出國報告（出國類別：會議）

2018 年參加美國拉斯維加斯黑帽技術研習

服務機關 ： 中央警察大學、警政署刑事警察局
姓名職稱 ： 副教授高大宇、隊長陳詰昌
派赴國家 ： 美國
出國期間 ： 中華民國 107 年 8 月 2 日至 14 日
報告日期 ： 中華民國 107 年 9 月 28 日

摘要

網路犯罪手法日益變化並使用複雜的科技技術，中央警察大學副教授高大宇與警政署刑事警察局隊長陳詰昌前往參加美國黑帽大會技術研習課程與 DEFCON 研討會，藉由參與美國黑帽技術課程（資料外洩偵防與事件回復課程）、技術簡報及 DEFCON 駭客安全研討會，有助瞭解駭客常用工具和方法，進而知道如何保護網路、系統免受攻擊，並從事後續偵查。此外，亦可研析駭客攻擊方法及對應的蒐證技巧，拓展警察網路鑑識研究領域，吸取世界各地資安與網路鑑識專家實務經驗與理論精華，持續強化中央警察大學與國際學者及實務專家之交流與資訊分享，提升學術研究能量。

資通訊科技內涵廣泛，資安網路犯罪偵查人員須不斷充實精進，期透過「基本防護」、「基礎安全」及「組織管理」等不同面向，保護資訊系統使用者的安全與隱私，並視流程化、服務性的網路犯罪組織為組織危機，資安公司更須不斷改寫自動化工具程式，強化資安措施，朝程式自動化方式蒐集相關稽核紀錄，作為數位證據，進一步嚇阻資安犯罪。綜整整理本次參加會議值得我們學習的發展方向，計有「延續國際合作機制，提升相關研究水準」、「加強學術及實務機關互動學習，持續發展擅長的專業技術領域」及「持續理論結合實務的研習活動，維持跨機關或跨境的良好互動關係」等三項，期許中央警察大學及警政署能持續發展各系、各教師或各員警擅長的專業技術領域，加強學術及實務機關的互動學習與成長，持續申請國際合作研究計畫或參與國際學術組織，藉由國外前瞻性之研發技術與成果引進，提升國內警政或資安相關研究水準。

目錄

一、前言

各國為分享資安情資及推廣防禦技術，定期召開資安相關研討大會，促進金融科技、飛彈防禦國防系統等新興科技技術的資安發展趨勢交流與分享。其中，Black Hat 及 DEF CON（被視為 Black Hat 的姐妹會議）係全球最知名的資安駭客技術會議之一，每年定期於美國拉斯維加斯的鄰近地點一同舉辦，107 年 Black Hat 簡報會是 8 月 4 至 9 日，DEF CON 駭客安全研討會則是 8 月 9 至 12 日，讓許多資安人員能夠一次參加兩大會議，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搶旗競賽（CTF；capture the flag）。

每年在美國拉斯維加斯的 Black Hat 及 DEF CON，是資安與駭客界的兩大會議，討論最新發現的電腦安全弱點、攻擊方法與防禦技術。早期研討會著重各系統未發現弱點攻擊技術的發表，演講者常受到 FBI 等執法機關的關切，發表的攻擊手法往往會造成系統危害。現今，許多駭客轉而成立或加入一些資安公司，近年研討內容，亦融入資安公司相關產品技術的發表議題。

（一）Black Hat：著重資安學術研究，由 Black Hat 組織邀請資安公司合辦

1997 年開始舉辦 Black Hat，以拉斯維加斯場次最為盛大，每年有來自全球 50 多個國家，超過 6,000 人參加。本次 Black Hat 2018 大會議題十分多元，主題分述如下：

1、Black Hat 教育訓練主題：包含應用程式安全、稽核與測試、 認證、加解密、軟體開發、電腦鑑識、硬體安全、惡意程式分析、系統規劃、網路安全、逆向工程、系統管理與無線安全等課程。

2、Black Hat 簡報會主題：包含深層木馬、零時差攻擊、防禦零時差攻擊、應用程式安全、木馬與惡意程式、電腦鑑識、硬體安全、網路安全、無線網路安全、虛擬實境、逆向工程、新一代網頁服務與資安深度探討等領域之技術研討與演講。

（二）DEF CON：著重駭客攻擊實務，由 DEF CON 通訊公司主辦

DEF CON 為年度地下駭客大會（2018 年為第 26 屆），議題包含資訊設備軟硬體攻擊手法的研討與展示，早期以發表未公佈之攻擊手法與弱點為主，但因該會所發表弱點常造成社會重

大危害與損失，近年來發表弱點須經相關單位與廠商同意後才可發表。研討內容涵蓋深層木馬、應用程式安全、惡意程式、網路安全、及無線網路安全等系列專題演講。

二、研習目的

為期許充實最新資安技術與能量，本次參加一年一度的駭客年會（如圖 1、圖 2），期能快速掌握最新的資訊犯罪攻防及偵查技術，跟與會的各國資安人員請教及技術交流，蒐集最新的資安攻擊與防禦技術，提供科技執法參考。本次研習目的，摘述如下：

