作者：羅欣然
Microchip 應用工程師

淺談 Microchip 的 32 位元 MPU 系統安全設計

小百科

隨著網路技術蓬勃發展與應用多樣化，資訊交流便利且多元，已快速滲透人類的食、衣、住、行、育、樂等各層面，深切影響我們的生活方式。

資料交換管道眾多且容易，導致資訊安全的重要性越來越高，具備安全功能 (Security function) 的設備會更為普及。只要有資訊交流的需求，就需要 Security function 保護重要的資料。Microchip 的 32 位元的 Microprocessors (MPU) 提供全方位資訊安全應用解決方案，其提供資訊安全保護可以從軟硬體設計等多個層面來討論：

◆ Trusted Boot

Trusted Boot 的另一個名稱叫做 Root of Trust，它是 Security 系統架構中的根基，整個系統軟體、資料和客戶的 IP 等保護工作都是建構在 Trusted Boot 之上。當設備接上電源後，第一個執行的程式就放在 MPU 內部 Read-Only Memory (ROM) 裡面，ROM 的程式除了進行系統初始化外，還會找尋連結到 MPU 外部 Non-Volatile Memory (NVM) 內是否存放一個可供執行的程式，接著 MPU 就會執行此程式。如果 MPU 的 Secure Boot 預設啟動，ROM 的 Secure Boot 機制會檢查此程式是否通過 MPU 的 Security 功能認證，而 MPU 只會執行被認證的程式。

Microchip 的 MPU Secure Boot 提供兩種程式加密認證方式，分別為 AES-CMAC 模式和 RSA 模式。關於 AES-CMAC 模式，CMAC 全稱是 Cypher-Based Message Authentication Code，基於 AES 對稱加密方式實現資料認證，通訊雙方共享同一對稱金鑰來認證身分。而 RSA 模式則使用 RSA 非對稱式加密和 X.509 證書進行身分確認。在這兩種模式下，唯有通過 Secure Boot 認證的程式才會被 MPU 執行。

◆ Secure Storage

儲存在 MPU 外部 NVM 的機密資料、Secure Keys、Certificates 或客戶重要 IP 等都有機會被駭客竊取，MPU 硬體必須有能力提供安全的記憶體空間，存放這些敏感的資料。Microchip 的 MPU 提供 Fuse 記憶空間，可以用來存放 Secure Keys、Certificates 或客戶重要 IP 資料，確保其資料不會被有心人士竊取。如果資料處理時必須將資訊儲存於 RAM 內，也可利用擾碼加密 (Scrambling) 或 On-the-Fly Encryption 機制來保護資料。

◆ Secure Communications

對於 IoT Cloud 或 Networking Communication 的相關應用，MPU 系統在應用層下，也提供 OpenSSL 或 TLS 等方式進行資料交換時的加密保護。

◆ Secure Firmware Update

借助 ARM® TrustZone® 架構和第三方軟體的支援，在 Linux® 環境下，MPU 利用 Security 系統架構，提供遠端 MPU 韌體更新功能，令更新的過程更加安全可靠。

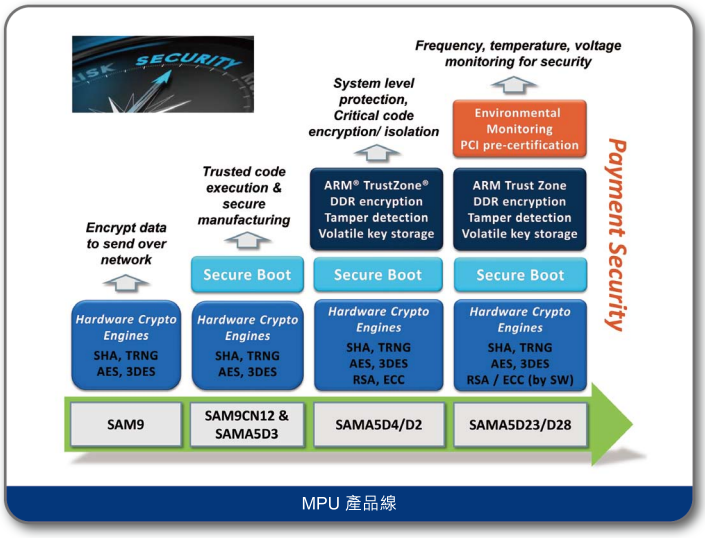
◆ Firmware Protection

系統也提供 Firmware 更新保護。進行 Firmware 更新過程中，只有通過系統認證過 Firmware 才可以使用。Firmware 本身也會被加密處理，以防駭客竊取 Firmware 加以破解，讓客戶敏感的資料外流。

◆ Trusted Device ID

MPU 的 Secure Boot 提供 Pairing Mode，可對 Root of Trust 程式加密保護。執行程式加密的過程中，使用硬體 ID 配對過後的密鑰來進行加密。這樣加密後的程式會跟硬體綁定，以確保加密程式無法在其他同類型設備上運作，更進一步加強本機的安全保護。

Microchip 的 MPU 產品線提供完整 Security 硬體支援，SAMA5 和部分 SAM9 系列皆具備 Secure Boot 功能，而 SAMA5D4/D2 更支援 Tamper Pins Detection 和 ARM TrustZone 架構。所有 MPU 產品線，都具有硬體加密引擎 (Hardware Crypto Engines)，可利用硬體執行加解密演算法。



在工業應用上，ATSAMA5D2 通過 PCI compliance 認證，此為支付產業 (Payment Industry) 相關應用設備的認證標準，代表 Microchip 的 MPU 在工業應用上符合最高等級的安全需求，客戶可以使用此優秀的平台開發具備 Security 需求的設備應用。

此外，Microchip 的 MPU 為了提供全方位的 Security 平台開發，我們跟 Sequitur Labs 合作，MPU 整合 EmSpark™ Security Suite 架構，在 Linux 環境下設計滿足 Security 需求的 IoT 設備相關應用。

如想進一步了解 Microchip 的 32 位元 MPU、Security 及軟體開發相關介紹，請參考官方網站：**https://www.microchip.com/design-centers/32-bit-mpus**，亦歡迎與我們經驗豐富的設計團隊聯繫。

聯繫信息 > Microchip 台灣分公司
電郵：rtc.taipei@microchip.com　　技術支援專線：0800-717-718
聯絡電話：• 新竹 (03) 577-8366　• 高雄 (07) 213-7830　• 台北 (02) 2508-8600