出國報告（出國類別：其他國際會議）

Blackhat USA 2013 & DEF CON 21
出國報告

服務機關：行政院資通安全辦公室
姓名職稱：周智禾 諮議
派赴國家：美國拉斯維加斯
出國期間：102 年 7 月 30 日至 102 年 8 月 6 日
報告日期：102 年 10 月 23 日

摘　　要

Blackhat USA 2013 及 DEF CON 21。近年來，網路攻擊事件頻傳，資訊安全問題已成為國際關注之重要議題，各國亦定期召開資安相關會議以交流最新資安發展趨勢，包含 Blackhat、DEF CON 及 RSA Conference 等。其中，Blackhat 係由 Blackhat 公司所舉辦之知名網路安全攻防技術研討會，而 DEF CON 則為全球最盛大的資訊安全會議，兩者均由美國每年於拉斯維加斯舉辦，內容包含豐富的資安趨勢論壇及最新的資安軟硬體設備展覽，已成為國際間每年重要的資訊安全會議。

本(102)年 Blackhat 係於拉斯維加斯 Caesars Palace 召開 2 日研討會(7 月 31 日至 8 月 1)，並邀請美國國家安全局局長(Keith B. Alexander)及美國太空總署噴射推進實驗室研究員(Brian Muirhead)擔任大會專題演講者；DEF CON(第 21 次)則於拉斯維加斯 Rio Hotel 舉辦為期 3 日研討會(8 月 2 至 4 日)，會議包含多場次的資安研討會及相關競賽。

透過上開二會議，我們可以觀察到近來掘起的資安技術及標準、最新的駭客研究，會議中亦發表許多被揭露出的安全議題，包括雲端、行動裝置、網頁技術及滲透測試相關議題等。本次會議主題除了傳統的網站應用安全議題外，車載(Vehicle)系統安全性及行動裝置駭侵技術的議題亦在此次的會議中受到相當程度的重視。

目　　錄

壹、會議介紹

一、會議名稱

2013 年黑帽大會(Blackhat USA 2013)

第 21 屆戰備大會(DEF CON 21)

二、會議時間

Blackhat USA 2013：2013 年 7 月 31 至 2013 年 8 月 1 日 (美國時間)

DEF CON 21：2013 年 8 月 2 至 2013 年 8 月 4 日(美國時間)

三、會議地點

Blackhat USA 2013：凱撒皇宮大酒店(Caesars Palace Hotel)

DEF CON 21：里奧酒店(Rio All-Suite Hotel)

四、會議相關文件

Blackhat USA 2013 相關資料請詳見網站(http://www.blackhat.com/)

DEF CON 21 相關資料請詳見網站(http://www.defcon.org/)

貳、參加會議目的

每年於美國所舉辦的 Blackhat 及 DEF CON 會議是資訊安全產業最重要的會議之一，亦是受到世界矚目的資安焦點，資訊安全專家會透過此交流平臺發表最新的系統或軟體漏洞，或是提出資安防護方面的議題，包括尚未公開的弱點揭露、攻擊程式的撰寫、新型態惡意程式的利用技術、逆向工程技術及數位人員鑑識等。無論是在攻擊或防禦上，Blackhat 與 DEF CON 會議都提供資訊安全專家不同的思考方向，瞭解目前最新的資安技術，作為攻擊或防禦的重要參考依據。

本次出國參加 Blackhat USA 2013 與 DEF CON 21，主要希望能從這些議題中瞭解最新資安威脅並掌握國際發展趨勢，除了提升本身對資安議題的認知外，亦期望藉由演講中所獲取的新知與技術，瞭解目前駭客最新的技術，增廣資訊安全上見聞，俾提供業務或決策方面上的協助。

參、會議過程及重點議題

一、會議過程

Blackhat USA 2013 共包括 6 天，前 4 天為教育訓練(7 月 27-30 日)，後 2 天則為 Briefings(7 月 31 日及 8 月 1 日)，而 DEF CON 21 則包含 3 天的 Briefings(8 月 2-4 日)，上開 2 會議內容如表 1，本次出國行程主要參加 Blackhat USA 2013 及 DEF CON 21 的 Briefings 部分。

表 1：Blackhat USA 2013 及 DEF CON 21 會議內容

會議名稱	日期	內容
Blackhat USA 2013	7 月 27 日	Trainings
	7 月 28 日	Trainings
	7 月 29 日	Trainings
	7 月 30 日	Trainings, Executive Summit
	7 月 31 日	**Briefings**, Arsenal, Sponsored Workshops
	8 月 1 日	**Briefings**, Arsenal
DEF CON 21	8 月 2 日	**Briefings**
	8 月 3 日	**Briefings**
	8 月 4 日	**Briefings**

(二) Blackhat USA 2013

為期 2 天的 Blackhat Briefing，每天的議程皆以 Keynote 揭幕，議程有別以往分為 8 個大類，本次平行的議程達 9 個，而每個議程透過 11 種類別進行交叉描述，該 11 種類別包括 AppSec、DDoS、Malware、Cellular、Hardware/Low Lovel、Social、Mobile、SCADA、Network、Defense、Exploit Development、Management、Crypto 及 Consumer 等，包含了 49 個現場實機展示，至少 35 個零日(zero-day)攻擊，議程詳見表 2 及表 3。

表 2：Blackhat USA 2013 第 1 天 Briefing 議程(7 月 31 日)

時間	議題
0900-1000	Keynote Speaker: General Keith B. Alexander

1015-1115	➢ Mainframes: The Past Will Come to Haunt You (Philip Young) ➢ BlackberryOS 10 From a Security Perspective (Falf-Philipp Weinmann) ➢ With BIGDATA comes BIG responsibility: Practical exploiting of MDX injections (Dmitry Chastuhin) ➢ New Trends in FastFlux Networks((Wei Xu + Xinran Wang) ➢ CrowdSource: An Open Source, Crowd Trained Machine Learning Model for Malware Detection (Joshua Saxe) ➢ Lessons from Surviving a 300Gbps Denial of Service Attack (Matthew Prince) ➢ Combating the Insider Threat at the FBI: Real-world Lessons Learned ➢ Beyond the Application: Cellular Privacy Regulatory Space (Christie Dudley) ➢ Legal Considerations for Cellular Research (Marcia Hofmann) ➢ Java every-Days: exploiting Software Running on Three Billion Devices((Brian Gorenc +Jasiel Spelman) ➢ How to Build a SpyPhone((Kevin McNamee)
1145-1245	➢ Black-box Assessment of Pseudorandom Algorithms (Derek Soeder + Christopher Abad + Gabriel Acevedo) ➢ Shattering Illusions in Lock-Free Worlds: Compiler/Hardware Behaviors in OSes and VMs (Marc Blanchou) ➢ Password Hashing: The Future is Now (JP Aumasson) ➢ Power Analysis Attacks for Cheapskates (Colin O' Flynn) ➢ Denying Service to DDoS Protection Services (Allison Nixon) ➢ Denial of Service as a Service – Asymmetrical Warfare at its Finest (Robert Masse) ➢ What Security Researchers Need to Know About Anti-Hacking Law (Marcia Hofmann) ➢ Just-in-time Code Reuse: The More Things Change, the More they Stay the Same (Kevin Snow + Lucas Davi) ➢ A Tale of One Software Bypass of Windows 8 Secure Boot (Yurity

