出國報告（出國類別：其他-國際會議）

「國際資訊安全會議(DEF CON 25)」出國報告

服務機關：行政院主計總處主計資訊處
姓名職稱：王興娟分析師
派赴國家：美國（拉斯維加斯）
出國期間：106 年 7 月 27 日至 106 年 7 月 30 日
報告日期：106 年 10 月 17 日

摘　　要

自 105 年發生跨國駭客集團攻擊我國銀行 ATM 事件、證券業遭到 DDoS 攻擊勒索及不停變種的綁架勒贖軟體，過去很難想像這麼多的網路駭客攻擊事件，會對我國產業及政府機關產生高度攻擊興趣，隨著個別攻擊案例不停發生，我們已經可以了解到，未來是一個網路攻防越趨頻繁的年代。

近期伴隨著綁架勒贖軟體，可以發現駭客要求付贖金的管道，許多會結合虛擬貨幣（如 Bitcoin 機制等），又因為虛擬貨幣使用開放原始碼進行設計及交易不記名等特性，其衍生出來的應用空間及資訊安全風險，亦成為本次會議討論的重點。

因應我國政策開放，目前有許多第三方支付已經提供民眾服務，其 Pay 送訊息流程，亦結合智慧型手槍權限管理、電子錢包應用，甚至透過駭客工具可自動找到資訊系統漏洞位置等，亦在本次會議引發熱烈討論。

對於雲端應用，智慧型裝置等安全性，因民眾使用需求日漸龐大，駭客攻擊因此如影隨形，透過本次大會，亦了解雲端及智慧型裝置之相關應用與攻擊手法，進而引發相關的安全防禦機制。

有鑑於此，資通安全問題已成為國際關注之重要議題，我國總統更宣示資安等於國安，行政院更成立資通安全處，積極推動資通安全管理法，針對八大行業優先納入適用，並成立第四軍種「資通安全電軍」，皆為迫切希望政府機關及各產業增加投入資訊安全防禦縱深之資源，並降低駭客各種管道攻擊的威脅。

各國為分享資安情資及推廣防禦技術，亦定期召開資安相關研討大會，促進最新資安發展趨勢交流與分享，包含以色列 Cyber Week、RSA Conference、Blackhat、DEF CON 等。除了新興科技技術（如：FinTech、飛彈防禦國防系統等）以外，其中 DEF CON 係全球最知名的駭客技術會議之一，每年定期於美國拉斯維加斯舉辦，內容包含豐富的資安趨勢論壇、駭客技術、駭客攻擊手法、駭客工具、最新資安軟硬體設備展覽及國際間最重要的奪旗競賽（Capture the Flag，CTF）。

本（106）年（第 25 次）DEF CON 於拉斯維加斯 Caesars Palace 會議中心舉辦，為期 4 日（本年 7 月 27 至 30 日），會議內容包括各項軟體的最新漏洞發表、分析工具，以及時下最熱門的區塊鏈（Block chain）安全議題；而代表我國參賽的隊伍（HITCON）則自 103 年起連續 4 年入選最後決賽，本年最後獲得第 2 名的佳績。

經參加本次會議後，有感近年駭客攻擊手法不斷翻新，各機關依資安責任等級要求，強化資安防禦縱深後，仍要不段掌握最新之駭客攻擊手法及工具，以提升整體資安防禦技術能量；由政府機關主動與相關資安社群合作並分享資安情資，進一步帶動資安人才培育，充實我國資安能量。

目　　次

壹、 會議介紹

一、 會議名稱

DEF CON 25

二、 會議時間

106 年 7 月 27 日至 106 年 7 月 30 日

三、 會議地點

美國拉斯維加斯 Caesars Palace 之會議中心

四、 會議相關文件

會議相關資料請詳見網站

(https://www.defcon.org/html/defcon-25/dc-25-index.html)

貳、 參加會議目的

DEF CON 為世界級駭客大會，亦被稱為「黑客秘密大派對」，每年在美國內華達州的拉斯維加斯舉辦，全球許多大公司代表、專業資安駭客、廠商、政府機關、學研界等資安專業人員，皆會前往一同共襄盛舉此年會。

本次出國主要目的，希望了解目前世界各國之新興科技應用現況，除針對虛擬貨幣、雲端運算、電子錢包、智慧型手槍、行動裝置等已成熟機制世界推動服務方式外，更希望藉此了解如何在機關業務推動上，帶來一些新的想法。

另希望可由會議各類議題中，瞭解最新駭客攻擊手法、駭客攻擊工具並掌握國際資訊安全發展趨勢，除了提升本身對駭客攻擊手法的認知外，亦期望藉由演講中所獲取的資訊安全新知與技術，瞭解目前駭客最新的技術，俾提供未來機關強化防禦縱深或深化資訊安全制度上之協助；另藉由參觀不同分析工具，例如 solgraph 及 oyente 等，只要給予程式碼與 ABI 就可定位出潛在有弱點的程式碼，以瞭解如何利用不同的分析工具，找出潛在的系統弱點；最後，則是體驗備受矚目的奪旗賽（Capture the Flag，CTF），見證與過去不同的電腦架構、指令集及全新運算規則如何在網路攻防戰上攻擊與防守應用之重要里程碑。

