行政院及所屬各機關出國報告

（出國類別：開會）

出席「Black Hat Europe 2019」 出國報告

服務機關： 財政部財政資訊中心
姓名職稱： 林柏勳 助理程式設計師
派赴國家： 英國
出國期間： 108 年 11 月 30 日至 12 月 7 日
報告日期： 109 年 2 月 10 日

摘要

近年來資安意識普及，並隨著資通安全管理法公布，資安防護日漸受到我國政府重視，為掌握國際資安發展趨勢及熱門研究，爰安排此次國際會議。

Black Hat 是全球最受歡迎以及技術性的資訊安全系列活動之一，在過去 20 多年來 Black Hat 研討會每年提供資安專業人才分享他們的研究與發現，讓與會者獲取到目前世界最新資安研究、開發以及趨勢，並且常有一些重大資安漏洞在會議中被公布。

在資通訊技術不斷地蓬勃發展下，財政部財政資訊中心(以下簡稱本中心)為強化財政部整體資安防護能量，以提升民眾使用資訊服務之安全性，於 105 年底創立資安健檢及數位鑑識團隊(以下簡稱資安團隊)，提供財政部及所屬機關(構)資安技術服務，包含網站滲透測試、資安健診以及資安事件調查等，故本次研討會之行程著重於資安漏洞發表、資安事件反應以及新興資安研究分享。

目錄

壹、目的

網際網路隨著資通訊技術的發展，漸漸的隨時隨地伴隨在你我左右，加上物聯網以及 FinTech (金融科技) 等新興網路服務的興起，駭客與資安防護的角力越演越烈，所涵蓋的範圍也越來越廣泛，讓資安人員面臨的挑戰日漸增多。資安防護宛如提防刺客，敵暗我明總是防不勝防，然而市面上資安防護產品也絕無可能提供百分之百的防護，因此強化資安人員的職能勢在必行。

國際間的資安聯防在現今資訊戰的白熱化下逐漸受到重視，另外駭客集團(中國、北韓以及俄羅斯等)跨國性的犯罪時有所聞，並且越趨頻繁發生，因此我國在資安情資獲取與研究下，與世界接軌確有必要性，以面對不斷進化的攻擊手法、技術及挑戰。

為強化資安職能、掌握最新的國際資安趨勢及駭客面向之攻擊手法，選擇出席世界最具知名度以及技術性國際資安研討會之一的 Black Hat，Black Hat 近年固定於美國、亞洲及歐洲舉辦系列活動，基於時程的安排，便選擇了歐洲場次。

貳、過程

一、 會議簡介

此次 Black Hat Europe 在英國倫敦的 ExCel 國際會展中心舉辦，倫敦是英國最大的城市，也是全球最富裕、經濟最發達、商業最繁榮、生活水平最高的城市之一，在政治、經濟、文化、教育、科技、金融、商業、體育、傳媒、時尚等各方面影響著全世界。

Black Hat 與 DEF CON 皆為世界最具盛名的資安系列活動，資安專家、研究員、分析師等，若要發表研究或最新的發現，最難錄取的即是這兩個活動，例如：臺灣知名資安專家 Orange(蔡政達)，連續三年在 DEF CON 及 Black Hat USA 發表研究，其發表內容包含 SSL VPN 遠端程式碼執行漏洞等。

Black Hat 與 DEF CON 的創辦人都是 Jeff Moss ，在活動性質上卻不盡相同，DEF CON 最具知名度的就是搶旗賽(CTF)，在 DEF CON 駭客或資安專家間可以輕鬆的交流、切磋，並享受競賽等，而 Black Hat 是相對正式的研討會，不僅常有突破性的資安研究發表，甚至也另外提供訓練課程，參加者可以實作到最新的滲透測試技術或防禦技巧，從中獲取實際的資安技能。

另外 Black Hat 強調於研討會中所聽到的發表，與廠商及贊助無關，意即參加者不會花了 25 分鐘或 50 分鐘，結果只聽到資安廠商在台上推廣自家產品，另外每場發表的內容，是經過 Black Hat 審查委員會嚴格的審查，甚至可能提供發表者修改建議以澄清其陳述中存在的任何問題，讓與會者能更融入於發表中。

