106 年度委託研究報告

建置基站資安檢測環境計畫(第 2 期)
委託研究案期末報告(附錄)

計畫委託機關：國家通訊傳播委員會

中華民國 107 年 5 月

目　　錄

附錄一 出國參訪報告

考察芬蘭行動寬頻資安檢測技術、資安最新趨勢與新興電信網路最新發展

目次

圖目錄

表目錄

第一章、 參訪目的

有鑑於於目前電信技術大多由歐美國家所引領，許多先進行動寬頻資安技術也會在國外發表，本計畫希望藉由參訪國外行動寬頻資安檢測實驗室、研究中心，蒐集國外最新行動寬頻資安威脅與防護技術、國際標準組織與政府之資安防護規範，以做為本計畫建置基站資安檢測平臺及制定檢測項目與檢測規範草案之參考。

本團隊在研究過程中發現，國際上少有設置行動寬頻網路安全實驗室之機構，此次特別約訪到 Nokia 設置於芬蘭總公司埃斯波(Espoo)之 Nokia Security Center(原設置於德國柏林，2017 年遷移至 Espoo)，參訪其行動寬頻網路安全實驗室及資安攻擊實例與防護解決方案，期能透過與 Nokia 行動寬頻網路安全專家交流最新行動寬頻資安威脅與防護方式，及國際標準組織最新動態；另約訪芬蘭國家技術研究中心(VTT)期能了解歐盟及芬蘭政府於行動寬頻資安及未來新技術發展之動態；與行動寬頻資安檢測軟體開發商 Synopsys R&D Center，進行資安檢測技術交流。

希望透過本次國外參訪與技術交流，蒐集到行動寬頻資安最新趨勢、行動寬頻資安檢測技術、國際標準最新之資安防護資訊，及新興電信網路發展等相關資訊。

第二章、 參訪行程

一、 總行程規劃

本次參訪天數共 8 天，共安排 5 天之參訪行程，3 天為飛機飛行時間，總行程規劃如下表。

表 1、總行程表

日期	行程	地點
9 月 23 日-9 月 24 日	台北➔芬蘭赫爾辛基➔芬蘭奧盧(Oulu)	啟程至芬蘭奧盧
9 月 25 日	參訪行動寬頻資安檢測軟體開發商 Synopsys R&D Center	奧盧(Oulu)
9 月 26 日-9 月 28 日	參訪電信設備製造商 Nokia Security Center	埃斯波(Espoo)
9 月 29 日	參訪芬蘭國家技術研究中心(VTT)	埃斯波(Espoo)
9 月 29 日-9 月 30 日	芬蘭赫爾辛基➔台北	歸途

二、 日行程規劃

本次參訪首日安排至芬蘭之研發重鎮奧盧(Oulu)，拜訪行動寬頻資安檢測軟體開發商 Synopsys R&D Center，直接與 NCC 購買之未知漏洞模糊檢測軟體(Defensics)研發人員進行技術交流；參訪第 2 天至第 4 天，為本次參訪行程之主要重點-電信設備製造商 Nokia Security Center，因該單位為全球少數因行動寬頻資安議題所成立之單位，故此行希望透過該單位之相關經驗，以及藉由該團隊專家參與國際標準組織 SA Group 討論，學習行動寬頻資安防護技術及國際標準最新趨勢，故於行程中安排 3 天之交流；第 5 天參訪行程特別到芬蘭國家技術研究中心(VTT)，該中心之角色如我國之工研院，為北歐最大應用研究組織，透過與 VTT 交流希望可了解目前北歐國家對行動寬頻網路安全、5G 與 IoT 之最新發展。各單位之參訪日程及議題如下表。

表 2、日行程規劃

日期	參訪單位	討論議題
9/25	Synopsys R&D Center	• Defensics Introduction • Roadmap session 　– Defensics2017.09 and 2017.12 release contents 　– Upcoming new suite releases • Demo session 　– OSX Bluetooth testing demo 　– NFS vulnerability presentation and demo • TTC feedback session • Protecode introduciotn
9/26	Nokia Security Center	• NetGuard Portfolio introduction • Live demo • NetGuard Identity and Access Manager- 　– The demo shows how the system enables fine-granular access control to administrative interfaces for a system which itself only has a coarse access control inbuilt. • Endpoint Security-Live demo 　– The demo shows how an attacker hijacks the video feed of an CCTV camera (IoT device). 　– The demo shows how a mobile phone gets infected and how the attacker harvests personal data and remotely takes pictures of the subscriber.
9/27	Nokia Security Center	• DDoS detection and mitigation over future networks 　– Context of a network critical application: Remote Surgery via Cloud 　– Requires reliable bandwidth/latency 　– Sensitive medical/patient data stored in this cloud for the operation 　– Potential prime target for DDoS+Stealing data • Interconnection Security 　– SS7 Security- Live Demo 　– Diameter Security 　– IoT & Interconnection • Compliance & Regulation from GSMA & 3GPP & ITU Security guideline Worldwide security deploys status and audit requirement.

日期	參訪單位	討論議題
9/28	Nokia Security Center	• Nokia LTE Public Safety − Introduction − Spectrum & Standardization − E2E Ecosystem & Architecture − Deployment options − E2E Portfolio − LTE Public Safety cases − Live Demo • Compliance & Regulation from GSMA & 3GPP & ITU Security guideline Worldwide security deploys status and audit requirement.
9/29	VTT	• Tour of Millimeter-wave lab • VTT introduction • TTC introduction • 5G & IoT testbeds TAKE-5 & 5GTNF • TTC projects and expectations • 5GPPP-ENSURE project • SDN security demo • Discussion on collaboration opportunities

第三章、 參訪單位

一、 Synopsys R&D Center

Synopsys 是全球半導體設計與製造軟體的領導廠商，且其位於芬蘭的 R&D Center，為 Synopsys 公司於 2015 年 4 月所併購的一家資訊安全檢測軟體公司-Codenomicon，該公司致力於發展通訊協定弱點的模糊測試，主要產品為 Defensics 未知漏洞模糊檢測工具，該檢測工具為 1996 年芬蘭奧盧(OULU)大學所研發，是世界上最早研究模糊測試的工具，目前已普遍被各國電信業者、通訊設備製造商、政府機關、軟體開發公司、金融業及醫療保健產業等所採用。Synopsys 於芬蘭設置未知漏洞檢測軟體(Defensics)研發中心及檢測實驗室，展示其軟體於行動寬頻網路之相關資安檢測及應用。

二、 Nokia Security Center

有鑒於 LTE 全 IP 化之網路及小型基站網路之發展，行動網路之安全威脅提升，因此 Nokia 在 2014 年於德國柏林設立 Nokia Security Center，該中心建構了一套完整的 4G / LTE 測試網絡，與相關安全檢測工具，成立之目的為洞察各種行動寬頻網路之威脅，提供業者保護行動寬頻網路安全之解決方法及建議。2017 年該公司將 Nokia Security Center 遷移至總公司於埃斯波(Espoo)展示中心，與 Nokia Executive Experience Center 同一個地點，期能為客戶提供更完整的展示環境與全方位的產品體驗。

三、 VTT Technical Research Centre

北歐研究機構芬蘭國家科技研究中心(VTT) 成立於 1942 年，隸屬芬蘭就業與經濟部（MINISTRY OF ECONOMIC AFFAIRE AND EMPLOYMENT，簡稱 MEE）的國有研究機構，員工人數約 2,470 人，約 68%為技術人員，14%為研究人員，博士佔總員工人數之 25%。VTT 為北歐最大的研發組織，其成立宗旨為推動技術產業化，提供客戶高科技解決方案及創新服務，研究範圍涵蓋電子學、資訊技術、工業系統、生物工程及建築運輸等領域。其藉由在交叉學科研究領域的優勢，把新技術轉變為產品，分拆出 21 家新創公司，分享收益，並為超過 1,500 家不同領域的客戶提供服務，包括對產品和服務的未來預測和策略研究、知識產權和授權服務，以及全面的測試和認證服務等。

該單位除在芬蘭 6 個城市設置辦公室及實驗環境外，並在韓國、巴西及比利時設有分支機構，在科學研究領域屬世界一流水準。VTT 是芬蘭國家創新體系的重要組成部分，其於行動通訊網路(2G、3G、4G and 5G)之發展及網路安全領域皆有提供相關技術研發與服務，對北歐行動寬頻技術之發展具有重大之貢獻。

第四章、 參訪紀要及過程

一、 9/25 Synopsys R&D Center 參訪紀要

第一天我們抵達位於芬蘭北部工業及研發重鎮-奧盧(Oulu)，Oulu 被認為是歐洲的生活實驗室之一，居民在社區範圍內實驗許多新技術，此地區係以先進技術文明，ICT 產業自 80 年代起飛，至今已經發展到全球規模，芬蘭許多企業的研發單位皆設置於此地的研發園區中，研發園區設置的區域鄰近芬蘭著名之奧盧大學，奧盧大學也因此與產業有許多的產學合作，該研發園區公司許多員工也是由奧盧大學畢業。

第一天的參訪行程為行動寬頻資安檢測軟體開發商 Synopsys R&D Center，該單位致力於研發通訊協定弱點的模糊測試，主要產品為 Defensics，也是 NCC 為本計畫採購的檢測工具之一，模糊測試是一種透過自動測試達到發現漏洞的技術，屬於軟體測試中黑箱測試的一部份，工作原理是以自動或半自動的生成隨機數據輸入到一個程式中，並監視程式之異常行為，如系統當機、資訊洩露、延遲等現象缺陷，以發現可能的程式錯誤或協定漏洞，管理未知漏洞所造成的威脅。NIST、GSA 都將其視為安全檢測基礎套件，美國某些電信業者(如 Verizon)亦要求其所購入之通訊設備須先進行 Defensics Fuzzy Test。

本計畫主要將此軟體用於行動寬頻基站對基站，及基站對 EPC 信令交握須使用的基礎通訊協定(SCTP、S1-AP、X2-AP…etc.)檢測。而本計畫之測試標的物(基站)，為國際上各電信業者及檢測實驗室較少聚焦之範疇，因此此行本計畫團隊執行檢測之人員，希望藉由直接與研發人員的技術交流，能學習到其操作原理，及測試案例，可供本計畫於檢測規劃及執行，甚至做為訂定檢測規範草案時之參考。

此行與 Defensics 軟體研發人員首先向我們介紹目前該軟體未來研發目標與發展重點，也向我們實際演示最新開發功能包含麥金塔系統藍芽裝置弱點、網路檔案服務(NFS) 弱點檢測，與提供客戶端自行開發檢測平臺之軟體開發套件(Software Development Kit，簡稱 SDK)等，該軟體同時也開始朝向雲端發展，未來希望讓用戶端可以直接將欲分析的軟體上傳至此系統進行分析並取得報告，其中主要包含弱點評估、高度侵權回報、誤用影響及資訊洩漏等。以下為會議中討論議題之紀要。

圖 1、與 Synopsys R&D Center 與會人員合影

(一)Defensics 現有產品維護及未來發展策略

基於目前因應各式行動裝置需求，相應的通訊協定過於繁雜，因此該公司目前為符合國際資安檢測需求，該產品發展策略開始朝向未來 IoT 等行動通訊協定及 user friendly 的方向研發。針對該公司研發人員的介紹，將其主要發展方向歸納如下：

增加新通訊協定支援與持續更新既有產品配套。

與軟體整合平台(Software Integrity Platform，簡稱 SWIP)結合，以提升系統在發展生命週期(System Development Life Cycle，簡稱 SDLC)中，能兼顧的安全與品質，下圖 2 所示。

增進對於無線相關通訊協定的支援，尤其是 IoT 與行動通訊方面。

延續客戶使用經驗並廣泛結合於現有產品，以增加用戶體驗的黏著性。

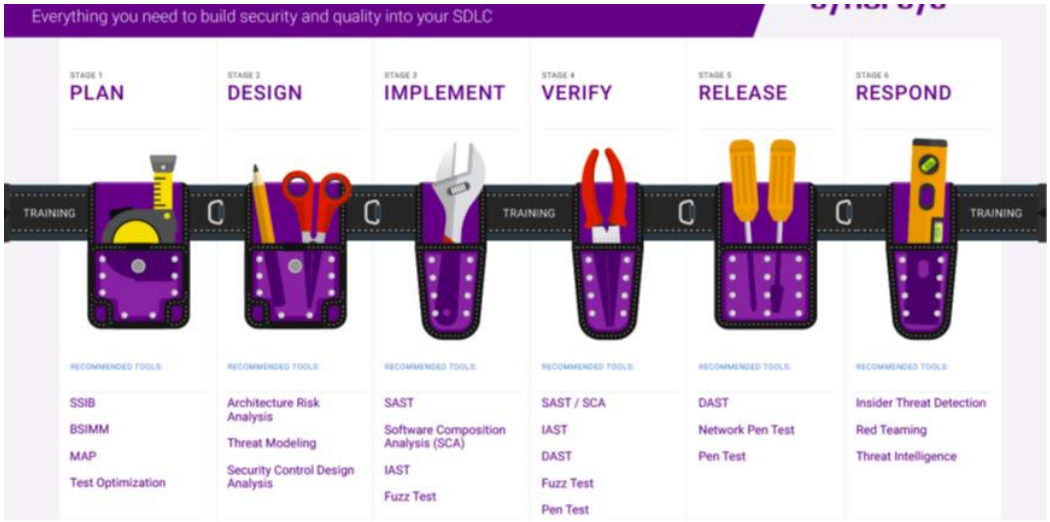


圖 2、Software Integrity Tool belt

資料來源：Synopsys

(二)當前最新研發之弱點檢測工具展示

在弱點檢測的領域，該產品使用一連串有系統的變異通訊信令或封包，輸入目標系統所提供的服務或程序，藉以觸發可能存在但尚未被發掘的弱點，該公司稱此方法為模糊測試，如下圖 3 所示。此種做法有益於早駭客一步發現弱點，且在駭客發動零日攻擊(Zero day attack)前發佈修補程式，讓使用單位有足夠的應變時間，以對存在弱點的系統進行修補，以便免進一步擴展成重大的資安事件。

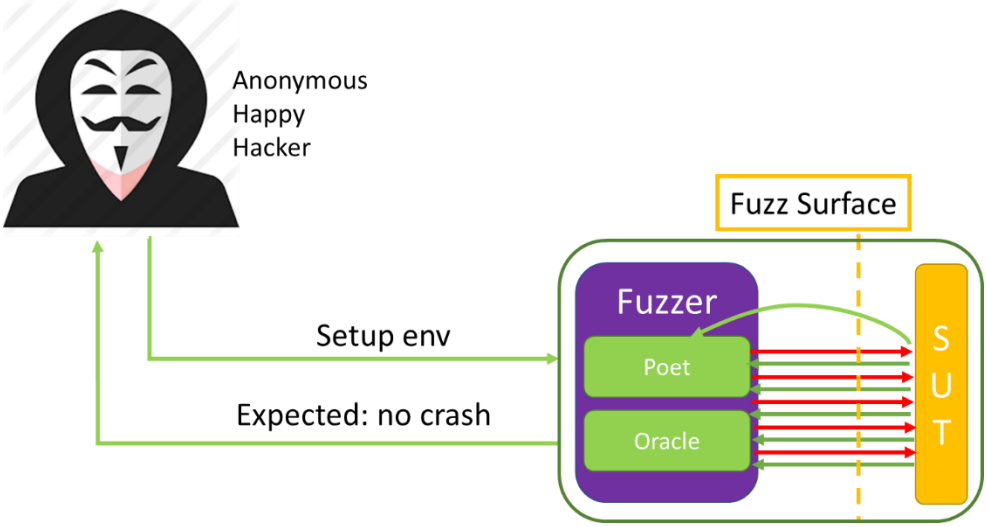


圖 3、模糊測試概念圖

資料來源：Synopsys

1. 麥金塔系統藍芽裝置弱點檢測展示(OSX Bluetooth testing demo)

此一檢測主要是針對麥金塔系統上的藍芽通訊裝置進行弱點檢測，該檢測工具所造成之檢測結果將造成系統失效。目前該公司對於 L2CAP 已提供 windows 系統藍芽裝置的檢測支援，本次展示是新開發針對麥金塔系統的檢測，如該弱點未修補，則將導致藍芽系統因緩衝區溢位(Buffer Overflow)而崩潰。多數弱點均已被 NIST-CVE 所公告，故本次展示主要用以檢測弱點是否存在而非發掘未知弱點。本次測試僅針對安裝 OS X 10.11 的麥金塔電腦。經查詢該公司網站，目前 L2CAP Test Suite[1]僅提供 windows platform，因此推測 OS X 是近期最有可能發佈的新功能更新版本。

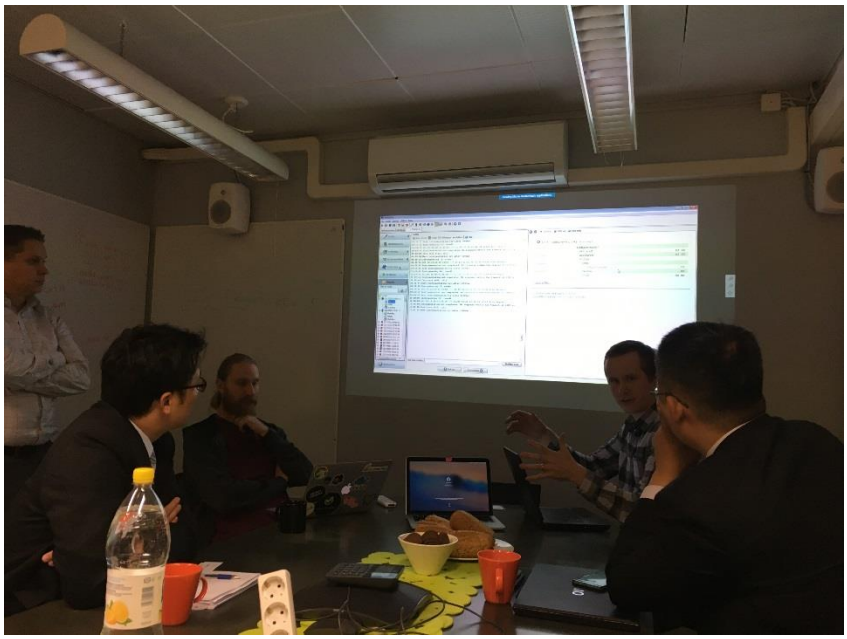


圖 4、Defensics 研發人員操作及說明 OSX Bluetooth testing

2. 網路檔案服務(NFS) 弱點檢測展示(NFS vulnerability presentation and demo)

網路檔案服務(NFS) 弱點檢測係針對系統上使用存在 2017 年 4 月 18 日 NIST[2]所公告的通訊協定弱點進行檢測，該弱點存在於使用網路檔案系統(Network File System，簡稱 NFS) v2 (RFC 1094, 1989.03)與 v3 (RFC 1813, 1995.06)版本協定的 Ubuntu Linux 核心版本為 4.11 或 4.12，若目標系統未有適當的修補，則可能造成 Ubuntu 4.12 Kernel

[1] Synopsys, L2CAP Test Suite Data Sheet.
[2] NIST, CVE-2017-7645.

panic 或 Ubuntu 4.11 NFS service crash。

推敲其造成的原因，為某些可能引發暴力攻擊的舊 C 語言程式碼被沿用，以及指標運算結果被儲存在未指定型態的整數變數，且呼叫時未經適當輸入驗證所造成。本次測試僅針對安裝 Ubuntu 系統的電腦。經查詢該公司網站，目前 NFS3 Server Test Suite[3]並未說明適用的作業系統版本。而在會議中的簡報也說明了，本次實作的弱點在 2000 年 12 月之後發佈的 NFSv4 (RFC 3130)的新版本中已被修正，但在許多真實案例中可以發現，許多資安事件的發生，大多是因為許多公司仍在使用舊有存在許多漏洞的系統所造成。

(三)新功能軟體開發套件簡介

因應檢測趨勢日益朝向客製化、自動化及平台整合前進，該研究團隊為滿足客戶的需求趨勢，提供客戶端自行開發檢測平台時可直接透過應用程式介面(Application Programming Interface，簡稱 API)呼叫此一檢測軟體之軟體開發套件(Software Development Kit，簡稱 SDK)功能，相關使用之概念描述如下圖 5 所示。

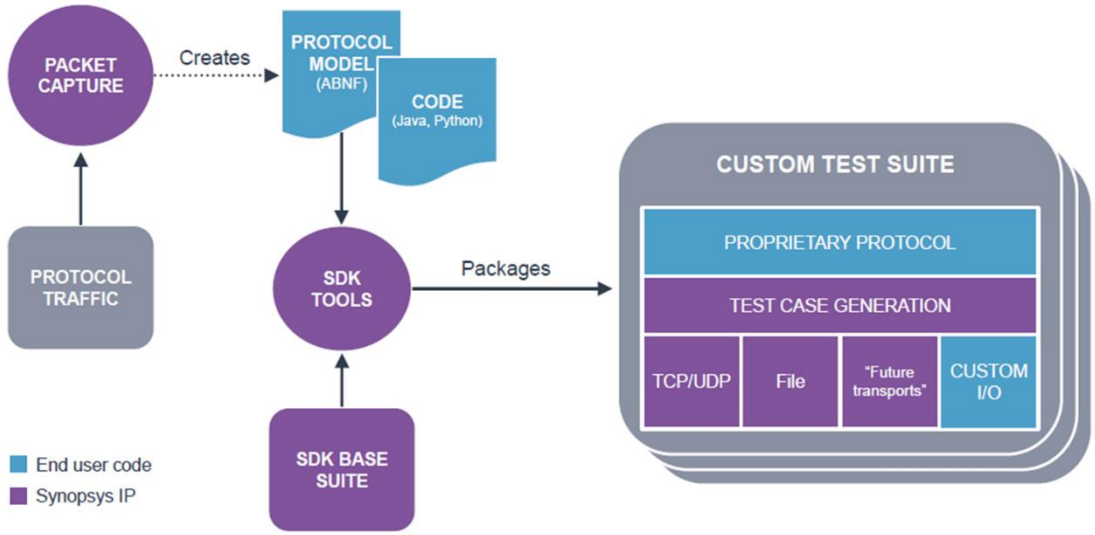


圖 5、軟體開發套件使用概述

資料來源：Synopsys

該套件目前僅支援透過 JAVA 與 python 程式語言呼叫，且需要另外購買授權才能使用，目前授權方式仍在研擬中。對於經費無虞及需要自行開發整合式使用者介面的檢測單位，此功能應有機會可簡化部分測試流程並提高自動化測試之品質。

[3] Synopsys, NFS3 Server Test Suite Data Sheet.

(四)新產品軟體組合分析工具(Protecode SC)簡介

許多軟/韌體公司，為了加速產品開發流程，因而使用 open source 與第三方提供的軟體模組，但這樣的使用可能造成資訊安全弱點以及誤用了有知識財產權的程式碼。基於這樣的出發點，該公司發展出此產品，該產品基於雲端系統，讓用戶端可以直接將欲分析的軟體上傳至此系統進行分析並取得報告，其中主要包含弱點評估、高度侵權回報、誤用影響及資訊洩漏等，相關流程如下圖 6 所示。

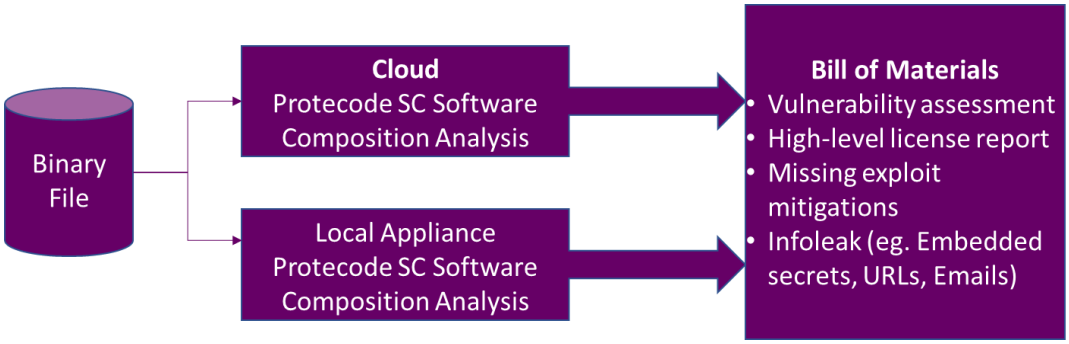


圖 6、Protecode SC 使用概述

資料來源：Synopsys

此工具被定位為一個全方位的管理解決方案，用以避免快速開發的過程中，導致複雜軟體供應鏈的風險，並協助進行持續風險改善。主要是藉由對編譯後的軟體二進制檔進行分析，並產生該軟體引用之 open source 與第三方軟體的評估列表。

由於技術細節事關商業機密，無法取得詳細說明。但從依據該公司研發人員的說明以及相關資料顯示，該軟體主要是透過二進制碼比對的方式尋找並對應相符的特徵以產生回報；與資訊工程的逆向工程對軟體進行反編譯及語法語意剖析方式不同，速度較快但精確度仍有待驗證。

(五)TTC feedback session

透過此次參訪，本中心工程師透過與 Defensics 研發人員的技術交流，詢問了許多有關資安檢測以及本計畫檢測所碰到的問題，相關提問摘要如下。

1. 開發團隊如何開發及驗證各種協定之未知漏洞模糊檢測工具？

於此次參訪過程中發現，該研發中心並不像一般想像之行動寬頻網路或資安網路實驗室一般，設置模擬網路環境，因此參訪人員特別詢問，該軟體研發人員是如何開發及驗證檢測軟體之可用性，尤其在行動寬頻網路相關的協定檢測上。該公司研發人

員表示，他們係利用公開模擬軟體，模擬各種場域測試之網路協定，來進行開發，另外他們的產品因為為許多設備製造商的研發部門所使用，所以研發人員也可以協助於其環境中進行相關軟體之驗證。

2.　如何驗證該弱點確實會造成資訊安全問題，或該弱點是可被利用的？

該研發技術人員表示，因駭客發現弱點，以及確認弱點可被利用，並進行系統是一連串的程序，而 Defensics 之檢測工具開發，係屬於第一階段之發現弱點，但並不會去印證此弱點是否可被利用。然而進一步對照實例展示過程以及先前之使用經驗，可以很明顯的發現該檢測軟體主要是在嘗試於透過各種可能位元組合，發掘出目標系統在開發過程中未被的發現問題。由此可見，若以白帽駭客的訓練過程加以驗證，該檢測軟體主要為找到攻擊切入點，僅為白帽駭客訓練過程的其中一項，後續仍需要藉由弱點利用與滲透測試等工具，進一步達成駭入目標系統奪取主控權以獲取所需資訊的週期循環。由此可再次印證，一個完整的攻擊流程，並非透過單一工具可輕易達成，這也是對方回應此問題的主要考量。

此外展示過程中，仍以驗證某系統所實作之通訊協定存在已公告之弱點為主，而非發現未知弱點，而證實方式則是以造成特定通訊協定服務崩潰為主，而非從中獲取機敏資訊並加以利用。以及經詢問，所有測試均有其預設(或假設)條件需要達成 (例如僅能作用在特定版本的硬體與系統上，假設該測試套件是被設計用於探測 Ubuntu Linux 4.11 與 4.12 系統上的通訊協定弱點，則相同的通訊協定於 BSD、UNIX、Windows、OS X…等系統上，或將系統安裝於虛擬環境，並不會被探測出弱點)，模糊測試才可能有預期的反應結果並非一體適用。基於此一現象，建議使用此工具進行弱點探測的人員進一步觀察，當對於該工具產生之結果有所懷疑時，應進一步交叉比對與驗證。

3.　是否可提供基站相關協定的測試流程供本中心檢測人員參考？

此次與該公司研發團隊的交流，本中心資安組工程師希望可得到研發人員操作的測試案例做為本計畫平臺使用，以節省本中心在檢測案例開發及除錯之時間，因本中心基站資安檢測屬較為特殊之案例，會議中，雙方也得到如何最快可得到芬蘭技術人員之支援方式，此行參訪在資安技術交流上頗有收穫。

二、　9/26-9/28 Nokia Security Center 參訪紀要

第 2 天到第 4 天共 3 天的時間，我們來到此行最主要的參訪單位-Nokia Security Center，交流最新行動寬頻資安威脅、資安技術、國際標準動態與相關解決方案。Nokia Security Center 與 Nokia 總部座落於芬蘭南部且毗鄰芬蘭首都赫爾辛基的城市埃斯波(Espoo)，為僅次於赫爾辛基的第二大城，芬蘭著名的阿爾托大學、VTT 及 Nokia 皆座落於此，許多芬蘭公司之總部亦設置於此。

Nokia 自 2013 年 9 月將手機相關業務出售給微軟(Microsoft)後，更專注於行動通訊網路(如核心網路與基站)相關領域的發展，尤其是在網路基礎建設部分。於 2015 年 4 月併購 Alcatel-Lucent 後，與瑞典 Ericsson、中國 Huawei 並列全球前三大電信業網通廠商，並藉此併購提升 Nokia 在路由器與光通訊平台的優異技術。以目前路由器市場來說，Alcatel-Lucent 是僅次於 Cisco 且領先 Juniper 的第二大供應商，主要動力來自邊緣路由器(Edge Router)的優異表現，及小型核心路由器(small core router)業務的快速成長。此外結合雙方的研發優勢，亦將使 Nokia 在未來技術研發領域佔據一席之地，這些領域包括：資通安全、5G、電信設備、軟體定義網絡、雲計算、大數據分析及物聯網等。而資通安全議題為近年來相當受到矚目的重點，因此 Nokia 期望透過所提出的一系列解決方案，來解決不斷變化的安全威脅。

在 3 天的參訪過程中，Nokia 專家除簡報說明外，以實際演示方式，與我們交流，而該團隊之專家，同時也是參與 3GPP SA3 Group 的討論成員，SA WG3 主要是負責系統的安全與隱私、確定安全架構及協定等，因此在國際標準行動寬頻網路安全標準制定的動態上也獲取許多新的資訊。

圖 7、TTC 參訪人員與 Nokia 安全專家合影

三天的交流議題包含了 Nokia 行動寬頻網路安全的解決方案、NFV 安全解決方案、核心網路安全、網路互連的安全(包含 SS7 漏洞安全、DDoS 攻擊演示等)、終端安全(包含 IoT)、公共安全等等，相關參訪紀要摘要如下。

■ **9/26 Nokia Security Center 參訪紀要**

(一) NetGuard Portfolio introduction

由於行動寬頻上網已為全球上網用戶的主流媒介，全球對行動寬頻網路安全也日益重視，因此 Nokia 在成立 Security Center 的研發團隊後，也希望從產品面提供電信業者 Nokia Security 資通安全的解決方案。其目標由近而遠分別是提供安全的產品、完整的安全產品線，最後建立全面的資通安全生態系統。為了能逐步實現此目標推出了 NetGuard Security 方案，該團隊基於未來 5G 及物聯網的應用可能直接或間接對整個行動通訊系統造成威脅，而更專注提供端點對端點的資通安全解決方案，該團隊深信唯有如此才能同時涵蓋網路連接、用戶資料傳輸及通訊設備，以提供最大程度的安全保證。

這個解決方案稱為 NetGuard Portfolio，其中"portfolio"原詞是指「檔案夾」、「文件」等等，但用在商業術語中則是指為了分散風險，將數個產品放在一個名目之下的總稱，

其主要基於下列常見議題作出因應，歸納如下：

1. 設備與使用者驗證，以確保他們以正確的身份進入系統，且不會影響網絡。
2. 透過存取控制(權限管理)來確保正確的用戶和正確的設備只執行應有的指令。
3. 確保來自設備的資訊在通過安全的通道傳輸，以避免在通過不安全的網路時被篡改。
4. 確保資訊的機密性，使得資料接收端是唯一可以讀取數據的。
5. 確保到此行動通訊網絡的所有設備的狀態和可用性。
6. 產生足夠安全的密碼，並在設備受到安全威脅時，允許鎖定或解除設備的運作。
7. 必須具備適當的遠端應用安全修復程序，以在檢測出弱點時排除安全威脅。

基於上述的內容，該團隊以 SOAR(Security Operations, Analytics and Response)平台技術將這些常見的議題分為三個主要類別，如圖 8 所示，並分別提出對應之方案。

圖 8、SOAR 概念圖

資料來源：Nokia

1. **維運上的安全(Security Operations)**

此部分屬維運上的安全系統，Nokia 藉由精心設計的監控程序，以機器學習的分析各式資訊，使得平台在遭遇威脅時能主動作出因應。在這個方面，主要透過三個部份來達成，首先是

❶安全管理中心(Security Management Center)：達成其概念如圖 9 所示。

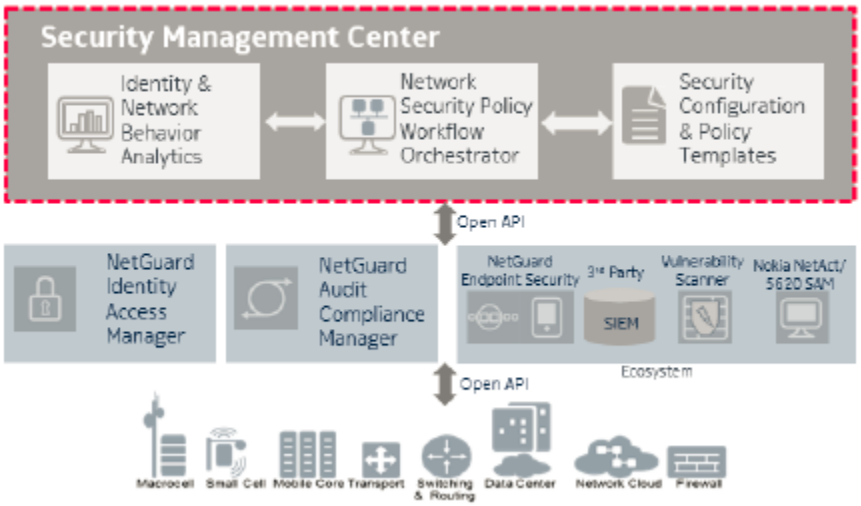


圖 9、Security Management Center 概念圖

資料來源：Nokia

整個安全管理中心架構是針對大型企業或電信業者因應來自各方的資訊安全挑戰而設計，其中透過 Open API 讓網路上的各式元件能接受來自平台的管理以及進行資訊交換(例如存取記錄、稽核紀錄、安全政策佈署與各式威脅感知事件等)，最後將所有資訊匯集於安全管理中心進行分析與安全政策一致性比對，分析結果如圖 10 所示，以藉由機器學習的過程，讓防禦機制自動化運作降低一線人力的需求，並提升防禦策略的準確度。如此可使的客戶端專注於自家的主要業務，即便在初期人員或技術不足的狀況下，也能因應多數新興的威脅。

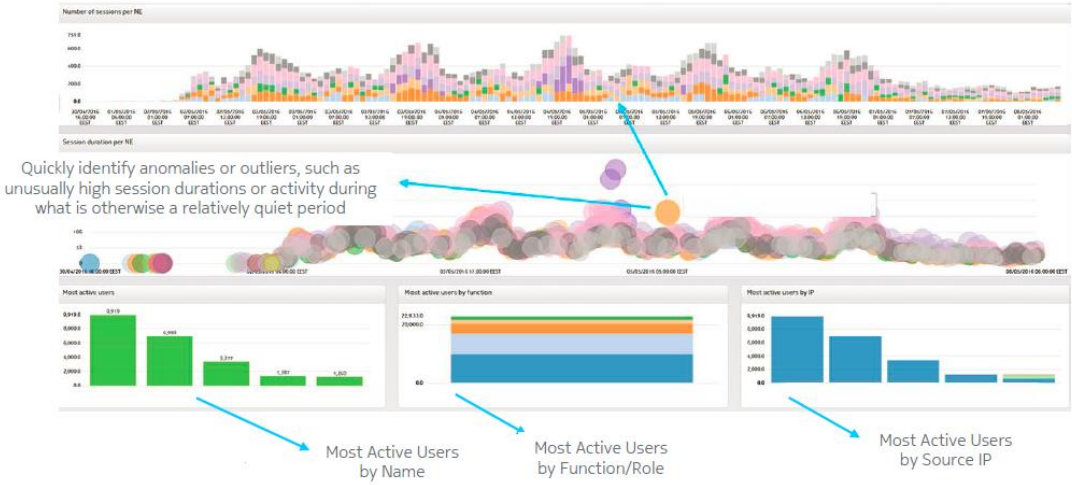


圖 10、Security Management Center 分析結果

資料來源：Nokia

❷識別與存取管理(Identity Access Manager)：

是整個管理中心重要的元件之一，主要由單一登入（Single Sign On，簡稱 SSO）的機制構築使用者在系統中的存取權限及安全管制，並且可進一步紀錄使用者於遠端登入設備時即時的操作過程，其概念如圖 11 所示。在實際展示過程中，此方法透過適當的壓縮與儲存可將錄製的畫面資訊儲存於系統中，作為後續稽核與異常事件佐證之用。此種方法與 Cisco 所發展的 TACACS+異曲同工，然基於命令字元儲存的 TACACS+儲存上更有效率，而 NetGuard 提出的方法則可以看到最多的操作細節，並且能安全的實作於虛擬化與雲端系統上。

整個系統的存取控制係採單一登入機制對所有使用者進行管理，使用此種機制的優點主要可簡化管理且避免使用者需要因應不同系統具備多組帳號密碼，但缺點是僅使用單因子驗證狀況下(如帳號/密碼管制)，容易因帳號密碼洩漏而遭駭客入侵。而主講者針對此一狀況，建議應導入多因子認證方式進行系統保護，同時 TTC 工程師也對其帳號資料庫所採取的保護措施與機制進一步詢問，希望能確認該團隊對於重要的帳號資料庫也建立適當的保護(包含所採用的通訊協定與機制)，但未得到相關說明。

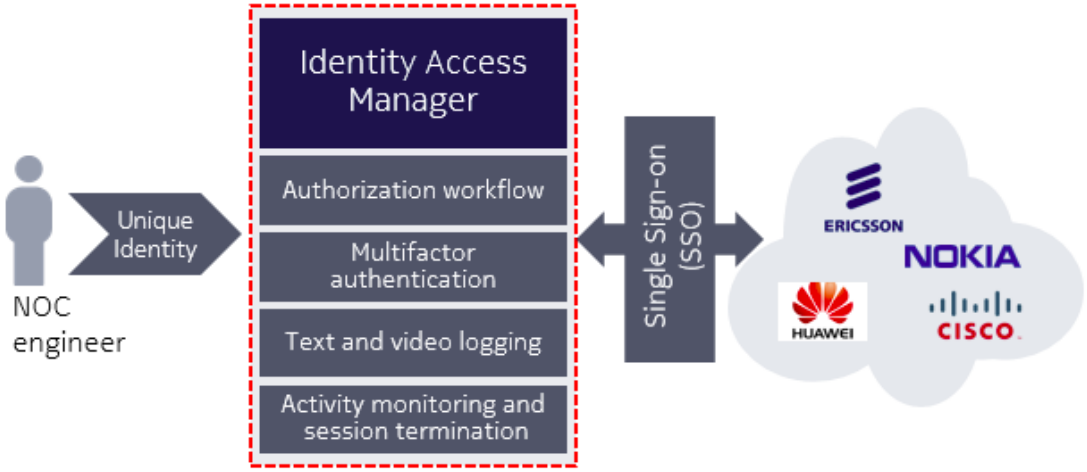


圖 11、識別與存取管理概念圖

資料來源：Nokia

❸一致性之稽核管理(Audit Compliance Manager)：

由於安全性設定疏失(Security Misconfiguration)為 OWASP Top 10 自 2010 年起，直到 2017 年公告的 RC1 版都還是常見十大弱點之一，有鑒於此，該團隊考量用戶端可能因為錯誤的配置而能讓駭客有可乘之機，因而為了安全管理中心額外開發一致性設定稽核管理元件，主要管理不同廠牌設備於網路上配置是否合規，其運作概念如圖 12 所示。

此功能係以自動化的機制比對設定檔，據主講者表示，只要該網路設備能透過相關的網路管理協定(例如 SNMP)對其進行管理，無論其設定之複雜度，皆可經由此元件以一致性的設定樣板對其進行設定檔管理，因此其號稱的 Agentless 技術，可跨實體、虛擬及軟體定義網路設備以達成所宣稱之功能。經查相關功能於資訊網路應用已行之有年，尤其是在 Unix 及 Unix like 相關系統，均有對應的自動化工具可以完成類似功能。

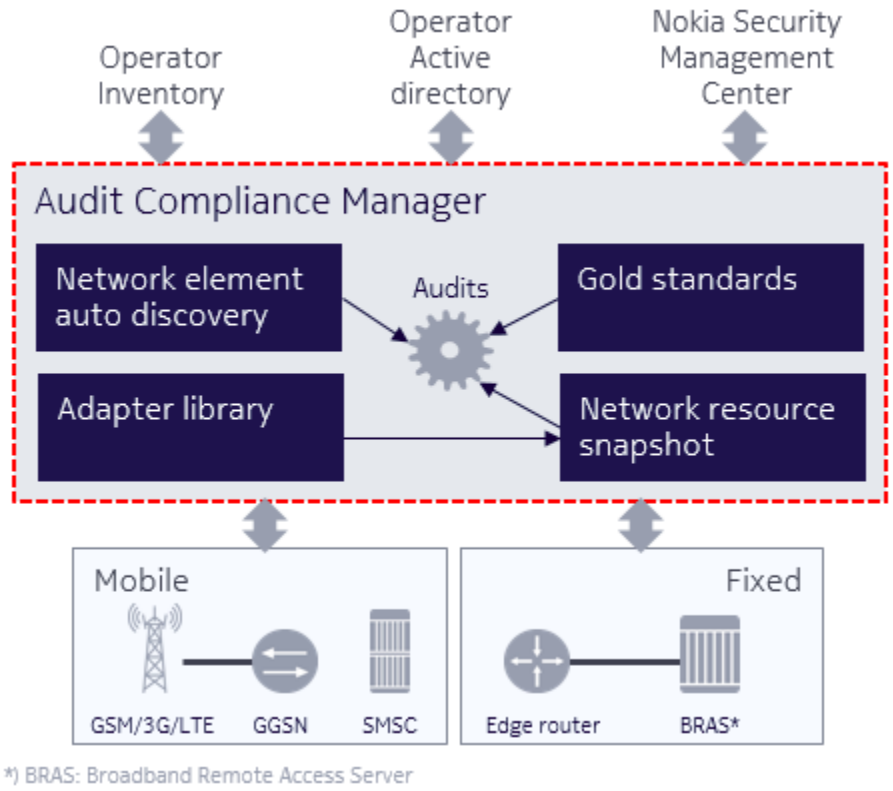


圖 12、一致性之稽核管理概念圖

資料來源：Nokia

2. 網路安全(Network Security)

Nokia 網路安全相關產品的設計，係從保護行動通訊與網路基礎設施著手，來防止來自企業外部的攻擊與惡意軟體的入侵，此次 Nokia 專家分享了以下三大類的解決方案，包含針對第七號信令系統(SS7)漏洞攻擊的防禦、核心網路的安全、SDN 的安全，皆為本計畫研究之重點。

(1) 信令安全

此部分主要討論廣泛被使用的第七號信令系統(Signaling System No. 7，簡稱 SS7)，這個超過 35 年的老舊封閉式通信網路系統，在此系統中應如何識別其安全問題並減輕這些問題所帶來的威脅。如下圖 13 所示，NetGuard 提出了 SS7 防火牆的概念，共可提供兩種配置模式分別為 Monitoring 及 Protect Mode。

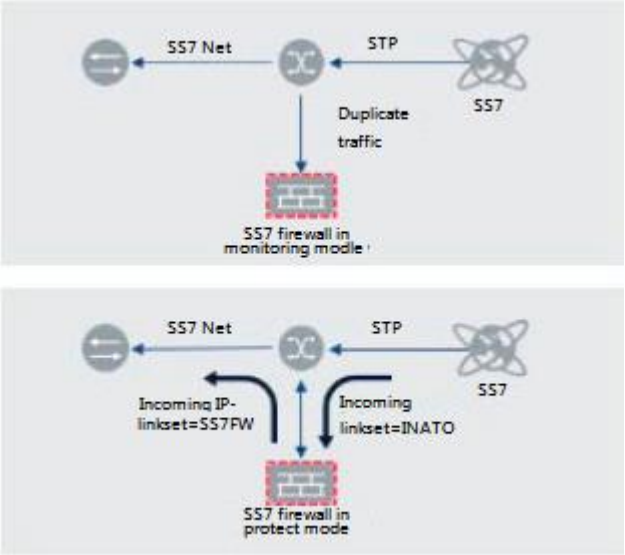


圖 13、SS7 防火牆的配置概念圖

資料來源：Nokia

主講者表示，該防火牆主要是透過識別並過濾發話來源端與收話目的端號碼做為控制基礎，一旦非允許的收發雙方與建立連線，則可能會發出警告或直接阻斷該訊務，其主要透過使用 Rapid deployment of the analysis solution，據稱是一種入侵檢測系統 (Intrusion-detection system，簡稱 IDS)，能夠分析來自 SS7 的主動式威脅。

經參訪成員之間討論，認為該防火牆概念與目前 IT 所使用的一致，但更為單純，如同第四層防火牆僅提供來源與目的之比對，而不具備 IDS 之類第七層的分析能力。而後續的實作展示，證實了參訪成員們的推測是合理的，此外我們也參考了 ITU 在 2016 年 6 月 29 於瑞士所舉辦的 Workshop on “SS7 Security"的簡報資訊[4、5]，其中 GSMA 於 IR.82 中所定義的五種類別的 operation codes 如下表。

[4] Minrui Shi, “Alternative Solutions for the improvement of SS7 security” , 2016/6/29.
[5] Pascal Dejardin, “Observations on SS7 Network Security”, 2016/6/29.

表 3、Operation Codes

Categories	Classification	Operation Codes	Filters
Cat.1	Home exclusive	SRI, Send IMSI, ATI, ATM, SP..	Block OpCodes
Cat.2	Roaming Home>Visited	PSI/L, PRN, CL, ISD, DSD	Check HLR
Cat.3	Roaming Visited>Home	UL, FwdSM, SAI, RegSS, PrUSS	Check Location
Cat.4	SMS interconnection	SRI4SM, MT-FwdSM	Home Routing
Cat.5	Call control >Home	CAMEL IDP	Check SCP

資料來源：ITU

下圖 14 所呈現的是所有展示案例使用的拓璞結構，其中除了分析元件本身外，防火牆還分為主要與邊界兩種，而主要防火牆的部分，推估應進一步主導了所有的防禦策略佈署與管制措施。

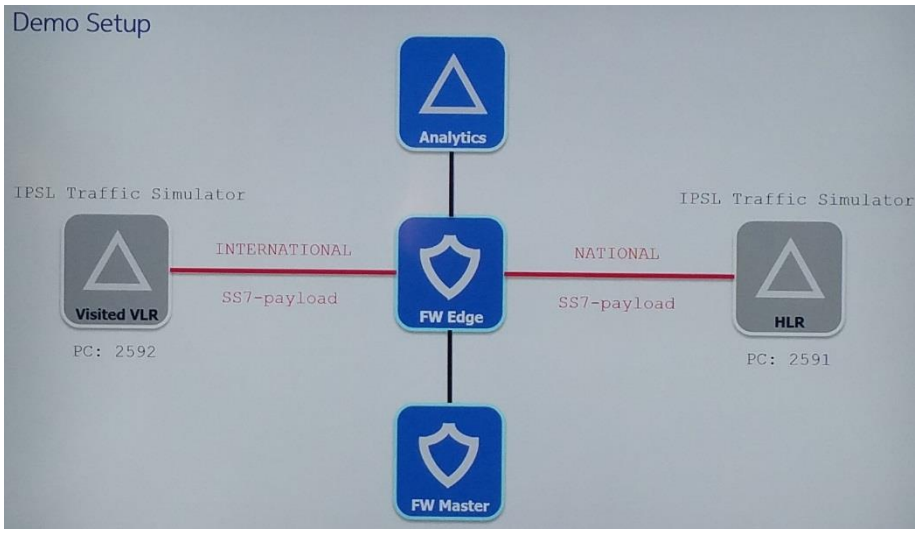


圖 14、展示案例拓璞結構

資料來源：Nokia

在介紹過程中，TTC 工程師也詢問主講者關於防火牆效能的疑惑，主講者提及此防火牆的檢查並不會對於實際上的信令傳遞造成影響，且防火牆本身所耗用

的效能極低。關於此點說明，則建議若有實際之佈署需求應做進一步的驗證，以確保與其聲明內容相符。

(2) 核心網路安全

由於核心網路的組成與維運相對複雜，因此威脅可能來自於外部或與其他業者的界接，因此在策略上，Nokia 所提的解決方案建議，係於各網域相互連接的重要交換節點上佈署防火牆措施，並提供可信賴的網域名稱解析系統（Domain Name System，簡稱 DNS)服務，如下圖淺藍色節點所示。

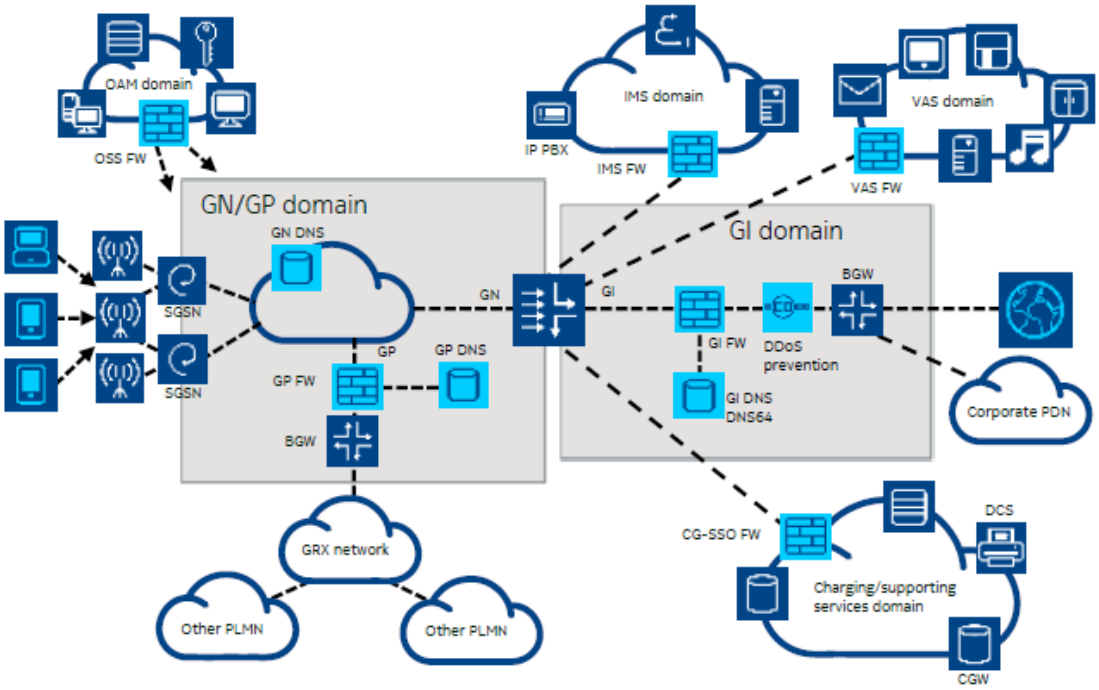


圖 15、核心網路安全配置結構

資料來源：Nokia

DNS 服務是一種無狀態的通訊協定，攻擊者除了可以輕鬆地掩飾其身份，由於 DNS 查詢是不對稱的，所以產生的回應數目可能是查詢數目的數倍之多，這表示 DNS 系統本身會使得攻擊被放大。攻擊者只需要傳送一個資料封包就可能讓 DNS 系統產生數倍之多的回應，導致業務停擺。

為此在核心網路的部分，基於分封交換核心網的安全考量，除了提供行動通訊系統主要服務的閘道器、數據/語音交換器以及行動通訊服務伺服器之外，提供行動裝置及各式加值服務使用安全的 DNS 也是防禦重點之一。會透過 DNS 攻擊來闡述核心網路的重要性，主要是 DNS 遭到分散式阻斷服務攻擊，除了可能被

癱瘓服務外，也可能造成骨幹網路的壅塞。因此在後續的展示中，主講者透過模擬的方式，展示該團隊所研發的散式阻斷服務攻擊防禦機制進行阻斷，並確保正常的流量仍可運作無虞，由於是模擬的攻擊行為，主講者表示，拿實際的流量測試在芬蘭是犯法的，因此無法從其他方面來評估所採取的演算法確實能有效的抵禦攻擊，但透過主講者實際展示的過程中，TTC 工程師認為其效果對比現有多數流量清洗服務(如 Arbor 或 Radware)，未來發展仍相當可期，展示內容如圖 16 所示。

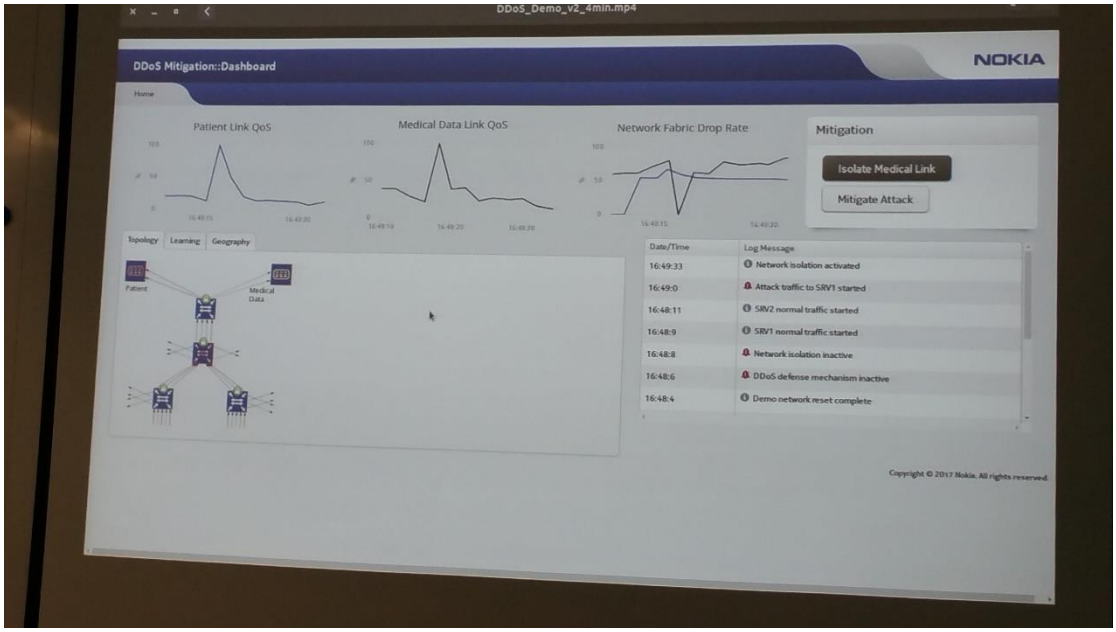


圖 16、阻斷服務攻擊防禦機制效果展示

資料來源：Nokia

(3) 軟體定義網路架構

由於軟體定義網路(Software Defined Networking，簡稱 SDN)和網路功能虛擬化(Network Function Virtualization，簡稱 NFV)使得資料中心與行動通訊服務有更高的佈建彈性，因此對電信業者或企業的資料中心網路服務來說，可以藉此獲得自動處理與動態因應變化的好處，如此除可節省支出之外，網路佈署能支援隨成長規模而調整，同時也可減少日常維運的開銷，讓網路可透過程式演算法的方式來進行控制，進而藉由搭配一些可程式化的網路設備元件，能讓網路的設計、部署、管理、規模延展更為容易。簡而言之，這項機制能讓網路做到服務自動提供與彼此協作，降低平時管理網路環境所需的時間，並減少人為出錯的機會，改善服務可用性與可靠度。

然而 Nokia 考量到這樣的環境可能在 NFV 服務元件遭受攻擊時，相當不容易找出受攻擊的元件並加以排除，這是所有建構雲系統服務的企業都將面臨的考驗。因此該團隊設計將 NetGuard 防火牆置於虛擬網路功能(虛擬機)與硬體的虛擬層(Hypervisor)之間，如下圖 17 所示，以維護各個虛擬功能模組的安全。

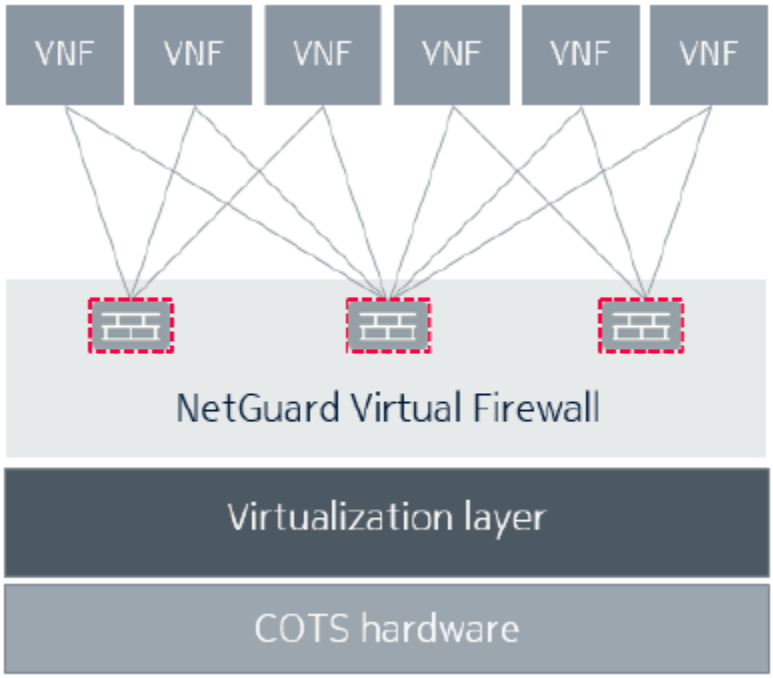


圖 17、虛擬防火牆配置概念圖

資料來源：Nokia

3. 終端安全(Endpoint Security)

在終端安全(Endpoint Security)的構面上，則是透過終端裝置(如 IoT 裝置、手機)驗證、簽章與加密，及以網路為中心的惡意軟體、殭屍網路與威脅偵測機制共同形成防禦體系。Nokia 安全專家在終端安全上特別提出以下兩種解決方案建議。

(1) 電信業者提供終端安全服務

此解決方案係以網路為中心的防禦機制，使用者向電信業者申請安全的加值服務，電信業者在前端就能以使用者為導向，佈署相關的資訊安全服務，以保護終端使用者的資訊安全，如下圖 18 所示。此種作法的另一個好處是電信業者可以擁有大量的資料分析提升機器學習的準確度，並且與大量爆發的狀況下，發出簡訊提供使用者告警，而使用者無需犧牲原本運算能力，可就有限的終端裝置進行攻擊與惡意行為的防堵。此方式可能適用於企業內部，但用於電信業者的一般

用戶效果應相當有限，尤其是額外訂閱資訊安全服務將增加用戶額外的費用，且效果可能不明顯的狀況下，容易削弱用戶的使用意願，從技術觀點而言此方案相當值得參考，但實務面則仍有待市場考驗。

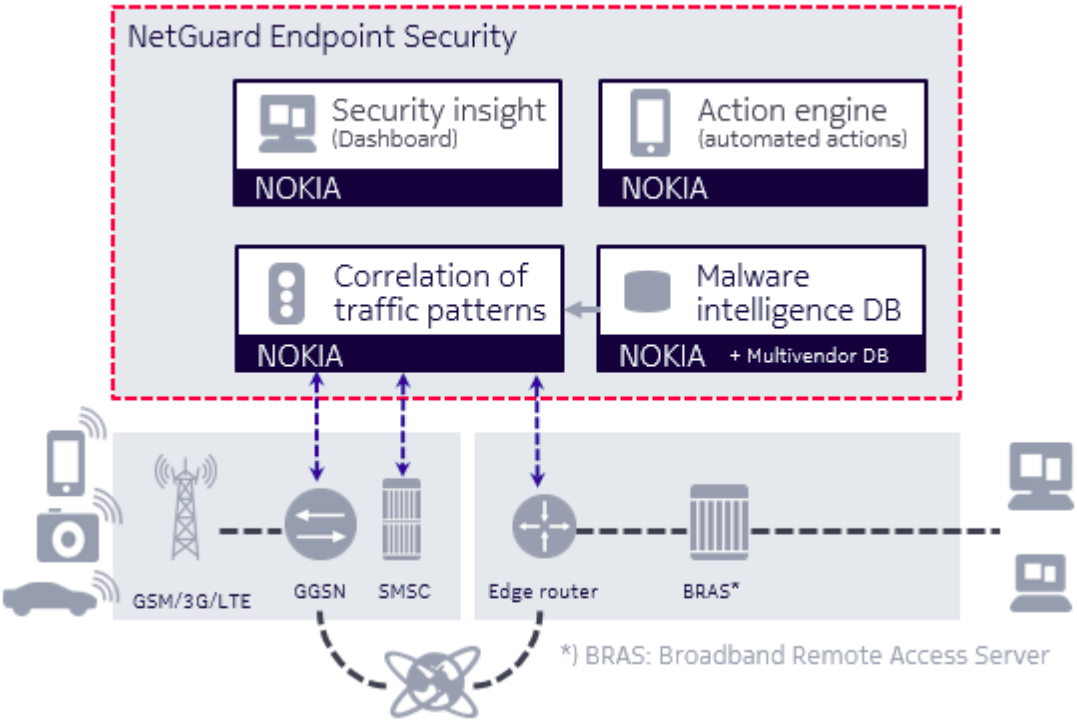


圖 18、電信業者提供終端安全服務概念圖

資料來源：Nokia

(2) IoT 之安全保障-數位憑證結合 IPSec

此外另一個主張的重點就是適當的利用公開金鑰基礎建設(Public Key Infrastructure，簡稱 PKI)作為設備與移動裝置的身份識別，並結合 IPSec 協定以保護端點之間的通訊安全，其概念如圖 19 所示，所有設備欲連線至核心網路，都需持有由數位憑證認證機構(certification authority，簡稱 CA)發行合法 X.509 憑證，並使用此憑證與安全閘道器(Security Gateway)建立連線，以與核心網路內的各種服務伺服器進行連結，以提供裝置連線行動網路相關服務。

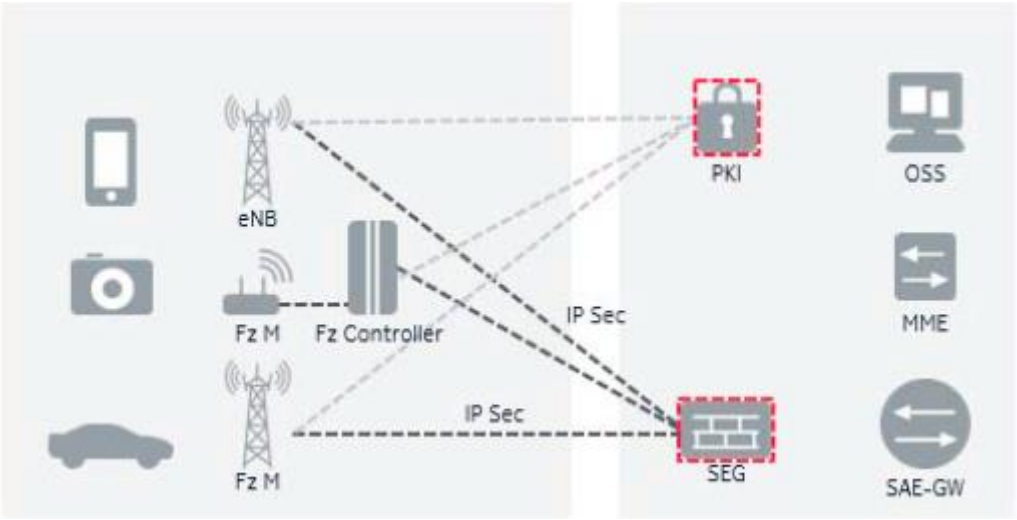


圖 19、端點通訊安全架構圖

資料來源：Nokia

由於該團隊宣稱該公司出產的基站均完整的整合 IPSec 協定，加解密對於通訊性能影響甚微，且可完整相容於 3GPP 規範，因此營運商使用相關設備時可確保具備足夠的安全性並擁有效能保障，且該公司提出的管理架構目前全球已有 30 多個營運商正在使用中。此外對於 IoT 的保護也可進一步透過相同的方式達成，如圖 20 所示。

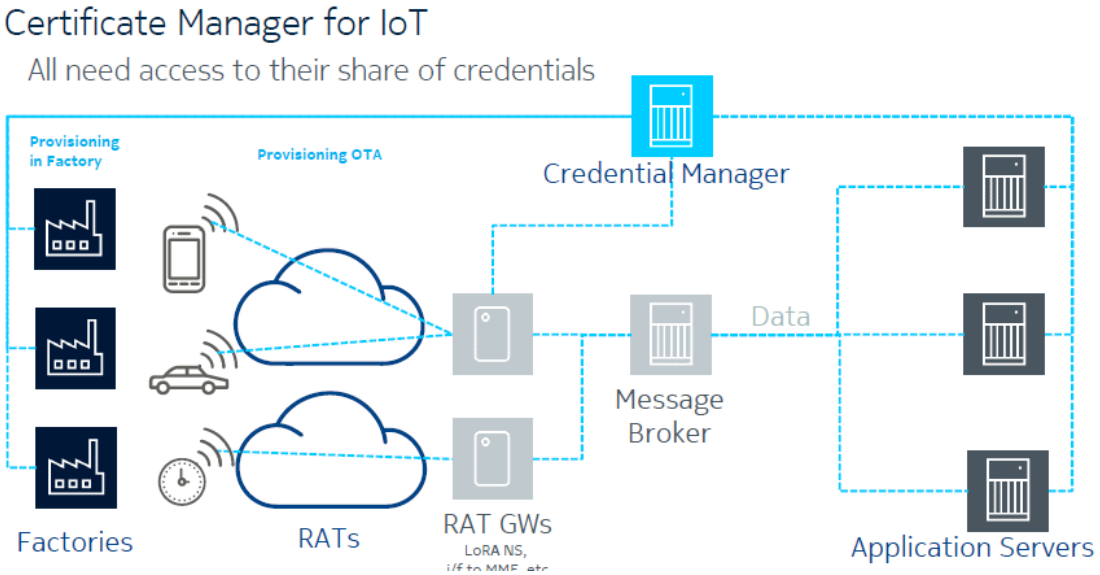


圖 20、端點通訊安全應用於 IoT 概念圖

資料來源：Nokia

總結前述與 NetGuard 平台相關之各部分元件，透過圖 21 的說明加以整合，使參訪人員對於 Nokia 所提出的安全架構與做法有更為完整與全面的概念。該平台係以網

路攻擊的流程開發資安防禦技術並規劃全方位之解決方案(如圖 22)，此邏輯，非常值得本計畫於規劃檢測流程及檢測規範時之參考。

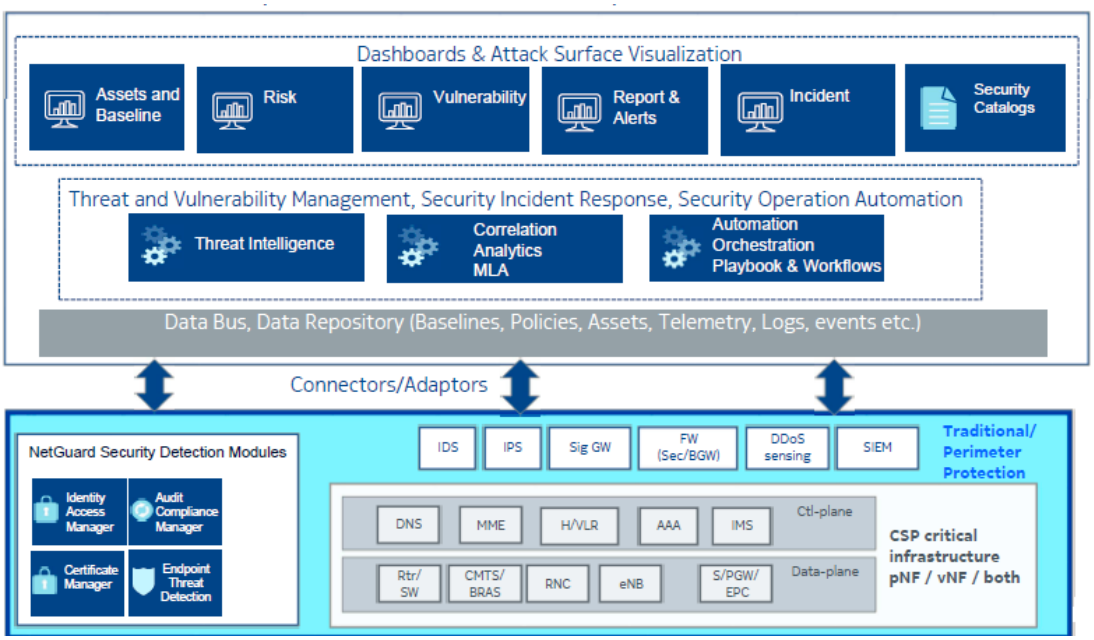


圖 21、行動通訊安全整合與分析架構圖

資料來源：Nokia

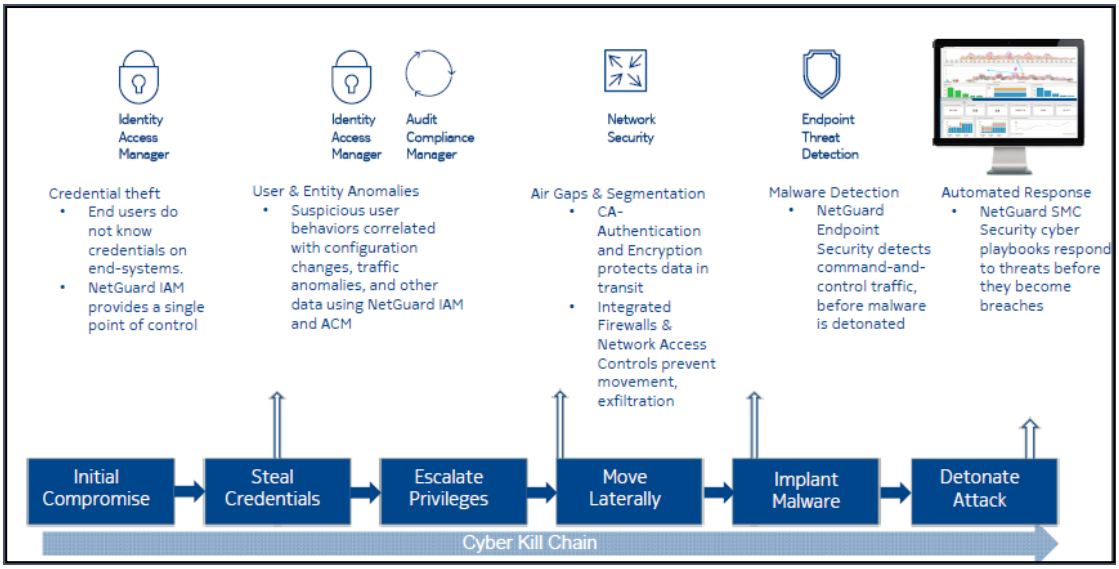


圖 22、NetGuard 平台之資安防禦技術

資料來源：Nokia

(二) 安全中心實際案例與平台展示

Nokia 安全專家於詳細的簡報介紹後，帶我們到 Nokia Security Center 進行實際攻

擊案例及該公司平台的展示，展示內容摘要如下。

1. NetGuard Security Management Center 展示

Nokia 安全專家首先與我們介紹 NetGuard Security Management Center 平台，展示透過統一單一認證方式，控制系統管理接口，進行細部的控制與訪問。

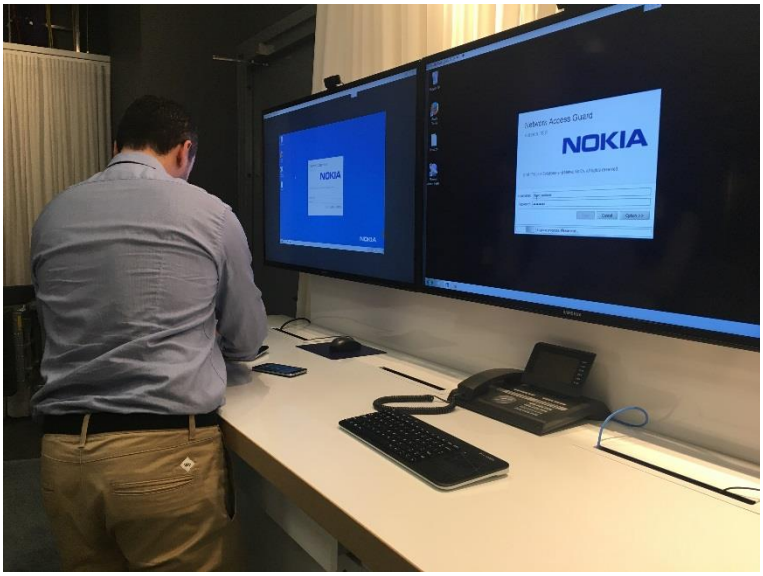


圖 23、Nokia 安全專家操作 NetGuard 平台單一認證功能

2. Endpoint Security 展示

(1) 實際演示攻擊者如何劫持 CCTV 攝像機的視頻傳送

在演示過程中，Nokia 安全專家請資安組蔡主任手持手機進行影像對話。於過程中即遭駭客進行影像視頻的劫持。

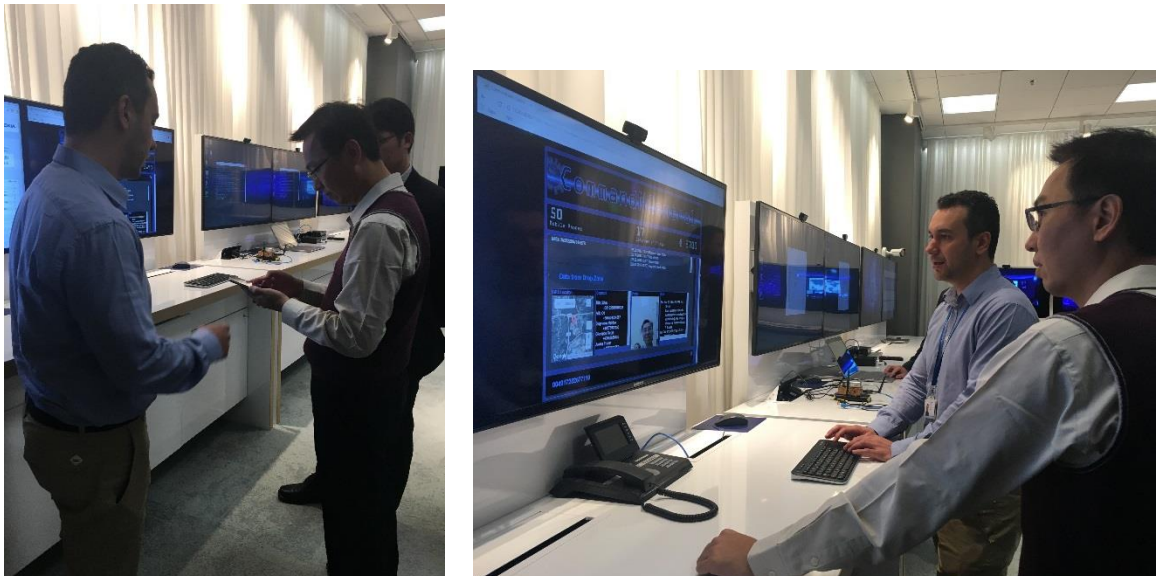


圖 24、Nokia 安全專家展示 CCTV 影像攻擊

(2) 終端安全攻擊監視與分析系統展示

Nokia 專家隨後展示，該公司於終端安全攻擊監視與分析的警示系統，包含相關數據，以及受影響的用戶，與對電信業者的影響。

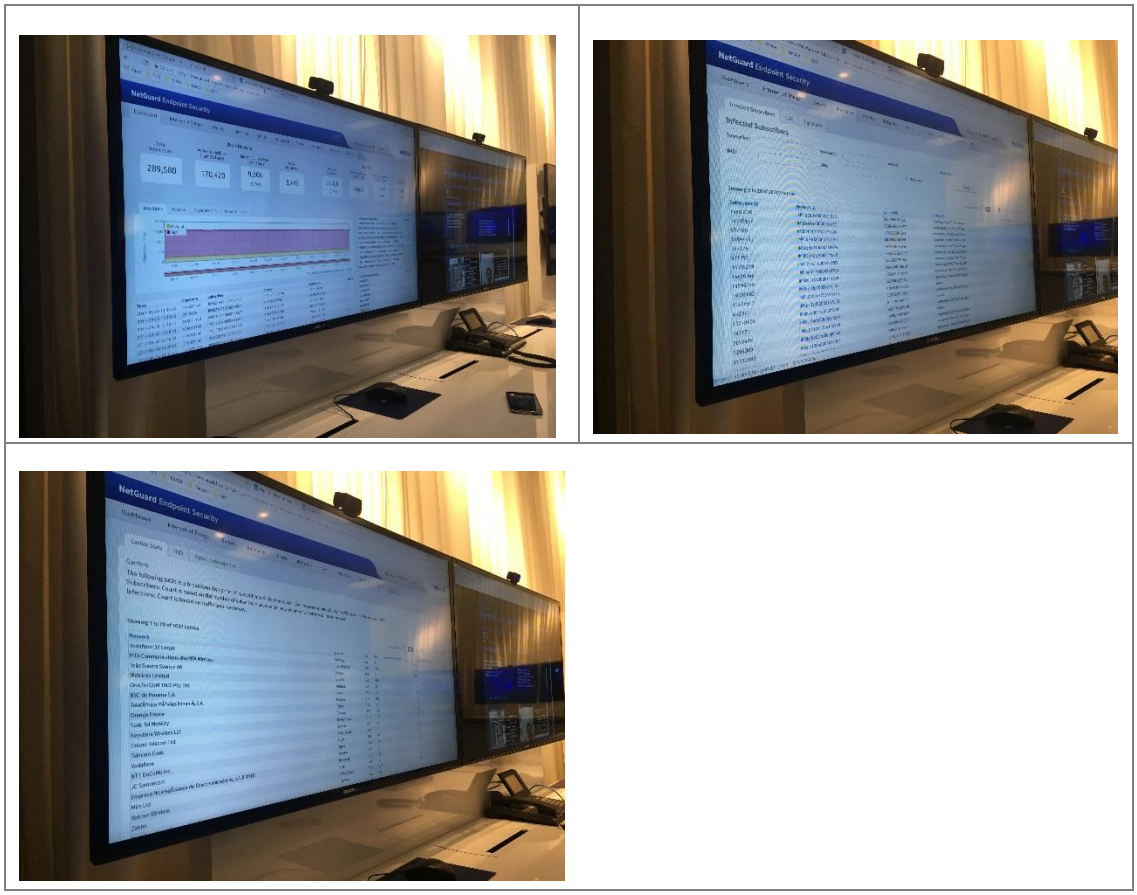


圖 25、終端安全攻擊監視與分析

Nokia 專家同時展示該平台所連結的資料庫，呈現全球各國惡意軟體感染的地圖。

圖 26、Malware Infection Map

(3) 未加密通訊的威脅展示-竊取 VoIP 語音通訊內容

Nokia 安全專家實際演示在 LTE 網路中竊聽 VoIP 的攻擊，其假設情境是駭客透過自製裝置 (Banana Pi 簡易型單板電腦 + USB 網路卡 + 行動電源)，如圖 27 所示，透過非法進入基站機房中串接該裝置，讓駭客可竊取所有流經該裝置的網路流量，且在當前 LTE 為全 IP 化的環境下，語音通訊的內容也都能被還原，是相當值得參考的案例，TTC 資安組工程師也希望藉由此案例於 TTC 資安實驗室中建置演示。

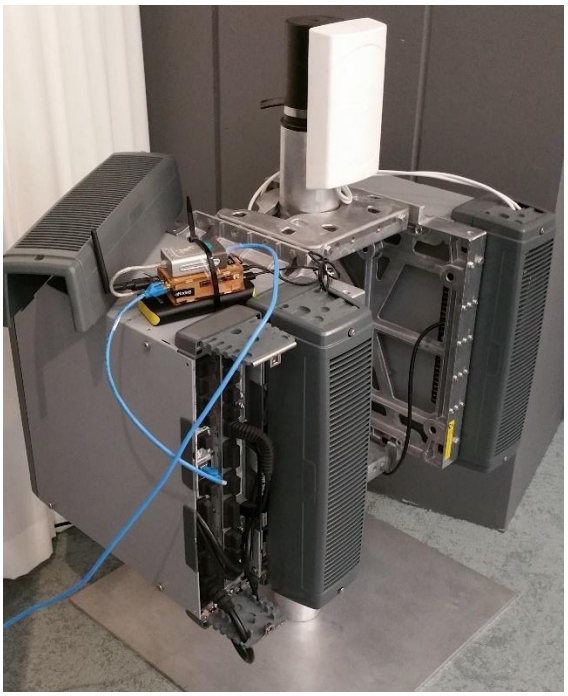


圖 27、資料竊取裝置及其串接基站展示

■ **9/27 Nokia Security Center 參訪紀要**

(一) DDoS 的檢測與解決方案

Nokia 安全專家與我們分享，以 SDN 與 NFV 架構下的攻擊案例，Nokia 透過 DDoS 的分析工具(如圖 28)，將攻擊流量進行分流，來緩解 DDoS 對網路所造成的影響，相關分析的資料庫，Nokia 專家也提到可從加拿大的大學所公開的 DDoS 資料庫取得，該解決方案，透過事先分析，讓對流量影響小且影響時間短的封包通過，影響較大的流量則進行分流的控管。

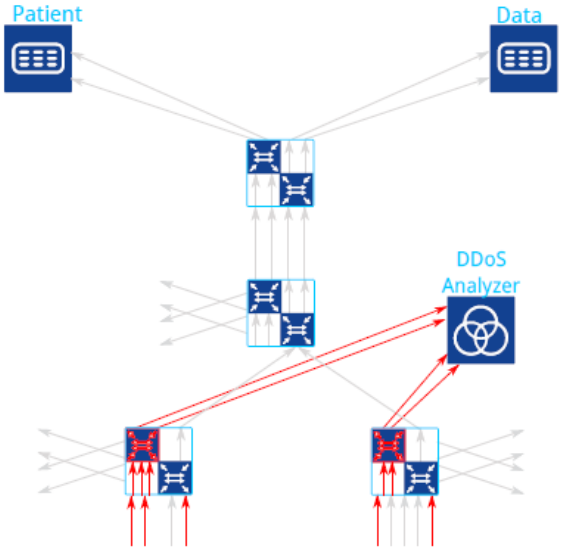


圖 28、DDoS Analyzer

資料來源：Nokia

(二) SS7 與 Diameter 安全問題探討

近年國際上已發生多起駭客利用電信業者廣泛使用於國際漫遊網路中的第七號信令系統(Signaling System 7，簡稱 SS7)協定漏洞，使駭客可繞過特定身份驗證過程，獲得更多權限進行惡意攻擊，甚至破解雙因素認證，取得用戶銀行帳戶密碼，並竊取手機用戶的銀行帳戶金額。此議題 2016 年起已受到各國政府及國際標準組織的重視。此行拜訪 Nokia Security Center，SS7 協定漏洞的解決方案也是國內主管機關希望本中心蒐集國際解決方案的重點之一。

Nokia 專家 Dr. Silke，與我們分享，SS7 所建構的通信漫遊網路，早被廣泛運用在 2G、3G 網路漫遊通訊中，但多數使用 SS7 均未考量各局端相互之間的認證、傳輸過程加密與資訊完整性檢測，在沒有任何防禦機制的保護下，SS7 協定漏洞所造成的威脅，包含有竊聽、位置追蹤、詐騙、服務阻斷、信譽損失、資料通訊劫持、網路帳號/密碼竊取(部分網路服務是透過簡訊傳遞驗證訊息，如網路銀行轉帳交易、線上刷卡)等，同時也分享了許多近年 SS7 漏洞引起的真實案例。

SS7 是一種局間信令系統。和其他局間信令系統一樣，SS7 一般不負責用戶終端和局端之間用戶線上面信令的傳輸和處理，只負責局交換機之間、局交換機和其他電信設備之間的信令傳輸和處理。需要注意的是，和其他信令系統一樣，SS7 不負責進行具體語音訊號的傳輸，但是它負責協調各種電信設備，使各種電信設備能夠準確地

建立語音鏈路，為用戶提供服務。和同樣屬於共通頻道信號的六號信令系統比較，第七號發信系統採用多功能模組化設計，如圖 29 所示，是一種更適用於數位通訊網路的信令系統。

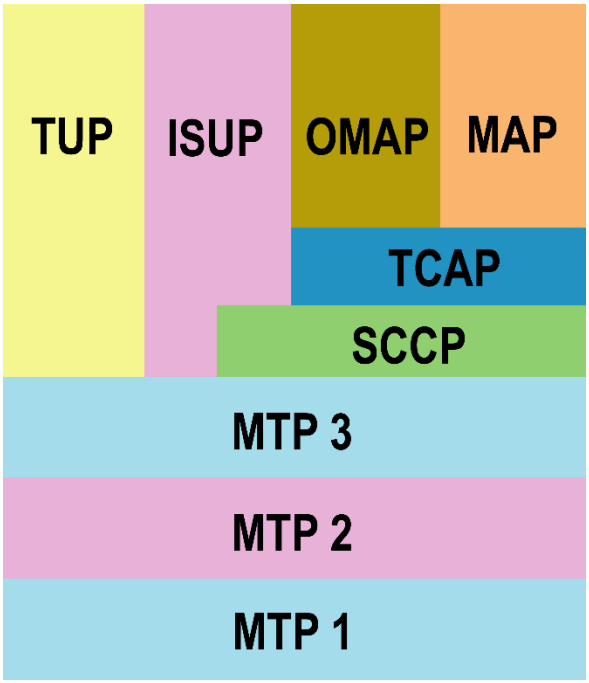


圖 29、SS7 多功能模組架構圖

關於此議題，主講者也曾發表於其所撰寫的論文[6]中。關於 SS7 所建構的通信漫遊網路，雖然與網際網路無關，但在人的溝通上扮演一樣重要的角色，尤其是在網際網路尚未發達的期間。但這古老且迄今仍廣泛被使用的通信系統，也將面臨遭受各式攻擊的挑戰[7、8、9]，在沒有任何防禦機制的保護下，可遭到的攻擊有竊聽、位置追蹤、詐騙、服務阻斷、信譽損失、資料通訊劫持、網路帳號/密碼竊取(部分網路服務是透過簡訊傳遞驗證訊息，如:高鐵購票刷卡驗證碼)等。

在多數使用 SS7 均未考量各局端相互之間的認證、傳輸過程加密與資訊完整性檢測的狀況下，可能導致的資訊安全威脅均已被 GSMA 於 IR.82 中所定義，因此在實機展示的過程中，展示了 6 個 test case 及 Nokia 防火牆的過濾與阻擋功能

[6] Silke Holtmanns, Interconnection Security Standards–We Are All Connected, Journal of ICT, Vol.4_1, p.p. 1-18, 2016.
[7] The Register, “Someone checked and, yup, you can still hijack Gmail, Bitcoin wallets etc via dirty SS7 tricks”, 2017/9.
[8] SECURITYWEEK, “Hackers Exploit SS7 Flaws to Loot Bank Accounts”, 2017/5.
[9] Forbes, “Hackers Can Steal Your Facebook Account With Just A Phone Number”, 2016/6.

