出國報告（出國類別：其他）

建置行動寬頻基站資安檢測美國參訪出國報告

服務機關：國家通訊傳播委員會

姓名職稱：吳簡任技正銘仁、李技正福懿

派赴國家：美國

出國期間：105 年 1 月 24 日至 1 月 31 日

報告日期：105 年 4 月 29 日

摘要

為強化國內行動寬頻網路資安管理能力，蒐集國內外行動通信相關基站資安管理經驗及國際標準，研析適合我國環境之管理方針，以研議行動寬頻網路資訊安全相關規範及未來發展政策。透過參訪先進國家的經驗，了解其電信主管機關、檢測實驗室、研究中心等行動寬頻資安檢測標準發展。

透過參訪了解目前美國政府機關與電信業者的互動關係，蒐集研析先進國家之行動寬頻基站資安及相關檢測技術現況，並就法規上或是在共同協防上的流程、國外政府針對電信設備或是基礎設施相關資安問題的處置方式及後續規範的制定進行探討，作為我國未來建置基站資安檢測環境的參考。

目 錄

壹、 目的

目前的電信技術大多由歐美國家所引領，許多先進的規格也都在國外發表。因此出國參訪至美國地區，了解其電信主管機關、檢測實驗室、研究中心等行動寬頻資安檢測標準發展，並蒐集相關資訊。

透過參訪了解國外政府機關與電信業者的互動關係，探討法規上或是在共同協防上的流程，及國外政府針對電信設備或是基礎設施相關資安問題的處置方式，以及後續規範的制定等議題，作為我國規劃建置基站資安檢測環境的參考。

貳、 行程

行程如下：

■ 行程

日期	行程活動	地點	備註
105 年 1 月 24 日 105 年 1 月 25 日	台北-洛杉磯	洛杉磯	去程
105 年 1 月 26 日	洛杉磯-華盛頓	華盛頓	
105 年 1 月 27 日	美國國家標準局（NIST）	華盛頓	NIST 專家針對行動 APP、IOT 物聯網、虛擬化架構、認證、DOS 攻擊及軟體測試方法進行介紹及說明
105 年 1 月 28 日	美國國家標準局（NIST）	華盛頓	上午：LTE 安全討論，討論內容包含空中介面攻擊、IPSEC 傳輸網路加密、軟體弱點 下午：參訪 ITL LAB 及 Net-Zero House Tour 最後：NIST 風險管理方法總結
105 年 1 月 29 日	美國聯邦通信委員會（FCC）	華盛頓	LTE 安全標準與議題
105 年 1 月 30 日 105 年 1 月 31 日	華盛頓-台北	華盛頓	回程

■ **NIST 議題**

105 年 1 月 27 日		
Time	**Title**	**Speaker**
10 am	Welcome	Charles Romine Director, ITL, NIST
10:10 am	Insights on Security Research at NIST	Matthew Scholl Chief, CSD, ITL, NIST
10:30 am	Vetting the Security of Mobile Applications	Stephen Quirolgico, NIST
11:00 am	A Multilayer Overview of IoT Security Inefficiencies	Konstantin Kolias GMU
11:30 am	Security Recommendations for Deployment of Virtualized Infrastructures	Ramaswamy Chandramouli, NIST
12:00 pm	Lunch	
1:00 pm	Understanding Authentication	Kim Schaffer, NIST
1:30 pm	PIV Progress	Hildegard Ferraiolo, NIST David Cooper, NIST
2:00 pm	Secure Indirection Networks for Efficient DDoS Attack Mitigation	Konstantin Kolias, GMU
2:30 pm	Break	
3:00 pm	Minimizing Attack Graph Data Structures	Peter Mell, NIST
3:30 pm	Combinatorial Methods in Software Testing	Rick Kuhn, NIST
4:00 pm	Adjourn	

105 年 1 月 28 日		
Time	**Title**	**Speaker**
10 am	Discussion on LTE Security	Nelson Hastings, NIST Jeff Cichonski, NIST
12:00 pm	Lunch	
1:00 pm	Forensics Tour	Richard Ayers, NIST
2:30 pm	Net-Zero House Tour	David Yashar, NIST
3:30 pm	FISMA and the NIST Risk Management Framework	Ronald Ross, NIST Kelley Dempsey, NIST
4:00 pm	Adjourn	

■ **FCC 議題**

105 年 1 月 29 日		
Time	**Title**	**Speaker**
10:00am	Welcome	Ena Dekanic, Attorney Advisor/Asia Specialist Global Strategy and Negotiations Division
10:05am	Security Standards and Security Issues	Jeff Goldthorp, Associate Bureau Chief & Acting Chief, Cybersecurity and Communications Reliability Division Public Safety and Homeland Security Bureau (PSHB)
11:30am	5G—Mobile Broadband in mmW Bands	Michael Ha, Deputy Chief Policy & Rules Division Office of Engineering and Technology (OET)

參、 參訪單位

一、 美國國家標準局 NIST - ITL

美國國家標準局（NIST）在制定標準方面已有多年的經驗，在學界與產業界皆扮演著重要的基礎規格制定者角色。不管在安全或是新穎科技，所提出的建議都被相關領域研究者所重視。如 NIST 在 2009 年所撰寫有關於雲端產業的定義，就有多達 1,670 篇引用，可見其影響力於國際學術界有舉足輕重的地位。

本次參訪之資訊科技實驗室（Information Technology Laboratory，簡稱 ITL）其領域包含通訊科技、通訊測試、公眾安全通訊及無線與通訊頻率領域。資訊科技實驗室亦專精於先進網路、電腦安全、軟體與系統、統計工程學等項目，可以讓我們了解相關領域制定標準的流程與規範。ITL 極力在資訊測量科學上擴大規模，藉著與工業界、學術界和其他 NIST 實驗室合作，以推進科學與工程。ITL 研究人員已經制定了詳細的協議，並建立評估標準和測試數據庫的操作標準，而 ITL 制定指標、測試和工具，如資訊的複雜性、高可信賴軟體、時空協調的行動無線計算，及信息的質量、完整性和可用性的問題。對於未來要針對行動寬頻基站來制定資安檢測規範，可參考 NIST 以往的經驗，作為行動寬頻基站檢測規範訂定之參考。

二、 美國聯邦通訊委員會 (FCC)

FCC 是聯邦通信委員會（ Federal Communications Commission,簡稱 FCC）是美國獨立政府機構，直接對美國國會負責，於 1934 年由通訊法(COMMUNICATION ACT)建立，它負責常規的州際、國際通信，如：電視機，電線、衛星、電纜方面的工作，涉及美國 50 多個州、哥倫比亞以及美國所屬地區，為確保與生命財產有關的無線和有線通信產品的安全性，主要負責規定所有民間無線電頻譜使用，州際通信（包括固定電話網，衛星通信和有線通信）和所有從美國發起或在美國終結的國際通信。該委員會主導美國通信政策。

FCC 負責電磁相容方面的測試認證，FCC 對於工作頻率在 9KHZ 以上的電子產品所產生的電磁干擾均有管制。電子電器類產品銷往美國，需申請 FCC 認證，並標註由 FCC 認證。FCC 委員會調查和研究產品安全性的各個階段以找出解決問題的最好方法，同時 FCC 也包括無線電裝置、航空器的檢測等等。

肆、 參訪紀要及過程

一、美國國家標準局 NIST - ITL

ITL 實驗室安排 13 個議題，每日從早上 10 點開始到下午 4 點，由本會及財團法人電信技術中心（以下簡稱 TTC）、交通大學(以下簡稱 NCTU)與 ITL 實驗室電腦安全部門重點研究領域及成果共同進行交流，以下就相關探討議題摘錄如下：

(一) Insights on Security Research at NIST

由 ITL 實驗室電腦安全部門的主管 Matthew Scholl，為大家說明 NIST 在 Security 研究領域方面的歷史、 重要性，與其提供的各種服務。網路世代的崛起，各式各樣的線上服務與應用也如雨後春筍般地出現。在龐大商機的背後，其實也隱含各種潛在的攻擊與威脅，而威脅的範圍極大，一般美國企業相信每年因私有資訊被竊所造成的損失，從十億上看到幾兆。故為了因應這樣的威脅與損失，ITL 被賦予的主要任務包括：

- Applied and Computational Mathematics
- Advanced Network Technologies
- Computer Security
- Information Access
- Software and Systems
- Statistical Engineering

以 NIST 的角度，主要的研究著重於：

- 制定標準、準則、工具與量測方法，由 Computer Security 部門主責。
- 提供各院校與組織相關的電腦安全教育，以提高電腦或網路使用者的警覺性，由 National Initiative for Cybersecurity Education 小組負責。
- 提供各種身分（識別碼）的管理系統，由 National Strategy for Trusted Identities in Cyperspace 小組負責。
- 依據所制定的各種標準，規劃全國電腦安全的發展藍圖，由 National Cybersecurity Center of Excellence 小組負責。
- 改善電腦安全的基礎建設，以提昇美國關鍵基礎建設的安全與回復。關鍵基礎建設包含電力系統、水利系統、交通系統等，當這類系統的電腦控制系統受到攻擊時，將嚴重影響人民生活與企業運作，所造成的損失難以估計。因此，為防範未然，NIST 專責制定相關標準，並協助處理相關問題。

Matthew 也提出 Computer Security 部門目前的研究範例，包括風險管理、系統配置相關的準則、安全管理的自動化、弱點管理、虛擬機與雲端運算、大型金鑰管理框架與管理系統、下世代的密碼學（新密碼演算法、輕量、量子化加密等等），行動安全（包括行動 App 的測試準則、行動 App 的軟體品質需求、行動裝置的信任）、網路安全、軟體品管與使用性、識別碼管理系統等等。Matthew 強調，制定標準或開發安全工具時，除了傳統的安全與隱私等考量因素，回復能力也相當重要。此外，還必須要考慮到不同世代的文化變化與差異，才能提供較完善的法則與估測方式。

(二) Vetting the Security of Mobile Applications

這場演講由 Computer Security 部門的 Stephen Quirolgico 介紹如何檢測行動 App 的安全性。Stephen 先介紹 DARPA 的 TransApps，一套應用於軍事上的行動安全的 Android 應用程式。TransApps 以戰爭為場域，解決士兵使用行動應用時的不安全設定（配置）等問題，例如因不當設定造成敏感性資料被未授權存取、未經授權的網路通訊等等。TransApps 於 2010 年開始啟動，一年半後，正式應用於阿富汗戰場，使用者約有 3000 多人。透過一個彈性的框架，TransApps 希望能廣納各方提供的服務與應用，提供地理環境的分析、文化分析等服務。重點是，這些服務都必須要運行於一個安全的環境。為了提供此安全環境，NIST 也與美國國防部合作，以用戶應用場域為基礎，利用功能性回歸測試和定量性能測試，協助進行 TransApps 的安全性評估。為此，在測試行動 App 方面，NIST 也制定出標準測試流程，並開發出 AppVet 系統（開源套件，可於 github 上取得），以檢測行動 App 的漏洞與安全問題。Stephen 並以 DARPA 的 TransApps 為例，說明 AppVet 的應用情形，如下圖所示。

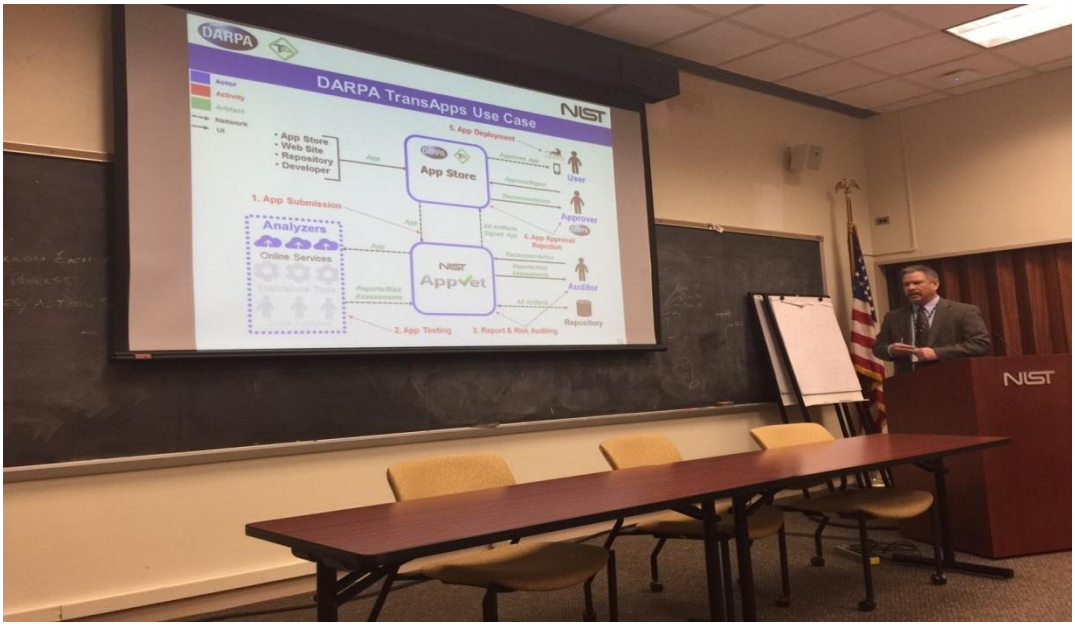


圖 1 ： Stephen Quirolgico 以 DARPA TransApps 為例，說明 AppVet 的運作流程

(三) A Multilayer Overview of IoT Security Inefficiencies

主講人 Constantinos Kolias 為 George Mason University 資訊部門的教授，開始講述 Internet of Thing（IoT）的安全。IoT 是一種新型的網路通訊架構，主要的概念是透過機器與機器間的互動，來達到生活便利、資料搜集、功能控制的作用。IoT 早在 1999 年就有被 Kevin Ashton 所提出，IoT 也可以透過機器間的通訊來達到自我設定的目地。相對於現有的網路架構，使用者就不會再是這種網路架構的中心，一切以資料和機器為主。這樣子的網路架構在於能夠大量的搜集環境的情況，以及自動的回應現有的環境。因為全部的通訊都是機器自動去處理，當預設的事件發生時，也能夠快速地、自動地通知管理者。然而，IoT 這種網路環境，因為少了人的參與，可能會擴大被感染裝置攻擊的威脅。

