物聯網資訊安全特性與原則初探

馮明惠博士、吳國華博士
資策會 智慧網通系統研究所

IDC 認為資安是物聯網系統最優先考慮的因子 [2]，這可由最近駭客遠端關閉正在疾駛的切諾基型吉普車（Jeep Cherokee）引擎與將連網家電當成殭屍網路[1,2]等駭人新聞看出端倪。依據 AT&T 的調查 [5]，2014 年約有 4300 萬件資安事件，比起 2013 年增加 48%；阻斷服務攻擊（DDoS）也多了 62%，75%企業董事會不管資安影響 [6]。隔年，AT&T 再度調查 [7] 指出 2015、2016 間物聯網資安漏洞就增加 458%；90% 受調查企業對自身物聯網系統資安缺乏信心；只有 14%受調查企業之連網設備執行稽查工作，38% 受調查企業使用裝置管理系統或軟體，餘近五成的是估計或根本不知道自己有那些連網設備。

歐美政府也正視這個問題紛紛投入研究，2016 年 11 月美國白宮發行 Guidelines for IoT Cybersecurity，強調以工程手段(Engineering-based Approach)直接於物聯網技術上建立資安系統；2016 年 7 月歐盟 (EC) 與 ECSO (European Cyber Security Organization) 簽署公私合作夥伴(PPP; Public-Private Partnership)計畫，將透過 Programme Horizon 2020 計畫投資 4 億 5 仟萬歐元，投入資安研究。本篇報告探討物聯網資安特性與原則，茲分調查物聯網資訊安全特性、物聯網資訊安全策略原則與結語章節說明。

物聯網資訊安全特性

大家紛紛投入物聯網發展，但有很多問題與特性是需要被解決，因此本節先討論物聯網必須被解決基本問題 [8]，茲說明如下：

- 過期物聯網設備應該要如何處理？

駭客都會利用軟體漏洞或弱點進行侵入與攻擊，即便現在是安全的，也不保證沒有漏洞或弱點，尤其在終端設備上更顯得脆弱，不斷有人被攻擊，不斷更正修補軟體，不

[1] http://www.storm.mg/article/129445
[2] http://www.appledaily.com.tw/realtimenews/article/new/20160806/923172/

斷軟體更新，這程序會不斷循環，直到天荒地老。軟體更新可以使用召回或線上兩種更新方法，線上更新當然是最方便與節省成本的方法，缺點是比較有資安議題；當然也可採召回方式，是比較貴，但相對較安全。這中間取捨當然由廠商衡量與考量。

當物聯網設備舊了、供應商倒了、被併購了或是停產時，設備不再進行保固，不被保固設備是很脆弱，那該如何是好！拿另一台更替？找另外供應商？這些都需要互通支持。

- 如何互通？

假設家裡要架設警報系統、遠端操控空調系統、門禁系統等，若每套系統各自附手機軟體供使用者控制用，三套就要有三個手機軟體，十套就有十個手機軟體，一個家庭不同系統，若彼此不互通，就會有這樣結果。因此，互通就變得很重要。

目前市面物聯網系統至少有 360 套平台，超過 100 種標準，包含多樣多廠牌連網設備、手機軟體、雲端、中央資料庫與系統整合等，要串起這些元件或系統供應商之生態鏈是非常不容易；基於商業利益考量，串接生態系已經很難，又要彼此資料交換是安全的，那就變得更難了。

- 如何防範駭客行為？

除先前提過駭客入侵例子外，網路監視器[3]、藍芽智慧鎖、德國鋼廠都曾被駭而造成損失，駭客也有多類型，有竊取機密國家級、有勒索犯罪級、有好玩級的，駭客目前已變成一個產業，也上下游分工，因此任何人都可以因為利益或自身需求向駭客取得服務。駭客行為會不勝枚舉，如何防範是需要技術協助，也需要管理實務加以防範。

- 沒有防火牆網路，如何防護？

過去企業用防火牆擋住外界所有資料交換來維繫資訊安全，利用虛擬私有網路（Virtual Private Network, VPN）來維繫少量例外之資料交換。其最重要精神就是