Black Hat 也設有展覽攤位，提供資安廠商、資安專家或是學生展示開發工具或研究成果。

二、 會議摘要

本次 Black Hat 將所有議程進行主題分類，例如惡意程式(Malware)、數位鑑識/資安事件反應(Data Forensics/Incident Response)、行動裝置(Mobile)以及各類型應用安全(Applied Sec)等，針對 Web 應用安全類型中我挑選了「新漏洞利用技術-Java 反序列化攻擊」進行介紹，其中講者發表了 Java 反序列化攻擊的最新漏洞利用技術，並且可加以利用其他攻擊路徑完成遠端命令執行。

而在資安事件反應及惡意程式上，我選擇「進階 VBA 巨集之攻擊與防禦」進行介紹，講者來自歐洲太空總署，發表在 VBA 巨集的攻防中最新的技術和工具。

最後在各類型應用安全中，我挑選倫敦生活中常見的非接觸式支付(或稱感應式支付)的漏洞發現進行介紹，講者分享他們研究如何繞過 30 英鎊的支付限制。

(一) 新漏洞利用技術-Java 反序列化攻擊

Java 反序列化(Deserialization)攻擊早在 2015 年被提出，後續甚至出現利用此漏洞而完成遠端命令執行(Remote Command Execution, RCE)的攻擊，進而成為 Java 歷史中最嚴重且關鍵的安全問題之一。

圖 1、FoxGlove Security 團隊於 2015 發表反序列化攻擊

(資料來源: Black Hat Europe)

序列化是指將 Java 物件轉換成位元組串流(Byte Stream)，反序列化則是相反，將位元組串流轉換回 Java 物件，常用在調用遠端的方法(Method)或者將物件傳輸或儲存的時候。

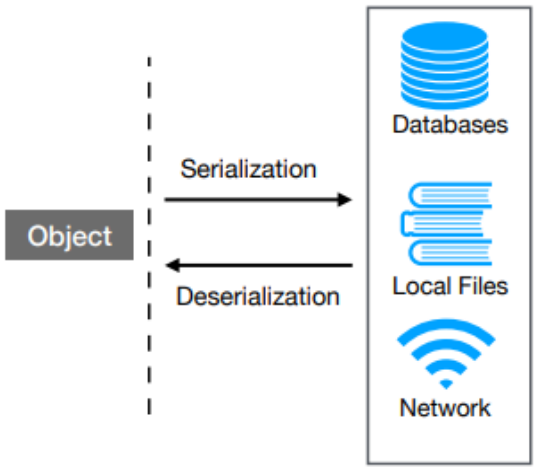

圖 2、序列與反序列化示意圖

(資料來源: Black Hat Europe)

現今開發人員常會通過黑名單(Black list)、過濾器(Filter)以及利用 Java agent(Runtime Application Self-protection, RASP)的方式防範反序列化攻擊，造成攻擊者非常難以找到可以利用的 RCE 漏洞。

然而在這次的 Black Hat Europe 中，講者發表從其他面向發現的防護缺陷，例如利用 JDBC(Java DataBase Connetivity)有弱點的參數(queryInterceptors、autoDeserialize)一步一步進行攻擊。