	Bulygin + Oleksandr Bazhaniuk + Andrew Furtak) ➢ TLS 'Secrets' (NextGen$) ➢ Million Browser Botnet (Jeremiah Grossman + Matt Johansen)
1415-1515	➢ End-to-end Analysis of Domain Generating Algorithm Malware Family (Jason Geffner) ➢ Pass the Hash and Other Credential Theft and Reuse: Mitigating the risk of Lateral Movement and Privilege Escalation(Mark Simos + Patrick Jungles) ➢ Flying In the Dark - All the Things Not to Do When Hacking Hardware (Matthew Watchinski) ➢ Universal DDoS Mitigation Bypass (Tony Miu + Albert Hui + Wai Leng) ➢ Legal Aspects of Full-spectrum Computer Network (Active) Defense (Robert Clark) ➢ BIOS Security (John Butterworth +Corey Kallenberg +Xeno Kovah) ➢ I Can Hear You Now: Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell (Tom Ritter + Doug DePerry +Andrew Rahimi) ➢ Lawful Access Panel (Matt Blaze & Brewster Kahle &Jennifer Valentino-DeVries & Alan Davidson) ➢ Evading Deep Inspection for Fun and Shell (Opi Niemi + Antti Levomaki)
1530-1630	➢ JavaScript Static Security Analysis Made Easy with JSPrime (Nishant Das Patnaik +Sarathi Sabyasachi Sahoo) ➢ How to grow a TREE (Taint-Enabled Reverse Engineering Environment) from a CBASS (Cross-platform Binary Automated Symbolicexecution System) (Nathan Li + Loc Nguyen +Xing Li + James Just) ➢ Maltego Tungsten As a Collaborative Attack Platform (Roelof Temmingh + Andrew MacPherson) ➢ Untwining Twine (Jon Chittenden + Anson Gomes) ➢ LTE Booms with Vulnerabilities (Ankit Gupta)

	➢ A Practical Attack Against MDM Solutions (Daniel Brodie + Michael Shaulov) ➢ TOR… ALL-THE-THINGS! (Jason Geffner) ➢ Truncating TLS Sessions to Violate Beliefs (Ben Smyth + Alfredo Pironti) ➢ Buying into the Bias: Why Vulnerability Statistics Suck (Jericho + Steve Christey) ➢ Clickjacking Revisited: A Perceptual View of UI Security (Devdatta Akhawe) ➢ OPSEC Failures of Spies (Matthew Cole) ➢ Let's Get Physical: Breaking Home Security Systems and Bypassing Building Controls (Drew Porter + Stephen Smith)
1700-1800	➢ The Web IS Vulnerable: XSS Defense on the BattleFront (Greg Wroblewski + Ryan Barnett) ➢ Malicious File for Exploiting Forensic Software (Takahiro Haruyama + Hiroshi Suzuki) ➢ Predicting Susceptibility to Socialbots on Twitter (Chris Sumner + Randall Wald) ➢ BinaryPig - Scalable Malware Analytics in Hadoop (Zachary Hanif + Telvis Calhoun + Jason Trost) ➢ Smashing the Font Scaler Engine in Windows Kernel (Ling Chuan Lee + Lee Yee Chan) ➢ Pixel-Perfect Timing Attacks with HTML5 (Paul Stone) ➢ Hacking, Surveilling, and Deceiving Victims on Smart TV (SeungJin 'Beist' Lee) ➢ How CVSS is DOSsing Your Patching Policy (and wasting your money) (Luca Allodi + Fabio Massacci) ➢ Hiding @ Depth - Exploring, Subverting, and Breaking NAND Flash Memory (Josh 'mOnk' Thomas) ➢ Mactans: Injecting Malware Into iOS Devices via Malicious Chargers (Billy Lau + Yeongjin Jang + Chengyu Song)

表 3：Blackhat USA 2013 第 2 天 Briefing 議程(8 月 1 日)

時間	議題
0900-1000	Keynote Speaker: Brian Muirhead
1015-1115	➢ CMX: IEEE Clean File Metadata Exchange (Mark Kennedy + Igor Muttik) ➢ Mobile Malware: Why the Traditional AV Paradigm is Doomed, and How to Use Physics to Detect Undesirable Routines (Guy Stewart) ➢ Pass-the-Hash 2: The Admin's Revenge (Skip Duckwall) ➢ Abusing Web APIs Through Scripted Android Applications (Daniel Peck) ➢ Big Data for Web Application Security (Mike Arpaia + Kyle Barry) ➢ The SCADA That Didn't Cry Wolf - Who's Really Attacking Your ICS Devices - Part Deux! (Kyle Wilhoit) ➢ Mobile Rootkits: Exploiting and Rootkitting ARM TrustZone (Thomas Roth) ➢ Fully Arbitrary 802.3 Packet Injection: Maximizing the Ethernet Attack Surface (Andrea Barisani + Daniele Bianco) ➢ Bluetooth Smart: The Good, the Bad, the Ugly, and the Fix! (Mike Ryan) ➢ Honey, I'm Home!! – Hacking Z-Wave Home Automation Systems (Behrang Fouladi + Sahand Ghanoun) ➢ The Factoring Dead: Preparing for Cyptopocalypse (Alex Stamos + Thomas Ptacek + Tom Ritter)
1145-1245	➢ Bochspwn: Identifying 0-Days via System-Wide Memory Access Pattern Analysis (Mateusz 'j00ru' Jurczyk + Gynvael Coldwind) ➢ Energy Fraud and Orchestrated Blackouts: Issues with Wireless Metering Protocols (wM-Bus) (Cyrill Brunschwiler) ➢ Dissecting CSRF Attacks and Countermeasures (Mike Shema + Sergey Shekyan + Vaagn Toukharian) ➢ Hunting the Shadows: In-Depth Analysis of Escalated APT

