層通訊功能模組關係概念圖

資料來源：Tutorials Point³⁴³

由於 E-UTRAN 本質上是一種正交分頻多工(OFDM)通訊技術，可支援分頻雙工(FDD)與分時雙工(TDD)模式，以及多種不同的頻寬(1.4M~20MHz)。不同於傳統 2G/3G 無線存取網路會連接到 3GPP 核心網路的電路交換領域(Circuit-switched Domain)，LTE 的 E-UTRAN 無線存取網路只會連接到純封包交換領域(Packet-switched Domain)的演進數據分組核心網路(EPC)網路。

因此，整個 E-UTRAN 無線網路通訊協定已針對以網際網路通訊協定(IP)為基礎

³⁴³ Tutorials Point, LTE Network Architecture, 2012/11/14.

的即時與非即時應用與服務進行最佳化，通訊堆疊關係如圖 6-4 所示。從介面連接與信令交握方面而言，基地站掌控了提供 E-UTRAN 用戶平面(User Plane)與控制平面(Control Plane)在 eNodeB 與用戶端裝置(User Equipment; UE)間的資料傳輸協定，其中用戶面包含封包資料匯聚通訊協定(PDCP)、無線連結控制(RLC)、媒體存取控制(MAC)、實體層(PHY Layer)等元件，控制面則是由無線資源控制模組(RRC)所構成。

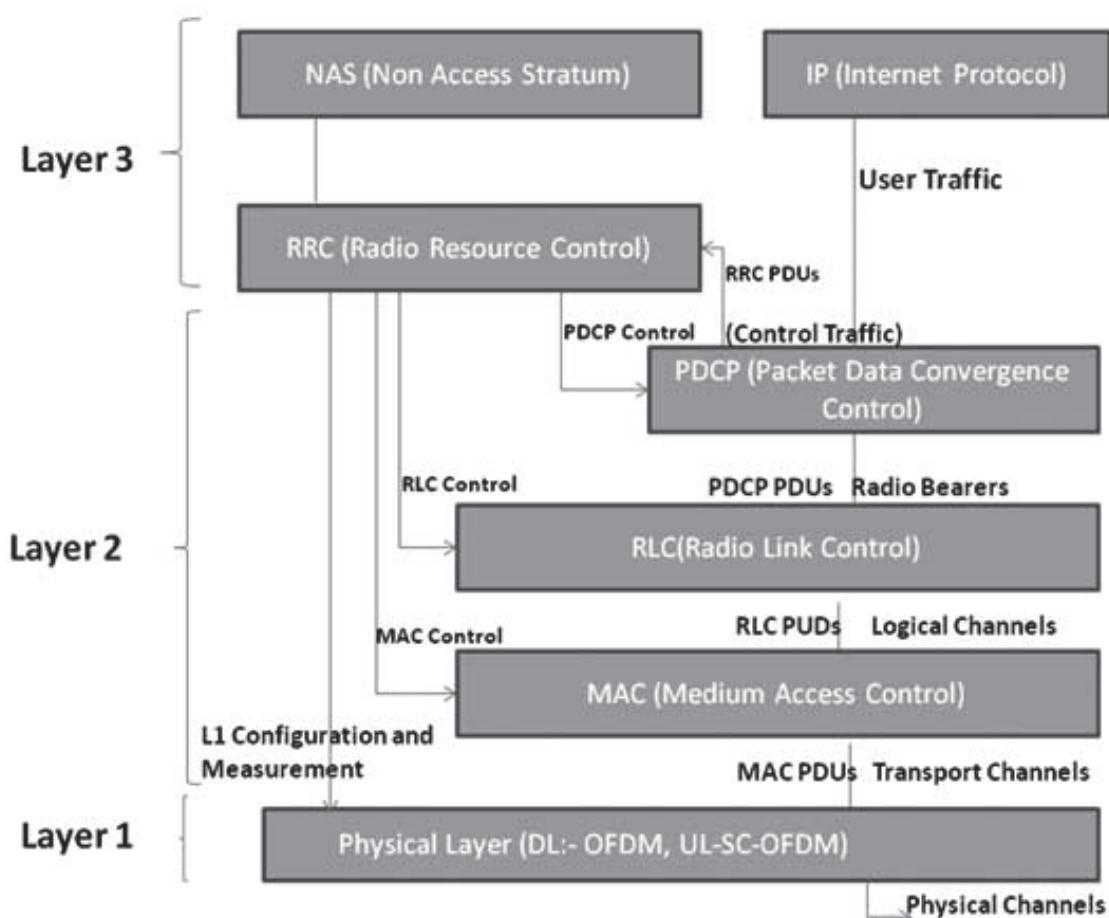


圖 6-4 E-UTRAN 通訊堆疊圖

資料來源：Tutorials Point

從上述可知，E-UTRAN 無線網路通訊協定主要是針對 UE 與基地台端(eNodeB)的無線存取傳輸部分進行定義，因此在這個架構下只會有一個元件即演進節點 B (Evolved Node B)也被稱為 E-UTRAN 節點 B(E-UTRAN Node B)。

通常行動電信基地台的總類大致可以分成兩類，分別是大型基站(Macro Cell)與小型基站(Small Cell)。其中，Macro Cell，是一般所認知的行動電信基地台，電波覆蓋範圍約為 2 公里~40 公里，發射功率為 40W~100W，可以容納的用戶可以 256~1000 個用戶以上。而 Small Cell 是一種低功率的無線接入節點或小型基站，發射功率為 10mW~10W，涵蓋範圍由 10 公尺至於 1~2 公里，可以被用來當成行動通訊數據卸載 (Mobile data offloading) 之用。Small Cell 又可依涵蓋範圍與可容量用戶量細分成超微型基地台(Femtocell)、微型基地台(Picocell) 與小型基地台(Microcell/Metro)等。其中 Picocell，發射功率為 250mW，適用於室內與室外公共區域，例如商業大樓、人群聚集的大型廣場及巴士/火車站等處，可容納 64~128 用戶，涵蓋距離為 200~500 公尺左右，可有效補充網路容量，可幫助電信商以最小的發射功率、干擾，做到對行動用戶的服務。Microcell 則是一種戶外式的小型基地台，發射功率為 2W~10W，適用於小型城市，可容納 128~256 個用戶，涵蓋距離為 2 公里~5 公里以內。未來步入 5G 與物聯網時代，當前多數行動數據流量都需要透過 Macro Cell 來處理的情形將會改變，Small Cell 與其他異質網路都將會是扮演未來行動通訊與物聯網分攤數據流量負擔的重要角色，此外為降低 LTE 的佈建成本，並進一步擴大訊號覆蓋範圍，包括 AT&T、威瑞森(Verizon)、沃達豐(Vodafone)、Sprint、SK Telecom 和西班牙電信(Telefonica)等主要 LTE 電信業者，皆已開始積極部署 LTE Femtocell。對於基地站的佈署與應用情境如圖 6-5 所示。

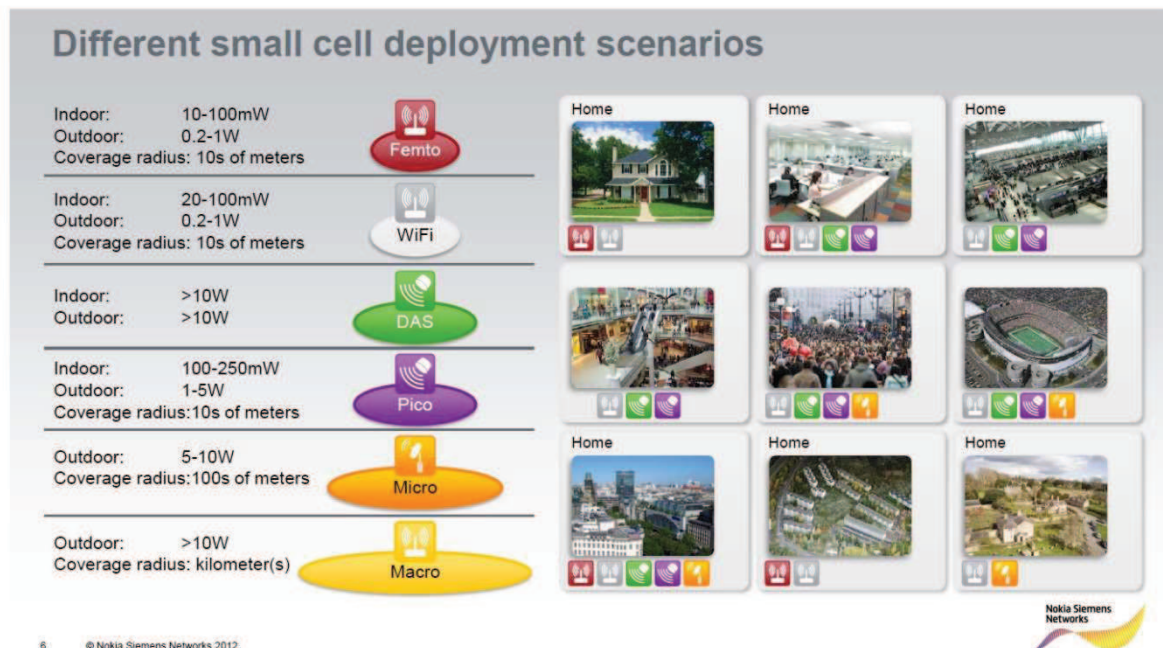


圖 6-5 各種基站佈署情境比較

資料來源：Nokia Siemens Network³⁴⁴

eNodeB 是利用 S1 傳輸介面與 EPC 網路進行溝通，更明確的說，eNodeB 是利用 S1-移動管理實體(S1-MME)傳輸介面與移動管理實體(MME)進行溝通；另一部分 eNodeB 與 eNodeB 之間的通訊信令則是經由 X2 傳輸介面進行溝通；至於與服務閘道(S-GW)的通訊則是透過 S1-U 傳輸介面進行。S1 介面通訊概念如圖 6-6 所示。

³⁴⁴ 3G4G blog, Small Cells: Comparison and Deployment Scenarios, 2012/11/14.

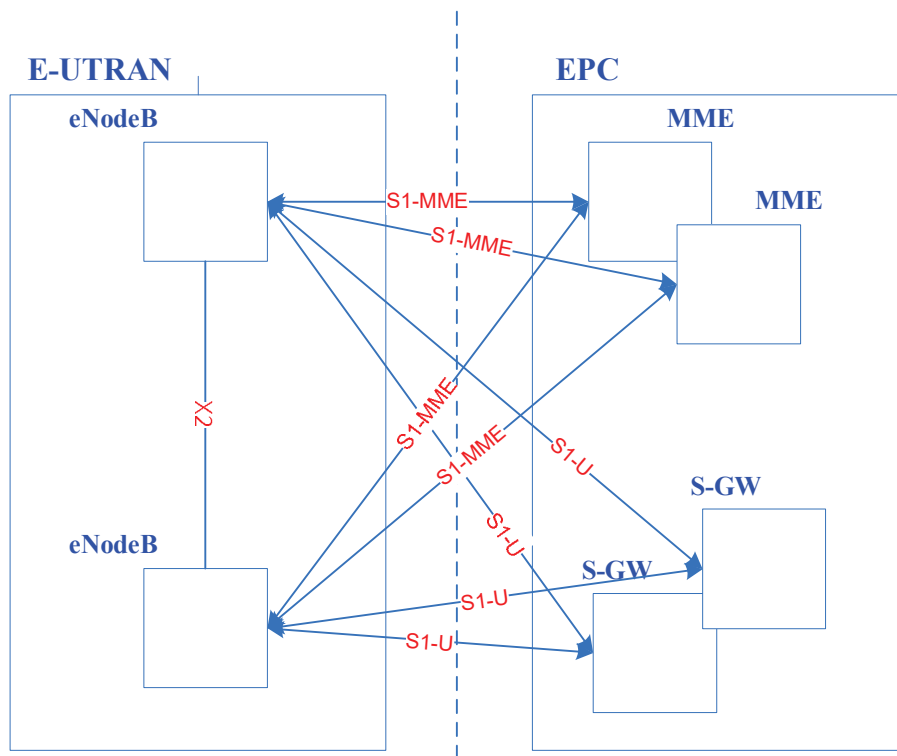


圖 6-6 S1 通訊介面連接概念圖

資料來源：新通訊 2009 年 10 月號 104 期³⁴⁵

基於這樣的通信機制，eNodeB 可能存在的安全缺陷，將連帶的對於 LTE/SAE 系統安全造成莫大的威脅。從圖 6-7 不同世代基地台的演化與擔負之任務架構觀之，主要是由於 E-UTRAN 的接取網路捨棄了傳統的 RNC/NodeB 的兩層式架構，採用由 eNodeB 的組成的單層式架構，其優點是使整個通訊系統架構趨於扁平化，以達到簡化信令與縮短延遲的目的，但這樣的方式也可能導致一系列的安全問題。

³⁴⁵ 新通訊, NAS/MAC/PHY 各司其職 LTE 通訊協定預埋 4G 伏筆, 2009/10.

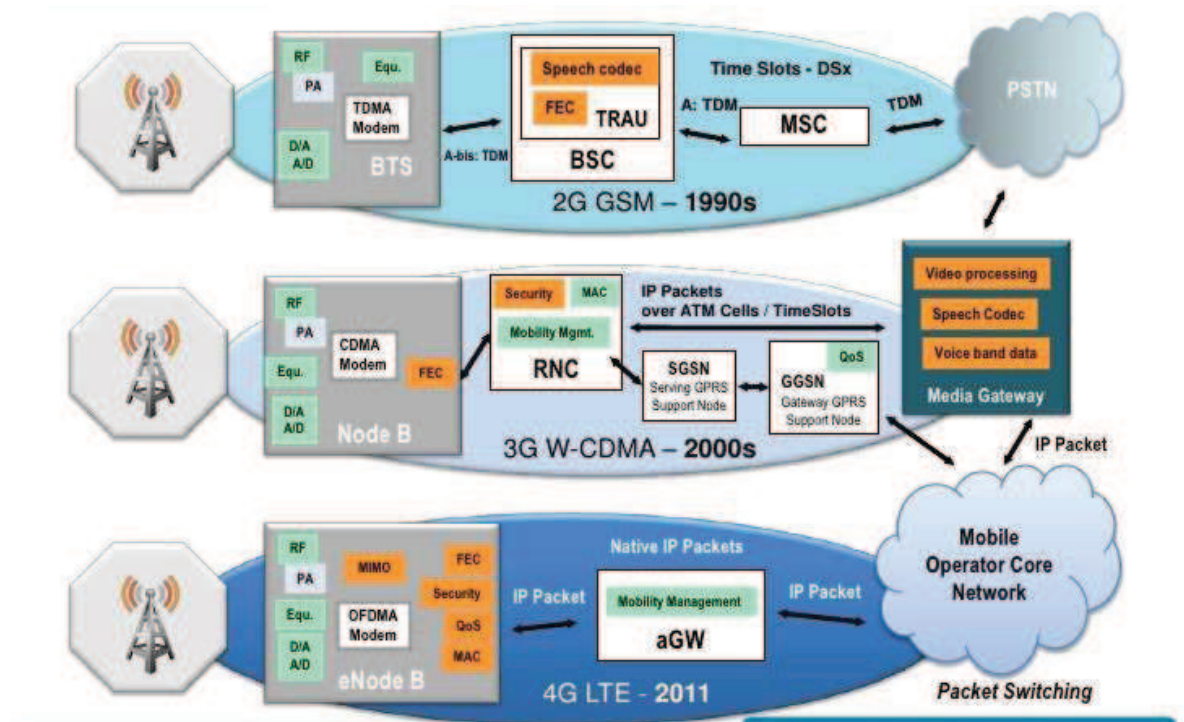


圖 6-7 不同世代基地台的演化與擔負之任務

資料來源：4GWE conference³⁴⁶

此外也有研究指出³⁴⁷，由於目前 X2 換手機制如圖 6-8 所示，面臨的缺乏後向安全性以及易遭受去同步化攻擊，因為這些缺點，難以確保過程中不會發生資料遭竊取或是竄改的情況發生，因此衍生出的機密性(Confidentiality)與完整性(Integrity)威脅也是相當重要的議題。為了防堵惡意基地台造成換手執行中的安全疑慮，該研究也嘗試設計並提出一個完整的安全機制，以防堵攻擊者的惡意攻擊竊取資訊。

³⁴⁶ Jim Johnston, Evolving the Evolved Packet Core, 2011/2/2.

³⁴⁷ 楊朝成，強化 4G LTE 認證及換手機制，國立中興大學資訊管理學系，2015/7.

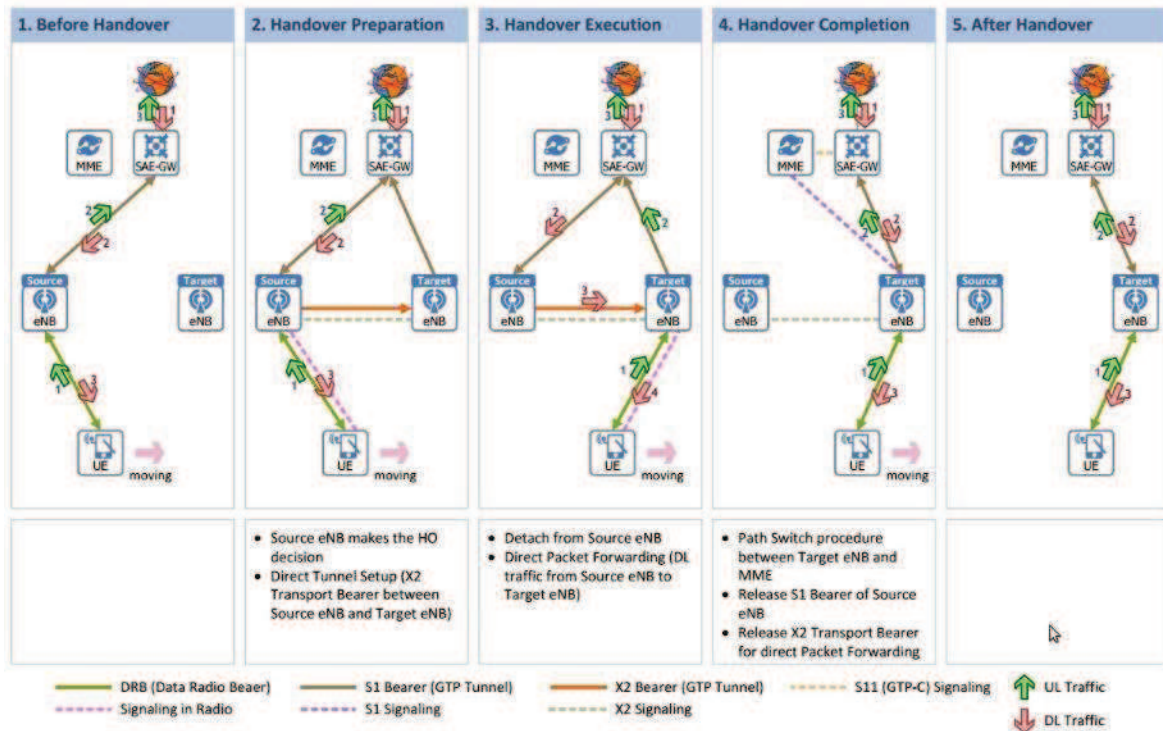


圖 6-8 X2 介面換手流程示意圖

資料來源：3GLTEInfo.com

為此本團隊所提出的檢測平臺，基於可檢測所有種類基站之理念，如圖 6-9 所示，以前述所提及的基站介面、信令與通道特性為考量基礎，在未來的測試中，將分別從小型基站(Small cell)與大型基站(Macro cell)中，各擇定一組進行測試，並進一步納入以偵知基站本身安全威脅與可能面臨之風險之資安弱點檢測技術，在種種條件與限制的考量下，設計出可涵蓋所有類型基站檢測之平臺，而這樣的設計將有利於使用主動或被動或以同步進行的方式，尋找出可能的危險因子，後續藉由對這些危險因子的分析、解構與彙整成結構化之資料形式，以作為政府機關後續在制定相關政策或使用單位擬定防禦策略的參考依據。

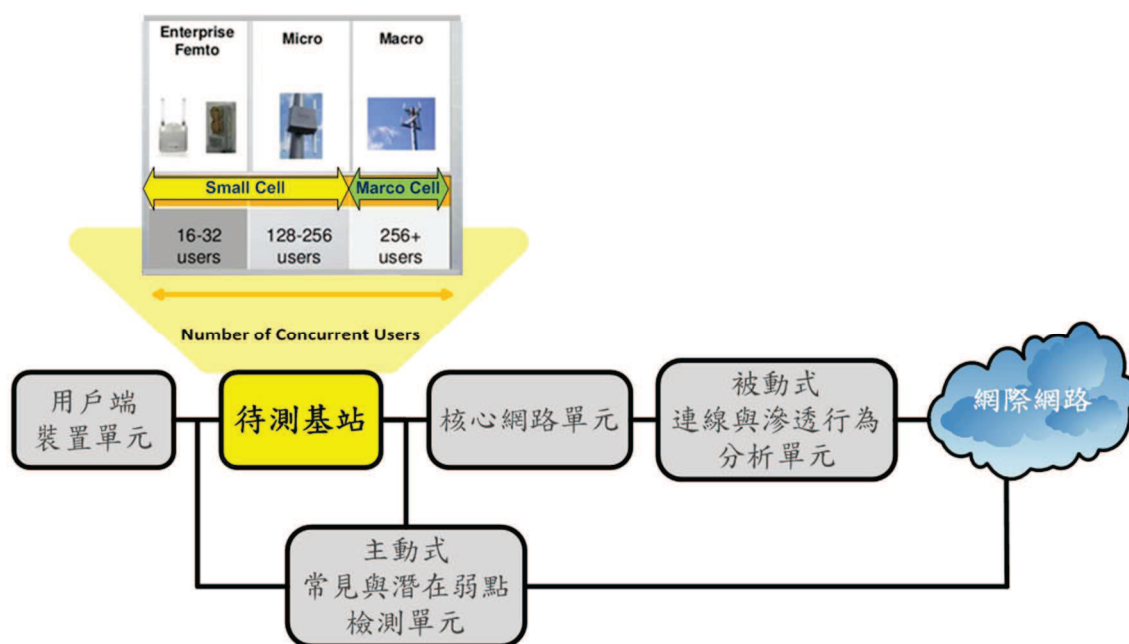


圖 6-9 基站資安檢測平臺-可應用之基站設備檢測類別圖說

資料來源：本團隊整理

二、用戶端裝置單元(User Equipment，簡稱 UE)

由於用戶端裝置，不論是在基礎或進階資安測試方面都是主要的關鍵角色之一，而傳統上通常會將檢測分成兩個階段進行，先在實驗室而後在現場進行。因此實驗室測試最先是採取深入的符合性與功能性測試形式，先利用單一用戶裝置透過進行小規模測試，取得重複且精確的結果，以確保符合 3GPP 規範，而現場則需要透過適當的設備以取得完整的網路涵蓋及效能資訊，在本平臺的規劃下，用戶端裝置單元可以經由使用工程手機與用戶端模擬器參與測試。

考量單純使用工程手機，可能不容易重現高容量性能狀況下的基站受攻擊時的狀況，因此通常需要在相對複雜的實際環境下進行，但由於實際環境下的變因太多且不易控制，所以實驗室一般會採取用戶端模擬器進行大量用戶的模擬測試，以此評估基站的堅實性與可靠度。除此之外，還能進一步將小規模測試所發現的異常現象加以擴大，以模擬實際環境中用戶連線高負載的場景，透過變因控制重現依據特定目的(例如：各式攻擊或異常行為)所製造的容量測試。再者，變因控制又可進一步透過工程手機與用戶端模擬器兩者的共同搭配，先由用戶端模擬器製造大量且正常的交握程序，再由

工程手機結合其他設備進行攻擊與擾亂信令，以試圖影響正常營運的方式，透過本平臺進一步反應出精確的檢測數據與結果。

此外在 LTE 無線漫遊的機制中允許使用者任意的漫遊至各地，行動通訊協定主要特點就是每個節點之間可藉由訊號的傳遞收發，直接相互溝通且做連結，無法確保不會發生資料遭竊取或是竄改的情況發生。在設計此檢測平臺過程，也務實考量種種可能的狀況，以盡可能呈現所有營運環境中真實狀況的考量作為本單元之目標。

因此為了避免測試結果與實際環境有落差，因此我們在此單元中，將也將平臺規劃設計成可分別透過工程手機與用戶模擬器進行測試的場景，如圖 6-10 所示，希望藉此消彌所有測試過程中不可控的變因，以求得更精確且可靠的結果。以下將分別對工程手機以及用戶端模擬器的應用做進一步的說明。

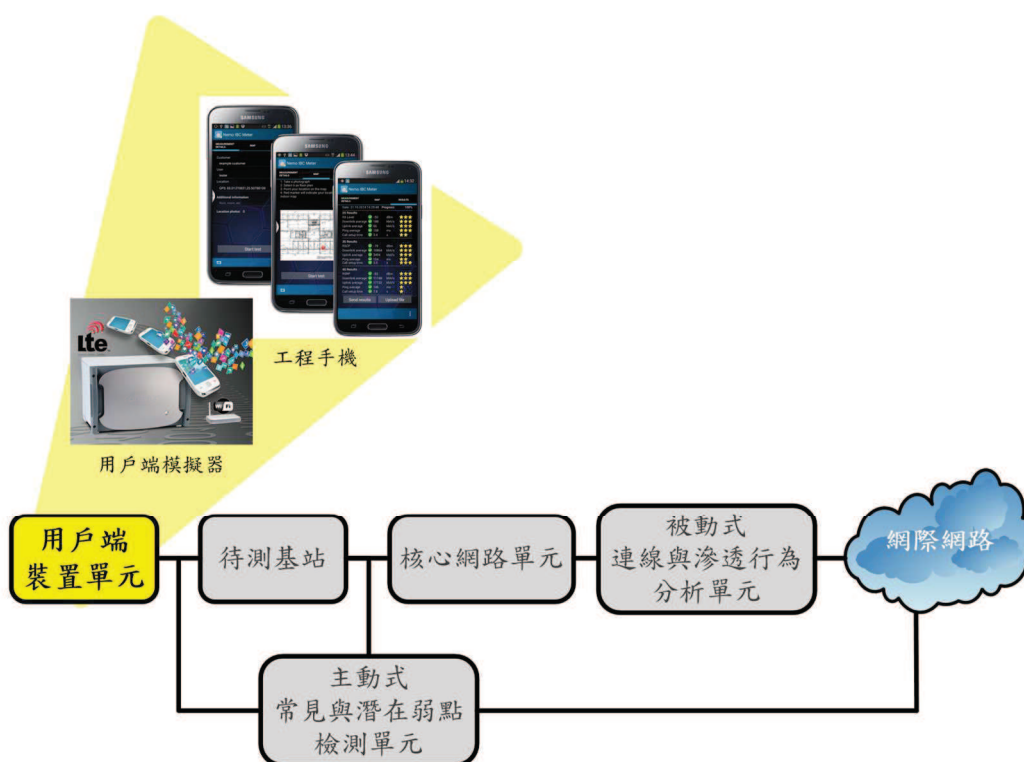


圖 6-10 基站資安檢測平臺-可應用之用戶端設備類別圖說

資料來源：本團隊整理

(一) 工程手機

一般而言，「工程手機」與「商用手機進入工程模式」有著本質上的差異，以 Android 作業系統手機而言，工程模式通常是指在撥號鍵盤中輸入一些數字指令之後，進入的一種操作模式，在這個模式中，手機自動列出可以透過點選的方式測試手機的基本功能(螢幕壞點、螢幕觸摸、傳感器、LED 燈、相機、閃光燈、實體按鍵等等)，或透過指令執行取得手機內部細節資訊的各項進階功能(電池細節資訊查詢，處理器測試等等)。

而工程用的測試手機則是在商用手機上安裝廠商所開發的專屬軟/韌體，通常是電信業者或開發商為了確保行動通訊網路的品質，所提供專業的量測和監測功能之手持式檢測設備，以診斷通訊網路空中介面(Uu)、行動應用的服務品質(QoS)與體驗品質(QoE)等狀態之用，且能進一步對特定設備的系統、頻段、載波、SC、通道和 PCI 下達強制鎖定命令等行為。簡而言之，工程用的測試手機只是使用不同軟/硬體系統(例如 Anite 的 Nemo Handy 手機與 ASCOM 的 TEMS Pocket)的一般商用手機，檢測人員可透過這些手機專業的附加功能進行無線通訊的詳細檢測，與提高自動化程度並簡化流程，使檢測人員能利用更少資源完成更多工作並有益於專注自身核心領域。此外也可透過將測試、分析和驗收流程自動化，及量測分析通訊過程基站之間進階的點對點資訊交換內容，並進一步從量測資料的蒐集到後期處理與分析，透過動態線條(Line graph)、柱狀圖表(Bar graph)及文字(numeric)即時顯示 RF 涵蓋訊號、L3/RRC 信令及 KPI 參數於手機視窗，並支援包含 LTE、LTE Cat.6 及 VoLTE 等無線網路量測，以透過不同測試項目蒐集各網路涵蓋及效能之相關資訊。

此外從資訊安全的觀點來看，2015 年的歐洲黑帽大會 Altaf 等人展示了如何透過偽基站繞過 LTE 手機的安全措施³⁴⁸，其中包含了包含定位資訊暴露隱私的問題，及電波覆蓋式攻擊造成連線中斷(包含讓受害的用戶端裝置)的資訊安全問題，如圖 6-11 及圖 6-12 所示；從這些測試所帶給人們的警訊顯示，本團隊認為長遠而言，這樣的研究成果所揭露的資訊只是開端，後續將可能面臨新一波的考驗。

³⁴⁸ Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi and Jean-Pierre Seifert, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems", 21-24, 2016/2.

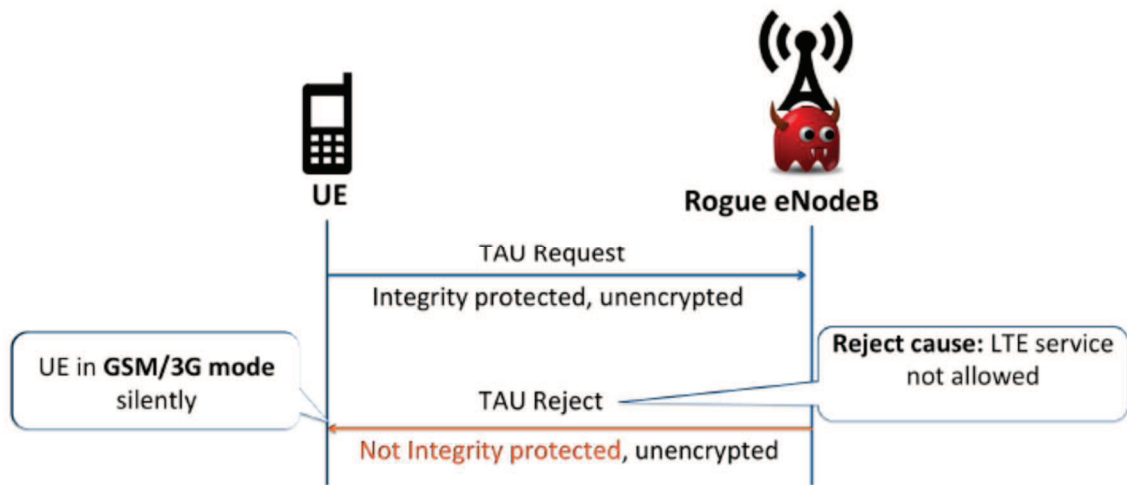


圖 6-11 對用戶端設備進行 LTE 服務阻斷行為

資料來源：Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

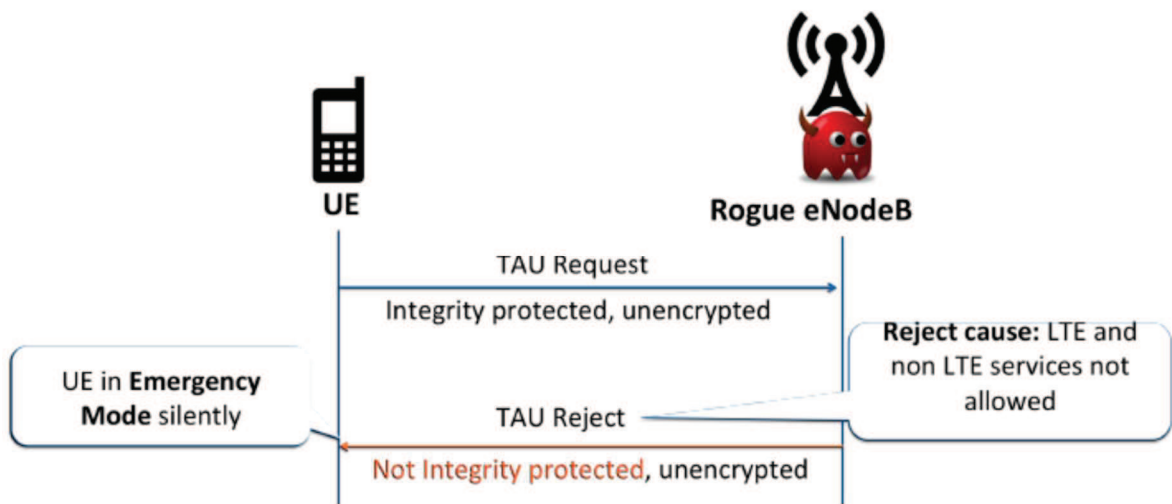


圖 6-12 對用戶端設備進行所有服務阻斷行為(進入緊急模式)

資料來源：Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems

因此透過工程手機來進一步發掘可能的問題，亦是本平臺相當重要的一個部分，期望藉由檢測框架的輔助與平臺結合，能在事態擴大前找出可行的因應方案，以提供主管機關與業者在政策面與實務面執行的參考依據。

（二）用戶端模擬器

許多電信業者及供應商認為，與真正網路服務中使用真正的手機 UE 裝置相比，在 RF 使用 UE 模擬器是折衷方式，主要是可以在實驗室模擬實際營運環境中，大量使用者的各種行為，以找出異常的關鍵因素。但對於問題的搜尋及性能確認，大量使用者裝置模擬後所造成的複雜度，仍然需要能透過信令堆疊的追蹤對所有階度進行檢測以取得詳細的測試結果，UE 信令堆疊之間關係圖如圖 6-13 所示。而適當的用戶模擬器將可提供檢測過程中對於實際環境的可控變因模擬，使得測試將能更接近電信商的營運環境與遭遇之狀況。

此外無線通訊實驗平臺設計通常需要考量，若涉及 Uu 信號，由於 Uu 介面的信號強度可能受到施測當時的環境因素(溫度、濕度、電子設備干擾等)的影響，因此實驗中的部分裝置將採用模擬器，以避開這些可能干擾實驗結果的因素，使得部分實驗參數是可控制的，而所設計之實驗仍能滿足可重複性的要求。如此，針對不同裝置，實驗者便可瞭解不同裝置在相同實驗環境下的行為表現，並據以提出實驗分析報告與改善建議。

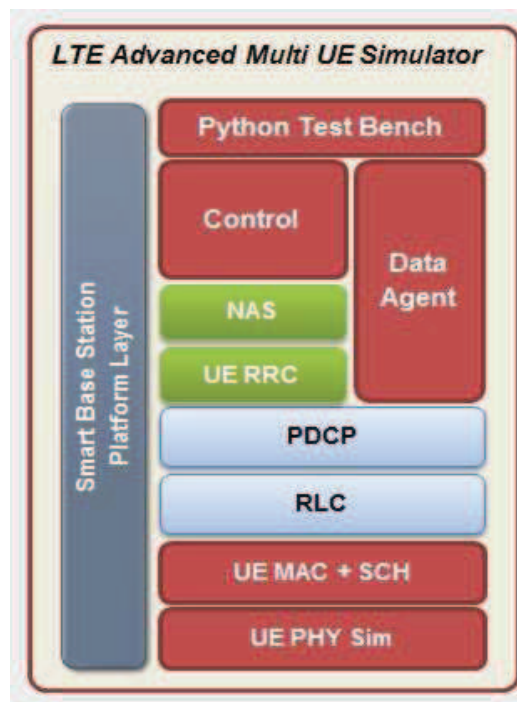


圖 6-13 大量用戶端裝置之信令堆疊關係圖

資料來源：sooktha.com

以換手機制為例，當 UE 移動時，所接收到的訊號強度會受到地形環境的影響，為了維持網路的連線品質，當訊號強度衰弱時，用戶端設備會選擇一個訊號較強的基地台，進行換手的動作。在行動寬頻通訊網路中換手決策是由 UE 所決定的，換手過程可分成決策、準備、執行及結束等四個階段，決策階段透過各種資訊與需求，決定是否須要啟動換手機制；準備階段會針對將被啟動換手機制的 UE，在目標 Cell 準備好該 UE 所需的相關配置；執行階段會下達換手命令讓 UE 更換到目標 Cell 之下，結束階段會在 UE 切換到目標 Cell 後執行，目的是讓 LTE 核心網路的管理機制因應此次換手做相對應的變更。

由於行動寬頻通訊網路中的使用者裝置在連線狀態下，從原先的 Cell 轉移到相鄰的 Cell 的換手機制，LTE 做為一套支援行動式 UE 的無線通訊協定系統，為了以維持良好的連線品質，對於換手機制也有一套相關的機制與規範。以確保 S-GW 及 P-GW 這些通往資料網路的閘道，會把屬於 UE 的網路資料傳向服務該 UE 的基地台，因此 MME 會負責控管 UE 的資料傳送路徑，以確保網路資料會轉向透過適當的 S-GW 及 P-GW 送往該 UE 所屬的基地台。

測試平臺另一個主要的考量通常是為了安全性的理由³⁴⁹，攻擊者可能藉由換手 (Handover) 的執行程序中，偽裝基地台對換手之間的訊息傳遞進行竊取、竄改資料，藉此得到相關的機密資訊。LTE 架構是一個平坦 (Flat) 的架構，容易受到攻擊，藉由全 IP 網路亦提供了直接的路徑對基地台進行惡意攻擊，當攻擊者破解基地台，可進一步危害整個 LTE 網路通訊系統。因此在換手的過程會一併更換無線通訊中使用的安全性金鑰，以避免在安全性金鑰被長期使用之後，攻擊者利用金鑰未更換這點攻擊網路，因此通常會配合換手動作且變換金鑰的特性，達成基地台金鑰變換的目的，相關流程如圖 6-14 所示。本團隊為了能使平臺精確的掌握與控制換手的時機，以及研析換手過程可能衍生的問題，也將能模擬大量用戶的用戶端模擬器納入平臺框架內，期能使測試結果更客觀且具有公信力。

³⁴⁹ Chan-Kyu Han and Hyoung-Kee Choi, "Security Analysis of Handover Key Management in 4G LTE/SAE Networks", IEEE Transactions on Mobile Computing, 2014.

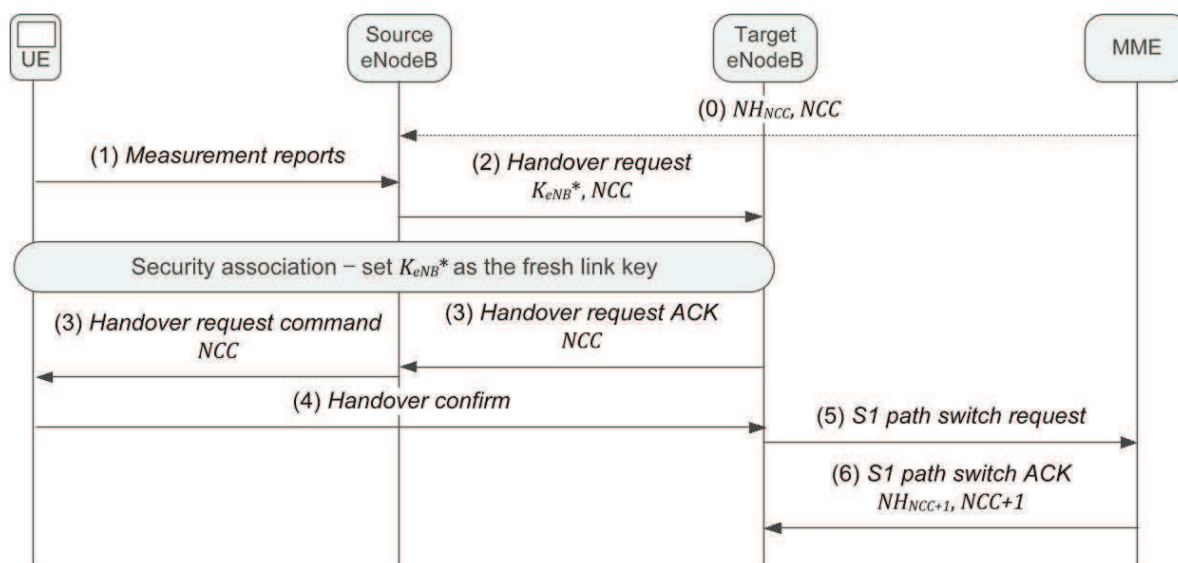


圖 6-14 換手(Handover)程序的金鑰交換流程

資料來源：IEEE Transactions on Mobile Computing, 2014

三、 核心網路單元(Evolved Packet Core，簡稱 EPC)

長程演進計畫是由第三代合作夥伴計畫(3GPP)所推出的下一代無線通訊技術，目的在於提供使用者更為高速、便利的無線服務。和過去的電信技術如全球行動通訊系統(GSM)、通用行動電信系統(UMTS)比較起來，除了調變技術外，另一個差異是核心網路的架構改變。過去的架構為了同時支援電路交換服務如電話、簡訊等，以及數據分封交換服務如上網瀏覽、資料下載等，所以後端網路往往存在兩套獨立的線路系統。相較於傳統 3G 網路系統，EPC 的網路架構相對地扁平化。

主要的組成元件如圖 6-15 虛線標示框線內所示，包含行動管理裝置(Mobility Management Entity，簡稱 MME)、服務閘道器(Serving Gateway，簡稱 S-GW)、數據封包網路閘道器(Packet Data Network Gateway，簡稱 PDN GW)、計費規則功能實體(Policy and Charging Rules Function，簡稱 PCRF)及家庭用戶伺服器(Home Subscriber Server，簡稱 HSS)，元件間緊密地合作達成用戶端行動性、政策管理和安全性等功能，為用戶端提供一個穩定的 IP 連結通道，連結網際網路。其中包括控制面(Control Plane)和用戶封包面(User Plane)，並且主要由 MME 擔負起核心網路控制的指揮者，協調閘道器以及 HSS，以進行用戶的管理包括管理手機用戶的登入連線(Attach)、離線(Detach)、安全性相關的認證、授權，計費等功能；並適時地建立、修改或拆除用來傳送用戶數

據封包的承載(EPS Bearer)；以及管控手機用戶端的行動漫遊，包含基地台 eNode-B 之間換手服務(Handover)，或者處於閒置模式(Idle Mode)時，用戶位置的追蹤、呼叫等功能。

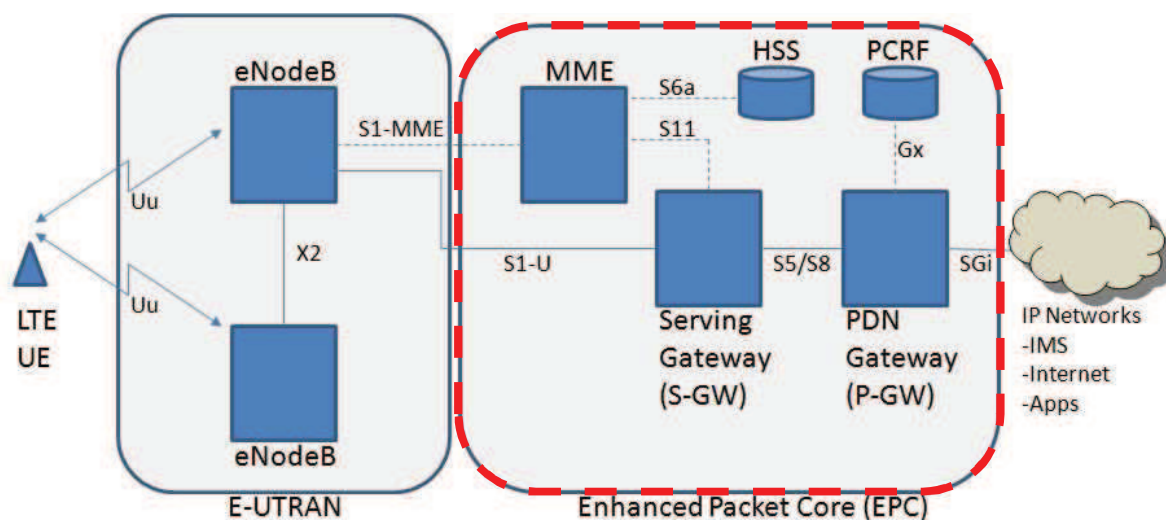


圖 6-15 核心網架構與基礎元件示意圖

資料來源：SECforce³⁵⁰

從標準制定的技術發展藍圖可以看出，在 4G 的建構環境下，電路交換網路已被網路語音通訊協定(VoIP)所取代。早先在 GPRS 標準制定的年代觀之，為了在 IP 網路上提供傳統的電信服務，甚至更進一步支援更多元化的多媒體服務，這些制定標準的專家就從圖 6-15 架構加以衍生後，提出一個宏大的系統--IP 多媒體子系統(IP Multimedia Subsystem，簡稱 IMS)如圖 6-16 虛線框線所示。

³⁵⁰ Thanos Polychronis, "4G LTE: Architecture and Security Concerns", 2014/05/06.