圖 1：Black Hat 報到會場

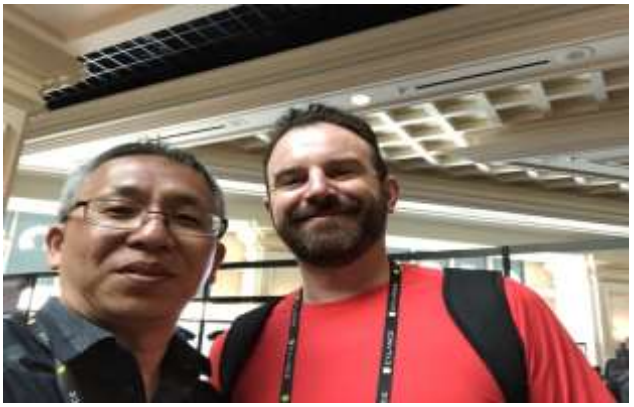
圖 2：Black Hat 會場與資安專家研討

（一）拓展警察網路鑑識研究領域

藉由參與美國黑帽技術課程（資料外洩偵防與事件回復課程）、技術簡報及 DEFCON 駭客安全研討會，拓展警察網路鑑識研究領域，吸取世界各地資安與網路鑑識專家實務經驗與理論精華，以提升本校學術研究及國際警察界之聲譽與地位。

（二）研析駭客攻擊方法及對應的蒐證技巧

網路犯罪手法日益變化並使用複雜的科技技術，藉由參加本案研習課程，可研析駭客攻擊方法及對應的蒐證技巧，持續強化本校與國際學者及實務專家之交流與資訊分享，期結合實務需求，研發及傳承偵防科技犯罪的專業技能，提升理論與實務結合之研發能量，建構科技執法之專業形象，加強打擊科技犯罪行為。

（三）研析提升警察資安防禦或執法效能的方法

參與國際性網路犯罪及數位鑑識相關技術課程或研討會議，藉以拓展國際學術交流領域、

空間，可擴展國際視野與研究能量，並可加強吸取國內外網路犯罪偵防經驗，研議妥適的犯罪偵防技巧、程序與策略。以順應世界化潮流，研析積極有效的改善策略，提升警察資安防禦或執法效能。

三、研習過程

本次會議訓練與聆聽會議內容，區分「Black Hat 教育訓練主題」、「Black Hat 簡報會主題」及「DEF CON 26 駭客安全研討會」等三部分，說明如下：

（一）Black Hat 教育訓練主題：107 年 8 月 4 至 7 日

近年，美國發生 Reddit、Eqifax、Yahoo!、Uber 等數起重大資料外洩事件，外洩內容包含客戶個人資料外，尚有信用卡、健保等機敏資料。電子郵件詐騙、進階持續威脅（APT；advance persistent threat）、勒贖病毒等為常見造成資料外洩原因，亟需加強資料外洩預防概念與處置方法技術。此次參訓課程名稱為資料外洩偵防與事件回復課程（data breaches： detection, investigation and response），訓練重點在資料外洩預防、偵測及處理，並將資料外洩視為組織危機，進行危機管理及危機溝通（如圖 3、圖 4）。該課程提供事件處理實驗室實作手冊，可於課後進行練習。訓練重點主題摘述如下：

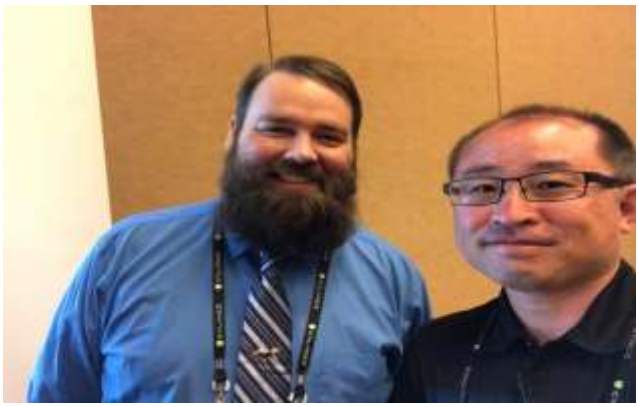

圖 3：Black Hat 訓練課程講師合影 1

圖 4：Black Hat 訓練課程講師合影 2

1、主題一、資料外洩五項風險因素

機密資料具有價值，在儲存、處理或傳輸過程均存在外洩風險，舉凡未經授權存取機密資料便算資料外洩。五項風險因素分述如下：

（1）保留（retention）

資料保存系統時間越長，外洩風險隨之增加。

（2）擴散（proliferation）

資料拷貝份數愈多，外洩風險隨之增高。

（3）存取（access）

存取人數愈多、方式愈多元，外洩風險愈高。

（4）流動性（liquidity）

資料格式的流動性（即可複製的再處理性）愈高，外洩風險愈高。如影像檔較文字檔難進行後續處理，外洩後難以再利用或匯入資料庫，外洩風險較文字檔低。

（5）價值（value）

資料價值愈高，外洩風險愈高；如資料內容含信用卡資料或健保就醫紀錄等個人資料，外洩風險較畢業學校紀念冊等紀錄高。

2、主題二、秉持 3C 信任對策，儘早處理危機

為降低資料外洩風險，機敏資料應採取避免蒐集（abstain from collecting）、用完即丟（dispose）及降低資料價值性（devalue）等作法，避免衍生風險。資料外洩事件處理非常複雜，可稱為是組織危機（crisis）。危機溝通前，遭駭組織應釐清資料外洩範圍（含遭駭客存取系統清單、駭客活動歷程及行為、存取資料範圍、入侵系統方式、資料是否持續外洩），並迅速保留入侵偵測系統（IDS；intrusion detection system）、網路流（network flow）、代理伺服器（proxy）等稽核紀錄及相關證據資料。面對這類危機，必須秉持能力（competence），品格（character）和關懷（caring）的三 C（competence-character-caring）信任對策，讓使用者對組織持續維持信任度。

