行政院及所屬各機關出國報告

（出國類別：其他-國際會議）

參加「DEF CON 26 資訊安全年會」報告

服務機關：財政部財政資訊中心
姓名職稱：陳俊呈設計師
派赴國家：美國
出國期間：107 年 08 月 08 日至 107 年 08 月 14 日
報告日期：107 年 10 月 30 日

摘要

本(107)年度第 26 屆 DEF CON 資訊安全年會(DEF CON 26) 於 8 月 9 日至 12 日在拉斯維加斯的 CAESAR'S PALACE 及 FLAMINGO 飯店的會議中心進行為期 4 天的研討會，會議內容包括各種軟硬體設備的漏洞發表、各式駭客攻擊方法，以及時下熱門的物聯網(IOT)及人工智慧資訊安全議題。本文對此次出國參加 DEF CON 26 資訊安全年會的目的加以說明，並介紹此研討會舉辦之相關內容，包含技術專題發表(PRESENTATIONS)，會場上有許多資訊安全領域的專家進行主題演講並展示各種可能的漏洞與破解方式，本文中對關鍵基礎設施、惡意軟體 Signature 產生技術、App 應用程式安全、語音辨識技術破解以及大量 PCAP 資料分析技術進行介紹。此研討會中並舉行各式競賽(CONTESTS)與活動，其中 CAPTURE THE FLAG(CTF)為一年一度之國際駭客競賽盛事，另外還有各式各樣的 VILLAGES 活動，包含 Recon Village、Data Duplication Village、Social Engineering Village 、Lockpicking Village、Soldering Skills Village、Wireless Village、Hardware Hacking Village 等主題之教授活動，其中 Lockpicking Village 是 DEF CON 研討會的傳統，每年皆會介紹各種開鎖技巧。最後透過參加此資訊安全年會，對人才培育、資訊安全檢測、資訊安全情資分析技術發展提出些許建議。

關鍵詞：DEF CON 26、資訊安全、駭客攻擊手法。

目次

壹、目的

為瞭解目前資訊安全領域發現之新型態攻擊手法與各種可能之漏洞及新興之資安議題，故本中心派員參加 DEF CON 26 資訊安全年會，藉此汲取最新之資訊安全觀念。電腦網路攻擊手法牽涉眾多資安議題，駭客運用各種可能之漏洞進行攻擊，分析研究這些議題，可發展相對應之資安防禦策略。故此次參加 DEF CON 資訊安全年會，研習主題以資安防護相關業務為主，並關注未來資訊安全發展動態，期望透過此會議掌握近一年來國際間資安發展情勢與駭客攻擊手法之變化，汲取與本中心核心業務相關之資安防護新知。關注新興的資安防護議題，如：物聯網(IoT)、智能汽車、NFC 等資安防護與攻擊手法、智能合約(Smart Contract)及加密貨幣等新型態的資安議題，以瞭解近年新興的駭客攻擊手法。

圖 1：DEF CON 26 會場情況

貳、研討會介紹

每年暑假在美國拉斯維加斯舉行的 DEF CON 研討會是國際上資訊安全領域的一大盛事，DEF CON 會議不開放預先報名，只允許現場以現金購票入場，其入場採用的識別證(Badge)相當特別，此識別證也是駭客技術的展現，其預留擴充性可讓有興趣的人進行改造。

圖 2：DEF CON 26 之 Badge

而在 DEF CON 舉行之前，另一盛大的資訊安全研討會 Black Hat 每年也在拉斯維加斯舉行，Black Hat 與 DEF CON 主要的差異為 Black Hat 的議程安排較為正式與華麗，偏重於資安領域學術研究，而 DEF CON 會議之形式則較為自由，著重於駭客攻擊實務，在 DEF CON 會議中還有各種競賽同時舉行，晚間則會舉行搖滾音樂會，其較類似於地下駭客之年度技術交流會議與嘉年華會。

今年的 DEF CON 會議已邁入第 26 屆，據主辦單位統計此會議超過 2 萬多人參

加，此會議已經是全球最大的資安技術發表會議，同是也是政府及各大公司招募資安人才的管道之一。此會議之演講採多議程並行方式進行，今年有 4 個平行議程(DEF CON 101、Track 1、Track 2、Track 3)分散於 CAESAR'S PALACE CONFERENCE CENTER 及 FLAMINGO EXECUTIVE CONFERENCE CENTER 兩間飯店中。

在 DEF CON 會場中除了有資訊安全技術演講外，還有各式有趣的競賽(CONTESTS)，讓參加的人有機會參與各種資訊系統漏洞的破解，寓教於樂。其中最著名的應為 Capture the Flag(CTF)競賽，每年均吸引世界各國好手組隊參賽事前的各種預賽，取優勝的隊伍進入最後的決賽，今年全世界有 25 隊前往 Las Vegas 的 DEF CON 26 會場參加最後的競賽活動。

因為 DEF CON 會議是一個非常大的研討會，故在會場中放置各式看板讓參加者可即時看到此會議的相關資訊。會議從早上 10 點到傍晚 6 點，每個小時有 4 個 Tracks 同時進行，共有上百場議程，每一間會議室幾乎都擠滿了人，晚到者就只能站在場後聽講，大部分議題的時間都在半個到 1 個小時之間，其內容主要分佈在 IOT、硬體、無線網路及非主流系統攻擊等技術議題上。

圖 3：DEFCON 26 會議 Track 現場情況

參、過程

DEF CON 研討會涉及的領域主要為軟體安全、計算機架構、無線網路竊聽、硬體修改及其他易受攻擊的資訊安全領域。會議除了前述領域的技術分享外，還有多種競賽項目，如 AI VILLAGE JEOPARDY、BADGELIFE CONTEST、WIRELESS CTF、OSINT CTF…等比賽，這些比賽中，最著名的應該就是 CAPTURE THE FLAG(下稱 CTF)奪旗賽。

一、 CAPTURE THE FLAG 競賽

每年 DEF CON 的 CTF 舉行前，全世界有意願參賽的隊伍都會先參加資格賽(DEF CON 各大種子賽的冠軍隊伍是當然入圍決賽的成員)，透過資格賽選拔，優勝隊伍再於 DEF CON 研討會舉行期間前往拉斯維加斯進行最後的決賽，此次第 26 屆 DEF CON (DEF CON 26) CTF 主辦單位邀請全球 25 隊隊伍參加今(107)年 8 月 9 日至 12 日舉行的 CTF 決賽，比賽過程中，各支競賽隊伍都使用專用軟體，並利用特別的網路結構，對網路中的伺服器進行攻防比賽。

CTF 比賽的題目多分佈在網路、作業系統與應用程式之攻擊手法研究、對攻擊行為進行分析，瞭解攻擊行為與手法、病毒和防毒軟體之研究、對二進位檔或不明資料進行逆向工程之解析、對開放原始碼之軟體進行安全性檢測之過程與方法、各種後門或木馬程式的設計與研究、網頁伺服器與資料庫的安全性議題、防火牆及入侵偵測/防禦系統的技術現況、目前各種作業系統安全性強化的技術、隱藏傳輸通道(Covert Channel)，將特定資料隱藏於其它正常資料串流或協定中傳送的方法等。

今年臺灣首度有兩隊進入 DEF CON 的 CTF 決賽，分別為 HITCON 和 BFS 團隊，HITCON 團隊自 103 年起連續 5 年進入 CTF 的決賽。而代表我國參賽的另一隊伍 BFS 團隊是由交大 Bamboofox、臺大 Balsn、中央大學 DoubleSigma 以及中科院 Kerkeryuan 等四隊組成，其在入圍賽以第 22 名的成績成為臺灣第 2 隊入圍 DEF CON 26 CTF 決賽

的隊伍。本(107)年度冠軍由曾經在 2015 年獲得 CTF 冠軍的韓國隊 DEFKOROOT 獲得，美國隊 PPP 獲得第 2 名，而臺灣隊 HITCON 也不負眾望獲得第 3 名的好成績。另外，此次新入圍的臺灣隊 BFS 亦獲得第 12 名的成績，表現不俗。

圖 4：CAPTURE THE FLAG(CTF)現場比賽實況

二、 VILLAGES 介紹

DEF CON 研討會上每年都舉行各式各樣的 Villages 活動，各種 Villages 活動是 DEF CON 的一大特色，這些活動不是單向的演講而是完全的動手參與，內容涉及軟硬體破解、無線網路、生物、社交工程、加解密、防禦技術，甚至是自動汽車破解技術。以下介紹幾個參觀的 Villages：

