iii PRIDE
資策會40週年

物聯網資安檢測技術培析

高傳凱 博士

資策會 資安所 聯網安全檢測組組長
TAICS TC Network and Security WG1 組長

前言

- 當萬物皆連網後，過去IT上常見的資安問題，原封不動的出現在OT上，最遭的是無論是IT或是OT發生資安問題，都會擴及到整個IoT上。
- 物聯網與傳統IT在資安上最大的「進化」是，對於駭客來說突破口變多了。
- 究竟物聯網有哪些特性?該特性又會引發什麼樣的資安問題?我們必須了解病症的原因，方可配置合適的療程(i.e., 管理原則)。

2019 © 資訊工業策進會 Institute for Information Industry

核能電廠攻擊事件

核電廠遭Stuxnet蠕蟲感染，入侵該電腦並且製造一個秘密的「後門 (back door)」

- 2010年9月，伊朗核能發電廠受到Stunex蠕蟲感染，表示僅有部份員工電腦受到感染，而非主要系統。

P.S. Stuxnet主要的攻擊目標為Siemens的SCADA系統

- 駭客如何做到：

1. 雖然該核電廠之SCADA與Internet是不相通的，但Stunex會透過USB傳染。
2. 如果偵測到對象是使用Wince作業系統，即入侵該電腦製造一個後門，連上網際網路，再由位於其它國家的伺服器下指令。
3. 如未偵測到WinCE運作，Stunex會自我複製到其它的USB端散播病毒。
4. 此外，還可透過共享資料夾、印表機後台處理程序來擴散。

- 如何防範：

1. 更新!!!但對工廠來說難度很高。

2019 © 資訊工業策進會 Institute for Information Industry

2016資安大事件-Mirai

2016年10月，600,000 IP camera、DVR、路由器和其他物聯網設備遭到入侵，並被用於大規模的Bot Net，以發起網際網路迄今為止遭受的最大的拒絕服務（DDoS）攻擊(1.7 Tbps)。

Source: Norse

2019 © 資訊工業策進會 Institute for Information Industry

2017資安大事件-想哭

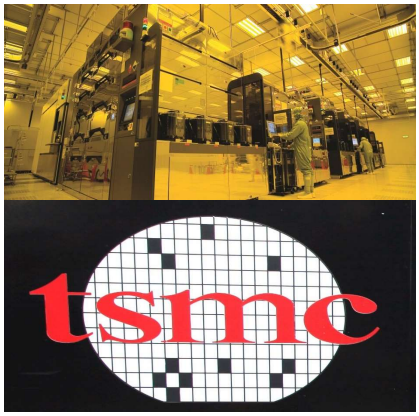
Source: Wikipedia.

全世界約150個國家的大規模感染

1. 在2016 年 8 月 “Shadow Brokers” 駭客組織號稱入侵了美國國家安全局(NSA)下屬的駭客組織” Equation Group” 竊取了大量機密檔，並將部分檔案公開到Internet，這家駭客組織還公佈了NSA的一些駭客工具，“永恆之藍” 便是其中一個利用445埠進行攻擊的工具 。
2. 想哭(WannaCry)利用NSA的「永恆之藍」（EternalBlue）漏洞利用程式透過網際網路對全球執行Windows作業系統的電腦進行攻擊，是一加密型勒索軟體兼蠕蟲病毒，該病毒利用AES-128和RSA演算法惡意加密用戶檔案以勒索比特幣。
3. 「永恆之藍」利用了某些版本的微軟伺服器訊息區塊（SMB）協定中的數個漏洞，而當中最嚴重的漏洞是允許遠端電腦執行程式碼。
4. 至少有150個國家遭受WannaCry攻擊。

2019 © 資訊工業策進會 Institute for Information Industry

2018資安大事件-台積電產線大中毒



機台產線遭感染，全台產線大當機

1. 2018年8月，台積電新竹晶圓廠，在周末安裝新機台後準備上線，但人員未依SOP規定於上線前先執行掃毒。
2. 新機台內藏WannaCry變種病毒，開機後自動掃描同一網路內的所有電腦主機，發動永恆之藍漏洞攻擊。
3. 因TSMC所有半導體廠都連接到同一個內網，擴散感染到北、中、南廠房，主要中毒機台是win7，與海外廠之間因為有防火牆，因而阻止了WannaCry。
4. 多廠產線中斷，更多產線機臺或天車系統，因WannaCry變種病毒而發生當機或重開機情況，其中又以7奈米、12奈米等先進製程產線的中毒災情較大。

