智慧家庭 (4)：資安不容妥協

Infineon：智慧與便利不能以犧牲「安全」爲代價

■文：任芷萍

隨著智慧家庭與物聯網 (IoT) 掛勾，網路資安自然越發備受關注。誰都不想這個高度私領域被外人一覽無疑，更遑論可能因此損傷人身和財產。在汽車電子與大功率控制 (包括汽車動力系統) 表現不俗的英飛凌 (Infineon)，投入智慧卡與安全領域已 25 年，安全控制器的全球出貨量逾 200 億顆，亦是行動 M2M 通訊的先驅。英飛凌智能卡與保密晶片業務事業處經理田沛灝細數他們在的標竿里程碑：2014 年每十張發行的支付卡中，有四張是採用英飛凌安全晶片；全球有高達 75% 人口所持有的法定官方證照，皆是由英飛凌晶片驅動。

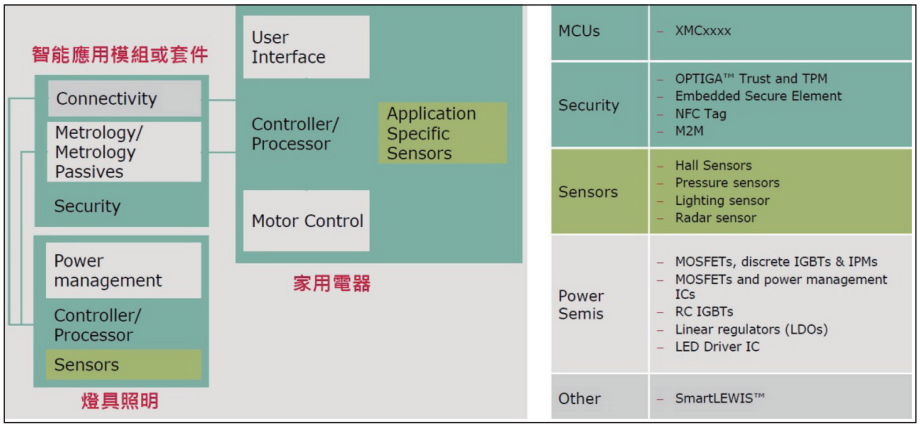
照片人物：英飛凌智能卡與保密晶片業務事業處經理田沛灝

嵌入式安全設計需求日盛

如今，英飛凌在認證、可信賴平台模組 (TPM) 和行動安全市場堪稱數一數二；每兩台可攜式商務電腦，就有一台配備英飛凌的 TPM。田沛灝表示，除了遵循 ISO 標準、用於支付／行動通訊／證照／交通／付費電視系統卡的開放式規格安全控制晶片，因應市場變化，英飛凌 10 年前開始發展多元通訊介面的「嵌入式安全」產品，包括智慧家庭應用；不過，嵌入式設計只是其中一個選項，採用標準 OPTIGA 安全晶片／ TPM、NFC 標籤以及 M2M 安全通訊模組亦是可行方案，端視用戶對安全功能的期待與規劃。

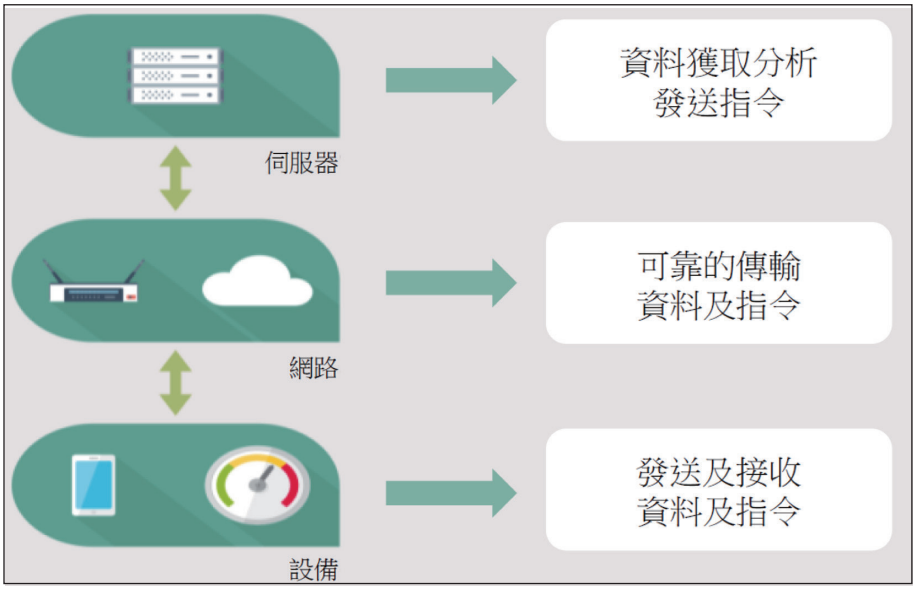
英飛凌認為，智慧家庭根本特性是「基於網路及其儲存資料執行動作」，包括：記錄並分析資料、即時監控和預警、遠端控制以及遠端更新等，須分別從伺服器、網路和設備三個層次來為資安把關。首先，位於最上層的伺服器可能因發送錯誤指令導致觸發意外事件，將非公開資料發送給非法接受方；網路傳輸資料或指令有被竊聽的風險，因而洩露關於基礎設施運行的資訊；最終設備可能被注入偽造資料、擾亂控制過程而做出危險或不當反應，或被用於掩蓋物理攻擊。「可惜，目前許多 IoT 並未正確選用對的安全機制」，田沛灝據實以

