# 物聯網中的硬體安全性

■作者：Ted Marena 美高森美公司 SoC/FPGA 產品總監
enny Yao 美高森美公司助理行銷工程師

根據 McKinsey 的一份研究報告指出，安全性和隱私性均被視為未來物聯網 (IoT) 增長的關鍵性挑戰 [參考文獻 1]，其中一個關注重點就是終端使用者可存取的 IoT 設備之安全性。從商業連網的 HVAC 系統和無線基地台直至工業電力線通訊 (PLC)、航空網路、網路閘道系統，甚至發電廠的關鍵能源基礎設施等一系列各式各樣的應用領域中，都可發現這些設備的蹤跡。

威脅向量林林種種，有真實的，也有假設的。事實證明，為免受到已知威脅的危害，單單倚賴軟體安全功能是不夠的，幸好現今的 FPGA SoC 器件可用來實現一種可一路擴展到 IC 層面的可調節安全方案，將有助於提供全方位、可調節的安全性，同時以小佔位面積維持低功耗系統的運作。

事實上，幾乎任何連接至其他設備，還有終端使用者可存取的設備，均存在危險性。

以汽車領域為例，一則虛假的先進駕駛輔助系統 (ADAS) 訊息把關於面前車輛的速度和方向的錯誤資訊發送至其他車輛或基礎設施 ( 統稱為 V2X) 系統，便可能會引起事故；此外，惡意的資料操作也可能會造成交通中斷，使整個城市陷入混亂。

在工業環境中，使用者可存取的設備，包括智慧電網現場控制器和公用事業流的監控器，很可能會讓惡意攻擊有機可乘。這類已經聯網的遠端設備越來越多，由於它們通常具有遠端接近性，所以對惡意駭客極具吸引力。醫療保健產業的攻擊向量，來自與病患監控相關的使用者可存取設備。在通訊基礎設施中，4G/LTE 網路的無線小型蜂巢系統同樣容易受到攻擊，它們通常經由第三方存取供應商的網路安裝在街道上。與大型營運商相比，這些協力廠商網路的安全性較為鬆懈，容易成為駭客和破壞者的獵物，被使用來存取那些極易遭受 GPS 干擾、詐騙，以及其他時間安全性漏洞的網路。

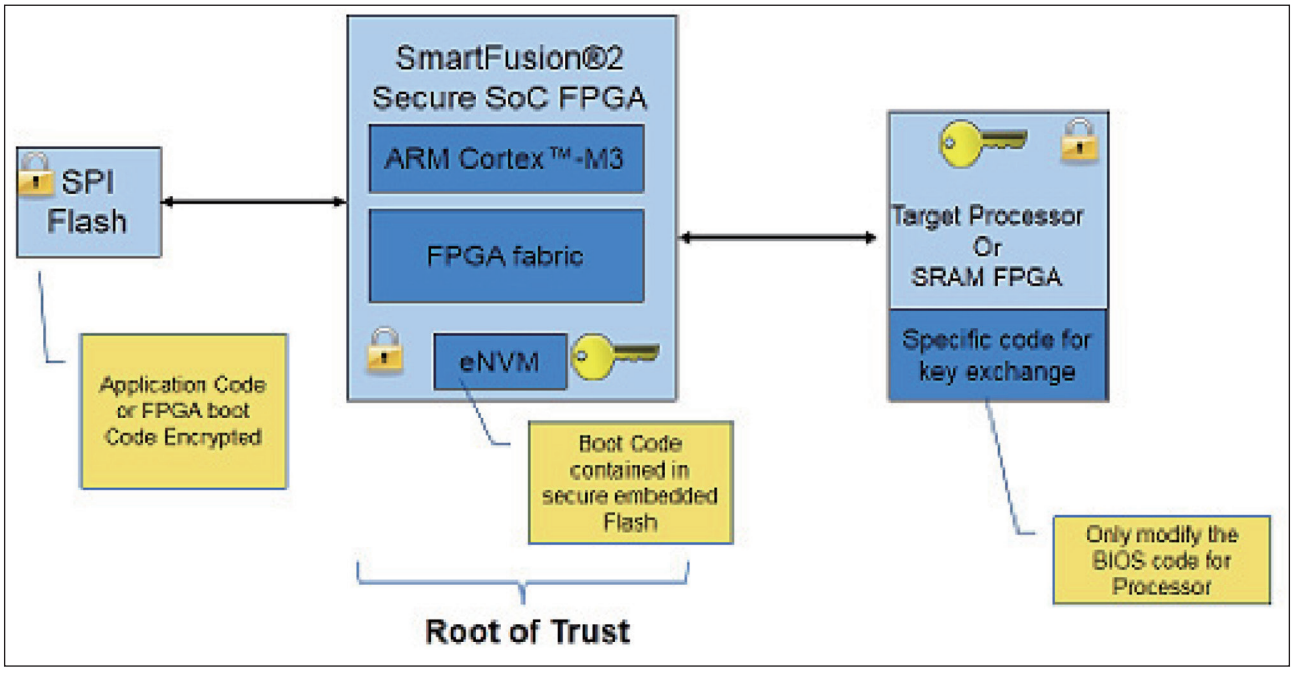
最近一家商用航空公司的航班受到駭客控制，這個例子 [參考文獻 2] 就是與使用者可存取的聯網設備有關。根據法院的檔案指出，美國 FBI 正在調查這起事件，懷疑一名乘客將膝上型電腦插入到座椅下方的電子盒，從而存取機載娛樂 (IFE) 系統，而後再接入到其他重要系統，包括為飛機引擎提供動力的飛機推力管理電腦。