（1）能力（competence）對策

有能力處理危機，不推卸責任。如不幸發生資料外洩事件，依照事件反應標準作業流程，執行準備、偵測與分析、回復及事件處理後作為等步驟。

（2）品格（character）對策

面對資料外洩事件經過及後續處置進度，應由組織承辦或負責人毫無掩飾地親自說明與溝通，讓個資外洩事件危機變為一日故事。

（3）關懷（caring）對策

充分關懷客戶或使用者，儘早落幕重獲客戶或使用者的信任。

3、主題三、秉持 DRAMA 危機管理原則，妥適因應資料外洩事件

資料外洩可能衍生詐欺、資料交易、情報蒐集、勒贖等問題，事件發生時應秉持 DRAMA（develop-realize-act-maintain-adapt）危機管理原則，妥適因應。

（1）事前準備（develop）

事前做好準備工作，勝過事後處理。如孫子兵法所稱：勝兵先勝而後求戰，敗兵先戰而後求勝。

（2）前驅（realize）

釐清資料外洩徵兆，如遭遇密碼攻擊，可看到大量猜密碼紀錄。

（3）緊急處理（act）

資料外洩後，緊急應變與保存分析證據，找出受害範圍及外洩原因，快速負責任地處理，降低傷害。

（4）維持長治久安之道（maintain）

尋求法律訴訟諮詢，針對長期及短期危機所在，研擬減輕傷害計畫，編列經費購買資訊安全工具。

（5）採納建議（adapt）

投資更多預算、人力在資訊安全方面，聘任資安員工或顧問。

4、主題四、網路雲端資料的四階段評估風險

愈來愈多企業將資料上傳至網路雲端環境，面對潛在的資料風險，組織應妥善評估雲端資料的風險議題。

（1）準備階段

- 瞭解資安政策：資料上傳至非組織可完全支配之雲端廠商，是否符合組織政策。
- 妥善選擇雲端廠商：避免雲端業者伺服器可能遭未經授權第三者任意存取，應妥善選擇優質雲端廠商。
- 瞭解雲端儲存資料：避免將不必要資料上傳雲端，降低資料外洩風險。

（2）執行階段

- 資料加密方式：加密上傳雲端資料，多一層保障。
- 認證機制管控：避免使用弱密碼，制訂雲端認證機制權限控管政策。
- 建立存取與分享規範：組態設定錯誤可能造成資料外洩，應建立存取雲端檔案規範，檔案應區分公開、內部、限制或機密等級。

（3）管理階段

- 雲端資料擁有權：雲端廠商服務條款不一，如 Google 服務條款可自由運用使用者資料，Dropbox 服務條款可讓信任的第三方存取使用者資料。
- 雲端託管位置：雲端業者素質參差不齊，雲端伺服器位置所在位置不詳。

（4）稽核階段

- 安全評估：系統安全漏洞評估。
- 落實規範：符合 ISO/IEC 27001:2013 等相關資安規範。
- 事件反應與通知：發生事件時，廠商通知使用者的處理程序。

