IoT 設備資安防護指南

臺灣學術網路危機處理中心團隊(TACERT)製

目　錄

一、前言

近年來資訊科技及網路技術的快速發展，連接網路的設備已從原本定點有線連接網路的電腦(PC)、可移動無線連接網路的筆記型電腦(NB)到透過 4G 網路連線的手機，如今已經進入到萬物皆可連網的時代，無論是家電、個人裝置、公共建設甚至於車子，未來所有東西將皆可連上網路，進入一個物聯網的時代。

二、物聯網的定義

物聯網(Internet of Things)以下簡稱 IoT，廣義的定義為「可透過各種連線方式連接網路的設備」皆可視為 IoT 裝置，圖 1 將可簡易的表達 IoT 的概念。而 IoT 的目的是為了「透過將真實的物體聯結上網，以達到控制、分享、分析及應用」。

圖 1. IoT 概念圖(圖片來源：http://www.business2community.com/)

三、物聯網設備特性及面臨風險

有鑑於 IoT 的設備特性讓 IoT 能逐漸的蓬勃發展，但也同時間出現相關的風險，也逐漸的造成威脅，因此下列將分別說明 IoT 設備的特性及 IoT 設備面臨的風險。

IoT 設備的特性

1. **成本低廉**：IoT 設備多為單一功能之設備，因此在製作成本上相對低廉。
2. **可高度客制化**：IoT 設備通常為單一機板加上附加功能元件所組成，可針對不同需求進行客制化。
3. **應用層面廣**：IoT 設備的應用層面廣，如運輸物流、健康醫療、智慧環境或公共教育等應用。
4. **數量眾多**：綜合上列特性，因此 IoT 設備可預期數量眾多。

IoT 面臨的風險

1. **系統更新及漏洞修補不易**：IoT 設備通常會以公板方式客制化生產，且生產數量眾多。因此當發現 IoT 系統有問題或是存在漏洞時，往往需要使用者進行手動修補，有時可能面臨無修補程式可供修補的狀況。
2. **安全認證問題**：IoT 設備為能連接網路及控制設備，因此除了有線網路介面外，可能還有像藍芽、無線網卡等介面。但有時因成本考量，可能使用較舊規格的產品進行設計組成，而這此舊有規格產品所使用的安全認證可能較為簡易或存在漏洞，此時可能面臨有心人士透過這些不安全的通訊協定來進行入侵動作。
3. **遭受非法應用**：當一種 IoT 設備遭到破解入侵後，因 IoT 設備的特性意謂著採取相同設計或硬體的設備皆存在於此風險中。而當有心人士取得足夠數量的 IoT 設備之控制權限後，將可進行相關非法應用，如

殭屍網路(Botnet)的組成、分散式阻斷服務攻擊(distributed denial-of-service attack, DDoS)的攻擊及挖礦(Mining)的應用等。

4. **連接埠安全**：IoT 設備通常會內建一些方便管理的功能，這些功能會有特定連接埠。然而一些管理裝置所用的連接埠，可能因為通訊協定本身的問題或是設定上的不良，導致駭客很容易透過這些連接埠來入侵這些設備，來進行上述的非法存取應用，或是用於入侵內部網路的跳板。

四、物聯網設備常見的連接埠

物聯網設備通常會開啟某些連接埠，來進行管理或是特殊應用程式的連線。但由於使用者可能未設置高強度密碼、協議本身漏洞或是設定不良，導致這些連接埠很容易遭到駭客入侵。以下是一些常見開啟的連接埠：

1. Telnet (Teletype)：Telnet 是基本管理協定，通常位於 23 連接埠，傳輸過程以明文方式，容易遭受到駭客攔截。建議關閉 Telnet 連線，並改以 SSH 連線，或是透過 IPSec 對連線進行加密。連線密碼也建議使用高強度密碼。
2. SSH (Secure Shell)：SSH 是常見的遠端管理協定，通常位於 22 連接埠，其連線過程都經過加密，許多 IoT 裝置都會內建。若是密碼設定不良，一旦被駭客入侵，駭客能完整操控設備。建議設定高強度密碼，如果裝置支援，可以改用憑證 (certificate)進行登入並關掉密碼登入，並限制連線位置，在特定網路下才能連線到物聯網裝置。
3. SMB/SAMBA：通常位於 405 連接埠，SMB 或是 SAMBA 可以透過網路，進行網路分享、資料傳輸等工作，但是目前有安全漏洞，可能會遭到特定漏洞攻擊。容易遭到駭客用來水平感染。建議不要使用 SMB 或是更新 SMB 至最新版本。