[3] http://www.appledaily.com.tw/appledaily/article/headline/20150714/36663892/

隔離，不交換，就不會有資安問題。但物聯網系統就是利用公眾網路存取控制裝置，故傳統有圍牆網路概念已經不見了；另物聯網裝置通常要省電、計算能力差，要執行複雜加密運算是吃力的。此外，當為數眾多裝置連上網路，如何判定是合法裝置也是一大議題。因此，物聯網系統之資安就變得很不一樣。

- 資料必須穿過小網接上大網，安全性如何保證？

物聯網系統會依據需求採用不同無線網路系統,有可能是GPRS、3G、4G、LTE、Satelitte、WiFi、Bluetooth、DECT、Z-wave、ZigBee、LoRa…，資料傳輸必須經過大大小小不同無線網路，在不同通訊技術之界接(漫遊)，如何讓資料不要遺失與確保資料安全呢？譬如車禍現場需要緊急診斷病患，利用遠端醫療系統讓醫生即時診斷遠端車禍現場的病患，在這例子裡，如何讓病患與醫生間通訊是安全的；如何讓現場設備安全收集資料與後送；如何讓正確設備或人員加入這個系統；如何讓這些資料安全通過這麼多大大小小網路，並保持連線且不延遲；如何將需要即時處理的就放在前端應用程式執行等，這些都是必須考慮與解決的問題。

- 如何提供安全預設密碼機制之操作？

目前市售分享器、防火牆、監視器等設備都會有個預設密碼，是人人可查得到，這種方法時時常有侵入事件，如何利用簡單、安全身分認證機制取代原先預設密碼機制是一件重要事情。

物聯網資訊安全策略原則

發展物聯網是高度分工與整合，設計、製造、建置，網路與平台服務將會有不同人提供，為了資訊安全，美國國土安全部在 2016 年 11 月提出發展物聯網系統資訊安全策略原則 [9]，值得拿來參考、借鏡與討論，茲說明如下：

- 具備整體資安系統設計是較經得起考驗

企業常因商機之故，未審慎考慮資安而直接投入，一旦發生資安事件，輕則時機延誤，重則系統停擺造成損失。若能在設計就考慮各種威脅與中斷之狀況與相對應處理方法，日後營運時資安事件將會大大降低；就算發生，也可避免緊急採購昂貴資安產品來補

強。以下有些管理實務可供參考：

1. 需要強化目前裝置預設密碼之安全機制：目前預設密碼常常被破解而造成損失，需要採用其他方式認證機制取代原來預設密碼之機制。
2. 採用新的作業系統:很多廠商採用Linux製造其裝置或系統,老舊版本隱含漏洞多，更新最新版本可修補已發現到的漏洞。
3. 採硬體安全模組強化資訊安全保護：將資安做成晶片提供加密與身分驗證等。
4. 設計時考慮裝置失能時，如何持續運作物聯網系統：預先埋入管控各元件失能時持續提供服務之風險。

- 採納資訊安全更新與漏洞管理

系統只要有漏洞就會引來攻擊，因此持續修補更新與漏洞管理是可以降低威脅。包含故障設備對系統之影響、各項產品使用期限、以及維修成本都應該在設計階段考慮進來；當資安軟體更新失能時，製造商必須衡量召回之費用與被攻擊的損失風險。美國國家通訊與資訊管理委員會(NTIA)提出物聯網更新與修補流程，是可加以參考。以下有些管理實務可供參考：

1. 利用自動且安全傳輸更新機制：漏洞修補需要自動更新，並且利用加密方法確保更新完整性與安全性。
2. 軟體更新也需考慮到協力廠商軟體之漏洞與資安改善，以確保客戶最新最完整防護。
3. 發展漏洞自動偵測機制：要有機制從駭客社群與研究單位即時獲取重要漏洞情報，有利設計與漏洞回應。
4. 制定相關漏洞披露的政策：包括已確定是安全漏洞之相對處理實務；相關披露資訊包含所有報給國際資安事件處理小組(CSIRT)之漏洞報告，美國官方網路防衛機構(US-CERT)、美國工業控制系統電腦危機處理中心(ICS-CERT)與其他區域資安事件處理單位發佈之技術警示與重大資安事件之漏洞與解決辦法。
5. 發展過期物聯網設備處理策略：並非所有設備都有無限期資安漏洞修補與更新，開發者需要考量到設備使用年限到期之前需與製造商與客戶溝通風險與使用日期。

