出國報告（出國類別：開會）

出席「國際駭客年會(DEF CON 27)」報告

服務機關：國家通訊傳播委員會
姓名職稱：蘇思漢　簡任技正
派赴國家：美國（內華達州拉斯維加斯）
出國期間：108 年 8 月 7 日至 107 年 8 月 13 日
報告日期：108 年 10 月 21 日

摘要

DEF CON 是國際最知名的資安盛會，每年 7 月底或 8 月初，固定在美國內華達州拉斯維加斯舉行，吸引世界各個國家的駭客、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（以 HITCON BFKinesiS 為名）連續 6 年參與盛會，最後獲得 CTF 競賽第 2 名的好成績，僅次於美國 Plaid Parliament of Pwning 團隊。

在軟體化模組成為 5G 網路的內涵、物聯網、人工智慧逐漸的發展，各種連網設備及應用程式進入到各行各業之後，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 是世界最知名的資安大會，通常在美國內華達州拉斯維加斯每年的 7 月最後一週或 8 月第一週舉辦。會議中有各種研討會、技術展示，以及各種系統漏洞的揭露。由於通信網路屬於國家關鍵基礎設施，而且 5G 網路在未來將成為全世界最重要的通信網路基礎設施，本會做為電信事業監理機關，為蒐集資安相關資訊、技術及未來趨勢，以為推動資安防護工作及制定相關政策之參考，因此派員參與會議。

有別於 4G 封閉式的核心網路架構，5G 為彈性支援各種潛在可能、複雜的應用服務與建置型態，其核心網路採用以服務為本之架構（Service-Based Architecture，SBA)，並引入網路功能虛擬化（Network Function Virtualization，NFV）、軟體定義網路（Software Defined Network，SDN）等革命性新設計；同時分離傳統基地臺基頻單元（Base Band Unit，BBU）為中央單元（Centralized Unit，CU）及分布單元（Distributed Unit，DU）實現網路切片（Network Slicing）及高彈性、可規模化之網路架構，以提供高速率、低延遲之應用服務。

此外，5G 的架構允許第三方服務提供者在面臨高速運算需求下，可透過電信業者的多接取邊緣運算（Multi-access Edge Computing，MEC）提供服務。以上發展，使 5G 網路大量使用資訊科技的軟體化系統與開放軟體介面，致使 5G 網路所面臨之資通安全威脅相較封閉的 4G 網路更為多樣且嚴峻。尤其 5G 網路將採用物聯網持續發展，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。

圖 1、DEF CON 27 的 logo（來源：DEF CON 27 官網）

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大型會議之一，由 Dark Tangent（本名 Jeff Moss）於 1993 年 6 月創立，每年固定於 7 月下旬或 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 27 屆（DEF CON 27）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的奪旗（Catch the Flag, CTF）競賽。近幾年為培養國內資安專業人才，臺灣 HITCON 團隊均派員參加比賽，也有不錯的成績。

(二)DEF CON 27 會議內容：

本屆會議於 108 年 8 月 8 日至 11 日在美國內華達州拉斯維加斯 Bally's & Paris、Flamingo、Planet Hollywood 等飯店舉辦。會議期間於各飯店同時舉辦多場演講及展示，以及多達 100 場以上的研討會，和 37 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。

由於美國總統大選將於 109 年舉行，CNN 也特別到拉斯維加斯 DEF CON 報導駭客們並非全是壞人，也希望做出好的貢獻，因此對電子投票系統進行資安檢查，並展示系統的弱點。此外，CNN 也報導了一種 deepfake 的偽造軟體，這種軟體可以模擬他人的表情並配上聲音，因此擔心被有心人士用來製作假新聞影響選舉[1]。

[1] https://www.cnn.com/2019/08/08/tech/def-con-vegas-lawmakers/index.html

與會者僅需在註冊處（Registration）繳交現金 300 美元，即可獲得一個電子識別證，但是其實並無預先或現場報名註冊的程序，因此大會並無留存與會者的身分。主辦單位統計 107 年參與人數超過 25,000 人，估計 108 年會議也大約有相當的參加人數。DEF CON 27 的議程如下：

1. 第一天（8 月 8 日）議程

FIRESIDES LOUNGE

FRIDAY

DO NO H4RM: A HEALTHCARE SECURITY CONVERSATION
Friday at 20:00 in Sin City Theatre at Planet Hollywood
Christian "quaddi" Dameff, Jeff "r3plicant" Tully MD, Suzanne Schwartz MD, Marie Moe PhD, Billy Rios, Jay Radcliffe

PANEL: DEF CON GROUPS
Friday at 22:15 in Sin City Theatre at Planet Hollywood
Brent White / B1TK1LL3R, Jayson E. Street, Darington, April Wright, Tim Roberts (byt3boy), Casey Bourbonnais, s0ups

SATURDAY

MEET THE EFF - MEETUP PANEL
Saturday at 20:00 in Sin City Theatre at Planet Hollywood
Kurt Opsahl, Camille Fischer, Bennett Cyphers, Nathan 'nash' Sheard, Shahid Buttar

WE HACKED TWITTER! AND THE WORLD LOST THEIR SH*T OVER IT!
Saturday at 22:15 in Sin City Theatre at Planet Hollywood
Mike Godfrey, Matthew Carr