(一) RECON VILLAGE

此 Village 透過舉行黑客松(hackathon)方式，讓參加者運用 OSINT(Open Source Intelligence)/Recon(reconnaissance)工具進行網路情資蒐集比賽。Recon Village 以開放空間形式進行，包括會談、展示、研討形式討論、OSINT CTF 競賽(Jeopardy Style OSINT CTF)等，其關注在 Reconnaissance 偵察的重要性。其核心目標為教育大眾對偵察及開放情資來源(OSINT)重要性的認識，並展示即使是關於被偵察目標洩漏的小信息也可能對個人或組織造成災難性損害。

(二) DATA DUPLICATION VILLAGE

DEF CON 提供會議相關資料與一些破解所需資料的拷貝服務，參加者可自行攜帶 6TB SATA (6TB SATA 512byte sector(512e)7200 RPM)磁碟前來拷貝。其提供的資料包含彩虹表(rainbow table)(是一個用於加密 Hash 函數逆運算的預先計算好的表，常用於破解加密過的密碼 Hash)及 infocon.org(https://infocon.org/)與所有 DEF CON 的資料。今年並安排了磁碟複製、磁碟鑑識、資料備份、資料復原與資料管理的講座。

(三) SOCIAL ENGINEERING VILLAGE

此 Village 安排社交工程的專家進行演講並嘗試實驗，瞭解可能運用來破解人類心理防禦的技巧，檢查社交工程的防禦機制是否產生作用。

此 Village 舉行了 SECTF 的競賽遊戲，模擬當一個人被囚禁在一棟大樓裡，是否可以順利逃脫？其模擬的情況為參賽者被捕獲並戴上手銬，並在監獄牢房裡被戴上腳銬，為了逃脫，必須解開手銬、撬開鎖以逃出牢房，並正確通過 3 個臉部表情(其為 Paul Ekman 博士的臉部表情)的識別，並通過 laser 網格找到通往自由的道路。

圖 5：SOCIAL ENGINEERING VILLAGE 與 RECON VILLAGE HACKATHON 看板

(四) SOLDERING SKILLS VILLAGE

此 Village 主要教授硬體焊接技巧，提供硬體破解的方法與資源。它提供建立、修復與修改 Badge 和其他電子設備的場所與工具，讓有興趣的人可以聚集在一起合作破解各種 Badges。

(五) LOCKPICKING VILLAGE

LOCKPICKING VILLAGE 是 DEF CON 研討會的傳統之一，每年皆會介紹各種開鎖技巧，並舉辦開鎖競賽，在駭客世界中認為開鎖也是一種破解的挑戰。此 Village 中介紹鎖的基本結構與運作方式，並讓參與者透過動手實作方式瞭解各種鎖的弱點與破解技巧。

圖 6：LOCKPICKING VILLAGE 展示之開鎖工具

(六) PACKET HACKING VILLAGE

Packet Hacking Village 介紹封包偵測與分析技術，並安排相關的 WORKSHOP 讓參與者可以透過實作方式進行交流，此 Village 透過教育方式啟發與會者網路封包安全之重要性，同時專注於網路攻防演練中藍隊之防禦技術。

此 Village 中綿羊牆(Wall of Sheep)為與會者提供一個友好的提示，如果使用開放式網路且採用不安全的通訊協定，那麼帳號與通訊內容將會被攔截下來且公布在綿羊牆上，此為滿有趣的一項活動。

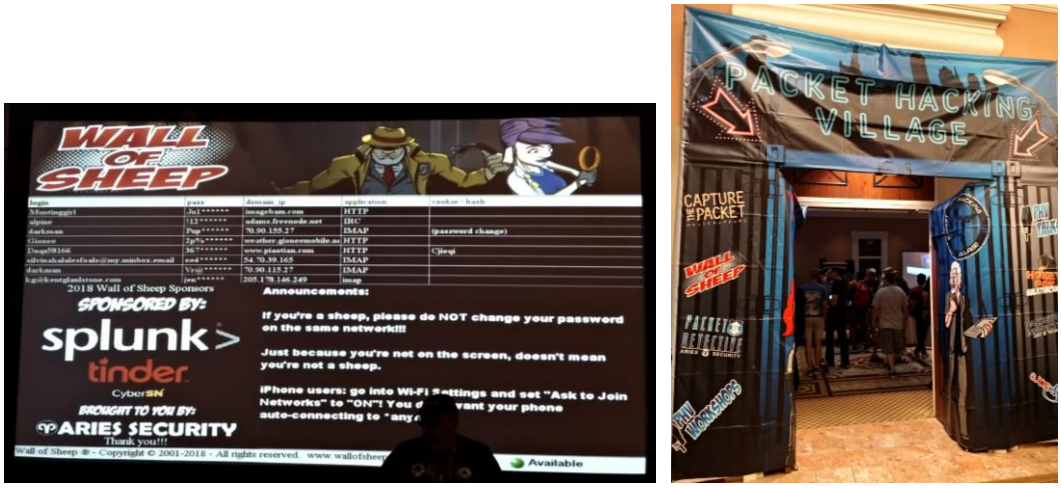

圖 7：PACKET HACKING VILLAGE 現場實況

(七) AI VILLAGE

AI VILLAGE 是一個人工智慧與資訊安全專家聚集在一起學習和討論人工智慧的運用與可能濫用造成資訊安全風險的地方。人工智慧技術在資訊安全領域已開始被廣泛使用，如惡意軟體之檢測與網絡流量分析，但同時使用人工智慧技術的系統，也為駭客開闢了新的攻擊方向。

此 VILLAGE 有一些 workshop 對 ADVERSARIAL MACHINE LEARNING 進行研究討論，其是利用對抗例(adversarial example)造成深度學習模型判斷錯誤這種攻擊手法，這是目前 AI 領域新的駭客攻擊手法。例如：Papernot 等在 2016 年發表針對影像辨識的深度學習服務進行攻擊，其透過 API 取得部分分類結果後，在 local 端另外建構一

個訓練的 local model，從 local model 中找出可用的對抗例(adversarial example)，之後轉移(transfer)回去攻擊目標 API。所謂對抗例(adversarial example)，是一種刻意製造讓機器學習模型判斷錯誤的輸入資料。過去的研究就發現用 ImageNet、AlexNet 等資料集訓練出來的影像辨識模型，輸入端只需要微小的變動，輸出結果就會有大幅度的改變。這樣的結果顯示深度學習模型的結果可能是不穩定的，而且可能被駭客惡意利用而有資訊安全疑慮。

圖 8：AI VILLAGE 現場實況

(八) IOT VILLAGE

IOT Village 是由安全諮詢及研究公司 Independent Security Evaluators(ISE)這家公司所組織的，其提供有關物聯網設備安全性強化的宣傳和專業知識分享。IOT Village 由資訊安全研究專家主持 workshop 討論與分析目前 IOT 系統可能存在的漏洞，此外 IOT VILLAGE 運用現成的物聯網設備進行 IOT CTF 競賽。

近年來物聯網設備(IOT)在市場上越來越多，但是 IOT 製造商普遍缺乏資訊安全威脅的觀念，故 IOT 已成為駭客攻擊的新興目標，從過去時有所聞的 IP Cam 遭駭，家中隱私曝光到現在的智慧電燈被駭燈光亂閃、智慧門鈴被駭門鈴亂響及與人身安全有切身關係的車用 GPS 或手機 GPS 遭駭，所有欠缺資安防範的 IOT 裝置，如無人機、

無人自動車、智慧工廠、IP Cam 等都可能遭駭。

圖 9：IOT VILLAGE 議程

(九) BLUE TEAM VILLAGE

近年來駭客攻擊在任何環境中都很容易被執行，這意味著有效的防禦是很困難的。資訊安全維護者(Blue Team)必須維持資訊資產及面對管理制度和資源限制，並且與攻擊方(Red Team)相比，通常較缺乏關於如何最好地保護其資訊環境的公開信息。這使得資訊安全防護者感覺有點遺漏了大部分有利於攻擊者(紅隊)的內容。

此 Village 提供資訊安全維護者(Blue Team)聚集的區域，學習基本和先進的防禦技術，交換過往遭遇資訊安全攻擊的訊息。BLUE TEAM VILLAGE 在 DEF CON 中是用於推廣防禦性安全知識。對攻擊者(Red Team)而言就是要攻打系統，找出入侵管道，其使用的技巧就是滲透測試、系統弱點掃描、網站弱點掃描、行動 App 檢測、IoT 檢測、社交工程等技巧。對防禦者(Blue Team)而言就是要建構縱深防禦的銅牆鐵壁，其使用的設備工具通常為防火牆、DDoS 防禦系統、IPS/IDS、WAF、APT 防禦設備、SOC 監控中心、端點防毒/防駭系統，以部署層層保護，防範未知之攻擊。