參、 會議過程及重點議題

一、 會議議程

DEF CON 25 演講議程自 7 月 27 日(四)至 7 月 30 日(日)，共分為 4 個廳進行演講，包括「101 Track 」、「Track 2」、「Track 3」及「Track 4」，議程詳如附錄之表 1 至表 4。

二、 重點議題

(一) CTF 競賽

DEF CON CTF 比賽分為線上預賽和現場決賽，預賽採用解題模式（jeopardy），預賽排名前面的隊伍才能晉級參加拉斯維加斯的現場決賽，現場決賽於 106 年於 7 月 28 至 30 日舉行，比賽連續進行三天，考驗駭客加解密、破解、漏洞入侵、防禦的技術，除了防守本身系統，修補系統漏洞外，也要掌握敵方系統漏洞攻打，才能獲得高分。

今年特別不同於去年真人駭客與機器人的大對決，除了回到真人駭客攻防競賽，主辦方在比賽前一天早上才公布，將不依照目前任何一種電腦架構，發布了一個新的 CPU 架構和指令集 cLEMENCy，尤其是將重新定義了 1 個 Byte 是 9 個 bit 的全新電腦運算規則)；由於前一天才早上才公布新架構，全部參賽隊伍需重新開發工具，不只是考驗團隊開發能力，更考驗著駭客對 CPU 運作和 OS 層級核心知識的了解。為長四天的開發及攻防比賽，團隊的應變力、耐力、分工默契全一覽無遺展現

在此次比賽中。

圖：臺灣代表隊 HITCON 攻防現場

圖：DEF CON CTF 各隊攻防現況看板

2017 DEF CON CTF 駭客攻防總決賽（搶旗攻防賽）最終結果揭曉，在全世界 15 強駭客戰隊中，臺灣代表隊 HITCON 勇奪

第二名，僅次於多次奪冠的美國隊 PPP，打敗了來自中國、韓國、俄羅斯、以色列、德國、匈牙利等國駭客高手。資安專家表示，HITCON 關鍵獲勝最大原因為團隊在過程中幾乎「零內耗」，成員合作具有極佳默契，成員就各自擅長的題目主動認領，從工具的改寫到解題的分工，幾乎是一個自動化進化的優秀團隊，徹底發揮了整個團隊的優勢，獲得佳績。

表 1：本年 DEF CON CTF 比賽最終成績

Place	Team	Final Score	Country
1	PPP	33850	美國
2	HITCON	30631	臺灣
3	A*0*E	19730	中國大陸
4	DEFKOR	18474	韓國
5	Tea Deliverers	13941	中國大陸
6	Pasten	11332	以色列
7	Shellphish	10452	美國
8	Eat Sleep Pwn Repeat	9369	德國
9	RRR	9088	韓國
10	Lab RATs	8564	歐洲
11	hacking4danbi	8521	韓國
12	Team Rocket ☠	8496	歐洲
13	Bushwhackers	6894	俄羅斯
14	koreanbadass	6766	韓國
15	!SpamAndHex	4405	匈牙利

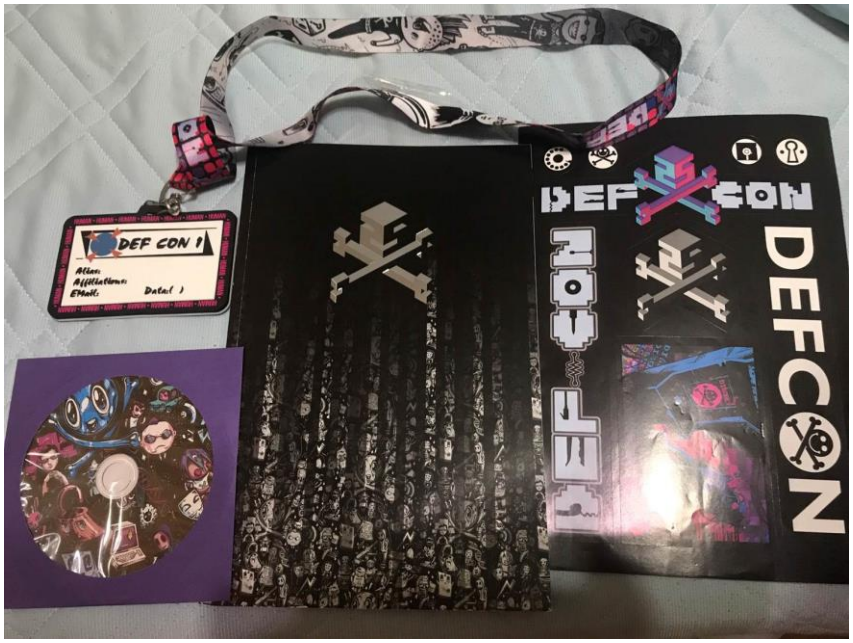
（資料來源：iThome 網頁）　　圖：DEF CON 25 HITCON 獲獎照

