ホワイトペーパー

コネクテッドワールドにおけるセキュリティとは

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 Kimberly Dinsmore（シニアエンジニア）

2019 年 9 月

概要

「セキュリティ」とう言葉について誰かに質問すると、何かしらの回答がすぐ返ってきます。しかし、電子デバイスの分野に限定したとしても、回答者のおかれた状況によってその返答は大きく異なってしまいます。一般消費者にとって、「セキュリティ」とは通常、指定した人以外は自分の個人データが利用できないことを意味します。しかし、マイクロコントローラを搭載した製品の場合、保護すべきエンドユーザーの個人情報が組込まれていることはありません。ここで、「セキュリティ」という言葉の別の側面を考えてみましょう。ソフトウェア開発者にとっての「セキュリティ」とは、コードを盗むことができないことを意味します。また、 OEM にとっての「セキュリティ」とは、誰も自社製品をクローンコピーして販売することができないことを意味します。スマートフォンなどのインターネットデバイスを使ったサービスを提供するサービスプロバイダーにとっての「セキュリティ」とは、多くの場合、誰も適切な許可または対価の支払いなしにサービスを利用できないことを意味します。政府にとっての「セキュリティ」とは、DDoS 攻撃の一部として、ウィルスを侵入させたインターネットデバイスを武器として使用させないことを意味します。これらのセキュリティに関する定義はすべて、市場セグメントに関係なく、マイクロコントローラおよびそれを内蔵した製品に適用されていることは間違いありません。

セキュリティの専門領域に入るとすぐに、膨大な数の耳慣れない専門用語や略語で溢れており、思考が停止してしまうかも知れません。本ホワイトペーパーでは難解な専門用語を避けながら説明を進めて行きますので、ご安心下さい。それでは 1 つ質問ですが、 MCU が組込まれたシステムにセキュリティをどのように組込めば良いのでしょうか。この質問に 1 つずつ回答することで解説を進めて行きます。

ステップ 1：最初からセキュリティの設計に取り組む

新製品の開発を開始するとき、経営陣は進捗状況を確認したいと考えています。つまり、経営陣とってはプロトタイプが機能することが重要であって、安全が確保されている必要はありません。セキュリティ機能は、経営者や投資家を感動させる派手なデモやってくれることはありません。開発の最終段階までセキュリティ機能の開発を延期できることは魅力的ですが、その誘惑に負けないでください。セキュリティ機能の立上げには時間がかかり、多くの場合、経営陣へ啓発を促すことも必要になります。しかし、セキュリティ開発を後付けできないことは、これまで何度も証明されています。セキュリティはアドオンではありません。 これは、製品アーキテクチャ基盤の基本要素です。 後から追加しようとすると、殆どの場合、完全に再設計することになってしまいます。バイト単位で生成・送信されたデータストリームは、暗号化されたデータブロックに変換できませんし、ベタ書きのプレーンテキストの秘密キ

ーは、魔法のように安全に保存されたデバイス固有のキーとすることもできません。

ステップ 2：開発する製品は業界または政府の規制下にありますか？

この要件は、セキュリティに関するあなたの考えを覆すかもしれません。業界で特定の暗号化機能スイートが必要な場合は、同じレベルの保護を提供する代替手段がある場合でも、その正確なスイートを使用する必要があります。金融取引とエネルギーメーターは、その代表例で、特定の規制が存在し、それを遵守する必要があります。これから開発する製品の規制要件を調査・理解し、製品が使用される地域の政府規制を必ず開発仕様に含めてください。

ステップ 3：何を保護するのか？

ほとんどの企業は、コストを調べることで GDPR（欧州連合一般データ保護規則）のリストを決定します。そのため、GDPR の罰金が高額になっています。政府は、金銭的なインセンティブがなければ、企業はセキュリティ侵害を予防するよりも積極的にセキュリティ侵害を管理する可能性が高いことを認識しています。このリストを作成する最初のステップは、通常、デバイス自体とデータ（ファームウェア、キー、および顧客情報）に焦点を当てています。しかし、デバイスを超えてシステム全体を検討して下さい。 データが機密であるとは考えないかもしれませんが、誰かが通常動作中のデバイスを悪用して、DDoS 攻撃のような有害な影響を与えることができるかも知れません。デバイスが重要な機能を担っている場合、その機能を不適切に変更できるものから保護する必要があります。 キーを使用してサービスを有効にする場合、サービス自体が保護される必要があります。