在各種新興科技快速產生的情況下，越來越多企業組織成立專職的資安團隊以強化內部資訊安全，定期地執行弱點掃描、滲透測試，甚至攻防演練，以及基礎的軟硬

體盤點、更新、備份等。在資訊安全事件發生前，紅隊(Red Team)成員負責找出企業隱含的漏洞威脅，經由各種模擬演練與攻擊測試，找出資訊系統未知的漏洞與風險。藍隊(Blue Team)成員則負責資安事件的應變與處理，當企業組織遭受駭客攻擊時，找出問題根源，界定受駭範圍及損失，第一時間停止災害並制定修復計畫。

圖 10：BLUE TEAM VILLAGE 現場實況

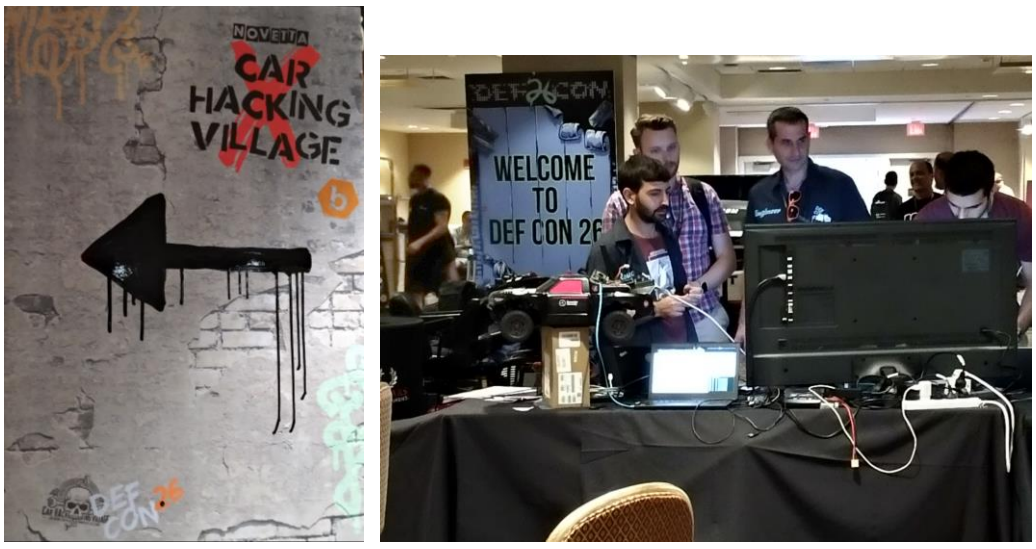

圖 11：CAR HACKING VILLAGE 現場實況

三、 技術專題發表(PRESENTIONS)

DEF CON 資訊安全研討會中的技術專題發表(PRESENTIONS)，每年都是以 4 個平行議程(Tracks)方式進行，大會邀請來自世界各地的資訊安全研究者或駭客級專家進行各種資安新知的主題演講與展示各種系統漏洞的破解。今年參與 DEF CON 26 研討會的人數相當多，整個會場人潮相當擁擠，熱門議題的議程幾乎都是呈現爆滿的情況，以下針對一些熱門主題介紹：

(一) Hacking PLCs and Causing Havoc on Critical Infrastructures

講者 Thiago Alves 是一個 OpenPLC (open-source Programmable Logic Controller)專案的發起者，其說到目前 PLCs 的問題為非常昂貴、依賴舊有的技術、使用不安全的協定進行通訊、大部分的公司寧願用上 patch 的方式維護系統而不願意重新設計、為專有軟體(closed source)，故有 OpenPLC 這樣的專案產生。OpenPLC 是基於易使用的軟體開源可編譯邏輯控制器，其是根據 IEC 61131-3 標準建立，此標準定義了 PLC 的基本軟體架構與編譯語言。OpenPLC 主要用於工業和家庭自動化、物聯網和 SCADA 等。

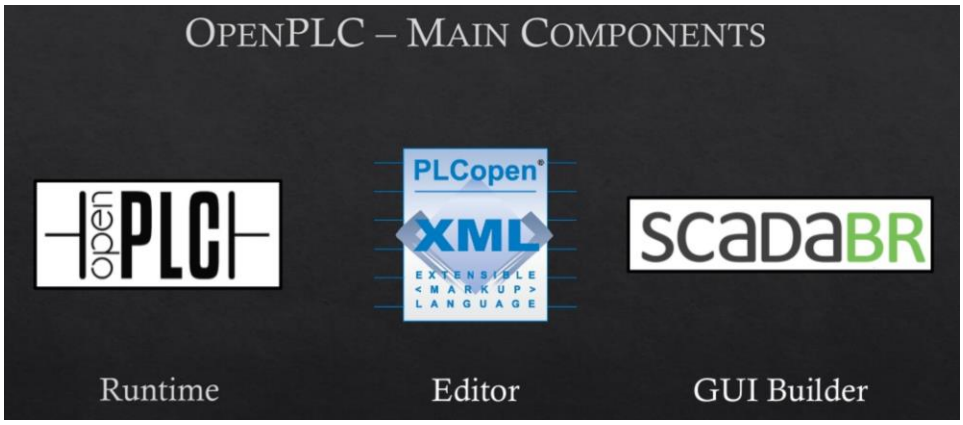

圖 12：OpenPLC 主要的構成元件

PLC 通訊用的是 SCADA 協定，其具有下列的問題：大部分協定是從舊有的 Serial

RS-485 網路衍生出來，其不具有 authentication、integrity、confidentiality。在 SCADA 協定中最常被使用的通訊協定是 MODBUS，其特性為非常簡單、以 serial networks 為基礎、其將指令編碼到函式碼中、其為開放式不需要版權。