	Attacks (Fyodor Yarochikin + Jeremy 'Birdman' Chiu + Tsung Pei Kan + Benson Wu) ➢ The Outer Limits: Hacking The Samsung Smart TV (Aaron Grattafiori + Josh Yavor) ➢ Revealing Embedded Fingerprints: Deriving Intelligence from USB Stack Interactions (Andy Davis) ➢ UART THOU MAD? (Toby Kohlenberg + Mickey Shkatov) ➢ Android: One Root to Own Them All (Jeff Forristal) ➢ Stepping p3wns: Adventures in Full Spectrum Embedded Exploitation (Ang Cui + Michael Costello + Salvatore Stolfo)
1415-1515	➢ Using Online Activity as Digital Fingerprints to Create a Better Spear Phisher (Joaquim Espinhara + Ulisses Albuquerque) ➢ Hot Knives Through Butter: Bypassing Automated Analysis Systems (Abhishek Singh + Zheng Bu) ➢ Above My Pay Grade: Cyber Response at the National Level (Jason Healey) ➢ ') UNION SELECT `This_Talk` AS ('New Optimization and Obfuscation Techniques')%00 (Roberto Salgado) ➢ Out of Control: Demonstrating SCADA Device Exploitation (Brian Meixell) ➢ Funderbolt: Adventures in Thunderbolt DMA Attacks (Russ Sevinsky) ➢ Press ROOT to Continue: Detecting OSX and Windows Bootkits with RDFU (Mario Vuksan + Tomislav Pericin) ➢ What's on the Wire? – Physical Layer Tapping with Project Daisho (Dominic Spill + Michael Ossmann + Michael 'Dragorn' Kershaw) ➢ Implantable Medical Devices: Hacking Humans (Barnaby Jack)
1530-1630	➢ CreepyDOL: Cheap, Distributed Stalking(Brendan O'Connor) ➢ Post Exploitation Operations with Cloud Synchronization Services (Jake Williams) ➢ Virtual Deobfuscator - A DARPA Cyber Fast Track Funded Effort

	(Jason Raber) ➢ Is that a Government in Your Network or are you Just Happy to See Me? (Eric Fiterman) ➢ Compromising Industrial Facilities from 40 Miles Away (Lucas Apa + Carlos Penagos) ➢ RFID Hacking: Live Free or RFID Hard (Fran Brown) ➢ SSL, Gone in 30 Seconds – A BREACH beyond CRIME (Angelo Prado + Neal Harris + Yoel Gluck) ➢ Exploiting Network Surveillance Cameras Like a Hollywood Hacker (Craig Heffner) ➢ Rooting SIM Cards (Karsten Nohl)
1700-1800	➢ OptiROP: Hunting for ROP Gadgets in Style (Nguyen Anh Quynh) ➢ Defending Networks With Incomplete Information: A Machine Learning Approach (Alexandre Pinto) ➢ Teridian SoC Exploitation: Exploration of Harvard Architecture Smart Grid Systems (Josh 'mOnk' Thomas + Nathan Keltner) ➢ Bugalyze.com - Detecting bugs using decompilation and data flow analysis (Silvio Cesare) ➢ Hacking Like in the Movies: ➢ Visualizing Page Tables for Local Exploitation (Georg '0xff' Wicherski + Alexandru Radocea) ➢ Home Invasion v2.0 – Attacking Network-Controlled Hardware (Daniel Crowley + David Bryan + Jennifer Savage) ➢ Multiplexed Wired Attack Surfaces (Michael Ossmann + Kyle 'Kos' Osborn) ➢ Owning the Routing Table - Part II (Gabi Nakibly) ➢ Spy-jacking the Booters (Brian Krebs + Lance James)

(二) DEF CON 21

本年 DEF CON 21 之 Briefings 議程為期 3 天，分為 5 個 Track，每天自上午 10 時至

下午 6 時，內容包含固有的議程、競賽(Social-Engineer Capture the Flag、warlock game 及WiFi Sheep Hunt 等)、Skytalks 及多個Village(Lockpick、Wireless、Hardware Hacking 及 Tamper Evident)，亦提供電影與音樂欣賞。DEF CON 議程詳見表 4 至表 6。

表 4：DEF CON 21 第 1 天議程(8 月 2 日)

時間	議程
1000-1200	➢ Proliferation（Ambassador Joseph R.DeTrani） ➢ Torturing Open Government Systems for Fun, Por\\rofit and Time Travel（Tom Keenan） ➢ Welcome & Badge Talk（The Dark Tangent, LosT） ➢ The Growing Irrelevance of US Government Cybersecurity Intelligence Information（Mark Weatherford） ➢ I Can Hear You Now：(Doug Deperry & Tom Ritter） ➢ The Secret Life of SIM Cards（Karl Koscher & Eric Butler） ➢ Adventures in Automotive Networks and Control Units（Charlie Miller & Cris Valasek） ➢ Hacking Driverless Vehicles（Zoz） ➢ All Your RFz Are Belong to Me – Hacking the Wireless World with Software Defined Radio（Balint Seeber）
1200-1400	➢ Backdoors, Government Hacking and The Next Crypto Wars （Christopher Soghoian） ➢ The Dirty South – Getting Justified with Technology （David Kennedy & Nick Hitchcock） ➢ DragonLady: An Investigation of SMS Fraud Operations in Russia （Ryan W. Smith Tim Strazzere） ➢ 10000 Yen into the Sea （Flipper） ➢ Making Of The DEF CON Documentary（Jason Scott Rachel Lovinger ➢ ACL Steganography - Permissions to Hide Your Porn（Michael Perklin） ➢ Prowling Peer-to-Peer Botnets After Dark （Tillmann Werner ）

	➢ Offensive Forensics: CSI for the Bad Guy （Benjamin Caudill） Pwn'ing You(r) Cyber Offenders （Piotr Duszynski） ➢ Business Logic Flaws In Mobile Operators Services （Bogdan Alecu）
1400-1600	➢ Protecting Data with Short-Lived Encryption Keys and Hardware Root of Trust（Dan Griffin） ➢ Evil DoS Attacks and Strong Defenses（Sam Bowne & Matthew Prince） ➢ MITM All The IPv6 Things（Scott Behrens & Brent Bandelgar） HTTP Time Bandit（Vaagn Toukharian & Tigran Gevorgyan） ➢ Meet the VCs （Panel） ➢ Ask the EFF: The Year in Digital Civil Liberties（Panel） ➢ Google TV or: How I Learned to Stop Worrying and Exploit Secure Boot（Amir Etemadieh & Panel） ➢ Kill 'em All - DDoS Protection Total Annihilation!（Tony Miu & Wai-Leng Lee） ➢ How to use CSP to Stop XSS（Kenneth Lee） So You Think Your Domain Controller is Secure?（Justin Hendricks） ➢ The ACLU Presents: NSA Surveillance and More（Panel）
1600-1800	➢ A Password is Not Enough: Why Disk Encryption is Broken and How We Might Fix It （Daniel Selifonov） ➢ VoIP Wars: Return of the SIP（Fatih Ozavci） ➢ Getting The Goods With smbexec（Eric Milam） Abusing NoSQL Databases（Ming Chow） ➢ The Government and UFOs: A Historical Analysis（Richard Thieme） ➢ Decapping Chips the Hard Way（Adam "Major Malfunction" Laurie & Zac Franken） ➢ Unexpected Stories - From a Hacker Who Made It Inside the Government.（Peiter "Mudge" Zatko） ➢ Examining the Bitsquatting Attack Surface （Jaeson Schultz） Please Inject More Coins（Nicolas Oberli）

	➢ How my Botnet Purchased Millions of Dollars in Cars and Defeated the Russian Hackers（Michael Schrenk）

表 5：DEF CON 21 第 2 天議程(8 月 3 日)