ステップ 4：開発する製品やシステムの脆弱性を想定していますか？

繰り返しになりますが、デバイスとそれを展開したインフラストラクチャの両方を考慮してください。デバイスに焦点を当てた場合、明らかな技術的脆弱性はインターネット接続にあります。 非 Linux 系デバイスの IP 接続は一般にセキュリティ攻撃の標的ではないため、MCU ベースの製品は多少有利ですが、送信データが標的になるかは議論の余地が残ります。もし、インターネット経由でファームウェア更新を実行して、そのコードを保護したい場合 、IP 接続は明らかな脆弱になります。デバイスが IP 接続されていない場合でも、外部へのすべての接続を検証してください。 ここで製品の動作環境を見るとき、人的要素も考慮することを忘れないでください。 どんな最先端のセキュリティ技術でも、賄賂をもらった関係者による行為は、残念ながら回避することはできません。よって、悪意のある行為や、または単にいたずらをやりたい関係者が存在しどんな行為を引き起こすかを想定しておく必要があります。

ステップ 5：誰を信頼しますか？

「誰も信用するな」という格言があるように、セキュリティソリューションにはコストがかかる事実を回避することはできません。しかし、存在しない脅威に対してあなたの製品を保護することにお金を投入する必要はありません。オンサイト（信頼できる施設）で製造している場合、おそらく安全なプログラミングソリューションに投資する必要はありません。 ただし、オフサイト（業者委託）でデバイスのプログラミングをする場合、またはキーやその他の機密データを使用してデバイスをプログラムする必要がある場合は、安全なプログラミングソリューションが必要になる場合があります。

ステップ 6：対応範囲を定義して下さい

十分な時間とリソースがあれば、どんなセキュリティも突破することは可能です。よって、どこまでの保護が必要かその範囲を明確にする必要があります。 指定したデバッガー以外のアクセスを禁止することはとても簡単で有効なセキュリティ対策です。一方、 動作中の MCU を開封して電子顕微鏡で動作解析する行為は、技術的にも大変困難なので対抗措置が必要かは判断が分かれるかも知れません。これらの制限は、対象製品の規制当局によって定義される場合もありますが、多くの場合、単に常識的なものです。 たとえば、ファームウェア IP を保護することが主目的である場合、サイドチャネル解析に耐性のある MCU は必要ありません。

ステップ 7：計画を立てて下さい

設定した対応範囲内で、信頼できる技術要素を活用して、脆弱性から資産を保護する方法を決定して下さい。脅威モデル、脅威分析、セキュリティ評価、またはセキュリティポリシーと呼ばれることもありますが、この作業には、開発リソースと予算のバランスを取るために十分な時間を費やして下さい。最終ステップは、何らかの事故が起きた場合に非常に重要です。 製品に必要なセキュリティを組込んでいたのかを検証される場合、十分な対応を実施したことを証明できれば、あなたに過失があったとする主張に対抗する証拠として役立ちます。

脅威、脆弱性、および信頼できる関係者の組み合わせは、組み込みデバイスの数と同じくらい多様ですが、幸いなことに、そこにはいくつかの共通するテーマと同じソリューションが存在しています。

保存したデータの保護

デバイスセキュリティの基本要件は、デバイスにデータを安全に保存できることですが、セキュリティの世界のすべてのものと同様に、安全な保管場所についてはさまざまな側面があります。 デバイスに外部接続がない場合、デバイスに搭載された MCU は、すべてのデバッガーおよびプログラマーからのアクセスを無効化または保護することにより、非常に簡単にセキュリティを保つことができます。MCU のフラッシュメモリを再プログラミングすることでデバイスが誤って破損しないようにする必要がある場合、多くの MCU にはフラッシュの一部またはすべてを OTP として指定する機能があり、MCU の自己プログラミングでも消去または再プログラミングを防ぐことができます。ただし、デバイスに外部接続機能がある場合は、MCU のコードとデータを論理的に「信頼できる」カテゴリと「信頼できない」カテゴリに分け、「信頼できる」データへのアクセスを「信頼できる」コードのみに制限することを検討してください。信頼領域を確保する最適な方法は、メモリ保護ユニット（MPU）や Arm®TrustZone®などのメカニズムを介してハードウェアで実施する方法です。 しかし、この方法でも完璧なセキュリティを確保できるわけではありませんが、「信頼できる」領域を攻撃対象からそらす効果はあります。