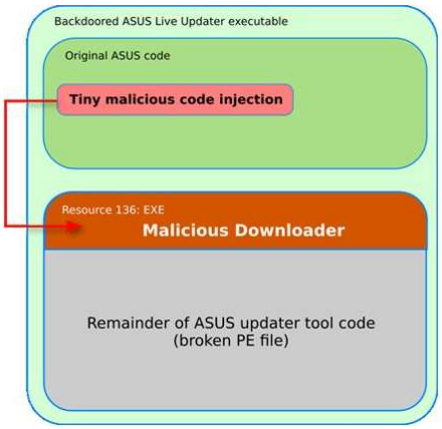
傳言: 由高階主管夾帶有病毒的USB，提供生產線機器使用。

- 如何防範：

1. 時時刻刻做好備份

2019 © 資訊工業策進會 Institute for Information Industry

2019資安大事件-華碩軟體更新檔遭植入後門



Source:卡巴斯基

1. Live Update是華碩在自家筆電所附上的工具程式，主要是為了幫助使用者保護與增強設備安全，可透過這款工具，獲得自動且即時的軟體更新。
2. 駭客入侵Live Update伺服器，將木馬程式植入華碩的軟體更新包，並用取得的華碩數位簽章對該軟體進行合法簽署。
3. 根據卡巴斯基的調查，他們統計到有5萬7千名卡巴斯基用戶，下載並安裝了具有後門的華碩Live Update版本，同時他們還估計，在全球可能有超過一百萬的用戶受影響。
4. 卡巴斯基也在蒐集的230份惡意程式樣本中，發現600多個MAC位址清單，這些裝置可能才是這次攻擊行動的主要目標。

2019 © 資訊工業策進會 Institute for Information Industry

2019資安大事件-美國政府單位陸續遭勒索軟體攻擊

2019年3月，亞特蘭大市政府遭到勒索病毒攻擊，公家機關被要求關閉無線網路以及電腦5天，8千名市政府員工受到影響，駭客向亞特蘭大市政府勒索市值5.1萬美元的比特幣。
2019年4月，美國德州的波特郡（Potter County）政府系統遭受勒索軟體入侵，造成許多員工半個月來，仍只能仰賴最傳統的紙筆來工作，而且不能上網。
2019年5月，巴爾的摩市政府第二度遭勒索軟體攻擊，市政府關閉大多數的伺服器，但報案、火災、郵件快遞或311市民服務都可正常運作。

Source: Marylandstater

2019 © 資訊工業策進會 Institute for Information Industry

物聯網相關處罰案例不斷

- 世界各地開始漸漸有應對手段，相關物聯網資安法規相繼推出，2017年歐盟推出史上最嚴格資料保護規定GDPR，並對科技巨擘Google祭出5,000萬歐元的天價裁罰
- 許多國際大廠所生產的物聯網設備，遭受美國聯邦貿易委員會(FTC)，以具連網設備未於研發階段實施必要的資安檢測為由，相繼開出鉅額裁罰
  - 偉易達(VTech)IoT連網玩具，遭罰65萬美元
  - ASUS、HTC認罪協商，要被美國政府稽核20年
  - D-link被以普遍認知安全強度不足為由遭監管10年
  - Facebook50億美元的罰款
- 英國針對「劍橋數據案」分析違法取得與使用Facebook個資事件爆發以來，估計約有8700萬筆臉書上的個人資料遭到違法使用，因此英國ICO對FB裁罰50萬英鎊。

2019 © 資訊工業策進會 Institute for Information Industry

物聯網6大特性(1/2)

- **威脅的影響範圍、影響程度較大**
  - 由於萬物相連，一旦受到攻擊，不僅會給IoT設備單體，而且很可能會給透過網路關連的IoT系統，IoT服務器整體造成影響
  - Ex: 駭客透過拉斯維加斯賭場大廳魚缸中的智慧溫度計入侵，進入到賭場的資料庫撈出投入大量金額的賭客清單
- **IoT設備的生命週期較長**
  - 汽車的平均年數為12～13年，工控設備使用期間大多為10年～20年，而IoT設備的裝置大多設想為長達10年以上長期使用
  - Ex: 2018年8月，台積電產線大中毒，主要中毒機台是win7
- **對IoT設備的監視不容易進行**
  - 由於許多IoT設備沒有像電腦、智慧手機等那樣的畫面等，因此難以透過人眼進行監視
  - Ex: 2016年10月(Mirai)，600,000 IP camera、DVR、路由器和其他物聯網設備遭到入侵，並被用於大規模的Bot Net，以發起網際網路迄今為止遭受的最大的拒絕服務(DDoS)攻擊(1.7 Tbps)

2019 © 資訊工業策進會 Institute for Information Industry

物聯網6大特性(2/2)