（資料來源：iThome 網頁）　　圖：DEF CON 25 HITCON 慶功照

(二) DEF CON Welcome & Badge Talk

過往 DEF CON 的識別證（Badge），都設計藏有一個 Code 讓參與研討會者來進行小活動，參賽者必需蒐集識別證掛帶上的 Code，再套上大會特別提供的公式，組譯出一組按鍵順序，登打進今年的造型識別證上，才可看到特殊設計晶片破解後的燈光，DEF CON 25 的各式 Badge 造型詳見下圖。

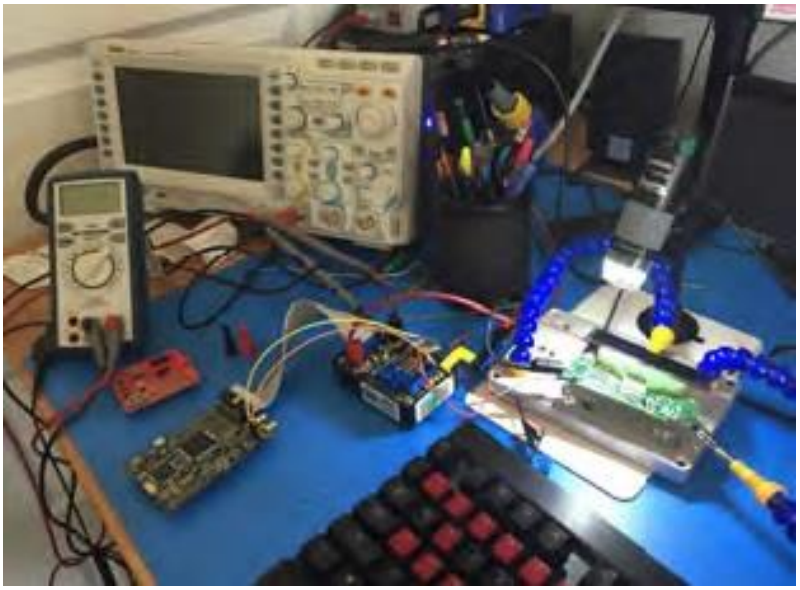
資料來源：Twitter 網頁(@Queercon)　圖：DEF CON 25 的各式 Badge 造型



圖： DEF CON 25 的骷髏頭造型 Badge

(三) Breaking Bitcoin Hardware Wallets

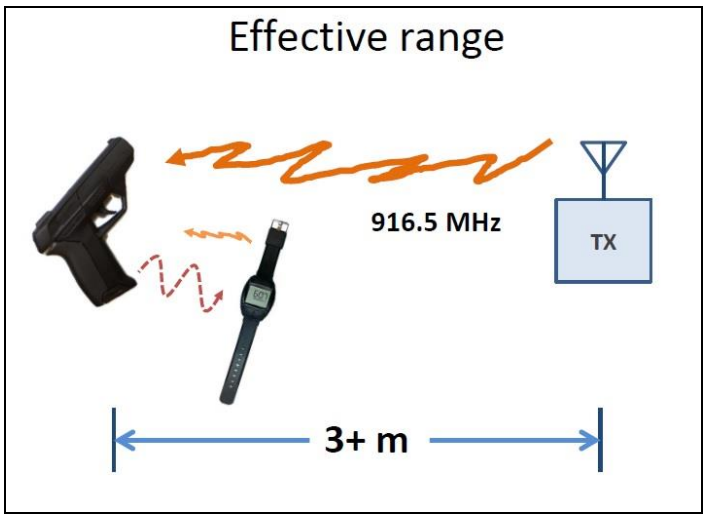
本場演講中，演講者提出了用開放原始碼軟體 Chip Whisperer 與 fault injectione 故障方式攻擊硬體錢包。駭客利用一個 70 美元的示波器工具（Oscilloscope tool 是一種能夠顯示電壓信號動態波形的電子測量儀器）、STM32F205 易受故障攻擊的特性、KeepKey 在 PIN 驗證上的時序分析錯誤及 TREZOR 裝置沒有啟用時鐘安全系統等弱點， 將 Bitcoin 輕易的從硬體錢包中移走，因此在程式開發階段，開發人員需確認每個功能之正常，以及系統故障時，系統觸發程序之安全性。



圖：藉由電流、電壓改變，修改韌體，攻擊硬體錢包

(四) Popping A Smart Gun

Smart Gun 智慧型手槍，為預防手槍誤發射或未經授權使用，設計的一款智慧手槍，智慧手槍在使用時，需搭配智慧型手錶，在有限距離內，才能進行發射（可參考下方圖說明），但在今年 DEF CON 會議，演講者分享可藉由 15 美元的磁鐵，讓扳機控制器失去作用，上鎖智慧手槍在未搭配智慧型手錶的情形下，直接發射出子彈；未來，智慧型手槍廠商將針對此一破解，儘速修正此漏洞。



圖：智慧型手槍只能在有限距離內發射

圖：磁鐵讓智慧型手槍的扳機控制器失去作用

(五) Hacking Smart Contracts

Porosity 是 Solidity 的分析工具，只要給予程式碼與 ABI 就可定位出潛在有弱點的程式碼。在會議上，演講者示範了一段含漏洞的程式，此程式使用一個新契約 C 內的 fallback function，去呼叫 withdrawBalance，SendBalance 會持續將錢匯給 C，而不會執行到餘額歸零那行。藉由分析工具 Porosity，會指出漏洞與所在程式碼位置，找到 reentrant 弱點。