デバイス ID

製品をインフラストラクチャに接続する場合、製品を一意に識別する何らかの方法が必要になります。各デバイスに一意の ID を付与するには、さまざまな方法があります。 一部の MCU には固有の ID が既に組み込まれていますが、これらは単純なシリアル番号である場合がほとんどです。よって、中央のコマンドセンターでどのデバイスがどこに展開されているかを把握するためには、シリアル番号と配置場所のマッピングテーブルを作る必要があります。これはこれで便利ですが、暗号化された一意の ID は、転送中データの保護などのセキュリティソリューションを追加する場合更に役立ちます。

暗号化 ID は、さまざまな暗号化手法の資産として活用されますが、デバイス ID を暗号化キーとする場合もその１つで、 ２つの基本的なオプションがあります。

- 同一のキーでデータの暗号化と復号化の両方を行う対称暗号化の場合、コマンドセンターは、各デバイスの対称キーを知っている必要があります。

- 非対称暗号化の場合は、2 つのキーが必要です。1 つはデータの暗号化用で、もう 1 つはデータの復号化用です。この２つの機能は入れ替え可能で、デバイスは 1 つのキーをプライベートに所有するができます。

注意が必要な部分は、どうやって最初にデバイス上にキーを保存するかです。コマンドセンターは、キーを知っているか、キーが信頼できることを知っておく必要があります。これはプロビジョニングと呼ばれます。御社のセキュリティ評価の結果、信頼できる技術者が信頼できる設備を使って製品をインストールしてプロビジョニングできると判断した場合、御社は、その設備と人員でキーを生成または書込みする工程を御社ソリューションに含めることが可能です。ただし、一般消費者によって製品が組み込まれる場合は、デバイスを安全にプロビジョニングする必要があります。 これは、安全なプログラミング処理で実行可能です。

転送中のデータ保護

転送中のデータを保護するには、機密性、データ整合性、データ発信元、エンティティ認証、および否認防止の 5 つの目標があります。この５つの点は、このホワイトペーパーで説明できる内容ではありませんので、通信インフラストラクチャとは何かに絞って説明します。デバイスが閉じたインフラストラクチャ内の専用バスを介して通信している場合、データ保護要件を満たすためのソリューションは、デバイスが Wi-Fi 接続を介してインターネットに接続されている場合とはまったく異なります。後者は好ましくないシナリオですが、IoT デバイスの最も一般的な使用例でもあります。IP 接続を介して転送データを保護する基本的な構成要素は、暗号 ID です。 暗号 ID は少し過剰に見えるかもしれませんが、製品が IP 接続されている場合は必須要件になります。

セキュアなプログラミング

ほとんどのセキュリティソリューションと同様に、セキュアプログラミングは複数の問題を解決でき、複数のオプションが利用可能です。セキュアな量産ソリューションは、暗号化されたファームウェアイメージを配信することで、IP 盗難、クローニング、および過剰生産の問題を解決できます。これを可能にするためには、特定のデバイスプログラマ内でのみ配信データの解読でき、書込んだデバイスの正確

な数を報告する監査レポートを受け取る必要があります。デバイス固有のキーを MCU に書き込む安全なプログラミングソリューションもあります。さらに高度なソリューションも存在します。これは、MCU 自体が非対称キーペアを生成し、公開キーをエクスポートし、その公開キーを含む署名付き証明書を受信して保存し、最終製品の認証に使用できる監査レポートと承認済み証明書一式の両方を生成できます。このソリューションを実現するには、MCU エコシステムパートナーによる強力なサポートが必要となります。

「セキュリティ」は「１つで何にでも対応可能な」ソリューションではありません。 開発フェーズのスタート時に製品の範囲要件を決定し、強力なパートナーネットワークを持つ献身的なシリコンベンダーがサポートする MCU で、必要となるハードウェア機能、ソフトウェアサポート、ソリューションデモを備えた MCU を選択することが重要です。セキュリティは手ごわい機能に思えるかもしれませんが、堅牢なエコシステムサポートを備えた適切な MCU を選択することで、今日のコネクテッドワールドに対応可能な安全な製品を開発することが可能です。