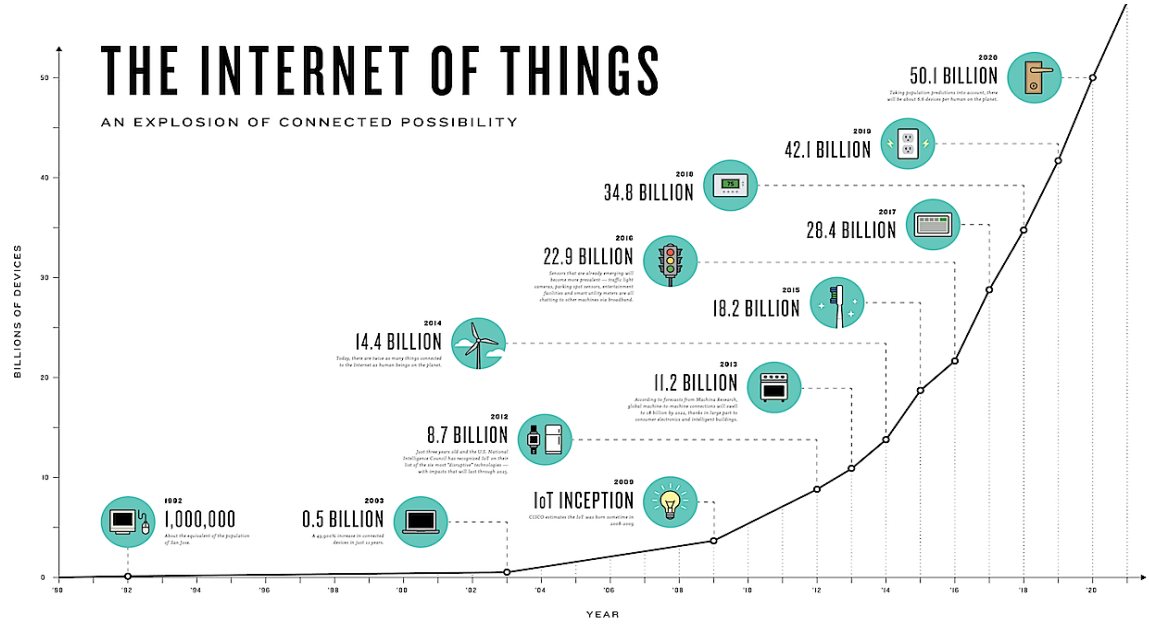


圖 2 ：IoT 裝置的預估，資料來源：Constantinos Kolias 教授所提供

在談到攻擊之前，IoT 現有的應用範疇非常廣泛，包含智慧家電、運輸、購物、工業、家庭照護等。智慧家電像是家庭的自動化、自動節能、或是家庭安全性。IoT 在運輸上現有的應用可以是道路安全、交通流量管制，在工業環境中，小裝置可以幫助品質控管、錯誤發生的預測、生產力改進。家庭照護像是病人狀態的監控、遠端治療、個人化的小裝置，都可以是利用 IoT 來實現。由於以上的應用，現有的 IoT 裝置有些許的安全疑慮，例如 90%的 IoT 裝置會搜集個人隱私資料，如何妥善的保護這些資料，會是一個重要的議題。除此之外，由於 IoT 裝置為了成本考量，通訊的演算法難以採用較安全的加密演算法。

著名的網路組織 OWASP 也針對 IoT 裝置可能遭遇到的安全弱點列舉下列十點：

- 不安全的網頁介面

- 不安全的雲端介面
- 無效率的認證/授權
- 無效率的行動介面
- 不安全的網路服務
- 不安全的網路配置
- 無傳輸層自動加密
- 不安全的軟體/韌體
- 隱私資料
- 無實體安全性

為了有系統的衡量 IoT 的安全性，Kolias 教授將 IoT 裝置劃分成幾個基本元件。這些基本元件能夠組合成各種 IoT 的應用環境，所以非常適合用來分析安全性。IoT 基本元件可分為：

- Sensor: 負責搜集資料
- Snapshot: 一個固定時間所有裝置的狀態
- Cluster: 一群 Sensor
- Aggregator: 將 Sensor 的資料轉成資訊
- Weight: 加權 Sensor 的資料權重
- Communication Channel: 被搜集的資料如何被傳遞
- External Utility: 將資料傳輸到此網路
- Decision Trigger: 創造結果

一個利用 IoT 控制燈泡的家電環境可以藉由著 iBeacon 的方式來控制燈泡如圖 3。

Model Element	Realization
Sensor	Beacon based proximity sensor
Snapshot	Every few (e.g. 5) seconds (depending on the room)
Cluster	1 proximity sensor per room (more if the room is too big)
Aggregator	Determine presence and location of a specific user
Weight	Static

Communication Channel	BLE between tag and sensor, ZigBee between gateway and lights, WiFi between smartphone and gateway
Ext. Utility	Cloud application for lights
Decision	Turn on lights to preferred color. Turn off lights.

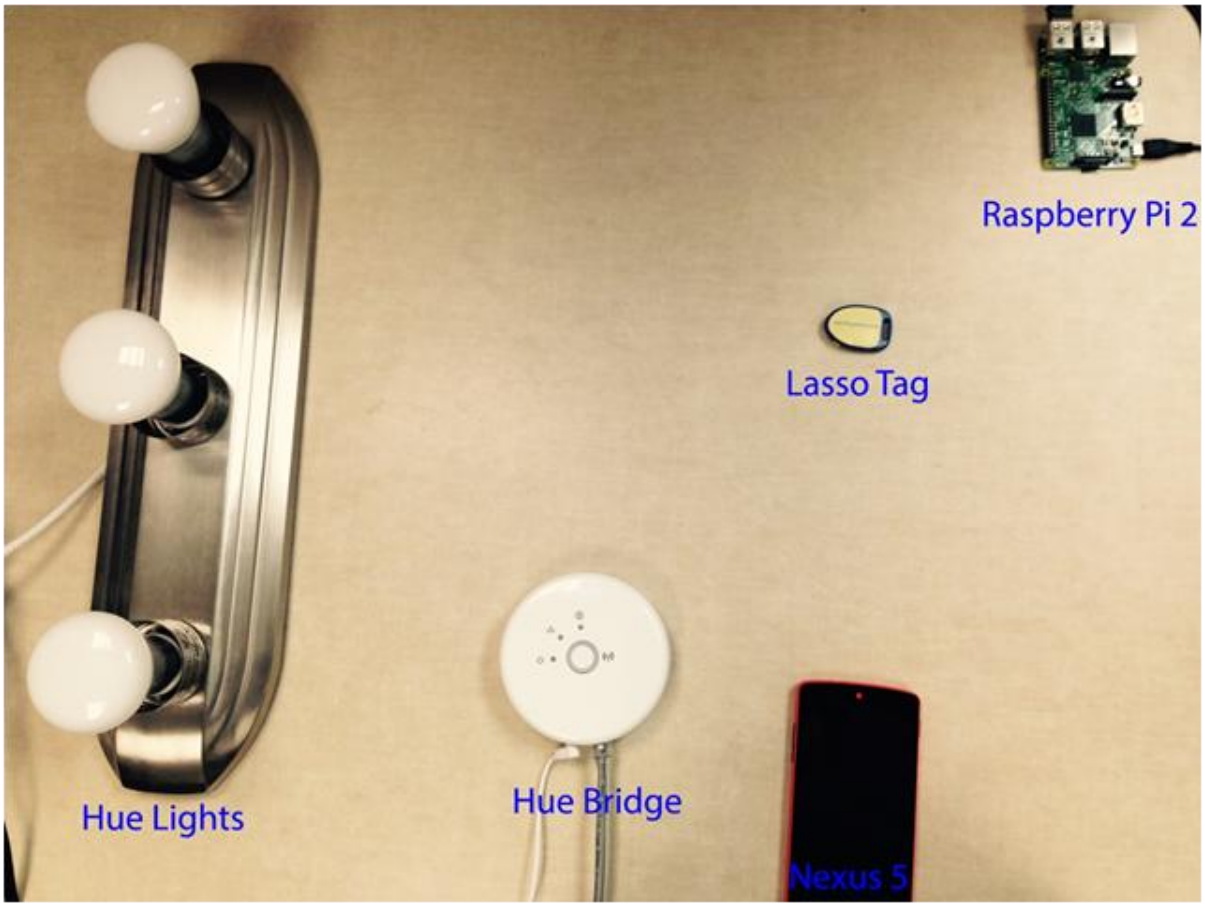


圖 3： IoT 環境的實際範例與功能對照圖，資料來源：Constantinos Kolias 教授所提供

iBeacon 是 Apple 提出的 IoT 通訊協定，Kolias 教授說明由於 iBeacon 的封包格式裡面有一種每個裝置都不一樣 UUID，一但設置了之後，以後的通訊都是固定的，這讓攻擊者可以追蹤該 IoT 的裝置。除了理論證明以外，Kolias 教授做了一個裝置來搜集 UUID，並且來追蹤目標。除了這個實驗之外，還有介紹數種 IoT 的環境以及威脅。最後提到 IoT 裝置網路的威脅，因為 IoT 裝置都需要連接網路，利用內部網路做傳輸，如果有惡意攻擊者用更強大的無線訊號迫使 IoT 裝置連上，則該偽裝的無線存取點可以破壞此 IoT 環境的可用性，造成 DoS 攻擊。或是因為 IoT 裝置間因為缺乏加密機制，讓攻擊者很容易得可以進行中間人攻擊，來竊取或是竄改資料。最後，Kolias 教授提出了幾個看法以及防禦措施。主要告訴我們近年 IoT 裝置的安全性還是很薄弱。

(四) Security Recommendations for Deployment of Virtualized Infrastructures

由 Dr. R. Chandramouli，簡稱 Mouli 來為我們介紹虛擬化基礎建設的佈建。一剛開始介紹什麼是虛擬機器，或是 Hypervisor。一個虛擬機器，virtual machine 可以簡稱 VM，能夠保護外部的環境，隔離內部的應用程式。現在大多用在網頁服務。因為網頁伺服器可能會因為軟體的漏洞，讓攻擊者取得網頁伺服器的系統權限，如果可以將整個網頁伺服器的軟體隔離在虛擬機器裡面，則可以提供比較好的保護。而已虛擬機器的架構來看，內部被隔離的環境稱之為 Guest System，外部的環境稱之為 Host System（或是 Hypervisors）。目前除了虛擬一台電腦一外，還有針對一個網路環境做虛擬，可以有單一網路，或是虛擬交換機。更進階的是可以有防火牆的功能。

虛擬機器的主要功能是提供

- Execution Isolation for VMs: 針對每一個虛擬環境做隔絕。
- Devices Emulation & Access Control: 提供裝置模擬以及 Guest 對該裝置的存取控制。
- Execution of Privileged operations by Hypervisor for Guest VMs: 幫 Guest System 執行具有系統權限的指令。
- Management of VMs (also called VM Lifecycle Management): 虛擬機器的管理。
- Administration of Hypervisor Platform and Hypervisor Software: 提供 Hypervisor 管理。

Hypervisor 的種類其實還可以再略分兩種，一種是直接安裝在實體機器上，不透過作業系統來管理硬體。另外一種是需要安裝在作業系統上，透過作業系統來管理硬體裝置。而現有的硬體架構有針對虛擬化環境做強化，像是比 ring 0 在更高權限的 ring -1，透過 CPU Root & Non-Root Mode 來達成，或是提供硬體的 Page Table，針對記憶體的虛擬化。CPU 和記憶體是電腦系統中很重要的東西，如果這兩個元件的虛擬化可以透過硬體輔助的話，則可以大大加快速度。

在 Mouli 的研究中，他著重在 Hardware-assistance for virtualization，主要有幾個特性。第一，不用修改安裝在上面的作業系統。作業系統上的弱點以及安全設定都可以完全的得知，方便用來修補或是更新。第二，可以直接使用驅動程式，不需要加以修改。驅動程式因為各家廠商的裝置不一，所以驅動程式的支援是令人頭痛的問題。透過這種虛擬機器，可以完全的套用現有的驅動程式，得到完整的更新支援。第三，處理器因為支援兩種模式 Root Mode 和 Non-Root Mode，可以有效的防止被惡意代碼攻擊。第四，因為有硬體的分頁表（page table），所以有更好的記憶體保護。最後，這種虛擬機器因為需要重新調整 DMA 操作，所以可以抵擋 VM Escape attacks，因為 DMA 操作的能力可以被侷限住。