-THURSDAY-

	DC 101 IN TRACK 4
10:00	**Exploiting Windows Exploit Mitigation for ROP Exploits** Omer Yair
11:00	**Breaking Google Home: Exploit It with SQLite (Magellan)** Wenxiang Qian, YuXiang Li, HuiYu Wu
12:00	**Are Quantum Computers Really A Threat To Cryptography? A Practical Overview Of Current State-Of-The-Art Techniques With Some Interesting Surprises** Andreas Baumhof
13:00	**Intro to Embedded Hacking – How you too can find a decade old bug in widely deployed devices. [REDACTED] Deskphones, a case study.** Philippe Laulheret
14:00	**Web2Own: Attacking Desktop Apps From Web Security's Perspective** Junyu Zhou, Ce Qin, Jianing Wang
15:00	**DEF CON 101 Panel** Highwiz, Nikita, Will, n00bz, Shaggy, SecBarbie, Tottenkoph
15:30	

2. 第二天（8 月 9 日）議程

-FRIDAY-

	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	**Behind the Scenes of the DEF CON 27 Badge** Joe Grand (Kingpin)	**Hacking Congress: The Enemy Of My Enemy Is My Friend** Former Rep. Jane Harman, Rep. James Langevin, Jen Ellis, Cris Thomas, Rep. Ted Lieu	**Behind the Scenes: The Industry of Social Media Manipulation Driven by Malware** Olivier Bilodeau, Masarah Paquet-Clouston	**Duplicating Restricted Mechanical Keys** Bill Graydon, Robert Graydon
11:00	**Don't Red-Team AI Like a Chump** Ariel Herbert-Voss	**The Tor Censorship Arms Race: The Next Chapter** Roger Dingledine	**All the 4G Modules Could Be Hacked** XiaoHuiHui, Ye Zhang, ZhengHuang	**Evil eBPF In-Depth: Practical Abuses of an In-Kernel Bytecode Runtime** Jeff Dileo
12:00	**Process Injection Techniques - Gotta Catch Them All** Itzik Kotler, Amit Klein	**Phreaking Elevators** WillC	**Infiltrating Corporate Intranet Like NSA_Pre-auth RCE on Leading SSL VPNs** Orange Tsai, Meh Chang	**API-Induced SSRF: How Apple Pay Scattered Vulnerabilities Across the Web** Joshua Maddux
13:00	**HackPac: Hacking Pointer Authentication in iOS User Space** Xiaolong Bai, Min (Spark) Zheng	**HVACking: Understand the Difference Between Security and Reality!** Douglas McKee, Mark Bereza	**No Mas—How One Side-Channel Flaw Opens Atm, Pharmacies and Government Secrets Up to Attack** phar	**More Keys Than A Piano: Finding Secrets In Publicly Exposed Ebs Volumes** xBen "benmap" Morris
14:00	**Harnessing Weapons of Mac Destruction** Patrick Wardle	**Are Your Child's Records at Risk? The Current State of School Infosec** Bill Demirkapi	**How Deep Learning Is Revolutionizing Side-Channel Cryptanalysis** Elie Bursztein, Jean Michel Picod	**Practical Key Search Attacks Against Modern Symmetric Ciphers** Daniel "ufurnace" Crowley, Daniel Pagan
15:00	**MOSE: Using Configuration Management for Evil** Jayson Grace	**Change the World, cDc Style: Cow tips from the first 35 years** Joseph Menn, Peiter Mudge Zatko, Chris Dildog Rioux, Deth Vegetable, Omega	**100 Seconds of Solitude: Defeating Cisco Trust Anchor With FPGA Bitstream Shenanigans** Jatin Kataria, Rick Housley, Ang Cui	**Relaying Credentials Has Never Been Easier: How to Easily Bypass the Latest NTLM Relay Mitigations** Marina Simakov, Yaron Zinar
16:00	**Please Inject Me, a x64 Code Injection** Alan Weinberg	**I Know What You Did Last Summer: 3 Years of Wireless Monitoring at DEF CON** d4rkm4tter (Mike Spicer)	**Surveillance Detection Scout - Your Lookout on Autopilot** Truman Kain	**The JOP ROCKET: A Supremely Wicked Tool for JOP Gadget Discovery, or What to Do If ROP Is Too Easy** Dr. Bramwell Brizendine, Dr. Joshua Stroschien
16:30	**Poking the S in SD cards** Nicolas Oberli	**Can You Track Me Now? Why The Phone Companies Are Such A Privacy Disaster** U.S. Senator Ron Wyden	**Breaking The Back End! It Is Not Always A Bug. Sometimes, It Is Just Bad Design!** Gregory Pickett	**Re: What's up Johnny?—Covert Content Attacks on Email End-to-End Encryption** Jens Müller