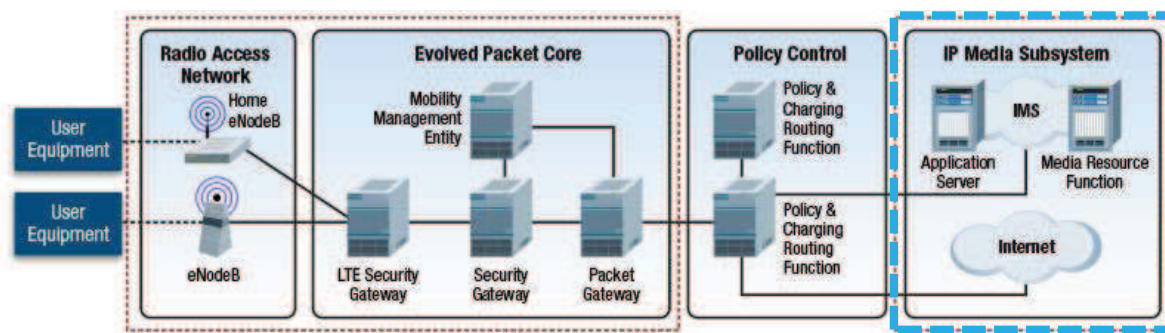


圖 6-16 核心網架構與基礎元件並內納入 IP 多媒體子系統之示意圖

資料來源：COTS Journal³⁵¹

IMS 的通訊協定完全沿用自 2002 年代，即已經在 Internet 上被廣泛採用的 VoIP 標準——會談啟始協定(Session Initiation Protocol，簡稱 SIP)，以此作為網路協定的基礎，配合上其他網際網路工程工作小組(Internet Engineering Task Force，簡稱 IETF)所制定的協議標準，再加上電信業者所重視的計費、認證相關模型，構成一套完整的解決方案，不但支援電話服務、簡訊服務，甚至網路視訊會議也都能完整支援。因此本質上 SIP 是一系列 IP 通訊協定族的組合，主要包括扮演溝通呼叫控制信令的 SIP、媒體能力協商的 SDP (Session Description Protocol)、以及進行即時媒體傳輸的 RTP (Real-time Transport Protocol)與擔任媒體傳輸控制任務的 RTCP (RTP Control Protocol)等等。由於很早就開始發展，所以 IMS 其實在 3G 時代就已經大致發展完備，只是當年的時空背景下，業者仍保留大量 2G 時代的電信交換基礎設施，是故 3G 標準制定語音服務有 PS/CS 兩套管道可以供業者自由選擇，故大多數業者遷就成本考量，採用分封交換的 VoLTE 方案的普及化時程，也就往後一直順延到今天才逐步浮上檯面。

因此現今標準³⁵²的制訂也順勢而為的將基於 LTE 的語音方案（Voice over Long-Term Evolution，簡稱 VoLTE）納入 IMS 相關服務之中，把語音服務（控制和媒體層面）當成資料封包的串流，在 LTE 數據承載網路中傳輸，這意味著不再必須維護和依賴傳統的電路交換語音網路，也能更有效地利用頻寬³⁵³。VoLTE 完整服務架構請參考

³⁵¹ COTS Journal, "LTE Networking Aids Battlespace Visualization Systems", 2013/12.

³⁵² GSMA, "GSM Association Official Document IR.92 - IMS Profile for Voice and SMS", 2013/3/3.

³⁵³ 新通訊, "汰換老舊電信語音服務 VoLTE 跨網互通技術有譜", 2016/10.

圖 6-17 所示。

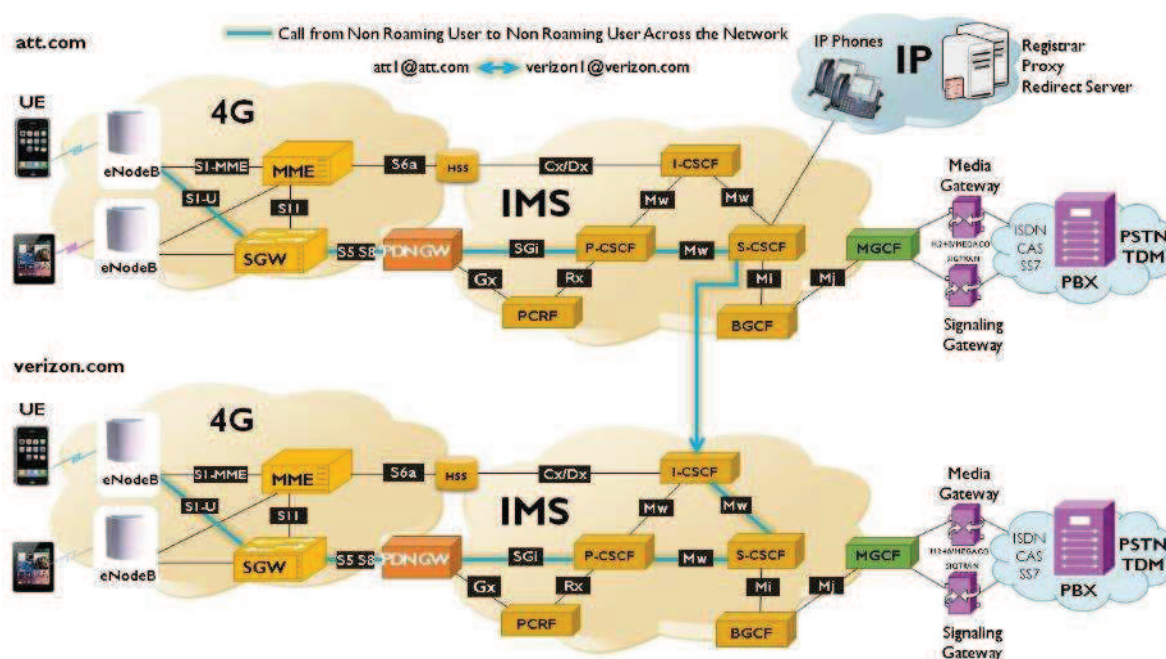


圖 6-17 核心網路與 VoLTE 結合的完整服務架構

資料來源：gl.com

在 VoLTE 系統架構中，則分別由 E-UTRAN 無線接取網路提供無線基礎接取服務，EPC 核心網路系統提供 IP 基礎接取服務，IMS 系統提供 IP 應用服務控制，實現諸如語音、視訊等多媒體業務。透過 VoLTE 的最佳化技術使的封包標頭比單純使用 VoIP/LTE (如圖 6-18 虛線框線內所示) 更小，且 VoLTE 的語音和數據容量更為原來 3G UMTS 的三倍以上，或為 2G GSM 的六倍以上。雖說目前 VoLTE 與市面上 LINE、WeChat、Skype 等通訊軟體可以提供的服務差異不大，都一樣是透過網路傳遞語音，也能進行視訊電話，但這兩者主要的分別在於，VoLTE 是直接透過電信業者的 VoLTE 網路直接撥接電話；而通訊軟體要透過通訊軟體業者主機經過多次串接與選徑以連接另一個帳號，因此訊號的傳遞就不像 VoLTE 那樣直接，而通訊品質上也有著相當程度的差異。

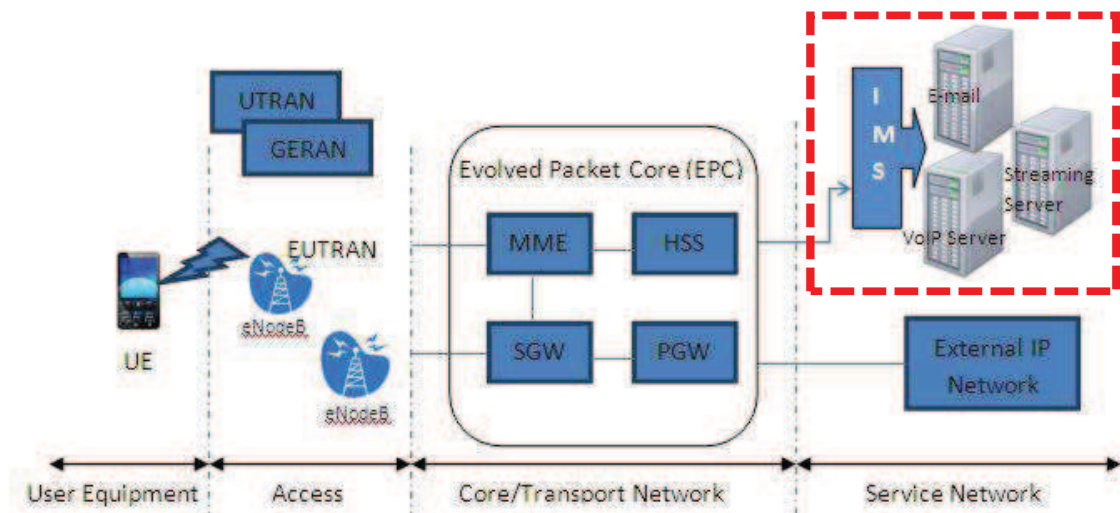


圖 6- 18 IP 多媒體子系統使用 VoIP/LTE 之示意圖

資料來源：Journal of Cyber Security and Information Systems³⁵⁴

考量上述各種及未來新技術的衍生，使得基站可能遭遇不同類型的核心網路及提供不同的服務而日趨複雜，因此本著前瞻與創新研究的理念，建構出可於三種施測基本組套衍生並支援透過多種不同核心網路架構之檢測平臺，如圖 6-19 所示，三種基本組套分別為

- 1.基於信令應答之核心網路模擬器(EPC Emulator)；
- 2.基於實際硬體設備之核心網路(Real EPC)及
- 3.基於網路功能虛擬化之核心網路(NFV)。

待測基站無論從廠商自主檢測或第三方公正實驗室的評估，期能得到最公正與客觀的檢測結果並能交互比對。接著將針對此三種架構之內容，分別加以說明。

³⁵⁴ Daksha Bhasker, "4G LTE Security for Mobile Network Operators", Journal of Cyber Security and Information Systems, 2013/9/10.

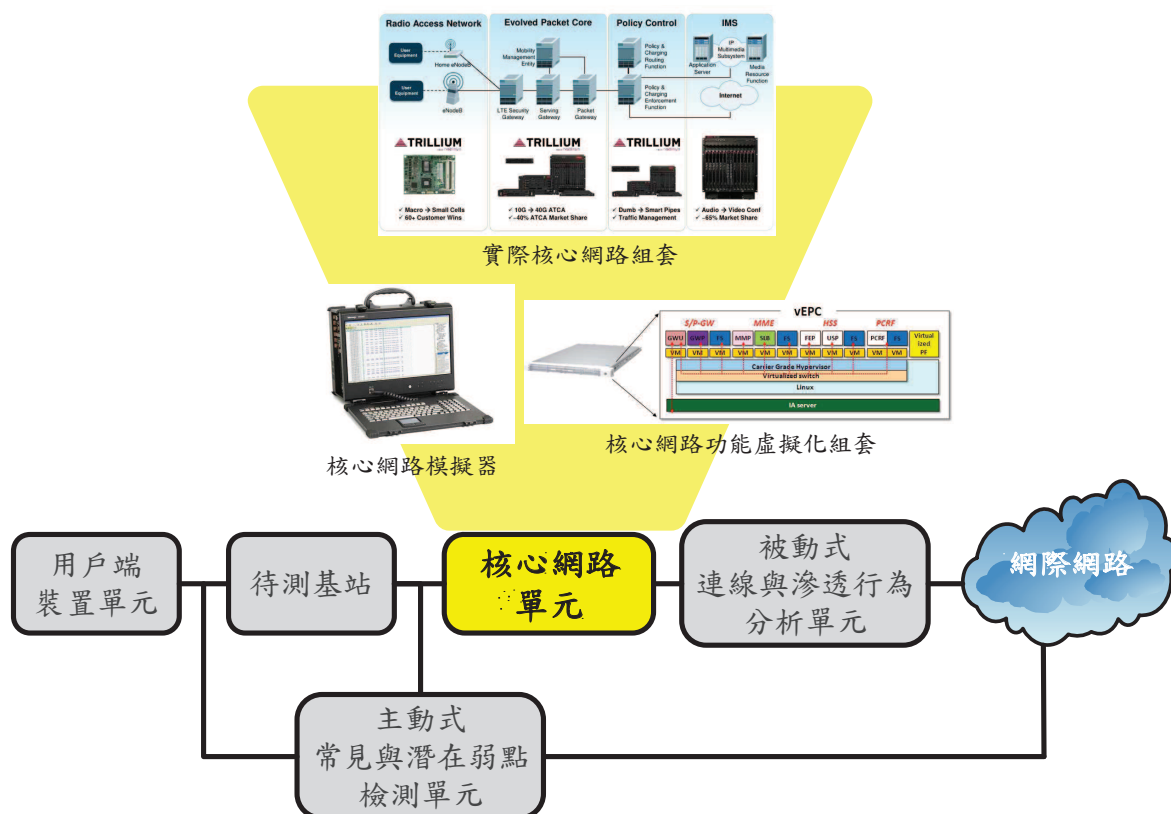


圖 6-19 基站資安檢測平臺-可應用之基本核心網路組套類別圖說

資料來源：本團隊整理

(一) 基於信令應答之核心網路模擬器(EPC Emulator)

一般而言，核心網路模擬器是用於基地台產線生產測試和產品品質控管、維修驗證等目的所研發信令測試儀器。在快速有效、節省成本的前提下，量測 LTE 必要測試項目，包括網路連線、資料傳輸速率、最大傳輸功率、接收靈敏度等，涵蓋待測物(DUT)功能等主要項目。近來多數的核心網路模擬器已內建參數設定編輯器(Configuration Editor)與測試項目編輯器(Test Plan Editor)，方便使用者簡易編輯，讓使用者可以彈性的撰寫、編輯測試項目判別合格/不合格的測試條件，更靈活的檢測測試項目是否達到標準。測試參數設定檔與數據結果也可即時顯示並且可以儲存在紀錄檔以作為後續的分析之用，經本團隊於第一期專案的評估驗證後，證實模擬器有別於實際或 NFV 構成之核心網路，其高度彈性的能力有助於模擬核心網路遭駭客入侵時的異常行為分析。此外多數模擬器均配備完整 LTE 網路環境，如圖 6-20 所示，在單機中整合了基地台(eNodeB)、移動管理實體(MME)、服務閘道(Serving Gateway, S-GW)及數據封包

網路閘道器(PDN Gateway)，除效能考量外，使其可輕鬆模擬商業化的 LTE 網路。實驗室則可採用信令模式測試，對基地台可能的弱點進一步測試，並且觀察基地台受攻擊後的反應，有利於為基礎建設的安全做把關。

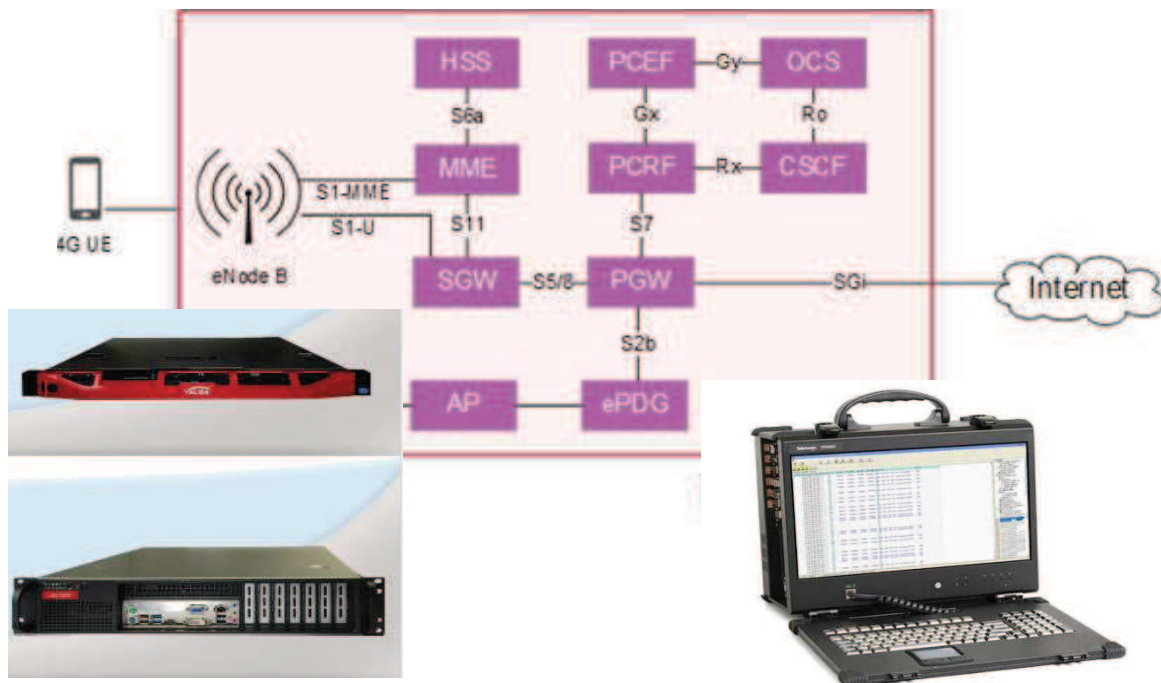


圖 6- 20 LTE 核心網路模擬器架構圖

資料來源：valid8.com

透過模擬器支援 LTE 基站之測試，可模擬 S1 及 X2 介面與基站界接，以進行控制面(Control plane)及用戶面(User plane)測試。除了基本的於功能性測試(functional)及附載測試(load testing)外，也可藉由實驗室針對基站可能存在的已知弱點，撰寫專屬檢測信令流程並依測試需求發送，驗證在待測基站的各相關介面與通訊協定傳送情況，以達成相關的弱點驗證需求，此一優點是為求營運效能與標準符合性的實際核心網路或網路功能虛擬化系統所難以比擬的。

(二) 基於實際硬體設備之核心網路(Real EPC)

以目前多數電信業者的電信基礎設施來看，核心網路架構仍是基於實際硬體設備，LTE 的核心網路架構是基於 IP 網路協定的 EPC，其最大的目的是傳遞行動網路 IP 的資料封包外，並能建置不同的存取網路，來提供更多各式的服務。其中至少包含了下

列基本元件與功能：

1. 行動管理實體 (MME：Mobility Management)

負責核心網路的控制功能。行動管理實體(MME)概念上由 SGSN 的控制平面組成。控制平面終止的協議在行動管理實體(MME)終結，行動管理實體(MME)管理終端的移動，只要用戶端裝置仍在行動管理實體(MME)的共享池(Pool)範圍內移動，相同的行動管理實體(MME)就會維持對用戶端的控制。其執行的移動管理和會話管理功能如下：

- (1) 手機連線(Attach)和離線(Detach)處理，允許手機在網路上註冊和解除註冊。
- (2) 安全的 3A 機制，行動管理實體(MME)實施認證，授權和審計 (Authentication, Authority, Accounting)的安全功能，分別用來識別用戶身分，許可網路的連線和追蹤用戶的行為。
- (3) 管理演進的數據封包系統承載(Bearer)，行動管理實體(MME)管理演進的數據封包系統承載(Bearer)的建立，改變和拆除。
- (4) 對閒置模式(Idle Mode)手機的移動管理，行動管理實體(MME)管理閒置模式 (Idle Mode)手機的移動，追蹤其位置。

2. 數據封包網路閘道器(PDN GW)

數據封包網路閘道器(PDN GW)與服務閘道器(Serving GW)功能非常近似 3G 系統的 GGSN 節點。主要的強化是增加了數據封包的緩衝(Buffering)，來支援演進系統的尋呼與和非 3GPP 的互聯。數據封包網路閘道器(PDN GW)提供與外部世界連接的介面，數據封包網路閘道器 (PDN GW)/服務閘道器 (Serving GW) 可以被視為用戶平面的一個節點，而且也會被用於執行部分與服務品質 (QoS) 相關的指令。參與的控制平面功能如下：

- (1) 管理演進數據封包系統承載(Bearer)，數據封包網路閘道器(PDN GW)/服務閘道器(Serving GW)基於策略控制功能(Policy Control Function)的請求，觸發承載 (Bearer)的建立。
- (2) 作為 IP 移動錨點的呈現點。數據封包網路閘道器(PDN GW)作為移動錨

點，對固接網路部分隱藏了用戶移動。當手機連線到網路，從數據封包網路閘道器 (PDN GW)分發 1 個 IP 位址，並且假設該閘道器為手機的移動錨點。之後不論著手機的切換轉移到哪個行動管理實體(MME)或服務閘道器 (Serving GW)，則手機的 IP 呈現均會維持在原有的數據封包網路閘道器(PDN GW)上。

3. 數據網/服務閘道器 (Serving GW)

主要提供以下用戶平面功能。

- (1) 服務品質(QoS：Quality of Service)的策略控制與執行(Policy Control and Enforcement)，為了簡化應用(Application)對承載(Bearer)的請求，增加電信業者對網路資源的控制，以有效限制用戶的濫用可能性。演進的數據封包系統的服務品質(QoS：Quality of Service)是透過網路進行控制。該項功能協助控制流量，採用合適的服務品質(QoS：Quality of Service)級別，執行限速來防止用戶超出其約定的流量。下行的流量控制由數據封包網路閘道器 (PDN GW)/服務閘道器(Serving GW)實施，上行的流量則由演進基站(eNode-B) 控制。
- (2) 計費功能則負責為用戶的流量使用收費，並採用相關業務指定的費率計費。
- (3) 合法的監聽，為在法律許可的範圍內，由授權的官方司法機構實施。

4. 家庭用戶服務(Home Subscribe Server，簡稱 HSS)

HSS 是一個中央資料庫，儲存了包含與用戶相關的訊息和訂閱相關的訊息。主要功能包括了:移動性管理、呼叫和會話建立的支援、用戶認證和存取授權機制。

5. 計費策略規範功能(Policy Charging Rule Function，簡稱 PCRF)

是業務數據流和 IP 承載資源的策略與計費控制策略決策點，它為 PCEF(策略與計費執行功能單元)選擇及提供可用的策略和計費控制決策。業者在導入 PCRF 後，在網路中就可實施 QoS 保障技術，這樣電信業者也就可以在網路中提供用戶差別服務和業務的差異化服務。電信業者也可以輔以 GGSN 與 PCRF 的互控，實現對用戶的每個

業務頻寬進行限制，這樣可以防止網路中的資源濫用，其中一個典型情形是特定套用可能會消耗大量的可用網路資源。提供用戶在網路中使用不同策略組套(例如:常見的資費方案差異)，電信業者才能基於 PCRF 對每個用戶的網路流量或每個用戶所使用的組套，限制用戶的話務與網路之使用。因此電信業者所使用的整個策略與計費控制 (Policy and Charging Control，簡稱 PCC)架構(如圖 6-21 所示)就是以 PCRF 為核心所建立的，以下為相關功能元件之說明。

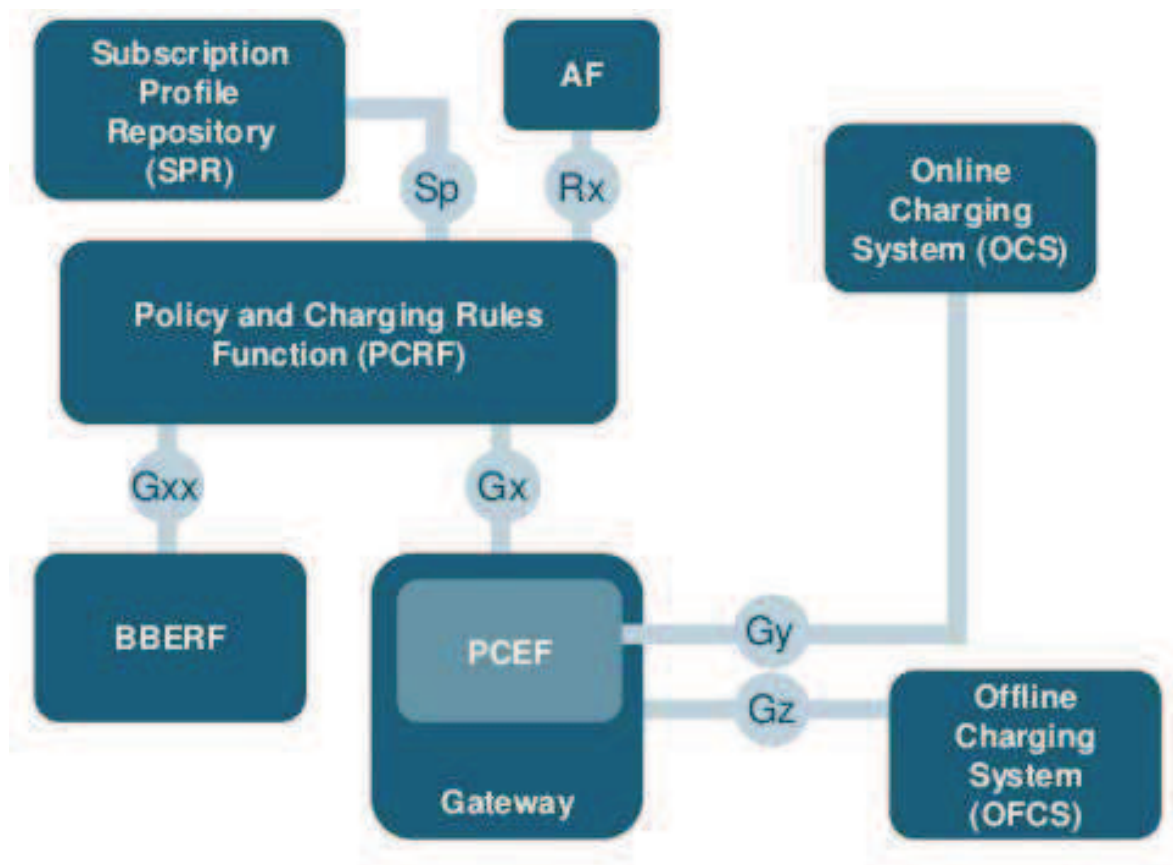


圖 6-21 策略與計費控制架構

資料來源：Radisys Corporation³⁵⁵

- (1) PCEF (Policy and Charging Enforcement Function) 策略和計費執行功能，主要包含業務數據流的檢測、策略執行和基於流的計費功能。該功能實體位於開道，例如 GPRS 的 GGSN 開道、EPC 的 P-GW、WLAN 中

³⁵⁵ Radisys, "Core Network Optimization: The Control Plane, Data Plane & Beyond", 2012/11/01.

是 PDG，也可獨立部署。

- (2) AF (Application Function) 套用功能，該功能實體是提供套用業務單元，主要對 IP 連線接入網 (IP-CAN) 用戶面行為進行動態策略/計費控制。這些業務需要動態策略和計費控制。AF 通過 Rx 參考點，傳送 PCRF 需要的動態會話訊息，接收 IP-CAN 的特定訊息和 IP-CAN 承載層事件的確認。
- (3) OCS (Online Charging System) 線上計費系統，該功能提供基於用戶和業務數據流的信用控制功能。主要由線上採集、計費控制、批價、餘額管理等模組構成，實現了線上計費功能，並配合其它計費網元設備（觸發基於會話、事件的線上計費事件請求設備，如 SCP、CCG、ISMP 等）進行實時話務控制。
- (4) OFCS (Offline Charging System) 離線計費系統，該功能提供基於用戶和業務數據流的計費功能。主要功能包括客服、業務管理、計費、結算、帳務處理、系統管理等。是一個針對話單和帳戶的後付費處理系統。
- (5) SPR (Subscription Profile Repository) 用戶屬性儲存器，用戶屬性儲存邏輯實體包含有與所有簽約用戶或簽約相關的訊息，SPR 提供的簽約訊息包括（每一個 PDN 的）：簽約用戶允許的業務；每個允許業務的優先權（可選）；簽約用戶允許的 QoS 訊息；簽約用戶業務的計費相關訊息，如接入類型、位置訊息和使用次數；簽約用戶的類型等。SPR 可能與電信業者網路中分布的多個資料庫關聯。SPR 與 PCRF 通過 Sp 參考點進行互動。
- (6) BBERF (Bearing Binding and Event Report Function) 承載綁定及事件報告功能，它是承載綁定、上行承載綁定校驗及當 Gxx 存在時向 PCRF（策略與計費規則功能）進行事件報告的策略執行點。該功能實體位於閘道器中，如基於 S5/S8 界面，使用 PMIP(代理移動 IP)實現 3GPP 接入的 S-GW(服務閘道)，HRPD(高速分組數據)中的 HSGW(HRPD 服務閘道)，非 3G 接入場合下的 A-GW(接入閘道)。
- (7) TDF (Traffic Detection Function) 流量檢測功能是執行應用程式檢測和報告檢測到應用程式和其服務數據流量描述向給 PCRF.如果 TDF 檢測不出這些訊息則由 TDF 執行存取控制、資料流的重新導向以及進行頻寬限

制。如果能檢測到應用程式相關訊息,則會提交 PCRF 產生決策交由 PCEF 執行控制。

以上為電信業者的核心網路設備可能會具備的基本元件概述,雖然電信業者可能會依據實際業務狀況增加(例如: VoLTE, 又稱為「IMS Profile for Voice and SMS」, 利用 LTE 的網路的封包機換來產生語音通話, 以提供包括語音、即時視訊、文字、檔案交換、影音串流等整合式多媒體通訊服務, 可應用於固網、行動網路、或是兩者匯流的網路, 將帶來更清晰的語音和視頻通話質量、更快的呼叫接續速度。) 或減少部分元件, 參考圖 6-22 所描述之各實體元件彼此堆疊界接關係。另一方面從整體行動通訊網路運作的觀點來看, 基本上透過整合服務閘道(S-GW)、移動管理實體(MME)、封包資料網路閘道(PDN GW)三個功能元件, 再加上由 UE 與 eNodeB(eNB)組成的 E-UTRAN 無線存取網路最重要的四個功能元件, 即可構成最基本的 LTE 網路架構。

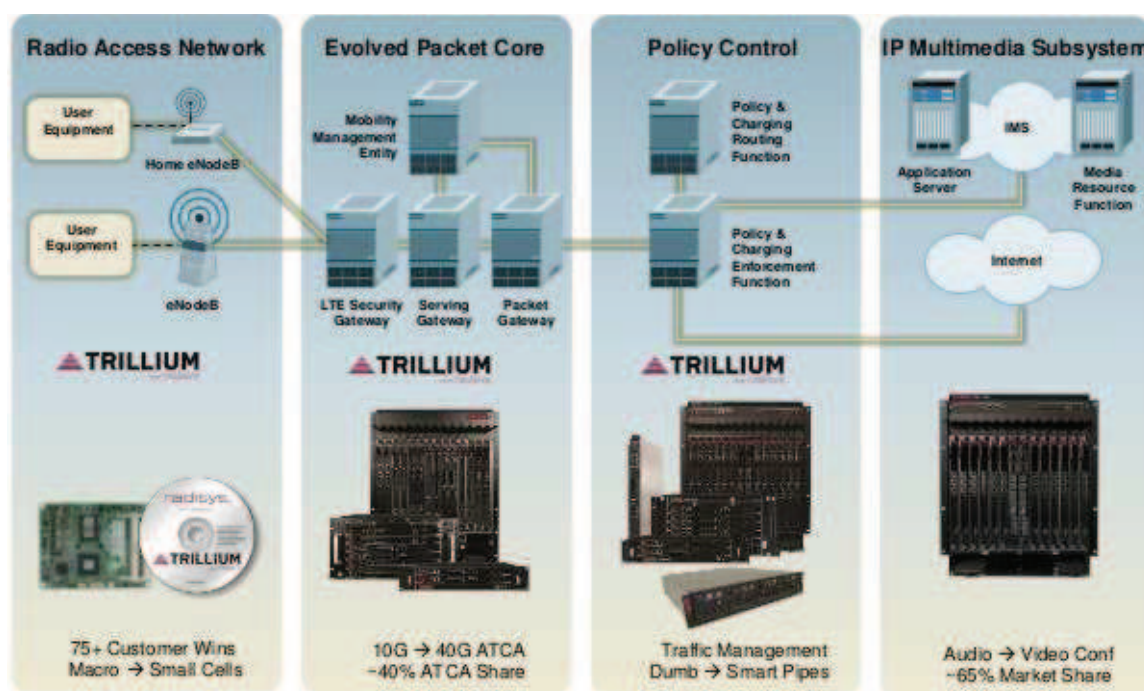


圖 6-22 實體核心網路設備、元件與架構對應示意圖

資料來源：Radisys Corporation³⁵⁵

為使本平臺可提供近似於實際營運的檢測環境, 本檢測框架展現除了可透過核心網路模擬器進行模擬與檢測外, 亦可透過結合實際設備所構築的核心網路進行檢測, 雖基於商業考量, 無法透過業者的實際核心網路連線, 但仍可透過工業技術研究院的

4G⁺網路接取與應用測試實驗室這類場域(如圖 6-23 所示)所提供實際核心網路環境進行，以避免因過度專注於實驗環境下的檢測，卻忽略了真實環境所可能遭遇的問題，進而提升整體檢測品質與測驗報告的公信力。

圖 6-23 4G⁺網路接取與應用測試實驗室

(三) 基於網路功能虛擬化之核心網路(NFV)

從產業發展趨勢觀之，3GPP 標準制定進程已經步入真正意義的 4G LTE-A (Release 13/14)世代，而雲端虛擬化技術在 IT 業的日益成熟及成功又驅使行動網路採用新的實現方式及新的商業模式，同時前十年迅速發展的諸多 IT 新技術也啟發了對

行動網路架構及業務部署的重新思考。

面對 2020 年以後人類間甚至萬物間資訊聯網社會的無線行動通訊需求，第五代行動通訊(5G)被業界視為一項寄以厚望地革命性技術，在無線接取技術面上的革新理所當然，但是在核心網路上的面向上，會不會有稱之為革命性的改進呢？5G 行動通訊系統將是一個全方位服務多技術融合的網路，通過 ICT 技術的演進和創新，來滿足未來包含廣泛資料和連接的各種業務的快速發展需要，最終滿足以用戶端為中心的無線聯網需求，其中一個重要關鍵就在於軟體定義網路(Software-Defined Networking, SDN)以及搭配網路功能虛擬化(Network-Function Virtualization, NFV)兩項技術的發展。SDN 和 NFV 之間有著一些關鍵差異性，不過二者卻有四個易造成混淆的共通點。首先，二者都是起源於用戶需要更大彈性與互通性，而不是為了尋求某種特別的技術。其次是時間點，也就是這兩種概念幾乎是在同一時期問世。第三是並存，它們可以，而且實際上也被放在一起使用。最後 NFV 和 SDN 也都會搭配一些其他的新技术使用。

軟體定義網路(SDN)架構概念是由 Stanford 大學 Nick McKeown 教授於 2009 年 IEEE INFOCOM 研討會中首度發表，當時還只是學術界探討的一項新式網路架構，以及僅少數新創公司投入相關研發。在 2012 年 7 月，Nick McKeown 教授與 Scott Shenker 教授等人所創辦的 SDN 先驅廠商 Nicira 發展的網路虛擬化技術，被 AT&T、NTT、Google 等大廠所採用，並被 VMware 以 12.6 億美金併購。同年，網路服務巨擘 Google 宣布用來串連其全球 12 個 IDC (Internet Data Center) 的 G-Scale 網路全面採用 SDN 網路架構，讓原本只有 30~ 40% 的網路頻寬使用效率提升 3 倍，達到 95% 的網路使用效率，因而讓 SDN 引起強烈的關注。其後更引發了一波傳統網路設備大廠併購 SDN 新創廠商以快速卡位 SDN 市場的風潮。同時，除了 Google 之外，數家國際大廠也開始進行 SDN 解決方案的研發或 Field Trail，例如 NTT、AT&T、中國電信、中國移動與中華電信等等電信業者，以及 Facebook、Yahoo、微軟等等大型網路服務廠。

其概念是讓軟體來控制網路，充分開放網路能力，是一種具有控制信令與用戶數據分離(C-U Split)、網路功能集中控制、開放應用程式界面 API 這三大特徵的新型網路架構和網路技術。通過引進 SDN 的概念，可以將封閉垂直一體的傳統電信網路架構一舉轉為彈性化、開放、高度整合、服務導向及確保服務水準的分層架構。在引入 SDN 後，面臨的新挑戰是如何進行網路功能重構，如何設計新增介面協定，進而基於 SDN 實現架構的優化以及端到端信令流程的優化。另一方面，大量的複雜控制機制集

中到 SDN 控制器上運行，也降低了 SDN 交換器的採購、管理與替換等成本，連帶解決了被單一網通設備製造商綁定的問題。

與 SDN 部分概念相仿，網路功能虛擬化(NFV)的理念之一也是在於解除特定軟硬體功能元件，被市場支配性廠商綁定的問題；其採用雲端虛擬化為主的 IT 手段改造 4G/5G 核心網路，採用泛用型伺服平臺(General Purpose Platform, GPP)構建電信基礎環境，如圖 6-24 黑色框線內所示，GPP 設備市場規模遠大於專用電信設備，單位計算性能價格比遠低於電信設備，並且成本下降和更新週期的幅度數倍於電信設備，這樣能夠以更低成本更快地引進新 IT 技術和新 IT 設備，維持硬體設備性能優於競爭對手。

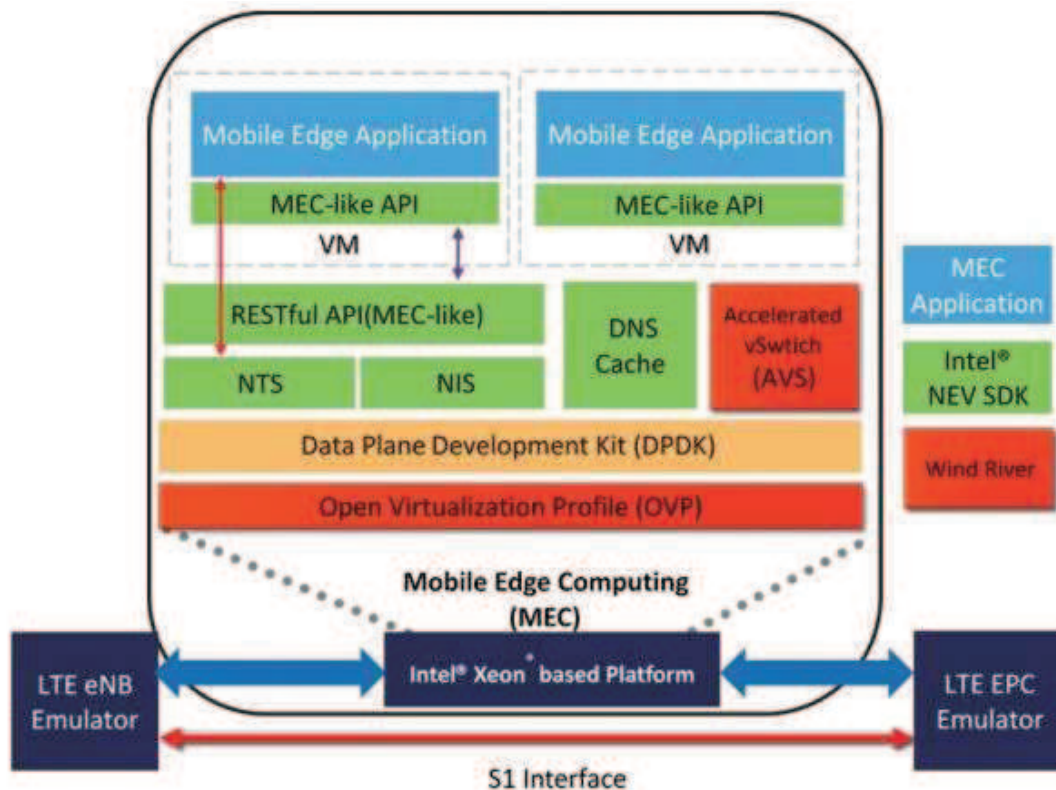


圖 6-24 以 Intel 通用型伺服器平臺構建之電信基礎環境

資料來源：微閱號³⁵⁶

目前 NFV 標準及推動主要由 ETSI(European Telecommunication Standards Institute)轄下一個專責 ISG(Industry Specification Group)的組織負責推動，其主要目標在提供 4G/5G 核心網路彈性與資源的有效利用。ETSI ISG NFV 在 2012 年底由十三個全球具指標性電信業者所發起，包含 AT&T、BT、CenturyLink、China Mobile、Colt、DT、KDDI、NTT、Orange、Telecom Italia、Telefonica、Telstra、Verizon 等所共同主導。未來核心網路將毋須再使用昂貴且複雜的專屬軟硬體設備，只要採用一般通用目的伺服器(通常是 x86 Server)和 IP 路由器、乙太網路交換器即可組成，使得核心網路部署更進一步降低成本，也減少了對單一解決方案提供商的依靠或被捆綁。也因此，產業界

³⁵⁶ 微閱號, 挺進 5G 時代, 怎能不瞭解 MEC?, 2017/4/15.

公認無線接取網路每一代幾乎都是一場革命(Revolution)，而核心網路技術被認定是不斷的演進(Evaluation)。

透過 NFV，既有專用 4G 核心網路的相關網路設備的功能以軟體的方式虛擬化，如圖 6-25 所示。經由雲端運算(Cloud Computing)相關技術，硬體資源虛擬化為多個 VM(Virtual Machine)，利用雲端計算的快速部署能力，使得各個 EPC 軟體網路元件(Network Entity)容量配置調整週期從數周縮短到數分鐘，大幅提升 EPC 網路元件部署和更新的敏捷性，並實現設備容量按需求(On Demand)動態彈性擴充，確保系統的可維護性，負載平衡機制提升系統服務水準，每個 VM 可以遷移和重生，在本地或異地相互熱備援，進一步確保網路的高可靠性。

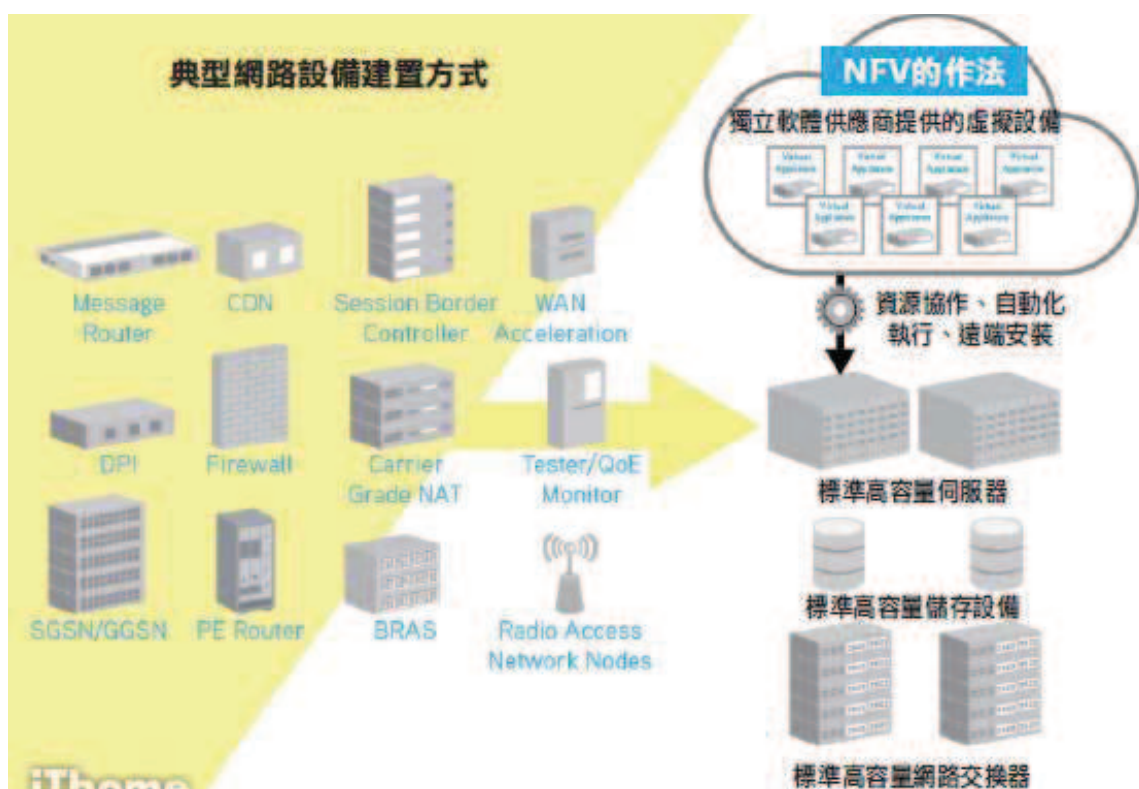


圖 6-25 傳統核心網路設備與 NFV 架構的比較

資料來源：iThome³⁵⁷

為此 ETSI 提出的 NFV-MANO(NFV Management and Orchestration)架構³⁵⁸參考圖

³⁵⁷ iThome, 資料中心網路環境面臨重大變革：SDN 與 NFV 崛起，軟體將主宰網路, 2012/11/14.