此講者對工業控制系統的 PLC 有深入的瞭解，其利用對工業控制協定 MODBUS 的 FRAME 中 Function Code 的調整控制進行攻擊。

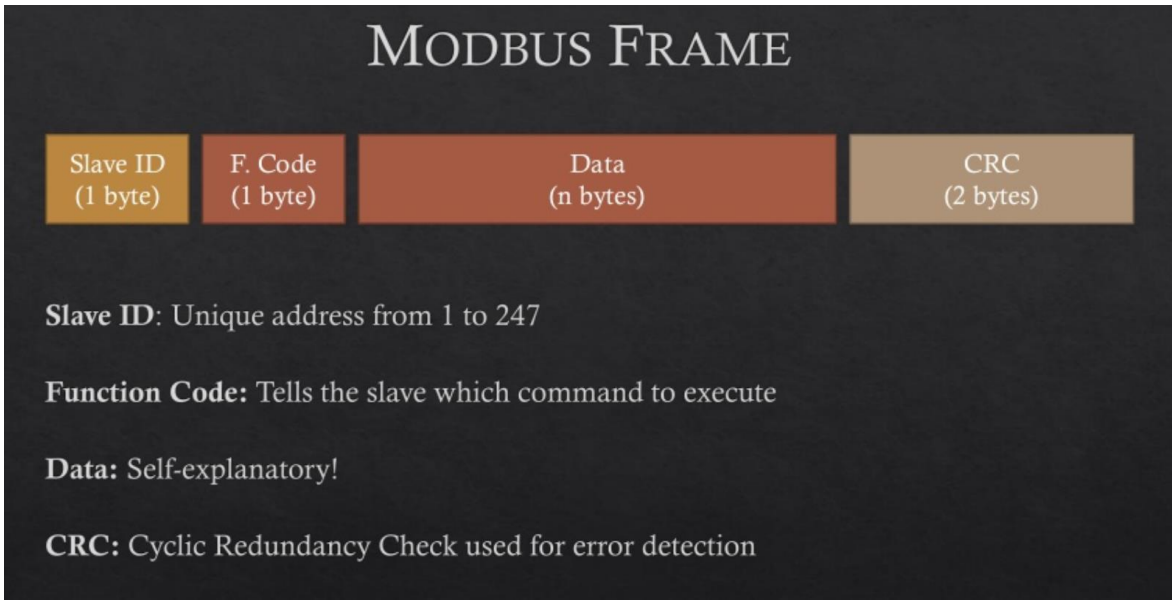

圖 13：MODBUS FRAME 示意圖

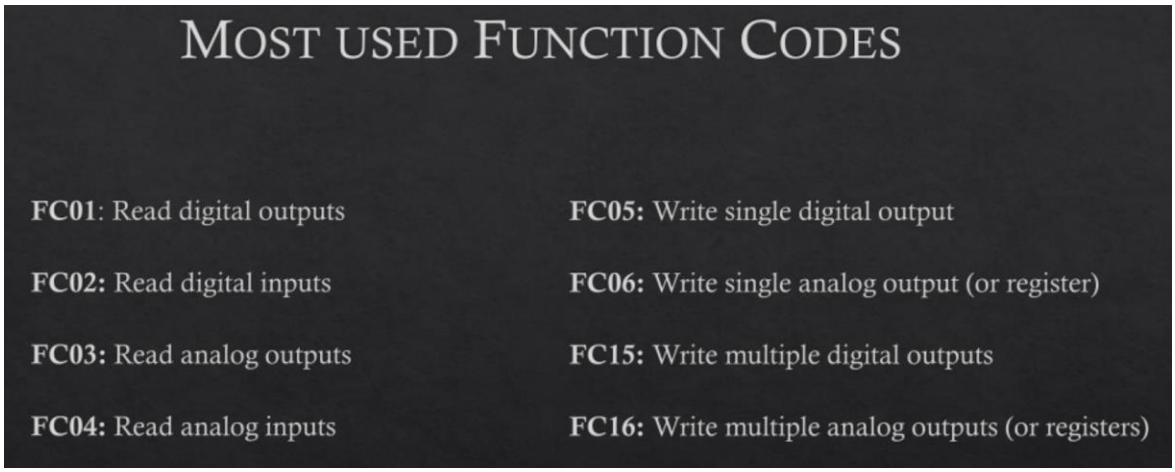

圖 14：MODBUS 協定常用的 FUNCTIONCODES

圖 14 為 MODBUS 可運用之 Function Codes，圖 13 為 MODBUS FRAME 在 TCP 上對應的位置，故攻擊者可以很容易地找到要更換 Function Codes 的地方，攻擊的步驟

為 Interruption、Interception、Modification 和 Injection。

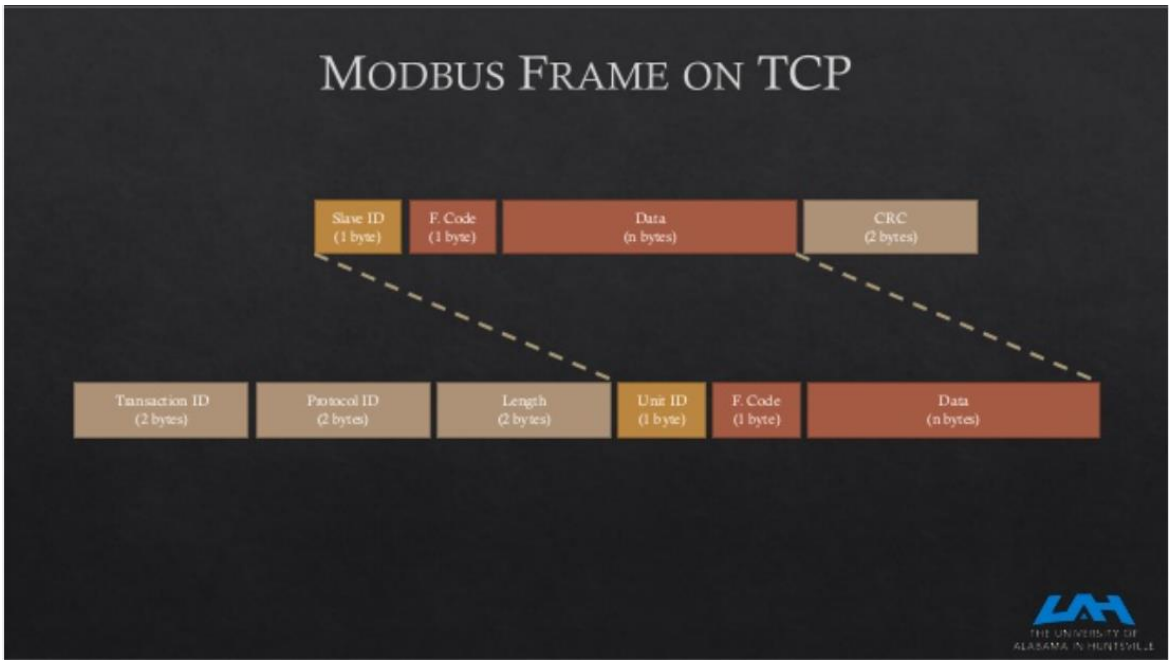

圖 15：MODBUS FRAME 在 TCP 協定上對應的位置

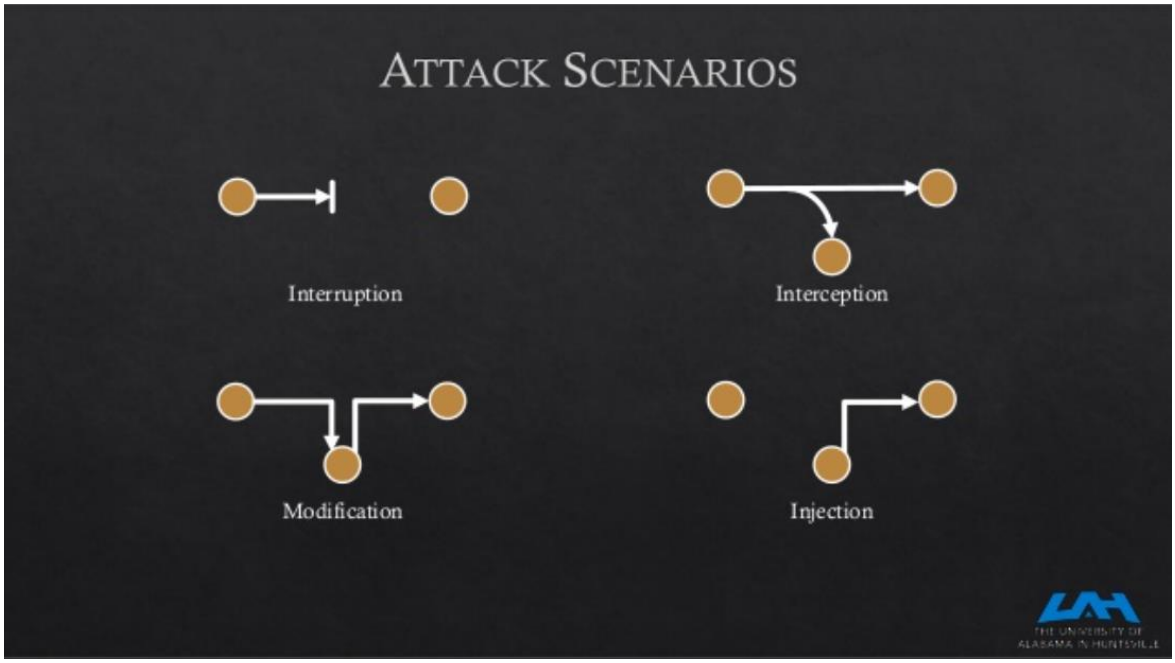

圖 16：運用 MODBUS 協定進行攻擊之情境

(二) Looking for the perfect signature: an automatic YARA rules generation algorithm in the AI-era

此講者 Ruo Ando 運用機器學習技術，使用 YARA 規則產生演算法自動化生成識別惡意程式碼的 Pattern。其指出惡意軟體的 Signature 是唯一的 Pattern，其可以明確的表示惡意程式碼，當惡意軟體產生演化時，其新的 Signature 需要經常性的重新產生。Signature 主要分為 Syntactic signatures 及 Semantic signatures 兩種。Syntactic signatures 是以字串或是指令的順序為基礎，Semantic signatures 是以抽象的程式行為為基礎。

