ホワイトペーパー

ソフトウェア IP と機密データの保護

ルネサスエレクトロニクス IoT インフラストラクチャビジネスユニット

Markus Vomfelde（シニアマネジャー）、

Brad Rex（シニアプロダクトマーケティングマネジャー）、

Zachary Ellis（シニアマーケティングスペシャリスト）

2020 年 1 月

概要

昨年発行したホワイトペーパーで「コネクテッドワールドにおけるセキュリティ」について解説しましたが、今回は、MCU やその応用製品に保存されたデータを保護するための技術や、データ保護の必要性について詳細に説明します。ある架空のデバイス開発を例に、データ保護のニーズがどこにあるのか、また潜在的な攻撃シナリオに対してどのようなレベルのセキュリティを実装すべきかついて解説します。この開発例を検討することで、御社がこれから開発するデバイスに保存されるデータのセキュリティ計画や、必要なセキュリティ対策の実施方法に役立つと考えます。

デバイスに保存されたデータを保護する理由とは

ローカル（デバイス内に）保存されるデータには、操作中に実行されるアプリケーションプログラムと操作中に使用されるローカルデータの 2 種類があります。アプリケーションプログラムには製造元のノウハウや IP（知的財産）が含まれているため、デバイスの製造元は、その IP が盗まれたり、再利用されたり、コピーされたりするのを防ぎたいと考えます。IP データは通常デバイスに保存されますが、デバイスは同じ属性を持つため、データは別の同一のデバイスにも転送および更新が可能です。ローカルデータは、製造最終段階のデバイスのセットアップ中やデバイスの動作中に保存されます。すべてのデバイス内部には、デバイスごと異なるデータが存在し、通常アプリケーションコードよりも頻繁に更新されます。ローカルデータにはデバイスの使用環境に関係する機密情報が含まれている可能性があります。例えばデータが、デバイスを使うユーザーに関係する情報の場合、これを保護したいという動機になります。 データ保護の動機はメーカーやユーザーで異なってはいますが、外部アクセスからのデータ保護は、両タイプのデータについて必須な条件となっています。

デバイスはインターネット接続されますか？

これは、セキュリティの実装度に関わる非常に重要な質問です。ネットワーク接続が無くスタンドアロンで動作するデバイスの場合、攻撃の可能性は物理的アクセスに限定されます。デバイスメーカーのデバイス内 IP を保護するという課題は残りますが、ユーザーデータに関しては、攻撃者がデバイスに物理的にアクセスすることは困難であるため、ユーザーデータへのアクセスや攻撃はきわめて困難と考えます。次の接続レベルは、インターネットに接続しないローカルネットワーク環境で動作するデバイスです。 この環境では、攻撃者はデバイスへの攻撃を開始する前にローカルネットワークに侵入する必要があります。よって、デバイスをしっかり外部アクセスから保護し、ローカルネットワークへの入り口にならないように保護する必要があります。最後に、インターネットに直接接続されるデバイスの場合、最高レベルのセキュリティの実装が必要となります。潜在的な攻撃は、ローカル接続とは比較できないほど多く、グローバルで無尽蔵のコンピューティングパワーで攻撃可能なため、デバイス内に保存されているデータへの攻撃は今後ますます増加していくと考えます。

アプリケーション事例と必要なセキュリティ

デバイス内のデータ保護について、もっと詳しく説明するために具体的なアプリケーションで説明します。ここで紹介するデバイスは、製品化されたものではありませんが、実際のデバイスセキュリティ要求を反映するのに十分な応用例です。