其次是關於 Diameter 協定相關的資訊安全議題討論，由於 SS7 本身容易受到攻擊，連帶也使得負責 LTE 網路漫遊傳輸的協定-Diameter 安全受到關注，尤其是這個服務掌管了 AAA 機制，攻擊者可能藉此得到更多用戶資料。對電信業者而言，用戶身份識別是至關重要的，只有確認了用戶的身份，才能知道所提供的服務應該向誰收費，同時也能防止非法用戶對網路進行破壞。而在確認用戶身份後，將可依據用戶所申請的服務類別、等級與內容，由系統授予相應的使用權。在用戶使用系統資源時，也需要有相應的系統來統計用戶所對資源的佔用情況，據此向客戶收取相應的費用，因此行動網路中各類資源的使用，都需要有認證、授權和計費進行管理。

談到 AAA (Authentication, Authorization, and Accounting，簡稱 AAA or Triple A) 協定所提供的服務，RADIUS 是常用的協定之一，相對簡單、易於管理且擁有良好的擴展性，因此在 IT 領域廣泛被應用。但基於協議本身的缺陷，例如基於 UDP 的傳輸、過於簡單的機制、沒有重傳機制和集中式計費服務等，使得這個協議僅適用於行動通訊網路內 GGSN 或 P-GW 與外部網路建立會話時的認證請求。隨著新的技術的發展與導入(如無線、數位用戶線路、行動 IP 和乙太網路)和網路的快速擴充，日益複雜的路由器和接入伺服器大量投入使用，對 AAA 協定衍伸了更進一步的需求，這使得傳統的 RADIUS 難以勝任。

在 4G 的網路中行動 IP 將被廣泛使用，而當這些行動 IP 用戶端要接取網路，並使用營運商提供的各項業務時，就需要嚴格的 AAA 過程。AAA 伺服器要對這些行動終端進行認證，授權允許用戶使用的業務，並收集用戶使用資源的情況，以產生計費信息。這就需要採用新一代的 AAA 協議 Diameter。在 IETF 的 AAA 工作組同意將 Diameter（為直徑，意味著 Diameter 協議是 RADIUS 協議的升級版本）協議作為下一代的 AAA 協議標準。Diameter 協定的實作方式與 RADIUS 類似，也是採用 AVP，屬性值對（採用 Attribute-Length-Value 三元組形式）來實現，但是其中詳細規範了錯誤處理, 故障換手機制, 採用 TCP 協定，支持分散式計費等。

此外延續先前討論有關核心網路及防火牆機制的安全議題，考量 SS7 用於行動網路的界接模式，如圖 30 所示，由於 SS7 本身容易受到攻擊，連帶也使得 Diameter 服

務成為攻擊者覬覦的目標[10、11]，尤其是這個服務掌管了 AAA 機制，攻擊者可能藉此得到更多用戶資料。主講者在會議中主要透過 Send Routing Info for SM Request、Denial of Service using Cancel Location Request、DoS using Insert Data Request 及 One Time password Interception using SMS 四個案例說明 Diameter 相關的攻擊手法分析。

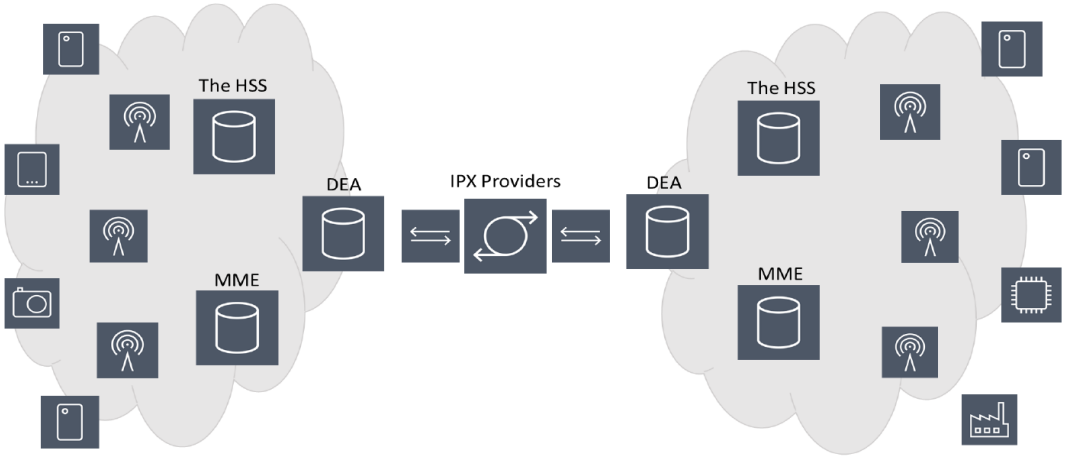


圖 30、SS7 用於行動網路的界接模式

資料來源：Nokia

總結先前提出關於攻擊與威脅的手段，主講者提出 IPSec 是一個好的方法，但不能完全相容於既有的應用，例如某些 SS7 系統或老舊的電信網路、營運商之間相互接界的考量以及部份老舊節點不易升級等，因此提供了一些對策讓企業與營運商參考，包含了從資料流的監管與偵測、善用防火牆與路由機制減輕遭受攻擊時的損害，以及密切注意相關組織(如 GSMA)發佈的官方資訊或參與相關會議。

(三) 國際標準與各國安全指引參考

Nokia 安全專家 Dr. Silke 也是參與 3GPP SA3 Group 的討論成員，SA WG3 主要是負責系統的安全與隱私、確定安全架構及協定等，在行動寬頻安全防護的建議中，她認為，時時關注國際標準組織及各國安全指引的脈動，加入國際標準組織安全標準的討論或加入會員取得資安攻擊國際最新資訊，其實是資安防護中非常重要的一環，因次她在會議中，也分享了目前國際標準與各國在行動寬頻網路安全標準之防護建議上的最新的資訊(如圖 31)。

[10] Silke Holtmanns, Yoan Miche and Ian Oliver, “Subscriber Profile Extraction and Modification via Diameter Interconnection, International Conference on Network and System Security”, 2017/7/26.
[11] Kotte, B., Holtmanns, S., Rao, S., “Detach me not - DoS attacks against 4G cellular users worldwide from your desk”, Blackhat Europe, 2016.

透過此難得之機會，因本計畫研究團隊的研究中已知道 3GPP 在完成 MME 安全 TS 33.117 檢測標準的制定後，正著手討論 eNodeB 的檢測標準，會議中我們也與 Dr. Silke 詢問了是否得知目前最新進度，但因 Dr. Silke 表示她並無參與這個標準的討論團隊，但可幫忙詢問另有參與的同事，協助了解最新進度。

GSMA

- Input to FS.11, FS.07, IR.88
- Rapporteur of FS.19
- Proactive vulnerability result sharing in GSMA

3GPP

- NDS/IP rapporteurship
- Thousands of security contributions e.g. Network security Rel-14

Regulator discussions

- USA FCC Q1/2017 (CSRIC V WG10)
- Nordic regulators (ongoing for diameter)
- potentially ENISA (Europe) (Q4/2017)

Communities

- Long standing cooperations between Nokia Bell Labs and reserach organizations (universities, labs etc)
- Active participation in conferences

圖 31、最新資安相關之國際標準資訊分享

資料來源：Nokia

(四) SS7 攻擊與防護之實際演示

Nokia 安全專家同時並實際演示 GSMA IR.82 Ca1~Cat3 中 6 種 test case，及運用該公司防火牆解決方案可產生之防禦效果。經參訪成員與 Nokia 專家間的討論，認為該防火牆概念與目前 IT 所使用的一致，但更為單純，如同第四層防火牆僅提供來源與目的之比對，而不具備 IDS 之類第七層的分析能力。本團隊在研析 SS7 漏洞相關解決方案的同時，發現防火牆之解決方案，也是 GSMA IR.82 所提的建議之一。

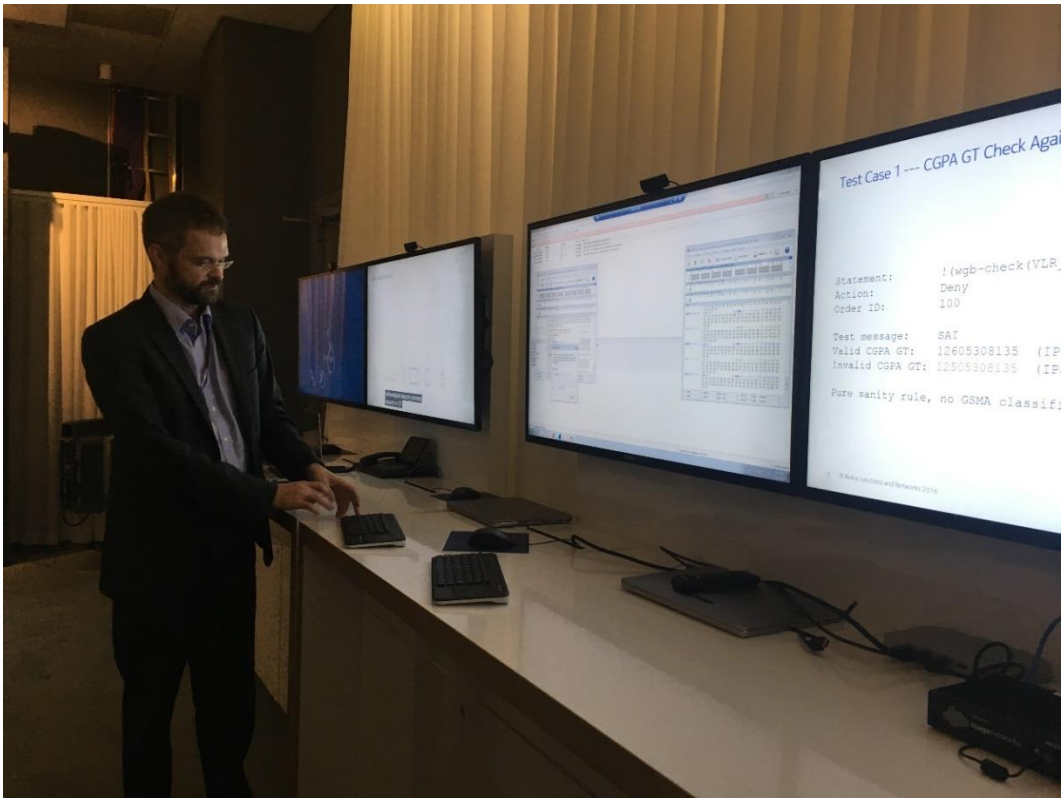


圖 32、Nokia 安全專家演示 SS7 6 種 test case

■ **9/28 Nokia Security Center 參訪紀要**

(一) Nokia LTE Public Safety

1. Spectrum & Standardization

每個國家都會保留特定的頻譜作為公共安全使用(如圖 33)，TTC 林副執行長也特別與主講者交流，目前台灣在公共安全分配的頻段與以色列相同使用 Band27 (851-869MHz)，但碰到並沒有設備可支援的問題，主講者也提出這的確是一大挑戰。在與主講者的互動討論中，也提到若未來政府採用 RAN Sharing 的模式也許也是一種解決方案。

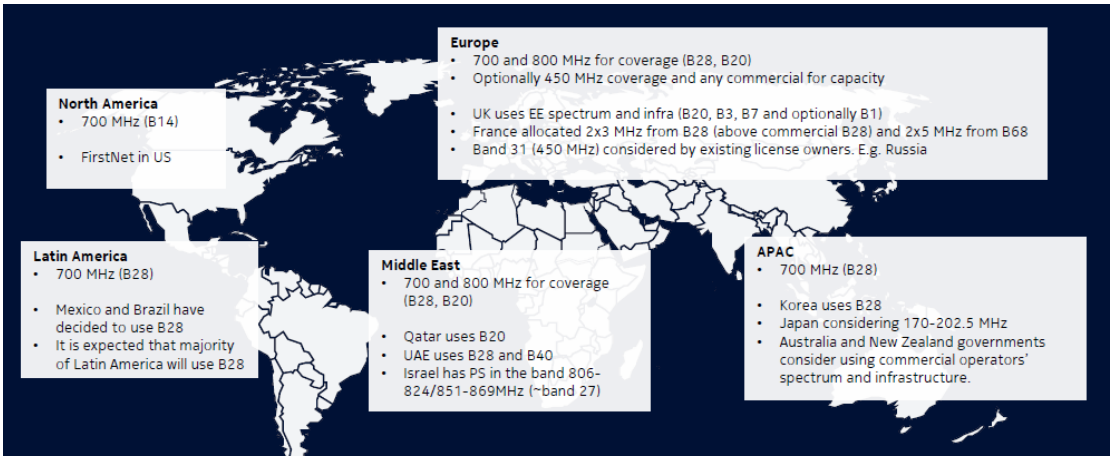


圖 33、各國公共安全之頻段規劃

資料來源：Nokia

2. Nokia Public Safety E2E Ecosystem

在 3GPP 每一次釋出的標準中也都對於公共安全也都有相應的內容，主要是提供重大災難發生時，第一線救難人員彼此或與救災中心之間能夠建立通訊與資訊分享，並確保救難人員的安全，為此 Nokia 提出了一個完整的緊急通訊方案，主要架構如下圖 34 所示。

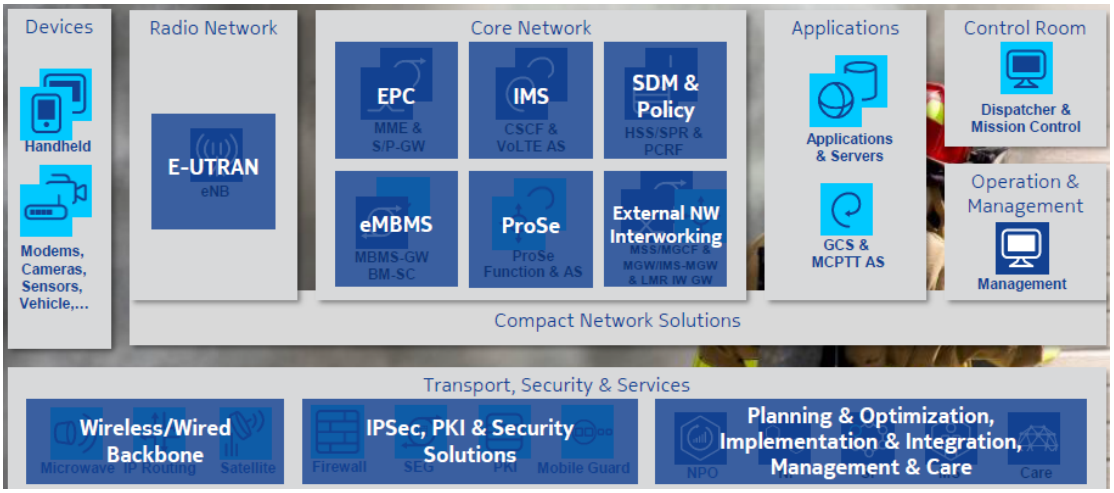


圖 34、緊急通訊方案與架構

資料來源：Nokia

基於要國家政府佈署完整的緊急通訊網路基礎架構，Nokia 認為混合式的架構更能夠在災害發生的時候發揮作用，主要是由於佈建專屬緊急通訊網路成本過高且平常時用不到；而混合式架構則可以透過商用系統設置緊急通訊頻段，且由各國政府於緊

急時刻徵用，一方面節省維護成本，另一方面可以涵蓋更多的救災範圍，其佈署模式如圖 35 所示。為此也實際展示了相對應的方案，包含可透過群組設定讓公共安全行動裝置持有者間相互分享資訊的方案，以及整合式 LTE 行動套件(將核心網路與無線基地台整合在一起，有人力背負及車載系統兩種形式)，希望藉由各種型態的相互整合，使救災行動能更深入各災區且團隊反應速度更快，相當值得政府單位參考。

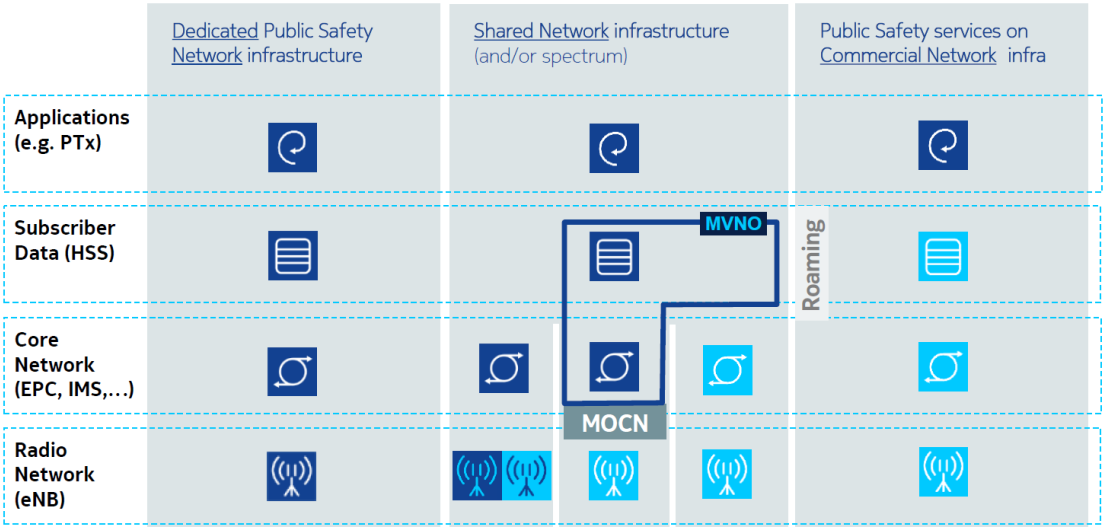


圖 35、緊急通訊網路佈署模式

資料來源：Nokia

對於生理狀態監測的 IoT 支援也被考量在內，如圖 36 所示，穿戴式裝置所發出的各種生理資訊，結合行動裝置所提供的地理位置訊息，以即時監測受災者生理狀態(知道位置在哪裡，哪個人應該要先救)。

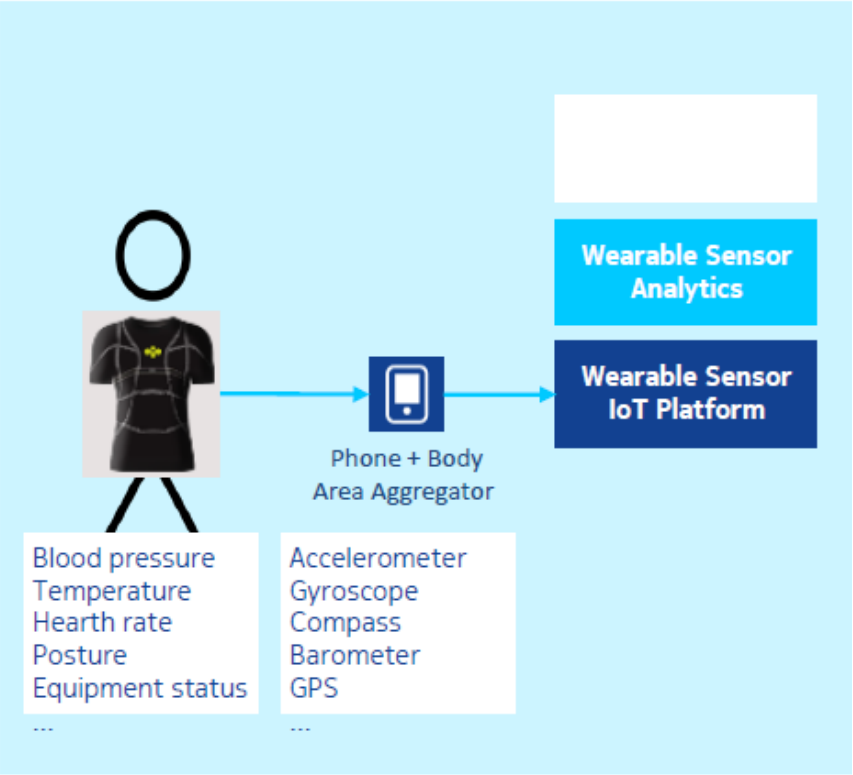


圖 36、公共安全結合 IoT 應用範例

資料來源：Nokia

3. Nokia Executive Experience Center 參觀及展示

Nokia Executive Experience Center (簡稱 EEC)為 Nokia 總公司展示最重要及最新研發的展示中心，因此在參訪最後一天，Nokia 台灣業務也特別安排芬蘭總公司人員帶領 TTC 參訪人員參觀 EEC，進行 Nokia 最新研發項目如 VR、手機以及公共安全的實際體驗等，Nokia 人員也非常用心的於 EEC 參訪入口特別製作本中心 Logo 表示對我們的歡迎。在公共安全議題上則是透過一系列的實機展示以及影片做總結，希望透過這樣的方式帶領參訪者能更實際感受到 Nokia 對於未來願景的擘畫，以及所投注的資源與努力。

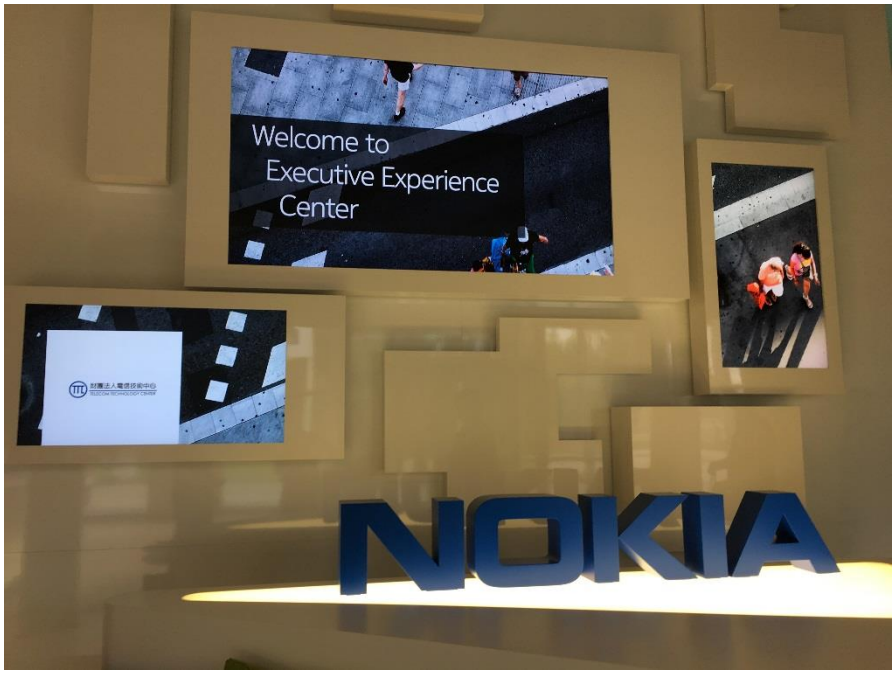
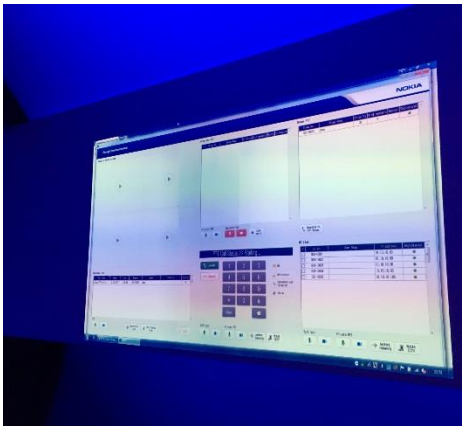


圖 37、EEC 入口及本中心 Logo

圖 38、VR 產品體驗



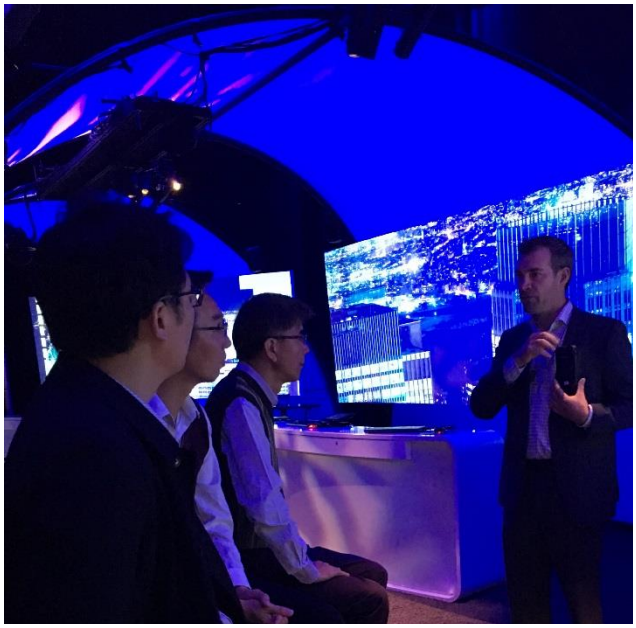


圖 39、展示公共安全裝置的控制與通訊

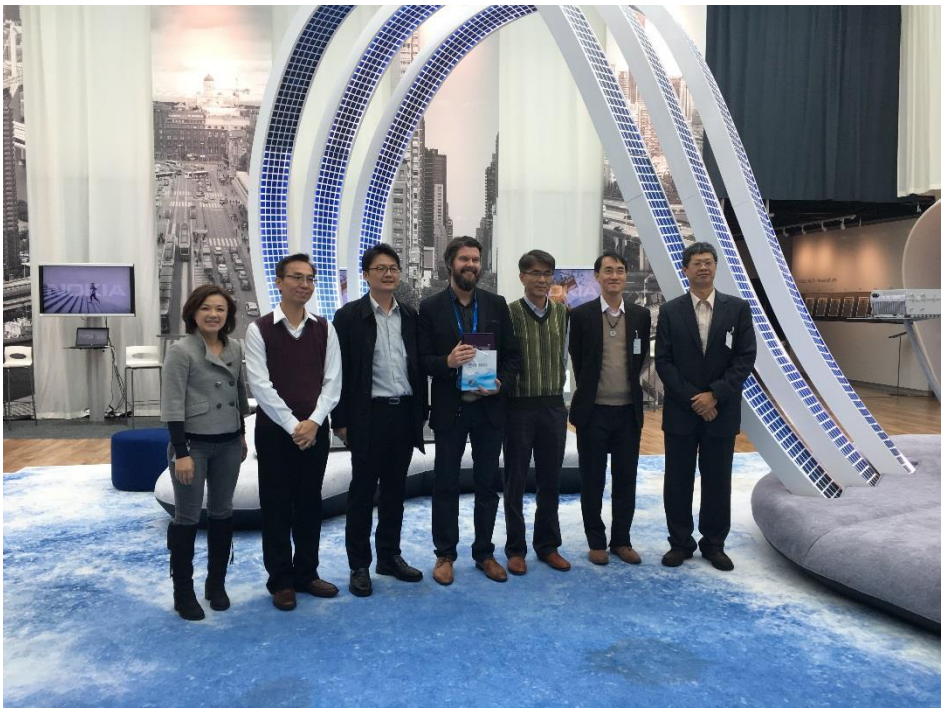


圖 40、與 Nokia 參訪安排窗口於 EEC 合影

三、　9/29 VTT Technical Research Centre 參訪紀要

第五天參訪行程特別約訪到芬蘭國家技術研究中心(VTT)，該中心之角色如我國之工研院，VTT 為北歐最大應用研究組織，研究範圍涵蓋電子學、資訊技術、工業系統、生物工程及建築運輸等學科領域。VTT 是芬蘭國家創新體系的重要組成部分，其

於行動通訊網路(2G, 3G, 4G and 5G)之發展及網路安全領域皆有提供相關技術研發與服務，對北歐行動寬頻技術之發展具有重大之貢獻。

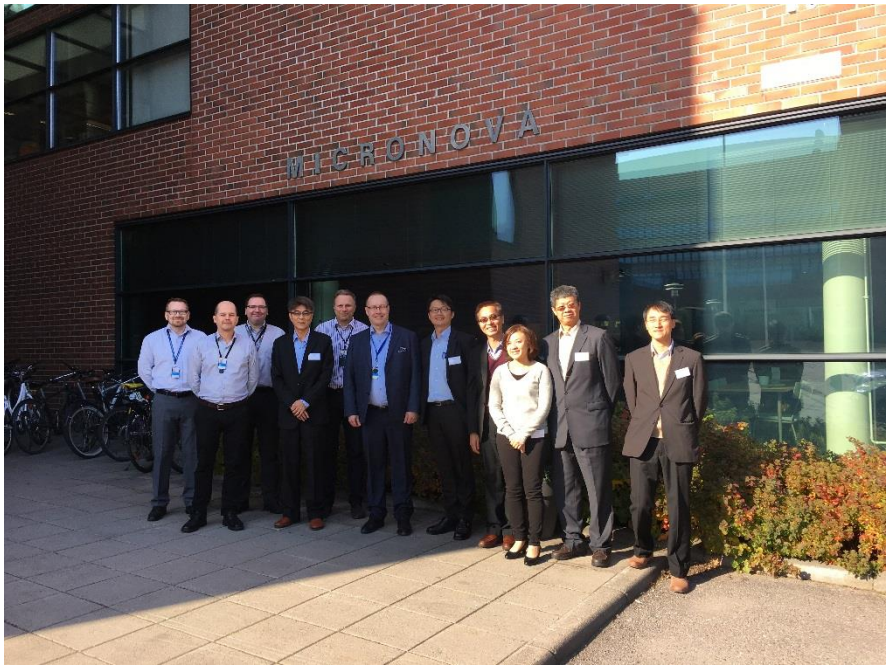


圖 41、與 VTT 與會專家合影

此次安排行程中，由於參訪單位時間之安排，與本參訪團隊時程之限制，無法參觀到該單位於 OULU 的 Network Security Center 及 5G 實驗室，聯絡窗口也特別從 OULU 分公司，到 Espoo 總部，並邀集相關專家與我們交流 5G、IoT 及 SDN Security 之最新技術發展，在與 VTT 的交流中發現，芬蘭政府對於 5G、IoT(尤其是智慧電網)的發展非常的重視。交流重點摘要如下：

(一) 建置 5G 實驗網路(5GTF)，進行技術面、政策面與產業面之研究

從交流過程中發現，芬蘭政府已積極與國際接軌並佈建 5G/IoT 的實驗網路- 5G Test Network Finland (簡稱 5GTNF)，5GTNF 整合了四個國家的實驗網路，從 2015 年起芬蘭政府每年投入約 2,500 萬歐元於 5GTNF，此實驗網路涵蓋了所有相關的 5G 研究領域(如圖 42 所示)，包含：

1. 技術面-從可程式化核心網路基礎設施（包括利用軟體定義網路 SDN 和網路功能虛擬化 VNF 概念）到密集和異質接取網路配置（例如包括小型基站和物聯網）。

2. 政策面-與 FICORA 芬蘭通信監管機關合作，進行頻譜規劃，期能以有效與智能的方式使用可用頻譜，包括不同的頻譜共享技術和行動通信中超高頻頻段的使用。

3. 產業面-目標則是確保芬蘭 5G 測試網路環境能符合 5G PPP、3GPP、ETSI 及 ITU 的規範，成為所有 5G 測試平臺，進一步促成芬蘭成為 5G 技術和服務測試的國際合作對象。

為了落實這些目標，VTT 成立了不同專案，包含 FUHF (Future of Ultra High Frequencies)、CORE++ (Cognitive Radio Trial Environment++)、5GTN (5G Test Network) 及 TAKE-5 (5th Evolution Take of Wireless Communication Networks)，其中 5GTN 專案，是由奧盧大學及 20 多個不同產業和 VTT 合作，該平臺也預計於今年底前完成支援 3GPP R13 的 NB-IoT 與 LTE-M 技術布建，連結在不同城市地點(埃斯波、奧盧、圖爾庫及上維耶斯卡)的通訊網路，以垂直式發展滿足運動到照護需求等服務，並結合可擴展的環境(穿戴式裝置、物聯網及醫療通訊)，提供測試和開發關鍵的 5G 技術組件和相關支持功能(如圖 43 所示)。

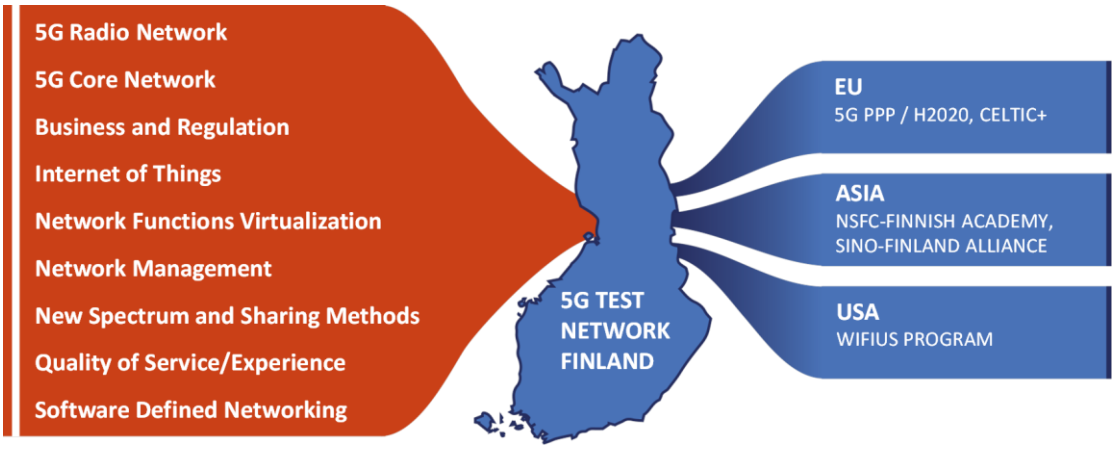


圖 42、5GTF Scope

資料來源：VTT

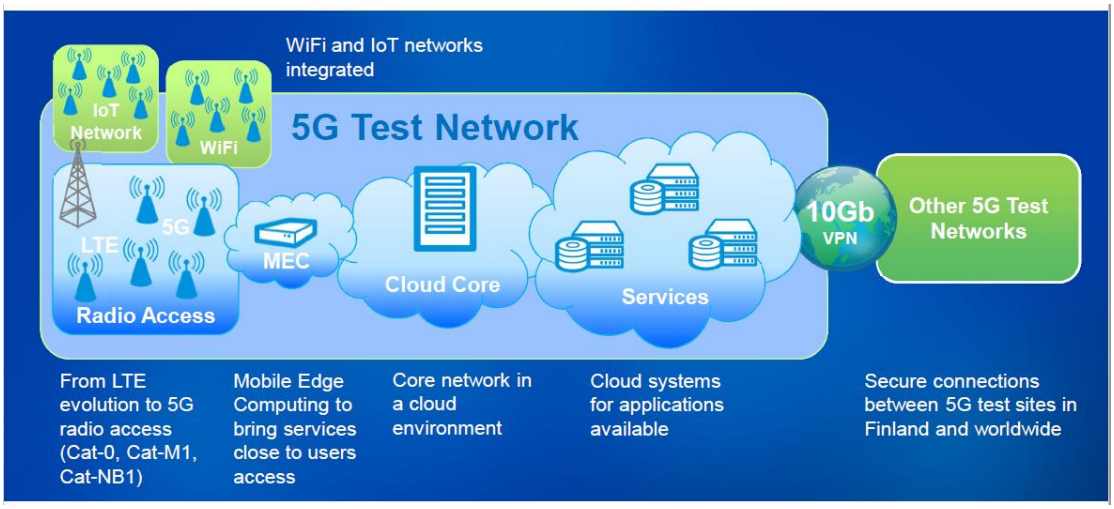


圖 43、5GTN Use Cases

資料來源：VTT

(二) 5G 服務創新研發平臺(TAKE-5)

TAKE-5 (5th Evolution Take of Wireless Communication Networks)主要是建立一個跨學科、開放的研究平臺，對 5G 網路和服務創新進行調查和實驗，將現有不同項目開發中的研究網路，匯集成一個通用的共享測試平臺，以測試和驗證 5G 網路功能。TAKE-5 由 VTT 建立一組核心網路架構，將全國不同地的測試點及不同的合作夥伴整合到其核心網路內(請參見圖 44 及圖 45)。

其應用主要是結合無線電 WiFi、行動網路、網際網路和雲端運算等方面推動 5G 行動網路的發展。第一個重點是將不同技術無線接取網路，透過 OpenStack 在同一核心網路內介接的技術；第二個是專注於網路與雲端技術，即網路虛擬化，並將所有傳統無線與行動技術提供互通性整合；第三個是具備傳輸速度提高與低延遲性的特性，系統處理能力須確保能正確分配資源予用戶應用，以滿足使用者體驗(Quality of Experience，簡稱 QoE)。

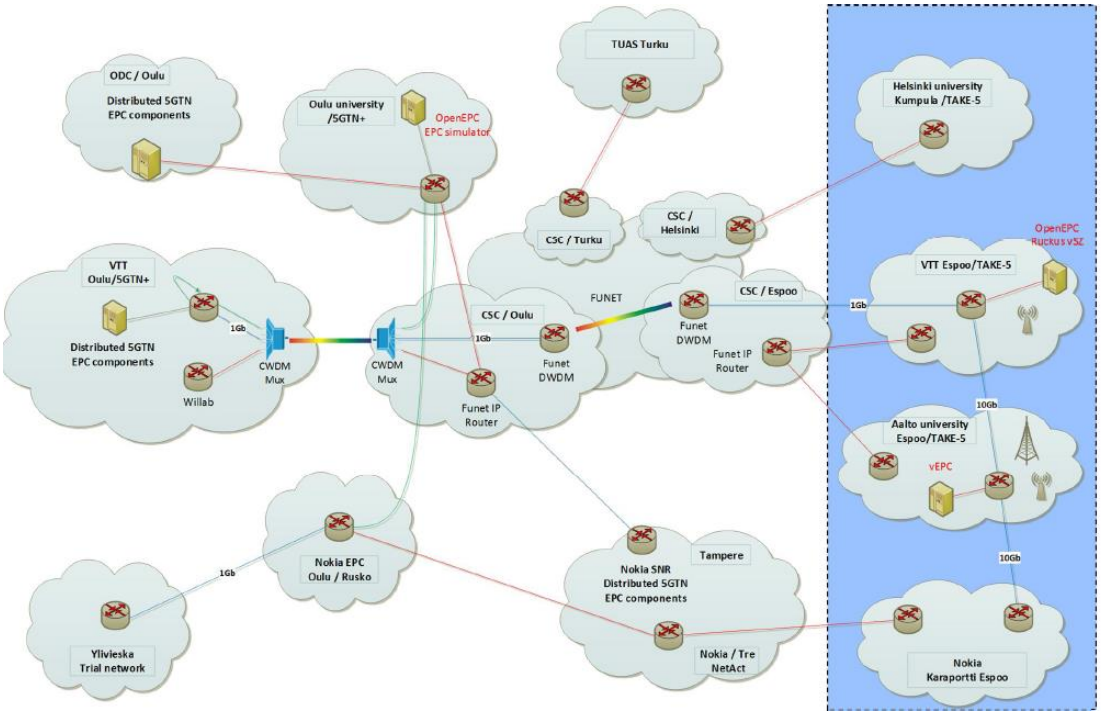


圖 44、TAKE-5 Testbed Cooperation

資料來源：VTT

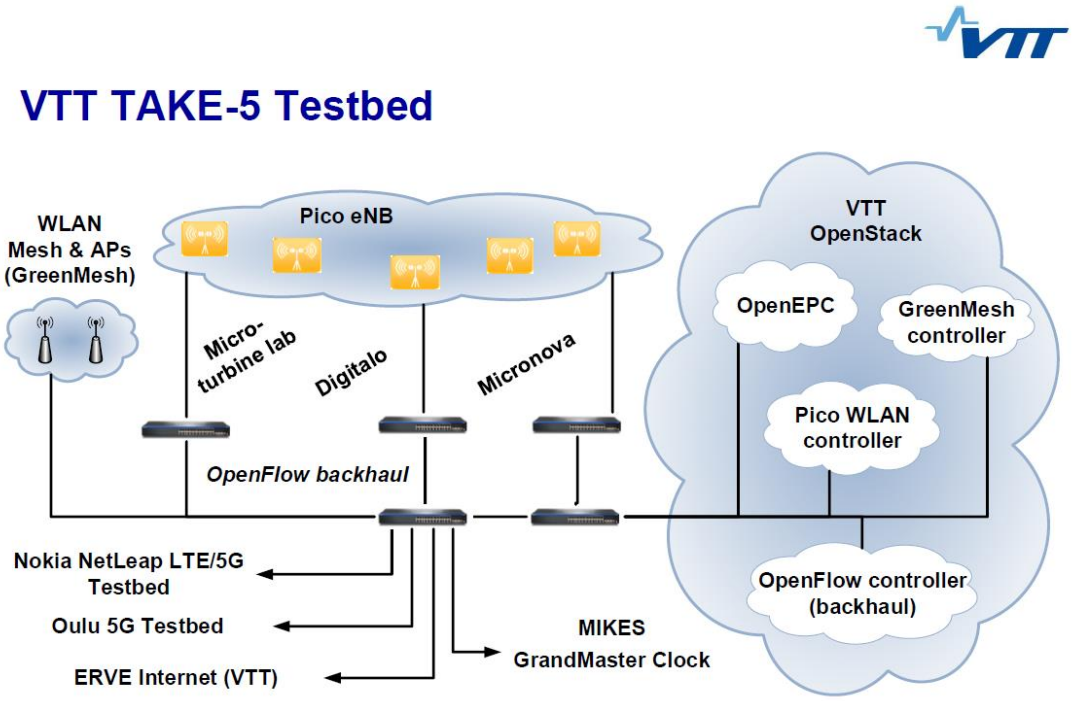


圖 45、VTT TAKE-5 實驗平臺

資料來源：VTT

VTT 專家也跟我們分享了該中心於此平臺開發之一些實際應用案例。

1.　智慧電網(Smart Grid)遠端遙控與監測

VTT 專家表示這一個測試平臺的使用個案已被應用於智慧電網遠端遙控與監測的自動化工業系統，來驗證系統的可靠性、彈性及可接近性(如圖 46)。在討論過程中，TTC 林副執行長也對此平臺與 VTT 主講者有許多交流，詢問 VTT 是否有開發在智慧電網上的 Simulation Tool，也得到正面的回應，因該平臺並非於 Espoo 的實驗室中，所以無法實際展示，林副執行長也向對方分享本中心也被台電委託有關此部分安全上的研究，也許後續可以有更多的資安技術經驗交流。

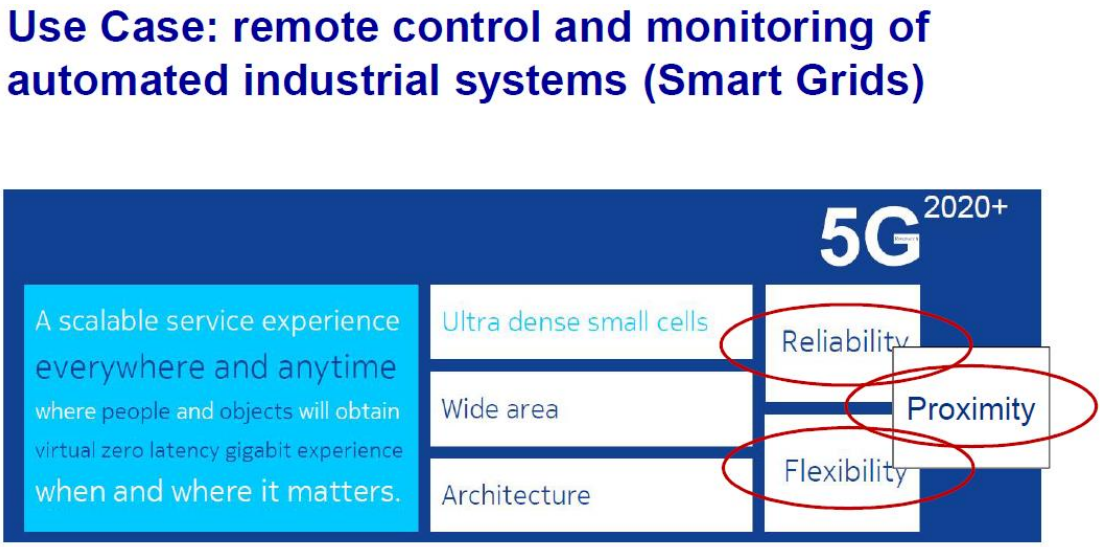


圖 46、VTT TAKE-5 智慧電表使用案例

資料來源：VTT

2.　異質網路規劃

該中心與我們介紹，他們所開發利用機器人於室內與室外執行的 3D 傳播模式的網路效能量測，及室內 LTE-WiFi 涵蓋範圍及品質量測 (in multiple floors)，該中心利用機器人,參考位置及室內地圖量測市內多樓層的 LTE-WiFi 涵蓋範圍及品質量測等，林副執行長也特別分享本中心受 NCC 委託量測各業者的網路效能，也了解到 VTT 也有執行此業務，但相關細節因簡報人員非執行此業務人員，所以細部執行方式較難與我們詳細說明。

TAKE-5 這種針對各種技術及應用實現的實驗網路對電信業者來說是至關重要，因為 SDN 的技術具有破壞性創新，無線接取網路 RAN 可透過 multi RAN 雲端化的支持，未來可創造具有成本效益的 RAN，但必須具有安全又無縫遷移路徑規劃，確保既有服務不會中斷，另一面當電信與網路互相融合時，在 5G 端點到端點間的網路安全，會跨越雲端與虛擬化組件，這些重大的安全威脅，是一項挑戰，也是創新和新商機，5G 帶來了新的技術優勢，但必須進行適當的技術與經濟分析，才能為製造商、電信營運商、服務和內容提供商提供經營持續性的優勢，也是後續可以持續關注的焦點。

(三) 積極參與歐盟 5G-PPP 贊助的專案及安全項目研究

芬蘭 VTT 技術研究中心負責 5G-PPP 贊助的大型專案 5G-Ensure 協調及聯繫的角色，技術上由 Thales(法國)管理。合作夥伴包括阿爾卡特朗訊貝爾實驗室(法國)、愛立信、南安普敦 IT 創新中心(英國); NEC(德國)、Nixu(芬蘭)、Orange(法國)、SICS ICT(瑞典)、Thales Alenia Space España(西班牙)、義大利電信，Trust-IT 服務(英國)和牛津大學等 16 個機構參與。其目標是為了推動 5G 在法規、標準、與安全協會公約的基礎上，建立起安全架構，滿足大眾安全與隱私的要求，如圖 47 所示。

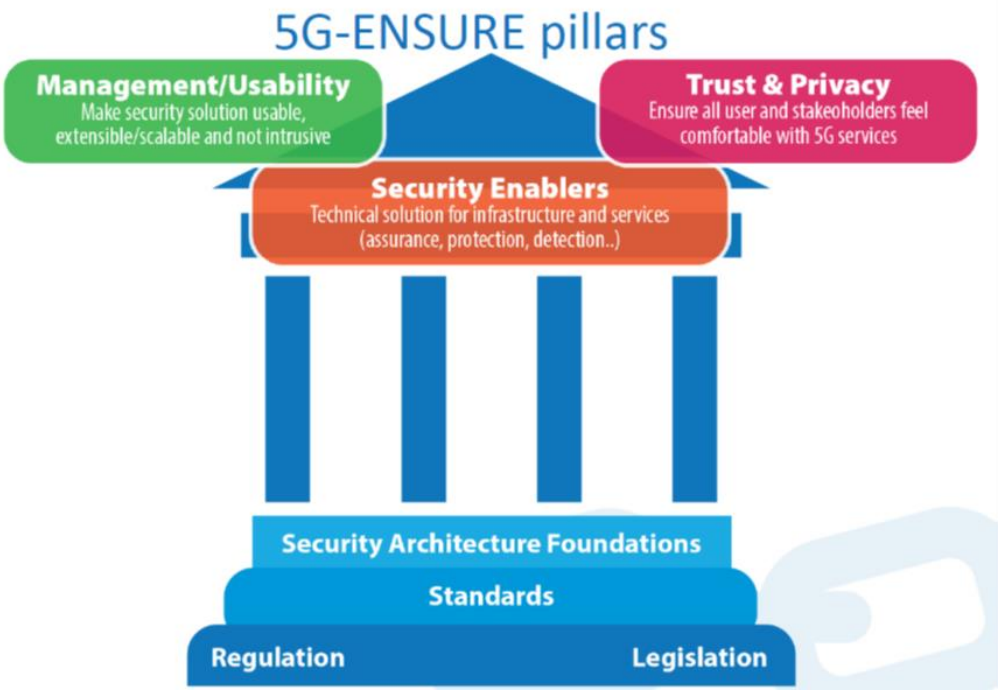


圖 47、5G-ENSURE 安全架構

資料來源：VTT

5G 的實驗網路初步已具有通訊和運作能力，透過這個專案推動全新的安全解決

方案，目前已開發出 17 個安全項目，並釋出相關規範和軟體，以展示其整合的成效，在驗證其維運與可行性方面，經由法國和芬蘭的互連節點，其測試平臺環境包括：端到端、多重區域、多重 5G 營運商，以小規模上展示了 5G 網路安全環境，其配置已識別威脅案例，符合初步規劃的 5G 安全和隱私要求。每個安全項目除了提供安全增強的功能，其整合起來的附加價值，足以改善接取控制、隱私、信任以及網路管理和虛擬化安全性。目前行動寬頻的安全架構是建立在 3GPP TS 33.401 的基礎上，其中網路的安全功能以安全區域、安全層和安全特徵來表示， 這些架構在 5G 系統會被修正，以納入 5G 依賴的軟體定義網路絡和網路虛擬化,以及支持多網域和垂直應用的案例。

因此，實體網路與邏輯網路方面，安全定義都應被重新審視，這些都與 5G 信任模型密切相關，並且會與管理及所有權相結合。隨著架構的起草實施，每個 5G-ENSURE 項目都會與網路單元關聯，顯示了安全的加強和需要的提升，這個專案仍持續進行中，且其結果勢必影響歐盟法規及 3GPP 的標準訂定，也將成為 5G 關注的議題。

由交流過程中得知，VTT 主要在 5G-PPP 的 5G-ENSURE 專案中負責 5G 安全的研究與溝通協調，VTT 專家也跟我們分享，目前已經研究及歸納出 5G 安全標準推動的方向包含身份認證(AAA)、隱私保護、安全監控、不同連接網路的信任安全、SDN 的網路安全等，但主講者已表示，這些方向目前尚未被詳細定義出該如何規範，另外在討論中雙方的交流中大家也一致認同，在未來 5G、IoT 的網路中，並非僅止於規範電信業者網路的安全，製造商對於各種設備、裝置製造的安全應該也要被規範。

VTT 專家也建議，想要得到目前 5G 最新資安標準發展，建議本中心可加入國際標準組織的討論，以掌握最新國際動態。

(四) SDN 網路安全研究

VTT 專家與我們分享該中心於 SDN 網路安全之相關研究，主講者首先說明，該中心於 5G 專案中也致力於 SDN 網路的研究，例如 SDN 網路於智慧電網的運用，如何於無線網路之接入與管理，整合 SDN 與小基站的佈建方式，及協助規劃電信等級的 SDN 網路等。因此在確保 SDN 網路的安全上，該中心也有相關研究及關注。

VTT 專家也說明了相關攻擊案例，並提出以異常攻擊的監控方式，並將攻擊流量阻斷或分流的方式解決(如圖 48)，蔡主任也詢問了 VTT 是否有蒐集各種攻擊資訊，主

講者表示是有的；林主任也細部詢問主講者所提的阻斷隔離的方式，也得到主講者簡略解說。

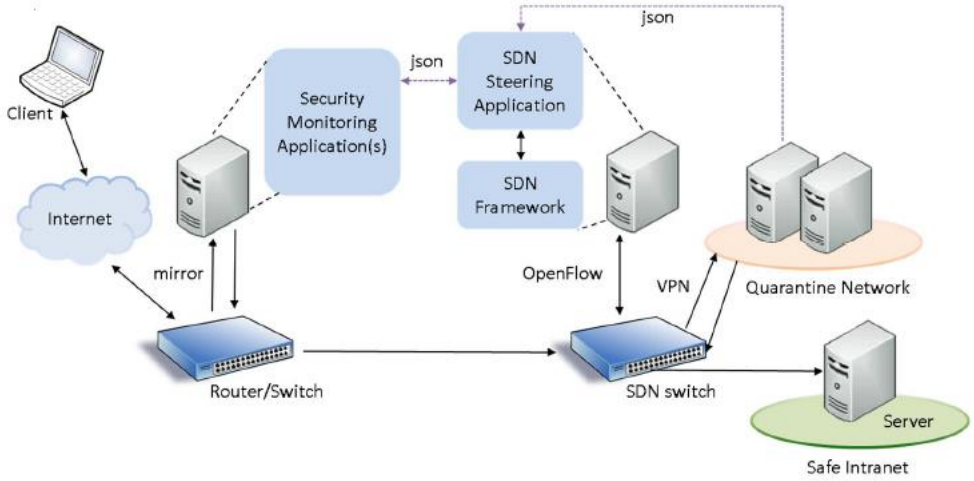


圖 48、Security Monitoring for Anomaly Detection with SDN

資料來源：VTT

第五章、 參訪心得與建議

一、 參訪心得

芬蘭為人口數僅約 550 萬人的國家，為 GDP 高、社會福利高的國家，早在 1995 年率先於首都赫爾辛基推動網路新都計畫，曾經是全球競爭力第一名的國家。芬蘭國土面積為台灣的九倍大，全國有 69%的土地被森林覆蓋，原本靠木材加工、造紙和林業機械等行業成為其經濟支柱，但由於網路媒體的興起，芬蘭造紙業的需求也大量降低，因此政府轉而重視電子業的研發，大力投入研發資金。也造就曾經興盛一時的 Nokia。當 2013 年 Nokia 將手機事業出售給微軟時，對芬蘭國內的確為一大衝擊，時至今日，已非全球競爭力第一名之國家，其經濟發展也逐漸率退中，但長久以來，芬蘭政府仍積極鼓勵創新技術，發展 ICT，在此次參訪中，發現芬蘭政府已投入 5G 與 IoT 的實驗網路平臺並結合產官學研各層面之合作與研究，並積極參與國際標準的制定，可見其對未來 5G 及物聯網發展的重視。

此次本參訪團隊透過與 Synopsys Defensics 研發團隊直接的技術交流，充分了解該軟體於檢測流程中的角色及原理，對於本計畫在檢測流程開發上有很大的幫助。而在與 Nokia 3 天的技術交流過程中，Nokia 安全專家與我們分享各種行動寬頻網路安全的解決方案，與面對各種通信協定的漏洞，及阻斷式攻擊的影響時的防禦方式，並分享與獲得國際間最新資安標準及趨勢等資訊，獲益良多。

對於行動寬頻網路安全研究多年的安全專家 Dr. Silke，特別與我們分享她對於未來行動寬頻網路安全攻擊的因應措施，在網路攻擊日新月異下，她認為在物聯網裝置安全上，設置憑證為最重要的安全防護機制，發放憑證之平臺也是未來發展物聯網時的一大重點。除憑證外，搭配設置 IPSec 的連接網路，與積極參與並加入國際標準組織，可獲得最新攻擊資訊及資安標準動態，被專家認為是最佳的解決方案。針對 IPSec，目前此方案為國內電信業者所排斥，本參訪團隊同時也向 Nokia 專家表達，若能提供國外電信業者 IPSec 佈建方式及對網路頻寬影響經驗之分享，對國內推行 IPSec 將為一大幫助。而對於積極加入國際組織並參與標準的討論，的確是目前國內較為欠缺的一環。

在藉由本次參訪 VTT 的過程中，可以清楚了解到芬蘭政府對於 5G 的未來發展極為重視，其積極與各產學間及國際間合作設置實驗平臺，除進行技術的開發上，也在

實驗平臺進行未來網路安全的研究，該中心具備各種最新的研發技術，未來相關研究上可與該單位再進一步做相關的議題交流。

二、 參訪建議

此次參訪交流上，除資安技術上的交流外，對於未來行動寬頻網路的發展與防禦獲益良多，經由此次參訪，提出以下參訪建議。

(一) 國內政府或電信業者應積極參與國際標準組織之安全議題討論

此次參訪過程中，Nokia 專家指出，GSMA 會對其會員公告，全球最新攻擊資訊(如 SS7)，而在參加國際標準組織的資安討論中，也可以得知最新國際資安防護措施與標準動態，此建議在與 VTT 專家對談中，該中心專家也特別提出此建議，實為國內政府與電信業者應考量的重點。

(二) 終端設備設置安全憑證為行動寬頻網路安全防護第一道防線

Nokia 在提供的相關攻擊解決方案中，建議物聯網設備皆應設置安全憑證，此為資安攻擊防護重要的一環，該公司在基站設備上亦具備設置安全憑證的功能，此方法也是防範偽基站的一種解決方案，故終端設備設置安全憑證為行動寬頻網路安全防護第一道防線，於未來在規劃物聯網安全或防止偽基站措施上，安全憑證的確是一個須考量的重點。有鑑於未來物聯網之普及，發放安全憑證的平臺將會是未來一個很重要的角色，本中心亦可考量是否將此納為未來發展策略之一，以中立第三方角色，扮演發放安全憑證平臺角色。

(三) 設置 IPSec 為行動寬頻網路安全防護重點

Nokia 安全專家再三強調，網路設置 IPSec 為行動寬頻網路安全防護重點，其客戶中也有三十多家電信業者已採用，但國內電信業者擔心影響到網路效能，此方案目前仍受到國內電信業者的拒絕，因此設備製造商若願意提供國際電信業者實際的佈建經驗供國內政府及電信業者參考，協助在國內推動 IPSec 行動寬頻網路安全防護。

(四) Nokia 全方位的行動寬頻安全解決方案，可作為本計畫檢測規劃之參考

Nokia 安全團隊在規劃行動寬頻安全解決方案時，亦是先模擬駭客攻擊流程來規劃及開發各種防禦工具，此思考邏輯亦可作為本計畫在規劃檢測項目及檢測流程時之參考。

(五) 歐盟與美國相同，並無強制性之基站資安檢測規範

因本計畫目標為訂定基站資安檢測規範草案，因此於國外參訪過程中，除檢測技術的交流外，也期望能取得國際上其他國家對於基站資安管理或檢測規範之相關經驗，於第 1 期計畫中，本計畫團隊已參訪美國與韓國，了解到美國及韓國皆未對電信業者的基站資安具有強制性的檢測規範，在行動寬頻網路安全的保障上，皆以自律性方式，請電信業者自行確保其網路的安全。此行於參訪芬蘭的交流過程中也發現，歐盟在基站資安檢測的範疇上亦無強制性的檢測規範。但本計畫團隊在持續關注國際標準動態中發現，3GPP 於 2017 年 9 月已提出基站安全保證標準(Security Assurance Specification，簡稱 SCAS)草案[12]，可供本計畫訂定基站資安檢測規範之依循及參考。

在第 1 期計畫及本計畫此次參訪所得到的國際經驗中，了解到目前歐美對於基站資安皆無強制性之檢測規範，認為電信業者應確保其所提供之行動寬頻網路服務的安全性，所以一致採取自律性之管理方式。

[12] 3GPP TS 33.216, “Security Assurance Specification (SCAS) for the evolved Node B (eNodeB) network product class (Release 15)”, 2017/9.

參考書目

1. Synopsys, L2CAP Test Suite Data Sheet, [Online]. Available: https://www.synopsys.com/software-integrity/security-testing/fuzz-testing/defensics/protocols/bt-l2cap.html
2. NIST, CVE-2017-7645, [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2017-7645
3. Synopsys, NFS3 Server Test Suite Data Sheet, [Online]. Available: https://www.synopsys.com/software-integrity/security-testing/fuzz-testing/defensics/protocols/nfs3-server.html
4. Minrui Shi, “Alternative Solutions for the improvement of SS7 security”, 2016/6/29 , [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Documents/Abstracts_and_Presentations/S1P3_Minrui_Shi.pdf
5. Pascal Dejardin, “Observations on SS7 Network Security”, 2016/6/29, [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Documents/Abstracts_and_Presentations/S1P4_Pascal_DejardinV2.pdf
6. Silke Holtmanns, “Interconnection Security Standards–We Are All Connected”, Journal of ICT, Vol.4_1, p.p. 1-18, 2016, [Online]. Available: https://www.riverpublishers.com/journal/journal_articles/RP_Journal_2245-800X_411.pdf
7. The Register, “Someone checked and, yup, you can still hijack Gmail, Bitcoin wallets etc via dirty SS7 tricks”, 2017/9, [Online]. Available: https://www.theregister.co.uk/2017/09/18/ss7_vuln_bitcoin_wallet_hack_risk/
8. SECURITYWEEK, “Hackers Exploit SS7 Flaws to Loot Bank Accounts”, 2017/5, [Online]. Available: http://www.securityweek.com/hackers-exploit-ss7-flaws-loot-bank-accounts

9. Forbes, “Hackers Can Steal Your Facebook Account With Just A Phone Number”, 2016/6, [Online]. Available: https://www.forbes.com/sites/thomasbrewster/2016/06/15/hackers-steal-facebook-account-ss7/#616b564167de

10. Silke Holtmanns, Yoan Miche and Ian Oliver, “Subscriber Profile Extraction and Modification via Diameter Interconnection, International Conference on Network and System Security”, 2017/7/26, [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-64701-2_45

11. Kotte, B., Holtmanns, S., Rao, S., “Detach me not - DoS attacks against 4G cellular users worldwide from your desk”, Blackhat Europe, 2016, [Online]. Available: https://www.blackhat.com/eu-16/briefings.html#detach-me-not-dos-attacks-against-4g-cellular-users-worldwide-from-your-desk

12. 3GPP TS 33.216, “Security Assurance Specification (SCAS) for the evolved Node B (eNodeB) network product class (Release 15)”, 2017/9.

附錄二 3GPP TS33.216 V15.0.0 中譯版

第三代合作夥伴計畫;

技術標準小組 - 服務與系統細節;

演進式基站 (eNodeB) 網路設備類別

之 安全保證規範 (SCAS)

(第 15 版)

關鍵字

LTE，資訊安全，安全保證，網路，設備，層級

3GPP

地址

3GPP 技術支援辦公室地址

650 Route des Lucioles - Sophia Antipolis

Valbonne - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

網址

http://www.3gpp.org

目次

前言

此技術規範文件是由第三代合作夥伴計畫 (3GPP) 所撰寫，國立中山大學應用密碼實驗室翻譯為正體中文。

本技術文件的內容正由技術標準小組 (TSG) 持續研議中並且可能在正式的許可後修改其內容。若是技術標準小組修改本技術文件的內容，技術標準小組將會發布更新發布日期的文件並以下列規則改變版本號碼：

版本 x.y.z

並且：

x 第一位版號：

1 提交予技術標準小組作為附加內容。

2 提交予技術標準小組以待審核。

3 或以上代表技術標準小組已審核並通過該版本號之文件。

y 第二位版號會因為任何對於技術內容的更動而增加，例如增加，修正，或更新技術內容，等等。

z 第三位版號會因為需要對文件做出純粹編輯方面的更動而增加數字。

1. 適用範圍

本份技術文件包含演進式基站(eNB)之網路設備類別的開發目標，技術需求，還有相關測試案例。文件是基於所發布的通用型安全保證需求目錄所撰寫，並對於其中的需求與測試案例做出了具體的修改，同時也確立了專門用於演進式基站網路設備類別的需求與測試案例。

2. 參考引用

以下文件所包含之條文，透過引用於本文件之中，視同本文件所包含之條文。

- 引用文獻包含具體引用 (引用時標明發表日期，編輯版號，或發行版號等) 與非具體引用。
- 具體引用時，不包含其往後之修訂版本。

- 非具體引用時，視同引用最新版本。當引用文件為第三代合作夥伴計畫之文件 (包含行動特別小組之文件) 時，非具體引用視為引用本文件發行時該文件之最新版本。

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.117: "Catalogue of general security assurance requirements".

[3] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[4] 3GPP TR 33.926: "Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes".

3. 定義與縮寫

3.1 定義

在本文件的範圍內，所使用的名詞與定義將依照第三代合作夥伴計畫之文件 TR 21.905 [1] 與以下的規則作使用。本文件中所定義之名詞若在第三代合作夥伴計畫之文件 3GPP TR 21.905 [1] 中已有定義時將優先於該文件之定義。

3.2 縮寫

在本文件的範圍內，所使用的縮寫與簡稱將依照第三代合作夥伴計畫之文件 TR 21.905 [1] 與以下的規則作使用。本文件中所定義之縮寫若在第三代合作夥伴計畫之文件 3GPP TR 21.905 [1] 中已有定義時將優先於該文件之定義。

4. 演進式基站之特定安全需求與相關測試案例

4.1 引言

演進式基站之特定安全需求包含源自其自身特定的安全性功能需求，以及文件 TR 33.926 [4] 中所描述對演進式基站的威脅所導致的安全需求。

而與其他網路設備類別通用的安全需求和測試案例已經於文件 TS 33.117 [2] 中描述，所以就不再在本文件中重複。

4.2 對於演進式基站之特定安全需求的具體調整與相關測試案例

4.2.1 引言

本小節包含對於演進式基站之特定安全需求的具體調整與相關測試案例。.

4.2.2 基於第三代合作夥伴計畫之規範與測試案例的演進式基站之安全性功能需求

4.2.2.1 基於第三代合作夥伴計畫之規範 – TS 33.401 [3] 的演進式基站之安全性功能需求

4.2.2.1.1 控制層資料機密性保護

需求名稱： 控制層資料機密性保護

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 5.3.4a 條款中所述：「演進式基站應提供 S1 與 X2 介面上之端點間控制層資料封包之機密性保護。」

威脅性參考： 文件 TR 33.926 [4] 第 A.2.2.1 條款 – 控制層資料機密性保護。

安全性目標參考： 待公布

測試案例：

本條款中所提及之需求是以文件 TS 33.117 [2] 第 4.2.3.2.4 條款中所提及之程序進行測試。

4.2.2.1.2 控制層資料完整性保護

需求名稱： 控制層資料完整性保護

需求參考：待公布

需求描述： 如文件 TS 33.401 [3] 第 5.3.4a 條款中所述：「演進式基站應提供 S1 與 X2 介面上之端點間的控制層資料封包之完整性保護。」

威脅性參考： 文件 TR 33.926 [4] 第 A.2.2.2 條款 – 控制層資料完整性保護。

安全性目標參考：待公布

測試案例：

本條款中所提及之需求是以文件 TS 33.117 [2] 第 4.2.3.2.4 條款中所提及之程序進行測試。

4.2.2.1.3 用戶層資料於演進式基站之加密與解密

需求名稱： 用戶層資料於演進式基站之加密與解密

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 5.3.4 條款中所述：「演進式基站應負責加密與解密 Uu 介面，S1 與 X2 介面中的端點之間的用戶層封包」

威脅性參考：文件 TR 33.926 [4] 第 A.2.2.3 條款 – 用戶層資料於演進式基站之加密與解密。

安全性目標參考：待公布

測試案例：

本條款中所提及之需求是以文件 TS 33.117 [2] 第 4.2.3.2.4 條款中所提及之程序進行測試。

4.2.2.1.4 用戶層資料完整性保護

需求名稱： 用戶層資料完整性保護

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 5.3.4 條款中所述：「演進式基站應負責處理 S1 與 X2 介面上端點間之用戶層封包之完整性保護。」

威脅性參考： 文件 TR 33.926 [4] 第 A.2.2.4 條款 – 用戶層資料完整性保護。

安全性目標參考：待公布

測試案例：

本條款中所提及之需求是以文件 TS 33.117 [2] 第 4.2.3.2.4 條款中所提及之程序進行測試。

4.2.2.1.5 接取層之完整性演算法選擇

需求名稱： 接取層演算法選擇

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 7.2.4.1 條款中所述：「服務網路應依據用戶裝置所支援的安全功能以及當前服務網路所設定之受許可之安全功能列表，選將使用的擇演算法。」

如文件 TS 33.401 [3] 第 7.2.4.2.1 條款中所述：「每個演進式基站都應透過網管系統設定其可使用之演算法列表。應有一表列出完整性演算法，另有一表列出加密演算法。這些列表應由電信業者所決定之優先順序作排序。」。

威脅性參考： 待公布

安全性目標參考： 待公布

測試案例：

測試目的：

確認演進式基站所選擇之演算法為所設定之列表中的最高優先順序者。

測前環境：

測試環境中之演進式基站已設定所允許之安全演算法列表並對其優先度排序。

測試步驟

1) 用戶裝置傳送一連結請求訊息至演進式基站。

2) 演進式基站收到 S1 介面內容設定請求訊息。

3) 演進式基站傳送**安全模式指令**訊息。

4) 用戶裝置回應一**接取層安全模式完成**訊息。

預期結果：

演進式基站傳送**安全模式指令**時所包含所選擇的演算法應是列表中的最高優先順序，並且存在於用戶裝置的演進式封包系統之安全功能列表中。

接取層安全模式完成訊息中的訊息認證碼應認證通過，並且應選擇正確的接取層之保護演算法且正確的實施之。

預期之證明證據格式：

日誌紀錄檔之抽樣副本。

4.2.2.1.6 驗證無線資源管理訊息完整性保護

需求名稱： 檢查無線資源管理訊息之完整性

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 7.4.1 條款中所述：「行動裝置與演進式基站對於失敗的無線資源管理完整性驗證都應有相關的應對。當偵測到完整性驗證失敗時 (如有瑕疵或是缺找完整性訊息驗證碼)，相對應的訊息應被捨棄。」

威脅性參考： 待公布

安全性目標參考： 待公布

測試案例：

測試目的：

確認當完整性驗證失敗時 (如有瑕疵或是缺少完整性訊息驗證碼) 有正確得捨棄訊息。

測前環境：

測試環境中的演進式基站須開啟無線資源管理訊息之保護設定。

測試步驟

正面測試：

演進式基站收到含有正確完整性訊息驗證碼之無線資源管理訊息。

負面測試：

演進式基站收到含有錯誤或缺少完整性訊息驗證碼之無線資源管理訊息。

預期結果：

正確的捨棄了負面測試中的無線資源管理訊息。

預期之證明證據格式：

日誌紀錄檔之抽樣副本。

4.2.2.1.7 演進式封包系統完整性演算法EIA0之選擇

需求名稱： 演進式封包系統完整性演算法零號（EIA0）之選擇

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 5.1.4.2 條款所述：「只有在無授權的緊急電話時才能選擇使用演進式封包系統完整性演算法零號。」

威脅性參考： 待公布

安全性目標參考： 待公布

測試案例：

測試目的：

確認有正確使用接取層之NULL完整性演算法。

測前環境：

測試環境包含用戶裝置與演進式基站。可以模擬替代用戶裝置。

供應商應提供使用文件描述演進式封包系統完整性演算法EIA0之啟用與禁用方式。

測試步驟

正面測試：

1) 演進式基站收到一份用戶裝置安全功能列表中只含有 EIA0 的 S1 介面內容設定訊息。
2) 演進式基站傳送接取層安全模式指令到用戶裝置。

負面測試：

1) 演進式基站收到一份包含 EIA0 與其他演算法的用戶裝置安全功能列表。
2) 演進式基站傳送接取層安全模式指令到用戶裝置。

預期結果：

只有在正面測試中才能選擇使用演進式封包系統完整性演算法EIA0。

預期之證明證據格式：

日誌紀錄檔之抽樣副本。

4.2.2.1.8 演進式基站的金鑰更新

需求名稱： 演進式基站的金鑰更新

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 7.2.9.1 條款中所述：「基站金鑰、無線資源管理加密金鑰、無線資源管理完整性金鑰、用戶層加密金鑰，與用戶層完整性金鑰的金鑰更新應由演進式基站觸發，在相同的無線承載識別碼與基站金鑰時，封包資料匯聚協定中的 COUNT 欄位可重複使用。」

威脅性參考： 待公布

安全性目標參考： 待公布

測試案例：

測試目的：

確認演進式基站進行eNB金鑰更新時，包含封包資料匯聚協定中的 COUNT 欄位值。

測前環境：

可以模擬替代用戶裝置。

測試步驟

1) 演進式基站傳送接取層安全模式指令給用戶裝置而用戶裝置也回應接取層安全模式指令。
2) 用戶裝置傳送一個包含封包資料匯聚協定中的 COUNT 欄位值於無線資源控制層訊息或是用戶層訊息給演進式基站。用戶裝置持續傳送包含逐漸遞增的封包資料匯聚協定中的 COUNT 欄位值於無線資源控制層訊息或是用戶層訊息內，直到步驟 3 發生，或是有封包資料匯聚協定中的 COUNT 欄位值。
3) 演進式基站觸發基站內細胞切換。

預期結果：

演進式基站觸發基站內細胞切換以更新eNB金鑰。

預期之證明證據格式：

日誌檔的部分中能呈現資料匯聚協定中的 COUNT 欄位值與基站內細胞切換行為。這部分的呈現可以是螢幕截圖的方式。

4.2.2.1.9 接取層安全模式指令執行程序

需求名稱： 接取層完整性演算法選擇

需求參考： 待公布

需求描述： 演進式基站應以序列表中最高優先順序之完整性演算法保護**安全模式指令**訊息。

威脅性參考： 文件 TS 33.401 [3] 第 7.4.2 條款

安全性目標參考： 待公布

測試案例：

測試目的：

確認有正確的選擇並執行接取層完整性演算法。

測前環境：

測試環境包含用戶裝置。可以替代模擬用戶裝置。

測試步驟：

演進式基站傳送**安全模式指令**訊息。用戶裝置以**安全模式完成**訊息作為回應。

預期結果：

1. 演進式基站選擇序列表中最高優先順序且存在於用戶裝置的演進式封包系統之安全能力表中的完整性演算法。演進式基站檢查**安全模式完成**訊息中的訊息驗證碼是否正確。
2. **安全模式完成**訊息中的驗證MAC訊息，而也正確的選擇並執行了接取層完整性演算法。

預期之證明證據格式：

包含測試結果的系統截圖。

4.2.2.1.10 預防 X2 換手中的降等攻擊

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 7.2.4.2.2 條款中所述：「在路徑改變訊息中，目標演進式基站應將從來源演進式基站所收到的用戶裝置演進式封包系統之安全能力表傳送給行動管理實體。」

威脅性參考： 待公布

安全性目標參考： 待公布

測試案例：

測試目的：

確認有正確預防 X2 換手中的降等攻擊。

測前環境：

測試環境中應有來源演進式基站與目標演進式基站，可以模擬替代來源節點。

測試步驟：

目標演進式基站正確傳送路徑改變訊息到行動管理實體。

預期結果：

路徑改變訊息中包含用戶裝置的演進式封包系統之安全能力表。

預期之證明證據格式：

包含測試結果的系統截圖。

4.2.2.1.11 演進式基站改變時的接取層保護演算法選擇

需求名稱： 演進式基站改變時的接取層保護演算法選擇。

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 7.2.4.2.2 條款與第 7.2.4.2.3 條款中所述：「目標演進式基站應根據其本身之排序過的演算法列表選擇用戶裝置演進式封包系統之安全能力表中最高優先順序的演算法 (這包含完整性演算法與加密演算法)。若是所選擇的演算法與來源基站節點所選擇的不同應透過換手指令通知用戶裝置。」

威脅性參考： 待公布

安全性目標參考： 待公布

測試案例：

測試目的：

確認有正確選擇接取層保護演算法。

測前環境：

測試環境中應有來源與目標演進式基站與行動管理實體，可以模擬替代來源節點與行動管理實體。

測試步驟：

測試 1:

來源演進式基站在切換請求訊息中傳送來源基站所使用的加密演算法與完整性演算法給目標演進式基站。

目標演進式基站驗證這些演算法並選擇其列表中最高優先順序的接取層演算法。目標演進式基站將所選擇的演算法加入換手指令中。

測試 2:

行動管理實體傳送用戶裝置演進式封包系統之安全能力表給目標演進式基站。

目標演進式基站自**換手指令**中之列表中選擇其最高優先順序之接取層演算法。

以上的測驗假設目標演進式基站所選擇的演算法與來源演進式基站所選擇的演算法是不同的。

預期結果：

同樣對於兩項測試：

1. 用戶裝置驗證換手指令訊息中的訊息驗證碼。
2. 換手指令中的MAC碼驗證通過，而也正確的選擇並執行了接取層完整性演算法。

預期之證明證據格式：

包含測試結果的系統截圖。

4.2.2.1.12 演進式基站對於無線資源管理訊息與用戶層的下行加密

需求名稱： 演進式基站對於無線資源管理訊息與用戶層的下行加密

需求參考： 待公布

需求描述： 如文件 TS 33.401 [3] 第 7.2.4.5 條款中所述：「演進式基站應在傳送接取層安全模式指令訊息之後開始加密無線資源管理層與用戶層之下行資料。」

威脅性參考： 待公布

安全性目標參考： 待公布

測試案例：

測試名稱： TC_eNB_DL_Cipher

測試目的： 確認演進式基站在傳送接取層安全模式指令訊息之後會正確執行無線資源管理層與用戶層之下行封包加密。

測前環境：

- 測試環境中的用戶裝置要與演進式基站網路設備連線，可以模擬替代用戶裝置。.
- 測試人員可以存取接取層安全性內容與其中的密鑰 (例如：無線資源管理層與用戶層的加密密鑰)。
- 測試人員可以存取 Uu 介面並且有透過用戶裝置所開啟的除錯端口擷取 Uu 介面訊息的能力。

測試步驟：

1) 用戶裝置應由測試人員開機以觸發註冊程序 (連接與安全模式指令)。
2) 測試人員可以利用任何封包分析軟體對於 Uu Medium Access Control (MAC)介面執行封包擷取。
3) 測試人員篩選出演進式基站與用戶裝置之間的接取層安全模式指令訊息，與之後的無線資源管理層和用戶層的下行封包。
4) 測試人員根據接取層安全模式指令訊息中所存在的參數 (如：演算法名稱與演算法識別碼) 進行測驗。

   情境 1: 若參數中指示應使用無效加密演算法，測試人員應證驗步驟 3 中所篩選出的下行封包是未加密的狀態。

   情境 2: 若參數中所選擇的演算法是例如SNOW, AES, ZUC 等，測試人員應證驗步驟 3 中所篩選出的下行封包是加密過後的狀態。

   測試人員同時要檢查這些封包是否是依照接取層安全模式指令訊息中所選擇的演算法作加密。

附註： 本條款中所提及各項需求的施測方式是依照文件 TS 33.117 [2] 第 4.2.3.2.4 條款中所提及的測試方式進行。

預期結果：

- 所有在接取層安全模式指令訊息之後的下行封包都被加密，但是選擇無加密演算法的情形為例外。

預期之證明證據格式：

Evidence suitable for the interface, e.g. Screenshot contains the operation results.