4. FTP (File Transfer Protocol)：FTP 能夠讓物聯網裝置進行檔案傳輸，連接埠通常為 21，然而 FTP 本身也未加密，容易遭到駭客攔截，也是駭客利用來傳遞惡意軟體的方式。建議設定高強度密碼、並關閉允許匿名登入。如果裝置允許，建議使用 FTPS (File Transfer Protocol over SSL，通常使用 21 連接埠)或是 SFTP (Secure Shell on File Transfer Protocol，通常使用 22 連接埠)。

五、校園常見物聯網設備及其可能面臨的風險

談到校園內常見的物聯網設備，大致可分為下列三項，分別敘述如下。

1. **印表機(事務印表機)**

現今的印表機及辦公室使用的事務印表機大部份都可以連網且有提供網頁服務供設定使用，於 2017 年 2 月因印表機使用之 Port 9100 遭利用，列印出勒索訊息之事件，及部份印表機提供網頁服務無管控設定，遭更換網頁等，皆是目前印表機常見的風險。

2. **網路攝影機(監控系統)**

目前眾多網路攝影機可能使用公板及共用系統進行建構，於 2016 年 9 月時因攝影機遭入侵造之 Mirai Botnet 形成，之後造成全球性 DDoS 攻擊盛行。其原因在於網路攝影機使用之後端連線服務預設開啟，且使用預設帳密，更因系統限制無法修改預設帳號密碼，僅能透過韌體更新方式關閉後端連線服務。另外，因網路攝影機本身即是提供監控服務，且多數皆有提供網頁服務。在未修正預設帳密的狀態下，可藉由網頁服務來取得監控端影像，造成環境資訊外洩的可能性。

3. **網路附加儲存設備(Network Attached Storage,NAS)**

因為資料備份的需求，有越來越多的學校添購 NAS 設備以因應其需求。而當 NAS 設備安裝上線時，針對預設帳號密碼未進行相對應的

處理，因此可能遭有心人士取得內部資料。同時因 NAS 系統本身可能存在相關漏洞，因此亦需定時檢查更新，以修補相關漏洞。

六、OWASP IoT TOP 10

下列表格是 OWASP(Open Web Application Security Project, 開放網路軟體安全計畫)組織針對物聯網裝置安全問題進行統計，歸納出物聯網常見的十項安全性問題，下面將會對各個問題逐一解釋。

表 1. OWASP IoT TOP 10

編號	說明
I1	Weak, Guessable, or Hardcoded Passwords (弱密碼、可猜測密碼或裝置預設密碼)
I2	Insecure Network Services (不安全的網路服務)
I3	Insecure Ecosystem Interfaces (不安全的環境設定介面)
I4	Lack of Secure Update Mechanism (缺乏安全的更新機制)
I5	Use of Insecure or Outdated (使用不安全或已遭棄用的組件)
I6	Insufficient Privacy Protection (不充分的隱私保護)
I7	Insecure Data Transfer and Storage (不安全的資料傳輸和儲存)
I8	Lack of Device Management (缺乏設備管理)
I9	Insecure Default Settings (不安全的預設設定)
I10	Lack of Physical Hardening (缺乏實體安全強化)

I1 - Weak, Guessable, or Hardcoded Passwords

使用過於簡單的密碼，或是裝置預設的密碼，將會導致駭客非常容易猜測到裝置密碼。一旦駭客登入裝置後，便能全權控制裝置。建議更改預

設密碼並確認密碼強度。

I2 - Insecure Network Services

使用有安全疑慮的網路服務(例如：telnet 或是 ftp)或是有不需要的服務都會成為駭客入侵入口的風險。建議確認網路服務的必要性以及避免不安全的網路服務。如果仍需保存具有風險的網路服務，建議利用 IPSec 等方式進行額外保護。

I3 - Insecure Ecosystem Interfaces

使用不安全的介面連接設備，例如網頁 API 控管不當、缺乏有效認證機制或是連線偽進行加密等。這些會導致駭客利用這些管理相關服務，間接控制物聯網裝置。建議加以管控 API，並設置完善的存取控制。