因為要建立虛擬環境的基礎建設，所以在這邊需要討論系統設置的特色。最先遇到的是連接的管理介面，主要是探討每個虛擬環境中的網路介面，還有如何將特定的服務導至正確的目標，像是 SSH, DNS, DHCP 等，最後還需要限制哪些 IP 是不能存取的，用來虛擬沒有連線的情況。裝置驅動軟體的選擇也是一個挑戰，為了讓虛擬機器可以有數種的硬體資源，在建立一個虛擬機器映像檔時，需要指定可以接受的硬體資源。為了有效的利用虛擬機器的資源，分配驅動軟體時，應該考慮安裝最合身的軟體，例如像是最原始的作業系統、認證過後的驅動程式、裝置共有的程式碼等。最後，硬體資源分配是指如何動態地調整虛擬環境的資源。要注意不能讓單一個虛擬環境佔據了所有的硬體資源，否則會造成阻斷式攻擊。再來是要注意讓每個虛擬環境「公平」的分配處理器的資源，或是遵守一個可調整的比例分配。

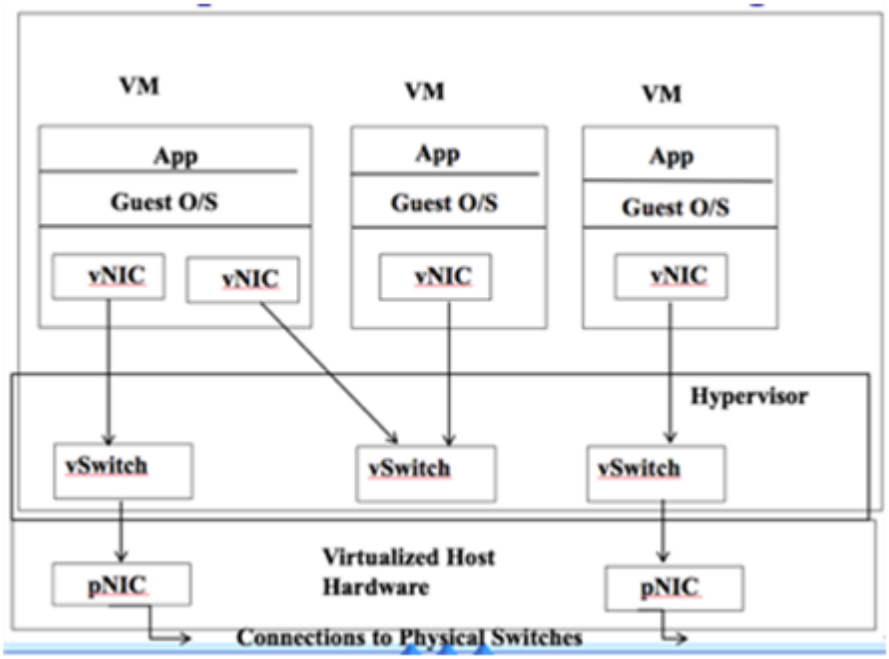


圖 4：虛擬機器以及網路環境示意圖，資料來源：Mouli 所提供

在管理每個 VM 運行時的狀態，也會有相對應設置的考量，創建一個虛擬的映像檔以及映像檔案的管理，對於大量的基礎建設的虛擬平台是一個繁複的工作。為了避免映像檔案損毀或是遭受到惡意的修改，對於虛擬映像檔的完整性驗證是一個必要的工作。而虛擬映像檔案的命名也是很重要，由於現在的軟體更新十分迅速方便，在命名時，需要明確的指出作業系統的版本，更新代號等等。安裝時，需要遵守兩大原則來確保安全性。第一個原則是保持更新，使用最新版本的軟體，因為現在的資安攻擊可以在漏洞公布後，很快的產生攻擊程式碼，這也是所謂的 Zero-day 攻擊，使得作業系統需要常常的更新。如果在大量的虛擬環境基礎建設中，沒有保持作業系統的更新，可能會造成大量的系統被攻擊，另一方面，儘可能安裝主要的作業系統版本，讓群眾的力量來保持該作業系統的安全性。除此之外，為了避免不必要的軟體可能造成的漏

洞，選配軟體時應該以最小原則（Minimality principle）來挑選，如果必要的話，虛擬環境內部裡面仍需要安裝防毒軟體，防堵已知的病毒攻擊。

網路的連結是基礎設施的一大重點，在虛擬環境中可以分做虛擬網卡（vNIC）、虛擬交換機（vSwitch）兩大種類。第一個是用來實作虛擬裝置間的通訊，第二個是用來建立區域網路。虛擬網路架構的設定是非常困難的，原因在於為了支援動態的調整，如何有彈性的設計虛擬環境的網路分佈是一個很重要的議題。但是因為時間的關係，最後 Mouli 很快速的瀏覽了一遍區域網路的設置。

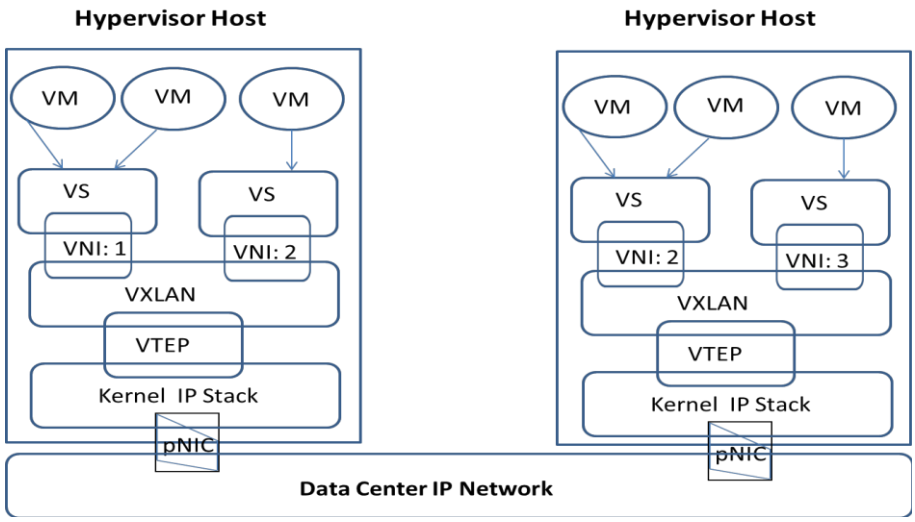


圖 5：虛擬網路架構圖，資料來源：Mouli 所提供

(五) Describing Authentication

由 Kim Schaffer 討論身份認證的議題。 身份認證主要由三個步驟所組成：識別（Identify），認證（Authenticate），授權（Authorize）。識別的內容是在於區分來做認證不同的個體，像是區分兩個人，兩台機器，或是兩種生物。識別的技術可以由名稱、圖像、區域等資訊來劃分。認證是核對該識別出來的個體，來判斷是否為系統已知的對象。這邊需要有雙方彼此才知道的資訊，或是一個交換過的資訊。最後是授權，也是身份認證的最主要目的，將適當的權力給予該認證過後的個體，授權的內容可以是存取能力、對物體操作、對其他個體的互動等。

舉例來說，一個門禁系統要用攝影機來認證進入的訪客，第一個工作就是要先有能力識別一個訪客，並且從該訪客取得資訊。可能的方法是利用臉部辨識的技術，來對進入的訪客做識別。再來是認證，這邊除了比對系統內已有的人臉資訊以外，還可以有多重因素（Multi-factors）認證的概念，也就是說，輸入的認證資訊可以是很多種的。例如比對完人臉之後，打開輸入密碼的小鍵盤，輸入正確之後才能真正的開啟那一道門。這邊採用了人臉和記憶密碼來當作認證的資訊。最後是授權，認證成功之後，會得知認證對象應該有的權力，如果這個使用者認證成功，卻沒有授權進入這道門，則門還是不會打開。

認證的方式有許多種，像是密碼認證、生物識別認證。而認證的過程可以是人對機器認證或是機器間的認證。機器間的認證比較簡單，都是數位化的關係，大部分都是以金鑰的方式來做認證。而人與機器認證的方式比較多樣，主要可以分做 Something you know（密碼）、Something you have（裝置）、Something you are（生物資訊識別）。還有比較進階的認證方式，像是連續性的認證過程，像是行為上生物資訊，像是敲鍵行為、滑鼠使用特徵、步態認證、手寫簽章、語調分析等。更新穎的研究還有利用認知生物識別 cognitive biometrics 來進行認證，像是每個人生理無意識的反應，像是腦波 electroencephalogram (EEG), 心電圖 electrocardiogram (ECG), 神經刺激反應 electrodermal response (EDR), 血壓 blood pulse volume (BVP)等等。許多資訊都可以用來區分個體，而如果特定集合的特徵足夠獨特，則可以用來做認證。

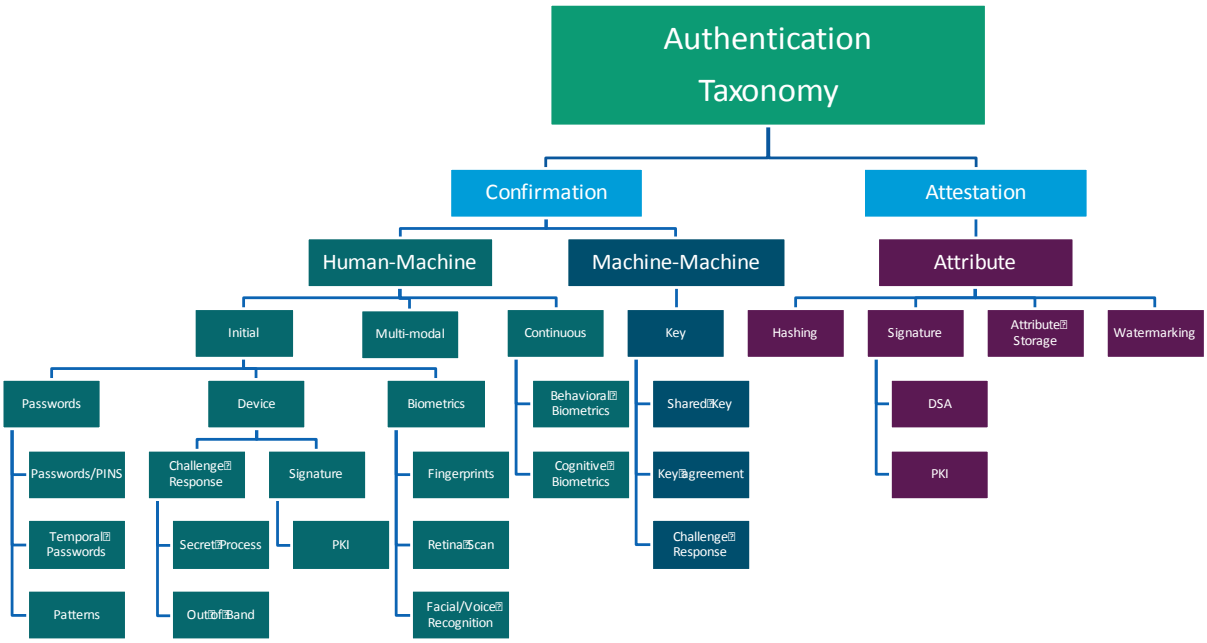


圖 6：身份認證種類以及內容，資料來源：Kim Schaffer 所提供

認證在生活上已經非常頻繁，而且許多認證機制已經被自動化，讓使用者察覺不到。舉例來說，一個使用者在一個有 HTTPS 保護的網站上購物，中間的過程包含了三種認證。第一個是網站與使用者裝置間的 TLS 連線，TLS 需要憑證來驗證對方的身份，雖然目前 HTTPS 只有單方認證，並不會認證使用者身份，但是現有的瀏覽器一旦無法驗證連線網站的身份，都會警告使用者該網站的身份可疑。第二個認證是該網站對此使用者的認證，目前一般的網站都僅用密碼來當作認證的方式，使用者輸入之前在該網站設定的密碼後，讓網站比對是否相同。確定使用者身份之後，才能夠確保購物的清單屬於該連線用戶。最後是信用卡的驗證，利用信用卡上的資訊來作身份的確認，包含信用卡號碼，背後的三碼安全碼，有效日期等。

