從萬物聯網談資訊安全

◎蔡一郎

網際網路發展至今，已是無處不連網的時代，我們隨時可透過網路的連結，取得所需要的資料。物聯網（IOT, Internet Of Things）是近來熱門的話題，配合巨量資料以及行動通訊的發展，透過網路際網與傳統的電信通訊，提供了資料的傳輸與交換，也讓所有連上物聯網路且可以被獨立定址的設備，建立成一個龐大的資訊網路。其中許多的裝置或設備可以在運作的過程中，自動地產生資料，並與其他的裝置或設備進行資料的傳輸或交換，其間人類已不再是唯一會產生資料的來源；人工智慧配合自動控制，已演變成物聯網路中的智能控制系統，用以因應裝置或設備的功能或是所在的環境。智能控制系統早期應用於智慧家庭、智慧建築等，現在更擴大成為智慧城市，而物聯網則讓原本地理上的邊界更為模糊。現今雲端服務架構的成形，已成為目前資訊服務的主流，各種私有雲、公有雲以及混合雲的發展，讓一般使用者更容易透過網路取得各式各樣的應用服務。

物聯網路與雲端應用服務已緊密結合，其中許多針對性的網路威脅，尤其對於政府單位或是大型企業形成了巨大的資安威脅。持續性的進階滲透威脅（APT, Advanced Persistent Threat）攻擊是目前最常

見的手法，攻擊者除利用資安分析的工具，例如：Kali Linux、Meltego 等現有的工具之外，也常見到自行開發成專屬或是客製化的攻擊工具，持續地對攻擊目標進行探測、分析、滲透。遭受攻擊的對象除了一般的使用者之外，也包括系統的管理者；在過往的幾個資安事件中，不難發現許多入侵的管道，是組織或企業對外服務的業務窗口，一封與業務相關的釣魚郵件，就足以讓整個安全防禦的架構瓦解。

行動化通訊的時代，帶來新的資訊安全議題，從 BYOD（Bring Your Own Device，攜帶自己的設備辦公）對組織或企業在資安管理上的衝擊來看，雖然組織或企業本身可以降低初期投資於設備上的成本，但對於後續的配套措施卻較為薄弱；當員工把設備帶進工作的場所後，接觸組織或企業內部機敏資料的機會大增，因為傳統的資訊安全管理方式，大多數未跟上時代的轉變，員工仍可使用合法的登入帳號、密碼，透過這些資安風險較高的設備連上內部的網路，而這些類型的設備大多數具備自主的通訊能力，可以透過 3G、4G 的電信網路或是接取公共的無線網路，此對機敏資料的保護邊界已造成影響。

目前物聯網路的設備，除了傳統的通訊方式之外，也已發展出可在物聯網設備彼此涵蓋區域範圍內的通訊方式，例如：FireChat 等，這類型的應用可以不需要透過電信服務商的網路環境或是無線網路

的提供，就可以透過彼此設備之間的無線訊號，例如：WiFi、Bluetooth 等訊號，構築成一個接近點對點（P2P, Peer-to-Peer）的通訊方式。在以往幾次的社會運動中，我們可以看到這些新興通訊方式對於傳統資通訊架構的挑戰，在群眾聚集的區域，彼此之間可以透過這類型的通訊方式，仍然可以傳送訊息；當然離開了裝置與設備聚集的區域，還是得利用網際網路才行。未來只要使用者的人數夠多，也許有機會在都會區建構出一個不需要傳統網路就能傳送訊息的方式。

目前許多提供物聯網路服務的供應商，大多採用虛擬化與分散式的服務架構，可依據使用者或裝置所在地點，提供適地適時的客製化服務，因此對於服務供應商而言，如何強化本身在雲端服務環境中的安全防禦，間接地成了保護物聯網的重點之一，其中對於隱藏其中的 APT 攻擊，則是重要的防禦重點，因為一封與受攻擊員工業務相關的電子郵件，就有可以成為入侵層層防護下的重要管道。至於內部對外的行為分析，以往可以不如分析外部對組織內進行的攻擊活動重要，但時勢所趨之下，目前內部網路環境的異常通訊，往往成為追蹤網路攻擊的重要參考資料，畢竟攻擊與防禦的技術，兩者的重要性是相對的。

雲端安全聯盟（CSA, Cloud Security Alliance）目前已開始重視物聯網對於雲端服務造成的安全問題，因此已著手發展相關軟體定義防禦邊界（SDP, Software Defined Perimeter），透過物聯網設備間所建構出來的通訊環境，類似 FireChat 接近點對點的通訊架構，配合控制與資料分流的設計，期望能打造一個可以自主定義的物聯網環境。在目前走向軟體工程的世代以及因應個人化服務的時代，許多網路服務的提供方式，因應上述兩個趨勢已有所轉變，我們可以更容易與便捷地在終端裝置上使用網路應用服務，也可以快速地進行金融上的交易等，這些都有賴防禦邊界建置的完成。從使用者端的應用軟體對資料的處理開始，接著考慮不同裝置間的通訊安全，以確保資料在傳輸過程無法遭到側錄與竊聽，再者評估資料儲存的方式以及對於資料安全上的防禦機制，以達到就算資料遭竊仍然無法解開其中的內容。

裝置端的安全防禦目前是發展的重點之一，從 Google 投入生物識別技術及行動裝置加入指紋辨識的裝置開始，都顯示未來在物聯網路中，如何識別一個合法的使用者，對於安全防禦邊界的建立是相當重要的；可以改善傳統上單純使用帳號、密碼登入網路或存取資料的方式，增加使用者或裝置在存取資料上的識別度；而在裝置上開始採用非 WiFi 或是傳統電信網路的通訊方式已是目前的趨勢，我們不難

從 Apple 開始採用 iBeacon 技術、Google 開始推 Nearby 技術就可以略知一二。

行動裝置、雲端服務加速了物聯網路的發展。物聯網世代下的資訊安全防禦，因應規模與架構上都與傳統的資通訊服務環境不同，因此對於物聯網裝置、設備、載具、通訊方式以及使用者族群的多樣化，對資安威脅而言更顯得困難與複雜，畢竟現階段的基礎設施仍然根基於傳統的資通訊環境，而在這之上所發展的服務架構，其開發已影響了原本的防禦架構。以傳統的資訊安全防禦為例：許多組織或企業，在網路安全的防禦上都會建置防火牆、入侵偵測系統等相關的資安設備，而這些設備在歷經殭屍網路的威脅之下，除了得轉變原本的防禦面向之外，還得因應與日俱增的新型態惡意程式所帶來的威脅，且要不斷進行特徵比對規則的調整，才能趕上目前惡意程式的成長速度。而物聯網路除可結合現有的資通訊環境之外，亦已發展出自主的通訊方式，這樣的改變直接影響了預先設立的防禦邊界，因此，面對物聯網所帶來的新興資安威脅，採用具有彈性以及客製化的防禦機制，已成為當下發展的重點。如何提供一個容易導入且操作簡單的防禦架構來因應由不同的裝置、設備所形成的物聯網路，成了最重要的課題之一，因此，雲端安全聯盟所推動的軟體定義防禦邊界的概念，若能配合不同的裝置與服務的屬性，進行客製化的架構調整，除可提供使用

者便利的使用之外，對於雲端服務供應商（CSP, Cloud Service Provider）而言，更能快速地配合使用者在行動裝置上的軟體或是物聯網設備上的運作系統環境，建構一個安全的物聯網路，以保護在物聯網路中進行交換的資料以及設備的安全。