Technical Article

以低功率無線 MCU 解決關鍵無線連線網路安全挑戰

Sainandan Reddy、Benjamin Moore 和 Bhargavi Nisarga

隨著無線連線技術創新，連接裝置的能力現在已經擴展至日常電子產品，進而將智慧功能帶入家庭和車輛 (請參閱图 1)。更多的智慧意味著更多的功能和特色：遠端監控和控制裝置的能力、雲端運算的增強能力，以及更快速的軟體更新。

然而，隨著我們的世界越來越緊密相連，保護這些產品免遭入侵也日益重要。從保護儲存的個人或敏感應用程式資料，到保護傳輸資料和實體裝置安全，在設計中實作無線連線的工程師需要在設計程序早期處理系統級安全功能，同時也需符合網路安全標準與法規的相關要求。

同樣地，協助擴展連線的無線微控制器 (MCU) 也需要滿足不斷變化的安全挑戰，以及網路安全標準和法規。

在本文中，我們將探討連網汽車和智慧住宅應用中不斷變化的無線連線安全挑戰，特別是汽車門禁、智慧型恆溫器、智慧型感測器和電子鎖，以及專為因應這些挑戰而設計的 MCU。

图 1. 使用智慧型手機管理汽車門禁

English Document: SSZTD63

汽車門禁面臨的網路安全挑戰

Bluetooth® 低功耗 (BLE) 無線連線用於汽車門禁解決方案，以進行測距和車輛鑰匙定位。安全威脅可能會導致汽車門禁安全受到威脅，並可能導致車輛或物品遭竊。

OEM 需要考慮多個層級的存取安全性，包括：

- **無線訊號測距安全：**操縱測距訊號可能會改變距離估計結果，使車輛鑰匙比實際距離更接近車輛。這些威脅依賴於無線技術，無線實體層和介質存取控制規格中的安全功能通常可解決此類威脅。例如，在最新的 Bluetooth 通道探測規格中，使用往返時間 (RTT) 封包交換和以標準化攻擊檢測器度量 (NADM) 為基礎的緩解措施，解決了對以相位為基礎的測距距離估計操作的威脅。
- **用於設定測距程序的通訊資料的通訊協定級安全性：**通訊協定級和應用程式級威脅包括無線操作期間的嗅探、中間人攻擊和重播攻擊。規定相關密碼編譯措施來加密正在通訊的資料，並驗證車輛鑰匙為有效實體，可減少攻擊。但是，加密安全性的安全性僅與用於加密或身分驗證的鑰匙相同。
- **最終應用程式操作的應用程式級安全性 (開啟車門、啟動引擎)：**在無線連線裝置中，透過無線傳輸或遠端接收的操作資料，可能會危及裝置運作或資料通訊安全性所使用的密碼編譯金鑰 (例如透過惡意軟體注入)。因此，Bluetooth LE 無線 MCU 必須以可信任方式支援通訊協定與應用程級的密碼編譯作業，以保護金鑰安全。透過安全啟動、安全韌體更新和安全偵錯存取，來確保裝置韌體運作的安全都是必要的措施。

此外，許多地區也有汽車網路安全法規，例如國際標準化組織 21434 等標準，要求在裝置開發與維護期間遵循相關網路安全程序。

智慧型恆溫器面臨的網路安全挑戰

智慧型恆溫器 (請參閱 图 2) 是在檢視智慧住宅技術時所面臨之優點與威脅的絕佳範例。這些裝置可讓屋主隨時隨地調整家中溫度，並透過整合式 Wi-Fi® 連線最佳化能源使用。

图 2. 客廳中的 Bluetooth 智慧型恆溫器

不幸的是，連線能力增加可能會使恆溫器受到威脅。例如，駭客可能會在無線傳輸惡意製作的訊框，以中斷恆溫器的運作，或迫使恆溫器離開網路。故意將裝置從網路中踢出並在重新連接後監控傳輸，使其可以使用暴力或字典攻擊來擷取和解密資料，進而導致使用者或供應商資料和憑證暴露。透過網際網路向恆溫器傳送惡意資料或程式碼 (例如惡意軟體)，或在恆溫器與遠端雲端伺服器間傳輸資料，即可透過遠端中間人攻擊來擷取資料。

