出國報告(出國類別：其他(國際會議))

「國際資訊安全會議(DEFCON 26)」出國報告

服務機關：　行政院資通安全處
姓名職稱：　周智禾科長、余柏賢設計師

派赴國家：　美國 (拉斯維加斯)
出國期間：　107 年 8 月 9 日　　至 107 年 8 月 12 日
報告日期：　107 年 11 月 2 日

摘要

本次參加第 26 屆的 DEF CON 駭客年會(以下簡稱 DEF CON 第 26 次會議)，除了參加各分項研討會了解目前最被駭客廣泛使用的入侵與防禦技巧外，也藉由研討會瞭解國際上最新的攻擊趨勢與技術、現階段資安發展方向及未公開弱點的入侵攻擊手法等等，並在各家廠商的展區與各國資安人員進行交流，以了解當前資安產業趨勢，作為未來對於國內攻防演練、資安稽核等相關業務之參考。

DEF CON 第 26 次會議於本(107)年 8 月 9 日至 8 月 12 日循例於美國拉斯維加斯舉行，本次會議較偏向資安社群的研討會，討論的內容除了傳統的學術論文外，尚包含了 IoT、CAR、ICS、AI 人工智慧、無線網路等，其涉及領域非常廣，除了現場展示與分享資安技術的平台，DEFCON 還會舉辦許多活動，例如: 社交工程競賽、開鎖比賽以及針對 BADGE 的破解與製作，本年更針對小朋友舉辦競賽(DefCon Voting Machine Hacking Village)，主辦單位向參賽者提供了美國 6 個州的選舉網站「複製品」，讓他們嘗試利用駭客技術，入侵不同選舉網站的複製版本並操縱投票結果，其中最讓人印象深刻是一名 11 歲的參賽者成功在 10 分鐘內，入侵佛羅里達州模擬選舉網站，把某位候選人的票數增加兩倍，另，超過 30 名兒童也在 30 分鐘內成功入侵其他不同的模擬選舉網站。

最後，則是 DEF CON 第 26 次會議的核心競賽項目「Capture the Flag」(CTF)，本次賽制不同以往，並非以單純的網路攻防為主，而是以混合的方式，將類似搶灘遊戲的「山丘之王」(King of the hill)的比賽方法加上網路攻防賽制，以占領伺服器服務的時間多寡來決定分數高低，參賽隊伍必須保護本身伺服器不被攻陷，同時研究伺服器漏洞，寫成攻擊程式(Exploit)攻擊其他參賽隊伍，藉此取得其他隊伍伺服器中的金鑰(Token)或旗幟(Flag)後，將攻擊成功的 Token 或 Flag 提交計分。

目次

壹、目的

本次主要任務為參加今年度國際間最受關注且為期 4 天(8 月 9 日至 8 月 12 日)的 DEF CON 第 26 次會議，在會議中觀摩及學習來自世界各國的資安專家、學界代表及駭客們所分享的各種漏洞攻擊手法、資安技術及各種不同領域的新興議題與挑戰，其中包含了工控與智慧電表安全、車輛入侵與控制、IoT 與嵌入式系統安全、智慧手機安全、數位鑑識、惡意程式逆向分析及人工智慧與資安領域的結合應用等。

本次參加 DEF CON 第 26 次會議的目的包括：

1.掌握最新的資安動態、產業脈動、理論型的攻擊手法及偵測分析技術，並瞭解於 DEF CON 第 26 次會議擺攤的各家資安廠商、個人工作室所提供的服務及技術亮點，以此強化本身資安知識並掌握未來資安趨勢。

2.掌握時下各領域的資安專家研究成果，瞭解軟硬體安全，並進行資安技術交流。

3.瞭解世界各國資安專家、學者及駭客們的研究成果，如入侵特定目標時透過某些工具及技術可更迅速達到入侵的目的並可更有效的隱藏自己，又或是透過現有工具搭配達到反偵查的效果。