（二）Black Hat 簡報會主題：107 年 8 月 8 至 9 日

Black Hat 簡報會主題眾多（如圖 5 至圖 8），簡述本次所獲較具心得的主題。摘述如下：

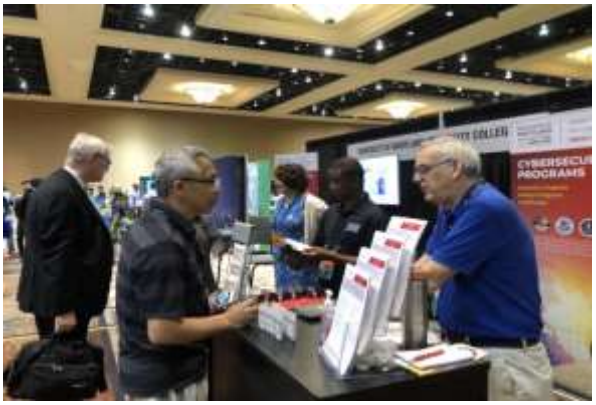

圖 5：Black Hat 參觀美國馬里蘭大學網路安全管理與政策中心攤位

圖 6：Black Hat 與美國馬里蘭大學網路安全管理與政策中心教授商討後續可行合作

圖 7:Black Hat 與知名駭客 Kevin Mitnick 研討資安議題

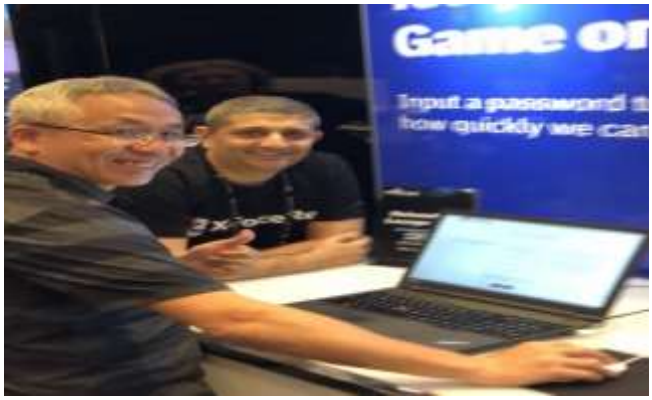

圖 8：Black Hat 體驗破解密碼軟體之速度

1、主題一：手機權限管理，降低資安威脅

題目：KeenLab iOS Jailbreak Internals Userland Read-Only Memory can be Dangerous

講者：Liang Chen, senior security researcher at KeenLab of Tencent

不同作業系統手機（如 Android、ios），有不同的核心架構、權限管理與保護手法，手機存在韌體漏洞問題或軟體設計缺陷，衍生不同手機資安議題。駭客發現漏洞後，為持續利用該漏洞，會利用軟體工具維持存取權限，控制手機，以便日後從後門進入並持續獲得儲存資料。使用者應避免變更原有手機的權限管理，降低資安威脅。

2、主題二：駭客攻擊工業用物聯網

題目：Breaking the IIoT Hacking industrial Control Gateways

講者：Thomas Roth, security researcher and founder of level down security

隨著物聯網的日漸普及，越來越多的工業用物聯網日益興盛。駭客開始覬覦並嘗試從逆向工程中獲得有效資料。工業用物聯網的資安問題，是大家都有的問題，因工業用物聯網負責監控管理如核能發電廠資料採集與監控系統(SCADA，supervisory control and data acquisition)之重要設備，為具有監控程式及資料收集能力的電腦控制系統。駭客可以藉由入侵工業用物聯網，再利用產業控制閘門，連接不同協定的 TCP/IP 網路。由於，許多工業用物聯網使用的資訊系統及安裝檔均相同的，容易使所有工業用物聯網擁有同樣軟體資安漏洞。當工業用物聯網相互連通，則駭客可以連接網路的產業閘門；這樣形同網路上有上千個工業設備是敞開，使任何人皆能夠讓這些工業用物聯網相互串連銜接，把它們串聯在一起。

現在很多工業用物聯網的軟體都明顯過期且沒有更新，漏洞也缺乏維護管理。有存取權限就有被攻擊的可能性，舉凡實體的直接存取、公開的 IP 位址、使用 VPN 並使用固定 IP 位址及

不安全的 Wi-Fi 密碼等等，均是容易被攻擊或存取的態樣。駭客進行攻擊時，會檢查韌體漏洞，發掘潛在的攻擊目標。目前工業用物聯網尚未有一套完整的安全防堵機制，這也是現今物聯網最需要加強資訊安全的部分。

3、主題三：應用乙太坊、區塊鏈與智慧合約

題目：Blockchain Autopsies - Analyzing Ethereum Smart Contract Deaths

講者：Jay Little, security researcher at Trail of Bits

（1）乙太坊與乙太坊虛擬機

乙太坊（ethereum）是可程式化的區塊鏈，為一系列定義去中心化應用平臺協議，它的核心是乙太坊虛擬機（EVM；ethereum virtual machine），可以執行任意複雜演算法的程式碼。開發者能夠使用現有 JavaScript 和 Python 等程式語言，在乙太坊模擬機上建立應用程式。乙太坊不是給使用者進行比特幣交易，而是允許使用者按照自己意願建立複雜的操作。形成如加密貨幣在內的多種類型的去中心化區塊鏈應用平臺。

（2）乙太坊點對點區塊鏈資料庫的維護與更新

乙太坊區塊鏈資料庫由眾多網路節點維護和更新，適合點與點間自動進行直接交互活動的跨網路應用。每個網路節點都運行乙太坊模擬機並執行相同指令，維持整個區塊鏈的一致性，卻也讓乙太坊運算效率較傳統電腦更慢且貴。然而，去中心化的一致性，也讓乙太坊高故障容錯性，保證零停機，使區塊鏈上的儲存資料保持穩定狀態，得協調點對點的複雜財務智慧合約的自動化應用，故比特幣能讓使用者不藉助金融機構或銀行等媒介便能進行貨幣交易。

（3）開放原始碼的乙太坊虛擬機反組譯工具，危及智慧合約安全性

1995 年，Nick Szabo 提出「智慧合約（smart contract）」一詞，指一套數位形式的承諾，合約參與者可依據該合約執行承諾的協議。包含誰簽屬合約（Who）？簽署什麼合約內容（What）？何時簽屬合約（When）？乙太坊虛擬機建立在乙太坊區塊鏈的程式碼環境，能處理乙太坊系統內的智慧合約。但當駭客攻擊乙太坊時，可能篡改智慧合約程式，可能利用 Porosity 等乙太坊虛擬機反組譯工具，識別出智慧合約的原始碼與存在漏洞，形成資安威脅。反之，資安人員亦可透過該工具進行智慧合約的正反面安全測試檢查，才能嚴格評估智慧合約及虛擬貨幣的可信度及穩定性，提升智慧合約穩定性，尋求大眾接受虛擬貨幣的可用性及安全性。