時間	議程
1000-1200	➢ From Nukes to Cyber – Alternative Approaches for Proactive Defense and Mission Assurance（Lt. Gen. Robert Elder USAF (Retired)） ➢ Dude, WTF in my car?（Alberto Garcia Illera & Javier Vasquez Vidal） ➢ Do-It-Yourself Cellular IDS（Sherri Davidoff & Panel） ➢ Predicting Susceptibility to Social Bots on Twitter（Chris Sumner & Randall Wald） ➢ Insecurity - A Failure of Imagination（Marc Weber Tobias & Tobias Bluzmanis） ➢ The Politics of Privacy and Technology: Fighting an Uphill Battle（Eric Fulton & Daniel Zolnikov） ➢ The Road Less Surreptitiously Traveled（Pukingmonkey） ➢ Fear the Evil FOCA: IPv6 attacks in Internet Connections（Chema Alonso） ➢ Key Decoding and Duplication Attacks for the Schlage Primus High-Security Lock（David Lawrence & Panel）
1200-1400	➢ Defeating Internet Censorship with Dust, the Polymorphic Protocol Engine（Brandon Wiley） ➢ Home Invasion 2.0 - Attacking Network-Controlled Consumer Devices（Daniel "UnicornFurnace" Crowley, Jennifer "SavageJen" Savage, & David "Videoman" Bryan） ➢ BoutiqueKit: Playing WarGames with Expensive Rootkits and Malware（Josh 'Monk" Thomas） ➢ Legal Aspects of Full Spectrum Computer Network (Active) Defense（Robert Clark）

	➢ DEF CON Comedy Jam Part VI, Return of the Fail （Panel） ➢ Privacy In DSRC Connected Vehicles（Christie Dudley） ➢ RFID Hacking: Live Free or RFID Hard（Francis Brown） ➢ Android WebLogin: Google's Skeleton Key（Craig Young） Building an Android IDS on Network Level（Jaime Sanchez） ➢ We are Legion: Pentesting with an Army of Low-power Low-cost Devices（Dr. Philip Polstra）
1400-1500	➢ Phantom Network Surveillance UAV / Drone（Ricky Hill） ➢ Stalking a City for Fun and Frivolity（Brendan O'Connor） ➢ Defeating SEAndroid（Pau Oliva Fora） Doing Bad Things to 'Good' Security Appliances（Phorkus（Mark Carey）& Evilrob（Rob Bathurst）） ➢ Pwn The Pwn Plug: Analyzing and Counter-Attacking Attacker-Implanted Devices（Wesley McGrew） ➢ Hardware Hacking with Microcontrollers: A Panel Discussion （Panel）
1500-1600	➢ Safety of the Tor Network: a Look at Network Diversity, Relay Operators, and Malicious Relays（Runa A. Sandvik） ➢ Hacking Wireless Networks of the Future: Security in Cognitive Radio Networks（Hunter Scott） ➢ How to Hack Your Mini Cooper: Reverse Engineering Controller Area Network（CAN）Messages on Passenger Automobiles（Jason Staggs） ➢ An Open Letter - The White Hat's Dilemma: Professional Ethics in the Age of Swartz, PRISM and Stuxnet （Alex Stamos）
1600-1700	➢ De-Anonymizing Alt.Anonymous. Messages（Tom Ritter） ➢ BYO-Disaster and Why Corporate Wireless Security Still Sucks （James Snodgrass（PuNk1nPo0p）& Josh Hoover（wishbone）） ➢ Electromechanical PIN Cracking with Robotic Reconfigurable Button Basher（and C3BO）（Justin Engler & Paul Vines） Data Evaporation from SSDs（Sam Bowne） ➢ PowerPreter: Post Exploitation Like a Boss（Nikhil Mittal）

	➢ Suicide Risk Assessment and Intervention Tactics（Amber Baldet）
1700-1800	➢ Noise Floor: Exploring the World of Unintentional Radio Emissions（Melissa Elliott） ➢ GoPro or GTFO: A Tale of Reversing an Embedded System（Todd Manning & Zach Lanier） JTAGulator: Assisted Discovery Of On-Chip Debug Interfaces（Joe Grand aka Kingpin） ➢ DNS May Be Hazardous to Your Health（Robert Stucke） ➢ OTP, It won't save you from free rides!（bughardy & Eagle1753） ➢ How to Disclose or Sell an Exploit Without Getting in Trouble（James Denaro）

表 6：DEF CON 21 第 3 天議程(8 月 4 日)

時間	議程
1000-1100	➢ The Cavalry Isn't Coming: Starting the Revolution to Fsck it All!（Nicholas J. Percoco & Joshua Corman） ➢ gitDigger: Creating useful wordlists from public GitHub repositories（Jamie Filson (WiK) & Rob Fuller (Mubix)） Made Open: Hacking Capitalism（Todd Bonnewell） ➢ Exploiting Music Streaming with JavaScript（Franz Payer） ➢ Defense by numbers: Making Problems for Script Kiddies and Scanner Monkeys（Chris John Riley）
1100-1200	➢ The Dark Arts of OSINT（Noah Schiffman & Skydog） ➢ The Dawn of Web 3.0: Website Mapping and Vulnerability Scanning in 3D, Just Like You Saw in the Movies（Teal Rogers & Alejandro Caceres） ➢ Java Every-Days: Exploiting Software Running on 3 Billion Devices（Brian Gorenc & Jasiel Spelman） ➢ Resting on Your Laurels Will Get You Pwned: Effectively Code Reviewing REST Applications to Avoid Getting Pwned（Abraham

	Kang & Dinis Cruz)
1200-1300	➢ EMET 4.0 PKI Mitigation (Neil Sikka) ➢ Combatting Mac OSX/iOS Malware with Data Visualization (Remy Baumgarten) A Thorny Piece Of Malware (And Me): The Nastiness of SEH, VFTables & Multi-Threading (Marion Marschalek) ➢ HiveMind: Distributed File Storage Using JavaScript Botnets (Sean Malone) ➢ This Presentation Will Self-Destruct in 45 Minutes: A Forensic Deep Dive into Self-Destructing Message Apps (Drea London & Kyle O'Meara)
1300-1400	➢ Stepping P3wns: Adventures in Full Spectrum Embedded Exploitation (and defense!) (Ang Cui & Michael Costello) ➢ Transcending Cloud Limitations by Obtaining Inner Piece (Zak Blacher) Utilizing Popular Websites for Malicious Purposes Using RDI (Daniel Chechick & Anat (Fox) Davidi) ➢ Defending Networks with Incomplete Information: A Machine Learning Approach (Alexandre Pinto) ➢ Fast Forensics Using Simple Statistics and Cool Tools (John Ortiz)
1400-1500	➢ EDS: Exploitation Detection System (Amr Thabet) ➢ Open Public Sensors, Trend Monitoring and Data Fusion (Daniel Burroughs) Collaborative Penetration Testing With Lair (Tom Steele & Dan Kottman) ➢ Blucat: Netcat For Bluetooth (Joseph Paul Cohen) ➢ Forensic Fails - Shift + Delete Won't Help You Here (Eric Robi & Michael Perklin)
1500-1600	➢ Conducting Massive Attacks with Open Source Distributed Computing (Alejandro Caceres) ➢ PowerPwning: Post-Exploiting By Overpowering PowerShell (Joe