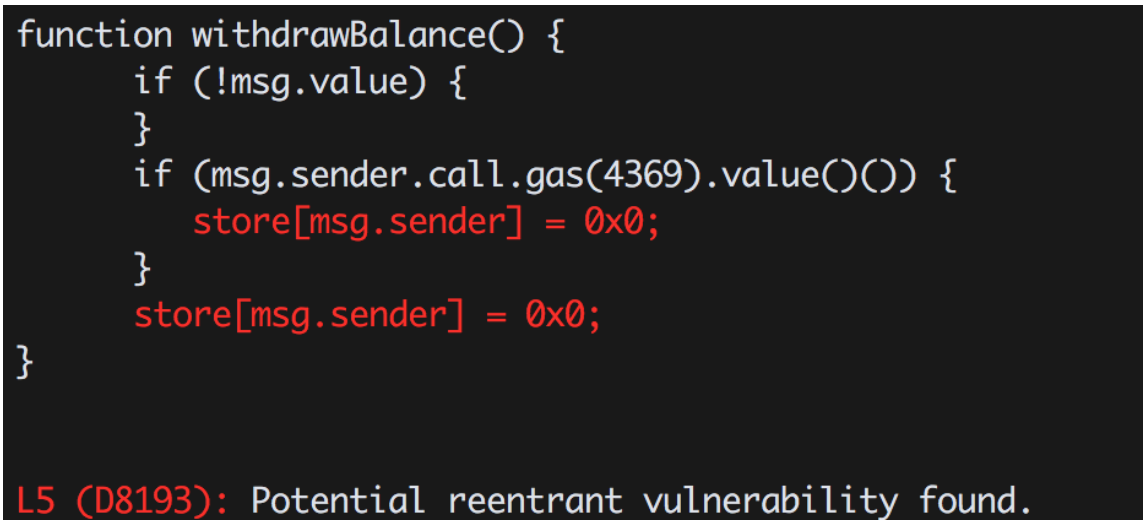


圖: Porosity 執行結果，找到 reentrant 弱點

(六) Phone System testing

演講者一開始於會議中簡單介紹了電話基本裝置，其中用戶電話交換機（PBX）可連接企業內部電話，也可以將這些電話與公共交換電話網（PSTN）連接在一起。會議中演講者 Snide/Owen 示範使用不同的方法對電話交換機進行攻擊（如下圖），攻擊後，通話的內容可被錄音，駭客可藉由此方法竊取通話內容之敏感通話資料。

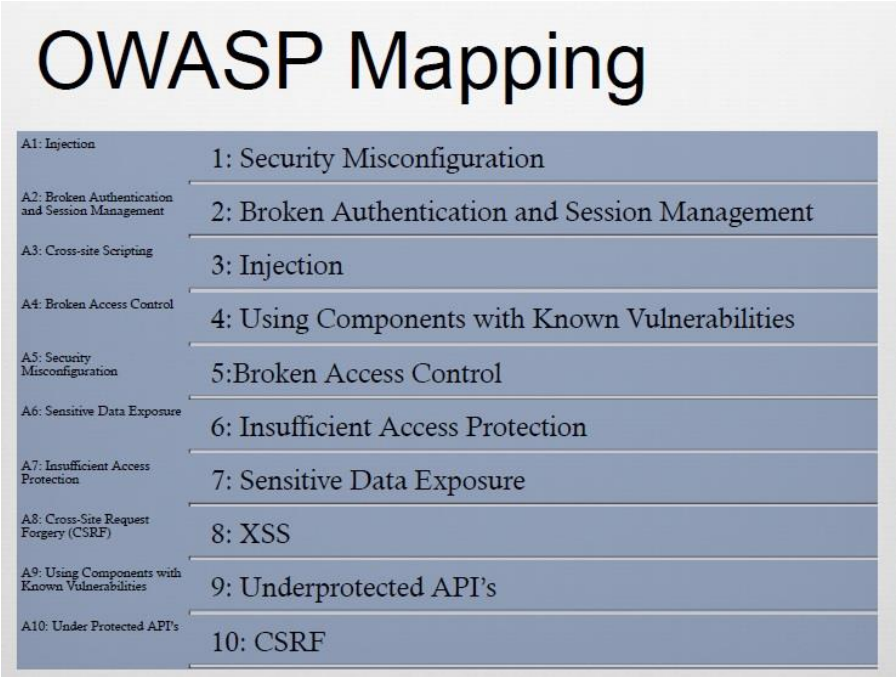


圖:示範使用不同的方法對電話交換機進行攻擊

肆、 心得建議

伴隨著資訊愈來愈發達，全世界早已是個地球村，資安問題已不是單純電腦中毒這麼簡單的問題，從早期的亂槍打鳥病毒感染，只要執行解毒程式或最嚴重整台電腦重新格式化即可解決問題，始作俑者純屬惡作劇心態，演化至近年來，攻擊手法與時俱進，電腦只裝防毒軟體再也無法保証實際運作安全，攻擊者可能早已潛伏一段時間，盡其可能收集所有資訊，針對政府機關為了獲取機敏性資料，針對公司企業則為取得高額獲利為目的。