（三）DEF CON 26 駭客安全研討會：107 年 8 月 9 至 12 日

DEF CON 26 駭客安全研討會致力提倡資訊安全研究，意欲在黑帽駭客未經授權惡意入侵他人資通訊系統外，聚集研析、維護資訊安全秩序的白帽駭客資安人才。資安經驗、技術與人才培育，需要政府與企業的長期贊助與投入。在此研討會中，可不斷觀察新的攻擊行為，進而產生新的偵查、防制或鑑識技術。透過不間斷地國際交流的技術切磋與資訊安全的議題發展，希望能傳承資訊安全的技術與能量，帶給臺灣的偵查資安犯罪環境做出貢獻。

圖 9：DEF CON 研討會場

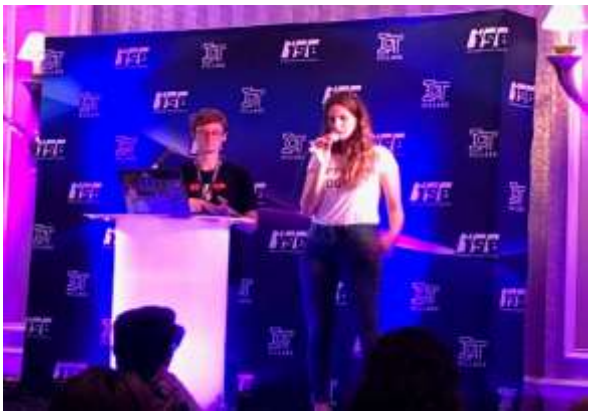

圖 10：DEF CON 之 IOT 專題研討會場

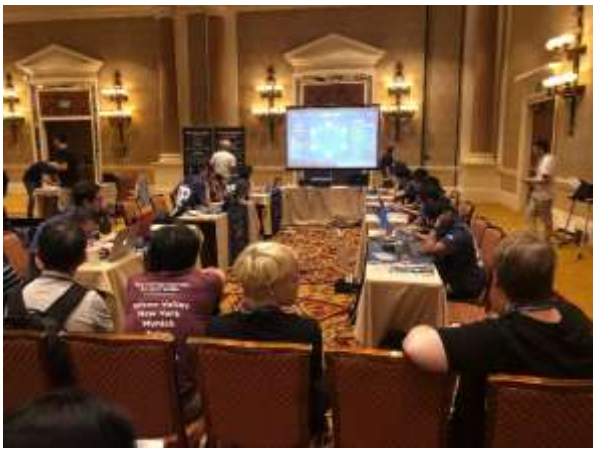

圖 11：DEF CON 之搶旗賽專題研討會場 1

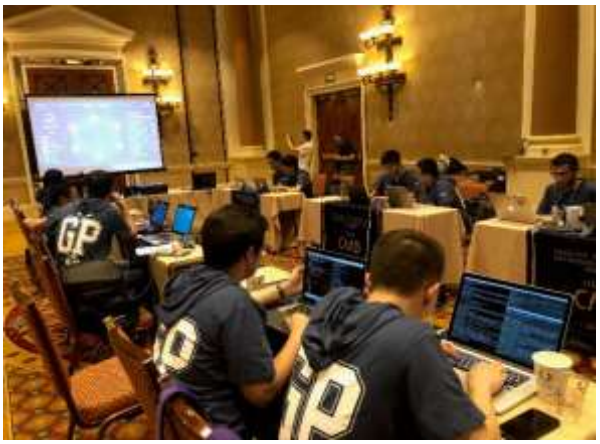

圖 12：DEF CON 之搶旗賽專題研討會場 2

1、主題一：模糊偵查惡意軟體

- **題目：Fuzzing Malware For Fun & Profit. Applying Coverage-guided Fuzzing to Find and Exploit Bugs in Modern Malware**
- **講者：Maksim Shudrak, Senior Offensive Security Researcher, Salesforce**

演講者使用模糊邏輯方式找出惡意軟體的攻擊行為，該模糊偵查惡意軟體主要功能包含分析惡意軟體、發現攻擊漏洞，期發覺惡意軟體的加密手法，偵測惡意軟體的遠距離程式執行控制或關閉殭屍設備技巧，防止系統遭遠距離拒絕服務攻擊侵害，尋求解決之道，並評估可能帶

來的利益。網路分散式阻斷攻擊，以物聯網為基礎，進行 Tb 級的攻擊模式，透過中間人攻擊方式安裝木馬，達到操控目標主機或獲取相關資料為目的。演講者們撰寫偵查惡意軟體時，遇到的挑戰議題包含初步逆向惡意軟體工程的需求、發現惡意軟體功能、選取中間媒介設備檔案、網路流量加密及偵查惡意軟體穩定性等。期待未來的偵查惡意軟體工作，可自動發現目標、增加偵查惡意軟體穩定性及視覺化圖形呈現，以防衛惡意軟體，提升網路安全防護能量。

2、主題二：控制物聯網權限

- 題目：Your Watch Can Watch You! Gear Up for the Broken Privilege Pitfalls in the Samsung Gear Smartwatch
- 講者：Dongsung Kim, Graduate Student, Sungkyunkwan University & Hyoung-Kee Choi, Professor, Sungkyunkwan University