³⁵⁸ ETSI, "Network Functions Virtualisation (NFV); Management and Orchestration", GS NFV-MAN 001 641

6-26 所示，這個開放架構將傳統的核心網路建構成為分層模組化設計，階層之間的通訊和介面採用產業標準協定，以確保模組間的互通性，這個平臺的開放和模組化本質，促成了互通性和更大的客戶選擇性，允許客戶針對特定的 vEPC 需求，選擇搭配適當的解決方案。

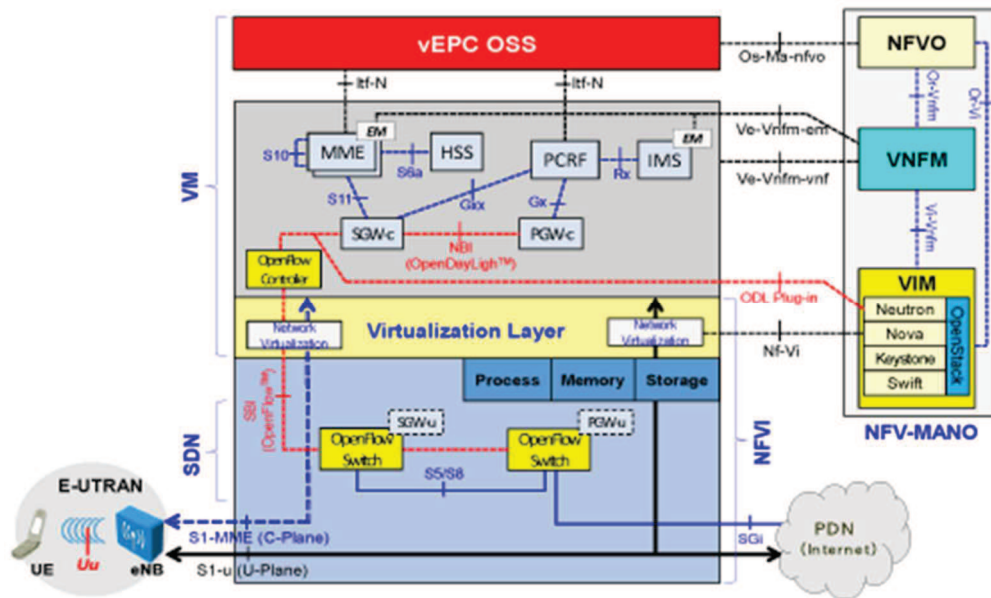


圖 6- 26 ETSI 提出之新式 vEPC 概念框架

資料來源：新通訊 2016 年 3 月號 181 期³⁵⁹

由於 NFV 與 SDN 技術雙方的核心概念頗有相通之處，兩者具備互補整合之高度條件，因此目前 4G 核心網路實現虛擬化的工作中，多將 NFV 與 SDN 相提並論，兩者間未來可能的發展出的協同運作模式亦值得探討。SDN 負責 Layer-4 以下的網路基礎設施暨低層網路流量轉送的處理；而 NFV 則專責 Layer-4 以上的網路上層應用服務設施彈性靈活的資源調度，兩者相輔相成，營造出未來高效優化的電信業者整合服務平臺。

基於前述的各種優勢，說明了而 SDN/NFV 一旦崛起，勢必將對既有電信網路不論技術或佈局產生衝擊。而目前核心網路上最重要的功能除了 EPC 之外就是 IMS，其虛擬化方案分別被稱為 vEPC 及 vIMS，由於 IMS 功能相對單純的多，亦常常也將其

V1.1.1, 2014/12.

³⁵⁹ 新通訊, "當 SDN 遇上 NFV 虛擬化 5G 核心網路掀革", 2016/03.

視為 vEPC 的一部分看待。也因此 vEPC 為近年已成為網路通訊產業的熱門議題，有多家全球性大型電信業者看好其發展潛力，已經共同成立 NFV 標準及推動組織，其主要目標在提供 4G/5G 核心網路彈性與資源的有效利用。目前新加坡電信公司 M1³⁶⁰ 已經與華為公司合作，並於 2017 年完成 vEPC 的佈署，使該公司的核心網路更具彈性且能有效利用資源。而日本 NTT DOCOMO 也早在 2016 年攜手 Ericsson 共同建置並開始營運³⁶¹。工業技術研究院也在其 4G⁺試驗場域與提供了兩組 vEPC 的實驗環境，期能為互通性測試提供完整的試驗環境。由此可見 vEPC 的導入已儼然成為主流趨勢。

雖然 vEPC 還在持續演進中，目前還沒有專家敢斷言它未來會呈現何種樣貌，可以確定的是它被公認將在 2020 年前掀起下一波電信網路產業新革命。因此，本檢測平臺架構也本著前瞻的思維，及時俱進的技術能量，將網路功能虛擬化之機制納入檢測架構中，期能使原本基站已完備的檢測技術能量，在平臺的輔助下更能有效發揮。

四、 主動式常見與潛在弱點檢測單元

由於 4G/LTE 的技術變遷，發展出完全以 IP 為基礎的全新介面與協定，電信營運商升級 4G/LTE 行動架構，為無線用戶提供更快速、覆蓋範圍更廣且更穩定的高效能寬頻服務，因此也開始嘗試導入軟體定義網路及網路功能虛擬化，以為 LTE 網路能提供新的功能與服務。在 LTE 網路方面，像 S1 介面這種位於基地台端與演進封包核心之間的新型協定，2G 與 3G 時代並不存在。因此，必須考量使用額外資安功能來保護基地台端，因為它是終端用戶開始進行通訊時的第一個接觸點，最容易受到惡意攻擊。至此如何保護 LTE 網路裡的無線電接入網，是通訊服務供應商必須正視的課題；如果在基站端產生資訊安全的侵害，就可能出現斷電、服務品質打折、訂戶資料遺失或遭竊、惡意阻斷服務攻擊或癱瘓終端用戶功能的惡意程式。在這些新的協定與介面之下，4G/LTE 網路的安全不比 2G 或 3G 網路，因而必須更小心處理資安問題。

此外軟體定義網路與網路功能虛擬化的目的在於提升網路彈性，同時提供更機動的隨選服務與頻寬。可降低整體網路運作成本，也是推廣軟體定義網路的另一項重點。

³⁶⁰ THE FAST MODE, “Singapore's M1 to Roll Out Cloud-based Virtual Enhanced Packet Core (vEPC)”, 2017/5.

³⁶¹ THE FAST MODE, “NTT DOCOMO Leverages Ericsson's Open NFV Platform for Multi-Vendor vEPC”, 2016/3/14.

這些正在進行及未來可望出現的網路與技術變革，代表資訊安全必須額外加入現有或未來的網路規畫。此外，也必須具備適當元件與組態以確保服務品質、避免合法的網路故障並抵禦惡意攻擊。以虛擬化的 IP 多媒體子系統與會談邊界控制器為例，就跟企業逐漸改用軟體定義資料中心的趨勢一樣，採用軟體定義網路將加速通訊服務供應商在資安方面的需求。就短期而言，行動通訊網路的資訊安全必須整合並支援這樣的變化趨勢；長遠來看，類似的脫鉤與變遷現象也一樣會發生在電信業者所提供的服務。其中必須特別小心維護軟體定義網路控制器，因為這不僅止有益於全面管控，基於同樣理由它也是駭客夢寐以求的目標。

會談邊界控制器具備了某些資安功能，例如阻斷服務攻擊防護、入侵預防／偵測系統以及加密功能。有了以軟體為基礎的會談邊界控制器，便可將這些功能虛擬化，廠商的技術發展路徑也能更進一步邁向虛擬化。或許在次世代的電信級防火牆當中，網際網路金鑰交換（IKE）功能也可以虛擬化，藉此打造一個更彈性且相對安全的營運環境，然而軟體定義網路的環境還是有資安風險。因此整體而言，軟體定義網路雖非全新願景，因為企業界已開始將資料中心朝向軟體定義網路發展，雖然對通訊服務業者來說仍屬新概念，部分資安方面的問題其實與資訊網路相當類似。

全面採用 IP 架構雖然帶來資安方面的挑戰，但 4G 的另一個要素就是驗證與加密功能更為提升。以 E-UTRAN 為例，透過無線電介面傳送的資料全經過加密。相反地，部署小型基地台等各種趨勢日趨受歡迎。小型基地台提高了網路存取能力，卻很容易遭到竄改，而駭客也有機會可利用這些存取點並找出其中弱點。

然而隨著網路技術的蓬勃發展，網路上的惡意活動愈來愈頻繁，弱點掃描技術也是資訊安全的重要技術之一，可以視為是主動式防禦方法。善用弱點掃描的技術可以幫助檢測者或防禦端瞭解所設備是否存在弱點，進而遮蔽或修補弱點以將風險降到最低，其主要是偵測並掃描位於基站上的各個通訊埠或進入點(如:系統登入畫面)的弱點資訊後，與自身的資料庫進行比對(為確保掃描時所需之弱點與漏洞的詳細資訊，通常會透過與多數公認規模較大的弱點資料庫進行了整合，例如：BID³⁶²、US-CERT³⁶³、

³⁶² Security Focus Bugtraq ID database.

³⁶³ United States - Computer Emergency Readiness Team.

CVE³⁶⁴、MSKB³⁶⁵、OVAL³⁶⁶)，並將分析出的相關弱點或漏洞資訊產生報表，以供檢測者快速瞭解並與分析風險等級，並協助提出修正建議。但「水可載舟，亦可覆舟」此技術對於惡意的攻擊者而言，同樣也是一種得力的攻擊工具，攻擊者一旦透過這些技術取得了目標主機或設備的相關弱點，後續便可以利用這些弱點針對基站進行攻擊行為。

此外弱點掃描工具大多數與滲透測試工具相互搭配，原因在於當利用弱點掃描工具取得基站的弱點資訊後，通常會進一步利用多種方法以驗證弱點確實存在與瞭解其危害程度，而這些方法中，滲透測試工具常為檢測人員所採用。目前業界有多款弱點掃描與滲透測試工具，但大多各自掌握自己的強項，且彼此間缺少整合性。為此，本平臺的框架式設計，可輕易地克服這樣的問題，除了可整合多種掃描與滲透工具外，更能讓多種不同工具的結合所產生的報表相互交叉比對，以避免爭議並進一步提升檢測的準確度與公信力。

為了能精確且有效率的檢測出基站可能存在的弱點，並對照環境中可能產生的威脅後，以提出適當的建議與因應策略，故此單元中，本平臺在常見與潛在弱點檢測單元規劃分別進行靜態與動態測試兩種策略進行，分別說明如下：

- 靜態測試：不測試程式本身，而直接尋找程式中可能存在的缺陷或評估程式碼品質的行為。主要是在單元測試行為中，對技術、設計文件進行評核，程式無法執行或需要對原始程式進行規範符合性檢查時該使用這種策略。
- 動態測試：從運作中的待測基站，輸入測試資料，檢查運作結果與預期結果的差異，從而判斷系統中是否存在缺陷的過程。而動態測試又可透過下列三種測試技術進行，分別是：
 - 黑箱測試：測試人員完全不考慮基站內部的邏輯結構和特性，只依據基站的需求規格說明書，檢查基站的功能是否符合它的功能性說明的測試方法。主要是在進行基站系統測試時使用。
 - 白箱測試：使用被測基站內部如何工作的資訊，允許測試人員對基站內部邏

³⁶⁴ Common Vulnerabilities and Exposures.

³⁶⁵ Microsoft Knowledge Base article.

³⁶⁶ Open Vulnerability and Assessment Language.

輯結構及有關資訊來設計和選擇測試案例，對基站的邏輯路徑進行測試。其測試基於涵蓋整體的程式碼、分枝、路徑及條件。

- 灰箱測試：基於被測試基站的系統功能介面上設計測試案例。通常是作為黑箱測試的補充或在黑箱發現缺陷以後，進一步分析原因確認問題時採用。

基於上述兩種測試方法與三種測試技術，並依據待測基站廠商支援程度依序進行，採取先由工具進行自動化檢測，後續再由專業的檢測人員進行分析與異常測試驗證。本平臺架構提供極佳的檢測彈性與擴充能力，使得檢測機制與工具可依據實際狀況及檢測的精細度要求，並對特定的問題以及未來可能因應的檢測需求進行擴充與升級。因此平臺進行本單元的檢測工作時，對於不斷在第三方弱點揭露系統被公告的共通弱點，以及與廠商在生產基站系統過程所導致的潛在弱點，都能透過各式檢測機制進行深層的問題發掘，此外也藉由導入潛在弱點檢測與滲透工具，以提升檢測平臺對於深層弱點的偵知能力，因此檢測結果將包含已知和未知的弱點，相關主動式檢測機制說明如圖 6-27 所示。以下將針對所使用的相關測試與評估工具分別加以說明。

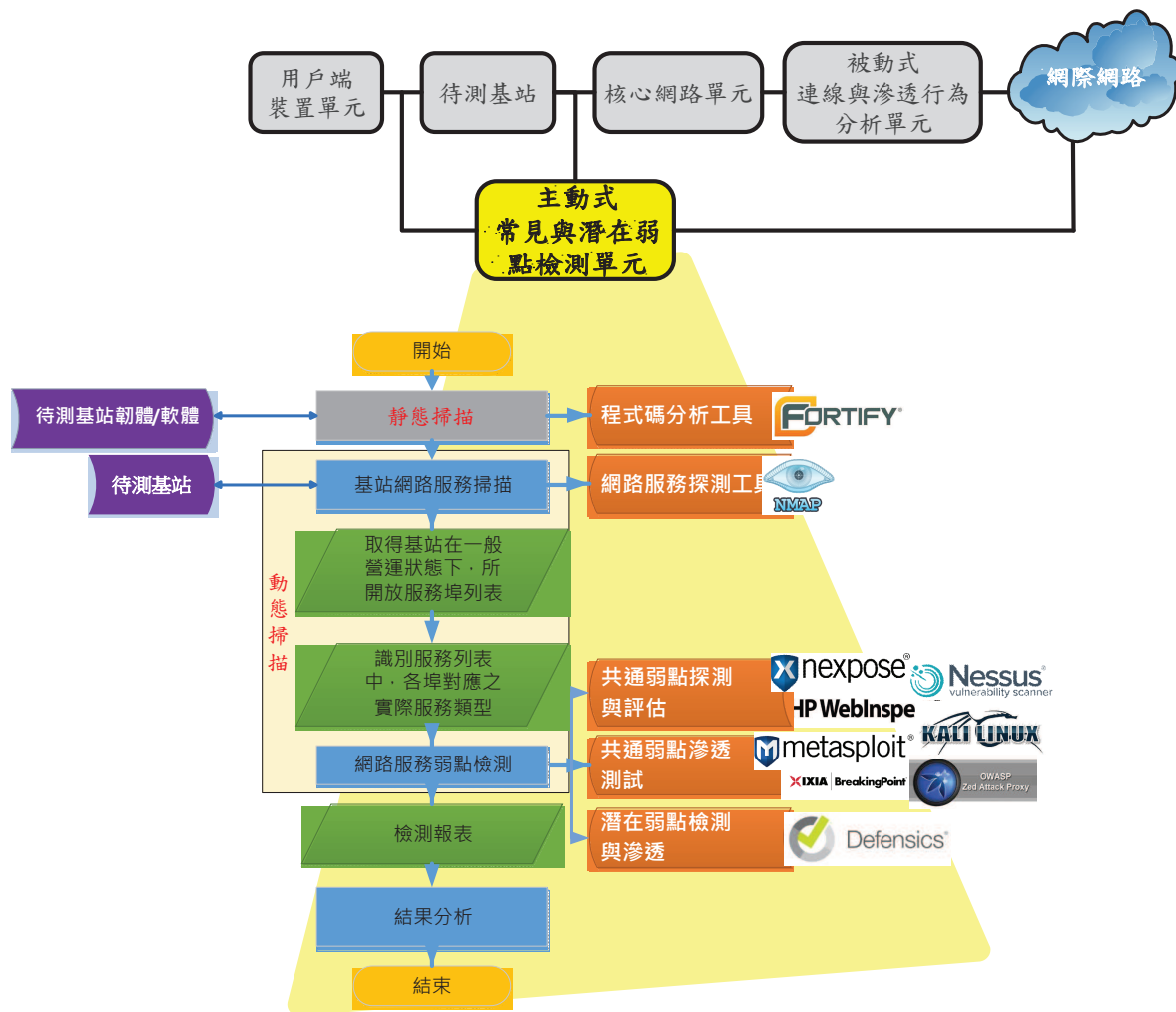


圖 6-27 基站資安檢測平臺-主動式常見與潛在弱點檢測組套圖說

資料來源：本團隊整理

(一) 程式碼分析工具

當所有焦點都一窩蜂的開始重視資訊安全，談論哪一家應用程式防火牆（WAF）比較好，哪一家的滲透測試工具比較厲害，哪一個白帽駭客身手矯健可深入系統如入無人之境，當我們把焦點放在錯誤的位置上，真正的問題就可能因此無法完整顯現。Software Security: Building Security In³⁶⁷ 一書的作者 Gary McGraw 提倡在傳統的開發

³⁶⁷ McGraw, "Software Security: Building Security In", Addison-Wesley's Software Security Series, Pearson 647

流程中，將資訊安全的檢核點（他稱為 Touchpoint）放入。在傳統的需求訪談中，我們只會詢問應用程式的範圍、功能/非功能列表、功能/非功能數量概估等等，而在 Gary McGraw 認為在需求訪談時就必須加入資訊安全要求，比如搭配組織的資安政策等等。而在架構與功能設計時必須作風險評估，傳統的風險評估的估算方式如圖 6-28 所示。

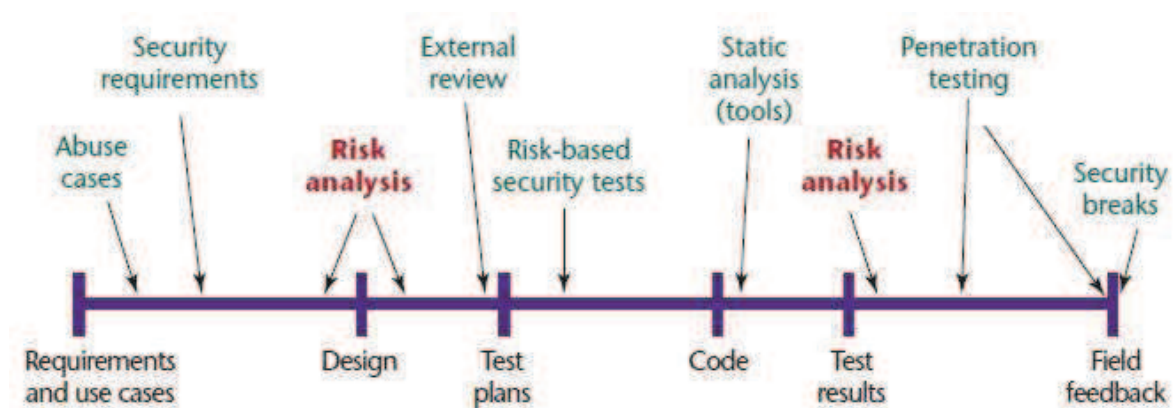


圖 6-28 傳統的風險評估的估算方式

資料來源：synopsys.com

但傳統的風險評估方式無法明確的指出風險所在的弱點，也不能標示出可能的攻擊者，因此目前資安業界所使用的風險評估方式為：

- 列舉要保護的系統範圍，識別出系統重要的資產（assets），並進行重要性排序。
- 瞭解保護的對象與可能的攻擊者，進行威脅塑模（Threat Modeling）。

接著在系統測試計畫裡，要將一般的測試個案化身為考慮資安的測試個案，稱為功能安全測試（Risk Based and Functional Security Testing）。除了原本考量的功能性測試之外，每個測試個案還都必須盡可能將該個案所擁有的功能安全缺失給測試出來。而這樣的 Security testing 技術包括：

- 身分偽冒：試著以非授權者身分進入系統。
- 修改資料：將修改後資料送入系統，或修改簽章雜湊值。

- 記錄竄改：是否可能有記錄檔無法運行的狀況，或被寫入假記錄的狀況？資料揭露：是否能用更高權限帳號使用非授權的資料，或讓應用程式無法執行產生錯誤記錄檔，供駭客查看。
- 拒絕服務：將過多資料餵給處理程序，造成無法服務正常資料。

完成安全功能測試後，接著就是進行原始碼檢測。可分為人工與自動化。傳統的人工原始碼檢測就是以人工方式檢查原始碼，找出程式不合理的邏輯、不一致的命名，或架構編寫不好的地方。然而人工原始碼檢測效率不佳，而且還必須有高素質的人力，當然，也可以聘請所謂的「專家」協助，但是這些專家都非常昂貴。有了資訊安全考量後，原始碼檢測的水準取決於人員的資訊安全能量是否足夠，而足量的資安能力才有辦法讓檢測人員真正能「看得出」不安全的程式，通常訓練一位資安檢測人員必須耗用許多時間與資源。

以常見的 Unix/Linux 系統為例，雖然內建的 grep 指令就是一種最簡單也最直覺的靜態分析方法。Grep 指令的搜尋字串能力，用來對付程式碼最好不過；缺點則是 grep 並不瞭解他掃描的是什麼檔案。註解、字串、宣告與函式呼叫也都只是比對的字元一部份而已，且無法透過加入程式語言的語彙規則以分辨有風險的函式呼叫。此外，雖可透過將基本的語彙分析能力實作在分析工具，作為先期分析過程，包括 ITS4³⁶⁸、FlawFinder³⁶⁹與 RATS³⁷⁰等工具，將程式碼轉為符記（token，這也是編譯器進行編譯的第一步），再讓符記與弱點函式庫進行比對。即使語彙分析工具比 grep 指令強了很多，但是沒有針對語意進行分析，誤報率很高。將程式碼轉譯為符記比起直接將原始碼載入比對引擎要來的好，但是要透過這樣的方式瞭解程式碼運作仍有一大步要走，雖然有些高安全風險的程式碼辨視度很高，不需要再進行語意分析就可正確判斷，但大部分都不是這麼好判斷。

而現在自動化原始碼檢測效率是人工檢測的數百倍以上，內建安全知識庫，並可持續運行，較成熟的自動化原始碼檢測工具除了有語意/資料流分析，支援多種語言，多層次分析、可依需求使用不同的分類方式查找風險弱點...等能力。此類型之工具通

³⁶⁸ ITS4. [Online]. Available: <http://www.cigital.com/its4/>

³⁶⁹ FlawFinder. [Online]. Available: <http://www.dwheeler.com/flawfinder/>

³⁷⁰ RATS. [Online]. Available: <http://www.securesoftware.com/>

常會以污染標示元 (taint flag) 自動標示出受污染的變數源，稱為 Source，這個污染源通常是網頁的輸入或是程式參數輸入點，變數經過一連串的傳遞，到達可能會引發真正安全風險的函式呼叫，稱為 Sink，也就是事件的引爆點。這樣的安全風險解決方式通常是，撰寫一檢查輸入變數值的函式，且檢查邏輯還需要依據該變數屬性撰寫。

但自動化原始碼檢測為了提高精確度，分析工具必須採用許多編譯器的技術，例如將原始碼編譯為中繼檔 (AST、abstract syntax tree) 這種語意分析技術納入。有了 AST 技術，下一步要決定分析範圍。分析範圍分成三種：

- A. Local analysis 一次檢查一個函式，不考慮函式之間的關係。
- B. Module-level analysis 檢查一個類別，或整個編譯單元，所以要考慮同一編譯單元函式之間的關係，但是不檢查跨模組之間的函式關係。
- C. Global analysis 必須分析整支程式，所以必須考慮所有函式之間的關係。上下文的關連性 (context) 分析也必須在分析範圍裡決定。若要減少誤判，要檢查的上下文關連性範圍勢必變大，但是得花很多計算時間。

一個成熟的原始碼檢測工具能藉由將整個資料流程串起且加以分析，對於多層次的系統架構從前端網頁，中間層的商业邏輯，到後端的資料庫語法形成完整的架構概念。再者從一個完整的檢測專案來看，找出安全風險弱點並不足夠，還需要有稽核機制可以協助精準追蹤具有高度風險弱點問題。因此一套適當的程式碼分析工具除了給專業人員使用外，對於訓練入門的資安檢測稽核人員，也能透過系統化的訓練，循序漸進的成為具備資安專長的檢測人員。

(二) 網路服務探測工具

如果想知道待測基站目前正在運作的服務，相信多數的檢測人員腦海裡浮現的第一個解決方案，應該就是利用網路服務探測掃描工具來進行掃描。藉由這工具可以檢測目標主機是否上線、邏輯通訊埠開放情況、偵測運行的服務類型及版本資訊、偵測操作系統與設備類型等資訊。通常被用以做為評估網路系統安全的先期步驟，而駭客也會用相同的方法來蒐集目標電腦的網路設定，從而計畫攻擊的方法。

這類工具通常在資訊蒐集階段，就會被用於蒐集目標機主機的基本狀態資訊，而其掃描結果也可以作為後續弱點掃描、弱點利用和權限提升階段的輸入。其主要功能

如下：

- 通訊埠掃描:用於掃描待測基站上的通訊埠狀態。透過掃描可以將識別通訊埠為開放 (Open)、關閉 (Closed)、過濾 (Filtered)、未過濾 (Unfiltered)、開放或遭過濾 (Open|Filtered)、關閉或遭過濾 (Closed|Filtered) 的狀態。
- 版本偵測:用於識別待測基站上運行的應用程序與程序版本。通常此類工具可以識別數千種應用服務的簽名 (Signatures),檢測數百種應用協議。而對於無法識別的應用服務，會預設顯示該應用服務的指紋(Fingerprint)。
- 操作系統偵測:用於識別待測基站的作業系統類型、版本編號及設備類型。
- 防火牆/IDS 躲避和欺騙:藉由多種內建的機制來規避防火牆、IDS 的阻擋和檢查機制，便於秘密地探查位於網路保護機制後方目標設備的狀況。基本的躲避方式包括：碎片躲避、IP 誘騙、IP 偽裝、MAC 地址偽裝。
- 腳本(script)引擎: 此種功能是這類工具最強大而靈活的特性之一，可以用於增強主機探測、通訊埠掃描、版本偵測和作業系統偵測等功能，還可以用來擴展成為進階的功能，如:web 掃描、弱點發現和弱點利用等。通常此類腳本庫預設就已經可以提供 350 多份檢測的腳本。

對於本檢測平臺而言，精確網路服務探測為對基站進行資安檢測重要的先導程序，不論用於識別有弱點的服務並建立檢測模型，以利後續採用適當的檢測工具進行檢測；或未來電信業者採用後，針對特定弱點建立防禦策略，在整個檢測流程與框架的範疇中，都是不可或缺的重要環節。

（三） 共通弱點探測與評估工具

本平臺在這個階段採用共通弱點探測與評估工具，是一個可以自動執行網路安全審核和弱點評估程式，主要是偵測並掃描位於基站上的各個服務通訊埠或節點的弱點資訊後，與多數公認規模較大的弱點資料庫進行整合比對，並將分析出的相關弱點或漏洞資訊產生報表，以供管理者快速瞭解並進行設備管理的修正決策，其架構如圖 6-29 所示。

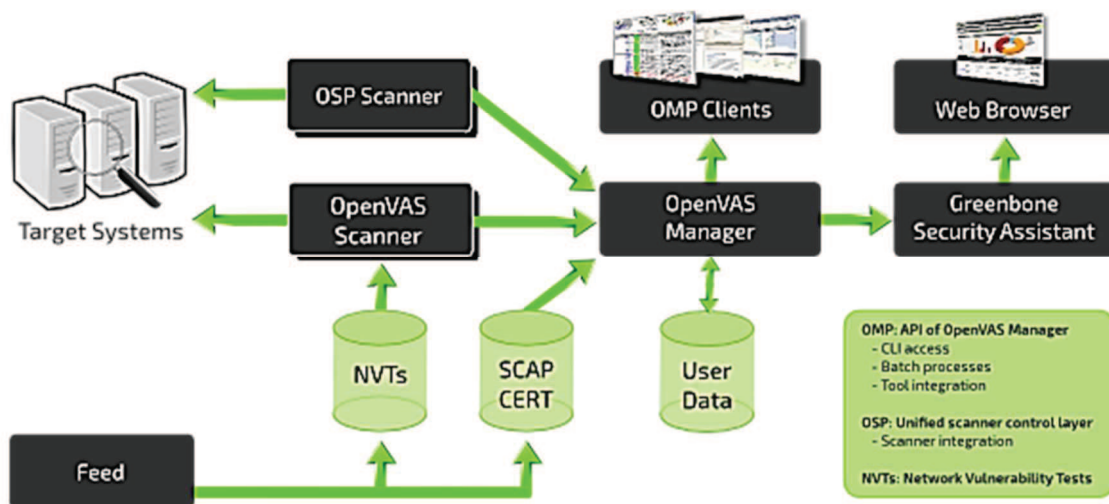


圖 6-29 共通弱點探測與評估工具---以 OpenVAS 為例

資料來源：greenbone.net

在此所指的弱點評估(Vulnerability Assessment; VA)與滲透測試(Penetration Test; PT)的差別是在於，滲透測試會進一步驗證存在評估期間所發現的弱點。此外在完成評估後，工具就能根據弱點本身能被利用的難易程度，對此弱點進行攻擊的技術水準及對此系統所造成的衝擊來計算弱點所屬風險等級，一般區分下列四種等級：

- 高風險(High Risk): 可能讓不具經驗的攻擊者直接取得管理者權限，導致系統中斷、拒絕服務攻擊、執行命令、敏感資訊的揭露等。
- 中風險(Medium Risk): 可能讓稍有經驗的攻擊者直接取得非管理者層級權限，但攻擊者可能可以利用進一步的 hacking 技術來取得管理者權限。
- 低風險(Low Risk): 可能讓具有經驗的攻擊者間接取得某種等級的使用者存取權。
- 一般資訊(Information Risk): 此類弱點僅揭露不具價值的資訊或是根本無法利用來進行攻擊。

透過報表(如圖 6-30 所示)，就可以清楚地看出這些掃描的資訊與結果，包括所檢測基站的 IP 與所開啟的服務通訊埠、掃描時間和風險的描述與相對應的解決方法。藉由 Nessus 的檢測，很容易檢測與管理系統，從掃描報表可以得知目前系統上存在怎樣的弱點，得以及早修補這些漏洞，從而降低被攻擊的可能。

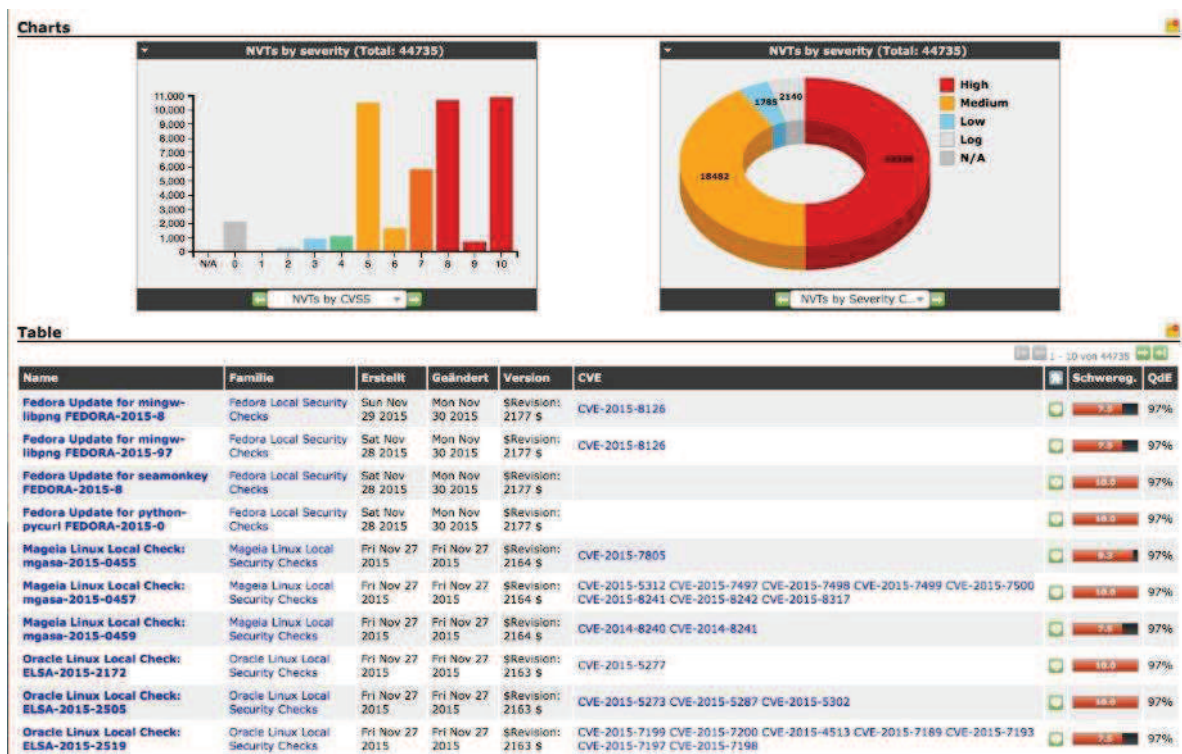


圖 6-30 共通弱點探測與評估結果報表---以 OpenVAS 為例

資料來源：pentestit.de

(四) 共通弱點滲透測試工具

共通弱點滲透測試工具主要是用於檢測基站資訊安全弱點，可以協助進行滲透測試 (penetration testing) 及入侵檢測系統之開發。這類型的工具通常透過開放原始碼框架(Framework)的形式呈現，如圖 6-31 所示，即一套針對遠程主機進行開發和執行「exploit 代碼」的工具，此外部分工具中還包含 Opcode 資料庫、shellcode 檔案、安全研究等內容的重要子項目。其中主要分為兩類利用(exploit)攻擊方法，即主動式和被動式利用。主動式利用是針對目標基站的弱點主動的進行攻擊以獲得控制權限，被動利用是針對目標基站進行被動的監聽然後獲得相應的操作。

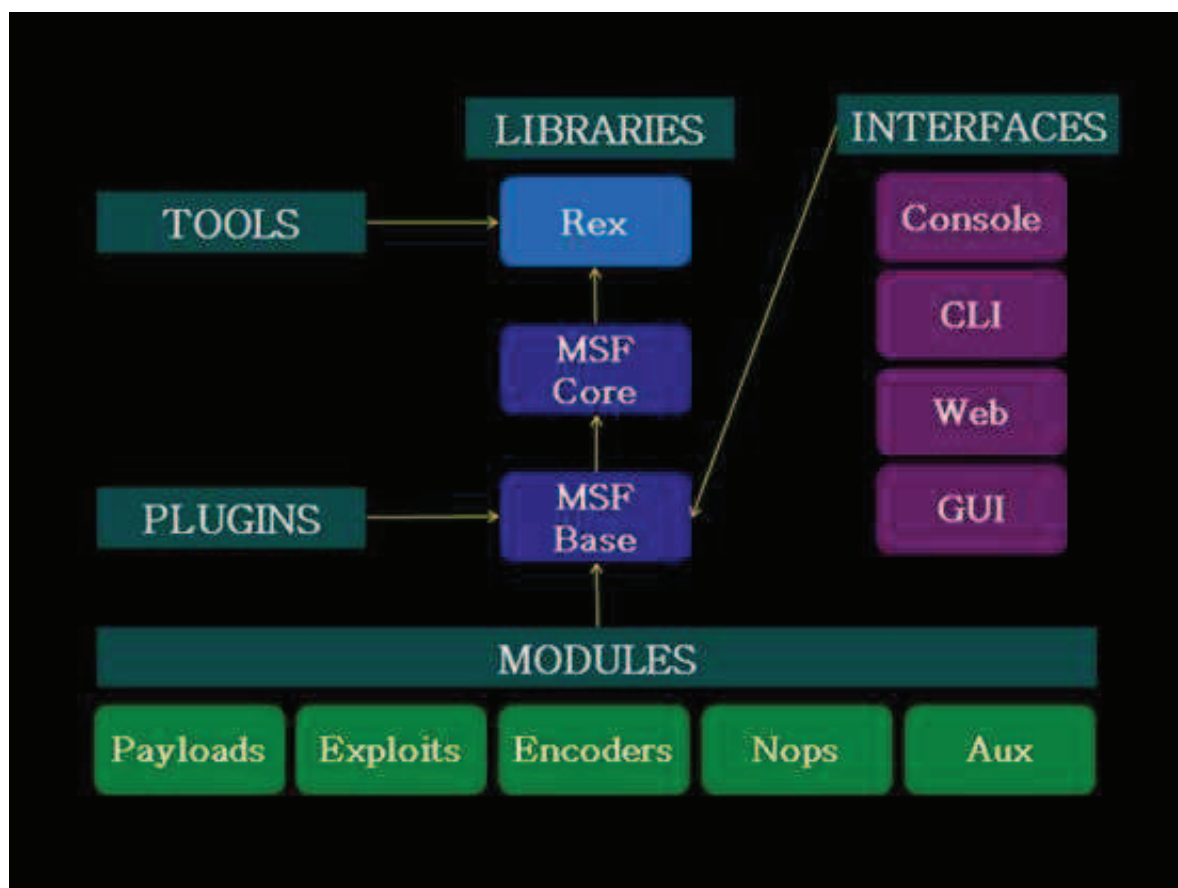


圖 6-31 共通弱點滲透測試工具開放原始碼框架-以 Metasploit 為例

資料來源：hydrasky.com

緩衝區溢位，這是一種非常普遍、非常危險的弱點，在各種作業系統、應用程式中廣泛存在，在當前網路與分布式系統安全中，被廣泛利用的 50% 以上都是緩衝區溢位，可能導致程序運行失敗、系統當機、重新啟動等，也可以利用其獲得非授權指令，甚至系統特權，進而進行各種非法的操作。透過以下的簡單說明，來闡述這類的工具是如何利用系統弱點進行攻擊的方法。緩衝區溢位是指當系統本身的系統向緩衝區內填充數據，當位填充數時超過了緩衝區本身的容量，而這些「溢出」的數據被覆蓋在原本合法使用該區塊的數據上，理想的情況是程序檢查數據長度並「不允許」輸入超過緩衝區長度的字符，但是絕大多數程序都會「假設」數據長度總是與所分配的儲存空間相匹配，這就為緩衝區溢出埋下隱患。此外，多數作業系統都會使用的緩衝區又被稱為「堆疊」，在各個操作進程之間，指令會被暫時儲存在堆疊當中，因此堆疊也會出現緩衝區溢出的狀況。緩衝區溢位的威脅中，最為危險的是堆疊溢位，因為攻擊者可

以利用堆疊溢位，在函數返回時改變返回程序的地址，讓其跳轉到任意地址，帶來的危害一種是程序崩潰導致拒絕服務，另外一種就是跳轉並且執行一段惡意代碼，比如得到 shell，然後為所欲為。因此攻擊者透過相關工具往程序的緩衝區寫超出其長度的內容，造成緩衝區的溢出，從而破壞程序的堆疊，造成程序崩潰或使程序轉而執行其它指令，以達到攻擊的目的。

通常往緩衝區中任意填東西造成它溢位，一般只會出現"分段錯誤"(Segmentation fault)，而不能達到攻擊的目的。最常見的手段是通過製造緩衝區溢位使程序產生一個用戶 shell，再通過 shell 執行其它命令。如果該程序屬於擁有最高權限之帳號 root 所有且具備 suid 權限的話，攻擊者就獲得了一個有 root 權限的 shell，如此就可以對系統進行任意操作了。緩衝區溢出攻擊的目的在於擾亂具有某些特權運行的程序的功能，這樣可以使得攻擊者趁亂取得程序的控制權，如果該程序具有足夠的權限，那麼整個基站系統就被控制了。一般而言，攻擊者攻擊 root 程序，然後執行類似"exec(sh)"的執行代碼來獲得 root 權限的 shell。為了達到這個目的，攻擊者必須達到如下的兩個目標：①在程序的地址空間裡安排適當的程式碼；②通過適當的攻擊暫存器和記憶體內容，觸發程序跳轉到入侵者安排的地址空間執行。每當一個函數呼叫發生時，呼叫者會在堆疊中留下一個活動紀錄，它包含了函數結束時返回的地址。攻擊者通過溢出堆棧中的自動變數，使返回地址指向攻擊代碼。通過改變程序的返回地址，當函數調用結束時，程序就跳轉到攻擊者設定的地址，而不是原先的地址。這類的緩衝區溢出被稱為堆棧溢出攻擊 (Stack Smashing Attack)，是目前最常用的緩衝區溢出攻擊方式。

透過此類工具對基站進行檢測，可以瞭解所欲檢測的基站目前所開放的服務資訊與相關弱點，並及時發現需要加強防禦的部分，或是在評估此風險的嚴重性後，根據相關的分析結果擬定防禦策略，以在惡意攻擊者出現前先進行防範。一般而言都透過下列基本步驟進行：

- A. 選擇並配置一個攻擊代碼(exploit, 利用漏洞來進入目標系統的代碼)；
- B. 檢查目標系統是否會被此代碼影響 (可選)；
- C. 選擇並配置一個有效負載 (payload, 在成功進入後在目標系統上執行的代碼)；
- D. 選擇編碼方式，使入侵預防系統，忽略已被編碼的有效負載；
- E. 執行攻擊代碼。

這類允許任何攻擊代碼和任何有效負載進行隨意組合的模組化結構，是這類以框架為基礎的檢測工具之主要優勢。檢測者可通過不同的搭配，在有限的弱點條件下導入不同的攻擊負載。此外框架式的結構也可以通過添加模組進行攻擊範疇與精細度的擴展，允許檢測者、攻擊模組發展單位及有效負載的開發組織專注於寫出所需的功能，而無需處理其他問題。

此外在選擇攻擊代碼和有效負載時，需要目標系統的部分資訊以提升滲透精準度，例如其作業系統的版本和安裝的網路服務，而這些資訊可透過前述的網路服務探測工具進行蒐集，而共通弱點探測與評估工具則可提供所探測到目標基站的弱點資訊，最後才透過共通弱點滲透測試工具將弱點掃描數據導入，並通過對比已發現的弱點和擁有的攻擊代碼模組來發動準確而有效的攻擊檢測，如圖 6-32 所示。本平臺所規劃的框架中，展現了分進合擊的協作能力，透過多項元件的結合與各元件的擴展功能，以務求精準測試及符合國際上對於各式弱點的評估依據，為後續資料庫建置提供最具參考價值之資訊。

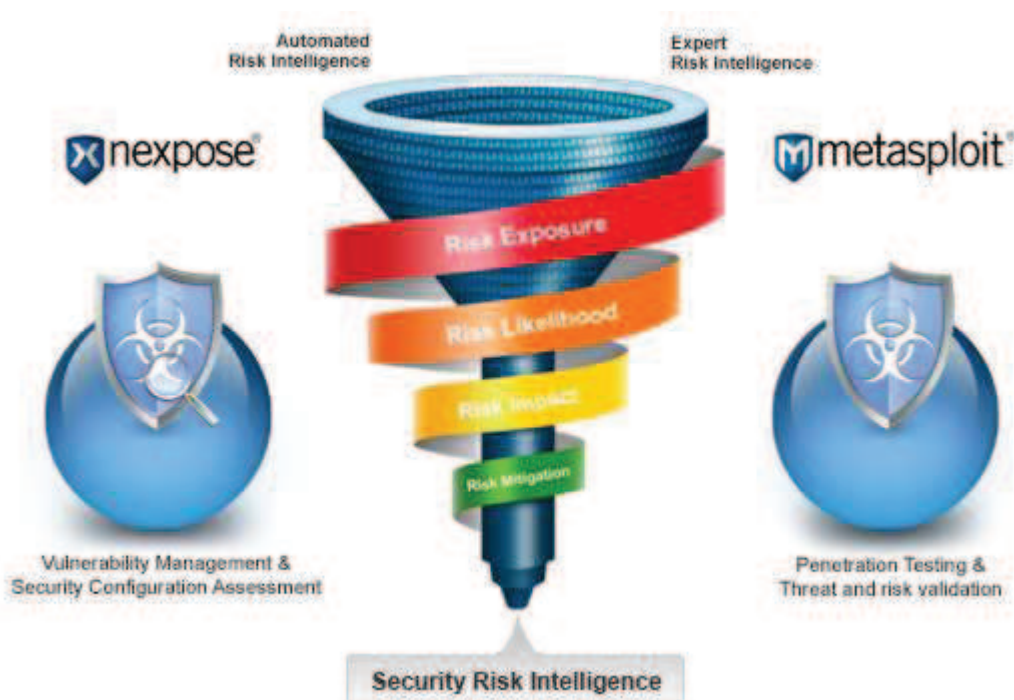


圖 6-32 共通弱點探測、評估與滲透測試整合-以 Nexpose 搭配 Metasploit 為例

資料來源：bockytech.com.tw

（五）潛在弱點檢測與滲透工具

本平臺在架構中使用了基於模糊測試理論(一種測試未知漏洞的方法論)的工具，其工作原理是通過有系統地向受測系統發送無效或意外輸入，從而有效地暴露軟體缺陷，是一種介於完全的手動滲透測試與完全的自動化測試之間的安全性測試類型。模糊測試通常被用於黑箱測試，通常可將工具分為兩類，一是變異測試通過改變已有的資料樣本去生成測試資料，另一種則是生成測試則透過對程式輸入的建模來生成新的測試資料。模糊測試的執行過程大致如下：

- A. 準備好隨機或者半隨機方式生成的數據；
- B. 將準備好的數據導入待測系統進行測試；
- C. 觀察過程中待測系統的狀態；
- D. 根據狀態分析並判斷是否存在缺陷。

一般而言會先觀察並嘗試抓取到待測基站和核心網路之間的通信數據，根據記錄下來的網路封包分析出之間的通信協議，然後根據協定的定義，自行編造數據發起攻擊，嘗試找到可能的弱點，之後再基於上述的流程導入模糊測試的方法。執行潛在弱點檢測與滲透工具的主機只要產生和發送數據的能力足夠強，就能將產生攻擊資訊的任務交給機器去完成，避免人工編造攻擊資訊耗用過多資源的問題。因此可以有效地把檢測人力用於異常通訊行為的分析。雖然模糊測試領域內有一些自動化的協定分析手段，但從效率和效果上來說，在面對複雜協定的時候，人工分析的方式更為有效。

儘管模糊測試(fuzz testing)和滲透測試(penetration test)都是屬於安全測試的方法的一環，它們的差別在於滲透測試一般是模擬駭客惡意入侵的方式對待測物進行測試，因此通常對於測試者的專業能力要求很高，且因應待測物的特性不同，而難以被大規模應用。模糊測試能夠充分利用機器本身，隨機產生和發送數據；同時又能夠導入資安專家在安全檢測方面的建議，具有不確定性，也沒有明顯的針對性，因此只要將準備好的那些雜亂的程序插入其中，然後等待bug的出現，而與滲透測試產生結果不同的是，出現的問題通常是檢測人員無法預知的。

