出國報告（出國類別：開會）

出席「國際駭客年會(DEF CON 26)」報告

服務機關：國家通訊傳播委員會
姓名職稱：林永裕 科長
派赴國家：美國（拉斯維加斯）
出國期間：107 年 8 月 8 日至 107 年 8 月 15 日
報告日期：107 年 11 月 12 日

摘要

DEF CON 是國際最知名的資安盛會，每年 8 月固定在美國拉斯維加斯舉行，吸引來自不同國家的駭客、資安專家、執法人員，甚至有犯罪背景的人士參加。會議期間，除了多場專題演講外，同時有各種針對不同主題的「主題村（Village）」進行研討及展示，以及資安攻防奪旗（Catch The Flag, CTF）競賽，我國 HITCON 團隊在今（107）年取得第三名的佳績。

今年 8 月 3 日，就在 DEF CON 26 會議舉辦的 6 天前，上市公司台積電發生資安事件，導致大規模感染而影響生產線運作，震撼了全世界。這個事件讓大眾瞭解，即便是台積電這種相當重視資安的高科技公司，仍然有可能發生資安事件。因此，隨著物聯網的發展，各種連網應用將拓展到各行各業，相關資安問題也會隨著影響幾乎所有人的生活。資安將不再只是電腦病毒的單純問題，而是民眾應該重視並隨時做好資安防護的工作。

目次

壹、目的

DEF CON 是世界最有名的資安相關會議，會議有各種研討會及技術展式，以及各種系統的漏洞揭露。電信網路屬於關鍵基礎設施，本會身為主管機關，為蒐集最新資安相關資訊、技術及未來趨勢，做為推動資安防護工作及制定相關政策之參考，因此需派員參與會議。

以台積電發生重大資安事件為例。該公司因未確實執行標準作業程序，使帶有 WannaCry 變種病毒的新機臺，在未經網路隔離及防毒系統處理的人為疏忽下，就連接到台積電的生產網路當中，再加上該公司的生產網路全部連結在一起，造成竹科、中科、南科廠區的相關設備受到大規模感染。這次事件使該公司生產機臺停擺 3 天，影響當季營收約 2%，損失高達新臺幣 52 億，是我國史上最大資安事故。

由台積電的案例可以瞭解，即使相當重視資安的高科技公司，也會因為未確實做好資安防護工作，而造成重大的損失。尤其物聯網持續發展，不只高科技產業，將來幾乎所有的事物都可能會連上網路，自然也就提高了資安的風險，而一旦涉及民眾生命財產安全的關鍵基礎設施，發生嚴重的資安事件，其後果將是難以想像。

為了瞭解最新資安技術發展及趨勢，確實有必要積極參與資安相關國際會議，透過交流與合作，來提升我國資安防護的能量，以維護產業發展，保障民眾生活以及國家安全。

貳、過程

一、會議介紹

(一)DEF CON 會議簡介：

DEF CON 是全球最知名的資安技術會議之一，由 Dark Tangent（本名 Jeff Moss）於 1993 年 6 月創立，每年固定 8 月上旬在美國內華達州拉斯維加斯舉行，它也是最早的網路安全會議之一，吸引全球許多駭客、廠商、政府機關、學界等資安專業人員，前往共襄盛舉。今年是第 26 屆（DEF CON 26）會議。

DEF CON 會議內容豐富，包含駭客攻擊手法展演、駭客軟硬體設備展售、各項軟硬體的最新漏洞發表，及國際資訊安全發展趨勢。與會者除透過交流及分享資訊安全新知與技術，也有機會參與會議期間各種不同的 CTF 競賽。近幾年為培養國內資安專業人才，我國 HITCON 團隊均派員參加比賽，也都有不錯的成績。

(二)DEF CON 26 會議內容：

本屆會議於 107 年 8 月 9 日至 12 日，在美國拉斯維加斯 Caesars Palace 飯店及 Flamingo 飯店舉行。會議期間同時舉辦多場演講及展演，以及多達 200 場以上的研討會，和 25 個「主題村（Village）」，各主題村也各自舉行小型研討會、演講或訓練課程。由於今年適逢美國期中選舉，因此以美國投票系統為主題的 Village 就受到外界矚目，也吸引當地媒體的報導。尤其在以兒童為主要參與對象的 r00tz Asylum Village，在會議期間教導與會的小朋友如何駭進模擬的投票系統，就引起媒體不小的討論。

由於與會者無需事前報名，因此主辦單位不諱言可能有不肖人士參加會議，創辦人 Jeff Moss 在閉幕式上也公布數起騷擾及偷竊事件的統計資料。DEF CON 26 議程詳如下列：

第一天（8 月 9 日）議程

SPEAKING SCHEDULE

FIRESIDE HAX

FRIDAY

OH NOES! A ROLE PLAYING INCIDENT RESPONSE GAME

20:00-22:00 in Roman Chillout

Bruce Potter & Robert Potter

DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION

20:00-22:00 in Octavius 9

Christian "quaddi" Dameff MD & Jeff "r3plicant" Tully MD

DISRUPTING THE DIGITAL DYSTOPIA OR WHAT THE HELL IS HAPPENING IN COMPUTER LAW

20:00-22:00 in Octavius 13

Nathan White & Nate Cardozo

SATURDAY

EFF FIRESIDE HAX (AKA ASK THE EFF)