	Bialek） Evolving Exploits Through Genetic Algorithms（Soen） ➢ BYOD PEAP Show（Josh Yavor） ➢ Let's Screw with Nmap（Gregory Pickett）
1600-1700	➢ Revealing Embedded Fingerprints: Deriving Intelligence from USB Stack Interactions（Andy Davis） ➢ The Bluetooth Device Database（Ryan Holeman） ➢ C.R.E.A.M. Cache Rules Evidently Ambiguous, Misunderstood（Jacob Thompson）

二、重點議題

(一) Blackhat USA 2013

1、Keynote Speaker: General Keith B. Alexander

Blackhat USA 2013 第一天議程的專題演講係由美國國家安全局(NSA)局長亞歷山大將軍擔任開幕主講嘉賓，對於最近全球非常矚目的棱鏡計畫(PRIME)，美國國家安全局以該極具爭議性的情報蒐集計畫挫敗全球 54 恐怖襲擊，並強調其必要性。國家安全局用來蒐集有關涉及美國公民的通信公司，包括 Google、Microsoft、Yahoo、Apple 及 Facebook 等，亞歷山大將軍試圖打消美國公司提供不受限制地訪問客戶數據的概念，並提及只有少數的國家安全局分析師有權搜索電話的原始數據和電子郵件，且指出該計畫受到聯邦法官和國會的監督。

棱鏡計畫的監聽對象包括任何在美國以外地區使用參與計劃公司服務的客戶，或是任何與國外人士通信的美國公民，一直是美國對抗恐怖攻擊的至關重要因素之一，已成功阻止 13 個在美國的恐怖攻擊。例如，從一個在巴基斯坦的恐怖分子被攔截的電子郵件，阻止了恐怖份子在 2009 年紐約地鐵爆炸陰謀，亞歷山大將軍說這本來是自 911 起在美國本土最大的恐怖襲擊事件，美國國家安全局監控巴基斯坦「基地」組織成員的電子郵件，從而逮到在美國丹佛科羅拉多州嘗試製作爆裂物，陰謀攻擊紐約地鐵的阿富汗移民納吉布拉查茲（Najibullah Zazi）。接著美國國家安全局提供信息給聯邦調查局(FBI)查茲先生的電話號碼過濾，使當局發現一個先前未知的號碼，即另一個同謀梅杜賈尼恩(Adis

Medunjanin)，亞歷山大將軍提到 2009 年 9 月 6 日截獲的信息，聯邦調查局有 7 天的時間使用這些信息來阻止攻擊。

棱鏡程序屬於外國情報監視法案第 702 節，讓美國國家安全局收集的數據為外國情報目的。它僅適用於位於國外的外國情報，如反恐為目的的外國人士溝通。亞歷山大將軍說美國政府不會單方面從美國公司的服務器獲取信息。

亞歷山大將軍於演講後被問及「是否認為美國國家安全局傷害美國科技企業爭取海外顧客的能力」，其回答「企業希望公開政府向他們要資料的情況，這些企業也應該要如此做，實際上，政府向企業要的資料很少」，我們對這樣的計畫仍有些疑問，但也讓我們在進行資安情蒐與防禦時，有著另一層的思考方向。

2、Binary Pig- Scable Malware Analytics in Hadoop

在過去的 2 年半中，Endgame 團隊獲得 2 千萬個惡意軟體樣本，相當於大約 9.5 TB 的 binary 樣本。在 McAfee 報告中提到，目前每天收到大約 10 萬個惡意軟體樣本，在 2012 最後一季共累計收到 1 千萬個樣本。這種大量的惡意軟體提供機器學習研究(Machine learning)的挑戰和機會。尤其是以對惡意軟體進行靜態分析，提取用於執行大規模機器學習的功能集合的影響更大。

由於惡意軟體研究歷來是逆向工程的領域，大多數現有的惡意軟體分析工具被設計用來處理一台計算機上的單一的二進制文件或多個二進制文件，因此在面對新 TB 這麼大規模惡意軟體的分析上並沒有特別處理。資安研究人員以簡單技巧，應用在大規模應用靜態分析技術以建立自己的解決方案上，就顯得非常重要。

早期嘗試處理這些數據的方法，並不能很好地擴展來處理大量增加的樣本。因此一旦惡意軟體蒐集數量的增加，分析系統將會處於過大的負載與管理，同時還必須考慮長期超頻處理所可能產生的硬體故障。

為瞭解決這個問題，該團隊在過去兩年中專注於設計一個基於 Hadoop 的專用系統框架，使得大規模研究可以更容易執行，並擴大數據集的重複使用。Hanif 等人提出開放框架 BinaryPig，可達 TB 數百萬樣本惡意程式分析。這個框架是建立在 Apache Hadoop 的 Apache PIG 和 Python。它解決了可擴展的惡意軟體處理的問題，包括處理日益龐大的數據規模，改善工作流程的發展速度，實現並行處理的二進制文件與大多數現有的工具。

這個系統採用模塊化(modular)設計並且可提供擴展(extensible)，希望這將有助於在處理大量的惡意軟體的安全研究人員和學者。

此外，演講者也展示了這個框架的勘探和使用技術，同時未來作者亦將此成果作為開放原始碼(Apache 2.0 License)釋放，以提供相關研究人員使用。

3、I Can Hear You Now: Traffic Interception and Remote Mobile Phone Cloning with a Compromised CDMA Femtocell

行動通訊網路是由許多小型無線單元(Cell)組成，即基地台，針對其位置或應用，各個基地台可能有著不同的涵蓋範圍、系統容量、與輸出功率。依其涵蓋範圍(或稱輸出功率)，將其分類成大型基地台(Macrocell)、微型基地台(Microcell)、特微型基地台(Picocell)與 Femtocell；微型、特微型基地台主要是針對稠密的行動電話使用區域，用以增加網路容量，如車站、購物商場等。而 Femtocell(毫微微蜂窩基地台或低功率家用基地台)涵蓋範圍更小，主要是用來彌補其他基地台無法涵蓋的區域及提升數據傳輸速率，通常用於住宅或小型商業環境。

由於電信業者提供或出售 femtocell 給使用者，以補足室內電信網路收訊，導致 femtocell 在美國的日益普及(在台灣仍在測試階段)，演講者透過毫微微蜂窩基地台，類似一個小型的手機信號器，轉換 3G 使用者的 ADSL 或光纖上網頻寬為無線 3G 訊號(詳見錯誤! 找不到參照來源。)。因此當使用者的手機在訊號範圍內時，手機會連接到這個毫微微蜂窩，並且將它視為一個標準的手機信號器，因此該手機上的傳送/接收任何電話，傳送簡訊、Email，亦或瀏覽網路等行為，都會提供一份複製給攻擊者，對受害者完全不會顯示任何跡象，甚至不會通知受害者。