貳、過程

DEF CON 第 26 次會議於本年 8 月 9 日至 8 月 12 日在美國拉斯維加斯的 Caesars Palace 及 Flamingo Las Vegas 飯店舉行，其中，大部份的 track 及參與者都在 Caesars Palace 中，僅有部份特別議題在 Flamingo Las Vegas 進行。

一、議程

本次行程主要是由熱愛技術的各駭客社群所舉辦的研討會，每日同時間點會有 4 個不同的 track 分別在不同廳進行，包括「DEF CON 101」、「Track 1」、「Track 2」及「Track 3」，相關議程如下。

1.DEF CON 第 26 次會議-8 月 9 日議程

圖 1　DEF CON 第 26 次會議議程(一)

2.DEF CON 第 26 次會議-8 月 10 日議程

-FRIDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	Syntfuzz: Building a Grammar Based Re-targetable Test Generation Framework Joe Rozner	Badge/DT Welcome	De-anonymizing Programmers from Source Code and Binaries Rachel Greenstadt & Dr. Aylin Caliskan	Securing our Nation's Election Infrastructure Jeanette Manfra
10:30				Please do not Duplicate: Attacking the Knox Box and other keyed alike systems m010ch_
11:00	An Attacker Looks at Docker: Approaching Multi-Container Applications Wesley McGrew	NSA Talks Cybersecurity Rob Joyce	One-liners to Rule Them All Egypt	Lora Smart Water Meter Security Analysis Yingtao Zeng
12:00	It's Assembler, Jim, but not as we know it: (ab) using binaries from embedded devices for fun and profit Morgan "Indrora" Gangwere	Vulnerable Out of the Box: An Evaluation of Android Carrier Devices Ryan Johnson	Breaking Paser Logic: Take Your Path Normalization Off and Pop 0days Out! Orange Tsai	Who Controls the Controllers - Hacking Crestron IoT Automation Systems Ricky "HeadlessZeke" Lawshae
13:00	Dissecting the Teddy Ruxpin: Reverse Engineering the Smart Bear Zenofex	Compromising online accounts by cracking voicemail systems Martin Vigo	Finding Xori: Malware Analysis Triage with Automated Disassembly Amanda Rousseau & Rich Seymour	One-Click to OWA William Martin
13:30	You can run, but you can't hide. Reverse engineering using X-Ray. George Tarnovsky	Dragnet - Your Social Engineering Sidekick Truman Kain	Attacking the Brain: Customize Evil Protocol to Pwn an SDN Controller Feng Xiao	Fasten your seatbelts: We are escaping iOS 11 sandbox! Min Zheng
14:00	UEFI exploitation for the masses Mickey Shkatov	GOD MODE UNLOCKED - hardware backdoors in x86 CPUs Christopher Domas	4G - Who is paying your cellular phone bill? Dr. Silke Holtmanns & Isha Singh	Revolting Radios Michael Ossmann & Dominic Spill
15:00	Weaponizing Unicode: Homographs Beyond IDNs The Tarquin	Bypassing Port-Security In 2018: Defeating MacSEC and 802.1x-2010 Gabriel Ryan	Playback: a TLS 1.3 story Alfonso Garcia Alguacil & Alejo Murillo	Privacy infrastructure, challenges and opportunities yawnbox
16:00	Automated Discovery of Deserialization Gadget Chains Ian Haken	Your Peripheral Has Planted Malware - An Exploit of NXP SOCs Vulnerability Yuwei Zheng	Practical & Improved Wifi MitM with Mana Singe	Your Voice is My Passport _delta_zero
17:00	Your Bank's Digital Side Door Steven Dannaman	I'll See Your Missile and Raise You A MIRV: An overview of the Genesis Scripting Engine Alex Levinson	Panel - The L0pht Testimony, 20 Years Later (and Other Things You Were Afraid to Ask)	Reverse Engineering, hacking documentary series Michael Lee Nirenberg

圖 2　DEF CON 第 26 次會議議程(二)

