◎資通安全宣導

—誰在看著 你家客廳?—

「物聯網」(IOT, Internet of Things)簡單來說，就是將日常生活物品嵌入感應器及晶片，使該等物品能透過網路被遠端操作或自行感知主動運作，以提供人類生活更多的便利性。由於嵌入的感應器能感知許多狀況，且晶片能智慧判斷，故這些物品已衍生出各種更貼心的緊急救護等加值服務。

⊙食衣住行「萬物皆可上雲端」操作

近年各類家電及交通工具等日常生活用品，總是愛冠個「智慧型」或「雲端化」, 讓愛潮流的人們趨之若鶩。這些「智慧型」東西好不好用是一回事，然已讓以往只在個人電腦上才會發生的中毒、受駭事件，蔓延至各種家庭用品中。目前智慧型手機的普及，已成功地讓民眾不分男女老幼習慣地將自己的生活日常大小事皆委由手機處理，但也讓每個人輕易地將個人基本資料、私人相片、金融資料等等私密訊息，曝露在網路環境之下。「物聯網」時代來臨，所生產的產品，更強調具備智慧操作及連網功能。我們當然可以相信商品文宣上所宣稱的美好遠景，但也不可輕忽「物聯網」所帶來的更駭人聽聞的資安犯罪問題。 例如圖 1 之左中圖所示，在個人健康照顧(Healthcare)領域中，有各種手錶、衣帽等穿戴式裝置記錄個人健康資訊，可在發生意外等緊急狀況時自動通知救護車；在家中，則可用於喇叭、冷氣機、嬰兒監視器等。右中圖的自動化駕駛(Transportation)，亦充滿著美好遠景，現已有特斯拉等公司將自動化的電動車商品化。

⊙潛藏在「物聯網」中的魔鬼

「物聯網」有數不清的好處，但也更大的負面風險，原因就是「物聯網」設備的「數量」及「種類」過多，這也是「物聯網」時代的資安問題遠大於 PC 時代的主因。

現將「物聯網」的資安問題分析如下：

一、 資安攻防有個術語叫攻擊面(attack surface)，攻擊面越小的系統，其安全性越高；而「物聯網」的特色就是設備又多又雜，讓攻擊者在攻擊「物聯網」相關系統時擁有極大優勢，造成「物聯網」之資安風險難以克服。

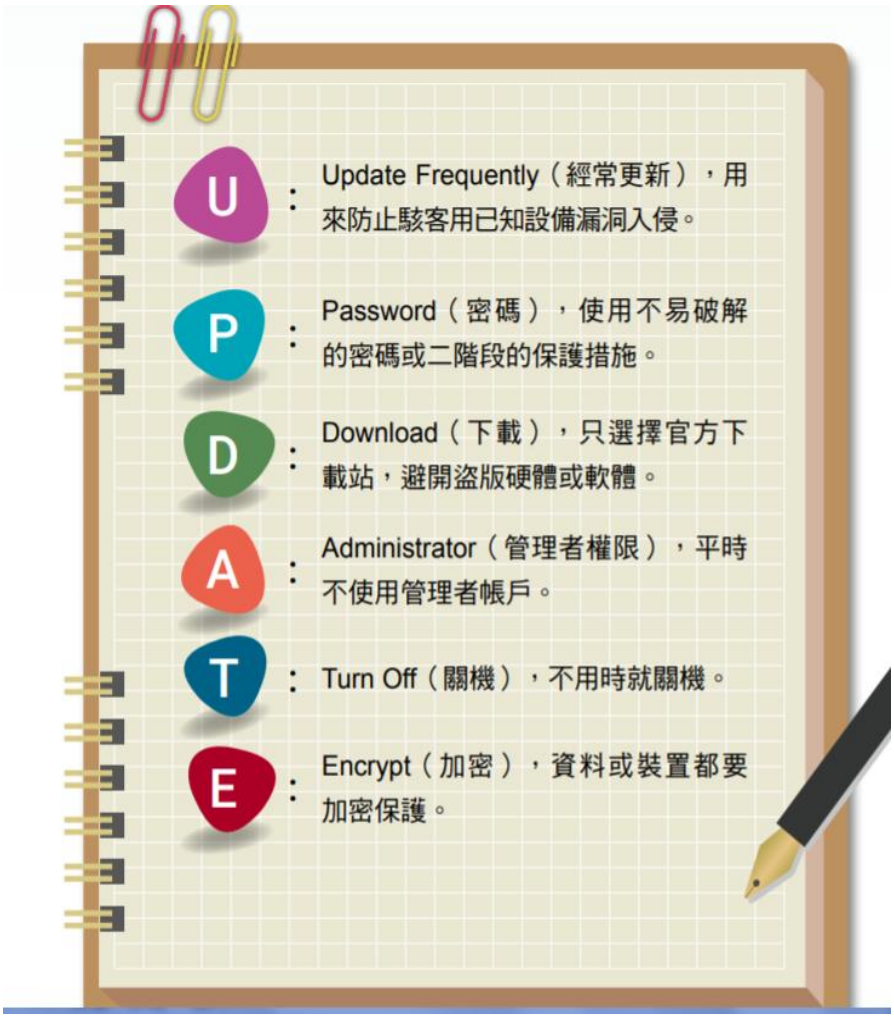
二、 資安領域有個「水桶理論」，即整個系統的安全性取決於最低安全程度的設備。「物聯網」的應用常常需結合數種設備：如手機遠端居家監控應用，需要結合監視器、監視設備主機、路由器、手機等等不同設備，任一環有資安問題發生，就會導致整個監控系統曝露於風險之中。

三、 「科技始終來自於人性」，Nokia 的一句帶著人文味道的廣告詞，同樣也適用於駭客犯罪，因為「漏洞始終來自於人性」，「物聯網」設

備結合數種裝置，只要有任一裝置的使用者輕忽裝置安全措施的設定，就會讓駭客有機可乘。

⊙ 無法停止轉動的時代潮流

這是個群眾極易被科技推動的時代，我們無法抗拒這波「物聯網」潮流的到來，只能去適應並找出生存法則與之共存。馬克・古德曼（Marc Goodman）所著的「未來的犯罪」(Future Crimes）一書中即探討「物聯網」所帶來的各種未來犯罪型態。下引述該書所提供之「UPDATE」口訣予進 入「物聯網」時代的人們，明瞭如何簡單保護自己的方式。期盼各位讀者在盡享「物聯網」時代便捷的同時，亦能充分保有自己的隱私及資料安全。這是個群眾極易被科技推動的時代，我們無法抗拒這波「物聯網」潮流的到來，只能去適應並找出生存法則與之共存。馬克・古德曼(Marc Goodman)所著的「未來的犯罪」(Future Crimes）一書中即探討「物聯網」所帶來的各種未來犯罪型態。下引述該書所提供之「UPDATE」口訣予進入「物聯網」時代的人們，明瞭如何簡單保護自己的方式。期盼各位讀者在盡享「物聯網」時代便捷的同時，亦能充分保有自己的隱私及資料安全。



臺中榮民總醫院關心你也提醒你！