5G 智能邊緣肩負重任 嵌入式系統的資安怎解？

■文：任芸萍

5G 時代正式來臨！但眾所期盼的高頻寬、低延遲，恐將對物聯網 (IoT) 連接更具破壞力，網路即時檢測迫在眉睫。5G 資料中心需支援自動化和雲端技術，讓內容服務供應商 (CSP) 可透過加值服務做配置和管理，為用戶 IoT 設備提供在線安全保護，或由用戶自行控管帳戶中的 IoT 設備訪問權限。然而，5G 從集中式網路過渡到軟體定義網路 (SDN) 的過程，由於少了居中的網路監控檢查點，將使網路漏洞更加複雜；所幸，虛擬網路的「安全即服務」(SaaS) 平台可讓用戶遠端獲取安裝或更新，營運商亦可用機器學習識別、消除各種應用程式威脅。

ResearchAndMarkets 預估到 2025 年，全球 5G 安全市場總額將達 65 億美元，「基礎設施安全」是營收貢獻最高的分眾市場，達 25.6 億美元，而「通訊安全」是增長最快者，年複合成長率 (CAGR) 為 49.2%。5G 的另一個重要標記是邊緣運算 (Edge Computing)，結合物聯網、雲端和邊緣運算，保護在容器 (Container) 中運行的設備、應用程式和微服務的安全需求變得更加重要，而公鑰基礎結構 (PKI) 是有效且具有成本效益的方式，例如，以某種方式將身份綁定到密鑰、對某些內容進行身份驗證。這幾年，「私有路由 PKI」的需求正在激增。

Arm「PSA」：爲物聯網奠定平台安全架構

多數組織希望藉此明確限定誰能獲得憑證並控制設備，造成導入更多依「產品線」為單位的信任根 (RoT) 碎片。因為物聯網製造商並不想讓旗下設備與用戶其他 IoT 設備在相同的信任根上驗證身份；反之，多數用戶也傾向將不同設備予以適度區隔。著眼於物聯網碎片化特性，在邊緣設備市佔甚高的安謀 (Arm) 於 2017 年發表首個通用框架——平台安全架構 (PSA)，意在為萬物聯網奠定信賴基礎，讓 Arm-based 產品能在共同的安全基礎上互通，由分析、規劃 (設計)、執行和認證四階段組成，可提供具代表性的物聯網威脅模式及安全性分析。

圖 1：Arm PSA 四大階段

資料來源：https://developer.arm.com/architectures/security-architectures/platform-security-architecture；筆者整理

PSA 讓硬體與韌體規格皆可建構在關鍵安全原則的基礎上。特別一提的是：PSA 不受作業系統種類限制，可支援 Arm 旗下所有即時作業系統 (RTOS) 和 Arm Mbed OS 物聯網作業系統，以及軟體廠商夥伴的作業系統。其中，執行階段的三組 PSA API，可確保跨設備硬體信任根實現跨應用程式 (互操作性)，包括 RTOS 和軟體開發人員的 PSA 功能 API、安全專家的 PSA 韌體框架 API，以及晶片製造商的 TBSA API。Arm 還為其安全 IP 系列產品新增兩項元件：

- Arm TrustZone CryptoIsland：在晶片內部運行的智慧卡層級安全機制，CryptoIsland-300 為第一代解決方案，鎖定需要高層級分析與安全性的應用，包括低功耗廣域網路 (LPWA)、儲存及車用等；
- Arm CoreSight SDC-600 安全除錯管道：SDC-600 整合一個專屬的驗證機制用來除錯存取，支援完整除錯功能且不損及系統安全，在物聯網裝置的各個生命週期階段皆適用。

Arm 隨後在 2018 年推出首套 PSA 威脅模型與安全分析 (TMSA) 文件——考量哪些資產該受到保護？推測可能遭遇到的威脅？面向一些熱門物聯網裝置 (如：智慧水錶、網路攝影機、資產追蹤裝置) 發表新 TMSA 範本以及開源參考實作韌體「Trusted Firmware-M」(支援 Cortex-A 應用處理器)，從基礎架構到部署建置皆包羅在內；Arm 並設立專案軟體開發團隊，專門負責適合連結 MCU 的安全處理環境 (Secure Processing Environment, SPE)。解決了基本的資安結構問題，「合規性」是另一挑戰，尤其是面臨區域性法規的歧異。