3.DEF CON 第 26 次會議-8 月 11 日議程

圖 3　DEF CON 第 26 次會議議程(三)

4.DEF CON 第 26 次會議-8 月 12 日議程

-SUNDAY-

	DEF CON 101	Track 1	Track 2	Track 3
10:00	The Mouse is Mightier than the Sword Patrick Wardle	Rock appround the clock: Tracking malware developers by Android "AAPT" timezone disclosure bug. Shelia A. Berta & Sergio De Los Santos	Defending the 2018 Midterm Elections from Foreign Adversaries Joshua M Franklin	For the Love of Money: Finding and exploiting vulnerabilities in mobile point of sales systems Leigh-Anne Galloway
11:00	Searching for the Light: Adventures with OpticSpy Joe Grand (Kingpin)	Breaking Extreme Networks WingOS: How to own millions of devices running on Aircrafts, Government, Smart cities and more. Josep Pi Rodriguez	Politics and the Surveillance State. The story of a young politician's successful efforts to fight surveillance and pass the nation's strongest privacy bills. Daniel Zolnikov	Demystifying MS17-010: Reverse Engineering the ETERNAL Exploits zerosum0x0
12:00	Breaking Smart Speakers: We are Listening to You. Wu HuiYu	Last mile authentication problem: Exploiting the missing link in end-to-end secure communication Thanh Bui	Attacking the macOS Kernel Graphics Driver Yu Wang	Designing and Applying Extensible RF Fuzzing Tools to Expose PHY Layer Vulnerabilities Matt Knight
13:00	Trouble in the tubes: How internet routing security breaks down and how you can do it at home Lane Broadbent	Man-In-The-Disk Slava Makkaveev	Micro-Renovator: Bringing Processor Firmware up to Code Matt King	barcOwned - Popping shells with your cereal box Michael West
13:30		Asura: A huge PCAP file analyzer for anomaly packets detection using massive multithreading Ruo Ando	Lost and Found Certificates: dealing with residual certificates for pre-owned domains Ian Foster	Edge Side Include Injection: Abusing Caching Servers into SSRF and Transparent Session Hijacking idiomarcil
14:00	Betrayed by the keyboard: How what you type can give you away Matt Wixey	Your Watch Can Watch You! Gear Up for the Broken Privilege Pitfalls in the Samsung Gear Smartwatch Dongsung Kim	Hacking BLE Bicycle Locks for Fun and a Small Profit Vincent Tan Kwang Yue	One bite and all your dreams will come true: Analyzing and Attacking Apple Kernel Drivers Xiaolong Bai & Min Zheng
15:00	Closed	Panel DCGroups	What the Fax!? Yaniv Balmas	Fuzzing Malware For Fun & Profit. Applying Coverage-guided Fuzzing to Find and Exploit Bugs in Modern Malware Maksim Shudrak
16:30	Closed	Closing Ceremonies	Closed	Closed
17:00				

圖 4　DEF CON 第 26 次會議議程(四)

二、重點與發現

(一)What the FAX

此議程講解傳真機可能遇到的安全問題，傳真機雖然在現在的資訊社會中已經很少人在用了，但對很多政府機關，大型企業仍然保留傳真機，由於其採用的通訊協定已經很久沒有更新，所以可能產生相關的資安問題，講者 Yaniv Balmas 與 Eyal Itkin 為 Checkpoint 的資安研究員。

(1)fax 的歷史與現狀

講者主要先說明 FAX 的歷史，從 1846 年被發明以來，經歷了一百多年的時間，一直到現在慢慢的被電子郵件所取代，感覺上似乎已經不是那重要了，但為什麼講者對 FAX 有深入研究的想法，主要原因為他們發現利用 google 搜尋時，有近三億筆的資料，在目前資訊的架構中，很多都已經使用複合式的設備來取代傳統印表機，複合式的設備可能是有接網路的多功能事物機，如果可以使用傳統的電話線路，進行攻擊，有可能可以躲避所有現有的防禦機制，詳見圖 5 與圖 6。

