Smart Mobility (4)：從「供應鏈管理」落實資安

以 Safety 爲依歸 用 Security 堆疊資安

■文：任芷萍

不論是自駕車或車聯網，「資安」都是首要議題；高度依賴資訊流驅動的交通、運作模式，若不幸訊號被竊聽、攔截或竄改，輕則蒙受財物損失、重則危及生命！

為消費大眾熟知的防毒軟體大廠趨勢科技 (Trend Micro)，其實觀察汽車領域已有五年之久。全球消費市場開發協理許育誠謙虛地說，當初他們雖不敢確切預言智能車演進的具體進程，但一直深信這是個極具潛力的市場。果然，在電動車 (EV) 興起後，人們對於汽車資安的關注度直線上升，包括安全 (Safety) 和保全 (Security) 兩方面；而被鎖定的攻擊目標也從車商轉變為車體本身——內網從 CANbus 下手，外網以閘道器 (Gateway) 為入侵門戶。再者，過去資訊較隱晦、資安弱點不見得會被公開，也是近年汽車資安給人「旱地拔蔥」之感的原因。

照片人物：趨勢科技全球消費市場開發協理許育誠

汽車電氣化程度變高，「受駭」態勢隨之迅猛

許育誠回顧 2012 年，汽車「受駭」事件還只有個位數，但 2015～2018 年倏然陡增 200 多件個案，其中有一半的案例是與罪犯事件有關；驚人的是，今年才剛過完第一季，就已高達 39 個案例是屬於資料盜取與車輛竊取！有實體 (physical) 和遠端 (remote) 兩種攻擊手法——前者多從車上診斷系統 (OBD) 的通訊埠入侵，後者又可再細分為短距、長距；毫無懸念，長距離駭客的影響更廣泛而巨大，有六大途徑：

1. 伺服器或數據橋接：充電樁／租借站側錄資料即屬此類，約 20%；
2. 被動無鑰進入系統 (Passive Keyless Entry and Start Systems, PKES)：透過「守株待兔＋盲掃」分工合作偷車，由於破解工具已經可以在市面上取得，目前此類攻擊比最大，約 33%；
3. ODB 之類的編／解碼車機：直接撤銷 (revoke) 車機原始金鑰，約 11%；
4. 手機應用程式植入後門，盜取金

鑰竊取車輛，約 10%；

5. 中控式車用資訊娛樂系統 (IVI)：從外部互聯網或內部匯流排侵入，約 8%；
6. 最後一種的類別則是屬於「附帶損害」(Collateral Damage)，主要是因為許多車內系統也採用一般通用的 Wi-Fi、藍牙、USB 及攝影機等不同系統。當這些系統被發現有漏洞，也意味著它們也存在於車內系統。例如，2017 被揭露的 KRACK WPA2 漏洞就是一個典型案例，此類附帶損害約 18%。

其中，PKES Relay 攻擊時有所聞，今年第一季全球已經有 22 起竊車案件都與 PKES Relay 攻擊有關，近日才又傳出經由共享汽車 APP 偷竊百輛賓士車的消息，空曠停車場尤易中標。許育誠說明，採用 PKES 的汽車會持續發出低頻訊號，即使靜止時也不例外；竊賊往往是兩人一組，一人專司聽取特定車型的低頻訊號，一人手持掃描裝置在停車場亂槍打鳥式的隨機尋找車主的遙控鑰匙所在，如果訊號對上了，負責掃描的人就會把訊號以高頻傳給守株待兔者，進行完美的 PKES 的 Relay 攻擊。這還只是單點襲擊，當汽車電氣化程度普及後，匯流排通訊、乃至聯網車 (Connected Cars) 需求亦逐漸增溫。