在這次演講中，演講者展示如何侵入毫微微蜂窩軟體，從而能夠讓他們假冒傳統基站並引誘不知情的手機用戶登錄，並且攔截正在活動中的語音/簡訊/數據流量，並解釋如何能夠複製一個移動設備，進而進行實體的訪問。

4、Hunting the Shadows: In Depth Analysis of Excalated APT Attacks

APT 攻擊是一種新興的威脅，並取得了近年來的頭條新聞。然而，針對性的網絡攻擊仍存在了許多神秘的色彩，在此次攻擊行動的規模評估。台灣一直是一個長期的目標，

這些網絡攻擊，由於其高度發達的網絡基礎設施和敏感的政治立場。在此場次，從台灣過來的團隊透過獨特的機會，監視，偵查，調查，並減輕攻擊了大量的政府和私營部門的公司。本報告將介紹我們的研究結果有針對性的網絡攻擊，在此次攻擊行動，台灣 Xecure 實驗室和中央研究院的一個聯合研究。透過已經開發了一個完全自動化的系統，XecScan2.0(http://scan.xecure-lab.com)配備了獨特的動態和靜態惡意軟件取證技術分析性質和行為的惡意的二進制文件和文件漏洞(沙箱)。該系統進行實時的 APT 分類及聯營公司的分析內容與現有的知識基礎。在我們的實驗中，分析和的 XecScan 系統成功識別超過 12,000 APT 的電子郵件，其中包括的 APT 惡意軟件和文件侵入。有了這個演示，分析和組樣品從近期 Mandiant 的 APT1(61398)的報告，並會在台灣發現的樣本比較的關係之間 APT1 樣品和討論 APT1 黑客活動背後的歷史。在這個演示中，並發布一個免費的，可公開訪問的門戶我們協作 APT 分類平台和訪問 XecScan2.0 API 的。

5、Rooting SIM Cards

手機 SIM 卡為目前世界上部署最廣泛的計算平台，然其安全性卻是鮮為人知，SIM 卡的主要目的是除了識別用戶外，他們大多提供可編程的 Java 運行。

主講者德國 Karsten Nohl 公佈其最近研究的結果，發手機 SIM 卡所使用的加密技術 DES(Data Encryption Standard)存在一個嚴重漏洞，駭客可利用該漏洞取得並修改 SIM 卡上的數位金鑰(digital key)，接著發送簡訊病毒來感染手機，之後便能竊聽手機或是竊取手機上的所有訊息與資料，甚至可以透過手機購買商品並完成付費。主講者表示使用一般電腦，可在 2 分鐘內就能控制 1 台手機。

DES 自 1970 年被提出後，已廣泛被使用在各項應用上，後續為加強安全性，許多廠商改採安全性較強的 3DES(Triple DES)，然現今世面上許多手機 SIM 卡仍採舊的 DES 加密方式，根據 Nohl 近年測試結果，部分地區約有四分之一的用戶仍使用 DES，因此據以推估全球約有 7.5 億支手機受到影響。

(二)DEF CON 21

1、Google TV or: How I Learned to Stop Worrying and Exploit Secure Boot

Google TV 帶來了 Android 作業系統從移動環境中進入消費者的客廳，然而不幸的是，內容供應商開始從 Google TV 平臺中阻止一些流行節目的內容，此外，第一代 Google TV 硬體使用的是 Intel 的 x86 晶片組，而非傳統 Android 系統所使用的 ARM，此舉阻礙了大多數正常的 Android 應用程式。在前一次 DEFCON 會議中，我們討論了在第一代 Google TV 的硬體和軟體中發現的漏洞，本次演講則針對新發布的第二代設備，其中包括更廣泛的 OEM 廠商類型，如華碩(Asus)、索尼(Sony)、 樂金(LG)、瑞旭(Vizio)、Hisense 和 Netgear。

主講者的展示包括新發現且未公開的硬體漏洞、軟體漏洞及製造商的錯誤，並詳細討論如何利用新的安全啟動(Secure Boot)環境的 Marvell 晶片組。為了繞過 Google TV 上的安全啟動，主講者公布兩個獨立的漏洞，這將允許用戶在 Google TV 設備上執行未經簽章的 bootloader，其中一個影響，也可以用於對多種其他嵌入式設備的權限提升的 Linux 核心的特定設置。

2、Exploiting Music Streaming with JavaScript

隨著音樂產業的轉變，從實體通路到數位傳輸，他們已經忘記了最重要的一件事，即數位版權管理(Digit Right Management, DRM)。許多瀏覽器為基礎的音樂串流媒體服務並未使用 DRM 來保護他們的音樂，因此造成了他們的音樂作品被人任意取得及散佈。

主講者詳細介紹與演練了使用 JavaScript 來規避一些基於瀏覽器的音樂串流服務的安全性，通過數種音樂播放器程式碼的逆向工程分析，它是可以模仿音樂播放器下載歌曲，許多難以使用逆向工程進行分析的服務，仍然可以利用攔截的流量和下載歌曲相同的請求。這場演講說明了音樂串流的基本知識，展示了基於瀏覽器的流量記錄來識別和下載音樂文件，並介紹了使用 JavaScript 繞過安全性檢查以成功模仿成合法的播放器，最終說明 Google 瀏覽器(Chrome)的擴展程序將允許用戶可非法下載歌曲。

3、How to Hack Your Mini Cooper: Reverse Engineering Controller Area Network (CAN) Messages on Passenger Automobiles

本場演講介紹車輛通訊系統網路的原理並評估其安全性，雖然通訊系統已具有一定程度的可靠度，但是相關的安全性確鮮少套用至車輛系統應用中，主講者的研究著重於控制區域網路(Controller Area Networks, CANs)以及 CAN 訊息的驗證性及有效性之缺

乏，目前用以保護 CAN 網路資料安全的方法，主要依賴在 CAN 匯排流及外部世界實體介接上 CAN 訊息識別碼的使用上，就像我們所知道的，架構於不安全之上的安全並不是真正的安全，這些訊息識別碼可以被逆向工程及被偽造成不同的結果。

這次演講主要討論 CAN 訊息的逆向工程方法，這些使用逆向工程所解出來的訊息可以搭配便宜的 Arduino 硬體，用來注入至 2003 年款的 Mini Cooper 之 CAN 匯排流中，此外，Jason Staggs 展示一個概念證明關於如何建立自己的 rogue CAN 節點，及潛在的操縱車輛的關鍵元件，概念證明展示如何使用逆向工程方法以充分控制組合儀表。

4、MITM All The IPv6 Things

在 2011 年，Alec Waters 展示了如何在 IPv4 的網路上覆蓋一個惡意 IPv6 的網路，使攻擊者可以使用 IPv4 流量進行中間人攻擊(man-in-the-middle, MITM)，並破壞端對端(end to end)安全模型。這種攻擊非常的強大，但需要使用到一系列複雜的手動系統配置和設定，包括使用實驗性質及過時的技術，此外，技術的更新使得 Alec Waters 所提出的攻擊在某些平台(如 Windows 8)上無效。