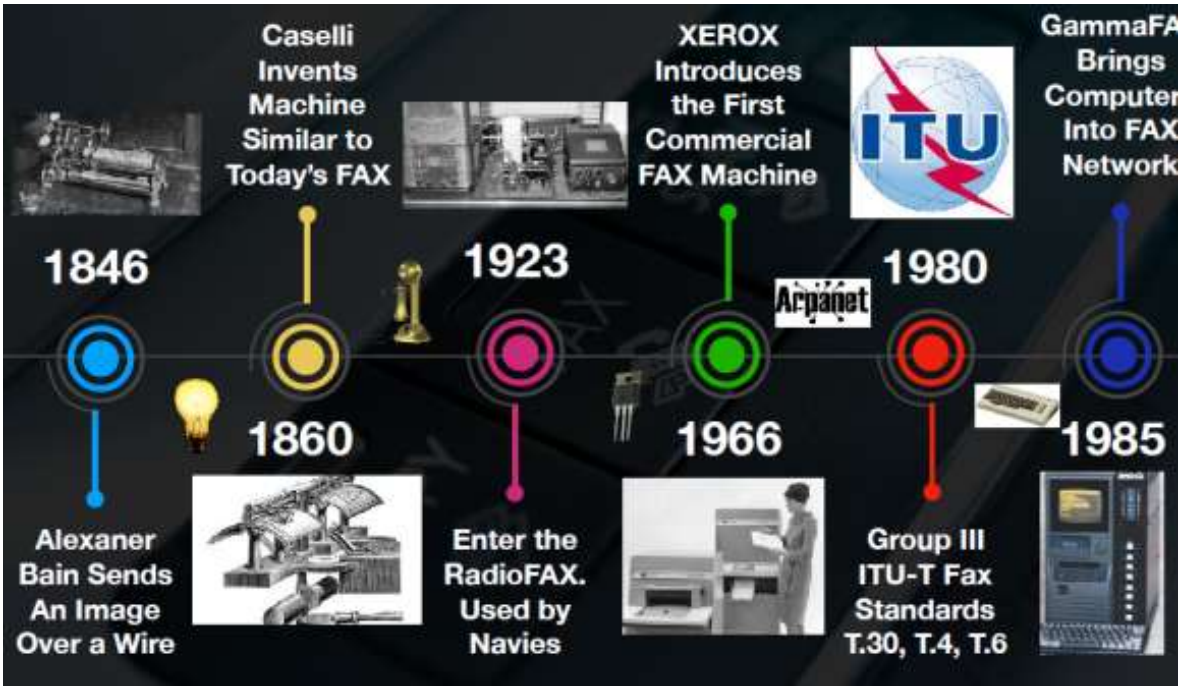

圖 5　fax 的歷史

圖 6　使用現狀

(2)攻擊的流程

一開始先挑選標的，由於 HP 的多功能事務機的市占率較高，所以選定以 HP 的設備為標的。講者一開始設法取得設備的韌體，進行靜態逆向分析與 Jtag 動態的分析，但無法發現可疑之處，所以他們參考了 CVE2017-9765 緩衝區溢位的弱點，利用 ITU T.81(JEPG)傳檔不會加密的特定，選定傳輸 JEPG 檔案，來嘗試攻擊，後來發現在傳真機的圖檔解析器在解析圖檔時，會出現溢位的狀況，所以他們製作了特定的檔案，傳輸給攻擊標的，即可接管該設備，並利用該設備串接的網路入侵到其他電腦，主機詳見圖 7。