GlobalPlatform SESIP：助力「合規性」認證

由安全數位服務和設備標準行業協會 GlobalPlatform 發佈的「物聯網平台安全評估計畫」(SESIP) 定義了可信賴評估 IoT 平台安全性和終端設備安全性的獨

圖 2：SESIP 五個保證級別、標記和定義

資料來源：https://trustcb.com/iot/sesip/；筆者整理

立認證標準，在提供合規性框架方面處於領先地位，涵蓋許多最佳實踐準則和法規要求，包括：美國 NISTIR 8259 建議、歐盟 EN303645 標準、英國針對消費者物聯網的法規建議安全性，以及俄勒岡和加利福尼亞 (SL-327) 物聯網安全和數據收集法律，讓最終用戶可循設備的獨立審核安全聲明作為選購依據，設備開發人員亦可借助預先認證的組件，經濟高效地滿足安全要求並加速上市。

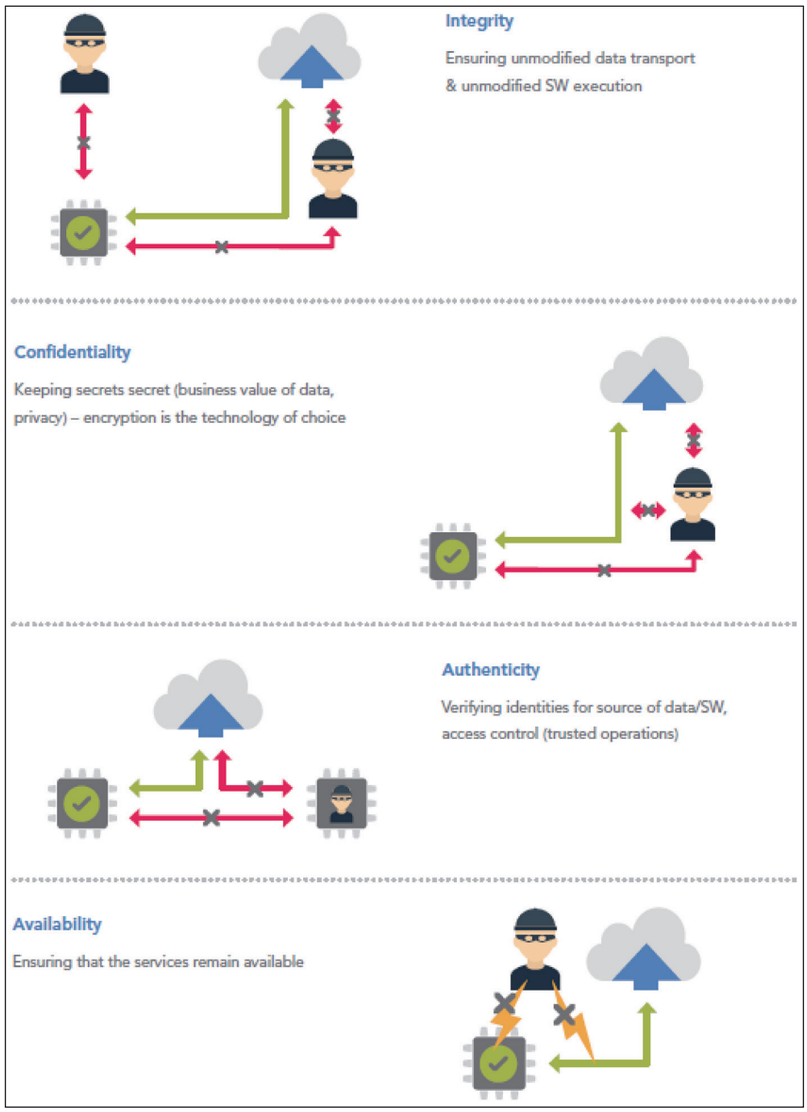
這將有助營運商採購、保險並提高對供應商安全聲明的可見性以管理網路風險。SESIP 旨在對單個物聯網平台組件進行認證，提供安全功能及其抵禦實體、邏輯和軟體攻擊能力的認證。SESIP 平台歸 TrustCB 所有，它也是 Arm PSA 的主要合作夥伴，差別在於：Arm 在硬體級別具有很高的規範性，而 SESIP 更偏重於動態認證。RISC-V International 亦與 GlobalPlatform 攜手為物聯網設備 IC 和 SoC 的開發制訂開放標準，包括在受信任的執行環境 (TEE) 中執行程式的處理器。2019 年，與 GlobalPlatform 相容的 TEE 發貨數量較前一年增加 50%。