- **IoT設備側和網路側對環境、特性的相互了解不充分**
  - IoT設備連接到網路後，可能無法滿足所需的安全、性能。特別是連接的網路環境，應注意可能使IoT設備側的安全要件發生變化。
  - Ex: 2018年10月，富士通（Fujitsu）高階無線鍵鼠之2.4G傳輸遭注入攻擊，導致相連電腦遭受駭客控制
- **IoT設備的功能、性能受限**
  - 感知器等資源有限的IoT設備，有可能不適用密碼等安全對策。
  - Ex: 駭客透過拉斯維加斯賭場大廳魚缸中的智慧溫度計入侵，進入到賭場的資料庫撈出投入大量金額的賭客清單
- **可能進行開發者未曾設想的連接**
  - 以往從未連接到外部的裝置被連接到網路，可能發生IoT設備生產廠家、系統及服務開發者當初未曾設想的影響。
  - Ex: OWASP 2018 IoT top 10第1名就是弱密碼、預設密碼漏洞

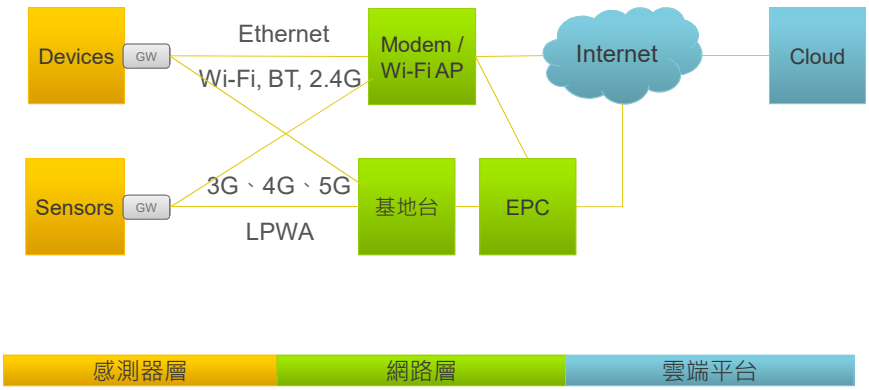
2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安特性

- 萬物相連受害範圍大增，各個區段的網域要確實隔離(範例)
- 因IoT設備的生命週期長，因此必須做到在本公司 Web頁面刊載，在設備、系統上顯示消息，通知支援期間、預告及通知支援期間結束期間，若遇高風險狀況，可從技術上限制其連接到網路。
- 由於許多IoT設備沒有像電腦、智慧手機等那樣的畫面，被入侵也不知，因此須提供警示機制。
- 設備連上網且壽命長，因此透過軟體安全性更新方式，讓物聯網安全隨駭客能力同步升級已為大勢所趨。
- 輕量化設備沒有配置防火牆等防護功能，因此必須搭配其它高安全功能設備給予保護(如: security gateway)
- 資料必須穿過小網接上大網，如沒自信/能力為資安把關，可以把風險轉嫁，雲端可選用Amazon、google等，網路層可選擇電信網路(如:中華電信)提高安全性
- 預設密碼的氾濫，改預設密碼這件事必須讓使用者都認知到，或從技術上強制要求更改預設密碼

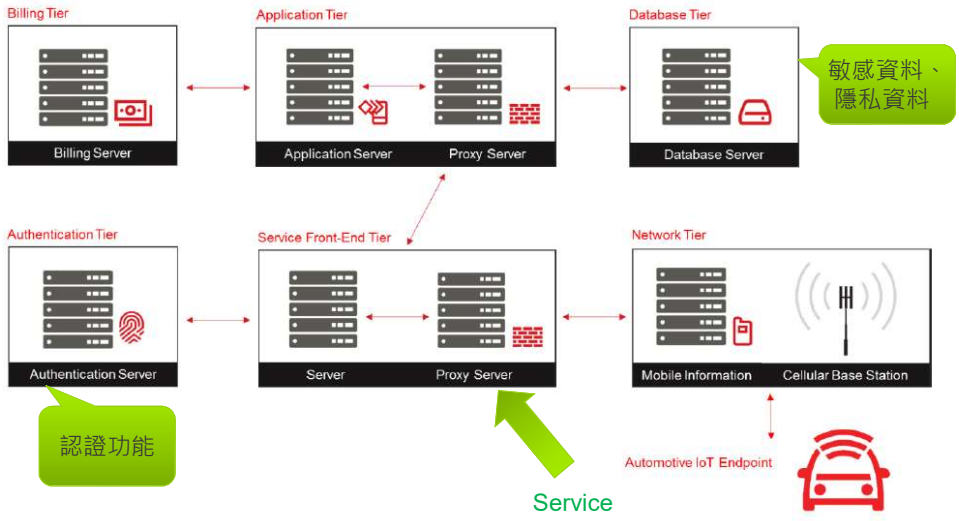
2019 © 資訊工業策進會 Institute for Information Industry