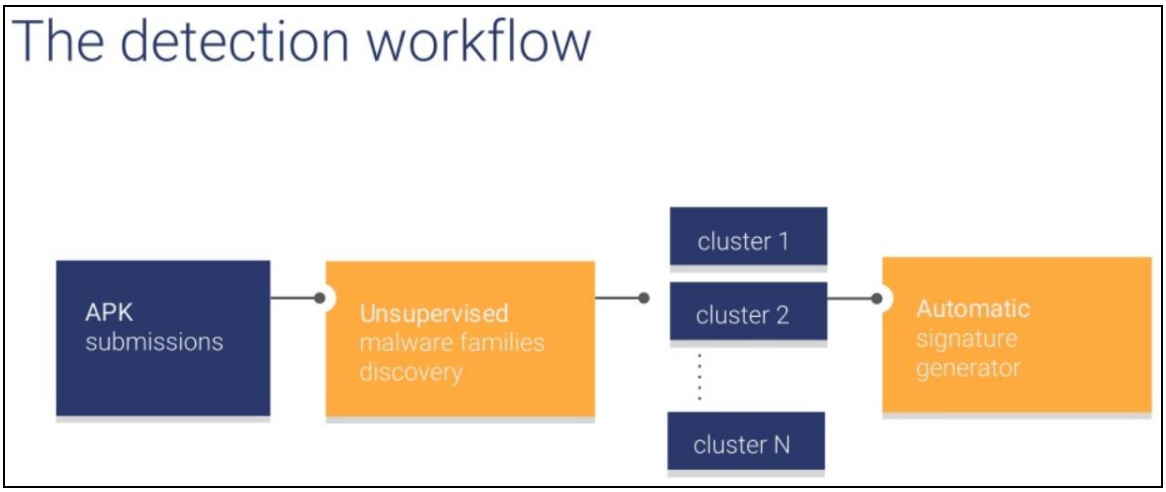

圖 17：對於惡意程式 Singnature 偵測產生的流程

這個講者其研究的目標是以 Android 平台的惡意軟體為目標，其並不只是運用機器學習進行分類而已。其運用非監督式演算法進行惡意軟體族群的尋找，接著進行分群，之後自動化的產生惡意軟體的 Signature。其屬性的分析包含了動態及靜態分析，分析的品質會影響 Signature 產生的流程。

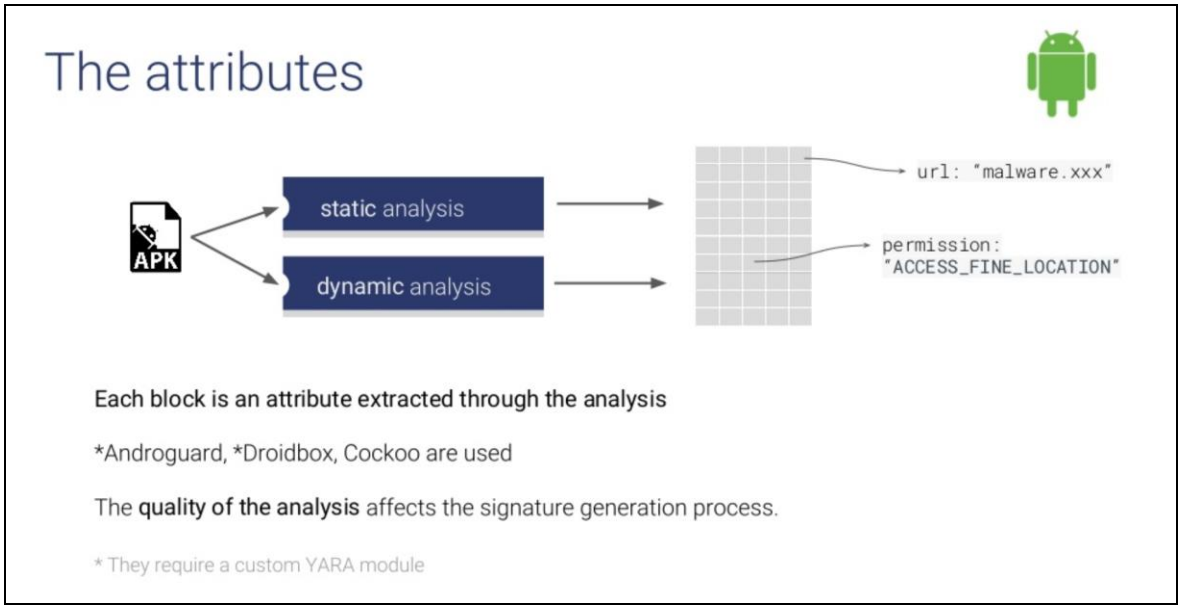

圖 18：透過分析的過程萃取出惡意程式的屬性

從展示的結果來看，其比一般方式識別出多一倍的惡意程式樣本。有鑑於新的惡意軟體變種速度非常快，防毒軟體很難保持其 Signature 的最新狀態，防毒軟體掃描時會產生大量的誤判。此講者應用人工智慧技術來解決惡意軟體 Signature 生成的問題，其期望能夠開發出一種自動產生惡意軟體 Signature 的演算法，以減少惡意程式威脅，提高防毒軟體檢測品質。其介紹 YaYaGen(YARA 規則產生器)，一個自動產生 Android 惡意軟體 Signature 的工具。其運用 Koodous 專案中的數百萬個應用程式來進行效能評估，顯示其提出的演算法可以在幾分鐘內產生辨識 0-day 惡意軟體的準確規則，優於用人工建構的惡意軟體規則。

(三) All your family secrets belong to us - Worrisome security issues in tracker apps

此演講者 Dr. Siegfried Rasthofer 公佈一些具有漏洞可用來追蹤使用者行蹤的 App，並會導致個人敏感資訊外洩。其揭露 Google Play Store 上有數以千個 App 可用於監控您及家人行蹤的 App 應用程式。

App Name	Google Play Store Installations
Couple Tracker App	5-10 m
My Family GPS Tracker KidControll GPS Tracker Rastrear Celular Por el Numero Phone Tracker By Number Couple Vow Real Time GPS Tracker Ilocatemobile	5m
Family Locator (GPS) Free Cell Tracker Rastreador de Novia Phone Tracker Free Phone Tracker Pro Rastreador de Celular Avanzado	100-500k
Rastreador de Novia Localiser un Portable avec son Numero	50-100k
Handy Orten per Handynr	10-50k
Track My Family	1k

圖 19：Google Play Store 上被大量安裝且有漏洞的 App

很多應用程式與服務都存在嚴重的資訊安全問題，這些應用程式使用自己開發的演算法而不是經過嚴謹驗證的加密技術來進行資料儲存與傳輸，甚至有些 App 根本不對他們傳輸的資料做保護，並使用未加密的 http 協定，甚至可以讓攻擊者輕易瀏覽其後端系統，其後端系統通常儲存用戶的位置訊息。有些 App 應用程式甚至可以完全繞過用戶身份驗證程序，或是透過 API 的缺陷，讓攻擊者提取到所有用戶憑證，攻擊者可進一步看到消息、圖片和位置資訊的完整通訊紀錄。總結來說，網路上不安全的 App 應用程式，可能導致使用者在他們的設備上不知不覺地安裝了間諜軟體。

對於 App 應用程式，駭客可以從 Observer、Tracking Provider 或是 Monitored Person 的位置進行攻擊，取得追蹤使用者的資料。

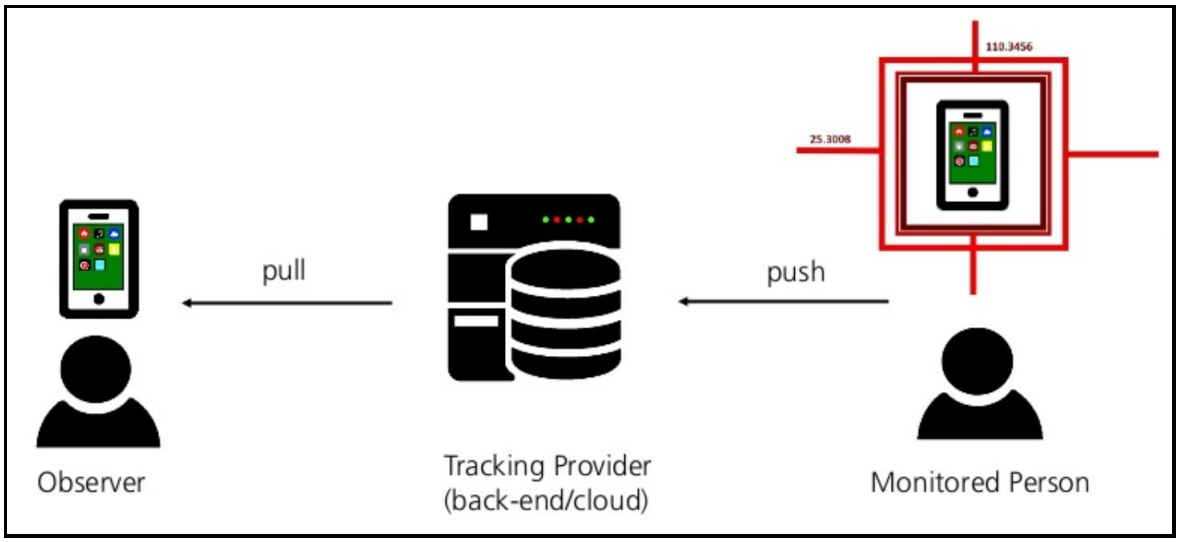

圖 20：App 應用程式，Observer、Tracking Provider 與 Monitored Person 位置示意圖

常見的 App 應用程式攻擊就是利用所謂的中間人攻擊(Man-in-the-Middle Attack)手法，是一種從中竊聽兩端通訊內容的攻擊手法，駭客不僅能從中接收資料，還能從中插入自己的資料，因此使用者所傳輸的資料不僅可能外流，更可能遭到竄改。

