参考資料

Technical Article

低消費電力ワイヤレス マイコンで、ワイヤレス コネクティビティの重要なサイバーセキュリティ上の課題を解決

Sainandan Reddy Reddy、Benjamin Moore、および Bhargavi Nisarga

ワイヤレス コネクティビティの革新に伴い、デバイスの接続能力を日常的な電子機器に拡張し、家庭や自動車にインテリジェンスが持ち込まれるようになっています (図 1 を参照)。インテリジェンスの強化とは、多くの機能や特長を意味します。デバイスのリモート監視と制御、クラウド コンピューティングによる拡張機能、ソフトウェアの更新迅速化などです。

ただし、身の回りの世界でコネクテッド (ネットワーク接続) 機能が強化されている現状で、これらの製品を侵入から保護することは不可欠です。保存された個人または機密のアプリケーション データの保護から転送中や物理デバイスのセキュリティの保護まで、設計にワイヤレス コネクティビティを実装するエンジニアは、設計プロセスの早期にシステム レベルのセキュリティ機能に対処しながら、サイバーセキュリティ規格や規制関連の要件を満たす必要があります。

同様に、コネクティビティの拡張を助けるワイヤレス マイコン (MCU) は、進化するセキュリティ課題やサイバーセキュリティ規格・規制を満たす必要もあります。

この記事では、ネットワーク接続型の車載とスマートハウスの各アプリケーションで進化する、ワイヤレス コネクティビティ セキュリティの課題を紹介します。特に、カーアクセス、スマート サーモスタット、スマート センサ、電子ロックなどを取り上げます。また、これらの課題に対処できる設計を採用したマイコンも紹介します。

図 1. スマートフォンを使用した車両アクセス

カー アクセスに関するサイバー セキュリティの課題

Bluetooth® Low Energy (BLE) ワイヤレス コネクティビティは、カー アクセス ソリューションで自動車のキーの距離と位置の特定に活用されています。セキュリティの脅威は、カー アクセスのセキュリティの侵害につながり、車両や持ち物の盗難につながる可能性があります。

OEM は、次のような複数のレベルでアクセスセキュリティを検討する必要があります。

- **無線信号の距離測定のセキュリティ:** 距離測定信号を操作すると推定結果が変化し、車両のキーが実際よりも車両に近い位置に表示される可能性があります。これらの脅威は、ワイヤレステクノロジーに依存しており、通常、ワイヤレス物理層およびメディアアクセス制御仕様のセキュリティ機能が、このような脅威に対処します。たとえば、最新の Bluetooth チャネル サウンディング仕様では、ラウンド トリップ タイミング (RTT) パケット交換と正規化された攻撃検出器メトリック (NADM) ベースの緩和を使用して、位相ベースの距離推定動作に対する脅威に対処します。
- **距離測定手順をセットアップするために通信したデータに対するプロトコル レベルのセキュリティ:** プロトコルレベルおよびアプリケーションレベルの脅威には、無線運用中のスニフィング、中間者攻撃、およびリプレイ攻撃が含まれます。通信データを暗号化し、有効なエンティティとして車両キーを認証するための関連する暗号化対策を規定することで、これらの攻撃を軽減できます。ただし、暗号化セキュリティは、暗号化または認証に使用されるキーと同等の安全性しかありません。
- **エンド アプリケーション操作向けのアプリケーション レベルのセキュリティ (車両ドアのオープン、エンジン始動):** ワイヤレス コネクティビティ デバイスでは、無線またはリモートで操作されたデータを受信することで、(たとえばマルウェアへの注入を通じて) デバイスの動作やデータ通信セキュリティに使用される暗号化キーが侵害される危険性があります。したがって、Bluetooth LE ワイヤレス マイコンがプロトコル レベルやアプリケーション レベルの暗号化動作を、キーを保護できる信頼できる方法でサポートすることが重要です。セキュアブートを使用したデバイスファームウェアの動作の保護、ファームウェアのセキュアな更新、セキュアなデバッグアクセスはすべて必要です。

加えて、多くの地域で車載サイバー セキュリティに関する規制が存在します。ISO 21434 などの規格は、デバイスの開発と保守の際に、関連するサイバーセキュリティ プロセスに準拠することを要求しています。

スマート サーモスタットのサイバーセキュリティの課題

スマート サーモスタット (図 2 を参照) は、スマートハウステクノロジーが直面する利点と脅威の良い例です。これらのデバイスを採用すると、家の所有者はどこにいても家の温度を調整し、内蔵の Wi-Fi® コネクティビティを活用してエネルギー使用を最適化することができます。

図 2. リビング ルームに設置された Bluetooth スマート サーモスタット

残念なことに、コネクティビティが強くなるとサーモスタットが脅威にさらされる可能性があります。たとえば、ハッカーが悪意を持って作成したフレームを無線で送信して、サーモスタットの動作を中断したり、強制的にネットワークから切断したりする可能性があります。デバイスを意図的にネットワークから切り離し、再接続後の送信を監視することで、総当たり攻撃または辞書攻撃を使用してデータをキャプチャおよび復号化することができ、ユーザーまたはベンダーのデータと資格情報が漏洩する可能性があります。インターネット経由でサーモスタットに悪意のあるデータやコード (マルウェアなど) を送信するか、リモートのクラウド サーバーとの間でデータを送信することで、リモートの中間者攻撃によりデータをキャプチャできます。