除了上述的威脅之外，任何使用者可存取的設備也很容易面臨到智慧財產權 (IP) 盜竊和產品反向工程的威脅，我們需要從器件級別開始的端至端分層安全功能，才能夠保護這些設備，以避免發生 IP 盜竊、反向工程、篡改，以及複製等情形，同時防止它們被利用作網路攻擊工具。今天的 FPGA 器件結合了設計安全性 ( 包括防篡改措施的晶片級保護 )、硬體安全性 ( 電路板級和供應鏈 )，以及資料安全性 ( 涵蓋設備收發的所有通訊 ) 來支援這項戰略。

一個硬體安全性不足的聯網設備，一旦遭受終端使用者的駭客攻擊，其設計 IP 便可能遭到竊取。除了保護 IP，設計安全性還包括避免反向工程。如果沒有建基於硬體的安全性，使用者可存取產品的 IP 便很有可能會被竊。在 2012 年，美國超導公司 (AMSC) 的股價在短短一天內下跌 40%，在五個月期間蒸發了 84%，其主要原因就是該公司的風力渦輪機演算法缺乏安全措施的保護 [參考文獻 3]。

為了保護設計，應當將配置位元串流加密和保護。具有篡改保護、歸零和安全金鑰儲存的設備，能夠大幅降低攻擊成功的機會。硬體應當能夠分辨未經授權的存取和篡改，在檢測到篡改時進行歸零。

圖 1：在圖中的例子中，美高森美 SmartFusion2 安全 SoC FPGA 器件被用作儲存金鑰的信任根，並且對處理器所引導的資料加密




若要進一步對設計提供更好的保護，硬體安全設備應當能夠抵禦差分功率分析 (DPA) 攻擊。DPA 只要使用並不昂貴的電磁探針和簡單的示波器便可發現加密金鑰，所以我們建議工程師使用具有 DPA 授權對策的設備，來確保擁有足夠的設計安全性。

保護可存取產品的另一個原因是硬體安全性，包括確保電路板運行的代碼是可信的，以及建構產品的供應鏈是安全的。信任根 (root of trust) 是硬體安全性的起點，也是建構產品的基礎硬體器件，它應當具有先前所提及的全部設計安全特性。首先建立起硬體信任根，才可以真正安全地使用較高級別的安全功能，例如，硬體信任根器件可以用來儲存金鑰，並且加密處理器啓動時所引導的資料。安全引導是保護啓動代碼避免受到攻擊的關鍵，即使駭客能夠存取這類產品，也無法重寫引導代碼，也無法對處理器安裝任何惡意軟體。圖 1 中的例子說明了如何使用這種方法來保護處理器。

供應鏈安全性是硬體安全中經常被忽略的一個環節，如果企業擁有自己的製造設施，自然能夠確保其產品不會被複製或過度生產；然而，大多數電子產品都是由第三方的外包商製造，並且多數是在國外製造，為了保護公司產品不會被過度生產，可以善用硬體信任根設備中的功能。例如，如果一個器件具有金鑰儲存，便可以利用它來加密產品的位元串流或韌體，使得僅僅具有特定金鑰的器件可以被程式設計。這是有效的，不過，只有設備具有內置授權許可的 DPA 對策才是真正安全的。