經由統一規範、已知硬體漏洞訊息交換以及克服這些漏洞所需的功能，使上述合作雙方可更新每個組織的各自技術文檔和框架，以滿足不斷發展的安全要求。預計短期到中期的示例將集中於 TEE 的應用程式介面、微控制器 (MCU) 的保護配置文件和相應的安全性增強，更有利於協作式開源硬體開發。恩智浦 (NXP) 去年同時獲得 SESIP 與 Arm PSA 認證，產品線涵蓋 MCU、應用處理器 (AP) 和交叉處理器 (兼具 AP 性能、MCU 低功耗與即時操作特性)。NXP 表示，如此可將敏感的數據資產與用戶的應用程式予以隔離。

NXP：坐擁 PSA 和 SESIP 認證，亦不缺席國際資安標準制訂

基於 ROM 的安全啓動過程、利用安全儲存設備的密鑰創建硬體信任根的好處是：從硬體引導程式、建立信任鏈、加載程式、操作系統到應用程式軟體的整個軟體堆

圖 3：設計上的安全性取決於——完整性、機密性、真實性與可用性，須將它們組合到系統中以提供端到端的安全性，應對潛在攻擊並兼顧成本及安全效益



資料來源：https://www.nxp.com.cn/docs/en/white-paper/NXP-FROM-IOT-TO-IOTRUST-WP.pdf

疊，每步皆經過嚴謹身份驗證；有數款交叉處理器和 MCU 還集成了 SRAM 的物理不可複製功能 (PUF)。使用 SRAM 固有自然變化生成「按需密鑰」及「可信賴運算群組」(TCG) 定義的設備身份組合引擎 (DICE) 安全標準，可增強 PKI 或非對稱加密的安全性。憑藉這些安全設計，NXP 嵌入式處理器可達到或超過 PSA 和 SESIP 一級標準，部分系列甚至可達二級。

不只坐擁 PSA 和 SESIP 認證，NXP 還與世界各國政府和國際機構建立聯繫，對於協調安全預期、認證、要求和法規助益匪淺——例如，NXP 已與《信任憲章》中的歐洲網路安全組織 (ECSO) 等物聯網主要參與者以及歐盟網路與資訊安全局 (ENISA) 密切合作；同時，積極參與 ISO、FIDO、GlobalPlatform 和 NFC 論壇等標準化組織，以促進安全互操作性。針對關鍵應用，NXP 亦通過 ISO/IEC 15408-1 ...3 等全球安全通用標準和 CC (Common Criteria) EAL 6+ 認證 (註：CC EAL 是目前最全面的評價準則，共分為七級)。

順帶一提，NXP 日前發佈升級版 MIFARE DESFire EV3 IC 產品 (掃描範圍更大、交易速度更快)，其軟、硬體支援開放式加密演算法，也已通過 CC EAL 5+ 認證；它還具有交易計時器可減輕中間人攻擊 (MITM)，並利用唯一「安全獨特 NFC」(Secure Unique NFC, SUN) 訊息傳遞功能，為每次點擊生成唯一的身份驗證訊息，然後將該訊息發送到伺服器進行驗證以防止非法複製。DESFire EV3 將集成到 NXP 的 MIFARE 2GO 雲端服務中，基於 MIFARE 產品的數位化憑證及 NXP 生態系統簡化行動／穿戴設備的集成工作，協助推展非接觸式交易。