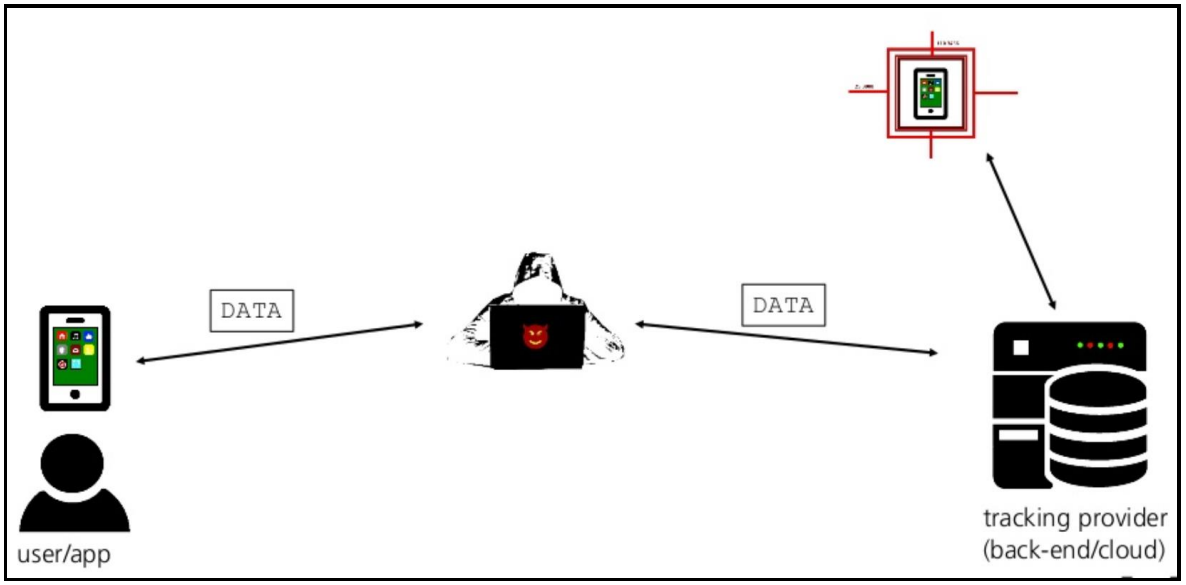

圖 21：中間人攻擊示意圖

(四)　Your Voice is My Passport

金融機構、家庭自動化產品與辦公室中越來越多使用語音聲紋辨識作為認證方式，透過運用機器學習，Text-to-Speech 技術可以使用錄音語音來產生合成的、高品質的目標音頻，透過此音頻生成技術產生足以欺騙語音驗證演算法的聲音，此講者(_delta_zero)使用免費的機器學習模型和有限的預算去驗證語音辨識系統確實有可能被針對性的 Text-to-Speech 技術模擬攻擊所欺騙。

其基本思路為使用者給予演算法所需的文本，然後其會生成該文本等效的音頻表示(例如：Mel Spectrograms)。其建構模型學習文本和音頻之間的對應關係，運用深度類神經網路(deep neural network)去分析標記(轉錄)的音頻資料。通常此模型是根據單獨一個人的聲音進行訓練，一般而言深度學習模型需要大量標記數據，所以其運用了開源資料集(例如 Blizzard, LJ Speech)。

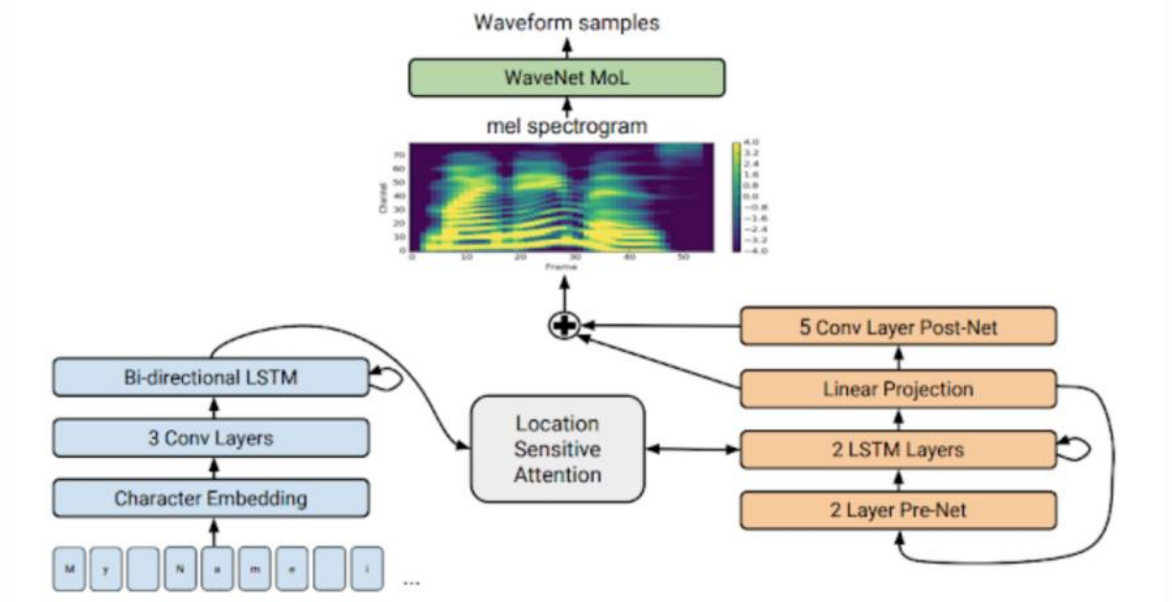

圖 15：Tacotron 的模型架構，下半部描述字母的序列與頻譜(spectrogram)的對應方式

此講者運用 Lyrebird (https://lyrebird.ai/)的工具產生目標句子之語音，並運用 Apple Siri 與 Microsoft Speaker Recognition API 進行概念性驗證(Proof of Concept)測試。在語音合成工具的選用上，幾個開源程式碼模型中，以 Tacotron 及 Wavenet 最為人所熟知。

WaveNet 可以產生逼真的擬人聲音，但在產生過程中需要大幅度的調校(tuning)。而 Tacotron 極大地簡化了這個調校過程，因此講者採用 Tacotron 進行擬人語音的產生。此方法可以用在機器學習語音辨識系統上對抗例攻擊(Adversarial Attacks)使用，或是運用此機器學習技術進行網路釣魚(Phishing)攻擊、變臉攻擊(DeepFakes)以及機器人式的社交工程攻擊(Robotics/Social Engineering)

(五) Asura: A huge PCAP file analyzer for anomaly packets detection using massive multithreading

講者 Ruo Ando 介紹他處理巨大 PCAP 檔時，使用多執行緒方法提升處理速度的研究專案。大量流量日誌的檢查給資訊安全分析人員帶來相當沉重的負擔。過去，在運用合理計算資源分析非常大的 PCAP 檔案時，很少有關於可擴展性的研究報告。Asura 是一個便利攜帶的可擴展 PCAP 文件分析器，其運用大規模多執行序檢測異常封包。Asura 的並行封包轉儲存檢查是基於各不同任務進行分解，因此處理此大型 PCAP 文件的大量執行序，並無需考慮進行資料分解時，其對應參數的選擇，Asura 旨在通過盡可能多的執行序來擴展處理大型 PCAP 文件。實驗過程中，在處理公開的 PCAP 資料集時，Asura 可以從 7000 萬(約 18GB)正常封包資料中識別出 750 個被標記為惡意的封包。Asura 檢查 7000 萬個封包，通過運用商用工作站，需要 1000-5000 多個執行序才能在大約 350-450 分鐘的時間內計算完成。

圖 16：講者介紹 Asura 這個專案背後的想法

網路攻擊或是惡意程式行為分析，大多的使用者多使用Wireshark 對 PCAP 檔進行分析，實務上確實常面臨 PCAP 資料量過大無法有效分析之問題，故此技術對於遭受網路攻擊時，需要從大量的 PCAP 檔案中查找線索應是有幫助的應用。