物聯網架構圖



2019 © 資訊工業策進會 Institute for Information Industry

Service ecosystem

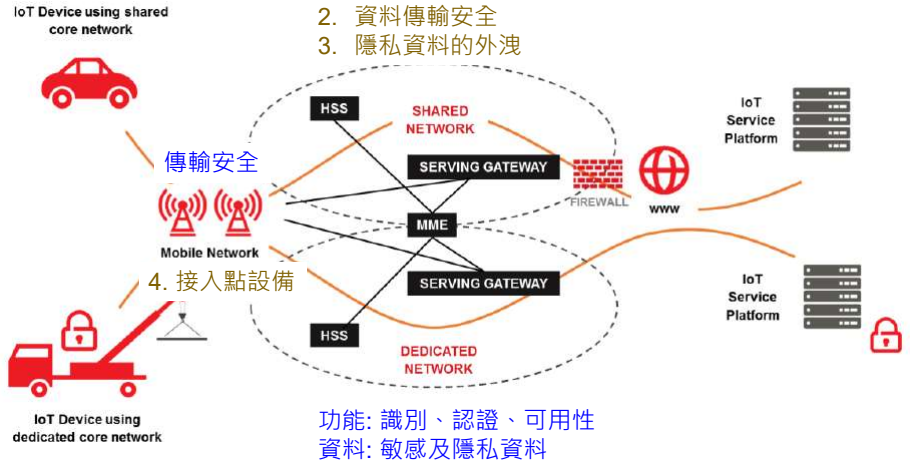


圖片來源: GSMA IoT Security Guideline

2019 © 資訊工業策進會 Institute for Information Industry

Private Network Configuration

網路層資產:
1. 互動的功能
2. 資料傳輸安全
3. 隱私資料的外洩

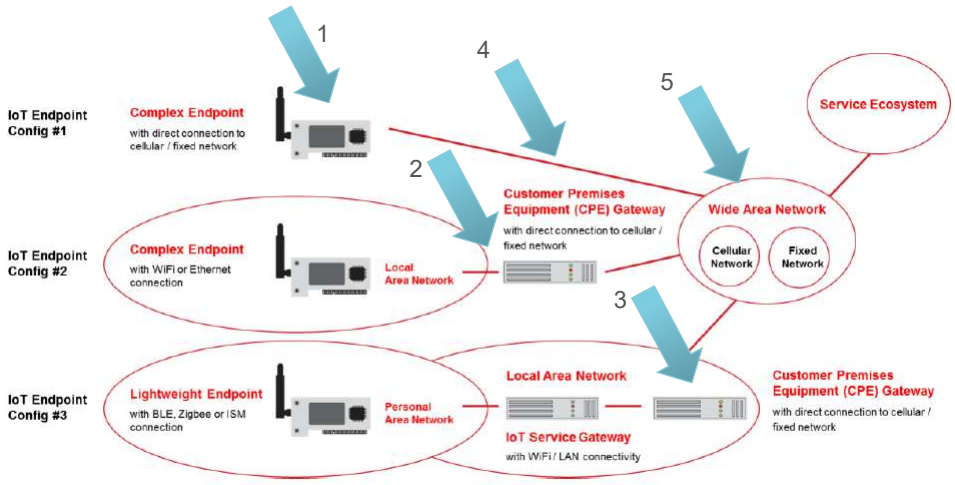


功能: 識別、認證、可用性
資料: 敏感及隱私資料

圖片來源: GSMA IoT Security Guideline

2019 © 資訊工業策進會 Institute for Information Industry

Endpoint Configuration



圖片來源: GSMA IoT Security Guideline

2019 © 資訊工業策進會 Institute for Information Industry

物聯網10大資安威脅

1. 成為DDoS的殭屍主機 (Zombie Device)
2. 傳輸的資料與隱私外洩 (Transmitted Data and Privacy Leakage)
3. API攻擊 (API attack)
4. 韌體敏感資料外洩 (Hard coding password, key, etc in firmware)
5. 密碼破解 (Password Cracking)
6. 中間人攻擊 (Man-in-the-middle)
7. 工程師後門 (Engineer Backdoor)
8. 網頁管理介面攻擊 (Injection)
9. 勒索/挖礦病毒 (Ransomware / Mining Malware)
10. UPnP裝置攻擊 (UPnP Attack)