3. 第三天（8 月 10 日）議程

-SATURDAY-

	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	**Weaponizing Hypervisors to Fight and Beat Car and Medical Devices Attacks** Ali Islam, Dan Regalado (DanuX)	**Rise of the Hypebots: Scripting Streetwear** finalphoenix	**Information Security in the Public Interest** Bruce Schneier	**EDR Is Coming; Hide Yo Sh!t** Michael Leibowitz, Topher Timzen
11:00	**Your Car is My Car** Jmaxxz	**HAKC THE POLICE** Bill Swearingen	**Hacking Your Thoughts - Batman Forever meets Black Mirror** Katherine Pratt/GattaKat	**Meticulously Modern Mobile Manipulations** Leon Jacobs
12:00	**How You Can Buy AT&T, T-Mobile, and Sprint Real-Time Location Data on the Black Market** Joseph Cox	**Defeating Bluetooth Low Energy 5 PRNG for Fun and Jamming** Damien Cauquil (virtualabs)	**Why You Should Fear Your "mundane" Office Equipment** Daniel Romero, Mario Rivas	**Zombie Ant Farm: Practical Tips for Playing Hide and Seek with Linux EDRs** Dimitry Snezhkov
13:00	**RACE - Minimal Rights and ACE for Active Directory Dominance** Nikhil Mittal	**GSM: We Can Hear Everyone Now!** Campbell Murray, Eoin Buckley, James Kulikowski	**Tag-side attacks against NFC** Christopher Wade	**SSO Wars: The Token Menace** Alvaro Muñoz, Oleksandr Mirosh
14:00	**SELECT code_execution FROM * USING SQLite; -- Gaining code execution using a malicious SQLite database** Omer Gull	**I'm on your phone, listening - Attacking VoIP Configuration Interfaces** Stephan Huber, Philipp Roskosch	**Zero bugs found? Hold my Beer AFL! How To Improve Coverage-Guided Fuzzing and Find New Odays in Tough Targets** Maksim Shudrak	**Next Generation Process Emulation with Binee** Kyle Gwinnup, John Holowczak
15:00	**Get Off the Kernel if You Can't Drive** Jesse Michael, Mickey Shkatov	**Reverse-Engineering 4g Hotspots for Fun, Bugs and Net Financial Loss** g richter	**State of DNS Rebinding - Attack & Prevention Techniques and the Singularity of Origin** Gerald Doussot, Roger Meyer	**.NET Malware Threats: Internals And Reversing** Alexandre Borges
16:00	**Reverse Engineering 17+ Cars in Less Than 10 Minutes** Brent Stone	**NOC NOC. Who's there? All. All who? All the things you wanted to know about the DEF CON NOC and we won't tell you about** The DEF CON NOC	**Confessions of an Nespresso Money Mule: Free Stuff & Triangulation Fraud** Nina Kollars, Kitty Hegemon	**Vacuum Cleaning Security: Pinky and the Brain Edition** jiska, clou (Fabian Ullrich)
16:30	**Unpacking Pkgs: A Look Inside Macos Installer Packages And Common Security Flaws** Andy Grant		**Go NULL Yourself or: How I Learned to Start Worrying While Getting Fined for Other's Auto Infractions** droogie	**Apache Solr Injection** Michael Stepankin

4. 第四天（8 月 11 日）議程

-SUNDAY-

	TRACK 1	TRACK 2	TRACK 3	TRACK 4
10:00	**Backdooring Hardware Devices By Injecting Malicious Payloads On Microcontrollers** Sheila Ayelen Berta	**Adventures In Smart Buttplug Penetration (testing)** smea	**Hacking WebAssembly Games with Binary Instrumentation** Jack Baker	**Your Secret Files Are Mine: Bug Finding And Exploit Techniques On File Transfer App Of All Top Android Vendors** Xiangqian Zhang, Huiming Liu
11:00	**The ABC of Next-Gen Shellcoding** Hadrien Barral, Rémi Géraud-Stewart, Georges-Axel Jaloyan	**SDR Against Smart TVs: URL and Channel Injection Attacks** Pedro Cabrera Camara	**Exploiting Qualcomm WLAN and Modem Over The Air** Xiling Gong, Peter Pi	**Say Cheese - How I Ransomwared Your DSLR Camera** Eyal Itkin
12:00	**I'm In Your Cloud... Pwning Your Azure Environement** Dirk-jan Mollema	**Malproxying: Leave Your Malware at Home** Hila Cohen, Amit Waisel	**HTTP Desync Attacks: Smashing into the Cell Next Door** albinowax	**Help Me, Vulnerabilities. You're My Only Hope** Jacob Baines
13:00	**[MI CASA-SU CASA] My 192.168.1.1 is Your 192.168.1.1** Elliott Thompson	**Sound Effects: Exploring Acoustic Cyber-weapons** Matt Wixey	**Owning The Clout Through Server-Side Request Forgery** Ben Sadeghipour, Cody Brocious (Daeken)	**Want Strong Isolation? Just Reset Your Processor** Anish Athalye
14:00	**Firmware Slap: Automating Discovery of Exploitable Vulnerabilities in Firmware** Christopher Roberts	**Cheating in eSports: How to Cheat at Virtual Cycling Using USB Hacks** Brad Dixon	**The Ether Wars: Exploits, counter-exploits and honeypots on Ethereum** Bernhard Mueller, Daniel Luca	**Contests Awards Ceremony** Contests & Events
15:00	**Closed**			
16:00	**Closing Ceremonies** The Dark Tangent & Goons			

(三)CTF 競賽：

DEF CON 會議有一項重要的活動就是奪旗（CTF, Catch the Flag）競賽，臺灣在本屆獲得參賽資格的隊伍是 HITCON BFKinesiS（應該是 107 年的 HITCON 與 BFS 聯手組隊），已經在這項 CTF 競賽中，連續於 103 年、104 年、105 年、106 年、107 年分別獲得全球第 2 名、第 4 名、第 4 名、第 2 名、第 3 名的好成績。臺灣 HITCON 戰隊的領隊李倫銓認為，若以 CTF 競賽作為資安人才的培訓的指標，名次不是最好的參考基準，反而是以各國可以入圍參加 CTF 決賽的隊伍數量，代表資安人才培育數量的增加，才能慢慢將資安的能量從量變進展到質變。

由於 107 年增加到 25 隊參賽，包括網路和出題的伺服器都出現服務中斷的現象，因此 108 年回復傳統，來自各國僅有 15 隊獲得參加決賽。主辦單位 O.O.O.（Order-of-the-Overflow）的 CTF 賽制已不再是單純的網路攻防（Attack and Defense），而是混合 King of the Hill 的賽制，除了考驗參賽隊伍挖掘漏洞的能力之外，也考驗隊伍防守的能力。

經過激烈的競賽後，結果由美國 Plaid Parliament of Pwning 隊獲得冠軍，臺灣的 HITCON BFKinesiS 戰隊則獲得亞軍的好成績，中國大陸 Tea Deliverers 則獲得季軍。

圖 2、CTF 競賽會場情形（來源：iThome）

圖 3、臺灣 HITCON 戰隊 BFKinesiS 領獎（來源：iThome）

SCOREBOARD AT GAME END

All event data will be released in few days, and most of it was available (with a delay) to players during the first two game days.