駭客使用的媒介即是連網設備，隨著智慧型家用產品快速推陳出新，連網裝置數量不斷增加，資安廠商發佈最新報告指出，106 年前 6 個月統計，透過家用路由器所發生的網路入侵總數超過 180 萬次，臺灣受到攻擊次數排名全球第九，故只要設備連網就可能置身於駭客攻擊環境之下，相關的資安防護及受駭範圍影響之資料保護都應事先評量並預防。另一項最常讓使用者受駭的方式即是惡意連結社交工程電子郵件，只要開啟郵件或其夾帶附件，便會自動連結並下載惡意程式伺機而動，連網設備因此變成駭客達成目標的助手，故使用者在讀取郵件之前，應特別留意寄件者是否為平日往來之對象，並先以文字模字讀取郵件內容，以判別是否為異常郵件。

本總處因應多變之資通安全環境，自 98 年起以主計資訊處導入資訊安全管理制度（簡稱 ISMS）並取得 ISO 27001 認證，至 104 年以全總處（16 個單位 57 個科室）為導入範圍並於 104 年 11 月底完成全總處 ISO 27001 新版驗證，成為全國部會級機關中第 3 個完成全機關通過資訊安全管理制度驗證之組織。另為配合行政院資通安全相關業務推動，本總處自

104 年提升為資安責任等級 A 級機關，多了許多資安防護應辦事項，業管資訊系統需完成資安分類分級及相關等級之資安防護基準要求，但公務機關資源有限，設備僅能依年限更換、依計畫或預算購置，所需人力亦同步增加。本處資訊業務原已十分繁重，還要顧全本總處及所有資訊系統之資安防護，是項不容易達成的任務。然藉由此次國際研討會的機會，吸收一些新知識及他人經驗，希望對本總處未來的資通安全防護，提供幾點參考建議：

一、加強本總處資安設備防護功能：

本處本年度進行網路架構調整及資源擴充，並配合資安考量進行網路區塊分隔。全年度 24 小時進行資安監控防護，定期進行弱點掃瞄，以及網路防火牆、入侵防禦、垃圾郵件過濾等防護工作。為使資安設備達到最佳防護效果，建議定期檢視設備之預設 Policy 設定。如：A 系統為內網系統，則不可能連線至外網。B 系統和 C 系統無相關，則 2 系統不可能出現連線行為。多少稱為大量異常連線應即時發出警訊等。適當的 Policy 設定可以幫助管理者減少管理工作，並及時接收異常作業警訊以獲得適當處置。

二、落實資訊系統分級與資安防護：

有關行政院資通安全處訂定「政府機關（構）資通安全責任等級分級作業規定」及「資訊系統分級與資安防護基準作業規定」，本於撙節原則，將機關（構）及業管資訊系統，依資通安全重要性與以分級，完成相關等級之資安防護基準要求；另輔以定期進行內外網弱

點掃瞄，並針對外網中風險及所有高風險，通知應用系統及設備管理者盡速完成漏洞修補，以及核心資訊系統進行滲透測試，皆可及早發現及早修補，有效降低漏洞之風險。本總處十月底統計約業管54個資訊系統，核心資計系統計有5個，近2年為因應行政院規定及網路攻防演練之準備，核心資訊系統皆已進行過滲透測試，未來建議檢視近50個資訊系統，依其重要性決定是否需要或逐年進行滲透測試。

三、提升本總處同仁資安防護意識：

本總處對外有多項防護設備持續進行資安防禦，如：網路防火牆、入侵防禦、垃圾郵件過濾等。但科技始終來自於人性，資安事件有很高的比例是起因於惡意連結社交工程電子郵件。根據統計有91%的APT（Advanced Persistent Threat）攻擊是以此方式潛伏進機關內部，藉由木馬屠城等方式侵入機關內部主機，蒐集各種機敏性資料，平均潛伏時間長達 598 天，藉由長時間的潛伏，慢慢地將受駭環境探索地一清二楚，進而有效突破各階層的防禦，所謂家賊難防，外部再多的資安設備亦很難防禦內部攻擊，而受駭者也很難察覺自己受到攻擊或是已變成加駭方。本總處目前是每季辦理社交工程電子郵件演練，另定期辦理資通安全事件通報、資訊系統災害備援等演練，演練成果尚屬優異並符合行政院網路攻防演練合格標準，但仍屬本總處重要防禦機制無法懈怠，需要全體同仁共同努力防護，故掌握當前最新資安威脅趨勢，持續提升同仁資安防護意識亦為本

總處資安防護之重要課題。

四、培訓本總處資安專業技術人力：

本次活動發現我國駭客社群屢屢於國際資安競賽嶄獲佳績，我國代表 HITCON 已連續多年進入 DEF CON 的 CTF 決賽，本年超越去年的第 4 名，最終獲得第 2 名的佳績，顯見我國資訊安全團隊實力在國際排名持續進步。本總處雖有資訊部門及多名資訊人員，但資安專責人員有限，有關駭客等相關資安專業技術，仍屬欠缺與不足，建議後續主動參與相關資安社群，增加駭客攻擊及防禦等相關資安專業課程，或與相關資安社群及各大學校資訊安全研究室合作，借重其技術能量協助本總處進行資安健診、網路攻防及資安事件處理，定期遴選適合人員，參與此類駭客研討會等，藉由深化資安人才的培育，厚實本總處資安人才能量。