在本團隊基於嚴謹的考量下設計並加入了潛在弱點檢測與滲透工具，這個階段的測試主要是檢測人員使用駭客的手法並配合未知潛在弱點檢測工具，進行諸多零時差

弱點(未被發布的弱點)測試，嘗試入侵基站系統並找出這些可能的弱點，並且在後續提出詳細報告，且納入檢測資料庫做為未來研擬防禦策略的參考依據。

五、 被動式連線與滲透行為分析單元

從專業的檢測實驗觀點而言，適當且完整的資訊安全測試，對於待測設備而言應至少考量如下三個要素：可能面對的威脅、遭遇威脅處理的方法、訂定所需要達成的目標。其中，所需要達成的目標就是確保行動寬頻網路的資通安全，而在主動式常見與潛在弱點檢測單元，本平臺對待測基站進行可能面對的各種威脅評估，因此為了觀察待測基站正常營運狀況下與在遭遇威脅處理的行為，本團隊設計被動式連線與滲透行為分析單元，希望能對待測基站的正常/異常行為有更深一層的瞭解與分析，也期望能更客觀完整呈現檢測結果。

一般而言，如需達成上述的檢測需求，通常需要透過結合一連串的監測與分析功能來完成，如圖 6-33 所示。但隨著網路攻擊的手法不斷翻新，傳統的多層次式偵測與分析配置面對這類已不能單獨用攻擊、蠕蟲或病毒來加以描述的這些威脅，且可能也已經無法有效識別這些當前最廣泛也最具威脅性的網路混合式攻擊。例如：HTTP GET Flooding，能運用殭屍網路(BotNet)，以發散的來源 IP，及看來完全正常的應用系統封包來躲避追查。此外這樣的傳統架構也間接造成了檢測環境的複雜性，需要檢測人員擁有更高的統合操作管理技能，以避免各個檢測機制之間對於惡意行為識別的不一致，而導致發生誤判或漏判的狀況。



圖 6-33 獨立式惡意軟體與行為分析架構

資料來源：solution-gr.co.jp

隨著網路應用多樣化，網路架構的規模、複雜度大幅成長，易遭受網路攻擊之可能性也隨之提高。然而，攻擊者可免費或低價取得攻擊工具與技術，防禦者則因防禦技術跟不上攻擊技術發展的速度，而急需找出適當的解決方案，以解決所面臨的各種威脅。面對這樣的威脅與攻擊發展進程，傳統的資訊安全檢測方式已不敷使用，更無法靠單一產品或單一方式來偵知攻擊，必須站在全方面的角度來思考面對目前及未來的資訊環境，並做出最快速的反應。為了有效提升檢測效率與準確性，本平臺透過整合式威脅管理(Unified threat management，簡稱 UTM)的方式，針對網路安全威脅，在原有的安全閘道概念的基礎之上，藉由同時將防火牆、入侵防禦偵測、防毒掃描、應用程式內容過濾等安全機制整合的管理方案，使所有安全機制在一致性的安全策略下相互配合，協同工作，除了一般企業常用於當成防禦機制外，此類整合性工具用於檢測過程中觀察待測物反應也有相當的助益，其概念架構如圖 6-34 所示。

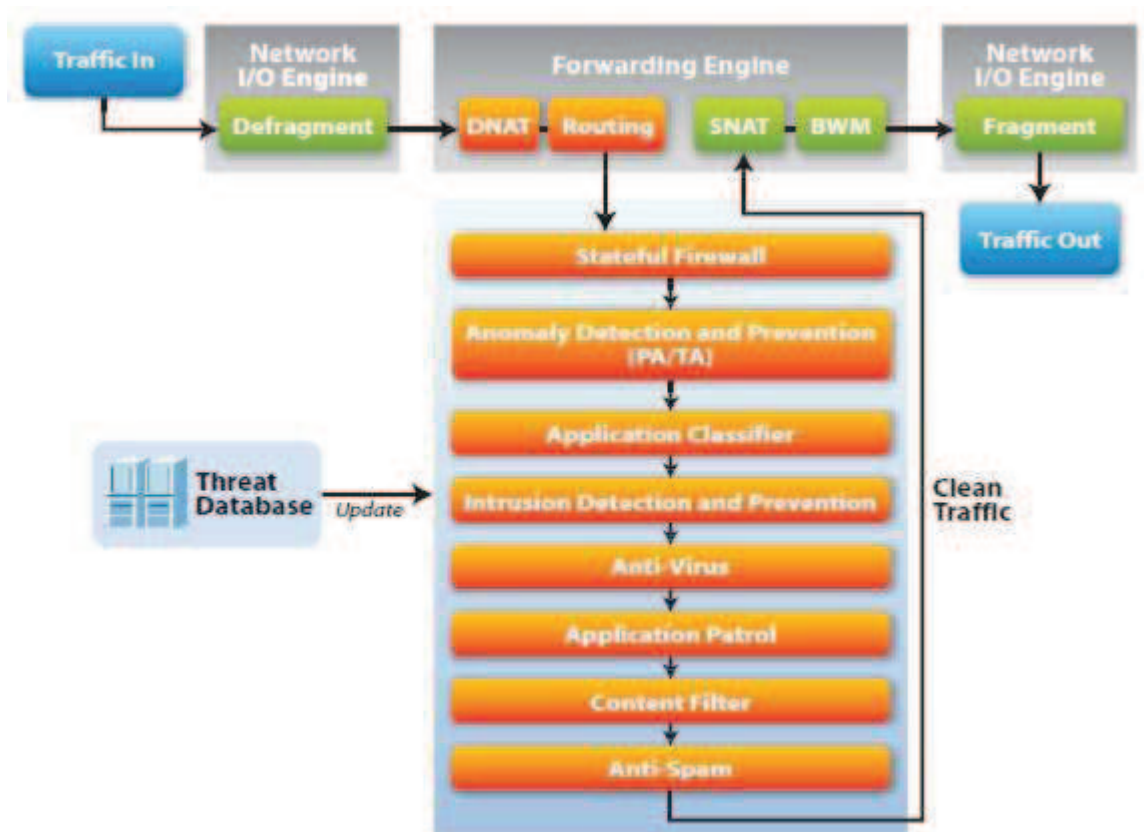


圖 6-34 整合式惡意軟體與行為分析概念架構

資料來源：zyxelguard.com

檢測平臺的設計若僅從安全工具的面向去考量是否導入相關的弱點掃描工具是不夠完整的，應將專業檢測人員的知識技能、防火牆、入侵偵測防禦系統與弱點掃描技術相互結合，則可以更有效地提高資訊安全檢測的能量。因此，本平臺規劃之被動式連線與滲透行為分析單元，如圖 6-35 所示，透過整合相關分析工具，以系統性與架構性的方式，針對各類惡意行為與軟體進行特徵比對，此外更進一步導入先進持續威脅分析工具，對於各種可能的潛在威脅行為進行判讀與分析，藉由被動式偵測的輔助，使平臺的檢測與評估結果能更為完整，以下針對各個階段所使用的檢測分析工具分別加以說明。

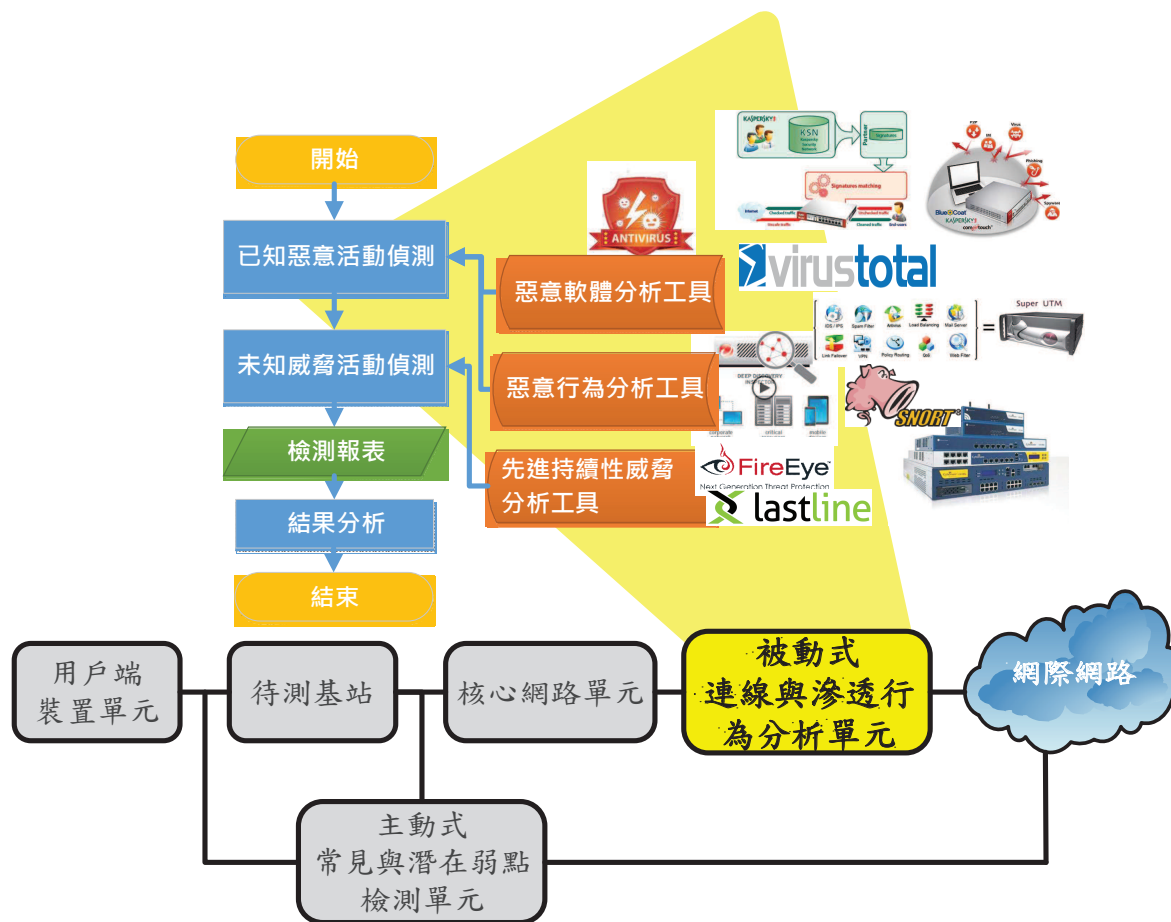


圖 6-35 基站資安檢測平臺-被動式連線與滲透行為分析組套圖說

資料來源：本團隊整理

(一) 惡意軟體分析工具

在檢測過程中，為了確認基站本身是否會發生無意或有意的連線下載行為，以及下載的內容是否可能具備威脅性，因此在本平臺也導入惡意軟體分析工具，來肩負此一重要把關與分析，因應目前大部分病毒和蠕蟲利用網路擴散感染的特性，一方面先行過濾來可能自網際網路的各種病毒蠕蟲威脅和惡意程式入侵，另一方面則可監視基站本身是否有異常的行為，以達到多元化檢測及深層測試的目的。雖然目前有網站(如: [virustotal.com](https://www.virustotal.com))提供惡意軟體檢測，但基於需要能即時從網路流通的來往封包過濾出惡意軟體，這類需要依靠使用者上傳以進行分析的方式並不適合，因此一般常見的檢測機制，通常會使用硬體防毒閘道，或具備防毒功能的防火牆，來針對此部分加強檢測，在完成已知型態之惡意軟體檢出後，才進一步將有疑慮的部分藉由人工上傳進行分析

比對，以更有效率的得到精確之檢測結果。

由於病毒猖獗且加速演化，從單純的惡性程式執行檔，轉為透過網路共享、後門漏洞及系統弱點入侵或竊取系統資訊的混合式病毒。在弱點越來越多的情況下，也有更多的網路病毒開始利用系統的漏洞進行攻擊和傳播。而從基站廠商發佈更新到攻擊者利用這個弱點進行傳播的病毒出現的時間越來越短，病毒留給基站廠商及電信業者進行系統修補的時間也越短。但是如果不及時修補基站的弱點，這些利用弱點傳播的病毒就可能輕鬆繞過電信業者的防禦機制直接感染基站。惡意軟體分析工具攔截與偵測病毒的速度與效率必須更高，因此多數此類的工具亦同時結合防毒、入侵偵測(IDS, Intrusion Detection System)、入侵防護(IDP, Intrusion Detection and Prevention)以及弱點管理，以達到完全偵測的目的。

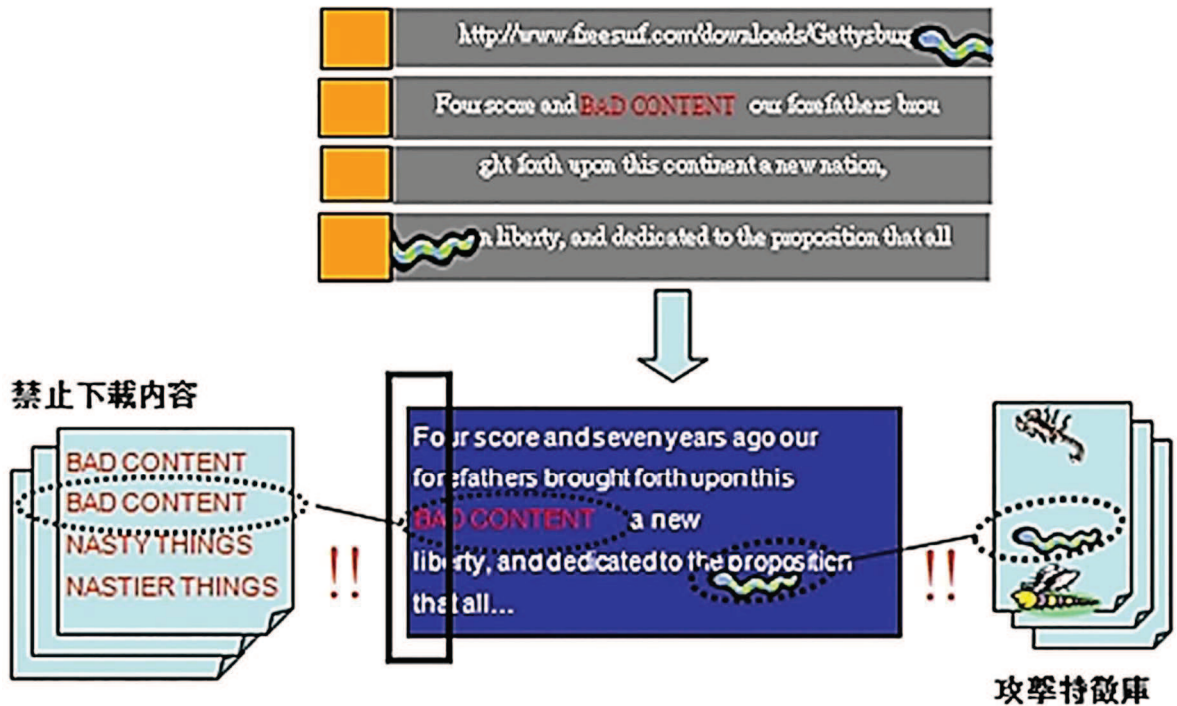
在基站檢測過程中，若基站使用正常行為下載惡意軟體，並自動安裝於本身的系統，也可能造成資安風險。此外這類工具通常伴隨著資料外洩防護(Data Leak Prevention; DLP)或稱為資料遺失防護(Data Loss Prevention)方案共同進行檢測，以安全政策及分類規則為判別基礎，並透過內容比對偵測資料內容風險程度，以確定是否有機敏資訊如通訊金鑰、關鍵安全參數等資訊，遭到受感染或受惡意使用者控制的基站洩漏。因此在平臺中也納入了惡意軟體分析的機制，針對機敏資訊與惡意軟體加以識別與分析。

(二) 惡意行為分析工具

資料遭駭客入侵的頻率與規模日益增加，傳統方法無法因應各類最新的攻擊手段所帶來的威脅，因此透過惡意行為分析工具來防止惡意與異常行為並透過記錄資訊，進行詳細的分析或作為證據之用。透過這類的工具主要使用特徵比對法(Signature based)與異常行為比對法(Anomaly based)來進行通訊內容與行為的檢測，如圖 6-36 所示。

完全的內容層檢測

1. 重新組裝數據包



2. 完整比較攻擊特徵庫和蠕蟲樣本庫

圖 6-36 特徵與異常行為比對概念圖

資料來源：syscom.com.tw

特徵比對法主要是針對已知的攻擊特徵，經由系統比對後將攻擊攔截下來，而異常行為比對法則以多種演算法或其他比對方式，來判斷可能的未知攻擊手法，兩者配合使用，將可有效提升當駭客使用一般工具入侵時的防禦率。與傳統防火牆相似，都是放在開道端偵測並抵禦攻擊，一般是用在偵測 OSI 架構中的網路層(Layer 3)及傳輸層(Layer 4)封包，並針對流量中的 IP 位址、連接埠(Port)號碼來設定相關的通行規則，只要符合這些屬性的正常封包便可放行。其運作方式如圖 6-37 所示。

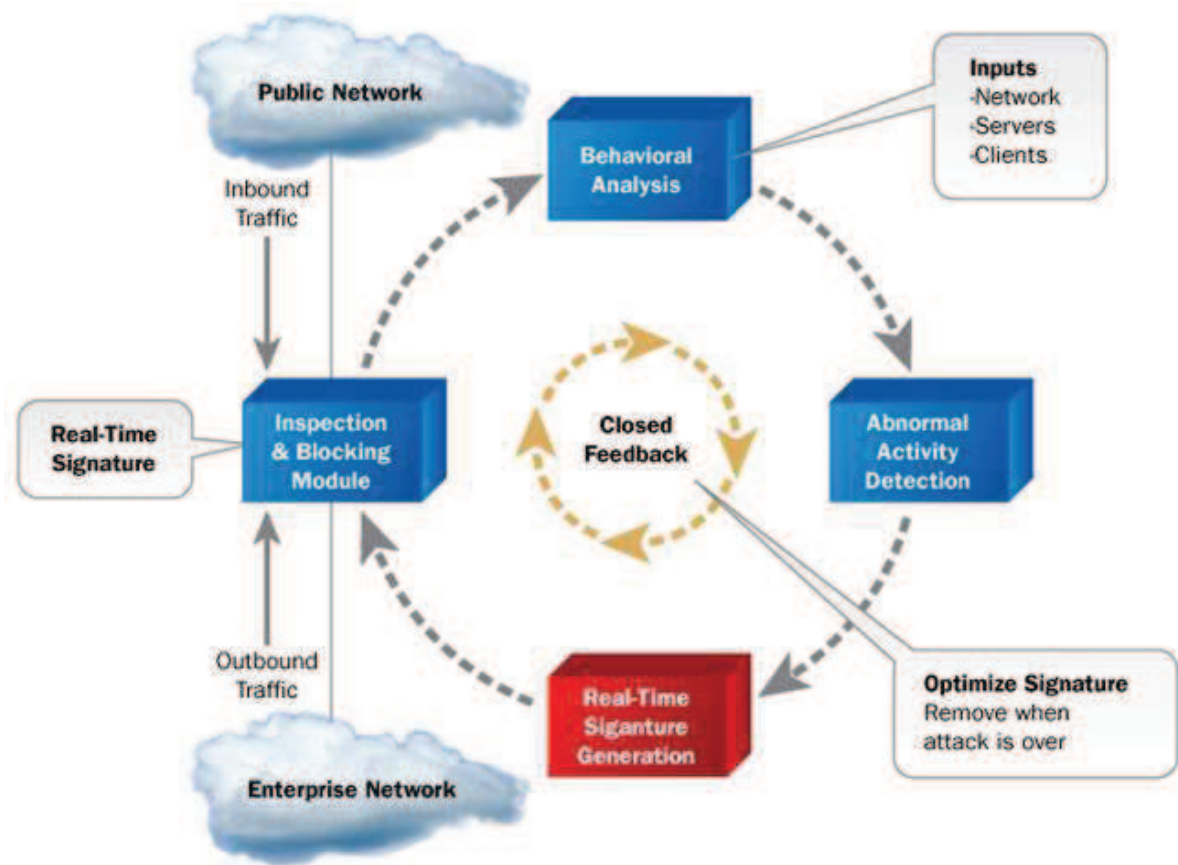


圖 6-37 特徵與異常行為比對流程圖

資料來源：webroam.ir

傳統防火牆是發展歷程逾 20 年的老技術，僅能依據 IP 或 MAC 位址等基本資訊，簡單比對來者是否名列黑名單，如果是便加以攔阻，如果不是就予以放行；惡意人士相當嫻熟防火牆運作原理，也不斷研究如何以正常外表包覆惡意軟體的方式，藉此矇混過關。也由於傳統防火牆機制不會檢查封包內容，對於利用合法網址和連接埠從事的破壞活動，是無法進行阻攔的，所以入侵偵測防禦系統就可以比對封包特徵並攔阻或發出警告的特性，自動過濾出傳統防火牆難以辨識的惡意封包，甚至還能結合行動通訊系統所使用的特殊協定或慣性行為模式比對，進一步記錄可疑連線，達成與傳統防火牆互補性的效果。

本平臺透過整合資訊安全領域常用的入侵偵測防禦系統(Intrusion Detection and Prevention System，簡稱 IDP 或 IPS)工具模組來達成，在流經與直接從基站發出的網路封包，將依據平臺設計的檢測路徑穿越，由過程中所有發現的異常或攻擊的行為，

將被此工具完整紀錄並進行分析。此工具雖通常被用於企業的閘道抵禦攻擊，但在檢測環境中，其即時檢測的核心理念，能有效協助檢測人員快速分析出異常與威脅通訊，並提供詳細的事後分析資訊。通常具備下列主要功能。

1. 線上作業(In-Line)：只有線上作業才能使執行即時的偵測與防護，過濾所有異常封包，確認所有可能包含異常活動或可疑內容。使檢測人員能在警報發出的當下，立即確認步驟並針對異常行為重複測試與確認。
2. 高精確的偵測能力：辨識攻擊特徵的能力必須準確無慮，因為誤報可能導致檢測人員投注額外的資源做檢測。此外透過定期線上更新的方式獲取新的攻擊特徵，與國際上的攻擊資訊同步，使平臺檢測結果更具公信力。
3. 高效能與低延遲：由於在實際運作時的封包處理速度必須接近線速 (wire speed)，而且設備在啟用所有攻擊特徵後是必須達到宣稱的執行效能，如此才能避免基站與核心網路之間造成通訊異常，且達到仿真檢測之效果。

電信業者藉由設備走向 IP 化及網路化來提升管理、營運效率的同時，對於國家關鍵基礎設施網路的資安風險，監管單位當然也不能等閒視之，而透過惡意行為分析工具通常都具有豐富的特徵資料庫可供比對，甚至可以透過日誌分析、安全性資訊和資安事件管理平臺(Security Information Event Management，簡稱 SIEM) 關聯分析等途徑，協助檢測實驗室深入挖掘出埋藏在正常表象之中的異常行為，並作為業者或政策制定單位進行相關決策重要的參考依據，為此在平臺的設計中，納入惡意行為分析工具以協助檢測人員在測試的過程，對基站的所有通訊過程與行為進行深度的分析，並將分析結果也納入檢測報告，以與其他工具評估結果交叉比對，減少誤判或漏判的機會，也有益於提升評估結果的可信度。

(三) 先進持續性威脅分析工具

進階持續性威脅(Advanced Persistent Threat，簡稱 APT)不是一種新的攻擊手法，也不是可以藉由阻止或破壞一次攻擊就讓問題消失。APT 可以被視為更像是一個網路攻擊活動而不是單一類型的威脅；可以想成是進行中的過程。防毒軟體可能可以阻止 APT 攻擊所使用的惡意程式，但並不意味著停止攻擊。就其性質而言，APT 是一段持續的攻擊。如果一個戰術行不通，就會再嘗試另外一個。APT 主要的攻擊步驟如圖 6-38 所示。

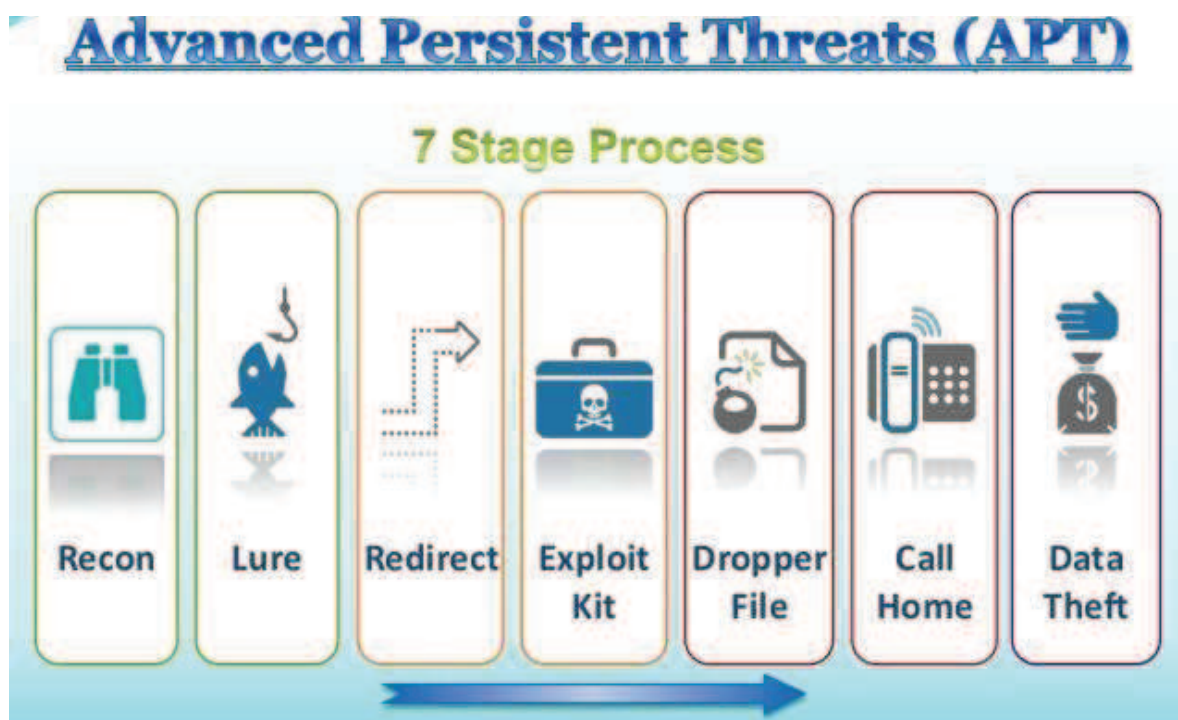


圖 6- 38 進階持續性威脅運作流程圖

資料來源：Electronics Corporation of India Ltd, ECIL³⁷¹

現在常見的傳統式防火牆（Firewall）與整合式威脅管理防火牆（Unified Threat Management，簡稱 UTM）已經無法有效防禦 APT 目標式攻擊威脅，因為這是一種具針對性、複雜化與客製化的攻擊。過去所發生過的大規模病毒攻擊事件，往往是有人藉由所謂的 0-day 弱點，在未發布修正程式的空窗期將惡意程式大量散播，短時間內就能癱瘓企業網路與主機，並造成難以估計的損失，不過一旦發布了修補程式後，這類型的病毒便很難繼續進行攻擊。而駭客就是利用未被公佈之軟體／系統弱點（零時差攻擊 Zero Day Attack）進行惡意程式的製作，以閃避防毒軟體的偵測，例如最常見的就是 Microsoft 的 Word、Excel、Power Point 以及 Internet Explorer，因為這些是現在最普及的文書處理軟體及瀏覽器，而更具有威脅性。當駭客透過特製的惡意程式來攻擊企業內部系統，通常這類惡意程式只屬於該企業의 客製化惡意程式，使得現有防

³⁷¹ Abhinav Biswas, “Insights Into Modern Day Threat Protection”, Electronics Corporation of India Ltd, ECIL, 2015/5/2.

毒軟體因樣本數的不足，而無法有效的偵測。

這類的攻擊若是其目標為存在著弱點的基站，若是某特定型號基站，亦可被視為只屬於特定用途且為電信業者客製化的惡意程式，則駭客就可利用這樣的優勢取得基站的控制權，進一步竊取相關重要資訊。進階持續性威脅也可能穿越過傳統的安全防護機制，並且持續潛伏在電信業者組織內部。由於這些攻擊的隱密性與持續性，使得電信業者組織內部很可能已遭到入侵，只是還不知道而已。鑒於並非所有威脅都有辦法預防，假設滲透無可避免，應該將目標轉移至改善偵測、預防及事件應變能力之上。

由基本面來看，符合下列三項特點，一般就被認為這攻擊是進階持續性威脅 (APT)：

- 出於經濟利益或競爭優勢
- 長期持續的攻擊
- 針對特定的公司、組織或平臺

所以企業與政府通常是 APT 進階持續性威脅的目標，要注意 APT 進階持續性威脅是長期且多階段的攻擊，早期階段可能集中在蒐集關於設備的網路設定和作業系統的詳細資訊，接著，受駭的設備或主機作為跳板，對網路內其他主機、設備或用戶端進行情報蒐集，安裝 Rootkit 或其他惡意軟體去取得控制權或是跟命令與控制伺服器 (C&C Server) 建立連線。再下來的攻擊可能集中在複製機密或是敏感數據來竊取知識產權。

從實務面來看，APT 是長期的過程導向攻擊，是攻擊者動機和攻擊手段改變下的產物。防毒軟體，通訊加密，弱點掃描和上修正程式 (Patch) 都是很好的作法。但是這些還不足以去應付 APT，所以假設會被攻擊成功(或基站出廠時，即由於種種因素被植入惡意程式)的前提下，我們必須即時的監控網路流量和電腦上的活動，包括隔離設備和蒐集資料以作鑑識分析之用。萬一攻擊發生了，能夠儘快偵測到攻擊和遏制它所造成的影響才是最主要的目的。

然而面對這類新型態的攻擊，可能是經過偽裝再以隧道連線、甚至以加密或其他方式入侵，若將資訊安全沙箱 (Sandbox) 技術納入於檢測機制中，即便今天出現了新型的惡意程式碼，透過沙箱技術會將疑似惡意程式碼引入沙箱，以試圖確認其行為與

意圖。因此沙箱透過模擬建置出待測物的執行環境，檢測人員可以在這個安全隔離的環境下執行並觸發其程式碼，並根據程式碼所執行的活動而非其屬性來進行觀察與分級。這樣的設計主要是將隱藏的惡意軟體困在沙箱裡，開啟執行檔並使用密閉的網路流量等等。讓檢測人員可在沙箱的安全環境下執行、觀察惡意程式碼的運作，例如：執行檔案／磁碟的存取行為、網路連線、微軟註冊機／系統組態變更等。為了分析惡意軟體，沙箱會模擬不同的操作系統與技術，執行多個程式碼評估程序，執行的先後順序則是根據惡意軟體在不同組態下的活躍程度來排定，進而加速辨識惡意程式碼。

為此本平臺所導入的先進持續性威脅分析工具將會於網路層進行掃描與分析，其主要架構如圖 6-39 所示，並透過沙箱分析系統，以及對網路、電子郵件及端點的整合式偵測，提供進階的偵測系統來偵測 APT 攻擊，有效的偵測 C&C 通訊連線及一般防護無法偵測到的隱匿攻擊活動。



圖 6-39 沙箱技術與整合式威脅管理共構運作流程圖

資料來源：netfos.com.tw

第二節 驗證行動寬頻基站資安檢測平臺

本節主要說明依前述建構行動寬頻基站資安檢測平臺之規劃，完成各設備之間的相互介接及整合功能驗證測試，確認平臺可正常運行，並能有效配合執行本計畫之基站資安檢測，提供檢測平臺檢測相關驗證紀錄，以做為後續進行實際資安檢測、研擬並提出檢測規範與作業程序建議作業內容，最後產出適用於行動寬頻環境之專屬弱點檢測資料庫。透過此一平臺提供相容性、功能性與安全性之相關測試，讓各種行動網路節點裝置在入網上線之前，確保其具備基礎之相容能力與安全性。整體檢測平臺之

元件配置概念圖如圖 6-40 所示，藉由實體與邏輯架構併呈的繪製方式，描述各階段檢測所使用之設備及相互間的對應關係，以提供此整合式平臺的完整輪廓，讓使用者能在參考各元件之應用說明後，即可有效的施測並取得報表。以下將藉由檢測架構中，待測基站面對各種機制之探測，可能於檢測流程呈現反應的畫面呈現，加以說明。



圖 6-40 行動寬頻基站資安檢測平臺配置概念圖

資料來源：本團隊整理

一、一般性功能項目與相關驗證程序說明

本章第一節所規劃的待測基站、用戶端設備及核心網路之概念，並和工業技術研究院 4G+網路接取與應用測試實驗場域進行實作，採用下列兩種類型之基礎配置架構進行檢測與分析，如圖 6-41 所示。

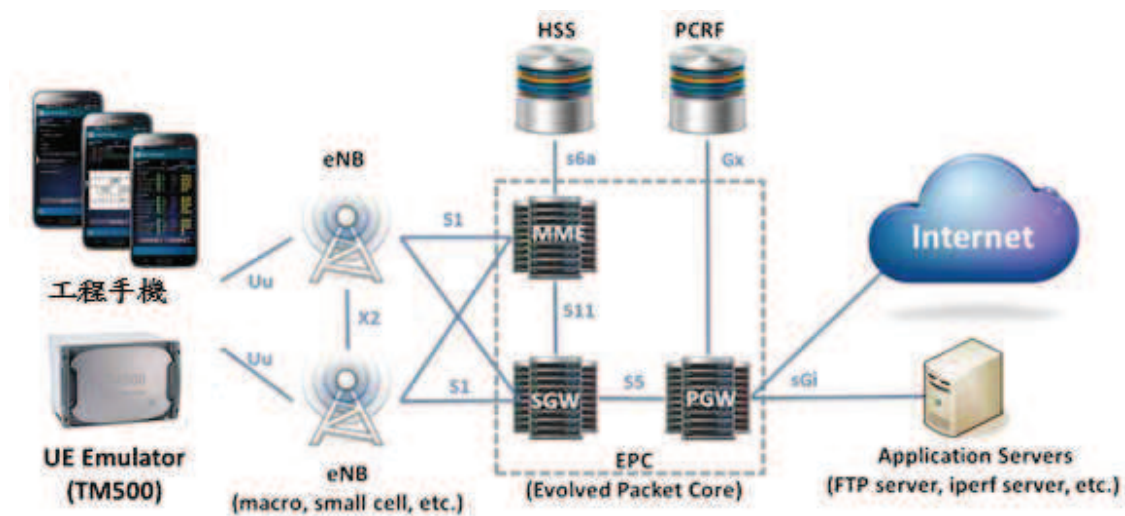


圖 6-41 一般性檢測實作基本架構圖

資料來源：ITRI 4G+實驗場域測試中心及本團隊整理

在檢測過程，首先透過工程手機進行基本信令檢測，其中包含訊號量測、網路效能測試，利用腳本 (Script) 自動測試功能，由特定設備的系統、頻段、優選載波鎖定、攪亂碼 (Scrambling code，簡稱 SC)、頻道和 PCI 鎖定下達強制命令進行 3GPP 信令符合性檢測，除了即時顯示如圖 6-42 的畫面所呈現相關資訊外，完成檢測後亦將所有射頻和信令資料都記錄到手機記憶體中，以日誌檔案格式匯出並分析。

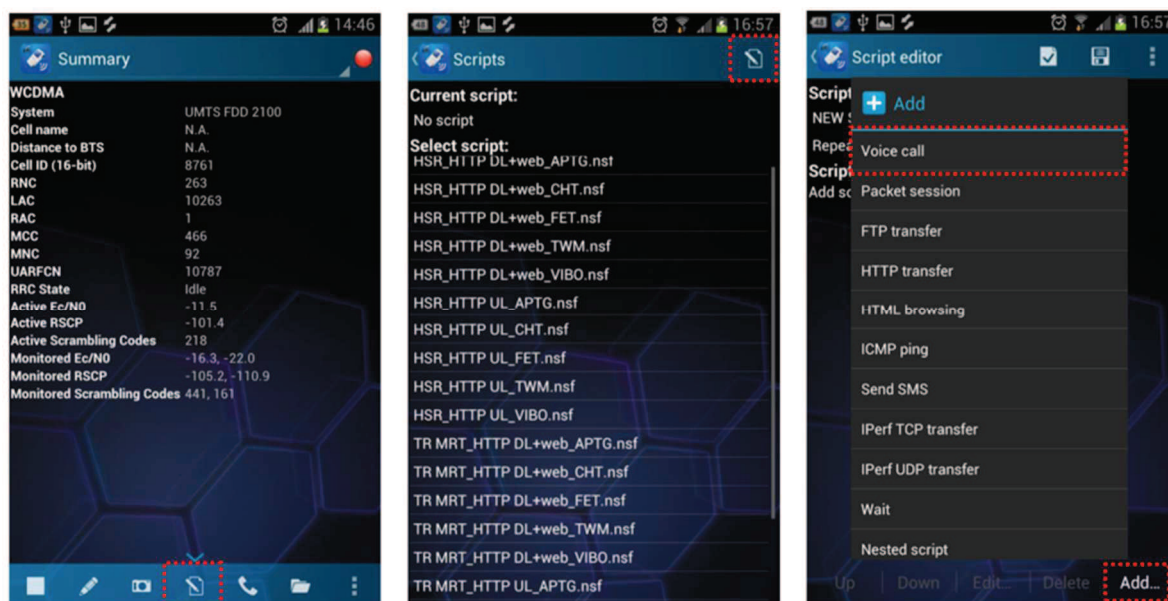


圖 6-42 工程手機檢測畫面範例

資料來源：本團隊整理

相較於單一 UE，通常多個 UE 的測試，難以透過同時操作多組工程手機的方式進行，因其複雜度相對較高，故此時就需要借助 UE 模擬器進行測試，如圖 6-43 所示，為了模擬實際通訊狀況使用不同獨立 UE 測試，每個 UE 均試圖個別與網路互動，因此整個通訊系統評估也會變得複雜。每個模擬的 UE 將各自產生獨立 3GPP LTE 協定層功能，以確保對於 LTE 手機的代表性，除了透過產生檢驗各項功能所需的詳細的診斷數據外，將進行信令的覆蓋，或蓄意傳輸損壞數據，以模擬異常情況，以測試系統響應與強健性，藉以驗證待測基站對於 3GPP 規範的符合性。

	UE 0	UE 1	UE 2	UE 3	UE 4	UE 5	UE 6	UE 7	UE 8	UE 9	UE 10	UE 11	UE 12	UE 13	UE 14	UE 15	UE 16	UE 17	UE 18	UE 19	UE 20	UE 21	UE 22	UE
4 (Generic)																								
Type	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Simula	Sim
4 (Simulated)																								
pure IMSI	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True	True
10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	10101	101
INC Length	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
length	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
process control para...	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
is control class	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
PLMN indication	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
PLMN use indicati...	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
i lists	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...	Click t...
asset User	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
USIM	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
PN Info	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
lists	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
rtication key	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
4 (Simulated: Fr...																								
pure Frequency sett...	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
ency Type	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
owlink Intra Frequ...	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
link Intra Frequency	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
link Intra Frequency	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
link Intra Frequency	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
ng Value	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False
4 (Simulated: M...																								
is Mitigation Algorithm	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False	False

圖 6-43 UE 模擬器大量使用者連線畫面範例

資料來源：signaltestinc.com

由於一般性檢測與分析除了 Uu 介面的信令外，另一個主要目標在於檢測待測基站負責定義待測基站和移動管理實體/服務開道器間控制訊息與資料封包的溝通傳遞的 S1 傳輸介面，以及待測基站之間互相連接溝通的 X2 傳輸介面，所支援的通訊協定，包含 SCTP 與 GTP 通訊協定。除了利用 IP 封包來封裝使用者平面與控制平面的訊息外，上面還會疊加其他不同的協定，以提供路由、完整性及機密性保護等相關的通訊機制。

在核心網路單元將透過對於基站與核心網路所有組成項目之間的通訊進行信令的行為分析檢測，如圖 6-44 所示，以確保所有進入進階資安檢測與分析階段之基站都能符合 3GPP 之規範，並且避免造成後續檢測過程，將不符合規範誤判為資安問題之狀況。

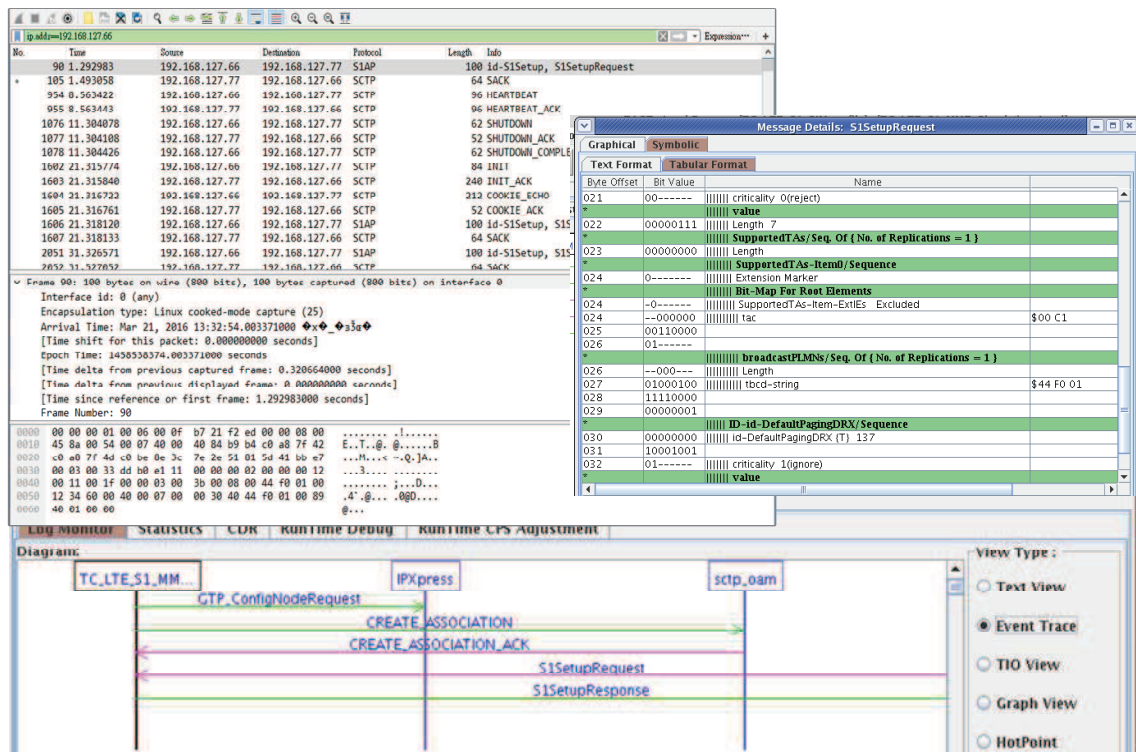


圖 6-44 核心網路信令交握畫面範例

資料來源：本團隊整理

二、進階資安功能項目與相關驗證程序說明

基站在處理通訊時的安全性，也需要對其資訊安全做進一步的評估，為確保檢測平臺能對待測基站進行完整的檢測與分析，本平臺參考了 Information Systems Audit and Control Association (簡稱 ICSA) 所提出的 LTE 資訊安全威脅與管理的切入點如圖 6-45 所示，進行審視與分析並考量實際應用情境之佈署，整合資訊安全與弱點評估之相關軟與硬體，對待測基站的資訊安全進行檢測程序，透過對應之檢測工具驗證範例畫面，依序說明各檢測程序中，提供可能之弱點與威脅。其中，本平臺對於虛線所框列與基站相關的威脅，進行檢測與分析，主要包含封包竊聽、攻擊的重新導向、中間人攻擊與阻斷式服務攻擊，以及其他可能因 UE、EPC 與 IMS 受攻擊後所連帶造成的威脅。

因此，為了能快速有效的識別待測基站在遭遇上述這些威脅時，可能造成的影響，本平臺在進階資安功能項目與相關驗證程序，將分別透過後續所介紹的靜態與動態分

析，以及對基站同時進行各種動態的主動與被動式行為分析，來加以識別待測基站可能存在的弱點，為監管單位與業者從資訊安全管理上以宏觀的角度，提供可行的參考與因應策略。

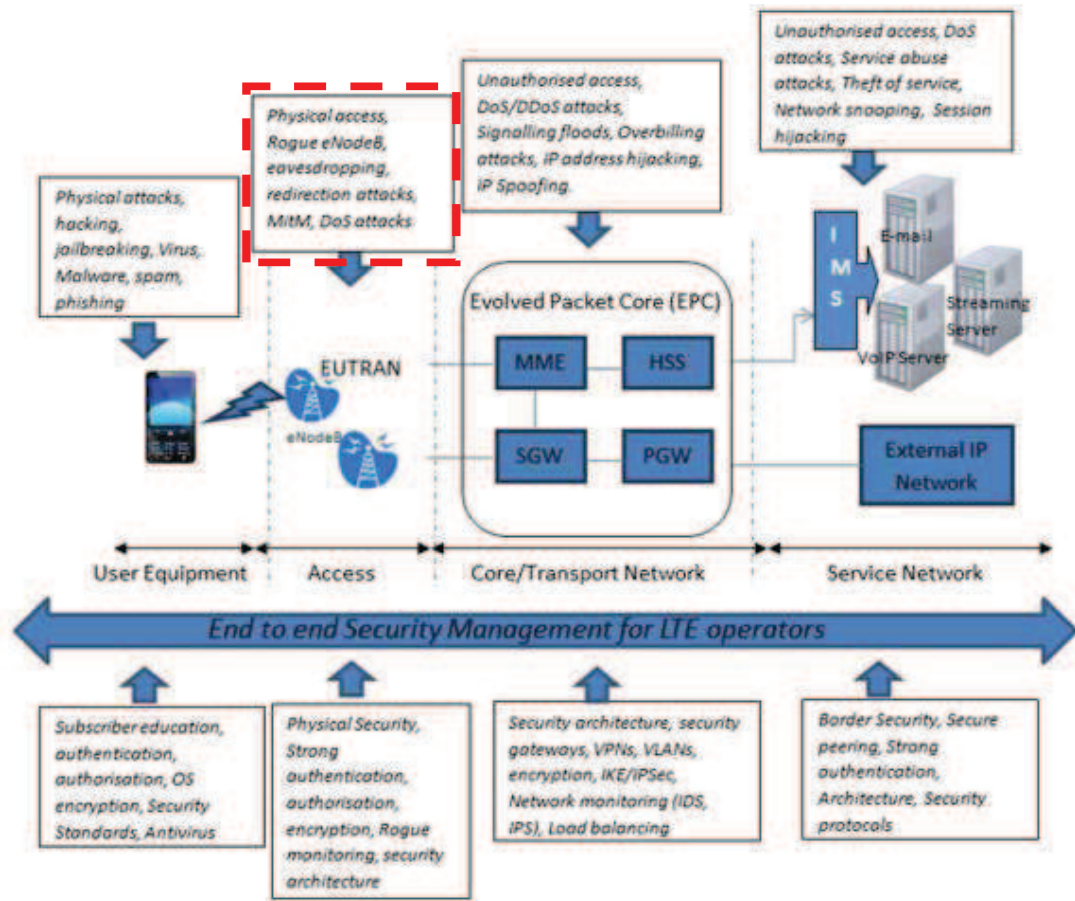


圖 6- 45 LTE 資訊安全威脅與管理的切入點

資料來源：isaca.org

1. 靜態程式碼掃描

為了識別基站軟體與韌體的資訊安全風險，除了透過一系列的弱點檢測與滲透測試工具，對標的物進行各種檢測與評估外，越來越多的企業和組織發現，保護軟體安全最有效的方式，是在軟體與韌體的開發週期就導入軟體安全保證(Software Security Assurance，簡稱 SSA)的主動式方法，以系統化的方式消除軟體中的安全弱點風險。軟體安全保證(SSA)採用在應用軟體開發階段就做到安全保護，而不是在軟體部署之後，因此本平臺亦規劃使用靜態掃描工具對待測基站提供服務的韌體進程式碼弱點