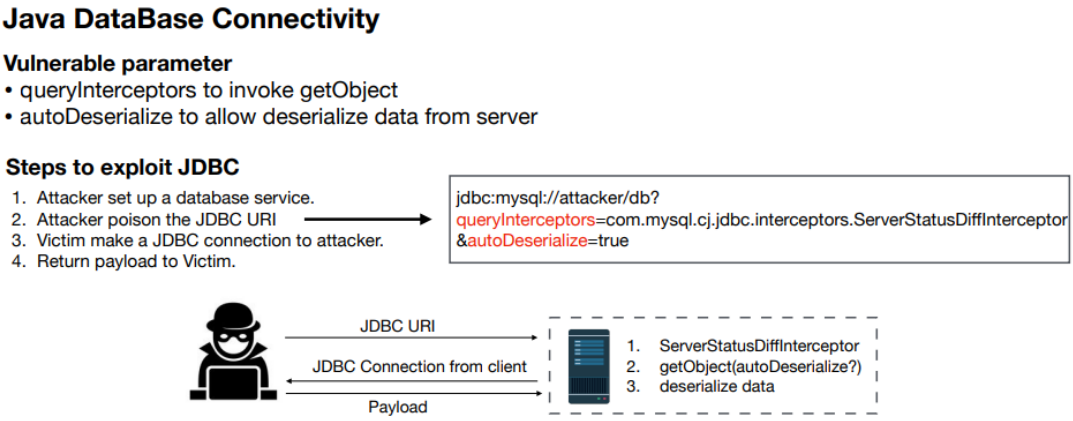

圖 3、JDBC 攻擊手法

(資料來源: Black Hat Europe)

或者利用 NTLM(NT LAN Manager)已知的 CVE 漏洞進行串接，而導致 RCE 的攻擊產生。

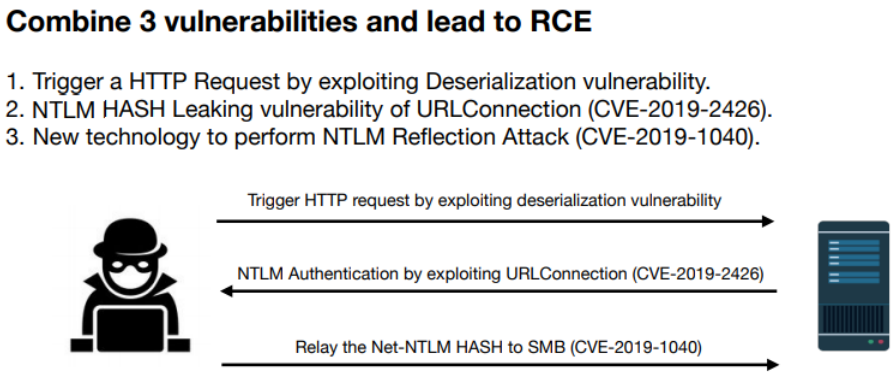

圖 4、利用反序列化以及 NTLM 漏洞完成 RCE 之流程

(資料來源: Black Hat Europe)

講者最後也提供了一些建議給在場的與會者，如果是開發及維運人員，講者建議:

-不要反序列化不信任的資料。

-不要傳送 HTTP 請求到不信任的伺服器。

-不要藉由 JDBC 連接到不信任的資料庫。

-加密序列化後的位元組碼(Bytecode)。

而如果是資安研究人員則建議:

-使用黑名單防範反序列化攻擊時，請仔細審核資安政策，或者嘗試使用白名單的方式降低風險。

-利用其他面向模糊化應用系統。

-靜態分析可以簡單地找到 JDBC 的弱點。

(二)　進階 VBA 巨集之攻擊與防禦

1. VBA 巨集介紹與基礎攻擊

VBA 巨集目前仍常見應用於惡意程式中，通常都被拿來做 Downloader 或 Dropper 但其實 VBA 巨集能做到所有惡意行為，比如執行命令(command)、鍵盤側錄以及 Shellcode 的注入。

(從 1997 年以來，巨集在 Microsoft Office 中就可以很輕易的被執行)

圖 5、VBA 巨集能做到的事

(資料來源: Black Hat Europe)