We strive to be fully transparent and welcome recalculations. For more info see our philosophy.

TOTAL		Attack		Defense		KoH	
973	Plaid Parliament of Pwning	1442	Plaid Parliament of Pwning	213	Plaid Parliament of Pwning	769	HITCON⚔BFKinesiS
▲772	HITCON⚔BFKinesiS	1006	HITCON⚔BFKinesiS	159	A*0*E	664	Plaid Parliament of Pwning
▲590	Tea Deliverers	815	Tea Deliverers	156	HITCON⚔BFKinesiS	477	A*0*E
▼564	A*0*E	656	mhackeroni	147	mhackeroni	459	Tea Deliverers
▲556	mhackeroni	646	Samurai	132	r3kapig	443	KaisHack GoN
▼399	Samurai	510	A*0*E	130	Tea Deliverers	405	Sauercloud
▼375	Sauercloud	499	r00timentary	127	Sauercloud	377	mhackeroni
▲359	r00timentary	339	SeoulPlusBadAss	111	r00timentary	370	SeoulPlusBadAss
▼331	SeoulPlusBadAss	292	saarsec	100	Samurai	333	TokyoWesterns
▼284	Shellphish	131	r3kapig	98	Shellphish	269	Shellphish
284	r3kapig	114	Sauercloud	88	KaisHack GoN	173	saarsec
▼281	KaisHack GoN	109	Shellphish	75	SeoulPlusBadAss	123	Samurai
▼235	saarsec	106	CGC	58	saarsec	59	CGC
▼215	TokyoWesterns	96	TokyoWesterns	54	TokyoWesterns	46	r00timentary
▲110	CGC	8	hxp	35	CGC	5	hxp
67	hxp	2	KaisHack GoN	34	hxp	0	r3kapig

圖 4、CTF 競賽成績（來源：DEF CON 27 官網）

(四)會議花絮：

每個人在 DEF CON 27 會議註冊處繳交最低 300 美元入場費後（其他還有 600、900、1,200 以上等額度），可拿到一個石英材質圓盤狀的電子入場證，此證件沒有特殊作用，只有 LED 會慢慢發亮，而且它與 107 年的電子入場證不同，沒有連結電腦的接頭。（如下圖）

圖 5、107 年電子入場證（來源：DEF CON 27 官網）

圖 6、108 年電子入場證（來源：個人）

此外，會場 SWAG 禮堂則是專門販售紀念品、駭客的軟硬體工具，甚至是萬能鑰匙（如下圖）

圖 7、紀念品販售會場（來源：個人）

二、會議重點摘要

(一) BREAKING GOOGLE HOME: EXPLOIT IT WITH SQLITE (MAGELLAN)

1、講者：Wenxiang Qian (Senior security researcher at Tencent Blade Team)、YuXiang Li (Senior security researcher at Tencent Blade Team)、HuiYu Wu (Senior security researcher at Tencent Blade Team)

2、時間：8 月 8 日

3、摘要：

來自中國大陸的騰訊公司刀鋒團隊（Tencent Blade Team）在過去幾年間，使用了幾種新方法來識別 SQLite 和 Curl 中的多個關鍵漏洞，這是兩個最廣泛被使用的基本軟體庫。他們將這兩組影響了許多設備和軟體的漏洞分別命名為“Magellan”和“Dias”。

他們又利用這些漏洞嘗試入侵了一些最受歡迎的物聯網設備，例如 Google Home with Chrome。並且還利用此漏洞入侵最廣泛使用的 Web 服務器（Apache + PHP）和開發人員最常用的工具之一（Git）。

他們以演示方式分享如何嘗試從硬體及軟體方面破解 Google Home，獲取和分析最新的韌體，並通過 Fuzz 和年度檢視來發現 SQLite 和 Curl 的漏洞。通過這些方法，他們在 SQLite 找到了漏洞，編號為 CVE-2018-20346、CVE-2018-20505、CVE-2018-20506，命名為“Magellan”，一組共三個堆疊緩衝區溢位和堆疊數據洩漏的漏洞。另外在 Curl 發現了漏洞，編號為 CVE-2018-16890、CVE-2019-3822，命名為“Dias”，為一組兩個遠端內存洩漏和堆疊緩衝區溢位的漏洞。

考慮這些漏洞影響了許多系統和軟體，他們發布了漏洞警報，通知易受攻擊的供應商，這次會議是首次揭露這兩組漏洞的細節，並重點介紹一些新的漏洞探討技術。最後，他們也提供基礎軟體庫開發人員一些