4.2.3

適合該介面的證據，例如包含測試結果的螢幕截圖。

4.2.3 技術基準

4.2.3.1 引言

本小節包含基本的技術需求規範。

4.2.3.2 資料與資訊保護

4.2.3.2.1 資料與資訊保護 – 總則

並無對於文件TS 33.117 [2]中的 4.2.3.2.1 條款進行特定於演進式基站的更動。

4.2.3.2.2 資料與資訊保護 – 預防未授權之資訊揭露

並無對於文件TS 33.117 [2]中的 4.2.3.2.2 條款進行特定於演進式基站的更動。

4.2.3.2.3 儲存媒體中的資料與資訊保護

並無對於文件TS 33.117 [2]中的 4.2.3.2.3 條款進行特定於演進式基站的更動。

4.2.3.2.4 傳輸途中的資料與資訊保護

並無對於文件TS 33.117 [2]中的 4.2.3.2.4 條款進行特定於演進式基站的更動。

4.2.3.2.5 個人資料存取之日誌紀錄

並無對於文件TS 33.117 [2]中的 4.2.3.2.5 條款進行特定於演進式基站的更動。

4.2.3.3 保護資料的可用性與完整性

並無對於文件TS 33.117 [2]中的 4.2.3.3 條款進行特定於演進式基站的更動。

4.2.3.4 認證和授權

並無對於文件TS 33.117 [2]中的 4.2.3.4 條款進行特定於演進式基站的更動。

4.2.3.5 會話保護

並無對於文件TS 33.117 [2]中的 4.2.3.5 條款進行特定於演進式基站的更動。

4.2.3.6 日誌紀錄

並無對於文件TS 33.117 [2]中的 4.2.3.6 條款進行特定於演進式基站的更動。

4.2.4 作業系統

並無對於文件TS 33.117 [2]中的 4.2.4 條款進行特定於演進式基站的更動。

4.2.5 網頁伺服器

並無對於文件TS 33.117 [2]中的 4.2.5 條款進行特定於演進式基站的更動。

4.2.6 網路設備

並無對於文件TS 33.117 [2] 中的 4.2.6 條款進行特定於演進式基站的更動。

4.2.7 其他對於演進式基站的安全性功能需求

並無對於文件TS 33.117 [2] 中的 4.2.7 條款進行特定於演進式基站的更動。

4.3 對於演進式基站強化要求與相關測試案例

4.3.1 引言

本小節包含對於演進式基站強化要求與相關測試案例。

4.3.2 技術基準

並無對於文件TS 33.117 [2] 中的 4.3.2 條款進行特定於演進式基站的更動。

4.3.3 作業系統

並無對於文件TS 33.117 [2] 中的 4.3.3 條款進行特定於演進式基站的更動。

4.3.4 網頁伺服器

並無對於文件TS 33.117 [2] 中的 4.3.4 條款進行特定於演進式基站的更動。

4.3.5 網路設備

並無對於文件TS 33.117 [2] 中的 4.3.5 條款進行特定於演進式基站的更動。

4.3.6 其他對於演進式基站系統安全強化要求之特定調整與相關測試案例

並無對於文件TS 33.117 [2] 中的 4.3.6 條款進行特定於演進式基站的更動。

4.4 對於演進式基站基礎滲透測試之特定調整與相關測試案例

並無對於文件TS 33.117 [2] 中的 4.4 條款進行特定於演進式基站的更動。

附錄 A (資訊提供):

更動紀錄

Change history							
Date	**Meeting**	**TDoc**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**New version**
11-2016	SA3 85					文件建立	0.0.1
11-2016	SA3 85					實作 S3-161904,S3-161905, S3-161905	0.1.0
02-2017	SA3 86					實作 S3-170474	0.2.0
05-2017	SA3 87					實作 S3-171519, S3-171520, S3-171521, S3-171522	0.3.0
08-2017	SA3 88					實作 S3-172126, S3-172127, S3-171870, S3-171854, S3-172128	0.4.0
09-2017	SA#77					提交予以提供資訊與審核	1.0.0
09-2017	SA#77					提升至版號控制版本 + 增加 EditHelp 之編輯性更動	15.0.0

附錄三 NIST SP 800-187 Guide to LTE Security

NIST 特別出版品 800-187

LTE 安全準則

Jeffrey Cichonski Joshua
M. Franklin Michael
Bartock

本出版品得免費取自：
https://doi.org/10.6028/NIST.SP.800-187

電　腦　　安　全

NIST
國家標準科技研究院
美國商務部

LTE 安全準則

Jeffrey Cichonski
Joshua M. Franklin
應用網路安全部門
資訊科技實驗室

Michael Bartock
電腦安全部門
資訊科技實驗室

本出版品得免費取自：
https://doi.org/10.6028/NIST.SP.800-187

2017 年 12 月

(美國商務部)

美國商務部
Wilbur L. Ross， Jr.，秘書

國家標準科技研究院
Walter Copan， NIST 董事暨標準科技商務次長

權限

本出版品由 NIST 根據 2014 年聯邦資訊安全現代化法案(Federal Information Security Modernization Act 簡稱 FISMA，美國法典第 44 卷第 3551 條以下，公法(簡稱 P.L.)113-283)之法定責任所制定。NIST 負責制定資訊安全標準與準則，包括聯邦資訊系統的最低要求，但是，除非經相關聯邦官員基於其政策權限明文批准將其適用於國家安全系統之情況外，此等標準與準則並不應適用在國家安全系統。本準則符合美國行政管理和預算局(Office of Management and Budget)A-130 公告的要求。

本出版品內容不得牴觸商務次長基於法定權限所制定，且有拘束聯邦機構效力之標準與準則，亦不得將本出版品解讀為變更或取代商務次長、OMB 董事、或其他任何聯邦官員之既有權限。非政府組織得自願使用本出版品，且不受美國著作權法案規範，但是，我們希望您能標示出處。

國家標準科技研究院特別出版品 800-187
Natl. Inst. Stand. Technol. Spec. Publ. 800-187，共 49 頁(2017 年 12 月)
代碼:NSPUE2

本出版品得免費取自:
https://doi.org/10.6028/NIST.SP.800-187

本文件為充分敘述實驗程序或概念可能提及某些商業組織、設備或材料，但不代表 NIST 的推薦或認可，亦不代表這些商業組織、設備或材料最適用於本文件所提的情形。

本出版品可能提到 NIST 根據其法定責任所制定的其他出版品。既使相關手冊尚未完成，聯邦機構亦得使用本出版品中的資訊(含概念與方法)。 因此，在各出版品完成之前，現有的規定、準則及程序對其相關領域仍然有效。為規劃和過渡之目的，聯邦機構應密切注意這些 NIST 新出版品的進展。

我們鼓勵各組織在公開評議期間審查所有草稿內容，並提供 NIST 意見回饋。除以上所述外，更多 NIST 網路安全出版品可見於 https://csrc.nist.gov/publications。

有關本出版品之意見請寄到:

國家標準科技研究院
收件人:應用網路安全部門 資訊科技實驗室
100 Bureau Drive (收發室 2000)Gaithersburg， MD 20899-2000
電子郵件:LTEsecurity@nist.gov

可依據資訊自由法(Freedom of Information Act， FOIA)公開所有意見

電腦系統技術報告

國家標準科技研究院(NIST)之資訊科技實驗室(ITL)藉由為國家測量和標準基礎設施提供技術指導來增進美國的經濟與公共福利。資訊科技實驗室(ITL)開發測試、測試方法、參考數據、概念實施與技術分析之證據，以促進資訊技術的發展生產性使用。資訊科技實驗室(ITL)的職責包括為聯邦資訊系統中除國家安全相關資訊以外，具有成本效益和隱私之相關資訊，開發管理、行政、技術與物理的標準與準則。特別出版品 800 系列描述了資訊科技實驗室(ITL)在資訊系統安全方面的研究、指導方針和推廣工作，以及與業界、政府和學術機構的合作活動。

摘要

蜂巢技術(cellular technology)已經成為大部分人的主要網路入口，而社會中扮演著越來越重要的角色，而造成此一轉變的主要原因之一可能與第四代(4G)長期演進技術(Long Term Evolution，LTE)蜂巢技術的部署有關。本文件可作為 LTE 網路運行和探索 LTE 安全架構的基礎指南，並分析 LTE 網路遭受到的威脅與證實的緩解措施。

關鍵字

蜂巢安全、網路、長期演進技術、第三代合作夥伴計劃(3rd Generation Partnership Project， 3GPP)、LTE、通訊、無線

致謝

作者群希望感謝提供公眾意見的所有人，以及協助他們審閱本報告草稿和提供技術內容的同事，包括任職於 NIST 之 Tim Grance、Sheila Frankel、Sanjeev Sharma、Gema Howell、Michael Ogata、Nelson Hastings、Tracy McElvaney 與 Murugiah Souppaya。作者群亦感謝加拿大電信網路保護(Canadian Telecom Cyber Protection)工作小組所為的技術貢獻。最後，作者群特別感謝慕尼黑應用科學大學(Munich University of Applied Sciences)的 Alf Zugenmaier。

目標讀者

本文件介紹 LTE 的高級概念，並詳細討論 LTE 技術的安全機制，有技術背景的讀者最好了解基礎網路概念和一般網路安全。本文件旨在協助評估、採用及操作 LTE 網路的人士，特別是電信工程師、系統管理員、網路安全從業人員和安全研究人員。

商標資訊

目錄

附錄索引

圖目錄

表目錄

1 簡介

近幾十年以來，蜂巢技術在整個社會引起巨大的改變。除了提供電話服務外，蜂巢設備還可以儲存和處理個人資訊、提供企業連接、並且作為許多人的主要網路入口。電話、平板電腦、筆記型電腦、可穿戴裝置、車載蜂巢數據機，以及其他行業之特定設備都可以存取蜂巢網路。美國的蜂巢基礎設施正從較舊的第二代(2G)和第三代(3G)蜂巢技術，轉換成為諸如長期演進網路(LTE)等較新的第四代(4G)技術。現在，LTE 已是美國各地主要的空中介面技術，並正為全球各國迅速採用中。

1.1 目的與範圍

本文件旨在提供各組織有關基於 LTE 技術的蜂巢網路安全功能的資訊。LTE 網路甚少以獨立的方式部署，而是與前幾代蜂巢系統相整合，然而，3G 與 2G 網路不在本文件技術概述的範圍內。由於 2G 與 3G 網路係和 LTE 網路一同部署，因此在本文件有關威脅和緩解措施的部分，將會討論到這些較舊的蜂巢系統。

本文件主要內容在分析傳統上由無線網路提供商擁有及／或經營之系統的安全，但亦包含為操作行動裝置內與蜂巢基礎設施通訊之系統單晶片(System of a Chip， SoC)而編寫韌體的組織。無線網路提供商，亦稱為行動網路業者(mobile network operators, MNOs)，經營蜂巢 LTE 的空中介面、回程線路(backhaul)、核心網路及使用者行動裝置的部分，包括通用積體電路卡(Universal Integrated Circuit Card, UICC)的硬體式憑證與用戶全球識別卡(Universal Subscriber Identity Module， USIM)的應用軟體。本文件中有對這些所有組織的完整描述。

除另有說明外，本文件範圍不包括行動裝置硬體、行動裝置作業系統(例如 Android、Blackberry、iOS、Windows 手機)，以及第三方行動裝置應用程式。本文件分析對象不包括第三代合作夥伴計劃(3GPP)網路(例如 WiFi、WiMAX、3GPP2)、諸如裝置與裝置間之蜂巢通訊和蜂巢物聯網(internet of things， IoT)等的現有 3GPP 特徵，以及空中下載(over-the-air， OTA)管理更新至蜂巢平台、和網路支援服務(例如網域名稱服務 Domain Name Services， DNS)、網路時間協定(Network Time Protocol， NTP);也沒有敘述蜂巢網路供應鏈的相關問題。最後，IP 多媒體子系統(IP Multimedia Subsystem， IMS)，一個提供像是 LTE 語音(Voice over LTE， VoLTD)服務之現代化平台，也不包括在本文件中。

1.2 文件架構

本文件的其他內容分為以下各主要部分:

- 第 2 節為 LTE 標準與技術的概述，
- 第 3 節為 LTE 架構的詳細說明，
- 第 4 節指出 LTE 網路的威脅，

- 第 5 節提供緩解措施和其他方法來加強 LTE 安全，以及
- 第 6 節包含結論與未來的研究。

本文件亦包含附錄的佐證資料:

- 附錄 A 為本出版品中縮略語和首字母縮寫詞的定義，以及
- 附錄 B 則是制定本文件的參考文件列表。

1.3 文件常用語

本文件主要使用 LTE／演進封包系統(Evolved Packet System， EPS)的術語。因此，為釐清其涵義，已熟悉非 LTE 系統之蜂巢概念和術語的人士，可能需要參照附錄的縮略語和首字母縮寫詞。

- 所謂「蜂巢」與「蜂窩」使用時可互相置換。
- 所謂「基地台」泛指與行動裝置通訊蜂巢塔的標準通用術語，常用於討論 2G、3G 與 4G 系統交互作用時。每一套標準針對基地台使用一特定稱呼，而 LTE 採用演進的節點 B(evolved Node B)，它可以簡稱為 eNodeB 或 eNB。本文件通常使用 eNodeB 這個縮寫，但是引用標準或特定之加密金鑰時，則使用 eNB 這個縮寫。
- 所謂「行動裝置」係指使用者設備(UE)的標準泛稱術語。
- LTE 標準大量使用演進封包系統(EPS)這個名詞，而它在本文件中可以與「LTE」這個名詞互相置換。
- LTE 標準大量使用演進封包核心(Evolved Packet Core, EPC)這個名詞，而它在本文件中可以與「核心」這個名詞互相置換。

2 LTE 技術之概述

蜂巢網路是由覆蓋無線電設備之蜂巢站組成，含有分佈式覆蓋區域的無線網路。蜂巢站(或稱基地台)通常由無線電信業者、網際網路服務提供者、或可能由政府機構擁有和經營。無線電信業務或行動網路業者(mobile network operator， MNO)為終端用戶提供服務，可能本身擁有蜂巢站，也可能付費以利用蜂巢基礎設備-例如行動虛擬網路業者(mobile virtual network operator， MVNO)。行動網路業者將蜂巢無線電設備分配在大範圍的地理區域上，並且將它們連接回通常是自己擁有與經營的後端核心網路。在蜂巢服務接收不良的區域(例如建築物內部)，行動網路業者可能會直接提供終端用戶信號增強器或小型基地台以便操作。

在使用 LTE 之前，蜂巢系統是在傳統有線電話系統後塑造的，而傳統的有線電話系統為打電話的用戶提供一個專用電路，以確保達到最低程度的服務保證。與過去電路交換的蜂巢網路相比較下，LTE 網路利用封包交換。LTE 網路在終端用戶的行動裝置與數據網路上的 IP 服務之間，提供始終如一的網際網路協定(Internet Protocol, IP)連接，同時在基地台間到的移動過程中仍然保持連接(例如行動力 Mobility)。

LTE 是第三代合作夥伴計劃(3GPP)定義之行動寬頻通訊標準，而 3GPP 是一個全球性標準的開發組織。隨著對高速行動網路的需要持續增長，LTE 網路之實施正在全球展開，而其安裝量亦不斷增加。於技術規範(Technical Specification, TS)22.278 [9]中，3GPP 為 LTE 系統列出許多需要達到的高階目標，包括:

- 用更少等待時間提供更高的數據速度
- 為先前的蜂巢系統建立安全基礎
- 支援目前和下一代蜂巢系統與其他數據網路之間的互相操作
- 在維持現有服務品質的同時，亦能提高系統性能
- 維持與傳統系統之間的互相操作

以下部分解釋了 LTE 技術的基本概念與架構、網路協定及 3GPP 安全的演進。

2.1 3GPP 標準的演進

全球行動通訊系統(Global System for Mobile Communications, GSM)是一種 2G 電路交換的蜂巢技術。雖然全球行動通訊系統(GSM)最初並非由 3GPP 定義，但是 3GPP 已經掌握了這些標準並加以維護、加強，以作為未來開發的基礎。3GPP 對全球行動通訊系統(GSM)的第一次擴展即為整合封包無線傳輸服務(General Packet Radio Service, GPRS)，稱為 2.5G 技術。整合封包無線傳輸服務(GPRS)是通過蜂巢網路發送非語音數據的第一種方法，緊接著是全球行動通訊系統(GSM)增強數據率演進(Enhanced Data Rates for GSM Evolution, EDGE)，有時也稱為 2.75G 技術。

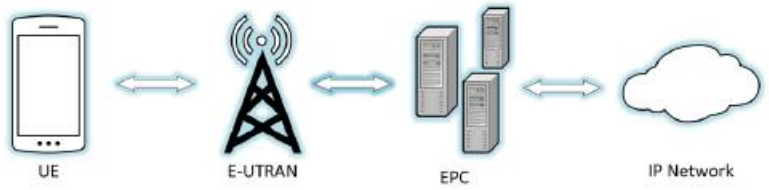
3GPP 定義的第一個語音標準為通用行動通訊系統(Universal Mobile Telecommunications System, UMTS)，這是 3G 電路交換技術。UMTS 開發後不久，3GPP 封包交換技術即演進出多個變異，統稱為高速封包存取(High Speed Packet Access, HSPA)，雖然某些行動裝置可能將高速封包存取

(HSPA)連接視為 4G，但應該稱它是 3.5G。創造 HSPA 旨在增加連接上行線路和下行線路的數據總處理量。

LTE 需要支援更高數據率和品質服務不斷成長的需求，亦需要能夠快速地支援新的技術發展，而 LTE 封包交換基礎讓技術的升級／更新以及降低整個網路的複雜性都變得更加容易。為實現這些目標，3GPP 引進 LTE 第 8 版(此版本已於 2008 年 12 月 11 日凍結)。之後，所有 LTE 版本都建立於此一基準之上。3GPP 定義了專用於 LTE 技術要求的一系列規範，即所謂的 36 系列。3GPP 還定義了一系列安全規範，即所謂的 33 系列。每一 3GPP 系列皆包含技術報告(TR)和技術規範(TS)文件。技術報告內會探討對 LTE 功能的最新要求，並且提出和評估可能的解決方案。一旦對該功能單一解決方案達成協議，即將其標準化於技術規範中。本文件係以 3GPP 公布的第 12 版 which was frozen on March 13, 2015 [1].

2.2 LTE 概念

以下部分敘述本文件使用與討論到的重要高階概念與 LTE 網路元件。需要了解的基本概念之一，即為整體的網路架構：行動裝置(UEs)透過無線電信號連接到基地台，構成 E-UTRAN，而基地台發送和接收往來核心網路之間的 IP 封包。核心網路有大量出入連接節點，包括網際網路和其他蜂巢網路的連接。圖 1 用以說明這個高階概念。



(圖 1-高階蜂巢網路)

與早期蜂巢網路技術(即語音利用電路交換技術、數據利用封包交換技術組成的混合網路)相比，LTE 僅利用封包交換、以 IP 為基礎的技術。在 LTE 架構中，語音透過數據連接使用的通訊協定之在網路中傳輸，即 LTE 語音(VoLTE)，它類似與網際網路協定電話(Voice Over IP, VoIP)。在美國，LTE 語音(VoLTE)正為行動網路業者所廣泛採用部署中。行動網路業者仍然利用傳統電路交換的蜂巢網路，來處理語音撥打和簡訊服務(short message service, SMS)，即電路交換回退(circuit switched fallback, CSFB)機制。

2.2.1 行動裝置

行動裝置為蜂巢網路中的主要終點，透過無線電信號與基地台互相發送和接送資訊。行動裝置由兩個不同的系統所組成：與使用者互動之通用行動裝置作業系統(例如 Android、iOS、Windows 手機)，以及用來存取蜂巢網路之電話子系統。電話子系統包含一個特殊的應用處理器，稱為基頻處理器，它有自己的作業系統用來與蜂巢網路互動，通常由蜂巢系統單晶片(SoC)製造商所開發。

LTE 標準將行動裝置視為使用者設備，其可以是具有行動作業系統的終端、基頻處理器、與 LTE

無線電、以及內含安全標準資訊用於取得網路存取的抽取式硬體憑證。這種抽取式硬體憑證通常被稱為 SIM 卡，但 LTE 標準使用「通用積體電路卡(Universal Integrated Circuit Card, UICC)」這個名詞。通用積體電路卡基本上是一個智能卡，它用來運行被稱為全球用戶識別卡(Universal Subscriber Identity Module, USIM)的 Java 應用程式。全球用戶識別卡與蜂巢無線電和之後的行動網路相連接。通用積體電路卡則含有加密金鑰(提供給使用者前由行動網路業者持有)。

蜂巢網路使用兩種不同的識別碼:國際行動用戶識別碼(International Mobile Subscriber Identity，IMSI)和國際行動裝置識別碼(International Mobile Equipment Identifier, IMEI)。國際行動用戶識別碼是營運商用來長期識別用戶身份，而國際行動裝置識別碼則是用來識別網路上的特定行動裝置，它儲存在行動裝置的內部快閃記憶體上，但也可以儲存在通用積體電路卡上。

以下是使用者設備內含元件的綜合列表:

- **使用者設備(UE)**:蜂巢裝置(手機、平板電腦、LTE 數據機等)含有以下元件:
  - **行動設備(ME)**:無硬體憑證之行動裝置終端。
  - **通用積體電路卡(UICC)**:儲存個人資訊、加密金鑰，並負責運行 Java 應用程式以存取網路之的智能卡。這張智能卡應插入行動設備中。
  - **國際行動設備識別碼(IMEI)**:用在蜂巢網路中識別行動裝置之終端識別碼。
  - **國際行動用戶識別碼(IMSI)**:用在蜂巢網路中識別用戶的用戶身份。

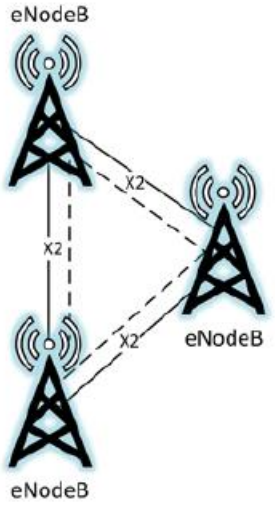
除國際行動設備識別碼和國際行動用戶識別碼外，行動網路業者也可以利用其他的 LTE 識別碼，包括全球唯一臨時識別碼(Globally Unique Temporary Identity, GUTI)與暫時行動用戶識別碼(Temporary Mobile Subscriber Identity,TMSI)。全球唯一臨時識別碼可以為網路識別使用者設備，而不需要提供長期身份(即國際行動用戶識別碼)。後面將會討論用明文發送國際行動用識別碼的安全影響。基於不同原因使用不同的識別碼，例如為了限制永久身份被暴露、減少裝置存取網路多個服務時被追蹤。

2.2.2 演進的通用陸面無線存取網路(E-UTRAN)

無線存取網路(Radio Access Network，RAN)已隨著時間演進成為演進的通用陸面無線存取網路(Evolved Universal Terrestrial Radio Access Network, E-UTRAN)。使用者設備連接 E-UTRAN 以便將數據發送到核心網路。E-UTRAN 是一個由基地台組成的網狀網路。基地台或演進的節點 B 調制並解調無線電信號以便與使用者設備通訊。接著，eNodeB 作為中繼點創造並發送 IP 封包往來核心網路。蜂巢網路的設計是:當已連接的使用者設備改變位置時，把對 E-UTRAN 中的一個無線電存取裝置的連接傳遞到下一個。這種無縫交遞能力使得裝置能持續連接，把中斷減到最少，從而在蜂巢網路中提供所謂的「行動力」。eNodeB 利用 X2 介面相互通訊，主要發送控制信號以允許 LTE 網路通訊，進而實現使用者設備的行動力。在切換期間，運行中的 eNodeB 必須將所有 UE context[13]、蜂巢參數和有關 UE 的其他資訊移轉給接手的 eNodeB。

[13] UE Context 係一數據結構，含有使用者設備與使用者識別碼、安全參數和使用者設備的行動現況。

LTE 利用指名介面(named interface)的概念來輕鬆識別兩個端點間的通訊連接。LTE 技術中的指名介面(例如 X2 介面)係指兩個端點間的邏輯連接，而在本例中即為兩個 eNodeB。LTE 中的指名介面負責發送與接收特定訊息和數據。這在物理上可以透過各種方式加以實現，而同一物理連接亦可以共享多個指名介面。這個物理連接可以是諸如光纖、乙太網、微波、衛星連線等的各種網路技術。



(圖 2 -E-UTRAN)

與物理蜂巢塔和無線電設備組成的典型基地台不同，基地台可以有不同的外觀尺寸。小型蜂巢有較小的外觀尺寸、以較低功率傳輸、能擴展網路覆蓋範圍，並且增加網路最終容量。

以上資訊整合列表如下:

- **演進的通用陸面無線存取網路(E-UTRAN)**：提供無線行動力的所有元件：
  - **演進的節點 B(eNodeB 或 eNB)**：演進的節點 B，俗稱為基地台。
  - **小型蜂巢**：與典型的 eNodeB 相比，具有較小範圍和較小容量的低功率基地台，例如家用 eNodeB(HeNB)、Donor eNodeBs(DeNB)和中繼節點(Relay Nodes, RN)。

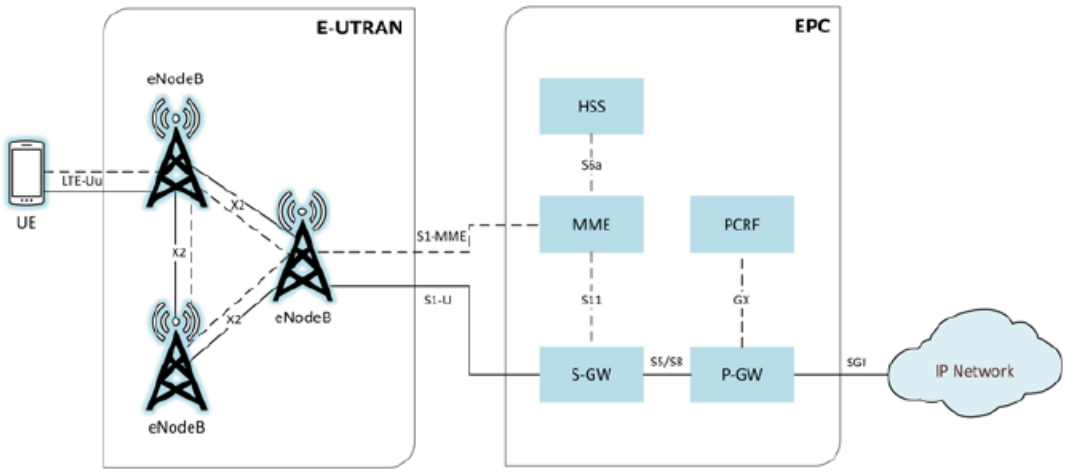
2.2.3 演進的封包核心

如圖 3 所示，演進的封包核心(EPC)是 LTE 網路用來安排路線和計算的大腦。使用者設備(UE)透過基地台收到行動管理實體(Mobility Management Entity, MME)產生的控制信號，而行動管理實體(MME)執行各種功能，包括管理和儲存 UE Context、創建臨時識別碼、呼叫、控制認證功能和在服務閘道(Serving Gateway, S-GW)與封包數據網路(PDN)閘道(P-GW)間作出選擇。使用者流量會透過行動管理實體(MME)發送。服務閘道(S-GW)將使用者設備(UE)固定，以便在 eNodeB 之間切換，以及安排封包數據網路閘道(P-GW)與 E-UTRAN 間的資訊路線。封包數據網路閘道(P-GW)是使用者設備(UE)預設的路由器，在 3GPP 與非 3GPP 服務間進行傳輸，分配 IP 位置給 UE 並提供封包數據網路(PDN)的存取。

下列整合與定義演進封包核心(EPC)中的元件：

- **演進的封包核心(EPC)**：LTE 網路用來安排路線和計算的大腦。
  - **行動管理實體(MME)**：不與使用者流量互動之主要網路信號節點。有各種功能，包括管理／儲存 UE Contexts、創建臨時識別碼(IDs)、發送呼叫、控制認證功能和在服務閘道(S-GW)與封包數據網路閘道(P-GW)間作選擇。
  - **服務閘道(S-GW)**：傳輸使用數據、為在 eNodeB 間切換而固定使用者設備(UEs)、以及安排封包數據網路閘道(P-GW)與 E-UTRAN 間的資訊路線。
  - **封包數據網路閘道(P-GW)**：分配 IP 位置、安排封包路線及與非 3GPP 網路互連。
  - **家庭用戶伺服器(Home Subscriber Server, HSS)**：存有用戶數據及秘密金鑰 K 的主資料庫。
  - **認證中心(Authentication Center, AuC)**：在家庭用戶伺服器(HSS)內，將長期身份映射到預設之加密金鑰、在認證過程中進行加密計算。
  - **策略與計費規則功能(Policy and Charging Rules Function, PCRF)**：與服務品質(QoS)、計費、及存取網路資源有關的規則與策略，經分發到封包數據網路閘道後，交由策略與計費規則功能(PCRF)執行。
  - **IP 多媒體子系統(IMS)**：通往公共交換電話網路(PSTN)、多媒體服務(例如 VoLTE、即時訊息、視訊)、及呼叫多媒體服務的閘道。
  - **回程線路**：無線網路與核心網路間之連接。這個連接可以是光纖、衛星連接、乙太網路線、微波等等。
  - **封包數據網路(PDN)**：任何外部的 IP 網路(例如網際網路)。使用者設備(UEs)得於任何時間點連接到一個或多個封包數據網路(PDNs)。
  - **存取點名稱(Access Point Name, APN)**：作為封包數據網路(PDN)的識別碼，同時也是演進封包核心(EPC)與封包數據網路(PDN)之間的閘道。使用者設備(UE)必須為連接的每一個封包數據網路(PDN)指定存取點名稱(APN)。

圖 3 描述了以上介紹的元件，並顯示這些網路元件之間的流量。藉由參考本圖，可將 LTE 網路基本元件間之互相連接關係視覺化，並且得描述尚未討論到的概念。圖中的實線代表使用者流量，而虛線則代表控制信號流。



(圖 3 – LTE 網路架構)

2.2.4 LTE 網路拓撲

LTE 網路至少包含一個使用者設備、一組 eNodeBs、組成 E-UTRAN 之其他無線存取設備，以及受行動網路業者控制之寬頻核心網路。E-UTRAN 透過所謂的回程線路與演進封包核心(EPC)相互連接。從安全觀點，最重要的是必須注意到 E-UTRAN 和演進的封包核心可能處於完全不同的地理位置。因此，連接兩者的介面可能會或也可能不會完全涵蓋在行動網路業者(MNO)的私有網域內。本節將會論及各種運作網路(operational network)的拓撲，像是 LTE 網路之固定和部署。

固定式 LTE 網路是利用小型蜂巢站提供大地理範圍覆蓋的典型蜂巢網路實施例。在這種架構下，核心網路元件通常置於不同位置。內含 eNodeBs 的蜂巢站透過回程線路與演進封包核心(EPC)連接，而回程線路之連接可以藉助多種技術(例如微波、衛星、光纖等)。行動網路業者(MNO)常會部署這類型的網路架構。雖然 LTE 網路為了 有效運行需要相同的功能性元件，但這些元件的數量與位置則完全取決於行動網路業者(MNO)的網路設計。有可能網路業者採用數個提供主要功能的演進封包核心(EPC)，並讓這些元件負載平衡，以提供更高的可用性。

固定式 LTE 網路示例之一是利用分散各處且含有 eNodeBs 的許多蜂巢站，這些蜂巢站全部連接回一個或多個演進封包核心，以便為大範圍區域提供網路覆蓋。多個 eNodeBs 透過 X2 介面相互連接，該 X2 介面負責在使用者設備(UE)移動時從一個 eNodeB 到下一個 eNodeB 做區段切換。最終，E-UTRAN 的元件透過回程線路或 S1 介面與演進的封包核心(EPC)相互連接和通訊。為提高可用性和可靠性，在各 E-UTRAN 與各演進的封包核心(EPC)之間可能存在多對多的關係。

與固定式 LTE 網路相反，部署式 LTE 網路是一種能被部署在無 LTE 覆蓋或覆蓋被中斷的區域的簡易型網路。部署式網路能夠移動並包裝成不同的外觀(例如安裝在車輛、拖車、背包上)。這些類型的 LTE 架構可用來建立自足網路、或連接到既有 LTE 或其他網路。部署式網路使用的硬體通常更為小巧，並且僅能處理固定式 LTE 網路一小部分的總處理量和容量。

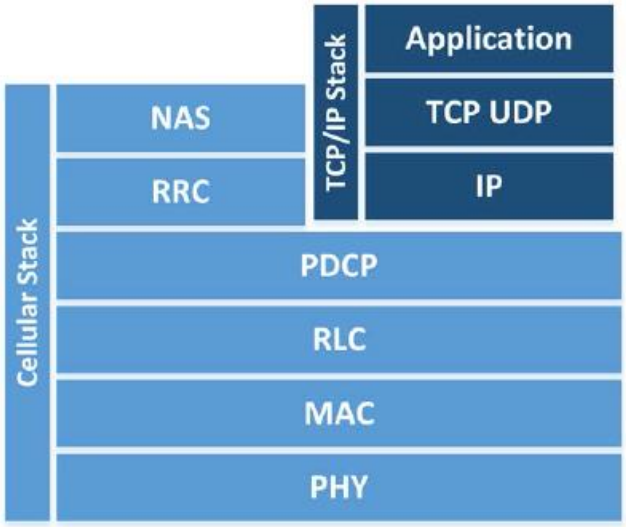
車載基地台(Cell on Wheels 又稱 COW)是商用部署式 LTE 網路的一個示例。這些 COW 是包含 LTE 網路所有元素的環境，並且安裝在拖車、或是在某些情況下安裝在車輛。COW 通常仍然需

要接回核心網路。這些類型的部署式網路可用於對既有網路需求增加時(例如大型運動賽事)提供額外的容量，也可用於沒有網路覆蓋的區域，像是在自然災害現場為急救人員提供通訊方式。部署式網路可在市場上取得，也可向網路設備供應商購買。

2.3 LTE 網路協定

以下協定用於透過空中介面的通訊(使用者設備 UE 與 eNodeB 之間的無線電連接)。此一協定套組稱空中介面的協定堆疊(通常分為三層)。從邏輯上而言，這些協定為在其上運作的所有 TCP／IP 流量奠定了基礎。這些協定有：

- 無線資源控制模組(Radio Resource Control, RRC)在第三層運作；
- 封包數據匯聚通訊協定(Packet Data Convergence Protocol, PDCP)在第二層運作；
- 無線連接控制模組(Radio Link Control, RLC)在第二層運作；
- 媒體存取控制模組(Medium Access Control, MAC)在第二層運作；以及
- 實體存取(Physical Access, PHY)在第一層運作。



(圖 4－LTE 協議堆疊)

蜂巢堆疊空中介面的每一協定負責執行一系列的功能，並在兩個邏輯平面(即使用者平面或控制平面) 之一上運作。使用者平面是負責承載透過網路發送的使用者數據(例如透過語音通訊、簡訊服務 SMS、應用程式流量發送)，而控制平面是則是負責承載連接使用者設備(UE)所需的所有信號通訊。為了使技術演進，路徑稍微有點分歧，3GPP 規範將蜂巢協定分為兩層：非存取層(Non-Access Stratum, NAS)與存取層(Access Stratum, AS)。存取層(AS)是使用者設備(UE)與 eNodeB 之間透過射頻(Radio Frequency, RF)通道產生的所有通訊，而非存取層(NAS)則由使用者設備(UE)與行動管理實體(MME)間的所有非無線信號流量組成。使用者 TCP／IP 及其他應用程式的所有流量皆透過使用者平面傳輸。建立、維持及終止使用者設備(UE)與行動管理實體(MME)之間空中介面的控制平面，則負責主管無線資源控制模組(RRC)協議。封包數據匯聚通訊協定(PDCP)、無線連接控制模

組(RLC)、媒體存取控制模組(MAC)和實體存取(PHY)層構成空中介面的基礎，並且是用戶及控制平面的一部分。上述控制及用戶平面在這些協議上運行。

無線資源控制模組(RRC)執行各種控制任務，例如播送系統資訊、建立與 eNodeB 的連接、呼叫、執行認證、建立承載、以及傳送非存取層(NAS)訊息。封包數據匯聚通訊協議(PDCP)執行標頭壓縮、封包重新排序、重新傳輸、以及存取層安全(含完整性與機密性保護)。如同技術規範(TS)33.401 規定，封包數據匯聚通訊協議(PDCP)層必須出現所有的加密保護(含機密性與完整性)[5]。無線連接控制模且(RLC)準備將透過空中介面傳送的封包，並將數據傳送到媒體存取控制模組(MAC)層。它也執行封包重新排序和重新傳輸之操作。媒體存取控制模組(MAC)執行多工技術、通道調度、服務品質(QoS)活動、與建立到實體存取(PHY)層數據之邏輯定址。實體存取(PHY)層提供錯誤管理、信號處理、與將數據調制進出空中介面。

E-UTRAN 與演進的封包核心(EPC)之間的元件介面有自己的通訊協定，故未在此列出。

2.4 LTE 承載

在 LTE 網路中，傳輸使用者流量之前，必須建立端點之間的連接；這些連接稱為承載。承載是兩個端點之間的連接，它包含與該連接之流量等級、比特率、發送順序、可靠度、優先順序、及服務品質相關的特定資訊。承載可以跨越數個介面。應注意的是，承載有兩個主要類型：信令無線電承載與傳輸承載。信令無線電承載建立在控制層，以便於使用者設備(UE)與 eNodeB 間、與 eNodeB 與行動管理實體(MME)間的信令通訊。傳輸承載則沿著使用者平面的路徑建立，以便於將使用者數據傳輸到其指定端點。

必須建立以下三種專用於傳輸無線資源控制模組(RRC)與非存取層(NAS)訊息的信令無線電承載[30]：

- **信令無線電承載 0(SRB0)**：負責建立使用者設備(UE)與 eNodeB 間之無線資源控制模組(RRC)連接。
- **信令無線電承載 1(SRB1)**：負責交換安全資訊、測量報告、回退參數和切換資訊。
- **信令無線電承載 2(SRB2)**：負責傳輸測量資訊和非存取層(NAS)訊息。SRB2 總是在建立 SRB1 與啟動安全措施後才設定。

一旦建立各個信令無線電承載(SRBs)後，使用者設備(UE)即透過特定 eNodeB 連接到核心網路，並準備好發送和接收使用者數據。在整個 LTE 網路中，使用者流量必須經過數個連接點(從使用者設備 UE 到 eNodeB、從 eNodeB 到服務閘道 S-GW 等等)，因此，為了讓使用者流量能夠穿梭在 LTE 網路中，即必須建立數個承載。為了讓使用者設備具備完整的網路連接性，必須按照以下順序建立這些承載[29]：

- **數據無線承載(Data Radio Bearer, DRB)**：建立在使用者設備(UE)與 eNodeB 間的空中介面上(亦稱為 Uu 介面)。它可在使用者設備(UE)與 eNodeB 間直接通訊使用者數據。
- **S1 承載**：建立在 S1-U 介面的 eNodeB 與相關服務閘道(S-GW)之間。

- **E-UTRAN 無線存取承載(E-UTRAN Radio Access Bearer, E-RAB)**：數據無線承載(DRB)與 S1 承載的組合，用以建立使用者設備(UE)與服務閘道(S-GW)的連接。
- **S5／S8 承載**：建立在使用者數據平面的服務閘道(S-GW)與相關封包數據網路閘道(P-GW)之間。
- **EPS 承載**：E-RAB 與 S5／S8 承載的組合，用以提供從使用者設備(UE)到相關封包數據網路閘道(P-GW)之間的使用者平面連接。
- **外部承載**：建立在封包數據網路閘道(P-GW)與使用者設備(UE)必須存取之演進封包核心(EPC)外部資源之間，例如與網際網路之連接。
- **端到端服務**：演進封包系統(EPS)承載與外部承載的組合，用以提供從使用者設備(UE)到演進封包核心(EPC)外部相關資源之間的使用者平面存取。

於使用者設備(UE)附著的整個過程中必定需要建立承載。

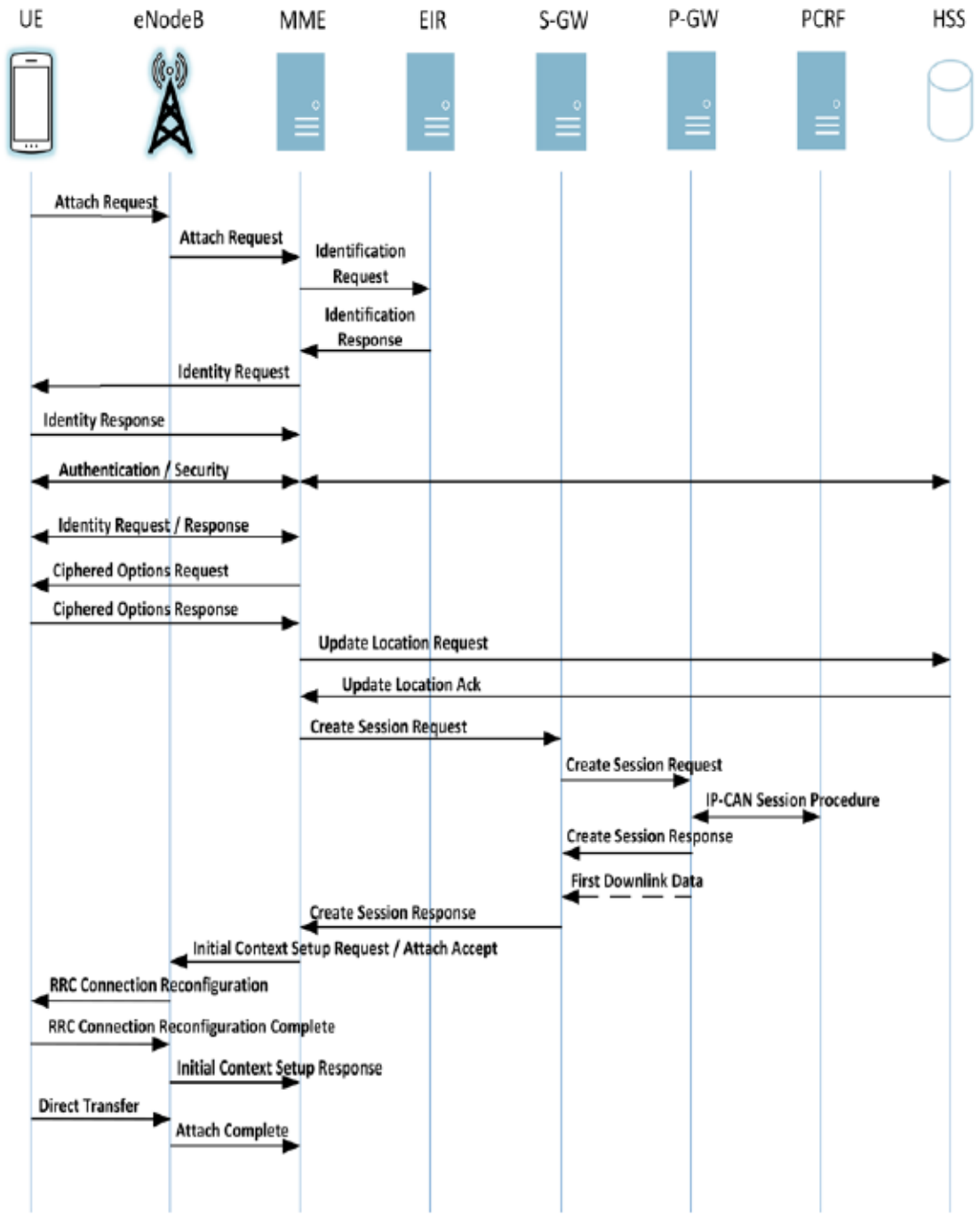
2.5 使用者設備(UE)附著

在使用者設備(UE)能夠加入 LTE 網路並存取語音和數據服務之前，必須經過向 LTE 網路標識自己的一個程序。這個程序稱為*初始附著程序*，其負責處理使用者設備(UE)到 LTE 演進封包核心(EPC)的識別資訊通訊，以確保使用者設備(UE)能存取該網路。若該過程成功後，將提供使用者設備(UE)預設連接，而該連接裡含有 LTE 網路適用和執行的計費規則。附著過程定義於技術規範(TS)23.401，並以圖 5 說明如下 *—用於存取 E-UTRAN 之整合封包無線傳輸服務(General Packet Radio Service, GPRS)加強*[2]。

初始附著程序始於使用者設備(UE)透過 eNodeB 對行動管理實體(MME)的附著請求。這項請求包含國際行動用戶識別碼(IMSI)、追蹤資訊、加密參數、非存取層(NAS)序列號、與有關使用者設備(UE)的其他資訊。附著請求以非存取層(NAS)訊息的方式發送，接著 eNodeB 將附著請求連同該使用者設備(UE)所屬的蜂巢資訊，一併傳送給行動管理實體(MME)。對於使用者設備(UE)接連的每個封包數據網路(PDN)，皆建立一個演進封包系統(EPS)的預設承載，始得在網路連接過程中，使用者與使用者設備(UE)有不中斷(always-on)的 IP 連接。

假使策略與計費規則功能(PCRF)對利用演進封包系統(EPS)預設承載的用戶或裝置有特定之策略與計費控制規則，可以將該規則事先定義於封包數據網路閘道(P-GW)，並且於封包數據網路閘道(P-GW)本身的附著時開啟。於附著時，得啟動一個或數個專用承載建立程序，以便為特定的使用者設備(UE)建立演進封包系統(EPS)承載。同樣的，於附著程序中，使用者設備(UE)也可以請求分配 IP 位置。行動管理實體(MME)從使用者設備(UE)取得國際行動裝置識別碼(IMEI)後，搭配裝置識別碼紀錄器(Equipment Identity Register)作檢查，藉以驗證該使用者設備(UE)之國際行動裝置識別碼(IMEI)是否在黑名單上。接著，行動管理實體(MME)將國際行動裝置識別碼(IMEI)的軟體版本傳遞給家庭用戶伺服器(HSS)與封包數據網路閘道(P-GW)。一旦使用者設備(UE)通過了初始附著程序，行動管理實體(MME)為其指定一組全球唯一臨時識別碼(GUTI)。全球唯一臨時識別碼(GUTI)同時儲存於使用者設備(UE)與行動管理實體(MME)中，在該使用者設備(UE)未

來的附著程序中，可能可以取代國際行動用戶識別碼(IMSI)而使用。



(圖 5－初始附著)

一旦成功地完成附著程序，將透過第 3.3 節定義之認證與金鑰協商(Authentication and Key Agreement, AKA)協定認證使用者設備(UE)。

3 LTE 安全架構

本節更詳細地敘述 LTE 提供之認證、加密保護機制、硬體保密機制與網路保護。在[9]有關於 LTE 安全的高階討論，而[7]則記錄對 3GPP 作出安全決策和假設之基本原理的理解。大部分的技術安全要求都在 LTE 主要的安全規範－3GPP 技術規範(TS) 33.401－演進封包系統(EPS)安全架構[5]之中。

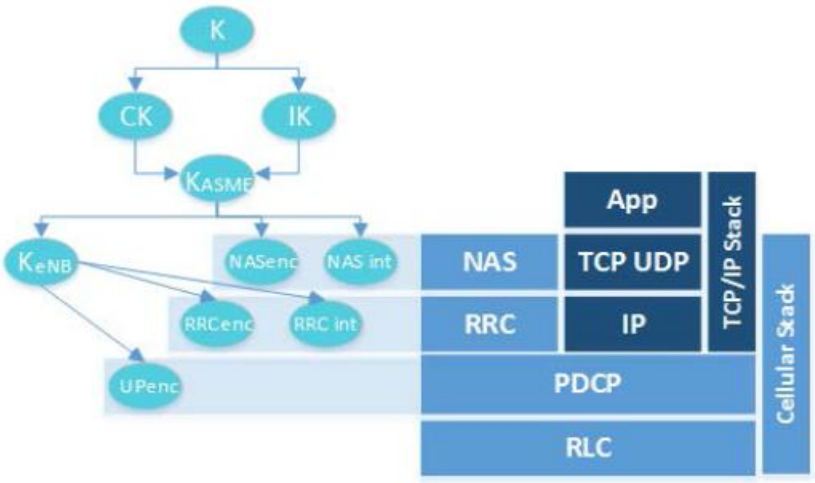
3.1 加密概述

較舊的 2G 蜂巢系統中，其用來保護空中介面與執行用戶認證功能的加密性演算法並未對外公開。與我們討論相關的全球行動通訊系統(GSM)的演算法家族有 A3、A5 與 A8。A3 提供用戶認證、A5 提供空中介面保密、而 A8 則與 A3 相關，提供用戶認證的功能，但是存在 SIM 卡 內。通用行動通訊系統(UMTS)引進了商用蜂巢系統使用的第一個對外公開的加密性演算法。通用行動通訊系統(UMTS)使用通用行動通訊系統加密性演算法(UEA)和通用行動通訊系統完整性演算法(UIA)作為兩大分類的術語。UEA1 是一種 128 位元的區段加密法，稱為 KASUMI，它與日本加密法 MISTY 有關。 UIA1 是訊息認證代碼 (MAC)，也是以 KASUMI 為基礎。UEA2 是一種與 SNOW 3G 有關的資料流加密法，而 UIA2 用相同的演算法計算訊息認證代碼(MAC)[27]。LTE 係建立在從部署 2G 與 3G 加密演算法學到的經驗之上。

LTE 引進一套新的加密演算法，以及與全球行動通訊系統(GSM)和通用行動通訊系統(UMTS)明顯不同的金鑰結構。有三套機密性與完整性的加密演算被稱為演進封包系統的加密演算法(EEA)和演進封包系統的完整性演算法(EIA)：EEA1 和 EIA1 是以 SNOW 3G 為基礎，非常類似通用行動通訊系統(UMTS)使用的演算法；EEA2 和 EIA2 是以進階加密標準(Advanced Encryption Standard, AES)為基礎，而 EEA2 在 CTR 模式中由進階加密標準(AES)定義，EIA2 則由 AES-CMAC 定義(即以訊息認證代碼為基礎的加密法)；EEA3 與 EIA3 皆以中國演算法 ZUC 為基礎[5]。在 LTE 引進這些新演算法的同時，網路實務普遍仍為了傳統裝置及蜂巢部署的向後相容而使用舊的演算法。

大部分的 LTE 金鑰長度為 256 個位元，但目前某些實務中只使用 128 個最低有效位元。本規範將使金鑰的系統範圍從 128 位元升級到 256 位元[14]。在 LTE 中，控制與使用者平面可能使用不同的演算法和金鑰大小。圖 6 說明各種金鑰及其於相關協定中的利用。

[14] 3GPP 33.401 第 4.1 節 a [7]



(圖 6－保護網路堆疊的金鑰)

下表敘述各種 LTE 金鑰大小，以及源自相同金鑰分級架構的其他金鑰[5][15]。

Key	Name	Length (bits)	Derived in Part From
K	Master Key	128	N/A: Pre-shared root key
IK	Integrity Key	128	K
CK	Cipher Key	128	K
KASME	MME Base Key	256	CK, IK
NH	Next Hop	256	KASME
KeNB*	eNB Handover Key	256	KASME, KeNB
KeNB	eNB Base Key	256	KASME, NH
KNASint	NAS Integrity Key	128	KASME
KNASenc	NAS Confidentiality Key	128	KASME
RRCenc	RRC Confidentiality Key	128	KeNB, NH
RRCint	RRC Integrity Key	128	KeNB, NH
UPenc	UP Confidentiality Key	128	KeNB, NH

(表 1－加密金鑰的要摘要資訊)

3.2 硬體的安全

通用積體電路卡(UICC)是用於行動裝置模組的下一代用戶識別卡(Subscriber Identity Module, SIM)，

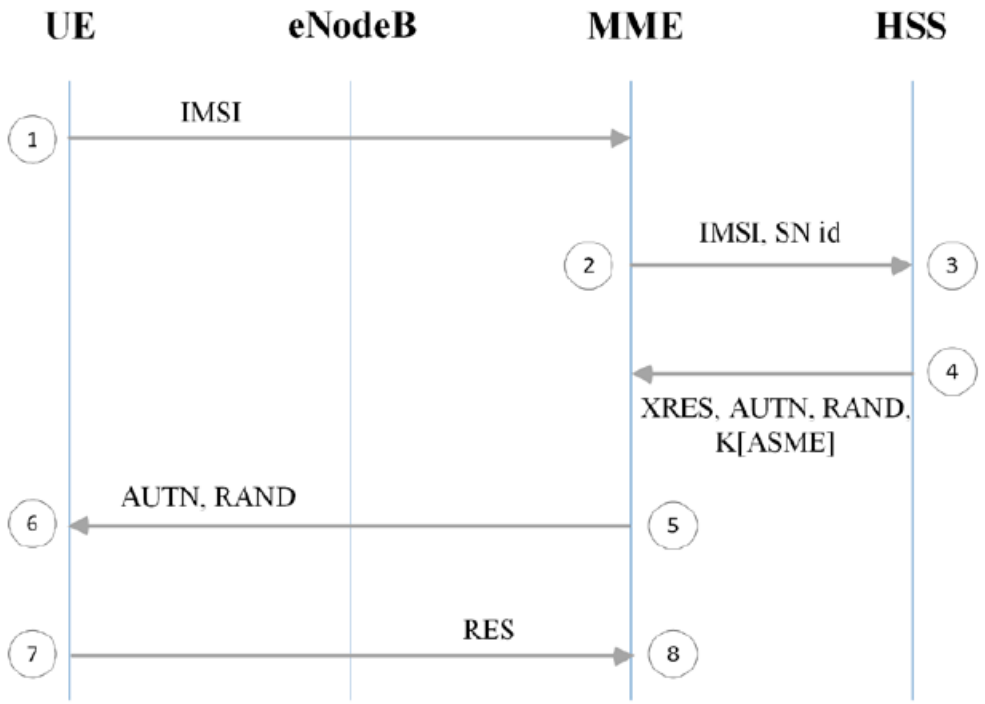
15 3GPP TS 33.401 圖 6.2-2

也是 LTE 安全架構的基礎。通用積體電路卡(UICC)用戶全球識別卡(USIM)應用程式，而該程式執行 LTE 蜂巢網路所需的全部安全關鍵操作，像是認證和其他加密函數。通用積體電路卡(UICC)是一種防竄改的行動儲存裝置，使用者可利用它把蜂巢服務從一個蜂巢裝置移動到另一個蜂巢裝置，同時也有儲存聯絡人及其他使用者資料的功能。通用積體電路卡(UICC)內含處理器、ROM、RAM、具有網路意識，還可以運作各種功能的小型 Java 應用程式，其功能範圍從維護、更新、甚至是電玩。通用積體電路卡(UICC)亦能用於身份識別服務和近距離無線通訊(Near Field Communication, NFC)。

從安全觀點而言，通用積體電路卡(UICC)最重要的一項功能就是儲存加密金鑰與憑證。在 LTE 中，通用積體電路卡(UICC)係與預設的長期加密金鑰(稱為 *K*)是一起提供的。這個金鑰同時儲存於防竄改的通用積體電路卡(UICC)和(家庭用戶伺服器 HSS 的)核心網路中，而且永遠不會從這兩個位置移除[15]。LTE 加密結構裡的其他所有金鑰皆衍生自 *K*，並與區域主金鑰合稱為 *KASME*。通用積體電路卡(UICC)與家庭用戶伺服器(HSS)和行動管理實體(MME)合併執行諸如加密操作及用戶認證的安全功能。關於儲存 LTE 安全性內容方面，通用積體電路卡(UICC)亦扮演了重要的角色。安全性內容包含加密金鑰、使用者設備(UE)安全功能，以及附著過程產生且未來系統存取時可以再利用的其他安全參數。通用積體電路卡(UICC)亦儲存國際行動用戶識別碼(IMSI)與國際行動裝置識別碼(IMEI)，兩者皆用於支援身份識別。某些模組的行動設備作業系統執行 3GPP 技術規範(TS) 121.111[31]規定的 UICC PIN，以便在通用積體電路卡(UICC)上安裝一個 PIN。由於通用積體電路卡(UICC)可以從行動裝置上移除，再插入另一個行動裝置以提供服務，因此，通用積體電路卡(UICC)上的 PIN 可以防止別人竊取其他使用者的通用積體電路卡(UICC)，而取得未經授權的網路存取。

3.3 使用者設備認證

行動手持裝置用來認證 LTE 網路的主要 LTE 認證機制稱為認證與金鑰協商(AKA)協定。LTE 使用認證與金協商(AKA)的規定可見於 3GPP 技術規定(TS) 33.401 [5]。認證與金鑰協商(AKA)協定以加密方式證明通用積體電路卡(UICC)與行動網路業者(MNO)知悉秘密金鑰 K。從安全觀點而言，此等方式有效地認證了通用積體電路卡(UICC)，而非使用者或行動裝置。認證與金鑰協商(AKA)協定之運作和其詳細描述如下：



(圖 7)－認證與金鑰協商協定

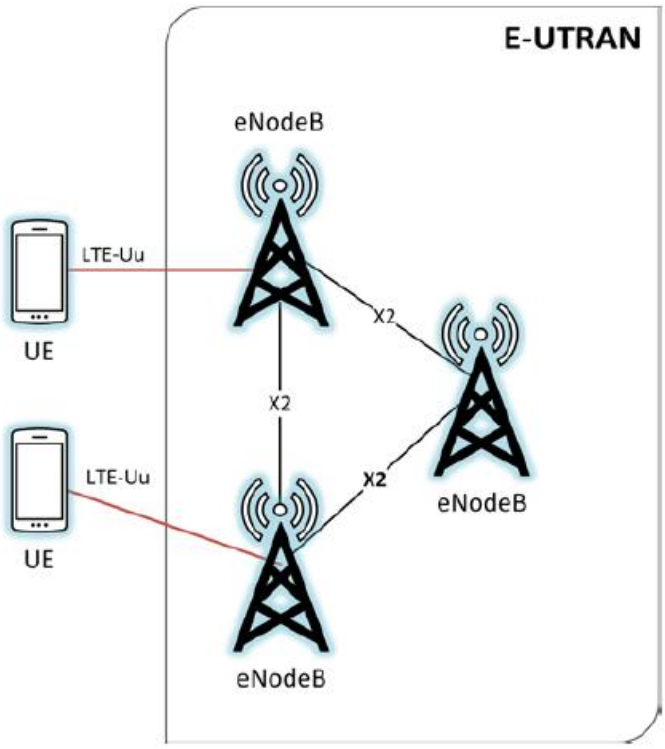
認證與金鑰協商程序發生於第 3.3 節所述之使用者設備(UE)附著過程中，並提供通用積體電路卡(UICC)與 LTE 網路之間的雙方認證。

認證與金鑰協商(AKA)從使用者設備(UE)向相關行動管理實體(MME)提供識別碼開始(圖 7 步驟 1)。這個識別碼可以是永久的，像是國際行動用戶識別碼(IMSI)，也可以是暫時的。臨時識別碼的示例，包括暫時行動用戶識別碼(TMSI)以及全球唯一臨時識別碼(GUTI)。將識別碼提供給核心網路後，行動管理實體(MME)將該識別碼連同其他加密參數和服務網路識別碼(SN iD)一併提供給家庭用戶伺服器(HSS)／認證中心(AuC)後(圖 7 步驟 2)，將利用這些數值產出一個認證向量(authentication vector, AUTN)。為了計算認證向量(AUTN)，家庭用戶伺服器(HSS)／認證中心(AuC)還需要將隨機亂數(random nonce, RAND)、秘密金鑰 K、以及序號(Sequence Number, SQN)輸入加密函數。此函數會產出兩個未來用於衍生加密金鑰的加密參數，以及預期結果(XRES)與認證憑證(認證向量 AUTN)(圖 7 步驟 3)。這個認證向量將傳回給行動管理實體(MME)儲存(圖 7 步驟 4)。此外，行動管理實體(MME)將認證向量(AUTN)與隨機亂數(RAND)傳給使用者設備(UE)，其後使用者設備(UE)再傳到用戶全球識別卡(USIM)的應用程式(圖 7 步驟 5)。用戶全球識別卡(USIM)使用與家庭用戶伺服器(HSS)／認證中心(AuC)使用的相同加密函數，傳送認證向量(AUTN)、隨機亂數(RAND)、秘密金鑰 K 及其序號(SQN)(圖 7 步驟 6)。被標示為 RES 的結果被傳回行動管理實體(MME)(圖 7 步驟 7)。若預期結果(XRES)值等同於 RES 值，即為認證成功，而允許使用者設備(UE)存取網路(圖 7 步驟 8)。

3.4 空中介面的安全

使用者設備(UE)與 eNodeB 利用通常稱為空中介面的射頻(RF)連接進行通訊，其稱為 Uu 介面。兩

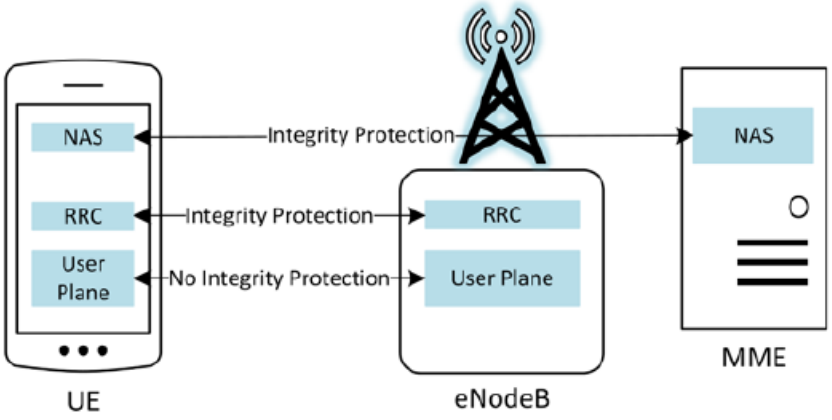
個端點將 IP 封包調制成能與空中介面通訊的射頻(RF)信號；接著，這些裝置把射頻(RF)信號解調成使用者設備(UE)和演進封包核心(EPC)皆可理解的 IP 封包。eNodeB 為這些封包安排到演進封包核心(EPC)的路線，而使用者設備(UE)則利用 IP 封包來執行某些功能。這些無線電波從使用者設備(UE)的天線傳送到空中，直到到達 eNodeB 的天線為止。這種空中通訊不一定是私人的，也就是說，在路徑內的任何物體都可以攔截這些無線電波。關於其發生於網路何處，則圖示如下：



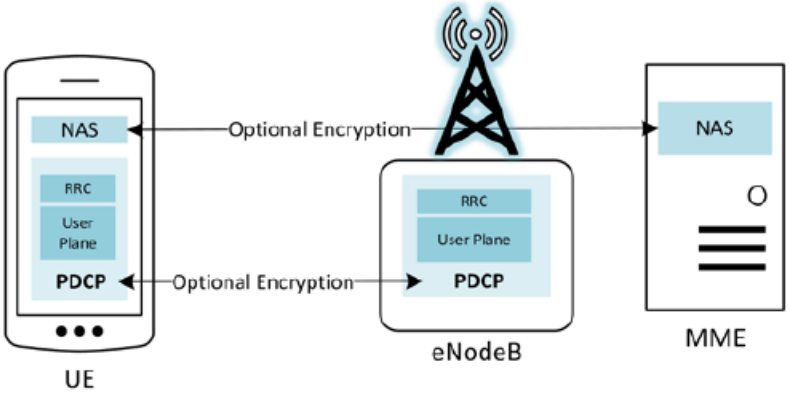
(圖 8－特別標示出的空中介面)

3GPP 技術規範 33.401 指出，非存取層(NAS)與無線資源控制模組(RRC)的控制平面訊息必須有完整性保護。3GPP 技術規範(TS) 33.401 5.1.4.1 規定：「必須為非存取層(NAS)與無線資源控制模組(RRC)信令提供完整性保護與重送保護」。這指明了，在 Uu 介面傳輸的使用者平面封包並沒有完整性保護。具體規定可見於 3GPP 技術規範(TS) 33.401 5.1.4.1 規定：「eNodeB 與使用者設備(UE)間的使用者平面封包在 Uu 介面上不受完整性保護。」

在 Uu 介面上，於使用者設備(UE)與 eNodeB 間傳輸控制平面與使用者平面封包能夠受機密性保護，但這是選擇性的。根據 3GPP 技術規定(TS) 33.401 5.1.4.1 規定：「業者可以選擇在封包數據匯聚通訊協定(PDCP)層內完成對使用者平面的機密性保護。」空中介面的機密性，為空中發送訊息提供更高一級的保證，不會被外部實體破解。LTE 在 3GPP 技術規範(TS) 22.101 [6]明定加密指標的功能；這項功能旨在讓使用者能看到網路存取加密的現況。不幸的是，這項功能並未被現代的行動電話作業系統廣泛利用。圖 9 與圖 10 有助於說明 LTE 於網路何處提供完整性和加密性。



(圖 9─完整性保護之需求)



(圖 10─機密性保護之需求)

當 LTE 網路必須協商指定連接的安全參數時，並沒有明文規定其順序。技術規定(TS) 24.301 [0]允許在無安全保護的情況下發送以下 7 種訊息：

- 請求身份識別(若請求識別參數為國際行動用戶識別碼 IMSI 時)；
- 請求認證；
- 拒絕認證；
- 拒絕附著；
- 接受卸離(非關機)；
- 拒絕更新追蹤區域；
- 拒絕服務。

需要受保護的訊息發送後，網路必須建立安全參數並協商演算法。建立參數係從發出安全模式命令(Security Mode Command, SMC)開始。安全模式命令(SMC)要求使用者設備(UE)與服務網路必須啟動加密演算法協商，以便選擇以下適用的演算法：無線資源控制模組(RRC)加密、Uu 介面上的

完整性保護、Uu 介面上的使用者平面加密，以及使用者設備(UE)和行動管理實體(MME)間之非存取層(NAS)加密與非存取層(NAS)完整性保護。從重要的一點，必須應注意網路係基於使用者設備(UE)的安全性能，以及服務網路上可用安全性能的預設清單來選擇演算法。

獨立存取層(Access Stratum, AS)與非存取層(NAS)等級的安全模式命令(SMC)程序，需要在協定堆疊的每個相關部分配置安全保護。獨立存取層的安全模式命令(AS SMC)用於配置對無線資源控制模組(RRC)與使用者平面等級的保護，而非存取層的安全模式命令(NAS SMC)則用於配置對非存取層(NAS)的保護。

一旦認證與金鑰協商(AKA)開始運作，並且發送非存取層(NAS)與選擇性的存取層安全模式命令(AS SMC)後，即產生安全性內容。安全性內容結集了用以保護非存取層(NAS)或存取層(AS)的區域金鑰及參數，但是，長期資訊(例如 K)或其他識別碼(例如國際行動裝置識別碼 IME 和國際行動用戶識別碼 IIMSI)不會儲存在安全性內容中。通常情況下，只會儲存金鑰等級源自 KASME 及以下的金鑰。使用者設備(UE)自 eNodeB 註銷後，可重覆使用先前的安全性內容，以避免認證與金鑰協商(AKA)的多餘運作(多餘運作會增加網路擁塞，且需要核心網路額外的運算能力)。

3.5 演進通用陸面無線存取網路的 安全

無線電存取網路及相關介面構成 LTE 網路中的 E-UTRAN 部分，其介於手機和行動網路業者核心網路中間的位置。切換是蜂巢網路最重要的功能之一，它讓使用者有能力移動(例如在高速公路上行駛)並且保持呼叫連接。基地台通常需要相互通訊以實現這種「行動力」，而這是透過 X2 介面達成的。3GPP 規定了許多的安全機制，用以確保相關呼叫資訊的安全切換。

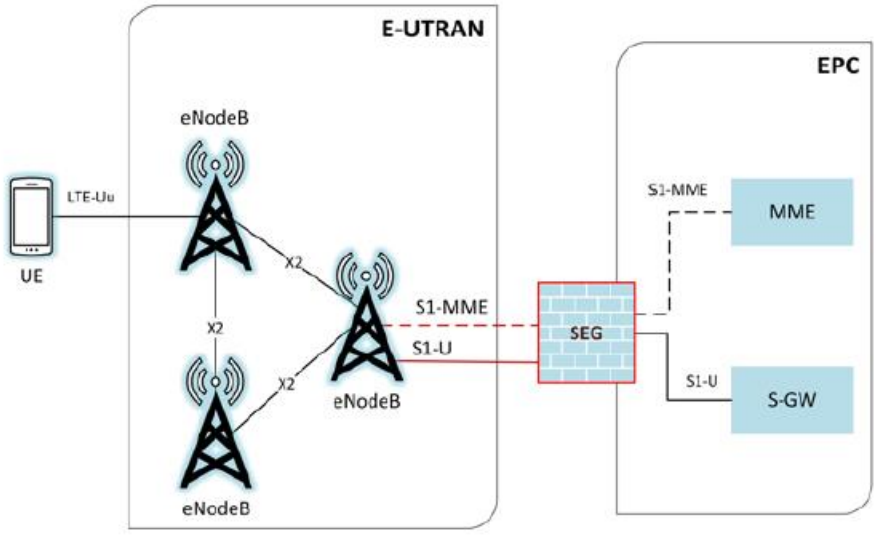
現有的兩種切換：X2 切換和 S1 切換。在 S1 切換過程中，行動管理實體(MME)在切換發生前就已經發覺將會發生切換；但在 X2 切換過程中，行動管理實體(MME)不會察覺，而且轉換完全透過 X2 介面只在 eNodeBs 之間產生。兩種切換方式都有特殊的安全考量。對於 S1 切換，行動管理實體(MME)可在斷開連接之前刷新用於保護空中介面的加密參數，至於 X2 切換，刷新後新金鑰資料僅能在切換之後，為下一次切換而提供。

當發生切換時會產生新的金鑰，雖然沒有產生新的主區 域金鑰(即 KASME)，但是會從舊的金鑰分離出部分新區域。除其他加密參數與新 eNodeB 的呼叫 ID 外，還會利用 KeNB 來產生 KeNB*，後者將用來保護切換後產生的新區域。值得注意的是，來源基地台與行動管理實體控制金鑰之派生，以及新的 eNodeB，皆不代表知悉用於原 eNodeB 區域的金鑰。

3.6 回程線路的安全

3GPP 已明定了提供各種 LTE 網路介面機密性保護的選擇性性能。第 3.4 節討論過位於 Uu 介面供使用者設備(UE)與 eNodeBs 之間，以及位於 X2 介面供 eNodeBs 相互之間可選擇的機密性保護。根據 LTE 技術規定 33.101，S1 介面的 eNodeBs 與演進封包核心之間的機密性保護也是選擇性的。3GPP 明定，根據 3GPP 技術規範(TS) 33.2104 使用網際網路安全協定(IPsec)，應設定 NDS／IP 以便為 S1 介面提供機密性，但規範進一步規定，若 S1 介面是「被信任(trusted)」或「受物理保護的(physically protected)」，則業者可選擇要不要機密性保護。不過，3GPP 規範並未針對「被信任」或「受物理保護的」作進一步的定義。

S1 介面連接的端點通常相隔數英里。LTE 網路發送的任何數據，從基地台到演進封包核心(EPC)設備為止，可能需要被傳送數英里。提供回程線路連接的物理手段有很多，包括某些技術：微波、衛星、乙太網、地下光纖等。為了提供 S1 介面的物理保護，行動網路業者(MNO)必須對該網路連接經過的每個位置都有安全控制。蜂巢行動網路業者(MNO)很可能未擁有或經營用於 LTE 網路流量回程線路的物理連接，這使得行動網路業者(MNO)難以確保 S1 介面受有物理性的保護。網路業者可以利用其他網路的安全措施(例如多重通訊協定標籤傳輸的虛擬私有網路 MPLS VPN、第 2 層虛擬私有網路 layer 2 VPN)來保護穿過 S1 介面的流量，以確保這個介面受到妥善照顧(trusted)。



(圖 11- 對 S1 介面的保護)[16]

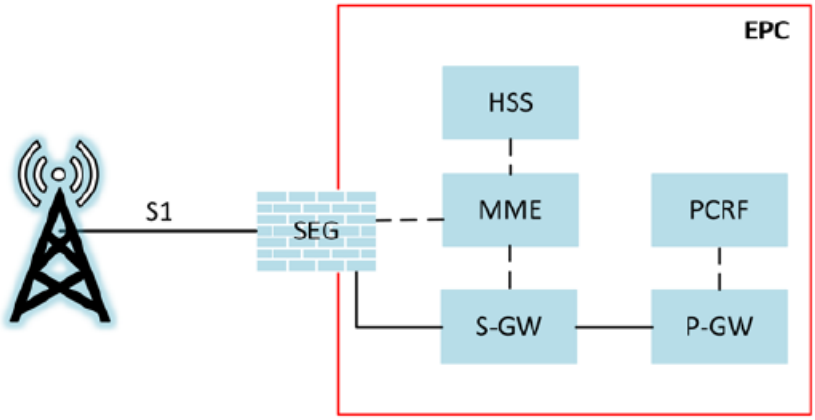
All-IP 系統為早期的蜂巢網路帶來從所未見的安全問題。在 LTE 之前，若想要攔截蜂巢網路上的流量，對手需要有專門的硬體設備，但是 LTE 在 eNodeB 與演進封包核心間(EPC)的傳輸機制皆是基於 IP 的傳輸，攔截流量只需要基本的網通經驗、電腦、網線以及存取交換機。若 S1 介面沒有機密性，則被攔截所有流量都會以明文(clear text)形式發送出去。

3GPP 技術規範(TS) 33.210 規定：「基於本地 IP 通訊協定的每個網路層都應有安全措施。這些網路層使用的安全協定是 IETF 定義於 RFC-4301 與 RFC-2401 之網際網路安全協定(IPsec)的協定[17]」該 3GPP 文件引進了安全網域(Security Domains)、以及在這些網域邊緣使用安全閘道(Security Gateways, SEG)或防火牆以提供安全性的概念。安全網域是「由單一管理機構管理的網域」[3]，這種描述對 LTE 網路很重要。然而，安全網域的定義並不明確，可能導致對安全網域有不同的解讀與使用說明。安全網路可能是指：演進封包核心(EPC)的所有元件及其相互通訊皆由相同的數據中心託管，並由行動網路業者(MNO)控制其物理安全的情形。但是，也可以是指：既使所有核心元件的地理位置分散全國各處，但因為是由同一管理團隊管理這些元件，因此，行動網路業者(MNO)

[16] 3GPP TS 33.210 V12.2.0 (2012.12) 第三代合作夥伴計劃；技術規範服務與系統；3G 安全；網域安全(NDS)；IP 網路層安全 (第 12 版) [3]

