安全性的需求

隨著最近物聯網（IoT）的崛起，目前有 140 億個裝置是相互連結的。然而，這種成長趨勢也是相當明顯，在 2020 年以前預期會有超過 500 億個裝置將會相互連結。隨著這些裝置的互連，系統也需要開放遠端存取與控制。

相對的，這種情況也呈現出安全性水準的不足。此份白皮書將討論目前有關嵌入式系統安全性的問題，並披露未提供正確等級安全性所將造成的破壞性影響。

介紹

這是一系列用來檢查安全性需求、應用以及實現方案的四篇白皮書中的第一篇。此四篇白皮書將會特別針對瑞薩電子 RX 家族進行檢查。RX 家族是由 32 位元高性能與低功耗微控制器（100 µW/MHz）所組成。

白皮書 1：安全性的需求

雖然此份白皮書是專注在安全性的需求方面，但也可以應用在所有的瑞薩微控制器家族上。

白皮書 2：安全性的應用

介紹可以應用在 RX 微控制器家族的各種安全性方法。

白皮書 3：可信任的 IP 安全驅動器

介紹使用於 RX 微控制器家族的安全性通用驅動器平台。

白皮書 4：雲端連結

介紹如何將 RX 家族微控制器連結至雲端。

安全性

本文檔中引用的安全性定義為「實體保護承擔保護責任的資源的能力」。

在嵌入式系統當中，這種保護涵蓋了軟體與硬體資源。國際電信聯盟（ITU）X.800 定義了如下的安全性服務：

- 存取控制——存取控制是為了確保特定資源只會提供給獲得授權的人進行存取。
- 資料機密性——機密性是為了確保資訊免於遭到未經授權的披露。
- 資料完整性——資料完整性是用以確保數位資訊未受損壞而且只能夠由獲得授權方加以存取與修改。完整性牽涉到維持資料的一致性、準確性、以及可信度。
- 資料來源認證——資料來源認證是在傳輸過程中資訊未遭修改的屬性，並且接收方可以驗證訊息的來源。這種認證類型不一定包含不可否認性。
- 不可否認性——不可否認性是避免使用者稍後否認其執行動作的能力。

我需要對我的應用設定安全性嗎？

對於任何嵌入式系統而言，強烈建議將安全性列入考量。假如嵌入式系統包含您想要保護的任何資源，那麼安全性就是必要的。另一種比較好的問法是，需要何種等級的安全性？這必須透過調查可能的威脅，然後相對於暴露資源的價值來說，哪些安全性原則具有經濟意義，接著才能夠決定。

在連結到網際網路時應特別考慮，因為這會導致威脅的顯著增加。

威脅與攻擊

威脅和攻擊通常被互聯網工程任務小組（IETF）的’Request for Comments’（請求註釋）(RFC）4949 文檔定義為：

- 威脅——存在違反安全的可能性，其存在於可能破壞安全性並且造成損害的某種情況、能力、行動、或是事件時。也就是說，威脅是一種可能會利用漏洞的危險。”
- 攻擊——一種來自於智慧型威脅的系統安全性攻擊；亦即一種蓄意企圖規避安全性服務並且違反系統安全性原則的智慧型行為。

漏洞利用代碼

漏洞利用代碼就是要利用系統漏洞時所需要的代碼（或順序步驟）。其可能會善加利用軟體、硬體、或是系統中所使用協定中的錯誤。

為了要修正軟體中的漏洞，可以安裝韌體更新系統，如此軟體得以更新以修正威脅。請注意對於 IoT 裝置而言，更新的機制是至為重要的，然而設計者必須要確保更新機制的安全性，如此更新機制才不會變成了攻擊的指向工具（vector for an attack）。

對於物聯網的特殊威脅

物聯網（IoT）裝置有三種威脅領域特別會讓物聯網系統易於受到攻擊。

- 網路：物聯網端點可以從幾乎是世界上的任何地方，透過網際網路或是其它網路（例如電話）進行遠端存取。使用於許多 IoT 裝置的無線連結尤其脆弱。
- 現場：物聯網裝置通常可以進行實體存取，以及相互連結。這會使它們曝露在額外的硬體攻擊中，而這對於有連結網路但是實體上受到「槍、守衛、以及閘門」保護的系統來說一般是不需要加以考慮的。
- 容易取得：樣品通常很容易透過購買或是盜竊取得，然後可以在敵人閒暇時加以分析。

對於物聯網裝置的攻擊

物聯網應用裝置被認為是「元件設置所在的系統，而以網路連線的裝置則僅透過傳送訊息進行溝通與協調」。在其最簡單的形式當中，物聯網應用裝置可以被視為如同客戶端與伺服器的兩個節點。本篇文獻評論中所討論到的安全性問題將會專注在對於用以確保客戶端與伺服器間通訊安全性演算法的評估上。這些演算法在嵌入式系統中實現，藉以提供足以對抗威脅的安全性等級。對於這類系統的威脅可以分為被動式與主動式攻擊兩大類別。

被動式攻擊

被動式攻擊是一種分析嵌入式系統並嘗試使用從系統濫用所蒐集而來之資訊的攻擊。主動式攻擊則試圖修改系統資源以為其帶來好處。

- 竊聽——也稱為側錄（sniffing），是由擷取客戶端與伺服器間資料的封包以及讀取像是密碼、或者會話令牌（session tokens）之類的敏感資訊所組成。無線感測器網路（WSNs）擁有攻擊者對其進行竊聽的絕佳條件。因為受到天線的限制，WSN 是由許多會將發射資料重複送至下一個節點的節點所組成。為了要降低攻擊的可能性，必須建立一個由第 4 節中所提到的演算法則所組成的物理層。