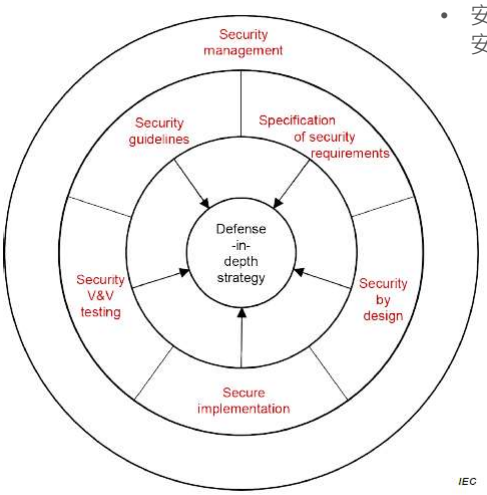
2019 © 資訊工業策進會 Institute for Information Industry

風險評估

- 在不同應用對象，貴重資產不同:
  - 民 => 隱私資料在消費者市場相當重視。
  - 工 => 對工控設備而言，可用性為最優先考量。
  - 軍 => 對高敏感性單位，CIA同等重要。
- 面對不同程度的攻擊，會影響可接受風險的決斷
  - 等級1：正常使用者誤操作，導致資安事件的發生
  - 等級2：惡意使用者藉由自動/半自動漏洞利用工具，進行無差別攻擊
  - 等級3：針對特定組織/廠商所做的複雜且多面向的攻擊
    - 例如: 西門子SCADA的APT攻擊，國際大廠容易成為此對象
  - 等級4：國家級駭客，利用國家資源針對特定目標進行駭客攻擊
    - 例如: 烏克蘭大停電事件等這類型國家關鍵基礎設施。

2019 © 資訊工業策進會 Institute for Information Industry

安全保證策略



- Security Management
  - 安全管理實踐的目的是確保在整個產品生命週期中對安全相關的活動進行充分的計劃，記錄和執行。
- Specification of security requirements
  - 該過程用於記錄產品所需的安全功能以及預期的產品安全要求。
- Security by design
  - 識別產品所面臨的威脅、評估風險、考量安全需求及檢視安全設計。
- Secure implementation
  - 透過白箱檢測方式的源碼靜態分析，以避免具資安風險的編程內容及不安全函式庫
- Security V&V testing
  - 實際測試產品是否存在資安漏洞，評估產品潛在風險，預先檢視產品上線後所可能面臨的資安攻擊
- Security guidelines
  - 產出一份文檔，描述如何根據產品安全要求，配置和維護產品的防禦深度策略

2019 © 資訊工業策進會 Institute for Information Industry

資安檢測

2019 © 資訊工業策進會 Institute for Information Industry

資安服務業務

資安諮詢輔導顧問

Standard
技術法規制定

合規測試

CSTI

資安工具研發

滲透測試
(IoT Devices, …)
執行方法: NIST SP 800-115

資安管理強化

資安鑑識

2019 © 資訊工業策進會 Institute for Information Industry

資安檢測

白箱檢測

源碼檢測

Tool:
Checkmarx
Fortify

Pros:
High coverage
Find issues in early stage

黑箱檢測

弱點掃描

Tool:
Acunetix
Nessus
CMARS

滲透測試

Tool:
Kali
Burp Suite.
hashcat
…

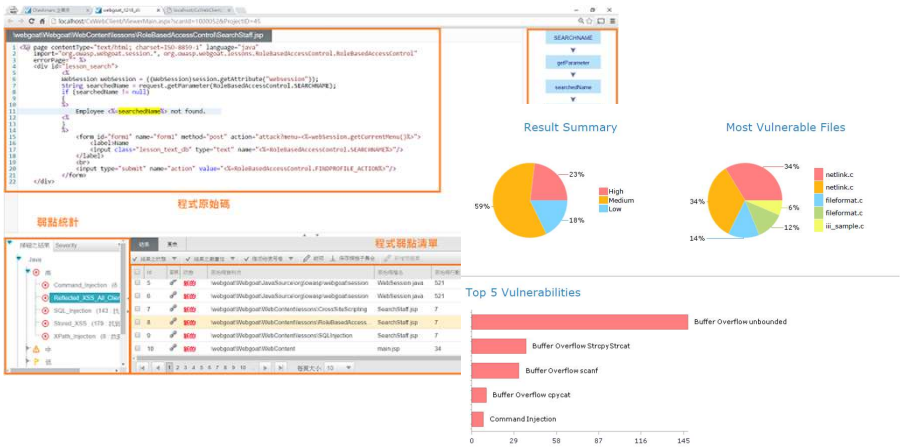
Pros:
No need source code
Low false rate