[17] 為了避免原文和本文間的引用衝突，省略該引用內容的例示。

將所有核心元件定義為單一安全網域的情形。機密性保護從使 eNodeB 在 S1 介面穿梭的網際網路安全協定(IPsec)通道開始(有可能不是物理性保護)，結束於演進封包核心(EPC)託管的安全網域邊緣的安全閘道。



(圖 12－安全閘道的圖例)

使用 S1 介面上的網際網路安全協定(IPsec)需要網際網路安全協定(IPsec)通道尾端的端點提供預設金鑰或數位憑證。儲如公開金鑰基礎建設(Public Key Infrastructure, PKI)等的可擴充系統，可能被用於商用的 LTE 網路。基於端點預設的策略，可利用網際網路金鑰管理(Internet Key Exchange, IKE)不間斷地產生用以建立加密連接的安全參數。網際網路安全協定(IPsec)通道兩側的端點(即 eNodeB 與 SEG)內含公開金鑰基礎建設(PKI)系統手動或不間斷提供的數位憑證或預設金鑰。若未事先提供數位憑證，可利用憑證授權中心(Certificate Authority, CA)發給數位憑證，並且必須可以通過 LTE 網路的端點。有關公開金鑰技術的更多資料，請參考 NIST SP 800.32 [26]。

3.7 核心網路的安全

如前所述，3GPP 已明定 LTE 網路中各種連接可選擇的安全性能。然而，既使 3GPP 在其標準中提到 LTE 已採用 All-IP 網路，但因為沒有針對演進封包核心(EPC)量身訂作的安全準則，所以對於演進封包核心(EPC)安全的重視必須更甚於 2G／3G [3]。傳統 IP 網路安全準則與操作程序可能會有幫助。既然核心網路處理大部分的控制平面信令，其安全需求即成為主要考量。

如技術規定(TS) 33.210 規定，LTE 網路在邏輯上和物理上必須區分為不同的安全網域。若有任何核心元件位在不同的安全網域內，則其相互之間的交流即需要透過安全閘道(SEG)提供路線，並利用網際網路安全協定(IPsec)提供加密與完整性保護[3]。由於安全網路的定義不明，若將業者的核心網路視為一個安全網域，就代表 LTE 核心元件間的標準通訊缺少安全措施，在這種情況下，在核心內傳送的所有信令及使用者流量將會變成明文傳送，沒有任何機密性保護。但是，若將核心不同部分定義於存在不同安全網域，其相互之間的交流即需要利用網際網路安全協定(IPsec)加密。為確保使用者和控制資訊在核心網路的適當位置上受到保護，應該謹慎考慮如何定義網路的安全網域。在不同核心元件之間可採取機密性保護，以便於保護使用者與信令傳輸。

目前，3GPP 正為 3GPP 節點制定安全保證方法(Security Assurance Methodology, SECAM)，主文

件：技術報告(TR) 33.805「3GPP 網路產品之網路產品安全保證與強化要求的研究方法(含可行的相關測試案例) [8]」。依規劃，技術報告(TR) 33.805 會有附件，附件中將列出每個核心元件安全考量。3GPP 首先將為行動管理實體(MME)建立安全保證規範(SCAS)試用版。一旦完成對行動管理實體(MME)的安全保證規範(SCAS)，3GPP SA3 工作小組(定義 LTE 安全標準的團隊)將繼續進行其他網路產品等級適用的安全保證規範(SCAS)。目前仍在草擬的行動管理實體安全保證規範(MME SCAS)，即技術報告(TR) 33.806，將可以為行動管理實體(MME)提供安全保證的規格。3GPP 正與 GSMA 的網路設備安全保證團隊(NESAC)合作建立一套認證程序與解決方案，以根據安全保證規範(SCAS)的要求進行評估產品。

3GPP 標準沒有針對核心網路安全的強制安全規範或要求，因此，安全保證規範(SCAS)的未來發展可能需要針對個人核心元件中實施特定的安全管制。

4 對 LTE 網路的威脅

本節按相關威脅種類分組，探討 LTE 網路威脅的一般類型。值得注意的是，3GPP SA3 工作小組探討了對 LTE 網路的威脅並撰寫了一份文件，列出本節將討論的威脅[7]。除 3GPP 外也有許多針對威脅的分析(例如[16]、[17]與[18])，本節分析時也會提到。以下列出的許多威脅已透過學術研究加以確認，而其他則是在現實世界中對已部署蜂巢系統發生攻擊的記錄及報告。各組織可利用本節所述之高階威脅類別，作為自己詳細威脅模型的起點。

有些威脅可能影響網路的可用性與恢復力，而有些威脅僅限制使用者數據的完整性與機密性。此外，本節所述的大部分威脅僅影響網路的有限部分。隨著可取得之低成本 LTE 軟硬體[21]增加，於是降低了實現後述大部分威脅的複雜性[19] [25]。

4.1 一般網路安全性威脅

LTE 基礎建設的元件(例如 eNodeB、行動管理實體 MME、服務閘道 S-GW)可以在商用硬體、韌體及軟體上運作，使得它容易受到通用作業系統或其他軟體應用程中中已知軟體缺陷影響(例如 FreeBSD 和其他*nix 變種)。雖然可能對系統做大量的客製化，但應該要識別和理解所使用之商用硬體與和知名作業系統。這代表這些系統需要有適用當配置，並且定期修補已知的漏洞，像是美國國家弱點資料庫(National Vulnerability Database)列出的已知漏洞[28]。以下小節將討論針對特定網路元件及 LTE 網路管理的惡意軟體威脅。

4.1.1 對使用者設備(UE)的惡意軟體攻擊

感染行動裝置作業系統、其他韌體及已安裝之應用程式的惡意程式碼會阻止使用者設備(UE)存取蜂巢網路。惡意軟體會直接攻擊基頻作業系統(baseband OS)及其相關韌體。攻擊基頻作業系統可能改變存取網路的重要配置檔案(configuration files)，或者阻止重要路徑的運作，例如解讀基地台信令的路徑。這些都會導致服務被阻斷。

4.1.2 影響無線存取網路(RAN)基礎建設的惡意軟體攻擊

安裝於行動裝置或感染行動裝置作業系統和其他韌體的惡意軟體，可能是對業者無線網路基礎建設發動攻擊的殭屍電腦網路的一部分。分散式阻斷服務攻擊(Distributed Denial of Service, DDoS)可以藉由持續性的攻擊請求或高寬頻資訊和服務請求發動。行動裝置應用程式發出大量更新請求時，業者的無線網路基礎建設會出現偶發性的分散式阻斷服務攻擊(DDoS) [11]。惡意軟體亦能危害基地台的作業系統，導致意外與不良設備行為。

4.1.3 影響核心基礎建設的惡意軟體攻擊

感染業者核心網路基礎建設的惡意軟體根據其感染的元件可能會記錄網路活動、變更重要通訊閘道的配置，以及查覺使用者流量(例如通話流量、SMS／MMS)。這些類型的威脅先前已被全球行動通訊系統(GSM)網路所察覺[22]，但是到目前為止，在 LTE 基礎建設的後端還沒有發生這類攻擊的實例。對行動管理實體(MME)的分散式阻斷服務攻擊(DDoS)可透過持續性的攻擊請求來發動。

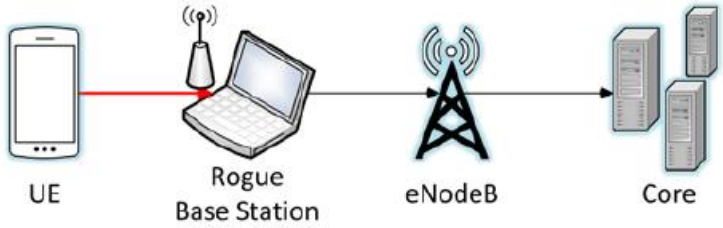
4.1.4 未經授權存取運算與存取管理(OAM)網路

運算與存取管理(Operational and Access Management, OAM)網路是蜂巢網路運算的重要部分，為地理位置分散的元件提供遠程存取。這些運算與存取管理(OAM)網路介面能快速存取網路元件，以

便行動網路業者(MNO)從單一的中心位置管理及調整網路。設計不良、配置管理鬆懈，以及這些管理網路和介面缺欠強化都會對網路的操作穩定性造成嚴重的安全風險。未經授權存取管理介面，可能會惡意地或無意地造成重要網路系統的配置錯誤。

4.2 偽基地台

流氓基地台是未經許可的基地台，並非真正行動網路業者(MNO)擁有與經營的基地台。他們散布一個偽裝成合法業者網路的蜂巢網路，利用下架(commercial off-the-shelf, COTS)硬體便宜地取得建造這些裝置所需的硬體。2G(GSM)基地台作業所需的軟體是可以自由取得的開放原始碼軟體[20]，而且可以配置來操作流氓基地台。



(圖 13－流氓基地台的示例)

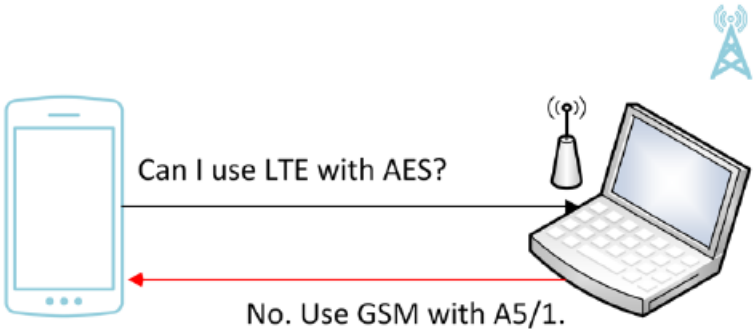
偽基地台利用行動手持裝置會連接到業者網路內正在廣播且最高功率的基地台的這項事實，因此，當偽基地台在物理上接近某個正在以較高功率傳輸的行動手持裝置時，該手持裝置可能會試圖連接到惡意網路[23]。行動手持裝置被設計成能向後相容較舊的蜂巢系統，可以在移動時提供始終如一的使用者體驗，而偽基地台即利用向後相容以及舊式蜂巢系統的弱點。在撰寫本文時，大部分的偽基地台是傳播 2G 全球行動通訊系統(GSM)蜂巢網路。全球行動通訊系統(GSM)提供的安全性保護欠缺手持裝置與蜂巢網路之間的雙向認證，以及有足夠長度的金鑰的堅固密演算法。此外，亦未強制要求對 2G 全球行動通訊系統(GSM)的空中介面加密。

4.2.1 裝置與身份追蹤

如前所述，國際行動用戶識別碼 IMSI(通用積體電路卡 UICC)與國際行動裝置識別碼 IMEI(手持裝置)皆作為唯一的身份辨識。這兩種識別卡可用以顯示某個行動手持裝置的擁有者，以及裝置的物理位置。今日，人們經常將他們的行動裝置帶在身邊，若利用偽基地台來攔截某個地區的流量(例如您的住所)，則偽基地台的業者可能可以辨別出特定人士是否居住在特定區域內。因為竊聽者可以確定用戶是否在給定位置上，這對隱私權會造成威脅。地理定位所需的資料可經過信令通道取得，並於手持裝置附著和認證過程通過空中介面發送。

4.2.2 降級攻擊

攻擊者利用偽基地台高功率播送，可迫使使用者降級到全球行動通訊系統(GSM)或通用行動通訊系統(UMTS)。於撰寫本文時，通用行動通訊系統(UMTS)用來保護空中介面機密性和完整性的加密演算法並沒有已知的嚴重弱點。但是，不幸的是，2G 全球行動通訊系統(GSM)用來保護其空中介面機密性和完整性的加密演算法卻存在嚴重的缺陷。2G 加密演算法破洞的示例為 A5/1 與 A5/2[15]。根據附著於偽基地台時協商出的演算法，選擇用來保護空中介面的空中介面加密演算法，可能被密碼破壞、導致喪失呼叫與數據機密性。



(圖 14－簡化的降級攻擊)

雖然全球行動通訊系統(GSM)不在本文討論範圍內，但在真實世界利用全球行動通訊系統(GSM)網路來連接 LTE 網路，而使得其亦為本文所及。

4.2.3 阻止撥打緊急電話

利用偽基地台的攻擊者可能阻止靠近偽基地台的行動裝置存取緊急服務。這發生在偽基地台無法將使用者流量轉發給行動網路業者(MNO)時。如果緊急情況下發生這種攻擊，會使受害者無法得到公共安全服務與急救人員的援助。這種攻擊是可察覺的，因為使用者設備(UE)會認為是有蜂巢服務但卻無法撥打或發送／接受數據。這種攻擊利用在撥打緊急電話但無法使用首選網路而選擇的其他向量。在撥打緊急電話時，使用者設備(UE)可能附著並試圖透過偽基地台發送呼叫，既使該基地台並未偽裝成合法基地台，但因為偽基地台不會適時地轉發緊急呼叫，故存在有風險。

4.2.4 未認證的拒絕訊息

如第 3.4 節所述，在使用者設備(UE)附著過程中，協定出安全參數前可以發送某些訊息。拒絕附著訊息即為這些未認證訊息的之一，它會阻止使用者設備(UE)完成附著程序。迫使使用者設備(UE)參與使用者設備附著程序的偽基地台可以發送這種未認證的附著拒絕訊息。為回應所收到的這種訊息，使用者設備(UE)不會再嘗試附著在這個或其他 LTE 網路。既然可以在使用者設備(UE)認證網路之前就發送拒絕附著訊息，它自然也就無法區別偽基地台與真正的基地台。如此一來，在使用者設備(UE)執行強制重開機之前，都可以發生服務阻斷(DoS)。某些基頻在收到這類拒絕附著訊息時並不會自動嘗試重新連線[25]。

同樣的，偽基地台也可以用同樣的方式發送拒絕更新追蹤區域的訊息，也可以造成與拒絕附著訊息相同的效果。

4.3 竊聽空中介面

若業者不對 Uu 介面的使用者平面 LTE 流量進行加密，則可能發生複雜的竊聽攻擊。攻擊者需要適當的設備來擷取與儲存使用者設備(UE)與 eNodeB 間的無線電通訊。此外，攻擊者需要軟體辨別特定的 LTE 頻率，以及使用者設備(UE)用來通訊的時間間隔，以便將擷取的流量解調為 IP 封包。

4.4 通過被綁架家庭基站發動攻擊

家庭基站(Femtocells)讓使用者能夠在家中或其他區域設置一個小型基地台。這些小型基地台為

eNodeB 接收不良無法一致覆蓋的地區提供核心網路的存取。使用者設備(UE)附著到裝置，如同典型的 eNodeB 一般，但這些裝置通常會利用使用者家中的網際網路連接，透過網際網路服務提供者(Internet Service Provider, ISP)連回到行動網路業者(MNO)的核心。LTE 從第 8 版開始已經標準化家庭基站，並稱之為演進的家庭節點 B(HeNodeBs 或 HeNBs). HeNBs 被要求連接回 HeNB 閘道(HeNB-GW) 必須有網際網路安全協定(IPsec)，以保護進出行動網路業者(MNO)核心網路的流量[4]。

若攻擊者實際佔有 HeNB，便有無限的時間來找出 HeNB 上的瑕疵。可以類似偽基地台的使用方式來利用被綁架的 HeNB，但後者還可以存取用來保護蜂巢連線的加密金鑰。這些金鑰能使攻擊者存取尚未發送回核心網路的明文流量。常見的攻擊方式是利用主機作業系統和驅動程式中的實施漏洞[14]。

4.5 無線電干擾攻擊

干擾攻擊是利用用於發送／接收資訊之無線電頻道來中斷蜂巢網路存取的一種方式。具體而言，這種攻擊是在給定的波段上，藉由以高功率傳送靜態及／或雜訊的方式把信號的雜訊比降低。因為可用不同方式達成這類攻擊，故需要的技能等級和專業設備也不同。以 LTE 頻譜中的特定頻道為目標，並限定在特定時間以避免偵測的干擾，通常稱為智慧型干擾(smart jamming)。在大範圍的射頻(RF)頻率上播送雜訊則被稱為愚笨型干擾(dumb jamming)。

4.5.1 干擾使用者設備(UE)的無線電介面

對於阻止使用者設備(UE)傳送信令到 eNodeB，可能存在有低成本、高複雜度的攻擊方式。維吉尼亞州理工大學(Virginia Tech) [12]與其他機構[13]皆指出，由於相較之下 LTE 空中介面協定使用的 LTE 控制信令較少，故可能會發生這類攻擊。需要進一步的研究來確定這類攻擊的複雜度、嚴重性和成功可能性。

4.5.2 干擾 eNodeB 的無線電介面

基地台可以實體(例如光纖)或無線(例如微波)連接到其他基地台。這些連結通常用於執行呼叫切換作業。如 4.5.1 所述，干擾 eNodeB 用來相互通訊的無線連結是可行的，儘管在理論上，這類用在使用者設備(UE)的智慧型干擾，可被修改成以通訊 eNodeB 為目標，而阻止 eNodeB 傳送與 eNodeB 射頻(RF)的通訊。

3GPP SA1 工作小組指出，這類攻擊「…可通過特殊的硬體啟動，而且對它不可能執行任何對策。然而，干擾攻擊卻是可以被偵測與通報的」。[7] 這表示這類干擾攻擊在 LTE 威脅類型的範圍內。

4.6 竊聽回程線路和核心

回程線路連接負責 LTE 核心與 eNodeBs (蜂巢站)之間的數據連接。在本文件第 3.6 節，探討了回程線路的安全以及基於功能選擇的標準，為這個重要的介面提供了機密性。若 LTE 網路在回程線路介面未採用機密性保護，則從蜂巢站發送與接收的通訊就很容易被竊聽。若是惡意行為人能夠存取網路設備退出 S1 介面的話，那麼攔截通訊也將顯得微不足道。

4.7 對網路基礎建設發動實體攻擊

蜂巢站是含有 eNodeB 運作與作業需要之所有必要設備的實體位置。雖然，這些地點有時設有柵欄並受實體安全系統的保護，但還是有可能繞過這些防禦措施。若運行所需的設備被夠線或以某

種方式銷毀，則可能發生阻斷服務攻擊。舉例來說，竊取銅非常普遍，而這即可能造成服務被阻斷。若攻擊者能控制運行 eNodeB 的系統，則亦可能發生更難以偵測且更狡猾的攻擊。

4.8 攻擊 K

加密金鑰使 LTE 能夠提供許多強大的系統內建安全功能。如第 3.1 節所討論，有許多不同金鑰用來保護不同的 LTE 通訊層，而這些金鑰皆從一個名為「K」的秘密預設金鑰中衍生而出。這個金鑰存在網路的兩個地方：一是在通用積體電路卡(UICC)上運行的用戶全球識別卡(USIM)，另一個是在業者的家庭用戶伺服器(HSS)／認證中心(AuC)。用戶全球識別卡(USIM)的製造商若負責將金鑰燒錄到用戶全球識別卡(USIM)上，則該製造商亦能取得 K。根據將 K 燒錄到通用積體電路卡(UICC)上的過程，惡意行為人很可能取得這個負責 LTE 所有加密功能的秘密金鑰。若行為人取得 K，他們就有可能冒充網路使用者，也有能力解密來自這個金鑰 K 使用者的通訊。

4.9 竊取服務

通用積體電路卡(UICC)是一種通過使用可以從行動裝置上移除的小卡片。來自行動網路業者(MNO)的服務綁定在使用者的通用積體電路卡(UICC)上。這代表，可以從一個行動裝置竊得通用積體電路卡(UICC)後，插入其他的行動裝置，以達成竊取服務(含語音與數據服務)的目的。另一種竊取服務的手段是：由可以存取家庭用戶伺服器(HSS)或策略與計費規則(PCRF)的內部人員來授權未經批准地存取網路。例如，在行動網路業者(MNO)不知情的情況，員工為自己利益啟用並出售通用積體電路卡(UICC)。

5 緩解措施

本節針對上一節所述的各種威脅提出緩解措施。第 5 節提出的緩解措施與第 4 節所述之威脅並沒有一對一的關係，由於本份分析中仍然未解決的威脅，代表各領域的研究仍在進行中。各個緩解措施至少可用來解決第 4 節所述威脅之一。值得注意的是，關於上一節列出的各項 LTE 威脅，3GPP SA3 工作小組已討論並撰寫一份詳細文件[7]，而各組織可將本節列出的高階緩解措施用以解決威脅模擬練習中發現的威脅。

蜂巢網路採用數個以下的緩解措施，而大部分對日常使用者而言都不太可能實現。變革主要操之在行動管理業者(MNO)、行動裝置作業系統開發者及硬體製造商的手中。行動網路業者(MNO)能夠試著實施本節所述的許多緩解技術；然而，在硬體、韌體和軟體不支援這些對策的情況下，可能仍然存在著挑戰。因此，與生態系統合作為商用蜂巢設備研究、開發及實施這些安全功能是非常重要的。

若這些緩解措施對使用者有重要性，則使用者需要向適當對象請求加裝這些安全保護。列出的許多緩解措施可能只需要修改某個已實施功能的配置，這在短期之內就可以做到。其他的則需要更新行動裝置作業系統的軟體、及／或寬頻處理器，或修改 3GPP 標準，這就需要更多時間來執行。

5.1 網路安全業者的推薦措施

LTE 基礎建設公司(例如：eNodeB、行動管理實體(MME)、服務閘道(S-GW))依靠專用系統執行其網路功能。在這些系統上運行的核心軟體通常是通用的作業系統，因此，按照當今業界一般資訊科技系統應用的相同方式，將推薦的電腦安全措施(包括網路、實體及人員安全)應用在這些零件上是很重要的。可以在行動管理業者(MNO)的 LTE 基礎建設上，謹慎地計劃並實施諸如補丁管理、配置管理(例如禁用現場網路(field network)設備上的串行埠(serial port))、識別與存取管理、惡意軟體偵測及入侵偵測和防禦系統等保護機制。這些程序和保護機制可以量身訂作，為特定的 LTE 系統提供最好的支援與保護。

可用於解決以下威脅：4.1、4.1.2、4.1.3、4.1.4

5.2 賦予空中介面機密性

雖然對非存取層(NAS)和無線資源控制模組(RRC)的完整性保護是強制性的，但是業者卻可以選擇是否對 LTE 系統內的空中介面加密[5]。透過使用者加密金鑰(UP_{enc} key)，賦予 Uu 介面的使用者平面加密保護能阻斷被動的竊聽攻擊。由於在空中介面上施以機密性保護可能會讓蜂巢網路產生較長等待時間(遲延)，也可能嚴重影響使用者設備(UE)的電池，因此，施以機密性保護時應採用更多測試、試運行、及適合的硬體和階段性做法。

可用於解決以下威脅： 4.3

5.3 使用加密指示(Ciphering Indicator)

如第 4.2 節所述，2G 全球行動通訊系統(GSM)的認證程序不執行行動裝置與基地台之間的雙方認證，這使得非 LTE 的流氓基地台可以對正與 LTE 連接的使用者設備(UE)發動降級攻擊；這樣的全球行動通訊系統(GSM)連接並未受機密性保護。現在的行動裝置不提供使用者選擇，故使用者

無法得知使用者設備(UE)與 eNodeB 的連接是否有加密。3GPP 提供一項稱為加密指示機制，警告使用者有未加密的連接。

3GPP 技術規範(TS) 22.101 將加密指示定義為：通知使用者關於使用者平面機密性保護現況的指示功能。這項功能可以設定為出現在使用者行動裝置上的使用者介面通知。行動管理業者(MNO)也可以藉由用戶全球識別卡(USIM)的設定停用這項功能。3GPP 指出，使用者設備(UE)的預設行為必須服從用戶全球識別卡(USIM)內含的設定。然而，使用者設備(UE)也可以提供使用者介面選擇忽略用戶全球識別卡(USIM)的設定，並提供使用者其使用者平面機密性保護現況的指示，但是「加密本身不受這項功能的影響，使用者仍能選擇如何進行加密」[6].

對於希望知道其無線蜂巢連接是否有加密的使用者而言，這項指示功能是有幫助的，但它也需要行動裝置作業系統供應商(例如 Apple、Google、Microsoft)或寬頻製造商(例如 Qualcomm、Intel、Samsung)提供新的軟體。

*用於解決以下威脅：*4.3

5.4 用於連接 LTE 網路之使用者定義選項

流氓基地台通常利用全球行動通訊系統(GSM)欠缺雙向認證這點，而現在的行動裝置不讓普通使用者選擇其行動裝置*僅*連接到 4G LTE 網路、特定行動網路業者的(或行動虛擬網路業者 MVNO 的)網路、或特定的實體蜂巢站。若是使用者能確認其行動裝置只會連接到 4G LTE 網路，並透過 LTE 的認證與金鑰協商(AKA)協定達成該使用者設備(UE)與 eNodeB 間的雙向認證，就不可能受到流氓基地台攻擊，使全球行動通訊系統(GSM)的連接降級。

值得注意的是，許多使用者設備(UE)的優先選擇的網路技術清單，根據其平台在測試模組也可能有相似的選項。目前還不清楚這個選項是否能阻斷因連接流氓基地而正受攻擊的使用者設備(UE)。目前功能並不在安全方面，而是提供對抗流氓基地台的重要防禦。使用者定義選項未廣泛設置在使用者設備(UE)中，可能需要行動裝置作業系統供應商(例如 Apple、Google、Microsoft) 及／或寬頻製造商(例如 Qualcomm、Intel、Samsung)提供軟體更新。這個選項對於通知希望僅連接 LET 網路的使用者是有幫助的。

用於解決以下威脅： 4.2.1、4.2.2、4.2.3

5.5 確保 S1 介面的機密性保護

實體與邏輯安全皆可用於保護 LTE 網路回程線路連接的安全。將裝置置於物理上的安全位置是保護回程線路連接安全以及免於惡意行為很重要的一步，用密碼保護穿過回程線路連接的 IP 流量也很重要，還可以提供更高一階的保證，而這可以利用 NDS／IP 來實現。執行 S1 介面上的機密性保護可能會造成蜂巢回程線路連接遲延，需要進一步研究以了解這種遲延是否顯著降低服務和總處理量。

用於解釋以下威脅： 4.6

5.6 加密核心網路元件間的公開介面

在不顯著影響網路資源可用性的前提下，得以某些方式保護核心網路節點之間介面的機密性，例

如可能是透過 3GPP 技術規範(TS) 33.210 定義的機制。3GPP 與 ETSI 將提供保護這些介面的指南。

用於解決以下威脅：4.6

5.7 使用用戶識別卡(SIM)／用戶全球識別卡 (USIM)密碼

如前所述，某些現代的行動設備作業系統採用 3GPP 技術規範(TS) 121.111 [31] 規定的用戶全球識別卡(USIM)密碼，得以透過通用積體電路卡(UICC)預設的密碼對用戶全球識別卡(USIM)使用者進行認證。啟用通用積體電路卡(UICC)密碼能在通用積體電路卡(UICC)被竊或遺失時，防止未經授權的網路存取。竊取通用積體電路卡(UICC)並將其插入其他行動裝置之人，可能需要輸入密碼才能繼續操作。登入失敗達 10 次後，許多通用積體電路卡(UICC)會鎖住，需要使用者的行動網路業者(MNO) 提供解鎖密碼，才可以再次啟用該用戶全球識別卡(USIM)。若用戶識別卡(SIM)／用戶全球識別卡 (USIM)密碼增加了額外的認證或讓使用者設備(UE)啟動程序變慢，則會讓使用者體驗降低。

用於解決以下威脅：4.9

5.8 使用臨時識別碼

用戶的永久識別碼，即國際行動用戶識別碼(IMSI)，是使用者設備(UE)附著到 LTE 網路時發送給 eNodeB 的第一個參數。國際行動用戶識別碼(IMSI)有時以明文格式透過空中介面傳送，這在某些情況下是不可避免的。3GPP 定義了行動網路業者(MNO)可利用的多種臨時識別碼，以避免透過空中介面發送這類敏感的識別碼，例如 LTE 中的全球唯一臨時識別碼(GUTI)。當使用全球唯一臨時識別碼(GUTI)時，追蹤使用者即變得更加困難。全球唯一臨時識別碼(GUTI)需要設定為透過 *NAS GUTI Reallocation Command* 定期刷新，以確保它是一個真正的臨時識別碼[19]。

用於解決以下威脅：4.2.1

5.9 第三方串流(Over-the-Top)方案

若行動網路業者(MNO)未加密使用者的流量，或發生被動式竊聽攻擊時，使用第三方串流服務可以提供使用者數據強大的認證、完整性和機密性保護。這項緩解措施可有效地將行動網路業者(MNO)的網路作為「笨水管(dumb pipe)」，而使用者能利用在一般行動裝置作業系統上運行的應用程序，提供影像、聲音或其他某些通訊服務。此外，第三方串流方案亦可作為深層的防禦手段，選擇不只是依賴其行動網路業務提供機密性保護。

用於解決以下威脅： 4.2.2、4.3、 4.4、 4.6、4.8

5.10 未經認證的拒絕訊息反應

當出現有能力拒絕網路存取的非法訊息時，使用者設備(UE)的可能緩解措施是繼續搜尋其他可用的網路，同時忽略拒絕服務的網路。可以測試寬頻韌體，以便於了解當未經認證的拒絕訊息出現時這些系統會有什麼反應。為確保寬頻處理器在收到非法拒絕訊息時，不會有造成非預期服務中斷的反應，則需要進行更進一步的研究與開發。

用於解決以下威脅： 4.2.4

5.11 蜂巢站設備的實體安全

蜂巢設備的實體安全對防止影響可用性的故意和意外事件是很重要的。3GPP 技術規範(TS) 33.401 標準提到「有實體保護的」系統與介面，強調了對這類保護的需求，但並沒有進一步敘述實際上應該有什麼樣的實體安全管制。然而，NIST SP 800.53 的實體與環境保護管制家族算是適於著手的合理管制清單[33]。美國國家公共安全電信會議(National Public Safety Telecommunications Council, NPSTC)對公共安全的論述中，亦認為實體存取管制的確有助於保護蜂巢站的安全[34]。舉例而言，該文件建議柵欄與大門應上鎖，並實施諸如錄影監控等的偵測方法。

用於解決以下威脅：4.7

5.12 偵測流氓基地台

如前所述，流氓基地台可能降低蜂巢裝置和相關設備的安全性。雖然有些人認為這類技術仍在開發階段，但確實有可能偵測流氓基地台的存在。行動裝置應用程式可用於偵測流氓基地台，但需要在較舊的裝置模組上使用特定的晶片組[35]。有不同的方法可用於偵測。一種方法是接收源自基地台播送的訊息中所包含的訊息，並且根據已知良值(known-good value)檢查該資訊。另一種方法是儲存已知基地台清單，並在發現新基地台時警告使用者。在此情況下，需要由使用者做出最終決定。統包方案(turnkey solutions)也可用於此一目的，它將偵測流氓基地台的存在。任一種技術都有侷限，可能產生誤報，但這是一個活躍的研究領域，對擔慮流氓基地台存在的各個組織是有幫助的。

用於解決以下威脅：4.2.1、 4.2.2、 4.2.3、 4.2.4

6 結論

與以前的蜂巢網路相比，LTE 提供的安全功能顯然更為強大。蜂巢網路與使用者設備(UE)間的額外雙方認證，以及使用能公開審查且足夠長度金鑰的加密演算法，對改良蜂巢網路安全性有正面的做法。LTE 加密金鑰體系加入增強版的金鑰隔離，以及完整性保護的強制要求都有助於提高標準。

然而，LTE 系統獨立部署 – 它們與既有的蜂巢基礎建設併存。今日，許多不同產業繼續將較舊的蜂巢系統用於滿足各種需求。考量到這一點，不難發現為什麼 LTE 網路通常被安置與全球行動通訊系統(GSM)與通用行動通訊系統(UMIS)網路配合使用。這種蜂巢網路的跨世代部署方式可能導致整個蜂巢的安全性下降。最普遍的例子就是為了支援傳統的安全配置，而需要有寬頻韌體來維持向後相容。

這些技術的相關連接，為已分佈於各洲各地的複雜系統帶來了其他的複雜性。傳統上，蜂巢網路使用單獨的網路傳送呼叫信令的資訊。特別是已經使用數十年的 SS7 網路，它與蜂巢網路技術不同，正面臨其特有的安全挑戰。3GPP 規定了 LTE 專用的 Diameter 版本，雖然它仍未被廣泛採用，但可部分用以解決使用 SS7 的相關問題。隸屬美國聯邦通訊委員會(Federal Communications Commission, FCC)的通訊安全性、可靠性與互通性諮詢委員會(Communications Security, Reliability and Interoperability Council, CSRIC)第 10 工作小組，對 SS7 的安全問題提出一份報告，但是在完全解決這些威脅之前，仍然需要進行更多工作[32]。行動網路業者(MNO)及所有相關人士對這個技術進行其自己的安全分析是很重要的，以便於了解如何適當地緩解這種信令技術帶來的風險。既然任一行動網路業者(MNO)網路的弱點，會對其他連接的網路有不利影響，所以安全分析應該要涉及其他行動網路業者(MNO)解決他們網路中的這些風險的方法。

LTE 僅利用 IP 技術這點是與舊蜂巢網路的主要區別。LTE 不利用電路交換，而是選擇轉向單純的封包交換系統。但是，IP 是一種已經商品化的技術，已為資訊技術從業人員所理解，所以這可以是一種挑戰、同時也可以是一種機會。攻擊者可能借助既有工具來利用以 IP 為基礎的網路，攻擊在行動網路業者(MNO)網路中的 LTE 核心和其他相關蜂巢基礎建設。相反的，這也可讓 LET 網路可以立即應用以 IP 為基礎的既有防禦技術。希望應用這些技術將為提高系統安全性帶來新穎的作法。

以下清單，重點列出在 LTE 安全架構中欠缺適當管控、或尚有未解決威脅的區域：

- **對使用者流量的預設機密性保護**：根據 LTE 標準，在系統預設配置中，並未提供使用者流量的機密性保護。除了某些情況(例如緊急呼叫)外，預設啟用使用者流量加密，可提供終端用戶立即可用的安全措施。
- **禁止使用者流量的完整性**：如第 3.4 條所述，雖然 LTE 標準規定對重要信令流量提供完整性保護，但卻明文禁止使用者流量的完整性。
- **欠缺對抗干擾攻擊的保護**：這領域的研究正在進行中，也提出了緩解措施，但是仍不清楚這些緩解措施是否有適當地調查並考量納入 LTE 標準。

- **運算與存取管理(OAM)網路**：運算與存取管理(OAM)網路的架構及管理方式可能存在漏洞。

雖然本文著重在 LTE 及其安全架構的基本原則，但仍有許多概念超出了我們分析的範圍。這些概念中，有些是建立於 LTE 架構之上的服務，而有些則是來自於對 LTE 網路的特定實施和利用。去理解這些概念帶來的以下安全含意是很重要的，並且也需要更進一步的研究：

- 多媒體子系統(IMS)的安全分析，
- LTE 語音的(VoLTE)安全分析，
- 對抗干擾攻擊的保護，
- 啟用使用者設備(UE)的網路集成，
- 用於公共安全的 LTE，
- 空中更新的安全影響，
- 複數業者核心網路(MOCN)，以及
- 網路功能虛擬化(Network Function Virtualization, NFV)的安全性。

本文件指出了對 LTE 網路的威脅，並敘述針對這些問題的可能緩解措施。探討與啟用本文件所述之緩解措施仰賴於行動裝置作業系統供應商、寬頻韌體開發者、標準組織、行動網路平台與終端用戶的協調合作。由於 LTE 是國家主導的蜂巢通訊技術，因此就本文提出的問題研發解決方案，並持續進行相關研究是一項重要的任務。

附錄四 ETSI TR 103 456 版本 1.1.1 (2017-10)

技術報告

網路；
實施網路與資訊安全指令(NIS)

參考代碼

DTR/CYBER-0021

關鍵字

網路安全、資安防護武裝、資訊安全、隱私

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

本文件可自網站下載：
http://www.etsi.org/standards-search

本文件有電子版及／或紙本。未經歐洲電信標準化協會(European Telecommunications Standards Institute, ETSI)事前書面授權，不得修改本文件電子版及／或紙本的內容。若此等版本及／或印刷內容有任何不一致之處，將以 ETSI 秘書處網路伺服器中保存之 PDF 版本為準。

本文件的使用者請注意，本文件可能會改版或變更。關於本文件與 ETSI 其他文件的現況，請查閱：
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

若您發現本文件有任何錯誤，請將您的意見寄到：
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

目次

智慧財產權

相關專利

本文件相關或可能相關的智慧財產權皆已告知歐洲電信標準化協會(ETSI)。這些相關智慧財產權(若有)的有關資訊對**歐洲電信標準化協會(ETSI)的成員及非成員**皆公開，並可見於歐洲電信標準化協會(ETSI) 秘書處 ETSI SR 000 314：*「智慧財產權(IPRs)；有關 ETSI 標準且已通知歐洲電信標準化協會(ETSI)之相關或可能相關智慧財產權*」。最後更新請見歐洲電信標準化協會(ETSI)網路伺服器(https://ipr.etsi.org/)。

根據 ETSI 的智慧財產權政策，歐洲電信標準化協會(ETSI)未進行包括智慧財產權檢索在內的調查。不保證 ETSI SR 000 314(或 ETSI 網路伺服器公布的更新版)未引用的其他智慧財產權是否是、或可能是、或可能成為與本文件相關。

商標

本文件可能含有所有權人主張及／或註冊的商標及／或商品名稱。除歐洲電信標準化協會(ETSI)的財產以外，歐洲電信標準化協會(ETSI)對這些標的不主張所有權，亦不主張有權使用或重製任何商標及／或商品名稱。本文件提及此等商標，不代表 ETSI 認可與商標相關的產品、服務或組織。

前言

本份技術報告 (TR)由歐洲電信標準化協會(ETSI)網路安全技術委員會(CYBER)制作。

簡介

歐盟議會和理事會 2016 年 7 月 6 日 EU 2016/1148 指令「有關歐盟網路和資訊系統的高階共同安全措施」[i.1] (一般稱為 NIS 指令或 NISD)，其所涉及的法律措施包括：

- 要求成員國有適當的配置，例如有電腦安全事件應變小組(Computer Security Incident Response Teams, CSIRTs)管轄的國家 NIS 主管部門，並制定國家資訊安全策略；
- 通過合作小組建立成員國之間的合作架構，以支援和促進成員國之間的戰略合作與資訊交換，包括電腦安全事件應變小組(CSIRT)的網路，以促進特定網路安全事件之自願合作以及分享風險相關資訊；以及
- 要求成員會提供：有關成員國指定為關鍵服務業者區域經營(包括在指令規定之區域內經營)、特定數位服務提供者實施適當安全措施，以及於服務因嚴重事件有顯著影響時應通知國家相關主管機關的架構和必要義務。

這些法律措施分別又帶來一系列通用的網路安全技術需求，包括：

- 結構性地分享風險和事件資訊；

- 事件通知；
- 以結果為重點的網路安全風險管理實踐及控制，以辨別及保護資產、偵測異常分析和潛在事件，並對可能影響網路與資訊系統的事件做出應變與恢復；以及
- 藉由國際合作改善安全標準和資訊交流，並透過協調標準來促進 NIS 發布全球的通用標準。

本文件根據歐洲電信標準化協會(ETSI)作為區域性及全球性組織的能力，提供符合其要求的實施準則，彙集業界的專業知識與全球網路安全知識(含其本身的網路安全技術規範與報告)。

情態動詞術語

本文件中「**應該**」、「**不應該**」、「**得**」、「**不需要**」、「**將**」、「**不會**」、「**能**」及「**不能**」將依歐洲電信標準化協會(ETSI)撰稿規則第 3.2 條規定解讀(表示意見的口語格式)。
除非直接引用原文，否則在歐洲電信標準化協會(ETSI)文件中**不允許**出現「**應**」與「**不應**」。

報告總結

本文件就目前可用的和全球主要網路安全社群正在開發的技術規範提供準則，旨在滿足與實施 NIS 指令相關的法律措施和技術要求，包括資訊分享、基於網路之風險和事件、與必要的防禦措施。本準則包含：事件通知之考量點與網路安全風險管理的最佳實踐。本文件提供比 NIS 指令或歐盟網路與資訊安全局(ENISA)標準化差異報告更廣泛的網絡安全背景，以促進重要的新興全球開放平台演進，並且包含協調跨網路與跨部門實施，以及協調成員國法律與作業環境的相關挑戰的對策。

1 範圍

本文件根據歐盟議會和理事會 2016 年 7 月 6 日 EU 2016/1148 指令「有關歐盟網路和資訊系統的高階共同安全措施」[i.1] (一般稱為 NIS 指令或 NISD)，就目前可用的和全球主要網路安全社群正在開發的技術規範提供準則，旨在滿足與實施 NIS 指令有關基於風險和事件之網路資訊分享、以及保障基本安全利益所需之必要防禦措施的法律措施和技術要求。
本文件旨在讓供所有需要將 NIS 指令合法轉換為國家立法而考量其效果、使用或實施之人利用，其中包括為在特定產業中被 NIS 指令定義為關鍵服務業者(Operator of Essential Services, OES)而需要更新法規或準則的國家監管機構，或有意提供為數位服務提供者(Digital Service Providers, DSP)提供準則的國家政策制定者。本文件亦得為關鍵服務業者(OES)與數位服務提供者(DSP)本身實施相關準則時使用。本文件的目的並非用以基於組織風險方法選擇或使用技術規範或要求以達成最有效的產業實施。

2 參考文件

2.1 規範性參考文件

本文件未參考規範性的參考文件。

2.2 資訊性參考文件

參考文件有時有限定(指明出版日期及／或出版編號或版本編號)、有時無限制。有限定的參考文件僅適用被引用的版本，而無限定的參考文件則適用該文件的最新版本(含其修正版)。

備註：本節內的超連接是歐洲電信標準化協會(ETSI)發布當時的有效網址，不保證未來亦有效。

以下參考文件非適用本文件所必要，但有助於使用者了解特定主題的領域。

[i.1] 2016 年 7 月 6 日有關整個歐盟網路和資訊系統的高階共同安全措施的歐盟議會和理事

會指令(EU) 2016/1148[i.l]

備註：可見於 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG.

[i.2] 2016 年 11 月歐盟網路與資訊安全局(ENISA)「改善歐盟標準化政策中網路與資訊安全的 NIS 標準化建議」V.1.0

[i.3] ETSI TR 103 305：「網路；有效網路防禦之重點資安控制項目」

[i.4] ETSI TR 103 421: 「網路；網路防禦之網路閘道」

[i.5] 2016 年 7 月 5 日布魯塞爾，歐盟數位，歐盟網路與資訊安全(NIS)指令之置換

[i.6] ETSI TR 103 331：「網路；結構化威脅資訊分享」

[i.7] ETSI TS 102 165-1：「網路；方法與協定；第 1 部分：威脅、弱點、風險分析(TVRA)的方法與實施」

[i.8] ETSI ETR 340：「電信安全；安全管理技術準則」

[i.9] ITU-T X.700 系列建議書 (ISO/IEC 10160)：「資訊技術 – 開放式系統相互連接 – 系統管理」

[i.10] 建議 ITU-T X.800 系列(ISO/IEC 10181, ISO/IEC 11586)：「資訊技術 – 開放式系統相互連接 – 開放式系統的安全架構，通用上層安全」

[i.11] 建議 ITU-T X.1300 系列:「網路安全」

[i.12] 建議 ITU-T X.1050 系列:「安全管理」

[i.13] 建議 ITU-T X.1200 系列: 「網路安全」

[i.14] 建議 ITU-T M.3000 系列: 「管理計劃之安全」

[i.15] ISO/IEC 15408：「資訊技術—安全技術—IT 安全之評估標準」

[i.16] ISO/IEC 27000 系列：「資訊技術—安全技術—資訊安全管理系統」

[i.17] IEC 62443：「工業通訊網路—網路與系統安全」

[i.18] ISACA：COBIT 5 系列

[i.19] ETSI GS ISI 001 (所有部分)：「資訊安全指標(ISI)」

[i.20] ETSI TR 103 303：「網路；關鍵基礎建設背景下的 ICT 保護措施」

[i.21] 2017 年 ETSI 安全週刊

備註：可見於 http://www.etsi.org/etsi-security-week-2017.

[i.22] ETSI 安全週刊，NFV 安全指導

備註：可見於 https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/04_NFVTUTORIAL/ETSI_ISG NFV_TUTORIALMATERIAL.pdf.

[i.23] ETSI 安全週刊，5G 安全：政府觀點

備註：可見於 https://docbox.etsi.org/Workshop/2017/201706_SECURITYWEEK/06_5GSECURITY/S02/NCSC_HAI GH.pdf.

[i.24] 2012 年 Sean Barnum：「MITRE Corporation，以結構性威脅資訊表示(STIX™)標準化網

路威脅情報資訊」
[i.25] ISO/IEC 15408：「IT 安全評估標準」
[i.26] 1995 年 10 月 24 日有關處理個資的個人保護及該個資移轉自由的歐盟議會和理事會指令(EU) 95/46/EC
[i.27] 2000 年 12 月 18 日有關機構與組織處理個人資料與資料移轉自由對個人的保護，歐盟議會和理事會(EC)法規 (EC) No 45/2001
[i.28] ITU-T X.1500 系列建議書：「CYBEX 網路安全資訊交換」
[i.29] U.S. NIST 網路安全框架
備註：可見於 https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
[i.30] ETSI TR 103 305-4：「網路；有效網路防禦之重點資安控制項目；第 4 部分：促進機制」
[i.31] CCRA：「資訊技術安全評估之共同標準」第 1.0 版
備註：可見於 https://www.commoncriteriaportal.org/cc/.
[i.32] 德國聯邦內政部：「資訊基礎建設保護之國家計劃」
備註：可見於 http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf.
[i.33] 德國聯邦內政部：「關鍵基礎建設保護(CIP)之實施計劃」
備註：可見於 http://www.qcert.org/sites/default/files/public/documents/GER-PL-CIP%20Implementation%20Plan-Eng-2007.pdf.
[i.34] IETF draft-ietf-inch-requirements-03：「事件資訊交換之格式(FINE)規定」
[i.35] IETF draft-ietf-inch-iodef-02：「事件數據交換格式、數據模式與 XML 實施」
[i.36] IETF draft-ietf-inch-rid-00：「事件處理：即時的跨網路防禦」
[i.37] IETF draft-ietf-inch-implement-00：「事國際資通訊安全事件訊息交換格式(IODEF) 實施準則」
[i.38] ITU-T X.1500 建議書：「網路安全資訊交換之概述」

3 定義與縮寫詞

3.1 定義

本文件適用 NIS 指令[i1]使用的名詞與定義。

3.2 縮寫詞

本文件適用以下縮寫詞：

ANSSI 全國網路與資訊安全局(Agence Nationale de la Sécurité)
BSI 德國聯邦資訊安全局(German Federal Office for Information Security)
CCDB 共同準則發展委員會(Common Criteria Development Board)
CCRA 共同準則相互承認協議(Common Criteria Recognition Agreement)

CDXI 網路防禦資料交換與協力基礎建設(Cyber defence Data eXchange and Collaboration Infrastructure)

CERT 電腦緊急事件應變小組(Computer Emergency Response Teams)

CIA 機密性、完整性、可用性(Confidentiality, Integrity, Availability)

CIP 重要基礎建設保護(Critical Infrastructure Protection)

CIS 網路安全中心(Center for Internet Security)

COBIT 資訊系統和相關技術控制目標(Control Objectives for Information and related Technology)

CPNI 國家基礎建設保護中心(Centre for the Protection of National Infrastructure)

CSAF 共通安全諮詢架構(Common Security Advisory Framework)

CSIRT 電腦資安事件應變小組(Computer Security Incident Response Team)

CTI 網路威脅情報(Cyber Threat Intelligence)

CTIP 網路威脅情報計劃(Cyber Threat Intelligence Program)

CVRF 共通弱點通報架構(Common Vulnerability Reporting Framework)

CYBEX 網路安全資訊交換(cybersecurity information exchange)

CybOX 網路可觀測事件表達(Cyber Observable expression)

DIB 國防工業基地(Defense Industrial Base)

DMARC 基於網域的訊息認證、通報及一致性(Domain-based Message Authentication Reporting and Conformance)

DNS 網域名稱系統(Domain Name System)

DSP 數位服務提供者(Digital Services Providers)

ENISA 歐盟網路與資訊安全局(European union agency for Network and Information Security)

FIRST 資安事件應變小組論壇(Forum of Incident Response and Security Teams)

FYROM 馬其頓共和國(Former Yugoslav Republic Of Macedonia)

GDPR 歐盟資料保護規範(General Data Protection Regulation)

IAD 資訊保證處(Information Assurance Directorate)

ICT 資訊與通訊技術(Information and Communication Technology)

IETF 國際網路工程研究團隊(Internet Engineering Task Force)

IODEF 國際資通訊安全事件訊息交換格式(Incident Object Description Exchange Format)

ISAC 資訊分享與分析中心(Information Sharing and Analysis Centre)

ISACA 資訊系統稽核暨控制協會(Information Systems Audit and Control Association)

ISI 資訊安全指標(Information Security Indicators)

IT 資訊技術(Information Technology)

IXP 資訊交換站(Internet eXchange Point)

MACCSA 協作式網路情境意識多國聯盟(Multinational Alliance for Collaborative Cyber Situational Awareness)

MAPP 成熟度評估、描寫與計劃(Maturity Assessment, Profile and Plan)

MEC 行動邊緣運算(Mobile Edge Computing)
MILE 輕量級交換託管事件(Managed Incident Lightweight Exchange)
MISP 惡意軟體資訊分享平台(Malware Information Sharing Platform)
MS 成員國(Member State)
MSRC 微軟資安應變中心(Microsoft Security Response Center)
NATO 北大西洋公約組織(North Atlantic Treaty Organization)
NCIRC 北約處理電腦資安事件應變能力(NATO Computer Incident Response Capability)
NCSC 國家網路安全中心(National Cyber Security Centre)
NFV 網路功能虛擬化(Network Function Virtualization)
NII 網路資訊基礎建設(Network Information Infrastructure)
NIS 網路與資訊安全(Network and Information Security)
NISD 網路與資訊安全指令(NIS Directive)
NIST 美國國家標準技術研究院(National Institute of Standards and Technology)
OASIS 資訊標準架構促進會(Organization for the Advancement of Structured Information Standards)
OES 關鍵服務業者(Operators of Essential Services)
OSSI 資安與對策資訊辦公室(Office of Security and Strategic Information)
OTT 過頂(Over The Top)
RID 即時跨間防禦(Real-time Inter-network Defense)
SDN 軟體定義網路(Software Defined Networking)
SGDSN 國防和國家安全局秘書長(Secretariat-General for National Defence and Security)
STIX 結構性威脅資訊表示(Structured Threat Information eXpression)
TAXII 指標資訊的可信自動交換(Trusted Automated eXchange of Indicator Information)
TC 技術委員會(Technical Committee)
TLD 頂級網域(Top-Level Domain)

4 NIS 指令之概論

4.1 NIS 的背景

NIS 指令(NISD)側重在加強國家層級的網路主管機關，增加彼此間之合作，並為主要產業引進安全規定。

NIS 指令有兩個主要目標 [i.5]：

1) 確保國家主要基礎建設有高度的網路安全；
2) 建立歐盟成員國之間的有效合作機制，以進一步達成此一目標。

網路資訊安全領域是多象限網路安全領域的許多象限之一，可以具體化成以下一系列的相關問題：

a) 何謂網路安全？
b) 受影響之人或事？即何謂網路環境？
c) 能夠採取的保護措施？
d) 能夠偵測威脅的方法？
e) 能夠阻止和進行其他補救方法？
f) 有哪些法律救濟？

NIS 的範圍與網路安全的範圍有相當程度的重疊，但 NISD 著重在問題 c)、d)與 e)。事實上，需要考量全部 6 個問題以保證 NIS 具備 NISD 各條款的規定。網路安全領域中各網路 NISD 的關係，如以下圖 1 所示：

Cyber security：網路安全
Focus of the directive：指令重點

(1)何謂網路安全？
Freedom from harm or danger: 免於傷害或危險
Minimizing threats to the cyber environment: 將對網路環境的威脅降到最低
What causes？造成原因
Unintentional threats：非故意的威脅
Intentional threats：故意的威脅
Risk analysis：風險分析
Protective measures：保護措施
Detection measures：偵測方法
Remedial measures：補救方法

(2)受影響之人或事？(網路環境)？
Persons：人
Objects：事物
Infrastructure including SCADA：基礎建設(含 SCADA)
Extrinsic actions and consequences：外來行為與後果
Resources and assets：資源與資產

(3)能夠採取的保護措施？
Resilient infrastructure：彈性/迅速恢復精力的基礎建設
Network/ application integrity：網路/應用完整性
Encryption/ VPN (esp. for signaling) ：加密/虛擬私有網路(VPN) (特別是信令)
Identity management：身份管理
Routing & resource constrains：路徑與資源限制
Data retention and auditing：數據保存與審計

Real-time data availability：即時數據可用性

(4)能夠偵測威脅的方法？

Forensic analysis：辯論分析

(5)能夠阻止和進行其他補救方法？

Investigatory measures：調查手段

Blacklist / whitelist：黑名單/白名單

(6)有哪些法律救濟？

Contractual service agreements and federations：外包服務協議與聯盟

Tort：侵權行為

Intergovernmental agreements and cooperation：跨政府部門協議與合作

Regulatory/ administrative law：法規/行政法

Criminal law：刑法

Provide data for analysis：提供分析用數據

Provide basis for actions：提供行動基礎

Reputation sanctions：聲譽制裁

Deny resources：拒絕資源

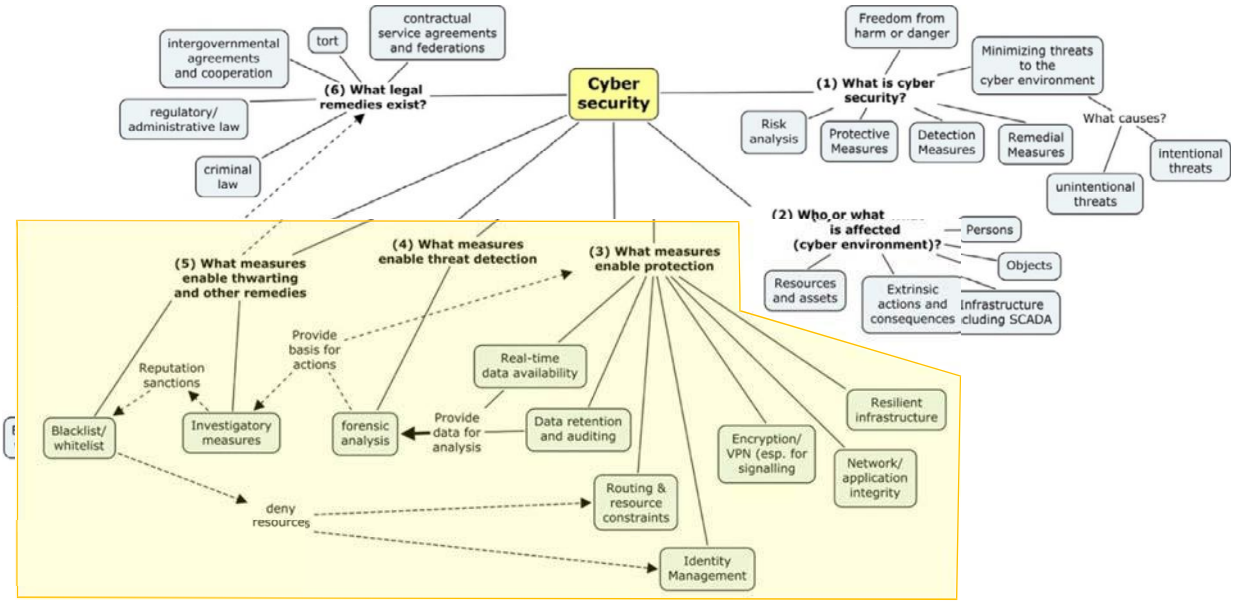


圖 1：NISD 與網路安全關係的可視圖 [i.2]

對抗網路與資訊系統攻擊的防禦與任何其他系統有一樣的基本架構模組。安全風險評估與管理經典的機密性、完整性、可用性(Confidentiality, Integrity, Availability, CIA)模組，構成眾所周知的(威脅、安全象限 security-dimension、對策)三元素，例如攔截、機密性和加密。CIA 模式的作用最常發生在兩方面：

- 風險分析；以及
- 對策部署。

CIA 模式一體適用於 NIS 與其他任何網路安全領域。

從圖 1 可以看出，各方塊之間需要有大量的結構化資訊交換活動。關於表 1 列舉的結構資訊交換需求，NIS 指令內已明定了相關條款。

表 1：NIS 指令中，有關結構化網路安全資訊交換的條款

防禦措施資訊	關於風險 (靜態的)： • 關於網路與資訊系統提供或可存取的數據或相關服務，基於特定之可信度為前提，抵制任何危及該數據或相關服務所儲存或傳送或處理之可用性、真實性、完整性或機密性的行為 (第 3 條) • 管理對網路與資訊系統安全等構成的風險，確保網路與資訊系統的安全層級與呈現的風險相當，以預防並分析涉及網路與資訊系統安全的資安事件影響力(第 14 與 15 條) 關於資安事件處理 (動態的)： • 支援資安事件偵測、分析、遏制與回應的所有 程序 (第 3 條)
網路安全風險資訊	可能對網路與資訊系統安全有不利影響，且可合理識別的任何情況或資安事件(第 3 與 8 條)
資安事件資訊	實際上對網路與資訊系統安全有不利影響的任何資安事件： • 已知資安事件的性質，例如安全違反(security breaches)的類型(第 8a 條 3c 前言) • 有助於資安事件有效處理的資訊 (第 14 條 2a) • 使主管機關或 CSIRT 能夠判定資安事件的跨境影響(第 14 條 2)，包
備註： 表 1 引用文件請參照 [i.1]。	

這些條款構成本文件中多數指導原則的基礎。雖然 NIS 指令要求資訊分享，然而我們並不預期受 NISD 規範的組織會實施一套不受監管的自動化系統，向其監管機關或成員國(Member State, MS)主管機關通報，但希望能以某種形式自願分享威脅情報。實施 NISD 之際，強制通報與自願分享之間有很重要的差異，因此，任何準則都應為自願合作和分

享威脅情報保留空間。

4.2 ENISA 對標準化的建議

歐盟網路與資訊安全局(ENISA)在 NIS 標準化差異報告中提出以下建議，可用來擴大資訊分享的技術基礎 [i.2]：

- 根據全球認可的 STIX/TAXII/CyBOX 平台採用威脅交換的開放標準，作為數據語法和語義及必要傳輸協定之 EN 定義，與實施該標準的附屬指南。
- 擴大現行標準定義之風險分析與防禦措施能力，以解決成員國為減緩國家與區域層面的風險所需要的條款。應作為擴大現有的 ETSI TS 102 165-1 [i.7]、ETSI TR 103 305 [i.3]、ISO/IEC 15408 [i.25] 與相關 ISO/IEC JTC1 27000 系列標準 [i.16]能力 EN。

值得注意的是，不太可能將 NIS 與資訊與通訊組織(ICT)標準機構已制定之大量網路安全通用條款做區別。另外，網路資訊基礎建設(Network Information Infrastructure, NII)、NIS 與網路安全在提供資源、攻擊來源或防禦措施方面在地理上無法相互孤立，而為有效實施國家資訊安全而必須分享資訊時應考量到這種分散帶來的複雜性。因此，NII 許多功能將利用全球市場上的軟體與硬體來實現。

4.3 個人資料之處理

NIS 指令於第 2 條規定處理個人資料應按照指令 95/46/EC [i.26]與法規 No 45/2001 [i.27]，並根據第 15 條規定與個資保護主管機關配合，不得以其他方式威脅個資所有人。如 NIS 解譯性前言所述：「*很多情況下，資安事件會造致個人資料之損害，因此，主管機關及個資保護機構應合作並交換所有相關資訊，以著手對付因資安事件造成的個資侵害*」[i .1]。至於，合作的相關規定則出現在前言條款(72) [i. 1]。因為 NIS 指令之目的亦在滿足這些相同規定，以簡化 NIS 指令的附屬條款，故本文並不探討有關個資的保護。

5 網路威脅情報分享：資安事件與風險

5.1 簡介

5.1.1 背景

本條用於實施表 1 各項列舉條款產生於 NIS 指令的資安事件通報規定。此外，NIS 指令第 7 條規定此應作為國家「*確定實現及維持網路與資訊系統高度安全性的戰略目標及適用政策與監管措施*」政策的一部分[i.1]。

某些實施也需要限定對象。例如：在 NIS 指令第 14(3)條規定：關鍵服務業者「*通報(不得無故拖延)主管機構或電腦資安事件應變小組(CSIRT)會嚴重影響其繼續提供關鍵服務*

的資安事件」。再者，在 NIS 指令第 14(4)條指出受關鍵服務中斷影響的使用人數、資安事件持續時間，與資安事件影響區域的地理分佈，都可能是判定某一資安事件影響是否「*嚴重*」的相關標準。雖然未賦予義務，指令仍強調「*資安事件的相關資訊對一般大眾和產業越來越有價值，特別是中小型企業*」[i.1]。

實行資安事件通報規定時遵循以下的典範實務是很重要的，能夠讓主管機關或電腦安全資安事件小組(*CSIRT*)採取行動以減少重大資安事件的影響，同時亦不會使該機關／電腦安全資安事件小組(CSIRT)負擔過重或造成額外的生態系統風險：

- 依規定(根據國家法律)，關鍵服務業者和數位服務提供者必須通報的資安事件，其通報範圍應侷限在夠小的範圍內，以避免與歐盟其他法律和法規重疊或導致通報規定重覆；

- 若規定應通報時，應考量不同風險與重要性，以及不同服務支援技術架構的多樣性來制定通報門檻；以及

- 關於關鍵服務業者，限定及架構資安事件通報門檻的國家方法需要充分協調一致，以便讓這些業者的安全應變小組集重著力在從資安事件中恢復，而非遵守零散的規定。

5.1.2 資安事件範圍

依 NIS 指令關鍵服務業者需要通報的資安事件應侷限在夠小的範圍內，以避免與歐盟其他法律和法規*重疊*或導致通報規定重覆。特別是，適用報通規定的範圍不應與歐盟 GDPR 的規定重疊，避免發生一次資安事件卻必須向多個監管機構進行多次揭露，造成效率低下與資源分散。舉例來說，為 GDPR 資料違反通報規定所涵蓋之機密性違反資安事件。

根據第 14(3)條，NIS 指令之資安事件通報規定涵蓋：對關鍵服務業者(重點強調)而言「*嚴重影響關鍵服務**連續性**的資安事件*」(重點強調)。NIS 指令第 16 (3)條規定，數位服務提供者通報「*對提供服務有實質影響的資安事件*」[i.1]。服務的連接性，係指他們能夠隨時支援使用者存取他們及／或依賴他們的可用性。相反的，違反連接性則可能影響使用者機密保障的能力，但未必影響使用者存取資訊或服務的能力。

此外，如同第 4 條對資安事件的定義一般，NIS 指令之資安事件通報規定應侷限在有「實際不利影響」的資安事件。可能造成影響的資安事件(例如試圖違反)則不在通報規定的適用範圍內，以便確保主管機關／CSIRTs 不會被不重要的資訊淹沒，而是獲得更多具優先性且可依法追訴的資訊。另外，對於關鍵服務業者和數位服務提供者隔離惡意攻擊和減輕網路入侵影響的策略，與其相關的這些優先保護資訊，如果暴露給攻擊者，可能會助長他們更快速、更有效地發展攻擊性技術。

5.1.3 資安事件通知門檻

何種資安事件符合第 14(3)條敘述的「嚴重影響」可能因服務和技術架構而異。因此，NIS 指令之資安事件通報門檻應考量不同關鍵服務的不同風險與標準，以及不同服務支援技術架構的差異。具體而言：

- 在不同情況下，受關鍵服務中斷影響的相關使用人、資安事件影響區域的地理分佈，與資安事件持續時間的重要性可能不同。例如：對於信貸機構的網頁來說，其連續性／可用性的影響，就不同於石油生產、精煉、儲存或傳輸業者網頁的連續性／可用性。
- 考量 NIS 指令衡量資安事件影響嚴重性的標準，對於不同的服務提供者及在不同等級的基礎建設上，「使用者」與「地理影響」可能有不同意義或有不同的測量方式。某些情況下，對關鍵服務業者而言，將「使用者」當成「使用情況」而非個人可能更為相關。其他情況下，根據歐盟的隱私權法案，可能限制關鍵服務業者追蹤作為客戶的「使用者」，這可以係指數個個人的終端用戶，而不是每個個人的終端用戶。同樣的，根據提供服務的方式，關鍵服務業者有不同量測資安事件地理影響的方式，而(例如)這種方式可能與國界不一致(例如以特定數量的國家受影響作為通報資安事件的門檻)。再者，為滿足各項需求的彈性活動，對受影響的「使用者」人數，或受影響的「地理」範圍的衡量，可能會隨著時間而改變。

確保對不同服務與架構進行適當校正，符合 NIS 指令以風險為基礎的明文規定，即對不同類型服務的處理方式，應根據其暴露的風險而為。

此外，判定引發連續性／可用性「中斷」的標準亦應符合較高的門檻，以優先化並確保能著重在重要資安事件上。換句話說，判定嚴重影響的門檻只可以是：當整個服候或服務的核心功能受影響時。既使是大範圍的非核心功能或附屬功能(即服務的非主要功能)被中斷或中斷時間很長，皆不應視為達到通報的門檻。同樣的，只有資安事件出現但尚未因容錯移轉而被吸收時，才需要衡量對關鍵服務的影響與適用資安事件通報的規定。除非有實際且需通報的影響結果，否則不需要通報該資安事件。

考量到不同背景對於政府衡量影響關鍵服務業者之資安事件重要性的影響，可以透過從產業角度建立的公私合作關係制定相關規定。尤其是，對於關鍵服務業者以及經常支援可能適用通報規定之服務的技術提供者(例如新成立的 NIS 合作小組)，可以利用其觀點以確保這些規定的範圍與門檻，足以讓通報有助於主管機關／CSIRT 履行其任務，同時不會讓生態系統面臨更高的風險。

5.1.4 方法之協調

界定範圍與架構化資安事件通報門檻的方法應妥善協調，以使關鍵服務業者的安全反應小

組能專注在資安事件反應與從資安事件中恢復，而不是忙著遵守分散的規定。若資安事件通報規定的範圍夠窄，不同服務適用其相關的門檻，則各規定可能朝向略為一致的方向前進。持續致力於協調，將帶來更高效率與跨境合作。

5.1.5 資安事件分類指標及度量

對組織／公司與國家來說，一個簡單又高標準的資安事件分類與相關指標和度量，對衡量其安全管制的有效性、對其整體安全裝置取得共識，以及(可能)根據最新統計數字進行自我評量皆越來執重要。今日，幾乎一致認可這種快速達成網路安全真正量化的方法。這些指標應置於一般參考架構通用管制的相關級別(如第 6 條所述)，而結構化威脅情況交換(STIX)中可見更詳細、更多的技術資安事件分類則置於更低級別，以增加統計數字生產的可能性[i.6]。有了 ETSI 資訊安全指標(ISI)即可以藉此產出標準化度量[i.19]。

5.2 概念、模式與技術方法

從歷史上來看，有關資安事件、弱點、風險與救濟等資訊形式的網路威脅情報，通常是非結構化且只限於組織或產業範圍中流通。運用傳統電信網路廣泛、快速交換這些資訊的需求，現在可以透過電話和電子郵件寄送稽核資訊的方式完成。直到以廣泛分布的網際網路協定為基礎的網路出現，因為有越來越多的攻擊和其他資安事件發生，才需要擷取及交換威脅情報。附錄 A 是敘述了簡要的歷程。

在過去五年中，結構化威脅情報交報(STIX)平台，以及其對指標資訊的可信自動交換(TAXII) 和網路可觀測資安事件表達(CybOX)的下行規範已成為不同產業及政府機構之間交換網路威脅情報的主要方式，而其亦持續在 OASIS 內部發生演變[i.6]。STIX 通常被認為是滿足諸如 NIS 指令條款與 ENISA 專案技術報告等網路威脅情報規定的主要通用手段[i.2]。

5.3 網路威脅情報的組織實務

5.3.1 簡介

NIS 指令明定的各個部門，對於交換網路威脅資訊通常有自己的規則與做法 – 雖然如第 5.2 條所述有朝通用模式及表達方法演進的趨勢。 圖 2 描述了這些組織的數量與多樣性。本文件試圖就可用產業規範如何讓這些組織根據 NIS 指令交換威脅情報及防禦資訊的共同操作提供指導。

European union 歐盟

European commission 歐盟委 會

European network and information security agency 歐盟網路與資訊安全局

Cooperation group 合作小組

Network and information security committee 網路與資訊安全委員會

Member state 成員國
Competent authority 主管機關
Computer security incident response team 電腦安全資安事件反應小組

Excluded from the Directive 排除於指令外
Ref: Official Journal of the European Union, 17 Jul 2016 參考文件：2016 年 7 月 17 日歐盟公報

Public or private entity 公有或私有組織
Operator of essential services pursuant to art. 14 2 and 2ac + annex II
根據第 14 條 2 與 2ac 及附錄 II 定義的關鍵服務業者
1. Energy 能源
2. transport 運輸
3. banking 銀行
4. financial market infrastructures 金融市場基礎建設
5. health sector 健康產業
6. drinking water supply and distribution 飲用水供應與分配
7. digital infrastructure 數位基礎建設
Third party 第三方
Qualified auditor 合格審計師

Digital service providers pursuant to art. 15a 2+annex III
根據第 15a 條 2 及附錄 III 定義的數位服務提供者
1. online marketplace 線上市集
2. online search engine 線上搜尋引擎
3. cloud computing service 雲端運算服務
Representative for a for a digital service provider 數位服務提供者的代表人
Micro and small enterprises 微型與小型企業
General publicand businesses, particularly small and medium-sized enterprises
一般公司，特別是中小企業

Public electronic communication networks or publicly available electronic communication service providers under EU Directive 2002/21/EC
歐盟指令 2002/21/EC 規定之公共電子通訊網路或供公眾使用之電子通訊服務提供者
Trust service providers under Regulation 910/2014 of the European Parliament and of the Council of 23 July 2014
2014 年 7 月 23 日歐盟議會與理事會法規 910/2014 規定之信賴服務提供者
Others not identified 未提及的其他組織

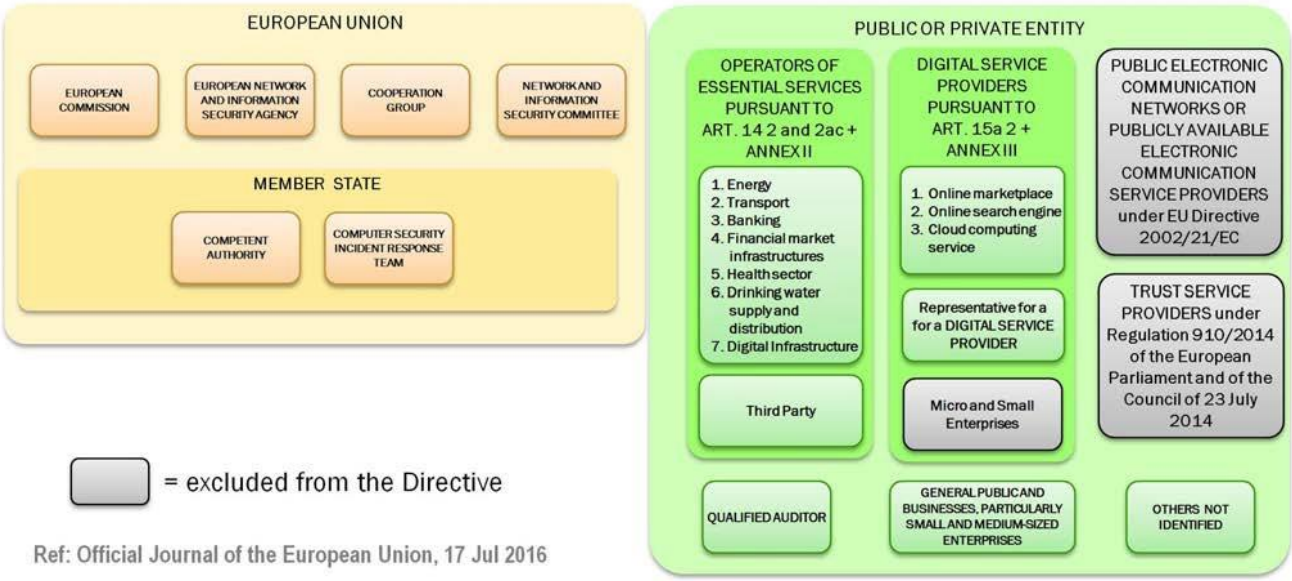


圖 2：認定涉及網路威脅情報交換的 NIS 指令組織

5.3.2 關鍵服務業者

根據第 14-15 條及附錄 II，關鍵服務業者在 NIS 指令中有其他論述[i.1]。這類業者包括能源、運輸、銀行、金融市場基礎建設、健康產業、飲用水供應與分配，以及定義為包含資訊交換站(IXPs)、網域名稱系統(DNS)服務提供者及頂級網域(TLD)名稱登記處的「數位基礎建設」。

這些產業中的威脅情報分享通常仰賴於專門且通用的封閉平台和資訊分享與分析中心(ISACs)。有些如第 5.3.4 條所述。然而，越來越多的這些服務正朝向通用的共同操作式平台，例如結構性威脅資訊表示(STIX)[i.6]。

5.3.3 數位服務提供者

同樣的，根據第 16-17 條及附錄 III 數位服務提供者在 NIS 指令中也有其他論述[i.1]。有些提供者被定義為包含「線上市集、線上搜尋引擎，以及雲端運算服務」的服務。這些產業中的威脅情報分享通常亦仰賴於專門且通用的封閉平台和資訊分享與分析中心(ISACs)。有些如第 5.3.4 條所述。然而，越來越多的這些服候正朝向通用的共同操作式平台，例如結構性威脅資訊表示(STIX)[i.6]。

5.3.4 專門、有限使用、結構化的威脅情報分享平台

專門且有使用限制的威脅情報分享平台及活動部分示例如後。若確認平台已發布的資訊性引用文件，則可在 ETSI TR 103.331 [i. 6]找到。

- **IODEF 與 RID**：國際資安資安事件訊息交換格式(Incident Object Description Exchange Format, IODEF)與即時網間防禦(Real-time Inter-network Defence, RID)是最早、也最普

遍的結構化威脅情報交換平台 – 可追溯到最早成形的網路電腦緊急資安事件反應小組(CERT)，且多數到今日仍然存在。這些規範已發展演變為國際網路工程研究團隊(IETF)輕量級交換託管資安事件(MILE)委員會的 RFC，並在 ITU-T X.1500 CYBEX 系列建議書中重申[i. 28]。

- **CSAF 與 CVRF**：有些供應商及提供者社群已使用共通弱點通報架構(Common Vulnerability Reporting Framework, CVRF)若干年，現在已被資訊標準架構促進會(OASIS)標準化成共通安全諮詢架構(Common Security Advisory Framework, CSAF)。

- **NATO CDXI 與 NCIRC**：荷蘭海牙的北大西洋公約組織(NATO)的通訊與資訊局網路防禦及保證資訊分享，網路防禦資料交換與協力基礎建設(Cyber Defence Data Exchange and Collaboration Infrastructure, CDIX)為北大西洋公約組織(NATO)電腦資安事件應變小組能力(NCIRC)的一部分，而在北大西洋公約組織(NATO)成員國內，網路防禦資料交換與協助基礎建設(CDXI)用於交換網路安全情報。

- **CTIP**：網路威脅情報計劃(Cyber Threat Intelligence Program, CTIP)是美國衛生與公眾服務部、資安與對策資訊辦公室(Office of Security and Strategic Information, OSSI)於 2014 年所制定。資安與對策資訊辦公室(OSSI)的網路威脅情報計劃(CTIP)監測與分析各方面有關醫療衛生與公共衛生領域的網路威脅情報；及時提供可依法起訴的網路威脅資訊；以及徵求該領域的回饋與資訊需求。

- **MISP**：惡意軟體資訊分享平台(Malware Information Sharing Platform, MISP)是由一群創建開放式威脅資訊分享工具的開發者所提倡。隨著惡意軟體資訊分享平台(MISP)的擴張，該平台不僅涵蓋惡意軟體指標，也涵蓋詐欺或漏洞的資訊。此一平台還包含了核心的惡意軟體資訊分享平台(MISP)軟體及大量支援用工具和格式(核心格式、MISP 分類法、警告清單)。本平台為某些電腦安全事件應變小組(CSIRTS)所使用。

- **MAPP**：成熟度評估、側寫、計劃(Maturity Assessment, Profile, Plan, MAPP)是一種結合其他威脅分享度量以產生現況報告的專有分析引擎。

- **MSRC 與 OpenIOC**：微軟資安應變中心(Microsoft Security Response Center, MSRC)與開放感染指標(Open Indicator of Compromise, OpenIOC)分別屬於微軟資安技術中心及 Mandiant(FireEye 資安公司)專有的威脅情報交換平台。兩者皆為關鍵服務業者及數位服務提供者使用的眾多選擇之一。

- **MACCSA**：協作式網路情境意識多國聯盟(Multinational Alliance for Collaborative Cyber Situational Awareness, MACCSA)曾是一個實驗項目，指在鼓勵使用結構化表述來交換威脅情報。

6 風險分析在保護 NIS 所扮演的角色

6.1 簡介

本條涉及實施表 1 許多不同條款的 NIS 指令的網路風險管理規定。指令要求關鍵服務業者(OES)與數位服務提供者(DSP)實施網路風險管理措施。對於關鍵服務業者(OES)，NIS 指令第 14(1)條規定「*成員國應確保關鍵服務業者確認並採取適當技術與組織性措施，管理其營運所用之網路與資訊系統的安全風險……考量到最新技術，這些措施應確保網路與資訊系統的安全水準與其所曝風險相當*」[i.1]。

關於數位服務提供者(DSP)，指令第 16(1)條也有類似規定(儘管受到前言(49)、(60)與(66)的 DSP 低干涉方法的規範)：「*成員國應確保數位服務提供商確認並採取適當技術與組織性措施，管理其於本聯盟內提供如附錄 III 所述服務所用之網路與資訊系統的安全風險…考量到最新技術，這些措施應確保網路與資訊系統的安全水準與其所曝風險相當，並且應考量以下因素：(a)系統與設施的安全；(b)資安事件之處理；(c)業務連續性管理；(d)監督、稽核與測試；皆符合國際標準。*」

網路安全風險管理是一種有關評估組織環境風險、了解對組織至關重要的資產、資源及程序，並採取確保組織持續改善其保護、偵測威脅與應變與其資產、資源及程序相關資安事件的辦法。在 NISD 與第 14(1)及 16(1)條的背景下，網路安全風險管理實務與安全措施相關，應著作這些步驟的重要性，而非規定實施對技術生態快速發展而言不夠靈活動規範性安全控制。

產業經驗已從網路安全風險所習得的教訓中[i.9]，衍生出一套有關安全措施的最佳實務與原則，其特點有 [i.18]：

•**風險基礎**：由於了解沒有組織能擁有無限的安全資源，故風險基礎與優先化安全措施將確保組織能夠做出與其各種風險環境最相關的安全調查決策。風險基礎與優先化安全措施能夠反映出組織的特定業務動力與安全考量。

•**促進溝通**：清楚明定優先化網路風險管理最佳實例的安全措施，其亦應以能促進溝通的制定方式，建立可用於安全人員、管理人員和行政人員以及供應商與買方之間的共通語言及參考點，加速組織內外的跨境溝通。特別是建立共通語言將有助於加速組織內橫向和從向交流，使行政人員得以更好地了解網路風險管理工作，並做出更明智的安全資源決策。