これを軽減するために、設計者は最新の Wi-Fi セキュリティ規格に従う必要があります。この規格では、認証、キー アグリーメントと暗号化に関する実績のある暗号化アルゴリズムを概説し、Wi-Fi Protected Access 3 のような管理フレームを保護するためのプロトコルを義務付けています。これらのデバイスは、インターネットで送信されるデータを保護するために、最新のネットワーク セキュリティ プロトコル (Transport Layer Security v1.3 など) をサポートする必要があります。さらに、デバイスはこれらのプロトコルを効率的に実行し、実行中に使用されるキーを安全に格納する必要があります。

スマートセンサと電子ロックに関するサイバーセキュリティの課題

スマートセンサ (モーション、ドア、窓のセンサ) や電子ロックなどのバッテリ動作デバイスは 図 3 に示すように、ZigBee®、Thread、Matter のようなメッシュ テクノロジーを使用する傾向が強くなっており、低消費電力要件を満たすと同時に、スマートハウスのハブを経由してクラウドに接続します。スニフィング、中間者攻撃、デバイスの乗っ取りなどのセキュリティの脅威は、デバイス データや安全な操作を侵害する可能性があります (たとえば、悪意のある行為者に許可された電子ロックアクセスなど)。極端な場合、侵害されたデバイスがスマートハウスネットワークやエコシステムに悪影響を及ぼす可能性があります。

図 3. 電子ロックとスマートセンサを装備したスマートホーム

これらのネットワークを保護するには、信頼できるデバイスだけがネットワークに参加できるように、センサーとハブ間の通信チャネルを保護する必要があります。

Matter は、開発を簡略化し、スマートハウス製品でプロトコル レベルのセキュリティを向上させることを意図した設計を採用しています。Matter は、機密性のための Advanced Encryption Standard、完全性のためのセキュアなハッシュアルゴリズム、キー交換とデジタル署名のための楕円曲線暗号などの強力な暗号スイートによって通信チャネルを保護すること

に加え、証明書とパスコードベースのプロトコルを使用してスマートハウス デバイスを認証し、正規の製品のみがエコシステムに参加することを保証します。

ワイヤレス マイコンによるセキュリティ上の脅威の軽減

セキュリティリスクを低減するために、ワイヤレス マイコンは、セキュアなデータ通信、セキュアなキー交換、相互認証、セキュアなキーストレージ、セキュアなファームウェア更新、セキュア ブート動作を実現する必要があります。

CC2745P10-Q1、CC2755R10、CC3551E などのワイヤレス マイコンは、セキュリティ機能を内蔵しており、マルウェアやデバイスの乗っ取り攻撃に起因するリスクを軽減します。これらのマイコンは、セキュア ブートや、ロールバック保護機能を備えたセキュア ファームウェア更新などの基本的なセキュリティ機能をサポートしています。これらのマイコンは、統合型ハードウェア セキュリティ モジュール (HSM) に、ハードウェア アクセラレーション形式の暗号化操作、セキュア キー ストレージ、乱数生成を処理する専用コントローラを搭載しています。HSM は、暗号化操作とキー処理操作のための信頼できる環境を提供し、データプライバシーと高度なマルウェアリスクを軽減します。これらのマイコンが搭載している Arm®Cortex®-M33 コアは TrustZone-M をサポートしています。この結果、セキュアなソフトウェア動作に適した、信頼できる実行環境をさらに実現できます。

商標

すべての商標はそれぞれの所有者に帰属します。

重要なお知らせと免責事項

テキサス・インスツルメンツは、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、テキサス・インスツルメンツ製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した テキサス・インスツルメンツ製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている テキサス・インスツルメンツ製品を使用するアプリケーションの開発の目的でのみ、テキサス・インスツルメンツはその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。テキサス・インスツルメンツや第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、テキサス・インスツルメンツおよびその代理人を完全に補償するものとし、テキサス・インスツルメンツは一切の責任を拒否します。

テキサス・インスツルメンツの製品は、テキサス・インスツルメンツの販売条件、または ti.com やかかる テキサス・インスツルメンツ製品の関連資料などのいずれかを通じて提供する適用可能な条項の下で提供されています。テキサス・インスツルメンツがこれらのリソースを提供することは、適用されるテキサス・インスツルメンツの保証または他の保証の放棄の拡大や変更を意味するものではありません。

お客様がいかなる追加条項または代替条項を提案した場合でも、テキサス・インスツルメンツはそれらに異議を唱え、拒否します。

郵送先住所:Texas Instruments, Post Office Box 655303, Dallas, Texas 75265

重要なお知らせと免責事項

TI は、技術データと信頼性データ (データシートを含みます)、設計リソース (リファレンス· デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、TI の販売条件、または ti.com やかかる TI 製品の関連資料などのいずれかを通じて提供する適用可能な条項の下で提供されています。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。

お客様がいかなる追加条項または代替条項を提案した場合でも、TI はそれらに異議を唱え、拒否します。

郵送先住所：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265