為了緩解風險，設計人員必須遵循最新 Wi-Fi 安全標準，其中概述適用於身分驗證、金鑰協議和加密的經過驗證的密碼編譯演算法，以及用於保護管理框架的強制通訊協定，例如 Wi-Fi Protected Access 3。這些裝置需要支援最新的網路安全通訊協定 (例如傳輸層安全性 v1.3)，以保護網際網路傳輸的資料。此外，裝置也需要有效率地執行這些通訊協定，並安全地儲存執行期間使用的金鑰。

智慧型感測器與電子鎖面臨的網路安全挑戰

包括智慧型感測器 (運動、門窗感測器) 和電子鎖在內的電池供電設備越來越多地使用 Zigbee®、Thread 和 Matter 等網狀技術來滿足低功耗需求，同時仍可透過智慧住宅集線器連接至雲端。如嗅探、中間人和裝置接管等安全威脅可能會危及裝置資料或安全操作 (例如授予不良行為者電子鎖存取權)。在極端情況下，遭入侵的裝置可能會危及智慧住宅網路或生態系統。

保護這些網路需要保護感測器與集線器之間的通訊通道，以使只有受信任的裝置才能加入網路。

Matter 的設計旨在簡化智慧住宅產品的開發程序，並提供改良的通訊協定層級安全性。除了透過強大的密碼編譯套件 (如適用機密性的進階加密標準，適用完整性的安全雜湊演算法，以及適用金鑰交換與數位簽章的橢圓曲線密碼編譯) 來保護通訊通道，Matter 還會使用憑證和密碼架構通訊協定來驗證智慧住宅裝置，並確保只有正版產品才會加入生態系統。

以無線 MCU 緩解安全威脅

為降低安全風險，無線 MCU 應啟用安全資料通訊、安全金鑰交換、相互驗證、安全金鑰儲存、安全韌體更新和安全啟動操作。

CC2745P10-Q1、CC2755R10 和 CC3551E 等無線 MCU 提供整合的安全功能，以緩解惡意軟體和裝置接管攻擊造成的風險。其支援基本安全功能，例如安全啟動和具有回復保護的安全韌體更新。這些 MCU 具有整合式硬體安全模組 (HSM) 和專用控制器，用於處理硬體加速密碼編譯作業、安全金鑰儲存和隨機數字產生。HSM 為加密和金鑰處理操作提供了一個可信任的環境，進而有助於降低資料隱私和進階惡意軟體風險。這些 MCU 中的 Arm® Cortex®-M33 核心支援 TrustZone-M，進一步為安全軟體操作提供可信任的執行環境。

註冊商標

重要聲明與免責聲明

TI 均以「原樣」提供技術性及可靠性數據（包括數據表）、設計資源（包括參考設計）、應用或其他設計建議、網絡工具、安全訊息和其他資源，不保證其中不含任何瑕疵，且不做任何明示或暗示的擔保，包括但不限於對適銷性、適合某特定用途或不侵犯任何第三方知識產權的暗示擔保。

所述資源可供專業開發人員應用 TI 產品進行設計使用。您將對以下行為獨自承擔全部責任：(1) 針對您的應用選擇合適的 TI 產品；(2) 設計、 驗證並測試您的應用；(3) 確保您的應用滿足相應標準以及任何其他安全、安保或其他要求。

所述資源如有變更，恕不另行通知。 TI 對您使用所述資源的授權僅限於開發資源所涉及 TI 產品的相關應用。除此之外不得複製或展示所述資源，也不提供其它 TI 或任何第三方的知識產權授權許可。如因使用所述資源而產生任何索賠、賠償、成本、損失及債務等，TI 對此概不負責，並且您須賠償由此對 TI 及其代表造成的損害。

TI 的產品受均受 TI 的銷售條款或 ti.com 上其他適用條款，或連同這類 TI 產品提供之適用條款所約束。 TI 提供所述資源並不擴展或以其他方式更改 TI 針對 TI 產品所發布的可適用的擔保範圍或擔保免責聲明。

TI 不接受您可能提出的任何附加或不同條款。

郵寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265