20:00-22:00 in Roman Chillout

BEYOND THE LULZ: BLACK-HAT TROLLING, WHITE-HAT TROLLING, AND HACKING THE ATTENTION LANDSCAPE

20:00-22:00 in Octavius 9

Matt Goerzen & Jeanna Matthews

PRIVACY IS EQUALITY: AND IT'S FAR FROM DEAD

20:00-22:00 in Octavius 13

Sarah St.Vincent

-THURSDAY-

	101 Track
10:00	**ThinSIM-based Attacks on Mobile Money Systems** Rowan Phipps
11:00	**Pwning "the toughest target": the exploit chain of winning the largest bug bounty in the history of ASR program** Guang Gong
12:00	**Ring 0/-2 Rootkits: bypassing defenses** Alexandre Borges
13:00	**A Journey Into Hexagon: Dissecting a Qualcomm Baseband** Seamus Burke
14:00	**Wagging The Tail - Covert Passive Surveillance And How To Make Their Life Difficult** Si & Agent X
15:00	**Building the Hacker Tracker** Whitney Champion & Seth Law
15:30	**DC 101 PANEL** (Until 16:45)

第二天（8 月 10 日）議程

-FRIDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	**Synfuzz: Building a Grammar Based Re-targetable Test Generation Framework** Joe Rozner	**Badge/DT Welcome**	**De-anonymizing Programmers from Source Code and Binaries** Rachel Greenstadt & Dr. Aylin Caliskan	**Securing our Nation's Election Infrastructure** Jeanette Manfra
10:30				**Please do not Duplicate: Attacking the Knox Box and other keyed alike systems** m010ch_
11:00	**An Attacker Looks at Docker: Approaching Multi-Container Applications** Wesley McGrew	**NSA Talks Cybersecurity** Rob Joyce	**One-liners to Rule Them All** Egypt	**Lora Smart Water Meter Security Analysis** Yingtao Zeng
12:00	**It's Assembler, Jim, but not as we know it: (ab) using binaries from embedded devices for fun and profit** Morgan "indrora" Gangwere	**Vulnerable Out of the Box: An Evaluation of Android Carrier Devices** Ryan Johnson	**Breaking Paser Logic: Take Your Path Normalization Off and Pop 0days Out!** Orange Tsai	**Who Controls the Controllers - Hacking Crestron IoT Automation Systems** Ricky "HeadlessZeke" Lawshae
13:00	**Dissecting the Teddy Ruxpin: Reverse Engineering the Smart Bear** Zenofex	**Compromising online accounts by cracking voicemail systems** Martin Vigo	**Finding Xori: Malware Analysis Triage with Automated Disassembly** Amanda Rousseau & Rich Seymour	**One-Click to OWA** William Martin
13:30	**You can run, but you can't hide. Reverse engineering using X-Ray.** George Tarnovsky	**Dragnet - Your Social Engineering Sidekick** Truman Kain	**Attacking the Brain: Customize Evil Protocol to Pwn an SDN Controller** Feng Xiao	**Fasten your seatbelts: We are escaping iOS 11 sandbox!** Min Zheng
14:00	**UEFI exploitation for the masses** Mickey Shkatov	**GOD MODE UNLOCKED - hardware backdoors in x86 CPUs** Christopher Domas	**4G - Who is paying your cellular phone bill?** Dr. Silke Holtmanns & Isha Singh	**Revolting Radios** Michael Ossmann & Dominic Spill
15:00	**Weaponizing Unicode: Homographs Beyond IDNs** The Tarquin	**Bypassing Port-Security In 2018: Defeating MacSEC and 802.1x-2010** Gabriel Ryan	**Playback: a TLS 1.3 story** Alfonso Garcia Alguacil & Alejo Murillo	**Privacy infrastructure, challenges and opportunities** yawnbox
16:00	**Automated Discovery of Deserialization Gadget Chains** Ian Haken	**Your Peripheral Has Planted Malware - An Exploit of NXP SOCs Vulnerability** Yuwei Zheng	**Practical & Improved Wifi MitM with Mana** Singe	**Your Voice is My Passport** _delta_zero
17:00	**Your Bank's Digital Side Door** Steven Danneman	**I'll See Your Missile and Raise You A MIRV: An overview of the Genesis Scripting Engine** Alex Levinson	**Panel - The L0pht Testimony, 20 Years Later (and Other Things You Were Afraid to Ask)**	**Reverse Engineering, hacking documentary series** Michael Lee Nirenberg

第三天（8 月 11 日）議程

-SATURDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	**Through the Eyes of the Attacker: Designing Embedded Systems Exploits for Industrial Control Systems** Marina Krotofil	**It WISN't me, attacking industrial wireless mesh networks** Erwin Paternotte	**You're just complaining because you're guilty: A Guide for Citizens and Hackers to Adversarial Testing of Software Used In the Criminal Justice System** Jeanna Matthews	**You may have paid more than you imagine - Replay Attacks on Ethereum Smart Contracts** Zhenxuan Bai
11:00	**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
12:00	**Building Absurd Christmas Light Shows** Rob Joyce	**Tineola: Taking a Bite Out of Enterprise Blockchain** Stark Riedesel	**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
13:00	**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	**Looking for the perfect signature: an automatic YARA rules generation algorithm in the AI-era** Andrea Marcelli
13:30	**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
14:00	**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	**Playing Malware Injection with Exploit thoughts** Sheng-Hao Ma
14:30			**Sex Work After SESTA/FOSTA** Maggie Mayhem	**Fire & Ice: Making and Breaking macOS Firewalls** Patrick Wardle
15:00	**Project Interceptor: avoiding counter-drone systems with nanodrones** David Melendez Cano	**All your math are belong to us** sghctoma	**Reverse Engineering Windows Defender's Emulator** Alexei Bulazel	**Booby Trapping Boxes** Ladar Levison
16:00	**Outsmarting the Smart City** Daniel "unicornFurnace" Crowley	**80 to 0 in under 5 seconds: Falsifying a medical patient's vitals** Douglas McKee	**All your family secrets belong to us – Worrisome security issues in tracker apps** Dr. Siegfried Rasthofer	**Inside the Fake Science Factory** Dr. Isabella Stein
17:00	**CLOSED**	**The Road to Resilience: How Real Hacking Redeems this Damnable Profession** Richard Thieme	**Relocation Bonus: Attacking the Windows Loader Makes Analysts Switch Careers** Nick Cano	

