行政院所屬機關因公出國人員出國報告

（出國類別：會議）

赴日本出席 2015 年「第 18 屆攻擊、入侵和防禦國際研討會(RAID)」

服務機關：財政部財政資訊中心

姓名職稱：王國隆 設計師

派赴國家：日本

出國期間：104 年 10 月 31 日至 104 年 11 月 5 日

報告日期：105 年 1 月 30 日

摘要

「攻擊、入侵和防禦國際研討會(International Symposium on Research in Attacks、Intrusions and Defenses, RAID)」係每年舉辦一次的資安盛會，今年第十八屆會議於 2015 年 11 月 2 日至 11 月 4 日召開，選在結合現代與古典美的都市-日本京都舉辦，更突顯科技與古典結合的境界。

自 1998 年以來，來自歐洲、亞洲，北美等各地區的學者、政府與業界專家齊聚一堂，對入侵檢測領域的相關研究進行研討與分享，這幾年來成果豐碩，以今年為例，共有 119 篇論文投稿，經過主辦委員會嚴格的審查，選定 28 篇入選論文發表，其主題包括有：1、搭配硬體玩點酷玩意兒(Cool Stuff You Can Do With Hardware)； 2、網路(Networks)； 3、硬化(Hardening)； 4、攻擊檢測 I(Attack Detection I)； 5、網頁與網路(Web and Net)； 6、安卓(Android)； 7、隱私(Privacy)； 8、評估解決方案(Evaluating Solutions)； 9、攻擊檢測 II (Attack Detection II) 等 9 個領域，使為期 3 天的會議以緊湊的步調，完成這些領域的論文發表。

本次會議的重頭戲—專題演講，係邀請到任職於 Google 的馬克希朋(Mark Seaborn)，以「難以補丁的問題：在 DRAM 排錘錯誤和快取時序側通道的可能發展(Hard-to-patch problems: Exploitability of the DRAM rowhammer bug and cache timing side channels)」為題，描述自 2010 年在講者任職的 Google Project Zero 團隊發現的錯誤問題，提出近期在 DRAM DDR3 上所發現的排錘錯誤(Rowhammer bug)，已被證明能夠輕易地透過網頁實現，目前這個潛在製程上所造成的安全議題，馬克希朋提出其團隊發現的各種漏洞及其可能的解決方案，提供與會學者專家參考，另外，Project Zero 團隊研究人員在 2014 分析證明，統計出在市面上 2012 和 2013 製造的 DRAM DDR3 芯片很容易受到干擾錯誤，這是一項值得重視的特徵，可作為政府機關評估設備風險的重要參考。

目次

壹、 目的

「攻擊、入侵和防禦國際研討會(International Symposium on Research in Attacks、Intrusions and Defenses, RAID)」自 1998 年首次於比利時舉行，每年分別在美國、歐洲、澳洲等地舉辦，今年是第一次移師亞洲，由日本擔任主辦國，於初秋時節在古色古香的京都舉辦，除享有豐富的學術收穫外，更領略到紅葉翩翩的古都風情。

在第 18 屆攻擊、入侵和防禦國際研討會(RAID 2015 年)旨在匯集來自學術界，政府和業界領先的研究者和實踐者探討新的研究成果，凡涉及計算機和資訊安全的任何領域，對有關入侵檢測和預防所有主題都歡迎發表，包括的論文範圍有：