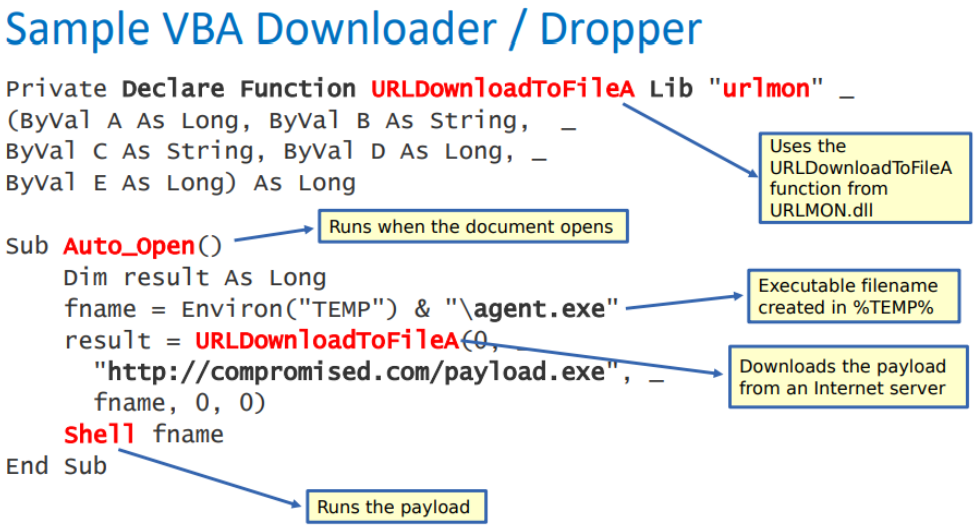

圖 6、VBA 巨集 Downloader/Dropper 之示例

(資料來源: Black Hat Europe)

如果對巨集這個詞感到陌生，但可能對黃色框框的安全性警告不陌生，很多使用者常不帶警覺性，甚至是習慣性的直接點”啟用內容”，當開始啟用後，會發生什麼事，可能是難以想像的。

圖 7、Microsoft Office 安全性警告

那為什麼從 1997 直到現代，VBA 巨集仍然被廣泛用於傳遞惡意程式？因為 VBA 巨集在有防毒、IDS 及 EDR 等資安防護下，仍可順利攻擊到終端使用者。

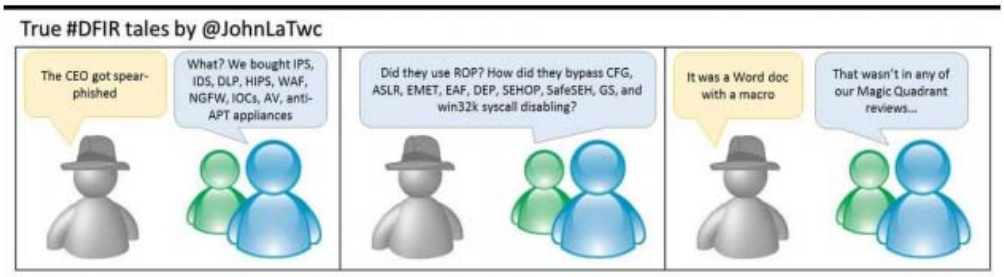

圖 8、VBA 巨集仍廣泛使用之示例

(資料來源: Black Hat Europe)

2. VBA 巨集防禦(分析)

講者則提供他開發的分析工具-olevba，工具支援常見的 Microsoft Office 的檔案格式(例如:doc 、xls 及 ppt 等)或者 VBA 的原始碼。

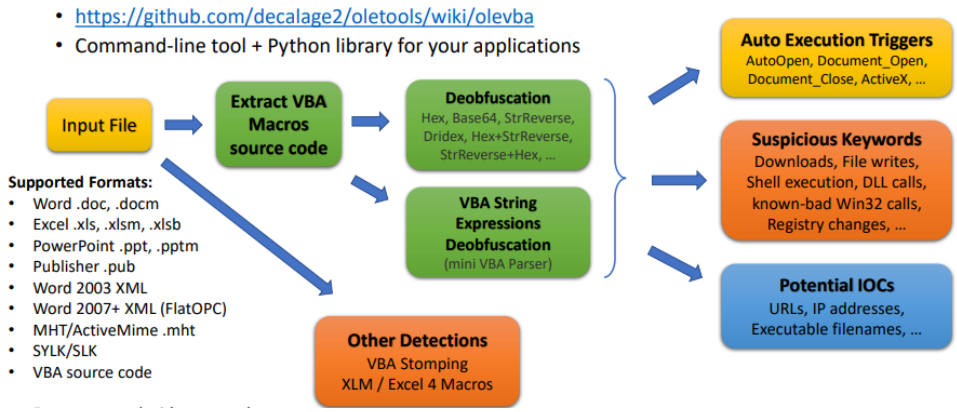

圖 9、VBA 巨集分析工具-olevba 運作流程

(資料來源: Black Hat Europe)

