簡化物聯網 (IoT) 節點的硬體安全實作

如何更快、更簡單地賦予 IoT 節點強大的安全性

■作者：Ramanuja Konreddy / Microchip

如何在物聯網 (IoT) 中整合超低功耗運算和連接性，正處於十字路口。一方面，物聯網節點可望改造汽車、工業、智慧家庭、醫療等領域的設計。

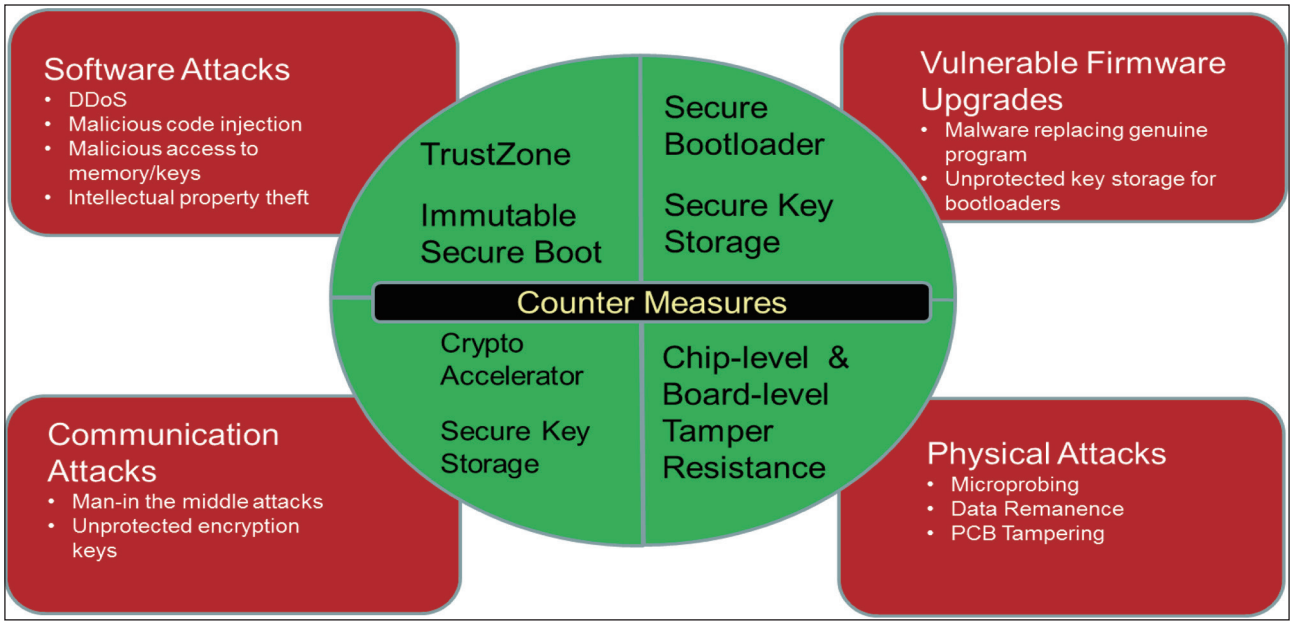
另一方面，惡意軟體－分散式阻斷服務 (DDoS) 的攻擊、榨光電池電力等各種與安全漏洞相關的新聞層出不窮，這些有可能危及物聯網的整體運作。因此，理所當然地，由於邊緣運算設備不夠安全而產生的這些安全漏洞，已成為物聯網開發人員最關注的部分。

愈來愈多的駭客攻擊鎖定未受保護的物聯網節點，這樣的趨勢可以從最近發生的一件事看出端倪：駭客利用賭場魚缸中的連網溫度計，從這個漏洞開始攻擊，進而入侵豪賭大戶資料庫。

這也顯示出，家庭中的恆溫器、冰箱和空調系統其脆弱的安全性，已讓整體家庭和建築自動化曝露在威脅下。或者，透過安全性欠佳的連網 CCTV 攝影機，銀行和商業機構也容易受到攻擊。

在此，值得一提的是，雖然傳統上是在伺服器和閘道器級別實現安全，然而，如果要在物聯網節點設計中強化安全性，則邊緣設備的功耗和體積成為限制所在。此外，安全應用程式的開發，可能會導致開發時間和成本顯著增加。

圖 1：IoT 節點面臨的物理和遠端的安全威脅，以及其各自的反制措施 (Counter Measures)，這些措施內建於嵌入式系統中以防止攻擊。



圖片提供：Microchip

本文將說明物聯網開發人員如何在維持低功耗的同時處理各種安全漏洞。此文並將介紹一個可讓開發人員在設計前期即採用的安全架構。最後，本文將介紹如何利用具有硬體安全功能的低成本微控制器 (MCU) 與架構相結合，以簡化安全性實作。