安全開發建議作為總結。

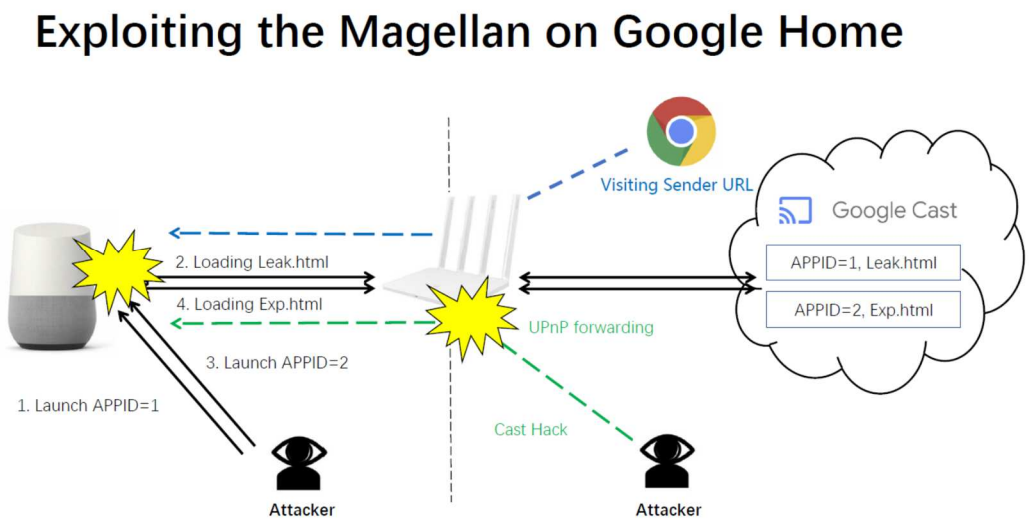

圖 8、利用 Google Home 漏洞示意圖（來源：簡報）

(二) ARE QUANTUM COMPUTERS REALLY A THREAT TO RYPTOGRAPHY? A PRACTICAL OVERVIEW OF CURRENT STATE-OF-THE-ART TECHNIQUES WITH SOME INTERESTING SURPRISES

1、講者：Andreas Baumhof (Vice President Quantum Technologies, Quintessence Labs Inc.)

2、時間：8 月 8 日

3、摘要：

講者先說明 Shor 整數分解運算法是加密機制（RSA/ECC）的一大威脅，因為它的運算將指數運算複雜度降低到只有多項式運算的複雜度。這意味著量子電腦可以將破解 RSA-2048 的時間縮短到僅僅 10 秒鐘。然而，目前受雜訊影響的 NISQ 型量子電腦局限於 16 位 RSA 密鑰。而且當前量子位元的品質還不夠好，誤差修正的成本至少是量子位元數量的 100 倍。

然而世界已經朝向量子電腦發展，但目前還沒有擁有足夠大的 Shor 運算法通用型量子電腦。量子鍛鍊法（Quantum Annealing）在 108 年 1 月

使用 97 個位元來計算一個 20 位的數字。當量子位元實際上足以算出更大的數字，假設線性可擴展性，“僅”需要大約 10,000 個量子位元來計算 2,048 位 RSA 密鑰。D-Wave 宣布推出一款具有 5,640 個量子位元的量子電腦，因此很快就能實現這一目標。

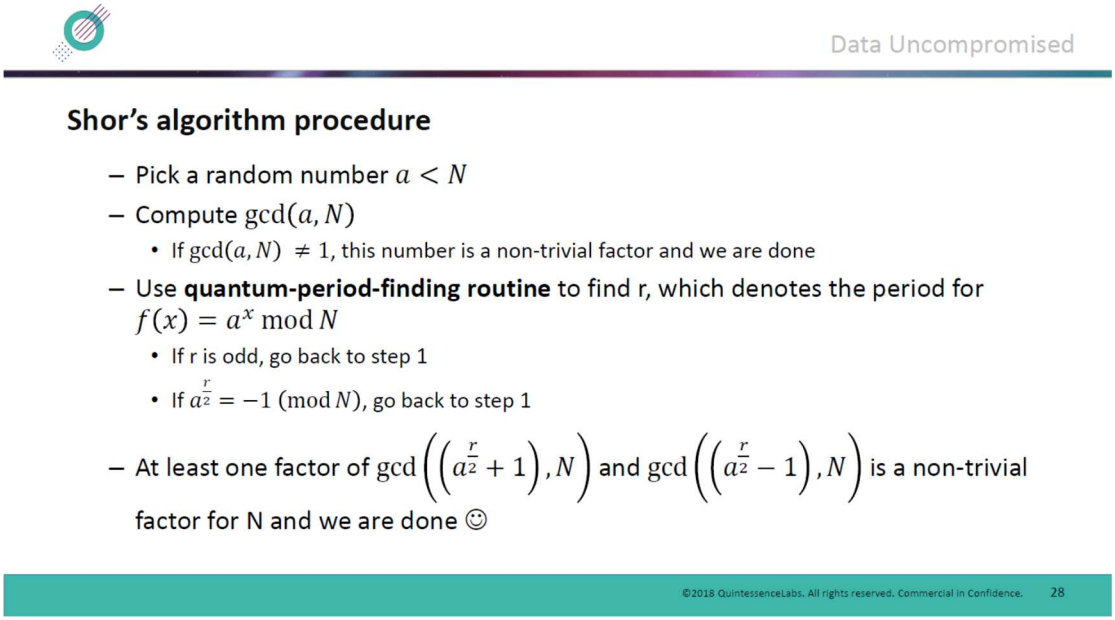

圖 9、Shor 運算法（來源：簡報）

(三) BEHIND THE SCENES: THE INDUSTRY OF SOCIAL MEDIA MANIPULATION DRIVEN BY MALWARE

1、講者：Olivier Bilodeau (Cybersecurity Research Lead at GoSecure Masarah Paquet-Clouston)

2、時間：8 月 9 日

3、摘要：

講者的調查始於分析物聯網殭屍網路，以發現社交媒體操縱（SMM）背後存在的結構化行業。SMM 是通過社交媒體上的關注者或活動來支付受歡迎程度的故意行為。

講者採取由下而上的方法，研究殭屍網路：建立 Honeypot，用惡意軟體感染它們，並對 Honeypot 流量進行中間人攻擊，以接取 C&C 和社交網路之間的 HTTPS 解密內容。然後，分析大數據集，從而發現社交媒

體操縱供應鏈的參與者。

調查路徑包括流量分析，各種 OSINT 方法，逆向工程軟體，自動使用和創建假帳號，論壇調查和定性分析。然後討論潛在的獲利能力，以及該供應鏈中的收入分配，證明每個銷售假冒產品收入最高的不是惡意軟體作者，而是供應鏈末端的操縱者。