一、 惡意軟件和殭屍網路的分析，檢測和解法。

二、 智慧型手機和其他嵌入式系統的安全。

三、 網路和防禦。

四、 Web 應用程式的安全性。

五、 對抗電腦和網路新攻擊。

六、 DoS 攻擊。

七、 內部攻擊檢測。

八、 形式化模型，分析和標準。

九、 欺騙系統和蜜罐中的漏洞分析。

十、 安全的軟體開發。

十一、 學習機的安全。

十二、 計算機安全可視化技術。

十三、 網路滲出。

十四、 線上洗錢和地下經濟。

十五、 硬體漏洞。

十六、 二進制分析和逆向工程。

十七、 數位驗證。

十八、 安全和隱私。

十九、 入侵檢測和預防。

探討主題相當廣泛與多元，歷年來提供世界各地專家學者一個資訊交流的平台，發表最近研究的成果，製作相關論文集於會議中共同研討，與會人員得以擴展國際視野及世界觀。

貳、 過程

一、「第 18 屆攻擊、入侵和防禦國際研討會(RAID)」舉辦地點簡介

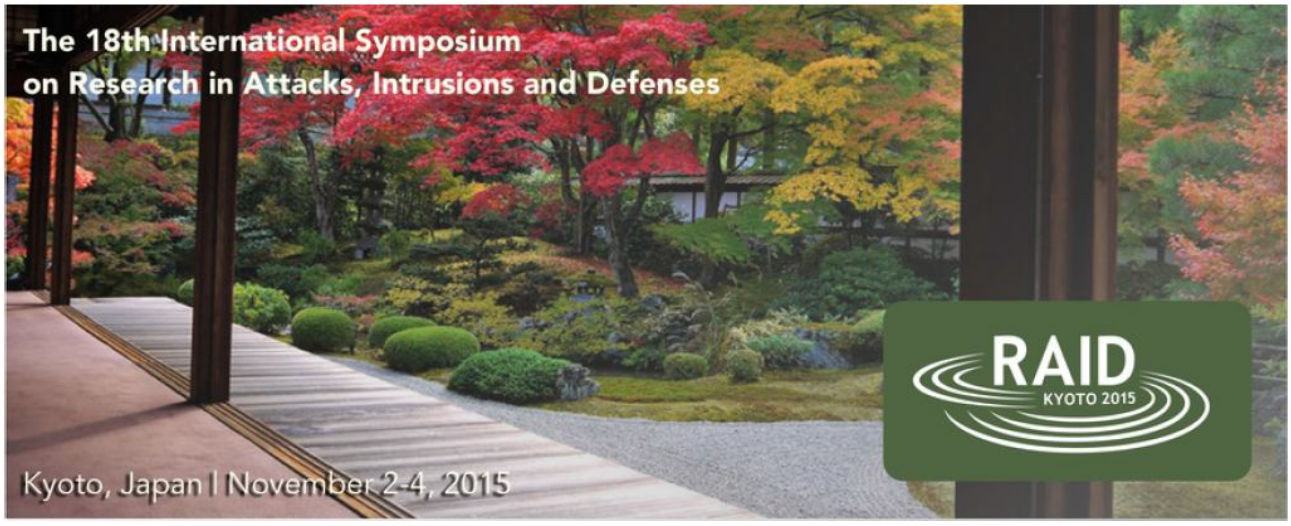
「攻擊、入侵和防禦國際研討會(International Symposium on Research in Attacks、Intrusions and Defenses, RAID)」已舉辦 18 次，2015 年是第一次移師亞洲地區，由日本擔任主辦國，日本國立奈良先端科技大學(Nara Institute of Science and Technology, NAIST)統籌此次會議，特別選在兼具古典與現代的都市—京都舉辦，京都位於日本關西地區，位置在日本國土的中央，南來北往的交通皆相當發達。一千數百年前，日本首都曾設置於大阪、奈良、京都等地，為政治、經濟、文化之中心，盛極一時，該地區流傳至今的文化財眾多，日本國寶約有 6 成位於關西，並有多處獲登錄為世界文化遺產的景點。此外，日本三大古典演藝活動，同時也是世界無形文化財的能劇、文樂、歌舞伎等皆發源自關西，並為日本代表性傳統文化－茶道、花道等之發源地。

▲此次會議的舉辦場地，位在京都車站南方的「京都テルサ」會議中心，交通相當便利。

2015 年 11 月 2 日報到當日，是這 3 天會議中唯一的下雨天，從九条地鐵站一路撐著雨傘搜尋方向走到會場，帶著一顆忐忑不安害怕迷路而遲到的心情到達會議中心，即受到接待人員熱烈的招待，展現日本人樂群好客的特性，也讓溼冷的身體頓時溫暖了起來。

▲2015 年 11 月 2 日報到時的接待櫃台

二、「第 18 屆攻擊、入侵和防禦國際研討會(RAID)」議程



Program

Monday, November 2, 2015

- 09:00 - 09:15 Opening (15 minutes)
- 09:15 - 10:15 Keynote (60 minutes)
- 10:15 - 10:30 Coffee Break (15 minutes)
- 10:30 - 12:30 Session 1: Cool Stuff You Can Do With Hardware (120 minutes)
- 12:30 - 14:00 Lunch (90 minutes)
- 14:00 - 15:30 Session 2: Networks (90 minutes)
- 15:30 - 16:00 Coffee Break (30 minutes)
- 16:00 - 17:30 Session 3: Hardening (90 minutes)
- 19:00 - 21:00 Banquet (120 minutes)