許多資訊設備皆會連結網路，形成日漸普及的物聯網，但因物聯網技術的尚未成熟，存在許多資訊安全漏洞；復因物聯網內含眾多記錄周圍環境資料特性成為駭客攻擊目標，物聯網的管理控制議題，屬值得深思討論的資訊安全問題。管理控制物聯網的方法，可區分為提升使用者使用物聯網的權限、要求物聯網提供服務以及資料庫的分析，以發現物聯網之資料。物聯網存在 Wi-Fi、藍芽、螢幕顯示、訊息通知與電子信箱等不同資安弱點，成為駭客的可能攻擊標的，分述如下：

（1）控制 Wi-Fi 權限

駭客控制 Wi-Fi 權限後，可利用 GPS 座標取得 Wi-Fi 定位，即使使用者關閉定位功能，惡意軟體仍能追蹤使用者的所在位置。

（2）控制藍芽權限

駭客取得藍芽連接權限後，可取得該設備的聯絡人通訊錄及輸入輸出等資料。

（3）控制螢幕顯示權限

駭客取得使用者設備的螢幕權限後，可觀察使用者的操作行為與查閱內容，藉此分析使用者行為。

（4）控制訊息通知權限

駭客取得物聯網的管理通知功能後，可選擇管理通知訊息顯示與否。惡意軟體亦可清除所有物聯網裝置的通知功能，並獲得所有通知紀錄。

（5）控制電子信箱權限

駭客取得使用者的信箱權限時，可管理信箱的通知訊息，惡意軟體可啟動信箱的應用程式、修正信箱的信件訊息及利用使用者的電子郵件信箱地址寄送信件給他人。

3、主題三：巨量資料分析：以巨量的網路封包資料為例

- 題目：Asur: A huge PCAP file analyzer for anomaly packets detection using massive multithreading
- 講者：Ruo Ando, Center for Cybersecurity Research and Development, National Institute of Informatics, Japan

網際網路及社群網站普及後，網路出現大量結構化、非結構化資料，收集資料變得相對容易。隨著大量網路資料的傳輸與分享，巨量資料常超出傳統軟體於可接受時間內的處理能力；分析大數據的需求隨之而生，巨量資料分析也成為當前熱門議題。警政資訊管理人員獲得大量資料後，為加速分析的速度與準確度，須先執行資料減量，進行篩選，去除重複性或無關分析資料；再透過分散式文件系統，分散式資料庫，雲端運算平臺，網際網路和可擴展的資料儲存系統等機制分析大量資料，大規模並行處理資料，尋求善用大數據的大量的（Volume）、多變的（Variety）、有價值的（Value）、快速的（Velocity）及準確性高的（Veracity）等特性，發現相關可用資料。

許多組織認為蒐集越多資料，就擁有越多資訊可供日後分析，但實際上，組織所能處理資料的軟硬體資源相當有限。因此，系統前端的資料篩選、資料減量成為資料處理重要步驟，也考驗資料處理者的理性判斷及組織策略考量。分析巨量資料時，須先選擇需要欄位再進行分析，以網路封包為例，可供選擇欄位如下所述：

（1）TCP 檔頭

TCP 檔頭包含來源連接埠（Source Port）、目標連接埠（Destination Port）。

（2）IP 檔頭

IP 檔頭包含總長度（Total Length）、封包生存時間（Time to live）、來源 IP 位置（Source IP Address）、目標 IP 位置（Destination IP Address）、選項（Options）、填充（Padding）。

4、主題四：入侵資訊資訊系統：以選舉為例

- 題目：Defending the 2018 Midterm Elections from Foreign Adversaries
- 講者：Joshua M Franklin, Hacker & Kevin Franklin, Hacker

隨著資訊系統的普及，越來越多的公家設備或服務使用電子化，美國等國家開始使用電子化的選舉系統，且可遠距離進行投票，但因選舉結果往對國家或社會大眾有重大影響，往往淪為有心人事進行攻擊目標，相關數位設備的保護與資訊安全防禦尤顯重要。為確保投票系統的安全性與結果計算的可靠度，資訊安全管理人員應從不同面向分析，了解網路選舉系統面臨的投票系統製造商、投票系統經銷商、投票者登入廠商與投票服務提供者等各種需求服務與挑戰。為有效防止該類型設備遭駭客入侵，可使用工具分述如下：

（1）查詢 Whois 資料庫

使用 Whois 資料庫，透過網域註冊的網域註冊時間、到期時間及網域名稱註冊商相關資訊等登記聯絡資訊，可查詢網際網路網域名稱的所有者資料，了解相關 IP 位址使用者之相關資訊。

（2）分析關注議題

利用資訊分析，可了解使用者關注的相關資訊議題，進行選情分析。

（3）統計運算工具

應用網路爬蟲等網路工具可加速網路分析，或加快統計運算相關資訊。

此外，臺灣有些票選活動也會透過電子選票方式進行票選，我們必須持續的保護網路票選或選舉，才能提供具可靠性、正確性、安全性的資訊系統，加強自身資訊安全防衛能力，即時回報系統漏洞與資訊洩漏是很重要的工作。政府機關應對所有重要資訊系統應進行雙重認證，保持可信任的認證，相同網域才能具備管理功能，限制內部網域內才能執行開源碼工具，了解使用程式內容與相關執行行為，避免工具程式暗藏木馬程式。