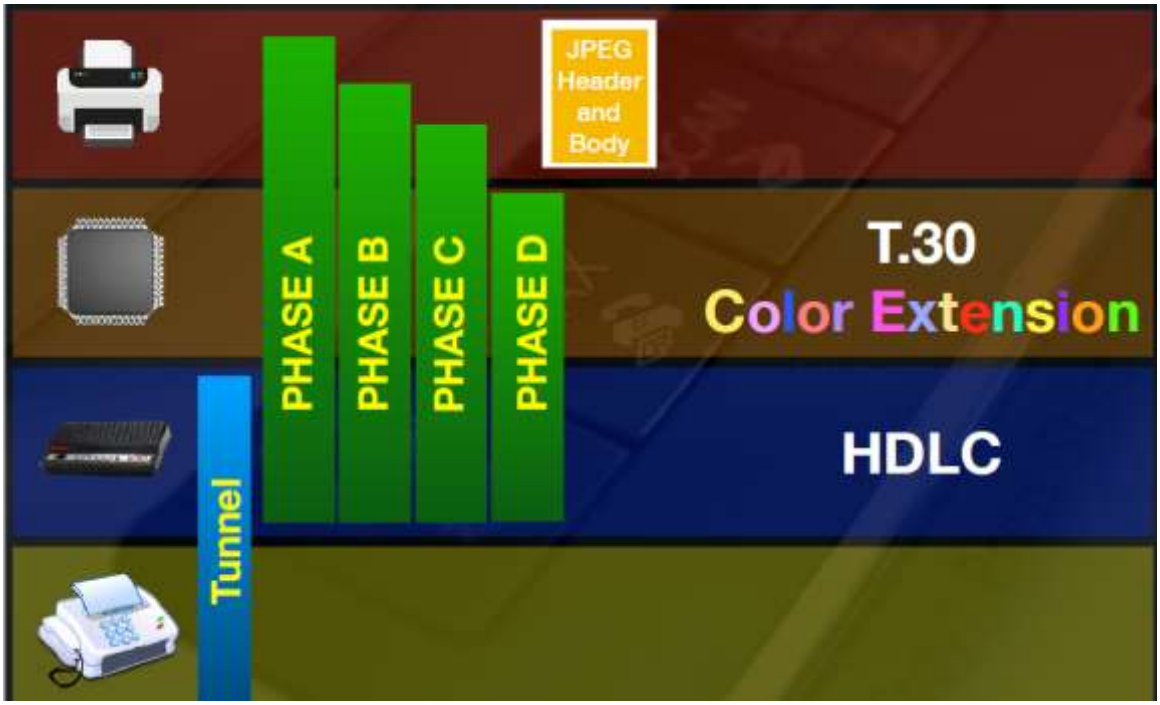

圖 7　傳送特定的 jpg 檔案達成攻擊目的

(二)De-anonymising Programmers from Source Code and Binaries

此議程為利用模糊理論與機器學習的方式，自動化分析程式碼的結構及撰寫的方式，並利用此方式與資料庫中的程式做比較，可以推測出此程式碼是由哪個程式員所寫出來的。

1.流程設計

若要進行機器學習，可先找出曾撰寫大量程式碼的作者，例如本作者從 github 等程式碼代管服務商理面找出 1600 位使用 C/C++語言的作者，並利用模糊分析和抽象語法樹演算碼(AST)將其所撰寫的程式原始碼進行分群分類，如圖 8 所示。