まず、会社の立ち入り制限区域へのアクセスを可能にする指紋センサー付きのドアロックがあるとしましょう。このセンサーは、非常に優れたアルゴリズムを搭載しており、このドアを頻繁に利用する 50 人分の指紋データを非常に小さいメモリサイズでデバイス内部に保存します。この機能は、この市場の顧客にとって非常に魅力的です。それは、デバイス内に登録されたユーザーがアクセスした場合、すぐにドアが開くからです。非登録の利用者がアクセスした場合、デバイスは会社の Wi-Fi ネットワークを介してサーバーに接続し、そこに保存されている指紋と比較し開錠します。この場合、ドアが開くのに時間がかかるため、デバイス内に保存されている指紋データは非常に有効です。また、この Wi-Fi ネットワークはインターネットにつながっており、製造元はデバイスのファームウェアを無線更新することが可能になっています。

デバイスメーカーは、アプリケーションプログラムにセキュリティを実装する方法を検討する必要があります。 このホワイトペーパーでは、デバイスに保存されているデータ保護の説明に注力し、操作やプログラム更新中にやり取りされるデータ（移動中のデータ）については説明対象としないのでご注意ください。

保護が必要な最初の種類のデータは、指紋アルゴリズム IP です。これはデバイス自体の価値と等価であり、攻撃者が直接またはデータ接続を介してデバイスにアクセスする攻撃から保護する必要があります。デバイスはネットワークに接続されているため、デバイス内の MCU を読み取り、コピー、または再プログラミングする行為から保護するだけでは不十分です。接続を介して、ソフトウェア IP のメモリダンプ攻撃からも保護する必要があります。

留意する必要がある 2 番目の種類のデータは、ユーザーデータです。この例では、保存されている指紋データとネットワークアクセスデータになります。上記で説明したように、攻撃者は、デバイスへの物理的なアクセス方法ではユーザーデータを取得するのが非常に困難なため、インターネット接続経由のアクセスの可能性が高くなります。よって、この攻撃に対するセキュリティ保護が重要です。ユーザー自身での対応が必要な部分は、ネットワーク自体の保護です。さらに、デバイス内にもセキュリティを実装しないと、システム全体のセキュリティ対策は完結できません。

IP を保護する

この応用例の保存データを保護するために、複数のセキュリティパーツが必要です。 データセキュリティに焦点を当てると、このデバイスには安全なデバイス ID を持つ MCU が使用され、信頼性が確立されていることが前提となります。次のホワイトペーパーではデバイス ID 機能に焦点を当て、どのような MCU が必要かについて説明します。

IP の保護に関しては、メーカーの IP セキュリティ計画と保護範囲に応じて、実装する保護レベルが決まります。開発の最初のステップとしては、使用する MCU が、不審なデバッガーアクセスによる再プログラミングに対する保護機能を提供している必要があります。この機能の実現には、さまざまな実装方法があるので、それらを詳細に比較検討し判断する必要があります。

多くのベンダーが、さまざまなセキュリティ機能や保護方法を提供しています。よって、提示されている機能や保護方法が、デバイスの意図しない変更を防ぐためだけでなく、データセキュリティ対策のために推奨されていることを確認する必要があります。次のレベルでは、セキュア領域と非セキュア領域をサポートするメモリを実装した MCU を使用する必要があります。これにより、MCU コアが IP ソフトウェアに直接アクセスできなくなり、意図しないデータダンプが簡単に実行できなくなります。

ここでも、さまざまなソリューションがあります。最も一般的な方法は、メモリ保護ユニット（MPU）の実装です。あるいは、ARM®ベースのマイクロコントローラーの TrustZone®を実装する方法です。最後は、IP をデバイスに暗号化して保存する方法です。この方法は、物理的な攻撃に対しても盗難耐性がはるかに高くなります。IP は暗号化され不揮発性メモリに記録されているので、カプセル化手法や電子顕微鏡解析といった方法でデータを読みだしても IP 内容の解読は不可能です。

しかし、MCU 内に保存されている暗号化キーに対して、外部読み取りや CPU からの直接アクセスを防止する必要があります。暗号化キーを MCU 内のセキュアな領域にしっかり保存することで、暗号化キーを読み出し、それにより IP データを復号し、不正に IP を解読する行為を阻止することができます。これは IP を保存する最も安全な方法ですが、アルゴリズム IP は暗号化されているので、MCU の RAM 上で実行可能なコードに復号化してから実行する必要があります。よって、MCU のセキュア領域には、アルゴリズムが復号化・実行される RAM 部分も含める必要があります。