四、參加心得

資通訊科技內涵廣泛，資安網路犯罪偵查人員須不斷充實精進，期透過「基本防護」、「基礎安全」及「組織管理」等不同面向，保護資訊系統使用者的安全與隱私。不管是最新的系統弱點、攻擊技術或是木馬隱藏與通訊技術，配合新的系統的發佈使用，相關新的攻擊、防禦與

偵查作為也要不斷的推陳出新。這次參加美國拉斯維加斯 Black Hat 及 DEF CON 會議，除參與訓練課程及聽取演講外，了解到各國為分享資安情資及推廣防禦技術，並更深入了解內容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搶旗競賽，實在收穫良多。未來，應視流程化、服務性的網路犯罪組織為組織危機，資安公司更須不斷改寫自動化工具程式，強化資安措施，朝程式自動化方式蒐集相關稽核紀錄，作為數位證據，進一步嚇阻資安犯罪。本次蒐集最新的資訊安全相關技術資料，期將所獲得技術應用警察科技教育或網路犯罪偵查作為中。

（一）資通訊科技內涵廣泛，須不斷充實精進

為期許充實最新資安技術與能量，參加一年一度的駭客年會，能跟各國與會資安人員請教、交流、蒐集最新資安攻擊與防禦技術，使我國能快速掌握最新的資訊犯罪攻防及偵查技術，以提供科技執法參考。每當資訊業者發佈使用新的資訊系統，新的系統弱點、攻擊技術、或木馬隱藏技術伴隨而來，新的防禦與偵查作為也要不斷的推陳出新。資通訊範圍廣泛，若沒有團隊合作，很難處理資訊安全問題，沒人可用一己之力完成所有資訊安全工作。網路犯罪偵查人員若什麼都會，就會都不專精，需要專注在證據識別、蒐集、檢查、分析與呈現的資料處理上。要有效率的合作，才能有效提升安全等級！

本次會議後，對現今流行科技與駭客思維、技術與犯罪手法有更深入了解，亦將持續蒐集新的資訊安全技術資料，期執行資訊安全控制與管理，期能更有效率地執行在符合資訊安全要求下，運作警政科技運用，並將所獲得技術應用警察科技教育或網路犯罪偵查作為中。例如，逆向工程透過反向技術過程，分析軟硬體產品的程式碼，推導設計原理、演繹處理流程、組織結構、功能效能規格等設計內涵，進而製作功能相近，又不完全一樣的產品。逆向工程有多種實現方法，主要有「分析網路封包」、「反組譯」及「反編譯」三項，亦可作為尋找侵犯專利權或智慧財產權的證據方法。

1、分析網路封包：進行通訊資料分析

協定逆向工程，會在電腦匯流排或網路連接處，使用 SoftICE 底層偵錯程式、JTAG 埠、匯流排分析工具、封包側錄工具或各種偵錯工具，截取通訊資料，以進行通訊資料分析。

2、反組譯：翻譯成組合語言程式碼

藉用 Interactive Disassembler、Reshape、NET Reflector 等反組譯工具，把程式的原始機器碼，翻譯成較便於閱讀理解的組合語言程式碼。

3、反編譯：重現高階語言程式碼

反編譯工具，將已編譯好的程式語言還原到未編譯狀態，找出程序語言原始碼。單一種反編譯工具通常只能侷限在1至2種程式語言。藉用Java Decompiler、Apktool、IDA PRO、EmilPRO 、Gapktool 等反編譯工具，可嘗試從程式的原始機器碼或位元組碼，重現高階語言形式的原始碼。

（二）保護資訊系統使用者的安全與隱私

任何資訊系統的設計與運用，須注意安全、維持安全，保護使用者的安全與隱私，並從「基本防護面（basic prevention）」、「基礎安全面（foundational security）」及「組織管理面（organizational management）」等三面向分述之：

1、基本防護面

基本防護面的硬軟體資產管理，包含持續性弱點管理、使用管理者權限監管、維持稽核紀錄、監控分析、行動裝置、筆記型電腦、工作站與伺服器的軟硬體安全認證等。

2、基礎安全面

基礎設施的資訊安全性，乃基於需求的無線存取或帳號監控存取控制，包含信箱與網頁瀏覽器的保護、惡意軟體的防禦、協定與服務的限制與控制、資料復原的能力、網路設備如防火牆、路由器與橋接器的安全認證、邊界防禦、資料保護等。

3、組織管理面

除基本防護與基礎安全外，組織管理也是資訊安全的重要一面，包含安全認知訓練、應用程式安全、突發事件的立即反應、滲透測試演練等。

（三）視流程化、服務性的網路犯罪組織為組織危機

目前正處於一個網路犯罪災害日漸頻傳且迫切需要監控的網路犯罪黃金時代，隨著資訊安全重要性的日漸提升，如何最大化資訊安全的應用，是一值得討論問題。預測網路犯罪趨勢如

下：

1、服務性的網路犯罪組織，降低犯罪困難度

網路犯罪者可透過滲透測試、逆向工程的獲得程式碼，當暗網（dark web）賣家提出「以網路犯罪為服務（cybercrime as a service）」時，讓許多未具專業網路使用者，能從事網路犯罪，並從中獲利。