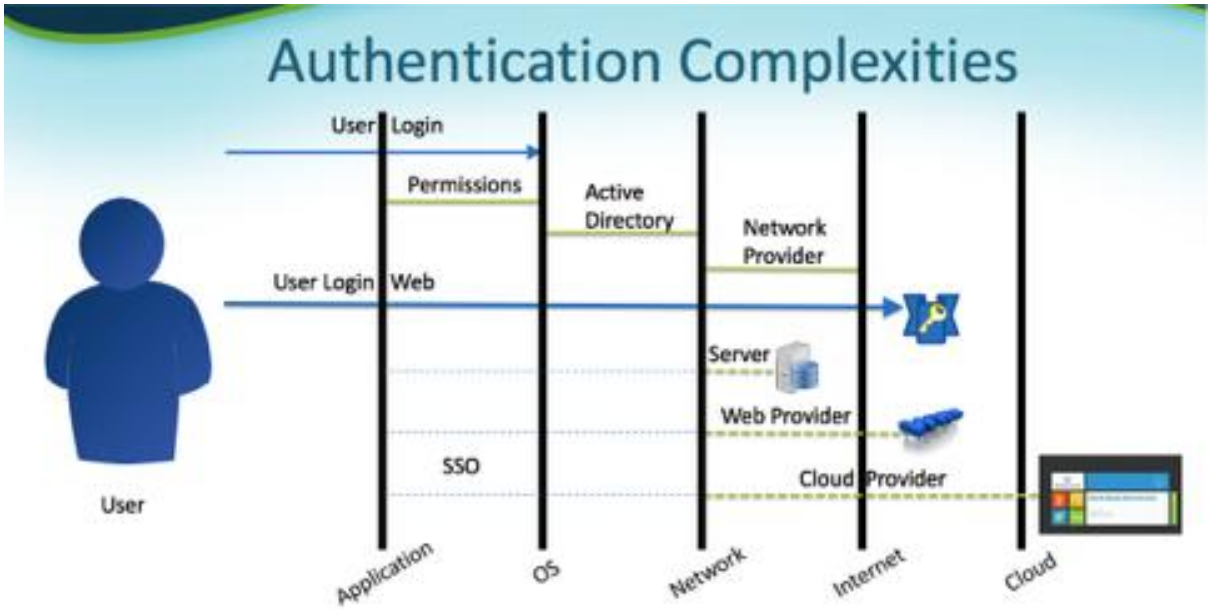


圖 7：網路交易所參與的身份認證流程說明，資料來源：Kim Schaffer 所提供

身份認證理所當然是越複雜越多樣所能提供的安全性越高。然而，在實際的使用情況中，太過繁複的身份認證方式會引起使用者反感。在實作一個系統的認證機制時，需要衡量身份認證的強度以及合適度。認證強度在於該認證機制是否能夠被有效率的破解，像是密碼長度、字元複雜性、偽造的難易度等等。認證資訊的安全度在於這個資訊夠不夠獨特？足以區別出所有的使用者。這個資訊會不會改變？像是生物識別資訊可能會因時間的關係而有所變化。再來是這個資訊容不容易保護？會不會很容易取得或是複製？以上的考量因素會決定認證的強度。

後續需要考量的是合適度，對於一個比較沒有經濟價值的系統，採用過度複雜的認證機制，並不是一個好的選擇。考慮使用性來說，第一個是認證的有效性，探討該認證系統的準確度，對於生物識別的認證來說，往往認證的準確度無法像數位密碼般，能夠百分之一百的準確。第二個是效率問題，進行這個認證過程中會不會太過耗時或是繁雜，整體認證資訊的比對與取得會不會需要大量的儲存空間、計算能力、運算時間等等。第三個是體驗的滿足感，使用者會不會直覺性的接收、採用該認證方式。

Kim 在這邊提出了一種衡量的方法，來說明身份認證在不同角色間的考量點。從資料本身的角度、使用者的角度及整體組織的角度來看，徹底的解析身份認證需要考慮的因素。

(六) U.S eID Effort The Personal Identity Verification (PIV) Standard

Hildegard Ferraiolo 是 PIV 計劃的主持人，PIV 為人員識別驗證的縮寫，Hildegard 主要負責全美國公家機關識別證的維護。聯邦政府目前有五百萬張智慧晶片卡用來做人員識別，主要的用途是管制實體建築的人員進出，利用識別卡來管制電腦設備的使用數位資源，或是用來做跨部會機關認證的機制。通常跨部會都會需要有 Two-factor authentication 強度以上的認證機制。目前 PIV 的技術已經發展成熟，NIST 本身也撰寫了許多規範與準則來要求 PIV 的安全性。

除此之外，PIV 技術不僅用卡片來做識別，目前美國聯邦政府也有考慮用智慧型手機當作識別的一種來源。原因在於卡片通常需要一個讀卡機，而且卡片是一個額外的攜帶品，有鑒於智慧型手機是現有人類的必需品，PIV 系統結合智慧型手機是未來的趨勢。此標準定義在 NIST SP 800-157 中，主要是利用公開金鑰基礎設施（PKI）架構，遵循著 X.509 的信任關係，來建立 PIV 的身份認證訊息。而生成的機密資訊（Derived Credential）是一種用來證明身份的識別，或是用來確定該用戶擁有該 PIV 卡片。在智慧型手機上的 Derived PIV Credential 中，可以嵌入在行動裝置中的軟體、特殊的嵌入式硬體或是存放在一個儲存裝置中的記憶卡、USB 或 UICC。在考量利用智慧型手機當作 PIV 的認證裝置時，還需要考慮智慧型裝置上的變異性，例如製造商、作業系統版本、網路連線能力、螢幕大小、輸入裝置、支援的通訊協定等。

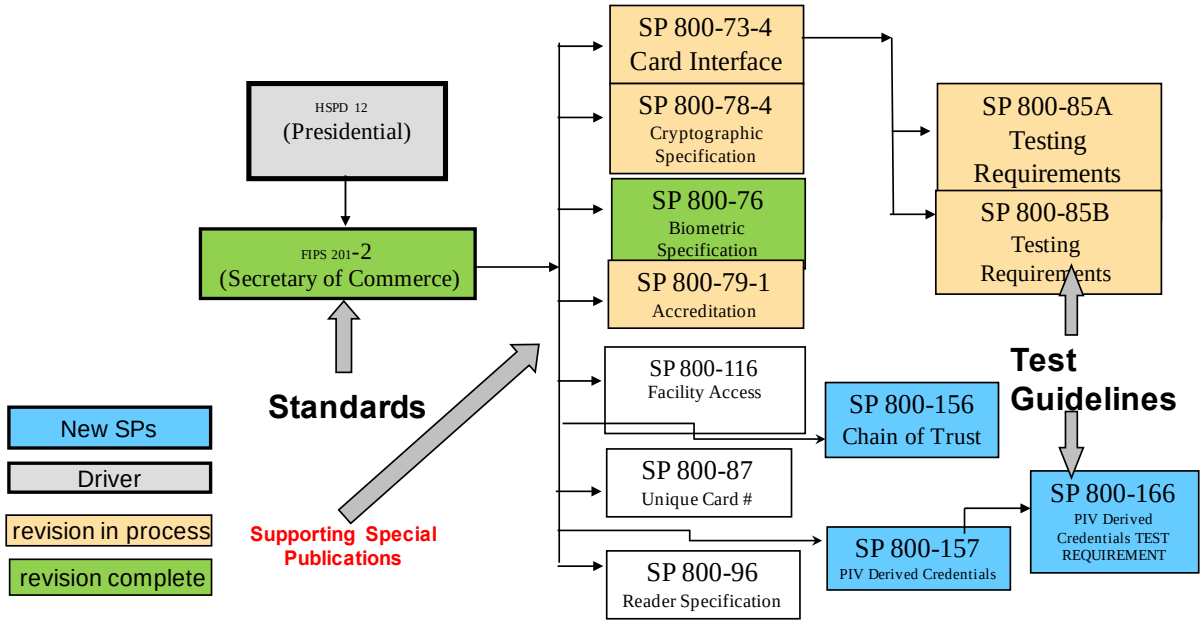


圖 8：與 PIV 相關之 NIST 標準，資料來源：Hildegard Ferraiolo 所提供

（七）Secure Indirection Networks for Efficient DDoS Attack Mitigation

由上午介紹 IoT 安全的 George Mason University 教授 Constantinos Kolias 主講。題目的內容是在說明如何降低 DDoS 攻擊所造成的影響。在報告的一開始首先介紹分散式阻斷式攻擊（Distributed Denial of Service, DDoS），DDoS 的定義是對特定的使用者，利用大量的且地區分散的機器來阻斷網路資源或是硬體資源。DDoS 仍然是現有網路上一個非常有效且嚴重的攻擊手法，可以造成銀行或交易網站實體金錢的損失，或是政府機關聲譽上的損失。

抵擋 DDoS 的方法主要有三種方式：過濾方式（Filtering-based approaches）、覆蓋網路架構式（Overlay-based defenses）、移動目標（Moving target defenses）。過濾方式的防護機制在於分析攻擊的流量，並且將可疑的流量丟棄，藉以避免目標被攻擊。但是這種方式需要網路設備的支援，才能有效的達到目標。第二種是利用 Overlay network 的特性來阻絕 DDoS 攻擊，Overlay network 因為路由的路徑不是固定，所以可以減緩及吸收分散式來源的攻擊流量。第三種是移動目標，此方式的做法是將被攻擊的目標移動到其他的網路環境中，讓使用者的服務不受到中斷。

DDoS 的攻擊手法日新月異，而且攻擊的強度越來越強。隨著全球計算裝置的成長，智慧型手機甚至也可以加入殭屍網路進行攻擊。如果僅靠著存取控制清單（Access Control List, ACLs）以不足夠分析各式各樣的 DDoS 攻擊流量。

Kolias 教授所提出的方法是一種建立在雲端環境的 DDoS 抵禦機制，主要可以用來抵擋網路層的 DDoS 以及運算層的 DDoS。他主要是利用第三種方法—移動目標，來達到抵禦 DDoS 的方式。他設計了一種 Shuffling 的程序，可以把攻擊者與一般使用者的流量分開，讓他們面對不同的伺服器。這樣一來，攻擊者既以為自己已經攻擊成功，而使用者仍能夠獲得網站的服務。該方法以用模擬法來驗證其有效性。

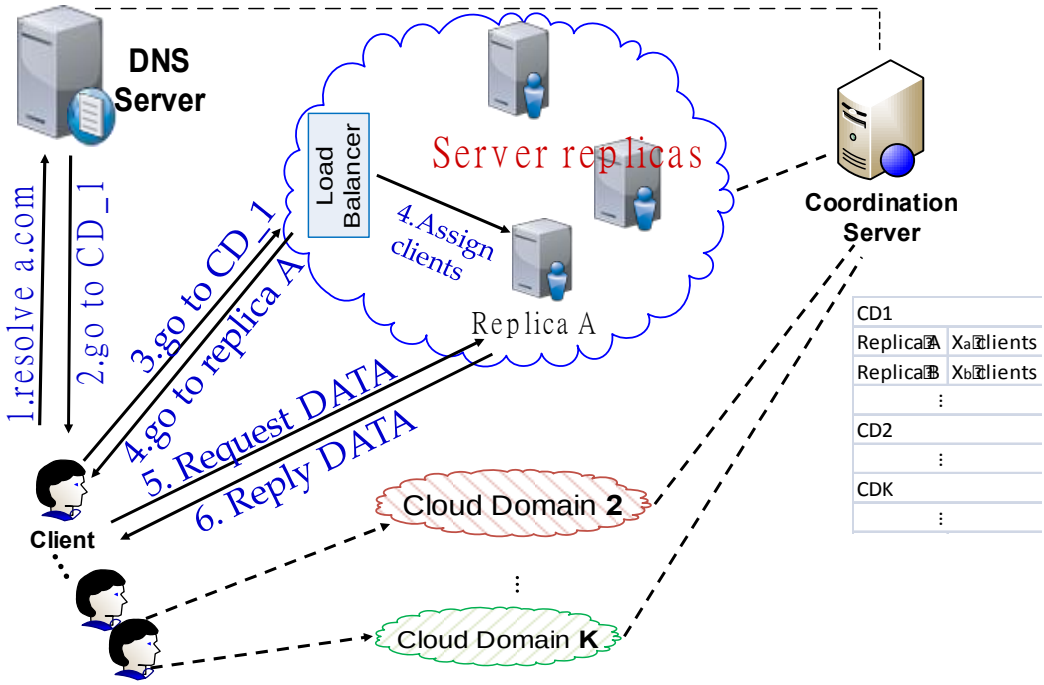


圖 9：由 Constantinos Kolias 所提出的 DDoS 防禦機制，資料來源：Constantinos Kolias 所提供

防禦系統主要架構可以分為附載平衡器（Load Balancer）、複本伺服器（Replica Servers）、協同伺服器（Coordination Server）。附載平衡器會將連線的客戶流量重新導到複本伺服器上。這邊重要的區別是 redirect 和 forward 不同，redirect 是告訴客戶需要轉往該連線目標，這樣一來可以有效地避免大量的偽造來源 IP 的請求。除此之外，也可以避免附載平衡器成為整個網路頻寬的瓶頸。複本伺服器是一群功能相同的伺服器。在平時沒有被受到攻擊的時候，複本伺服器不需要開啟太多，而當被受到攻擊的時候，備用的複本伺服器被啟動，用來接管部分原有的服務連線，接管的部分是利用 Shuffling 的演算法來將正常的使用者轉址到新的複本伺服器，最後是協同伺服器，它追蹤現有連接使用者與複本伺服器數量的關係，而且可以執行 Shuffling 演算法來舒緩 DDoS 攻擊。

Shuffling 演算法是由幾個參數所組成。在一個短暫的時間區間內，整個系統可以看作是有 N 個使用者，有 M 個是攻擊者，整個系統有 P 個複本伺服器。而演算法的目標是要去識別和救援多少好的使用者，讓這些好的使用者不會跟攻擊者座落在同一個伺服器。公式可以表達成如下：

$$E(S) = \sum_{i=1}^{P} p_i x_i = \frac{\sum_{i=1}^{P} \binom{N - x_i}{M} X_i}{\binom{N}{M}}$$

xi – Number of clients to be assigned to replica i,

pi – the probability that replica i is not assigned with any persistent bots.