伍、 會議照片

圖:DEF CON 後台

圖:DEFCON 駭客村

圖:娛樂時程表

圖: Wall of Sheep，當資訊被駭時，會顯示出名字和節錄密碼

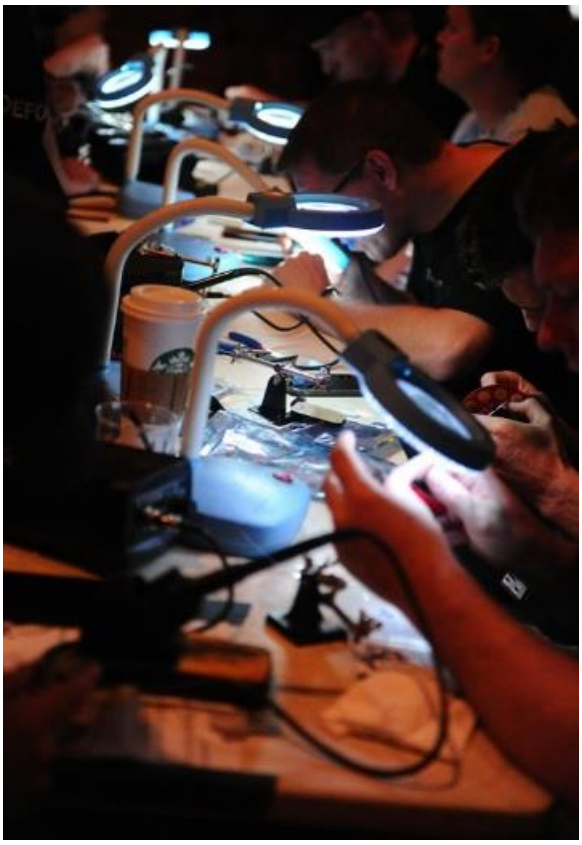


圖:選手們在試圖駭入駭客村的硬體設施

陸、 參考資料

一、 DEF CON 美國官方網站，

https://www.defcon.org/html/defcon-25/dc-25-schedule.html#Thursday

二、 iThome 官方網站，http://www.ithome.com.tw

三、 Google 新聞，http://news.google.com.tw

柒、附錄

表 1：DEF CON 25 會議第 1 日議程（106 年 7 月 27 日）

Time	101 Track1	101 Track2
10:00	There’s no place like 127.0.0.1 - Achieving reliable DNS rebinding in modern browsers Luke Young	Where are the SDN Security Talks? Jon Medina
11:00	From Box to Backdoor: Using Old School Tools and Techniques to Discover Backdoors in Modern Devices Patrick DeSantis	Opt Out or Deauth Trying !- Anti-Tracking Bots Radios and Keystroke Injection Weston Hecker
12:00	Porosity: A Decompiler For Blockchain-Based Smart Contracts Bytecode Matt Suiche	Jailbreaking Apple Watch Max Bazaliy
13:00	Amateur Digital Archeology Matt 'openfly' Joyce	Wiping Out CSRF Joe Rozner
14:00	Hacking the Cloud Gerald Steere & Sean Metcalf	See No Evil, Hear No Evil: Hacking Invisibly and Silently With Light and Sound Matt Wixey
15:00	Inside the “Meet Desai” Attack: Defending Distributed Targets from Distributed Attacks CINCVolFLT (Trey Forgety)	Real-time RFID Cloning in the Field Dennis Maldonado
15:30	Inside the “Meet Desai” Attack: Defending Distributed	Exploiting Old Mag-stripe information with New technology

	Targets from Distributed Attacks (cont.) CINCVolFLT (Trey Forgety)	Salvador Mendoza
16:00	DEF CON 101 Panel (Until 18:00) HighWiz, Malware Unicorn, Niki7a, Roamer, Wiseacre, & Shaggy	The Last CTF Talk You'll Ever Need: AMA with 20 years of DEF CON Capture-the-Flag organizers (Until 18:00) Vulc@n, Hawaii John, Chris Eagle, Invisigoth, Caezar, & Myles

表 2：DEF CON 25 會議第 2 日議程（106 年 7 月 28 日）

Time	101 Track	Track 2	Track 3	Track 4
10:00	macOS/iOS Kernel Debugging and Heap Feng Shui Min(Spark) Zheng & Xiangyu Liu	Welcome to DEF CON 25 The Dark Tangent	The Brain's Last Stand Garry Kasparov	Secret Tools: Learning About Government Surveillance Software You Can't Ever See Peyton "Foofus" Engel
10:30	Offensive Malware Analysis: Dissecting OSX/FruitFly via a Custom C&C Server Patrick Wardle	Hacking travel routers like it's 1999 Mikhail Sosonkin	The Brain's Last Stand (cont.) Garry Kasparov	Panel: Meet The Feds Andrea Matwyshyn, Terrell McSweeny, Dr. Suzanne Schwartz, &