主講者(Scott Behrens 和 Brent Bandelgar)重新檢視了 Alec Waters 所提出的攻擊，並試著應用在現今的作業系統，他們發現需要進行配置更新，可使上開攻擊成功使用在 Windows 8 的主機上，他們相關的步驟及設置打包成一個劇本(Sudden Six)，能快速且無聲的發動攻擊。這種攻擊現在可以應用在各種不同的平台和作業系統，並允許在 IPv6 流量中發動中間人攻擊。本場演講除了說明攻擊的原理，亦討論他們的自動化策略和所發現的一些漏動，並公開 Sudden Six 的配置應用程序，也於現場展示提供一個 Windows 8 的攻擊。

5、Defending Networks with Incomplete Information: A Machine Learning Approach

機器學習(machine learning)或是資料探勘(Data Mining)對一般人來說只是理論及數學算式，因此，本次演講的重點在於介紹機器學習的基本概念，這場演講在許多關鍵地方，從資安的角度點出很多關係到分析成敗的概念，例如：過去有些資安問題如垃圾郵件(SPAM)的過濾，如使用機器學習的方式處理或許並非最佳方法，因為可能在 Deterministic 模型可以做到更好的結果，因為 deterministic 模型的重點在於已有預先

系統化的專家知識，所以硬是要採用機器學習的方法去學習，恐怕無法有效地解決問題。

接著這個演講將整個機器學習在資安上面分析的流程進行描述，包含監督式學習與非監督式學習，分別說明其適用的情況為何，一般而言，在找尋新的攻擊樣態，非監督式學習的方法往往可以找出邊際行為或是新的樣態，這裡面的關鍵是如何設計以及調校裡面的參數，以及找尋關鍵的屬性，最後，這個演講提到了如何驗證的方式，整體而言，這個演講將機器學習帶入到了 hitcon 21 裡面，也讓與會者有一些新的發想。

6、Electromechanical PIN Cracking with Robotic Reconfigurable Button Basher (and C3BO)

密碼和 PIN 碼系統經常使用在移動設備上，一些破解這類系統的軟體方法通常是最簡單的，但是在某些情況下，有可能沒有比直接按按鈕更好的選擇。本場演講涵蓋自動密碼破解技術，使用兩個新的工具和討論這些攻擊各種密碼保護系統的實用性。

Robotic Reconfigurable Button Basher(R2B2)是一個約 200 美元的機器人，被設計以手動暴力破解方式或其他透過人工輸入密碼。R2B2 可以操作在觸碰式螢幕上或實體按鍵，R2B2 也可以處理更複雜的類型，如鎖定螢幕模式的追踪。

Capacitive Cartesian Coordinate Bruteforceing Overlay (C3BO)是電模擬觸摸電容式觸摸屏設備上電子設計的組合，C3BO 有沒有可移動部分，在某些情況下運作速度比 R2B2 來得快。這兩種工具都有開放源碼軟件，且有零件清單及詳細的建構指令，以及供 3D 打印的 STL 檔案可供下載，主講者亦在現場展示所設計的破解 PIN 碼的機器裝置。

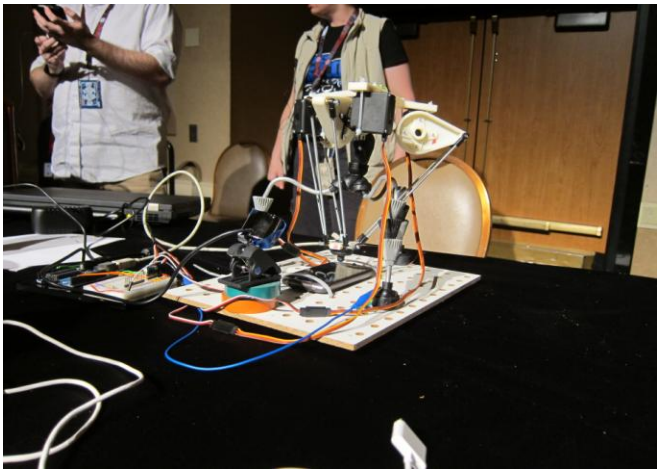

圖 1：Electromechanical PIN Cracking with R2B2 and C3BO

肆、心得建議

本年6月美國國家安全局(National Security Agency, NSA)的稜鏡計畫(PRISM)被揭露，這項計畫讓NSA和FBI可以從Microsoft、Yahoo、Google、Facebook、PalTalk、AOL、Skype、YouTube和Apple等各家公司中，獲取使用者的各種通訊資料，包含電子郵件、語音通話和社交資訊等，引起全國譁然以及各界質疑。本次Blackhat USA 2013第一天議程的專題演講係由美國國家安全局(NSA)局長亞歷山大將軍擔任開幕主講嘉賓，對於最近全球非常矚目的稜鏡計畫(PRIME)提出相關說明及成效。就民眾而言，認為通訊內容受到監聽，違反了憲法所賦予人民自由的權利；然以NSA的角度，認為其目的係為了維護國家及人民的安全，並不違反憲法本意，姑且不論其合理性及正當性，值得我們省思之處為國內目前電腦及行動裝置所使用的即時通訊軟體或應用程式，雖我國已訂有「通訊保障及監察法」，保障人民秘密通訊自由不受非法侵害，然前揭軟體或應用程式有許多係由國外廠商所開發製作，其面臨的問題在於如何確保即時通訊內容免於被非法侵害；另如因執法需要、或是為確保國家安全及維持社會秩序，需進行適當程度的通訊監察，我國是否已具備完善的技術能力或法令規章，均是值得深入探討的重要議題。

自本年起，本(資通安全)辦公室積極推動數項資安強化機制，包括建置二線監控，配合於本年9月9日修正「國家資通安全通報應變作業綱要」，要求各級政府機關(構)無論自建或委外資安監控(Security Operation Center, SOC)服務，應配合建立監控情蒐回傳機制，定期回傳予技術服務中心；為強化政府網際服務網(GSN)骨幹資安，刻正研議GSN骨幹相關資訊分析機制；為加強重大資安事件事中緊急應變能力，亦積極研擬政府機關資安紀錄保存機制，上述各項工作皆須處理及分析龐大資安資訊，已非傳統資訊處理技術可以滿足，爰亟需研究並規劃鉅量資料(Big Data)分析處理系統架構，包括資料傳輸、接收、處理、分析及儲存等技術。本次參加Blackhat USA 2013及DEF CON 21會議，有數個場次均談及鉅量資料分析，並資安事件及相關日誌進行分析，或是以資料探勘的方式找出攻擊的樣態，如應用hadoop平臺及平行運算以加速對惡意程式的分析，可作為本辦公室後續鉅量資料分析處理相關研究之參據。