分析，由開發者的觀點評估可能造成的資訊安全弱點。

如圖 6-46 所示，靜態掃描確實有利於探測出基站軟體/軟體於設計之初造成後續的資訊安全威脅。在檢測過程中除廠商提供的程式碼外，亦可能透過逆向工程對於編譯後之程式碼進行檢測，將可有助於分析人員瞭解待測基站的運作邏輯，以及這樣的邏輯下可能產生的弱點，並在後續的動態測試過程中加以驗證。而此檢測項目建議將基於廠商所提交之自我宣告，並自主送驗基站軟體或韌體，以證實其設計符合我國相關法規之要求。

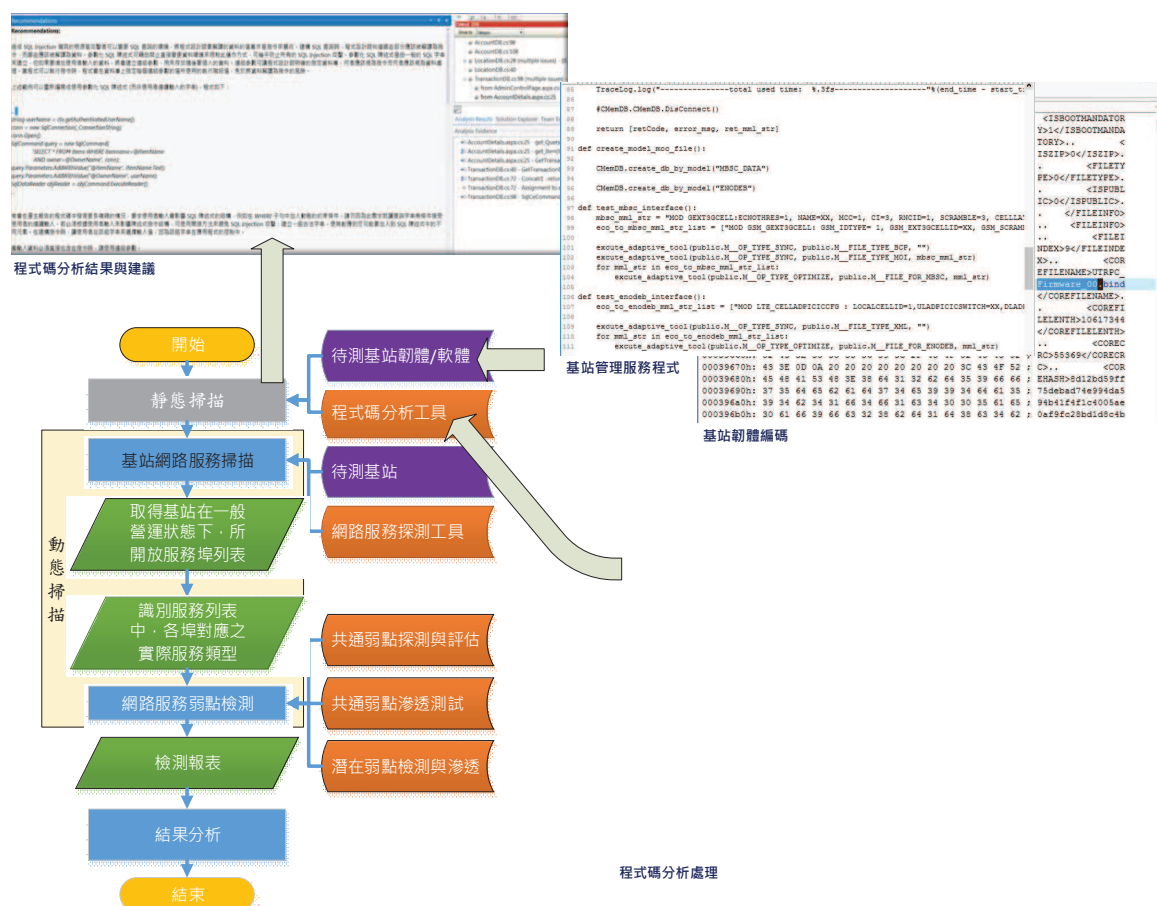


圖 6-46 基站軟體/軟體掃描畫面範例

資料來源：本團隊整理

2. 主動式基站服務弱點檢測與分析

在本平臺的待測的 LTE 網路與設備均已完整 IP 化，因此如圖 6-47 所示，掃描是攻擊者入侵目標最先所採取的主動式行為，藉由掃描取得一些有用的資訊，讓測試者

對欲檢測之基站可能提供的網路服務通訊埠，相關的服務種類與埠號之對應有基本的認識，如特定目標之 IP 位址、作業系統、網路及主機系統架構與主機上所執行的服務等。因此本平臺所設計的流程也依循這樣的方式，先搜尋基站上開啟了哪些通訊埠，並且進一步偵測出目標基站上所執行的作業系統類型及版本，最後分析出目標基站上正在執行或待命的網路服務，以及與目標基站 IP 位址之間的關係。藉由網路服務探測工具的操作，後續才針對特定的通訊弱點進行探測與分析，如此有效限縮分析的範圍，以得知哪些通訊埠最可成為被攻擊的目標；另一方面則可增加檢測的準確度，降低嘗試行為進行的次數。

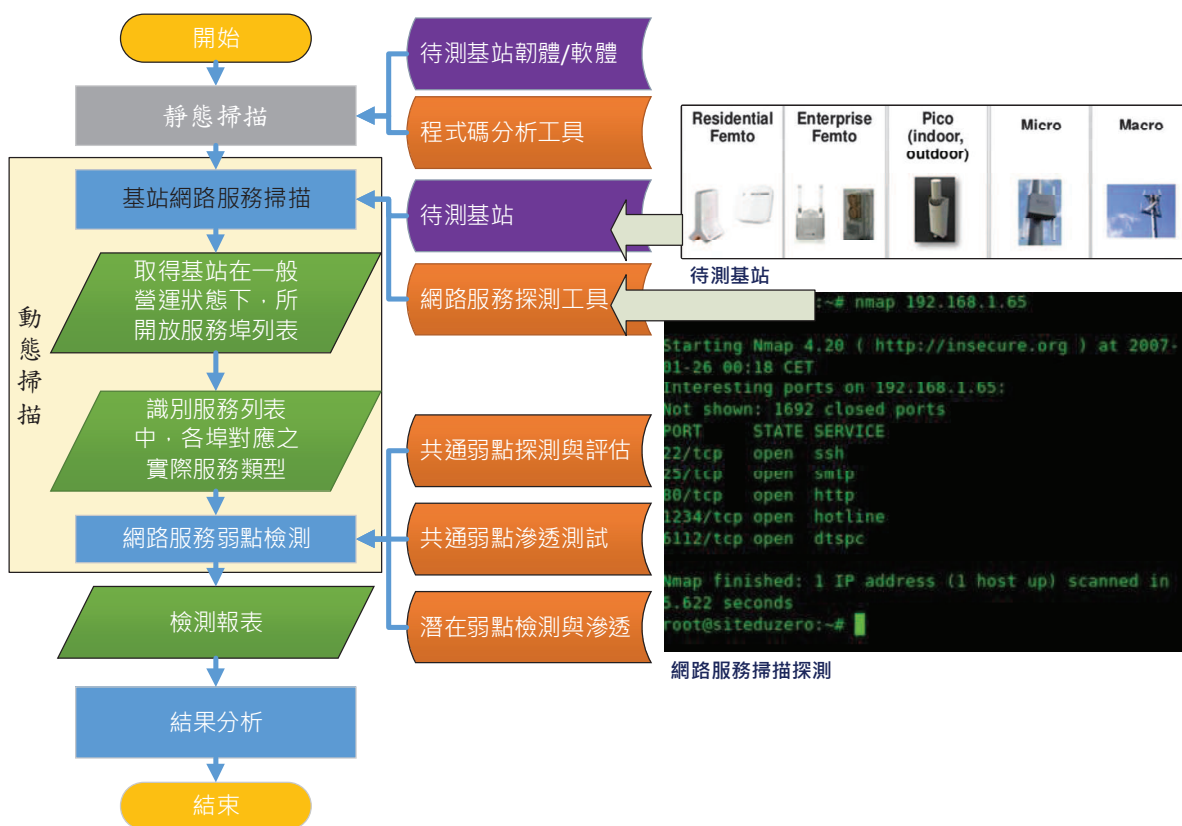


圖 6-47 基站服務掃描畫面範例

資料來源：本團隊整理

掃描大致分為 3 種類別，分別是首先是通訊埠端口掃描、網路架構掃描與弱點掃描。在完成通訊埠端口與網路架構掃描後，將進行基站的弱點掃描。此外針對探測後所發現的弱點，與國際公認的弱點資料庫，進行比對與分析風險等級，以確認該弱點將可能造成基站本身受到威脅程度，對於提供透過網頁提供管理設定的基站，本平臺

也採用網頁弱點檢測工具進行分析。利用共通弱點滲透測試工具對這些已被識別的弱點進行滲透測試，評估所這些被提列弱點的可被攻擊者進一步利用以取得基站控制權可能性，並加以分析可能造成資訊安全與資訊洩漏之危害程度。

完成基礎評估並識別弱點及威脅後，針對這些弱點與威脅列入後續的弱點資料庫外，透過潛在弱點檢測與滲透工具進一步分析，除既有已知已被國際弱點資料庫公告這些弱點外，是否存在其它尚未被公開(或發現)的潛在問題，例如:通訊協定實作不完整或程式對於例外攔截的定義不良等，而這些問題可能造成的威脅，也將在此階段進行分析評估。

圖 6-48 所示，在完成網路服務弱點檢測階段後，將可收集到對待測基站採取主動式檢測作業之詳細資訊與報表，並在檢視與分析判定後，匯整於最後的資料庫中，以提供參考與交換之用。

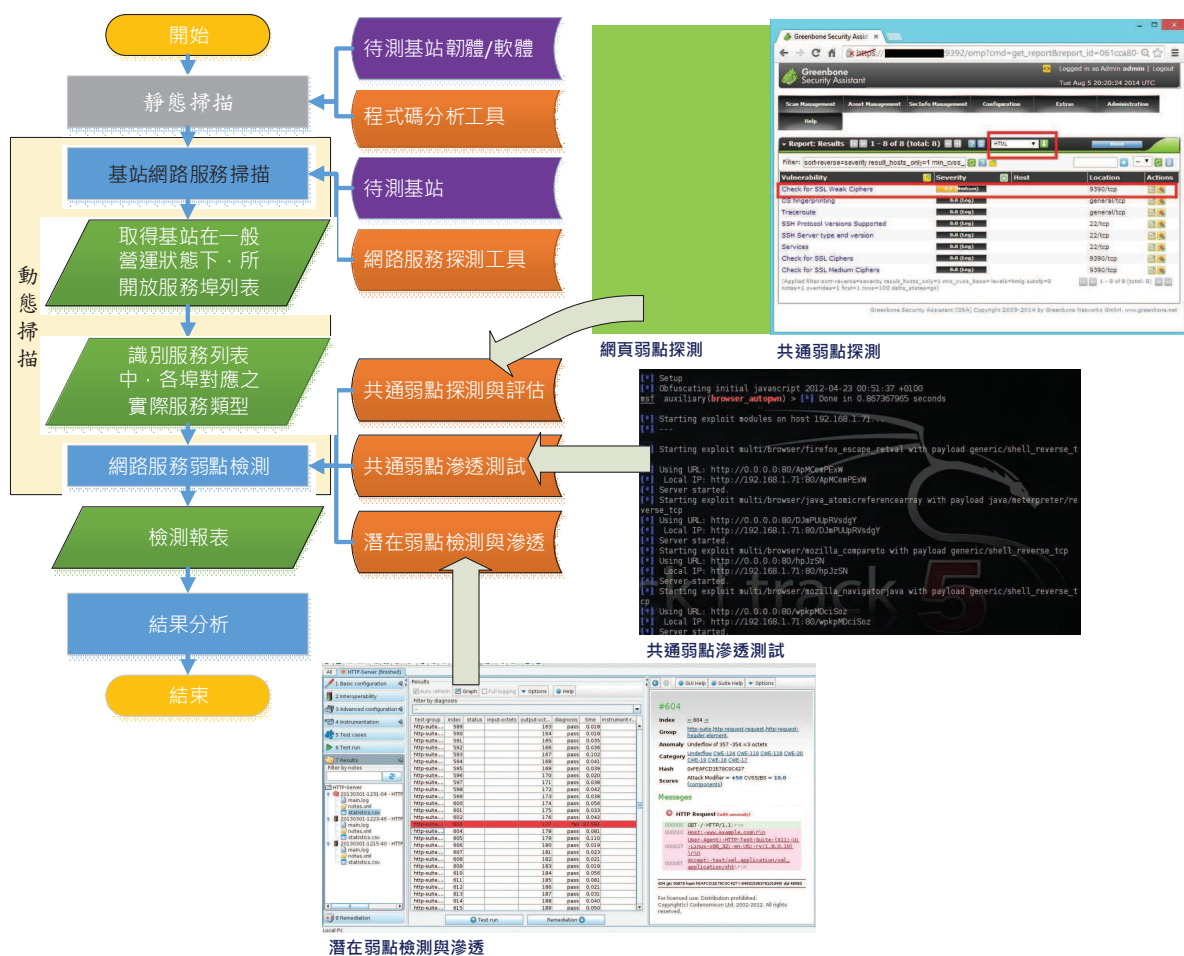


圖 6-48 網路服務弱點檢測畫面範例

資料來源：本團隊整理

3. 被動式基站連外行為檢測與分析

基站是國家通訊基礎建設，本團隊藉由設計的基站連外行為檢測機制，透過如圖 6-49 所示之動態介面清楚描述惡意之行為與傳遞路徑，以包圍式配置方式達到全面監測的目的並實作偵測機制，以對於一般性及進階資安功能檢測期間，可能觸發的各種可疑通訊行為加以攔截與分析，以務實與鉅細靡遺的檢測程序，進一步對基站的各種反應加以攔截與分析。此測項未來將由廠商先行提交自我宣告，敘述基站可能產生之自發性連外行為(例如校時)，並於測試階段查核其行為是否與宣告一致，並分析是否為符合國際上所定義之異常行為。

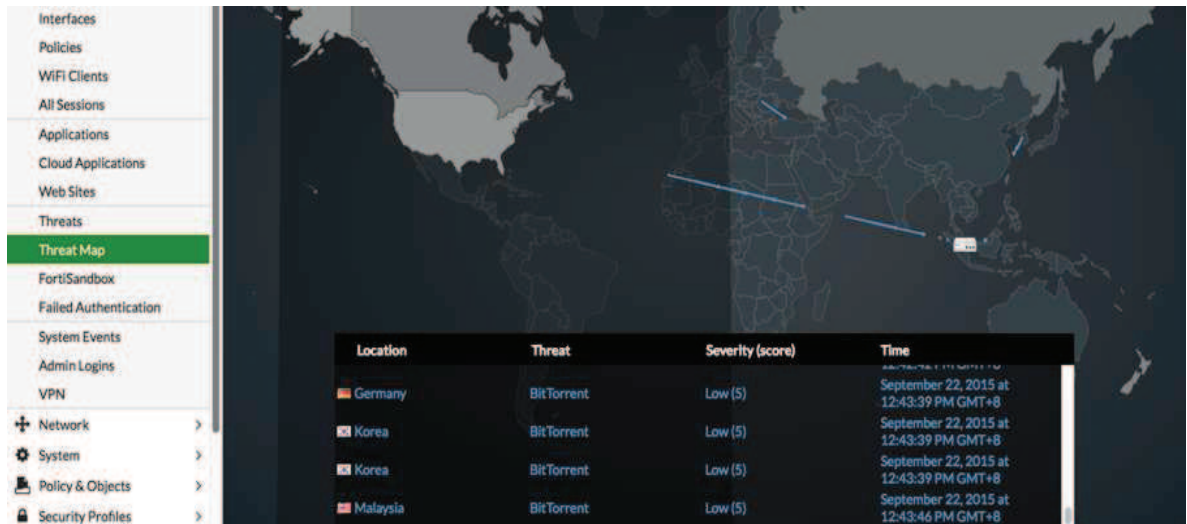


圖 6-49 動態惡意行為與傳遞路徑描述畫面範例

資料來源：fortinet.com

為了能快速且有效的過濾基站所發出的所有信令與資訊，規劃如圖 6-50 所示之偵測機制，結合具專門偵測惡意行為與軟體之特殊應用積體電路(Application-specific integrated circuit，簡稱 ASIC)的設計，能有效且快速的分析出各種國際上被定義之可能的威脅。

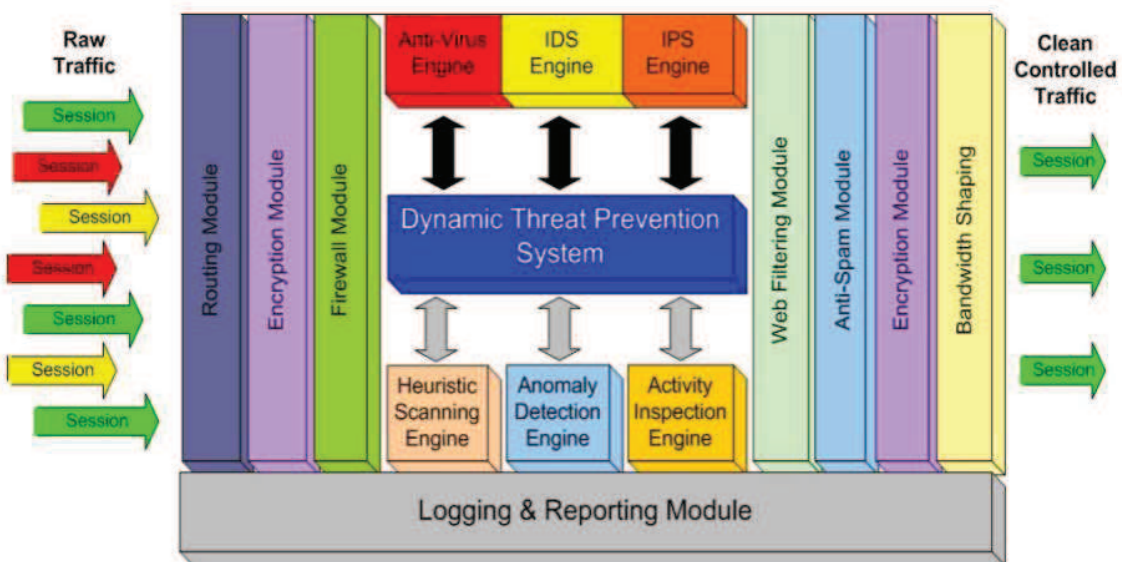


圖 6-50 已知惡意之行為與軟體偵測機制示意圖

資料來源：fortinet.com

在此架構之上，具備四組行為加速(Accelerated Behavior)和內容分析系統技術引擎的 ASIC 晶片(共包含 Signature scanning engine、Crypto acceleration engine、Firewall processing engine、Flow management engine)，讓基站網路在全速運轉下，能提供檢測人員即時的分析資訊與威脅示警，如圖 6-51 所示。

#	日期/時間	服務	Source	檔案名稱	Virus/Botnet	用戶	詳細資料	採取行動
1	06-16 15:10	HTTP	10.50.65.17	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
2	06-16 15:10	HTTP	10.50.65.17	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
3	06-16 15:03	HTTP	10.50.65.17	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
4	06-07 16:52	HTTP	10.50.65.6	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
5	06-07 16:52	HTTP	10.50.65.6	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
6	05-16 11:50	HTTP	10.50.65.6	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
7	05-16 11:50	HTTP	10.50.65.6	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
8	04-24 08:19	HTTP	10.50.65.13	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
9	04-10 16:18	HTTP	10.50.65.13	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
10	04-10 16:17	HTTP	10.50.65.13	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked
11	2015-12-23	HTTP	10.50.65.7	AutoPCBackup.a251a499b3d640cb8f0fa6cc94b351fe.exe	Riskware/MyWebSearch		host: 23.76.204.16	blocked
12	2015-11-26	HTTP	10.50.65.17	statistic.js	JS/Badarc.QVCitr		host: 218.251.112.155	blocked

#	1	Destination	218.251.112.155
FortiGuard沙箱校驗	2955ca4b803f41c03265b1554b1a098fe3b8bb285e34f5d71c314b0d3a98204	Source	10.50.65.17
Threat Level	critical	Threat Score	50
URL	http://218.251.112.155/statistic.js	Virus ID	4560308
Virus/Botnet	JS/Badarc.QVCitr	事件類型	infected
代理	Mozilla/5.0	來源埠	65533
偵測類型	Virus	參考資料	http://www.fortinet.com/ve?vn=JS%2FBadarc.QVC%21tr
子型式	virus	序號	3640226442
採取行動	blocked	提交到FortiGuard沙盒	false
方向	incoming	日期/時間	2017/6/16 下午3:10:54
日期/時間	06-16 15:10	服務	HTTP
檔案名稱	statistic.js	被重跳過	No-skip
目的地	80	類別	病毒
測試協定	6	虛假防火牆	root

#	日期/時間	威脅程度	Source	測試協定	用戶	採取行動	計數	攻擊名稱
1	15:19:35	critical	173.208.253.147	tcp		dropped		MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution
2	15:03:12	critical	182.110.118.170	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
3	14:39:04	critical	216.218.206.66	tcp		dropped		Backdoor.DoublePulsar
4	13:40:57	critical	103.82.41.129	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
5	12:14:32	critical	52.207.232.106	tcp		dropped		MS.IIS.WebDAV.PROPFIND.ScStoragePathFromUrl.Buffer.Overflow
6	12:10:59	critical	223.24.163.214	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
7	10:24:10	critical	203.109.101.59	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
8	09:46:57	critical	112.215.65.40	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
9	09:43:13	critical	183.91.12.156	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
10	09:37:13	critical	173.208.253.147	tcp		dropped		MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution
11	09:37:13	critical	173.208.253.147	tcp		dropped		MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution
12	09:07:24	critical	119.90.136.44	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
13	09:04:33	critical	134.249.158.83	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
14	09:03:12	critical	27.72.58.133	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
15	06:22:55	critical	200.109.102.57	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
16	05:29:08	critical	183.82.112.38	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure
17	03:12:06	critical	14.142.181.179	tcp		dropped		MS.SMB.Server.Trans.Peek.Data.Information.Disclosure

Source	173.208.253.147	Threat Level	critical
Threat Score	50	is_archived	0
事件序號No.	1688245695	事件類型	signature
來源埠	51853	協定號碼	6
參考資料	http://www.fortinet.com/ids/VID43796	威脅程度	critical
子型式	ips	序號	519560514
採取行動	dropped	攻擊名稱	MS.SMB.Server.SMB1.Trans2.Secondary.Handling.Code.Execution
攻擊識別碼	43796	方向	0
日期/時間	2017/8/23 下午3:19:35	日期/時間	15:19:35
服務	SMB	目的地	445

圖 6-51 已知惡意之行為與軟體偵測警示資訊

資料來源：本團隊整理

在分析已知惡意行為與軟體後，待測基地的行為將透過沙箱系統，對其可能衍生

的進階持續性滲透攻擊行為做更深入分析，相關偵測機制如圖 6-52 所示。



圖 6-52 進階持續性滲透攻擊行為偵測機制示意圖

資料來源：fireeye.com

平臺透過持續監測與分析攻擊行為的生命週期，以找出「既低調且緩慢」的攻擊行動，如圖 6-53 所示。對於橫跨多個威脅媒介的惡意軟體通訊，包含可能存在的零時差弱點、試圖避開傳統防禦隱藏在網際網路流量中的其他規避性攻擊，以及各種試圖尋找具有風險的系統與敏感資料之行為，進行深層的監測與分析。

10.100.11.59

6

4

2

0

Exploit.MultiFPayload_udfa

06/16/17 10:36:38

10-100-11-59.victim.crossfire

IPS

Malicious Capabilities Observed in the VM

Malicious Behavior: Yes

OS Change Summary

Malware detected

Malware	Severity	Total	Infections	Callbacks	Blocked	Botnets	Last CnC Server	Last Location	First Seen	Last Seen	Ports Used	Protocols
Exploit.MultiFlowPayload_udfa	*****	1	1	0	0	0			06/16/17 10:36:38	06/16/17 10:36:38	80	TCP
Trojan.Rebhip	*****	2	1	1	0	1	10.100.201.139		06/16/17 10:31:01	06/16/17 10:36:38	80, 81	TCP
SWF.MalAPILoadPayload	*****	2	2	0	0	0			06/16/17 10:34:07	06/16/17 10:36:17	80	
Backdoor.APT.SpyNet	*****	1	0	1	0	1	10.100.201.139		06/16/17 10:31:01	06/16/17 10:31:01	81	TCP

IPS Details

Signature Name	First Seen	Last Seen	Categories	Protocol	Reference
Adobe Flash Player Nellymoser DataSize Heap Buffer Overflow	06/16/17 10:30:49	06/16/17 10:30:49	exploit	http	CVE-2015-3113

Infection URLs

Initial Infection URL	# Visits	Total URLs	First URL at	Last URL at
10-100-201-139.attacker.crossfire/activity/	2	7	06/16/17 10:34:09	06/16/17 10:36:18

Malware Binaries

Md5sum	Filetype	Protocol	Encoding	Last analysis time	# Occurrences
c1a6afdc77b556284d2d4f73f1f1d79	exe	TCP (80)		06/16/17 10:36:38	2

Acknowledge the infections and callbacks above for the host at 10.100.11.59:

圖 6-53 混合式進階持續性滲透攻擊分析畫面範例

資料來源：本團隊整理

偵測或阻擋攻擊事件時提出告警時，檢測人員可透過管理介面檢視攻擊事件詳盡的資訊，如圖 6-54 所示，包括惡意程式在沙箱中的行為以及收集沙箱中的網路活動封包，以供資安分析人員瞭解攻擊歷程及手法，提供後續研擬相關的防禦措施，相關檢測程序如圖 6-55 所示。

Alerts

(as of 06/16/17 02:45:57 UTC)

Print PDF

Page: 1 of 2 prev 1 2 next | Hosts Alerts Callback Activity | Results per page: 20 | Duration From: 1 month ago | Going Back: 24 hours | Show ACK events: | Show Critical Detections: | Total: 26

ShowHide Filters

Type	Id	FT	Malware	Severity	Time (UTC)	Source IP	Target IP	URL/Md5sum	Location	SC Version	Badges
Malware Object	56537	zip	Malware.archive	*****	05/17/17 16:12:42	10.100.8.219	166.78.135.34	ee0c18be233b53777281f7d9a60c2d6		601.190	
Malware Object	56532	exe	Trojan.Rebhip	*****	05/17/17 15:18:06	10.100.9.150	10.100.201.66	4d023ccf29183601bf08a0bc8200b421		601.188	
Web Infection	21147		Trojan.Rebhip	*****	05/17/17 15:17:51	10.100.9.150		10-100-201-66.attacker.crossfire/activity/		601.188	
Malware Callback	92188		Backdoor.APT.SpyNet	*****	05/17/17 15:12:34	10.100.9.150	10.100.201.66			601.188	IPS
Malware Callback	92189		Trojan.Rebhip	*****	05/17/17 15:12:34	10.100.9.150	10.100.201.66			601.188	IPS
Malware Callback	92187		Trojan.Citadel	*****	05/17/17 12:46:43	10.100.9.114	213.186.33.19	http://bsmax.fr/misc/.Khjh2M@/.Khjh2M@//menu.php	FR	601.182	
Malware Object	56529	exe	Trojan.Rebhip	*****	05/17/17 11:58:29	10.100.9.134	10.100.201.65	7335f54688636021179b4458df96078b		601.182	
Web Infection	21143		Trojan.Rebhip	*****	05/17/17 11:58:14	10.100.9.134		10-100-201-65.attacker.crossfire/activity/		601.182	
Malware Callback	92175		Backdoor.APT.SpyNet	*****	05/17/17 11:52:55	10.100.9.134	10.100.201.65			601.180	IPS
Malware Callback	92174		Trojan.Rebhip	*****	05/17/17 11:52:55	10.100.9.134	10.100.201.65			601.180	IPS
Malware Object	56527	exe	Trojan.Rebhip	*****	05/17/17 11:28:54	10.100.9.133	10.100.201.61	cb1e3435ab18e6f3ac331915f475709		601.180	
Web Infection	21140		Trojan.Rebhip	*****	05/17/17 11:28:44	10.100.9.133		10-100-201-61.attacker.crossfire/activity/		601.180	
Malware Callback	92162		Backdoor.APT.SpyNet	*****	05/17/17 11:23:28	10.100.9.133	10.100.201.61			601.180	IPS

圖 6-54 惡意行為偵知紀錄畫面範例

資料來源：本團隊整理



圖 6-55 待測基站連外行為檢測與分析畫面範例

資料來源：本團隊整理

本平臺提供待測基站進階測試後續流程，將可能的弱點逐一定義並檢視，做適當的分析與研擬因應策略，具有公正性、客觀性與有效性，適合行動寬頻基站的資訊安全弱點之檢測，並提供詳細的資訊，以配合有相關需求之機關單位做為參考與行動之依據。

第三節 小結

由於通訊領域逐步邁入 IP 化的趨勢，導致通訊領域之裝置可能遭受電腦資訊領域相同的威脅，而這些威脅可能來自於基站本身引用或沿用原本電腦資訊領域所使用的元件或方案所致，未來業者再進一步使用 SDN 與 NFV 建構核心網路的狀況下，複雜的環境與基站可能存在的弱點交互影響之下，或許將進一步導致國家基礎建設遭遇

前所未有的威脅。

因此，本著前瞻的思維及設計理念，行動寬頻基站資安檢測平臺的構想即由此應運而生，參考基站基安檢測環境計畫(第 1 期)研究成果，從基本規劃框架著手落實前期的概念性平臺設計，進一步考量透過工程手機與用戶端模擬器連接待測基站的行為，以及三種基礎核心網路架構對待測基站連接所造成的影響，透過彼此交叉驗證以瞭解基站處理各信令的堅實性、可用性與通訊標準之相容性，藉此讓檢測人員瞭解並標示資安測試過程可能造成的不確定性因素，以避免基站在實作通訊堆疊方面不完整，進而造成誤判影響資安檢測的公正性。

在完成基礎檢測後，平臺將可透過導入一系列先進的檢測工具，從主動式的已知弱點掃描及滲透測試、各種駭客攻擊手法及程式，進而到未知弱點的探測與利用作為滲透基站的可行性評估等方式，對待測基站進行各種嚴謹的測試活動，以確認基站在複雜的營運環境下，依然能達到保障用戶資訊安全的能力。

而平臺在基礎檢測與資安檢測期間，全程透過一系列被動式的惡意行為感測偵知系統的嚴密監控，以觀察並分析基站在受測期間的一舉一動，一方面確認基站本身無惡意行為，導致用戶資訊、通訊內容、加密金鑰或關鍵安全參數洩漏；另一方面則識別基站是否藉由本身的相關更新機制，有意或無意的帶入惡意程式導致基礎通訊設施之間遭受感染或滲透。

本團隊也利用此平臺建立一系列的檢測項目以及測試組套，透過關聯式資料庫進一步彙整檢測結果後，擬定相關測試標準並據以提出適用於我國之檢測草案，以利主管機關在研擬政策方針時，提供具公信力且有紮實理論與技術基礎的參考依據，能為國家資訊基礎建設安全作嚴謹的把關。

第七章、行動寬頻基站資安檢測規範草案建議

本計畫研擬之檢測規範草案旨在提供基站安全功能驗證之基礎，以作為執行基站資安檢測的參考依據，針對 3GPP 組織對於基站相關標準之安全需求進行探討，歸納出檢測項目，以配合檢測需求提出行動寬頻基站資安檢測平臺檢測環境建議。

本計畫進行至期中時程後，2017 年 9 月 3GPP 釋出基站資安檢測標準 33.216 文件 R15 的版本，本計畫於 2017 年 12 月取得該標準，適時參考該文件要求，擬訂檢測項目，執行實測驗證，以便檢測規範草案能納入最新的國際標準，由於 3GPP 標準文件產出至設備商開發符合該標準要求之電信產品時程需 1 至 2 年不等，基於研究之全面性需求，儘可能將所有安全要求納入草案內。草案之檢測項目初步已與設備商與電信業者進行討論，檢視可能面臨因連網的環境所引發的資安問題，後續正式推行，建議仍宜逐項考慮國內行動寬頻網路佈建狀況與設備版別，在適用性的基礎上執行資安檢測，以建立我國之行動寬頻網路檢測能量，如圖 7-1 所示。



圖 7-1 檢測規範草案擬定流程

資料來源：本團隊整理

為落實草案之訂定與執行，本研究依檢測環境、檢測項目要求、檢測結果及合格判定標準與檢測作業程序四大主軸，展開相關檢測之程序，以便評估基站系統安全檢測之環節，各內容與架構說明如 7-2 所示。



圖 7-2 基站資安檢測規範草案架構

資料來源：本團隊整理

第一節 適用範圍

本規範草案所適用行動寬頻網路基站，係指國家通訊傳播委員會行動寬頻基地臺射頻設備技術規範³⁷²定義之基地臺(eNodeB)、微型基地臺、微微細胞接取點及毫微微細胞接取點。檢測種類區分為兩類 eNodeB(基地臺)及 HeNB (微型基地臺、微微細胞接取點及毫微微細胞接取點) 兩類。檢測規範草案旨在確保 4G 行動寬頻網路資訊安全，透過研析國際相關規範 3GPP TS33.320 以及 TS33.216 擬定檢測範圍及檢測項目，依據(1)資料保護、(2)應用程式安全、(3)通訊安全、(4)身分鑑別與授權安全、(5)作業系統安全、(6)實體防護六項安全構面，訂定行動寬頻基站產品安全技術要求。本規範檢測項目如表 7-1。

³⁷² 國家通訊傳播委員會，”行動寬頻基地臺射頻設備技術規範”，2015/11/24.

表 7-1 檢測範圍

安全構面	檢測 編碼	測試項目	基地臺	微型基地臺 微微細胞接取點 毫微微細胞接取點
資料保護	1.1	敏感性資料外洩防止(系統功能外洩)	√	√
	1.2	敏感性資料外洩防止(軟體外洩)		
	1.3	敏感性資料儲存保護		
	1.4	憑證唯一性	不適用	
應用程式安全	2.1	網站伺服器安全	√	√
通訊安全	3.1	系統使用協定或服務安全	√	√
	3.2	系統與對外之網路傳輸安全		
	3.3	控制層資料機密性保護		
	3.4	控制層資料完整性保護		
	3.5	存取層完整性演算法選擇		
	3.6	無線資源控制訊息完整性保護		
	3.7	基站金鑰更新		
	3.8	存取層安全模式指令程序		
	3.9	X2 交遞中降階攻擊防範		
	3.10	存取層演算法選擇		
身分鑑別與授權安全	4.1	系統功能存取控制	√	√
	4.2	身分鑑別有效性		
	4.3	系統預設帳號管控		
	4.4	密碼複雜度		
	4.5	通行碼變更機制		
	4.6	暴力及字典攻擊防護		
	4.7	通行碼顯示遮罩		
	4.8	通行碼認證錯誤處理機制		
	4.9	授權策略		

安全構面	檢測 編碼	測試項目	基地臺	微型基地臺 微微細胞接取點 毫微微細胞接取點
	4.10	角色存取控制		
	4.11	登出功能		
	4.12	操作逾時功能		
	4.13	登入權限控管		
	4.14	檔案系統存取權限控管		
作業系統安全	5.1	日誌檔敏感性資料外洩防止	√	√
	5.2	安全開機		
	5.3	軟體完整性		
	5.4	安全事件記錄功能		
	5.5	安全事件紀錄備存		
	5.6	安全事件紀錄存取控制		
	5.7	高權限系統功能存取控制		
	5.8	自動播放功能禁用		
	5.9	作業系統及網路服務安全		
實體防護	6.1	家用基站防拆保護	不適用	√
	6.2	實體介面安全管控		
	6.3	硬體憑證設計		

資料來源：本團隊整理

第二節 檢測環境建議

檢測環境旨在訂定基站資安檢測環境，將依據實現檢測作業之因素提出規劃建議，相關說明如下。

1. 檢測環境架構

說明與基站資安檢測相關的網路架構示意，包括測試元件與設備與檢測工具間的相對關係。

2. 設備

係指基站資安檢測所需之硬體設備，例如基站、測試主機、模擬器、測試終端等。

3. 工具

係指驗證安全需求之工具，例如協定檢測工具、滲透測試工具等。

4. 人員

係指基站測試人員、開發人員與資安檢測人員，同時說明人員須具備之專業知識與技能。

一、 檢測環境

本規範之檢測環境係基於 3GPP 所定義 4G LTE 網路架構，依檢測項目需求，連接相關檢測設備及工具進行檢測，在檢測的過程中，最大的困難點在於確保核心網路單元支援不同廠牌或系統之基站的可靠度以及穩定度，必須藉由完善的組態配置及驗證測試技術，才能維持檢測的完整性以及有效性，本研究依據行動寬頻網路元件屬性，區分用戶端裝置單元、核心網路單元及檢測設備及工具單元，完整的檢測環境架構如圖 7-3 所示。

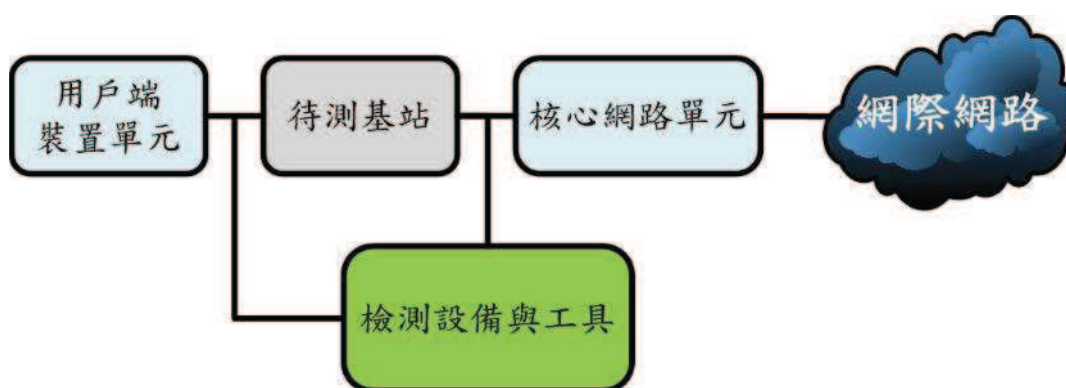


圖 7-3 檢測環境示意圖

資料來源：本團隊整理

二、 檢測設備與工具及人員要求

(一) 檢測設備與工具

由於行動寬頻網路的重要性和複雜性，使得控制信令與用戶資訊在不同單元間進行傳遞以便實現良好的通訊功能，在測試環境，通過其不同的測試項目，可以準確反映待測物於各測試條件下運作的表現。相關的功能要求說明如下：

1. 用戶端裝置、核心網路單元可使用商用設備與模擬器；模擬器須具備符合 3GPP LTE 通訊規範與本檢測規範要求項目。檢測單位應提供使用設備與模擬器功能之合理證據，證明其功能性符合本檢測規範描述的檢測要求。
2. 受測基站應符合 3GPP LTE 通訊規範。
3. 檢測工具應使用商業軟體(Commercial off the Shelf, COTS)和免費開放原始碼軟體(Free and open source software, FOSS)工具進行測試，需要具有相當的功能品質保證，確保檢測工具提供之合理證據，證明其功能性符合本檢測規範草案描述的檢測要求。

各網路單元的目的與功能與可運用及整合的設備綜整如表 7-2 說明。

表 7-2 網路單元與檢測設備一覽表

對應功能 元件名稱	目的與功能說明	可運用及整合的設備
用戶端裝置單元	使用者行為模擬，以檢測基站之符合性與功能性為主，並進一步模擬大量負載與變因控制對基站進行檢測。	• 工程手機 • 用戶端模擬器
受測基站	以介面、信令與通道特性為受測基礎之基站，對其施行資安弱點檢測。	• 符合 LTE 通訊規範之基站

對應功能 元件名稱	目的與功能說明	可運用及整合的設備
核心網路單元	核心網路行為模擬，作為基站與用戶端裝置之行動性、政策管理和安全性等功能之檢測使用。	• 核心網路模擬器 • 實際核心網路 • 虛擬化核心網路
檢測設備與工具	惡意/攻擊行為模擬，針對受測基站進行各式弱點掃描與探測。	• 程式碼分析工具 • 網頁弱點分析工具 • 通用弱點分析工具 • 滲透測試工具 • 未知弱點檢測工具

資料來源：本團隊整理

(二) 檢測人員要求

為建立符合主管機關公認之基站資安檢測人員資格，檢測人員應具備資安測試評估實務經驗達 2 年以上，且至少應具備下列任一有效之資訊安全相關證照：

1. 道德駭客認證(Certified Ethical Hacker, CEH)或國際網路資安認證(CompTIA Security+)有效之資訊安全相關專業證照。
2. 資訊系統安全專家證照(Certified Information Systems Security Professional, CISSP)
3. 資安分析專家證照(EC-Council Certified Security Analyst, ECSA)
4. 滲透測試專家證照(GIAC Penetration Tester, GPEN)

第三節 用語釋義

1. 加密(Encryption)

利用數學演算法處理電子資料，使資料不會以原來的形式呈現，達到保密的目的，並且可透過解密方式取得加密資料原文內容。

2. 敏感性資料(Sensitive Data)

用於認證的資料或直接識別或間接識別用戶的資料，例如用戶裝置的用戶名稱、

密碼、PIN、加密金鑰、IMSI、IMEI、MSISDNs 或 IP 位址，以及系統文件，例如：韌體檔案、更新程式、驅動程式或核心模組。

3. 安全事件日誌

專門記錄安全事件發生之日誌檔，安全事件包括系統管理者存取紀錄。

4. 營運、管理與維護(Operations, Administration, and Maintenance, OAM)

電信網路的管理模式之一，提供適當工具予電信營運業者對網路通訊設備進行本地與遠端管理作業。

5. 圖形用戶介面(Graphical User Interface, GUI)

以圖形方式顯示的電腦操作用戶介面。

6. 安全模式指令(Security Mode Command, SMC)

核心網路與基站間建立安全連線的訊息，例如在訊息中攜帶金鑰演算法資訊。

7. 安全模式完成(Security Mode Complete)

該訊息用於確認安全模式指令的成功完成。

第四節 檢測項目與要求

本研究依據行動寬頻網路之資安威脅、3GPP 現有安全機制及相關之資安檢測技術研究結果，深入與基站(eNodeB/HeNB)系統本身及其密切相關之空中介面與核心網路-MME 進行研究，以研擬基站資安檢測項目，建立基站網路通訊設備之安全機制，作為本計畫基站檢測之參考，擬訂六個安全防護面向，分別為資料保護、應用程式安全、通訊安全、身分鑑別與授權、作業系統安全、實體防護，考量不同面向可能面臨的資訊安全風險。

本規範草案之測試項目及參考資料來源整理於下表 7-3，其中通訊安全構面 3.3~3.10 的測試項目係參考 3GPP TS33.216，其餘資料保護、應用程式安全、通訊安全(3.1~3.2)、身分鑑別與授權安全、作業系統及實體防護等安全構面之測試項目則參考

3GPP TS33.117、OWASP IoT Top 10 及 3GPP TR33.820 的安全要求，以滿足更廣泛的機密性、完整性與可用性的安全要求，將安全風險進一步降低，得以確保基站安全。

由於 TS33.216 基站安全保證規範為 2017 年底最新公告之標準初稿，有些項目無具體測試步驟，僅連結至 TS33.117，故本檢測規範草案測試項目係基於 3GPP TS 33.117- Catalogue of general security assurance requirements 作為研究基礎，並跟對該標準之測試項目逐項評估與測試後發現：