Tuesday, November 3, 2015

- 09:00 - 10:30 Session 4: Attack Detection I (90 minutes)
- 10:30 - 11:00 Coffee Break (30 minutes)
- 11:00 - 12:30 Session 5: Web and Net (90 minutes)
- 12:30 - 14:00 Lunch (90 minutes)
- 14:00 - 15:30 Session 6: Android (90 minutes)
- 15:30 - 16:00 Coffee Break (30 minutes)
- 16:00 - 17:00 Session 7: Privacy (60 minutes)
- 17:00 - 18:30 Poster Session (90 minutes)
- 19:00 - 21:00 Reception (120 minutes)

Wednesday, November 4, 2015

- 09:00 - 11:00 Session 8: Evaluating Solutions (120 minutes)
- 11:00 - 11:30 Coffee Break (30 minutes)
- 11:30 - 13:00 Session 9: Attack Detection II (90 minutes)
- 13:00 - 13:15 Closing (15 minutes)

三、專題演講及研究論文發表之內容簡介

自 1998 年以來，來自歐洲、亞洲，北美等各地區的學者、政府與業界專家齊聚一堂，對入侵檢測領域的相關研究進行研討與分享，這幾年來成果豐碩，發表的論文不計其數，受到國際上高度的讚揚，今年也不例外，以下為「專題演講」及「研究論文發表」之內容簡介。

會議首日例行性安排一場專題演講(Keynote)，邀請到任職於 Google 的馬克希朋(Mark Seaborn)，以「難以補丁的問題：在 DRAM 排錘錯誤和快取時序側通道的可能發展(Hard-to-patch problems: Exploitability of the DRAM rowhammer bug and cache timing side channels)」為題，探討其任職於 Google 的 Project Zero 團隊自 2010 年發現 Rowhammer 的錯誤問題，提出硬體有時會有令人意想不到的資安問題—直接存取記憶體的恐怖性(Just accessing memory is scary)，讓與會人員思考，是否我們僅習慣於軟體的 bug，對硬體的 bug 顯得忽視或無所適從。

馬克希朋致力於沙盒(sandbox)的工作，他從事一些不同類型的Linux沙盒研究，以及跨多個作業系統和架構的 Google 瀏覽器在就地用戶端 (Native Client，NaCl)網絡上運行程式碼沙盒的研究工作。發現在 NaCl 沙盒可模擬出各種漏洞，並且近期

提出他所發現概念式證實(proof-of-concept)的漏洞，當介紹有關 rowhammer 的 DRAM 錯誤後，講者表明，它是可被證實的漏洞，且經進一步研究，可發展至時序側通道漏洞的陰暗世界。

這個問體是影響當代 DDR3 架構的動態隨機記憶體(DRAM)漏洞，雖不是全面性一定會發生，但運用沙箱(Sandbox)的程式重複測試，經研究確實有發生的機會，讓這個一般被視為可靠度問題，讓人進一步思考，是否應提升為資訊安全問題。