第四天（8 月 12 ）議程

-SUNDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	**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	**For the Love of Money: Finding and exploiting vulnerabilities in mobile point of sales systems** Leigh-Anne Galloway
11:00	**Searching for the Light: Adventures with OpticSpy** Joe Grand (Kingpin)	**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
12:00	**Breaking Smart Speakers: We are Listening to You.** Wu HuiYu	**Last mile authentication problem: Exploiting the missing link in end-to-end secure communication** Thanh Bui	**Attacking the macOS Kernel Graphics Driver** Yu Wang	**Designing and Applying Extensible RF Fuzzing Tools to Expose PHY Layer Vulnerabilities** Matt Knight
13:00	**Trouble in the tubes: How internet routing security breaks down and how you can do it at home** Lane Broadbent	**Man-In-The-Disk** Slava Makkaveev	**Micro-Renovator: Bringing Processor Firmware up to Code** Matt King	**barcOwned - Popping shells with your cereal box** Michael West
13:30		**Asura: A huge PCAP file analyzer for anomaly packets detection using massive multithreading** Ruo Ando	**Lost and Found Certificates: dealing with residual certificates for pre-owned domains** Ian Foster	**Edge Side Include Injection: Abusing Caching Servers into SSRF and Transparent Session Hijacking** Idionmarcil
14:00	**Betrayed by the keyboard: How what you type can give you away** Matt Wixey	**Your Watch Can Watch You! Gear Up for the Broken Privilege Pitfalls in the Samsung Gear Smartwatch** Dongsung Kim	**Hacking BLE Bicycle Locks for Fun and a Small Profit** Vincent Tan Kwang Yue	**One bite and all your dreams will come true: Analyzing and Attacking Apple Kernel Drivers** Xiaolong Bai & Min Zheng
15:00	**Closed**	**Panel** DCGroups	**What the Fax!?** Yaniv Balmas	**Fuzzing Malware For Fun & Profit. Applying Coverage-guided Fuzzing to Find and Exploit Bugs in Modern Malware** Maksim Shudrak
16:30	**Closed**	**Closing Ceremonies**	**Closed**	**Closed**
17:00				

主辦單位估計本屆會議有 2 萬 8 千人以上參加（上屆為 2 萬 5 千人），研討會有 2 千人以上註冊參加，小朋友則有 300 人以上參加，25 個主題村數量是去年的 2 倍。

(三)CTF 競賽：

DEF CON 會議一項重要的活動就是 CTF 競賽，我國在本屆首度有兩個隊伍參賽，除了已經在 103 年獲得該比賽全球第 2 名好成績，並連續於 104 年、105 年以及去年分別獲得全球第 4 名、第 4 名和第 2 名好成績的臺灣 HITCON 戰隊，連續第 5 次入圍決賽外，也首度有一個由臺灣大學 Balsn、交通大學 Bamboofox、中央大學 DoubleSigma 以及中科院 Kerkeryuan 等 4 個聯隊組成的新隊伍 BSF，以預賽第 22 名的成績，首度參加 DEF CON CTF 決賽。

今年有來自各國共 25 隊參賽，由全新主辦單位 O.O.O.（Order-of-the-Overflow）的 CTF 賽制和過往有些不同，不再是單純的網路攻防（Attack and Defense），而是混合 King of the Hill 的賽制，考驗參賽隊伍除了挖漏洞的能力外，也同樣考驗防守的能力。因為參賽隊伍眾多，包括網路和出題的伺服器都出現服務中斷的現象，明年應該只會維持過往 12～15 個隊伍參賽的傳統。

經過激烈的競賽後，結果由韓國隊 DEFKOROOT 獲得冠軍，美國隊 PPP 獲得第二名，臺灣 HITCON 戰隊獲得第三名的好成績，我國資安新血戰隊 BFS 此次參賽的成績表現不俗，初試啼聲就獲得第 12 名的好成績。

圖 1、CTF 競賽會場情形

圖 2、我國 HITCON 戰隊（來源：iThome）

Team Name	Overall Points	Attack	Defense	King of the Hill
DEFKOR0OT	940	400.0	376.577	163.676
PPP	914	314.25	400.0	200.0
HITCON	726	214.787	327.928	183.807
A0E	712	275.093	400.0	37.199
Sauercloud	672	175.299	331.532	165.864
Tea Deliverers	616	229.492	349.55	37.637
mhackeroni	547	182.239	351.351	14.223
binja	518	155.638	313.514	49.672
Dragon Sector	398	63.28	198.198	137.199
RPISEC	397	101.776	290.09	6.127
Samurai	396	102.272	228.829	65.646
BFS	384	117.142	255.856	11.816

圖 3、CTF 決賽成績（來源：Twitter）

(四)會議花絮：

DEF CON 26 會議有許多有趣的事物值得一提。首先是與會者在會議現場完成報名後，會拿到一個有閃爍燈光的電子入場證，此證件雖然沒有特殊作用，但可和電腦或其他入場證連接，發出不同的燈光模式。（如下圖）