圖 1：英飛凌在智慧家庭應用的全方位解決方案



資料來源：英飛凌

圖 2：英飛凌主張，智慧家庭應分為伺服器、網路和設備三個層次來看



資料來源：英飛凌

告。

她進一步點明，智慧化有助提升產品獲利，可從發展新功能／服務、節能減碳與客製化著手；而在琳瑯滿目的智慧家庭設備中，「作為中繼站的閘道器 (Gateway) 最該優先實施高規安全措施，至少能為內、外網建立基礎防線」。田沛灝強調，智慧家庭的資安不容小覷；這不僅可能讓家電設備曝露在全天候被操控的風險中，導致產品過熱、經濟損失，亦會減少電器設備的使用壽命。若居家網路監控攝影機資料被偷窺、竊取或篡改盜用、家庭成員作息被不良人士瞭若指掌，後果將不堪設想！一旦公共能源設施被駭，更可能慘遭時基操縱而導致技術和社會問題。

MCU 外掛安全引擎，硬體安防較穩固

「換個角度，開發者或設備製造商只要多花一些心思在建立安全防護網上，包括：可靠度、隱私與安防，則可捍衛產品價值和研發機密，利於在競爭中脫穎而出、保障收益來源，同時增進品質、降低善後成本並拉長產品在市場上的活躍期間；甚至透過為產品加值、實現和創造新的業務模式而獲得超額利潤」，田沛灝說。那麼，怎樣的安全防護才合格？她指出，常見的安防措施有以下幾大面向：認證、金鑰建立和管理、平台完整性、儲存資料保護、安全更新、安全通訊、審計以及產品生命周期管理，尤以前兩項最為關鍵，軟、硬體各有必須留意的重點。

田沛灝舉例，早期磁條式金融卡只要一刷，就能獲得確切而完整的資料，容易被側錄；但後來進化到新型晶片卡，因為內嵌微控制器 (MCU) 會以演算法加密保護資料，且感應時只負責確認讀卡機的合法性、不會告知具體細節，阻絕被竊聽的機會，這正是為何改採晶片認證的緣故。其次，金鑰管理有「對稱式」和「非對稱式」兩種，前者加、解密都是用同一把鑰匙，如：DES、Triple DES、AES……；後者則是將加、解密看作兩把鑰匙，且公鑰 (public key) 最好集中保管在伺服器、取代放在晶片卡，必須與永遠存在本機的私鑰 (private key) 比對成功才能動作。

不難理解，非對稱式金鑰安

防等級相對較高。如果比對不上，收受方便無法進行後續動作，且該次傳送的資料可設定自我銷毀；但缺點是那個如同「超級保險箱」的伺服器，身價著實不斐。她並透露，歐洲因將電力能源視為國有資產，智慧電表至少會以晶片卡做安防；但台灣的電表走的是 AES 對稱式金鑰，保全概念仍有待加強。田沛灝直言，以 MCU 外掛安全引擎的硬體實現方式，安防功能自然較為堅固；但基於性價比考量，MCU 加軟體演算法、以韌體方式呈現也不失為一種解方，而將憑證與經過認證的安全平台綁定，將安全認證個人化。