•**注重成果**：注意成果的方式提供組織在管理安全上有足夠的靈活度，以配合不斷變化的威脅及技術發展。

•**靈活性**：靈活的安全措施著重在網路風險管理程序，允許組織隨著時間將新習得的教訓融入

這些程序。這個程序中有一些關鍵要素，包括有負責計劃、開發、實施、測試、審閱及改善網路安全風險管理程序的正式負責人。

ETSI TS 102 165-1 處理方法第 6 條 [i. 7]提出對風險計算有用的成本效益分析。

起點應為跨部門的安全措施基準點，亦即將會有許多跨部門的安全措施。接著，可能有其他適用於特定部門的安全措施，這應該置於跨部門的基準點之上。跨部 門的基準點能支援政府安全評估人員與相互依賴部門間的效率。此外，也支持在政府與產業利害關係人間分享更多資訊與最佳實例。同時，在跨部門基準點上靈活地增加適用特定部門的相關安全措施，亦能確保能夠解決關於特定部門的風險。

6.2 概念、模式與技術方法

6.2.1 簡介

網路安全管理概念、模式及技術方法的大部分歷史，與第 5.2 條所述的網路威脅情報分享歷史類似。ETSI 及國際電信聯盟電信標準化部門(ITU-T)皆公布了一套網路風險管理的通用方法，例如重點資安控制項目。此外，其他諸如北大西洋公約組織(NATO)與共同準則發展委員會(CCDB)等專門機構公布的全球規範(如共通標準)，及國家主管機關制定的框架 – 如第 6.2.3 條所述。這些方法的細節層級與實施準則皆有不同。

這些網路安全方法很有用，因為它們解決了適用於多種環境的一系列風險與防衛措施。由於許多組織利用來自其部門和組織的技術及資源，而通用基準能滿足這些組織對供應商監管或契約的需求，並推動對個生態系統的網路安全最佳實例。因為越來越多的垂直部門進行橫向整合，所以跨部門方法特別具有價值。基準點可以確認各部門共同的最低要求，並根據部門的具體需求斟酌補充。

發展國家策略需要一致、跨越世代的方法，以確認、評估及管理風險與評估方法的實施狀況。在支援整個組織的協調以及能夠從內部衡量進度兩方面，方法的一致性是很重要的；而由於技術生態系統和威脅環境都在不斷發展中，方法能跨越世代也很重要。新技術為既有風險與新風險帶來其他的管理方式，而新威脅亦需要不同的風險緩解技術。

無論是置入網路安全架構或作為安全措施的基準點，整套的政策、成果、活動、實踐與控制都有助於網路安全的風險管理。系統安全、注意成果的方法可鼓勵需要採取可行措施的組織流程和控制。它們是互補助且有價值的零件。

6.2.2 重點資安控制項目

ETSI TR 103 305 [i.3] 及相關實施準則，提供了可廣泛利用的有效、可實施的控制方法。

ETSI 控制項目及相關實施準則由網際網路安全中心(Center for Internet Security, CIS)(一家獨立、專家、全球性的非營利組織)所開發與維護，並由 ETSI 制定，擷取並敘述前二十家企業產業級的網路安全最佳實踐以提升的網路安全。網際網路安全中心(CIS)持續開發、支援、正式通過與使用重點資安控制項目。控制項目反映了對網路安全生態系統各部分的實際攻擊與有效防禦的綜合知識，以確保控制項目是一套有效且具體的技術措施，可用於偵測、防止、應變及緩解這些攻擊帶來的損害。

控制項目不限於阻止系統受損，還涉及偵測已受損的機制，以及預防或中斷攻擊者的後續行動。透過這些控制項目所給定的防禦措施有：加強設備配置以減少初始攻擊的影響層面，確認受損機制以解決組織內部網路的長期威脅、中斷攻擊者植入惡意程式碼的指令與控制，以及建立可以維護及改進的、適合的、持續性的防禦及應變能力。重點資安控制項目揭示的有效網路防禦系統，其五個關鍵原則是：

•攻擊告知防禦：利用已損害系統的實際攻擊的消息，提供持續從這些資安事件中學習的基礎，以建立有效、實用的防禦方法，但僅限於已知可以阻止實際攻擊的控制項目。
•優先化：首先投入能最大程度降低風險及避免最危險威脅，並且能實施於運算環境中控制項目。
•指標：建立共通指標，為行政人員、IT 專家、稽核員及安全主管提供通用的語言，用以衡量組織內部安全措施的有效性，以便於快速地辨別與實行所需的調整。
•持續診斷與緩解：執行持續性的措施來測試及驗證現有安全措施的有效性，並有助於決定下一步驟的優先順序。
•自動化：自動化防禦能讓組織可利用可靠、可擴充及持續性的手段遵循控制項目及相關指標。

為了符合 NIS 指令，控制項目已為某些歐盟國家所採用，這是它的另一項優勢 [i.1]。

6.2.3 跨國家與政府之計畫

雖然，重點資安控制項目提出可適用於 NIS 指令，且最廣泛、可操作的網路防禦機制，但它們在過去幾十年間早已存在於大部分跨國家及政府的政策、架構及計畫。以下將敘述(尤其是對歐盟成員而言)最重要的項目。

共同準則發展委員會(Common Criteria Development Board, CCDB)曾是跨政府網路防禦最早的產物，而因為它著重在關鍵基礎建設上，故到目前為止仍然很重要。資訊技術安全評估的共同準則(以下稱共同準則)係由加拿大、法國、德國、荷蘭、英國及美國政府在 90 年代中期制定。共同準則(CC)係願意統一化安全評估標準，以避免重新評估進入國際市場商品下的產物，而共同準則第 1.0 版於 1994 年公布[i.31]。今日，有 26 個國家參加協定，包括大部分的歐盟成員。目前，共同準則(CC)正在發生重大變化 – 可能朝相容於重點資安控制項目的方式進行。

網路防禦是北大西洋公約組織(NATO)協力防禦的核心任務之一。在網路空間，北大西洋公約組織(NATO)的優先順序是先保護其通訊與資訊系統。盟軍則負責自己的網路防禦，但北大西洋公約組織(NATO)會提供他們多方面的協助，包括：

•透過專門的惡意軟體威脅分享平台，分享有關威脅的即時資訊；
•維持網路防禦小組的快速應變，以協助盟軍處理網路挑戰；
•為協助盟軍網路防禦能力有共同方法而開發目標；
•投入教育、培訓與練習，

與北約組織(NATO)有關的幾個機構也協助聯盟改善網路防禦。位於愛沙尼亞(Estonia)首都塔林(Tallinn)的北約桌越合作電腦防衛中心(Cooperative Cyber Defence Centre of Excellence)是北約認可的研究及培訓機構，負責網路防衛教育、研究和開發。它保留了大量的國家網路防衛戰略與架構以供參考。

表 2：歐洲國家與區域組織計劃與架構

歐洲區域之國	**ETSI EU 成**	**EU 成員**	**申根區**	**EFTA**	**歐洲理事**	**NATO 成員**	**CCRA 成**
阿爾巴尼亞 Albania	X	T			X	X	
安道爾 Andorra		O			X		
亞美尼亞 Armenia		O			X		
奧地利 Austria	X	X	X		X		C
亞塞拜然 Azerbaijan		O			X		
比利時 Belgium	X	X	X		X	X	
布魯塞爾 Belarus		O					
波士尼亞與赫塞哥維納 Bosnia & Herzegovina	X	P			X		
保加利亞 Bulgaria	X	X			X	X	

歐洲區域之國	ETSI EU 成	EU 成員	申根區	EFTA	歐洲理事	NATO 成員	CCRA 成
克羅埃西亞 Croatia	X	X			X	X	
塞普勒斯 Cyprus	X	X			X		
捷克共和國 Czech Republic	X	X	X		X	X	C
丹麥 Denmark	X	X	X		X	X	C
愛沙尼亞 Estonia	X	X	X		X	X	
芬蘭 Finland	X	X	X		X		C
法國 France	X	X	X		X	X	A
喬治亞 Georgia	X	O			X		
德國 Germany	X	X	X		X	X	A
希臘 Greece	X	X	X		X	X	C
匈牙利 Hungary	X	X	X		X	X	C
冰島 Iceland	X	O	X	X	X	X	
愛爾蘭 Ireland	X	X			X		
義大利 Italy	X	X	X		X	X	A
哈薩克 Kazakhstan							
科索夫 Kosovo		P					
拉脫維亞 Latvia	X	X	X		X	X	
列支敦斯登 Liechtenstein		O	X	X	X		
立陶宛 Lithuania	X	X	X		X	X	

歐洲區域之國	ETSI EU 成	EU 成員	申根區	EFTA	歐洲理事	NATO 成員	CCRA 成
盧森堡 Luxembourg	X	X	X		X	X	
馬其頓 Macedonia (FYROM)	X	C			X	A	
馬爾他 Malta	X	X	X		X		
摩爾多瓦 Moldava	X	O			X		
摩納哥 Monaco		O			X		
蒙特內哥羅共和國 Montenegro	X	T			X		
荷蘭 Netherlands	X	X	X		X	X	A
挪威 Norway	X	O	X	X	X	X	A
波蘭 Poland	X	X	X		X	X	
葡萄牙 Portugal	X	X	X		X	X	
羅馬尼亞 Romania	X	X			X	X	
俄羅斯 Russia	X	O			X		
聖馬利諾 San Marino		O			X		
塞爾維亞 Serbia	X	T			X		
斯洛伐克 Slovakia	X	X	X		X	X	
斯洛維尼亞 Slovenia	X	X	X		X	X	
西班牙 Spain	X	X	X		X	X	A
瑞典 Sweden	X	X	X		X		A

歐洲區域之國	ETSI EU 成	EU 成員	申根區	EFTA	歐洲理事	NATO 成員	CCRA 成
瑞士 Switzerland	X	O	X	X	X		
土耳其 Turkey	X	T			X		A
烏克蘭 Ukraine	X	O			X		
大英國協 United Kingdom	X	X			X	X	A
梵帝岡 Vatican City		O					
備註： 代碼 X = 成員 T = 轉化中 O = 可能成員 A = 授權成員 C = 消費成員							

過去十年來，國際電信聯盟電信標準化部門(ITU-T)與多個網路防禦機構與計劃建立了合作關係，並與北約、資安事件應變小組論壇(FIRST)、指標資訊的可信自動交換、國際網路工程研究團隊(IETF)及其他組織合作發布許多資訊保證處(Information Assurance Directorate, IAD)D的單項優勢軟體(best-of-breed, BoB)，和作為國際電信聯盟電信標準化部門(ITU-T)標準的國際資訊安全弱點認定機構(MITRE)平台。請見 ITU-T X.1500 系列建議書規範[i.28]– 尤其是有關漏洞及國家資訊交換的部分[i.6]。關於國家層面，大部分歐盟成員皆有網路防禦計劃與架構。其中，有幾個值得注意的：

英國國家網路安全中心(UK National Cyber Security Centre, NCSC)最近為其長久以來的國家基礎建設保護中心(CPNI)計劃加入了四個新創建的主動性網路防禦計劃，其包括：受保護的網域名稱系統(DNS)、基於網域的訊息認證、通報及一致性(DMARC)反偽造信件、網路檢查及釣魚網站和惡意軟體的緩解措施。在美國資訊保證處(IAD)開發後不久，國家基礎建設保護中心(CPNI)就頒布了自己版本的重點資安控制項目，作為可跨組織適用之高優先度資訊安全措施及控制項目，用以改善其網路防衛。在 NIS 指令下，它是英國架構的核心部分。

在法國，2013 年的國防與國家安全白皮書制定了其關鍵基礎建設的保護政策，作為強化國家復原力的手段。關鍵服務業者作為本系統的關鍵需要分析其所面臨的風險，並在其職責範圍內實施保護措施 – 特別是反恐安全計劃(VIGIPIRATE plan)。該政策包含永久性安全立場(網路安全)，並且納入專門針對威脅變化的加強保護措施。關鍵服務業者(OES)採用其產業限定的資訊技術安全措施。該政策在總理與國防和國家安全秘書長 Secretary General for Defence and National Security, SGDSN)之下，建立了由六個部分組成的全國網路與資訊安全局(National

Network and Information Security Agency, 簡稱 ANSSI)：

1)加強資訊系統安全；
2)加強網路安全研究；
3)強化人力的教育與培訓；
4)發展網路防禦中心；
5)推動國際合作；以及
6)促進產生國家網路防禦社群。

在德國，新成立的國家網路防禦中心是為應變德國政府電腦攻擊而成立的政府機構。無論是 2005 年針對政府與產業之「資訊基礎建設保護國家計劃」 [i.32]或是 2007 年「關鍵基礎建設保護(Critical Infrastructure Protection, CIP)實施計劃」[i.33] ，皆涉及 IT 危機應變並且為企業發生重大網路事件時，其關鍵業務流程的連續性管理提供建議。德國聯邦資訊安全局(German Federal Office for Information Security, BSI)作為國家網路安全機構，持續不斷地為德國及中央網路資安事件通報辦公室發布多項與網路防禦相關的德國聯邦資訊安全局(BSI)標準。

在適用 NIS 指令的實施範圍內，其他重要的網路防禦計劃及架構包括：

•澳大利亞信號理事會(Australian Signals Directorate)之減少網路資安事件的戰略(Strategies to Mitigate Cyber Security Incidences) ，以及保護資訊與通訊技術(Information and Communication Technology, ICT)系統的「前四項」和「主要八項」緩解政策，加上預防傳輸與執行惡意軟體的緩解政策的其他準則，以限制網路安全事件的範圍，並且偵測網路安全事件和應變。

•美國國防工業基地(U.S. Defense Industrial Base, DIB)電腦安全計劃，允許讓符合條件的國防工業基地(DIB)參與，以接收政府提供的資訊，以及來自其他參與之國防工業基地(DIB)的網路威脅資訊，藉此更深入了解敵對活動。這些平台是由多個美國政府的資安機構所開發的，提供資訊保證諮詢與許多其他的網路防禦資訊。

•美國 NIST 網路安全框架 [i.29] 是一套風險管理的操作框架，旨在幫助組織評估及改善資產和網路之辨認和保護、偵測異常情形與事件、以及回應和自事件中恢復的能力。該框架「提供網路安全成果的高階分類法，以及評估和管理這些成果的方法」，使組織能將網路安全風險管理整合入更廣泛的企業風險管理職能中，並領導安全優先事項及所需的投資。由於它具備風險基礎與注意成果的特質，它亦能使組織靈活地實施，持續改善其網路風險管理。於 2014 年公布的第 10 版，最初係針對關鍵基礎建設的業者，但它對被大部分主動進行風險管理的企業、甚至是政府組織所採用。ETSI TR 103 305-4 [i.30] 描述了 NIST 框架下控制項目的資訊性參考文件，以實施實際網路防禦能力 [i.3]。

6.3 網路防禦與網路安全風險管理實踐

6.3.1 簡介

與基準安全措施相關的網路防禦與網路安全風險管理實務，應著重在建立一套納入控制項目的安全風險、注意成果的架構或基準。此種方法能確保從一開始就將風險管理程序融入組織實務中。

從 1980 年代後期開始，整個電信／資訊與通訊技術(ICT)社群開始著手風險管理的多重安全管理、注意成果的規範，其中包括成立新團體以及在 1990 年代發布大量規範，一直持續到今日[i.9]至[i.18]。舉例而言，ETSI 在 1996 年關於安全管理技術的 ETR 介紹並指導如何確認監督和控制系統安全功能所需的安全管理功能，並提供在電信系統三個不同層面上，有系統安全、系統服務及安全機制相關的其他安全管理、注意成果規範的指示[i.8]。

網路安全風險管理的最佳組織實踐圍繞著幾個關鍵概念。如 ETSI TR 103 303 [i.20]所論述，整個保護週期包括：計劃、偵測、反應及恢復。所有措施，包括英國國家網路安全中心(NCSC)、AGDSN／法國全國網路與資訊安全局(ANSSI)與 NIST 的措施，都強調以下功能的重要性：識別、保護、偵測、應變及恢復。ETSI TR 103 303 [i.20] 舉出每個資安事件下的一些重點；例如 ETSI 建議在規範措施時應評估業務目標、資產管理、威脅評估、風險管理及事件應變計算。同樣的，關於識別功能，則有以下幾種措施：資產管理、業務環境、管理支配、風險評估及風險管理政策。這些措施亦包含更多細節及附有資訊性參考文件的子分類。

這種含有更多細節及資訊性參考文件的「事件」或「功能」構造，對組織實施網路安全風險管理實務時很有幫助，因為內部不同的利害關係人得以用適合的角度理解這份準則。作出安全授權決策的主管可理解並追蹤關於事件或功能的組織進度，而資訊安全實踐者能參考更詳細的準則或資訊性參考文件。這種網路安全風險管理的方法是可互相溝通的，並通過建立共同語言與參考點來增進跨界的溝通。

6.3.2 關鍵服務業者

關鍵服務業者的網路防禦及網路安全風險管理實踐通常仰賴專門且通用的封閉平台和資訊分享與分析中心(ISACs)。有些包含於之前討論的平台。然而，越來越多的這些服務正朝向通用的共同操作式平台前進，例如重點資安控制項目。關鍵服務業者的網路防禦及網路安全風險管理實踐應為一種可溝通的架構，它有風險基礎、注重成果且有靈活性。制定這種架構時應該突顯期望的安全成果以及參考可能的實施機制，包括相關控制項目(例如重點資安控制項目)。

6.3.3 數位服務提供者

數位服務提供者的網路防禦及網路安全風險管理實踐應為一種可溝通的架構，它有風險基礎、

注重成果且有靈活性。制定這種架構時應該突顯期望的安全成果以及參考可能的實施機制，包括相關控制項目(例如重點資安控制項目)。

7 問題與解決方案

7.1 簡介

實施 NIS 指令的問題和障礙是多樣化且在不斷地演進中，在這裡不太可能完全涵蓋所有問題。然而，ETSI 年度安全週刊的資料檔案[i.21]指明產業、組織及政府代表提供的最佳、不斷更新的問題與其進行中解決活動的數量，包括 NIS 指令特別關注者[i.1]。最近安全週刊的某些觀點將在後續子條款中提出，而 NIS 指令的相關重點有：

- 網路安全標準基本上無並分歧：
  - 標準太多，而許多標準都不可行或不特別有用。
  - 真正的需求朝向有用、可共同操作的標準
  - 無法線上自由取得、無不斷演進及良好版本管理的標準，降低了其價值且表現出網路安全的障礙。
  - 本份技術報告 (TR)網路安全技術委員會(CYBER)應找到生態系統，並專注在確認受最多產業支援且最有效的平台和規範。

- 沒有簡單或容易的網路安全解決方案：
  - 假使不斷演進的弱點龐大，則不太可能實現網路安全
  - 您可以做的是實施一套防禦措施(重點資安控制項目)，以及能降低風險的威脅分享措施 (STIX ensemble)。
  - 雖然加密有積極的好處，但必須注意端到端加密的不利影響。
  - 為控制網路安全風險，必須注意迅速發展的新產業平台(例如 NFV-SDN/5G)和量子電腦。

7.2 新的科技與服務

網路功能虛擬化+軟體定義網路。服務提供者有意使其網路具有靈活性，以有效地滿足越來越快的寬頻需求的挑戰，並能夠透過創新服務及新的業務模式創造收入來源。網路功能虛擬化(Network Function Virtualization, NFV)與軟體定義網路(Software Defined Networking, SDN)藉由提供敏捷創新的雲端技術和提高經濟能力，已然成為可能改變產業的範例。到 2020 年，SNS Research 預估軟體定義網路(SDN)與網路功能虛擬化(NFV)能夠讓(包括有線與無線)服務提供者在年度資本支出投資中節省高達 320 億美金，ACG Research 預估網路功能虛擬化(NFV)將減少 68%的資本支出與 67%的營運支出。網路功能虛擬化(NFV)+軟體定義網路(SDN)實施需要一系列新的和改變後的網路威脅資訊分享及網路防禦方法[i.22]。

5G 行動網路、行動邊緣運算(Mobile Edge Computing, MEC)與物聯網(IoT)。在 5G 中，網路架構有了重大變化，其利用網路功能虛擬化(NFV)+軟體定義網路(SDN)支援高動態網路，且利用網路切片(network slicing)支援多種不同類型用戶。這些功能依序支援大量新的行動及無線固定實施，包括運輸系統、智能基礎建設自動駕駛車輛、製造及機器人。行動邊緣運算(MEC)在行動網路的無線存取網路邊緣地帶運作強大的處理和儲存功能。新的安全模式必須被散布在支援基礎建議的所有部分，並且必須能共同操作[i.23]。

OTT 網路(Over the Top)服務與「全面加密」措施。今日出現的重大網路安全挑戰是 OTT 服務與「全面加密」措施的相互結合，其將在世界上某個服務埠與最終用戶之終端(甚至可以是行動裝置上的應用程式)間產生潛在的巨大流量。某些物聯網之實施也屬於這類情形。儘管這些步伐滿足今日的重大需求，但這些做法可能帶來不利影響，例如妨礙偵測惡意軟體及其他網路安全威脅，以及管理網路流量及滿足大量業務、組織和法規需求。我們需要有衡平措施以滿足現今的所有需求[i.4]。

7.3 新的技法

7.3.1 將 middlebox 安全協定用於網路防禦

使用伺服器對終端用戶傳送路徑加密的迅速增長，使網路管理及義務遵守產生嚴重困難，包括提供網路防禦。網路應用程式伺服器直接與終端用戶行動裝置上的軟體客戶互動時，流量加密即發生在彼此端點之間[i.4]。使用案例包含 NIS 指令範圍內的一系列業務與循規性義務。含有新標準基礎規範的網路閘道網路防禦相關活動有顯著增加。越來越多利用所謂的「middleboxes」來實施網路防禦功能，middleboxes 可以整合到通常存在網路邊界的流量路由器。網路閘道是實施網路防禦及其他關鍵功能的重點。

符合 NIS 指令的相關網路防禦技術要求有：

1) 保護並有控制地揭露可觀察流量；

2) 足以獲得與分析防禦措施的可觀察資訊；

3) 有能力制定作為網閘管理之一防禦措施。

Middlebox 安全協定功能能滿足以上網路防禦的要求 [i.4]。

7.4 協調各類網路、服務產業、成員國法律及運營環境的實施

實施網路與資訊安全(NIS)指令最具挑戰性的一點就是協調各類網路、服務產業與歐盟成員國

法律及運營環境的實施[i.1]。雖然如此，但是這個問題已超出本文件的討論範圍。

8 建議

8.1 關鍵服務業者

應鼓勵關鍵服務業者採用可共同操作的通用台平，例如用於網路威脅情報分享的結構性威脅資訊表示(STIX)，以及用於有效網路防禦的重點資安控制項目，以及像是 Middlebox 安全協定等重要功能，以因應加密流量帶來的挑戰[i.3]、[i.4] 與 [i.6]。

8.2 數位服務提供者

應鼓勵數位服務提供者採用可共同操作的通用台平，例如用於網路威脅情報分享的結構性威脅資訊表示(STIX)，以及用於有效網路防禦的重點資安控制項目，以及像是 Middlebox 安全協定等重要功能，以因應加密流量帶來的挑戰[i.3]、[i.4] 與 [i.6]。

8.3 網路與資訊安全之促進機制

一般而言，使用 ETSI TR 103 305 [i.3]第 4 部分所述的促進機制，包括隱私權影響評估、對國家網路安全架構之互映、網路衛生方案及治理策略，可以明顯地加強網路與資訊安全。

附錄 A；
網路威脅情報分享的歷史發展

在 1990 年代增長的網路威脅導致了電腦緊急應變小組(Computer Emergency Response Terms, CERTs)和電腦資安事件應變小組(Computer Security Incident Response Teams, CSIRTS)的成立。這些機構在 1990 年組成了一個名為資安事件應變小組論壇(Forum of Incident Response and Security Teams, FIRST)的國際組織。為了促進自動化，需要有結構化的威脅情報交換，在 2001 年，以阿姆斯特丹的跨歐洲研究暨教育網協會(Trans-European Research and Education Networking Association, TERENA)電腦資安事件應變小組的專案組(TF-CSIRT)， 在網際網路工程專案組(IETF)中成立資安事件處理工作組(INCident Handling Working Group, INCH)。資安事件處理工作組(INCH)依序產出四份文件規範[i.34]、[i.35]、[i.36] 與[i.37]，目前仍是該領域的概念基礎。

數據模式的概念如圖 A.1 所示：

CSIRT #1, CSIRT #1, IODEF (不用翻，上一段有說明)
Incident DB：事件資料
Translator：翻譯人員

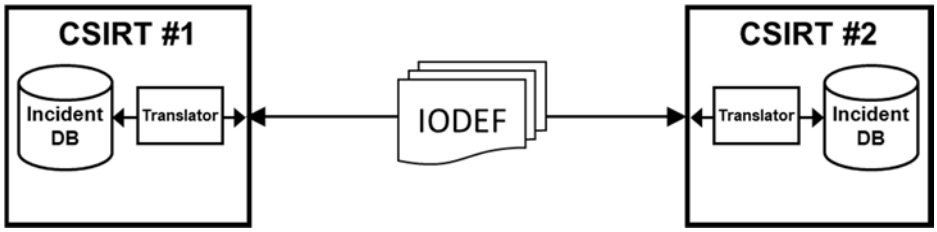


圖 A.1：IODEF(國際資通訊安全事件訊息交換格式)為基礎之威脅情報交換模式概念圖

網際網路工程專案組(IETF)的原有活動，在輕量級交換託管資安事件(Managed Incident Lightweight Exchange, MILE)工作組的支持下持續進行，而該工作組擴大了原有規範。

在 2000 年代，隨著 MITRE Corporation 開發了一系列交換結構化網路安全資訊的新方法，需求與工作顯著地攀昇，而這些方法在 2008 年代開始，為國際電信聯盟電信標準化部門(ITU-I)研究小組 17 表意文字小組(Q4/17)應用在網路安全，作為一個被稱為網路安全資訊交換(Cyber security information Exchange, CYBEX)的擴充架構。請見 ITU-T X.1500 系列建議書[i.28]。許多輕量級交換託管資安事件(MITRE)與其他規範在 ITU-T X.1500 系列建議書被認定為四個「交換叢集(exchange clusters) 」：

- 缺點、弱點及狀態
- 事件、事故與啟發
- 資訊交換政策
- 識別、發現與質問
- 身份擔保
- 交換協定

網路安全資訊交換(CYBEX)與 IETF 模型有點類似並且完全兼容，故兩者在本質上是相同的 – 僅允許包含本體模式更多樣且可充擴的交換機制配置，這些交換機制在 ITU-T X.1500 建議書附錄中有最新版(每年更新兩次)。請見圖 A.2。

Cybersecurity entities 網路安全實體

Cybersecurity information acquisition (out of scope) 網路安全資訊獲取(範圍外)

- Structuring cybersecurity information for exchange purpose 為交換目的建構網路安全資訊
- Identifying and discovering cybersecurity information and entities 識別與發現網路安全資訊與實體
- Establishment of trust and policy agreement between exchanging entities 在交換實體間制定託管與政策協議
- Requesting and responding with cybersecurity information 請求與回應網路安全資訊
- Assuring the integrity of the cybersecurity information exchange 確保網路安全資訊交換的完整性

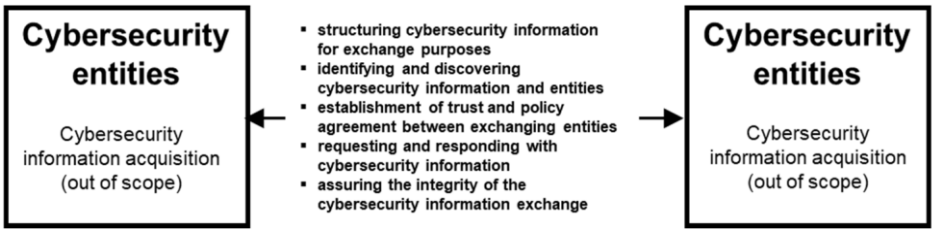


圖 A.2：以 ITU-T X.1500 建議書為基礎的情報交換模型概念[i.28]

在 2012 年，在討論如何擴大網路威脅情報交換能力的過程中，MITRE 研究員在白皮書上以 STIX(結構化威脅資訊交換)格式提出了統一但靈活的模式概念。請見 Barnum [i.24]。該論文論述了基本的價值主張。

「*組織有網路威脅情報能力變得越來越必要，這種能力的成功關鍵之一就是與夥伴、同事及選擇信任的其他人分享資訊。網路威脅情報與資訊分享將有助於使用大量複雜網路安全資訊*

組織專注及優先化今日所面臨的問題，為了易於處理，他們對於這些資訊的標準化、結構化表達有基本的需求。」

結構化威脅資訊交換(STIX)迅速成為網路安全的統一場論(Unified Field Theory)，並在隨後四年成為多個交換網路威脅情報社群的主要手段及工作成效。在 2015 年，智慧財產被移轉到資訊標準架構促進會(OASIS)標準組織，並且在其網路威脅情報技術委員會的管理下繼續進行，該委員會在數量、多樣性及活動方面迅速成長，以包含全球各地的組織。其活動包括維護幾個 Githubs，並提供可用的運行代碼以供實施。請見 https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti。於結構化威脅資訊交換(STIX)規範叢集，網路可觀測資安事件表達(Cyber Observable Expression, CybOX)是獲得威脅觀測的方法，而指標資訊的可信自動化交換(Trusted Automated Exchange of Indicator Information, TAXII)則是用以傳送這些威脅的協定。

指標資訊的可信自動化交換(TAXII)繼續快速發展在資訊標準架構促進會網路威脅情報(OASIS CTI)技術委員會的全球版，並於 2017 年 5 月通過 2.0 版，也將會繼續開發未來的版本。對於以標準化、結構化方式描述及交換網路威脅資訊的各種手段，ETSI TR 103 331 [i.6]提出了綜合性的敘述，包括結構化威脅資訊交換(STIX)使用案例、零件與架構的大量資訊。請見圖 A.3。

STIX Architecture 1.1.1.　結構化威脅資訊交換架構 1.1.1
Incident = 資安事件
Observable = 觀測
Threatactor =威脅行為人
Campaign = 活動
Indicator = 指標
TTP
Exploit target =利用目標
Cause of Action =訴因

Related observables (*) 相關觀測
Sub-observables (*) 次要觀測
Parameter observable(*) 參數觀測
observables(*) 觀測

Related incidents (*) 相關事件

Related threat actor (*) 相關威脅行為人
Associated actors (*) 聯合行為人

Attribution (*) 可歸責

Related campaign (*) 相關活動
Associated campaigns (*) 聯合活動
Historical campaigns (*) 歷史活動

Related indicators (*) 相關指標

Indicated TTP(*) 指標的 TTP
Related TTP(*) 相關的 TTP
Observed TTP(*) 觀測到的 TTP
Leveraged TTP(*) 利用的 TTP

Related Exploit Target (*) 相關的利用目標

Related COA(*) 相關的訴因
Suggested COA(*) 建議的訴因
Potential COA(*) 可能的訴因
COA requested (*) 起訴請求的訴因
COA taken(*) 採行的訴因

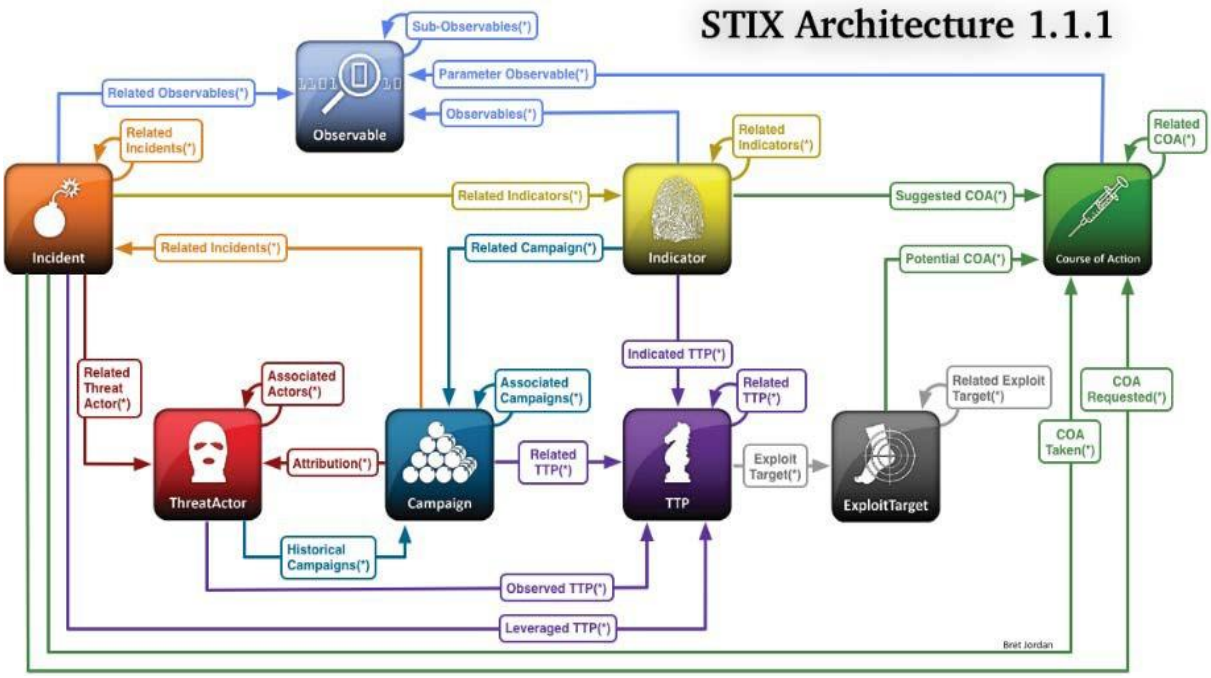


圖 A.3： STIX 各零件的數據模式[i.6]

歷程

文件歷程		
版本 1.1.1	2017 年 10 日	公布

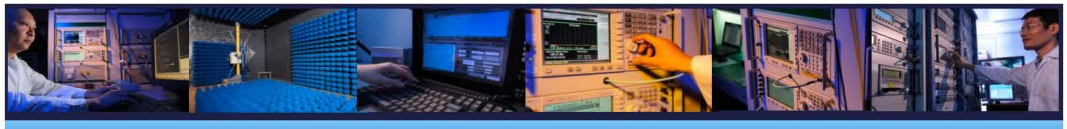
附錄五 座談會紀錄及意見回覆

研商行動寬頻基站資安檢測技術規範草案
座談會紀錄及意見回覆

一、座談會簡報

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

基站資安檢測規範草案座談



2018.4

財團法人電信技術中心

簡報大綱

- 基站安全風險
- 檢測規範適用範圍
- 檢測範圍及框架
- 檢測項目
- 檢測結果分享
  - 家用基站(HeNB)
  - 基站

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

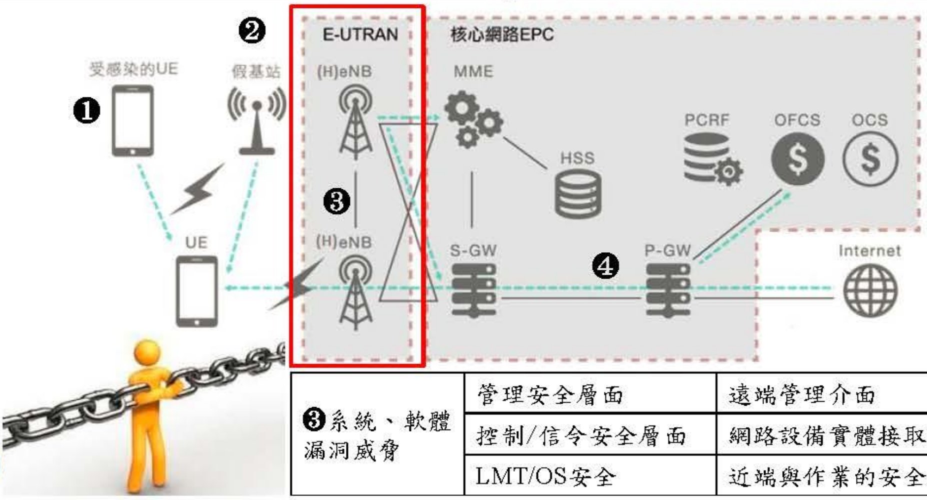
2

基站安全風險

- ☐ 基站(eNB)為邊界防禦的主體

❶行動裝置間的威脅、❷無線訊號的威脅	用戶安全層面	惡意的使用者終端裝置
	控制/信令安全層面	空中介面

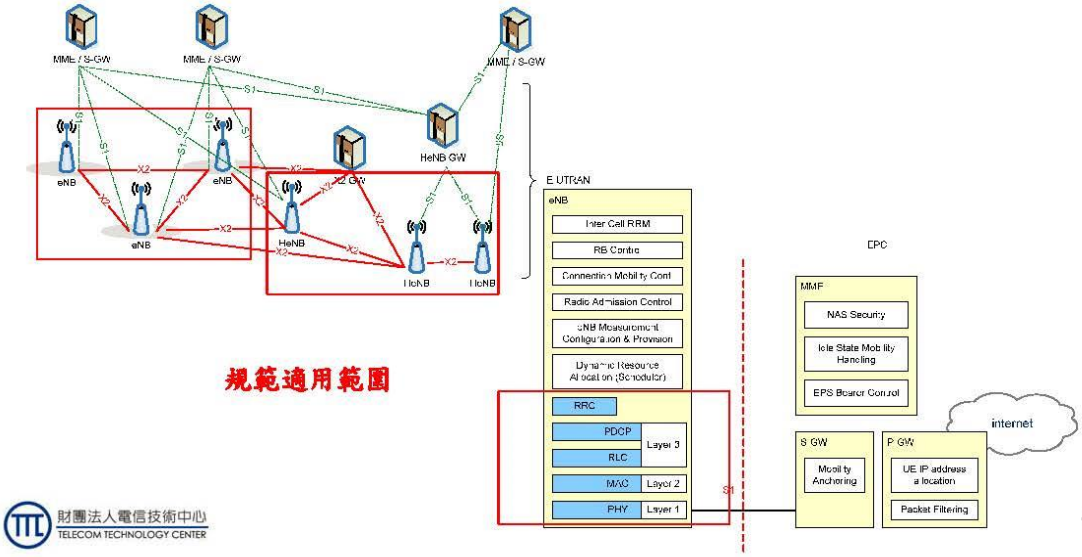
❹核心網路內部通訊介面或外部威脅	控制/信令安全層面	傳輸網路威脅



❸系統、軟體漏洞威脅	管理安全層面	遠端管理介面
	控制/信令安全層面	網路設備實體接取威脅
	LMT/OS安全	近端與作業的安全管理

檢測規範適用範圍

- ☐ 本規範適用行動寬頻基地台，包含大基站(eNodeB)與小基站(Small Cell)，並依(1)資料保護、(2)應用程式安全、(3)通訊安全、(4)身分鑑別與授權安全、(5)作業系統安全、(6)實體防護六項安全構面，訂定產品安全技術要求。



檢測範圍及框架(1/2)

資料保護 → 確保敏感性資料無論在傳輸或儲存時，都具有外洩防堵的能力

- 1.1 敏感性資料外洩防止(由系統功能洩露)
- 1.2 敏感性資料外洩防止(韌體外洩)
- 1.3 基站系統應確保敏感性資料進行加密處理再儲存
- 1.4 憑證具唯一性

應用程式安全 → 確認產品之網頁管理介面，是否存在已知資安漏洞

- 2.1 基站網站伺服器不應存在常見之網路應用系統安全弱點

通訊安全 → 包括網路服務、空中介面等是否符合通訊傳輸介面的安全要求

- 3.1 基站系統使用之協定與服務應採最小化設計
- 3.2 基站系統與對外之網路傳輸過程，應使用加密技術確保資料安全
- 3.3 控制層資料機密性保護

⋮

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

5

檢測範圍及框架(2/2)

身分認證與授權 → 確認產品設計上，能確保身分鑑別與授權機制之強度

- 4.1基站系統應禁止未經認證與授權使用系統各項功能
- 4.2每一個帳號至少要有一個身分鑑別因子方可鑑別成功
- 4.3基站系統預設帳號應可移除或設置停用

⋮

作業系統安全 → 確保作業系統具備資安防護能力，與已知資安漏洞的修補程度

- 5.1 日誌檔不能洩露個人資料
- 5.2 開機僅可透過合法的韌體
- 5.3基站系統應具備軟體完整性自我檢測機制

⋮

HeNB 實體防護 → 確認產品之實體設計，有考慮駭客實體入侵之防護能力

- 6.1 家用基站的防拆保護
- 6.2 實體介面的安全管控
- 6.3 硬體憑證的設計

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

檢測項目-資料保護

- 資料保護安全測試是為確認產品設計上，是否確保敏感性資料無論是在傳輸或儲存時，都具有外洩防堵的能力，包括敏感性資料存取控管、加解密演算法。

檢測編碼	檢測項目	檢測目的
1.1	敏感性資料外洩防止(由系統功能外洩)	確認系統功能不會洩露敏感性資料。
1.2	敏感性資料外洩防止(韌體外洩)	驗證裝置韌體是否含有敏感性資料外洩疑慮。
1.3	基站系統應確保敏感性資料進行加密處理再儲存	基站系統對於敏感性資料應採用適當且有效之加密技術，使資料不會以原來的形式呈現，達到保密的目的，並確保避免遭操作修改。
1.4	憑證唯一性	驗證憑證是否可被偽造。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

7

檢測項目-應用程式

- 應用程式安全測試是為確認產品設計上，網頁管理介面是否存在已知資安漏洞，以確保產品之網頁管理介面安全無虞。

檢測編碼	檢測項目	檢測目的
2.1	基站網站伺服器不應存在常見之網路應用系統安全弱點	基站網站伺服器不應存常見之網路應用系統安全弱點，包含有資料隱碼注入攻擊(SQL Injection)、跨框架腳本攻擊(Cross-Frame Scripting)、SSL會話重建程序攻擊(SSLv3/TLS Renegotiation Stream Injection)、網站伺服器設定配置不當(Web Server Misconfiguration)等，以及OWASP Top 10所載之網站安全威脅弱點。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

8

檢測項目-通訊安全(1/2)

- 確認產品設計上，是否符合通訊傳輸介面的安全要求，包括網路服務啟用限制、空中介面通訊安全、傳輸加密技術要求等，確保產品具備可靠之通訊傳輸功能。

檢測編碼	檢測項目	檢測目的
3.1	基站系統使用之協定與服務應採最小化設計	基站系統在預設條件下應只執行需要的協定和服務，業者實際維運階段之不同任務原因，可將原本未啟用協定與服務視需要予以暫時性啟用與做適當管理。
3.2	基站系統與對外之網路傳輸過程，應使用加密技術確保資料安全	基站系統與其他外部設備之網路傳輸過程中須加密保護，且不應使用或支援已被公開認定之弱加密技術。
3.3	控制層資料機密性保護	基站應對S1 /X2 參照點的控制層封包進行機密性保護。
3.4	控制層資料完整性保護	基站應對S1 /X2 參照點的控制層封包進行完整性保護。
3.5	存取層之完整性演算法選擇	(1) 服務網路(serving network)應依據UE所支援的安全功能與目前服務網路所設定許可之安全功能清單，選擇欲使用的演算法。 (2)基站應透過設定可用的演算法清單，包括完整性演算法清單，並由電信業者決定優先排序。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

9

檢測項目-通訊安全(2/2)

檢測編碼	檢測項目	測試目的
3.7	基站金鑰更新	當基站交遞時，為避免使用相同金鑰，基站應具備觸發基站金鑰(KeNB)的金鑰更新功能。
3.8	存取層安全模式指令程序	基站應從優先清單中，選擇最高順位之完整性演算法保護SECURITY MODE COMMAND訊息。
3.9	防範 X2 交遞中的降階攻擊	在路徑變更(path-switch)訊息中，目的基站應對MME傳送從來源基站接收的UE EPS安全性功能。
3.10	變更基站之存取層保護演算法選擇	(1) 目的基站應根據其本身演算法優先列清單選擇UE EPS之安全性功能最高順位的演算法 (包含完整性演算法與加密演算法)。若是所選擇的演算法與來源基站所選擇的不同，應透過交遞指令通知UE。 (2)驗證有正確選擇應用伺服器保護演算法。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

10

檢測項目-身分鑑別與授權安全(1/3)

- 確認產品設計上，於身分鑑別與授權機制之強度，包括權限控管、通行碼機制複雜度、身分鑑別機制強度等。

檢測編碼	檢測項目	檢測目的
4.1	基站系統應禁止未經認證與授權使用系統各項功能	登入至基站系統包含網路服務(SSH、SFTP、Web Service)、透過管理介面使用本機存取使用，都須完成身分認證與授權機制後才可以使用系統各項功能。
4.2	每一個帳號至少要有一個身分鑑別因子方可鑑別成功	基站系統的使用者身分鑑別機制須至少帳號與一個身分鑑別因子，包含加密金鑰(Cryptographic keys)、Token或密碼。
4.3	基站系統預設帳號應可移除或設置停用	基站系統預設帳號應可移除或設置停用
4.4	基站系統應支援與設定不同組合之密碼複雜性規格	基站系統應支援與設定不同組合之密碼複雜性規格
4.5	通行碼變更機制	基站系統應支援可提供隨時更改密碼之功能，並且系統預設密碼應於初次登入階段強制要求變更，且支援變更密碼內容不得超過特定重複使用次數功能設定。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

11

檢測項目-身分鑑別與授權安全(2/3)

檢測編碼	檢測項目	檢測目的
4.6	基站系統應具備暴力及字典攻擊的防護措施	基站系統應具備暴力及字典攻擊的防護措施，包含網頁介面設置CAPTCHA功能、嘗試登入失敗次數限制與鎖定帳號時間。
4.7	通行碼顯示遮罩	基站系統在通行碼的設計不會以原來的形式呈現，達到保密的目的，並確保避免遭操作修改。
4.8	通行碼連續輸入錯誤處理	基站系統應具備連續登入失敗處理機制，並可限制最大連續輸入失敗次數與強制鎖定可登入延遲時間。
4.9	授權策略	基站系統應具備依不同帳號給予不同授權之設定機制，確保受測物之授權策略，針對特定資訊僅給予具備權限之帳號存取。
4.10	基站系統應支援基於角色之存取控制	基站系統應支援基於帳號角色之存取控制。使用一系列控制方式來確定帳號如何進行系統功能存取與故障管理維護。
4.11	登出功能是否有效	基站系統應支援登入之帳號可隨時登出之功能，並於登出階段提供是否登出系統之提醒畫面。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

12

檢測項目-身分鑑別與授權安全(3/3)

檢測編碼	檢測項目	檢測目的
4.12	基站系統應支援操作逾時功能	基站系統應限制當帳戶操作逾時超出設定時間，系統即將該帳號給予強制登出。
4.13	登入之權限控管	基站系統應限制最高管理權限帳號不可從遠端登入，降低被攻擊的風險。
4.14	檔案系統存取權限控管	基站系統具備檔案系統存取權限控管機制，僅有授權之帳戶可修改作業系統層級之檔案、資料或系統檔案等。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

13

檢測項目-作業系統安全(1/2)

- 為驗證產品之作業系統上是否增加資安防護能力，與已知資安漏洞的修補程度。

檢測編碼	檢測項目	檢測目的
5.1	日誌檔不能洩露個人資料	驗證產品之個人資料是否不會明文顯示於日誌檔中
5.2	開機僅可透過合法的韌體	驗證產品是否只能經由指定的記憶體裝置啟動
5.3	基站系統應具備軟體完整性自我檢測機制	基站系統應具備軟體安裝時完整性檢測，確保基站廠商發佈之軟體與已安裝的軟體相同，驗證軟體是否已遭受修改
5.4	基站系統應提供安全事件記錄功能	基站系統應提供不同事件類型之安全紀錄，包含登入失敗、管理者存取、管理者操作行為、設定變更、重新開機、關機、當機、網路介面狀態改變

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

14

檢測項目-作業系統安全 (2/2)

檢測編碼	檢測項目	檢測目的
5.5	基站系統應提供可將安全事件紀錄功能轉移備存至外部系統	基站系統應提供可將安全事件紀錄功能傳輸備存至集中管理設備或其他外部系統設備，並傳輸過程使用加密技術保護
5.6	基站系統的安全事件紀錄應有存取控制限制	基站系統之安全事件紀錄應僅有特定權限帳號可以存取
5.7	確保高權限的系統功能必須經過身分鑑別	驗證擁有特殊權限的系統功能是否經過認證與授權方可使用
5.8	可卸除儲存媒體禁止啟用自動播放功能	驗證當產品被接入卸除式媒體(如:USB)時，是否會自動執行應用程式
5.9	作業系統及網路服務安全	系統本身不應存在重大風險已知弱點漏洞

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

15

檢測項目-實體防護

- 為確認產品設計上，有無阻礙駭客實體入侵之能力，包括增加產品外殼拆除難度、實體介面之存取控制等，通過此節的資安測試，可確保產品具備實體資安防護功能，由於僅家用基站是布建於終端使用者環境中，因此本節僅家用基站適用。

檢測編碼	檢測項目	檢測目的
6.1	家用基站的防拆保護	驗證產品具有拆解防護之設計，增加實體介面入侵之難度。
6.2	實體介面的安全管控	驗證連接產品實體埠時，可否存取作業系統之除錯模式。
6.3	硬體憑證的設計	驗證產品之硬體憑證是否可被徒手移除。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

16

HeNB檢測結果分享

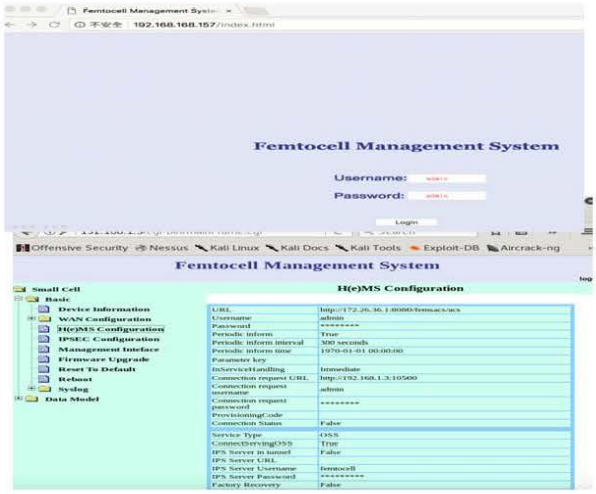
- HeNB目前初步檢測結果，最大風險來自於【身分鑑別與授權】，於檢測過程中，舉出已發現之嚴重風險案例如後：
  - 已發現之漏洞
    1. 網頁管理介面使用強度不足的預設密碼。如：admin/admin
    2. 網頁管理介面存在低權限帳號偷過更改cookies提權的漏洞
    3. 網頁管理介面存在XSS漏洞，可能造成導向釣魚網站等風險
    4. 網頁管理介面有顯示log資訊，從log資訊中可以擷取重要訊息進行分析
    5. 網頁管理介面的最高使用者權限為弱密碼，對於設備使用上有很大的風險
    6. 最高使用者的網頁管理介面可開啟telnet進去設備系統層
    7. 家用基站的硬體層接腳輕易被識別，可從UART port進去系統層
    8. root為弱密碼，容易被第三人提權成功
    9. 對IPsec下傳輸的封包進行解密，造成使用者資訊將洩漏

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

17

1.網頁介面(預設帳號)弱密碼風險

- 說明：網頁介面為弱密碼強度
- 影響：輕度資訊被瀏覽，可對設備重新開機。
- 檢測畫面：



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

18

2.網頁介面存在提權漏洞

- 說明：網頁介面可由低權限帳號提權
- 影響：重要4G設定檔參數被竄改。
- 檢測畫面：

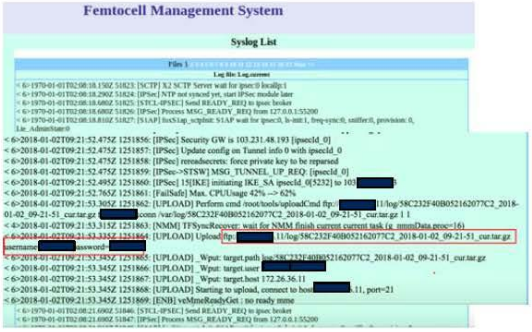
```
GET /cgi-bin/login.cgi?username=admin&password=admin&Submit=Login HTTP/1.1
Host: 192.168.1.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.2/
Cookie: sessionID=XTEKFIWTMOXXDVRH Mode=ENG
Connection: close
Upgrade-Insecure-Requests: 1
```

3.網頁介面存在XSS漏洞

- 說明：網頁介面存在XSS漏洞
- 影響：利用該漏洞使被攻擊者請求特殊操作，如：竊取cookies、導向釣魚網站等。
- 檢測畫面：

4.Log資訊洩漏

- 說明：下圖為預設初始帳號登入可觀看到的log資訊。
- 影響：可能會洩漏重要資訊如：其他server的IP和其他帳號密碼
- 檢測畫面：

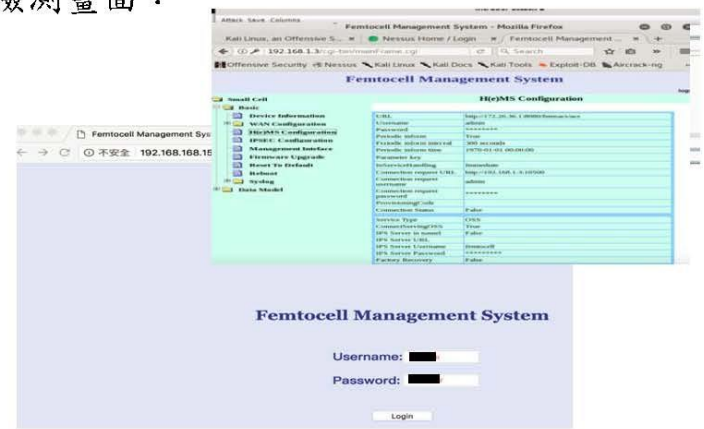


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

21

5.網頁介面(最高權限帳號)弱密碼風險

- 說明：網頁介面使用帳號為弱密碼強度
- 影響：網頁管理介面最高權限使用者，對設備各參數皆可進行調整。
- 檢測畫面：

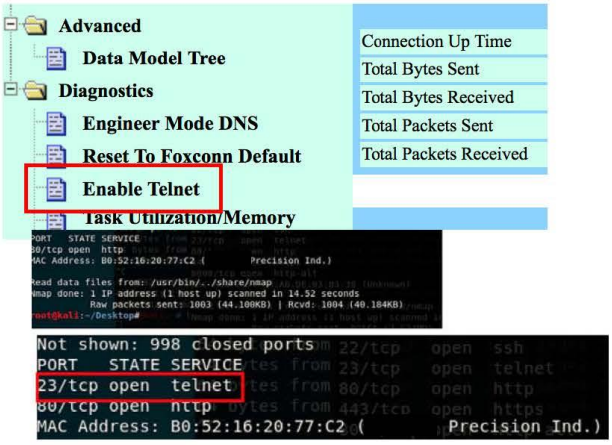


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

22

6.telnet連接至系統

- 說明：遠端管理介面為明文傳輸
- 影響：telnet傳輸帳號密碼時為明文，恐有被第三人竊取之風險。
- 檢測畫面：



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

23

7.硬體UART接腳

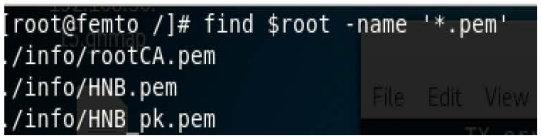
- 說明：UART接腳為未隱藏
- 影響：可藉由UART進入系統層。
- 檢測畫面：

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

24

8.最高權限帳號為弱密碼

- 說明：最高權限帳號為弱密碼
- 影響：從telnet連接或UART進入系統層，即可取得最高權限，使得該設備輕易可被第三人掌控
- 檢測畫面：

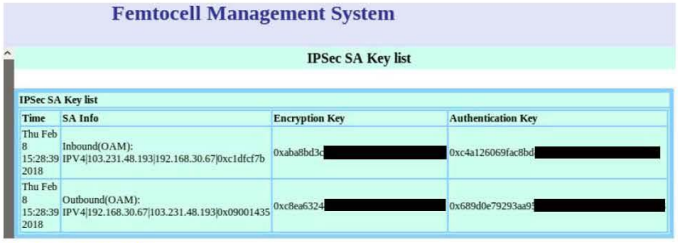


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

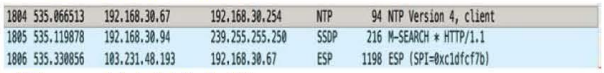
25

9.IPsec封包被解密

- 說明：網頁洩漏IPsec相關金鑰使加密封包被解密
- 影響：使用者資訊會被洩漏
- 檢測畫面：

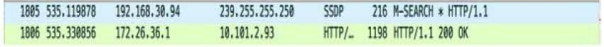


IPsec 封包(解密前)



1804	535.066513	192.168.30.67	192.168.30.254	NTP	94 NTP Version 4, client
1805	535.119878	192.168.30.94	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
1806	535.330856	103.231.48.193	192.168.30.67	ESP	1198 ESP (SPI=0xc1dfcf7b)

IPsec 封包(解密後)



1804	535.066513	192.168.30.67	192.168.30.254	NTP	94 NTP Version 4, client
1805	535.119878	192.168.30.94	239.255.255.250	SSDP	216 M-SEARCH * HTTP/1.1
1806	535.330856	172.26.36.1	10.101.2.93	HTTP/…	1198 HTTP/1.1 200 OK

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

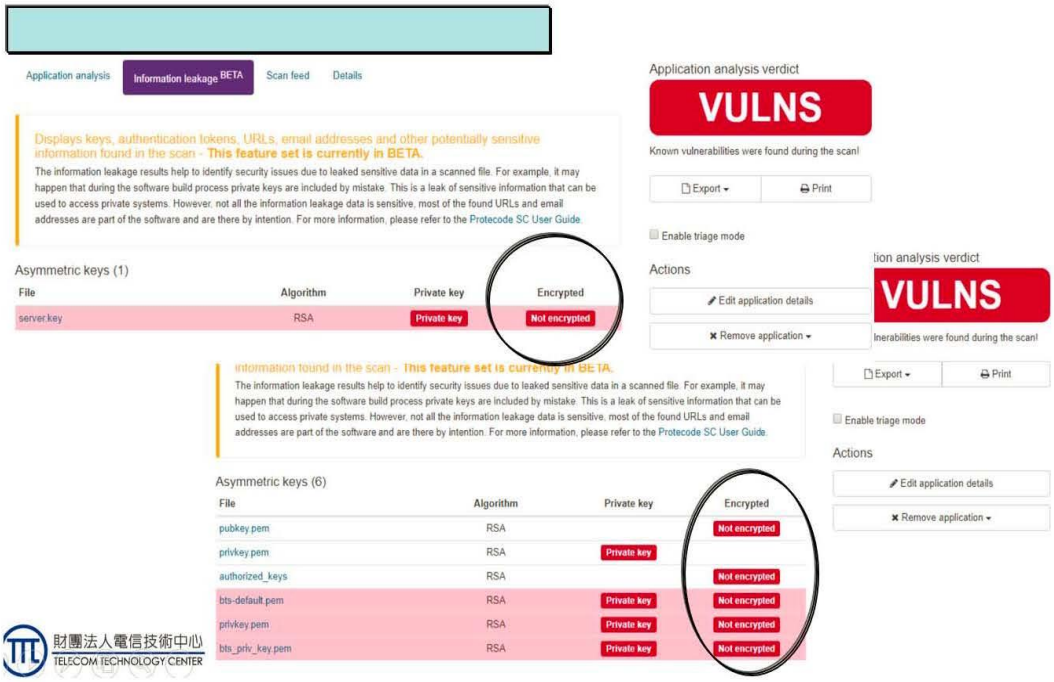
基站主要檢測結果分享

- 基站(eNodeB)目前初步檢測結果，主要韌體檔案內金鑰未加密、網站存有安全弱點、內建預設密碼初次登入無要求強制變更等，以下舉出幾個已發現：
  1. 基站韌體檔案內之金鑰檔無加密
  2. 網站伺服器檢測存有設定不當弱點 - Unprotected File
  3. 網站伺服器檢測存有設定不當弱點 - Response Headers
  4. 網站伺服器檢測存有設定不當弱點 - Restricted file access
  5. 網站伺服器檢測存有設定不當弱點 - SSL問題
  6. 系統內建預設密碼應於初次登入階段強制要求變更
  7. 基站系統使用之協定與服務應採最小化設計
  8. 基站系統應具備暴力及字典攻擊的防護措施

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

27

1. 基站韌體檔案內之金鑰檔無加密



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

28

2. 網站伺服器檢測存有設定不當弱點 - Unprotected File

High

Web Server Misconfiguration: Unprotected File

Summary:

Webinspect has detected an archive file with the .gz extension on the target server. The severity of the threats posed by the web-accessible backup files depends on the sensitivity of the information stored in original document. Based on that information, an attacker can gain sensitive information about the site architecture, database and network access credential details, encryption keys, and so forth from these files. The attacker can use information obtained to craft precise targeted attacks, which may not otherwise be feasible, against the application.

Execution:

Browse to https://10.0.0.86:443/jse/core/dom.js.gz and inspect the content. Response should be a return with HTTP status code 200 and should not match target site's file not found response.

File Names:

- https://10.0.0.86:443/jse/core/dom.js.gz
- https://10.0.0.86:443/jse/xui/xui.js.gz
- https://10.0.0.86:443/platform/lmtlib/lmtutil.js.gz
- https://10.0.0.86:443/login.html.gz
- https://10.0.0.86:443/jse/binaryproperty.js.gz
- https://10.0.0.86:443/jse/core/container.js.gz
- https://10.0.0.86:443/jse/base/util.js.gz
- https://10.0.0.86:443/jse/jse.js.gz
- https://10.0.0.86:443/jse/base/xpath.js.gz
- https://10.0.0.86:443/config/config.js.gz
- https://10.0.0.86:443/jse/base/eventqueue.js.gz
- https://10.0.0.86:443/jse/conf.js.gz
- https://10.0.0.86:443/jse/base/ajax.js.gz

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

29

3. 網站伺服器檢測存有設定不當弱點 - Response Headers

Web server information in HTTP headers

Web Server Misconfiguration: Response Headers (11309) View Description

CWE: 79

Kingdom: Environment

Page: https://192.168.170.42:443/images/nsn_logo.jpg

Request:

```
GET /images/nsn_logo.jpg HTTP/1.1
Accept: */*
Referer: https://192.168.170.42/protected/index.cgi
Accept-Language: zh-TW
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4 Center PC 6.0; .NET4.0C; .NET4.0E)
SLCC2; .NET CLR 2.0.5 Host: 192.168.170.42
Connection: Keep-Alive
Pragma: no-cache
Cookie: CustomCookie=WebInspect130381ZXC2D6926C48034330B4F2888C462D1CA0Y840B
```

Response:

```
HTTP/1.1 200 OK
Strict-Transport-Security: max-age=63072000; includeSubdomains
X-Frame-Options: sameorigin
Cache-Control: no-cache
Pragma: no-store
Content-Type: image/jpeg
Accept-Ranges: bytes
ETag: "658190923"
Last-Modi...TRUNCATED...
```

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

30

4. 網站伺服器檢測存有設定不當弱點 - Restricted file access

Restricted file access

Low Issues

Web Server Misconfiguration: Unprotected Directory (10233) View Description

CWE: 548

Kingdom: Environment

Page: https://192.168.170.42:443/protected/

Request:

```
GET /protected/ HTTP/1.1
Referer: https://192.168.170.42/protect...TRUNCATED...
```

Response:

```
HTTP/1.1 302 Found
Strict-Transport-Security: max-age=6307200...TRUNCATED...
```

Web Server Misconfiguration: Unprotected Directory (10233)

Summary

Directories that may be restricted to only certain users were discovered within your web application during a Directory Enumeration scan. Risks associated with an attacker discovering a directory on your application server depend upon what type of directory is discovered, and what types of files are contained within it. The primary threat, other than accessing files containing sensitive information, is that an attacker can utilize the information discovered in that directory to perform other types of attacks. Recommendations include restricting access to important directories or files by adopting a "need to know" requirement for both the document and server root, and turning off features such as Automatic Directory Listings that provide information that could be utilized by an attacker when formulating or conducting an attack.

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

31

5. 網站伺服器檢測存有設定不當弱點 - SSL問題

20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption

An attacker can exploit these flaws to conduct ma
the affected service and clients.

Although SSL/TLS has a secure means for choos
these versions will be used only if the client or se
this in an unsafe way that allows an attacker to d
recommended that these protocols be disabled e

NIST has determined that SSL 3.0 is no longer a
enforcement found in PCI DSS v3.1, any version
cryptography'.

42873 - SSL Medium Strength Cipher Suites Supported

Synopsis

The remote service supports the use of medium strength SSL ciphers.

Description

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

See Also

https://www.openssl.org/blog/blog/2016/08/24/sweet32/

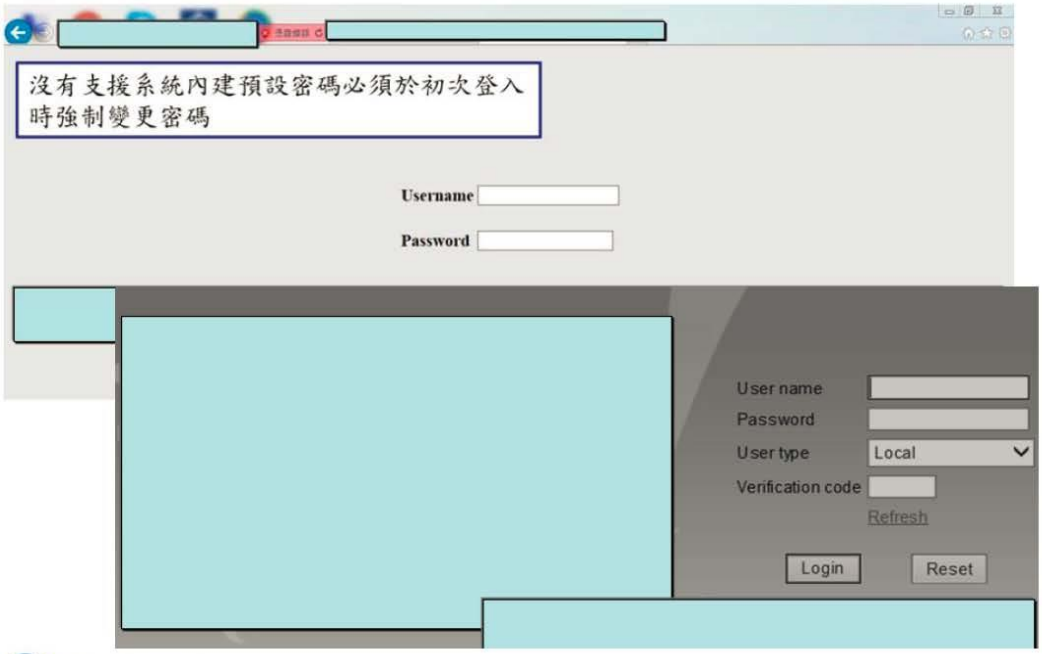
Solution

Reconfigure the affected application if possible to avoid use of medium strength ciphers.

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

32

6.系統內建預設密碼 應於初次登入階段強制要求變更



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

33

7.基站系統使用之協定與服務 應採最小化設計

```
root@kali:~#

tps://nmap.org ) at 2018-01-31 22:24 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or sp
ecify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.170.66
Host is up (0.0024s latency).
Not shown: 981 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
135/tcp  open  msrpc
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
990/tcp  open  ftps
993/tcp  open  imaps
995/tcp  open  pop3s
2000/tcp open  cisco-sccp
5060/tcp open  sip
8008/tcp open  http
8010/tcp open  xmpp
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 82.93 seconds
```

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

34

8.基站系統應具備暴力及字典攻擊的防護措施

```
File  Edit  View  Search  Terminal  Help
root@kali:~# [redacted] -l root -P passlist_revise.txt [redacted] ssh
Hydra v8.1 (c) 2014 by van [redacted] - Please do not use in military or secret service organizations, or for illegal purpo
ses.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-01-31 21:14:14
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwriting, you have 10 seconds to abort
...

[DATA] max 16 tasks per 1 server, overall 64 tasks, 1190968 login tries (l:1/p:1190968), ~1163 tries per task
[DATA] attacking service ssh on port 22

[STATUS] 139.00 tries/min, 139 tries in 00:01h, 1190829 todo in 142:48h, 16 active
[STATUS] 180.00 tries/min, 540 tries in 00:03h, 1190428 todo in 110:14h, 16 active
```

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

35

~THANK YOU~

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

36

二、 座談會會議紀錄

(一) 電信業者

1. 中華電信

研商行動寬頻基站資安檢測技術規範草案(場次1)會議紀錄

壹、時間：107年4月11日(星期三)上午9時30分

貳、地點：本會濟南路辦公室6樓中型會議室

參、主席：吳簡任技正銘仁 (蘇科長勇吉代)　　記錄：莊惠婷

肆、出席單位及人員：如附簽到表

伍、主席致詞(略)

陸、行動寬頻基站資安檢測規範草案說明(報告單位 TTC，略)

柒、中華電信發言重點：

一、 本檢測規範適用範圍，基站分類之定義請 TTC 參照行動寬頻基地臺射頻設備技術規範內容，使用詞定義一致化。

二、 本檢測規範草案許多測試項目，需由設備製造商進行確認，建議 NCC 評估是否未來將本檢測規範納入型式認證要求，避免電信業者系統建設後，才發生基地臺資安檢測無法通過的情況。

三、 電信業者設備廠牌型號眾多，逐款進行檢測及確認對電信業者實有困難。

四、 建議未來再與所有業者進行一次綜合性討論。

捌、會議結論：

一、 請中華電信於107年4月20日前回覆本檢測規範草案意見表予 TTC。

二、 請中華電信協助提供4G 基站前3項主要使用之廠牌型號供 TTC 參考。

三、 中華電信如有可作為測試場域之核網環境及基站等設備，可提供予 TTC 協助檢測，以完善本檢測規範草案。

玖、散會(上午10時50分)

研商行動寬頻基站資安檢測技術規範草案
會議簽到表-場次一

壹、時間：107 年 4 月 11 日（星期三）上午 9 時 30 分
貳、地點：本會濟南路辦公室 6 樓中型會議室(臺北市濟南路二段 16 號 6 樓)
參、主席：吳簡任技正銘仁
肆、出席者：

中華電信股份有限公司

陳泰祥 黃業恆
林尚達 陳瑋倫

財團法人電信技術中心

李明德 蔡志明
曾志強
黃川源
王慶豐 張竹筆

本會基礎設施事務處

李福彰

2. 遠傳電信

研商行動寬頻基站資安檢測技術規範草案(場次2)會議紀錄

壹、時間：107年4月11日(星期三)上午11時00分

貳、地點：本會濟南路辦公室6樓中型會議室

參、主席：吳簡任技正銘仁 (蘇科長勇吉代)　　記錄：莊惠婷

肆、出席單位及人員：如附簽到表

伍、主席致詞(略)

陸、行動寬頻基站資安檢測規範草案說明(報告單位 TTC，略)

柒、遠傳電信發言重點：

一、建議 NCC 考量未來5G 建設，在強調高速率低延遲的網路環境時，若加入過多加密機制，可能會達不到5G 所期望的速率。

二、電信業者遵守 ISO27001標準，基地臺係建置在受管理的網段中，安全性高。

三、電信業者維運與服務網段不同，無法以遠端 login 功能進行維運，安全性較高。

四、本檢測規範草案內容較偏 HeNB，建議檢測規範草案應分為基站及 HeNB。

五、建議本檢測規範納入 NCC 型式認證要求中，讓電信業者確保購置設備，能符合本檢測規範之要求。

六、建議本檢測規範草案邀請設備製造商座談。

捌、會議結論：

一、 請遠傳電信於107年4月20日前回覆本檢測規範草案意見表予 TTC。

二、 請遠傳電信協助提供4G 基站前三項主要使用之廠牌型號供 TTC 參考。

三、 遠傳電信如有可作為測試場域之核網環境及基站等設備，可提供予 TTC 協助檢測，以完善本檢測規範草案。

玖、散會(下午12時30分)

3. 台灣大哥大

研商行動寬頻基站資安檢測技術規範草案(場次1)會議紀錄

壹、時間：107年4月13日(星期五)下午13時30分

貳、地點：本會濟南路辦公室6樓中型會議室

參、主席：吳簡任技正銘仁　　記錄：莊惠婷

肆、出席單位及人員：如附簽到表

伍、主席致詞(略)

陸、行動寬頻基站資安檢測規範草案說明(報告單位 TTC，略)

柒、台灣大哥大發言重點：

1、 檢測項目1.4、3.2及第6大項檢測作業程序為家用基站，建議適用範圍應重新定義。

2、 檢測項目3.7，於作業檢測上，因 NAS 已為加密傳輸，依檢測步驟執行是否可行?