肆、心得及建議

一、 人才培育

經過參加本次 DEF CON 26 資訊安全年會後，深刻體認駭客技術包羅萬象，透過參加此類國際大型研討會是快速吸收新知的捷徑，建議後續可定期派員參加此類資訊安全年會，以掌握最新資訊安全知識及駭客破解技術之發展趨勢，對於人才培育建議如下：

1. 建議視參加之研討會規模決定派員之人數，以便能完整充分掌握該研討會之重要內容。此次參加 DEF CON 26 研討會發現此研討會規模極大，參加人數多達 2 萬多人，議題種類繁多，在研討會 4 天的時間裡並無法深入去聆聽瞭解各項新興的議題。
2. 駭客攻擊手法不斷更新，資訊安全專業人才的技術門檻也將跟著提高，DEF CON 研討會所展示的技術都是最新的，故本中心業務發展在採用新技術時也應一併進行資訊安全評估與資訊安全人員之教育訓練，依照其工作內容與技能需求(攻擊者與防護者角色)進行升級教育。

二、 資訊安全檢測能量提升

DEF CON 26 研討會的內容涵蓋目前新型態資訊技術之熱門資訊安全議題，參加 DEF CON 26 研討會後，深刻體會資訊安全領域並不只是侷限於傳統電腦主機與電腦網路之範疇，而是存在各種有大小型資訊系統的地方，如交通設備、智慧卡、POS 系統等等。隨著資訊科技的發展，伴隨著也衍生出新的資訊安全問題，當新技術出現時，也會帶來新的資訊安全議題，但在便利的同時，可能就忽略了安全性的議題，故當機關採用新的資訊技術進行業務推展時，也應一併評估其可能衍生之資安問題及其可能受駭範圍與對應的資安防護。對於本中心資訊安全檢測建議如下：

1. 目前 IOT 資訊設備眾多，多個主題皆在探討 IOT 設備之資訊安全，但對於本中心而言 IOT 設備之滲透測試方式尚未明確，或許可建置中心網頁、伺服器及 IOT 設備之標準弱點檢測與滲透測試流程，進行實務檢測，判斷該系統是否存在可能的資安風險。
2. 日前國家通訊傳播委員會(NCC)與經濟部共同發佈 IOT 設備資安驗證標章制度，雙方將成立物聯網資安標章，最快將於 108 年啟用，將優先用在網路攝影機的資安檢測上。此舉希望藉由政府帶頭推動物聯網資安驗證的標章制度，建立更安全且穩定的產業發展環境，透過資安技術、標準制定及嚴格檢測，來打造一個健全的物聯網資安產業的生態系，以提高 IOT 產業的國際競爭力。此外，電信管理法正式通過施行後，也將要求電信等通訊傳播業者使用的電信設備都必須通過資安檢測認證，本中心委外建置之機房也應加入此要求規範。
3. 機器學習與人工智慧的大量運用，運用對抗例(adversarial example)攻擊衍生的資訊安全問題，目前的檢測技術尚未能有效防止，故進行機器學習與人工智慧之運用時，應避免使用者有機會進行測試，以取得測試結果資料用以產生對抗例(adversarial example)進行攻擊。

三、 資訊安全情資分析技術發展

網路攻擊通常為一廣泛性或針對性的行為，但是因為網路跳板主機眾多，網路之隱匿性造成攻擊來源無法明確確認，單靠受駭電腦主機上遺留的訊息較難得到完整的訊息，故如何結合各環節之資安防護能量，透過情資交換，發現可疑活動線索，搭配分析工具，掌握攻擊手法，達到確認並阻絕攻擊來源之目標是重要課題，故除了資訊安全防禦技術之發展外，駭客攻擊情資交換也是重要方向。對於資訊安全情資分析技術發展之建議如下：

1. 資通安全管理法已經通過，其資通安全情資分享辦法第二條中明確定義資通

安全情資，包含資通系統之惡意偵察或情蒐活動、資通系統之安全漏洞、使資通系統安全控制措施無效或利用安全漏洞之方法、與惡意程式相關之資訊、資通安全事件造成之實際損害或可能產生之負面影響、用以偵測、預防或因應前五款情形、或降低其損害之相關措施、其他與資通安全事件相關之技術性資訊。故本中心應思考建構在駭客攻擊中取得完整正確的資訊安全情資之規範，以達成完整正確的資安情資交換。

2. 本部目前已推動數位證據保全作業，惟其情資之擷取僅針對 Windows 系列之 PC，建議可運用機器學習、人工智慧技術等克服大量 log 資料處理之困境，建構本中心伺服器與網路設備之快速情資擷取與分析流程。

伍、會議相關資料

一、 會議議程

8 月 **9** 日星期四

101 Track ThinSIM-based Attacks on Mobile Money Systems Rowan Phipps 
101 Track Pwning “the toughest target”: the exploit chain of winning the largest bug bounty in the history of ASR program Guang Gong
101 Track Ring 0/-2 Rootkits: Bypassing Defenses Alexandre Borges
101 Track A Journey Into Hexagon: Dissecting a Qualcomm Baseband Seamus Burke
101 Track Wagging The Tail - Covert Passive Surveillance And How To Make Their Life Difficult Si & Agent X
101 Track Building the Hacker Tracker Whitney Champion & Seth Law
101 Track

DC 101 PANEL Panel

8 月 10 日星期五

101 Track	Track One	Track Two	Track Three
Synfuzz: Building a Grammar Based Re-targetable Test Generation Framework Joe Rozner 	Welcome To DEF CON & Badge Maker Talk The Dark Tangent 	De-anonymizing Programmers from Source Code and Binaries Rachel Greenstadt & Dr. Aylin Caliskan	Securing our Nation's Election Infrastructure Jeanette Manfra
101 Track	Track One	Track Two	Track Three
Synfuzz: Building a Grammar Based Re-targetable Test Generation Framework cont.	Welcome To DEF CON & Badge Maker Talk cont.	De-anonymizing Programmers from Source Code and Binaries cont.	Please do not Duplicate: Attacking the Knox Box and Other Keyed Alike Systems m010ch_ 
101 Track	Track One	Track Two	Track Three
An Attacker Looks at Docker: Approaching Multi-Container Applications Wesley McGrew 	NSA Talks Cybersecurity Rob Joyce	One-liners to Rule Them All egypt & William Vu 	Lora Smart Water Meter Security Analysis Yingtao Zeng, Lin Huang, & Jun Li 
101 Track	Track One	Track Two	Track Three
It's Assembler, Jim, but not as we know it: (ab)using binaries	Vulnerable Out of the Box: An Evaluation of Android Carrier	Breaking Paser Logic: Take Your Path Normalization Off and	Who Controls the Controllers—Hacking Crestron IoT

from embedded devices for fun and profit Morgan ``indrora'' Gangwere 	Devices Ryan Johnson & Angelos Stavrou 	Pop 0days Out! Orange Tsai 	Automation Systems Ricky "HeadlessZeke" Lawshae 
101 Track Dissecting the Teddy Ruxpin: Reverse Engineering the Smart Bear zenofex 	Track One Compromising Online Accounts by Cracking Voicemail Systems Martin Vigo 	Track Two Finding Xori: Malware Analysis Triage with Automated Disassembly Amanda Rousseau & Rich Seymour 	Track Three One-Click to OWA William Martin 
101 Track You can run, but you can't hide. Reverse engineering using X-Ray George Tarnovsky	Track One Dragnet—Your Social Engineering Sidekick Truman Kain 	Track Two Hacking the Brain: Customize Evil Protocol to Pwn an SDN Controller Feng Xiao, Jianwei Huang, & Peng Liu 	Track Three Fasten your seatbelts: We are escaping iOS 11 sandbox! Min (Spark) Zheng & Xiaolong Bai 
101 Track UEFI Exploitation for the Masses Mickey Shkatov & Jesse Michael 	Track One GOD MODE UNLOCKED: Hardware Backdoors in [redacted] x86 CPUs Christopher Domas	Track Two 4G—Who is paying your cellular phone bill? Dr. Silke Holtmanns & Isha Singh	Track Three Revolting Radios Michael Ossmann & Dominic Spill 