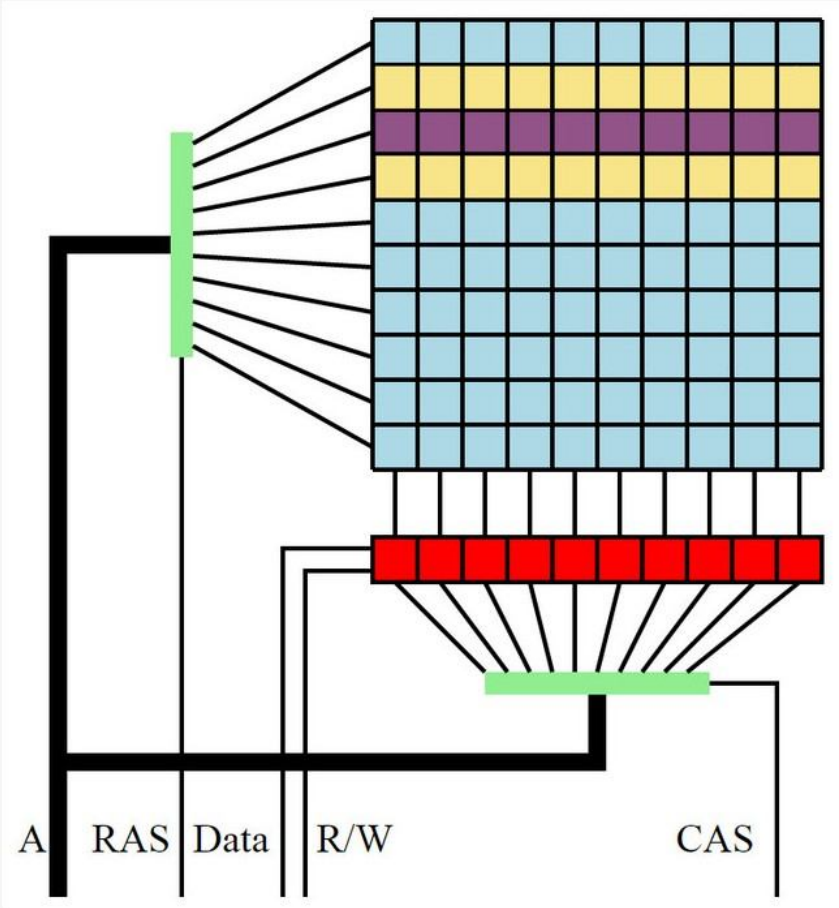
▲專題演講(Keynote)講者：馬克希朋(Mark Seaborn)先生

想要了解 Rowhammer 這個漏洞的運作原理，首先必須釐清 DRAM 的內部運作方式。在 DRAM 中每個記憶單一位元使用 1 個電容和電晶體所組成，這些記憶單元再透過交錯縱橫的線路連接起來，以讀取或是寫入資料時，就由這些交錯縱橫的線路來運送資料。

通常一堆記憶單元組成 1 組 bank，內部橫向線路所連結的記憶單元稱為 row，垂直稱為 column，這堆線路旁邊還會附加 row 解碼器、column 解碼器、用以信號放大和解讀的感測放大器等。而一顆顆的 chip 就是由一組數量不等的 bank 所組合而成，也就是我們在記憶體模組或是顯示卡上面常見的黑色長方形小晶片。

隨製程進步，記憶單元之間的間隔距離變得相當靠近，造成記憶單元進行存取

工作時，也會連帶影響鄰近的記憶單元電荷流失或轉變。Rowhammer 攻擊就是利用此原理，不斷地以 row 為單位，存取目標旁邊的記憶單元，從而影響目標記憶單元，從中得到意外結果。

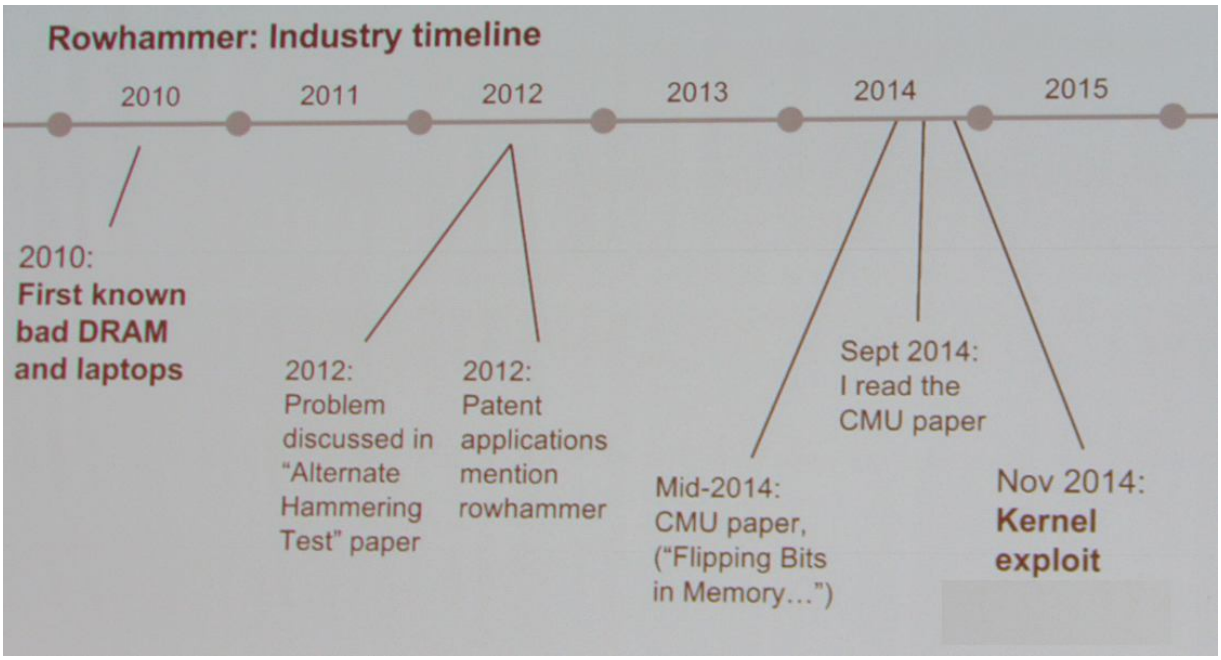


▲Rowhammer 攻擊的原理，透過不斷地存取紫色記憶單元，相鄰的黃色記憶單元內部資料將有所變化。（圖片取自維基百科）

這個硬體漏洞早在 2010 年已提出警告，不過當時僅是了解原理，並沒有人能夠進行有意義的實作，直到 2015 年初講者 Google 的 Project Zero 團隊才展示如何利用此漏洞，進行攻擊達到 2 種目標，其一為跳出 Google Chrome 網頁瀏覽器的 native-client 沙盒，另一種則是能夠在 Linux 作業系統中提升至 root 權限。