(四) ALL THE 4G MODULES COULD BE HACKED

1、講者：XiaoHuiHui (Senior Security Researcher, Baidu), Ye Zhang (Security Researcher, Baidu), ZhengHuang (Leader of Baidu Security Lab X-Team, Baidu)

2、時間：8 月 9 日

3、摘要：

如今越來越多的 4G 模組被內建到全球的物聯網設備中，例如自動販賣機，汽車娛樂系統，筆記型電腦，廣告看板和戶外錄影機等。但是沒有人對 4G 模組進行過全面的安全研究。講者進行了這項計畫，並測試了市場上主要品牌的 4G 模組（超過 15 種不同類型）。結果顯示它們都具有類似的漏洞，包括使用弱密碼進行遠端接取，命令注入 AT 命令/監聽服務，OTA 升級欺騙，通過 SMS 進行命令注入以及 Web 漏洞等。利用這些漏洞，講者獲得這些設備的 Shell 軟體。

除了以 Wi-Fi 來利用這些漏洞之外，講者還創建了一種通過虛擬基站系統進行攻擊的新方法，通過訪問行動通信網路的內部網路觸發，成功運行了遠端命令執行而無需任何必要條件。最後講者也演示如何利用這些漏洞攻擊各種品牌的汽車娛樂系統並獲得汽車的遠端控制權。

(五)INFILTRATING CORPORATE INTRANET LIKE NSA_PRE-AUTH RCE ON LEADING SSL VPNS

1、講者：Orange Tsai (Principal Security Researcher from DEVCORE, Member of HITCON, Member of CHROOT Security Group , Captain of HITCON CTF team), Meh Chang (Security Researcher from DEVCORE , Member of HITCON

CTF team)

2、時間：8 月 9 日

3、摘要：

電腦安全已經是一個公共政策議題。選舉安全、區塊鏈、突然終止通信（稱為變暗）、股市交易漏洞、物聯網安全、資料隱私、運算法安全性和公平性、關鍵基礎設施等，這些都是具有強大網際網路安全組件的重要公共政策議題。

雖然對涉及的資通技術的理解是制定良好政策的基礎，但資通技術專家很少參與政策討論。因此需要公共利益的資通技術人員，幫助制定政策，並致力於更廣泛的公共利益工作的機構和團體提供安全保障。另外，也需要政府、非政府組織、大學教授、媒體及私人公司內部的人一起努力。如此才能對公共安全和社會整體福利有幫助。

講者描述公共利益資通技術的現況，也提出了發展的方向。在網際網路時代的決定性政策議題是：我們的生活應該受資通技術控制多少，以什麼條件管理？透過 SSL VPN 可以保護企業資產免受網際網路資安風險的威脅，但是如果 SSL VPN 本身就很容易受到攻擊呢？

接觸了網際網路，信任及可靠性是保護內部網路的唯一方法。但是，在多個領先的 SSL VPN 上卻發現了預先驗證的遠端程式碼執行（RCE, Remote Code Execution)，近半數財富雜誌 500 大企業和許多政府機構都在使用。更糟糕的是講者發現了一個“神奇”的後門，它允許更改任何用戶密碼卻無需憑證！

為了展示這件事情，講者展示了從唯一暴露的 HTTPS 介面獲取 root shell，秘密地將伺服器及其所有者武器化，並濫用隱藏功能來接管所有 VPN 客戶端！

在這種複雜的閉源系統中，從盒子外取得 root shell 很不容易。講者採用先進的 Web 和二進制開發技術來獲得 root shell 的方法，這涉及利用 Web 架構中的缺陷，硬核 Apache jemalloc 等。在獲得 root shell 之後，講者說明後期開發及如何破解客戶端。另一方面，講者也推導出一般強化

操作，不僅可以緩解上述所有攻擊，還可以緩解任何其他潛在的 0-day 攻擊。

講者揭露了能危及數百萬設備的實際攻擊，經過發布這些技術和方法後，希望能激發更多資安研究人員避免開箱即用的想法，企業則可以應用立即緩解資安威脅，並認識到 SSL VPN 不僅僅是虛擬專用網，而且還可能是“網路的脆弱點”。

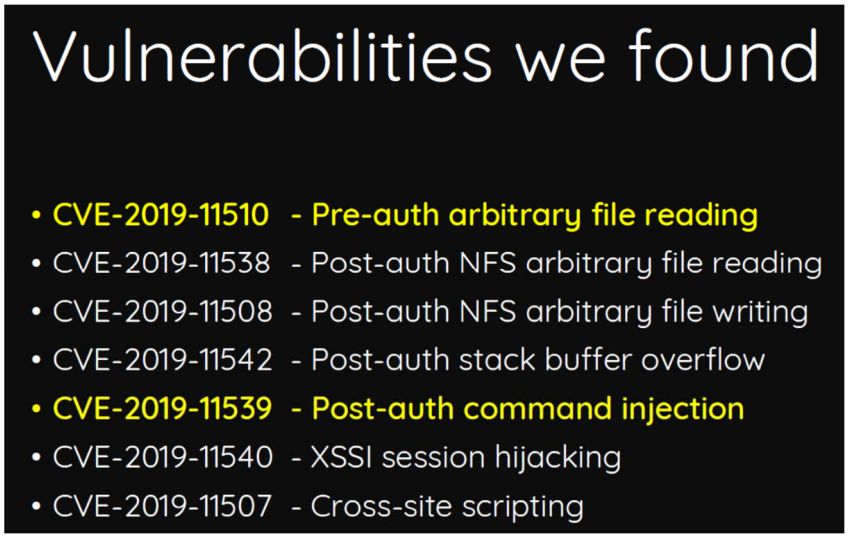

圖 10、臺灣 HITCON 找到的 SSL VPN 漏洞（來源：DEF CON 27 官網）

(六) GSM: WE CAN HEAR EVERYONE NOW!