			
101 Track Weaponizing Unicode: Homographs Beyond IDNs The Tarquin 	Track One Bypassing Port-Security In 2018: Defeating MacSEC and 802.1x-2010 Gabriel Ryan 	Track Two Playback: a TLS 1.3 story Alfonso García Alguacil & Alejo Murillo Moya 	Track Three Privacy Infrastructure, Challenges and Opportunities yawnbox
101 Track Automated Discovery of Deserialization Gadget Chains Ian Haken 	Track One Your Peripheral Has Planted Malware—An Exploit of NXP SOCs Vulnerability Yuwei Zheng, Shaokun Cao, Yunding Jian, & Mingchuang Qun 	Track Two Practical & Improved Wifi MitM with Mana singe 	Track Three Your Voice is My Passport _delta_zero & Azeem Aqil 
101 Track Your Bank's Digital Side Door Steven Danneman 	Track One I'll See Your Missile and Raise You A MIRV: An overview of the Genesis Scripting Engine Alex Levinson & Dan Borges 	Track Two The L0pht Testimony, 20 Years Later (and Other Things You Were Afraid to Ask) Elinor Mills, DilDog, Joe Grand (Kingpin), Space Rogue, Mudge, Silicosis, John Tan & Weld Pond	Track Three Reverse Engineering, hacking documentary series Michael Lee Nirenberg & Dave Buchwald 

8 月 11 日星期六

101 Track	Track One	Track Two	Track Three
Through the Eyes of the Attacker: Designing Embedded Systems Exploits for Industrial Control Systems Marina Krotofil & Jos Wetzels 	It WISN't Me, Attacking Industrial Wireless Mesh Networks Erwin Paternotte & Mattijs van Ommeren 	You're just complaining because you're guilty: A DEF CON Guide to Adversarial Testing of Software Used In the Criminal Justice System Dr. Jeanna N. Matthews, Nathan Adams, & Jerome Greco 	You may have paid more than you imagine—Replay Attacks on Ethereum Smart Contracts Zhenxuan Bai, Yuwei Zheng, Senhua Wang, & Kunzhe Chai 
101 Track	Track One	Track Two	Track Three
Hacking PLCs and Causing Havoc on Critical Infrastructures Thiago Alves 	Exploiting Active Directory Administrator Insecurities Sean Metcalf 	Compression Oracle Attacks on VPN Networks Nafeez 	Jailbreaking the 3DS through 7 years of hardening smea 
101 Track	Track One	Track Two	Track Three
Building Absurd Christmas Light Shows Rob Joyce	Tineola: Taking a Bite Out of Enterprise Blockchain Stark Riedesel & Parsia Hakimian 	You'd better secure your BLE devices or we'll kick your butts ! Damien "virtualabs" Cauquil 	Ridealong Adventures—Critical Issues with Police Body Cameras Josh Mitchell 

101 Track	Track One	Track Two	Track Three
One Step Ahead of Cheaters—Instrumenting Android Emulators Nevermoe 	In Soviet Russia Smartcard Hacks You Eric Sesterhenn 	Reaping and breaking keys at scale: when crypto meets big data Yolan Romailler & Nils Amiet 	Looking for the perfect signature: an automatic YARA rules generation algorithm in the AI-era Andrea Marcelli 
101 Track	Track One	Track Two	Track Three
House of Roman—a "leakless" heap fengshui to achieve RCE on PIE Binaries Sanat Sharma 	The ring 0 façade: awakening the processor's inner demons Christopher Domas 	Detecting Blue Team Research Through Targeted Ads 0x200b	Infecting The Embedded Supply Chain Zach & Alex 
101 Track	Track One	Track Two	Track Three
Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices Dennis Giese 	SMBetray—Backdooring and breaking signatures William Martin 	Digital Leviathan: a comprehensive list of Nation-State Big Brothers (from huge to little ones Eduardo Izycki & Rodrigo Colli	Playing Malware Injection with Exploit thoughts Sheng-Hao Ma 
101 Track	Track One	Track Two	Track Three
Having fun with IoT: Reverse Engineering and Hacking of Xiaomi IoT Devices Cont.	**SMBetray—Backdooring and breaking signatures** Cont.	Sex Work After SESTA/FOSTA Maggie Mayhem	Fire & Ice: Making and Breaking macOS Firewalls Patrick Wardle

			
101 Track Project Interceptor: avoiding counter-drone systems with nanodrones David Melendez Cano 	Track One All your math are belong to us sghctoma 	Track Two Reverse Engineering Windows Defender's Emulator Alexei Bulazel 	Track Three Booby Trapping Boxes Ladar Levison & hon1nbo 
101 Track Outsmarting the Smart City Daniel "unicornFurnace" Crowley, Mauro Paredes, & Jen "savagejen" Savage 	Track One 80 to 0 in under 5 seconds: Falsifying a medical patient's vitals Douglas McKee 	Track Two All your family secrets belong to us—Worrisome security issues in tracker apps Dr. Siegfried Rasthofer, Stephan Huber, & Dr. Steven Arzt 	Track Three Inside the Fake Science Factory Dr Cindy Poppins (AKA Svea Eckert), Dr Dade Murphy (AKA Suggy), & Professor Dr Edgar Munchhausen (AKA Till Krause)
101 Track Closed	Track One The Road to Resilience: How Real Hacking Redeems this Damnable Profession Richard Thieme	Track Two Relocation Bonus: Attacking the Windows Loader Makes Analysts Switch Careers Nick Cano 	Track Three **Inside the Fake Science Factory** Cont.

8 月 12 日星期日

101 Track	Track One	Track Two	Track Three
The Mouse is Mightier than the Sword Patrick Wardle 	Rock appround the clock: Tracking malware developers by Android "AAPT" timezone disclosure bug Sheila A. Berta & Sergio De Los Santos 	Defending the 2018 Midterm Elections from Foreign Adversaries Joshua M Franklin & Kevin Franklin 	For the Love of Money: Finding and exploiting vulnerabilities in mobile point of sales systems Leigh-Anne Galloway & Tim Yunusov 
101 Track	Track One	Track Two	Track Three
Searching for the Light: Adventures with OpticSpy Joe Grand 	Breaking Extreme Networks WingOS: How to own millions of devices running on Aircrafts, Government, Smart cities and more Josep Pi Rodriguez 	Politics and the Surveillance State. The story of a young politician's successful efforts to fight surveillance and pass the nation's strongest privacy bills Daniel Zolnikov	Demystifying MS17-010: Reverse Engineering the ETERNAL Exploits zerosum0x0 
101 Track	Track One	Track Two	Track Three
Breaking Smart Speakers: We are Listening to You Wu HuiYu & Qian Wenxiang 	Last mile authentication problem: Exploiting the missing link in end-to-end secure communication Thanh Bui & Siddharth Rao	Attacking the macOS Kernel Graphics Driver Yu Wang 	Designing and Applying Extensible RF Fuzzing Tools to Expose PHY Layer Vulnerabilities Matt Knight & Ryan Speers

			
101 Track Trouble in the tubes: How internet routing security breaks down and how you can do it at home Lane Broadbent 	Track One Man-In-The-Disk Slava Makkaveev 	Track Two Micro-Renovator: Bringing Processor Firmware up to Code Matt King 	Track Three barcOwned—Popping shells with your cereal box Michael West & magicspacekiwi (Colin Campbell) 
101 Track **Trouble in the tubes: How internet routing security breaks down and how you can do it at home** Cont.	Track One Asura: A huge PCAP file analyzer for anomaly packets detection using massive multithreading Ruo Ando 	Track Two Lost and Found Certificates: dealing with residual certificates for pre-owned domains Ian Foster & Dylan Ayrey 	Track Three Edge Side Include Injection: Abusing Caching Servers into SSRF and Transparent Session Hijacking Idionmarcil 
101 Track Betrayed by the keyboard: How what you type can give you away Matt Wixey	Track One Your Watch Can Watch You! Gear Up for the Broken Privilege Pitfalls in the Samsung Gear Smartwatch Dongsung Kim & Hyoung-Kee Choi	Track Two Hacking BLE Bicycle Locks for Fun and a Small Profit Vincent Tan 	Track Three One bite and all your dreams will come true: Analyzing and Attacking Apple Kernel Drivers Xiaolong Bai & Min (Spark) Zheng 

			
101 Track CLOSED	Track One PANEL: DEF CON GROUPS Brent White (B1TK1LL3R), Jeff Moss (The Dark Tangent), Jayson E. Street, S0ups, Tim Roberts (byt3boy), Casey Bourbonnais, & April Wright	Track Two What the Fax!? Yaniv Balmas & Eyal Itkin 	Track Three Fuzzing Malware For Fun & Profit. Applying Coverage-guided Fuzzing to Find and Exploit Bugs in Modern Malware Maksim Shudrak 
101 Track CLOSED	Track One DEF CON 26 Closing Ceremonies The Dark Tangent	Track Two CLOSED	Track Three CLOSED

二、 參考資料

1. DEF CON 26 官方網站，https://www.defcon.org/html/defcon-26/dc-26-index.html
2. DEF CON 26 議程表，https://www.defcon.org/html/defcon-26/dc-26-schedule.html