模糊測試

Tool:
Defensics

2019 © 資訊工業策進會 Institute for Information Industry

源碼檢測



2019 © 資訊工業策進會 Institute for Information Industry

系統弱點掃描

192.168.1.236

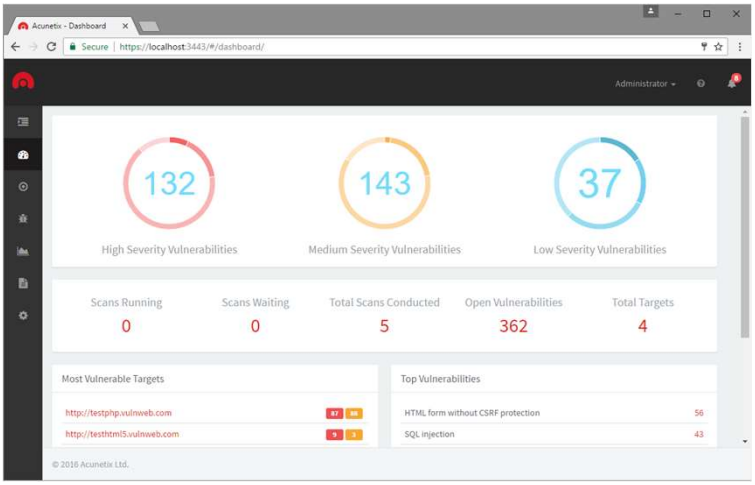
CRITICAL	HIGH	MEDIUM	LOW	INFO
0	0	4	0	35

Vulnerabilities Total: 39

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	57608	SMB Signing Disabled
INFO	N/A	10092	FTP Server Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10287	Traceroute Information

2019 © 資訊工業策進會 Institute for Information Industry

網站弱點掃描



2019 © 資訊工業策進會 Institute for Information Industry

模糊測試工具

目前支援模糊測試之協定
- **Wi-Fi Protocol**
- **Ethernet-related Protocol**
- **S1AP**
- **SCTP**
- **Modbus**
- **DLMS/COSEM**

智慧資安模糊測試技術雛形，利用**人工智慧學習技術** (Long/Short-Term Memory, LSTM) 及**智慧選擇8種變異方法** (功能碼變異、暫存器變異、payload長度異常變異等)，創建模糊測試資料進行模糊測試

2019 © 資訊工業策進會 Institute for Information Industry

行動APP資安檢測工具

2019 © 資訊工業策進會 Institute for Information Industry

各國物聯網資安管理政策

2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-美國(1/4)

- 美國國土安全部(DHS)
  - 保護物聯網策略原則(Strategic Principles for Securing the Internet of Things, 2016/11)
    - 目的：解釋物聯網的安全風險，並提供一套非約束性原則和最佳實踐建議，幫助利益相關者(開發人員、設備廠商、服務供應商、工業/企業級消費者)在開發、製造、實施或使用網路連接設備時考慮其安全性。
    - 六項原則：
      - 在設計階段納入安全考量
      - 改善安全更新和漏洞管理機制
      - 建立可靠的安全作法
      - 根據潛在影響確定安全措施的優先順序
      - 推動物聯網生態體系的透明度
      - 謹慎的設備連結

2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-美國(2/4)

- 加州議會通過全美首個IoT法案，要求每個IoT裝置都要有獨立密碼
  - 2018年9月通過，預計2020年1月1日實施的「物聯網裝置資訊隱私法案」（SB-327 Information Privacy: Connected Devices），要求製造商為IoT裝置提供合理的安全功能，以保障裝置及其資料的安全，不受非授權存取、破壞、使用、修改或是揭露。
  - 若裝置允許在本地網路以外用密碼存取，則該裝置必須每一台分配自有密碼，或強制使用者在首次連網時設定自有密碼。這意謂連網裝置不得再使用大家都一樣的預設密碼。

2019 © 資訊工業策進會 Institute for Information Industry

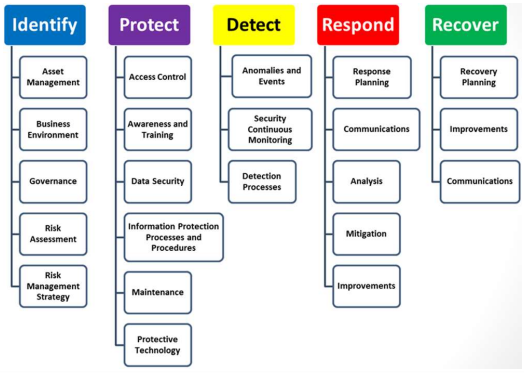
物聯網資安政策推行狀況-美國(3/4)