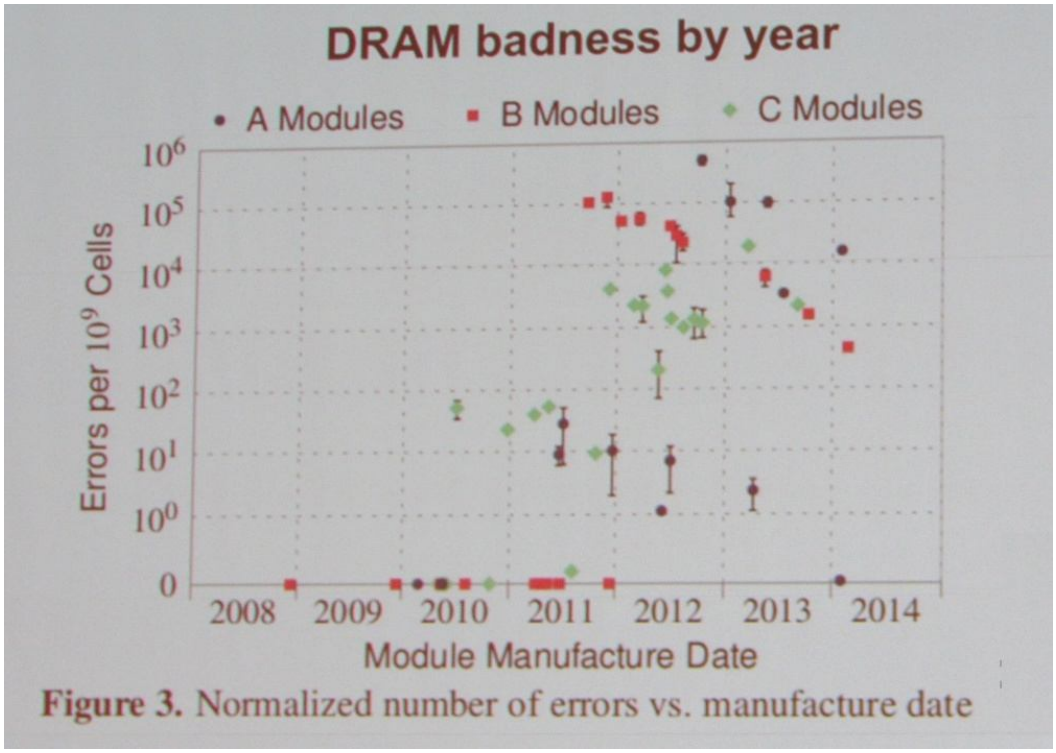
以下的時間表，描述講者馬克希朋的 Project Zero 團隊自 2010 年首次發現此項漏洞後，隨即針對此項問題所提出的研究，包括 2012 年提出可替代性的排錘(Rowhammer)試驗報告、2014 年在 CMU(美國卡內基梅隆大學)發表的記憶體位元置

換論文，及 2014 年排錘(Rowhammer)的核心漏洞等，該團隊皆持續關注與研究。



▲Rowhammer 漏洞探討的時間表

Project Zero 團隊所使用的驗證方式，必須先在目標裝置上植入特殊設計的程式碼，而近日所研究出的方法，使用 JavaScript 語言撰寫，只要裝置重複存取特定網頁即可執行，大大提升了此漏洞的可用性。目前講者的團隊已在 Intel 的 Haswell 、Sandy Bridge、Ivy Bridge 等架構處理器上確認此漏洞的可能。另外，Project Zero 團隊研究人員在 2014 分析證明，統計出在市面上 2012 和 2013 製造的 DRAM 芯片 DDR3 很容易受到干擾錯誤，這是一項值得重視的特徵，可作為我們評估設備風險的重要參考，可惜的是，講者僅標示 A、B、C 三種記憶體模組，基於對廠商商譽的保護，並未明白指出是哪個製造廠牌出產的，下面的統計圖表呈現各年代三種記憶體模組可能發生此類錯誤的機率。