OPTIGA 提供不同級別的安全機制

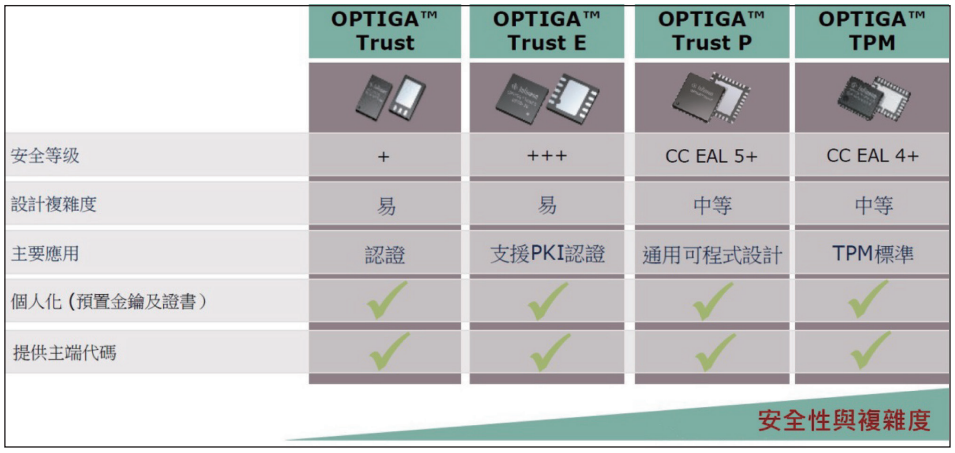
隨著 Amazon、Google 和 Apple 三大陣營招數盡出，時下開發者能運用的資源遠較以往豐沛許多，安防水準又是如何？田沛灝分析，Apple 素來堅持走自己的路、擁有特定支持者，對安防有較嚴謹的規範；Google 開始投入做硬體設備，有 OpenSSL 等明確的安全規範定義，仍不免傳出新併購 Nest 恆溫控制器被破解的消息；而近年因 AWS 限定期間免費雲端服務以及豐富開發套件而迅速擴張勢力的 Amazon，則以彈性與靈活度吸引意在速成者，但安全防護不具強制性，開發者須自行評估補強，而英飛凌 OPTIGA 系列可滿足不同安防需求。

田沛灝介紹，OPTIGA 現階段有四大產品線：入門款 Trust 僅供簡易認證，內置憑證金鑰，用戶可省下金鑰管理費用，又可避免先前有監視器業者因爆出漏洞、造成韌體被植入木馬的連環慘劇；Trust E 具備公開金鑰基礎建設 (PKI) 認證，採用橢圓曲線加密技術預先編程；Trust P 可產生並安全儲存加密金鑰，做單向及雙向驗證，防止惡意程式攻擊並控制存取，以保護軟體更新的安全性；最高階的 TPM 版本是基於「可信任運算集團」(TCG) 國際標準的獨立安全晶片，藉由在硬體內建置進階加密演算法，有效保護嵌入式系統的完整性與可靠性。

OPTIGA TPM 晶片已獲嵌入式系統安全專業廠商 Mocana 整合至該公司 Security of Things Platform 標準功能，安全密鑰、憑證和密碼皆被儲存在獨立於主處理器之外的 TPM 晶片，有效抵禦駭客攻擊、保護核心智財。「即使帳號與密碼都比對無誤，但平台仍有可能是假冒的！若誤導終端使用者錯連假平台登錄資料或更新程式，可謂後患無窮；而每個 TPM 的憑證都不同，就算極其不幸某一個設備遭到破解，也只限於那一個，不會禍及在外流通的成千上萬同類產品」，田沛灝最後如此提醒並總結。

英飛凌日前與中國合作夥伴在北京成立「智慧家庭聯網安全開放實驗室」，成員包括：美的智慧家居、華為消費者事業群、騰訊科技以及隸屬於中國工業和信息化部的中國電子技術標準化研究所；作為唯一外資企業的英飛凌，未來在智慧家電、乃至於搭載完整作業系統與使用者介面的運算裝置，如：閘道器、控制或娛樂系統，會有什麼突破式進展？能否在飛快成長的中國智慧家居市場搶得先機？姑且拭目以待。CTA

圖 3：英飛凌 OPTIGA 系列為智慧家庭提供基礎信任解決方案



資料來源：英飛凌