竊聽在第一次世界大戰時非常受到歡迎，只要透過利用地面返回電流就可以竊聽單線的敵方電話。

- 監控——這是最簡單的攻擊之一，攻擊者將會監控一套系統，搜集情報，直到可能造成更大的安全性威脅為止。舉例來說，監控加密通訊可能仍然會洩漏以大小、頻率、或是時序為基礎的訊息。

主動式攻擊

主動式攻擊會有積極的作法並且嘗試修改已發送以及正在傳輸中的訊息。這類攻擊可能包括：

- 偽裝（Masquerade）——這牽涉到使用讓接收者感知為其他人的身份來進行訊息的傳送或接收。這可能會造成破壞性的影響。有一個偽裝的例子就是網路釣魚電子郵件。
- 重播（Replay）——這種攻擊是用來攔截訊息後以較晚的日期傳送，藉以混淆通訊協定或是人員。要在通訊協定中避免此攻擊的話，有一種方法就是實現邏輯時間戳記。
- 訊息竄改（Message Tampering）——包含了在將訊息傳送至預期收件者之前進行攔截訊息以及修改內容的行動。訊息竄改的最常用型式就是中間人攻擊。這種攻擊需要攔截第一個訊息，並且修改安全金鑰以便使後續訊息可以輕易的解密。
- 阻斷服務（Denial of Service）——阻斷服務（DoS）攻擊會將整個分散式系統的性能降級，阻止系統的正常使用。這種攻擊可以藉由訊息使系統過載，因而導致系統失能來加以完成。
- 分散式阻斷服務（Distributed Denial of Service）——DDoS 是一種利用許多裝置（通常是 IoT 裝置）將攻擊集中在一個實體上的攻擊方式。

現今趨勢

根據開放網站應用程式安全計畫（OWSAP）：

- 60%具有使用者介面的裝置容易受到憑證薄弱等問題的影響。
- 70%的裝置使用未加密的網路服務。
- 70%的裝置以及雲端與行動應用裝置使攻擊者能夠通過帳戶列舉來識別有效的使用者帳戶。
- 80%的裝置以及雲端與行動應用裝置未能厲行要求密碼長度和複雜度足夠的策略。

隨著更多的裝置與系統連結到網路中，安全性漏洞的潛在危險與可能的影響正持續的攀升。對工廠進行的阻斷服務（DoS）或是分散式阻斷服務（DDoS）攻擊可能會引發系統過載，進而導致在關鍵時刻無法提供重要服務與通知。舉例來說，假如所連結的溫度監控與控制系統對於系統操作員的通知或是來自於系統的指令因為 DoS/DDoS 攻擊而遭到阻斷的話，那麼提供臨界溫度通知的工業冷卻系統就可能會嚴重受損。相同的，DoS/DDoS 攻擊可以干擾道路交通控制系統，導致其所服務的區域發生大規模的阻塞。

從國家安全的角度而言，其可能帶來的影響甚至更為驚人。國家安全局（NSA）承認在 2014 年間的美國實際上是處於網路戰爭狀態的，而且駭客已經在偵察任務中滲透進系統當中了。資深軍官指出有許多國家目前已經有能力將美國的電力與金融服務行業予以關閉。從個人使用者的觀點來看，消費者因為日益依賴連線裝置而會變得更加脆弱。使用連線的健康照護裝置例如嬰兒監視器、血糖計、心律調節器等會讓消費者的健康

與福利曝露在可能會導致這些裝置失效，或甚至更糟的施予錯誤的藥物劑量的惡意附加元件中。隨著消費者增加他們家屋的智能與互聯性，駭客竊取個人資料的風險也呈現指數性的升高。

為了要了解此問題的範圍，瑞薩電子最近徵詢了客戶們所認為在 IoT 市場中最危險的威脅。他們確定了以下 7 種類型的威脅：

- 不受信任的合約製造商複製軟體或硬體，或者是 MCU 或產品的安全性組態設定。
- 駭客藉由在安裝階段利用惡意軟體替換原版韌體來破壞產品。
- 駭客在韌體安裝期間發起竊聽攻擊，特別是當安全性參數不受阻礙的被置換時。
- 當系統韌體未受到物理保護而且攻擊者可以提取安全性參數時所產生的隱私威脅。
- 利用附加元件程式進行破壞或是竊取資訊的攻擊者。
- 駭客利用簡單的軟體更新會話將韌體替換為惡意軟體。
- 攻擊者會透過安全性漏洞製作漏洞利用代碼來破解安全性。IoT 產品應該要具有韌體更新功能以便立即的修補安全性漏洞。

對於 RX Secure Trust IP 的設計者而言，有一件事是顯而易見的。為了要確保設置於平台週邊的裝置確實是安全可靠的，它們必須要能夠因應所有以上列舉出來的威脅。它們必須要將安全性功能建構在平台當中，藉以在產品生命週期的每個階段提供保護。

結論

本文已經定義了安全性、攻擊、以及威脅這些術語。雖然大部份應用裝置都需要安全性，但是要找出適當等級的安全性需要依據應用裝置以及可使用的資源而定。

本文接著討論了物聯網裝置當前的安全趨勢，並描述了創建安全應用所面臨的挑戰。

本系列的下一篇文章將會介紹在微控制器中如何實現安全性服務。

撰寫：Dyfan Davies——瑞薩電子（歐洲）有限公司

文件編號：R01PM0054HT0000