WISeKey：邊緣設備智能提高，攻擊面隨之增加

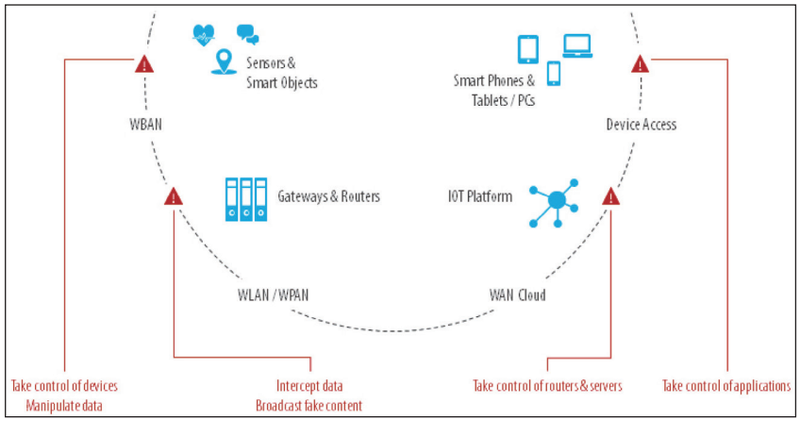
瑞士網路安全公司 WISeKey 相信協同物聯網、人工智慧 (AI)、數據分析、連通性和數位認證工作，可實現早期預警系統 (EWS)。例如，城市、政府和企業可創建一個全球感測器網路，將個人行為與匿名數位身份結合，檢測病毒傳播；但這將需要在全球範圍內進行標準化、安全性、信任、規劃和實施，並強調隱私，擬藉由以下步驟達陣：1. 發行包括真實性數位憑證的儲存設備；2. 加密反映至少一個與物理對象唯一相關的特徵訊息；3. 使用網路電腦，必要時檢查數位真實性憑證的有效性；4. 與驗證或認證機構合作，即時驗證數位真實性憑證狀態。

WISeKey 生態系的數位身份正在讓半導體安裝呈現指數級增長：安全晶片增長到 16 億個、RoT 增長到 50 億套。WISeKey OISTE RoT 是 TCG 的一組功能，RoT 充當單獨的運算引擎、控制嵌入它的 PC 或移動設備的 TCG 平台密碼處理器。RoT 與區塊鏈 (Blockchain) 的結合產生了一個新的 Trust 協定，允許區塊鏈擴展具有嵌入式安全性的可信交易，確保使用 RoT 信任的密鑰對提交到區塊鏈的每個交易做數位簽名，並結合垂直信任流程由信譽良好的第三受信任方透過區塊鏈提供的固有分散式信任進行驗證。

物聯網增加了網路攻擊風險，隨著邊緣設備智能提高，攻擊面也會增加。這種雙重信任模型解決了互聯網最大挑戰之一：彌合當前零散的信任域，包括許多政府使用的現有、不兼容的國家 RoT。一個具體應用是 WISeID，它使用身份的可信分佈式賬本技術儲存對象和人員身份，並為連接的對象提供數位憑證識別、身份驗證和驗證的能力，上述微服務費將藉由 WISeID 令牌收取。在美國，WISeKey 的晶片使用獨特的安全憑證 ID 和 SSH 加密密鑰來保護和認證超過 5,000 萬個路由器。這項技術還用於閉路電視 (CCTV)、數位視訊錄影機 (DVR) 和衛星天線。

IoT 設備晶片設計必須一開始就嵌入安全性，RoT 也必須嵌入連接的設備中；WISeKey 生態系統已擴展到智能卡、智能城市、無人機、防偽、智能照明、伺服器、行動電話等。WISeKey 在 IoT 邊緣擁有獨特優勢：VaultIC Secure Elements 可保護大數據，使用 AI 分析，可幫助工業應用檢測網路安全攻擊或在設備發生故障前預知。WISeKey 一系列通過經 Common Criteria 認證的防篡改微處理器，