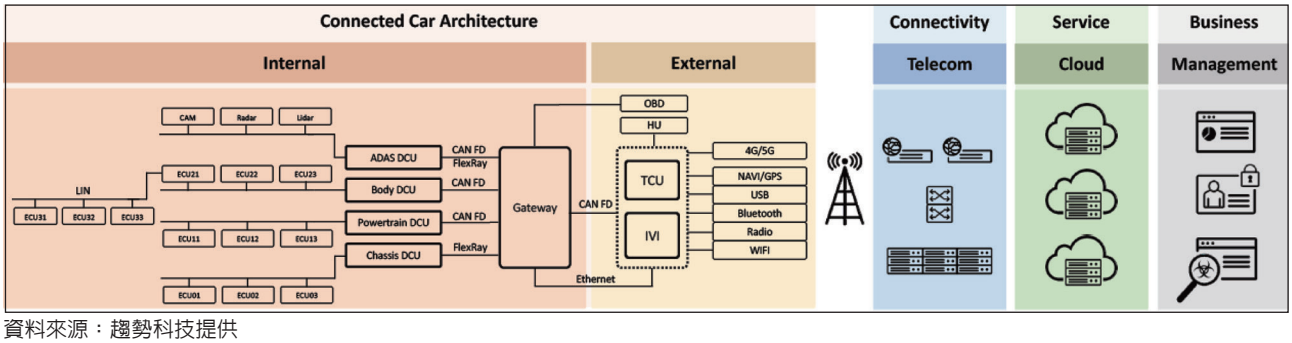
汽車聯網爲大勢所趨，供應鏈管理難在「稽核」

在汽車智能化的過程中，一樣存在資訊 (IT) 與操作 (OT) 的整合問題；而網路連接和底層通訊協定的增多，意味著所曝露的門戶和漏洞風險正悄悄升高且有擴散之虞。許育誠以 OBD 為例，早期車機裝置多自成封閉格局，但這樣「與世隔絕」(isolation) 作業環境因取得資訊有限，會造成診斷、除錯盲點，有必要藉由連網將來自於內、外部的所有行車記錄檔 (Log) 集中管理、並匯整為有意義的資料後外送，以協助判讀，但前提是得克服延遲 (Latency) 和檔案格式共通性；特別是自駕車須與「高精度地圖」緊密連動，對頻寬和運算力更是一大考驗。

為避免餵入錯誤資料而「誤入歧途」，GPS 導航裝置會有「防呆」機制 (例如，突然出現不尋常大轉彎導致跳動的線性軌跡變異過大)，此類「防呆」機制應該運用在其他的感測器上、而不是單純只做訊號傳送而已。另值得留意的是，取道 IVI 攻擊的佔比雖非最大，但威力不下於直接攻擊伺服器；若情節嚴重到需要召回 (Recall)，車廠損失將動輒逾百萬美元！因此，趨勢科技主張汽車資安應擴及零組件製造商，落實供應鏈管理 (SCM) 的稽核 (audit) 工作。不過許育誠提到，在他們與汽車工廠實際接觸時發現：「如何驗證出廠的產品沒問題」，是供應鏈成員心裡的一個痛點。

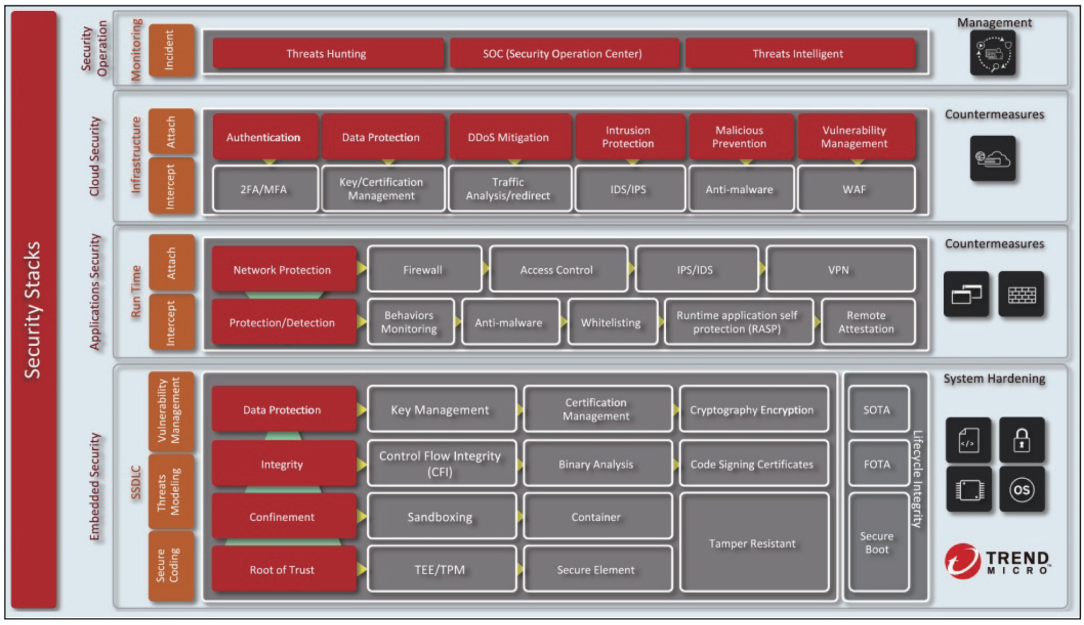
例如，在晶片廠商認知中，安全又好用的「可信賴平台模組」(Trusted Platform Module, TPM)，許多承包製造商 (OEM) 卻不熟悉編碼工程，無法稽核其供應商的產品是否達標？此時，通常只得全然信賴對方的自我宣告、或要求出具第三方驗證報告。有鑑於此，已有一些 OEM 自發成立聯盟，互相為援；另一個捷徑是加入可昭公信的既有生態系，趨勢科技與嵌入式系統大廠溫瑞爾 (Wind River) 的合作就是一例——將入侵防禦、URL 過濾和應用程式控制等套件預載於 Wind River Titanium Cloud，建構營運商等級的網路功能虛擬化