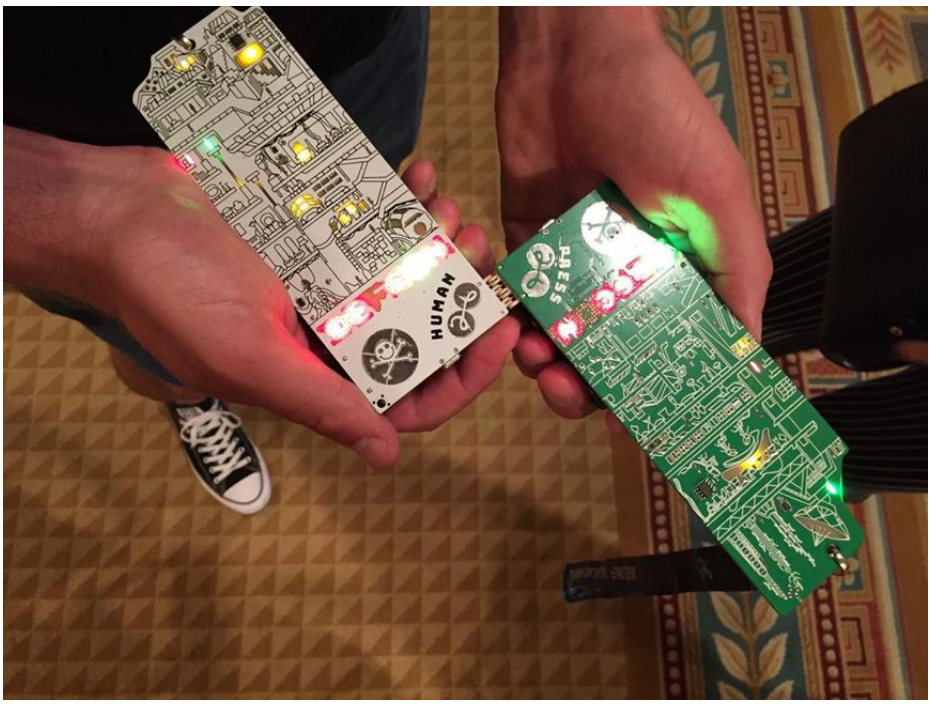

圖 4、電子入場證可相互連接（來源：DEF CON 26 官網）

會議期間可見到許多父母帶著子女全家一起與會，也有人帶著寵物出席會議。有人帶著來自不同主題村或自己精心設計的臂章（通常會發光），或是在造型打扮上別出心裁。另有駭客因不滿飯店空調不夠冷，在 Twitter 上發文教大家如何破解溫度設定。特別的是，會議期間並沒有賭場受到駭客攻擊的消息傳出。此外，會場有專門販售駭客的軟硬體工具，甚至是萬能鑰匙（如下圖）

圖 5、駭客工具販售會場

圖 6、各種萬能鑰匙

還有一個值得注意的地方，是會場會公布「綿羊榜」(Wall of Sheep)。所謂綿羊榜是指那些未做好資安防護的與會者，當他的帳號密碼資料遭到駭客截取時，就會被公布到綿羊榜的名單中。(如下圖)

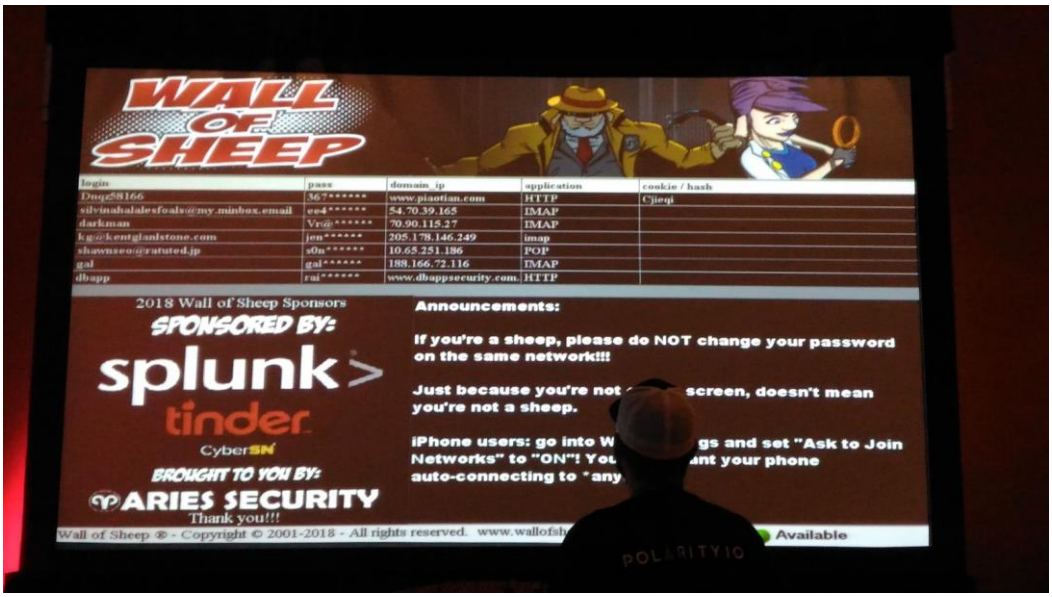

圖 7、綿羊榜

二、會議重點摘要

(一) Vulnerable Out of the Box: An Evaluation of Android Carrier Devices

1、講者：Ryan Johnson (Director of Research at Kryptowire)及 Angelos Stavrou

(CEO at Kryptowire)。

2、時間：8 月 10 日中午 12 點

3、摘要：

來自 Kryptowire 公司的講者說明該公司針對 6 家美國電信業者銷售的高、低階 Android 手機進行分析，在 25 款 Android 手機出廠時的韌體或預載程式上發現大大小小 35 個漏洞，包括任意程式執行、取得數據機與程式紀錄、移除裝置使用者資料、讀取或變更裝置用戶簡訊等等。輕微的漏洞只會造成裝置當機，但嚴重的漏洞則會讓駭客取得裝置的最高權限。