不過與現行的資安檢測相同，靜態分析在有些時候是不夠全面的，部分惡意程式可能會成為漏網之魚，因此講者也介紹了另一個分析工具-ViperMonkey ，ViperMonkey 是由自定義的 VBA 解析器與模擬器所組成。

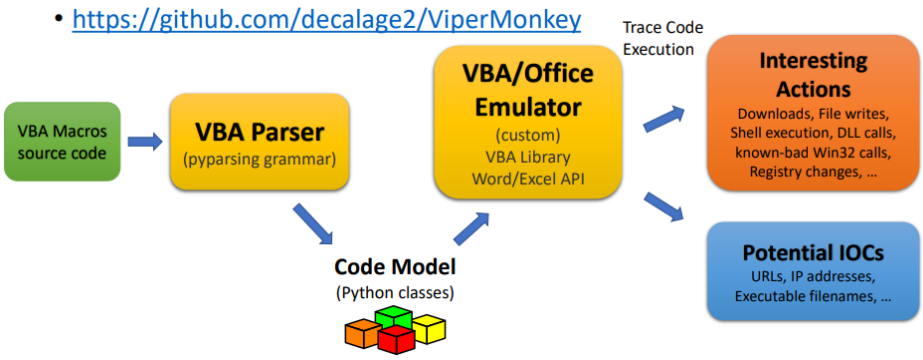

圖 10、VBA 巨集分析工具-ViperMonkey 運作流程

(資料來源: Black Hat Europe)

3. VBA 巨集攻擊進階技術

VBA Stomping

VBA 巨集是以 VBA 原始碼以及 P-code 儲存在文件檔案當中，P-code 就是已經預先解析好的位元組碼(Bytecode)，並且已經是可以直接執行的狀態。

所謂的 P-code 即是假設當一個文件檔案被開啟、並且執行巨集時，真正執行的巨集碼是被預先解析好的P-code 而不是 VBA 的原始碼。

(不過前提是 Microsoft Office 的版本有對應上)

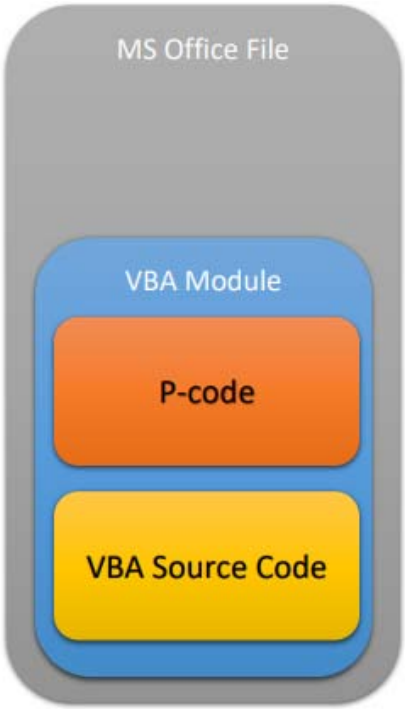

圖 11、VBA 巨集儲存於文件檔案中之示例圖

(資料來源: Black Hat Europe)

然而以往大多數的分析工具或者防範惡意程式軟體，通常只檢查 VBA 原始碼。

因此當攻擊者將 VBA 原始碼修改成無害的，而真正執行的 VBA 巨集是惡意的 P-code 時，是不會受到偵測並且能正常執行運作的。

因此 VBA Stomping 等新型的混淆技術，可以讓攻擊者將惡意指令傳遞給終端使用者並執行而不被發現，甚至出現自動化的混淆與即時匹配 Microsoft Office 版本的工具，讓 VBA 巨集的攻擊更邁進一大步，成為資安人員新的挑戰。

4.VBA 巨集防禦(偵測及防範)