I4 - Lack of Secure Update Mechanism

物聯網裝置可能缺乏更新機制，一旦使用的軟體有安全性漏洞，將無法自動修補，導致駭客可以利用已知的漏洞入侵設備。建議管理者定期去官方網站檢查是否有新的韌體更新，或是手動更新有漏洞的軟體，如果裝置廠商不再提供更新檔，請考慮汰換或是透過存取控制來限制漏洞服務。

I5 - Use of Insecure or Outdated

使用不安全或是過時版本的原件庫或是開發工具，提供駭客入侵的管道。建議使用者將元件或是程式庫更新到最新版。

I6 - Insufficient Privacy Protection

物聯網裝置會儲存一些個人機敏資訊，如果沒有妥善保存，可能會導致這些機敏資訊遭到洩漏，建議將機敏資料加密並加以限制存取對象。

I7 - Insecure Data Transfer and Storage

機敏資料在傳輸的過程中未加密(如：telnet、ftp)，駭客可以透過中間人攻擊，導致機敏資料外泄。建議使用具有安全性以及加密的協定，如：SSH(Secure Shell)或是 FTPS(FTP on SSL)等。

I8 - Lack of Device Management

物聯網裝置缺乏管控機制，導致使用者無法有效監控系統、流量以及更新等。建議使用者在放置物聯網裝置的環境下，架置監控系統來管理物聯網裝置。

I9 - Insecure Default Settings

物聯網裝置出廠時會有預先的設定，讓使用者能夠輕鬆使用，然而這些設定可能過於簡易或是設置不良，讓駭客有機會能夠透過不安全設定來入侵設備。建議使用者購入物聯網裝置後，依照所部屬環境進行最佳化設置。

I10 - Lack of Physical Hardening

物聯網裝置通常十分簡便，沒有內建防護機制，讓駭客能夠輕易地對設備進行攻擊。建議在布有物聯網裝置的網路架構中架設防火牆等實體防禦設備，降低物聯網被攻擊的風險。

七、物聯網防範應變機制

針對 IoT 設備所面臨的風險，可利用下列要點建立防範應變機制，如圖 2，以降低其受害風險。

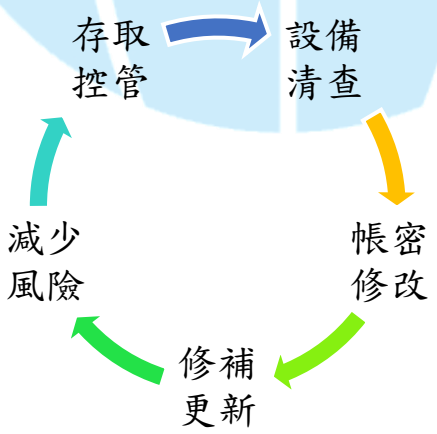

圖 2. IoT 防範應變機制

1. **設備清查**：清查單位內相關連網設備，並建立設備清冊，以了解單位

內設備分佈之狀況。同時可利用外部服務進行確認作業，如 Shodan，內部確認可利用 Nmap 軟體協助，相關操作可參考附件一、物聯網設備清查操作手冊。

2. **裝置管理**：將物聯網裝置以獨立網段輔以防火牆控管。或是利用 Software Defined Network 特性，集中管理物聯網裝置。

3. **帳密修改**：IoT 設備皆有通用預設帳號和密碼，出廠後需要由使用者進行修改，但通常使用者可能忘記修改造成安全風險。建議如預設帳號可停用的情況下，停用預設帳號並建立新帳號使用，如無法停用至少需變更預設密碼，以避免帳號猜測攻擊。

4. **修補更新**：IoT 設備亦需進行修補更新作業，以達到漏洞修補及系統更新的目的。如設備本身有自動更新功能，可開啟自動更新以即時更新。如需手動更新，建議每月至少需檢查是否有相關更新，或於重大漏洞被公佈時檢查。

5. **減少風險**：IoT 設備及提供的服務應遵循"最小權限原則"，減少可能被攻擊的面向。關閉未使用之端口，設備如非提供公開服務使用，建議將其網路設定轉為內網設定或將其網路匣道(Gateway)移除，以降低外部直接存取該設備之可能性。