- 美國物聯網資安國家標準
  - ANSI/CAN/UL 2900-1:2017 Software Cybersecurity for Network-Connectable Products, Part 1: General Requirements
    - 可聯網設備及產品的軟體資安一般要求

2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-美國(4/4)

- 美國2017年8月就物聯網資安訂定法規，例如針對政府部門採購IoT裝置進行規範的《IoT網路安全促進法案》（Internet of Things Cybersecurity Improvement Act of 2017）
- 2018年9月思科對美國國家標準暨技術研究院制定的《網路安全框架》(Cybersecurity Framework, CSF)，CSF受到日本、英國、義大利、以色列等國政府採用，便認為其可為廠商提供一致標準。



2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-歐盟(1/2)

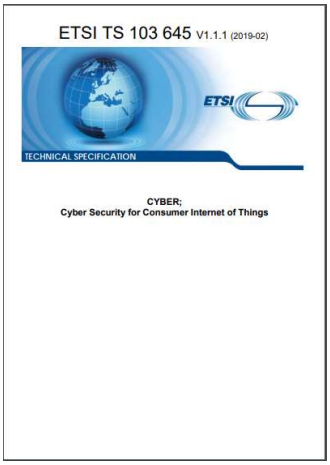
- 歐盟委員會(European Commission)
  - 歐盟通用資料保護規則(GDPR, 2018/5)
    - 取代歐盟在1995年推出的歐盟個人資料保護指令，該法案於2016年4月27日通過，兩年的緩衝期後，在2018年5月25日強制執行。
    - 適用在歐盟地區註冊的企業，或非歐盟註冊的企業，但在歐盟營運，有蒐集、處理或利用歐盟民眾個人資料的企業或組織等，都在GDPR的規範中。

資料來源：iThome網站

2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-歐盟(2/2)

- 歐洲電信標準協會(ETSI)
  - TS 103 645. Cyber Security for Consumer Internet of Things (2019/2)
    - 包括兒童玩具和嬰兒監視器，連網安全相關產品，如煙霧探測器和門鎖、智慧鏡頭、電視和喇叭、穿戴式健康追蹤器、智慧家庭和警報系統、連網家電或智慧家居助理。
    - 不得採用預設密碼。
    - 實施漏洞批漏政策，漏洞發現時需盡快公布。
    - 廠商需要確保客戶的敏感資料和身分認證資料等安全。



2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-日本(1/2)

- **日本推出物聯網專業檢定測驗**
  - 2016年7月，日本總務省·經濟產業省發表IoT Security Guidelines，以提供使用者安全安心地使用IoT設備為出發點，要求從IoT設備、系統、服務的供給者、經營者及使用者都能確保安全性。
- **日本要用3大資安對策迎戰2020奧運會**
  - 日本國家資訊安全中心(NISC)秘書長Mitsuaki ASHIDA強調，在2020年奧運的資安建置上，有三大重點項目，分別是安全的物聯網(IoT)、保護關鍵資訊基礎建設(Critical Information Infrastructure Protection，CIIP)以及人才招募(Human Resource)。

2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-日本(2/2)

- 日本總務省在2019年1月25日公布新的網路相關規定，要求自2020年4月起，日本上市的物聯網相關週邊與終端設備，需有相應的資安防護作為，而且政府將從2019年2月20日起進行為期5年的網路設備普查計畫：NOTICE。
- 修改國立研究開發法人情報通信研究機構「**電氣通信事業法**」，附帶條款的第8條第2項業務實施部分，要求
  - 針對特定通信埠(Port)或特定連線行為，並作成電子紀錄的義務
  - 不能使用過去大規模資安事件時最常見的100種密碼
  - 發生重大事件時，如3萬用戶連續12小時以上有使用障礙、或超過100萬用戶有2小時以上使用障礙時，立即向日本總務省報告
  - 不定期更換密碼與防護方式
  - 終端設備須具有防非法登錄功能，例如能切斷外部控制、要求變更初期預設ID和密碼、可時常更新軟體等
  - 唯有滿足標準、獲得認定的設備才能在日本上市。