幸運的是，分析和檢測工具也在不斷發展以解決所有高級攻擊技術。講者也解說，他在 olevba 是如何面對 VBA Stomping 此新型攻擊技術，首先 olevba 會將 P-code 反組譯(Disassemble)，並將所有相關關鍵字析取出來，例如函式名稱、呼叫的函式以及變數名稱等，再與 VBA 原始碼比對，如果少了任何相關的關鍵字，則代表 VBA 巨集可能是被 Stomping 過的(惡意的 VBA 巨集)。

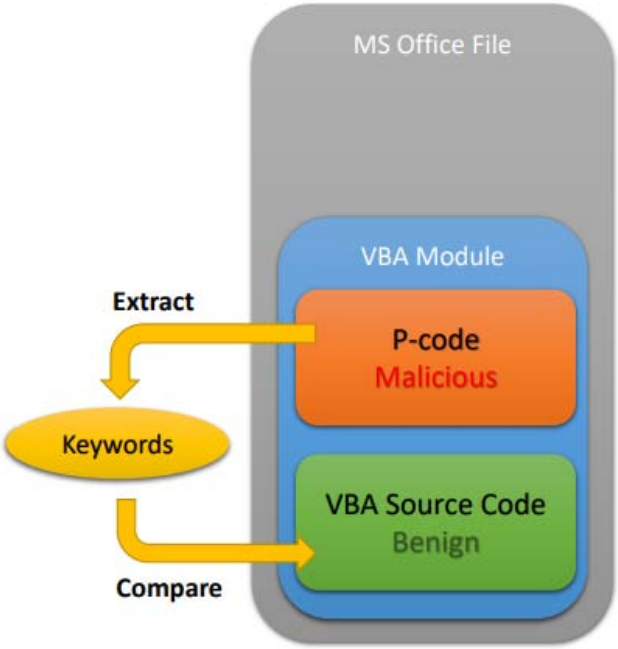

圖 12、olevba 如何偵測 VBA Stomping 之原理示例圖

(資料來源: Black Hat Europe)

講者也提到，防毒軟體是不足以偵測或防範惡意巨集，事實上多數的惡意巨集是存活了數個月而沒被偵測到。因此，講者介紹了惡意巨集偵測工具:

-MacroRaptor

-Mraptor_milter / MacroMilter

-Mraptor GUI

-Olefy

-Malicious Macro Bot

必且講者也提到：

點擊”啟用內容”按鈕的危險程度，等同於開啟一個來路不明的 EXE 執行檔。

(三) 第一次接觸-非接觸式支付中(Contactless Payments)的漏洞

非接觸式（NFC）支付於 2007 年推出，已經被廣泛使用了十年。非接觸式支付佔全球交易的 40%以上，正在迅速取代現金和晶片卡。

講者說明 NFC 與晶片卡的不同在於，NFC 包含了傳統模式(磁條)，而晶片則否，不過 NFC 跟晶片使用相同的金鑰與相同的記憶體區塊。

非接觸式交易為了避免被大量盜刷，在英國因此有了 30 英鎊的交易金額限制，而講者講解是如何破解這個限制，甚至未來可能可以定位目標受害者，完成遠端的盜刷。

非接觸式支付是使用 EMV 協定進行交易，而講者進行 EMV 協定的風險分析，他認為卡片本身的認證、交易的授權以及持卡人的驗證(CVM)都是 EMV 協定中的風險。