3、 基站之帳號密碼設定說明：設備廠商提供之基站，其帳號皆為固定不可變動，僅能做密碼之變更，業者於初次使用，即會進行密碼變更，不會使用廠商出廠設定之密碼。

4、 因電信業者於網路管理及維運上，皆已導入 ISO27001、27011，建議此規範應針對設備商進行要求，以簡化大基站之檢測作業。

捌、會議結論：

1、 初次登入強制要求變更密碼(檢測項目4.5)，請台灣大哥大協助帶回確認是否可執行。

2、 請台灣大哥大攜回此檢測規範草案內容，並與設備製造商分享，若未來採型式認證是否可配合。

3、 台灣大哥大如有可作為測試場域之核網環境及基站等設備，可提供予 TTC 協助檢測，以完善本檢測規範草案。

4、 請台灣大哥大於107年4月20日前回覆檢測規範草案意見表予 TTC。

玖、散會(下午14時50分)

研商行動寬頻基站資安檢測技術規範草案
會議簽到表-場次一

壹、時間：107 年 4 月 13 日（星期五）下午 13 時 30 分

貳、地點：本會濟南路辦公室 6 樓中型會議室(臺北市濟南路二段 16 號 6 樓)

參、主席：吳簡任技正銘仁

肆、出席者：

台灣大哥大股份有限公司

曾友修

財團法人電信技術中心

蔡明德 高傳紀

王慶璧 施惠婷 劉明 許任銘 王乾隆

本會基礎設施事務處

蔡孟吉 李福鄭

4. 台灣之星

研商行動寬頻基站資安檢測技術規範草案(場次2)會議紀錄

壹、時間：107年4月13日(星期五)下午15時00分

貳、地點：本會濟南路辦公室6樓中型會議室

參、主席：吳簡任技正銘仁　　記錄：莊惠婷

肆、出席單位及人員：如附簽到表

伍、主席致詞(略)

陸、行動寬頻基站資安檢測規範草案說明(報告單位 TTC，略)

柒、台灣之星發言重點：

1、 本檢測規範草案依循之國際規範3GPP TS33.216其適用之基站版別為 R14，規範內容是否適用於目前電信業者所使用的設備版別。

2、 已將此檢測規範草案內容與設備製造商討論，設備製造商認為內容較為簡略，是否可提供詳細之檢測方法、檢測程序予設備製造商參考

3、 本檢測規範草案之多項檢測項目，涉及基站設備本身問題(如加密)，許多內容須由設備製造商確認。

4、 建議本檢測規範草案納入既有射頻器材管制之型式認證，以避免做重複之檢測。

5、 電信業者於網路管理及維運上，皆遵從 ISO27001、27011，作業安全面沒有問題。

6、 基站本身的 Know How 還是在設備製造商，非電信業者能力範圍內。

7、 建議可考慮找設備製造商一起座談，諮詢設備製造商之意見。

捌、會議結論：

1、 因資訊安全無法靠單一方達成，需靠多方合作達成，建議台灣之星如有可作為測試場域之核網環境及基站等設備，可提供予 TTC 協助檢測，以完善本檢測規範草案。

2、 請台灣之星於107年4月20日前回覆檢測規範草案意見表予

TTC。

玖、散會(下午16時20分)

研商行動寬頻基站資安檢測技術規範草案
會議簽到表-場次二

壹、時間：107 年 4 月 13 日（星期五）下午 15 時 00 分

貳、地點：本會濟南路辦公室 6 樓中型會議室(臺北市濟南路二段 16 號 6 樓)

參、主席：吳簡任技正銘仁

肆、出席者：

台灣之星電信股份有限公司

訊極 洪大弼

李好章 [illegible]

彭雪章

財團法人電信技術中心

蔡明德 高[illegible]訊 黃川洋

[illegible]

王[illegible]隆 王慶豐 [illegible]

本會基礎設施事務處

[illegible] 李福[illegible]

5. 亞太電信

研商行動寬頻基站資安檢測技術規範草案(場次3)會議紀錄

壹、時間：107年4月13日(星期五)下午16時30分

貳、地點：本會濟南路辦公室6樓中型會議室

參、主席：吳簡任技正銘仁　　記錄：莊惠婷

肆、出席單位及人員：如附簽到表

伍、主席致詞(略)

陸、行動寬頻基站資安檢測規範草案說明(報告單位 TTC，略)

柒、亞太電信發言重點：

1、 檢測項目2.1之 TLS 加密沒有看到是規範哪一版，建議不要將版本鎖定。

2、 檢測項目5.4基站系統應提供安全事件記錄功能，其所列項目眾多，建議應明確列出具備哪些才是合標。

3、 檢測項目5.9其 CVE 弱點之 CVSS 分數應為多少分以上，建議應明定。

4、 本檢測規範草案之適用範圍與 NCC 規範不同，建議應調整。

5、 本檢測規範草案內容詳細，會後將再與設備製造商討論

6、 建議本檢測規範草案納入型式認證，在型式認證做檢測較為合理。因檢測項目很多，要求業者一一檢測比較困難。

7、 因業者設備會有汰舊換新的情況，建議檢測規範落實時應有日出條款及相關配套措施。

捌、會議結論：

1、 因資訊安全無法靠單一方達成，需靠多方合作達成，建議亞太電信如有可作為測試場域之核網環境及基站等設備，可提供予 TTC 協助檢測，以完善本檢測規範草案。

2、 本檢測規範未來採系統審驗或型式認證本會會再評估，亞太電信可提到意見表回覆中供本會參考。

3、 請亞太電信於107年4月20日前回覆檢測規範草案意見表予 TTC。

玖、散會(下午17時50分)

研商行動寬頻基站資安檢測技術規範草案
會議簽到表-場次三

壹、時間：107 年 4 月 13 日（星期五）下午 16 時 30 分

貳、地點：本會濟南路辦公室 6 樓中型會議室(臺北市濟南路二段 16 號 6 樓)

參、主席：吳簡任技正銘仁

肆、出席者：

亞太電信股份有限公司

李志豪 何佑陽 謝瑋芠
郭家騏 孔儀益

財團法人電信技術中心

蔣明德 高偉紀 黃[illegible]
[illegible]
王乾隆 王慶璽 [illegible]任銘

本會基礎設施事務處

[illegible]
李福[illegible]

(二) 設備商

1. Nokia

行動寬頻基站資安檢測技術規範草案
座談會會議紀錄

壹、時間：107 年 4 月 26 日(星期五)下午 14 時 00 分

貳、地點：TTC 板橋第三會議室

參、主席：林炫佑 副執行長　　記錄：莊惠婷

肆、出席單位及人員：如附簽到表

伍、行動寬頻基站資安檢測規範草案說明報告(略)

陸、Nokia 發言重點：

一、資料保護

(一) 檢測項目 1.2：

1. 本公司基站設備韌體是做為升版用途，Nokia 也設置了相關安全防護，若韌體被修改，該設備將無法使用。
2. 韌體更新的操作，非開放電信業者於網路下載，而是由 Nokia 工程師下載後再交給電信業者，且有設定個別編號。

(二) 基地台不儲存任何用戶資訊，如果取得金鑰被破解，對電信業者僅為損失一座基地台，並無法竊取任何資料。

(三) Nokia 基地台的金鑰須透過 Nokia 專屬軟體才可使用，沒有經 Nokia 專屬軟體，該金鑰無法使用。

二、應用程式安全

(一) 檢測項目 2.1：Nokia Web 介面並無提供修改的權限，且有限定使用者可使用的功能，且無提供使用者上傳的選項。

三、身分鑑別與授權安全：建議帳號密碼問題應從系統面管理與網管面搭配，而非只限定單一基站設備，營運商可設置一個認證伺服器，確認身分後才可登入。

(一) 檢測項目 4.5：Nokia 未來產品將會更改設計，若密碼沒有更改將會告警。

1

(二) 檢測項目 4.12：此項功能尚需與總公司確認。

(三) 檢測項目 4.13：因基地台數量龐大，營運商須靠遠端方式維護，故建議遠端的定義應再放寬，可將遠端定義為超過網管機房外的範圍，並可檢視業者實際發生的機率來定義。

四、作業系統安全

(一) 檢測項目 5.6：依電信業者營運經驗，安全事件紀錄都是存在網管。

五、目前電信業者其實定期會找白帽駭客測試，確保其行動寬頻網路之安全。

柒、會議結論：

一、會後將提供本團隊於工研院檢測之 Nokia Small Cell，在檢測項目 1.2 及 2.1 之測試結果畫面，及使用之檢測工具予 Nokia 參考。

捌、散會(下午 16 時 00 分)

財團法人電信技術中心

會議簽到單

時間：107年4月26日(星期四) 14:00~16:00

會議室：板橋_第三會議室

會議：行動寬頻基站資安檢測規範草案座談

主席：林炫佑副執行長 林炫佑

出席人員：

部　門/單　位	姓　名
Nokia	陳仁禪
Nokia	陳建華
TTC	廖志明

1

3

部 門/單 位	姓 名
董事會	黃川源
TTC	王慶豐
〃	蔡明德
TTC 應服組	范惠婷

2

4

2. Ericsson

行動寬頻基站資安檢測技術規範草案
座談會會議紀錄

壹、時間：107 年 5 月 11 日(星期五)上午 11 時 00 分

貳、地點：ERICSSON 會議室

參、主席：TTC 資安組 王慶豐 高級工程師　　記錄：莊惠婷

肆、出席單位及人員：

ERICSSON 李敬偉 協理

王方平 資深協理

林敬坤 資深經理

TTC 資安組 蔡明德 工程師

TTC 應服組 莊惠婷

伍、ERICSSON 發言重點：

一、 本公司產品設備皆遵循 3GPP 規範，已具備相當程度的安全性。

二、 建議行動通訊安全應考量的是整體電信網路系統面之安全，end to end 的安全性，而非僅只限單一元件設備。

三、 GSMA 在安全保證方法上，今年將認可兩家第三方檢測實驗室，針對設備之安全性進行檢測認證，目前 ERICSSON 總公司也在等待 3GPP 與 GSMA 共同發起的檢測認證，待 GSMA 通知後也會配合進行檢測。

四、 為避免設備商須進行重複之檢測認證，建議未來是否於大型基站進口時，檢附已通過國際組織檢測通過之證明文件即可。

五、 3GPP TS33.216 屬較新的規範，實際如何檢測仍需待 GSMA 正式要求 ERICSSON 配合檢測時才有辦法瞭解其每一測試項目之檢測方法及合格認定標準，故目前無法針對 TTC 所草擬之基站資安檢測項目內容一一回覆。

陸、會議結論：

一、 本團隊認同該公司對於資安要求之努力。

1

二、 感謝 ERICSSON 告知本團隊 GSMA 安全保證方法最新執行動態。

三、 本團隊認同行動通訊安全應涵蓋整體網路，但單一元件的安全，亦不可偏廢，建議廠商可在自我宣告表內，提供額外的安全證明，以彌補單一元件的風險。

柒、散會(下午 12 時 00 分)

2

三、 座談會意見回覆

(一) 中華電信

國家通訊傳播委員會

「建置基站資安檢測環境計畫」(第2期)

基站資安檢測規範草案意見表

敬啟者：

國家通訊傳播委員會委託財團法人電信技術中心辦理『建置基站資安檢測環境計畫』(第2期)之研究，為了解各界對於本計畫擬定之基站資安檢測規範草案之看法，特針對相關議題，徵詢各界寶貴意見，將於彙整分析後，研究規劃合宜之基站資安規範草案供主管機關參考，以提升基站安全性，促進我國資通訊產業之長遠發展。

請依所附文件：行動寬頻基站資安檢測規範草案，版本：V1.0(以下簡稱本規範)之內容回覆您寶貴的意見，敬請惠予協助，謝謝。

敬祝 鴻猷大展

財團法人電信技術中心 敬啟

一. 基本資料

1. 貴單位名稱：中華電信
2. 受訪者：陳[redacted]
3. 部門與職稱：資安處工程師
4. 聯絡電話：02-2355[redacted]
5. Email：[redacted]@cht.com.tw

1

二. 整體規範建議

意見回覆
標準適用性
無意見
可實施性
無意見。
完整性
無意見。
適用範圍
1. 由於此規範內容係參照3GPP TS33.216/117/320/820等規格，研擬行動寬頻基站 (含 eNode B 及 Small Cell) 設備主體本身應具備之資安防護，建議 NCC 可比照「行動寬頻基地臺射頻設備型式認證技術規範」規定辦理，將該規範列入 NCC 型式認證檢驗中執行，要求設備供應商於設備上市前通過該資安規範。 2. 基站分類之定義請 TTC 參照行動寬頻基地臺射頻設備技術規範內容，使用詞定義一致化。

2

意見回覆
其他建議
建議針對規範實施前之設備，不溯及既往，或以較低強度之規範要求。

3

三. 檢測項目建議意見

請就本規範所擬訂之檢測項目及內容，提供諮詢意見。

意見回覆
檢測項目及內容
無意見。

4

(二) 遠傳電信

國家通訊傳播委員會

「建置基站資安檢測環境計畫」(第2期)

基站資安檢測規範草案意見表

敬啟者：

國家通訊傳播委員會委託財團法人電信技術中心辦理『建置基站資安檢測環境計畫』(第2期)之研究，為了解各界對於本計畫擬定之基站資安檢測規範草案之看法，特針對相關議題，徵詢各界寶貴意見，將於彙整分析後，研究規劃合宜之基站資安規範草案供主管機關參考，以提升基站安全性，促進我國資通訊產業之長遠發展。

請依所附文件：行動寬頻基站資安檢測規範草案，版本：V1.0(以下簡稱本規範)之內容回覆您寶貴的意見，敬請惠予協助，謝謝。

敬祝 鴻猷大展

財團法人電信技術中心　敬啟

一. 基本資料

1. 貴單位名稱：遠傳電信股份有限公司
2. 受訪者：賴[redacted]
3. 部門與職稱：Network & Technology 技術經理
4. 聯絡電話：0989[redacted]
5. Email：[redacted]@fareastone.com.tw

1

二. 整體規範建議

意見回覆
標準適用性
請就標準適用性，如本規範內容是否適用國內行動寬頻網路環境等面向提供諮議意見。 1. 查規範著實協助所有通訊產業落實設備依國際標準進行開發，另方面也督促設備製造商重視資訊安全的重要性，在未來裝置多元化的狀況下，將可以有效降低類似過去所發生的 IPCAM 所引發的 DDOS 攻擊，本公司配合此法案之推動及導入。 2. 本草案所提及之3GPP 標準功能為在單一設備端之功能，然而電信業者之網路規劃與管控係以全面標準及制度化之考量為基礎，並在2010年時，於國家通訊傳播委員會之指導之下導入 ISO27001及27011增項之認證，並且每半年進行外部第三單位的稽核認證，本公司也於2014年獲得 BS10012認證，將相關的資訊安全提升至更高的水準。 3. 在現行電信業者建設之前，需取得國家通訊傳播委員會事業計畫書及建設計畫書的同意，並採購取得型式認證合格之設備。該技術規範草案應更具體實踐現行電信管制射頻器材審驗辦法第四條第二款之國際標準組織所定標準。有鑑於該法現行機制已順利運行一段長時間，為快速導入推動該部分資安檢測技術規範的前提下，建議電信管制射頻器材審驗辦法第四條具體化增加相關資安條文或附件，亦或是進行行政指導，可有效縮短修法時程。並要求設備商所提供之基地臺設備包括射頻及基頻設備，必需通過資安檢測後方能取得型式認證。 4. 現行各業者基地臺設備無論於門禁管制，帳號密碼之管控，皆已通過 ISO27001及 ISO27011增項之要求，各大型基地臺都以專線電路進行連接後端核心網路。非走專線電路之小型家用基地臺設備，為避免開網路後門，也導入 IPsec 之機制，並以 DMZ 架構為前提設置 security gateway，大幅降低單一基地臺設備的因資訊安全所造成的影響性。
可實施性
請就可實施性，如(1)技術上的可行性；(2)建置成本的合理性等面向提供諮議意見。 1. 本草案建議回歸至原始設備進口時需取得型式認證時同時進行，將可以提升可行性，並降低受測單位之成本。 **2.** 現行電信營運商之資安認證架構及基地臺設備加入營運提供服務流程，已經可以提供高品質資安管控，無需額外成本進行相關投入。
完整性
請就本規範所訂之檢測規範項目之完整性提供諮詢意見。 **請參考標準適用性回覆。**

2

意見回覆
適用範圍
請就本規範所擬訂之適用範圍，提供諮詢意見。 **請參考標準適用性回覆。**
其他建議
歡迎就本規範內容提出任何建議或修訂意見。 **請參考標準適用性回覆。**

3

三. 檢測項目建議意見

請就本規範所擬訂之檢測項目及內容，提供諮詢意見。

意見回覆
檢測項目及內容

4

(三) 台灣大哥大

國家通訊傳播委員會

「建置基站資安檢測環境計畫」(第2期)

基站資安檢測規範草案意見表

敬啟者：

國家通訊傳播委員會委託財團法人電信技術中心辦理『建置基站資安檢測環境計畫』(第2期)之研究，為了解各界對於本計畫擬定之基站資安檢測規範草案之看法，特針對相關議題，徵詢各界寶貴意見，將於彙整分析後，研究規劃合宜之基站資安規範草案供主管機關參考，以提升基站安全性，促進我國資通訊產業之長遠發展。

請依所附文件：行動寬頻基站資安檢測規範草案，版本：V1.0(以下簡稱本規範)之內容回覆您寶貴的意見，敬請惠予協助，謝謝。

敬祝 鴻猷大展

財團法人電信技術中心　敬啟

一. 基本資料

1. 貴單位名稱：台灣大哥大(股)公司
2. 受訪者：曾[redacted]
3. 部門與職稱：無線網路規劃暨管理處
4. 聯絡電話：+886-922[redacted]
5. Email：[redacted]@taiwanmobile.com

1

二. 整體規範建議

意見回覆
標準適用性
請就標準適用性，如本規範內容是否適用國內行動寬頻網路環境等面向提供諮議意見。 此規範(檢測項目)大部份適用於大基站(本公司未使用小基站)，項目1.4、3.2檢測作業程序為家用基站，適用範圍建議排除大基站
可實施性
請就可實施性，如(1)技術上的可行性；(2)建置成本的合理性等面向提供諮議意見。 項目1.4、3.2，技術上可行，但實務上及檢測作業程序為家用基站，建議修正檢測適用範圍。 項目3.7，於作業檢測上，因NAS已為加密傳輸，依檢測步驟執行是否可行?
完整性
請就本規範所訂之檢測規範項目之完整性提供諮詢意見。 針對大基站此規範之檢測規範項目完整，暫無其它意見。

2

意見回覆
適用範圍
請就本規範所擬訂之適用範圍，提供諮詢意見。 本公司已於2012年導入 ISO27001、27011資訊安全稽核，此 ISO 標準涵蓋面向依資產類別進行各項目的風險管控及稽核，其範圍及項目、細節等遠大於此規範所列，並每半年由第三方 ISO 單位進行實地稽核，可取代此規範之檢核。 建議針對設備商進行規範要求，以簡化檢測作業。
其他建議
歡迎就本規範內容提出任何建議或修訂意見。 暫無其它意見。

3

三. 檢測項目建議意見

請就本規範所擬訂之檢測項目及內容，提供諮詢意見。

意見回覆
檢測項目及內容
項目1.4、3.2檢測作業程序為家用基站，適用範圍建議排除大基站 建議針對設備商進行規範要求，以簡化檢測作業。

4

(四) 台灣之星

JP

2018/4/20 (週五) 上午 11:25

[redacted](彭[redacted]@tstartel.com>

RE: 覆1070413 13:30 研商行動寬頻基站資安檢測技術規範草案出席人員，請查照。

收件者 莊惠婷(ting)

副本 [redacted]

莊小姐,

關於行動寬頻基站資安檢測技術規範草案，本司意見如下，請參考。

1. 基地臺資安事屬重要，建議由源頭管理，務使有疑慮的設備勿建置於本國行動網路。
2. 因此建議基地臺各項資安查測，併入基地臺設備型式認證項目內，以做到源頭管理。
3. 業者依據電信管制射頻器材管理辦法第十一條規定建設取得型式認證的基地臺設備。
4. 既有設備驗證部分，考量設備機密及技術等因素，且台灣行動業者所使用基地臺廠牌僅限NOKIA/Ericsson二家，建議請原廠提供設備測試，以使測試趨於完善。

電信管制射頻器材管理辦法第十一條規定

需電臺執照之電信管制射頻器材，除法令另有規定外，應經型式認證、審驗合格，並應領有電臺架設許可證、電臺執照或專案核准文件，始得設置、持有。

以上

台星 彭[redacted]

(五) 亞太電信

2018/4/24 (週二) 上午 09:01

游[redacted]<[redacted]@aptg.com.tw>

FW: 研商行動寬頻基站資安檢測技術規範草案出席人數

收件者 莊惠婷(ting)

副本 [redacted]

您已於 2018/4/24 上午 09:20 回覆此訊息。

莊小姐您好，日安

有關行動寬頻基站資安檢測技術規範草案，本公司綜整意見如下，敬請　卓參：

一、建議修正草案內容第三節用語釋義大基站及小基站發射功率，應與現行動寬頻業務相關法令規範基地臺定義一致(P6)。

二、業者依網路佈建需求屬性不同所規劃採購之設備類型也有所不同，而國內業者目前所使用之基地臺，均由國外設備商引進，業者在選商時，亦從設備商已取得國內型式認證之廠牌型號為採購標的。

三、鑑於行動通信基地臺佈建綿密，其資安更是重中之重，為利業者採購符合資安規範之設備，建議基站之資安檢測，應回歸源頭辦理型式認證時，由設備商申請檢測，經由檢測合格後發予證書，卑使業者在選商時，做為必要規格要項之一。

四、誠如規範草案前言所述， 全國各地佈建了超過 8 萬座基地臺，且隨著 5G 時代來臨，未來小基站佈建需求更將愈來愈多，建議本檢測技術規範草案，應訂合理之日出條款，不溯及既往，以降低改善成本，避免耗費資源。

以上說明，若有任何疑義或未盡事宜，歡迎隨時與本公司聯絡，謝謝！

游[redacted]

亞太電信 網路技術中心 工程及電信監理部

附錄六 研討會簡報

行動寬頻基站資安研討會簡報

一、 行動寬頻基站資安研討會議程

時間	議程	主講人
13:00～13:30	報到	
13:30～13:50	主持人致詞 貴賓致詞	財團法人電信技術中心 林炫佑副執行長 國家通訊傳播委員會 吳銘仁簡任技正
13:50～14:10	建置基站資安檢測環境計畫介紹	財團法人電信技術中心 蔡志明主任
14:10～14:30	國際行動寬頻資安政策及規範最新脈動－國際資安政策	財團法人電信技術中心 陳志宇研究員
14:30～14:50	國際行動寬頻資安政策及規範最新脈動－國際標準規範	國立中山大學資工系 黃政嘉博士
14:50～15:10	休息(用茶點)／檢測展示參觀及交流	
15:10～15:40	行動寬頻基站資安檢測規範草案	財團法人電信技術中心 蔡明德工程師
15:40～16:10	HeNB檢測結果及防護建議	財團法人資訊工業策進會 高傳凱 博士
16:10～16:30	TTC行動寬頻資安檢測場域	財團法人電信技術中心 許任銘工程師
16:30～16:40	Q & A	
16:40～16:50	會議結束	

指導單位 國家通訊傳播委員會 NATIONAL COMMUNICATIONS COMMISSION

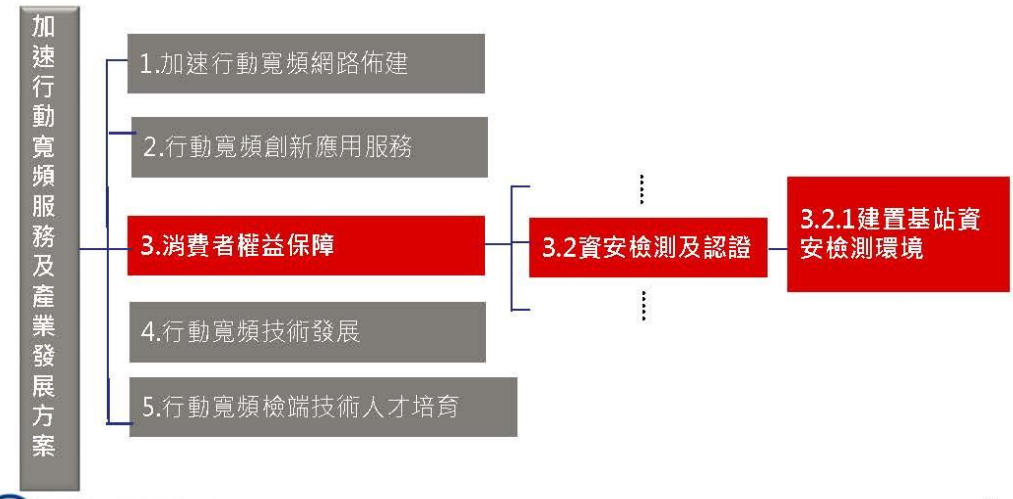
主辦單位 財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

二、 行動寬頻基站資安研討會簡報

1. 建置基站資安檢測環境計畫介紹

計畫背景-政策依據

- 本中心執行國家通訊傳播委員會「建置基站資安檢測環境計畫」委託研究案，該計畫為行政院科技會報辦公室「加速行動寬頻服務及產業發展方案」推動策略之一。



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

3

計畫目標

一、研析行動寬頻資安檢測技術
結合學界、研究機構及產業專家組成專業行動寬頻資安研究團隊，研析行動寬頻基站資安相關檢測規範及技術。

二、建構行動寬頻基站資安檢測平臺
整合國內既有檢測環境及NCC採購之檢測工具，建構一示範性之行動寬頻基站資安檢測平臺。

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

四、提升行動寬頻網路服務安全
協助電信業者及廠商，提升國內行動寬頻網路之服務安全。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

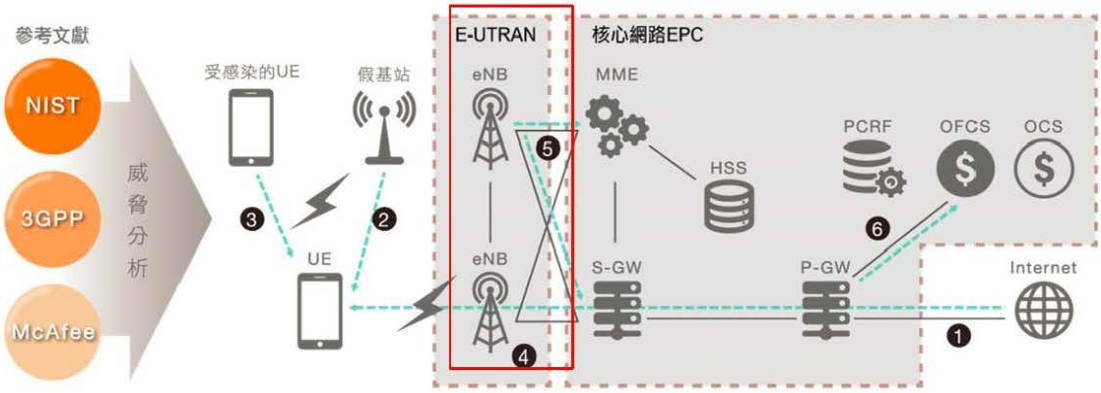
4

計畫概述-行動寬頻網路風險疑慮

行動寬頻網路(4G LTE)六大風險層面

❶外來網路訊務量威脅 ❷無線訊號威脅 ❸行動裝置間的威脅;
❹系統、軟體漏洞威脅 ❺核心網路內部通訊介面威脅 ❻干擾網路服務。

基站(eNB)為EPC核心系統主要入口➔易成為安全威脅目標

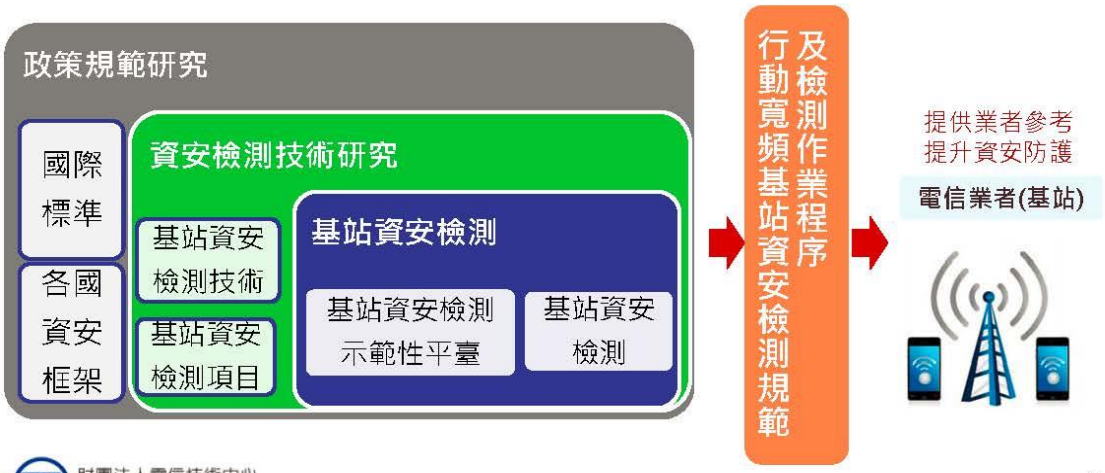


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

5

計畫概述-研究範疇

- 透過國際規範及資安檢測技術研究規劃基站資安檢測項目、建構基站資安示範性平臺執行實測驗證，最終參考實測結果，規劃適合國內環境之基站資安檢測規範草案與檢測作業流程，供產官學界參考。



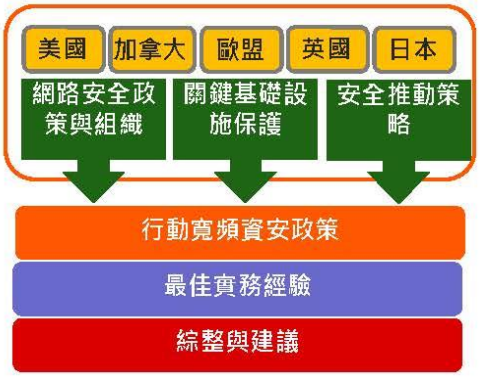
財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

執行成果-掌握國際資安標準最新脈動

掌握最新行動寬頻國際資安框架及標準最新脈動，供國內產官學界參考，並做為本計畫研擬行動寬頻基站檢測規範草案之依據。

國際資安框架



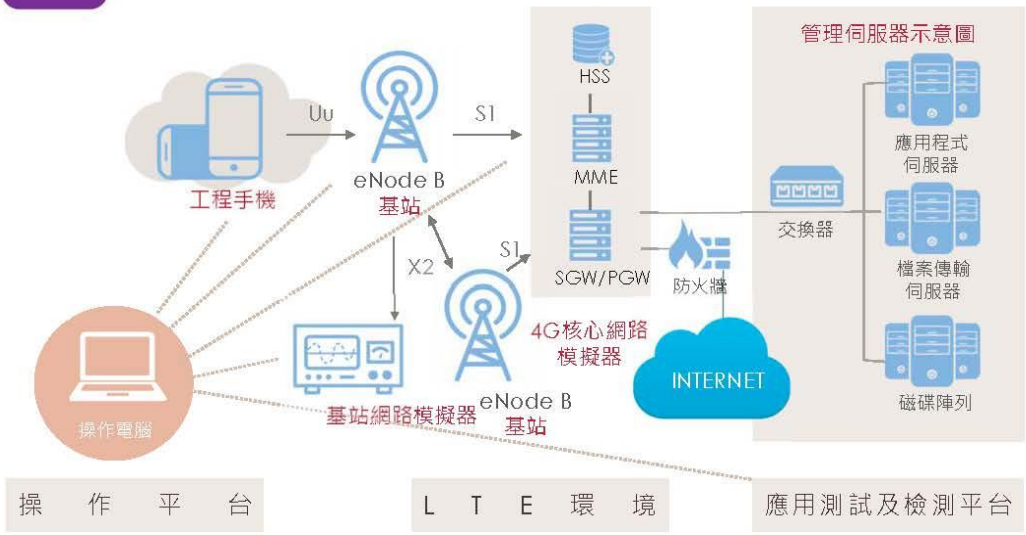
3GPP TS33標準系列最新脈動

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

7

執行成果-基站資安檢測示範性平臺

以模組化方式完成基站資安檢測示範性平臺組建，達成高彈性及高擴充性之目的。



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

8

執行成果-行動寬頻基站資安檢測規範草案

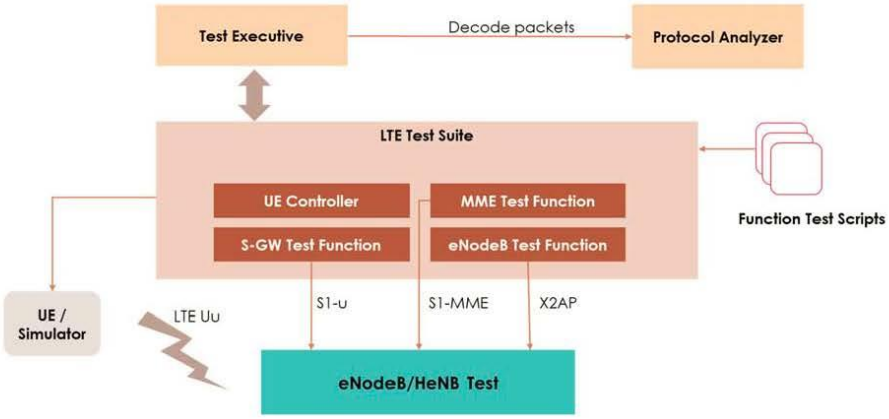
參考國際標準3GPP TS33.216及3GPP TS33.320、TR33.820，並經本團隊實測後，歸納出六大類及37項之檢測規範草案建議。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

9

執行成果-行動寬頻基站資安實測

本團隊以本計畫所提出之基站資安檢測示範性平臺架構及檢測框架，已完成3台基站(eNB)及2台HeNB實測，並綜整出基站資安風險及防護建議。



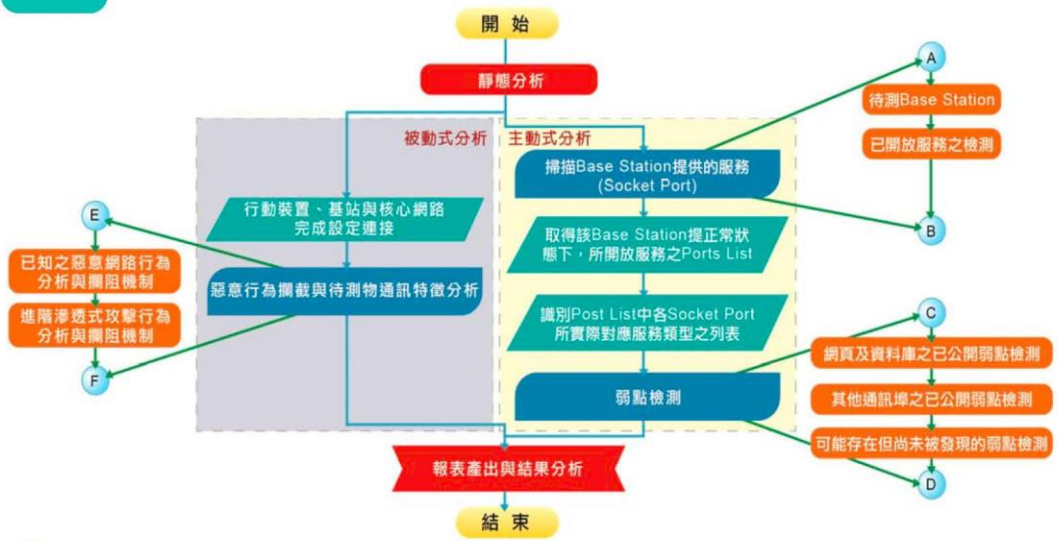
基站檢測框架

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

10

執行成果-行動寬頻基站資安檢測流程

從靜態分析、被動分析及主動式分析，提出基站資安建議之檢測流程及檢測方法。



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

11

效益與願景

本中心期能以本計畫所建置之基站資安檢測環境能量，持續延伸，提倡並輔導國內業者進行自主性檢測，協助行動寬頻資安網路風險之評估，在多方合作下，提升國內行動寬頻網路之安全。

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

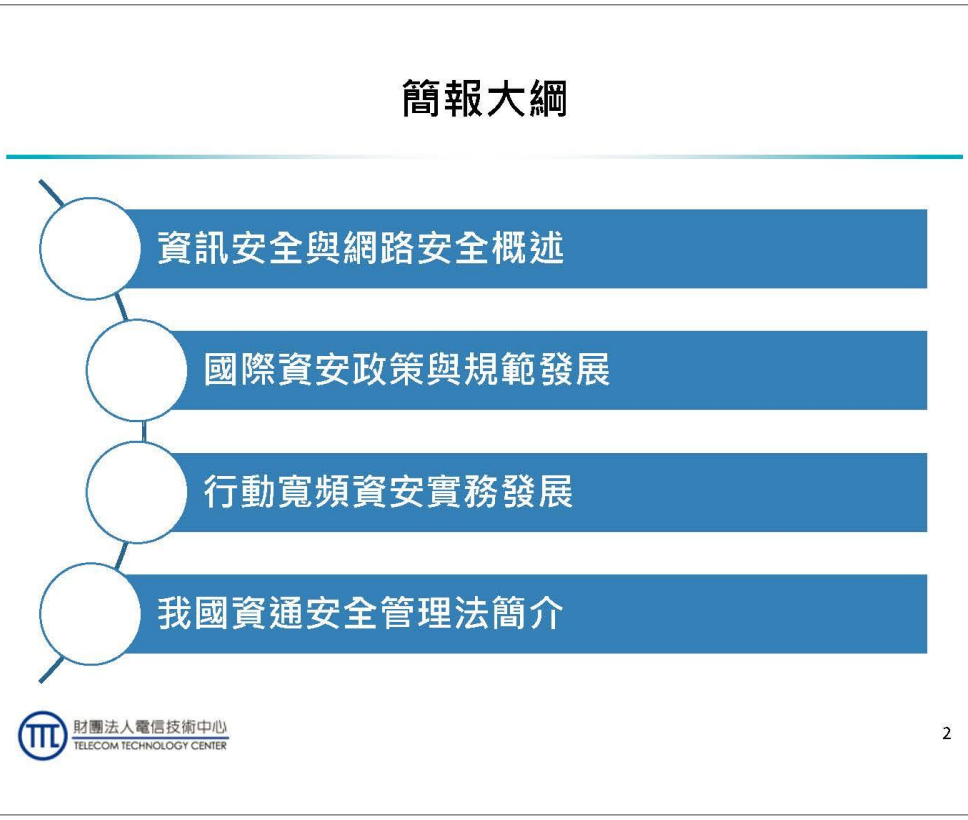
12

敬請指教

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

13

2. 國際資安政策最新脈動



簡報大綱

- 資訊安全與網路安全概述
- 國際資安政策與規範發展
- 行動寬頻資安實務發展
- 我國資通安全管理法簡介

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

3

資訊安全與網路安全

OSI網路7層	DoD網路4層(TCP/IP)	
應用層 (Application Layer)	應用層 (Application Layer)	資訊安全 (保護資料不洩漏)
展示層 (Presentation Layer)		
會議層 (Session Layer)		
傳輸層 (Transport Layer)	傳輸層 (Transport Layer)	網路安全 (保護網路不受侵害)
網路層 (Network Layer)	網路層 (Internet Layer)	
資料鏈結層 (Data Link Layer)	鏈結層 (Link Layer)	
實體層 (Physical Layer)		

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

4

資訊安全與網路安全

資安與網安相互整合發揮綜效

網路安全與資訊安全係指強化安全性的不同焦點，也影響政策與技術的不同著重點。兩者需相輔相成，否則無法發揮安全保障的效果。

1. 網路安全

網路整體防禦力的提升

強化網路本身的防禦力，例如以防火牆抵禦攻擊入侵、以身份驗證機制過濾不明使用者，以維護網路運作穩定。

2. 資訊安全

資料安全性的確保

將資料封存於安全的器具中，若不解密即無法獲得資訊。例如以加密技術儲存資料。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

5

簡報大綱

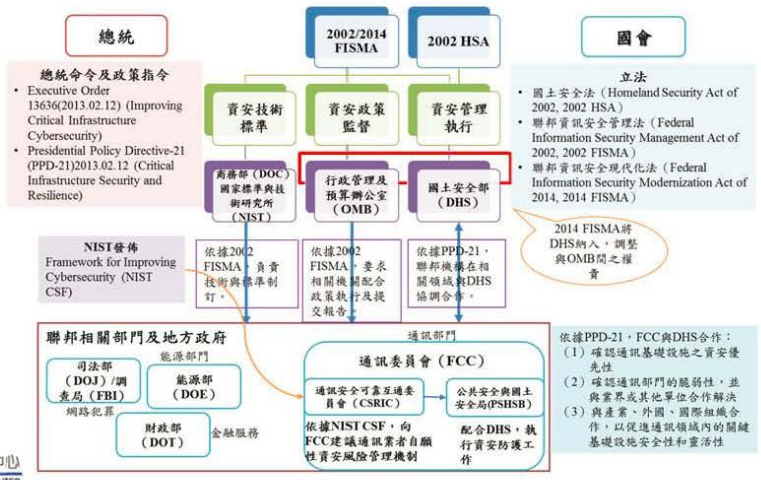
- 資訊安全與網路安全概述
- 國際資安政策與規範發展
- 行動寬頻資安實務發展
- 我國資通安全管理法簡介

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

美國資訊安全權責架構

- 政策執行與監督：資安政策之制定與監督-OMB，網路安全政策之執行-DHS，並就特定產業(能源、交通、通訊)與各產業主管機關協調合作。
- 資通安全標準制定：NIST，各產業主管機關依NIST制定之架構，提供指引。
- 通訊產業：FCC依NIST制定框架，提供有線/無線、廣電、Cable業者資安政策建議。

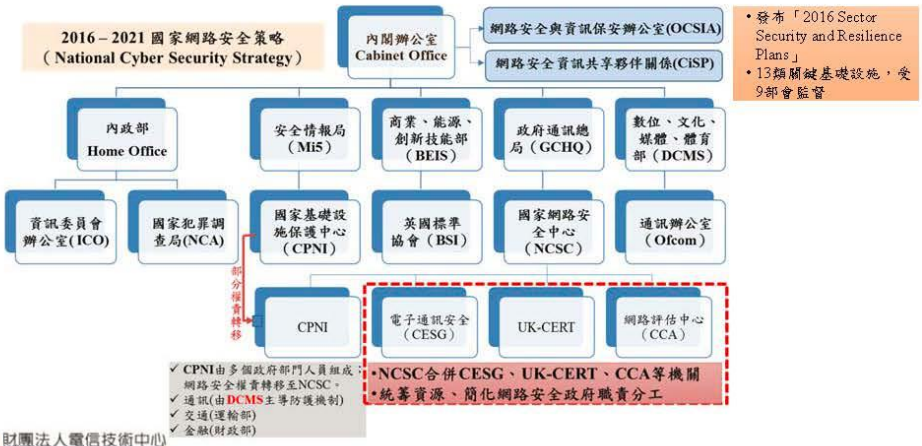


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

7

英國資安體系

- 政策執行：NCSC，負責英國網路安全主要事項，包括資通設備安全、人才培育。
- 資通安全標準制定：BSI，負責制定資通安全管理相關標準。
- 通訊產業：Ofcom依據2003通訊法有監督電信業者資訊安全之責任。
- 資訊共享：透過CiSP機制，分享威脅、風險和資訊交換，並向經濟體發出安全預警。
- 事件通報調查：資安事件須通報ICO，並負責調查(investigation)或稽核(audit)。

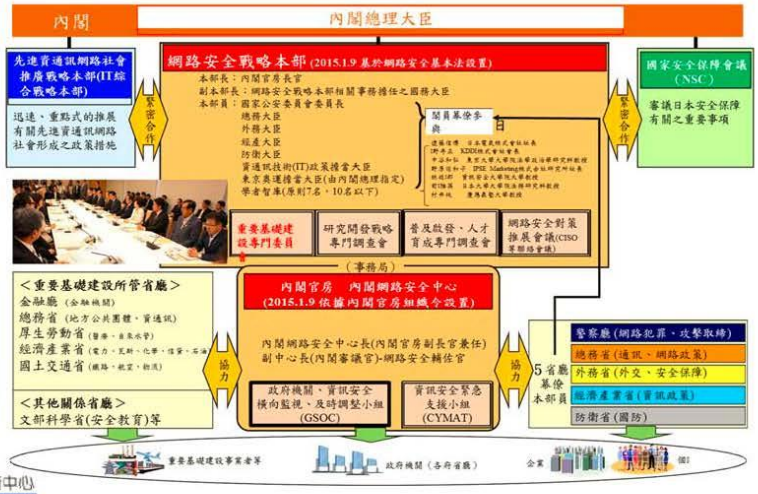


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

8

日本資安體系-日本網路安全政策推展體制 (2015.1.9)

- 政策執行：網路安全戰略本部。
- 資通安全標準制定：經產省，負責產業標準制定（JIS）。
- 通訊產業：總務省負責電信事業管理。



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

9

加拿大資訊安全權責架構

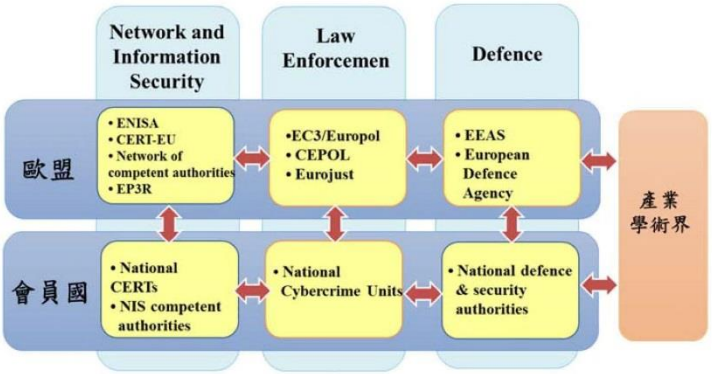
- 政策執行：加拿大資安主責機關為公共安全部，CCIRC為主要單位。
- 標準發展：CSTAC由民間通訊產業與政府公共安全部、通訊安全局、安全情報局等機關的高級主管所組成，針對網路安全威脅議題進行策略合作與資訊交流，亦負責以自律方式推動業者之資安防護。加拿大資安技術標準主要參酌外國標準，如ISO、美國NIST等。
- 通傳產業：CRTC為加拿大通傳產業主管機關，但目前並未具體負責資安相關責任。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

10

歐盟資安體系

- 歐盟係由網路安全局與會員國針對資安議題密切合作、提供資安意見與資安事件解決方案並協助：
  - 泛歐國家發展網路安全策略與建立資安能力
  - 資安事件與網路攻擊研究與分析
  - 支援歐盟制定與實現網路資訊安全政策與法規



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

ENISA : European Network and Information Security Agency
EP3R : European Public-Private Partnership for Resilience

EC3 : European Cybercrime Centre
CEPOL : European Union Agency for Law Enforcement Training
EEAS : European External Action Service

11

歐盟網路安全策略與相關法規

開放 安全 可靠

歐盟網路安全策略

- 實現網路韌性
- 徹底減少網路犯罪
- 發展網路防禦政策和能力
- 發展產業和技術性資源
- 建立完整網路空間政策促進歐盟核心價值

網路安全指令(NIS 指令)--2018年5月實行

- 要求會員國制定國家層級網路資訊安全(NIS)策略、指定國家層級「**主管機關和單一窗口及CERT**」落實指令、執行評估合規性及資訊合作交流。
- 建立行政機關和市場經營者的網路安全法律責任，應對網路安全採取適當的技術和組織措施，重大安全事件須通報主管機關。

一般資料保護規則(GDPR)--2018年5月實行

- 個資的**資料控制者(Controllers)**和**處理者(Processors)**施加安全義務(security obligations)，並強制性要求對個人資料洩漏有通報義務。

支付服務2指令(PSD2)--2018年1月實行

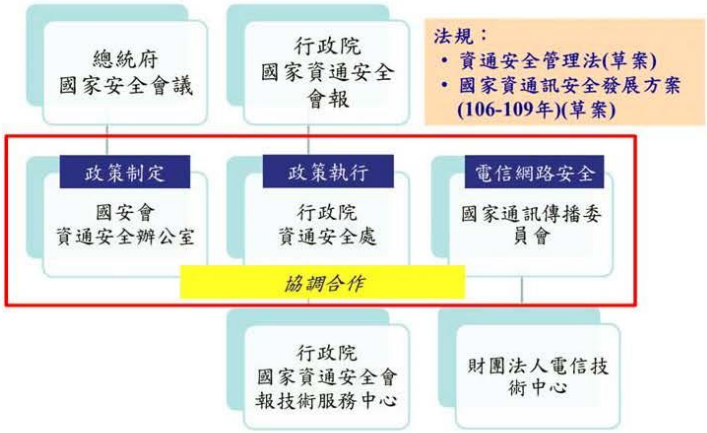
- 配合NIS指令新增管理、違反披露和監理審核的責任條款。
- 對於受影響的組織將有義務向監理機關報告安全事件。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

12

我國資安體系

- ❑ 政策執行：行政院資通安全處。
- ❑ 政策制定：國安會資通安全辦公室。
- ❑ 通訊產業主管機關：NCC。



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

資料來源：iThome, 2016/08/05

13

各國資安體系與任務比較

	美國	英國	日本	加拿大	我國
主要執行機關	國土安全部(DHS) 網路安全與通訊辦公室(CS&C)	政府通訊總局(GCHQ) 國家網路安全中心(NCSC)	網路安全戰略本部(跨部會) 內閣官房 網路安全中心	公共安全部(Public Safety)	行政院 資通安全處
通訊傳播部門主責	DHS (FCC協助)	NCSC (Ofcom協助)	總務省	創新部(ISED) 電訊安全諮詢委員會(CSTAC)	通傳會
技術標準	商務部(DoC) 國家標準技術研究所(NIST)	創新部(BIS) 英國標準協會(BSI)	經產省 JIS標準	公共安全部發展網路事件管理架(CIMF)	CNS國家標準 國際標準
政策監督	白宮 預算辦公室(OMB)	內閣辦公室	內閣官房	總理辦公室	總統府國安會 行政院資通安全會報
防護重點	聯邦重要安全系統	關鍵基礎設施	政府機關及關鍵基礎設施	關鍵基礎設施	關鍵基礎設施
產業資安政策	自律	自律	自律	自律	自律
立法	聯邦資訊管理法(FISMA) 國土安全法(HSA)	2003通訊法賦予Ofcom監督電信業者資料保護之責任	網路安全基本法		資通安全管理法(草案)及子法

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

14

各國資安體系歸納

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

15

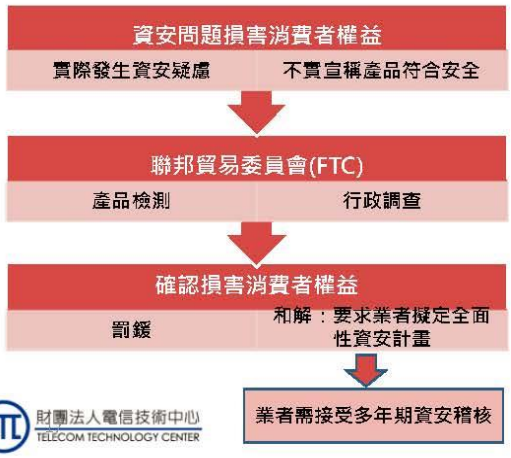
簡報大綱

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

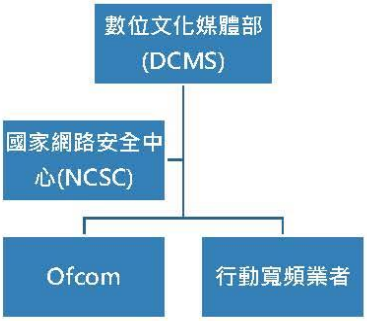
16

行動寬頻資安實務發展（1/6）

- 目前國際間對行動寬頻網路安全之規範主要在關鍵基礎設施上，僅美國及英國有訂定相關之電信事業資安要求：
  - 美國：FTC以消費者保護為基礎，要求電信相關行業(服務商及設備商)做好資安維護。



  - 英國：參考CBEST，推動網路漏洞安全測試計畫。
    - 收集網路威脅資訊
    - 設計攻擊及滲透測試
    - 評估業者網路防禦能力



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

17

行動寬頻資安實務發展（2/6）

國家政策及標準文件

- 國家政策及標準文件
  - 美國NIST SP 800-197 「LTE安全準則(Guide to LTE Security)」
  - 歐盟ETSI TR 103 456「網路與資訊安全指令(NIS指令)之實施(CYBER;Implementation of the Network and Information Security (NIS) Directive)」
- 國際組織技術標準
  - ISO 27001 系列
  - 3GPP TS 33 系列(3GPP Specification 33 series)

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

18

行動寬頻資安實務發展（3/6）

國家政策及標準文件

美國NIST SP 800-197「LTE安全準則(Guide to LTE Security)」

LTE技術架構	LTE安全架構	LTE網路威脅	LTE威脅緩解措施
• 3GPP標準演進 • 基地台到終端網路架構	• 加密 • 空中介面 • 回送網路（backhual） • 核心網路	• 一般網路威脅 • 偽基站 • 空中介面竊聽 • 小型基站攻擊	• 加密 • 身分認證 • 實體安全 • 網路安全

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

19

行動寬頻資安實務發展（4/6）

國家政策及標準文件

歐盟ETSI TR 103 456「網路與資訊安全指令(NIS指令)之實施(CYBER;Implementation of the Network and Information Security (NIS) Directive)」

歐盟NIS指令概述	網路威脅情報分享：資安事件與風險	風險分析在保護NIS所扮演的角色	問題與解決方案建議
• 標準化網路安全資訊分享措施 • 確保會員國之有效合作	• 通知門檻 • 概念、模式與技術方法 • 組織（關鍵服務業者、數位服務業者） • 情報分享平台	• 網路防禦與網路安全風險管理實踐 • 概念、模式與技術方法	• 新科技與服務之衝擊 • 關鍵服務業者與數位服務業者之建議

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

20

行動寬頻資安實務發展（5/6）

公私協力模式(Public Private Partnerships, PPP)
Huawei Cyber Security Evaluation Centre(HCSEC)

- 於2005年英國電信(BT)與華為簽約，成為其傳輸及接取方面之設備供應商；2007年1月華為對BT網路進行相關佈建
- 2008年英國軍情五處(MI5)發布中國可能透過華為通訊設備對英國國內通訊進行攔截或中斷
- 2010年由華為及英國政府同意成立一機構，旨於降低使用華為設備所可能產生的風險
- 2010年11月HCSEC於英國成立，又稱the Cell。由華為出資營運，但由英國通訊總部(GCHQ)共同監管
- 2013年6月情報安全委員會(ISC)提出報告質疑對於HCSEC的在機構自治與員工聘用上的中立性疑慮
- 2013年年底國家安全顧問(NSA)完成調查，基於有接觸華為核心設備需求與商業秘密因素，NSA可理解HCSEC之雇員出自華為的考量，但要求GCHQ亦須從管理面加強對HCSEC之掌控及考核
- 2014年6月HCSEC之監管董事會成立，自2015年起亦逐年發行HCSEC之年度查核報告；並委由安永(EY)會計事務所對其財務、營運及人員聘用進行稽核

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

21

行動寬頻資安實務發展（6/6）

公私協力模式(Public Private Partnerships, PPP)
Huawei Cyber Security Evaluation Centre(HCSEC)

HCSEC 主要業務

由於許多資安漏洞為經由後續下載之更新軟體進行攻擊，因此GCHQ認為HCSEC主要功能為在華為進行大規模更新前，將對其更新之軟體進行資安評估。

HCSEC隨機抽查檢驗即將佈建於英國關鍵基礎建設(CNI)之華為軟硬體產品，以確保產品符合資安要求。

HCSEC 主要效益

2014年研發出一系列弱點檢測工具，在抽象語法樹、符號執行引擎等基礎上，加速分析師在複雜且重複的程式碼中發現問題。

2015年檢驗出3項問題需藉特殊手段介入CSP的網路系統；此問題透過英國政府與CSP之間的標準處理程序解決。

2016年共檢驗20項產品與評估4項解決方案，其範圍涵括英國5家電信營運商。

提供政府及通訊服務提供者(CSP，電信營運商)相關之風險管理預警；開創政府與私人企業合作之新興模式。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

22

簡報大綱

- 資訊安全與網路安全概述
- 國際資安政策與規範發展
- 行動寬頻資安實務發展
- 我國資通安全管理法簡介

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

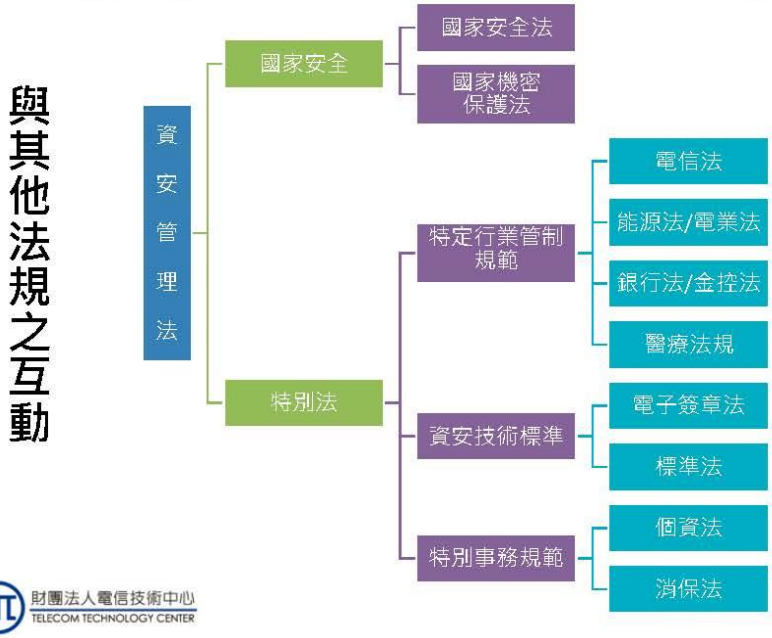
23

資通安全管理法規範重點

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

24

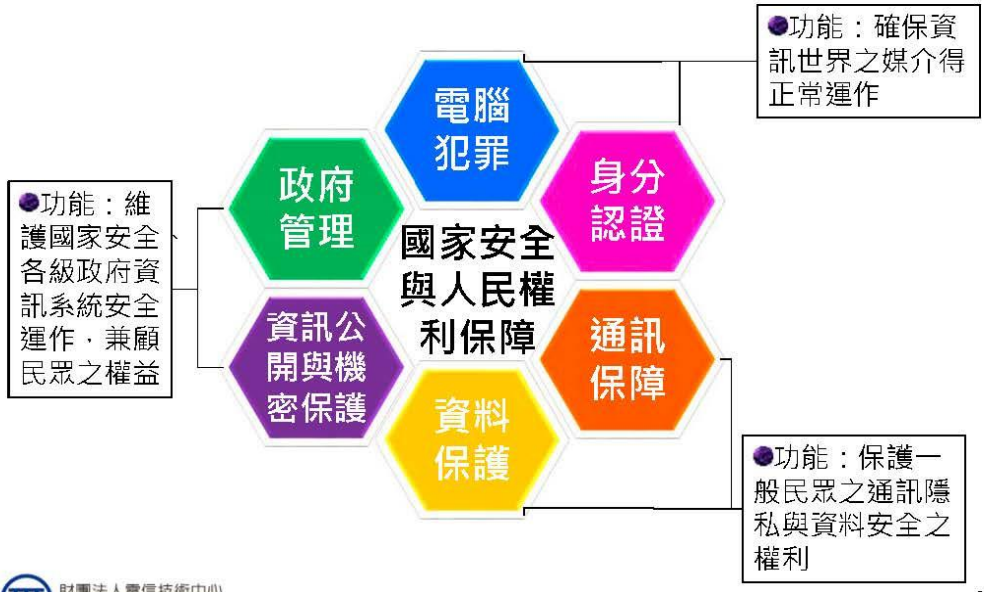
資通安全管理法與其他法規關連性



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

25

資訊安全所涉法規面向



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

26

結語：資安工作的持續精進

- 新型態的資安威脅仍不斷發生
  - 5G新技術的發展帶來新的資安風險挑戰
    - 網路功能虛擬化（NFV）
    - 軟體定義網路（SDN）
  - 小型、家庭基站增加電信業者的資安風險
  - 全IP化網路增加資安的挑戰
  - 偽基站的防制
  - 網路實體安全的維護

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

27

THANK YOU

財團法人電信技術中心

www.ttc.org.tw

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

28

3. 國際行動寬頻標準規範最新脈動

簡報大綱

- 3GPP 33系列基站安全相關技術規範
- 3GPP基站安全相關技術規範概述

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

2

簡報大綱

- 3GPP 33系列基站安全相關技術規範
- 3GPP基站安全相關技術規範概述

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

3

3GPP 33系列基站安全相關技術規範

- 3GPP為制定與推廣行動網路標準之國際標準組織。
- 計畫著眼「基站」的「安全性」，本團隊掌握3GPP安全技術規範33系列，關注其文件的更新動態與焦點。

文件編號	文件名稱	規範內容	發佈日期	檢測/威脅總數
TS 33.401	3GPP System Architecture Evolution (SAE); Security architecture	3GPP網路系統演進架構(SAE)及安全架構	Release8 2008-3-20	無
TS 33.117	Catalogue of general security assurance requirement	網通產品之通用安全保證要求	Release14 2015-9-22	70 項檢測
TR 33.926	Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes	3GPP網路設備類別之安全保證規範的威脅與關鍵資產	Release13 2016-6-17	63 項威脅
TS 33.216	Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class	特定於演進式基站節點(eNB)之安全目標、安全要求及安全檢測項目	Release15 2017-8-24	12項eNB專用檢測+原TS 33.117之70項檢測共82項

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

4

簡報大綱

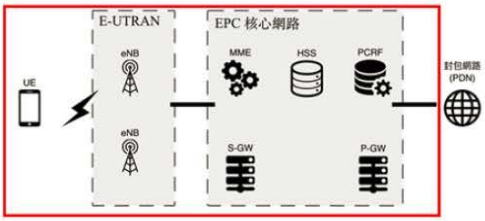
- 3GPP 33系列基站安全相關技術規範
- 3GPP基站安全相關技術規範概述

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

5

TS 33.401-各演進系統之安全架構(1/2)

- 規範內容說明
  - 規範目的：3GPP 提出 **SAE(3GPP System Architecture Evolution)之安全架構定義了LTE系統整體的安全及準則**。
  - 規範內容：包含EPC(Evolved Packet Core，演進數據分組核心網路)、E-UTRAN(Evolved Universal Terrestrial Radio Access Network，演進統一陸地無線接取網路)、EPS(Evolved Packet System，演進數據封包系統)的安全特徵與機制。
    - 定義各元件及階層架構之安全。
    - 定義各控制節點內及兩兩間連結通道的安全機制。
    - 金鑰生成與銷毀。



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

TS 33.401-各演進系統之安全架構(2/2)

◆近期更新重點

① EPC核心網安全性之加強

② eNB安全性之加強

③ LWA之安全架構

英文縮寫	英文全名	中文解釋
HSS	Home Subscribe Server	歸屬用戶伺服器
LWA	LTE-WLAN Aggregation	LTE與Wi-Fi整合技術
NAS	Non-access Stratum	非存取層
RAN	Radio Access Network	無線接取網路
RRC	Radio Resource Control	無線資源控制
WLAN	Wireless Local Area Network	無線區域網路

類別	新增項目
❶ EPC	7.2.4.4 NAS安全模式指令程式
❷ eNB	7.2.11 RRC連線中斷與恢復
❸ LWA	附件A 金鑰生成函式之A.16~A.19 LWA金鑰之生成
❷ eNB	附件E.3 主要與次要eNB間的雙向連線
❶ EPC	附件F.4 對HSS的妥協(Compromise)攻擊緩解與當HSS被妥協時的應對處理
❸ LWA	附件G LTE-WLAN聚合(Aggregation)安全
❸ LWA	附件H 使用IPsec協定完成LTE-WLAN RAN層整合
❶ EPC	附件I $HASH_{MME}$與$HASH_{UE}$

比較版本Release15 Ver. 15.2.0 2018-1-4 V.S. Release13 Ver 13.1.0 2015-12-18

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

7

TS 33.117-網通產品之通用安全保證要求(1/4)

❑ 規範內容說明

➢ 規範目的：為網通產品安全性要求的「目錄」，提出了**適用於一般網路設備類別**的測試案例、測試方法及目標。

➢ 檢測內容：包含網路設備、作業系統、網路伺服器等類別與存取認證、資料完整性、資料防護、漏洞檢測、模糊測試等測試案例。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

8

TS 33.117 網通產品之通用安全保證要求(2/4)

❑ 檢測項目

4.2.3 基本檢測項目
4.2.3.2 資料保護
4.2.3.3 系統可用性及完整性保護
4.2.3.4 認證與授權
4.2.3.5 Sessions防護
4.2.3.6 日誌檔

4.2.5 網頁伺服器
4.2.5.1 HTTPS
4.2.5.2 日誌檔
4.2.5.3 User sessions 的管控
4.2.5.4 網頁管理介面安全

4.3 強化安全需求相關之檢測項目
4.3.2 基本檢測項目
4.3.3 作業系統
4.3.4 網頁伺服器
4.3.5 網路裝置

4.2.4 作業系統
4.2.4.1 一般性作業系統需求及相關檢測案例
4.2.3.3 UNIX作業系統需求及相關檢測案例

4.2.6 網路裝置
4.2.6.1 資料保護
4.2.6.2 可用性與完整性保護

4.4 基本漏洞檢測要求
4.4.2 連接埠掃描
4.4.3 漏洞掃描
4.4.4 強健性與模糊測試

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

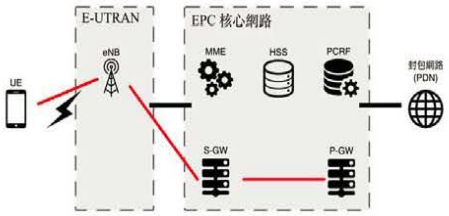
9

TS 33.117 網通產品之通用安全保證要求(3/4)

◆ 近期更新重點

- ➢ 新增了**4.2.6.2.3 GTP-U**的測試案例
  - GTP(GPRS Tunneling Protocol，GPRS通道傳輸協定)
  - GPRS(General Packet Radio Service，通用封包無線服務)
- ➢ **GTP**協定存在於網路層，起初作為**2G**系統的擴充協定，而現在也應用在**LTE**網路，作為**GPRS**核心網的主要協定，處理**UE** 和**PGW**間的溝通。
  - UE(User Equipment，使用者終端裝置)
  - PGW(Packet Data Network Gateway，封包資料網路閘道)

比較版本Release14 Ver. 14.2.0 2017-6-14
V.S. Release13 Ver 1.3.0 2016-5-23



GTP於EPS架構(右圖整體部分)內的作用範圍

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

10

TS 33.117 網通產品之通用安全保證要求(4/4)

◆ 近期更新重點

➢ GTP協定現在包含了以下三個部分：

- GTP-C(GTP-Control)：負責建立、管理與維持通道，Release13中已訂出GTP-C的測試案例。
- **GTP-U**(User Data Tunneling)：用在UE和PGW間用戶資料的傳輸，能相容IPv4、IPv6等封包格式，於Release14新增，目的在於避免攻擊者透過此通道傳送惡意資料，因此系統應要有能力檢查此封包。
- GTP'：用於傳輸計費相關的數據，目前尚未有測試案例。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

11

TR 33.926-網通設備之安全威脅與關鍵資產(1/4)

❑ 規範內容說明

➢ 規範目的：統整3GPP目前已發現網路設備類別相關的安全威脅，並定義GNP(Generic Network Product，通用網路設備)須被保護的關鍵資產。

➢ 規範內容：為一般網路設備共通的安全議題。

GNP關鍵資產	
用戶資料和憑證 (密碼)	Log資料
作業系統	GNP應用程式
組態資料 (GNP的IP位址、連結埠、VPN ID、管理對象等)	足夠的運算能力 (處理能力不會接近臨界點)
硬體 (大型電腦、電路板、電源供應器等)	受保護之GNP介面

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

12

TR 33.926-網通設備之安全威脅與關鍵資產(2/4)

- 規範內容說明
  - 附件針對單一網通元件安全威脅探討，包含以下部分：
    - MME(Mobile Management Entity，移動管理實體)：中管理UE的元件。
    - PGW：支援計費系統、LTE和非LTE技術的切換。
    - eNB(Evolved Node B，演進節點B)：即基站。

MME關鍵資產
行動數據的管理
路由路徑的選擇
MME介面

PGW關鍵資產
UE資料
PGW軟體
PGW介面

eNB關鍵資產
行動數據的管理
eNB軟體
eNB介面

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

13

TR 33.926-網通設備之安全威脅與關鍵資產(3/4)

新增威脅項目	
威脅5.3.4.7 竄改用戶Session	附件C：網路設備類別的eNB相關方面
附件B：網路設備類別的PGW相關方面	C.2.2.1 控制平面的資料保密防護
B.2.2.1 IP位址之連續使用	C.2.2.2 控制平面的資料完整性防護
B.2.3.1 傳送未認證的資料到其它UE	C.2.2.3 用戶在eNB中做的加解密
B.2.4.1 無作用的緊急PDN連接版本	C.2.2.4 用戶明文資料的完整性防護

比較版本Release15 Ver. 15.1.0 2017-9-21 V.S. Release13 Ver 13.1.0 2016-9-30

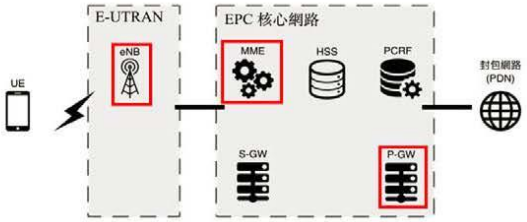
財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

14

TR 33.926-網通設備之安全威脅與關鍵資產(4/4)

◆ 近期更新重點

- 新增特定網通設備之重要資產與安全威脅於附件，包含**PGW**及**eNB**
  - PGW主要能讓UE從外部連線到系統且能支援計費系統，導致**此閘道將來可能成為攻擊者攻擊計費系統的標的**，因而特別將此項目獨立出來。
  - 附件內描述eNB的數種威脅皆為假設若沒有在無線通用網路與核心網之間、或是基站與基站之間做防護時會發生的情況。**eNB的相關測試案例可參考TS 33.216文件**。



附件之網通元件於EPS架構內的位置

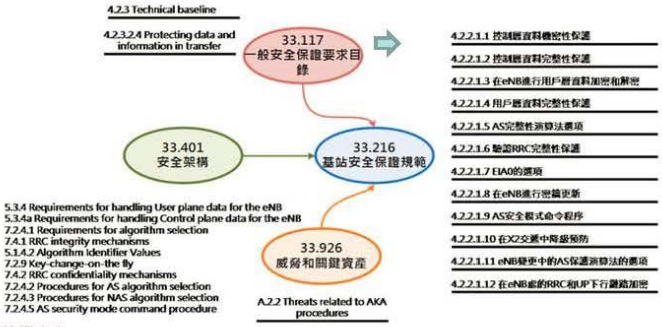
財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

15

TS 33.216- eNB之安全保證規範(1/3)

❑ 規範內容說明

- 因應5G的出現，3GPP組織同步於2016年底釋出TS 33.216的初版文件，並在2017年9月發表正式版。
- 規範目的：與TS 33.117相似，差別在於本份文件提出的是特定於**eNB網路產品的技術要求和測試案例**。
- 本規範的安全定義、安全要求、檢測內容幾乎繼承自前三份文件。



四份文件之關係圖

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

16

TS 33.216- eNB之安全保證規範(2/3)

- 規範參考之標準規範
  - TS 33.401的eNB相關架構之基本安全功能要求。
  - **基於TS 33.117的內容**，採用適合eNB的通用測試案例，增加部分TS 33.117內沒有的檢測內容，確立出eNB專用的測試案例。
  - TR 33.926所述特定於eNB的安全威脅導出之安全要求。如附件A的AKA(Authentication and Key Agreement，認證密鑰協商)安全威脅。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

17

TS 33.216- eNB之安全保證規範(3/3)

- 檢測項目

檢測項目	
4.2.2.1.1 控制層資料機密性保護	4.2.2.1.7 EPS完整性演算法零號選項
4.2.2.1.2 控制層資料完整性保護	4.2.2.1.8 在eNB進行金鑰更新
4.2.2.1.3 在eNB進行用戶層資料加密和解密	4.2.2.1.9 應用伺服器安全模式命令程序
4.2.2.1.4 用戶層資料完整性保護	4.2.2.1.10 在X2交遞中降級預防
4.2.2.1.5 應用伺服器完整性演算法選項	4.2.2.1.11 eNB變更中的應用伺服器保護演算法選項
4.2.2.1.6 驗證無線資源管理訊息完整性保護	4.2.2.1.12 在eNB處的RRC和用戶層的下行連結加密

- 4.2.3節以後之檢測項目和TS 33.117 4.2.3節以後之內容完全相同。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

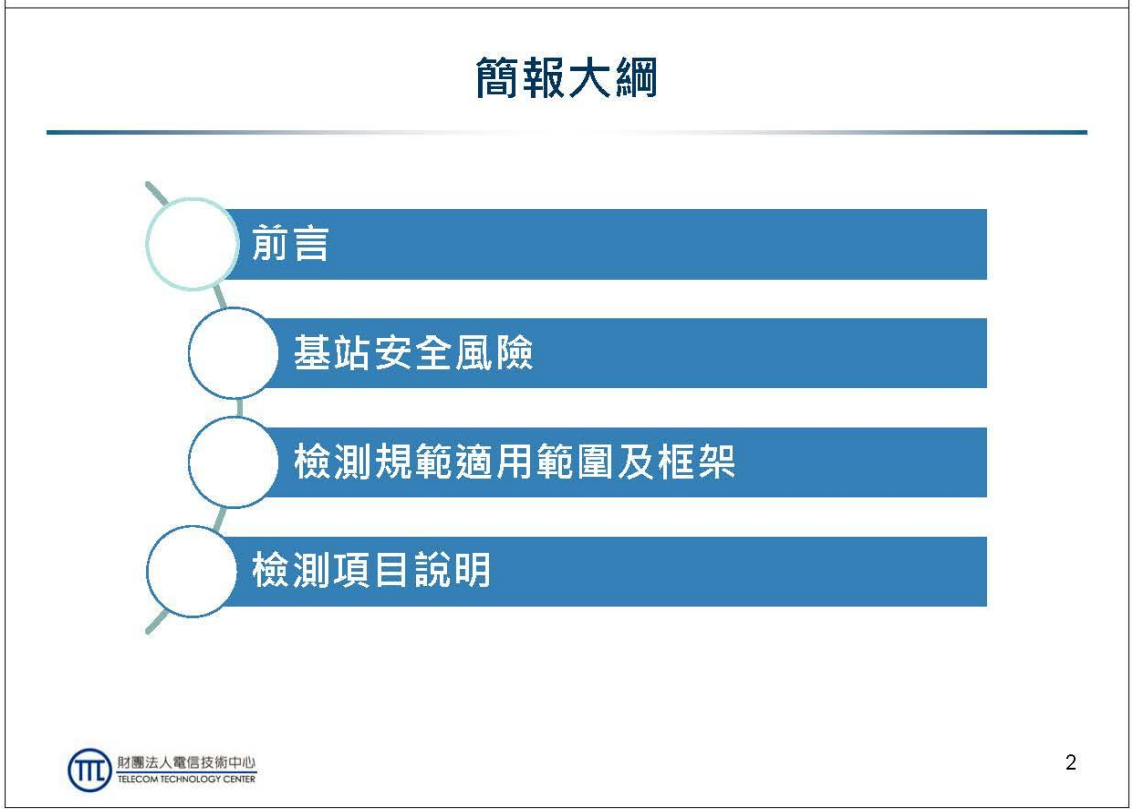
18

敬請指教

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

19

4. 行動寬頻基站資安檢測規範草案



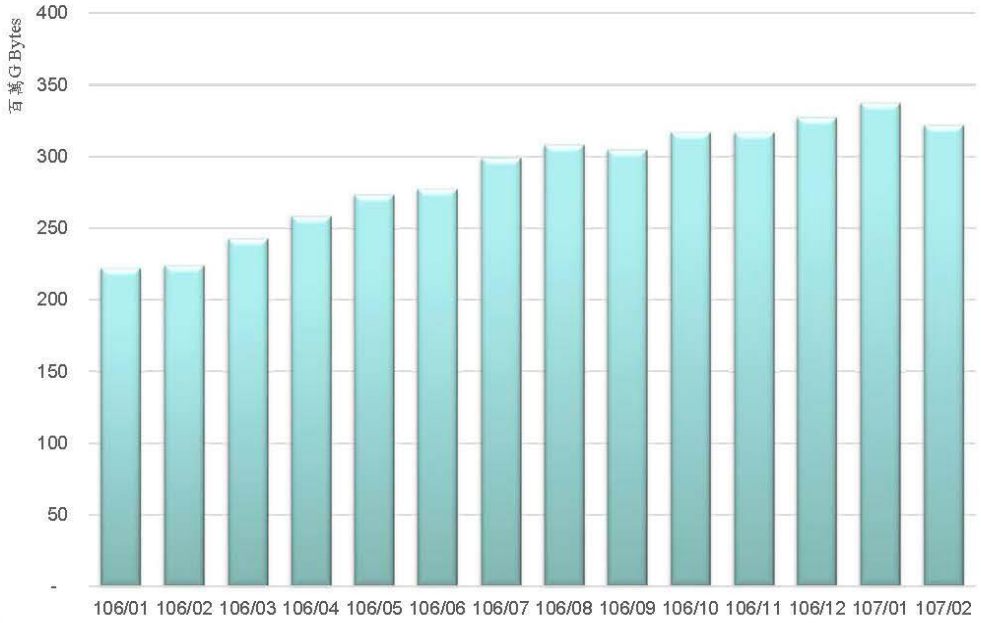
簡報大綱

- 前言
- 基站安全風險
- 檢測規範適用範圍及框架
- 檢測項目說明

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

3

4G數據傳輸量

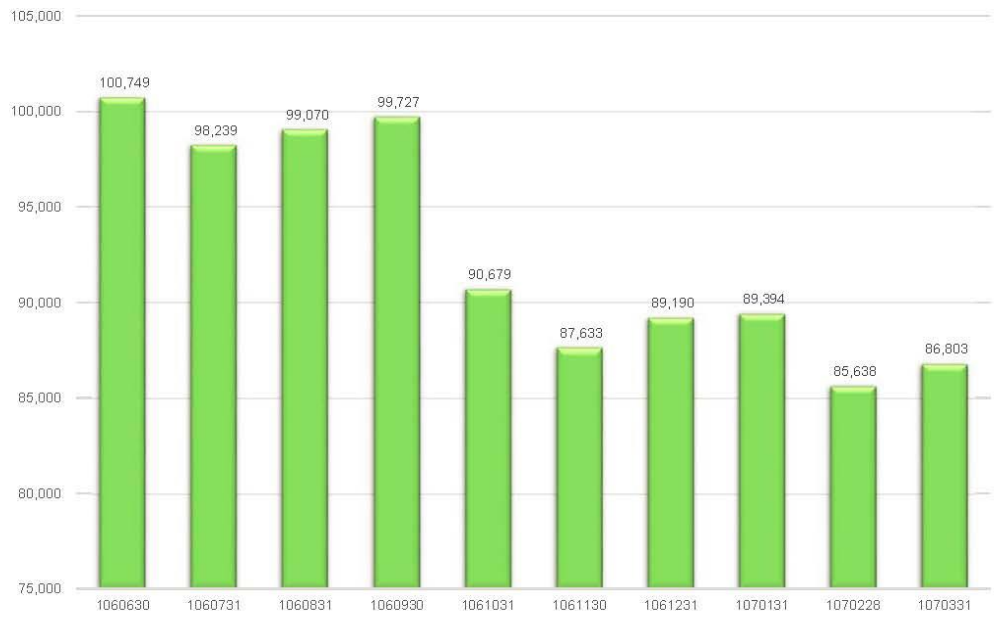


財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

Source: NCC,行動寬頻用戶每月平均數據用量

4

行動通信業務基地臺統計數

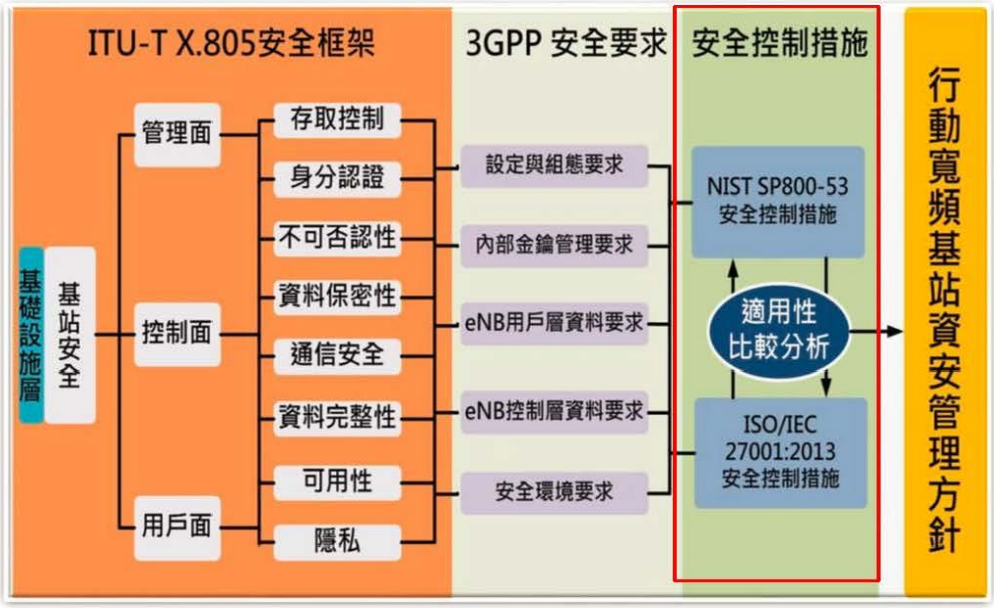


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

Source: NCC, 行動通信業務基地臺統計數

5

行動寬頻基站資安管理



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

簡報大綱

- 前言
- 基站安全風險
- 檢測規範適用範圍及框架
- 檢測項目說明

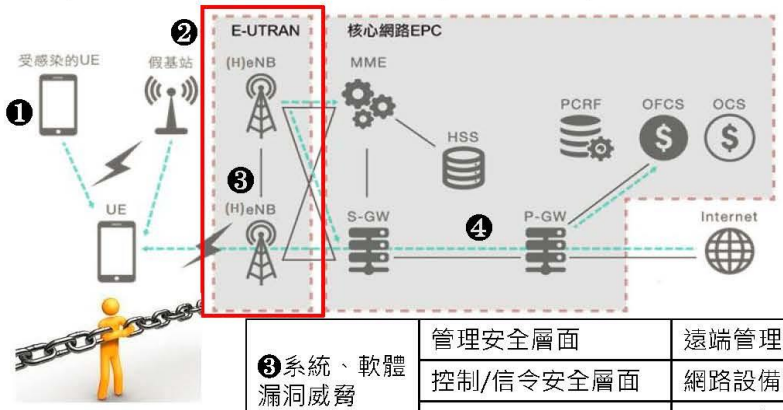
財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

7

基站安全風險

❑ 基站(eNB)為邊界防禦的主體

❶行動裝置間的威脅、❷無線訊號的威脅	用戶安全層面	惡意的使用者終端裝置	❹核心網路內部通訊介面或外部威脅	控制/信令安全層面	傳輸網路威脅
	控制/信令安全層面	空中介面			



❸系統、軟體漏洞威脅	管理安全層面	遠端管理介面
	控制/信令安全層面	網路設備實體接取威脅
	LMT/OS安全	近端與作業的安全管理

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

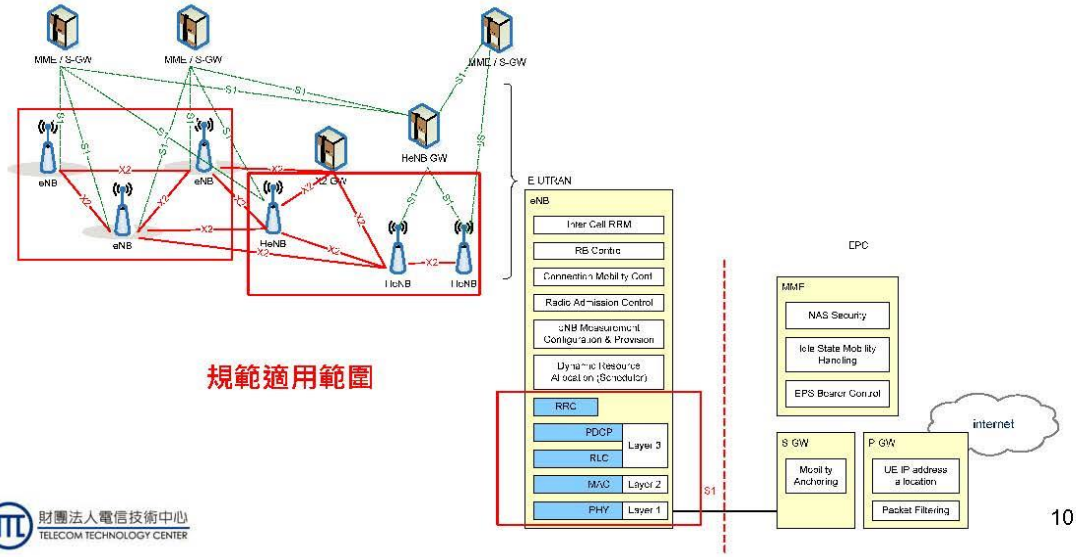
8

簡報大綱

- 前言
- 基站安全風險
- 檢測規範適用範圍及框架
- 檢測項目說明

檢測規範適用範圍

❑ 本規範適用行動寬頻基地台，並依(1)資料保護、(2)應用程式安全、(3)通訊安全、(4)身分鑑別與授權安全、(5)作業系統安全、(6)實體防護六項安全構面，訂定產品安全技術要求。



檢測框架

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

11

簡報大綱

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

12

檢測項目-資料保護

- 資料保護安全測試是為確認產品設計上，是否確保敏感性資料無論是在傳輸或儲存時，都具有外洩防堵的能力，包括敏感性資料存取控管、加解密演算法。

檢測編碼	檢測項目	檢測目的
1.1	敏感性資料外洩防止(系統功能外洩)	確認系統功能不會洩露敏感性資料。
1.2	敏感性資料外洩防止(韌體外洩)	驗證裝置韌體是否含有敏感性資料外洩疑慮。
1.3	敏感性資料儲存保護	基站系統對於敏感性資料應採用適當且有效之加密技術，使資料不會以原來的形式呈現，達到保密的目的，並確保避免遭操作修改。
1.4	憑證唯一性	驗證憑證是否可被偽造。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

13

檢測項目-應用程式

- 應用程式安全測試是為確認產品設計上，網頁管理介面是否存在已知資安弱點威脅，以確保產品之網頁管理介面安全無虞。

檢測編碼	檢測項目	檢測目的
2.1	網站伺服器安全	基站網站伺服器不應存在OWASP Top 10與CWE/SANS 前25 大最危險的程式設計錯誤(CWE/SANS TOP 25 Most Dangerous Software Errors)所載之弱點威脅。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

14

檢測項目-通訊安全(1/2)