圖 1：聯網車之內、外部網路架構，與電信連接、雲端服務和商業管理息息相關



資料來源：趨勢科技提供

圖 2：趨勢科技在網路資安堆疊的佈局 (紅色區塊標示處)



資料來源：趨勢科技提供

(NFV) 基礎軟體平台。

Be Ready！有些機會，一旦錯過就不再

以「深度封包檢測」(DPI; Deep Packet Inspection) 為核心，結合入侵檢測系統 (IDS)、入侵預防系統 (IPS) 及狀態防火牆等功能，為前端、邊緣到核心網路提供各種網路安全。作為 Wind River Titanium Cloud 生態系統一員，趨勢科技事先進行測試和驗證，讓服務供應商和電信設備製造商 (TEM) 可借助 Titanium Server 放心選擇經過「預驗證」的軟、硬體產品。隨著溫瑞爾在各種垂直應用的深化（參閱：《緊扣人心，從來就不能只靠產品本身！》http://compotechasia.com/a/tactic/2019/0318/41325.html 一文），趨勢科技未來在自駕車等交通運輸網路的部署，亦可搶得先機。

「事實上，全球十大車商的 IT 資安皆是採用趨勢科技的解決方案；然而資訊安全威脅變化極大，我們最憂心的一件事就是一旦有新型態的攻擊出現，資安公司無法及時地提供解決方案來解決客戶的問題！所以，我們必須 Be Ready」，許育誠說。他表示，將 DPI 用於車聯網，則能探查車內異常行為；唯汽車由於未知太多，基於管理決策授權邏輯的「白名單」會比黑名單更適合確保通訊協定免受攻擊。此外，「機器學習」(Machine Learning) 是探究未知最好的工具，建置於電子控制單元 (ECU) 中，可「異中求同」，找出對汽車安全的重大影響因子。他還強調，「Security」應以「Safety」為依歸，意即：生命安全順位高於一切！

許育誠認為，這需要健全法規和整體環境的成全；而 SCM 是一種「Multi-layers Defense」(多層次防衛) 概念，當中每個環節皆鬆懈不得，將「Security」當作顯學的以色列堪為楷模，在設計之初就堅守這個鐵律；不只視為內建 (built-in secure) 的基礎功能，還力求持續可行 (keep-it secure)。目前有許多的車商在研究如何運用區塊鏈的技術於生產履歷上就是一個很好範例，在區塊鏈的技術上趨勢科技也已著手進行研究。他總結，當汽車產業日趨開放，IT 雲端與 OT 底層的對接與跨域流動是合理且必要的發展，而投入相關供應鏈的業者越見活躍，也代表市場越大。換個角度看，集眾人之力糾錯，防毒將更有效率，也能提升行車安全。

趨勢科技亦志在完善從嵌入式系統、應用層、雲端到營運的資安堆疊，可對車聯網提供多層的安全防護保障。CTA