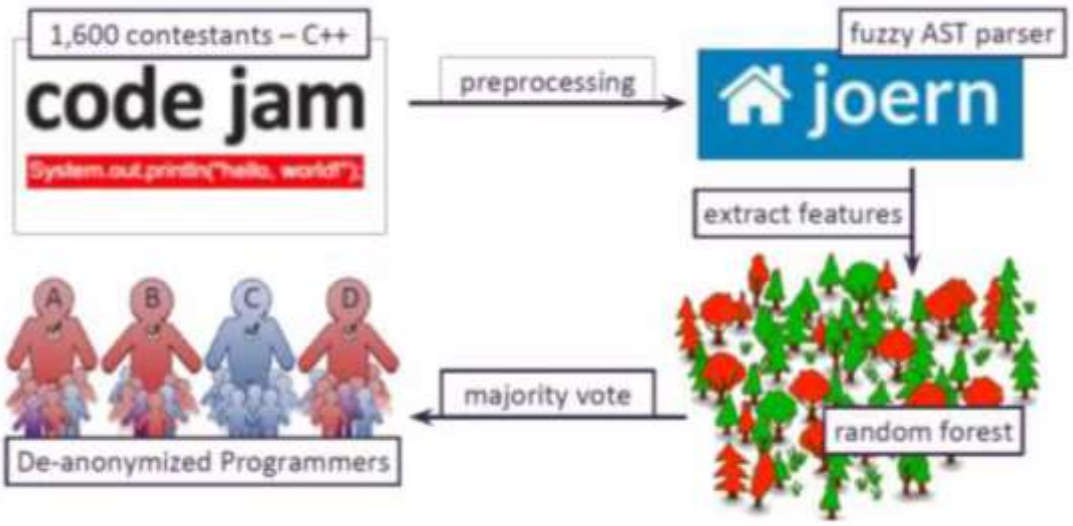

圖 8　利用 AST 演算法將程式碼進行分群分類

其中主要概念是採用語意分析，由於個別程式員在撰寫程式時，所採用的語法、架構、順序等都會有所差異，這和辨識人類自然語言的方式有點像，會有主詞、動詞及受詞等區別，因此作者利用如圖 9 的方式將程式進行拆解與分析。

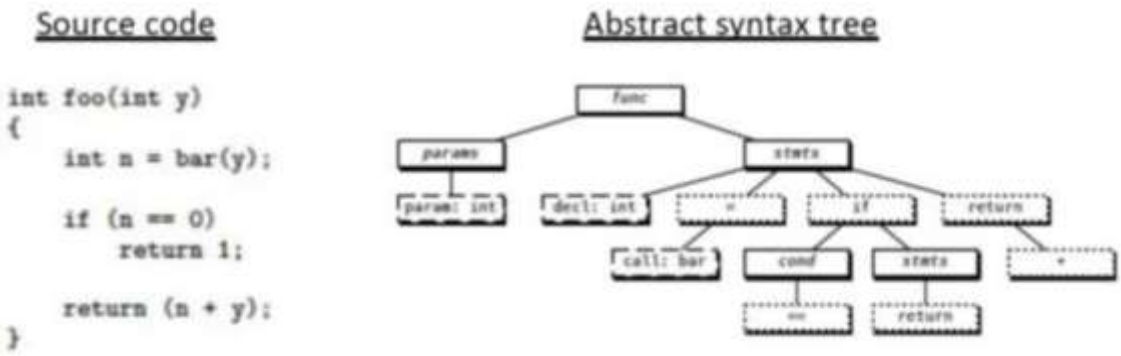

圖 9　利用語意分析的方式將程式拆解

2.程式碼混淆

現在由於大家越來越有資安的概念，深怕駭客對自己的程式碼進行原始碼分析後，找出相關的漏洞攻擊，因此許多人在撰寫程式的時候都會將完成的程式碼進行混淆，使得駭客在分析的時候可能要花上十倍的時間才能夠完成相同的事情。

但這就造就了另一個問題，如果程式碼被混淆過，我們仍有辦法判斷它是屬於相同的程式員所撰寫的嗎？其實答案是有機會的，但判斷的正確率會大幅降低，講者舉了一個例子，某個作者的程式碼正常情形時判斷正確的機率為 96%，但若是加上了混淆手法，判斷正確的機率則會降到 67%，但依然比其它現有的演算法準確度高上一截，如圖 10 所示。

圖 10　當程式碼被混淆的時候分析率會下降

3.無原始碼的程式分析

最常見的狀況是，當我們發現了一隻惡意程式，在沒有原始碼的前提下，是否有辦法進行深入的分析呢？講者表示當然是可以的，程式法分群分類如果僅是針對未編譯的程式碼，那早就有一堆人在做研究了，也有相當不錯的研究成果，但針對編譯過的程式碼，目前為止並沒有多少好的解決方案，因此作者提出了一套流程，針對 C/C++編譯過的程式，將其反組譯後進行分析，詳見圖 11。