物聯網節點的安全性

強大的物聯網節點設計，需要提供足以抵禦通信攻擊、惡意軟體和物理攻擊的安全性。為了防止通信攻擊或中間人攻擊，通常的做法是使用加密模組來執行加密、解密和身份驗證。

Arm TrustZone 技術能限制對於特定記憶體、周邊設備和 I/O 元件的讀取。它將微控制器 (MCU) 劃分為可信賴區域和不可信賴區域，並隔離敏感數據和非關鍵數據。安全啓動可確保 MCU 以已知的良好狀態啓動，且使用 Arm TrustZone 可建構有助抵消惡意軟體的環境。

藉由防篡改接腳 (anti-tampering pins)，IoT 節點的物理安全性可以進一步獲得強化，進而提供板級篡改保護。當電路板或周邊被篡改時，防篡改接腳可被程式化，以提供多種對應方式，包括消除機密。將防篡改防護進一步延伸至晶片級，這也是很重要的。這將有助於防止複製和知識產權 (IP) 被盜。

除了這三方面之外，很重要的是還必須建立一個硬體信任根 (hardware root of trust)，這可以透過安全啓動來實現，並能藉由安全密鑰配置機制進行強化。

物聯網節點開發人員必須在低功耗和安全性之間求取平衡。今日的應用需要低功耗和高度安全的設計，且不能影響效能，也不能增加開發時間和成本。對於依賴電池運作的物聯網邊緣設備而言，電力使用至關重要，而這需要能在增加強大安全性的同時，還能大幅降低功耗的 MCU。

最後，但並非不重要的是，低成本物聯網節點設計，需要以簡單的機制來實現安全性。這個機制能萃取出低級別的安全細節，以避免複雜性、陡峭的學習曲線和大量的開銷成本。

簡化嵌入式安全性

可簡化這些安全功能實作的 MCU 範例之一，是 SAM L11 微控制器，它在矽晶片設計階段就深度嵌入安全性。它的運作頻率是 32 MHz，記憶體配置了高達 64 KB 的快閃記憶體 (Flash) 和 16 KB 的靜態隨機存取記憶體 (SRAM)。為了說明開發人員應該在 MCU 的設計前期就導入安全性，我們將仔細檢視 SAM L11 中提供的四個關鍵安全元素。

1. 不可變的安全啓動 (Immutable Secure Boot)

SAM L11 包含一個 Boot ROM 設計，採用不可變的安全啓動。它具有板上加密加速器 (Crypto Accelerator，CRYA)，可加速用於加密、解密和身份驗證的 AES、SHA 和 GCM 演算法運算，以及用於符合 NIST 標準的 TRNG，進行隨機數生成。

2. 可信賴的執行環境

ArmTrustZone 技術允許在 SAM L11 內創建安全區域。當與不可變安全啓動結合使用時，能創建可信賴執行環境 (Trusted Execution Environment，TEE)，以有效抵消惡意軟體。TEE 使 IoT 節點能夠在遇到惡意軟體時採取補救措施。它能避免關鍵功能的停機時間，並顯著提高物聯網節點的可靠性。

3. 安全密鑰儲存

除了防止板級篡改的防篡改接腳外，SAM L11 還具有 256 位元 RAM 的主動屏蔽，可以抵禦晶片級微探測 (microprobing) 和數據殘留問題，為揮發性密鑰提供安全儲存。它還有一個專用的 2KB Flash，可以加密儲存非揮發性密鑰、驗證和其他敏感數據。裝置上的安全密鑰儲存，可以保護系統不受軟體和通信攻擊，並為開發人員提供能在偵測到篡改事件時清除敏感數據的選項。

4. 全面的安全解決方案架構

SAM L11 具有全面的安全解決方案架構支援，

該架構提供端到端的安全性，涵蓋範圍從矽晶片製造階段在安全設施進行設備密鑰配置，到應用程式開發期間安全模組的實現，以及在生命週期的任何時間進行遠端韌體升級。此架構包括 Trustonic 的 Kinibi-M 安全軟體，該軟體萃取較低等級的設備安全功能細節，並提供模組化和採用 GUI 的介面，讓開發人員可以針對應用來選擇相關的安全模組，例如用於保護韌體升級的啓動加載程式 (bootloader)，因此嵌入式開發人員不需篩選數百頁的數據表來了解如何建置安全的 bootloader。