▲Project Zero 團隊研究人員在 2014 分析證明，統計出在市面上 2012 和 2013 製造的 DRAM 芯片 DDR3 很容易受到干擾錯誤。

在 60 分鐘精彩的專題演講後，接下來是論文發表，今年共有 119 篇論文投稿，經過主辦委員會嚴格的審查，選定 28 篇入選論文發表，其主題包括有：1、搭配硬體玩點酷玩意兒(Cool Stuff You Can Do With Hardware)； 2、網路(Networks)； 3、硬化(Hardening)； 4、攻擊檢測 I(Attack Detection I)； 5、網頁與網路(Web and Net)； 6、安卓(Android)； 7、隱私(Privacy)； 8、評估解決方案(Evaluating Solutions)； 9、攻擊檢測 II (Attack Detection II) 等 9 個領域，使為期 3 天的會議以緊湊的步調，完成這些領域的論文發表。

以下為 3 天的論文主題，分別列表如後:

論文主題	作者
Monday， November 2， 2015	
Session 1: Cool Stuff You Can Do With Hardware 搭配硬體玩點酷玩意兒	
Ensemble Learning for Low-level Hardware-supported Malware Detection 對低階硬體支援的惡意程式檢測學習	Khaled N. Khasawneh; Meltem Ozsoy; Caleb Donovick; Nael Abu-Ghazaleh; Dmitry V. Ponomarev
Physical-layer Detection of Hardware Keyloggers 硬體鍵盤記錄器的物理層檢測	Ryan M. Gerdes; Saptarshi Mallick
Reverse Engineering Intel Last-Level Cache Complex Addressing Using Performance Counters 逆向工程使用性能計數器於英特爾最新快取複雜的尋址	Clémentine Maurice; Nicolas Le Scouarnec; Christoph Neumann; Olivier Heen; Aurélien Francillon
Hardware-Assisted Fine-Grained Code-Reuse Attack Detection 硬體輔助精細劃分的程式碼重用攻擊檢測	Pinghai Yuan; Xuhua Ding; Qingkai Zeng
Session 2: Networks 網路	
Haetae: Scaling the Performance of Network Intrusion Detection with Many-core Processors Haetae：擴大網路入侵檢測與多核心處理器性能	Jaehyun Nam; Muhammad Jamshed; Byungkwon Choi; Dongsu Han; KyoungSoo Park

Demystifying the IP Blackspace 揭秘 IP 黑洞	Quentin Jacquemart; Pierre-Antoine Vervier; Guillaume Urvoy-Keller; Ernst Biersack
Providing Dynamic Control to Passive Network Security Monitoring 提供動態控制被動式網絡安全監控	Johanna Amann; Robin Sommer
Session 3: Hardening 硬體	
Probabilistic Inference on Integrity for Access Behavior Based Malware Detection 基於完整性概率推斷存取行為的惡意程式檢測	Weixuan Mao; Zhongmin Cai; Xiaohong Guan; Don Towsley
Counteracting Data-Only Malware with Code Pointer Examination 對抗僅資料面的惡意程式碼指標檢查	Thomas Kittel; Sebastian Vogl; Julian Kirsch; Claudia Eckert
Xede: Practical Exploit Early Detection Xede：實用的早期檢測漏洞	Meining Nie; Purui Su; Qi Li; Zhi Wang; Lingyun Ying; Jinlong Hu; Dengguo Feng
Tuesday， November 3， 2015	
Session 4: Attack Detection I 攻擊檢測 I	
Preventing Exploits in Microsoft Office Documents through Content Randomization 通過內容隨機化防止 Microsoft Office 文件的漏洞	Charles Smutz; Angelos Stavrou
Improving accuracy of static integer overflow detection in binary 提高二進位靜態整數溢出檢測的準確度	Yang Zhang; Xiaoshan Sun; Yi Deng; Liang Cheng; Shuke Zeng; Yu Fu; Dengguo Feng
A Formal Framework for Program Anomaly Detection 正框架程式的異常檢測	Xiaokui Shu; Danfeng (Daphne) Yao; Barbara G. Ryder
Session 5: Web and Net 網頁與網路	