- 建立認可資安實務

有很多好用的傳統資通訊安全實務是可以拿來運用在物聯網系統，這些方法可以界定漏洞、偵測不法、資安事件處理回應機制、損失或中斷回復機制。美國國家標準技術研究所(NIST)因應 13636 美國總統執行命令所制定一套風險管理參考框架(NIST Cybersecurity Risk Management Framework)，是一套企業資安險管理檢驗準則，不僅僅適用於物聯網，是值得參考的資安框架。以下之管理實務可供參考：

1. 以現有資安防護實務當起始點，依據物聯網特性，彈性調整與創新方法應用在物聯網系統各環節。
2. 有些行業可依其特有執行方式與指導原則當起點，逐步加入資安實務。如國家高速公路交通安全管理局(NHTSA)之新式汽車資訊安全最佳實務與國家食品藥物管理局也制定上市後醫療器材資安管理原則草案。
3. 深度實踐資安防衛：應該採用完整資安防衛方法，分層防衛資安威脅與使用工具偵測惡意使用者，以彌補漏洞補強不足與更新失效時。
4. 參與資安漏洞分享平台，即時接收最新資安威脅與漏洞以保持最高警戒。這包含美國國土安全部門(DHS)的國家安全與通訊整合中心(NCCIC)、國家資安與通訊資訊中心等。

- 依影響程度分類資安方法優先等級

不同風險模型對不同系統或供應商(生態系)差異很大，譬如若發生資安事件，對核能電廠與零售業的衝擊是不同的，因此，是要依據可以承受影響程度再來決定採用風險方法。以下可供參考：

1. 了解裝置如何被使用與其使用環境，可幫助設計裝置、裝置操作與資安方法。
2. 採紅隊測試：先未施任何資安機制，測試整個系統資安容忍程度，並找出那個應用程式、網路或資料被攻擊或弱點後，再研擬可靠資安方法。
3. 連網之裝置需身分識別與認證，只有容許被容許設備進行服務存取，特別是工業與企業系統。

- 推動物聯網元件透明化

物聯網系統至少涉及前端裝置、網路、雲端與應用等等不同系統或供應商(生態系)，不同階段提供商若有漏洞會影響整個系統，因此開發者與製造商需要知道整個供應體

系之軟硬體及其可能產生之漏洞，廠商需提供清楚的軟硬體元件、模組、版本、漏洞等資訊以利風險管理。以下有些管理實務可供參考：

1. 執行應用系統風險鑑定，以鑑定內外部風險，供應商需含在風險鑑定的流程中，可清楚了解漏洞，並建立透明與信任機制，有利後續各元件軟體修補與更新之執行。
2. 建立漏洞公開機制，使的外部已知風險可以讓內部人了解。
3. 發展與採用軟體元件清單(軟體 BOM 表)，這可以當成整個供應體系管理資安風險之工具。

- 慎重小心設備連網

物聯網設備連網就有資安風險，尤其是工業設備，是否連網要評估裝置服務中斷對整個服務之影響。以下可供參考：

1. 確定物聯網設備連網用途，特別是工業用途的設備，若設備連網並不影響其主要功能，那就要考慮其效益。
2. 有些連網並非要上網際網路，只是在內網收集評估資訊，謹慎評估連上網際網路的效果。工業控制系統(ICS)系統就有專章規範[4]。
3. 內建控制連網機制，以便製造商、服務商與客戶依據目的控制連網或是擇性連網，以確保資訊安全。

結語

物聯網系統就是你我日常生活的應用系統，可能是便利找路、找公車的系統，也可能是安全自動車系統，一旦公車資訊外洩或許損失不大，但若是行駛中車子突然遭遇駭客攻擊，那恐會有傷亡風險，因此物聯網資安重要程度可想而知，各國對此已投入很多心力，主要期望是能夠盡快找出福國利民之安全物聯網系統。

美國國土安全部指出 [9]，傳統資安實務是可以有效降低資安風險，但現在物聯網系統相較傳統基本資安防護更形複雜，物聯網系統關聯的生態鏈太多，有前端製造、網路、雲端、系統整合商、物聯網設計與開發者，任何一個物聯網資安事件發生，往往不容