N – Total number of clients

S – "Good" clients to be identified from this shuffle,

M – Number of persistent bots, P – Number of shuffling replicas

找到一個最佳解 <x_1, x_2,…, x_P> ，讓整體的好的使用者能夠不受到攻擊者的影響。為了要尋找最佳解，可以採用動態演算法跟貪婪演算法兩種來計算。

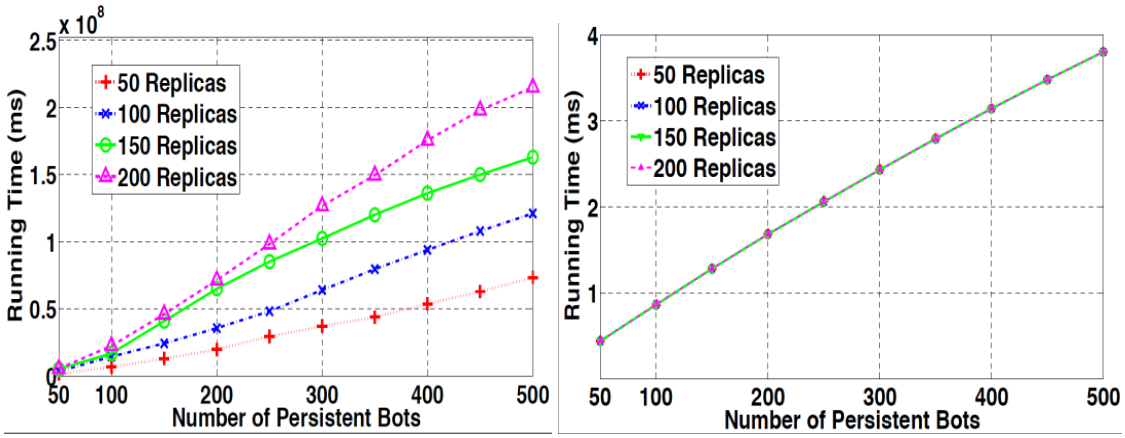


圖 10：利用不同的計算方式（DP v.s. Greedy）Shuffling 演算法實作之比較，資料來源：Constantinos Kolias

最後要去驗證實驗的有效性，可以採模擬驗證（Simulation-based Evaluation），雛型系統驗證（Prototype-based Evaluation）。模擬驗證是透過變更各種參數來發生大量規模的 DDoS 時，該系統能夠達到的效能。實際的開發的雛型系統是在一個小規模範圍內去驗證客戶在轉移或重新導向流量時，所造成的延遲。後者比較偏向系統實作，採用 Amazon Ec2 的平台來當作 Replica server 雲端平台。

（八）Minimizing Attack Graph Data Structure

Peter Mell 是 Computer Security Division 電腦科學家，介紹一篇發表在 The Tenth International Conference on Software Engineering Advances, 2015 年的論文，題目為該論文的標題。Attack graph 是一種用來表示攻擊者藉由著串連一堆攻擊行為來擴大威脅的影響性的圖形，分析該圖形可以讓資安人員能夠實作防禦的最佳化。但是 Attack graph 並不常見在一般商用的應用當中，原因是由於該圖形太過龐大，不容易人工分析，而且也圖形內的關係非常複雜，也不容易適合用電腦分析。現有的 Attack graph 的建立仍然太過龐大。

該篇論文就是為了要縮小此 attack graph 的大小，以降低分析的運算量。該研究利用弱點導向的方式來建立 attack graph。在用複雜度分析方法來比較現有不同的 attack graph 表示方法。結果表示 Peter 的研究不僅可以有最低的複雜度，而且也不會失去任何訊息。

為了建立 attack graph，一開始介紹變數使用（Variable Usage）方法，藉著表示最差情況 attack graph 可能的大小，該變數主要有三個

h = number of hosts in the network

v = maximum number of vulnerabilities on any host

c = maximum number of attacker privileges that can be achieved on a host through some set of vulnerabilities

而 h 應該是裡面最大的變數，因為他會隨著網路大小的成長而變大。

Disjunctive Normal Form (DNF) Interpretation of In-edges to a Node: 每個邊會有一個群組的標號，進入邊的群組事件發生時，則會產生出輸出邊的事件。這個分析技術會用在後來的 attack graph 之中。

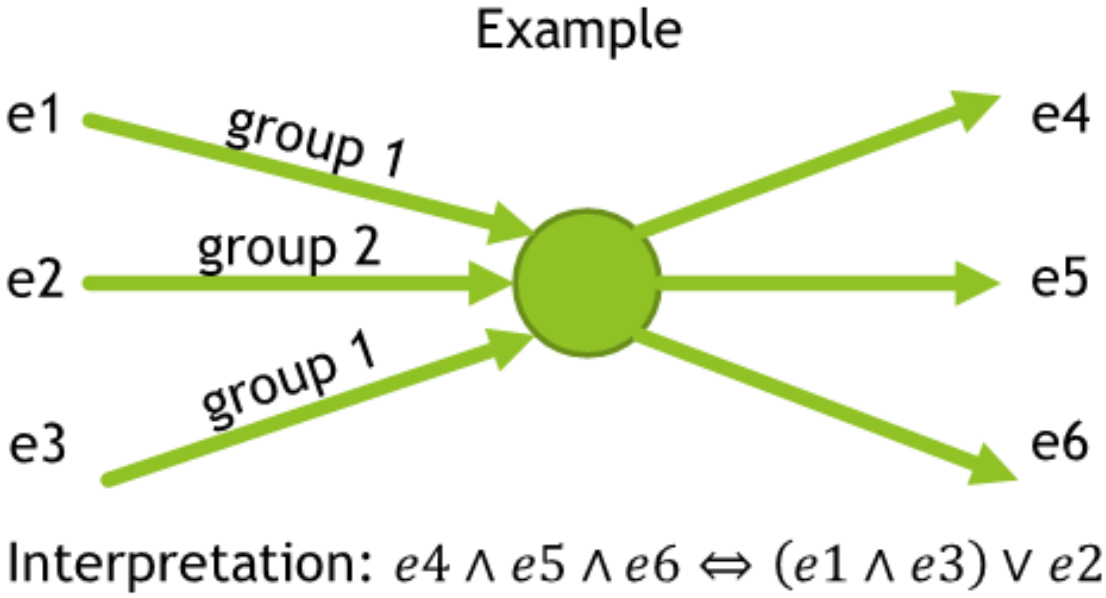


圖 11：DNF 示意圖，資料來源：Peter Mell

以下為各種方法介紹以及概況:

1. State Enumeration: 利用每個被攻擊的狀態來當作一個節點。每有一個邊代表有一個攻擊產生。每一層代表著不同的狀態，邊只會在相鄰的層做連接。而路徑的關係則代表著攻擊時不同的變化。最差圖的複雜性大小是 O(h!)

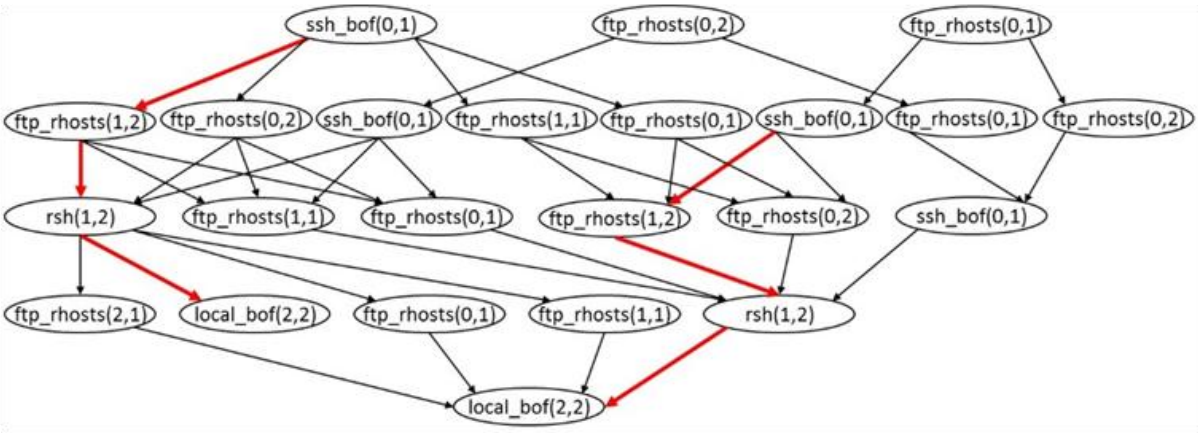


圖 12：State Enumeration 所建構的 attack graph 示意圖，資料來源：Peter Mell

2. Condition Oriented: 每個點代表攻擊成功後獲得的權限，邊是代表攻擊的名稱。利用 DNF 的解讀方式，來表示攻擊者可能的行為。最差圖的複雜性大小是 hc 的點和 (h^2)v(c^2)的邊。

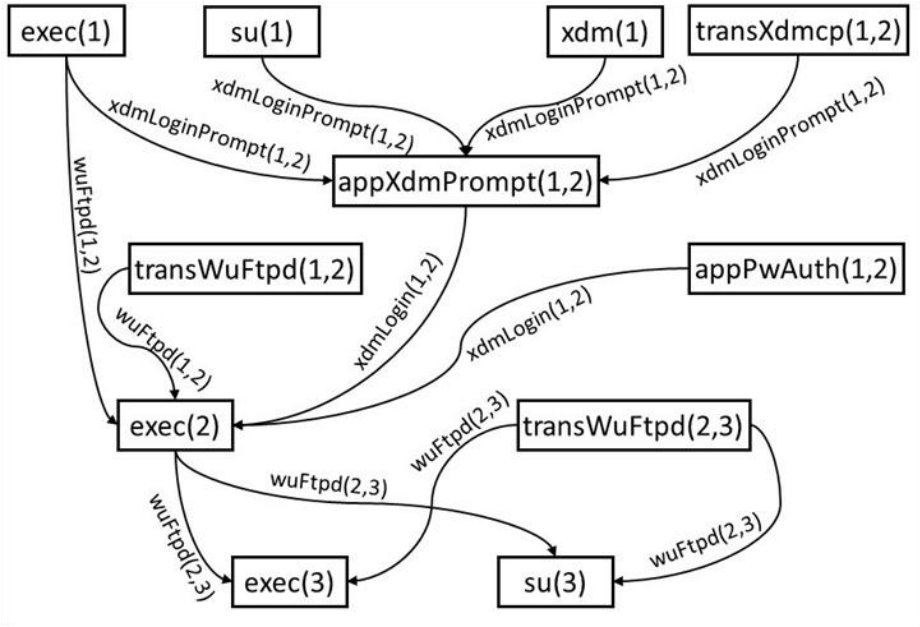


圖 13：Condition Oriented 所建構的 attack graph 示意圖，資料來源：Peter Mell

3. Exploit Oriented: 每個點代表著 exploit，並且會連接到初始點 initial condition。邊是攻擊者獲得權限的名稱。最差圖的複雜性大小是 h^2v 點和 h^3v^2c 邊

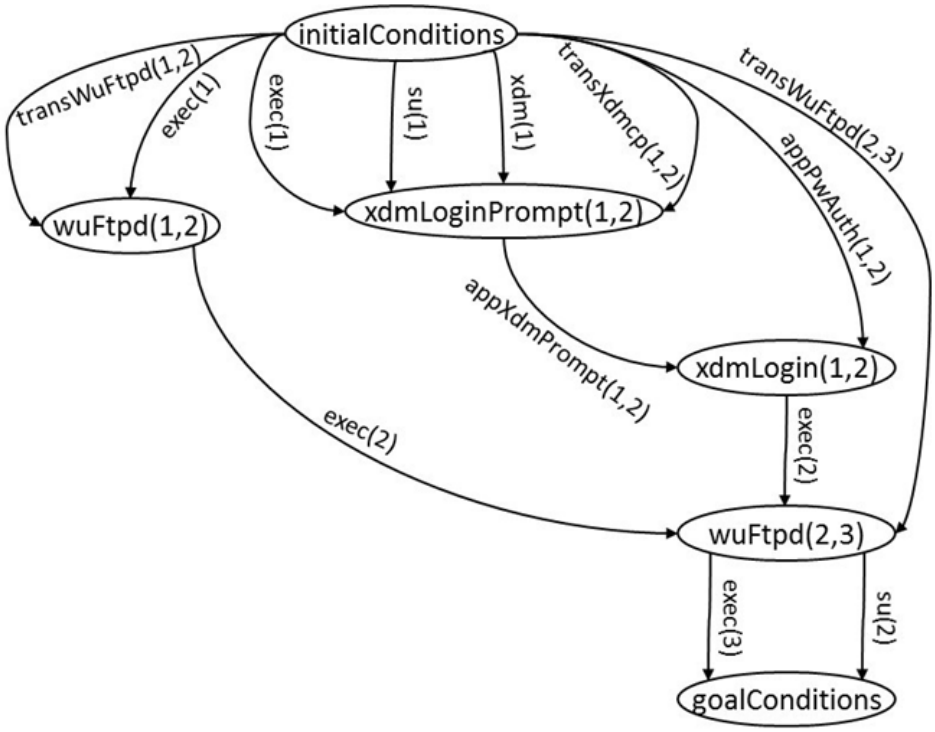


圖 14：Exploit Oriented 所建構的 attack graph 示意圖，資料來源：Peter Mell

4. Hybrid Condition/Exploit Oriented: 有兩種節點，condition 和 exploit，邊是沒有標記的。對於 condition 結點是利用 conjunction (and)，利用 exploit 結點的進入點是用 disjunction (or) 連接。最差圖的複雜性大小是 hc+h^2v 點和 2h^2vc 邊。