安全架構經完整定義，能為開發人員提供模組，使其可以在應用程序中快速實現安全 bootloader，這讓開發人員不用接受有關嵌入式安全的訓練，並且大幅縮減開發時間和成本。

深度嵌入於 SAM L11 微控制器的硬體安全功能，有助於嵌入式開發人員使用 Trustonic 的信任根 (Root of Trust, RoT) 流程，在 Microchip 的安全機制中執行密鑰配置。

圖 2 顯示此架構提供的各種模組，可以簡化安全性實作：

全面的安全解決方案架構，可協助剛接觸安全性的嵌入式開發人員，避免陡峭的學習曲線和過高的開銷費用。在很短的時間內，他們可以輕鬆地在各種應用程式使用案例中實現強大的安全性，如圖 3 所示。

此元件採用 picoPower 技術，可確保在活動和睡眠模式下的低功耗，且獲得了 EEMBC 所認證領先業界的 ULPMark 分數。它還提供各種省電模式和低功耗技術，讓開發人員可以利用此靈活性，方便地實現安全性，且不會影響功耗。

總結

物聯網邊緣運算設備的連結如此快速，快過這些設備建置安全性的速度。造成這種情況的原因之一，在於嵌入式應用領域總是在事後才考慮安全性，而造成這種趨勢的另一個因素，是現今市場上對於在 64 KB 或容量更低的 Flash 空間中整合強大安全