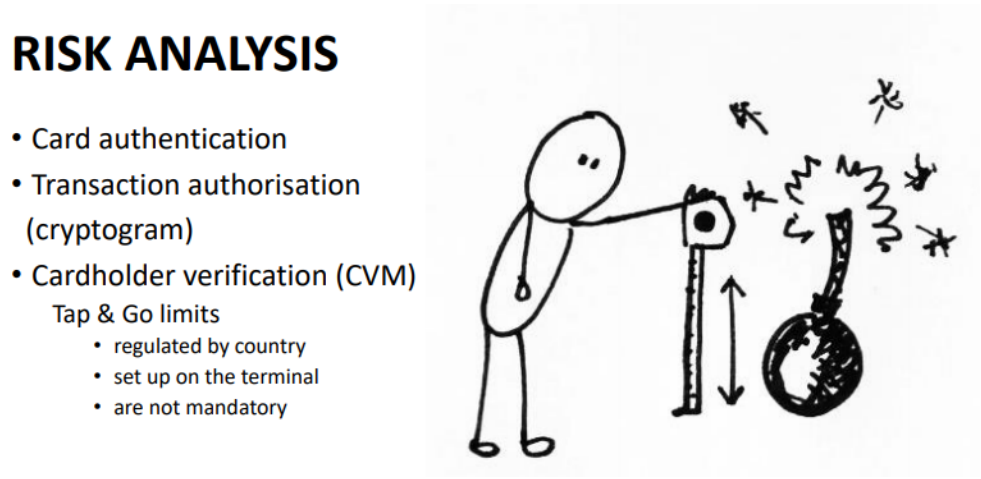

圖 13、非接觸式交易，EMV 協定風險分析

(資料來源: Black Hat Europe)

他也說明VISA卡在這種協定下是有漏洞的(可以繞過30英鎊的限制)，因為VISA少了一部分的驗證(與MasterCard相比)，在講者的實驗下，所有的VISA卡的加密程序以及一部分的VISA卡(包含英國、歐洲、美國與亞洲)是受到影響的，實作上，講者利用樹莓派成功攔截卡片與機器間的交易完成中間人攻擊(MITM)。

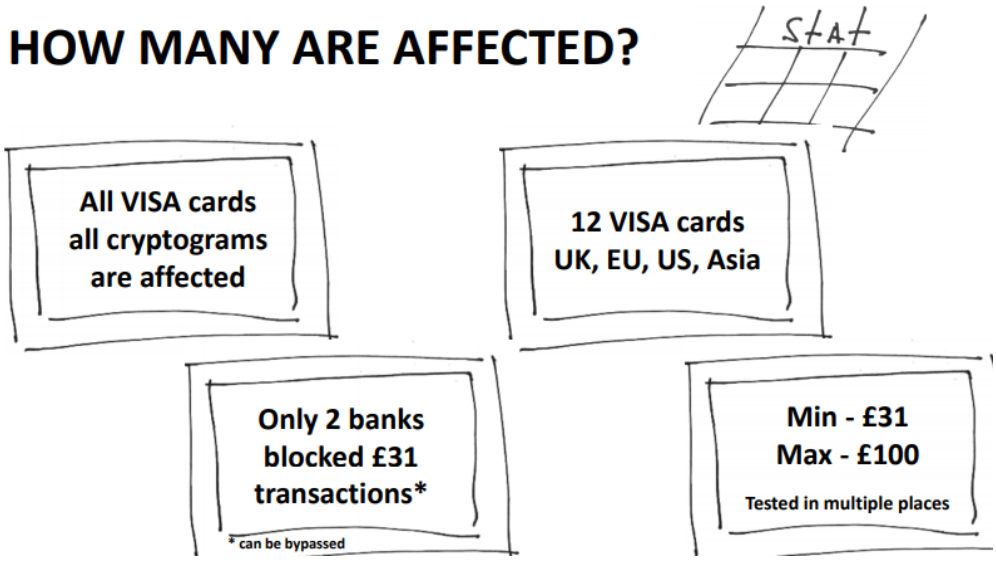

圖 14、非接觸式交易，EMV 協定漏洞影響

(資料來源: Black Hat Europe)

GPay(行動支付-Android Pay + Google Wallet)在手機上交易時，身分認證的要求始終是開啟的，講者實驗將協定中的身分認證參數從 true 改成 false，在不解鎖手機的情況下，就輕易繞過限制，並且也提到美國也是受到影響的範圍。

不過這個限制在我國使用 VISA 時是不存在的，意即我國在使用感應式卡片進行非接觸式交易時，這個攻擊手法並不適用。

參、心得及建議事項

十年前網頁系統開發常為了速度而捨棄安全，現今一個系統上線要經過大大小小的資安檢測（黑白箱測試），足見資安議題慢慢得到重視，十分感謝中心長官重視資安，並且給予我這個機會，參與這難得的國際資安盛會，實在是深刻難忘並受益匪淺。