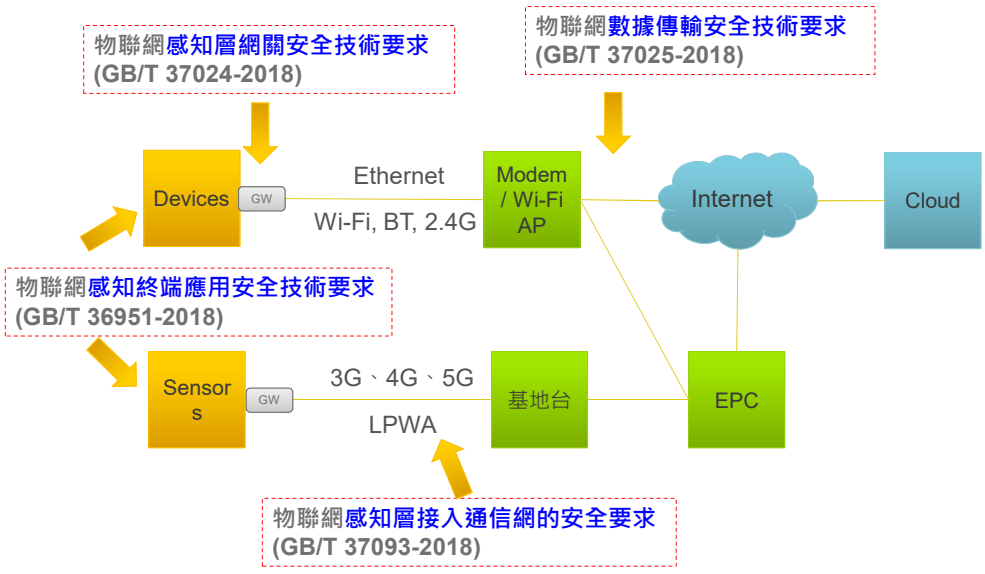
2019 © 資訊工業策進會 Institute for Information Industry

物聯網資安政策推行狀況-中國

- 2018年隱私條款專項工作專家評審會議召開
  - 2018年12月，信息安全標準化技術委員會秘書處在北京組織召開了「2018年隱私條款專項工作」的專家集中評審會。對40款網路產品和服務的隱私條款進行了評審，並希望通過評審工作給個人信息保護國家標準的完善提出工作建議，以便後續更好開展隱私條款專項工作。
- 27項信安標委歸口國家標準獲批發布
  - 2018年12月，信息安全標準化技術委員會發布了27 項國家標準，其中有5項物聯網安全方面的國家標準，將在2019年7月1日開始實施，預計中國的物聯網產品製造商，將會開始遭遇各機關(尤其政府單位)的取證需求，物聯網資安將會大幅躍進。

2019 © 資訊工業策進會 Institute for Information Industry

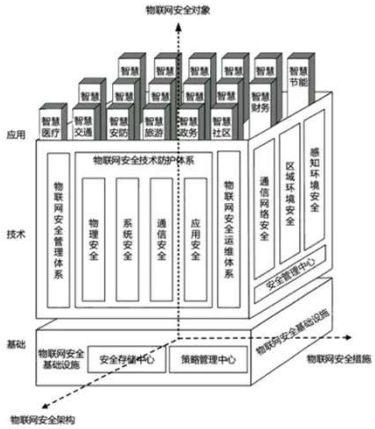
中國5項物聯網安全標準 (1/3)



2019 © 資訊工業策進會 Institute for Information Industry

中國5項物聯網安全標準 (2/3)

- 全國信息安全標準化技術委員會
  - 信息安全技術物聯網**安全參考模型及通用要求**(GB/T 37044-2018)
    - 此標準規定了物聯網安全參考模型，包括物聯網安全對象、物聯網安全架構和物聯網安全措施，並針對物聯網系統提出了安全通用要求。



  - 信息安全技術物聯網**感知終端應用安全技術要求**(GB/T 36951-2018)
    - 對物聯網感知終端安全的技術要求，包括感知終端的物理、系統、接入、通信和數據等。

2019 © 資訊工業策進會 Institute for Information Industry

中國5項物聯網安全標準 (3/3)

- 全國信息安全標準化技術委員會
  - 信息安全技術物聯網**感知層網關安全技術要求**(GB/T 37024-2018)
    - 對物聯網感知層網關安全技術要求，包括安全環境，設備安全，訪問控制，入侵檢測，安全審計以及安全保障等。
  - 信息安全技術物聯網**感知層接入通信網的安全要求**(GB/T 37093-2018)
    - 對感知終端和信息網絡接入安全要求，包括感知設備標識，接入認證，訪問控制、入侵防護，隔離防護，密鑰管理，日誌等技術等。
  - 信息安全技術物聯網**數據傳輸安全技術要求**(GB/T 37025-2018)
    - 對物聯網傳輸的一般數據和敏感數據的安全技術要求，有基礎級（一般數據）和增強級（敏感數據）兩種等級。

2019 © 資訊工業策進會 Institute for Information Industry


iii PRIDE
資策會40週年
Thank you
2019 © 資訊工業策進會 Institute for Information Industry