jAEk: Using Dynamic Analysis to Crawl and Test Modern Web Applications jAEk：使用動態分析抓測現代 Web 應用程式	Giancarlo Pellegrino; Constantin Tschürtz; Eric Bodden; Christian Rossow
WYSISNWIV: What You Scan Is Not What I Visit 你掃描到的不是我巡訪到的	Qilang Yang; Dimitrios Damopoulos; Georgios Portokalidis
SDN Rootkits: Subverting Network Operating Systems of Software-Defined Networks SDN Rootkits：軟體定義的網絡顛覆網路作業系統	Christian Röpke; Thorsten Holz
Session 6: Android 安卓	
AppSpear: Bytecode Decrypting and DEX Reassembling for Packed Android Malware AppSpear：二進位碼解碼和 DEX 重組惡意 Android 套件程式	Wenbo Yang; Juanru Li; Bodong Li; Junliang Shu; Wenjun Hu; Yuanyuan Zhang; Dawu Gu
HelDroid: Dissecting and Detecting Android Ransomware HelDroid：剖析和檢測 Android 勒索軟件	Federico Maggi; Nicolò Andronio; Stefano Zanero
Continuous Authentication on Mobile Devices Using Power Consumption， Touch Gestures and Physical Movement of Users 持續驗證行動裝置上的使用功耗，觸摸手勢和使用者的身體運動	Rahul Murmuria; Angelos Stavrou; Daniel Barbara; Dan Fleck
Session 7: Privacy 隱私	
Privacy Risk Assessment on Online Photos 網路線上照片的隱私風險評估	Haitao Xu; Haining Wang; Angelos Stavrou
Privacy is Not an Option: Attacking the IPv6 Privacy Extension 隱私不是一選項：攻擊 IPv6 的隱私擴展	Johanna Ullrich; Edgar Weippl
Wednesday， November 4， 2015	
Session 8: Evaluating Solutions 評估解決方案	

Evaluation of Intrusion Detection Systems in Virtualized Environments Using Attack Injection 使用攻擊注入的入侵檢測系統在虛擬化環境評估	Aleksandar Milenkoski; Bryan D. Payne; Nuno Antunes; Marco Vieira; Samuel Kounev; Alberto Avritzer; Matthias Luft
Security Analysis of PHP Bytecode Protection Mechanisms PHP 二進位碼保護機制的安全性分析	Dario Weißer; Johannes Dahse; Thorsten Holz
Radmin: Early Detection of Application-Level Resource Exhaustion and Starvation Attacks Radmin：應用層資源耗竭和飢餓攻擊的早期檢測	Mohamed Elsabagh; Daniel Barbara; Daniel Fleck; Angelos Stavrou
Towards Automatic Inference of Kernel Object Semantics from Binary Code 從二進位碼朝自動推論的核心物件語義	Junyuan Zeng; Zhiqiang Lin
Session 9: Attack Detection II 攻擊檢測 II	
BotWatcher: Transparent and Generic Botnet Tracking BotWatcher：透明和通用殭屍網絡追踪	Thomas Barabosch; Adrian Dombeck; Khaled Yakdan; Elmar Gerhards-Padilla
Elite: Automatic Orchestration of Elastic Detection Services to Secure Cloud Hosting 精英作業：自動業務流程的彈性檢測服務，以達安全的雲端管理	Yangyi Chen; Vincent Bindschaedler; Xiaofeng Wang; Stefan Berger; Dimitrios Pendarakis
AmpPot: Monitoring and Defending Against Amplification DDoS Attacks AmpPot: 監視和防範 DDoS 攻擊的放大	Lukas Krämer; Johannes Krupp; Daisuke Makita; Tomomi Nishizoe; Takashi Koide; Katsunari Yoshioka; Christian Rossow

此 28 篇入選論文發表中，令人感興趣的是會議第二天下午「Session 7: Privacy 隱私」之網路線上照片的隱私風險評估(Privacy Risk Assessment on Online Photos)一文，這篇論文展示了在網路蒐集到的照片其有關中繼資料(metadata)的研究，據發表者調查那些原始儲存中繼資料機制，無論多久後，這些已上傳到網路上各種照片託管服務仍舊向公眾開放，這些唯一資訊(例如相機序號)可被與其他匿名的照片連結找出其拍攝者為誰。

大家都知道，這個管道是網路線上意外洩露隱私的一個重要且令人感興趣的超大資料庫。除了原始數據外洩，許多照片包括可供任何人查看大量的中繼資料，其所產生的個人隱私問題更是令人印象深刻。

這篇論文是涵蓋關於照片的中繼資料隱私外洩問題的幾個不同面向，要提供這個解決方案，可以藉由要求執行最可能有害隱私漏洞的深入剖析，就中繼資料(metadata)重新鑑定改善去除，以保障這些資訊不被有心人利用。