1. 3GPP 標準部分測試項目是驗證產品在設計階段就納入安全考量，如作業系統層級、軟體服務運行於記憶體中程序(process)是否使用最高權限系統帳號執行、網路封包控管過濾的指令層級與組態檔案內的參數設定，這些並非購置設備的電信業者端的技術與維運人員或本計畫研究範圍內可以掌握。
2. 設備製造商已將許多安全配置細節包裝成其產品專利之操作介面，以因應行動通訊網路環境下面臨的各種突發狀況，讓電信業者的維運人員可以快速操作使用與調整，由於本計畫之測試工具基於經費限制下，無法涵蓋各廠商專利的網管功能，因此本團隊經評估後，將最多可執行之安全測試項目予以納入草案範圍內。
3. 於座談會中電信業者或設備商已明確表示，目前基站的設備版本為 R12 或 R13，要符合最新的 3GPP 安全標準(TS33.216)至少需 R14 以後的版本，目前設備研發尚需 1 至 2 年的準備期，才会有對應標準的產品上市。

基於上述原因，在測試過程中發現 3GPP TS33.216 及 TS33.117 許多測試項目內容要求都必須由基站製造廠商提供更進一步的資訊才可完成測試，因此，本計畫視實際現況的可執行性與適用性而整理出本檢測規範草案之測試項目如下。

表 7-3 檢測項目及參考來源一覽表

安全構面	檢測編碼	測試項目	參考來源
資料保護	1.1	敏感性資料外洩防止(系統功能外洩)	3GPP TS 33.117 – 4.2.3.2.2
	1.2	敏感性資料外洩防止(韌體外洩)	OWASP IoT Top Ten – I9
	1.3	敏感性資料儲存保護	3GPP TS 33.117 - 4.2.3.2.3
	1.4	憑證唯一性	3GPP TR 33.820 6.1(19)
應用程式安全	2.1	網站伺服器安全	3GPP TS 33.117 – 4.3.4

安全構面	檢測編碼	測試項目	參考來源
通訊安全	3.1	系統使用協定或服務安全	3GPP TS 33.117 – 4.3.2.1
	3.2	系統與對外之網路傳輸安全	3GPP TS 33.117 – 4.2.3.2.4
	3.3	控制層資料機密性保護	3GPP TS 33.216 – 4.2.2.1.1
	3.4	控制層資料完整性保護	3GPP TS 33.216 – 4.2.2.1.2
	3.5	存取層完整性演算法選擇	3GPP TS 33.216 – 4.2.2.1.5
	3.6	無線資源控制訊息完整性保護	3GPP TS 33.216 – 4.2.2.1.6
	3.7	基站金鑰更新	3GPP TS 33.216 – 4.2.2.1.8
	3.8	存取層安全模式指令程序	3GPP TS 33.216 – 4.2.2.1.9
	3.9	X2 交遞中降階攻擊防範	3GPP TS 33.216 – 4.2.2.1.10
	3.10	存取層演算法選擇	3GPP TS 33.216 – 4.2.2.1.11
身分鑑別與授權安全	4.1	系統功能存取控制	3GPP TS 33.117 – 4.2.3.4.1.1
	4.2	身分鑑別有效性	3GPP TS 33.117 – 4.2.3.4.2.1
	4.3	系統預設帳號管控	3GPP TS 33.117 – 4.2.3.4.2.2
	4.4	密碼複雜度	3GPP TS 33.117 – 4.2.3.4.3.1
	4.5	通行碼變更機制	3GPP TS 33.117 – 4.2.3.4.3.2
	4.6	暴力及字典攻擊防護	3GPP TS 33.117 – 4.2.3.4.3.3
	4.7	通行碼顯示遮罩	3GPP TS 33.117 – 4.2.3.4.3.4
	4.8	通行碼認證錯誤處理機制	3GPP TS 33.117 – 4.2.3.4.5
	4.9	授權策略	3GPP TS 33.117 – 4.2.3.4.6.1
	4.10	角色存取控制	3GPP TS 33.117 – 4.2.3.4.6.2
	4.11	登出功能	3GPP TS 33.117 – 4.2.3.5.1
	4.12	操作逾時功能	3GPP TS 33.117 – 4.2.3.5.2
	4.13	登入權限控管	3GPP TS 33.117 – 4.3.2.6
	4.14	檔案系統存取權限控管	3GPP TS 33.117 – 4.3.2.7
作業系統安全	5.1	日誌檔敏感性資料外洩防止	3GPP TS 33.117 – 4.2.3.2.5
	5.2	安全開機	3GPP TS 33.117 – 4.2.3.3.2
	5.3	軟體完整性	3GPP TS 33.117 – 4.2.3.3.5
	5.4	安全事件記錄功能	3GPP TS 33.117 – 4.2.3.6.1
	5.5	安全事件紀錄備存	3GPP TS 33.117 – 4.2.3.6.2
	5.6	安全事件紀錄存取控制	3GPP TS 33.117 – 4.2.3.6.3
	5.7	高權限系統功能存取控制	3GPP TS 33.117 – 4.2.4.1.2.1
	5.8	自動播放功能禁用	3GPP TS 33.117 – 4.3.3.1.3
	5.9	作業系統及網路服務安全	3GPP TS 33.117 – 4.4.3
實體防護	6.1	家用基站防拆保護	3GPP TR 33.820 – 6.1(24)
	6.2	實體介面安全管控	3GPP TS 33.117 – 4.3.2.6

安全構面	檢測編碼	測試項目	參考來源
	6.3	硬體憑證設計	3GPP TR 33.820 – 6.1(21)

資料來源：本團隊整理

針對各面向分別訂定檢測項目，各檢測面向之安全性、檢測項目、檢測作業程序、檢測結果及合格判定標準說明如下：

一、 資料保護

本規範資料保護安全測試旨在確認產品設計階段，是否具備敏感性資料傳輸或儲存時的外洩防堵能力，包括敏感性資料存取控管、加解密演算法等，確保產品具備防止敏感性資料外洩能力。

檢測項目	1.1 敏感性資料外洩防止(系統功能洩露)		
檢測依據	3GPP TS 33.117 – 4.2.3.2.2. Protecting data and information – Confidential System Internal Data		
檢測目的			
確認系統功能不會洩露敏感性資料。			
檢測初始條件			
應提供以下資料作為審查與檢測依據：			
(1) 填寫廠商自我宣告表，提供受測基站系統功能說明。			
檢測作業程序		檢測結果及合格判定標準	
(1) 檢視相關佐證文件。		系統內部機密資料不應被任一系統功能以明文方式洩露。	
(2) 確認文件敘述的系統功能，包括本地或遠端 OAM CLI 或 GUI、日誌訊息、警示、錯誤訊息、組態設定匯出檔，是否會洩露敏感性資料，以螢幕截圖記錄。			

檢測項目	1.2 敏感性資料外洩防止(韌體外洩)		
檢測依據	OWASP IoT Top Ten – I9. Insecure Software/Firmware		
檢測目的			
驗證裝置韌體是否有敏感性資料外洩疑慮。			
檢測初始條件			
應提供以下書面資料作為審查與檢測依據：			
(1) 受測基站韌體檔案。			
(2) 填寫廠商自我宣告表，提供韌體保護之加密演算法書面資料作為審查依據。			
(3) 填寫廠商自我宣告表，提供所有連接伺服器之宣告。			
(4) 受測基站使用之加密演算法書面資料。			
檢測作業程序		檢測結果及合格判定標準	
A. 情境 1：		下述兩個合格標準擇一通過即可：	
(1) 審閱受測基站使用之加密演算法書面資料。		A. 情境 1 合格標準：	
		1. 韌體加密演算法採用 FIPS 140-2 核可之加密演算法。	
B. 情境 2：		B. 情境 2 合格標準：	
(1) 對受測基站韌體進行拆解。		1. 未加密韌體檔案，通行碼保護機制採用 FIPS 140-2 核可之雜湊函數。	
(2) 解析檔案系統之路徑目錄。		2. 未加密韌體檔案，其私鑰不可被識別。	
(3) 檢視通行碼資料的保護是否採用 FIPS 140-2 核可之雜湊函數。		3. 未加密韌體檔案，不存在非公開之 E-mail 資料。	
(4) 確認私鑰是否可被擷取，以螢幕截圖記錄。		4. 未加密韌體檔案，不存在惡意或未宣告之 IP Address 資料。	
(5) 檢查是否存在非公開之 E-mail 資料，以螢幕截圖記錄。		5. 未加密韌體檔案，不存在惡意或未宣告之 URL 資料。	
(6) 檢查是否存在惡意或未宣告之 IP Address 資料，以螢幕截圖記錄。			
(7) 檢查是否存在惡意或未宣告之 URL 資料。			

檢測項目	1.3 敏感性資料儲存保護		
檢測依據	3GPP TS 33.117 - 4.2.3.2.3 Protecting data and information in storage		
檢測目的			
敏感性資料應採用適當且有效之加密技術，使資料不會以原來的形式呈現，達到保密的目的，並確保避免遭操作修改。			
檢測初始條件			
應提供以下書面資料作為審查與檢測依據：			
(1) 系統敏感性資料儲存區域與存取操作書面資料。			
(2) 填寫廠商自我宣告表，提供敏感性資料儲存保護演算法。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(3)中，系統敏感性資料以非明文(Plain-Text)方式顯示。	
(2) 依書面資料操作檢視是否可查看敏感性資料。			
(3) 檢視敏感性資料是否採用有效之加密技術，使資料以非明文(Plain-Text)顯示，以螢幕截圖記錄。			

檢測項目	1.4 憑證唯一性
檢測依據	3GPP TR 33.820 – 6.1(19) The authentication credential(s) of each H(e)NB shall be unique
檢測目的	
驗證憑證是否可被偽造。	
檢測初始條件	
(1) 此測項僅適用微型基站、微微細胞接取點及毫微微細胞接取點。 (2) 提供二台受測基站。 (3) 需要受測基站的最高權限進入系統層。 (4) 提供憑證存取說明書面資料。	
檢測作業程序	檢測結果及合格判定標準
(1) 將受測基站連接核心網路。 (2) 監聽後端鏈路封包，並擷取受測基站憑證。 (3) 檢視任二台受測基站憑證之 Fingerprint。	任二台受測基站憑證之 Fingerprint 是相異的。

二、 應用程式安全

本規範應用程式安全測試旨在確認產品設計階段，是否存在網頁管理介面的已知資安漏洞，確保產品網頁管理介面安全無虞。

檢測項目	2.1 網站伺服器安全		
檢測依據	3GPP TS 33.117 – 4.3.4 Web Servers		
檢測目的			
網站伺服器不應存在OWASP Top 10與CWE/SANS 前25 大程式設計錯誤 (CWE/SANS TOP 25 Most Dangerous Software Errors)所載之弱點威脅。			
檢測初始條件			
應提供以下書面資料作為審查與檢測依據：			
(1) 網站伺服器具管理權限之帳號密碼書面資料。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(2)中，掃描結果不應存在常見之網路應用系統安全弱點。	
(2) 使用安全檢測工具，視實際情況套用供應商提供之帳號與密碼登入網站伺服器，檢測網站弱點威脅，以螢幕截圖記錄。			

三、通訊安全

本規範通訊安全測試旨在確認產品設計階段，是否符合通訊傳輸介面的安全要求，包括網路服務啟用限制、空中介面通訊安全、傳輸加密技術要求等，確保產品具備可靠之通訊傳輸功能。

檢測項目	3.1 系統使用協定或服務安全		
檢測依據	3GPP TS 33.117 – 4.3.2.1 No unnecessary or insecure services / protocols		
系統在預設條件下，僅能執行需要的協定或服務，業者可依實際維運需求，將未啟用協定或服務予以暫時性啟用或適當管理。			
檢測初始條件			
應提供以下書面資料作為審查與檢測依據：			
(1) 填寫廠商自我宣告表，說明系統預設已啟用協定或服務。			
(2) 預設啟用協定或服務之描述文件。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(2)與步驟(3)中，確認與廠商自我宣告表一致。步驟(4)，確認已用協定或服務都是合理且具必要性。	
(2) 使用工具驗證系統啟用之協定或服務，與廠商自我宣告表一致，以螢幕截圖記錄。			
(3) 重啟系統，重新執行步驟(2)，使用工具驗證系統啟用之協定或服務，是否符合廠商自我宣告表，以螢幕截圖記錄。			
(4) 評估已啟用協定或服務的合理與必要性。			

檢測項目	3.2 系統與對外之網路傳輸安全
檢測依據	3GPP TS 33.117 – 4.2.3.2.4 Protecting data and information in transfer
檢測目的	
系統與外部設備之網路傳輸須加密保護，且不應使用已被公認之弱加密技術。	
檢測初始條件	
應提供以下書面資料作為審查依據：	
填寫廠商自我宣告表，說明網路傳輸的加密演算法，以及安全協定名稱與版本。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	(1) 若採用 TLS 安全通道，則測試結果須符合 3GPP TS 33.310 Annex E (TLS protocol profile)。
(2) 在 OAM 伺服器間建立安全通道，檢視安全協定與加密方式是否符合安全要求，以螢幕截圖記錄。	(2) 若採用 IKE 及 IPsec 安全通道，則測試結果須符合 3GPP TS 33.210 第 5.3 節 Profiling of IPsec 及第 5.4 節 Profiling of IKEv2。
(3) 側錄與保存步驟(2)網路傳輸過程之通訊封包。	

檢測項目	3.3 控制層資料機密性保護
檢測依據	3GPP TS 33.216 – 4.2.2.1.1 Control plane data confidentiality protection
對 S1 /X2 參照點的控制層封包進行機密性保護。	
檢測初始條件	
應提供以下書面資料作為審查依據：	
(1) 說明 S1 /X2 參照點控制層封包所支援機密性演算法之文件。	
(2) 應支援機密性演算法，例如：128-EEA1、128-EEA2。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(2)中，確認與廠商自我宣告表一致，並確認支援的安全功能正常運作。
(2) 建立安全連線，驗證加密演算法是符合受測基站支援的安全功能。	

檢測項目	3.4 控制層資料完整性保護
檢測依據	3GPP TS 33.216 – 4.2.2.1.2 Control plane data integrity protection
應對 S1 /X2 參照點的控制層封包進行完整性保護。	
檢測初始條件	
應提供以下書面資料作為審查依據：	
(1) 說明支援的 S1 /X2 參照點控制層封包完整性演算法之書面資料。	
(2) 應支援完整性演算法，例如：128-EIA1, 128-EIA2。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(2)中，確認與廠商自我宣告表一致，並確認支援的安全功能正常運作。
(2) 建立安全連線，驗證完整性演算法是符合設備所支援的安全功能。	

檢測項目	3.5 存取層完整性演算法選擇		
檢測依據	3GPP TS 33.216 – 4.2.2.1.5 AS Security Mode Command Procedure (AS integrity algorithms selection)		
檢測目的			
(1) 服務網路(serving network)應依據 UE 所支援的安全功能與目前設定許可之安全功能清單，選擇欲使用的演算法。			
(2) 透過設定可用的完整性演算法清單，由電信業者決定優先排序。			
檢測初始條件			
(1) 確認所選擇之演算法為所設定清單的最高優先順序。			
(2) 已設定安全演算法清單，並優先排序。			
檢測作業程序		檢測結果及合格判定標準	
(1) UE 對受測基站傳送連結請求訊息。		(1) 確認受測基站傳送 SECURITY MODE COMMAND 所選用演算法為清單的最高順位。	
(2) 受測基站收到 S1 介面內容設定請求訊息。		(2) 經由 UE 回傳的 SECURITY MODE COMPLETE 確認支援該演算法。	
(3) 受測基站傳送 SECURITY MODE COMMAND。			
(4) UE 回應 SECURITY MODE COMPLETE。			

檢測項目	3.6 無線資源控制訊息完整性保護		
檢測依據	3GPP TS 33.216 – 4.2.2.1.6 Verify RRC integrity protection		
檢測目的			
管控行動裝置與受測基站 RRC 的完整性驗證。			
檢測初始條件			
(1) 啟用受測基站的 RRC 訊息保護。			
檢測作業程序		檢測結果及合格判定標準	
(1) 受測基站接收含有正確完整性訊息驗證碼之 RRC 訊息。		確認受測基站接收的 RRC 連結請求含有正確的完整性驗證。	

檢測項目	3.7 基站金鑰更新
檢測依據	3GPP TS 33.216 – 4.2.2.1.8 Key refresh at eNB
檢測目的	
基站交遞時，為避免使用相同金鑰，基站應具備觸發基站金鑰(K _{eNB})的更新功能。	
檢測初始條件	
(1) 測試環境應具備 UE 及 MME，受測基站應包括來源與目的基站。	
(2) 可使用 UE 模擬器。	
檢測作業程序	檢測結果及合格判定標準
(1) 基站觸發細胞內交遞 (intra-cell handover)。	確認交遞後，基站已更新金鑰。
(2) 檢查交遞請求是否包含金鑰更新功能。	

檢測項目	3.8 存取層安全模式指令程序
檢測依據	3GPP TS 33.216 – 4.2.2.1.9 AS Security Mode Command Procedure
檢測目的	
受測基站應從優先清單中，選擇最高順位之完整性演算法。	
檢測初始條件	
(1) 測試環境應包括 UE 及 MME，確認受測基站正確選擇，並執行存取層完整性演算法。	
(2) 可使用 UE 模擬器。	
檢測作業程序	檢測結果及合格判定標準
(1) 受測基站對 UE 傳送 SECURITY MODE COMMAND 訊息，而 UE 也回應 SECURITY MODE COMPLETE 訊息。	(1) 確認受測基站的 SECURITY MODE COMMAND 選擇優先清單中最高順位的完整性演算法，且該演算法也存在 UE 端的 EPS 安全性功能中。
	(2) 確認 SECURITY MODE COMPLETE 訊息正確選擇與執行 AS 完整性演算法。

檢測項目	3.9 X2 交遞中降階攻擊防範		
檢測依據	3GPP TS 33.216 – 4.2.2.1.10 Bidding down prevention in X2-handovers		
檢測目的			
在路徑變更(path-switch)訊息中，目的基站應對 MME 傳送從來源基站接收的 UE EPS 安全功能。			
檢測初始條件			
測試環境應包括 UE 及 MME，受測基站應包括來源與目的基站。			
檢測作業程序		檢測結果及合格判定標準	
(1) 目的基站對 MME 傳送路徑變更訊息。		路徑變更訊息中包含 UE EPS 安全性功能，且正確選擇與執行 AS 完整性演算法。	

檢測項目	3.10 存取層演算法選擇		
檢測依據	3GPP TS 33.216 – 4.2.2.1.11 AS protection algorithm selection in eNB change		
檢測目的			
(1) 目的基站應依據其演算法優先清單選擇 UE EPS 安全功能最高順位的演算法 (包含完整性演算法與加密演算法)。若選擇的演算法與來源基站選擇的不同，應透過交遞指令通知 UE。			
(2) 驗證是否正確選擇存取層保護演算法。			
檢測初始條件			
(1) 測試環境應包括 UE 及 MME，受測基站應包括來源與目的基站。			
(2) 可使用 MME 模擬器。			
檢測作業程序		檢測結果及合格判定標準	
(1) 來源基站傳送的加密與完整性演算法，用於來源細胞(Cell)到目的基站的交遞請求訊息。		確認交遞請求的安全性演算法組態正確地選擇與執行。	
(2) 目的基站驗證這些演算法，並選擇優先清單中最高順位的 AS 演算法，目的基站將該演算法加入交遞指令。			

四、 身分鑑別與授權

本規範身分鑑別與授權資安測試旨在確認產品設計階段，具備身分鑑別與授權機制，包括權限控管、通行碼機制複雜度、身分鑑別機制強度等，確保產品具備堅實之身分鑑別與授權機制。

檢測項目	4.1 系統功能存取控制
檢測依據	3GPP TS 33.117 – 4.2.3.4.1.1 System functions shall not be used without successful authentication and authorization.
檢測目的	
使用網路服務(例如: SSH、SFTP、Web Service)登入系統、透過管理介面存取本機時，須完成身分認證與授權機制後，方可使用系統功能。	
檢測初始條件	
提供以下書面資料作為審查與檢測依據： 填寫廠商自我宣告表，說明所有遠端登入系統方式。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(2)中，確認完成認證與授權機制後，才可登入系統與使用系統功能。
(2) 依據書面資料嘗試登入系統，確認是否在完成認證與授權機制後，才可使用系統功能，以螢幕截圖記錄。	

檢測項目	4.2 身分鑑別有效性		
檢測依據	3GPP TS 33.117 – 4.2.3.4.2.1 Account protection by at least one authentication attribute		
檢測目的			
系統使用者身分鑑別的帳號至少須具備一項身分鑑別因子，例如加密金鑰 (Cryptographic keys)、Token 或密碼。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據：填寫廠商自我宣告表，說明身分鑑別帳號所支援的身分鑑別因子。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(2)中，確認認證與授權機制至少需要輸入一項身分鑑別因子，才可登入系統與使用系統功能。	
(2) 依據書面資料嘗試登入系統，確認認證與授權機制至少需要輸入一項身分鑑別因子，才可使用系統功能，以螢幕截圖記錄。			

檢測項目	4.3 系統預設帳號管控		
檢測依據	3GPP TS 33.117 – 4.2.3.4.2.2 Predefined accounts shall be deleted or disabled		
檢測目的			
系統所有預定義或預設帳號都應於初始化設定完成後應予移除或停用。否則應設定預防遠端登入或設定複雜度較高之密碼。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據：			
(1) 系統出廠預定義之帳號與密碼資料。			
(2) 帳號管理設定操作文件。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(2)中，確認系統要求強制更改登入密碼，若無強制更改密碼，則確認步驟(3)是否可以刪除或停用。如步驟(1)與步驟(2)無法完成，則至少要可將步驟(3)重置設定密碼複雜度才可符合判定標準。	
(2) 使用預定義帳號第一次登入系統，確認是否會強制要求更改登入密碼，以螢幕截圖記錄。			
(3) 依據帳號管理設定之操作文件，確認是否可將系統預定義帳號刪除或停用，以螢幕截圖記錄。			
(4) 依據帳號管理設定之操作文件，確認是否可將預定義帳號之密碼重置，且提高設定密碼複雜度，包含英文大寫、英文小寫、數字及特殊符號等，以螢幕截圖記錄。			

檢測項目	4.4 密碼複雜度
檢測依據	3GPP TS 33.117 – 4.2.3.4.3.1 Password Structure
檢測目的	
系統應支援與設定不同組合之密碼複雜度規格，規則如下：	
(1) 密碼長度不得低於最小長度 8 字元	
(2) 至少包含以下四種類型	
- 至少包含一大寫字母(A-Z)	
- 至少包含一小寫字母(a-z)	
- 至少包含一個數字(0-9)	
- 至少有一特殊字元(@#\$%&*)	
檢測初始條件	
提供以下書面資料作為審查與檢測依據：	
密碼修改操作文件。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(2)中，確認系統可將密碼複雜度規則套用至特定帳號。步驟(3)中，確認帳號可正常登入至系統。
(2) 使用管理員帳號登入系統，並將密碼複雜度規格套用至特定帳號，以螢幕截圖記錄。	
(3) 使用已修改密碼複雜度規則之帳號登入系統，以螢幕截圖記錄。	

檢測項目	4.5 通行碼變更機制		
檢測依據	3GPP TS 33.117 – 4.2.3.4.3.2 Password changes		
檢測目的			
系統應支援可隨時更改密碼之功能，且系統預設密碼應於初次登入階段強制要求變更，同時支援密碼變更不得超出重複使用次數的功能。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據： 密碼修改與相關設定之操作文件。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(2)中，確認系統有強制要求初次登入變更系統預設密碼。步驟(3)中，確認密碼變更機制，系統符合不得超過特定重複使用次數之要求。	
(2) 使用系統預設密碼之帳號登入，觀察系統是否要求初次登入強制變更系統預設密碼。			
(3) 使用管理員帳號登入系統，選擇特定帳號，並測試密碼變更機制是否符合不得超過特定重複使用次數之要求，以螢幕截圖記錄。			

檢測項目	4.6 暴力及字典攻擊防護		
檢測依據	3GPP TS 33.117 – 4.2.3.4.3.3 Protection against brute force and dictionary attacks		
檢測目的			
系統應具備暴力及字典攻擊的防護措施，包含網頁介面設置 CAPTCHA 功能、嘗試登入失敗次數限制與鎖定帳號時間。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據：登入失敗次數限制功能操作說明。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(2)中，確認系統在超出密碼輸入錯誤次數後，鎖定帳號。步驟(3)中，確認暴力破解工具無法執行。	
(2) 輸入不正確的密碼，確認系統是否於超出輸入錯誤限制次數後鎖定帳號，以螢幕截圖記錄。			
(3) 使用測試工具進行暴力破解，以螢幕截圖記錄。			

檢測項目	4.7 通行碼顯示遮罩		
檢測依據	3GPP TS 33.117 – 4.2.3.4.3.4 Hiding password display		
檢測目的			
通行碼不會以原文呈現，達到保密的目的			
檢測初始條件			
提供以下書面資料作為審查與檢測依據： 系統在通行碼呈現方式之書面說明。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。 (2) 於系統輸入通行碼之介面，觀察是否以遮罩形式呈現，以螢幕截圖記錄。		步驟(2)中，確認系統之通行碼以遮罩形式呈現。	

檢測項目	4.8 通行碼認證錯誤處理機制		
檢測依據	3GPP TS 33.117 – 4.2.3.4.5 Policy regarding consecutive failed login attempts		
檢測目的			
系統應具備連續登入失敗處理機制，並可限制最大連續輸入失敗次數與強制鎖定可登入延遲時間。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據： 系統連續登入失敗處理機制之書面說明。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。 (2) 依據書面資料設定連續登入失敗處理機制，以螢幕截圖記錄。 (3) 選擇特定帳號，並測試超出系統設定連續登入失敗的最大次數，觀察系統是否能啟用連續登入失敗處理機制，並限制鎖定該帳號於特定時間後才可重新登入，以螢幕截圖記錄。		步驟(3)中，確認系統啟用連續登入失敗處理機制。	

檢測項目	4.9 授權策略
檢測依據	3GPP TS 33.117 – 4.2.3.4.6.1 Authorization policy
檢測目的	
系統應具備依帳號別而有不同權限之設定機制。	
檢測初始條件	
提供以下書面資料作為審查與檢測依據：	
(1) 系統授權策略功能與操作之書面說明。	
(2) 填寫廠商自我宣告表，提供授權策略聲明。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(2)中，確認系統對帳號設定不同權限。
(2) 依據授權策略聲明，嘗試操作不在權限範圍內之功能，確認是否可正常操作或系統有無提示警語，以螢幕截圖記錄。	

檢測項目	4.10 角色存取控制		
檢測依據	3GPP TS 33.117 – 4.2.3.4.6.2 Role-based access control		
檢測目的			
系統應支援帳號角色存取控制，以進行系統功能存取與故障管理維護。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據：			
(1) 角色存取控制功能操作說明。			
(2) 說明可設定的權限清單。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(3)中，確認系統可依不同角色帳號，設定不同權限。	
(2) 建立分配不同角色的帳號，並設置不同存取權限，以螢幕截圖記錄。			
(3) 使用不同的帳號測試不同角色可允許的功能操作，以螢幕截圖記錄。			

檢測項目	4.11 登出功能		
檢測依據	3GPP TS 33.117 – 4.2.3.5.1 Protecting sessions – logout function		
檢測目的			
系統應支援帳號隨時登出功能，並於登出階段提供是否登出系統之提醒畫面。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據： 系統登出功能操作說明。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。 (2) 使用特定帳號登入系統，以螢幕截圖記錄。 (3) 嘗試帳號登出，確認系統是否顯示提醒畫面，並完成系統登出，以螢幕截圖記錄。		步驟(3)中，確認系統顯示登出提醒畫面與完成登出動作。	

檢測項目	4.12 操作逾時功能		
檢測依據	3GPP TS 33.117 – 4.2.3.5.2 Protecting sessions – Inactivity timeout		
檢測目的			
系統應具備帳戶操作逾時的時間設定功能，超出設定時間，系統應強制登出。			
檢測初始條件			
提供以下書面資料作為審查與檢測依據：			
(1) 設定逾時功能操作說明。			
(2) 說明系統內建逾時登出時間。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(3)中，確認系統是否依逾時設定對帳號進行強制登出。若無執行步驟(3)，則步驟(4) 確認系統是否依逾時設定強制登出該帳號。	
(2) 使用建立帳號登入系統，設定逾時登出時間，以螢幕截圖記錄。			
(3) 使用建立帳號登入系統，進行操作閒置，確認系統是否於逾時時間後，強制登出該帳號，以螢幕截圖記錄。			
(4) 若系統沒有逾時設定功能，使用建立帳號登入系統，依逾時登出時間說明文件，進行操作閒置，確認系統是否依逾時設定強制登出該帳號，以螢幕截圖記錄。			

檢測項目	4.13 登入權限控管
檢測依據	3GPP TS 33.117 – 4.3.2.6 Remote login restrictions for privileged users
檢測目的	
系統最高管理權限帳號應不得從遠端登入，降低被攻擊的風險。	
檢測初始條件	
提供以下書面資料作為審查與檢測依據：	
(1) 遠端登入說明文件。	
(2) 說明限制最高管理權限帳號遠端登入之功能操作。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(2)確認無法登入。
(2) 透過嘗試介面遠端登入系統，並使用 root 或最高權限帳戶，以螢幕截圖記錄。	

檢測項目	4.14 檔案系統存取權限控管
檢測依據	3GPP TS 33.117 – 4.3.2.7 File system Authorization privileges
檢測目的	
系統應具備檔案系統存取權限控管機制，僅授權帳戶可修改作業系統層級之檔案、資料或系統檔案等。	
檢測初始條件	
應提供以下書面資料作為審查與檢測依據：	
(1) 系統登入作業系統層級之操作介面與最高管理者帳號密碼。	
(2) 說明檔案系統存取權限控管機制之功能操作。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(4)確認步驟(3)特定帳號無法對檔案系統進行存取。
(2) 使用最高權限帳號登入作業系統層級之操作介面，以螢幕截圖記錄。	
(3) 依據書面資料對特定帳號行檔案系統存取權限設定，以螢幕截圖記錄。	
(4) 以步驟(3)特定帳號登入作業系統層級之操作畫面，測試是否可對被限制檔案系統進行存取，以螢幕截圖記錄。	

五、作業系統安全

本規範之作業系統資安測試旨在確認產品設計階段，作業系統資安防護能力與已知資安漏洞的修補程度，包括日誌檔管控、已知漏洞掃描、敏感性資料洩露等，確保產品具備系統層資安防護功能。

檢測項目	5.1 日誌檔敏感性資料外洩防止		
檢測依據	3GPP TS 33.117 – 4.2.3.2.5 Logging access to personal data		
檢測目的			
基站之敏感性資料應不會明文顯示於日誌檔中。			
檢測初始條件			
應提供以下書面資料作為審查與檢測依據：			
(1) 聲明受測基站有哪些敏感性資料可以明文存取。			
(2) 須填寫廠商自我宣告表，聲明各項日誌檔位置。			
檢測作業程序		檢測結果及合格判定標準	
(1) 依據聲明文件存取各日誌檔，檢視日誌檔明文顯示位置，是否與產品聲明一致。		(1) 日誌檔敏感性資料明文顯示位置與產品聲明一致。	
(2) 除文件所聲明，以明文顯示敏感性資料的位置外，檢視每一日誌檔中是否存在明文的敏感性資料，以螢幕截圖記錄。		(2) 須說明該日誌檔中敏感性資料以明文顯示之正當性。	

檢測項目	5.2 安全開機	
檢測依據	3GPP TS 33.117 – 4.2.3.3.2 Boot from intended memory devices only	
檢測目的		
基站僅能經由合法，且未經竄改的韌體啟動。		
檢測初始條件		
提供以下書面資料作為審查與檢測依據： 僅能從特定記憶體裝置啟動之設計文件。		
檢測作業程序		檢測結果及合格判定標準
審閱文件以確認受測基站啟動時，是否僅允許來自合法且未經竄改的韌體。		受測基站啟動時，僅允許來自合法且未經竄改的韌體。

檢測項目	5.3 軟體完整性		
檢測依據	3GPP TS 33.117 – 4.2.3.3.5 Network Product software package integrity		
檢測目的			
確保系統具備預載軟體的完整性。			
檢測初始條件			
須提供系統管理者權限。			
檢測作業程序		檢測結果及合格判定標準	
替換應用程式執行檔或網頁原始檔，驗證是否可被執行，以螢幕截圖記錄。		替換應用程式執行檔或網頁原始檔後，該軟體不可被執行。	

檢測項目	5.4 安全事件記錄功能		
檢測依據	3GPP TS 33.117 – 4.2.3.6.1 Security event logging		
檢測目的			
系統應提供不同事件類型之安全事件紀錄，例如：登入失敗、管理者存取、管理者操作行為、設定變更、重新開機、關機、當機、網路介面狀態改變。			
檢測初始條件			
供應商應提供以下書面資料作為審查與檢測依據：			
(1) 存取、設定啟用安全事件紀錄之操作文件。			
(2) 系統安全事件紀錄類型與格式之說明文件。			
(3) 填寫廠商自我宣告表，說明如何觸發每一個安全事件之操作。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		符合判定標準：步驟(2)中，確認系統是否	
(2) 依據觸發需求所列安全事件，確認系統有無確實記錄，以螢幕截圖記錄。		依據觸發安全事件，而產生對應的紀錄。	

檢測項目	5.5 安全事件紀錄備存
檢測依據	3GPP TS 33.117 – 4.2.3.6.2 Log transfer to centralized storage
檢測目的	
系統應提供可將安全事件紀錄功能備存至集中管理設備或其他外部系統設備，並於傳輸時加密保護。	
檢測初始條件	
應提供以下書面資料作為審查與檢測依據：	
(1) 安全事件紀錄傳輸至外部系統使用之標準文件。	
(2) 系統可支援傳輸安全事件紀錄之外部設備，並提供整合設定操作文件。	
檢測作業程序	檢測結果及合格判定標準
(1) 審查書面資料，確認已符合檢測初始條件要求。	步驟(3)中，確認系統與外部系統傳輸使用加密技術保護。步驟(4)確認集中式管理設備或外部系統確實儲存來自受測基站系統傳送時的相關安全事件紀錄。
(2) 觸發安全事件紀錄，將事件日誌傳送到外部系統，以螢幕截圖記錄。	
(3) 側錄與保存步驟(2)網路傳輸過程間之通訊封包。	
(4) 檢測集中式管理設備或外部系統是否儲存相關安全事件日誌，以螢幕截圖記錄。	

檢測項目	5.6 安全事件紀錄存取控制		
檢測依據	3GPP TS 33.117 – 4.2.3.6.3 Protection of security event log files		
檢測目的			
系統全事件紀錄應僅有特定權限帳號可以存取。			
檢測初始條件			
應提供以下書面資料作為審查與檢測依據：			
(1) 填寫廠商自我宣告表，提供安全事件紀錄位置。			
(2) 填寫廠商自我宣告表，提供安全事件紀錄存取策略。			
(3) 測試人員系統管理者權限。			
檢測作業程序		檢測結果及合格判定標準	
(1) 審查書面資料，確認已符合檢測初始條件要求。		步驟(2)中，確認可以存取安全事件日誌文件檔。步驟(3)，確認不可以存取安全事件日誌文件檔。	
(2) 使用具安全事件存取權限之帳號登入系統，確認是否可以存取安全事件日誌文件檔，以螢幕截圖記錄。			
(3) 使用無安全事件存取權限之帳號登入系統，確認是否可以存取安全事件日誌文件檔，以螢幕截圖記錄。			

檢測項目	5.7 高權限系統功能存取控制		
檢測依據	3GPP TS 33.117 – 4.2.4.1.2.1 Authenticated Privilege Escalation only		
檢測目的			
驗證擁有特殊權限的系統功能是否經過認證與授權方可使用。			
檢測初始條件			
(1) 提供一清單 A，說明哪些系統函數可以取得高權限與其組態設定規則。例如： sudo command and its configuration file /etc/sudoers. (2) 提供一清單 B，包括系統指令、GUI 功能及檔案，較高權限僅能執行特定的有限任務。此列表須包含： ● 設定高權限系統的指令與 GUI 功能。 ● 文件擁有者與權限設定。 ● 指令、GUI 功能及檔案的合理性 例如: root-owned files with SUID and SGID permissions (3) 提供使用者取得系統管理者權限的方法。			
檢測作業程序		檢測結果及合格判定標準	
(1) 判斷清單 A 的合理性外，並驗證是否經過身分認證後才能使用。 (2) 判斷清單 B 的正確性及合理性外，並驗證是否經過身分認證後才能使用。 (3) 驗證列表“B”中文件擁有者以外的人不具備寫入權限。 (4) 實際執行列表 B 所描述的內容。		(1) 產品不允許使用者透過另一個使用者帳戶，在沒有重新認證的情況下，取得系統管理者權限。 (2) 功能及檔案的執行權限，必須與使用者宣告一致。	

檢測項目	5.8 自動播放功能禁用		
檢測依據	3GPP TS 33.117 – 4.3.3.1.3 No automatic launch of removable media		
檢測目的			
驗證當基站接入卸除式媒體(如:USB)時，是否會自動執行應用程式。			
檢測初始條件			
(1) 無			
檢測作業程序		檢測結果及合格判定標準	
(1) 測試者接入卸除式媒體至受測基站。		受測基站在接入卸除式媒體時，不會自動啟動應用程式。	

檢測項目	5.9 作業系統及網路服務安全		
檢測依據	3GPP TS 33.117 – 4.4.3 Vulnerability Scanning		
檢測目的			
系統本身不應存在重大風險已知弱點漏洞			
檢測初始條件			
(1) 無			
檢測作業程序		檢測結果及合格判定標準	
(1) 將測試電腦連接受測基站。 (2) 啟動弱點掃描功能工具，對受測基站執行弱點掃描。 (3) 檢視弱點掃描報告是否存在 CVSSv3 評分為 7 分以上之資安漏洞。		作業系統與網路服務不存在 CVSS v3 評分為最高風險 7 分以上之資安漏洞。	

六、實體防護

本規範實體防護測試旨在確認產品設計階段，具備防止駭客實體入侵之能力，包括增加產品外殼拆除難度、實體介面之存取控制等，通過此節的資安測試，可確保產品具備實體資安防護功能，由於微型基站、微微細胞接取點及毫微微細胞接取點不一定佈建於可管制人員出入之環境，因此將面對來自實體層的資安威脅。

檢測項目	6.1 家用基站防拆保護		
檢測依據	3GPP TR 33.820 – 6.1(24) H(e)NB enclosure should provide indication of physical tampering		
檢測目的			
驗證家用基站具有拆解防護之設計，增加實體介面入侵之難度。			
檢測初始條件			
(1) 此測項僅適用微型基站、微微細胞接取點及毫微微細胞接取點。			
檢測作業程序		檢測結果及合格判定標準	
(1) 目視受測基站外殼是否一體成形。		(1) 受測基站須採用一體成形或防拆螺絲等	
(2) 目視受測基站外殼是否經防拆螺絲鎖住。		機殼防拆除保護設計。	
(3) 卸除未經上述 2 方式保護之外殼，檢視是否可碰觸晶片及主機板，拍照記錄。		(2) 若受測基站外殼為可拆卸之設計，外殼被卸除後，受測基站晶片及主機板無法被碰觸。	

檢測項目	6.2 實體介面安全管控		
檢測依據	3GPP TS 33.117 – 4.3.2.6 Remote login restrictions for privileged users		
檢測目的			
連接基站實體通訊埠時，是否存取作業系統之除錯模式。			
檢測初始條件			
(1) 此測項僅適用微型基站、微微細胞接取點及毫微微細胞接取點。 (2) 提供進入作業系統除錯模式之方法。 (3) 填寫廠商自我宣告表，提供進入作業系統層之方式。			
檢測作業程序		檢測結果及合格判定標準	
(1) 受測基站啟用作業系統除錯模式，開啟相應之管理介面連接工具。 (2) 測試電腦連接受測基站實體 console 埠。 (3) 確認是否透過實體 console 埠存取作業系統之除錯模式，以螢幕截圖記錄。		須通過身分鑑別方可存取作業系統之除錯模式。	

檢測項目	6.3 硬體憑證設計		
檢測依據	3GPP TR 33.820 – 6.1(21) Only authorized end-users shall be able to request modifications to membership of the Closed Subscriber Group		
檢測目的			
基站硬體憑證是否可被徒手移除。			
檢測初始條件			
(1) 此測項僅適用微型基站、微微細胞接取點及毫微微細胞接取點。 (2) 受測基站應存在硬體憑證之設計，否則此測項不適用。 (3) 填寫廠商自我宣告表，提供硬體憑證設計聲明。			
檢測作業程序		檢測結果及合格判定標準	
(1) 目視受測基站之硬體憑證設計是否位於受測基站外觀。 (2) 目視受測基站之硬體憑證設計是否位於具防拆保護之外殼中。 (3) 以徒手非破壞性的方式卸除硬體憑證，拍照記錄。		受測基站之硬體憑證不應被徒手卸除。	

第五節 小結

電信業者為提供行動通訊服務，在佈建基站等基礎設施時，考量訊號涵蓋、頻段、使用者容量及連網速度，以不同規格的基站進行佈建，例如以基地臺(eNodeB)建立基本涵蓋，以 HeNB (微型基地臺、微微細胞接取點及毫微微細胞接取點)強化小區域傳輸，未來 5G 的發展趨勢，因加入不同高頻的操作頻段，促使小型基站佈建量將大量增加，而製造廠商眾多，其設計方式不同，對於各種基站設備的資安狀況也將更難以掌握。

為保障消費者免於侵害，及確保行動寬頻系統基站環節的資訊安全，在現有的程序和作法不足之下，基站檢測規範草案為行動寬頻基站之資安防護標準化的一環，建立完善之標準檢測技術與驗證能量建置，藉由業者或設備進行抽檢，定期、主動針對市面設備進行檢測，以公開機制向社會展現主管機關為資安議題把關之態度，亦可督促業者重視資安問題

第八章、行動寬頻資安座談會及研討會辦理成果

第一節 行動寬頻基站資安檢測規範草案座談會

為使本計畫規劃之行動寬頻基站資安檢測規範草案能適用於國內電信網路實際營運環境，且更貼近實際電信業者需求，本團隊在 NCC 的協助下，邀請國內五家電信業者-中華電信、台灣大哥大、遠傳電信、亞太電信及台灣之星分別舉辦五場座談會(座談會簡報、會議紀錄及業者意見回覆請參見附錄五)，蒐集國內電信業者對本計畫規劃之基站資安檢測規範草案之建議。

另本團隊也分別訪談國內電信業者使用的兩家基站設備製造商 Nokia 與 Ericsson，瞭解設備製造商對於本檢測規範草案中之檢測項目建議。以下綜整國內電信業者及設備製造商之建議如下，與檢測規範草案相關之建議本團隊也已評估並納入內容修定中。

一、國內電信業者意見彙整

經電信業者之指正，建議本規範草案對基站分類之定義請 TTC 參照行動寬頻基地臺射頻設備技術規範內容，使用詞定義一致化。本團隊業已依此建議已進行修正，另在推行上之建議，業者認為於電信網路營運上已通過 ISO27001 及 ISO27011 增項之要求，且大型基地台都是以專線網路布建，安全性高，故建議此規範應納入 NCC 之型式認證中，但本計畫團隊在研析各國資安政策中，在國際上並無對基站有強制性資安檢測要求，故建議本規範草案原則上以自律為主。下表為各電信業者於會後之意見回覆摘要及本計畫團隊之回應。

表 8-1 電信業者意見摘要及本計畫團隊之回應

業者	意見摘要	本計畫團隊回應
中華電信	1.建議規範列入 NCC 型式認證檢驗中執行，要求設備供應商於設備上市前通過該資安規範。	型式認證為技術審驗，有鑒於國際上並無對基站有強制性之資安檢測要求，建議本規範草案原則上以自律為主。
	2.基站分類之定義請參照行動寬頻基地臺射頻設備技術規範內容，使用詞定義一致化	本團隊依業者意見，已參照國家通訊傳播委員會行動寬頻基地臺射頻設備技術規範之定

業者	意見摘要	本計畫團隊回應
		義，修訂基站資安檢測規範草案之基站分類用語，使用詞定義一致化。
	3.建議針對規範實施前之設備，不溯及既往，或以較低強度之規範要求。	建議電信商及早規劃，為安全認證及所有相關流程做好準備，同時關注基站的安全設計與開發，以維護行動通訊之安全。
台灣大哥大	1.檢測 1.4、3.2 檢測作業程序為家用基站，適用範圍建議排除大基站。	謝謝業者意見，本團隊已於表 7-1 檢測範圍項目新增各檢測項目之適用範圍。
	2.檢測項目 3.7，於作業檢測上，因 NAS 已為加密傳輸，依檢測步驟執行是否可行？	該檢測作業為確認交遞金鑰更新功能的啟用與否，無關加密金鑰之內容。
	3.本公司已於 2012 年導入 ISO27001、27011 資訊安全稽核，此 ISO 標準涵蓋面向依資產類別進行各項目的風險管控及稽核，其範圍及項目、細節等遠大於此規範所列，並每半年由第三方 ISO 單位進行實地稽核，可取代此規範之檢核。	通過 ISO27001 標準的驗證，僅代表組織建立起資訊安全標準的通用基準，強化資訊安全管理的運用，對於基站設備安全其所面臨的風險不應被視為安全無虞，而本計畫之草案應視為建立、實施、維持及持續改進基站安全的規範。
	4.建議針對設備商進行規範要求，以簡化檢測作業。	資安檢測可分事前/事中/事後，無論設備商或電信業者，均須確保其設備或服務之資訊安全。
遠傳電信	1.本草案所提及之 3GPP 標準功能為在單一設備端之功能，然而電信業者之網路規劃與管控係以全面標準及制度化之考量為基礎，並在 2010 年時，於國家通訊傳播委員會之指導之下導入 ISO27001 及 27011 增項之認證，並且每半年進行外部第三單位的稽核認證，本公司也於 2014 年獲得 BS10012 認證，將相關的資訊安全提	通過 ISO27001 標準的驗證，僅代表組織建立起資訊安全標準的通用基準，強化資訊安全管理的運用，對於基站設備安全其所面臨的風險不應被視為安全無虞，而本計畫之草案應視為建立、實施、維持及持續改進基站安全的規範。