[4] https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

易知道是哪個環節要負起責任，也就是說誘因不足，再者也沒有一套資安標準可以讓物聯網系統生態系可遵守，因此這問題遲遲未解。不過現在各國已意會到，相信各國會利用法令法規方式制定責任義務，目前很多公私部門投入探詢解決之道，如 [9, 10, 11, 12, 13, 14]，相信會越來越多投入。

國內相關政府與研發單位也密集注意這項發展，且有實際計畫執行[5]，也會提出台灣物聯網資訊安全策略原則、標準與最佳實務。而財團法人資訊工業策進會資安科技研究所長期專注於資通訊安全領域之政策規劃、推動及新技術研發等[6]，其中技術服務主要協助政府執行國家資通安全會報幕僚，提供政府機關事前安全防護、事中預警應變、事後復原等資安技術服務；技術研發包含新一代資安關鍵核心、新興資安整合技術、資安治理與風險管控技術、企業資料防護與資安監控技術，以符合政府及企業資安治理、個資保護等規範要求。智慧網通系統研究所過去深耕網路、能源、車載系統研發工作多年，面對物聯網時代來臨，將本著過去研發能量，聚焦物聯網核心平台(OneM2M)研發，研發物聯網安全平台，並與國內外廠商合作，整合智慧工廠、智慧能源、連網車等應用，期盼累積個多技術資產與使用情境(use cases)；建立物聯網平台之識別、身分驗證與裝置管理之授信平台，協助物聯網之發展。在能量累積過程中，會有各式各樣使用情境與設計參考，是可以提供產業分享與交流，期盼能加速物聯網之蓬勃發展。

參考

[1] 經濟部技術處, "第 1248 次業務會報簡報-物聯網產業技術研發佈局," March, 2016.

[2] A. Eric Sineath, "Why You Need a Strategy for IoT," *TAG IoT Symposium: Industry 4.0 and the Internet of Things,* July 19th, 2016.

[3] IDC, "Worldwide Internet of Things Forecast (2015-2020)," *http://www.idc.com/infographics/IoT/ATTACHMENTS/IoT.pdf,* May 2015.

[4] Cisco, "The Internet of Things: How the Next Evolution of the Internet Is," *https://www.cisco.com/web/,* April 2011.

[5] http://www.ithome.com.tw/news/110923

[6] http://www.iii.org.tw/About/Department.aspx?dp_sqno=7&fm_sqno=36

[5] AT&T, “What Every CEO Needs to Know About Cybersecurity -- Decoding the Adversary, Volume 1,” *AT&T Cybersecurity Insights V.*

[6] PwC, “US State of Cyber Security,” 2015.

[7] AT&T, “The CEO’s Guide to Securing the Internet of Things -- Exploring IoT Security, Volume 2,” *AT&T Cybersecurity Insights.*

[8] F. Beckman, “6 IoT Security Fundamentals that myst be solved,” *COMBITECH,* September 2016.

[9] U. D. o. H. Security, “STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT) Version 1.0,” November 15, 2016.

[10] NIST, “Improving Critical Infrsture Cybersecurity Executive Order 13636: Preliminiary Cybersecurity Framework”.

[11] NIST, “System Security Engineering --- Consideraations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure System,” November 2016.

[12] B. Weinberg, “Open source hygiene – Mitigating Security Risks from Development, Integration, Distribution and Deployment of Open Source Software,” *Black Duck Software,* June 5, 2015.

[13] iot.eclipse.org, “The Three Software Stacks Required for IoT Architectures,” September 2016.

[14] OWASP, “OWASP Top Ten Project,” *https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.*

[15] P. Cloud, “Securing the Internet of Things: Seven Steps to Minimize IoT Risk in the Cloud Services,” 2016.

[16] EY, “Cybersecurity and the Internet of Things,” March 2015.

[17] L. Neduchal, “Which IoT Changllenges Can You Transform Into Opportunities?,” *EY,* September 13th 2016.

[18] Jason Porter, Bob Bragdon, “Securing the Internet of Things: What the CEO Needs to Know,” *AT&T,* March 2016.