◎資訊安全宣導

智慧型汽車須以無線網路與外界傳遞訊息，故易遭駭客入侵，因此須借助相關資訊安全機制來保護資料在無線環境中的傳送。

－汽車也需要資訊安全－

當智慧變成顯學後，市場上到處充滿以智慧為名的產品，諸如智慧型手機、智慧型家電……，這些都不足為奇，連國內某潮牌汽車都號稱自己的車是智慧車，好像沒有生產智慧的產品就是落伍了。在這股智慧潮流中，到底智慧是如何達到的？它有沒有安全上的風險？小潘在看到此一科技趨勢後，首先就想到資訊安全的問題，因為汽車是一種涉及人身安全的運輸工具，它的智慧如果是利用電腦來達成，那麼它的風險是否也會從電腦而來呢？

在這個月的師生下午茶約會中，小潘把這個問題提出來與司馬特老師討論；老師聽完小潘的問題，喝口咖啡娓娓道來。自從 Google 推出無人駕駛車，將大量的資訊科技運用在汽車上後，大家才發覺資訊科技竟然也能使用在汽車上，殊不知把電腦運用在車上其實已經很久了。

以前電腦在汽車上的應用，大多用在燃油控制及車輛的安全控制上，像電腦噴油、ABS 等系統上，這些系統因為各自獨立在車輛上，程式碼有限，再加上沒有與外界溝通，所以很少人會談及汽車的資訊安全。當汽車開始變智慧之後，它所嵌入的系統、軟體、硬體就越來越多，甚至連網路通訊都加入了，汽車簡直變成一部在路上跑的行動電腦。大家都知道，凡是經由電腦控制的系統，且能與外部網路相連，這個系統就有可能遭受駭客攻擊；而軟體系統或多或少都會存在安全漏洞，所以駭客就有可能經由這個漏洞入侵，進而達到遙控汽車的可能。

汽車內部的資訊系統是由多個晶片組藉網路所組成，當它要具有智慧時，就必須與外界的系統相連，例如需要判斷有沒有塞車時，它就要與外界的路況系統連結；怎麼連結呢？當然要透過無線網路，所以惡意程式就可能透過這個管道進入汽車上的資訊系統。

小潘聽完非常震驚，因為現代汽車的驅動、煞車、轉向等各種系統都已經由電子自動控制，這些控制系統都是藉由駕駛透過手、腳下達指令，經過車內的電腦系統與網路來完成的；因此，駭客可透過各種途徑入侵，進而對其進行控制，就能對汽車做出攻擊。這些情節目前只出現在電影中，但未來有可能在實體世界中發生。

老師非常認同小潘的想法，喝口咖啡接著說下去。汽車資訊安全會變得越來越重要，除了嵌入式軟體外，也與技術發展的趨勢密不可分。除了汽車原廠所提供的功能之外，車主從零件市場上購買並安裝在車上的周邊產品種類也越來越多，安裝這些產品的同時，來自外部的病毒等威脅也有可能藉由這些管道進入車載系統。

小潘聽到這裏，馬上想到國內某潮牌汽車的車電系統，號稱跟國內某智慧型手機廠合作，透過特定的智慧型手機，就可以跟車上的系統相連，甚至於做到資訊同步顯示；這時，如果智慧型手機已經被入侵，那麼智慧型手機本身就可能變成入侵的管道，這不是很可怕嗎？

老師繼續回應小潘的想法，美國參議員 Edward Markey 在 2013 年針對美國的車載資訊系統安全問題進行調查，發現現行車載資訊系統幾乎都具備無線網路的功能，但對於諸如駭客入侵及個人資料外洩等資安問題卻毫無防備與對策。

車載資通訊（Telematics）的應用，與傳統的無線網路服務一樣，存在著資訊安全的隱憂，它們的共同需求都是要借助相關的資訊安全機制，來保護資料在無線環境傳送中的隱私權、防止身分與訊息偽造、防止有心人士利用此網路從事竊聽和惡意攻擊。但兩者最大的不同點在於，車載資通訊是使用在高速移動的環境中，它的資訊安全機制必須在有效的時間內提供完整的服務，讓行駛中的車輛在所處車用網路範圍內，能夠享有資料交換的安全性與隱私性的防護。

為了車載資通訊系統的資訊安全，IEEE（美國電子電機工程師協會）特別訂定 IEEE 1609 的標準，在 IEEE 1609.2 的通訊協定架構中，就對應用層及傳送訊息封包的安全做了規範。它的身分認證是採用非對稱式金鑰產生數位簽章，電子憑證必須透過數位簽章才能發送。傳輸中的加解密則是由兩個步驟來完成，由於對稱式金鑰的運算速度比非對稱式金鑰快，所以對於資料量大的資料訊息，是透過隨機亂數產生的對稱式金鑰，以 AES-CCM 加密演算法來加密，並將該加密資料的對稱式金鑰，再用非對稱式 ECIES NIST P256 演算法加密，一併傳遞給對方。

在華燈初上之時，這次的師生下午茶約會也近尾聲，小潘仍細細咀嚼老師的話。科技是中性的，即使網際網路隨時隨地都有駭客在攻擊，但人們還是沒有辦法不用它。智慧車是未來汽車的趨勢，產業也不能不往這個方向前進，只要我們能夠確保相對的安全，科技還是可以讓我們的生活更美好！

（作者魯明德為科技大學資訊管理系講師）