行動安全亦為近年來資安的熱門議題之一，包括通訊系統、應用程式及硬體裝置，

本次Blackhat USA 2013及DEF CON 21會議有眾多演講均涉及此一領域，包括智慧型手機、衛星導航系統、車載資訊系統、APP應用程式、BYOD(Bring Your Own Device)、藍牙(Bluetooth)及無線網路等，佔了整個會議議程相當高的比例，顯見行動安全已為現階段國際間所面臨的共同問題，研擬相關的資安技術及標準規範已是刻不容緩的議題。綜觀國內政府機關目前對行動安全相關的規範，雖已訂有各式參考指引或手冊，然面對資安威脅日新月異不斷演進，必須與時俱進，參考國際目前最新趨勢，據以檢討修正相關規範。

最後，Blackhat除每年定期於美國舉辦，先前亦曾於2008年於亞洲地區辦理過一次會議，時隔6年，預計於明年3月25至28日，假新加坡濱海灣金沙飯店(Marina Bay Sands Hotel)舉辦Blackhat Asia 2014，議程包括2天的Trainings(3月25至26日)及2天的Briefings(3月27至28日)，目前刻正廣徵論文發表(Call for Papers)，屆時，想必會有許多亞洲地區的資安專家參加，所談論的議題估計將涉及更多亞洲地區的資安現況及趨勢，資安相關人員可藉此難得的資安盛會與各界交流。

伍、會議照片

圖 2：Blackhat USA 2013 會議地點(Caesars Palace Hotel)

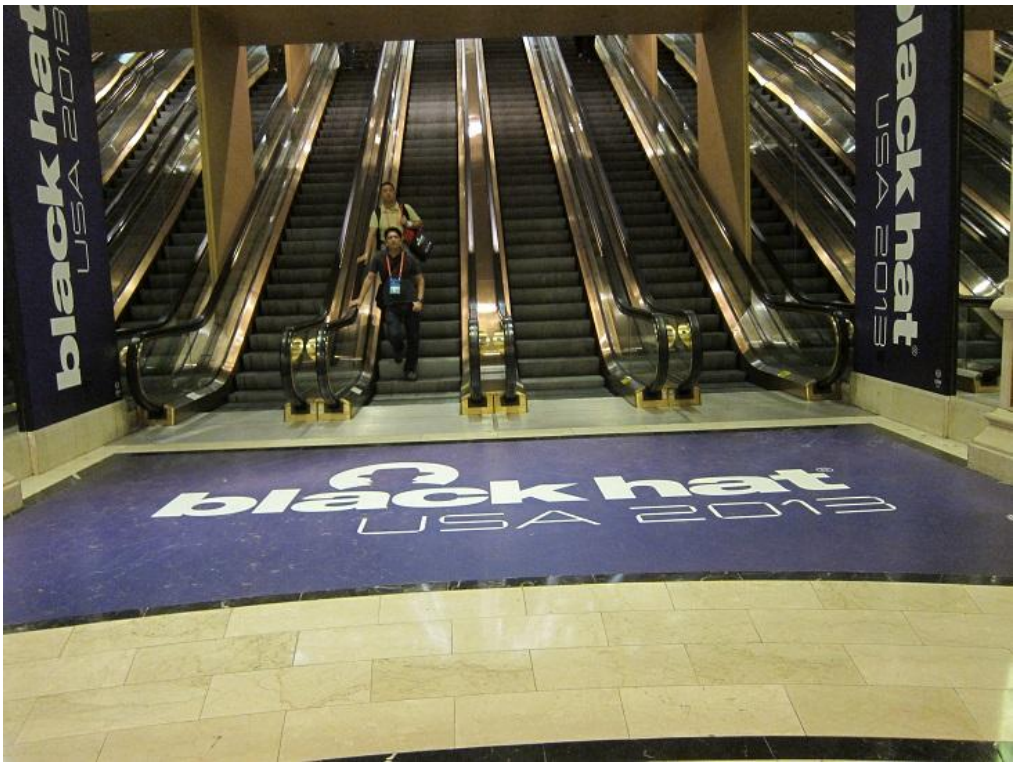

圖 3：Blackhat USA 2013 會議現場

圖 4：Blackhat 會議標誌

圖 5：Blackhat USA 2013 會議 Keynote 現場

圖 6：Blackhat USA 2013 會議-live onstage demonstration

圖 7：DEF CON 21 會議地點(Rio All-Suite Hotel)

圖 8：DEF CON 21 會議現場-1

圖 9：DEF CON 21 會議現場-2

圖 10：DEF CON 21 會議-綿羊牆

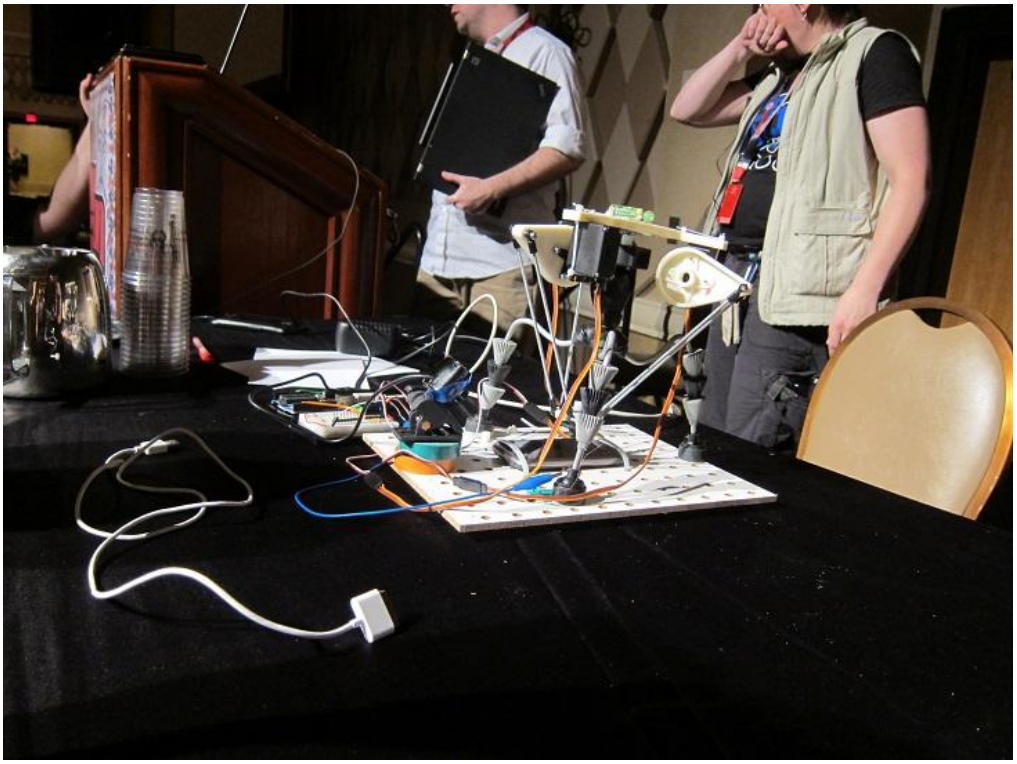

圖 11：DEF CON 21 會議-實機展示(破解手機 PIN 碼)