圖 4：IoT 擴展方便且可執行許多破壞性的應用程式，卻也為駭客遠程控制設備、攔截／操縱數據、篡改路由器／伺服器，甚至控制應用程式大開方便之門



資料來源：https://www.wisekey.com/solutions/iot-connected-devices/iot-security/

可實現對敏感資產的安全儲存和使用，並在現場唯一標識、認證和保護設備；其數位身份可透過本地 Webtrust 認證的 PKI 或作為雲端服務進行有效管理。

Microchip：無論規模大小，皆應建置嵌入式安全防護

根據《Fortinet 威脅態勢報告》顯示，去年全球 12 件大漏洞、有半數是瞄準 IoT 設備而來；而物聯網網路安全的未來，在於強大的「嵌入式保護」。微芯科技 (Microchip) 亦認為，攻擊數量將持續增長，且越來越多的事物被連接將導致漏洞持續增加，所以需要在設計之初，就為嵌入式系統的所有層級考慮安全措施，包括：設備儲存、通訊硬體和協定、節點 (Node)、閘道器 (Gatewaay)、設備管理系統和雲端運算等。值得留意的是，他們強調：所有類型的系統都需要安全性，但不一定需要相同類型的安全性；定義產品的安全類別，將可更好地評估。

這將確定重大威脅及可採取的保護設計安全措施。Microchip 說明，RoT 在受信任的嵌入式系統中可得到保護，作為保護應用程式的基礎——以密鑰驗證身份。如果密鑰被欺騙，則未經授權或惡意用戶可順勢控制系統交易，後患無窮，故應從最初就正確實現對嵌入式系統的信任。為避免創建偷窺／竊取密鑰的後門，需將加密原始功能和身份驗證密鑰都儲存在設計的安全容器中，Microchip 可配置的安全元件能發揮關鍵作用，且可與任何微控制器或微處理器 (MPU) 搭配使用：基於硬體的密碼加速器，還可顯著減少執行時間和功耗。

這些設備中還嵌入了高品質的亂數產生器和 EEPROM 的安全密鑰儲存。此外，還有防篡改和旁路 (bypass) 信道攻擊保護，阻止對嵌入式系統憑證的訪問。篡改通常有一個目標：以任何可能的方式提取密鑰，最直接的方式是探查晶片以查找儲存密鑰的憑證；而旁路攻擊是非侵入式、不會直接探查電路，乃依賴電路運行時從電路洩漏的訊息，涉及電源／電磁輻射 (EMI) 分析、定時匯流排監控、暫寄器、快取記憶體 (cache) 或隨機存取記憶體 (RAM) 攻擊。除了供身份驗證的密鑰和憑證之安全容器，Microchip 還為不同規模大小的設備提供安全配置。

其 CryptoAuthentication 系列的信任平台是一項三層服務，允許預先配置或完全自定義的安全元素，以及硬體安全儲存，有效防止密鑰被未經授權的用戶隱藏，應對各種規模項目的安全認證。惟有安全地在設備中配置密鑰，才能確保製造商在整個設備現場部署期間或整個生命週期內，都不會曝露密鑰。結合 Trust Platform，可在物聯網節點提供安全的身份驗證、耗材系統的防偽、附件身份驗證和智財權 (IP) 保護，以驗證任何系統的韌體。當然還有最決絕的作法是：將解密密鑰刻錄到 OTP (一次性編程) 自製晶片、安裝韌體並驗證後再使用。

如此一來，這些密鑰將永遠無法重新編程；據此創建的受信任平台模組，會將最終用戶的設備應用程式與網路以物理形式切分，或是以安全啓動模式，先在安全操作系統的啓動映像中驗證簽名後，再在網路接口執行作業系統，將其與晶片組和解密密鑰隔離。要不然，就是將設備與主網從根本上拆開；可能的話，將它們與外網完全隔離或另設獨立區域網以縮小攻擊面。

CTA