2、流程化的網路犯罪組織，不斷改寫程式自動化的資安措施

網路犯罪程序已日漸走向團隊犯罪流程化、套裝化，從一開始的運作流程、工具包裝、銷售執行、專業代客入侵、重複販售類似功能惡意程式等現象，流程化的網路犯罪會促進犯罪工具與手法日趨複雜與完備。

3、視服務性、流程化的網路犯罪為組織危機，朝程式自動化方式嚇阻資安犯罪

網路犯罪團體不會使用過時手法，犯罪手法均會積累過往的知識、技術與能力，轉換攻擊模式或特徵，再行持續攻擊。他們會持續改進犯罪工具，往往提供非專業攻擊者，購買網路犯罪服務，激進網路犯罪暗網黑市的不斷擴展。當犯罪者對犯罪工具或特徵不清楚，數位證據的識別、蒐集、檢查、分析與保存將更顯複雜。因此，資訊安全措施亦須朝向程式自動化，有效輔助人力，達到即時制止資安犯罪目的。

五、建議事項

網路普及與物聯網興起，資安議題將越顯重要。本次研習活動，從許多知名專家學者中，獲取新型態資安攻擊與防護技術，會議資安議題集中在區塊鏈、物聯網等新興科技的攻擊及防禦手法。綜整整理值得我們學習的發展方向如下：

（一）延續國際合作機制，提升相關研究水準

目前我國已有初步警政或資安國際合作機制，但相關連結運作仍須經費支持，若能持續申請國際合作研究計畫或參與國際學術組織，藉由國外前瞻性之研發技術與成果引進，將有效提升國內警政或資安相關研究水準。

（二）加強學術及實務機關互動學習，持續發展擅長的專業技術領域

本次活動學術及實務機關各派員出席研習活動，與會過程可就近、即時相互研討國內外案

例與資安議題，對於所獲得最新技術的消化與吸收，頗具效果。爾後，若有類似機會，建議持續跨機關選派合適人員參加研習活動，專注科技建警研究，輔助警察勤業務的順利運作，持續發展各系、各教師或各員警擅長的專業技術領域，加強學術及實務機關的互動學習與成長。期建立良好的中長期產官學合作團隊，持續提升本大學專業形象與重要性，與各執法機關彼此緊密合作關係，培育研發能量，並提供執法機關專業支援。

（三）持續理論結合實務的研習活動，維持跨機關或跨境的良好互動關係

數位時代帶來更多機會，物聯網、雲端運算及人工智慧的快速發展，打破原有藩籬，暴露更多、更具破壞性的網路攻擊威脅，卻也帶來嶄新機會；面對未來網路安全帶來的挑戰，可從防護、創新及夥伴關係面向著手，期培養網路安全能力，提升數位信任機制，滿足目前網路運作需求，刺激未來成長，以形塑一個值得信賴與開放的網路空間。本次活動行程過程中，看到跨機關或跨境的良好互動關係，非一朝一夕可建立，建議選派研究人員參與國際學術會議或研討會，加速提升研發團隊之專業與技術，提升相關人員資訊安全觀念與能力。除本次的美國拉斯維加斯舉辦的 Black Hat 及 DEF CON 資安駭客技術會議外，爾後可派員參加其他相關研討會議，見證各國政府、企業、學術研究的資安犯罪偵查、鑑識或防制成功經驗、發展方向或成果。舉例列舉如下：

1、以色列網路周

2018 年 6 月 17 至 21 日，以色列網路周（Cyber Week）有來自 60 多個國家的 6000 多名與會者，包含 50 多個圓桌會議、討論會、研討會和論壇，每年邀請企業、法人、政府組織、資安團體等全球產官學研界專家共襄盛舉，提供網路創意、連結產業應用機會，促進網路創新及資安產業合作。以色列資安產業發展，鎖定資安防禦、資訊戰及資安生態圈等主軸，該活動可提供我們許多發人深省的交流想法。

2、新加坡國際網路周

2018 年 9 月 18 至 20 日，第三屆新加坡國際網路周（SICW，Singapore International Cyber Week），參加者超過八千名，並同步舉辦國際刑警組織與歐洲刑警組織網路犯罪會議（INTERPOL-Europol Cybercrime Conference）、東協網路安全部長級會議（ASEAN Ministerial Conference on Cybersecurity）、東協網路犯罪檢察官圓桌會議（ASEAN Cybercrime

Prosecutors’ Roundtable Meeting)、全球網路專業論壇年會及全球穩定委員會聽證會網路空間。新加坡資安產業發展從國家角度思考資安威脅策略，鎖定強化關鍵資訊基礎設施、培育更安全的網路環境、深化網路安全能力及強化整合伙伴關係等面向，期結合國際資安團隊力量，強化該國資安環境。

3、印度網路法律、網路犯罪和網路安全國際會議

2018年11月14至16日將在印度新德里舉行網路法律、網路犯罪和網路安全國際會議(The International Conference on Cyberlaw, Cybercrime & Cybersecurity)，該會議致力於審查和分析新興的網路法律，網路犯罪和網路安全趨勢。提供為期3天會議，除提供互動課程外，亦由150多位國際演講者發表，能與世界各國優秀人才建立聯繫，類似活動宜普補助績優教師、學生或員警參與研習。