保存データを保護する

第２ステップとして、エンドユーザーがデバイスに保存するデータを決定する必要があります。この例では、一部の指紋データは高速照合ができるようにデバイスのローカル領域に保存されています。またデバイスは、すべての指紋データが保存されているサーバーへのアクセスを行うために、顧客ネットワークにも接続されています。よって、デバイスメーカーはファームウェアの更新を行うことも可能です。ユーザーデータに対するセキュリティ対策は、デバイス内の IP に対しても適用できます。運用段階で、どの程度のセキュリティ実装が必要か詳細に検討し決定する必要があります。ネットワーク経由で攻撃者にデータを提供する可能性のあるあらゆる種類のマルウェアのインストールを回避するために、デバイスは、例え一部のデータであっても、外部からの読み取り行為や再プログラミング行為から保護する必要があります。また、MCU が保存されたユーザーデータに不用意にアクセスすることを制限するため、信頼できるメモリ領域とそうでないメモリ領域の実装は非常に重要です。これにより、攻撃はより困難になり、少ないパフォーマンス低下でより強固な保護機能を提供できます。

最後に、指紋データの暗号化処理は MCU には大きな負担になりますが、万全なセキュリティ対策にはどうしても必要な手段です。アルゴリズムが動作を開始する前に、保存されているすべての指紋データを復号化する必要があるため、この処理に対する MCU 性能や処理時間を事前に考慮する必要があります。一般に、顧客施設内にあるデバイスへの物理攻撃は非常に困難なため、指紋データの暗号化処理が本当に必要な要件なのかは良く検討する必要があります。指紋照合アルゴリズムが入手できない状況で、保存された指紋データで攻撃者は何ができるでしょうか？さて、ネットワーク経由でのデータアクセスは少し状況が異なります。 この場合は、パフォーマンスへの悪影響はほぼゼロです。サーバーへアクセスする必要があるのは、1 日に 1～2 回だからです。もし誰かがデバイスに手を加え、ネットワークアクセスコードを暗号化されていないデータとして読み出すことができる場合、顧客ネットワークへのフルアクセスが可能になり、これはより危険で予測不能になる可能性があります。繰り返しますが、暗号化されたデータへの望ましくないアクセスを避けるために、データ自体よりも高いセキュリティで暗号化キーを保存する必要があることを強調します。そのための非常に効果的な方法は、各 MCU で一意にラップされたキーですが、この「キー管理」についてのトピックスは、このホワイトペーパー以降のシリーズで説明したいと思います。

結論

セキュリティを実装する方法とレベルの決定は、常に、アプリケーション、予想される攻撃者、およびそれらの保護するデバイスまたはデータへのアクセスに依存します。つまり、セキュリティを実装する度に、各開発プロジェクトの開始時に、この事を考慮して、セキュリティ実装のすべてのニーズに適合する MCU の選定を行う必要があることを意味します。ここでの例は、ローカルに保存されたデータに対してさまざまなセキュリティがあることを示しており、移動中のデータや無線による安全なプログラミングを考慮すれば、さらに追加のセキュリティ機能が必要になることを示しています。今後のホワイトペーパーの展開の中で、この情報を提供し、コネクテッドワールドに対応できる安全な製品設計をサポートしたいと思います。

ルネサスでは、このホワイトペーパーで説明した課題に対して、対応可能な MCU [1]を数多く提供しています。 詳細については、当社のウェブサイトをご覧ください。

参考資料

[1] RA Family of 32-bit Arm Cortex-M MCUs
RX Family of 32-bit MCUs
Synergy Platform of 32-bit Arm Cortex-M MCUs + qualified software