以節能/低成本微控制器實現IoT裝置安全

物聯網安全：從規格到程式碼

業界目前已經建立一個對開發人員友善的安全功能取用方法，它搭載了平台安全架構（PSA）功能性應用程式設計介面（Functional API），這也是 PSA 認證計劃的項目之一。

文／Hannes Tschofenig (Arm Distinguished Engineer)

PSA Crypto API 可以讓開發人員透明的取用常駐於晶片與晶片外的安全功能。更多的API，如儲存API、初始認證API或韌體更新API也都已經存在可用，並使取用安全功能更為簡單。剛開始它們雖然只能支援 Cortex-M 系列微控制器，但最近已可用在 Cortex-A 系列的處理器上。API的規格固然重要，但實作更是關鍵。就 PSA Crypto API 來說，我們可以在 Mbed TLS 內找到實作。

龐大生態系中的一個基礎元素

若要著眼於確保物聯網裝置的安全，這些API只是更龐大的生態系其中的一個基礎元素。「可信任韌體-M」（TF-M）與「可信任韌體-A」（TF-A）提供在TrustZone系統上運行的參考軟體，並且實作這些API。TrustZone提供軟體隔離的功能，並藉由把牽涉安全性的敏感程式碼與一般的應用程式碼彼此分開，降低受攻擊面。可信任韌體專案讓開發人員得以專注在非安全處理環境（NSPE）中運行的軟體實作，例如感測器監控應用程式，同時也照顧到安全功能。NSPE軟體可以使用PSA功能性API，以便取用安全領域內運行的 TF-M/TF-A 所提供的安全性服務。PSA功能性API的適用領域已經擴展至TrustZone以外，現在還包括雙核心的 Cortex-M 級的裝置，以及Corstone架構的系統單晶片（SoC）設計。TF-M 則是用來在同一顆SoC上，於 Cortex-A 系列處理器旁的 Cortex-M 系列處理器上運行。

FIDO聯盟最近針對安全裝置登入，發表了名為FIDO裝置登入（FDO）的規格。FDO若能成功運行，將可針對裝置進行配置，讓它們可以執行物聯網裝置管理協定。裝置管理讓管理物聯網裝置的公司，可以從遠端執行物聯網裝置，妥善運作所需的所有主要功能。這些功能包括：

- 配置作業憑證與相關的安全性配置，讓物聯網裝置與管理伺服器互動。
- 更新軟體與韌體以修正錯誤，並提供新的功能。
- 配置裝置（例如：連網功能、存取控制列

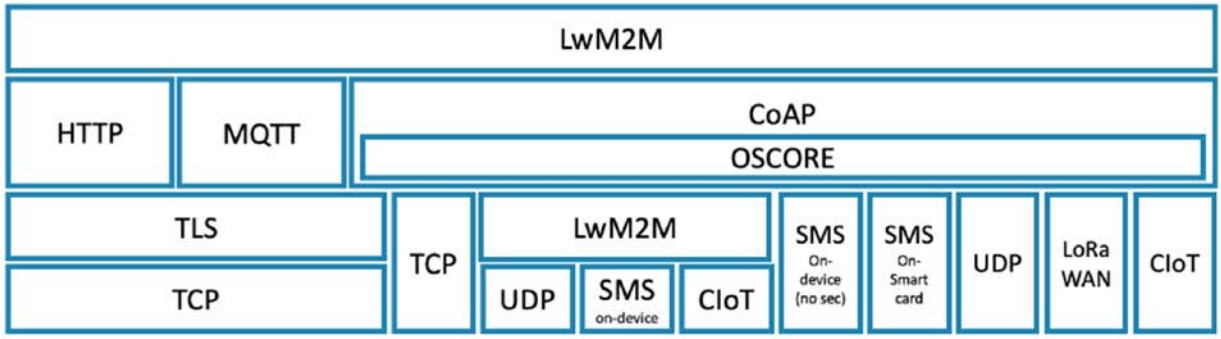

Figure 1: LwM2M v1.2 Protocol Stack

LwM2M v1.2 版本協定的堆疊

表）。

- 執行應用服務配置（例如對裝置進行配置，以便使用特定的應用功能，這一點可能取決於客戶、裝置所在的位置，或是用戶向服務供應商訂閱的服務類型）。
- 故障管理（例如搜集除錯記錄以供開發人員進行詳細的分析）。
- 感測器以及其它裝置特定資料的檢索。
- 控制致動器（像馬達）。

物聯網裝置的標準化生命週期管理

輕量級機器對機器（LwM2M）協定，是一種標準化的物聯網裝置管理協定。原本在2012年提議的這項協定，其用意是在條件受限的物聯網裝置上運行的少數標準化裝置管理協定之一。時至今日，LwM2M已可用於開源的實作。它已經經歷超過45家企業的大規模可交互運作測試，這幾年來，規格本身也經過數個迭代的演進。最新的 LwM2M v1.2 版本於2020年發表。進化至 v1.2 版本後，目前LwM2M可用在許多不同的傳送協定，包括MQTT、HTTP、CoAP over UDP 與TCP，甚至可以透過非網際網路協定（IP）架構的載送協定運行（如SMS、長距離低功耗廣域網路LoRaWAN，以及蜂巢式物聯網）。附圖說明協定的堆疊。今年(2021)它的規格在閘道器功能性方面進行強化，一個物聯網島可以用簡單的方式，以閘道器連接LwM2M基礎架構。

LwM2M與FDO都利用密碼函數以及可能使用的驗證，同時加入一個韌體更新的機制。為了利用 TF-M 與 TF-A 提供的功能，物聯網裝置上的FDO或LwM2M客戶端實作都必須使用PSA功能API，原因是安全性的服務已經接觸到搭載那些API的應用程式。例如，開源的 Pelion Cloud Client 實作，實際上就是使用 Mbed TLS 實作。它因此可以使用 PSA Crypto API（因為它是 Mbed TLS 的一環），便利地取用 TF-M 與 TF-A 所提供的服務。

LwM2M回應了所有物聯網裝置都需要的裝置管理使用場景需求，而開發人員則可透過一個開放且透明的開發流程，利用 OMA SpecWorks 在LwM2M方面的努力成果。LwM2M規格已經完成實作，而其中部份的實作已可用開源程式碼方式取得。OMA SpecWorks 利用複雜的測試規格籌劃「測試大會」，以便測試實作的規格符合所需。當協定的規格作業及API與參考實作結合，物聯網的開發人員將更能確保其物聯網裝置的安全。他們將受惠於該設計中所使用的尖端安全性技術。重要的是，所有這一切都可以利用節能且低成本的微控制器達成；這對於使用條件有限的物聯網設計，可說相當重要。