- 確認產品設計上，是否符合通訊傳輸介面的安全要求，包括網路服務啟用限制、空中介面通訊安全、傳輸加密技術要求等，確保產品具備可靠之通訊傳輸功能。

檢測編碼	檢測項目	檢測目的
3.1	系統使用之協定或服務安全	基站系統在預設條件下應只執行需要的協定和服務，業者實際維運階段之不同任務原因，可將原本未啟用協定與服務視需要予以暫時性啟用與做適當管理。
3.2	系統與對外之網路傳輸安全	基站系統與其他外部設備之網路傳輸過程中須加密保護，且不應使用或支援已被公開認定之弱加密技術。
3.3	控制層資料機密性保護	基站應對S1 /X2 參照點的控制層封包進行機密性保護
3.4	控制層資料完整性保護	基站應對S1 /X2 參照點的控制層封包進行完整性保護
3.5	存取層之完整性演算法選擇	(1) 服務網路(serving network)應依據UE所支援的安全功能與目前服務網路所設定許可之安全功能清單，選擇欲使用的演算法。 (2)基站應透過設定可用的演算法清單，包括完整性演算法清單，並由電信業者決定優先排序。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

15

檢測項目-通訊安全(2/2)

檢測編碼	檢測項目	檢測目的
3.6	無線資源控制訊息完整性保護	應管控行動裝置與受測物RRC完整性驗證情形。
3.7	基站金鑰更新	當基站交遞時，為避免使用相同金鑰，基站應具備觸發基站金鑰(KeNB)的金鑰更新功能。
3.8	存取層安全模式指令程序	基站應從優先清單中，選擇最高順位之完整性演算法保護SECURITY MODE COMMAND訊息。
3.9	X2交遞中降階攻擊之防範	在路徑變更(path-switch)訊息中，目的基站應對MME傳送從來源基站接收的UE EPS安全性功能。
3.10	存取層演算法之選擇	(1) 目的基站應根據其本身演算法優先列清單選擇UE EPS之安全性功能最高順位的演算法 (包含完整性演算法與加密演算法)。若是所選擇的演算法與來源基站所選擇的不同，應透過交遞指令通知UE。 (2)驗證有正確選擇保護演算法。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

16

檢測項目-身分鑑別與授權安全(1/3)

- 確認產品設計上，於身分鑑別與授權機制之強度，包括權限控管、通行碼機制複雜度、身分鑑別機制強度等。

檢測編碼	檢測項目	檢測目的
4.1	系統功能之存取控制	登入至基站系統包含網路服務(SSH、SFTP、Web Service)、透過本機管理介面存取使用，都須完成身分認證與授權機制後才可以使用系統各項功能。
4.2	身分鑑別有效性	基站系統的使用者身分鑑別機制須至少帳號與一個身分鑑別因子，包含加密金鑰(Cryptographic keys)、Token或密碼。
4.3	系統預設帳號之管控	基站系統預設帳號應可設置停用或修改初始預設密碼
4.4	密碼複雜性	基站系統應支援與設定不同組合之密碼複雜性規格
4.5	通行碼變更機制	基站系統應支援可提供隨時更改密碼之功能，並且系統預設密碼應於初次登入階段強制要求變更，且支援變更密碼內容不得超過特定重複使用次數功能設定。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

17

檢測項目-身分鑑別與授權安全(2/3)

檢測編碼	檢測項目	檢測目的
4.6	暴力及字典攻擊防護	基站系統應具備暴力及字典攻擊的防護措施，例如使用網頁介面設置CAPTCHA功能、嘗試登入失敗次數限制與鎖定帳號時間等功能。
4.7	通行碼顯示遮罩	基站系統在通行碼的設計不會以原來的形式呈現，達到保密的目的，並確保避免遭操作修改。
4.8	通行碼認證錯誤處理機制	基站系統應具備連續登入失敗處理機制，並可限制最大連續輸入失敗次數與強制鎖定可登入延遲時間。
4.9	授權策略	基站系統應具備依不同帳號給予不同授權之設定機制，確保受測物之授權策略，針對特定資訊僅給予具備權限之帳號存取。
4.10	角色存取控制	基站系統應支援基於帳號角色之存取控制。使用一系列控制方式來確定帳號如何進行系統功能存取與故障管理維護。
4.11	登出功能	基站系統應支援登入之帳號可隨時登出之功能，並於登出階段提供是否登出系統之提醒畫面。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

18

檢測項目-身分鑑別與授權安全(3/3)

檢測編碼	檢測項目	檢測目的
4.12	操作逾時功能	基站系統應限制當帳戶操作逾時超出設定時間，系統即將該帳號給予強制登出。
4.13	系統登入之權限控管	基站系統應限制最高管理權限帳號不可從遠端登入，降低被攻擊的風險。
4.14	檔案系統存取權限控管	基站系統具備檔案系統存取權限控管機制，僅有授權之帳戶可修改作業系統層級之檔案、資料或系統檔案等。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

19

檢測項目-作業系統安全(1/2)

- 為驗證產品之作業系統上是否增加資安防護能力，與已知資安漏洞的修補程度。

檢測編碼	檢測項目	檢測目的
5.1	日誌檔之敏感性資料外洩防止	驗證產品之敏感性資料是否不會明文顯示於日誌檔中
5.2	安全開機	驗證產品是否只能經由指定的記憶體裝置啟動
5.3	軟體完整性	基站系統應具備軟體安裝時完整性檢測，確保基站廠商發佈之軟體與已安裝的軟體相同，驗證軟體是否已遭受修改
5.4	安全事件記錄功能	基站系統應提供配置修改變更之安全事件紀錄

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

20

檢測項目-作業系統安全 (2/2)

檢測編碼	檢測項目	檢測目的
5.5	安全事件紀錄備存	基站系統應提供可將安全事件紀錄功能傳輸備存至集中管理設備或其他外部系統設備，並傳輸過程使用加密技術保護
5.6	安全事件紀錄之存取控制	基站系統之安全事件紀錄應僅有特定權限帳號可以存取
5.7	高權限系統功能之存取控制	驗證擁有特殊權限的系統功能是否經過認證與授權方可使用
5.8	自動播放功能禁用	驗證當產品被接入卸除式媒體(如:USB)時，是否會自動執行應用程式
5.9	作業系統及網路服務安全	系統本身不應存在重大風險已知弱點漏洞

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

21

檢測項目-實體防護

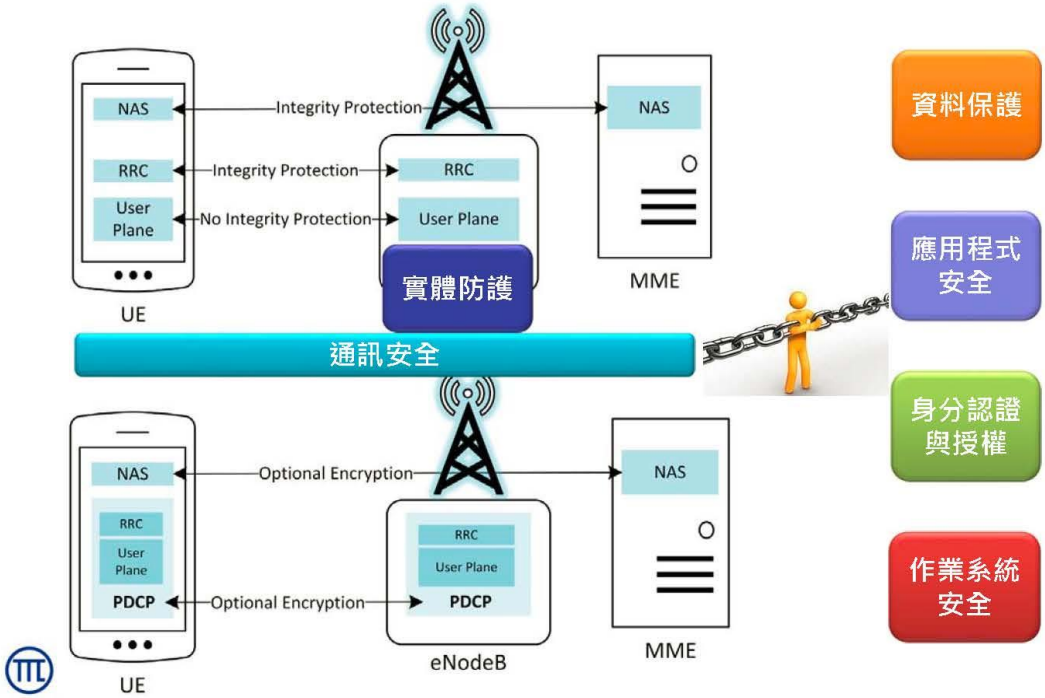
- 為確認產品設計上，有無阻礙駭客實體入侵之能力，包括增加產品外殼拆除難度、實體介面之存取控制等，通過此節的資安測試，可確保產品具備實體資安防護功能，由於僅家用基站是布建於終端使用者環境中，因此本節僅家用基站適用。

檢測編碼	檢測項目	檢測目的
6.1	家用基站的防拆保護	驗證產品具有拆解防護之設計，增加實體介面入侵之難度。
6.2	實體介面的安全管控	驗證連接產品實體埠時，可否存取作業系統之除錯模式。
6.3	硬體憑證的設計	驗證產品之硬體憑證是否可被徒手移除。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

22

確保基站資訊安全



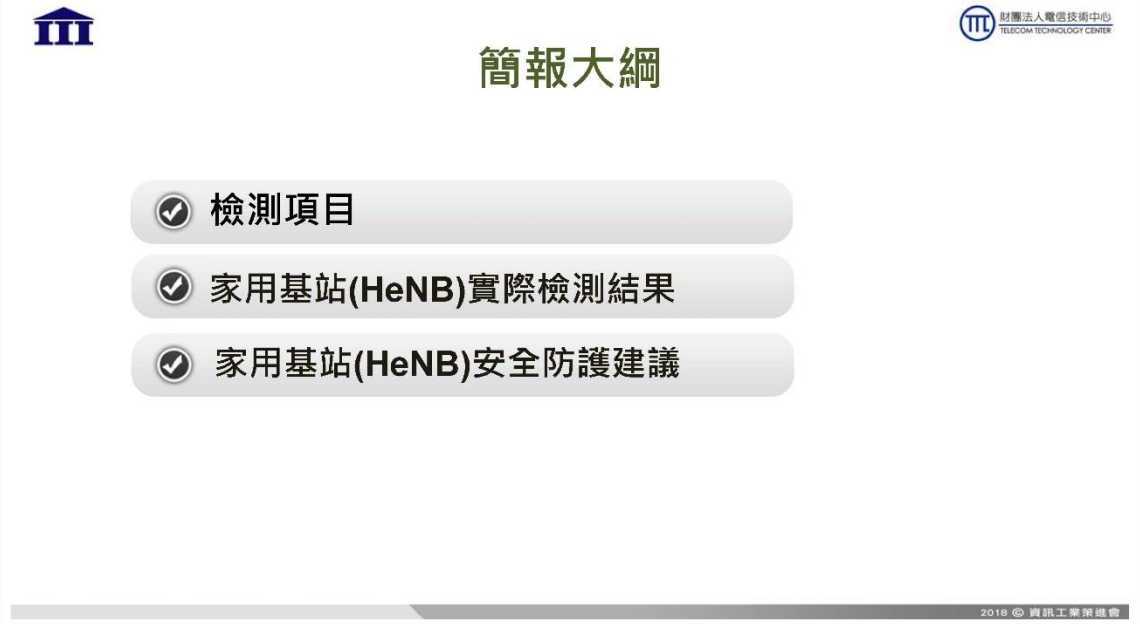
23

謝謝聆聽
敬請指教

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

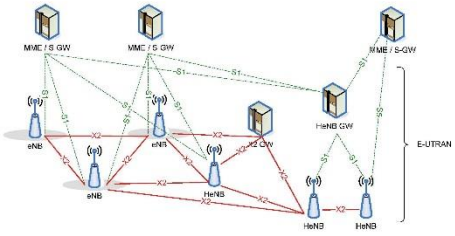
24

5. HeNB 檢測結果及防護建議



檢測項目

參照3GPP TS 33.320、TS 33.216，制定出並依(1)資料保護、(2)應用程式安全、(3)通訊安全、(4)身分鑑別與授權安全、(5)作業系統安全、(6)實體防護六項安全構面總計37項測項，訂定產品安全技術要求。



規範適用範圍

家用基站(HeNB)實際檢測項目

- HeNB目前初步檢測項目的結果：
  1. 基站網站伺服器不應存在常見之網路應用系統安全弱點
  2. 敏感性資料外洩防止(韌體外洩)
  3. 基站系統應確保敏感性資料進行加密處理再儲存
  4. 憑證唯一性
  5. 基站系統使用之協定與服務應採最小化設計
  6. 基站系統與對外之網路傳輸過程，應使用加密技術確保資料安全
  7. 控制層資料完整性保護
  8. 每一個帳號至少要有一個身分鑑別因子方可鑑別成功
  9. 基站系統應具備暴力及字典攻擊的防護措施
  10. 權限切換不須重新認證
  11. 通行碼顯示遮罩
  12. 基站系統應支援操作逾時功能
  13. 基站系統具備檔案系統存取權限控管機制
  14. 基站系統應提供可將安全事件記錄功能轉移備存至外部系統
  15. 系統本身不應存在重大風險已知弱點漏洞
  16. 家用基站的防拆保護
  17. 實體介面的安全管控

4

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

基站網站伺服器不應存在常見之網路應用系統安全弱點

OSS Configuration

URL	http[redacted]acs
Username	<script>alert('XSS by CFL lab')</script>
Password	••••••••

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

驗證裝置韌體是否含有敏感性資料外洩疑慮

```
server.document-root          = "/tmp/"
server.dir-listing            = "disable"
server.username               = "lighttp"
server.groupname              = "smacertmgr"
server.port                   = 1080
server.max-connections        = 12
server.max-request-size       = 250
server.bind                   = "192.168.252.1"

server.pid-file = "/tmp/swm_lighttpd.pid"
```

```
./FZM/_uImage-fzm-lsp-k2_20172160.bin.extracted/_37A0.extracted/openssl.cnf:207:#nsCaRevocationUrl
        = http://www.domain.dom/ca-crl.pem
./FZM/_uImage-fzm-lsp-k2_20172160.bin.extracted/_37A0.extracted/openssl.cnf:312:#nsCaRevocationUrl
        = http://www.domain.dom/ca-crl.pem
./FZM/SCFDFB1602v00_15918.txt:233:# https://jira3.int.net.     .com/browse/LTERLCR-9647
./FZM/SCFDFB1603v00_15918.txt:103 # https://jira3.int.net.     .com/browse/LTERLCR-10589
./FZM/SCFDFB1603v00_15918.txt:111 # https://jira3.int.net.     .com/browse/LTERLCR-10840
./FZM/SCFDFB1603v00_15918.txt:122 # https://jira3.int.net.     .com/browse/LTERLCR-11313
./FZM/SCFDFB1603v00_15918.txt:148 # https://jira3.int.net.     .com/browse/LTERLCR-11599
./FZM/SCFDFB1603v00_15918.txt:159 # https://jira3.int.net.     .com/browse/LTERLCR-10682
./FZM/SCFDFB1603v01_15918.txt:39:# https://jira3.int.net.n     com/browse/LTERLCR-11705
./FZM/SCFDFB1603v01_15918.txt:52:# https://jira3.int.net.n     com/browse/LTERLCR-11247
```

基站系統應確保敏感性資料進行加密處理再儲存

```
EnableCWMP=1
URL=http://[redacted]5.1:8080/femsacs/acs
Username=admin
Password=password
PeriodicInformEnable=1
PeriodicInformInterval=300
PeriodicInformTime=0
ParameterKey=SERV_B38_v58_31_PM_DONE
ConnectionRequestUsername=FAP_FC4008_1_B052162077C2
ConnectionRequestPassword=100515_47_B052162077C2
UpgradesManaged=1
DownloadProgressURL=http://192.168.30.15
```


憑證具唯一性

```
root@kali:/home/ahwan# openssl x509 -noout -fingerprint -sha256 -inform pem -in
rootCA.pem
SHA256 Fingerprint=EB:F2:A9:6D:C9:60:53:24:F5:17:8B:CC:86:FE:89:2C:5D:64:6E:FB:D
B:85:EE:D2:25:41:AF:FF:8C:59:E9:35
root@kali:/home/ahwan# openssl x509 -noout -fingerprint -sha256 -inform pem -in
HNB.pem
SHA256 Fingerprint=71:1E:FE:1B:0C:D2:6E:60:B5:D5:08:E4:FB:B0:B1:26:38:B7:3F:C3:3
E:D1:33:50:43:0D:EC:3E:48:F8:F1:74
```

基站系統使用之協定與服務應採最小化設計

```
PORT   STATE SERVICE
80/tcp open  http
MAC Address: B0:52:16:20:77:C2 (                Ind.)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.52 seconds
           Raw packets sent: 1003 (44.100KB) | Rcvd: 1004 (40.184KB)
root@kali:~/Desktop#
```

```
Not shown: 998 closed ports
PORT   STATE SERVICE
23/tcp open  telnet
80/tcp open  http
MAC Address: B0:52:16:20:77:C2 (                Ind.)
```


對外之網路傳輸過程，應使用加密技術確保資料安全

1398	183.812553000	192.168.30.15	103.231.48.193	ISAKMP	378	IKE_SA_INIT MID=00 Initiator Request
1399	183.822372000	103.231.48.193	192.168.30.15	ISAKMP	359	IKE_SA_INIT MID=00 Responder Response
1400	183.900007000	192.168.30.15	103.231.48.193	ISAKMP	1466	IKE_AUTH MID=01 Initiator Request
1401	183.984509000	103.231.48.193	192.168.30.15	ISAKMP	1342	IKE_AUTH MID=01 Responder Response
1402	184.499944000	fe80::b252:16ff:fe2…	ff02::2	ICMPv6	70	Router Solicitation from b0:52:16:20:77:c2
1403	184.668109000	192.168.30.15	103.231.48.193	ESP	158	ESP (SPI=0x0500aa30)
1404	184.673706000	103.231.48.193	192.168.30.15	ESP	162	ESP (SPI=0xcb727e0c)
1405	184.868464000	192.168.30.15	103.231.48.193	ESP	158	ESP (SPI=0x0500aa30)

```
0... .... = Critical Bit: Not Critical
Payload length: 12
Transform Type: Encryption Algorithm (ENCR) (1)
Transform ID (ENCR) (ENCR_AES_CBC (12))
Transform IKE2 Attribute Type (t=14,l=2) Key-Length : 128
  1... .... .... .... = Transform IKE2 Format: Type/Value (TV)
  Transform IKE2 Attribute Type: Key-Length (14)
  Value: 0080
  Key Length: 128
```

控制層資料加密及完整性保護

```
SecurityModeCommand    (3GPP TS 36.331 ver 10.6.0 Rel 10)

DL-DCCH-Message
  message
    c1
      securityModeCommand
        rrc-TransactionIdentifier: 1
        criticalExtensions
          c1
            securityModeCommand-r8
              securityConfigSMC
                securityAlgorithmConfig
                  cipheringAlgorithm: eea0
                  integrityProtAlgorithm: eia1

Data (hex):
32 00 10
```

預設未使用加密傳輸

每一個帳號至少要有一個身分鑑別因子方可鑑別成功

```
root@kali:~/Desktop# telnet 192.168.1.3
Trying 192.168.1.3...
Connected to 192.168.1.3.
Escape character is '^]'.

femto login: root
[root@femto ~]#
```

無需密碼即可進入

基站系統應具備暴力及字典攻擊的防護措施

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

Intruder attack 1

Attack Save Columns

Results | Target | Positions | Payloads | Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200			310	
1	1234455	200			310	
2	qwertt	200			310	
3	1qazxsw2	200			310	
4	[redacted]	200			310	
5	[redacted]	200			310	
6	admin	200			310	
7	engineer	200			348	
8	asxcdfg	200			310	
9	zzzzzzz	200			310	

Request | Response

Raw | Params | Headers | Hex

```
GET /cgi-bin/login.cgi?username=[redacted]&password=engineer&Submit=Login HTTP/1.1
Host: 192.168.1.3
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.3/index.html?login=faile
Connection: close
Upgrade-Insecure-Requests: 1
```


權限切換不須重新認證

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

```
GET /cgi-bin/login.cgi?username=admin&password=admin&Submit=Login HTTP/1.1
Host: 192.168.1.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Referer: http://192.168.1.2/
Cookie: sessionID=XTEKFIWTMOXXDVRH Mode=ENG
Connection: close
Upgrade-Insecure-Requests: 1
```

將 Mode=LOW 改為 Mode=ENG

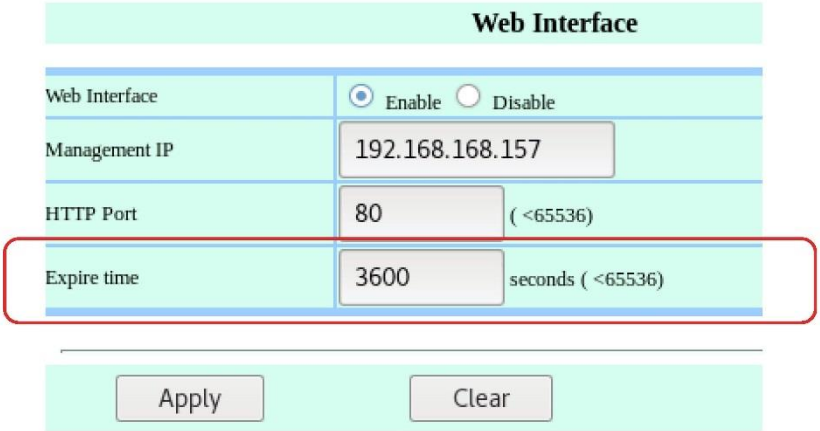
只用session的cookies來辨別身分 未通過

Mode= low

Mode= ENG

通行碼顯示遮罩

基站系統應支援操作逾時功能



安全事件記錄轉移至外部系統備存之通道應加密

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

```
< 6>2018-01-02T09:21:51.415Z 1251833: [SCTP] foxSctpRetryCb: connect[redacted] and wait for ipsec:0 localIp:1
< 6>2018-01-02T09:21:51.415Z 1251834: [SCTP] X2 SCTP Server wait for ipsec:0 localIp:1
< 6>2018-01-02T09:21:52.345Z 1251835: [ENB] veMmeReadyGet : no ready mme
< 6>2018-01-02T09:21:52.345Z 1251836: [ENB] cellDeInitChkTmrExpire: Wait S1 Setup ready!!!
< 6>2018-01-02T09:21:52.415Z 1251837: [SCTP] foxSctpRetryCb: connect[redacted] and wait for ipsec:0 localIp:1
< 6>2018-01-02T09:21:52.415Z 1251838: [SCTP] X2 SCTP Server wait for ipsec:0 localIp:1
< 6>2018-01-02T09:21:52.475Z 1251839: [STCL] [lo ] IPv6 ::1 sin6_scope_id=0
< 6>2018-01-02T09:21:52.475Z 1251840: [STCL] [eth0 ] IPv6 fe80::b252:16ff:fe20:77c2 sin6_scope_id=4
< 6>2018-01-02T09:21:52.475Z 1251841: [STCL] My IPv6 Address (linklocal): fe80::b252:16ff:fe20:77c2, sin6_scope_id=4
< 6>2018-01-02T09:21:52.475Z 1251842: [OAM] Start OAM tunnel[LTE], current WAN IP is 192.168.30.15 (init server ready)
```

231.48.193	ISAKMP	378	IKE_SA_INIT MID=00 Initiator Request
168.30.15	ISAKMP	359	IKE_SA_INIT MID=00 Responder Response
231.48.193	ISAKMP	1466	IKE_AUTH MID=01 Initiator Request
168.30.15	ISAKMP	1342	IKE_AUTH MID=01 Responder Response
::2	ICMPv6	70	Router Solicitation from b0:52:16:20:77:c2
231.48.193	ESP	158	ESP (SPI=0x0500aa30)
168.30.15	ESP	162	ESP (SPI=0xcb727e0c)
231.48.193	ESP	158	ESP (SPI=0x0500aa30)

系統本身不應存在重大風險已知弱點漏洞

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

192.168.7.45

CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	11	4	51

Scan Information

Start time: Mon Mar 12 20:26:22 2018
End time: Mon Mar 12 20:47:07 2018

Host Information

IP: 192.168.7.45
MAC Address: 00:AD:DE:03:03:30
OS: Linux Kernel 3.4.27-rt37-Cavium-Octeon+

CVSS v3.0 Base Score

192.168.7.45 47

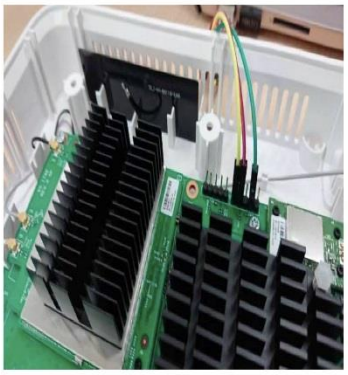
7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

家用基站的防拆保護

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

實體介面的安全管控



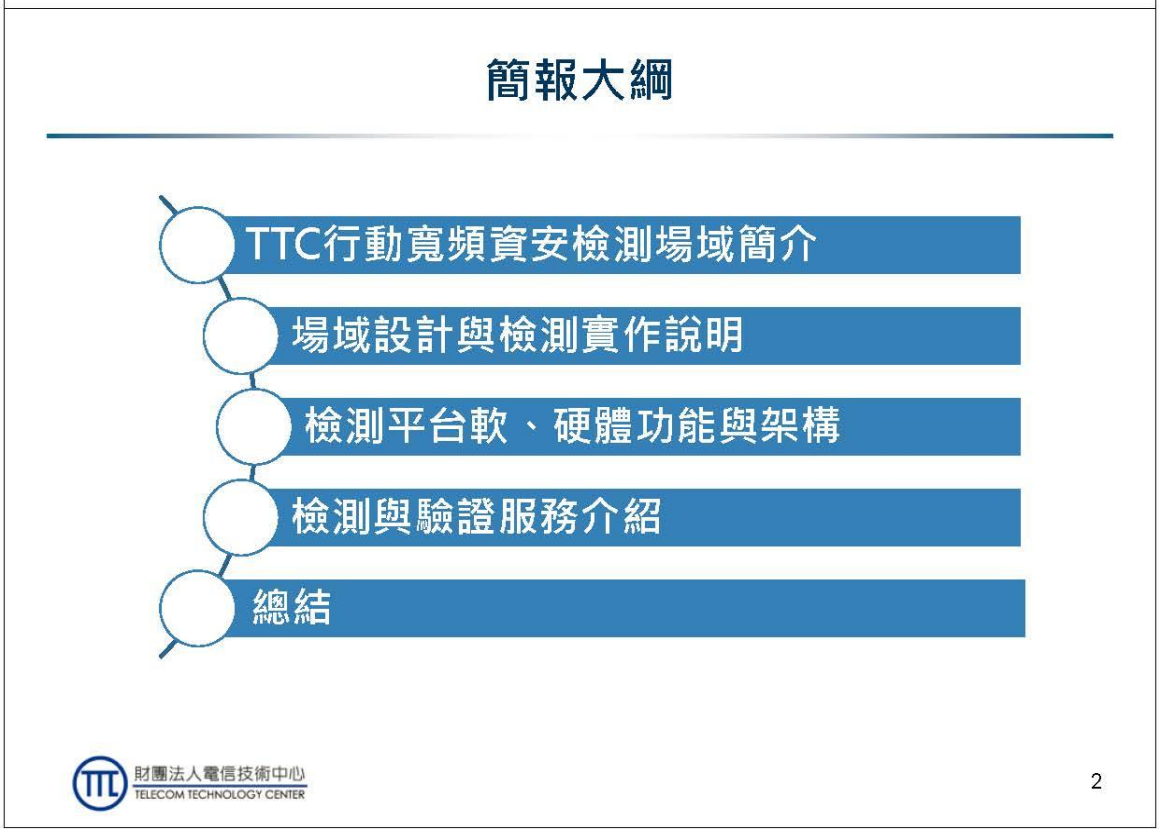
```
Broadcom Femto RFS
femto login: root
login[1312]: root login on 'ttyS0'
[root@femto ~]#      <  6>1970-01-01T00:00:56.670Z      140: [DNS] IP is not up
     <  6>1970-01-01T00:00:57.640Z      141: [MAIN] Wait 9 secs for IP ready
     <  6>1970-01-01T00:00:58.030Z      142: [QOS] IP is not up
i    <  6>1970-01-01T00:00:58.270Z      143: [OAM] IP is not up
d    <  6>1970-01-01T00:00:58.460Z      144: [PM] pmLoop wait CWMP ready uptime=59, currentUTC=58
     <  6>1970-01-01T00:00:58.460Z      145: [PM] Get next upload time is [964]
     <  6>1970-01-01T00:00:58.460Z      146: [PM] pmGetNextSampleTime() current uptime:64 utc:64
     <  6>1970-01-01T00:00:58.500Z      147: [TR069] cwmpInitCheck: bConnectServingOSS 0
     <  6>1970-01-01T00:00:58.500Z      148: [TR069] CWMP init check,  IP not ready !!!

uid=0(root) gid=0(root) groups=0(root),10(wheel)
[root@femto ~]#      <  6>1970-01-01T00:00:59.670Z      149: [DNS] IP is not up
```

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

家用基站安全防護建議

- 建議
  - ✓ 管理帳號的密碼強度需符合規範。
  - ✓ 使用的帳號權限需要區別，低權限帳號需要須完成身分認證與授權機制後才可以使用系統各項功能。
  - ✓ 網頁管理介面須通過弱點掃描，不可存在OWASP top10的風險。
  - ✓ 敏感資料的檔案如：日誌檔，需要限制權限存取。
  - ✓ 遠端存取系統的協定，不可使用明文傳輸的協定。
  - ✓ 家用基站硬體層的設計，須避免JTAG或是UART可以直接存取到debug mode 。
  - ✓ 敏感資料如：認證金鑰資訊，勿明文顯示。

6. TTC 行動寬頻資安檢測場域



簡報大綱

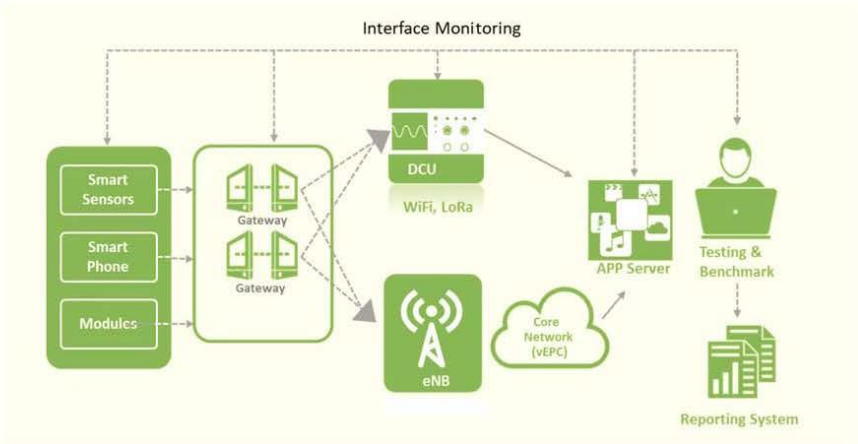
- TTC行動寬頻資安檢測場域簡介
- 場域設計與檢測實作說明
- 檢測平台軟、硬體功能與架構
- 檢測與驗證服務介紹
- 總結

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

3

TTC行動寬頻資安檢測場域

提供電信網路之基站系統，
一個完整的資安規範檢測及驗證場域。



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

4

特色

電信環境模擬

本場域可提供電信環境模擬功能，並用於進行行動寬頻資安相關標準之驗證與程序整合，協助檢測商用設備及應用情境於電信環境之安全性(Security)。

開放式平台

彈性模組化設計是平台與時俱進的重要關鍵，透過開放式的模組化設計，本場域可廣泛用於行動寬頻資安相關方案的測試及驗證。

驗證輔導

提供基站設備欲符合政府相關資安法規之前導測試，以實際檢測環境提供模擬試驗，並針對檢測結果提供專業建議。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

5

簡報大綱

- TTC行動寬頻資安檢測場域簡介
- **場域設計與檢測實作說明**
- 檢測平台軟、硬體功能與架構
- 檢測與驗證服務介紹
- 總結

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

模擬行動寬頻網路之場域

UE(LTE行動裝置)與 SIM卡

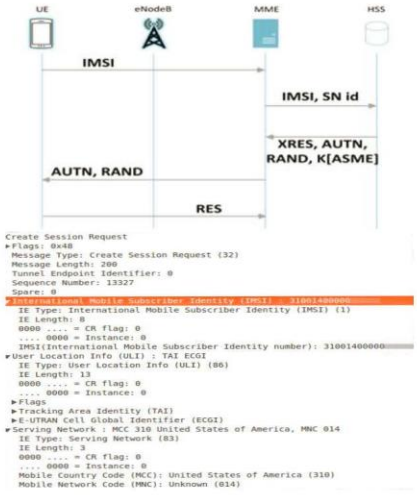
透過SIM卡裝置在智慧型手機上變成UE連接到檢測環境網路。

核心網路與eNB模擬器

1. 使用R&S CMW-500模擬器做為核心網路與eNB模擬LTE任何頻段與模式。
2. 使用模擬器或vEPC作為核心網路，以介接商用基站，完整模擬行動寬頻網路之行為。

完整的風險評估與檢測方案

提供全面且完整資安檢測程序，於場域中進行資安弱點的探索與模擬測試。

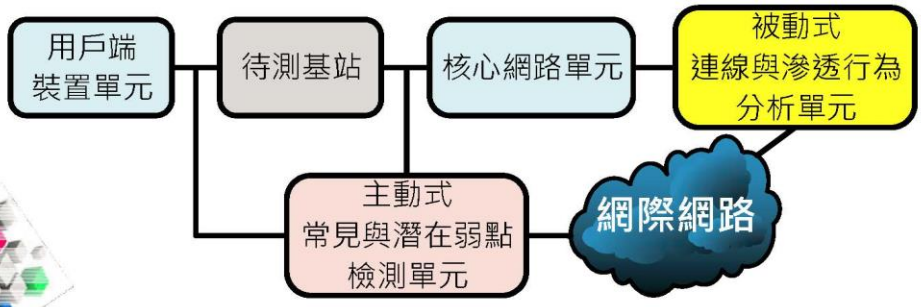


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

7

彈性的模組化資安檢測設計

易於更新、彈性與快速佈署的測試驗證場域。

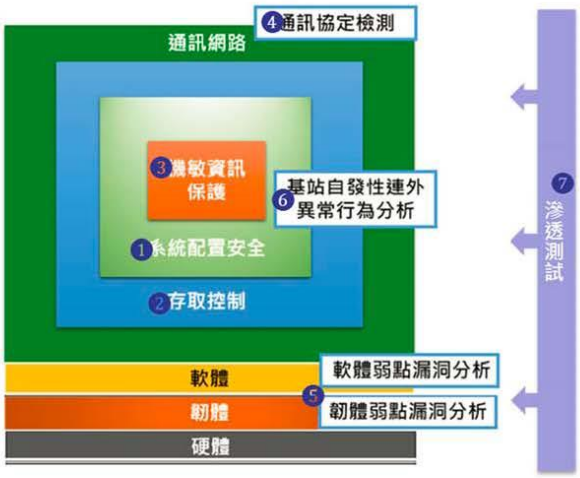


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

8

資安檢測維度的全面提升

參考3GPP TS33.216及NIST SP800-53歸納資安檢測類別及項目。



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

9

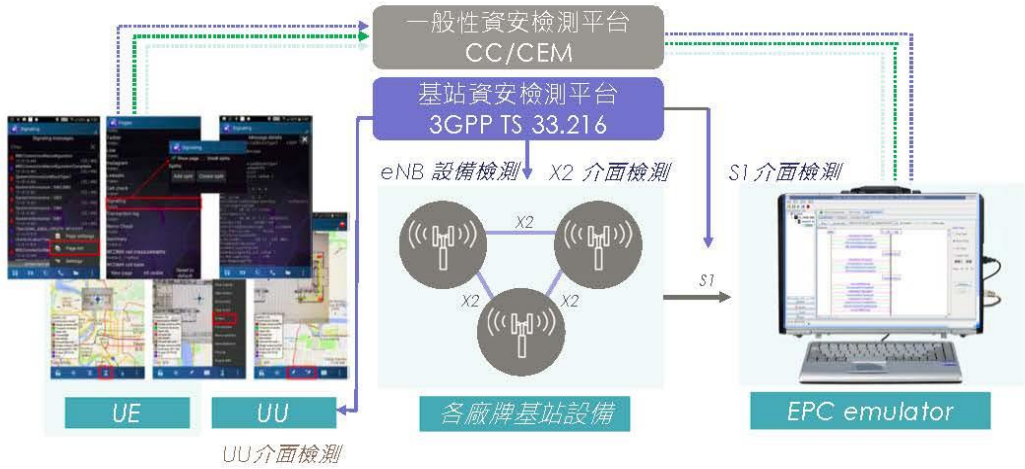
簡報大綱

- TTC行動寬頻資安檢測場域簡介
- 場域設計與檢測實作說明
- 檢測平台軟、硬體功能與架構
- 檢測與驗證服務介紹
- 總結

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

10

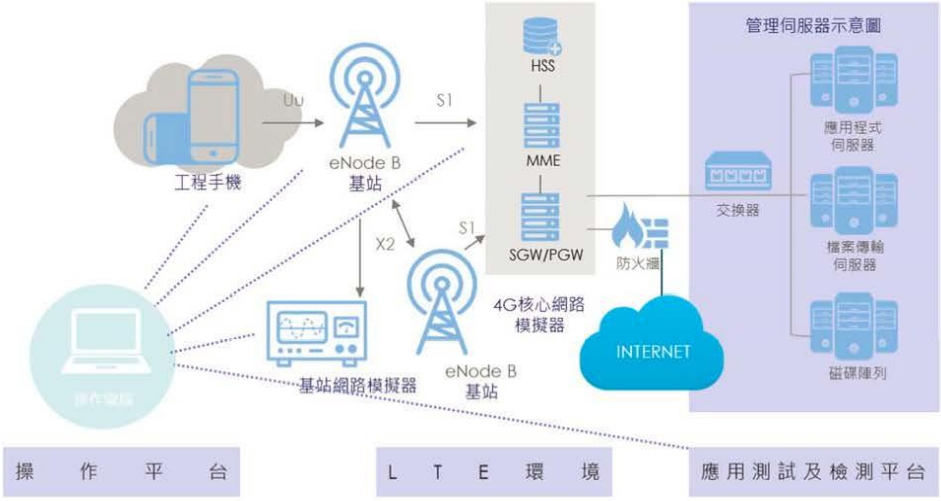
行動寬頻資安檢測平台概觀



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

11

行動寬頻資安檢測平台-硬體設備架構圖



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

12

行動寬頻資安檢測平台-硬體設備功能

操作平台

工程手機、UE模擬器

- 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。
- 此外，UE 模擬器能提供不同使用情境的設定，例如換手、移動速度等。

LTE 環境

基站、基站網路模擬器、核心網路模擬器

基站

- DUT待測物。提供基於3GPP與資安相關之檢測項目測試。

基站網路模擬器

- 提供LTE X2介面相關分析、協定驗證與端對端應用測試。
- 提供相鄰基站模擬，模擬換手、連線、重置及資源狀態報告等功能。

基站網路模擬器及核心網路模擬器

- 提供LTE S1介面相關分析、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。
- 提供LTE 核心網路網路元件MME、HSS、P/S GW模擬功能，供UE接入核網進行連線等測試。

應用測試及檢測平台

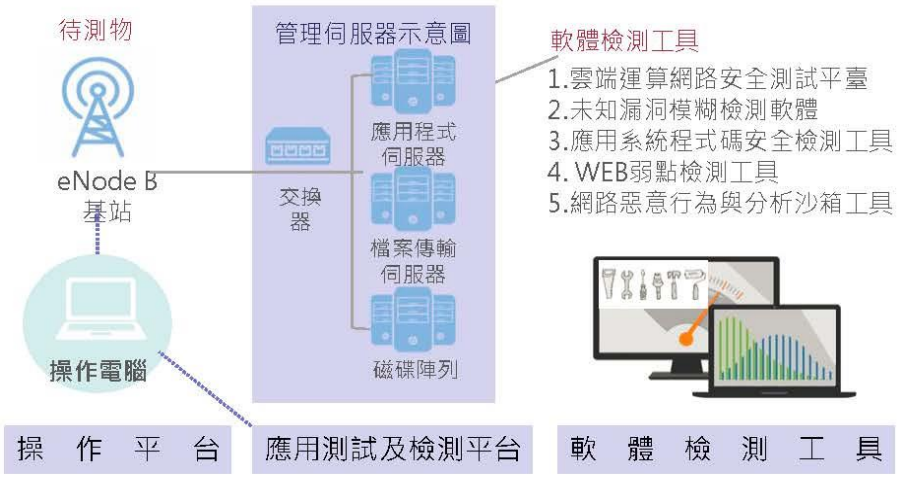
管理伺服器

- 含伺服器、磁碟陣列、交換機等設備、筆記型電腦。
- 執行檢測工具操作，腳本編譯，及檢測紀錄與基站行為表現紀錄之儲存。
- 以專業多維度的檢測報表，協助相關人員更快速而全面的了解待測物之安全性。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

13

行動寬頻資安檢測平台-軟體架構圖



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

14

行動寬頻資安檢測平台-軟體設備功能

雲端運算網路安全測試平臺

- 支援電信及資訊網路相關之應用通訊協定
- 支援基站設備之應用安全檢測功能，其中包含有
  - 阻斷式攻擊行為檢測，
  - CVE公告弱點檢測,
  - 通訊行為特徵檢測, 及進階持續性滲透攻擊

未知漏洞模糊檢測軟體-Fuzzy

通過有系統地向DUT待測物發送無效或意外輸入，尋找待測物是否存在某些可能被利用的原生性弱點，避免被攻擊者用以產生零日攻擊(Zero Day)之資安威脅。

應用系統程式碼安全檢測工具-白箱測試

有系統的找出程式碼中的弱點所在位置，並依據國際常見之分類方式，排定建議之弱點修補的優先次序。

WEB弱點檢測工具

- 黑箱動態偵測Web應用介面弱點。
- 協助檢測及稽核開發中或已上線的Web介面，檢查是否可能洩漏機敏資訊、被攻擊者利用或隱含特定資安威脅。

網路惡意行為與分析沙箱工具

建置一個可執行惡意程式的沙箱環境，透過通訊與執行緒行為比對，分析可能產生資安威脅的相關行為。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

15

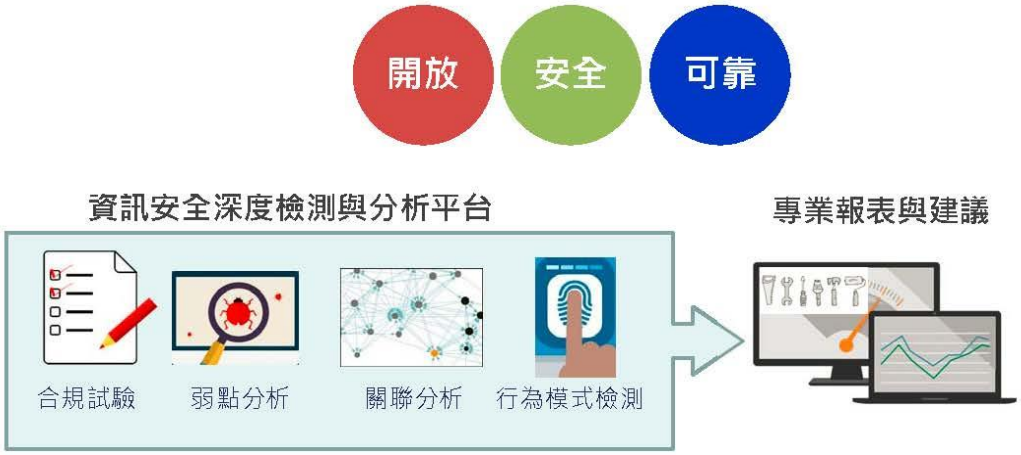
簡報大綱

- TTC行動寬頻資安檢測場域簡介
- 場域設計與檢測實作說明
- 檢測平台軟、硬體功能與架構
- 檢測與驗證服務介紹
- 總結

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

16

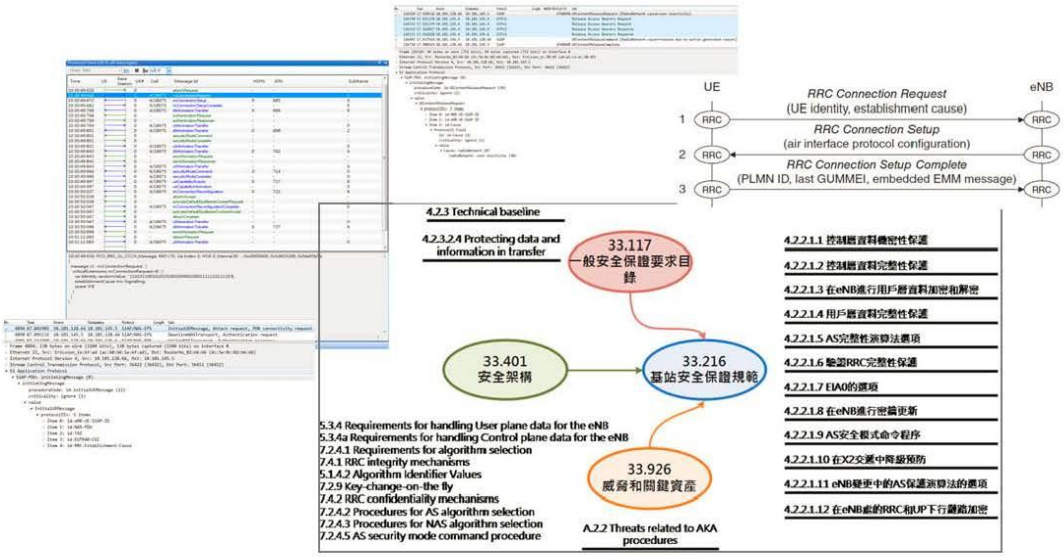
行動寬頻資安檢測場域服務



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

17

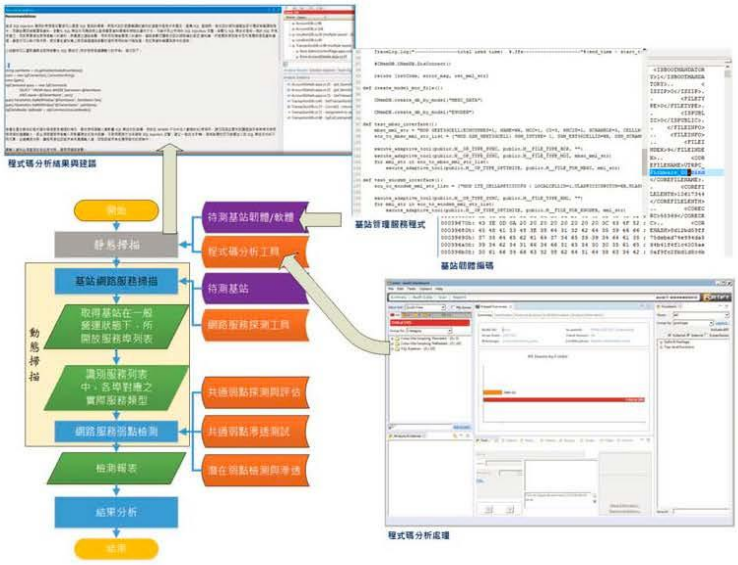
行動寬頻資安檢測場域服務-合規試驗



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

18

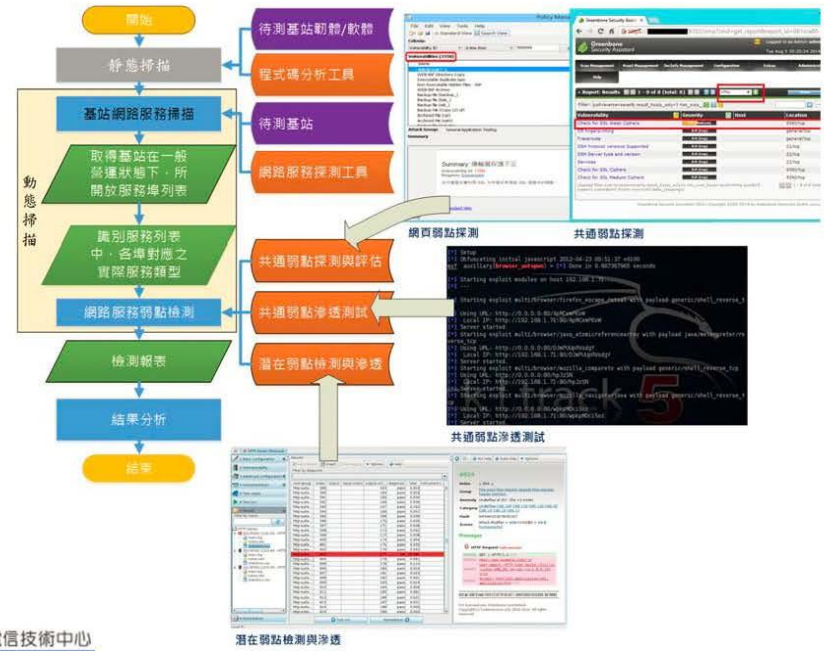
行動寬頻資安檢測場域服務-弱點分析



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

19

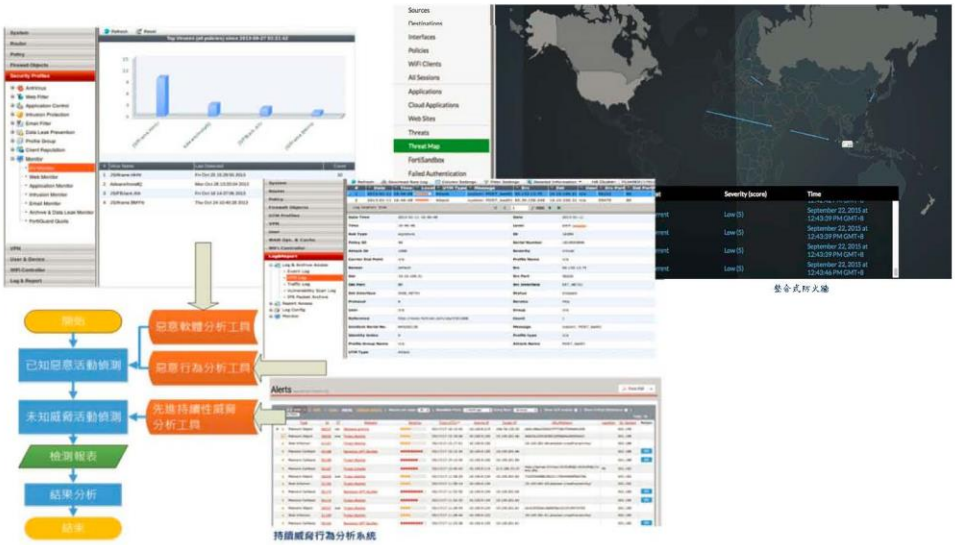
行動寬頻資安檢測場域服務-關聯分析



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

20

行動寬頻資安檢測場域服務-行為模式檢測



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

21

TTC提供全方位資通安全檢測與服務

設備端資安服務 | 網路傳輸資安服務 | 網路監控/管理資安服務

共同準則(CC)標準
- 共同準則(CC)標準檢測服務
- 共同準則(CC)標準驗證顧問服務
- 資安產品環境標準驗證顧問服務

密碼模組(FIPS 140)標準
- 密碼模組驗證顧問服務
- 密碼演算法驗證顧問服務

NCC資通設備安全檢測規範
- 10大項資通設備安全檢測服務
- IPCAM設備安全檢測服務

行動裝置App資安檢測顧問服務

前瞻新興傳輸資安
- 物聯網(IoT)資安議題研究
- 5G資安議題研究
- 寬頻網路攻防技術研究
- 金鑰加密技術研究

行動寬頻4G基站資安
- 行動寬頻基站資安檢測服務
- 行動寬頻基站威脅分析服務
- 行動寬頻資安檢測場域

行動寬頻4G資安顧問服務
- 行動寬頻資安技術顧問
- 行動寬頻資安管理顧問

ISO 27001標準認證顧問服務
- ISO 27001標準認證落差分析
- ISO 27001標準稽核服務

ISO 20000標準認證顧問服務
- ISO 20000標準稽核服務

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

22

簡報大綱

- TTC行動寬頻資安檢測場域簡介
- 場域設計與檢測實作說明
- 檢測平台軟、硬體功能與架構
- 檢測與驗證服務介紹
- 總結

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

23

總結

- ☑ 促進政府組織及企業之核心價值。
- ☑ 提升網路韌性及國際競爭力。
- ☑ 預防與降低網路犯罪。
- ☑ 發展專業網路防禦政策和能力。
- ☑ 連結產業和技術性資源。
- ☑ 建立完整之組織網路資訊安全政策。

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

24

敬請指教

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

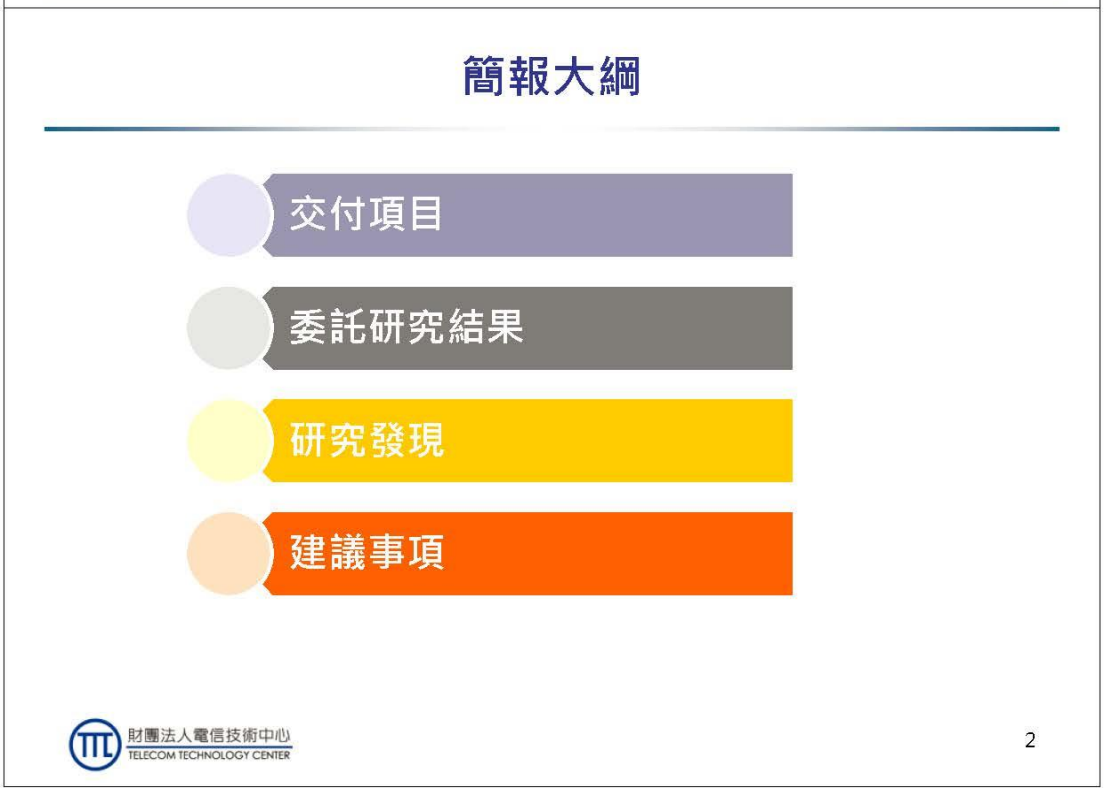
25

附錄七 期末審查簡報及審查意見回覆

建置基站資安檢測環境計畫(第 2 期)
期末審查簡報及審查意見回覆

一、 期末報告第 1 次審查會議

(一) 期末審查簡報



簡報大綱

- 交付項目
- 委託研究結果
- 研究發現
- 建議事項

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

3

交付項目(1/3)

交付標的		執行說明	章節
一、前瞻性資安技術研究	(一)國外參訪或研討	挑選國外行動寬頻網路發展較為先進之國家-芬蘭，參訪其檢測實驗室及研究中心。	附錄一
	(二)資安防護技術與服務之最新趨勢研究	最新行動寬頻網路最新資安議題與近年新興之前瞻資安議題與資安防護技術研析探討。 1.行動寬頻網路資安最新趨勢 2.資安防護技術與服務最新趨勢：主題包含SS7、5G、SDN及IoT	第三章第一節
	(三)資安檢測標準與檢測流程之最新趨勢研究	深入探討與基站資安相關之國際檢測標準及檢測流程最新趨勢發展，包含 1. 3GPP 33系列最新趨勢發展 2. GSMA 物聯網安全規範及網通設備安全認證方法 3. CC-最新通過CC認證之行動寬頻網路設備文件說明	第三章第二節
二、國際行動寬頻資安框架研究	(一)各國網路安全總體戰略、政策、法規、權責機關與任務分配。 (二)各國推動資通安全之技術規範、參考指引與最佳實務。	介紹美國、加拿大、英國、歐盟及日本等國網路保全策略，與相關權責機關架構之發展狀況，及國際間行動寬頻資安政策發展現況及最佳實務，綜整作為我國規劃網路安全政策之參考基礎。	第四章第一節~第七節

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

4

交付項目(2/3)

交付標的		執行說明	章節
三、行動寬頻資安技術研究	(一) 空中介面資安技術研究 1.偽基站資安技術探討 2.VoLTE資安技術探討研究	完成偽基站資安議題研究、實驗平臺與實驗項目規劃，及實測驗證，提出相關防護建議；另完成VoLTE造成基站(eNodeB)與核心網路(EPC)之可能資安威脅，及UE端之資安威脅研析，並提出建議之解決方案。	第五章第一節
	(二)基站資安檢測技術研究 1.基站資安檢測技術及項目研究 (1)一般性資安檢測項目研究 (2)進階資安檢測項目研究 2.HeNB資安檢測技術及項目研究 (1)HeNB資安檢測項目研究 (2)HeNB資安監測技術研究	完成eNB及HeNB基站資安檢測項目規劃，所有檢測項目包含測試案例名稱、參考資料、測試目的、資訊安全需求(CIA)、測試環境暨初始條件、測試方法及合格判定標準。	第五章第二節
	(三) 核心網路-MME資安檢測技術研究	完成MME元件架構及功能研究、介面安全性研究、相關介面弱點分析及安全威脅分析。	第五章第三節

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

5

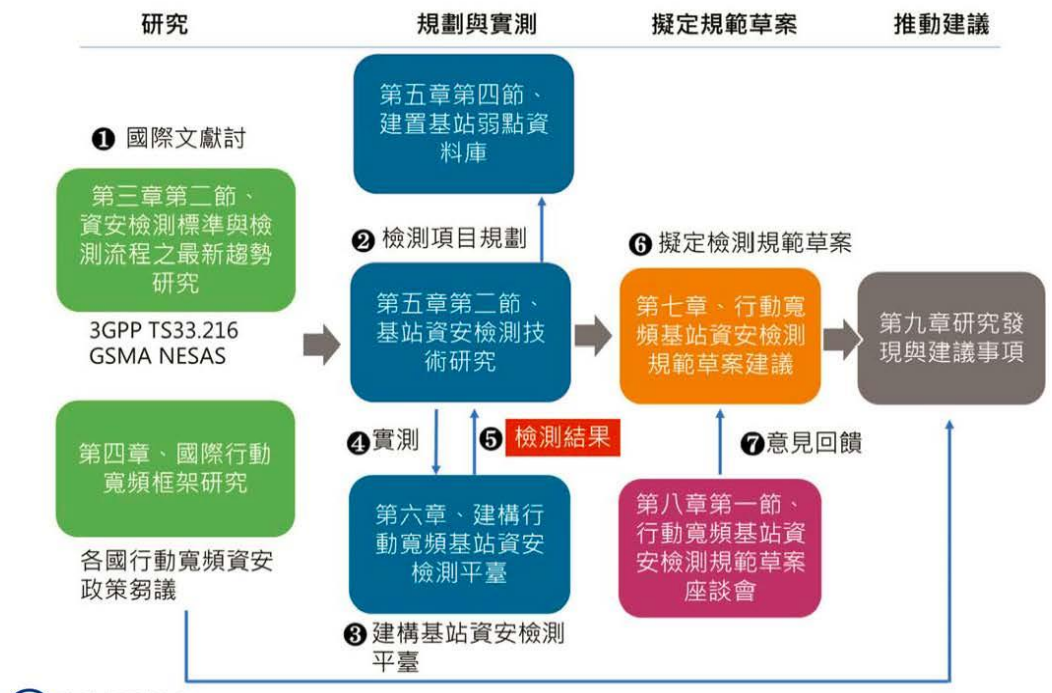
交付項目(3/3)

交付標的		執行說明	章節
四、建構行動寬頻基站資安檢測平臺	(一)研析行動寬頻基站資安檢測平臺架構 (二)驗證行動寬頻基站資安檢測平臺	依所規劃之檢測平臺完成架設，並完成整合驗證測試，確認本計畫所建構之行動寬頻基站資安檢測平臺可穩定運行，且所採購之檢測工具亦可進行基站資安檢測。	第六章第一節~第三節
五、行動寬頻基站資安檢測結果報告	(一) 一般性檢測 (二) 進階資安檢測 (三) HeNB資安檢測	完成第五章第二節規劃之基站資安檢測項目實測驗證，詳細說明每一測項之檢測結果與檢測畫面。	第五章第二節
	(四) 建置基站弱點資料庫	已依本團隊檢測之基站樣本結果，及參考NVD國際弱點資料庫，完成基站弱點資料庫之建置。	第五章第四節
六、行動寬頻基站資安檢測規範草案建議	(一) 檢測環境建議 (二) 檢測項目要求 (三) 檢測結果及判定標準建議 (四) 檢測作業程序	參照國際標準3GPP TS33.216、TS33.320及TR33.820，與本計畫檢測結果及座談會訪談建議，完成行動寬頻基站資安檢測規範草案建議。	第七章第一節~第五節
七、行動寬頻資安座談會及研討會辦理成果	(一) 舉辦行動寬頻基站資安檢測規範與作業程序建議座談 (二) 舉辦行動寬頻基站資安檢測環境推動研討會	(一) 完成5場電信業者，及2家設備製造商之座談會舉辦，辦理成果會議紀錄及意見已整理至期末報告中。 (二) 完成1場動寬頻基站資安研討會之舉辦，研討會之相關簡報、紀錄及意見已整理至期末報告中。	第八章第一節~第三節及附錄五、附錄六

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

主要工作項目研究步驟及各章節關聯性



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

7

簡報大綱

- 交付項目
- 委託研究結果
- 研究發現
- 建議事項

一、前瞻性資安技術研究 (第三章)

二、國際行動寬頻資安框架研究 (第四章)

三、行動寬頻資安技術研究 (第五章)

四、建構行動寬頻基站資安檢測平臺 (第六章)

五、行動寬頻基站資安檢測規範草案(第七章)

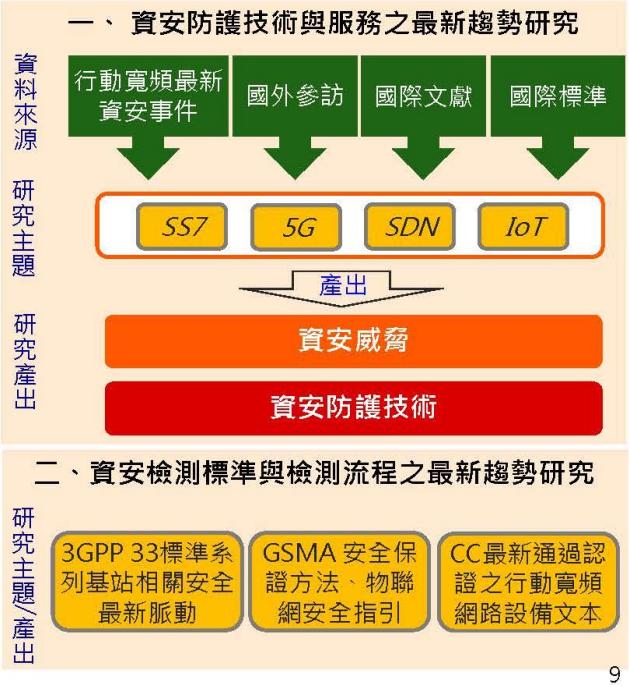
六、行動寬頻基站資安檢測結果 (第五章)

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

8

第三章 前瞻性資安技術研究

- 資安防護技術與服務最新趨勢研究
  - 近兩年行動寬頻資安事件多發生在SS7協定漏洞、偽基站及IoT等；
  - 本團隊深入近年資安議題及新興前瞻技術，包含SS7、5G、SDN、IoT之資安防護技術探討;
- 資安檢測標準與檢測流程最新趨勢研究
  - 基站資安檢測標準：3GPP 33系列。
  - 資安檢測流程：GSMA安全保證方法(NESAS)。



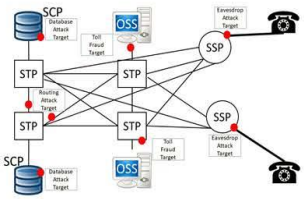
財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

9

一、資安防護技術與服務之最新趨勢研究(1/3)

- SS7資安威脅與防護建議

SS7各個節點攻擊方式



SS7網路包含三個節點-SSP、STP、SCP，可能遭受的攻擊包含修改、竊聽、阻斷、偽造。

SS7防護建議

參考文獻：美國 FCC CSRIC

互聯監控及過濾	建立互信圈
IPSec	信令基礎建設之安全評估
網路節點防止駭客攻擊	美國關鍵基礎設施保護
信令聚合	
資訊共享	支援用戶加密

參考文獻：歐盟 enisa

- 核心措施：檢測攻擊和妥協措施的最低限度措施
- 中級措施：為核心措施增加安全保證
- 高級措施：可以識別和減輕未知的攻擊

綜整建議

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

10

一、資安防護技術與服務之最新趨勢研究(2/3)

❑ 5G資安威脅與防護技術

	資安威脅	資安防護技術
5G	① 無線接入網威脅	強化元件基礎層的連網安全，採用適當的存取控制機制對使用者授權、識別。
	② SDN威脅	為SDN建造一個檢測系統。
	③ NFV威脅	可透過虛擬主級的防火牆對流經虛擬機器的封包做檢測、網路流量偵測。
	④基站安全	標準訂定機構必須為5G訂定良好的安全架構，讓布建實有標準依據。
	⑤網路安全威脅	強化各節點間互相認證機制、將安全需求納入5G訂定標準時的考量條件。
	⑥惡意軟體攻擊	偵測連網的合理IP數量，只要網路頻寬足夠可提供服務給真正需要的連網者。
	⑦AAA基礎架構惡意程式攻擊	評估網路轉發來的用戶安全資訊，並與應用伺服器協調提供更深層憑證或安全連線。
	⑧惡意程式攻擊SDN基礎設施	控制數據通過其他網路安全檢測措施，防止惡意程式取的基礎設施控制權限。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

11

一、資安防護技術與服務之最新趨勢研究(3/3)

❑ SDN及IoT資安威脅與防護技術

	資安威脅	資安防護技術
SDN	①電子欺騙攻擊	• 封包檢測 • IP位址防護
	②入侵式攻擊	• FlowGuard • FlowTag • NIMBLE
	③異常式攻擊	• NICE (No bugs In the Controller Execution) • FRESCO • Rate-Limiting • TRW-CB (Threshold Random Walk with Credit Based Rate Limiting)
	④阻斷服務攻擊與分散式阻斷服務攻擊	•辨別攻擊模式 •輕量級的DDos攻擊檢測 •基於Entropy的檢測 • Avant guard •高速流量檢測系統(High Speed Flow-level Detection System, HiFIND)
IoT	①惡意程式入侵	建議關閉IoT設備上的port 23或port 2323，或是在購買裝置後修改裝置的預設密碼並改為強密碼，避免被惡意程式暴力破解取得控制權。
	②殭屍病毒入侵	變更密碼、使用者禁用UPnP、最新版本更新。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

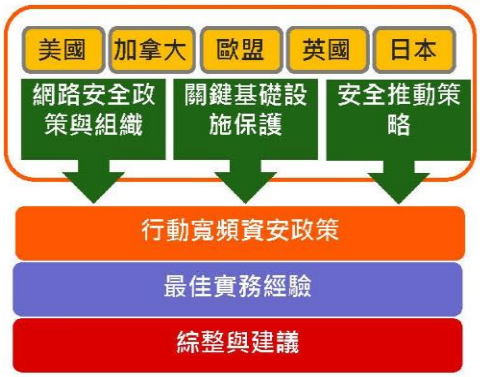
12

二、資安檢測標準與檢測流程之最新趨勢研究

- 掌握最新行動寬頻國際標準最新脈動，供國內產官學界參考，並做為本計畫研擬行動寬頻基站檢測規範草案之依據。
  - 基站資安檢測標準：3GPP 33系列安全標準
  - 行動寬頻資安檢測流程：GSMA NESAS
  - 物聯網安全指引：GSMA

第四章國際行動寬頻資安框架研究

- 期中報告已完成美國、加拿大、歐盟、英國、日本之網路安全總體戰略、政策、法規、權責機關與任務分配、資通安全之技術規範以及行動寬頻資安政策的蒐集與研析，並與我國比較，提出綜整與建議。
- 國際間對行動寬頻網路安全之規範主要在關鍵基礎設施上，僅美國及英國有訂定相關之電信事業資安要求。
- **期末補充美國與歐盟行動寬頻資安標準與政策文件，並以英國與華為合作之資安評估中心為例介紹公私協力模式。**
  - 美國NIST SP 800-197「LTE安全準則(Guide to LTE Security)」
  - 歐盟ETSI TR 103 456「網路與資訊安全指令(NIS指令)之實施(CYBER;Implementation of the Network and Information Security (NIS) Directive)
  - Huawei Cyber Security Evaluation Centre(HCSEC)



行動寬頻資安實務發展(1/3)

國家政策及標準文件

美國NIST SP 800-197「LTE安全準則(Guide to LTE Security)」

LTE技術架構	LTE安全架構	LTE網路威脅	LTE威脅緩解措施
• 3GPP標準演進 • 基地台到終端網路架構	• 加密 • 空中介面 • 回送網路（Backhual） • 核心網路	• 一般網路威脅 • 偽基站 • 空中介面竊聽 • 小型基站攻擊	• 加密 • 身分認證 • 實體安全 • 網路安全

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

15

行動寬頻資安實務發展(2/3)

國家政策及標準文件

歐盟ETSI TR 103 456「網路與資訊安全指令(NIS指令)之實施(CYBER;Implementation of the Network and Information Security (NIS) Directive)」

歐盟NIS指令概述	網路威脅情報分享：資安事件與風險	風險分析在保護NIS所扮演的角色	問題與解決方案建議
• 標準化網路安全資訊分享措施 • 確保會員國之有效合作	• 通知門檻 • 概念、模式與技術方法 • 組織（關鍵服務業者、數位服務業者） • 情報分享平台	• 網路防禦與網路安全風險管理實踐 • 概念、模式與技術方法	• 新科技與服務之衝擊 • 關鍵服務業者與數位服務業者之建議

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

16

行動寬頻資安實務發展(3/3)

公私協力模式(Public Private Partnerships, PPP)
Huawei Cyber Security Evaluation Centre(HCSEC)

HCSEC 主要業務

由於許多資安漏洞為經由後續下載之更新軟體進行攻擊，因此GCHQ認為HCSEC主要功能為在華為進行大規模更新前，將對其更新之軟體進行資安評估。

HCSEC隨機抽查檢驗即將佈建於英國關鍵基礎建設(CNI)之華為軟硬體產品，以確保產品符合資安要求。

HCSEC 主要效益

2014年研發出一系列弱點檢測工具，在抽象語法樹、符號執行引擎等基礎上，加速分析師在複雜且重複的程式碼中發現問題。

2015年檢驗出3項問題需藉特殊手段介入CSP的網路系統；此問題透過英國政府與CSP之間的標準處理程序解決。

2016年共檢驗20項產品與評估4項解決方案，其範圍涵括英國5家電信營運商。

提供政府及通訊服務提供者(CSP，電信營運商)相關之風險管理預警；開創政府與私人企業合作之新興模式。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

17

第五章行動寬頻資安技術研究

- 本團隊從空中介面➔基站➔核心網路-MME研究，完成資安威脅與防護建議之研究。
- 在基站資安檢測技研究，已產出基站之檢測項目並完成實測驗證，作為第七章基站資安檢測規範草案之參考，同時將檢測結果參考國際弱點資料庫，完成基站弱點資料庫之建置。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

18

一、空中介面資安技術研究-偽基站(1/3)

❑ 偽基站造成之資安議題 (上)

– 本團隊參考2018年3月美國大學研究使用LTE Inspector方式架設偽基站，以較好的訊息品質誘使UE選擇接取，研析相關文獻整理出偽基站造成之攻擊：包含監視用戶通話、信息、設備離線、跟踪用戶位置並發送虛假警報等相關資安議題。

偽基站之資安議題	說明
認證同步失敗攻擊 (Authentication Synchronization Failure Attack)	惡意UE偽造受害者 UE 發起 Attach(帶有受害者IMSI)，打亂 sequence number 的健全性，導致認證失敗
認證中間人攻擊 (Authentication Relay Attack)	受害UE向偽基站發起Attach程序，偽基站將訊息傳給惡意裝置UE ，向合法基站發起Attach程序，透過中間人的方式完成Attach程序
追蹤攻擊 (Traceability Attack)	透過偽基站傳送，只會有對應的受害UE回應complete，其餘皆會回應reject，確認特定的受害是否出現在偽基站所屬區域
Numb Attack	偽基站傳送Authentication Reject，因認證拒絕使UE失去服務
尋呼通道劫持 (Paging Channel Hijacking)	偽基站與合法基站相同的paging channel，發送empty paging message，讓受害UE認為不需要重新連接網路

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

19

一、空中介面資安技術研究-偽基站(2/3)

❑ 偽基站造成之資安議題 (下)

偽基站之資安議題	說明
Stealthy kicking-off Attack	paging內容夾帶受害UE之IMSI進行呼叫，受害UE會與原先核心網路斷開，並重啟attach程序
Panic Attack(假緊急警報攻擊)	偽基站發送具有假緊急警告的paging，為了確保這種假paging消息大量的送達UE，偽基站持續廣播該paging
Energy Depletion Attack(電力消耗攻擊)	偽基站知道受害UE的GUTI情況下，發送具有GUTI的尋呼消息，受害UE用加密服務請求消息進行響應，迫使受害UE不斷進行Attach
Link ability Attack(鏈接性攻擊)	偽基站使用paging訊息去證實受害UE是否有在覆蓋範圍內，造成地理位置資訊洩漏
Detach / Downgrade Attack(斷線/降等攻擊)	受害UE Attach偽基站時，偽基站發起detach_request，UE會失去服務或是降等，中斷受害者UE的網路服務

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

20

一、空中介面資安技術研究-偽基站(3/3)

- 偽基站實驗結果及防護建議
  - 偽基站造成通訊服務無法正常使用，只能影響小型區域，危害少數用戶。
  - 偽基站防護建議，大致可分為以下幾個層面：
    - ① LTE基站部署憑證進行認證。
    - ② 設計終端設備導入基站的識別。
    - ③ 提出對LTE細胞選擇過程的系統性修改。
    - ④ 電信服務供應商啟用加密演算法減緩偽基站所帶來的影響。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

21

一、空中介面資安技術研究-VoLTE(1/2)

- VoLTE之資安威脅及防護建議
  - VoLTE 是在蜂巢式網路（Cellular Network）執行，需透過 SIP信號指令幫助數據傳輸，然而其中漏洞有可能造成危害，本團隊整理出VoLTE相關資安威脅與防護建議如下。

資安威脅		描述	防護建議
惡意軟件	免費數據通道	惡意軟件更改VoLTE接口所指向目的地之路由規則，經由信令乘載通道達到將封包傳送至任意目標的最終目的。抑或繞過合法攔截LI，在不觸發CDR計費系統的情況下，將任意的字串插入至SDP封包的header中。	1.經由封包檢測系統(DPI)檢測流量傳輸是否合理，同時利用封包資料閘道(P-GW)監控SDP標頭檔。 2.更新計費系統，任何與數據流量類似的信號傳輸量到一定額便收取費用，同時監控來往路徑是否合理。
	阻斷服務(Denial of Service)攻擊	惡意軟件傳送大量偽造IP來源的訊息封包，因此伺服器端會建立多個通訊乘載通道（bearer）進而佔用無線介面 LTE-Uu之控制層面(Control-plane)資源。	1.界定SIP中Session信息量的最大閾值。 2.結合機器學習及欺詐管理系統設計(FMS)能同時收集和處理數據封包的流量檢測系統。
	通訊設備收集機密資訊	惡意軟件監控通訊流量的來往，並檢查受害者所收到之SIP訊息，當偵測到所回傳之「200 OK」信號，便能竊取標頭檔中包含有關通訊網路運營商服務器的類型、設備版本等機密資訊，使得攻擊者進一步利用這些訊息來針對此運營商之特定漏洞進行有效攻擊。	刪除「200 OK」中標頭檔有關通訊設備隱密資訊的訊息。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

22

一、空中介面資安技術研究-VoLTE (2/2)

- VoLTE之資安威脅及防護建議

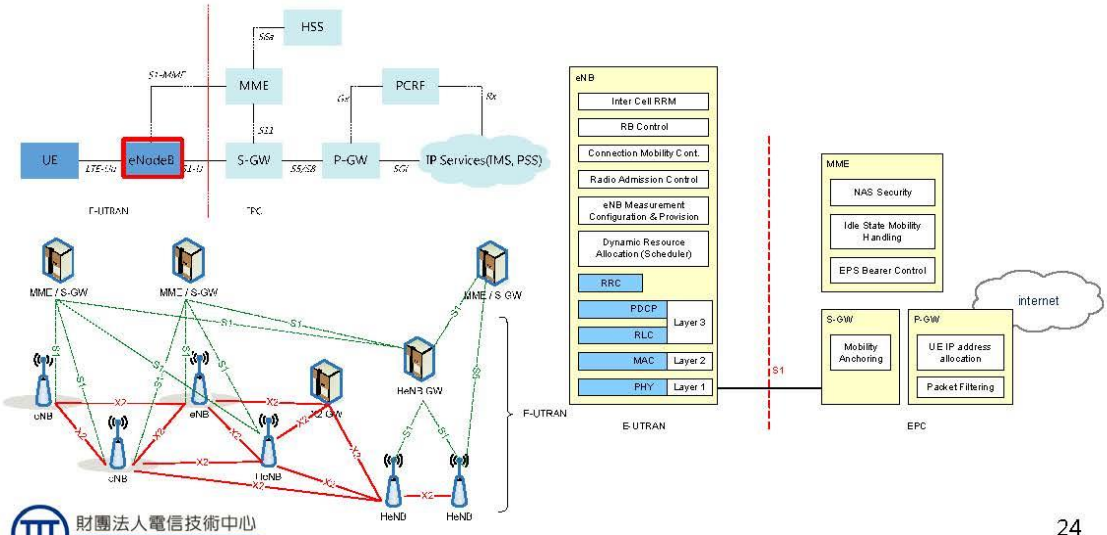
資安威脅		描述	防護建議
惡意用戶端	MSISDN欺騙	惡意用戶端於適當的呼叫流程中修改「INVITE」包含的MSISDN，且通訊封包只能經由P-GW傳送，只要通話發起人的消息格式正確，VoLTE並不會在發話者與接收者之間有多一步的驗證，進而實現語音釣魚攻擊(voice phishing)。	1.比較會話邊界控制器(SBC)的「INVITE」憑據。 2.透過TEID辨識符號設置加密金鑰判斷訊息真假。
	竊取IMEI信息	惡意用戶端在雙方尚未連接通話前獲取訊息當中串接於「+sip.instance」之後的IMEI，並在接收者不知情的狀況下立即結束通話，導致IMEI在神不知鬼不覺的狀況下被洩露。	過濾「183 Session Progress」中Contact標頭檔裡之隱密資訊。
	竊取詳細地理資訊	惡意用戶端建立通話的過程可得到SIP回傳訊息的「P-Access-Network-Info」，其中包含「utran-cell-id-3gpp」行動裝置連接網路的唯一標識，使得接收者的定位被準確抓取。	移除一般使用者行動裝置上之「P-Access-Network-Info」。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