業者	意見摘要	本計畫團隊回應
	升至更高的水準。	
	2.建議回歸至原始設備進口時需取得型式認證時同時進行，將可以提升可行性，並降低受測單位之成本。	型式認證為技術審驗，有鑒於國際上並無對基站有強制性之資安檢測要求，建議本規範草案原則上以自律為主。
	3.現行電信營運商之資安認證架構及基地臺設備加入營運提供服務流程，已經可以提供高品質資安管控，無需額外成本進行相關投入。	因資安事件層出不窮，本規範可於設備上線前進行檢測，降低業者營運風險。
台灣之星	1.基地臺資安事屬重要，建議由源頭管理，勿使有疑慮的設備勿建置於本國行動網路。	型式認證為技術審驗，有鑒於國際上並無對基站有強制性之資安檢測要求，建議本規範草案原則上以自律為主。
	2.因此建議基地臺各項資安查測，併入基地臺設備型式認證項目內，以做到源頭管理。	
亞太電信	1.建議修正草案內容第三節用語釋義大基站及小基站發射功率，應與現行動寬頻業務相關法令規範基地臺定義一致	本團隊依業者意見，已參照國家通訊傳播委員會行動寬頻基地臺射頻設備技術規範之定義，修訂基站資安檢測規範草案之基站分類用語，使用詞定義一致化。
	2.鑑於行動通信基地臺佈建綿密，其資安更是重中之重，為利業者採購符合資安規範之設備，建議基站之資安檢測，應回歸源頭辦理型式認證時，由設備商申請檢測，經由檢測合格後發予證書，俾使業者在選商時，做為必要規格要項之一。	型式認證為技術審驗，有鑒於國際上並無對基站有強制性之資安檢測要求，建議本規範草案原則上以自律為主。
	3.建議本檢測技術規範草案，應訂合理之日出條款，不溯及既往，以降低改善成本，避免耗費資源。	建議電信商及早規劃，為安全認證及所有相關流程做好準備，同時關注基站的安全設計與開發，以維護行動通訊之安全。

資料來源：本團隊整理

二、設備製造商之意見彙整

在與國內電信業者使用的基站設備廠商 Nokia 及 Ericsson 訪談中，設備商皆表示其產品於設計時皆依循 3GPP 標準之安全規範，Nokia 對檢測項目及本團隊於工研院測試結果有表示相關建議；Ericsson 建議行動通訊安全應考量的是整體電信網路系統面之安全，end to end 的安全性，而非僅只限單一元件設備。下表為設備商之意見摘要及本計畫團隊之回應。

表 8-2 設備商意見摘要及本計畫團隊之回應

業者	意見摘要	本計畫團隊回應
Nokia	1.針對此規範草案，檢視 Nokia 基站功能後，大多可符合檢測規範要求，唯以下檢測項目 4.5 通行碼變更機制，Nokia 未來產品將會更改設計，若密碼沒有更改將會告警；及 4.13 項目需再與總公司確認。	煩請廠商協助與總公司確認 4.13 項目是否符合本檢測規範草案之安全要求，並再回覆本中心。
	2.檢測項目 4.13 登入權限控管：因基地台數量龐大，營運商須靠遠端方式維護，故建議遠端的定義應再放寬，可將遠端定義為超過網管機房外的範圍，並可檢視業者實際發生的機率來定義。	建議廠商可在自我宣告表內，提供網管系統資通安全環境的證明，以符合安全要求。
	3.檢測項目 5.6 基站系統的安全事件紀錄應有存取控制限制：依電信業者營運經驗，安全事件紀錄都是存在網管。	
	4.在身分鑑別與授權安全上，建議帳號密碼問題應從系統面管理與網管面搭配，而非只限定單一基站設備，電信業者可設置一個認證伺服器來管理。	建議可在廠商自我宣告表內，提供網管系統身分鑑別與授權安全的管理證明，以符合安全要求。
Ericsson	1.本公司產品設備皆遵循 3GPP 規範，已具備相當程度的安全性。	基站設備安全是 3GPP 規範於 2017 年新公告的安全要求，設備商應針對其安全內容，對既有或未來設備持續改進以維持基站安全。
	2.建議行動通訊安全應考量的是整體電信網路系統面之安全，end to end 的安全性，而非僅只限單一元件設備。	本團隊認同行動通訊安全應涵蓋整體網路，但單一元件的安全，亦不可偏廢，建議廠

業者	意見摘要	本計畫團隊回應
		商可在自我宣告表內，提供額外的安全證明，以彌補單一元件的風險。
	3. GSMA 在安全保證方法上，今年將認可兩家第三方檢測實驗室，針對設備之安全性進行檢測認證，目前 Ericsson 總公司也在等待 3GPP 與 GSMA 共同發起的檢測認證，待 GSMA 通知後也會配合進行檢測。	因 GSMA 尚未公布任可之兩家第三方檢測實驗室訊息及檢測認證進度，謝謝廠商提供之最新資訊。
	4. 為避免設備商須進行重複之檢測認證，建議未來是否於大型基站進口時，檢附已通過國際組織檢測通過之證明文件即可。	資安檢測可分事前/事中/事後，無論設備商或電信業者，均須確保其設備或服務之資訊安全，建議未來可考量行動設備的整體現況及未來發展，審酌相關相互承認協定(MRA)之機制。
	5. 3GPP TS33.216 屬較新的規範，實際如何檢測仍需待 GSMA 正式要求 Ericsson 配合檢測時才有辦法瞭解。	謝謝廠商的回應。

資料來源：本團隊整理

第二節 行動寬頻基站資安研討會

為推廣本計畫研擬之行動寬頻基站資安檢測規範草案及檢測平臺，本團隊於 107 年 5 月 4 日於張榮發基金會國際會議中心舉辦行動寬頻基站資安研討會，並邀請國家通訊傳播委員會 吳銘仁簡任技正擔任指導單位貴賓。

本次研討會目的為向國內業界推廣與分享本計畫於執行期間與各界合作產出的研究成果及本團隊規劃之行動寬頻基站資安檢測規範草案，現場並設置攤位展示本計畫之基站資安檢測平臺環境架構及部分功能，邀集產官學代表參加，研討會也開放與參加來賓之交流時間，得到非常熱烈的迴響，並有 HeNB 設備商詢問是否可請 TTC 協助檢測之要求，雙方並留下聯繫方式，本中心也希望可介由本計畫之檢測平臺，協助業者於基站資安之檢測，甚至未來可提升之其他行動寬頻網路元件之檢測。

一、 行動寬頻基站資安研討會議程

本研討會舉辦時間為半天，研討會議程如下表 8-1，以下議程之簡報內容(請參見附錄六)皆印製手冊供現場來賓參考。

表 8-3 行動寬頻基站資安研討會議程

時間	議程	主講人
13:00~13:30	報到	
13:30~13:50	主持人致詞 貴賓致詞	財團法人電信技術中心 林炫佑副執行長 國家通訊傳播委員會 吳銘仁簡任技正
13:50~14:10	建置基站資安檢測環境計畫介紹	財團法人電信技術中心 蔡志明主任
14:10~14:30	國際行動寬頻資安政策及規範最新脈動 —國際資安政策	財團法人電信技術中心 陳志宇研究員
14:30~14:50	國際行動寬頻資安政策及規範最新脈動 —國際標準規範	國立中山大學資工系 黃政嘉博士
14:50~15:10	休息(用茶點)／檢測展示參觀及交流	
15:10~15:40	行動寬頻基站資安檢測規範草案	財團法人電信技術中心 蔡明德工程師
15:40~16:10	HeNB檢測結果及防護建議	財團法人資訊工業策進會 高傳凱 博士
16:10~16:30	TTC行動寬頻資安檢測場域	財團法人電信技術中心 許任銘工程師
16:30~16:40	Q & A	
16:40~16:50	會議結束	

資料來源：本團隊整理

二、 辦理成果說明

本次研討會參加人數踴躍，參加人員主要為五大電信業者代表，其次為基站及 HeNB 設備製造商，並有檢測實驗室之代表也到場參加，本次研討會參加人員可參見附錄 4。在研討會休息時間，本團隊開放基站資安檢測平臺與工具之參觀及交流，現場接獲許多技術人員之諮詢與交流。以下為研討會現場之剪影。



圖 8-1 主持人致詞-TTC 林炫佑副執行長

資料來源：本團隊整理



圖 8-2 貴賓致詞-NCC 吳銘仁簡任技正

資料來源：本團隊整理



圖 8-3 建置基站資安檢測環境計畫介紹-計畫主持人蔡志明主任

資料來源：本團隊整理



圖 8-4 研討會講者簡報剪影

資料來源：本團隊整理



圖 8-5 基站檢測平臺展示及交流

資料來源：本團隊整理



圖 8-6 研討會貴賓及講者合影

資料來源：本團隊整理



圖 8-7 研討會 Q&A

資料來源：本團隊整理

第三節 小結

本研究團隊透過座談會與個別拜訪方式和電信業者及基站設備製造商進行訪談，了解電信業者及基站設備製造商對行動寬頻基站資安檢測草案之看法，電信業者大多認為，因此規範草案屬單一設備之規範，且大多屬產品本身設計之要求，許多功能只限設備商的技術與開發人員可以掌握，建議未來可朝加入既有型式認證方式，以保障基站之安全性。

在基站設備製造商的訪談上，因本研究團隊於計畫國外參訪中，與 Nokia Security Center 交流了許多行動寬頻網路安全的議題，因此 Nokia 台灣分公司也十分關注本計畫檢測規範草案的發展，並對本檢測規範之項目內容已徵詢總公司意見，並提供本團隊許多電信業者在實務運作時之經驗參考；另外在對 Ericsson 的訪談上，該公司代表也與我們分享 GSMA 已與設備製造商有聯繫，希望今年可以由其認證的第三方實驗室針對 3GPP 安全保證規範對設備進行檢測，因相關檢測方式及內容尚未明確，故對於本計畫檢測規範草案內容及項目無法一一回應，但 Ericsson 表示，其產品一定會符合 3GPP 規範之安全標準，故建議國內應依循國際訂定的標準規範及認證流程，不建議另行訂定僅針對基站之檢測規範草案。

另外在本研究團隊舉辦的行動寬頻基站資安研討會，除電信業者皆積極參與外，此次研討會也吸引了國內製造家用基站廠商的參加，於研討會中也有熱烈的交流，未來也希望繼續延續本計畫建置之基站資安檢測平臺，提供國內業者更多的設備安全諮詢及檢測。

第九章、研究發現與建議事項

第一節 研究發現

一、 前瞻性資安檢測技術研究

(一) 資安防護技術及與服務最新趨勢

本團隊已針對近年國際最關注的 SS7 攻擊，以及國內電信業者已在積極發展的 5G、SDN 及 IoT 之資安攻擊與防護技術進行深入研析，對於新興技術發產上的安全可歸納以下幾個面向：

1. SS7 安全防護重點

在 SS7 防護建議上，國際多遵循 GSMA 之防護建議，但因本團隊無 GSMA 會員之資格，無法取得 GSMA 所定義之詳細防護建議及國際攻擊資訊之分享，本團隊仍設法蒐集最新 SS7 議題資訊，參考美國 FCC、歐盟 ENISA 最新研究及調查的報告，以及參訪芬蘭 Nokia Security Center 所得之相關資訊，綜整出以下 SS7 安全防護重點：

(1) 防禦攻擊-監控網路流量

監控異常之網路流量，已為目前電信業者網路普遍之功能，此為目前最基本之防禦攻擊措施。

(2) 緩解攻擊-過濾訊息

過濾發話來源端與收話目的端號碼做為控制基礎，一旦非允許的收發雙方與建立連線，則可能會發出警告或直接阻斷該訊務。

(3) 合作及訊息分享

GSMA 提供其會員全球最新 SS7 攻擊統計資訊，因國內並無 GSMA 會員，研究團隊僅取得次級資料，從不同的資料來源，包括歐盟與美國政府部門的報告及業界的研究，歸納出 GSMA SS7 防護建議文件及攻擊資訊，實為主管機關與電信業者可考量的重點；建議國內亦可於業者與主管機關間建立 SS7 攻擊訊息分享平臺，提升國內電信業者防禦 SS7 攻擊之能量。

(4) 加強網路節點安全

透過國際標準組織公布之內容，及時檢視電信網路弱節點，進行節點安全及流程之加強，以防禦不同的威脅。

2. 5G 網路的安全防護重點

5G 網路為提供更高的速率及更多物聯網之應用，所以在考量資訊安全的同時，須避免在加諸資安防護時產生的時間延遲，所以在資安防護的身分認證上的設計上將朝減少設備終端與認證伺服器間的物理距離及降低認證協議的複雜度來設計，並需減少認證切換產生的時間延遲及網路節點反覆加解密的情況。因 5G 新興技術涉及各式各樣垂直產業的應用服務，將帶來新型態行動網路架構，故於其相關安全防護技術上，建議須持續關注相關國際標準之動態。

3. SDN 網路安全防護重點

SDN 網路的攻擊方式即為一般網路常見之攻擊方式，包含電子欺騙攻擊(Spoofing Attacks)、入侵式攻擊(Intrusion Attacks)、異常式攻擊(Anomaly Attacks)以及阻斷服務攻擊(DoS Attack)與分散式阻斷服務攻擊(DDoS Attack)等，本團隊已綜整各種常見攻擊之防護技術供各界參考。

4. IoT 安全防護重點

近年許多攻擊實際案例多以 IoT 攻擊為主，本團隊從近兩年最新之 IoT 綜整出最常見隻攻擊趨勢：①惡意程式入侵及②殭屍病毒侵入攻擊，在 IoT 設備的防護上，密碼設定的強化及變更密碼是首要的防護重點，因此強制變更密碼的機制也建議 IoT 廠商應設計在產品中，以保障消費者的安全。

(二) 資安檢測標準與檢測流程之最新趨勢

國際標準組織如 3GPP 及 GSMA 所訂定之行動寬頻網路相關標準，為全球設備製造商及電信業者皆會遵循之指引，在此次參訪芬蘭經驗中，參訪單位 Nokia 及 VTT 皆建議我國應積極參與與關注上述兩個國際組織標準之訂定，同時也可取得國際間最新

之行動寬頻網路資安攻擊與防護訊息。

1. 3GPP 已訂定基站安全保證規範

本團隊在研析 3GPP 與行動寬頻基站相關之 33 安全系列標準文件時，發現 3GPP 於 2017 年 9 月最新發表了 TS33.216 eNodeB 安全保證規範，本團隊於基站資安檢測規範規劃上即以此規範為主要參考依據，另分析與此文件有密切關聯的 TS 33.117(網通產品安全)、TR 33.926(網通產品之安全威脅)與 TS 33.401(EPS 架構)三份文件內容，綜整出 3GPP 對基站安全及檢測之最新規範。

2. GSMA 訂定安全認證流程，預計 2018 年試行

在 GSMA 產品與製程安全性的認證流程-安全保證方法方面，該流程從供應商之生命週期安全認證出發，且訂定第三方檢測實驗室之認證標準，於訪談 Ericsson 的過程中，該公司人員表示 GSMA 已通過兩家檢測實驗室之認證，預計 2018 年將與設備製造商合作，透過認可的檢測實驗室依 3GPP 訂定之安全保證規範(SCAS)執行設備商產品之驗證測試。

二、 行動寬頻基站資安檢測

本團隊參考國際標準及實際檢測，完成基站(H)eNB 檢測項目、檢測技術與流程規劃，並於本計畫建議之行動寬頻基站資安檢測平臺中進行實測，以實測結果驗證檢測項目、檢測技術及檢測流程內容，並建立一套完整之基站資安檢測流程，將檢測結果連結國際弱點資料庫 CVE，建置基站弱點資料庫。

(一) 基站設備之安全需源自產品之設計

本團隊參考第 1 期研究之行動寬頻基站安全威脅及國際標準規範 3GPP TS33.216、TS33.320 及 TR33.820 等，規劃出基站與家用基站之檢測項目，並透過 3 家廠牌基站與 2 家廠牌家用基站的實測，瞭解國際標準所定的安全保證規範，如何於實際環境檢測，並得知哪些項目可落實，哪些項目可能牽涉到設備版別或一開始之產品設計，經由本計畫之檢測，本團隊成員也累積了基站資安檢測的技術能量。

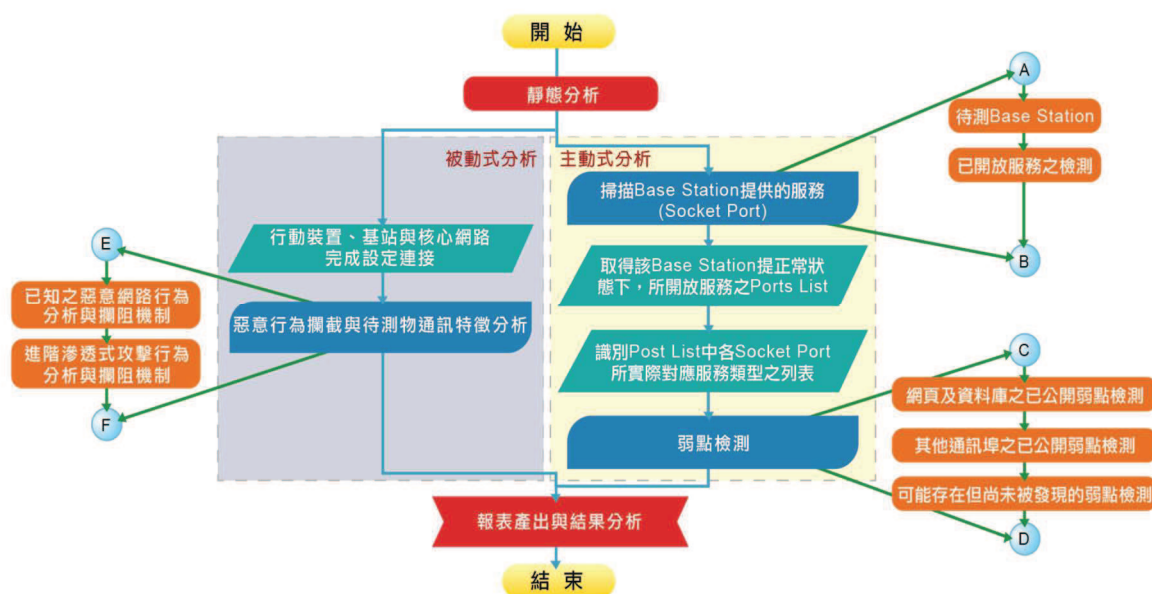
在測試過程中發現 3GPP TS33.117 許多測試項目內容要求，都必須從產品研發、設計、測試等階段去思考與理解，因為安全源自於設計，安全必須融入在製造產品的每一個階段，以至於 3GPP TS33.117 很多測試項目的需求都必須由基站製造廠商提供更進一步的資訊才可以完成測試，而非購置設備的電信業者的技術與維運人員可以掌握，製造商已經將許多細節包裝成簡易容易操作之介面，以因應行動通訊網路環境下面臨的各式各樣的突發狀況，讓維運人員可以快速操作使用與調整。

上述從實際檢測結果的發現，也同時印證了，3GPP 安全保證規範與 GSMA 合作建立的安全認證方法(NESAS)，該流程之認證即是從供應商之產品生命週期安全性驗證開始，以確保其產品商用化後之安全性。

(二) 建立基站資安檢測流程

本團隊在經過實測 3 家廠牌基站與 2 家廠牌家用基站的實測過程及經驗中，建立了一套完整的基站資安檢測流程與方法，此流程除可供本中心檢測人員檢測操作之依據外，同時可做為輔導廠商設備檢測，提供廠商參考之 SOP，以節省受測者執行檢測研究之時間，提高檢測效率。

本團隊從靜態分析、被動分析及主動式分析，提出基站資安建議之檢測流程及檢測方法如下圖。



資料來源：本團隊整理

（三）發掘現存基站安全漏洞

在家用基站檢測的過程中，發現身分認證的部分是極大的風險，不論在登入時或是在使用各項系統功能時，完成身分認證與授權機制。實體層部分，因為容易被使用者接觸，所以必須避免 JTAG 或是 UART 可以直接存取到除錯模式。若使用網頁管理介面，需避免 OWASP top10 的風險。敏感資訊像是日誌檔或是金鑰需要權限的存取控管和避免明文顯示。家用基站所使用的網路通訊埠須避免為有風險的協定，避免因為有漏洞或是明文傳輸造成危害。

另外在基站(eNodeB)目前初步檢測結果，發現主要安全問題為韌體檔案內金鑰未加密、網站存有安全弱點、內建預設密碼初次登入無要求強制變更等，本團隊希望透過本文所提供的建議可望加深基站的資安能量。

本團隊在檢測過程中發現之商用設備安全漏洞，在第一時間也通知並輔導廠商進行相關修正及更新，並協助重新檢測以確保其設備之安全性。

三、行動寬頻資安框架研究

（一）國際並無強制性之基站資安檢測要求

綜觀各國資安政策之發展，對產業面原則上以自律機制為主，主管機關並不強制規範業者之設備或服務需在上市或佈建之前通過資安檢測。此外，對於行動寬頻之基站設備，在技術標準中已包含一定程度之資安防護能力，例如身份驗證、網路實體邏輯的切分、限制可用的通訊接口等。因此，業者在上市或佈建之前，均會宣稱已符合相關技術標準之規範。

（二）國際間行動寬頻安全之最佳實務參考

本團隊深入研究國際資安政策及框架中發現，英國、美國、歐盟在推動行動寬頻網路安全上，有值得國內主管機關參考之實務操作經驗。

目前我國亦正建立國家資安防護體系，行動寬頻之資安防護必然為最重要之重點。參酌美國經驗，不僅行動寬頻主管機關之通訊委員會（FCC）、連相當於我國公平交易委員會之美國聯邦貿易委員會（FTC）亦以保障消費者不受侵害之理由，處理業者資安自律不足之問題。

歐盟標準組織 ETSI 於 2017 年 10 月發布了有關 NIS 指令實施之技術報告文件（ETSI TR 103 456），該文件就目前可用的全球主要網路安全社群正在開發的技術規範提供準則，旨在滿足與實施 NIS 指令相關的法律措施和技術要求，包括資訊分享、基於網路之風險和事件、與必要的防禦措施，主要包含事件通知之考量點與網路安全風險管理的最佳實踐。

美國 NIST 也依據聯邦資訊安全現代化法（FISMA）之規定，針對 LTE 網路安全提出 LTE 安全準則（Guide to LTE Security NIST SP 800-187），描述了資訊科技實驗室（ITL）在 LTE 資訊系統安全方面的研究與指導方針，也包括業界、政府和學術機構的合作活動。提供產官學界一個依循之準則。

針對行動寬頻設備安全之維護，NIST 自身並不重新制定相關技術標準，而是檢視業界是否已發展出有相應、可用且完整的標準。在行動寬頻設備安全議題上，國際標準組織 3GPP 已經提出行動寬頻設備之安全確保規範，並與第三方組織進行合作來提供第三方的安全檢測服務，以強化行動寬頻設備的安全。因此，NIST SP 800-187 亦陳述了 3GPP 工作小組在網路產品安全保證與強化之研究發展，提供業界促進行動寬頻設備安全的主要參考。

（三）政府訂定資安聯防框架，國際標準訂定各元件安全保證標準

由本團隊研究國際資安框架發現，政府角色主要在訂定資安聯防框架，在行動寬頻網路安全上，皆採業者自主要求及管理。針對至各網路元件之安全保證規範，設備製造商皆依循國際標準組 3GPP 所訂定之規範，設計其產品之安全性，GSMA 更設計了安全保證方法流程，希望業者可透過認證之第三方實驗室，來取得各元件之安全認證，此方法可做為未來國內業者採購設備時，對安全性的認定標準。

四、行動寬頻基站資安檢測平臺

本團隊結合 NCC 採購之檢測工具，以模組化方式完成基站資安檢測示範性平臺之組建，達成高彈性與高擴充性之目的。此平臺透過模組化方式建構，未來將可彈性使用，加入其他元件或檢測工具，擴展至其他設備之資安驗證場域，本計畫團隊已有實測驗證本計畫之檢測平臺可擴展應用於其他設備之檢測，如 Small Cell、MEC Gateway、Smart meter (瓦斯表)+NB-IoT 等。

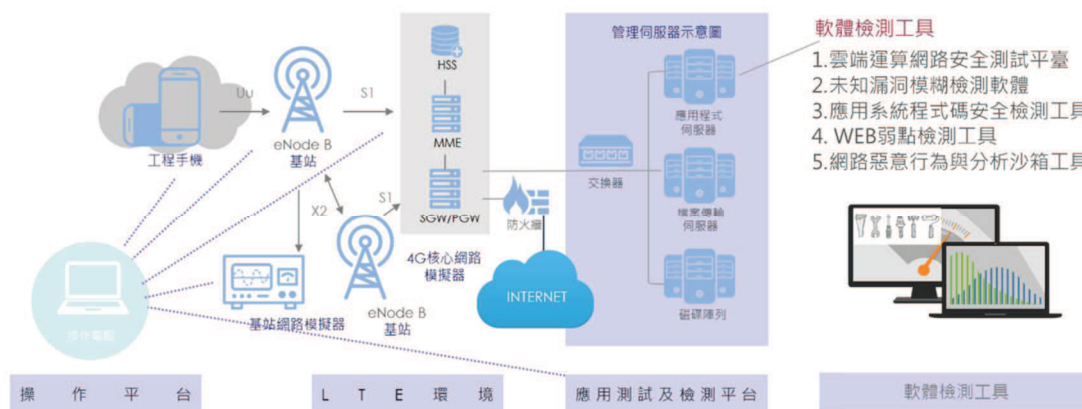


圖 9-2 行動寬頻基站資安檢測平臺

資料來源：本團隊整理

五、 行動寬頻基站資安檢測規範草案

本團隊透過研析國際相關規範 3GPP TS33.320 以及 TS33.216 與實測結果，擬定檢測範圍及檢測項目，依據(1)資料保護、(2)應用程式安全、(3)通訊安全、(4)身分鑑別與授權安全、(5)作業系統安全、(6)實體防護六項安全構面，訂定行動寬頻基站產品安全技術要求-基地臺(eNodeB)37 項；HeNB（微型基地臺、微微細胞接取點及毫微微細胞接取點）41 項，提出完整之行動寬頻基站資安檢測規範草案。

本草案擬定後也透過國內業者座談及訪談國內基站設備商蒐集相關意見，在交流過程中發現本檢測規範草案將來於實施時需注意的重點。

（一）版本適用性之考量

考量檢測規範草案未來的適用性，目前所引用以 2017 年 9 月公告之 3GPP TS33.216 R15 版本與 3GPP TS 33.117 R14.2 版本為主的檢測項目，因電信設備技術標

準領先於產品商用時程，部分檢測項目對應商用環境下的設備版本存在落差，意味著測試功能無法順利到位。經本計畫調查，目前國內電信業者所採用之 4G 基站等通訊相關設備仍以 3GPP 版本 R12 與 R13 為主，除後續研發及生產的設備才可能支援較新版本的相關功能，可以預期本檢測規範草案中的部分檢測項目與測試條件將無法全部落實於現行商用環境下的基站系統，因此草案之推行與實施，在公告前應與設備商與電信業者，逐條檢視其適用性。

（二） 平台功能性可能影響實測結果

檢測規範草案中各項檢測項目經本計畫所建置測試環境實測驗證，由於測試環境下，無論是基站數量、廠牌、規格，或是與基站介接的通信系統元件等預算因素限制下，致使測試環境條件無法與電信業者商用環境一致，部分檢測項目可能須視基站所搭配系統組態條件進行設定，由於測試環境中為核心網路模擬器或簡易版核心網路，缺乏商用核心網路網管系統的安全功能時，僅能以基站支援的基本安全功能為導向，因此檢測項目的實測驗證與商用環境下的測試結果可能也會存在差異性。

（三） 安全功能實現差異性

標準規範僅定義應具備的安全功能，並不會限定設計方式，因此設備商在設計、開發產品時均無制式形式，造成機密性、完整性、可用性方面的安全功能實現上存在極大的差異性，例如：核網網管系統本身具備遠端登入身分機制，但卻可以提供在專用線路的信任環境下進行較高權限的基站組態設定與維運作業，達到相同安全性的機制，本計畫建議可透過廠商自我宣告進行說明，指出基站、核網或加值系統功能與對應規範草案的安全功能，提供檢測單位作為判定是否符合檢測規範草案之要求。

為保障消費者免於侵害，及確保行動寬頻系統基站環節的資訊安全，在現有的程序和作法不足之下，基站檢測規範草案為行動寬頻基站之資安防護標準化的一環，建立完善之標準檢測技術與驗證能量建置，藉由業者或設備進行抽檢，定期、主動針對市面設備進行檢測，以公開機制向社會展現主管機關為資安議題把關之態度，亦可督促業者重視資安問題

(四) 由第三方檢測實驗室協助執行

依 GSMA NESAS 的安全認證方法上，其強調由第三方認證實驗室來執行相關檢測，該認證方法中，GSMA 也認可設備商或業者可以依照 NESAS 的規範申請檢測實驗室資格。檢測規範由第三方檢測實驗室推動之方法，為國際安全認證方法之所認可，使檢測上具有可信度及公正性，且可減少業者額外投資之最佳方式。

第二節 後續建議事項

一、研究面

(一) 應持續關注新興技術發展之資安議題

本計畫已經針對 5G、SDN 及 IoT 之資安威脅與防護進行研析，並特別說明了 GSMA 訂定之 IoT 安全指引，上述電信網路新興技術及應用之安全規範及技術仍不斷在發展中，本中心也將持續研究，納入 107 年資安旗艦計畫研析資安技術標準、規範或指引之基礎內容中。

(二) 持續關注並積極參與國際標準組織之安全議題討論

1. SS7 防護

本團隊在研析 SS7 防護相關文獻及參訪 Nokia Security Center 時所得資訊發現，GSMA 已提供完整之 SS7 防護指引及最新攻擊資訊予其會員參考，非會員則無法取得相關資訊，該協會提供之指引已為國際上各國發布 SS7 防護指引之主要參考文件。反觀國內，並無電信業者加入 GSMA 組織，故無法取得國際上最新攻擊與防護之資訊，故建議除透過研究持續關注相關規範指引之動態外，應鼓勵國內業者或法人加入該組織，以取得國際標準於資安攻擊之最新資訊，使國內之資安防護措施可與國際接軌。

2. 行動寬頻網路安全認證

本計畫在與電信業者及設備製造商訪談過程中，皆表示行動寬頻網路及設備安全皆依循國際標準組織 3GPP 之規範及 GSMA 之相關指引，3GPP 與 GSMA 合作訂定了

安全保證方法(NESAS)，其內容從供應商的產品生命週期開始訂定了完整的安全認證流程，及第三方檢測實驗室之認證內容，經訪談基站設備商的過程中也得知，GSMA 將於今年(2018 年)與設備商合作試行 3GPP 安全保證規範(SCAS)之檢測，建議應持續關注 GSMA 試行之進度，並與基站設備商保持良好聯繫，以瞭解國際組織對 3GPP 安全保證規範實際檢測方式。

二、 技術面

(一) 善用基站資安檢測平臺之檢測技術及工具

為使 NCC 採購之檢測工具能有效運用，建議將 HeNB 之資安檢測納入旗艦計畫

2.2 建構通傳事業資設備之安檢測機制，以輔導廠商進行檢測為目標，進而提升基站資安檢測平臺之技術及工具使用效益，最終期能帶動資通寬頻安全檢測，使平臺產生最大化之可利用價值及邊際效益，如以下說明：

1. 一般性檢測：針對使用者行為的模擬、行動寬頻基站(含家用基站)的信令結構安全性評估，以及鑑別基站之符合性與功能性，並進一步模擬大量負載與變因控制，在此階段將透過基準線量測模型，以介面、信令與通道特性為量測基礎，協助受測基站廠商了解自家產品的堅實性與可靠性。
2. 進階資安檢測：行動寬頻網路內部與外接網路都是 IP 封包的網路架構下，致使傳統網路攻擊者可能直接套用現有的網路攻擊來癱瘓行動寬頻網路或是攻擊特定受害者。透過主動式的惡意/攻擊行為工具，對待測基站進行各式弱點掃描與探測。其中包含了通訊弱點掃描與自動化分析程序，對於待測物是否存在 NIST 所公告的已知弱點進行完整評估，並針對這些已被識別的弱點進行滲透測試，以進一步證實這些被找到的弱點是否確實造成威脅，並協助待測物廠商進行修補。更進一步可依據廠商需求，針對廠商所開發的程式原始碼，提供專屬的程式弱點檢測與評估，除了基本的檢測內容外，尚可依據其專屬領域標準(如金融方面的 PCI-DSS)進一步提供相關的檢測報告。
3. 透過自動化分析工具，持續監測與分析待測設備在網路行為的表現，有利於廠商若使用非自行開發的模組，或第三方開放式系統平台作為產品元件之一時，可能發生

不明的威脅行為，在平臺檢測的過程中，即時的病毒、攻擊行為或各種進階式滲透攻擊可能的跡象，都能經由平臺在測試的過程中完整分析與回報。

4. 發展防禦策略，經由本平臺的檢測並觀察待測基站抵擋攻擊的能力，並參考最終之檢測報告以使廠商瞭解其可能存在的弱點以及可能遭遇的最新資安威脅，若已採購使用的單位，則能據以提前規劃因應未來需要採取的防禦策略。

基於整個 LTE 行動寬頻網路通訊協定已針對以網際網路通訊協定(IP)為基礎的即時與非即時應用與服務進行最佳化，在全面 IP 化的網路架構下資安檢測項目，不僅能對行動寬頻網路基站與家用基站進行資訊安全檢測，也能在適當的調整平臺參數後，延伸至其他連網設備進行資通安全檢測，評估並產生相關報表，發揮整體平臺最高效益。

(二) 平臺與場域之開放

依據資安即國安的戰略思維，電子化與資訊化為國家科技發展之重要策略，而資通安全將扮演關鍵的角色。因此國內各大專院校在培養一般性與跨領域之資通科技人才培育工作也積極地進行當中。但多數學校單位並無相關資源能自行建置完整的行動寬頻場域與資通安全檢測平臺，以培養國家未來行動通訊資安所需的專業人才。

鑑於資安威脅日益推陳出新，國際上在大學設置國家級資安教學與研究中心較著名的有韓國資訊與通信大學 (Information and Communication University, 簡稱 ICU) 之國際資安研究中心 (International Research Center for Information Security, 簡稱 IRIS), 韓國政府設有資訊部全力支援經費挹注 ICU 國際資安研究中心 (IRIS) 發展資安研究與教育，目前已成為亞洲重要的國際級資安學術研究重心，每年均有超過二十人以上的博士生或國外博士後研究人員 (其中有一半來自中國大陸) 到 ICU 之 IRIS 進行資安前瞻議題的研究工作。

資安人才之培植與訓練是長期性的工作，充足的資安人力，高水準的技術研發能量，透過本計畫促進產業的研究方案、快速的技術移轉與部署，刺激最尖端的應用經濟的發展，將可大幅提昇我國資安產業能量，達成具自行研發能力、產品檢測技術具自主能力、資安系統具創新整合與設計能力、入侵偵防與防護具自我管理能力等具體目標。

對資通安全產業的扶持與推動，代表政府國家資通安全技術能量的提升與重視，本計畫可從協助國家提昇行動寬頻資安學術研究水準與技術研發能量的觀點，除了透過檢測平臺運作，提升國內產業資訊基礎建設的防禦能量之外，將基站資安檢測平臺與場域各元件，模組化建構重延伸為 4G 網路安全檢測平臺電信網路開放場域，除了原本提供國產設備試驗及其相應之系統資安或效能證之試驗場域外，也能為未來國家資訊安全人才的培育，提供一個理論與實務並進的研究場域，以培育所需實務工程應用與基礎研究人才，乃希冀開放本平臺以協助政府推動人才培育，同時提昇我國資安科技之全球競爭力。

三、 政策面

(一) 建立國內 SS7 資安事件分享平臺

鑒於國內無法取得 GSMA 對其會員發布之國際最新攻擊資訊，故建議成立國內業者與政府間之 SS7 資安事件分享平臺，以做為國內 SS7 資安防護之參考。

歐盟 NIS 指令針對關鍵服務業者以及數位服務提供者需負擔資安威脅分享的義務，因此該文件也提出結構化的威脅情報分享平台(STIX)相關資訊可做為參考。

(二) 行動寬頻基站資安檢測規範草案之推展與落實

1. 輔導廠商檢測，使本計畫草擬之基站資安檢測規範更為完整

本計畫之基站資安檢測規範草案建議可延伸至 108 年資安旗艦計畫 2.2 建構通傳事業資通設備之資安檢測機制，進行 HeNB 廠商試行，修訂後研定為正式公告之 HeNB 資安檢測技術規範。

2. 主管機關與產業合作建立自願性檢測機制

於第 1 期計畫中，本團隊已參訪美國與韓國，瞭解到美國及韓國皆未對電信業者的基站資安具有強制性的檢測規範，在行動寬頻網路安全的保障上，皆以自律性方式，請電信業者自行確保其網路的安全。於本計畫於參訪芬蘭的交流過程中也發現，歐盟在基站資安檢測的範疇上亦無強制性的檢測規範。

在第 1 期計畫及本計畫此次參訪與國際資安框架研究中所得到的國際經驗中，瞭解到目前歐美對於基站資安皆無強制性之檢測要求，認為電信業者應確保其所提供之行動寬頻網路服務的安全性，所以建議可提供此指引規範，鼓勵業者採取自律性之管理方式。

3. 於基站資安檢測規範草案中，可納入通報及定期主動抽檢機制

由於行動寬頻服務的建立，其訊號涵蓋依據頻段及使用者密集程度，會以不同規格的基站加以佈建，例如以大型（Macro）基站建立基本涵蓋，以小型（Small）或微型（Micro or femto）強化小區域傳輸。未來走向 5G 的發展，小型基站佈建量可能大量增加，其生產廠商也較多，對於各類型設備的資安狀況也將較為複雜。

目前我國亦正建立國家資安防護體系，行動寬頻之資安防護必然為最重要之重點。參酌美國經驗，不僅行動寬頻主管機關之通訊委員會（FCC）、連相當於我國公平交易委員會之美國聯邦貿易委員會（FTC）亦以保障消費者不受侵害之理由，處理業者資安自律不足之問題。因此，我國主管機關在建立檢測技術能量的同時，建議可利用本中心之技術能量，一方面在使用者通報設備上的疑慮時可加以檢測，並於未來針對特定業者或特定類型設備進行抽檢，另方面則可定期、主動針對市面設備進行檢測，藉由公開機制向社會展現主管機關為資安議題把關之態度，亦可督促業者重視資安問題。

參考書目

1. Phil Goldstein, “Android phones on Verizon, AT&T face LTE security vulnerability, researchers say” in FierceWireless, 2015/10/19.
2. BlackHat EU, “LTE and IMSI catcher myths”, 2015.
3. 中國新聞網, “电信诈骗高发伪基站泛滥难监管, 建议多部门打组合拳”, 2016/1/8.
4. 新浪財經, “央视揭密伪基站冒充银行诈骗案件: 三条短信骗走五千块”, 2016/5/13.
5. The Hacker News, “Hackers Using Fake Cellphone Towers to Spread Android Banking Trojan”, 2017/3/22.
6. 2015 IEEE CSCN Conference : Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing.
7. NGMN, “NGMN 5G WHITE PAPER V1.0”, 2015/2/17.
8. Futuristic mobile technologies foresee, ITU towards “IMT for 2020 and beyond”.
9. 韓國電信官網, KT 5G-SIG.
[Online]. Available: <https://corp.kt.com/eng/html/biz/services/sig.html>
10. 商周, “台灣人還在癡癡等 4G... 日本 5G 都快上路了!”, 2013/10/14.
11. 5G-ENSURE, “5G-ENSURE publishes its 5GPPP security enabler open specifications V1”.
12. 張景皓, “新一代網路架構 SDN 顛覆傳統網路的控制模式”, 2012/11/19.
13. ONF White Paper, “Software-Defined Networking: The New Norm for Networks”, 2012/4/13.
14. Zanella Andrea; Bui Nicola; Castellani Angelo; Vangelista Lorenzo & Zorzi Michele, “Internet of Things for Smart Cities”, IEEE Internet of Things Journal, VOL. 1, NO. 1, 2014/2.
15. 謝錦星, “IoT 晶片設計的商機與挑戰”, 北美智權報第 119 期.
16. 陳曉莉, “Dyn 遭大規模 DDoS 攻擊, Mirai 殭屍網路脫不了關係”, 2016/10/25.
17. iThome, “美國大學遭到 DDoS 攻擊, 「凶手」竟然是校內的自動販賣機、路燈”, 2017/2/14.
18. NIST, “Guideline on Network Security Testing.”, 2003/10.
19. 國家通訊傳播委員會, “共通準則: 資訊技術安全評估共同準則第 1 部: 導論與通用模型第 3.1 版”, 2008/10.
20. 3GPP TS 33.401, “3GPP System Architecture Evolution (SAE); Security architecture(Release 13)”.
21. 3GPP TR 33.805, “Study on security assurance methodology for 3GPP network products(Release 12)”.
22. 3GPP TR 33.916, “Security Assurance Methodology for 3GPP network products

- (Release 13)”.
23. 3GPP TR 33.926, “Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes (Release 13)”.
 24. 3GPP TS 33.116, “Security Assurance Specification for the MME network product class (Release 13)”.
 25. 3GPP TS 33.117, “Catalogue of General Security Assurance Requirements (Release 14)”.
 26. GSMA 官網, Fraud and Security Group.
[Online].Available:<https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group>
 27. 3GPP TR33.820, “Security of H(e)NB”.
 28. 3GPP TS33.320, “Security of Home Node B (HNB) / Home evolved Node B (HeNB)”.
 29. J. Acharya, L. Gao, and S. Gaur, “Heterogeneous Networks in LTEAdvanced, 1st ed.”, 2014/5.
 30. Seongmin Park, Sekwon Kim, Kyungho Son and Hwankuk Kim, “Security Threats and Countermeasure Frame Using a Session Control Mechanism on VoLTE”, 2015/11.
 31. Ericsson White paper, “5G security”, 2015/6.
 32. 劉榮太, “夯技術 SDN 的資安課題”, 2014/1/27.
 33. Scott Hogg, “SDN Security Attack Vectors and SDN Hardening”, 2014/10/28.
 34. 趨勢科技, “威脅情報資源-萬物聯網(IoE)”.
 35. 3GPP TS 36.413, “Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)”.
 36. Common Vulnerabilities and Exposures, “CVE-2013-7395”.
 37. NIST 官網, National Vulnerability Database (NVD).
[Online].Available: <https://nvd.nist.gov/>
 38. cryptocurrenciesnews, “Stealing Bitcoin with a Name and a Phone Number”, 2017/9/22.
[Online].Available: <https://www.cryptocoinsnews.com/stealing-bitcoin-with-a-name-and-a-phone-number/>
 39. 林妍臻, “黑帽駭客大會：3G/4G 網路協定漏洞可能洩露用戶行蹤，目前無解”, 2017/7/27.
[Online].Available: <http://www.ithome.com.tw/news/115812>
 40. 蘋果日報, “物聯網資安攻擊加劇,常見 IP CAM 成資安漏洞”, 2017/6/8.
[Online].Available:<http://www.appledaily.com.tw/realtimenews/article/new/20170608/1135619/>
 41. iThome, “WannaCry 進化為蠕蟲，勒索軟體殺傷力大增”, 2017/5/22.
[Online].Available: <http://www.ithome.com.tw/news/114312>
 42. SC MEDIA, “SS7 vulnerability defeats WhatsApp encryption, researchers claim.”,

- 2016/5/13.
[Online].Available: <https://www.scmagazineuk.com/ss7-vulnerability-defeats-whatsapp-encryption-researchers-claim/article/530945/>
43. iThome, “駭客利用電信業者 SS7 協定漏洞破解雙因素認證，手機用戶的銀行帳戶遭盜領一空”，2017/5/5.
[Online].Available: <https://www.ithome.com.tw/news/113893>
44. iThome, “【IoT 攻擊無所不在】為什麼學校印表機會被入侵？”，2017/5/27.
[Online].Available: <http://www.ithome.com.tw/news/114128>
45. theguardian, “DDoS attack that disrupted internet was largest of its kind in history, experts say”, 2016/10.
[Online].Available: <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet>
46. Da Feed, "A critical Improper Authentication vulnerability in Uber allowed password reset for any account", 2017/5/18.
[Online].Available:<http://thecharlestendellshow.com/a-critical-improper-authentication-vulnerability-in-uber-allowed-password-reset-for-any-account/>
47. KrebsOnSecurity, “KrebsOnSecurity Hit With Record DDoS”, 2016/9/21.
[Online].Available: <https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/>
48. iThome, “【詳細圖解】駭客入侵一銀 ATM 流程追追追”，2016/7/25.
[Online].Available: <http://www.ithome.com.tw/news/107294>
49. TREND LABS 趨勢科技全球技術支援與研發中心, “<IOT 物聯網>多達 1,000 多種型號,12 萬臺網路攝影機,恐受殭屍病毒 Persirai 感染”，2017/5/11.
[Online].Available:<https://blog.trendmicro.com.tw/?p=50051#more-50051>
50. 數位時代, “Gogoro 三大資安風險揭密，小心所有物聯網產品！”，2016/7/25.
[Online].Available: <https://www.bnext.com.tw/article/40327/BN-2016-07-25-200710-44>
51. 科技新報, “烏克蘭電力系統遭駭原因是網路釣魚，如何加強資安防護引討論”，2016/4/26.
[Online].Available: <https://technews.tw/2016/04/26/ukraine-power-system-phishing-information-security-protection/>
52. Dialogic, “Common Channel Signaling (CCS)”.
[Online].Available: <https://www.dialogic.com/glossary/common-channel-signaling-ccs>
53. Malathi Veeraraghavan, Haobo Wang, “A Comparison of In-Band and Out-of-Band Transport Options for Signaling”, IEEE, 2005/4/18.
[Online].Available:
<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.8764&rep=rep1&type=pdf>

54. Lifewire, "PSTN (Public Switched Telephone Network)", 2017/3/14.
[Online].Available: <https://www.lifewire.com/pstn-public-switched-telephone-network-818168>
55. TechTarget, "PCS (personal communications service)".
[Online].Available: <http://searchnetworking.techtarget.com/definition/PCS>
56. The Hacker News, "How to Hack Someone's Facebook Account Just by Knowing their Phone Numbers", 2016/6/15.
[Online].Available:<https://thehackernews.com/2016/06/hack-facebook-account.html>
57. aculab, "What are point codes in SS7?".
[Online].Available: <https://www.aculab.com/questions/what-are-point-codes-in-ss7/>
58. Tekelec, "Database Administration Manual - Global Title Translation", 2012/1.
[Online].Available: https://docs.oracle.com/cd/E52590_01/doc.440/910-6277-001_rev_a.pdf
59. IEEE Digital Library, "Non-Circuit-Related Signalling".
[Online].Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=273201>
60. FCC, "The Communications Security, Reliability and Interoperability Council V Final Reports", 2017/3.
61. FICORA, "FICORA calls for a single information security level for mobile network in the Nordic countries", 2016/12/1.
[Online].Available:
<https://www.viestintavirasto.fi/en/ficora/news/2016/ficoracallsforasingleinformationsecuritylevelformobilenetworkinthenordiccountries.html>
62. ENISA, "Signalling Security in Telecom SS7/Diameter/5G", 2018/3.
63. Holtmanns, Silke, Siddharth Prakash Rao, and Ian Oliver. "User location tracking attacks for LTE networks using the interworking functionality." IFIP Networking Conference (IFIP Networking) and Workshops, 2016. IEEE, 2016.
64. Jensen, Kristoffer, et al. "Better Protection of SS7 Networks With Machine Learning." IT Convergence and Security (ICITCS), 2016 6th International Conference on. IEEE, 2016.
65. FICORA, "FICORA calls for a single information security level for mobile network in the Nordic countries", 2016/12/1.
[Online].Available:
<https://www.viestintavirasto.fi/en/ficora/news/2016/ficoracallsforasingleinformationsecuritylevelformobilenetworkinthenordiccountries.html>
66. NGMN "NGMN 5G WHITE PAPER", 2015/2/17.
67. 5G-PPP, "View on 5G Architecture", 2016/6.
68. IMT-2020 (5G) 推進組, "《5G 願景與需求白皮書》", 2014/5/28.