講者說明造成這些漏洞主要的原因，是因為供應鏈中的成員想要進行客製化、加入自己的程式或程式碼，卻同時擴大了攻擊面，而提高軟體出錯的可能性。韌體或預載程式上的漏洞將使消費者在安裝其它程式或進行無線通訊之前就已曝露在安全風險中，更嚴重的是，針對韌體的攻擊程式得以繞過 Android 的各種防禦機制，使威脅偵測、防毒軟體或其它技術無法偵測應用程式層背後的漏洞，因而無法抵抗韌體攻擊。

例如中興的 ZMAX Pro 允許駭客取得裝置用戶的所有簡訊，甚至是插入、變更或刪除簡訊，而 Vivo 的 V7 所預載的程式則能在未取得使用者授權之下擅自記錄螢幕畫面；Oppo 的 F5 可悄悄錄音並存至 SD 卡，還能執行命令；LG 的 G6 能夠鎖住用戶、取得核心紀錄；Asus 的 ZenFone 3 Max 內建的程式則能獲得各種錯誤報告、裝置資訊或 Wi-Fi 密碼，還能拍下螢幕畫面或執行命令。

Kryptowire 公司已於官網 (https://www.kryptowire.com/portal/android-firmware-defcon-2018/) 列出了所有手機型號與相關漏洞。

(二) What the Fax!?

1、講者：Yaniv Balmas (Security Researcher, Check Point Software Technologies)
及 Eyal Itkin (Security Researcher, Check Point Software Technologies)

2、時間：8 月 12 日下午 3 點

3、摘要：

來自 Check Point 公司的講者說明該公司發現駭客可針對內建傳真功能的印表機傳送攻擊程式，就能控制傳真機，同時搜尋和傳真機同一網路的電腦，利用攻擊工具 EternalBlue 植入惡意程式，再將竊取的資料透過傳真機外洩。

Check Point 是透過傳真機 PSTN 通訊協定，以及微軟在 2017 年 3 月所修補的 CVE-2017-0144 漏洞，這是一個攸關共享檔案與印表機資源的 SMB 協定漏洞，也是惡名昭彰的 WannaCry 及 Petya 勒索病毒所利用的漏洞。駭客只要有傳真號碼，就能攻陷企業印表機，而只要該印表機有連線內部網路，則同一網路的電腦也會受到駭客攻擊而受到控制。其手法如下圖：

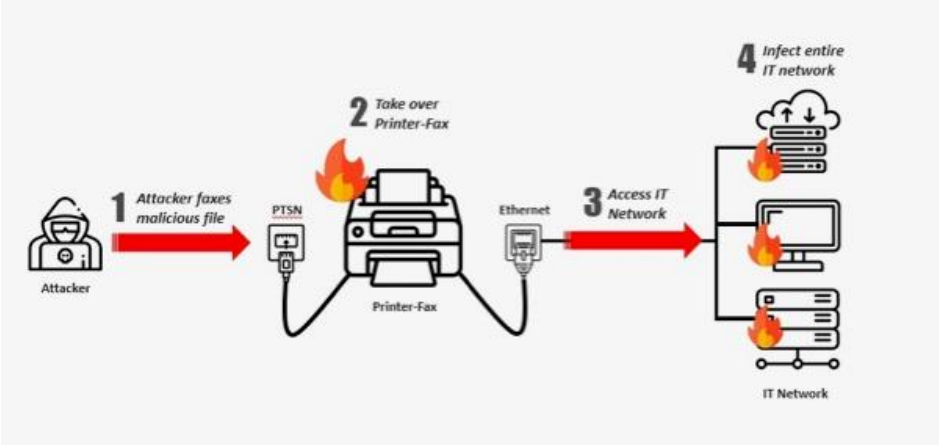

圖 8、駭客透過傳真機攻擊手法

講者在現場當眾展示攻擊 HP Officejet 系列的多功能印表機過程，並建議最好將公司的傳真機及內部網路隔開，並更新相關設備的軟體。目前 HP 已修補了相關漏洞。攻擊過程的影片網址如下：(https://www.youtube.com/watch?time_continue=49&v=1VDZTjngNqs)。

(三) A Journey Into Hexagon: Dissecting a Qualcomm Baseband

1、講者：Seamus Burke

2、時間：8 月 9 日下午 1 點

3、摘要：

行動電話的運作非常複雜，除了應用程式處理器外，還具有多個嵌入式處理器，可處理 WiFi、行動通訊、藍牙和其他信號。講者透過分析高通基頻處理器的硬體內部結構，追溯它多年來的演變，以及最新的內部 DSP 架構，和專有的 RTOS 系統，並介紹堆疊結構可能存在的漏洞，以及漏洞的解決措施。