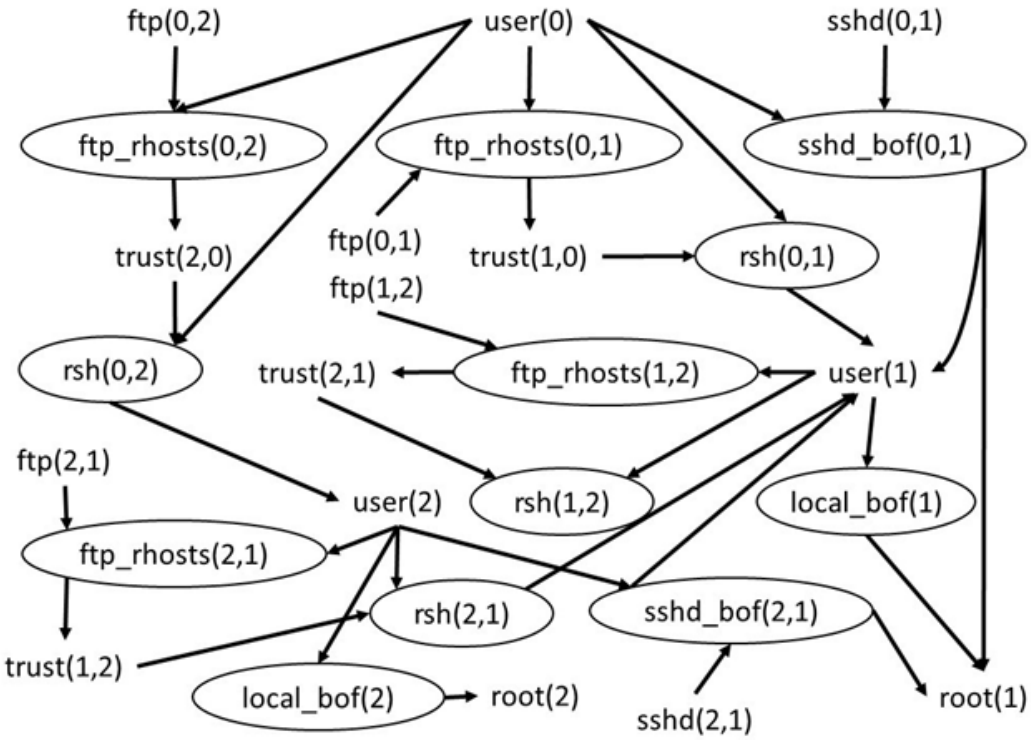


圖 15：Hybrid Condition/Exploit Oriented 所建構的 attack graph 示意圖，資料來源：Peter Mell

5. Vulnerability Oriented: 利用弱點當作結點，每個邊代表攻擊所能獲得的權限。利用 disjunction 來表達進入點的意思。最差圖的複雜性大小是 hv 點和 h2v2c 邊

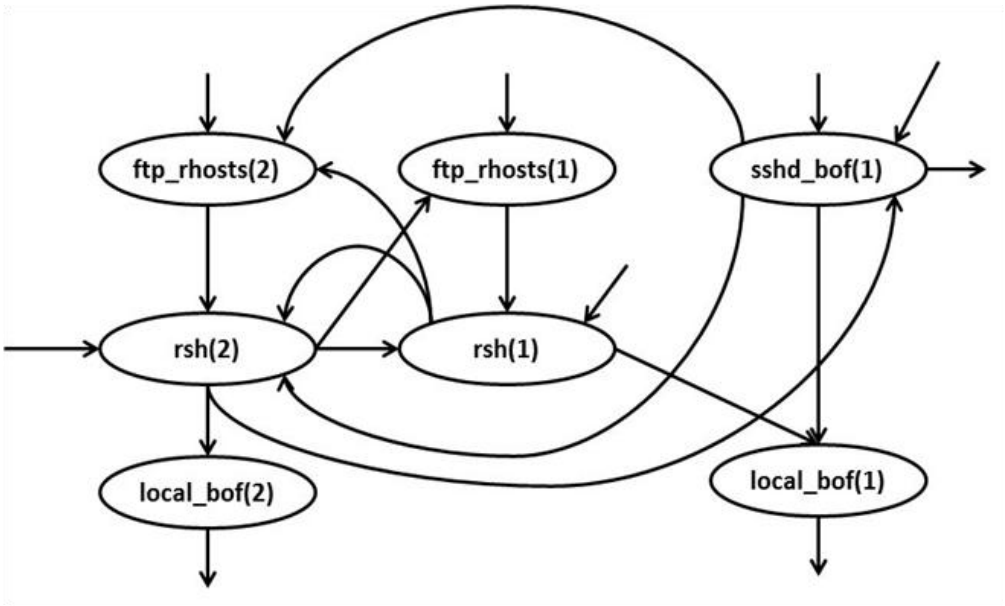


圖 16：Vulnerability Oriented 所建構的 attack graph 示意圖，資料來源：Peter Mell

6. Hybrid Condition/Vulnerability Oriented: 有兩種節點，condition 和 vulnerability。condition 到 vulnerability 的邊標記攻擊者的識別，vulnerability 到 condition 的邊是

不標記的。利用 DNF 來解讀 vulnerability 的點，利用 disjunction 來表示 condition 的點。最差圖的複雜性大小是 hc+hv 點 and h2vc+hvc 邊

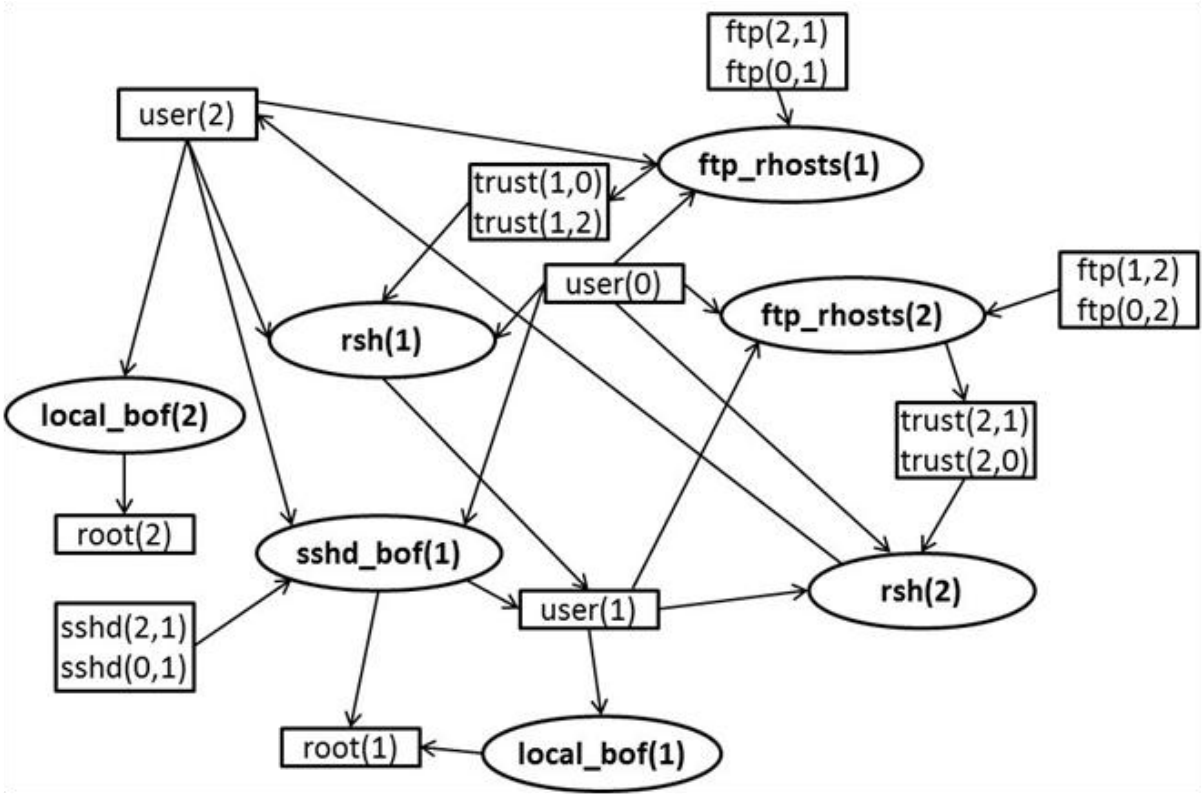


圖 17：Hybrid Condition/Vulnerability Oriented 所建構的 attack graph 示意圖，資料來源：Peter Mell

最後的結果表示 Peter 的表示圖有明顯少的點和邊，能夠降低分析的複雜度。

	Representation	Nodes	Edges	
✓	Condition	5140	436 290	← Abandoned 2002 Approach
✗	Exploit	218 146	7 189 929	
✗	Condition/Exploit	223 285	654 435	← Most Commonly Used
✓	Vulnerability	7825	272 920	} Newly Proposed
✓	Condition/Vulnerability	12 964	233 795	

圖 18：最後結果比較圖，資料來源：Peter Mell

（九）Combinatorial Methods in Software Testing

Rick Kuhn 講解對於軟體測試能夠精簡測試項目（Test Cases）但又不失測試覆蓋範圍（Test Coverage）的方法。軟體測試是一門很重要的學問，在一般的軟體開發中，測試所消耗的成本佔開發項目約 50%左右，對於高度科學的研究單位，通常需要消耗大於 85%的成本做測試。在他的研究中，能夠減少 20%的測試項目，又可以增加 20% ~ 50%的測試覆蓋範圍。

能夠縮減測試項目的原因是在於能夠有效的表達 interaction faults，也就是兩個變數的邏輯組合。例如在一個測試項目中，有一項為當溫度大於 10 ℃，而且門是打開的狀態，其中「溫度」跟「門」是兩個變數，而這個測試項目邏輯成立是這兩個條件，也就是說，這兩個項目其中一個不成立時，該測試項目也會包含其他變數不成立，而且這兩個項目中至少一個項目不成立的事實。如果只測試這兩個變數的關係，這可以讓其他變數的狀態改變可以被忽略。在這個例子中，這個測試條件是 2-way interaction，代表著是兩個變數的互動。

在一個測試系統中，或多或少都會有一些變數互動的關係。如果要完整的測試，必須將所有變數可能的組合列舉，實際地了解其結果。但是在 Rick 的觀察中，發現大多系統內，變數間的互動性不是很高，大多 3-way interaction 即可以涵蓋大部分的範圍，所以在他們的測試系統中，不會有超過 6-way interaction fault 的產生。這種隨機的測試可以比一般特定項目的測試還要完整，比起完整性隨機測試還要有效率。

舉例來說，這邊有一個十個選項的測試變數，如果要有完整的測試，需要跑 2^10 = 1,024 種測試。如果不考慮全部十個選項的組合，僅考慮 3-way interaction 的話，以排列組合來看是 C(10, 3) = 120 種選取方式，每個選項都會有 on, off 兩種，再乘上這種情況為 120 x 2^3 = 960。但是這個數量仍然太多，如果以 10 個選項看來，一個 test case 其實包含許多個 triples，數量為 C(10,3) = 120。但是有些測試項目會重複或沒有測試到，需要建一個表格來做測試，才能完整的包含所有 3-way interaction。要找出這樣子的表格是非常困難的，但是目前有好的演算法來尋找，主要測試項目的數量與 v^t log n 成比例。