69. ITU, “《Requirements related to technical performance for IMT-Advanced radio interface(s)》”, 2008.
70. NGMN 官網. [Online].Available: <https://www.ngmn.org/home.html>
71. 5G-PPP 官網. [Online].Available: <https://5g-ppp.eu/>
72. ITU, “Workplan, timeline, process and deliverables for the future development of IMT”, 2015.
73. ITU-R, “IMT Vision-Framework and overall objectives of the future development of IMT for 2020 and beyond”, 2015/9.
74. Balazs Bertenyi, "3GPP system standards heading into the 5G era", 3GPP, 2014.
75. 3GPP, ”Study on scenarios and requirements for next generation access technologies”, 2016/6.
76. 3GPP, “3GPP RAN progress on “5G””, 2016.
77. 工研院資通所,”3GPP RAN1 #87 會議報告”, 2016/12/30.
78. 工研院資通所,”3GPP RAN1 #86bis 會議報告”, 2016/11/30.
79. Arikan, Erdal. ”Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels. ” *IEEE Transactions on Information Theory* 55.7 (2009): 3051-3073.
80. Netmanias, “Korea Communication Review Q4 2015”, 2015.
81. 工業技術研究院, “5G 毫米波接取技術與挑戰”, 2015/8/14.
82. Shannon, Claude E. "A mathematical theory of communication." *ACM SIGMOBILE Mobile Computing and Communications Review* 5.1 (2001): 3-55.
83. 資策會產業情報研究所(MIC),“新世代行動網路接取架構發展分析：Cloud RAN”, 2014/5/28.
84. 資策會產業情報研究所(MIC),“營運商 5G C-RAN 發展動向分析”, 2016/2/26.
85. 5G-PPP, “Phase 1 Security Landscape”, 2017.
86. 壹讀,“如何確保 SDN 基礎設施的安全?”, 2015/3/18.
87. 台灣岱凱, “虛擬化環境的安全防護”, 2008/12.
88. 網管人,“淺談 DDoS 攻擊之手法與防禦”, 2009/6/25.
89. Cisco 思科,”思科自我防禦網路與網路存取控制”, 2005/9.
90. Huawei, “5G Scenarios and Security Design”, 2016/11.
91. NOKIA,”Security challenges and opportunities for 5G mobile networks”, 2017.
92. Ericsson,“5G SECURITY SCENARIOS AND SOLUTIONS”, 2015/6.
93. Huawei, “5G Scenarios and Security Design”, 2016/11.
94. Google, "This POODLE Bites:Exploiting The SSL 3.0 Fallback Security Advisory", 2014/9.
95. 黃開枝, 金梁, 趙華, “5G 安全威脅及防護技術研究”, 2015/6.
96. Seeker on Hacker@KCon, “偽基站高級利用技術 — 徹底攻破短信驗證碼”,

- 2016/9/6.
97. Martín Casado, Michael J. Freedman, Justin Pettit, Jianying Luo, Nick McKeown and Scott Shenker, "Ethane: taking control of the enterprise", 2007/8.
 98. Nick McKeown et al., "OpenFlow: enabling innovation in campus networks", 2008/4.
 99. IEEE INFOCOM 2009, "INFOCOM 2009 Keynote Talks", 2009/4.
 100. Amit Agarwal, "SDN@Google", 2012/7/17.
 101. AT&T, "ECOMP Architecture White Paper", 2016.
 102. Nav Chander, Courtney Munroe, Melanie Posey, "BT's Connect Intelligence IWAN SD-WAN Solution — New Communication Choices for the Cloud-Connected Enterprise", 2016/1/28.
 103. Open Networking Foundation, "SDN architecture", 2014/6.
[Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf
 104. Nick Feamster, Jennifer Rexford, Ellen Zegura, "The Road to SDN: An Intellectual History of Programmable Networks", 2014/4.
[Online]. Available: <http://dl.acm.org/citation.cfm?id=2602219>
 105. 張衛峰, "深度解析 SDN：利益、戰略、技術、實踐", 2014/6/6.
 106. 林傳筆, 盧皓威, 陳堃維, 王永祥, "軟體定義網路(Software-defined Network)之實作", 2014.
 107. 高娟, "既生瑜何生亮？解讀 ODL 和 ONOS 之爭", 2016/4/27.
[Online]. Available: <http://www.c114.net/news/16/a951499.html>
 108. 王韋程, "獲電信業及網路設備商支持 ONOS 躍居 SDN 控制器主流", 2017/1.
[Online]. Available: http://www.2cm.com.tw/technologyshow_content.asp?sn=1612280008
 109. 王韋程, 黃秉鈞, "軟體定義網路中邊界開道協議之實作", 2016/10/4.
[Online]. Available: <https://ictjournal.itri.org.tw/Content/Messages/contents.aspx?&MmmID=654304432061644411&CatID=654313611257131137&MSID=711463635567746312>
 110. ON.Lab, "ONOS Architectural Progress", 2014.
[Online]. Available: <http://onosproject.org/wp-content/uploads/2014/11/ONOS-architecture.pdf>
 111. Huawei, "ONOS 總覽". [Online]. Available: <http://developer.huawei.com/ict/cn/site-sdn-onos/article/onos-overview>
 112. OpenDayLight, "OpenDayLight：Platform Overview".
[Online]. Available: <https://www.opendaylight.org/platform-overview>
 113. 王浩丞 林盈達, "SDN 兩大控制器之比較：ONOS vs OpenDayLight", 2016/9/23.
 114. OpenDayLight, "Carbon-Fertile Ground for New Use Cases", 2017.

- [Online].Available: <https://www.opendaylight.org/carbon-fertile-ground-new-use-cases>
115. OpenDayLight, “KT Corporation Uses OpenDayLight to Deploy Transport-SDN WAN Network”. [Online].Available: <https://www.opendaylight.org/use-cases-and-users/user-stories/kt-corporation-uses-opensdaylight-to-deploy-transport-sdn-wan-network>
 116. digital spotlight-NETWORK WORLD, “SDN:AN EMERGING REALITY”, 2015/6.
[Online].Available: http://resources.idgenterprise.com/original/AST-0147450_NWW_SDN_4_July_2015_r1.pdf
 117. 曾惠敏 胡仁維 劉德隆, “使用隧道技術實現網路虛擬化”, 2013.
 118. VMware, “Reference Design:VMware® NSX for vSphere (NSX)Network VirtualizationDesign Guide”, 2014.
 119. 饒康立, “軟體網路虛擬化安全平台 VMware NSX 功能架構簡述”, 2016/5/5.
[Online].Available: http://www.netadmin.com.tw/article_content.aspx?sn=1605030001
 120. 王立恒, “VMware NSX 兩大未來戰略剖析”, 2016/5.
[Online].Available: <http://www.ithome.com.tw/news/105831>
 121. VMware, “VMware 客戶成功案例”.
[Online].Available:
<https://www.vmware.com/tw/company/customers.html#product=nsx>
 122. 高娟, “既生瑜何生亮？解讀 ODL 和 ONOS 之爭”, 2016/4/27.
[Online].Available:
http://www.2cm.com.tw/technologyslow_content.asp?sn=1612280008
 123. 王韋程, “獲電信業及網路設備商支持 ONOS 躍居 SDN 控制器主流”, 2017/1.
 124. 王韋程, “黃秉鈞,”軟體定義網路中邊界閘道協議之實作”, 2016/10/4.
 125. digital spotlight-NETWORK WORLD, “SDN:AN EMERGING REALITY”, 2015/6.
[Online]. Available: http://resources.idgenterprise.com/original/AST-0147450_NWW_SDN_4_July_2015_r1.pdf
 126. VMware, “Reference Design:VMware® NSX for vSphere (NSX)Network VirtualizationDesign Guide”, 2014.
 127. 饒康立, “軟體網路虛擬化安全平台 VMware NSX 功能架構簡述”, 2016/5/5.
 128. Danda B. Rawat, Swetha R. Reddy, “Software Defined Networking Architecture, Security and Energy Efficiency: A Survey”, 2016/10.
 129. 戴彬, 王航远, 徐冠, 杨军, “SDN 安全探讨：机遇与威胁并存”, 2014/8.
[Online].Available: <http://www.arocmag.com/article/01-2014-08-003.html>
 130. Danda B. Rawat, Swetha R. Reddy, “Software Defined Networking Architecture, Security and Energy Efficiency: A Survey”, 2016/10.
[Online].Available: <http://ieeexplore.ieee.org/document/7593247/>
 131. Danda B. Rawat, Swetha R. Reddy, “Software Defined Networking Architecture,

- Security and Energy Efficiency: A Survey”, 2016/10.
 [Online].Available: <http://ieeexplore.ieee.org/document/7593247/>
132. M. Dhawan, R. Poddar, K. Mahajan, and V. Mann, in Proc. Netw. Distrib. Syst. Security (NDSS) Symp., San Diego, CA, USA, “ SPHINX: Detecting security attacks in software-defined networks,” pp. 1–15, 2015.
 [Online].Available:<https://people.eecs.berkeley.edu/~rishabhp/publications/Sphinx.pdf>
 133. X. Du, M.-Z. Wang,X. Zhang, and L. Zhu, “ Int. J. Security Appl., vol. 8, no. 5,” pp. 119–130, 2014.
 134. J. H. Jafarian, E. Al-Shaer, and Q. Duan, in Proc. 1st Workshop Hot Topics Softw. Defined Netw., Helsinki, Finland, “OpenFlow random host mutation: Transparent moving target defense using software defined networking,” pp. 127–132,2012.
 [Online].Available:<http://conferences.sigcomm.org/sigcomm/2012/paper/hotsdn/p127.pdf>
 135. H. Hu, W. Han, G.-J. Ahn, and Z. Zhao, in Proc. 3rd Workshop Hot Topics Softw. Defined Netw., Chicago, IL, USA, “FLOWGUARD: Building robust firewalls for software-defined networks,” pp. 97–102, 2014.
 [Online].Available:<https://people.cs.clemson.edu/~hongxih/papers/HotSDN2014.pdf>
 136. S. K. Fayazbakhsh, V. Sekar, M. Yu, and J., “FlowTags: Enforcing network-wide policies in the presence of dynamic middlebox actions,” pp. 19–24. [Online].Available: http://www3.cs.stonybrook.edu/~sfayazbakhsh/flowtags_hotsdn13.pdf
 137. Z. Qazi et al., in Proc. Open Netw. Summit, Santa Clara, CA, USA, “Practical and incremental convergence between SDN and middleboxes,” pp. 1–15, 2013.
 [Online].Available: https://nsl.cs.usc.edu/~rmiao/publications/Zafar13_.pdf
 138. Syed Akbar Mehdi, Junaid Khalid, Syed Ali Khayam, “Revisiting traffic anomaly detection using software defined networking”, 2011.
 [Online].Available: https://link.springer.com/chapter/10.1007/978-3-642-23644-0_9
 139. 王蒙蒙, 刘建伟, 陈 杰, 毛 剑, 毛可飞, "软件定义网络:安全模型、机制及研究进展", 2016. [Online].Available: http://www.jos.org.cn/ch/reader/create_pdf.aspx?file_no=5020&journal_id=jos
 140. Seugwon Shin , Phillip Porras , Vinod Yegneswaran , Martin Fong , Guofei Gu , Mabry Tyson," FRESCO: Modular Composable Security Services for Software-Defined Networks ", 2013/4.
 141. Marco Canini, Daniele Venzano, Peter Perešini, Dejan Kostić, Jennifer Rexford," A NICE way to test openflow applications", 2012/4. [Online].Available: <http://dl.acm.org/citation.cfm?id=2228312>
 142. Peter Perešini, Dejan Kostić, Jennifer Rexford, Marco Canini, Daniele Venzano, " A NICE way to test openflow applications", 2012/4.

143. Myung-Sup Kim, Hun-Jeong Kong, Seong-Cheol Hong, "A flow-based method for abnormal network traffic detection", 2004/4.
[Online]. Available: <http://ieeexplore.ieee.org/document/1317747/>
144. Zhichun Li, Yan Gao, Yan Chen, "HiFIND: A high-speed flow-level intrusion detection approach with DoS resiliency", 2009/10.
[Online]. Available: <http://www.sciencedirect.com/science/article/pii/S1389128609003375>
145. Rodrigo Braga, Edjard Mota, Alexandre Passito, " Lightweight DDoS flooding attack detection using NOX/OpenFlow", 2010/10.
[Online]. Available: <http://dl.acm.org/citation.cfm?id=1989764.1990427>
146. Seyed Mohammad Mousavi, Marc St-Hilaire, "Early detection of DDos attacks against SDN controllers", 2015/3.
[Online]. Available: <http://ieeexplore.ieee.org/document/7069319/>
147. Seungwon Shin, Vinod Yegneswaran, Phillip porras, Guofei Gu, "AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks", 2013/11.
[Online]. Available: <http://dl.acm.org/citation.cfm?id=2516684>
148. Sadler, M., Prelicpean, D., Sowinski, M., & Cucu, V., "Magic or Mischief: A look into Disney's adaptation of IoT", 2016/11/27.
149. Gates, B., Myhrvold, N., Rinearson, P., & Domonkos, D., "The road ahead", 1995.
150. ITU, "The Internet of Things", 2005/11.
151. Rick Merritt, "IoT Consumer Groups Merge", EETimes, 2016/10/10
[Online]. Available: http://www.eetimes.com/document.asp?doc_id=1330605
152. Stackowiak, R., Licht, A., Mantha, V., & Nagode, L., "Big Data and the Internet of Things (pp. 185-190)", 2015.
153. Hong, J., Shin, J., & Lee, D., "Strategic management of next-generation connected life: Focusing on smart key and car-home connectivity". *Technological Forecasting and Social Change*, 103, 11-20., 2016.
154. 吕廷杰, "物联网的由来与发展趋势", *信息通信技术*, 4(2), 4-8., 2010.
155. 廖國男, 楊雪芳, 李炫昇, "以物聯網 (IoT) 概念運用行動載具 (iPAD) 於提升住院病人會診時效" *醫務管理期刊*, 16(4), 345-358., 2015.
156. 張書瑋, "物聯網來了! 會計大數據的挑戰", *會計研究月刊*, (357), 76-81., 2015.
157. Beecham Research, "M2M World of Connected Services: The Internet of Things", 2015/11/4.
158. Encore Media Group, "IoT TECH EXPO", 2017.
[Online]. Available: <https://www.iotechexpo.com/europe/>
159. Gartner, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", 2017/1.

160. Ericsson Mobility Report, “Internet of Things outlook”, 2016/6.
[Online].Available: <https://www.ericsson.com/en/mobility-report/internet-of-things-outlook>
161. 3GPP GERAN #62 會議,“Cellular System Support for Ultra Low Complexity and Low Throughput Internet of Things”.
162. 3GPP RAN #69 會議報告, 2015/10/15.
[Online].Available: http://std-share.itri.org.tw/Content/Files/Report/Files/3GPP%20RAN69%E6%9C%83%E8%AD%B0%E5%A0%B1%E5%91%8A_E1030.pdf
163. Nokia, ” LTE evolution for IoT connectivity”, 2017.
[Online].Available: <https://resources.ext.nokia.com/asset/200178>
164. Ratasuk, Rapeepat, et al. "Overview of narrowband IoT in LTE Rel-13.", 2016 IEEE Conference on Standards for Communications and Networking (CSCN), 2016.
165. 3GPP TR 36.888, “Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE, v.12.0.0”, 2013/6.
166. ETSI TS 102 690 v2.1.1, “Machine-to-Machine communications(M2M): Functional architecture”,2013.
167. Yun, Miao, and Bu Yuxin. "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid.", IEEE, 2010/8/26.
168. Khan, R., Khan, S. U., Zaheer, R., & Khan, S, “Future internet: the internet of things architecture, possible applications and key challenges”, (pp. 257-260), IEEE, 2012/12.
169. Suo, H., Wan, J., Zou, C., & Liu, J., “Security in the internet of Things: A Review”, 2012 international conference on (Vol. 3, pp. 648-651), IEEE, 2012/3.
170. Botta, Alessio, et al. "On the integration of cloud computing and internet of things", 2014 International Conference on. IEEE, 2014.
171. Zanella, Andrea, et al. "Internet of things for smart cities", IEEE Internet of Things journal 1.1 (2014): 22-32.
172. 张晨光, 刘岩, 许伟, “智能医疗器械信息安全问题研究与对策. 中国药物警戒, 12(6)”, 363-365, 2015.
173. Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper”, 2016.
[Online].Available: <http://www.rohde-schwarz.com/appnote/1MA266>
174. 张万春, 陆婷, 高音, “NB-IoT 系统现状与发展”, *ZTE TECHNOLOGY JOURNAL*, 2017.
175. 麥毅廷, 陳振庸, 楊峻權, 張朝欽, “在 3G 與 LTE 的異質網路下多重無線存取技術整合之評估”, *Journal of Computer Science and Educational Technology*, 2(1), 61-78, 2012.
176. 郭昱賢, & 林盈達, “LTE 架構, 協定與效能”, 2011.

177. Rohde & Schwarz, “Narrowband Internet of Things - Whitepaper”, 2016.
[Online].Available: <http://www.rohde-schwarz.com/appnote/1MA266>
178. Zayas, A. D., & Merino, P. (2017, May). The 3GPP NB-IoT system architecture for the Internet of Things. In Communications Workshops (ICC Workshops), 2017 IEEE International Conference on (pp. 277-282). IEEE.
179. Wang, Y. P. E., Lin, X., Adhikary, A., Grövlén, A., Sui, Y., Blankenship, Y., ... & Razaghi, H. S. (2016). A primer on 3gpp narrowband internet of things (nb-iot). arXiv preprint arXiv:1606.04171.
180. Mahmoud, Rwan, et al,"Internet of things (iot) security: Current status, challenges and prospective measures." Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for. IEEE, 2015.
181. ITSA 學習資源服務平臺,“物聯網安全”.
[Online].Available: <https://lrs.itsa.org.tw/course/view.php?id=683#section-0>
182. 聂元铭, 张红军, & 韩惠良,“物联网的安全层级防护策略研究. 信息网络安全, (6), 0-0”,2011.
183. 武传坤,“物联网安全关键技术与挑战. 密码学报”, 2(1), 40-53, 2015.
184. 刘宴兵, 胡文平, 杜江, "基于物联网的网络信息安全体系", ZTE TECHNOLOGY JOURNAL 23, 2011.
185. Shah, P. G., & Ambareen, J., “A Survey of Security Challenges in Internet of Things (IoT) Integration with WSN”, AUSJOURNAL, 2014.
186. J.P Anderson, “Computer Security Threat Monitoring and Surveillance”, 1980/4.
187. Ashoor, A. S., & Gore, S., “Importance of intrusion detection system (IDS)”, International Journal of Scientific and Engineering Research, 2(1), 1-4., 2011.
188. 蔡秉任,“針對未知攻擊辨識之混合式入侵偵測系統(碩士論文)”, 2014.
189. Al Ameen, M., Liu, J., & Kwak, K., “Security and privacy issues in wireless sensor networks for healthcare applications.”, Journal of medical systems, 36(1), 93-101., 2012
190. Padmavathi, D. G., & Shanmugapriya, M., “A survey of attacks, security mechanisms and challenges in wireless sensor networks”, 2009.
191. Ye, N., Zhu, Y., Wang, R. C., & Lin, Q. M., “An efficient authentication and access control scheme for perception layer of internet of things”, 2014.
192. Mlelwa, K. L., & Yonah, E. D. Z. O., “CHALLENGES THAT RESTRICT THE EFFICIENCIES OF SECURITY FRAMEWORKS IN E-COMMERCE: A REVIEW”, 2017/3.
193. 武传坤,“物联网安全架构初探”, 中国科学院院刊第 25 卷第 4 期, 2010/5/17.
194. Angrishi, K., “Turning Internet of Things (IoT) into Internet of Vulnerabilities (IoV): IoT Botnets”, 2017/2/13.
195. Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J., “DDoS in the IoT: Mirai and Other

- Botnets”. IEEE, 2017/7/7.
196. 大紀元, “鎖定陸製網路攝影機 恐 12 萬台染病毒”, 2017/05/12.
[Online].Available: <http://www.epochtimes.com/b5/17/5/12/n9135597.htm>
197. iThome, “全球 12 萬臺中國製網路攝影機, 恐受殭屍病毒 Persirai 感染”, 2017/5/11.
[Online].Available: <http://www.ithome.com.tw/news/114093>
198. Graham Cluley, “Persirai IoT botnet threatens to hijack over 120,000 IP cameras”, 2017/5/11.
[Online].Available: <https://www.tripwire.com/state-of-security/featured/persirai-iot-botnet-hijacks-over-120000-ip-cameras/>
199. Trend Micro, “Persirai: New Internet of Things (IoT) Botnet Targets IP Cameras”, 2017/5/9.
[Online].Available: <http://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/>
200. 3GPP 官網, [Online]. Available: <http://www.3gpp.org/about-3gpp/about-3gpp>
201. 3GPP TS 33.216, “Security Assurance Specification (SCAS) for the evolved Node B (eNodeB) network product class (Release 15)”.
202. GSMA, “Network Equipment Security Assurance Scheme Overview (Version 0.3)”, 2016/5/11.
203. GSMA, “FS.14 Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation (Version 0.7) ”, 2016/3.
204. GSMA, “Network Equipment Security Assurance Scheme – Vendor Development and Product Lifecycle Requirements and Accreditation Process (Version v0.21), 2016/6.
205. GSMA, “ FS.16 Network Equipment Security Assurance Scheme - Dispute Resolution Process (Version 0.3)”, 2016/3/16.
206. GSMA, “IoT Security Guidelines Overview Document”, 2016/2.
207. GSMA, “IoT Security Guidelines for Service Ecosystems”, 2016/2.
208. GSMA, “IoT Security Guidelines for Endpoint Ecosystems”, 2016/2.
209. GSMA, “IoT Security Guidelines for Network Operators”, 2016/2.
210. CC 官網, [Online]. Available:<https://www.commoncriteriaportal.org/>
211. 吳專吉・謝宛真(Wan-Chen Hsieh), ”資通產品安全性共同準則評估檢測技術發展現況, 國防部新季刊第四十一卷第四期”, 2013/10
212. NIST FISMA, H.R. 2458 - E-Government Act of 2002.
[Online].Available: <http://csrc.nist.gov/drivers/documents/FISMA-final.pdf> (last visited:2017/8/25).
213. NIST, “RISK MANAGEMENT FRAMEWORK (RMF) OVERVIEW”.
[Online].Available: <http://csrc.nist.gov/groups/SMA/fisma/framework.html> (last visited:2017/8/25).

214. WhiteHouse, “Executive Order -- Improving Critical Infrastructure Cybersecurity”, 2013/2/12.
[Online].Available: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity> (last visited:2017/8/25).
215. NIST, “Cybersecurity Framework”.
[Online].Available: <https://www.nist.gov/cyberframework>(last visited:2017/8/25)
216. WhiteHouse, “Presidential Policy Directive -- Critical Infrastructure Security and Resilience”, PRESIDENTIAL POLICY DIRECTIVE/PPD-21.
[Online].Available: <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil> (last visited:2017/8/25).
217. WhiteHouse, “Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”.
[Online].Available: <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal> (last visited:2017/8/25).
218. DHS, “Critical Infrastructure Sectors”.
[Online].Available: <https://www.dhs.gov/critical-infrastructure-sectors> (last visited:2017/8/25).
219. DHS, “Critical Infrastructure Cyber Community C³ Voluntary Program”.
[Online].Available: <https://www.dhs.gov/ccubedvp> (last visited:2017/8/25).
220. WhiteHouse, Executive Order -- Promoting Private Sector Cybersecurity Information Sharing, [Online].Available: <https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari> (last visited:2017/8/25).
221. DHS, “Cyber Information Sharing and Collaboration Program (CISCP)”.
[Online].Available: <https://www.dhs.gov/ciscp> (last visited:2017/8/25).
222. Public Security Canada, “Fundamentals of cyber security for Canada’s Critical Infrastructure Community”, p.5, 2016.
[Online].Available: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf>
223. Public Safety Canada, “Fundamentals of cyber security for Canada’s Critical Infrastructure Community”, 2016.
[Online].Available:<https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/2016-fndmntls-cybr-Scrty-cmmnty-en.pdf>
224. Public Safety Canada, “Report a Cyber Security Incident”.

- [Online].Available: <https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/rprt-en.aspx>
225. Government of Canada , “Cyber Incident Management Framework for Canada”, 2013.
[Online].Available: <https://www.publicsafety.gc.ca/cnt/rsrscs/pblctns/cbr-ncdnt-frmwrk/cbr-ncdnt-frmwrk-eng.pdf>
226. EU, “Special Eurobarometer 423 CYBER SECURITY REPORT”, 2014/10.
[Online].Available:
http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf
227. EU, ”Internal security strategy for the European Union Towards a European security model”, 2010/3.
[Online].Available:
https://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf
228. EU, “Europe 2020 strategy”,2010/5.
[Online].Available: https://ec.europa.eu/info/strategy/european-semester/framework/europe-2020-strategy_en
229. EU, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace”, 2013/2.
230. EU, “DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union”, 2016/7.
231. EU, “Green Paper on a European programme for critical infrastructure protection”, 2005/11.
232. EU, “COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection”, 2008/12.
233. European Commission 官網.
234. EU, “Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience”, 2009/3.
235. EU, “Achievements and next steps: towards global cyber-security”, 2011/3.
236. EU ENISA, “Stocktaking, Analysis and Recommendations on the Protection of CIIs”, 2016/1.
237. EU, “Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision”, 2013/12/8.
238. EU, “The Mid-Term Review on the implementation of the Digital Single Market Strategy A Connected Digital Single Market for All”, 2017/10.
239. UK Cabinet Office, “UK Cyber Security Strategy of the United Kingdom”, 2009/06.
240. 資策會科法所, 英國政府將設置兩個新的網路安全機關以維護國家網路安全, 葉

亭巖, 2009/7。

241. Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003, 2014-08.
242. UK Emergency Power Act 1920, ss. 1(1), 2(1).
243. POSTNOTE, Cyber Security of UK Infrastructure, The Parliamentary Office of Science and Technology, Number 554., 2017/5.
244. UK Cabinet Office, 2016 Sector Security and Resilience Plans.
245. National Cyber Security Centre 官網, “Cyber Security Information Sharing Partnership (CiSP)”.
246. National Fraud & Cyber Crime Reporting Centre 網站.
247. NCA Strategic Cyber Industry Group Cyber Crime Assessment 2016, 2016/7.
248. NSCS, The cyber threat to UK business 2016/2017 Report, 2017.
249. EU, DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, 2016/7.
250. Out-Law.com, “Network and Information Security Directive will be implemented in the UK despite Brexit vote, government confirms”, 2017/1/4.
251. 木暮仁, “中央官庁Webページ集中改ざん事件（2000年）”.
252. 内閣官房情報セキュリティセンター, “情報セキュリティ戦略元年— わが国の情報セキュリティ政策の現状 —”, 2007.
253. 情報セキュリティ政策会議, “我が国のサイバーセキュリティ推進体制の機能強化に関する取組方針”, 2014.
254. 内閣官房情報セキュリティセンター, “情報セキュリティ緊急支援チーム（CYMAT）設置について”, 2012.
255. 网络安全基本法第6條、第14條。内閣サイバーセキュリティセンター, “重要インフラ等に係るサイバーセキュリティ政策の概要”, 2016.
256. サイバーセキュリティ戦略本部, “重要インフラの情報セキュリティ対策に係る第4次行動計画”, 2017.
257. サイバーセキュリティ戦略本部, “「重要インフラの情報セキュリティ対策に係る第4次行動計画」のパブリックコメント案”, 2017.
258. Ofcom, Review of Security Guidance.
259. CBEST, Bank of England.
260. FTC, “Cases and Precedings: Lenovo, Inc.”, 2017/9.
261. NIST SP 800-187, “Guide to LTE Security”, 2017/12.
262. ETSI TR 103 456, “CYBER; Implementation of the Network and Information Security (NIS) Directive”, 2017/10.
263. 行政院國家資通安全會報, “行政院國家資通安全會報組織架構圖”, 2016/8/1.

264. 交通部, “國家關鍵基礎設施安全防護指導綱要”, 2014/12/29.
265. Yahoo 新聞, “4G 網絡存在 8 種漏洞, 用戶手機安全及私隱無保障”, 2018/3/5, [Online]. Available: <https://tw.news.yahoo.com/4g-%E7%B6%B2%E7%B5%A1%E5%AD%98%E5%9C%A8%E7%A8%AE%E6%BC%8F%E6%B4%9E-%E7%94%A8%E6%88%B6%E6%89%8B%E6%A9%9F%E5%AE%89%E5%85%A8%E5%8F%8A%E7%A7%81%E9%9A%B1%E7%84%A1%E4%BF%9D%E9%9A%9C-101438714.html>
266. The Hacker News, “Hackers Using Fake Cellphone Towers to Spread Android Banking Trojan”, 2017/3/22.
267. Hussain, S. R., Chowdhury, O., Mehnaz, S., & Bertino, E. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE.
268. C. Gessner and A. Roessler, "LTE technology and LTE test; a deskside chat," Rohde & Schwarz, 2009.
269. Ettus Research, [Online]. Available: <https://www.ettus.com/product/details/UB210-KIT>
270. Open LTE, [Online]. Available: <http://openlte.sourceforge.net/>
271. srsLTE, [Online]. Available: <https://github.com/srsLTE/srsLTE>
272. OpenAirInterface, [Online]. Available: <http://www.openairinterface.org/>
273. D. Herceg, "LTE transport security", *Proc. 34th Int. Conv. MIPRO*, pp. 1464-1467, May 2011.
274. M. Labib, V. Marojevic, J. Reed, "Analyzing and Enhancing the Resilience of LTE/LTE-A Systems to RF Spoofing", *IEEE Conf Standards for Commun. and Net. Proc.*, pp. 160-65, 2015-Oct.
275. 偽基站識別方法及裝置, 專利公開號: CN 106572450 A
276. 一種偽基站定位方法及系統, 專利公開號: CN 106162688 A
277. Shiomoto, Kohei, and Naoaki Yamanaka. "Circuit-switched network." U.S. Patent No. 6,731,628. 2004/5/4.
278. Radio-Electronics.com, “SRVCC Single Radio Voice Call Continuity”.
279. AT&T, “AT&T’s Voice Over LTE Network Reaches More than 27 Million Subscribers”, 2015/12/29.
280. 鄧勇志, “全球 VoLTE 市場前景看好 中國移動完成部署”, 2016/7/21.
281. 郭昱賢 林盈達, “LTE 架構、協定與效能”, 2011/9/30.
282. Chewe, Mutale. "VoLTE by IP Multimedia Subsystem.", 2015.
283. GSMA : VoLTE Service Description and Implementation Guidelines Version 2.0.
284. Ventuzelo, Patrick, Olivier Le Moal, and Thomas Coudray. "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone", 2017.

285. Cuevas, Antonio, et al. "The IMS service platform: a solution for next-generation network operators to be more than bit pipes." *IEEE Communications Magazine* 44.8: 75-81., 2006.
286. J.Rosenberg, H.Schulzrinne, G.Camarillo, A.Johnston, J.Peterson, R.Sparks, M.Handley, E.Schooler, "SIP: Session Initiation Protocol", 2002/6.
287. Ventuzelo, Patrick, Olivier Le Moal, and Thomas Coudray. "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone."
288. GSM Association. "VoLTE Service Description and Implementation Guidelines." 2014.
289. Johnston, Alan B. "SIP: understanding the session initiation protocol." Artech House, 2015.
290. Zhang, Shen, et al. "Automatic Detection of SIP-Aware Attacks on VoLTE Device." *Vehicular Technology Conference (VTC-Fall)*, 2016 IEEE 84th. IEEE, 2016.
291. 3GPP. ETSI TS 23.228. IP Multimedia Subsystem (IMS) Stage 2, 2011.
292. Li, Chi-Yu, et al. "Insecurity of voice solution volte in LTE mobile networks." *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2015.
293. CabelFree, "LTE S5/S8 Interface – Interfaces between the S-GW and P-GW", [Online]. Available: <http://www.cablefree.net/wirelesstechnology/4glte/lte-s5-s8-interface-s-gw-p-gw/>
294. Ventuzelo, Patrick, Olivier Le Moal, and Thomas Coudray. "Subscribers remote geolocation and tracking using 4G VoLTE enabled Android phone.", *SSTIC Conference*, 2017/6.
295. Park, Seongmin, et al. "Security threats and countermeasure frame using a session control mechanism on VoLTE." *Broadband and Wireless Computing, Communication and Applications (BWCCA)*, 2015 10th International Conference on. IEEE, 2015.
296. Jennings, Cullen, Jon Peterson, and Mark Watson. "Private extensions to the Session Initiation Protocol (SIP) for asserted identity within trusted networks.", 2002.
297. Hautakorpi, Jani, et al. Requirements from Session Initiation Protocol (SIP) Session Border Control (SBC) Deployments. No. RFC 5853. 2010.
298. Said, Siwar Ben Hadj, et al. "New control plane in 3GPP LTE/EPC architecture for on-demand connectivity service." *Cloud Networking (CloudNet)*, 2013 IEEE 2nd International Conference on. IEEE, 2013.
299. Liao, Hung-Jen, et al. "Intrusion detection system: A comprehensive review." *Journal of Network and Computer Applications* 36.1 (2013): 16-24.
300. Real Time Communication, [Online]. Available: "SIP Illustrated 2: SIP Message", <https://realtimecommunication.wordpress.com/2017/02/09/sip-illustrated-2-sip-message/>

301. Drage, Keith, Roland Jesske, and Christer Holmberg. "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3GPP." (2014).
302. Google Maps Geolocation API”, Google,2017/6/4, [Online]. Available: <https://developers.google.com/maps/documentation/geolocation/intro?hl=zh-tw,”>
303. 3GPP, TS 36.300 Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Release 14, 2017/6
304. 3GPP, TR 33.821 Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved (LTE) RAN / 3GPP System Architecture Evolution (SAE), 2009/6
305. GSMA NESAS, [Online]. Available: https://www.gsma.com/aboutus/wp-content/uploads/2017/03/FS.13-NESAS-Overview-Pilot-Release_0.3.pdf
306. Extension of time for telecom testing and security certification, [Online]. Available: <http://www.dot.gov.in/sites/default/files/2017%2003%2029%20Extension%20of%20Time%20for%20Telecom%20Testing%20and%20Security%20Certification.pdf>
307. Mandatory Testing and Certification of Telecom Equipments, [Online]. Available: <http://www.tec.gov.in/mandatory-testing-and-certification-of-telecom-equipments/>
308. FakeImageExploiter, [Online]. Available: <https://github.com/r00t-3xp10it/FakeImageExploiter>
309. Transport Layer Protection Cheat Sheet, [Online]. Available: https://www.owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
310. 3GPP. Technical Specification Group Services and System Aspects; Security of H(e)NB; Release 8, TR 33.820.
311. Chengzhe Lai, Hui Li, Yueyu Zhang, Jin Cao, “Simple and low-cost re-authentication protocol for HeNB,” China Communications, Vol.10, No.1, pp.105-115, 2013.
312. Chan-Kyu Han, Hyoung-Kee Choi, In-Hwan Kim, Building femtocell more secure with improved proxy signature. In: Global Telecommunications Conference, pp. 1–6 (2009) 8.
313. RCR Wireless News , “LTE MMEA Core Connector for LTE”, 2014/5/9. [Online]. Available: <http://www.rcrwireless.com/20140509/diameter-signaling-controller-dsc/lte-mme-epc>
314. Meyer, U., & Wetzel, S. (2004, October). A man-in-the-middle attack on UMTS. In Proceedings of the 3rd ACM workshop on Wireless security (pp. 90-97). ACM.
315. 3GPP TS 23.002 V14.1.0, 2017/3.
316. 3GPP TS 23.401 V15.1.0, 2017/9.
317. Olsson, M., & Mulligan, C. (2012). EPC and 4G packet networks: driving the mobile broadband revolution. Academic Press

318. 3GPP TS 36.410 V14.0.0 (2017-03)
319. 3GPP TS 29.274 V15.0.0 (2017-06)
320. 3GPP TS 29.272 V15.0.0, 2017/6.
321. LTE and Beyond, "Interfaces and their protocol stacks", 2012/1/8. [Online]. Available: <http://www.lteandbeyond.com/2012/01/interfaces-and-their-protocol-stacks.html>
322. HASSAN, Zakaria Zakaria; ELGARF, Talaat A.; ZEKRY, Abdelhalim. Modifying authentication techniques in mobile communication systems. In: Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2014 Third International Conference on. IEEE, 2014. p. 38-44
323. Chang, C. C., Lee, J. S., & Chang, Y. F. (2005). Efficient authentication protocols of GSM. *Computer Communications*, 28(8), 921-928.
324. Choudhary, Anilmit, and Randhir Bhandari. "Analysis of UMTS (3G) Authentication and Key Agreement Protocol (AKA) for LTE (4G) Network." *International Journal on Recent and Innovation Trends in Computing and Communication* 3.4 (2015): 2146-2149.
325. 3GPP TS 33.102: "3G security; Security architecture".
326. Orhanou, G., Hajji, S. E., Bentaleb, Y., & Laassiri, J. (2011). EPS confidentiality and integrity mechanisms algorithmic approach. *arXiv preprint arXiv:1102.5191*.
327. 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3"
328. Karandikar, A., Akhtar, N., & Mehta, M. (2017). *Mobility Management in LTE Heterogeneous Networks*. Springer Singapore.
329. Choudhury, H., Roychoudhury, B., & Saikia, D. K. (2012, June). Enhancing user identity privacy in LTE. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 949-957). IEEE.
330. ng4T, [Online]. Available: <http://www.ng4t.com/forensics.html>
331. Han, C. K., Choi, H. K., Baek, J. W., & Lee, H. W. (2009, October). Evaluation of authentication signaling loads in 3GPP LTE/SAE networks. In *Local Computer Networks, 2009. LCN 2009. IEEE 34th Conference on* (pp. 37-44). IEEE.
332. Purkhiabani, M., & Salahi, A. (2012). Enhanced authentication and key agreement procedure of next generation 3GPP mobile networks. *International Journal of Information and Electronics Engineering*, 2(1), 69.
333. Banescu, S., & Posea, S. Security of 3G and LTE. Faculty of Computer Science, Eindhoven University of Technology.
334. HUSSAIN, Syed Rafiul, et al. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE.

335. Bikos, A. N., & Sklavos, N. (2013). LTE/SAE security issues on 4G wireless networks. *IEEE Security & Privacy*, 11(2), 55-62.
336. CVE, [Online]. Available: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15326>
337. Anshu Tripathi, Umesh Kumar Singh, Taxonomic Analysis of Classification Schemes in Vulnerability Databases.
338. P1 Security, <http://www.p1sec.com/corp/>
339. Andrea F. Cattoni et al., "An End-to-End Testing Ecosystem for 5G the TRIANGLE Testing House Test Bed", *Journal of Green Engineering*, 2016/12.
340. Aleksandr Ometov, Pavel Masek, Jani Urama, Jiri Hosek, Sergey Andreev, and Yevgeni Koucheryav, "Implementing Secure Network-Assisted D2D Framework in Live 3GPP LTE Deployment", 2016 IEEE International Conference on Communications Workshops (ICC), 2016/5.
341. Almudena D'iaz-Zayas(B), Cesar A. Garc'ia-P'erez, 'Alvaro M. Recio-P'erez, and Pedro Merino-G'omez, "PerformLTE: A Testbed for LTE Testing in the Future Internet", 13th International Conference, WWIC 2015, Malaga, Spain, May 25-27, 2015.
342. K. Jijo George, A. Sivabalan, T. Prabhu and Anand R. Prasad, "End-to-End Mobile Communication Security Testbed Using Open Source Applications in Virtual Environment", *Journal of ICT Standardization*, 2015/7.
343. Jill Jermyn, Roger Piqueras Jover, Mikhail Istomin and Ilona Murynets, "Firecycle: A scalable test bed for large-scale LTE security research", 2014 IEEE International Conference on Communications (ICC), 2014/6.
344. Tutorials Point, LTE Network Architecture, 2012/11/14.
345. 3G4G blog, Small Cells: Comparison and Deployment Scenarios, 2012/11/14.
346. 新通訊, NAS/MAC/PHY 各司其職 LTE 通訊協定預埋 4G 伏筆, 2009/10.
347. Jim Johnston, Evolving the Evolved Packet Core, 2011/2/2.
348. 楊朝成, 強化 4G LTE 認證及換手機制, 國立中興大學資訊管理學系, 2015/7.
349. Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi and Jean-Pierre Seifert, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems", 21-24, 2016/2.
350. Chan-Kyu Han and Hyoung-Kee Choi, "Security Analysis of Handover Key Management in 4G LTE/SAE Networks", *IEEE Transactions on Mobile Computing*, 2014.
351. Thanos Polychronis, "4G LTE: Architecture and Security Concerns", 2014/05/06.
352. COTS Journal, "LTE Networking Aids Battlespace Visualization Systems", 2013/12.
353. GSMA, "GSM Association Official Document IR.92 - IMS Profile for Voice and SMS", 2013/3/3.

- 354. 新通訊, "汰換老舊電信語音服務 VoLTE 跨網互通技術有譜", 2016/10.
- 355. Daksha Bhasker, "4G LTE Security for Mobile Network Operators", Journal of Cyber Security and Information Systems, 2013/9/10.
- 356. Radisys, "Core Network Optimization: The Control Plane, Data Plane & Beyond", 2012/11/01.
- 357. 微閱號, 挺進 5G 時代, 怎能不瞭解 MEC?, 2017/4/15.
- 358. iThome, 資料中心網路環境面臨重大變革: SDN 與 NFV 崛起, 軟體將主宰網路, 2012/11/14.
- 359. ETSI, "Network Functions Virtualisation (NFV); Management and Orchestration", GS NFV-MAN 001 V1.1.1, 2014/12.
- 360. 新通訊, "當 SDN 遇上 NFV 虛擬化 5G 核心網路掀革", 2016/03.
- 361. THE FAST MODE, "Singapore's M1 to Roll Out Cloud-based Virtual Enhanced Packet Core (vEPC)", 2017/5.
- 362. THE FAST MODE, "NTT DOCOMO Leverages Ericsson's Open NFV Platform for Multi-Vendor vEPC", 2016/3/14.
- 363. Security Focus Bugtraq ID database.
- 364. United States - Computer Emergency Readiness Team.
- 365. Common Vulnerabilities and Exposures.
- 366. Microsoft Knowledge Base article.
- 367. Open Vulnerability and Assessment Language.
- 368. McGraw, "Software Security: Building Security In", Addison-Wesley's Software Security Series, Pearson Education, 2006.
- 369. ITS4. [Online]. Available: <http://www.cigital.com/its4/>
- 370. FlawFinder. [Online]. Available: <http://www.dwheeler.com/flawfinder/>
- 371. RATS. [Online]. Available: <http://www.securesoftware.com/>
- 372. Abhinav Biswas, "Insights Into Modern Day Threat Protection", Electronics Corporation of India Ltd, ECIL, 2015/5/2.
- 373. 國家通訊傳播委員會, "行動寬頻基地臺射頻設備技術規範", 2015/11/24.