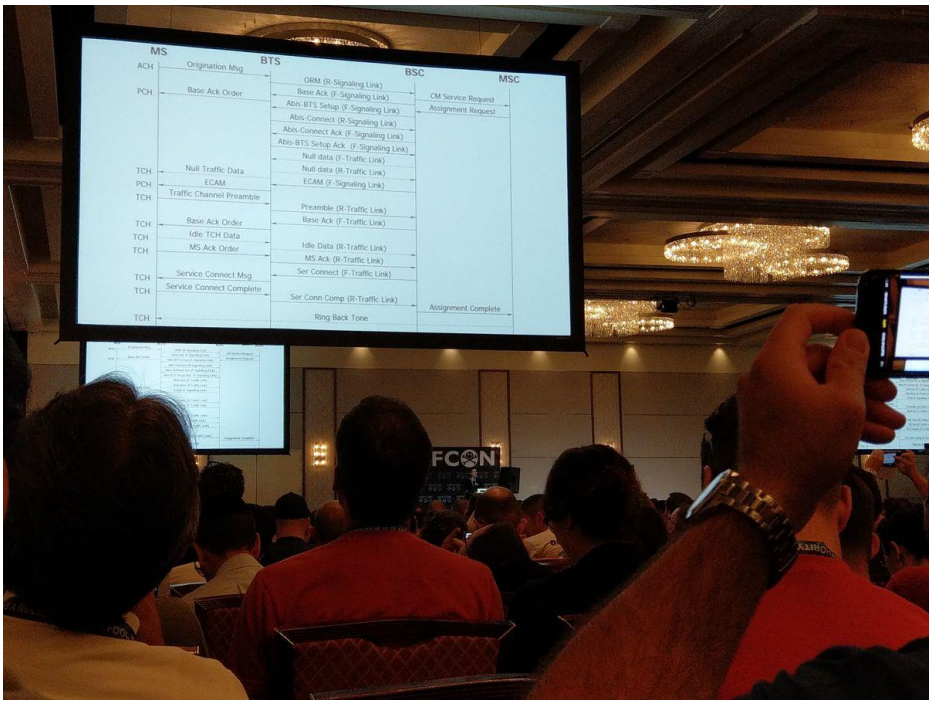

圖 9、行動通信訊號傳輸流程分析

(四) Wagging The Tail - Covert Passive Surveillance And How To Make Their Life Difficult

1、講者：Si 及 Agent X

2、時間：8 月 9 日下午 2 點

3、摘要：

身為駭客，有可能會被調查人員或其他人士跟蹤，為了保護人身自由，講者透過實例講解如何辨識跟蹤者，以及一旦發現被跟蹤時如何擺脫。例如跟蹤者通常是一個團隊，透過辨識特定型式的行動模式，確認

是否受到監視，以及利用大眾運輸工具來擺脫跟蹤等方法。

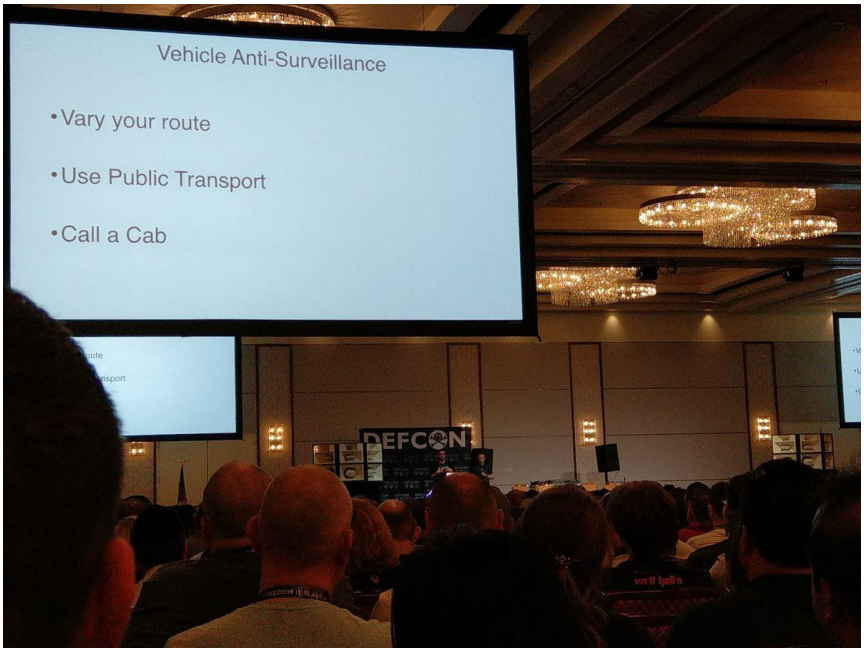

圖 10、如何反跟蹤

(五)Securing our Nation's Election Infrastructure

1、講者：Jeanette Manfra (Assistant Secretary, Office of Cybersecurity and Communications, Department of Homeland Security)

2、時間：8 月 10 日上午 10 點

3、摘要：

講者是美國國土安全部網路安全與通信辦公室助理秘書，她表示公平選舉是每個民主國家的核心，對國家安全至關重要。近年來，美國政府對選舉基礎設施面臨的潛在威脅越來越不安，並已就 2016 年總統大選的經驗汲取教訓。

針對即將舉行 2018 年的期中選舉，國土安全部已在 2017 年 1 月，將選舉制度指定為關鍵基礎設施，意即選舉基礎設施已成為政策制定和資源分配的優先事項。國土安全部與 8,000 個選舉管轄區以及 55 個州和地區的選舉官員直接合作，以協助他們保護自己的系統。隨著威脅環境的演變，國土安全部將繼續與地方合作，加強對威脅的辨識，分享及時

的威脅訊息，並為公私部門提供必要的網路安全工具和資源，以提高安全性。

(六)Lora Smart Water Meter Security Analysis

1、講者：Yingtao Zeng (Security Researcher at UnicornTeam, Radio Security Research Department of 360 Security Technology)、Lin Huang (Senior Wireless Security Researcher and SDR technology expert, 360 Security Technology)及 Jun Li (Senior Security Researcher, Radio Security Department of 360 Security Technology)

2、時間：8 月 10 日上午 11 點

3、摘要：

Lora 是目前相當熱門的物聯網系統，透過 Lora 網路，可以將水錶的資料用無線的方式傳輸，免除以往使用人力抄水錶的繁瑣工作。來自 360 Security Technology 公司的講者，透過將具有無線通信模組的水錶，以及 Lora 網路進行逆向工程和分析，來瞭解這種電錶的安全和隱私風險，包括使用磁鐵干擾水錶、偽造感應器電壓、截取用戶個資、假造上傳資料，以及 GPRS 中間人攻擊等。