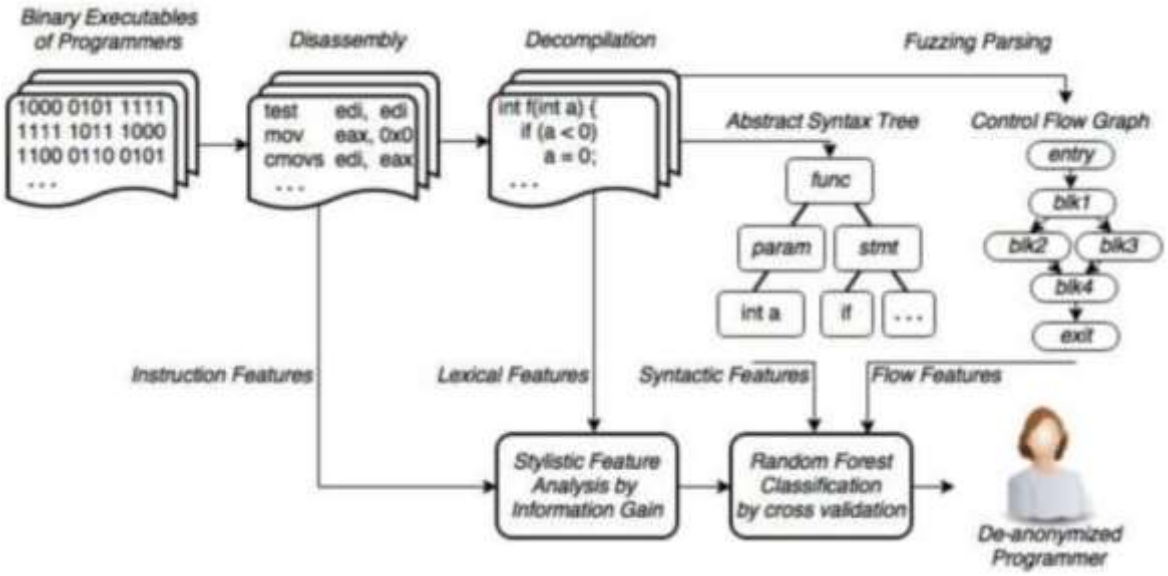

圖 11　無原始碼的程式反組譯分析流程

參、心得及建議

本次參加 DEF CON 第 26 次會議發現幾乎所有主題都在掌握新興議題與測試及前瞻性研究如下：

一、掌握新興議題與測試

今年的演講的領域很明顯的資安趨勢在工業控制系統安全、物聯網安全、智慧汽車及人工智慧以及醫療器材的議題等，這些資安的議題非常貼近民眾，且這些問題可能造成的衝擊，相較於傳統的資安問題，將產生更大的風險。針對這類問題的掌握程度及可能影響的層面可能都要投入資源進行研究，例如本年度政府機關(構)資通安全稽核作業及網路攻防演練皆納入了工控系統，以驗證台灣在這方面是否可能有相關的問題發生，並加強事前防範。

二、前瞻性研究

除了舊有議題的深入研究外，利用前瞻方式來解決現有的資安問題，或是模擬未來可能會發生的資安危害，也是非常熱門的研究內容，相較於過去幾年的駭客年會，大數據的應用及工業控制設備防護已逐漸變成了顯學，尤其是利用大數據和 AI 的方式，在各資安研究領域幾乎都占有一席之地，例如攻擊者透過 AI 設計惡意程式，並讓程式自動學習防毒軟體的監控及檢測機制，於防毒軟體檢測時可暫時停止可疑動作，當受害者傳輸特定資料時，再啟動側錄功能，並定期將前述資料傳送至攻擊者手中，此種攻擊方式是以往難以想像的，但由於有這方面的研究，讓我們有機會可以重新檢視現有的資安防護機制是否足夠應付未來的威脅。

肆、參考資料

[1] DEFCON 2018 官方網站, https://www.defcon.org/html/defcon-26/dc-26-index.html