23

二、基站資安檢測技術研究-檢測範疇

- 本計畫係以基站(eNodeB)為檢測標的，參考3GPP規範，依基站安全威脅規劃基站資安檢測項目。
- 檢測範疇包含與基站相關之Uu、S1、X2介面。



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

24

二、基站資安檢測技術研究-基站資安檢測項目(1/4)

❑ 一般性資安檢測項目

測試項目	測試目的
1. Initial RRC Connection Setup and Reconfiguration	驗證終端找到合適的cell後，可成功執行RRC connection establishment procedure與基站建立連線進入RRC_CONNECTED狀態。
2. UE Initial Attach (Uu介面)	驗證終端與基地台建立連線進入RRC_CONNECTED後，藉由RRC Connection Setup Complete向基站發起ESM PDN Connectivity Request與EMM Attach Request。
3. UE Initial Attach (S1介面)	驗證基地台收到終端的RRC Connection Setup後，將ESM PDN Connectivity Request與EMM Attach Request截取出來包裝成Initial UE message轉傳給MME。
4. S1 Release due to UE inactivity	驗證終端進入RRC_CONNECTED後，經過一段時間無資料傳輸(UE inactivity timer)觸發S1 release procedure，釋放SRB、radio bearer與S1 bearer進入RRC_IDLE。
5. Tracking Area Update	驗證終端週期性的Tracking Area Update (TAU)告知MME其仍然存在LTE的覆蓋範圍下，即使tracking area沒有改變。
6. Service Request	驗證終端處於RRC_IDLE狀態但需要傳送(Mobile Originated)資料時，觸發Service Request procedure進入RRC_CONNECTED，重建SRB、radio bearer與S1 bearer。
7. X2 Setup	驗證基地台與基地台之間可以透過X2介面建立連線。
8. Downlink NAS Transport	驗證下行NAS訊息(MME→終端)可正確的藉由S1介面(S1AP)與Uu介面(RRC)傳送。
9. Uplink NAS Transport	驗證上行NAS訊息(終端→MME)可正確的藉由S1介面(S1AP)與Uu介面(RRC)傳送。
10. IPSec Connection	驗證S1介面上，所有封包是否可透過eNB與MME/SGW之間的IPSec協定加密。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

25

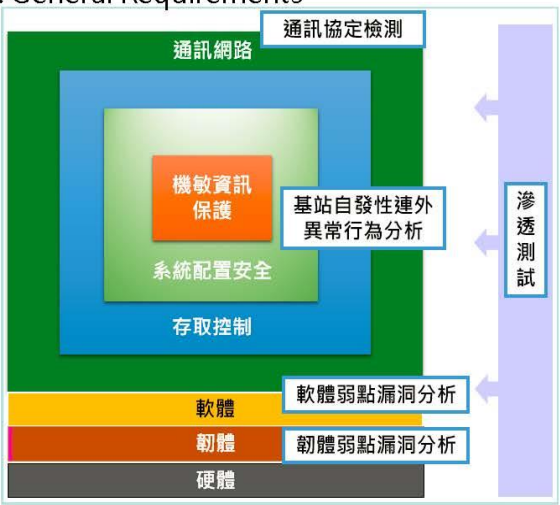
二、基站資安檢測技術研究-基站資安檢測項目(2/4)

❑ 進階性資安檢測項目

– 主要參考

(1) 3GPP 33.117 Catalogue of General Security Assurance Requirements

(2) UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

26

二、基站資安檢測技術研究-基站資安檢測項目(3/4)

❑ 進階性資安檢測項目

測試類型	測試案例	參考資料
系統配置安全	系統過載狀態時處理機制	3GPP TS 33.117 Section 4.2.3.3.1
	系統僅能由內部裝置啟動	3GPP TS 33.117 Section 4.2.3.3.2
	系統過載處理	3GPP TS 33.117 Section 4.2.3.3.3
	安全事件記錄	3GPP TS 33.117 Section 4.2.3.6.1
	網站伺服器日誌	3GPP TS 33.117 Section 4.2.5.2.1
	HTTP 使用者交談識別碼	3GPP TS 33.117 Section 4.2.5.3
	封包過濾	3GPP TS 33.117 Section 4.2.6.2.1
	網路介面堅實性需求	3GPP TS 33.117 Section 4.2.6.2.2
	GTP-C 過濾	3GPP TS 33.117 Section 4.2.6.2.3
	GTP-U 過濾	3GPP TS 33.117 Section 4.2.6.3
	網路核心功能最小化	3GPP TS 33.117 Section 4.3.3.1.2
	可移除裝置不可具備自動載入執行功能	3GPP TS 33.117 Section 4.3.3.1.3
	網站伺服器非以系統權限執行	3GPP TS 33.117 Section 4.3.4.2
	未使用之 HTTP 功能應關閉	3GPP TS 33.117 Section 4.3.4.3
	未存有不使用之附加元件	3GPP TS 33.117 Section 4.3.4.4
	無編譯器、直譯器或 shell 可使用	3GPP TS 33.117 Section 4.3.4.5
	不允許可利用 CGI 或其他腳本程式用以上傳資料	3GPP TS 33.117 Section 4.3.4.6
	網站伺服器內嵌腳本語言不得可執行系統指令	3GPP TS 33.117 Section 4.3.4.7
	網站伺服器存取權限	3GPP TS 33.117 Section 4.3.4.8
	不得存有網站伺服器相關預設文件檔	3GPP TS 33.117 Section 4.3.4.9
	不得瀏覽目錄資料夾列表	3GPP TS 33.117 Section 4.3.4.10
	HTTP 表頭不得揭露出網站伺服器資訊	3GPP TS 33.117 Section 4.3.4.11
	錯誤頁面包含網頁伺服器資訊	3GPP TS 33.117 Section 4.3.4.12
	最小化檔案關聯	3GPP TS 33.117 Section 4.3.4.13
	限制檔案存取	3GPP TS 33.117 Section 4.3.4.14
	CGI 或腳本語言應限定於特定目錄有執行權限	3GPP TS 33.117 Section 4.3.4.15
	流量分配	3GPP TS 33.117 Section 4.3.5.1
	動態內容不斷增長之處理機制	3GPP TS 33.117 Section 4.2.4.1.1.1

測試類型	測試案例	參考資料
弱點分析	系統使用之協定或服務安全	3GPP TS 33.117 Section 4.3.2.1
	限制可使用之服務	3GPP TS 33.117 Section 4.3.2.2
	未使用的軟體應予移除	3GPP TS 33.117 Section 4.3.2.4
	未安裝已不受支援之軟硬體元件	3GPP TS 33.117 Section 4.3.2.5
	緩衝區溢位防護	3GPP TS 33.117 Section 4.3.3.1.5
	連接埠掃描	3GPP TS 33.117 Section 4.4.2
	漏洞掃描	3GPP TS 33.117 Section 4.4.3

測試類型	測試案例	參考資料
通訊協定檢測	資料與資訊的傳輸防護	3GPP TS 33.117 Section 4.2.3.2.4
	ICMP 封包處理	3GPP TS 33.117 Section 4.2.4.1.1.2
	HTTPS	3GPP TS 33.117 Section 4.2.5.1

測試類型	測試案例	參考資料
存取控制	系統功能應該已驗證和授權下才得以使用	3GPP TS 33.117 Section 4.2.3.4.1.1
	帳號必須可以識別	3GPP TS 33.117 Section 4.2.3.4.1.2
	每個帳號都需要至少一個身分鑑別因子	3GPP TS 33.117 Section 4.2.3.4.1
	預先定義之帳號與通行碼應刪除或停用	3GPP TS 33.117 Section 4.2.3.4.2.2
	通行碼複雜性	3GPP TS 33.117 Section 4.2.3.4.2
	通行碼更改	3GPP TS 33.117 Section 4.2.3.4.3.2
	暴力及字典攻擊防護	3GPP TS 33.117 Section 4.2.3.4.3.3
	授權策略、角色存取控制	3GPP TS 33.117 Section 4.2.3.4.6.1, 3GPP TS 33.117 Section 4.2.3.4.6.2
	登出功能	3GPP TS 33.117 Section 4.2.3.5.1
	操作逾時功能	3GPP TS 33.117 Section 4.2.3.5.2
	高權限系統功能之存取控制	3GPP TS 33.117 Section 4.2.4.1.2.1
	系統帳號識別	3GPP TS 33.117 Section 4.2.4.2.2
	遠端登入控管	3GPP TS 33.117 Section 4.3.2.6
	檔案系統存取權限控管	3GPP TS 33.117 Section 4.3.2.7
	阻絕不明來源 IP 位址	3GPP TS 33.117 Section 4.3.3.1.1
	防止 SYN Flood 攻擊	3GPP TS 33.117 Section 4.3.3.1.4
	外部檔案系統掛載限制	3GPP TS 33.117 Section 4.3.3.1.6

測試類型	測試案例	參考資料
機敏資訊保護	防止敏感性資料外洩	3GPP TS 33.117 Section 4.2.3.2.2
	敏感性資料儲存保護	3GPP TS 33.117 Section 4.2.3.2.3
	日誌檔不可洩露個人資料	3GPP TS 33.117 Section 4.2.3.2.5
	軟體完整性	3GPP TS 33.117 Section 4.2.3.3.5
	日誌轉移至集中式管理	3GPP TS 33.117 Section 4.2.3.6.2
	安全事件日誌防護	3GPP TS 33.117 Section 4.2.3.6.3

基站自發性連外異常行為分析 | 堅實性與模糊測試 | 韌體分析

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

27

二、基站資安檢測技術研究-基站資安檢測項目(4/4)

❑ HeNB資安檢測項目

測試類型	測試案例	參考資料
敏感性資料保護檢測	用戶清單的存取控管	3GPP TS 33.320 session 8.2.2
	4G設定檔的存取控管	3GPP TS 33.320 session 8.1.4
	系統日誌的存取控管	3GPP TR 33.820 session 7.6.3.2
	密碼的儲存保護	3GPP TR 33.820 session 6.3
身分認證安全檢測	認證方式需要足夠強度	3GPP TR 33.820 session 7.4.1
	遠端管理介面的認證安全	3GPP TS 33.320 session 7.1
	憑證具唯一性	3GPP TS 33.320 session 7.2.3

測試類型	測試案例	參考資料
系統安全檢測	作業系統及網路服務安全	3GPP TS 33.320 session 5.1.2
	系統開機程序於應用層的保護	3GPP TS 33.320 session 6.1.1
	網頁管理介面的安全	3GPP TS 33.117 session 4.3.4.11
	日誌檔保存期限	3GPP TS 33.117 session 4.2.3.6.3
	日誌檔無法儲存的警示機制	3GPP TS 33.117 session 4.2.3.3.5
實體層安全檢測	家用基站的整機保護	3GPP TS 33.320 session 5.1.2
	硬體憑證的設計	3GPP TR 33.820 session 4.1

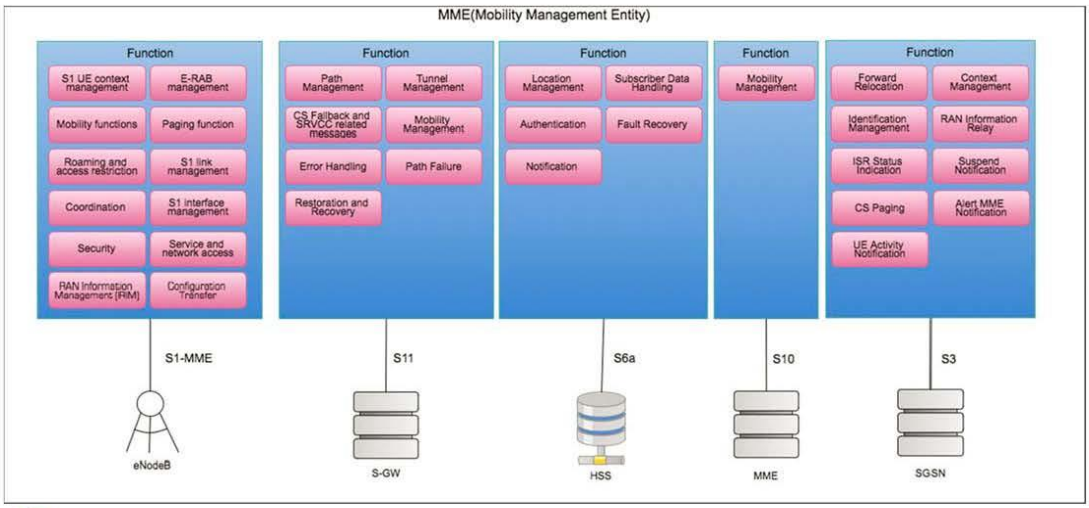
測試類型	測試案例	參考資料
韌體更新安全檢測	更新後安全參數的設置錯誤	3GPP TR 33.820 session 5.1.3
	韌體簽章驗證功能	3GPP TR 33.820 session 5.1.3
	韌體更新檔案的加密	3GPP TR 33.820 session 5.1.3
通訊協定安全檢測	後端接取鏈路的傳輸保護	3GPP TS 33.320 session 4.4.5
	首次連結核網的傳輸保護	3GPP TR session 5.1.1

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

28

三、核心網路-MME資安檢測技術研究(1/3)

- MME元件架構說明
  - MME扮演E-UTRAN與EPC間的重要橋樑，主要負責移動性管理功能，該元件對LTE網路扮演極為重要的角色。



三、核心網路-MME資安檢測技術研究(2/3)

- MME安全威脅與防護方式建議

3GPP TS 33.926 威脅項目	3GPP TS 33.401 安全項目	3GPP TS 33.116 檢測項目
A.2.2.2 重新同步	6.1.2 MME應保有同步參數(RAND、AUTN)	4.2.2.2.2 重新同步 檢測訊息回覆RAND與AUTS
A.2.2.3 完整性檢查失敗	6.1.4 當用戶身分無法被辨識或者完整性檢測失敗應回覆”用戶身分無法取得”	4.2.2.2.3 完整性檢測 檢測訊息完整性
A.2.3.1 降等威脅	7.2.4 安全模式與演算法選擇	4.2.2.3.1 降等預防 檢測所選的加密方式
A.2.3.2 NAS完整性加密的選擇與使用	7.2.4.4 NAS安全模式選擇最優先的完整性演算法	4.2.2.3.2 NAS 完整性演算法 檢測加密方式
A.2.3.3 NAS零號(NULL)完整性加密	5.1.4.1 零號完整性加密只在未授權的緊急通話時使用	4.2.2.3.3 NAS零號(NULL) 完整性防護 檢測零號加密使用
A.2.3.4 NAS 機密性加密	7.2.4.3.1 在確認NAS 安全性模式訊息給MME後，應啟用NAS 機密加密	4.2.2.3.4 NAS的機密性防護 檢測機密性加密

三、核心網路-MME資安檢測技術研究(3/3)

- MME安全威脅與防護方式建議

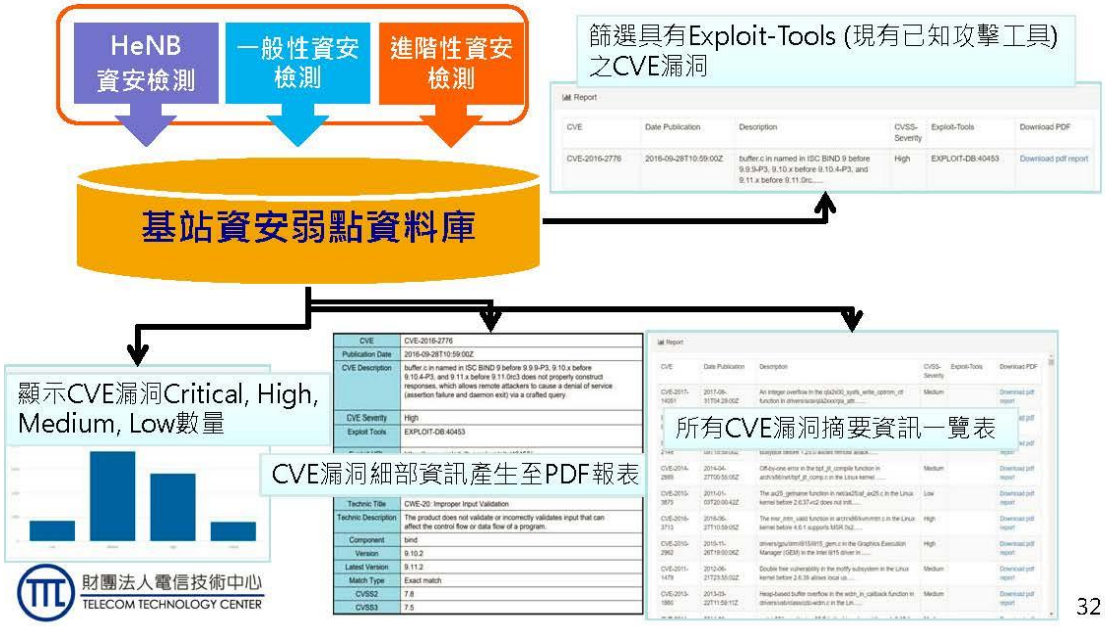
3GPP TS 33.926 威脅項目	3GPP TS 33.401 安全項目	3GPP TS 33.116 檢測項目
A.2.4.2 MME換手時，NAS完整性加密的選擇	7.2.4.3.2 MME換手 MME應根據排序中，選擇最優先的完整性加密方式	4.2.2.4.2 NAS 完整性演算法的選擇 檢測完整性加密
A.2.4.1 eNB換手時，降等攻擊	7.2.4.2.2 換手eNB時，MME應驗證從eNB收到UE安全模式，是相同於MME紀錄的UE 安全模式	4.2.2.4.1 換手時防護能力降低 記錄加密方式
A.2.2.4 傳遞EPS金鑰至SGSN	6.1.6 在MME與SGSN間，傳遞IMSI與UMTS金鑰 僅包括UMTS金鑰(CK與IK)	4.2.2.2.4 不傳輸EPS金鑰至SGSN 檢測傳遞資訊
A.2.2.5 傳遞未使用的金鑰至不同核網	6.1.5 在不同核網間，傳遞IMSI與金鑰未使用的金鑰或不同核心網路金鑰不應該在之間互相傳遞	4.2.2.2.5 EPS金鑰不傳輸於不同核網 檢測傳遞資訊
A.2.6 非緊急通道的釋放	15 IMS緊急通話 當MME或UE授權失敗時，MME或UE應釋放非緊急通道(bearers)	4.2.2.6.1 釋放非緊急通道檢測通道釋放行為

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

31

四、建置基站資安弱點資料庫

- 共蒐集**1,971**筆CVE已知漏洞，蒐集來源為基站韌體檔案分析之結果。

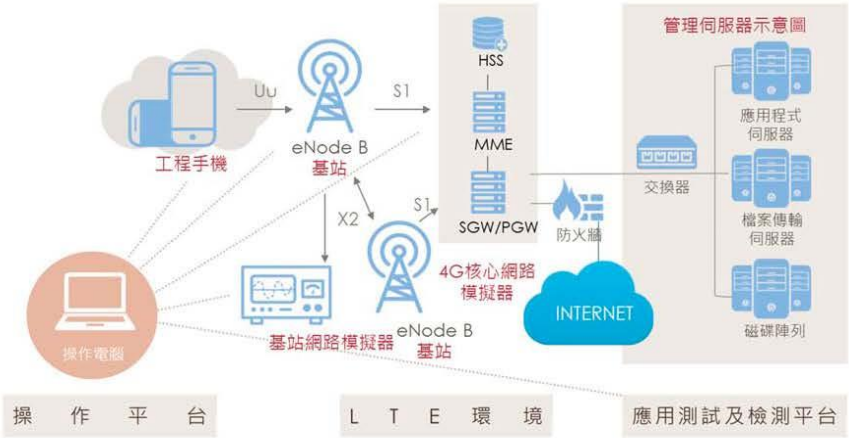


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

32

第六章建構行動寬頻基站資安檢測平臺

- 以模組化方式完成基站資安檢測示範性平臺組建，達成高彈性及高擴充性之目的。



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

33

第七章行動寬頻基站資安檢測規範草案

- 參考國際標準3GPP TS33.216及3GPP TS33.320、TR33.820，並經本團隊實測後，歸納出六大類及41項之檢測規範草案建議。

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

34

基站資安檢測結果

- 3GPP許多測試項目之要求，係從產品研發、設計、測試等階段角度來規劃， 許多測試項目對已在商轉環境下的基站並無提供相關介面功能，因而**不適用**。
- 少部分測試結果為**不通過**，並非CVE漏洞，經評估，這些項目可於後續商轉環境部署下，再做設定，或從系統層面角度調整，結合其他資安設備來達到阻隔與防護，而非以單一終端設備之觀點評估。

	N品牌			E品牌			H品牌		
安全構面	通過	不通過	不適用	通過	不通過	不適用	通過	不通過	不適用
1. 資料保護	2	1	1	1		3	2	1	1
2. 應用程式安全		1				1		1	
3. 通訊安全	10			8	2		10		
4. 身分鑑別與授權安全	9	3	2	3	3	8	11	2	1
5. 作業系統安全	6		3	6		3	5	1	3
6. 實體防護			3			3			3
總計	27	5	9	18	5	18	28	5	8

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

35

HeNB資安檢測結果

- HeNB資安檢測結果

	商用家用基站	商用家用基站(更新版)
不通過	13	8

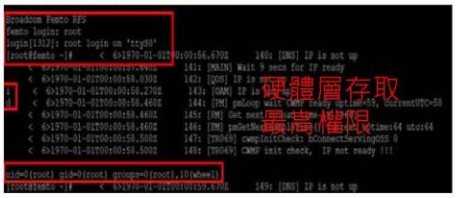
➢ 在檢測中，發現4項重大漏洞，已輔導業者進行修正，並提報國際漏洞資料庫

CVE編號	CVSS score (評分從0到10分，10代表最高風險)
CVE-2018-9112	9.8
CVE-2018-6312	9.0
CVE-2018-6311	7.2
CVE-2018-9111	5.4

- CVE-2018-9112

- CVE-2018-6312

- CVE-2018-6311



- CVE-2018-9111

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

36

基站/HeNB風險統計

- 本團隊檢測結果發現：
  - 相較於大型基站，HeNB處於高資安風險中，重大風險:3個，高風險:4個，發掘出的CVE分數也有2個9分以上。
  - HeNB的安全，包括傳輸加密、密碼複雜度等，都須仰賴電信業者網路的配置，因此HeNB確保自身的安全能力極為重要。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

37

簡報大綱

- 交付項目
- 委託研究結果
- 研究發現
- 建議事項

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

38

研究發現

一、前瞻性資安技術研究

(一)國際標準組織已訂定基站安全保證規範及安全認證流程。

(二)關注及參與國際標準組織以取得行動寬頻資安最新攻擊與防護動態之重要性。

二、國際行動框架研究

(一)國際經驗上並無對基站資安有強制性之檢測要求。

(二)國際經驗發現，政府訂定資安聯防框架，各元件安全保證標準則依循國際標準組織訂定之規範。

三、行動寬頻基站資安檢測結果

(一)發現商用基站現存之漏洞威脅：包含身分認證、網站管理介面、敏感資訊及HeNB實體層存在風險等，並已輔導業者進行修正。

(二)基站設備之安全除需從產品設計開始外，也應搭配電信業者的網管系統，結合其他資安設備來達到阻隔與防護。

四、行動寬頻基站資安檢測規範草案

(一)須考量基站設備之3GPP版本及其適用性。

(二)安全功能設定之差異性。

(三)推動第三方實驗室檢測之重要性。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

39

簡報大綱

- 交付項目
- 委託研究結果
- 研究發現
- 建議事項

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

40

建議事項

研究面

- 持續研究新興技術發展之資安議題，提供國內安全指引-5G、IoT。
- 持續關注國際標準組織之安全議題討論-3GPP TS33系列及GSMA NESAS執行進程。

技術面

- 善用基站資安檢測平臺之檢測技術及工具-輔導HeNB廠商進行檢測。
- 平臺與場域之開放-提供國產設備試驗及其相應之系統資安驗證之試驗場域。

政策面

- 主管機關與產業合作建立自願性基站檢測機制。
- 參酌國際標準，提倡由第三方檢測實驗室推動基站資安檢測規範。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

41

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

42

(二) 期末報告第 1 次審查意見回覆

「建置基站資安檢測環境計畫(第 2 期)」委託研究案
期末報告審查意見回覆

審查意見	意見回覆
一、P.599 有關建置基站弱點資料庫部分，採用韌體弱點分析面向切入，有別於 P1 Security 公司作法，惟宜評估或比較弱點資料庫之完整性是否足夠。	P1 Security 是商業性質的解決方案提供商，利用與電信業者的資安防護、弱點分析的顧問服務，建立其知識庫與資料庫，但多數屬於 3G 通訊；本平台的弱點資料庫是主要是參考 3GPP Security Assurance Specification (SCAS) for evolved Node B (eNB) network product class 標準，評估 4G 基站的韌體弱點，在研究預算限制下，利用不同廠牌的基站檢測結果，建置研究樣本的 LTE 弱點資料庫，尚無法涵蓋商業營運基站類型的完整性，因此未來若與 4G 業者持續合作，導入不同營運中的基站設備檢測，必能更為客觀且具一致性。
二、P.730-P.732 彙整國內電信業者及設備製造商意見，建議就所列意見提出回應說明，可處理作法或不為後續處理之理由。	依委員意見，就所列電信業者及設備製造商意見提出回應說明，請參見期末報告下冊 P.733-P.737。
三、第七章提出之資安檢測規範草案，建議補充說明是否已於本案建置之資安檢測平台實際驗證其可行性，另檢測結果如屬「不通過」或「不適用」之項目，如經評估應輔以商轉環境或結合其他設備判斷者，宜於檢測項目之檢測結果及判定標準作較完整之說明。	本計畫所提之基站資安檢測規範草案均已在資安檢測平臺進行相關實測驗證，確認其可行性。檢測結果如屬「不通過」或「不適用」亦與廠商討論，確認其正確性，另送檢之廠商可於自我宣告表內，提供額外的資通安全環境的證明，以符合檢測項目之安全要求。
四、本案提出之資安檢測規範草案，建議補充與 TS33.216 之差異比較，並就差異處說明差異原因及對檢測結果之影響。	依委員意見，已補充於期末報告第七章第四節(請參見期末報告下冊 P.693~P.696)。
五、本案最終目的是由 NCC 發布資安檢測規範(行動寬頻基站)，要求電信商提供使用基站產品進行	本團隊於基站資安檢測規範草案除徵詢電信業者意見外，另於 4/26 及 5/11 也分別與基站設備商 Nokia 及

1

審查意見	意見回覆
檢測，但 4/11 2 場、4/13 3 場檢測草案討論會，電信商建議及意見甚多，例如，是否由設備商來逐一說明。另，草案適用範圍和 NCC 規範並不相同等，所以本案未來的檢測程序是否應提供可行的方案供 NCC 參考。	Ericsson 徵詢對本計畫規劃之基站資安檢測規範草案意見，已將會議記錄附上(請參閱附錄五)；另草案適用範圍於座談會後已修正與 NCC 行動寬頻基地臺射頻設備技術規範之基地臺定義相同，請參閱期末報告下冊 P.687。
六、簡報 P.35 頁有測項不通過或不適用部分，其涉及需搭配 NOC 或 OAM 場域部分，是否有模擬器可模擬 NOC 或 OAM 的通訊協定，使檢測實驗室可完整檢測所有項目。	本計畫之檢測規劃均以實機為主，測項涉及需搭配 NOC 或 OAM 場域部分，因涉及各廠牌網管產品詳細的參數、專利及其價格不菲，一般模擬器無法模擬其功能，建議可在廠商自我宣告表內，提供 NOC 或 OAM 網管系統安全環境及功能證明，以符合安全要求。
七、大型基站的功能設定界面是否涉 SCADA 界面，請補充說明。	凡是具有系統監控和資料擷取功能，都可以稱之為 SCADA (Supervisory Control And Data Acquisition)，行動設備產業其慣用語為基站的網站伺服器（Web Server）或網管系統 Operations support systems (OSS)，均可提供資料採集與監控。
八、報告 P.219 表 3-24 之產品名稱內容，謹蒐集到華為基地台產品，請研究團隊再檢視是否有其他通信製造商之基站亦通過 CC 認證？	經本團隊確認，近年通過 CC 認證之通信基站相關產品，唯有華為的產品送審並通過，其餘資料大多與通信基站產品無關，故報告內呈現所蒐集到之的產品內容。
九、第 5 章有依實測訂定相關欄位，其中有合格判定標準欄(如 P.387)，但第 7 章第四節檢測項目與要求之各欄位，並無法對映至第 5 章，建請就檢測結果及判定標準建議(如 P.693)，應有有利判定合格之規範，請再檢視內容。	已依委員意見，對應第五章第二節基站資安檢測技術研究內容，修訂第七章第四節檢測項目與要求之欄位。請參見期末報告下冊 P.696~P.731。
十、第 7 章請就檢測所需的測試工具及規格，請一併增列。	依委員意見，已將測試工具及規格整理於期末報告第七章 P.691~P.692 表

審查意見	意見回覆
	7- 2 網路單元與檢測設備一覽表。
十一、上冊第 5 頁第 1 段請再說明清楚。	已依委員意見，修訂系統、軟體漏洞威脅之說明，請參見期末報告上冊 P.5。
十二、上冊第 76 頁美國國家通訊協調中心簡稱為 NCC?通訊訊息共享與分析中心簡稱為 ICAC?	已依委員意見，確認美國國家通訊協調中心簡稱為 NCC，並將通訊訊息共享與分析中心之簡稱修正為 ISAC，請參見期末報告上冊 P.76。
十三、下冊 P.333 手機將嘗試連接偽基站、P.334 手機將偽基站作為新的細胞選擇是指 handover 到偽基站嗎?	期末報告下冊 P.334 手機將嘗試連接偽基站、P.335 手機將偽基站作為新的細胞選擇並非指 Handover 到偽基站，而是指因偽基站功率較正常基站強，強迫手機連接，達到 LTE 控制通道欺騙的效果。
十四、是否了解 2 家通過 GSMA 認可的實驗室有接受華為送測的 eNB。	GSMA 依 NESAS 指引，通過 2 家檢測實驗室認證之資訊尚未正式對外公布，上述資訊係為本團隊訪問設備商 Ericsson 時得知，該設備商也尚未得知是哪 2 家檢測實驗室，僅告知 GSMA 有聯繫總公司，表示將於今年試行，Ericsson 將配合相關檢測。
十五、下冊 P.386(四)一般性資安檢測項目研究及測試結果內容比較像 4G protocol 測試，而(五)進階資安檢測項目研究及測試結果參照的是 TS33.117(一般安全保證要求目錄)，在用語上是否妥適?	期末報告 P.387 (四)一般性資安檢測項目研究及測試結果為確認 4G protocol 內的安全功能被支援與啟動。而(五)進階資安檢測項目研究及測試結果為因應不同廠牌需求，而有對應不同之系統設定配置，及確保基站在進行通訊以及接收控制訊號時與核心網路的安全性，因 TS33.117 為 3GPP 標準組織主要安全文件，有對應網路元件的一般安全要求，內容包含作業系統、網路伺服器設備等類別及存取認證、資料完整性、資料防護等測試案例，故佐以參考及引用。
十六、基站產品之資安源於產品研發、設計階段之規劃，爰電信業	型式認證為技術審驗，但資安檢測在國際上非強制性要求，原則上以自律

審查意見	意見回覆
者於座談會中建議應將基站資安檢測規範要求納入型式認證規範，惟與國際趨勢採自願性基站資安檢測不符。建議將基站檢測技術規範項目分屬設計面、服務操作面，以利設備商及電信業者參用。	為主。如項目分屬設計面、服務操作面，審酌目前在各國電信政策、標準組織及相關產業條件並參考外界對資安認證方式等前提下，仍以網路元件基站產品進行檢測較為適宜。電信業者也可以合格供應商的條件，要求設備商符合安全要求。
十七、請具體說明未來如何利用基站資安檢測平台之檢測技術及工具輔導國內 HeNB 廠商進行檢測，以開擴商機。	本團隊透過模組化方式建構基站資安檢測示範性平臺，可彈性加入其他元件或檢測工具，延伸至其他設備如 Small Cell、MEC Gateway、Smart meter (瓦斯表)+NB-IoT 等資安驗證場域，國內 HeNB 廠商，可利用本計畫之基站資安檢測平臺擴展應用於上述設備之檢測(請參閱期末報告下冊 P.753~P.755 第九章第二節二.技術面之建議)。
十八、請提供計畫成果之後續推廣措施建議，並說明本案引進之相關設備，如何發揮最大效益。	依委員意見，已詳細說明本計畫成果之後續推廣措施建議，請參閱期末報告下冊 P.752~P.756 第九章第二節之後續建議事項，並於技術面之善用基站資安檢測平臺及平臺與場域開放，增加本案引進之相關設備，如何發揮最大效益說明。
十九、請說明計畫主要成就及成果之價值，貢獻度，並說明達成量化指標或質化效益與原計畫預期效益之差異。	依委員意見，於續行討論簡報中詳細說明。
二十、計畫實際執行與原計畫目標之達成，是否遭遇困難，有否提出可行之因應對策。	原基站資安檢測平臺係以購置核心網路系統完成建置，有鑒於其購置費用龐大且已有實驗室購置，故配合 NCC 變更計畫，改以租賃核心網路之方式，完成本計畫基站資安檢測平臺建置及基站檢測項目之實測驗證。
二十一、請說明基站資安檢測之可檢測性及其效益，並說明測試時，可能面臨之實際困難及限制，並	本團隊確認待測基站能與測試平臺相通，透過通訊協定測試及相關之信令測試來實現基站檢測之可檢測性。基

審查意見	意見回覆
提出建議解決方案。	站資安檢測之可檢測性為基站在 S1 傳輸介面負責定義 eNodeB 和移動管理實體/服務閘道器間控制訊息與資料封包的溝通傳遞，及 eNodeB 之間互相連接溝通的 X2 傳輸介面，所支援的通訊協定，包含 SCTP 與 GTP 通訊協定，除了利用 IP 封包來封裝使用者與控制層的訊息，上面還會疊加其他不同的通訊協定來當作路由、機密性保護、完整性保護的實作機制。 其效益為分析基站通訊流程所涵蓋的 S1 介面、X2 介面或管理介面可能的威脅，提出風險評估以避免攻擊的發生，降低風險及提高安全為目標，以確保使用者的通訊安全及維護國家重要的基礎建設。 可能面臨之實際困難及限制為基站及核心網路在不同的硬體、軟體及韌體間其對於安全功能的支援程度不一，加上各廠牌的功能配置方式的差異性，其解決方案為檢測時必須由廠商提供自我宣告表包含產品文件或技術手冊，來設定基站待測物與檢測平台互通性的參數，必要時需有基站開發或技術人員一同參與，以確認功能正常狀態，滿足檢測的需要。
二十二、 針對 SS7、5G、SDN、IoT 於期末報告，請各獨立一小節說明此四大項之具體防護技術及建議。	於期末報告第三章第二節已針對 SS7、5G、SDN、IoT 個別獨立篇幅說明其具體防護技術及建議，請參閱期末報告上冊 P.62~P.171。
二十三、 請具體說明有輔導過的廠商之資安測試或研發之案例。	依委員意見，本團隊輔導廠商案例於續行討論簡報中說明。
二十四、 期末簡報，請納入期末報告。	依委員意見，已將期末簡報納入期末報告附錄中(請參見期末報告附錄七)。
二十五、 基站資安檢測結果，檢測評估可能有誤判，應提供原廠商確	為證實檢測項目之適用性及分析結果之正確性，本研究之檢測結果已於座

審查意見	意見回覆
認及收集其回應。	談會提供使用該設備的電信業者與設備商確認，並與之討論及蒐集其回應，以做為檢測方法確認之評估依據(請參閱期末報告下冊 P.736~P.737 及附錄五)。 不同的廠商有不同的回應方式，國外廠商皆表示須與總公司確認，對檢測項目及檢測結果無法一一回應，或回應未來的設備版本會有所改善；國內廠商則較為積極，會在短時間進行設備的安全功能更新。
二十六、 基站檢測規範每一測試，必須說明所依據之國際標準。	依委員意見，每一測試項目皆於檢測依據欄位說明所依據之國際標準，請參閱期末報告下冊第七章第四節檢測項目與要求之檢測依據欄位。請參見期末報告下冊 P.693~P.731。

二、 期末報告第 2 次審查會議

(一) 期末報告第 2 次審查會議簡報

簡報大綱

- 計畫實際執行與原計畫目標符合程度說明
- 委託計畫經費與人力運用之妥適度
- 計畫主要成就及成果(重大突破)之價值、貢獻度
- 後續工作構想及重點

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

3

計畫實際執行與原計畫目標符合程度說明(1/6)

- 計畫執行與原計畫規劃符合程度說明
  - 因104年計畫內容已與105年合併，本計畫實際執行成果皆符合原計畫內容及目標。

104年及105年計畫內容			實際執行說明	章節	符合程度
一、前瞻性資安檢測技術研究	(一)資安防護技術與服務最新趨勢研究	蒐集國內外電信與資安技術及標準發展之最新趨勢，探討行動寬頻相關應用資安與防禦技術，供產官學界參考。	透過國外參訪及文獻研析，針對SS7、5G、SDN及IoT四大主題，個別從其架構、資安威脅與最新攻擊趨勢進行分析，並提出資安防護建議。	第三章第一節	符合
	(二)資安檢測標準與檢測流程最新趨勢研究		深入與行動寬頻基站資安相關之國際檢測標準及檢測流程最新趨勢發展進行探討，包含基站安全保證規範3GPP TS33.216及其關聯性安全規範；檢測流程參考GSMA發表之網通設備安全認證方法；最後參考最新通過CC認證之行動寬頻網路設備文件。	第三章第二節	符合
	(三)國際行動寬頻資安框架研究		介紹美國、加拿大、英國、歐盟及日本等國網路安全策略，與相關權責機關架構之發展狀況，及國際間行動寬頻資安政策發展現況及最佳實務。	第四章第一節~第七節	符合

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

4

計畫實際執行與原計畫目標符合程度說明(2/6)

❑ 計畫執行與原計畫規劃符合程度說明

104年及105年計畫內容			實際執行說明	章節	符合程度
二、行動寬頻資安技術研究	(一) 空中介面資安檢測技術研究	利用行動寬頻網路運作過程中最基礎的空中介面資安技術研究，聚焦於行動寬頻基站資安檢測技術及方法，作為執行基站系統資安檢測採用技術之參考。	透過文獻分析及實驗方法，探討空中介面相關之資安議題，包含探討偽基站造成用戶端(UE)隱私之可能資安議題，提出可能之解決方案。另透過文獻分析，研析新一代的語音通信技術VoLTE對LTE網路所產生的安全漏洞與防禦技術。	第五章第一節	符合
	(二)基站資安檢測技術研究		參考國際資安檢測技術規範3GPP TS33.216、TS33.117、TS33.320及TR33.820，規劃基站資安檢測技術及檢測項目，其安全要求適用於所有基站類型，分別以一般性資安檢測、進階性資安檢測項目與家用基站分述。所有檢測項目包含測試案例名稱、參考資料、測試目的、資訊安全需求(CIA)、測試環境暨初始條件、測試方法及合格判定標準。	第五章第二節	符合
	(三)核心網路-MME資安檢測技術研究	於實際執行中	完成MME元件架構及功能研究、介面安全性研究、相關介面弱點分析及安全威脅分析。	第五章第三節	符合

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

5

計畫實際執行與原計畫目標符合程度說明(3/6)

❑ 計畫執行與原計畫規劃符合程度說明

104年及105年計畫內容			實際執行說明	章節	符合程度
三、行動寬頻基站資安檢測方針研究	行動寬頻基站資安檢測規範草案	依循前期計畫執行結果，研擬本計畫之行動寬頻基站資安檢測項(Test Case)，包含國際標準中之基礎功能檢測(如相容性及安全配置)、行動寬頻網路威脅之進階功能檢測(如偽基站偵測)與基站系統和其連結介面(如通訊介面檢測)之規劃及檢測。	參照國際標準3GPP TS33.216、TS33.320及TR33.820，與本計畫檢測結果及座談會訪談建議，完成行動寬頻基站資安檢測規範草案建議。內容包含： (一)檢測環境建議 (二)檢測項目要求 (三)檢測結果及判定標準建議 (四) 檢測作業程序	第七章第一節~第五節	符合
四、建構行動寬頻資安檢測平臺	透過國內學界及電信業者經驗，參照3GPP LTE 架構規範，建構行動寬頻(LTE)實驗環境，含UE、eNB、EPC 到網際網路(Internet)。並於該環境架構上架設IP 網路適用之一般性資安檢測平臺及基站資安檢測平臺。		依所規劃之檢測平臺完成架設，並完成整合驗證測試，確認本計畫所建構之行動寬頻基站資安檢測平臺可穩定運行，且所採購之檢測工具亦可進行基站資安檢測。	第六章第一節~第三節	符合

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

6

計畫實際執行與原計畫目標符合程度說明(4/6)

❑ 計畫執行與原計畫規劃符合程度說明

104年及105年計畫內容			實際執行說明	章節	符合程度
五、行動寬頻資安檢測	1. 一般性資安檢測項實測 2. 基站資安檢測項實測	針對行動寬頻網路中的『基站』進行實測，涵蓋基站系統(eNodeB /HeNB 等)其連接相關介面(S1與X2)、實體線路、設備及網路架構進行資安檢測，驗證系統配置安全與各項軟體弱點檢測項(Test Case)。	完成第五章第二節規劃之基站資安檢測項目實測驗證，詳細說明每一測項之檢測結果與檢測畫面，並進行以下分類說明檢測結果。 1.一般性資安檢測項目實測結果(基本通信協定及相關信令測試) 2.進階性資安檢測項目實測結果 3.家用基站資安檢測項目實測結果	第五章第二節	符合
	3. 建置基站弱點資料庫	於實際執行中	依本計畫檢測之基站/家用基站樣本結果，及參考NVD國際弱點資料庫，建置一基站弱點資料庫。目前已蒐集1,971筆CVE已知漏洞，蒐集來源為基站韌體檔案分析之結果。	第五章第四節	符合

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

7

計畫實際執行與原計畫目標符合程度說明(5/6)

❑ 計畫執行與原計畫規劃符合程度說明

104年及105年計畫內容		實際執行說明	章節	符合程度
六、行動寬頻基站資安檢測作業程序標準化	研析國際知名資通訊研究機構取得國外研究經驗、基站系統資安檢測標準作業程序、與先進國家法規政策參考資料。藉由一般性資安及基站資安實測驗證，提供行動寬頻資安檢測應具備之具體檢測項內容、方法、流程及指標，以完善我國基站資安檢測作業程序標準化之參考。	於行動寬頻基站資安檢測規範草案之檢測項目與要求中，每一檢測項目皆有詳細之檢測作業程序說明。	第七章第四節	符合
七、資安檢測標準作業程序座談會	邀集產官學界，針對本計畫建議之檢測作業程序進行座談，蒐集相關意見。	舉辦7場(5場電信業者;2場設備商)針對基站資安檢測規範草案及檢測流程之座談。	第八章第一節及附錄五	符合

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

8

計畫實際執行與原計畫目標符合程度說明(6/6)

❑ 計畫執行與原計畫規劃符合程度說明

104年及105年計畫內容		實際執行說明	章節	符合程度
八、行動寬頻基站資安檢測環境推動研討會	舉辦研討會，推廣本計畫研究建議之檢測環境、檢測方針及管理機制 ①本計畫研究提出之行動寬頻基站資安檢測環境(含檢測方針)建議方案推廣及研討 ②本計畫提出之行動寬頻基站資安管理方針推廣	完成1場動寬頻基站資安研討會之舉辦，邀集電信業者、設備商、檢測實驗室及學界等推廣本計畫之基站資安檢測規範草案及檢測環境。	第八章第二節及附錄六	符合
九、行動寬頻基站資安檢測環境推動研討會				符合

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

9

簡報大綱

- 計畫實際執行與原計畫目標符合程度說明
- 委託計畫經費與人力運用之妥適度
- 計畫主要成就及成果(重大突破)之價值、貢獻度
- 後續工作構想及重點

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

10

委託計畫經費與人力運用之妥適度

- 人力實際進用與原規劃差異說明：本計畫人力實際進用均依原規劃辦理。

計畫名稱	執行情形	105年度						
		研究員級	副研究員級	助理研究員級	助理級	技術人員	其他	總人力(人年)
建置基站資安檢測環境	原訂	6.3	4.3	7.9	4.0	0	0	22.5
	實際	6.3	4.3	7.9	4.0	0	0	22.5
	差異	0	0	0	0	0	0	0

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

11

簡報大綱

- 計畫實際執行與原計畫目標符合程度說明
- 委託計畫經費與人力運用之妥適度
- 計畫主要成就及成果(重大突破)之價值、貢獻度
- 後續工作構想及重點

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

12

計畫主要成就及成果(重大突破)之價值、貢獻度

- 本計畫所達成量化指標及質化效益與原計畫預期效益相符，所達成之績效指標如下：

一、學術成就(科技基礎研究)

績效指標類別	績效指標項目	105年度		達成說明
		原訂目標值	實際達成值	
B.合作團隊(計畫)養成	跨機構合作團隊(計畫)數	3	3	
C.培育及延攬人才	博士培育/訓人數	0	1	
D1.研究報告	研究報告篇數	1	1	研究報告：建置基站資安檢測環境計畫(第2期)

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

13

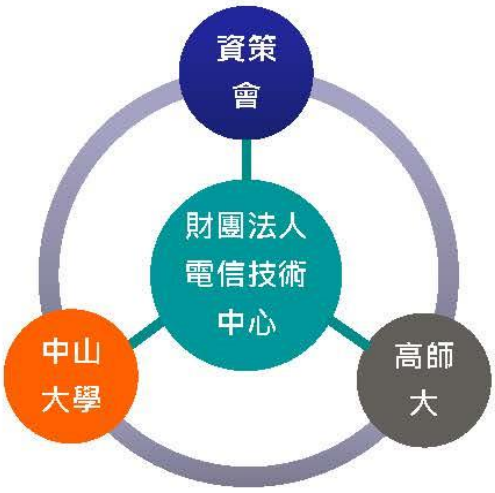
學術成就-B.合作團隊(計畫)養成/C.培育及延攬人才

- **合作團隊養成：**

財團法人電信技術中心，結合法人機構資策會之HeNB檢測能量；以及與學界：中山大學、高雄師範大學3個機構共組研究團隊，以各方之專長合作完成本計畫內容。

- **延攬人才:**

聘用1位中山大學博士生加入TTC資安組團隊中協助本計畫之延續工作。



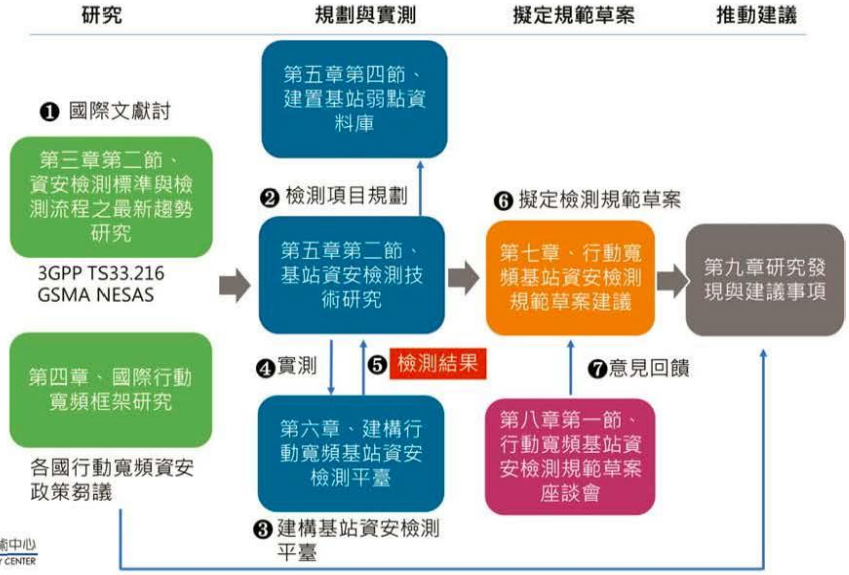
進一步培育國內行動寬頻資安產業所需之工程、技術服務人才。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

14

學術成就-D1.研究報告

- 本團隊將本計畫工作項目:行動寬頻資安技術研究、行動寬頻基站資安檢測規範草案、行動寬頻基站資安檢測程序、建構行動寬頻資安檢測平臺、行動寬頻資安檢測結果報告及座談會與研討會成果綜整至1份研究報告中。



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

15

計畫主要成就及成果(重大突破)之價值、貢獻度

二、技術創新(科技技術創新)

績效指標類別	績效指標項目	105年度		達成說明	重大突破
		原訂目標值	實際達成值		
H.技術報告及檢驗方法	新技術開發或技術升級開發之技術報告篇數	1	1	研究報告第五章第二結基站資安檢測技術研究	檢測過程，發現國內商用家用基站之嚴重安全漏洞，已同時通報並輔導廠商修正。
I1.辦理技術活動	辦理技術研討會場次	1	1	相關記錄：研究報告第八章第二節及附錄六	
	辦理技術說明會或推廣活動場次	1	7	相關記錄：研究報告第八章第一節及附錄五	

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

16

技術創新(科技技術創新)

H.技術報告及檢驗方法

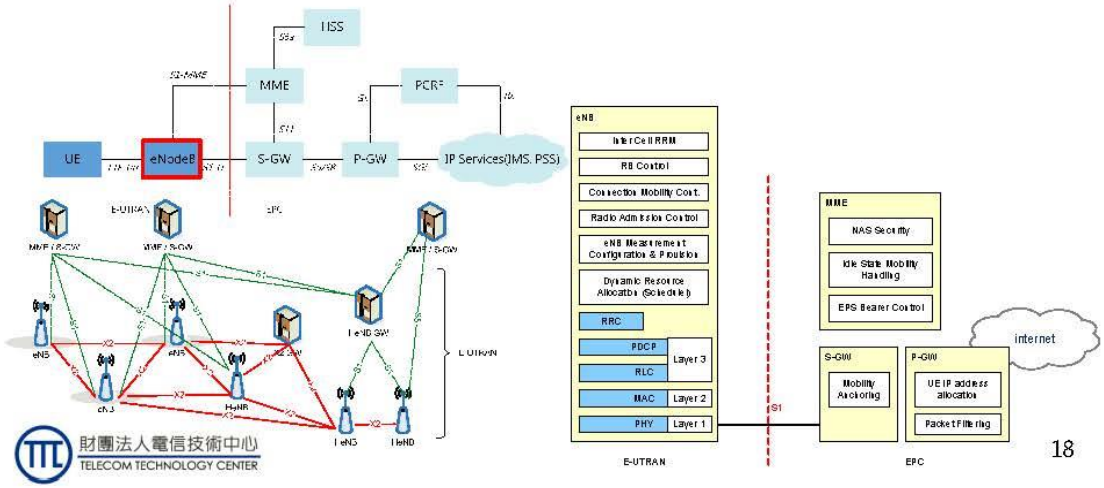
基站資安檢測項目研究

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

17

基站資安檢測技術研究-檢測範疇

- 本計畫係以基站(eNodeB)為檢測標的，參考3GPP TS33.216、TS33.117、TS33.320及TR33.820，依基站安全威脅規劃基站資安檢測項目。檢測範疇包含與基站相關之Uu、S1、X2介面。
- 本計畫參考國際標準規劃出基站一般性、進階性及HeNB資安檢測項目，並經實測驗證後，供基站資安檢測規範草案研擬時參考。每項檢測項目包含參考資料、檢測目的、測試環境暨初始條件、測試方法、合格判定標準建議，及實際測試結果報告。



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

18

基站資安檢測技術研究-基站資安檢測項目(1/4)

❑ 一般性資安檢測項目

測試項目	測試目的
1. Initial RRC Connection Setup and Reconfiguration	驗證終端找到合適的cell後，可成功執行RRC connection establishment procedure與基站建立連線進入RRC_CONNECTED狀態。
2. UE Initial Attach (Uu介面)	驗證終端與基地台建立連線進入RRC_CONNECTED後，藉由RRC Connection Setup Complete向基站發起ESM PDN Connectivity Request與EMM Attach Request。
3. UE Initial Attach (S1介面)	驗證基地台收到終端的RRC Connection Setup後，將ESM PDN Connectivity Request與EMM Attach Request截取出來包裝成Initial UE message轉傳給MME。
4. S1 Release due to UE inactivity	驗證終端進入RRC_CONNECTED後，經過一段時間無資料傳輸(UE inactivity timer)觸發S1 release procedure，釋放SRB、radio bearer與S1 bearer進入RRC_IDLE。
5. Tracking Area Update	驗證終端週期性的Tracking Area Update (TAU)告知MME其仍然存在LTE的覆蓋範圍下，即使tracking area沒有改變。
6. Service Request	驗證終端處於RRC_IDLE狀態但需要傳送(Mobile Originated)資料時，觸發Service Request procedure進入RRC_CONNECTED，重建SRB、radio bearer與S1 bearer。
7. X2 Setup	驗證基地台與基地台之間可以透過X2介面建立連線。
8. Downlink NAS Transport	驗證下行NAS訊息(MME→終端)可正確的藉由S1介面(S1AP)與Uu介面(RRC)傳送。
9. Uplink NAS Transport	驗證上行NAS訊息(終端→MME)可正確的藉由S1介面(S1AP)與Uu介面(RRC)傳送。
10. IPSec Connection	驗證S1介面上，所有封包是否可透過eNB與MME/SGW之間的IPSec協定加密。

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

19

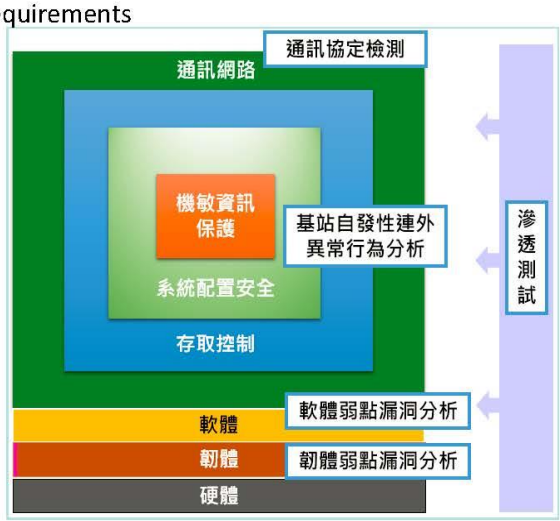
基站資安檢測技術研究-基站資安檢測項目(2/4)

❑ 進階性資安檢測項目

– 主要參考

(1) 3GPP 33.117 Catalogue of General Security Assurance Requirements

(2) UL 2900-1 Standard for Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements



財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

20

基站資安檢測技術研究-基站資安檢測項目(3/4)

❑ 進階性資安檢測項目

測試類型	測試案例	參考資料
系統配置安全	系統過載狀態時處理機制	3GPP TS 33.117 Section 4.2.3.3.1
	系統僅能由內部裝置啟動	3GPP TS 33.117 Section 4.2.3.3.2
	系統過載處理	3GPP TS 33.117 Section 4.2.3.3.3
	安全事件記錄	3GPP TS 33.117 Section 4.2.3.6.1
	網站伺服器日誌	3GPP TS 33.117 Section 4.2.5.2.1
	HTTP 使用者交談識別碼	3GPP TS 33.117 Section 4.2.5.3
	封包過濾	3GPP TS 33.117 Section 4.2.6.2.1
	網路介面堅實性需求	3GPP TS 33.117 Section 4.2.6.2.2
	GTP-C 過濾	3GPP TS 33.117 Section 4.2.6.2.3
	GTP-U 過濾	3GPP TS 33.117 Section 4.2.6.3
	網路核心功能最小化	3GPP TS 33.117 Section 4.3.3.1.2
	可移除裝置不可具備自動載入執行功能	3GPP TS 33.117 Section 4.3.3.1.3
	網站伺服器非以系統權限執行	3GPP TS 33.117 Section 4.3.4.2
	未使用之 HTTP 功能應關閉	3GPP TS 33.117 Section 4.3.4.3
	未存有不使用之附加元件	3GPP TS 33.117 Section 4.3.4.4
	無編譯器、直譯器或 shell 可使用	3GPP TS 33.117 Section 4.3.4.5
	不允許可利用 CGI 或其他腳本程式用以上傳資料	3GPP TS 33.117 Section 4.3.4.6
	網站伺服器內嵌腳本語言不得可執行系統指令	3GPP TS 33.117 Section 4.3.4.7
	網站伺服器存取權限	3GPP TS 33.117 Section 4.3.4.8
	不得存有網站伺服器相關預設文件檔	3GPP TS 33.117 Section 4.3.4.9
	不得瀏覽目錄資料夾列表	3GPP TS 33.117 Section 4.3.4.10
	HTTP 表頭不得揭露出網站伺服器資訊	3GPP TS 33.117 Section 4.3.4.11
	錯誤頁面包含網頁伺服器資訊	3GPP TS 33.117 Section 4.3.4.12
	最小化檔案關聯	3GPP TS 33.117 Section 4.3.4.13
	限制檔案存取	3GPP TS 33.117 Section 4.3.4.14
	CGI 或腳本語言應限定於特定目錄有執行權限	3GPP TS 33.117 Section 4.3.4.15
	流量分配	3GPP TS 33.117 Section 4.3.5.1
	動態內容不斷增長之處理機制	3GPP TS 33.117 Section 4.2.4.1.1.1

測試類型	測試案例	參考資料
弱點分析	系統使用之協定或服務安全	3GPP TS 33.117 Section 4.3.2.1
	限制可使用之服務	3GPP TS 33.117 Section 4.3.2.2
	未使用的軟體應予移除	3GPP TS 33.117 Section 4.3.2.4
	未安裝已不受支援之軟硬體元件	3GPP TS 33.117 Section 4.3.2.5
	緩衝區溢位防護	3GPP TS 33.117 Section 4.3.3.1.5
	連接埠掃描	3GPP TS 33.117 Section 4.4.2
	漏洞掃描	3GPP TS 33.117 Section 4.4.3

測試類型	測試案例	參考資料
通訊協定檢測	資料與資訊的傳輸防護	3GPP TS 33.117 Section 4.2.3.2.4
	ICMP 封包處理	3GPP TS 33.117 Section 4.2.4.1.1.2
	HTTPS	3GPP TS 33.117 Section 4.2.5.1

測試類型	測試案例	參考資料
存取控制	系統功能應該已驗證和授權下才得以使用	3GPP TS 33.117 Section 4.2.3.4.1.1
	帳號必須可以識別	3GPP TS 33.117 Section 4.2.3.4.1.2
	每個帳號都需要至少一個身分鑑別因子	3GPP TS 33.117 Section 4.2.3.4.1
	預先定義之帳號與通行碼應刪除或停用	3GPP TS 33.117 Section 4.2.3.4.2.2
	通行碼複雜性	3GPP TS 33.117 Section 4.2.3.4.2
	通行碼更改	3GPP TS 33.117 Section 4.2.3.4.3.2
	暴力及字典攻擊防護	3GPP TS 33.117 Section 4.2.3.4.3.3
	授權策略、角色存取控制	3GPP TS 33.117 Section 4.2.3.4.6.1, 3GPP TS 33.117 Section 4.2.3.4.6.2
	登出功能	3GPP TS 33.117 Section 4.2.3.5.1
	操作逾時功能	3GPP TS 33.117 Section 4.2.3.5.2
	高權限系統功能之存取控制	3GPP TS 33.117 Section 4.2.4.1.2.1
	系統帳號識別	3GPP TS 33.117 Section 4.2.4.2.2
	遠端登入控管	3GPP TS 33.117 Section 4.3.2.6
	檔案系統存取權限控管	3GPP TS 33.117 Section 4.3.2.7
	阻絕不明來源 IP 位址	3GPP TS 33.117 Section 4.3.3.1.1
	防止 SYN Flood 攻擊	3GPP TS 33.117 Section 4.3.3.1.4
	外部檔案系統掛載限制	3GPP TS 33.117 Section 4.3.3.1.6

測試類型	測試案例	參考資料
機敏資訊保護	防止敏感性資料外洩	3GPP TS 33.117 Section 4.2.3.2.2
	敏感性資料儲存保護	3GPP TS 33.117 Section 4.2.3.2.3
	日誌檔不可洩露個人資料	3GPP TS 33.117 Section 4.2.3.2.5
	軟體完整性	3GPP TS 33.117 Section 4.2.3.3.5
	日誌轉移至集中式管理	3GPP TS 33.117 Section 4.2.3.6.2
	安全事件日誌防護	3GPP TS 33.117 Section 4.2.3.6.3

基站自發性連外異常行為分析 | 堅實性與模糊測試 | 韌體分析

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

21

基站資安檢測技術研究-基站資安檢測項目(4/4)

❑ HeNB資安檢測項目

測試類型	測試案例	參考資料
敏感性資料保護檢測	用戶清單的存取控管	3GPP TS 33.320 session 8.2.2
	4G設定檔的存取控管	3GPP TS 33.320 session 8.1.4
	系統日誌的存取控管	3GPP TR 33.820 session 7.6.3.2
	密碼的儲存保護	3GPP TR 33.820 session 6.3
身分認證安全檢測	認證方式需要足夠強度	3GPP TR 33.820 session 7.4.1
	遠端管理介面的認證安全	3GPP TS 33.320 session 7.1
	憑證具唯一性	3GPP TS 33.320 session 7.2.3

測試類型	測試案例	參考資料
系統安全檢測	作業系統及網路服務安全	3GPP TS 33.320 session 5.1.2
	系統開機程序於應用層的保護	3GPP TS 33.320 session 6.1.1
	網頁管理介面的安全	3GPP TS 33.117 session 4.3.4.11
	日誌檔保存期限	3GPP TS 33.117 session 4.2.3.6.3
	日誌檔無法儲存的警示機制	3GPP TS 33.117 session 4.2.3.3.5
實體層安全檢測	家用基站的整機保護	3GPP TS 33.320 session 5.1.2
	硬體憑證的設計	3GPP TR 33.820 session 4.1

測試類型	測試案例	參考資料
韌體更新安全檢測	更新後安全參數的設置錯誤	3GPP TR 33.820 session 5.1.3
	韌體簽章驗證功能	3GPP TR 33.820 session 5.1.3
	韌體更新檔案的加密	3GPP TR 33.820 session 5.1.3
通訊協定安全檢測	後端接取鏈路的傳輸保護	3GPP TS 33.320 session 4.4.5
	首次連結核網的傳輸保護	3GPP TR session 5.1.1

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

22

技術創新(科技技術創新)

I1.辦理技術活動

研究報告第八章行動寬頻資安座談會及研討會辦理成果

-辦理技術研討會場次:1場

-辦理技術說明會或推廣活動場次:7場

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

23

行動寬頻基站資安研討會

- 本團隊於107/5/4舉辦1場行動寬頻基站資安研討會，參加人數共約90人，參加人員主要為五大電信業者代表，其次為基站及HeNB設備製造商，及檢測實驗室代表。
- 本次研討會目的為：行動寬頻基站資安國際標準動態說明及行動寬頻基站資安檢測草案之發表與基站資安檢測平臺開放場域之推廣。




財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

24

行動寬頻基站資安檢測規範草案座談會

- 於107年4月11日、4月13日、4月26及5月4日邀集五大電信業者及設備商Nokia、Ericsson，個別舉辦7場行動寬頻基站資安檢測標準座談會(5場電信業者; 2場設備商)，蒐集業者及設備商對基站資安檢測規範草案之意見，作為未來制定及執行之參考，並推廣本計畫基站資安檢測平臺，鼓勵業者提供基站設備送測。
- 座談會業者意見及本團隊回應請參見研究報告第八章第一節。




財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

25

計畫主要成就及成果(重大突破)之價值、貢獻度

三、經濟效益(經濟產業促進)

績效指標類別	績效指標項目		105年度		達成說明
			原訂目標值	實際達成值	
O.共通/檢測技術服務及輔導	輔導廠商或產業團體技術或品質提升、技術標準認證、實驗室認證、申請與執行主導性新產品及關鍵性零組件等	廠商家數	0	1	輔導廠商實例-國內HeNB廠商

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

26

檢測結果

No.	安全威脅	修正建議
1.	取得root權限此基站已成為殭屍網路的成員。	Root權限需設密碼，且密碼需高複雜度。
2.	由於後端網路對家用基站是採取信任的介接，可能會變成電信商後端網路的突破口	後端網路最好透過專線方式連接，或者網頁介面不能存在已知漏洞。
3.	硬體端的UART進入後即為最高使用者root權限。	硬體部分，不可以透過UART或是JTAG來存取到debug mode，或者是設定高複雜度之登入密碼。
4.	IPsec憑證會顯示在管理者權限之網頁上，因此可以利用憑證來與後端網路進行假身分的連接，或是對IPsec下傳輸的封包進行解密，造成使用者資訊將洩漏。	憑證資訊不可顯示在網頁上，必須加密保護。

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

27

輔導廠商過程(1/4)

1. 於發現漏洞後第一時間通報業者


使用[redacted]發現資安方面問題 收件匣 x [redacted]@iii.org.tw x

[redacted] Kao 1月24日

寄給 eservice、 蔡正煜、 許明淵、 黃川源、 dmliu

Dear Sir/Madam,

您好，我是資策會的員工，
由於本會有中[redacted]使用，
在使用過程中發現該產品有資安方面的問題，恐面臨資安威脅，

想跟貴司相關部門詢問，以進一步釐清問題，
感謝，

If you have any question, please do not hesitate to let me know.

best regards,
高[redacted] Kao

財團法人資訊工業策進會 Institute for Information Industry, III
資安科技研究所 Cybersecurity Technology Institute
105台北市松山區民生東路[redacted]
[redacted] Minsheng E. Rd.,Taipei,Taiwan, R.O.C.
Tel ：+886-2-660[redacted]
Email [redacted]@iii.org.tw

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

28

輔導廠商過程(2/4)

2. 業者於隔天致電了解情況，本團隊也寄出說明文件

[redacted] Huang [redacted]@iii.org.tw> 1月25日

寄給 [redacted]

Dear Sir,

您好：敝公司在使用貴公司之[redacted]時遇到資安相關的議題，敝公司的目的在促進台灣資通產業的發展，同時資安也是重視的一環，希望能夠修正各家廠商的資安風險提升台灣產商的資安能量的口碑。
經敝公司內部流程需通報CVE。此部分是待廠商修正漏洞之後才會公告。
故因此貴公司之[redacted]修正此漏洞之後請麻煩務必公告或mail告知，在此表示感謝。
本次測試是參照 3GPP TR33.820 、TS33.320、 TS33.216 以及通傳會之建置基站資安檢測環境計畫所建議之步驟測試完成。

W [redacted]基站漏洞POC...

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

29

輔導廠商過程(3/4)

3. 業者主管代表率隊與本團隊開會討論解決事宜

【會議通知】資安議題討論

[redacted]Huang <[redacted]@iii.org.tw> 1月29日 (11 天前)

寄給 [redacted]

Dear Sir,

邀請各位先進蒞臨本所討論資安相關議題，懇請不吝賜教。

財團法人資訊工業策進會資安科技研究所

【開會通知】

一、時　間：107年02月01日（星期四）上午09點30分

二、地　點：民生科服資安所[redacted]

靜候各位先進的大駕光臨，感激不盡。

[redacted] 敬上

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

30

輔導廠商過程(4/4)

4. 該業者後續回覆-107年2月6日業者提供新版韌體測試：

莊[redacted]
寄給 [redacted]

Dear 黃Sir,

針對貴所於1/24通報[redacted]客服信箱提醒本公司產品有資安方面問題，經1/25一早相關部門接獲通報後緊急的處理過程及後續如下：

1. 1/25 立即連絡貴所，取得更詳細的資訊。
2. 1/25 召集相關同仁討論後續處理對策，並通報高階主管。
3. 1/25 針對貴所提供資訊，與廠商討論修正內容如下：
   I. 修正密碼強度
   II. 增加密碼retry機制
   III. 加強root密碼保護
   IV. 2/2前完成系統修正並進行韌體更新
4. 2/[redacted]至貴所拜訪及請教。
5. 2/2 開始韌體更新
6. 2/6[redacted]提供新版韌體設備供貴所測試

以上資訊供您參考，謝謝，

Best regards,
莊[redacted]Chuang
[redacted]
[redacted]
M：09[redacted]
T：02-[redacted]
E：[redacted]

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

31

計畫主要成就及成果(重大突破)之價值、貢獻度

四、其他效益(科技政策管理及其他)

績效指標類別	績效指標項目	105年度		達成說明
		原訂目標值	實際達成值	
K.規範/標準或政策/法規草案制訂	參與制訂之政策或法規草案件數	1	1	研究報告第七章行動寬頻基站資安檢測規範草案
Y.資訊平台與資料庫	新建資訊平台或資料庫數	1	1	研究報告第五章第四節建置基站弱點資料庫
	更新或新增資料庫資料筆數	0	1,971	

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

32

其他效益(科技政策管理及其他)

K.規範/標準或政策/法規草案制訂

參與制訂之政策或法規草案件數1件

-研究報告第七章行動寬頻基站資安檢測規範草案

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

33

行動寬頻基站資安檢測規範草案

- 本計畫已參考國際規範3GPP TS33.216、TS33.117、TS33.320及TR33.820及計畫團隊實測結果，歸納出六大類及41項之檢測規範草案建議，期能供國內電信業者及設備商參考，作為基站安全之指引文件。

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

34

基站資安檢測結果

- 3GPP測試項目之要求，係從產品研發、設計、測試等階段角度來規劃， 許多測試項目對已在商轉環境下的基站並無提供相關介面功能，因而**不適用**。
- 少部分測試結果為**不通過**，並非CVE漏洞，經評估，這些項目可於後續商轉環境部署下，再做設定，或從系統層面角度調整，結合其他資安設備來達到阻隔與防護，而非以單一終端設備之觀點評估。

	N品牌			E品牌			H品牌		
安全構面	通過	不通過	不適用	通過	不通過	不適用	通過	不通過	不適用
1. 資料保護	2	1	1	1		3	2	1	1
2. 應用程式安全		1				1		1	
3. 通訊安全	10			8	2		10		
4. 身分鑑別與授權安全	9	3	2	3	3	8	11	2	1
5. 作業系統安全	6		3	6		3	5	1	3
6. 實體防護			3			3			3
總計	27	5	9	18	5	18	28	5	8

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

35

HeNB資安檢測結果

- HeNB資安檢測結果

	商用家用基站	商用家用基站(更新版)
不通過	13	8

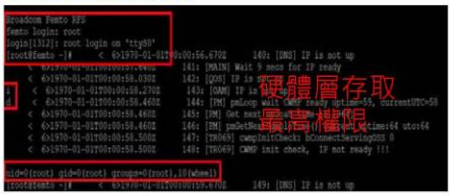
➢ 在檢測中，發現4項重大漏洞，已輔導業者進行修正，並提報國際漏洞資料庫

CVE編號	CVSS score (評分從0到10分，10代表最高風險)
CVE-2018-9112	9.8
CVE-2018-6312	9.0
CVE-2018-6311	7.2
CVE-2018-9111	5.4

- CVE-2018-9112

- CVE-2018-6312

- CVE-2018-6311



- CVE-2018-9111

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

36

其他效益(科技政策管理及其他)

Y.資訊平台與資料庫

研究報告第五章第四節建置基站弱點資料庫

-新建資訊平台或資料庫數: 1

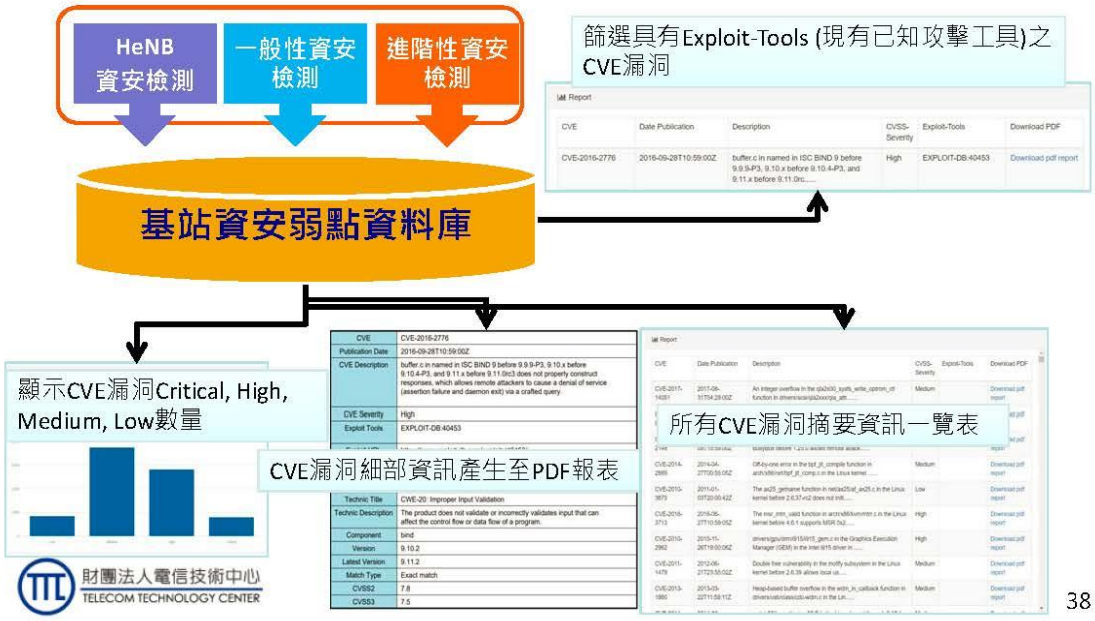
-更新或新增資料庫資料筆數: 1,971

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

37

建置基站資安弱點資料庫

- 共蒐集**1,971**筆CVE已知漏洞，蒐集來源為基站韌體檔案分析之結果。



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

38

簡報大綱

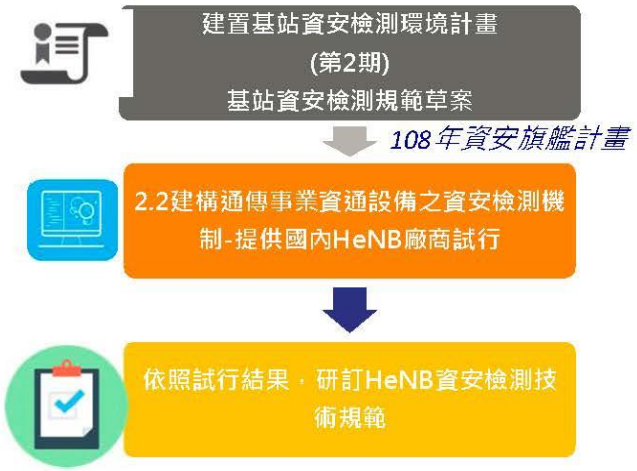
- 計畫實際執行與原計畫目標符合程度說明
- 委託計畫經費與人力運用之妥適度
- 計畫主要成就及成果(重大突破)之價值、貢獻度
- 後續工作構想及重點

財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

39

輔導HeNB廠商落實設備資安

- 建議將HeNB之資安檢測納入旗艦計畫 2.2建構通傳事業資通設備之安檢測機制，以輔導廠商進行資安檢測為目標，期能帶動我國HeNB設備安全水準，並使平臺產生最大化之可利用價值及邊際效益。
- 協助NCC推動基站資安檢測標準，提供後續推動時所需之支援與協助。

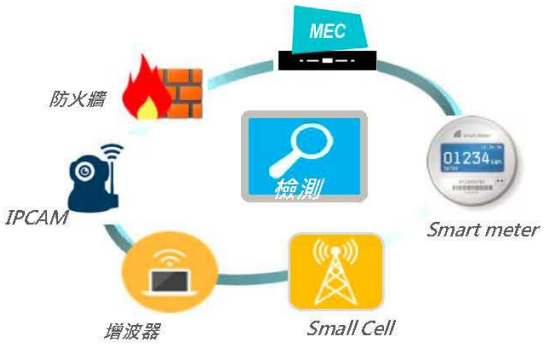


財團法人電信技術中心 TELECOM TECHNOLOGY CENTER

40

延續至其他行動連網設備資通安全檢測

- 本計畫之檢測平臺及工具，可在適當的調整平臺參數後，應用至其他連網設備資通安全檢測。
- 本計畫團隊已有實測驗證本計畫之檢測平臺可擴展應用於其他設備之檢測，如IPCAM、Small Cell、MEC Gateway、Smart meter (瓦斯表)+NB-IoT等。

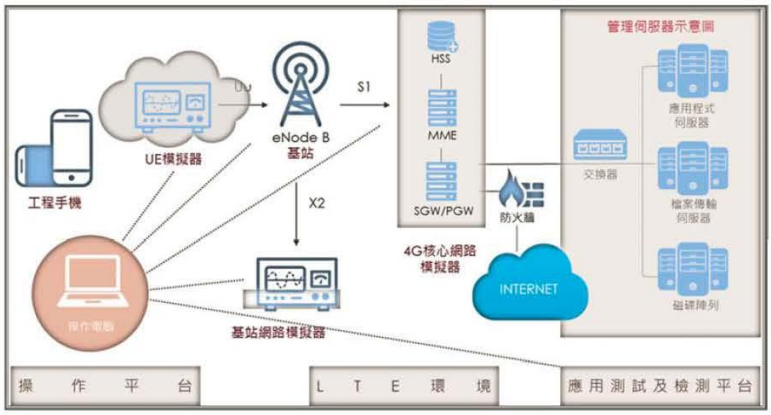


財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

41

延伸為4G網路安全檢測平臺之電信網路開放場域

- 規劃將基站資安檢測平臺與場域各模組化元件，建構延伸為4G網路安全檢測平臺之電信網路開放場域。
- 提供國產設備試驗及其相應之系統資安或效能證之試驗場域外，也能為未來5G及國家資訊安全人才的培育，提供一個理論與實務並重的研究場域。



財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

4G網路安全檢測平台-硬體設備架構圖

42

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

43

(二) 期末報告第 2 次審查意見回覆

「建置基站資安檢測環境計畫(第 2 期)」委託研究案
期末報告第 2 次審查意見回覆

審查意見	意見回覆
一、期末報告審查意見回覆第十八項，並無對應到審查意見之後續推廣措施建議，建議第九章第二節標題修正為後續建議事項，且對應內容頁數應為 P.753~P.757，並說明新增之內容。	已依委員意見修改第九章第二節標題為後續建議事項，並於第 1 次審查意見回覆內容補充說明新增之內容。
二、請補充說明期末報告下冊 P.694-P.695 基站資安檢測規範草案檢測項目參考國際標準來源之完整性，如 3GPP TS33.117 的項目編號某些沒有被採用之原因。	本計畫之基站資安檢測規範草案主要參考 3GPP TS33.216，該標準之測試案例除在基站基本安全需求有明確定義外，其他測試案例皆依循 3GPP TS33.117 之標準，故本檢測規範草案測試項目係基於 3GPP TS33.117 作為研究基礎，並對該標準之測試項目逐項評估與測試。本團隊於評估過程中發現，3GPP 標準規範許多測試項目為驗證產品設計階段應納入之安全考量，另外設備製造商也將許多安全配置包裝成產品專利之操作介面，以及設備版本等問題，非電信業者端或本計畫研究範圍內可掌握，因此本團隊視實際現況的可執行性與適用性，將最多可執行之安全測試項目納入草案範圍內，整理出本檢測規範草案之測試項目。依委員意見已將相關說明補充於 P.694 之段落中。
三、期末報告下冊 P.733~P.737 電信業者及設備製造商之座談會意見回應，尚未妥適(如: 認同該公司對於資安要求之努力或建議主管機關考量...等，應再修改)，可較具體說明研究團隊專業意見，供主管機關後續施政參考。	已依委員意見修訂座談會之意見回應，提出較具體之研究團隊專業意見，供主管機關參考，請參見期末報告下冊 P.733~P.737 表 8-1 及表 8-2。
四、請委託單位將期末審查第 1 次及第 2 次會議之審查意見回覆及簡報納入期末報告中。	已依委員意見將期末審查第 1 次及第 2 次會議之審查意見回覆及簡報納入期末報告，請參見期末報告附錄七。

1