1、講者：Campbell Murray (Global Head Cybersecurity Delivery, BlackBerry), Eoin Buckley (Senior Cybersecurity Consultant), James Kulikowski (Senior Cybersecurity Consultant)

2、時間：8 月 10 日

3、摘要：

講者說明用於保護行動通信網路通話服務的 A5/1 和 A5/3 密碼的安全性易受危害，將導致 GSM 通信被完全解密，他們使用免費的開源軟體解決方案及為此任務自行開發的工具。

這次研究的是 GSM 設計上的核心錯誤。實務上，技術標準要求 GSM 的訊息需要先使用卷積碼進行錯誤控制編碼後再加密。目前絕大多

數是使用 A5/1 或 A5/3 密碼執行加密。卷積碼為發送的訊息增加了冗餘碼，以識別用於 GSM 訊息的密鑰。

為了利用此漏洞，攻擊者只需捕獲傳輸並識別使用的 GSM 通道。技術標準定義了卷積碼，因此可以利用冗餘碼回復加密金鑰。

講者除了演示使用 A5/3 加密被動捕獲的 GSM 流量，並演示了一種新穎的解決方案，可以在不與行動通信設備或行動通信網路通信的情況下被破解密鑰。

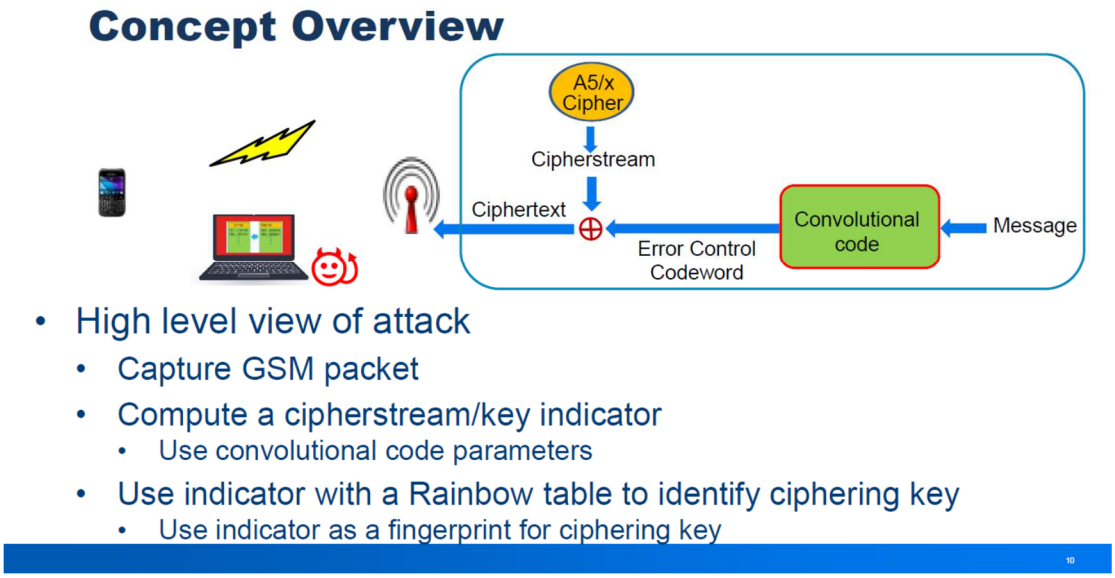

圖 11、GSM 攻擊示意圖（來源：簡報）

(七) I'M ON YOUR PHONE, LISTENING － ATTACKING VoIP CONFIGURATION INTERFACES

1、講者：Stephan Huber (Fraunhofer SIT), Philipp Roskosch

2、時間：8 月 10 日

3、摘要：

雖然所有類型的物聯網設備都可能連上網際網路，也暴露在駭客攻擊威脅下，但是最古老的 IoT 設備之一，幾乎無處不在的 VoIP 電話，似乎被人們遺忘了。

由於配置和管理的目的，VoIP 電話在設備上運行 Web 應用程式。講者就在 Web 應用程式和網路伺服器中發現了幾個關鍵錯誤漏洞（已經成為 CVE），因此可以劫持 VoIP 電話。

他們從簡單的 XSS 和 CSRF 問題開始，通過命令注入和內存損壞直到遠端程式碼執行，可以在這些設備上找到所有常見的漏洞。講者展示研究成果及使用的工具和策略。

此外，講者提供有用的 ARM shell 程式碼模式，腳本和技巧，駭客可以用它們來找尋漏洞。最後通過展示自動化工具是無法發現此類漏洞，因此，講者表示，仍然需要手動來進行 IoT 設備的滲透測試。