圖 2：端至端 (End-to-end) 安全解決方案

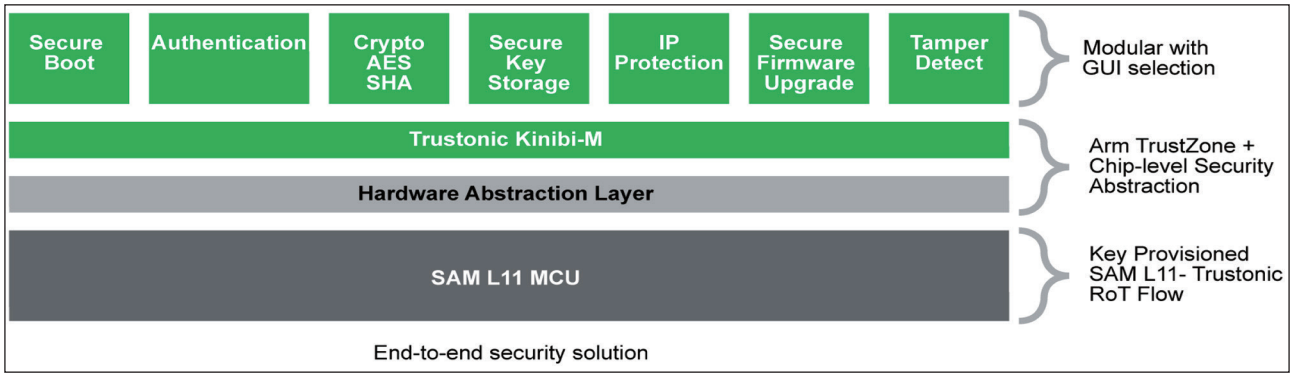


圖 3

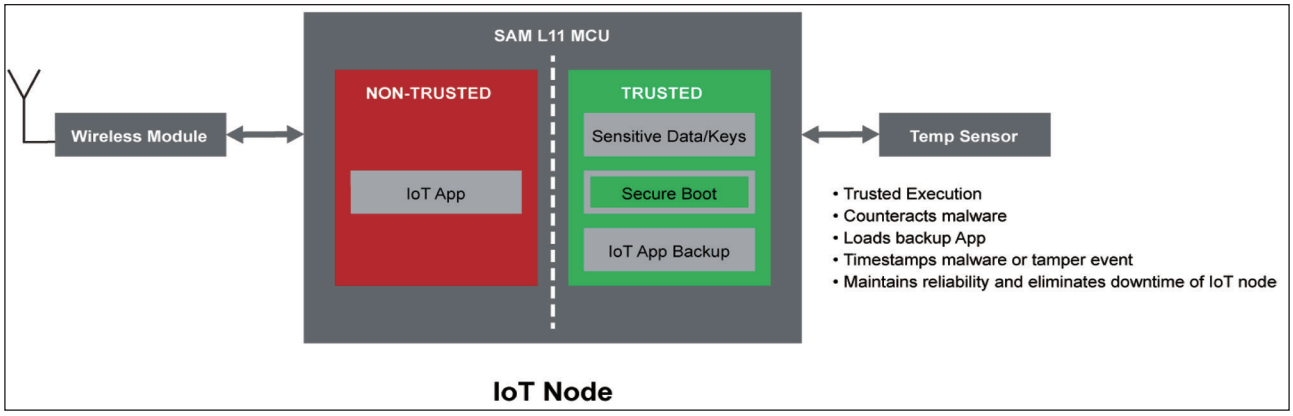
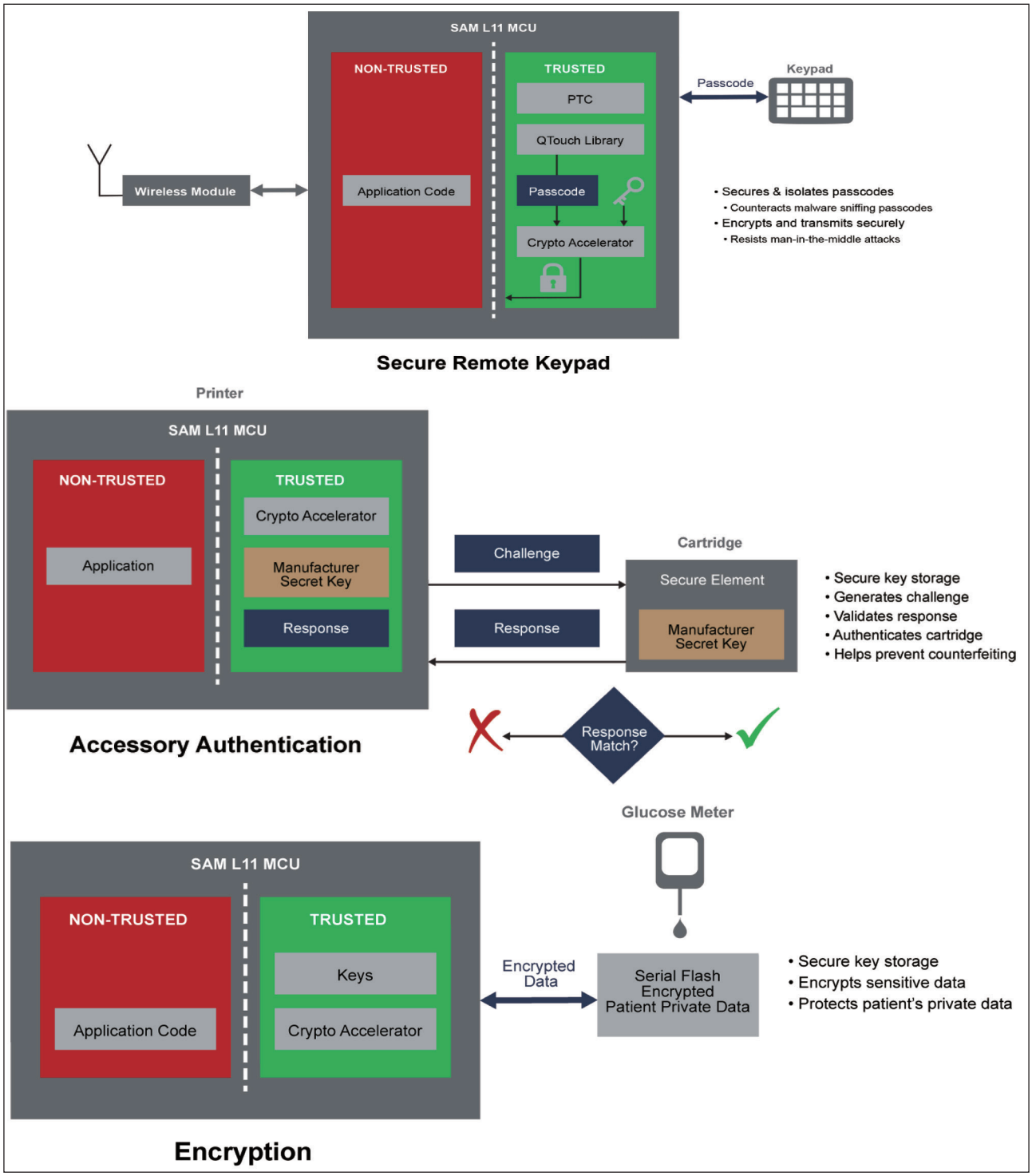


圖 3



性的 MCU，大部分並無法滿足 IoT 節點對於價格的既定要求。

然而，當嵌入式的安全漏洞正在為駭客提供新的攻擊媒介，新一代微控制器也正在協助物聯網節點開發人員，使其能夠輕鬆快速，並且有效地配置和部署安全功能。

本文說明這些安全 MCU 如何簡化安全實作，同時還能減少陡峭的學習曲線和開銷費用。CTA