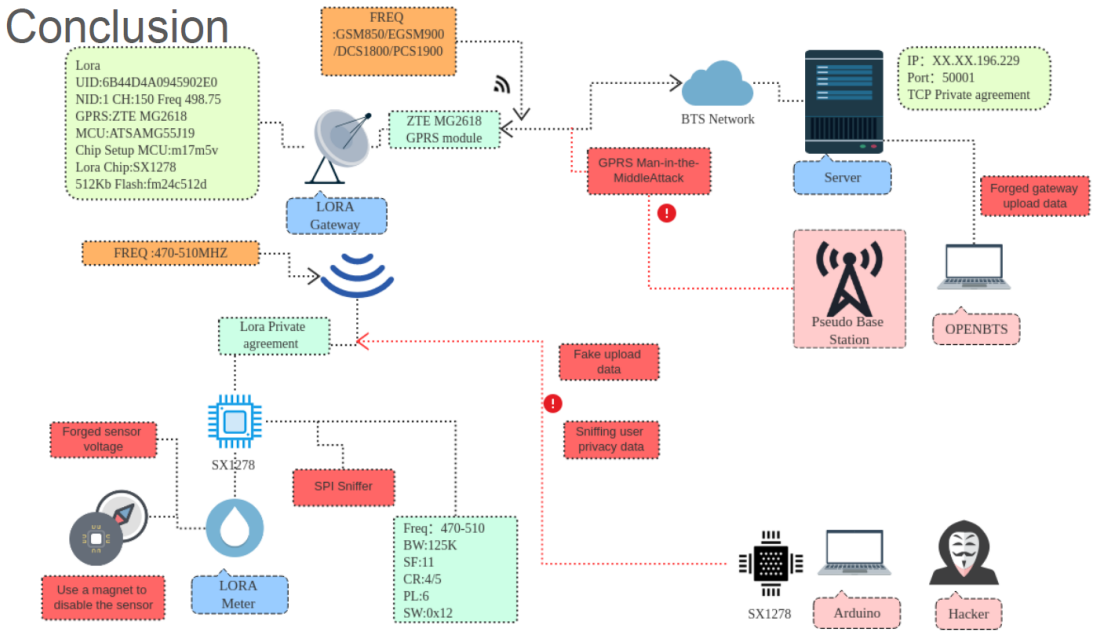

圖 11、Lora 水錶資安風險

(七)Your Bank's Digital Side Door

1、講者：Steven Danneman (Security Engineer, Security Innovation)

2、時間：8 月 10 日下午 5 點

3、摘要：

講者發現網路銀行的網站使用多重因子認證機制（MFA），但其合作的財務管理系統如 Quicken 等卻未採用。再進一步分析後，講者深入探索有 20 年歷史的開放式金融交易（OFX）協議以及支援它的 3,000 多家北美銀行，他發現有相當多的漏洞。

透過觀察 Quicken、QuickBooks、Mint.com 等服務如何蒐集支票帳戶交易、信用卡、股票投資組合和稅務資料，可以瞭解銀行資訊部門提供的軟體的安全性是相當脆弱的。因此，講者也展示並發布一個追蹤 OFX 服務的工具，並描述其功能及其安全性。

(八)Man-In-The-Disk

1、講者：Steven Danneman (Security Engineer, Security Innovation)

2、時間：8 月 12 日下午 1 點

3、摘要：

大多數作業系統都使用沙盒來防止惡意程式影響其他應用程式甚至損害作業系統本身，尤其 Google 不斷加強 Android 的沙盒保護，引進新功能以防止任何類型的攻擊繞過沙盒保護。但是講者發現外部存儲和網路的漏洞可被攻擊者利用來破壞資料，竊取敏感資訊甚至控制設備，從而繞過 Android 最新的沙盒保護。其攻擊手法如下圖：

