物聯網的資訊安全

◎魯明德

網際網路的出現，不但改變人與人的溝通模式，也改變了以往的商業模式。雖然有這麼大的改變，然而，在這個時期，人與人、人與資訊間的互動，大多還是以人為主體。而今資訊內容已無法滿足快速多變的環境，我們開始把網際網路應用到日常生活中，一旦生活周遭的物品可以上網，使用者就能利用行動裝置對它們進行遠端遙控。

當人與物之間的互動少了人為的操控，變成物體間可以自行溝通、運算、執行，而能達成我們要求的結果，則是一個物聯網（Internet of Things, IoT）的形成，也是智慧生活的概念。當溫度感測器偵測到室溫到達 28℃時，自動通知窗戶關閉、冷氣打開，這樣的生活豈不善哉？

科技新貴小潘也看到這個商機，基於對資訊的專業，他想到另一個問題，當所有的物品都可以透過有線或無線網路相連時，如果在資料的傳輸過程中遭到竊取或竄改，豈不是天下大亂？於是，小潘趁著新春期間的師生下午茶約會中，跟司馬特老師討論這個議題。

司馬特老師喝口咖啡後，就回應小潘提的物聯網議題，在維基百科中的定義，物聯網就是像家電一樣的物體網路，所以它是機器之間（Machine to Machine, M2M）的網路；而機器可以是廣義的機器，也可以是一個小感測器。惟不論是機器或感測器，面臨的資安問題都是一樣的，如果資安問題沒有處理好，物聯網要普及是不容易的。

物聯網所連接的機器，可以是電冰箱、冷氣機等大型家電，也可能小到是窗戶或門上的入侵感測器，所以在安全機制上，首先要有一個安全的啟動制，從電源接上的那一刻起，就要先透過數位簽章進行驗證，以確認該裝置上的軟硬體是否為真、沒有被竄改；設備上的軟

體經由數位簽章與設備進行驗證，確保是原來授權的軟體，以免不法軟體入侵。其次則是要做存取控制，裝置在安全啟動之後，作業系統會根據既定的權限規則，對網路上的機器進行存取控制，讓它們只能依預設的權限被驅動，並使用完成工作所需的資源。任一個元件如果被惡意竄改後，想要做出超出權限的工作，存取控制就是一種損害控管的機制，讓入侵者即使能成功侵入，但對系統的存取權限只能達到最小程度，受損的資訊也會被限制在那些認證資訊授權的網路中。

小潘聽到司馬特老師的說明，也有了頓悟；接著問：前面談的都是機器本身的安全機制，至於整個網路是否需要什麼安全機制來配合呢？司馬特老師喝口咖啡繼續說，物聯網是在現有的行動網路上，整合感測網路與應用平臺所合成的，所以行動網路上的認證、加密機制，都適用於物聯網上。在傳統的網際網路上，網路層的認證是負責網路層的身分認證，應用層的認證就負責應用層的認證，各自負責自己的工作。但是，物聯網上所使用的裝置，應用系統與網路通訊通常是緊密結合在一起，網路層的認證是必要的，應用層的認證則可視需要決定是否認證。

當物聯網上的應用服務由電信業者提供時，資訊的傳送已在網路層經過認證，應用服務即可利用這個認證，不需再進行應用層的認證。當物聯網的應用服務由第三方業者提供時，因為無法從第三方業者獲得金鑰等安全參數，這時就可採取獨立的應用層認證，不用考慮網路層認證。如果應用服務是對安全需求更高的產業，如金融業，則網路層的安全認證可能無法完全滿足業者的安全需求，這時將會採取更高等級的應用層認證。除了認證之外，在資訊傳輸的過程中還是需要有加密的機制；在網際網路上，網路層的加密方式是在每個傳輸節點上不斷進行加、解密，應用層的加密方式則是點對點的。業者可針對傳輸資料的重要性，考量營運成本，選擇採用那一種加密機制確保安全性。

小潘聽完司馬特老師的一番說明，對物聯網的安全機制有了深一層的了解，資訊安全不是物聯網的附加功能，而是物聯網裝置能否可靠運作的一個重要因素，必須從裝置本身及網路兩方面都做到安全、可靠，物聯網才會有明天。華燈初上，這個月的師生下午茶又接近尾聲，小潘帶著滿滿的收穫，踏上回家之路。