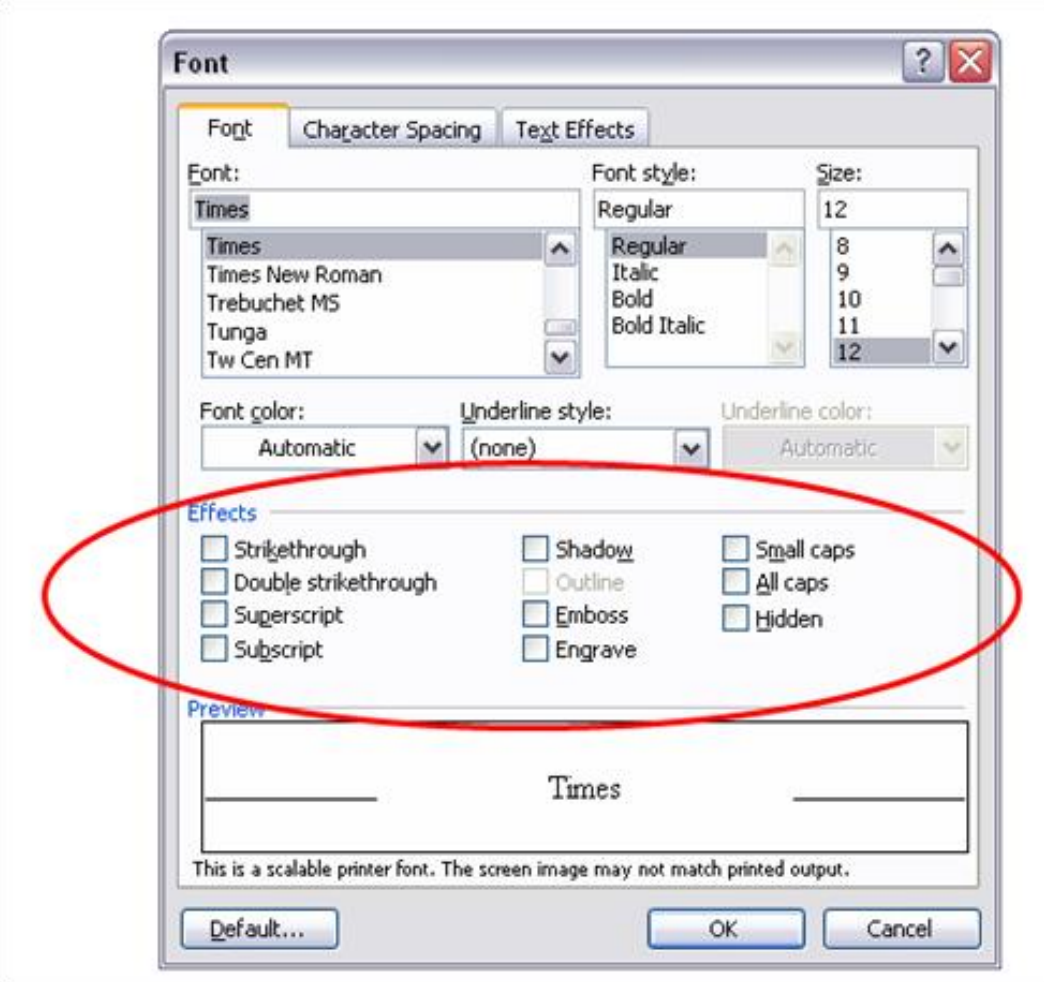


圖 19：一般測試項目，舉例有十個選項可以獨立選擇，資料來源：Rick Kuhn

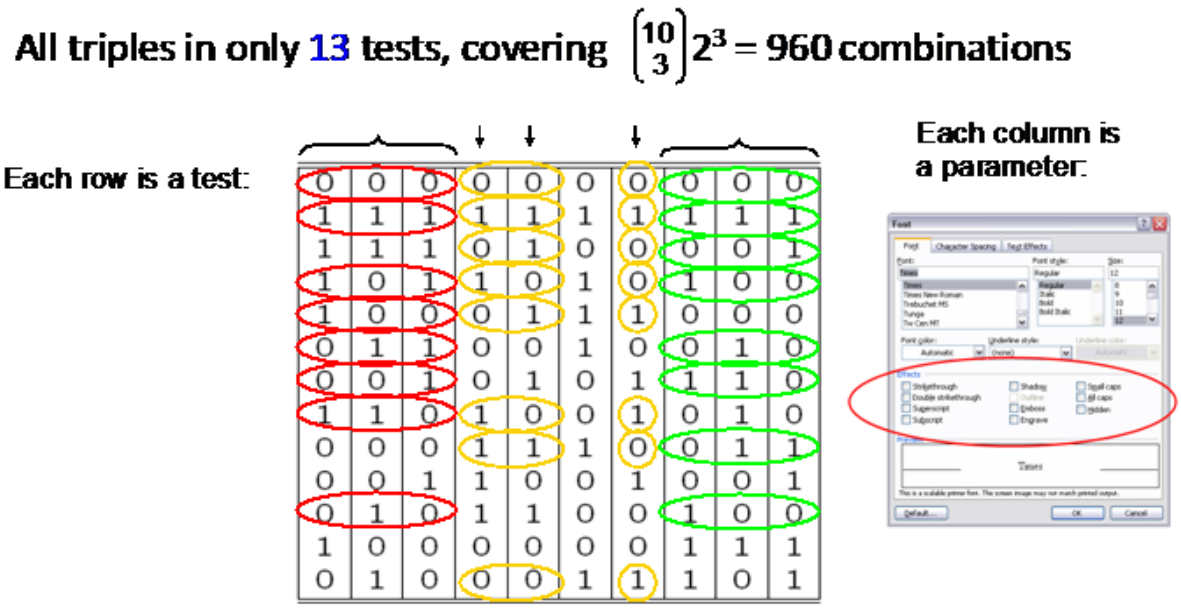


圖 20：十個選項最後的測試項目，可以縮減至 13 項，資料來源：Rick Kuhn

以實際的案例分析，有一個儀表板有 34 個 on-off 開關，如果要全部測試的話，需要有 1.7 x 10^10 個測試項目。但是如果僅考慮 3-way interaction ，則只需要 33 個測試項目，如果考慮 4-way interaction 的話，需要 85 個項目，對於這樣子的測試所需的項目，遠遠小於完整列舉的項目。在這個面向的測試方法中，持續不斷的改進 covering array 產生的演算法，能夠加快整體測試的效果。

Rick 也提到了 Sequence covering array，與上面 on-off 的例子不一樣，是考慮變數中排列的順序變化。當有 6 個變數時，測試 6 個變數的排列組合為 6! = 720。用一樣的概念來做測試，3-way 的測試可以縮減很少。

（十）Discussion on LTE Security

Nelson Hastings 和 Jeff Cichonski 為 NIST 中 public safety 的研究人員，早上兩個小時與我們討論 LTE 的安全性。以下為討論問答摘要。

Q1: 根據 NIST 一份報告中所列舉的攻擊，請問是有可能實現的嗎？

A1:上述報告內的攻擊都是根據現有的文獻所提出來的，都是有可能實際存在的。但是有些比較困難，有些比較簡單。像是 Radio Jamming 的技術，其實後續還有許多演進的版本，例如只針對特定的用戶以及特定的頻道做阻斷式攻擊。在投影片上僅列舉一些常見的種類。

Q2: 有沒有實際的攻擊樣本可以給予我們做後續測試平台建置的參考依據？

A2: 在 NIST 的部門內，並沒有所謂實際的攻擊樣本，也沒有廠商所提供的樣本。但是電信廠商會實際做一些攻擊的範例，目前並沒有聽到真實世界有對 LTE 網路架構從外部做攻擊，只有內部人洩露資料的新聞。

Q3: NIST 有計劃制定相關 LTE 的安全標準，或是撰寫威脅種類？

NIST 目前並沒有針對 LTE 安全規範做標準化，但是有些許相似的文件，來說明如何做安全計劃、風險評估、人員管理規範。由於標準規範並不會只座落在一個特定的商業範疇內，標準應該更寬廣的包含所有有關的產業。此外，相關的安全標準以及量測方式已經有 3GPP，DSMA 等組織做規範了，NIST 不需要再額外制定一個新的標準。

Q4: 在 NIST 一份報告中有關於 IPSec 的實驗數據，有更詳細的實驗環境說明嗎？

是設立在一個電信實驗室內，採用內部的網路，可能會和真實營運商的網路不完全相同。但我們相信結果應該不會差太多。

Q5: 報告中對於啟用 IPSec 上的運算開銷非常樂觀，台灣有些廠商說基地台開啟 IPSec 之後，效能驟降，請問有可能是什麼問題？

在我們的測試裡面，成本不是一個很大的問題。所以在設備上，若要啟用 IPSec，我們建議需要加購有 IPSec 功能的機器，來完成通訊保護的目的，而在製造商或是廠商的眼中，添加設備跟添加硬體裝置是一種成本上的增加，他們會以所支付的金錢相同的情況下來做實驗的判斷。在相同的金錢下，確實會無法有相似的輸出（throughput），但是在我們研究中因為成本不是我們主要的研究目的。我們討論的是理論值的上限，

就我們的研究看來，採購一台機器來增加 IPSec 功能，可以提升通訊的安全性，也可以有逼近原始輸出的頻寬。

Q6: NIST 會強制產業使用 IPSec，或是推動 IPSec 嗎？

目前並不會強制業者使用 IPSec，我們也沒有權力。NIST 是一個提供政府做技術服務的顧問單位，決策層面應該會由政府機關做宣布，機關主管可能類似 FCC。但 NIST 會告訴政府若現有網路不採用加密保護的機制會有什麼資訊安全的問題。

Q7: 營運商是否需要使用 IPSec 來保護可信任的線路，像是 backhaul link。

營運商目前不太會有 backhaul link，他們通常會請特別的電信商，或自己去拉專線，不會透過不安全的網路連線，讓核心網路暴露在外面，讓攻擊者可以遠端存取。

Q8: 行動軟體攻擊是否會造成 LTE 網路中的威脅？

目前看來應該是不會，即使有也不會太嚴重。

Q9: 請問 NIST 有對 eNodeB 或是 HeNB 的 OAM 做測試嗎？

OAM 是一個特別的設備，他們通常會建立在另外一個網路來做管理，或是一個內部網域，並不會公開讓一般民眾所存取。目前我們並沒有用到 OAM 的設備來幫我們做更新，這通常都會是設備製造商需要負責的服務項目。也就是營運商委託設備商做更新時，設備商為了方便管理，需要開發的設備儀器，這部分的技術合約通常都是以服務的方式進行。對於營運商來說，OAM 的測試比較不需要。

Q10: 如何確保一個 OAM 軟體沒有遭受到修改？

有可能，但是 OAM 的軟體通常會有憑證保護，而且 OAM 的啟動環境需要是安全的，現有的 OAM 標準裡面會描述需要透過一連串的啟動方式來確保 OAM 運行的系統是安全的。當然，如果是內賊所做，那還是有可能讓更新程序下載到惡意的程式碼。

Q11: TR 報告與 TS 的標準之差異？

TR 是一些學者、業者、主管機關的人一起下去集思廣益，去思考現有的架構需要什麼樣子的設計、需求、標準等。在撰寫 TR 中，每個答案都是個未知數，所以比較混亂。過了一段時間，隨著編輯者的審查，如果該文件撰寫的有條理、正確、符合現在的需

求，則會變成了 TS，當成標準發布。不然可能會凍結，停止更新。換句話說，TR 比較像是一個草稿，概念性的說明。TS 則是已經被驗證過，比較嚴謹的文件。

Q12: TR 33.820 中的威脅是不是真的都存在？

我們沒有閱讀 TR33.820，不過看他的狀況應該是還在草稿撰寫當中。所以裡面有些威脅應該還是在假設狀態中。你們應該可以在尋找一下有沒有其他 TS 的安全標準規範。

Q13: 現在有對 LTE 設備做安全檢測的標準規範嗎？

現在已經有針對 MME 做的安全評估文件，不過還在撰寫中。

Q14: 目前有沒有接收過 LTE 相關的攻擊事件？有沒有懲罰違反安全性的營運商？

我們並沒有接收到任何的攻擊事件。不過有一次是有可靠性的問題，在 2010 年的時候，華盛頓 DC 這邊發生了一陣手機連不上網路的情況，造成市區通訊大中斷，後來有警告營運者，應該要有些保障以及懲罰條款，但是我們並沒有立法或是強制性的規範來要求營運商需要達成某些安全性，可靠性比較屬於營運商比較在意的問題。

（十一）Mobile Forensic Tour

Richard Ayers 專門做 Mobile Forensic，又稱行動裝置鑑識。鑑識是指事發過程後，利用軟硬體的方式來回覆當初事發當時的情況，Forensic 被廣泛地用在犯罪調查，而該實驗室則是負責鑑識市面上各種手機。

鑑識的資料包含連絡人、行事曆、待辦事項、電子郵件、短訊、簡訊、網頁資訊、電子文件、照片、影片、聲音、GPS 地理位置、社交網路資料、用戶識別、裝置識別、電信服務商、通話紀錄、通話號碼。而資料取得的難易度從容易到難分別是，手動擷取、邏輯擷取、實體擷取、晶片脫離、晶片讀取。

- 手動擷取：用人工的方式獲得資料，像是看螢幕，或是手動操作手機利用電子文件或是圖片的方式，將資料傳出。。
- 邏輯擷取：手機透過連線，藉由有線（USB 或是 RS-232）或是無線（WiFi、 藍芽或紅外線）的通訊協定，來取得資料。
- 實體讀取：利用特殊的工具來對 flash 記憶體做讀取，像是 Joint Test Action Group（JTAG）的介面即可以對微處理器和記憶體做存取。
- 晶片脫離：不透過晶片的腳位，直接對裡面的針腳做讀取
- Micro 讀取：只針對邏輯閘做讀取。

鑑識受到的考驗是因為有許多種的介面裝置，例如 mini-USB、micro-USB，還有系統的原始碼是 closed source。裡面有介紹到 JTAG 來做資料的讀取。JTAG 是一種測試的介面，可以針對手機主機板的處理器、記憶體做測試。

（十二）Net-Zero House Tour

David Yashar 致力於開發綠能的環境。帶領我們參觀 NIST 針對綠能環境保護的研究。他帶領到我們一棟小屋，上面覆蓋著太陽能板，周邊空曠。第一站到了車庫，裡面滿滿的監控儀器，用來量測屋子裡面的溫度以及能量的損耗，該團隊在 2014 年成功的達成了「零能損耗」的目的，也就是該屋子能夠提供一整年的能源。為了達到這個目的，許多建築材料、建設工法需要重新的思考。為了精確的模擬，房子內部還會有一些機器來模擬人的活動，包括完整的淋浴、廚房、臥房、書房的擺設以及動作模擬。裡面有嚴格的溫度監控和精密的溫度循環系統。

（十三）FISMA and RMF - Kelley Dempsey

最後一個 NIST 的議程 Kelly Dempsey 所介紹的危機評估以及相關標準。首先介紹 Federal Information Security Modernization Act（FISMA）的內容，是一個對於風險評估的工作。 而 NIST 這邊有非常密切的合作，有許多安全標準已經被公開，而且還有許多正在撰寫的草稿也會公開讓一般使用者閱讀。線上的使用者可以回覆意見，會有人搜集整理帶入會議討論，再加入新的標準。