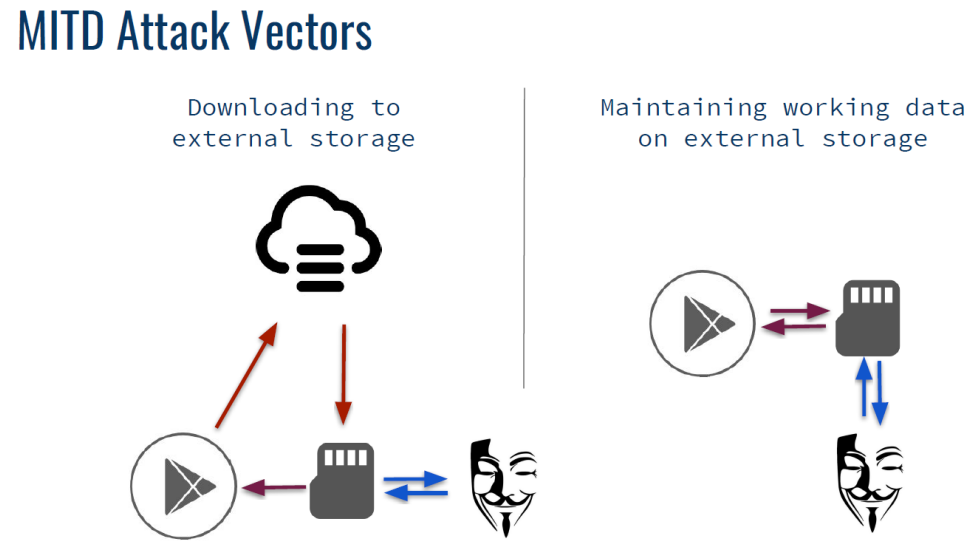

圖 12、利用外接記憶卡攻擊應用程式

講者建議外接記憶卡等儲存設備最好不要存放重要資訊、可執行檔，或是存放重要的 APP，以避免遭受攻擊而失去沙盒保護。

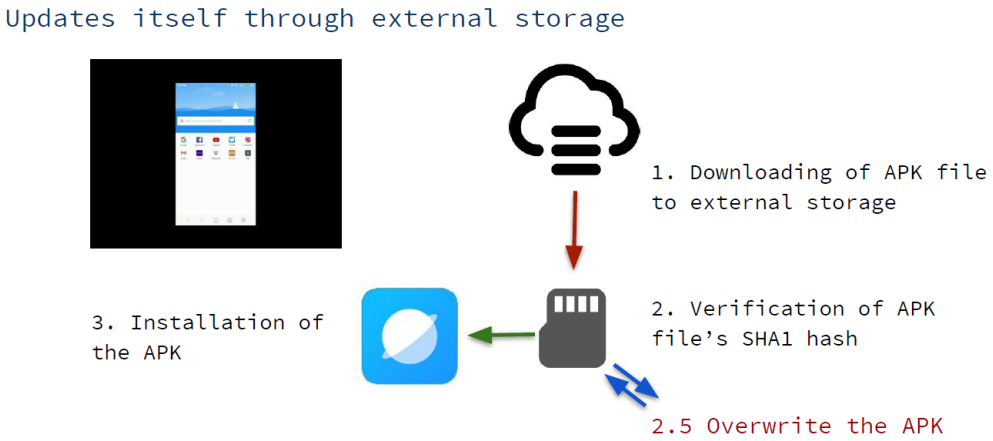

圖 13、APK 檔案遭竄改

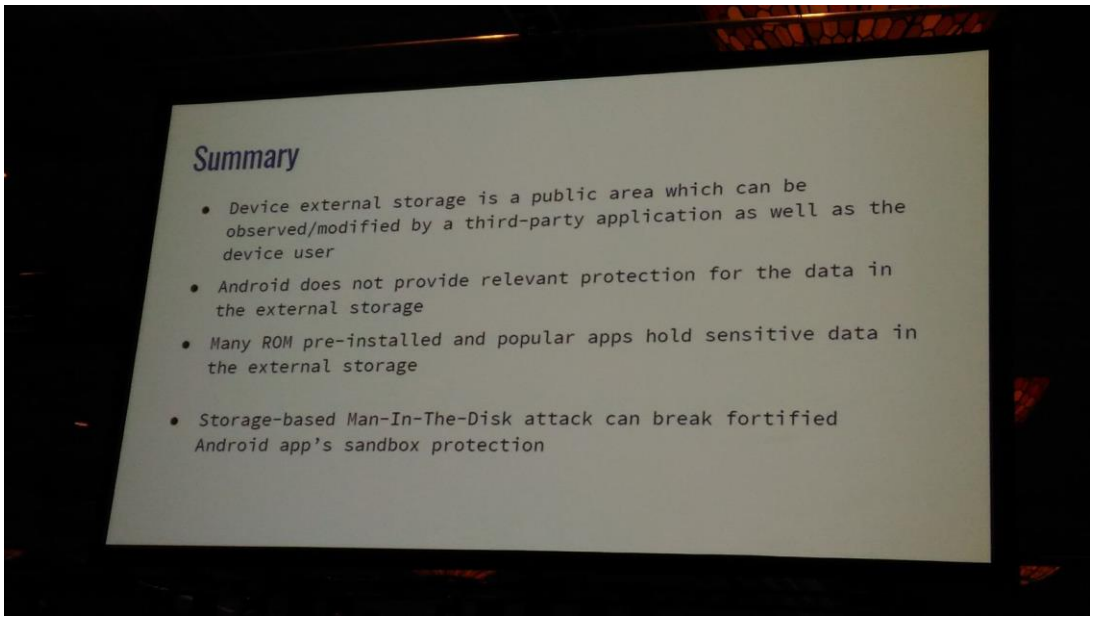
Summary
Device external storage is a public area which can be observed/modified by a third-party application as well as the device user
Android does not provide relevant protection for the data in the external storage
Many ROM pre-installed and popular apps hold sensitive data in the external storage
Storage-based Man-In-The-Disk attack can break fortified Android app's sandbox protection

圖 14、講者建議

參、心得及建議

一、我國資安實力獲國際肯定

代表我國參與 DEF CON 26 CTF 競賽的 HITCON 團隊，本屆獲得第 3 名的佳績，僅次於第 1 名的韓國 DEFKOROOT 及第 2 名美國 PPP。而第一次參賽就拿下第 12 名的我國 BFS 團隊，也同樣讓人驚豔。

由於我國資安實力受到國際肯定，今年在我國舉辦的 HITCON CTF 競賽被 DEF CON CTF 主辦單位指定為明年 DEF CON 決賽第一個種子賽事，吸引全球 1,800 個隊伍參賽，獲得冠軍的波蘭 Dragon Sector 隊，將直接晉級明年的 DEF CON CTF 總決賽。

二、資安需持續投資

隨著資通訊科技的進步，資安議題也日新月異。因此，不論是政府機關或是民間企業，都需要長期投入資源培養資安人才，才能因應各種資安挑戰。資通安全管理法的立法，就是看到這個趨勢，也提供公私合作的重要契機。由政府機關主動與相關資安社群合作，建立資通安全科技研發整體規劃與推動機制，並針對新興技術建置相關實驗場域，以提升國家整體資安自主技術能量，進一步帶動資安人才培育，循序充實各層級資安人才。

三、各行各業都應重視資安

物聯網的發展，讓各行各業都能透過網際網路擴大視野，但也同樣增加了資安的風險，所以資安議題已不止是資通訊產業的重要課題，而是任何與網路相連的事物都應該隨時重視，並隨時做好資安防護的工作。

肆、附錄

DEFCON 26 官網：https://www.defcon.org/html/defcon-26/dc-26-index.html

DEFCON 官網：https://www.defcon.org/index.html

DEFCON 26 資料庫：https://media.defcon.org/DEF%20CON%2026/

DEFCON YouTube 頻道：
https://www.youtube.com/channel/UC6Om9kAkl32dWlDSNlDS9Iw

iThome 官網：https://www.ithome.com.tw/

出國人員與會照片：