我從 Java 反序列化的攻擊中，更加了解了 SSDLC（安全應用系統開發週期）的重要性，尤其是當講者提到靜態分析可以輕易找到部分隱藏的弱點時，讓人深刻認知到，在開發時源碼檢測或威脅預測模組的實用性，也不免感到慶幸本中心的系統在進改館皆會執行源碼檢測，否則反序列化攻擊導致 RCE 的影響是足以破壞整個機關提供的服務，甚至造成資料外洩。除了源碼檢測以外，未來適時提供開發人員最新資安議題，從開發的根本避免漏洞發生，或許也是個進步的方向，但資訊爆炸時代，攻擊手法變化莫測，追逐國際資安情資的成本也應為本中心考量範疇。

中心資安團隊近期也針對資安事件調查進行訓練，在這段時間我也調查及分析了許多有趣的案例，因此當看完世界級的資安專家介紹進階 VBA 巨集攻擊與防禦時，讓我覺得上了一堂價值連城的課程，使自己未來能應用（攻防）的方式與知識增加了許多。而 VBA 巨集最常出現在社交工程攻擊手法中，攻擊者只要偽裝身分並夾帶含惡意巨集的附件，一般使用者是非常容易上當。社交工程演練一直以來都是中心最重視的資安防護一環，以期將資安事件發生的人為因子降到最低，並搭配 GCB（Government Configuration Baseline）的政策，避免 VBA 巨集攻擊影響。然而，雖從資通訊的管理讓人為因子造成資安事件的風險降低了，但從根本來說，內部員工似乎也因為過度仰賴管控措施致使資安意識成長有限（儘管有教育訓練）。舉例來說，曾有業務單位反過來指控資安單位，「不是說信件有什麼就可以點嗎？」，事實上教育訓練從不可能宣導有任何東西是絕對安全的，而是教育員工自我警惕，**提高警覺性、提升資訊素養與認知**，這才是作為杜絕人為因子造成資安事件的根本辦法，而不是用來作為點擊惡意郵件的藉口。

在倫敦，幾乎所有的消費都可以倚賴信用卡支付，在大眾運輸交通上甚至也在推動「Contactless（感應式支付）」支付方式，可以使用支援感應功能的卡片或者行動支付（例如 Apple Pay），將信用卡或手機靠近機器感應支付即可，讓我覺得科技進步帶來的方便，進而昇華了這段時間的體驗，所以我對探討 Contactless Payment 安全性的研究議題非常感興趣，也了解到其實方便的同時，可能也存在著安全問題。不過因為不是平常接觸的議題，當下在聽講者說明時其實沒有完全理解，為何 30 英鎊的限制被繞過是一個嚴重的漏洞，後續在了解英國於感應式支付的政策與當地的人文環境後，才理解到這個限制是為了避免被大量盜刷且為英國政府近年來標榜的政績，也明白這個漏洞在臺灣目前是不適用的。

以我國來說，資安法正式實行，彷彿為資訊安全的環境投入了一股活水，不過「資安」的存在幾乎是依附著「資訊」，而我國政府對資訊資源的投入仍有成長空間，因為資訊經費的不足造就的僅是更多的資安防禦破口。我曾看過一份資安趨勢報告，報告中探討有關全球進階持續性威脅（Advanced Persistent Threat, APT）以及惡意活動狀況，全球平均發現這些惡意活動的時間為 78 天，然而整個亞太地區卻是平均需要 204 天才會發現，讓我不禁思考這之間差距的原因為何，是亞太地區的技術落後？亦或者是亞太地區仍相對的不夠重視資訊與資安發展？這也許是往後可以繼續探討並研究的議題。

在這短短的時間中，我在倫敦學到了許多專業知識，也確實體會到了英國與臺灣的差異，我相信這段期間所增廣的見聞對未來一定有所助益，不管是於工作上還是於人生中。