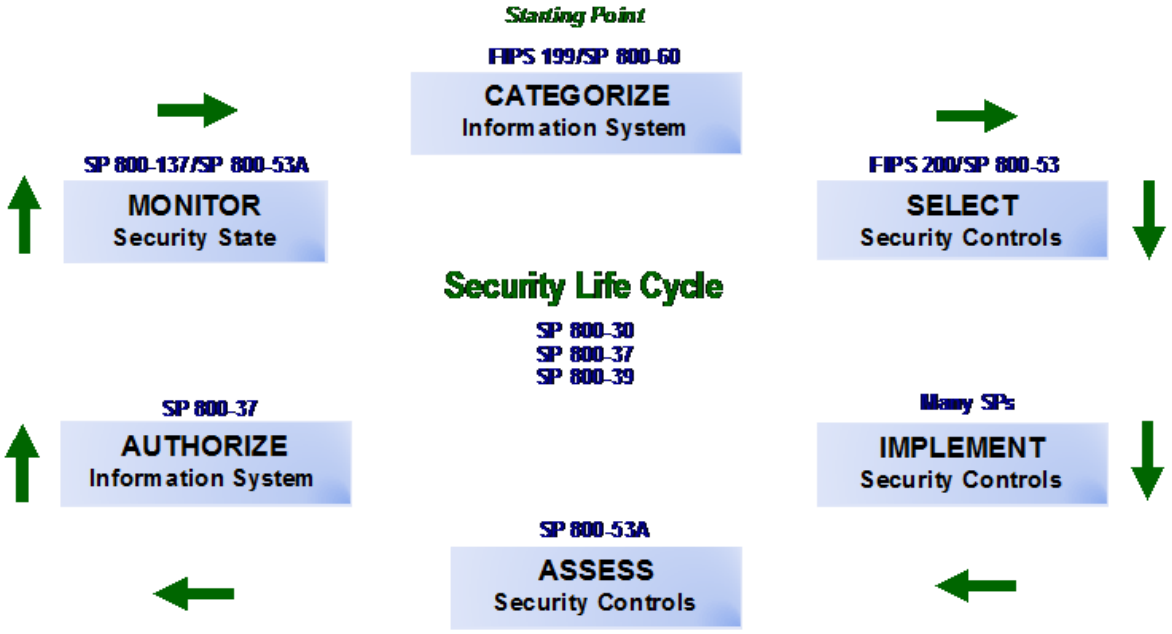


圖 21：安全生命週期循環，資料來源：Kelly Dempsey

在風險評估當中，可以分做六個步驟，以下為條列式說明：

- 分類（Categorize）：FIPS 199 有數種 Information 種類和系統種類可以參考。在 SP 800-60 Rev 1 中，將目前所遇到的問題對應到現有已知的分類。將資訊 和 資訊系統對應到安全類別中。SP 800-18 Rev1 是一個教學文件，如何為聯邦資訊系統發展一個安全規劃。
- 選擇（Select）：FIPS 200 中有 17 個安全相關的領域，介紹基本的安全控制方式，這些基礎還需要加以改進才能適用於各種資訊系統中。在 SP 800-53 提到聯邦資訊系統或組織的安全與隱私控制方法，有比較詳細的步驟說明。
- 實作（Implement）：實作因為比較跟系統相關，像是 RFID, Wireless, TLS, VoIP, Bluetooth 等等，所以會分別寫在許多的文件裡面。
- 評估（Assess）：在 SP 800-53A 中，有對制訂出來的 Security plan 做評估，有一張表格可以參考。
- 授權（Authorize）：SP 800-37 是目前還在制定當中作風險的評估，。
- 監控（Monitor）：SP 800-137 針對聯邦資訊系統或組織的監控的步驟。

二、美國聯邦通訊委員會 FCC

FCC 共安排二場會議，第一場會議由本會及財團法人電信技術中心（以下簡稱 TTC）、交通大學(以下簡稱 NCTU)與 FCC 進行 Security Standards and Security Issues 交流。第二場則由 FCC 進行 5G—Mobile Broadband in mmW Bands 介紹。

(一) Security Standards and Security Issues

Jeff Goldthorp 為 FCC Associate Bureau Chief 也是 Acting Chief, Cybersecurity and Communications Reliability Division ,Public Safety and Homeland Security Bureau (PSHB)。會議主要進行方式為本會及技術團隊簡單介紹我們想要瞭解及面臨的問題，再由 Jeff 進行應答。由 FCC 與會人士的安排，可發覺其對於本會本次的議題及接待極為慎重及重視，以下為問答重點摘要：

Q1:在美國，有沒有實際的 LTE 資安攻擊行為發生？

目前並沒有聽到真實世界有對 LTE 網路架構從外部做攻擊，只有內部人員洩露資料的新聞。

Q2: 在美國，FCC 對於中國製造的產品採取的態度

FCC 對於中國製造的通訊產品，並沒有採取任何禁止的行為。一些新聞訊息可能來自國防部(Department of Defense，DoD)或美國國家安全局(NSA)，但並非 FCC。

Q3: FCC 對於基站安全或基站管理是否有查驗機制

FCC 對於安全著重在與人體有害及通訊保障，因此 Public Safety 主要規範為電磁波檢查及 911 緊急通訊服務，Security 為電信業者範疇。

Q4:FCC 是否要求或是建議電信商，採用 IPSEC Backhaul

安全議題為電信商運營首要考量議題之一，為提供用戶有保障的服務，相信電信商針對其核心網路有層層防密考量，Backhaul 也會採取專線電路，不會透過不安全的網路連線，讓核心網路暴露在外面，讓攻擊者可以遠端存取。FCC 並不會硬性或是強制規定業者啟動。

Q5:FCC 是否有認可之實驗室，進行 LTE 一致性、相容性或是資安檢測。

FCC 主要是依據 1934 年通信法案所創立，主要負責執行 1934 年通信法案，FCC 規定及命令和通信授權的條款，並無實驗室進行 LTE 一致性、相容性或是資安檢測，此部份建議可參考 NIST PCRF。

(二) 5G—Mobile Broadband in mmW Bands

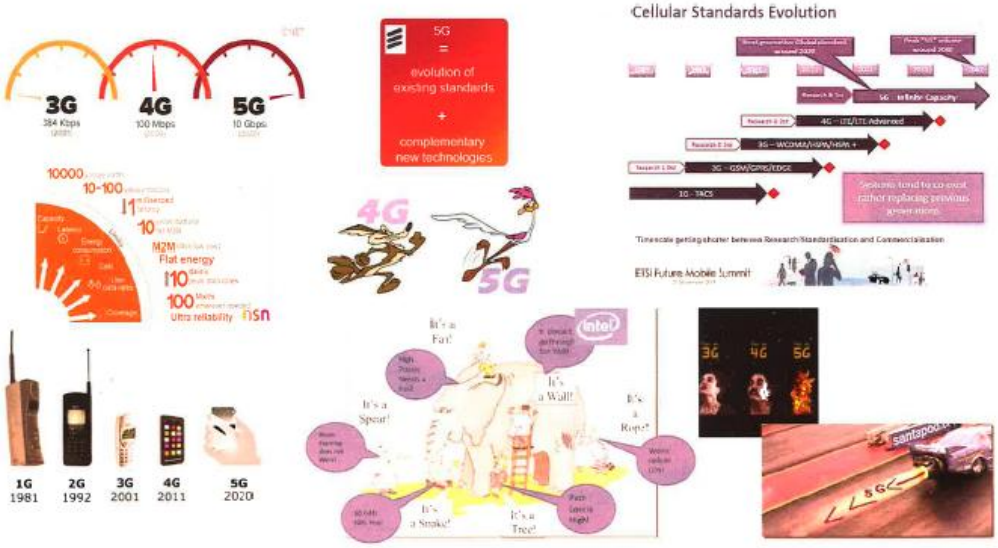
最後一場會議由 Michael Ha，其為 FCC Policy & Rules Division Office of Engineering and Technology (OET)的副主席，針對 5G—Mobile Broadband in mmW Bands 進行介紹。

在 ITU-R 確定 IMT-2020(5G)的願景、關鍵能力需求規範與發展時程後，接下來就是全球通訊業者，要開始忙著開發系統解決方案，並將其標準化。如何滿足一千倍的挑戰，大致可從三個維度來尋求解決之道；除佈建更多基地台，改善頻譜效率(Spectrum Efficiency)外，就是增加使用的頻譜寬度(Bandwidth)。然而在全球已經被凌亂分配的頻譜情況下找到可運行頻帶，則需往高頻頻帶尋找。

ITU-R 於是開始探討利用 6GHz 以上頻帶做為行動通訊 用之可行性，一般預期，未來在高頻應該要可以找到共通的 1GHz 頻帶，做為未來 5G 使用。如此，相較於 4G LTE-A 的 100MHz 運作頻譜寬度，就有十倍成長。

由於訊號在高頻傳遞，其傳遞衰減、雨衰、受地形地物阻擾等影響，品質會變得非常差，因此愈高頻愈不適合作長距離的行動通訊之用。不過，由於在高頻波長極短，可使用極小天線，因此可以將大量天線形成陣列天線(Array Antenna)，加上技術的進展，如 Massive MIMO、波束成型(Beamforming)、波束追蹤(Beam Tracking)等，讓大家對高頻用於行動通訊的應用抱著樂觀態度，也因此 FCC 也開始關注於毫微米波(Millimeter Wave, mmWAVE)通訊系統研究。

What is 5G?



- Components of 5G are being identified and under discussion/development
  - Throughput (>50x of 4G, or 5-10GBps) and latency (<1msec air latency) are often discussed
- The overall network architecture and end-user experience need further work

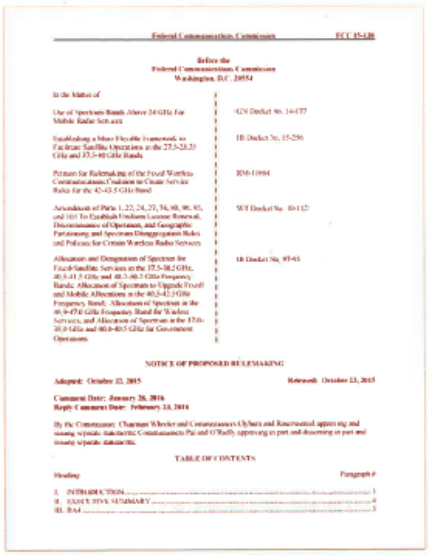
3

NON-PUBLIC. FOR INTERNAL USE ONLY

圖 22：FCC 5G 介紹

Expanding Use of the mmW Spectrum

- FCC Notice of Inquiry (NoI) adopted 10/17/14
- FCC Notice of Proposed Rulemaking (NPRM) adopted 10/22/2015
- NPRM proposes a mix of licensed and unlicensed use in the millimeter wave spectrum, and creates opportunities for sharing among different kinds of users; fixed/mobile; federal/nonfederal; terrestrial/satellite; and carrier networks/private networks
- Recommended by Technological Advisory Council



Before the
Federal Communications Commission
Washington, D.C. 20554

NOTICE OF PROPOSED RULEMAKING

TABLE OF CONTENTS

7

圖 23：FCC 頻譜使用說明

伍、 心得與建議

這次美國參訪，瞭解其資訊安全主要配置分工，FCC 負責政策規範，搭配 NIST 負責落實技術標準，國土安全部負責資安營運管理，國防部、國家科學基金會及各州政府負責資安技術研發補助，產業則自主發展。

以行動寬頻資安而言，FCC 並未有任何規管及查驗的規範，其認為 Security 應屬於電信商範疇，電信業者有責任建構一套安全不受使用者入侵、竊取資料之行動寬頻網路，如有資料外洩或是消費者權益受損，則有罰款機制。建議針對國內電信業者對所建置的行動寬頻網路，如因其系統網路安全事件，導致消費者權益受損，亦應給課予其適當責任。

NIST 為美國國家標準技術研究所，隸屬美國商務部，以促進美國的創新和產業競爭力，推進度量衡學、標準、技術以提高經濟安全並改善生活質量為目的。其每年經費由政府編列預算經議會通過後使用，沒有預算目標達成的壓力，能進行一些政府支持的研究。NIST 實驗測試，主要以研究為主，瞭解理論值上限或是針對未知的新領域進行涉獵。在與 NIST 交流討論中，NIST 對於行動應用程式安全風險評估與審驗，如基本資安檢測項目訂定、檢測項目所須檢測之各項檢查事項、預期之檢測結果及各結果之形成條件等已有成果，可供本會參考訂定相關規範時參考。

針對行動寬頻資安議題，與 FCC 及 NIST 交流後，得知目前並無任何透過基站為媒介而發生的資安事件，綜觀各文獻分析許多可能存在的風險、攻擊及威脅，在 3GPP 的標準規範建議、業者的防備及設備商的阻絕能力產品設計下，尚未發生。IPSec 及 Trusted Backhaul FCC 並無介入管制，僅只有 NIST 於研討會或是文獻發表上的建議。美國政府對於電信商的行動寬頻網路安全，是充分信賴電信商，其認為若有發生問題，最大的損失會是電信商，其有可能遭受消費者流失、信譽喪失、或是來自聯邦的罰款。然資安問題日趨嚴峻，國際標準組織 3GPP/GSMA 已開始規劃行動寬頻設備之資安認證規範，建議持續投入經費與人力來研究及注意國際行動寬頻資安認證規範之發展趨勢，以與國際接軌。

陸、 附件

■ 參考資料：

- Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE- https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf
- NIST publications – http://csrc.nist.gov/publications
- FCC Homepage- https://www.fcc.gov/

■ 照片

圖 24：Matthew Scholl 與本會吳銘仁 簡任技正合影

圖 25：Kim Schaffer 與本會吳銘仁 簡任技正合影

圖 26：FCC 大會議室合影