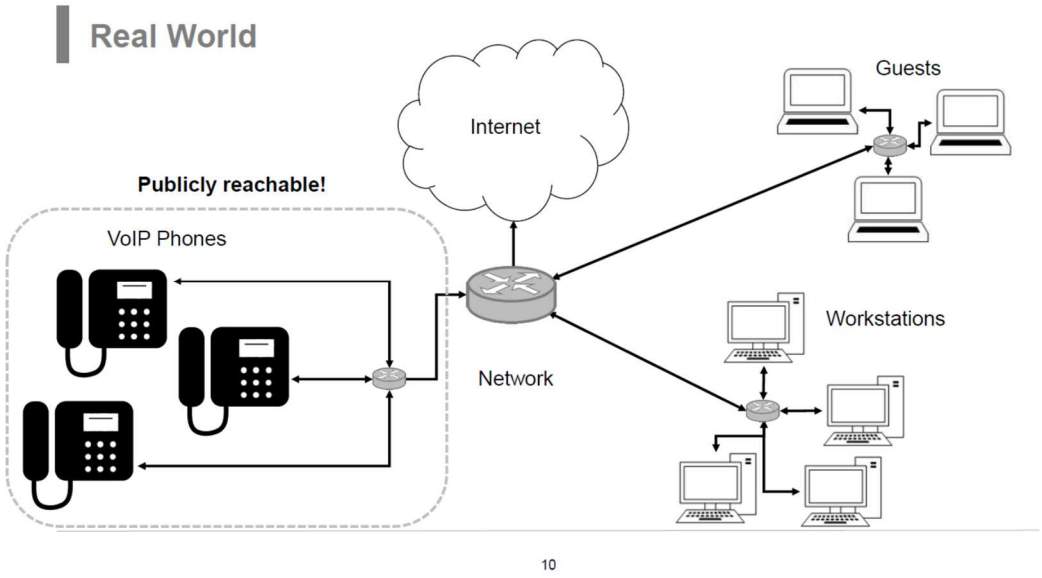

圖 12、VoIP 實際連線示意圖（來源：簡報）

(八) THE ABC OF NEXT-GEN SHELLCODING

1、講者：Hadrien Barral (Hacker), Rémi Géraud-Stewart (Hacker), Georges-Axel Jaloyan (PhD Student at ENS)

2、時間：8 月 11 日

3、摘要：

Shellcode 是簡短的可執行存根，只要可以執行程式碼，就可以在各種攻擊情形中使用 Shellcodes。除了明顯運作逆 Shell 之外，必須處理 shell 程式碼通常不是特別隱蔽的現實，部分原因是非可疑的存在可印的

字母。講者揭示了用於編寫以前從未所見，特別是英數字的 shellcode 和攻擊平臺的新方法。

(九) BACKDOORING HARDWARE DEVICES BY INJECTING MALICIOUS PAYLOADS ON MICROCONTROLLERS

1、講者：Sheila Ayelen Berta (Security Researcher)

2、時間：8 月 11 日

3、摘要：

微控制器負責控制各種有趣的系統，例如實體安全系統、汽車 ECU、信號燈、電梯、傳感器、工業系統關鍵組件、家用電器，甚至機器人。講者解釋微控制器如何進行後門處理，並回顧微控制器（microcontroller）的基本知識後，深入探討實現有效程式碼注入的三種方法。第一種方法包括定位韌體的入口點，並注入有效程式碼。第二種技術較複雜，該硬體外圍設備的程式碼程序，為 EUSART 通信提供後門注入惡意有效程式碼；通過檢查微控制器中斷向量處的 GIE，PEIE 和探詢過程，就能獲得正確的儲存器位址。最後，第三種技術允許通過操縱堆疊在 TOS 寫入儲存器位址來操控微控制器的程式流程。透過這種方式，就可以執行在原始程式中編寫的有效指令程式，像 ROP（Return-oriented programming）[2]鏈技術一樣執行。

[2] ROP （Return-oriented programming）是一種電腦安全漏洞利用技術，其中攻擊者使用對調用堆疊的控制，在現有程序碼中的子程序中的返回指令之前，間接執行挑選機器指令或機器指令組，類似於執行一個緒程式碼解譯器。

參、心得及建議

一、臺灣資安實力獲國際肯定

代表臺灣參與 DEF CON 27 CTF 競賽的 HITCON BFKinesiS 戰隊，在本屆最終獲得第 2 名的佳績（僅次於第 1 名的 Plaid Parliament of Pwning）。是自 103 年參賽以來，連續六年獲得佳績，讓人驚豔。

由於臺灣資安實力已受到國際肯定，每年在臺灣舉辦的 HITCON CTF 競賽已獲得 DEF CON CTF 主辦單位指定為來年 DEF CON 決賽第一個種子賽事，吸引全球為數眾多的隊伍參賽，而獲得 HITCON 競賽冠軍的隊伍，就可以直接晉級來年的 DEF CON CTF 總決賽。

二、資安需要持續投資

隨著資通訊科技的日新月異，資通訊設備已經深入人民生活且無處不在，加上商用電腦設備及開源碼軟體的結合，使得資安議題日益重要，亟需政府機關及民間企業關注，並需要長期投入資源，培養資安人才，才能因應各種資安威脅及挑戰。

在 108 年 1 月 1 日通過施行資通安全管理法之後，無論是政府機關、行政法人、八大關鍵基礎設施，都必須重視資安議題，也必須攜手合作，共同防範資安威脅。

臺灣的資訊及通信科技發達，大學院校設立相關科技眾多，因此政府應主動與相關資安團體合作，規劃整體資通安全科技研發與推動機制，建立新興技術相關實驗場域，以提升國家整體資安自主技術能量，帶動資安人才的培育，充實各行各業各階層的資安人力。

三、各行各業都應重視資安

由於 5G 網路將逐漸深入社會，加上物聯網的發展，AI 人造智慧的逐漸成

熟，各行各業除了能透過網際網路獲得更良好更精準的服務效能與品質之外，更重要的是，隨之而來的資安威脅及風險的提高，因此，資安議題已經不只是政府機關或者資通訊產業才需重要的議題，而是生活在現代化資訊社會只要使用了連網設備及服務的各行各業人士，都應該時時刻刻重視的事情。大家必須提高警覺，隨時隨地加強資安意識，避免錯誤的使用資通設備，才能不讓個人或者財務資訊洩漏。

肆、附錄

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

DEFCON 27 官網：https://www.defcon.org/html/defcon-27/dc-27-index.html

DEFCON 27 資料庫：https://media.defcon.org/DEF%20CON%2027/

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

iThome 官網：https://ithome.com.tw/news/132347

出國人員與會照片：