6. **存取控管**：針對 IoT 設備之存取進行相關控管，如 IoT 設備本身有相關存取控管機制者，可以設備本身進行相關設定。反之無相關機制者，可於單位前端網路設備如防火牆等，進行相關連線控管。

附件一、物聯網設備清查操作手冊

當進行設備清查時，使用人工方式逐一清查是最佳的清查方式，但清查過程需耗費較多的人力與時間，同時可能會有產生遺漏的狀況。因此可透過相關服務及工具來協助進行清查及確認，以確保清查結果的可靠性。此次利用 Shodan 服務加上 Nmap 工具來進行確認作業，下列為相關說明及操作方式。

一、Shodan 的介紹與語法

使用此網站搜尋功能需先註冊，官方網址:https://www.shodan.io/explore。Shodan 為基於物聯網的搜尋引擎，類以 google Search ，可搜尋到所有連接至 internet 的網路設備(其中也包括物聯設備)，要特別說明的一點是 Shodan 是以定時爬蟲的方式取得相關資訊，所以其資訊可能不是當下即時資訊，使用者必需再次確認。建議可利用表 2 的 Shodan 搜尋語法來更精準的取得設備資訊。

表 2. Shodan 搜尋指令說明表

保留字	說明
net	設定要搜尋的 IP 範圍,EX: net:8.8.8.0/24
country	設定要搜尋的國別,EX: country:TW
City:	設定要搜尋的城市別,EX: city:Taipei
Port	設定要搜尋的通訊埠 EX:port:23
os	設定要搜尋的作業系統 EX:os:linux
product	設定要搜尋的產品名稱 EX: product:FUJI
version	設定要搜尋的版本 EX: version: 2.0
hostname	設定要搜尋的網域名稱 EX: hostname:edu.tw

二、工具操作範例說明

下列以搜尋特定通訊埠或廠牌的兩個情境來說明工具操作流程。

(情境一)搜尋有開啟通訊埠為 23 的 IP

1.以 net:[單位 IP 範圍] port:23 來搜尋即可取得在範圍內有開啟埠 23 的 IP，並取得下列資訊，如圖 3 所示。

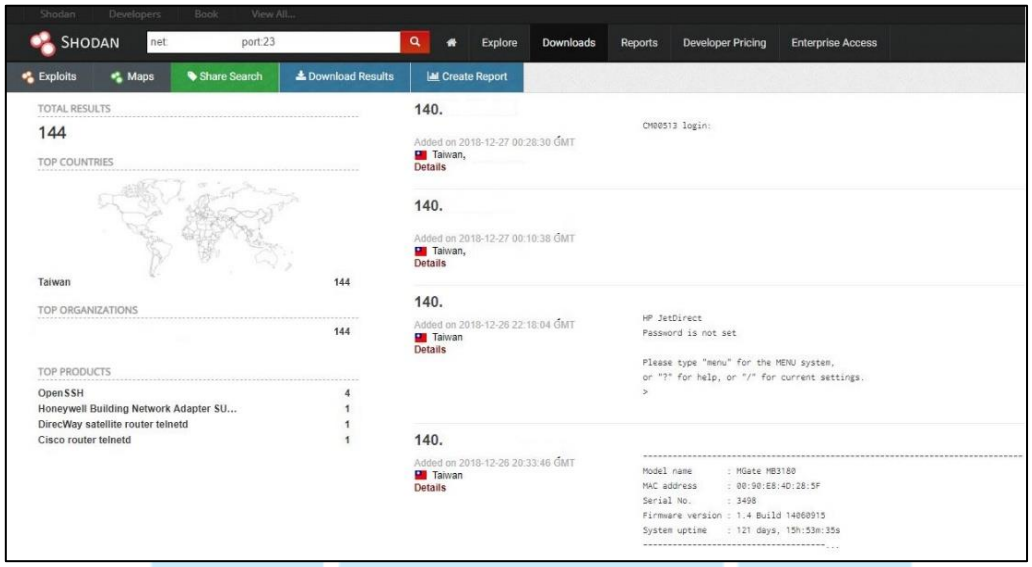

圖 3.使用 Shodan 搜尋有開啟通訊埠為 23 的掃描結果

2.隨機點選一台的詳細資訊（Details），發現該台為 IP 印表機如圖 4 所示。

圖 4.其中一台掃描結果的詳細資訊

3.再以 Nmap 於內部確認目前該台主機之 23 埠及 9100 埠是否開啟(圖 5 為確認開啟)