本次會議除發表上述 28 篇論文外，為免其他優秀論文有遺珠之憾，特於會議第 2 天 17:00-18:30 增闢 90 分鐘的海報發表(Poster Session)，共計有 25 篇研究海報獲選，分別張貼在會場走道供與會人員參閱，並舉辦作者現場發表，與會人員對有興趣的研究主題，可與作者面對面做零距離的請益與對談，過程相當熱絡與有趣，以下是海報發表的現場實況。

▲海報發表的現場實況

在 25 篇海報發表(Poster Session)中，有一篇日本早稻田大學 NTT 安全平台實驗室發表的「克隆或親戚？了解相似之安卓 Apps 的來源(Clone or Relatives? Understanding the Origins of Similar Andriod Apps)」為題的海報引起我的興趣，一般安卓 App 的開發者，不可諱言地運用類似 Clone 工具直接複製程式碼來使用，以降低開發成本，但這樣同時也

把一些惡意程式也複製過來，而引用者並不自知，反而無意間成為 App 惡意程式的散播者，造成重大的資訊安全議題，為評估 Clone 所造成的危害，該實驗室自行開發「APPraiser」架構，可辨別哪些 App 中是屬於有害的 Clone(克隆)，哪些是屬於無害的 Relatives(親戚)，經該實驗室「APPraiser」架構搜尋安卓官方或第三方 marketplace 超過 130 萬個相似型 Apps，發現安卓官方 marketplace 相似型 Apps 中無害的 Relatives 所佔的比例為 76%(相對安全)；但第三方 marketplace 中卻有高達 45%屬於有害的 Clone，且研究指出第三方 marketplace 中高達 80%的 Apps 是含有惡意程式，因此使用安卓第三方 marketplace 的 Apps 要提高警覺，以免成為惡意程式的受害者。

參、 心得及建議

此次會議的專題演講請到任職於 Google 的馬克希朋(Mark Seaborn)，以「難以補丁的問題：在 DRAM 排錘錯誤和快取時序側通道的可能發展(Hard-to-patch problems: Exploitability of the DRAM rowhammer bug and cache timing side channels)」為題，描述自 2010 年在講者任職的 Google Project Zero 團隊發現的錯誤問題，這個議題雖在資訊界未廣泛受到影響，但仍需持續關注其後續發展，畢竟現行 DDR3 的 DRAM 仍是主流產品，其暴露的風險有一定程度的機率存在。

近幾年來，由於積體電路製程的進步與行動化趨勢的發展，現今的電腦系統所使用的動態隨機存取記憶體(DRAM)，得以便宜的價格，享受大容量程式與資料暫存空間，行動產品以更小的體積容納更多的儲存空間，近期在 DRAM DDR3 上所發現的排錘錯誤(Rowhammer bug)，已被證明能夠輕易地透過網頁實現。

隨著半導體製程不斷地朝微縮發展，在相同的晶圓面積下可放置更多的電晶體線路，以提升效能，使細小的線路適用更低的電壓，耗電量也隨之降低，這是一個進步發展的趨勢，但也不一定是萬靈丹，譬如快閃記憶體(flash)就會受到影響，降低寫入次數。而現今各種運算裝置仰賴的DRAM，數年前也被找出因製程微縮發展，而出現的排錘(Rowhammer)硬體漏洞，近期則是在講者任職的谷歌 Project Zero 團隊指出此漏洞已可用這種重複行為來獲得對 x86-64 的 Linux 機器內的管理者帳號竊取授權。

講者最近的研究涉及兩個記憶體相關的問題：隨著“rowhammer”的錯誤發現，重複存取一個頁面的記憶體可能導致位元翻轉的另一頁，雖然大多數人認為這只是一個硬體可靠性的議題，但如前所述，發現它是可實際應證。由於軟體式沙箱(sandbox)的發展進步，攻擊者可能轉向開發比較深奧的問題，例如在硬體製程的漏洞，畢竟，軟體要補丁容易，用程式分派即可輕易完成，但硬體漏洞，除召回重換新品外，別無他法進行，研究中雖也指出目前有幾種方式能夠防堵，但對於消費者大眾來說還是有一定的困難度，使硬體補丁較軟體補丁來得困難與複雜。

以上是此次會議專題演講的重點心得，若政府機關對外服務的伺服器設備符合上述的風險存在，建議應妥善因應與評估，以避免遭到可能的危害。

最後，感謝本中心提供此次出席本國際會議的機會，除獲取資訊安全的寶貴知識外，更進一步與國際人士接觸，擴展視野，並藉由此次自行安排旅程，發現無論訂機票、入出國的通關、住宿及交通的安排，不如想像中的困難，皆可以自助的方式完成一趟國外之旅，應驗了國父所說知難行易的真理。