				Leonard Bailey
11:00	Rage Against the Weaponized AI Propaganda Machine Suggy (AKA Chris Sumner)	Weaponizing the BBC Micro:Bit Damien "virtualabs" Cauquil	Hacking Smart Contracts Konstantinos Karagiannis	Panel: Meet The Feds (cont.) Andrea Matwyshyn, Terrell McSweeny, Dr. Suzanne Schwartz, & Leonard Bailey
12:00	CITL and the Digital Standard - A Year Later Sarah Zatko	Open Source Safe Cracking Robots - Combinations Under 1 Hour! (Is it bait? Damn straight it is.) Nathan Seidle	A New Era of SSRF - Exploiting URL Parser in Trending Programming Languages! Orange Tsai	Hacking Democracy: A Socratic Dialogue Mr. Sean Kanuck
13:00	Controlling IoT Devices With Crafted Radio Signals Caleb Madrigal	Teaching Old Shellcode New Tricks Josh Pitts	Starting the Avalanche: Application DoS In Microservice Architectures Scott Behrens & Jeremy Heffner	Next-Generation Tor Onion Services Roger Dingledine
14:00	Using GPS Spoofing to Control Time	Death By 1000 Installers; on MacOS, It's	Breaking the x86 Instruction	How We Created the First SHA-1 Collision and

	David "Karit" Robinson	All Broken! Patrick Wardle	Set Christopher Domas	What it means For Hash Security Elie Bursztein
15:00	Assembly Language is Too High Level XlogicX	Phone System Testing and Other Fun Tricks "Snide" Owen	Dark Data Svea Eckert & Andreas Dewes	Abusing Certificate Transparency Logs Hanno Böck
16:00	Radio Exploitation 101: Characterizing, Contextualizing, and Applying Wireless Attack Methods Matt Knight & Marc Newlin	The Adventures of AV and the Leaky Sandbox Itzik Kotler & Amit Klein	An ACE Up the Sleeve: Designing Active Directory DACL Backdoors Andy Robbins & Will Schroeder	"Tick, Tick, Tick. Boom! You're Dead." — Tech & the FTC Whitney Merrill & Terrell McSweeny
17:00	Cisco Catalyst Exploitation Artem Kondratenko	Panel DEF CON Groups	MEATPISTOL, A Modular Malware Implant Framework FuzzyNop (Josh Schwartz) & ceyx (John Cramb)	The Internet Already Knows I'm Pregnant Cooper Quintin & Kashmir Hill

表 3：DEF CON 25 會議第 3 日議程（106 年 7 月 29 日）

Time	101 Track	Track 2	Track 3	Track 4
10:00	Persisting with Microsoft Office: Abusing Extensibility Options William Knowles	$BIGNUM Steps Forward, $TRUMPNUM Steps Back: How Can We Tell If We’re Winning? Cory Doctorow	Get-$pwnd: Attacking Battle-Hardened Windows Server Lee Holmes	The Spear to Break the Security Wall of S7CommPlus Cheng
10:30	Breaking Wind: Adventures in Hacking Wind Farm Control Networks Jason Staggs	BIGNUM Steps Forward, $TRUMPNUM Steps Back: How Can We Tell If We’re Winning? (cont.) Cory Doctorow	WSUSpendu: How to Hang WSUS Clients Romain Coltel & Yves Le Provost	(Un)Fucking Forensics: Active/Passive (i.e. Offensive/Defensive) Memory Hacking/Debugging. K2
11:00	Microservices and FaaS for Offensive Security Ryan Baxendale	Secure Tokin’ and Doobiekeys: How to Roll Your Own Counterfeit Hardware Security Devices Joe FitzPatrick & Michael Leibowitz	If You Give a Mouse a Microchip... It Will Execute a Payload and Cheat At Your High-stakes Video Game Tournament skud (Mark Williams) & Sky (Rob Stanley)	Evading Next-Gen AV Using Artificial Intelligence Hyrum Anderson

11:30	Abusing Webhooks for Command and Control Dimitry Snezhkov	Secure Tokin' and Doobiekeys: How to Roll Your Own Counterfeit Hardware Security Devices (cont.) Joe FitzPatrick & Michael Leibowitz	If You Give a Mouse a Microchip... It Will Execute a Payload and Cheat At Your High-stakes Video Game Tournament (cont.) skud (Mark Williams) & Sky (Rob Stanley)	All Your Things Are Belong To Us Zenofex, 0x00string, CJ_000, & Maximus64
12:00	Driving down the rabbit hole Mickey Shkatov, Jesse Michael, & Oleksandr Bazhaniuk	When Privacy Goes Poof! Why It's Gone and Never Coming Back Richard Thieme a.k.a. neuralcowboy	DNS - Devious Name Services - Destroying Privacy & Anonymity Without Your Consent Jim Nitterauer	All Your Things Are Belong To Us (cont.) Zenofex, 0x00string, CJ_000, & Maximus64
13:00	Demystifying Windows Kernel Exploitation by Abusing GDI Objects. 5A1F (Saif El-Sherei)	Koadic C3 - Windows COM Command & Control Framework Sean Dillon (zerosum0x0) & Zach Harding (Aleph-Naught-)	Twenty Years of MMORPG Hacking: Better Graphics, Same Exploits Manfred (@_EBFE)	A Picture is Worth a Thousand Words, Literally: Deep Neural Networks for Social Stego Philip Tully & Michael T. Raggo
14:00	Attacking	Trojan-tolerant	Linux-Stack	XenoScan:

	Autonomic Networks Omar Eissa	Hardware & Supply Chain Security in Practice Vasilios Mavroudis & Dan Cvrcek	Based V2X Framework: All You Need to Hack Connected Vehicles p3n3troot0r (Duncan Woodbury) & ginsback (Nicholas Haltmeyer)	Scanning Memory Like a Boss Nick Cano
15:00	MS Just Gave the Blue Team Tactical Nukes (And How Red Teams Need To Adapt) Chris Thompson	Tracking Spies in the Skies Jason Hernandez, Sam Richards, & Jerod MacDonald-Evoy	DOOMed Point of Sale Systems trixr4skids	Digital Vengeance: Exploiting the Most Notorious C&C Toolkits Professor Plum
16:00	Dealing the Perfect Hand - Shuffling Memory Blocks On z/OS Ayoul3	From "One Country - One Floppy" to "Startup Nation" - The Story of the Early Days of the Israeli Hacking Community, and the Journey Towards Today's Vibrant Startup Scene	CableTap: Wirelessly Tapping Your Home Network Marc Newlin, Logan Lamb, & Chris Grayson	Game of Drones: Putting the Emerging "Drone Defense" Market to the Test Francis Brown & David Latimer

		Inbar Raz & Eden Shochat		
17:00	Here to stay: Gaining persistency by Abusing Advanced Authentication Mechanisms Marina Simakov & Igal Gofman	Taking Windows 10 Kernel Exploitation to the next level - Leveraging write-what-where vulnerabilities in Creators Update Morten Schenk	Introducing HUNT: Data Driven Web Hacking & Manual Testing Jason Haddix	Popping a Smart Gun Plore

表 4：DEF CON 25 會議第 4 日議程（106 年 7 月 30 日）

Time	101 Track	Track 2	Track 3	Track 4
10:00	Unboxing Android: Everything You Wanted To Know About Android Packers Avi Bashan & Slava Makkaveev	I Know What You Are by the Smell of Your Wifi Denton Gentry	Breaking Bitcoin Hardware Wallets Josh Datko & Chris Quartier	Untrustworthy Hardware and How to Fix It Octane
10:30	Unboxing Android: Everything You Wanted To Know About Android Packers (cont.)	PEIMA (Probability Engine to Identify Malicious Activity): Using	BITSInject Dor Azouri	Ghost in the Droid: Possessing Android Applications with ParaSpectre

	Avi Bashan & Slava Makkaveev	Power Laws to address Denial of Service Attacks Redezem		chaosdata
11:00	Total Recall: Implanting Passwords in Cognitive Memory Tess Schrodinger	Backdooring the Lottery and Other Security Tales in Gaming over the Past 25 Years Gus Fritschie & Evan Teitelman	Exploiting Continuous Integration (CI) and Automated Build systems spaceB0x	Ghost Telephonist' Impersonates You Through LTE CSFB Yuwei Zheng & Lin Huang
12:00	The Black Art of Wireless Post Exploitation Gabriel "solstice" Ryan	Are all BSDs are created equally? A survey of BSD kernel vulnerabilities. Ilja van Sprundel	The Call Is Coming From Inside the House! Are You Ready for the Next Evolution in DDoS Attacks? Steinthor Bjarnason & Jason Jones	Genetic Diseases to Guide Digital Hacks of the Human Genome: How the Cancer Moonshot Program will Enable Almost Anyone to Crash the Operating System that Runs You or to End Civilization... John Sotos
13:00	Game of Chromes: Owning the Web with Zombie Chrome	Bypassing Android Password Manager Apps Without Root	Malicious CDNs: Identifying Zbot Domains en Masse via SSL	Revoke-Obfuscation: PowerShell Obfuscation Detection (And

	Extensions Tomer Cohen	Stephan Huber & Siegfried Rasthofer	Certificates and Bipartite Graphs Thomas Mathew & Dhia Mahjoub	Evasion) Using Science Daniel Bohannon (DBO) & Lee Holmes
14:00	Call the Plumber - You Have a Leak in Your (Named) Pipe Gil Cohen	Weaponizing Machine Learning: Humanity Was Overrated Anyway Dan "AltF4" Petro & Ben Morris	Man in the NFC Haoqi Shan & Jian Yuan	Friday the 13th: JSON attacks! Alvaro Muñoz & Oleksandr Mirosh
15:00	Bridging the Gap between DC and DEF CON: Fireside Chat with Congressmen James Langevin and Will Hurd Rep. James Langevin, Rep. Will Hurd, & Joshua Corman	25 Years of Program Analysis Zardus (Yan Shoshitaishvili)		
16:30	Closing Ceremonies			