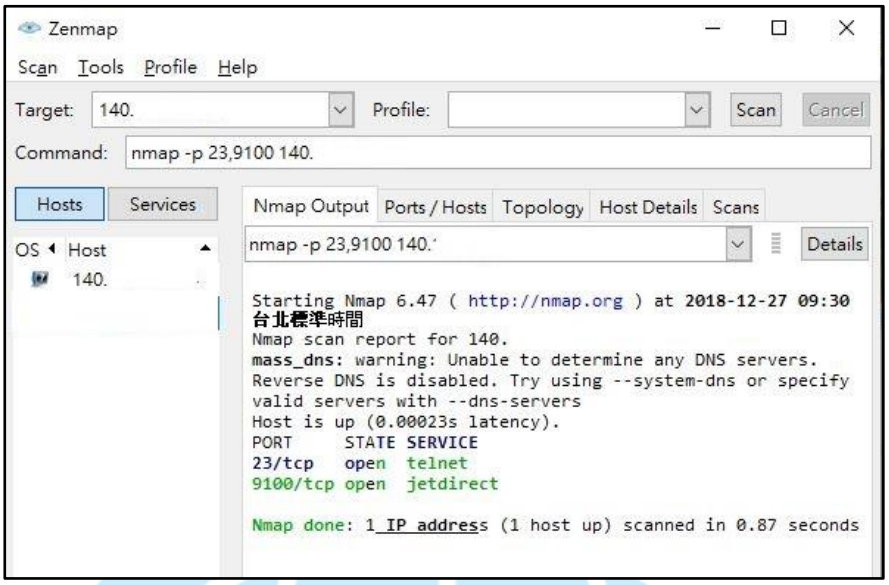

圖 5.以 Nmap 再次確認的結果

(情境二)搜尋產品為 FUJI 的主機

1.以 net:[單位 IP 範圍] product:"FUJI"來搜尋即可取得在範圍內，為 FUJI 產品的主機，如圖 6 所示。

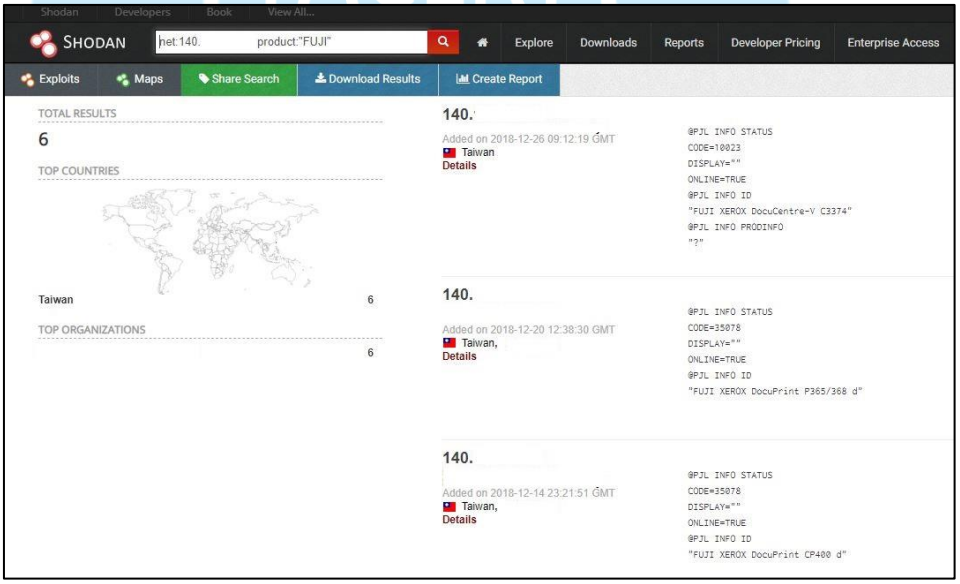

圖 6. 使用 Shodan 搜尋網段內含有 FUJI 產品的掃描結果

2.以 Nmap 再次進行確認。