連網硬體的最後一種安全類型是資料安全性。資料安全性可確保進出產品的通訊是可信和安全的。過去數年來，FBI 一直都在警告大眾，指出智慧電錶駭客攻擊已經蔓延開來了。這些駭客攻擊需要在實體上存取電錶，他們能夠從電錶收集安全代碼，並且存取其他連網設備。FBI 指出，來自不安全電錶的攻擊使得美國一些電力公司每年損失多達數億美元。

珍貴的資料無論在儲存或傳送過程中也必須加以保護，以確保它們具有安全的設計和信任根，從而建立起安全資料通訊。公共 / 私有金鑰交換是十分常用的安全資料通訊方法。簡單來說，此一服務中的兩個設備都共同掌握了公共金鑰，並且各自有自己私有的金鑰。最安全的私有金鑰類型是不必由人們產生的金鑰，如果硬體設備具有物理不可複製

功能 (PUF) 的特性，就可做到這一點。建基於 PUF 的設備會根據每個矽器件的獨特特性來產生一個金鑰，它是利用每個晶片的微小差異來產生的獨特金鑰。使用建基於 PUF 的器件來實現資料安全，能夠防止擁有金鑰的內部人員對產品進行駭客攻擊。

在公共和私有金鑰產生後，雙方開始通訊，具有公共金鑰的雲伺服器會將一個詢問問題寄發給每一設備，如果回應是正確的，才進行後續的步驟，以保障建基於私有金鑰加密之資訊的通訊。我們建議大家使用擁有公共金鑰基礎設施 (PKI) 和 PUF 的供應商來實現最高的資料安全等級。

隨著 IoT 設備數目持續以指數級的量級增加，硬體和嵌入式系統的安全威脅也日益受到關注，重要的是要認識到只有軟體安全是不夠的，特別是在使用者可以存取連網設備的情況下，這會使得整個系統很容易受到攻擊。過去曾經發生過許多安全事件，未來有可能會再次發生在任何系統中，不單威脅安全，甚至會危害國家安全。此外，系統中還有著安全性漏洞的風險，有可能因為資料被竊取或 IP 複製而帶來數百萬美元的損失。需要可確保硬體安全性、設計安全性，以及資料安全性的元件，才可防止這些威脅。FPGA 器件具有加密的位元串流、多個金鑰儲存單元、經過授權許可的 DPA 對策、安全的快閃記憶體、防篡改功能並加入了 PUF 功能，是保護現今使用者可存取連網硬體產品所不可或缺的關鍵。

## 參考文獻：

[1] http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_internet_of_things_sizing_up_the_opportunity

[2] http://www.upi.com/Top_News/US/2015/05/16/Hacker-took-control-of-United-flight-and-flew-jet-sideways-FBI-affidavit-says/2421431804961/

[3] http://www.bloomberg.com/bw/articles/2012-03-14/inside-the-chinese-boom-in-corporate-espionage CTA

## 愛立信物聯網加速器讓各行各業玩轉數據

愛立信宣佈推出「物聯網加速器」(IoT Accelerator) 解決方案。此解決方案將水平整合功能豐富的物聯網平臺與愛立信的服務以及市集，該市集－例如公共安全、公用事業、交通和智慧城市等區隔市場－可以使客戶與合作夥伴連結，並為解決方案帶來收益。物聯網加速器解決方案可視為一項服務，使客戶克服成本和複雜性等障礙，迅速開發和部署新的物聯網解決方案。

此物聯網平臺功能包括數據管理、計費、終端裝置管理、連接服務和數據分析。已規劃的配套擴展模組則包含自助服務入口、開發者環境和軟體開發套件。物聯網加速器將充分運用愛立信雲端系統以支援混合雲部署，並滿足資料主權 (data sovereignty) 和安全性的需求。此解決方案支援所有主要的連接標準，並將支援愛立信的蜂巢式大規模物聯網部署軟體解決方案，包括支持 3GPP 窄頻物聯網 (NB-IoT)、LTE Cat-M1 和 EC-GSM-IoT 技術，以滿足低功耗廣域應用的需求。

此解決方案將充分運用愛立信完整的服務產品組合，包含最初的安裝服務到業務諮詢、應用開發和維護、系統整合和產業轉型服務等項目。

物聯網加速器解決方案的目標市場包括應用程式知識庫和協作開發網站。它能使企業與產業生態系合作夥伴保持密切合作開發解決方案的同時，也能選擇將開發的解決方案提供給自己的客戶。

愛立信區域商務實驗室將為物聯網加速器客戶提供支援，並提供因應本地調整的全球執行能力。