ケーススタディ

スマート
Microchip 社の暗号対応 CEC1712 MCU と Soteria-G2 カスタム ファームウェアは、ルートキット、ブートキット等の悪質なマルウェアを阻止すべく設計されています。

コネクテッド
Microchip 社のソリューションを使うと、サーバ、通信機器、自律走行コネクテッドカーの OS、ADAS、その他の外付け SPI フラッシュから起動するシステムのセキュリティを保護できます。

セキュア
Microchip 社の Soteria-G2 カスタム ファームウェアを使うと、外付け SPI フラッシュメモリから起動する OS がハードウェア ルートオブトラストを使ってセキュアにブートできます。

データセンター プラットフォーム ファームウェアのレジリエンス

ネットワーク アーキテクチャ、クラウド インフラストラクチャ、スマート製品の設計、無線の進化、スマートシティの構築、自律走行車の運転等の分野で世代交代が進むたびに、コスト低減、効率向上、性能向上の新たな機会が多数生まれます。ハイパースケール データセンターと新しいデータストレージ構造は需要の増加に伴って成長しています。企業、政府、公共サービス、消費者、公共および民間の各種機関は全て、コネクテッド化が進む世界で新しい要素が発明されるたびにいち早くその進歩を利用する事を望んでいます。

新たな飛躍への一歩一歩を心待ちにしている集団は他にもあります。それはハッカーたちです。

最初のハッカーは、20 世紀初頭に悪ふざけで電話交換台にアクセスして電話回線を切り換えた 10 代の若者たちであったという人もいます。1960 年代にハッカーと言えば、新しいコードを考案する事で想定された性能の限界を超えて演算性能を高める、メインフレーム コンピュータ プログラマの事をしばしば意味しました。ハッカーは悪の称号ではなかったのです。メインフレームの操作方法を進歩させた人を意味し、同業者から尊敬される存在でした。次なる標的は通信事業者でした。才能のある者たちが、タダで遠距離通話をするためにネットワークに接続して長距離通話転送トーンを模倣するデバイスを研究しました。これらのフリーカー(電話ネットワークの知識を持った変わり者を表す造語) は、長距離電話を安くかけられるブラックボックスのグレーマーケットを生み出しました。電話ネットワークがソフトウェア ベースとの制御システムに移行する頃には、ハッカーの標的も台頭してきた PC コンピュータ ネットワーク等移行しました。そしてある時点でハッカーは一線を越え、無害な実験者から犯罪者へと変貌しました。

コネクテッドな未来では、セキュリティ ベンダーとメーカーによる対応が必要な各種ハードウェア、ソフトウェア、サービス停止が起きるでしょう。以前は想像もできなかった脆弱性が、善意の人たちだけでなく、悪意を持った者たちをも磁石のように引き付けています。

最近まで政府系機関と企業環境内では USB メモリドライブの悪用防止対策として、コンピュータの USB ポートを物理的にふさぐ措置が採られていました。今日そのような方法は、痛むからといって歯を抜いてしまうのと同じくらい時代遅れです。

先進技術がもつ引力のように人を引き付ける力は、データ改ざんまたは情報漏洩の脅威よりも (それらが起こらないうちは) はるかに強いようです。

無線ネットワーク事業者が 5G 時代が到来したと宣伝し、IoT 対応デバイスが大衆市場に普及する準備が整っていると主張しても、現実はもっと漸進的な過程をたどっています。データセンターとストレージ システムの設計者が将来のインフラストラクチャ ソリューションを開発している一方で、ハッカーはそれらの脆弱性を探しています。ハッカー コミュニティは、全国的な 5G アクセスと数十億の IoT ノードの到来を、貴重なデータへのバックドア アクセスと無秩序状態への入り口として捉えているかもしれません。ソフトウェアおよびハードウェア ベースの混乱に利用されるデバイスとシステムの数は、かつてないほど膨大になるでしょう。ハッカーのビジネスモデルは不正コードの新たな侵入口に狙いを定めてくるため、ボットとスクリプトを考慮する必要があります。

**ストレージ システムの設計者が
将来のインフラストラクチャ
ソリューションを開発している一方で、
ハッカーはそれらの脆弱性を探しています。**

セキュリティは Microchip 社の製品ポートフォリオの核心

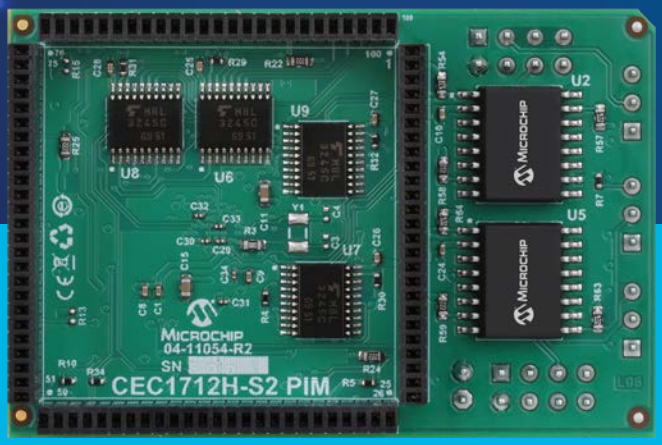
ハッカーによる攻撃にさらされているのはハードウェアとコンピュータ システムだけではありません。保護されていないシステム部品も攻撃に曝されています。セキュリティの世界は市場特有の要件に満ちており、市場の牽引役は常に変化しています。セキュリティ侵害が公になれば企業は業界での信用を失い、収益と株価が暴落する可能性があります。残念ながら、プラットフォーム ファームウェア レジリエンスに関する標準的なセキュリティ ガイドラインは普遍的に実施されていません。どんなセキュリティ手法でも規格、業界の自主規制、機能、コスト、顧客要件、安全性、性能、ネットワーク パラダイムと整合させるには、非常に多くの事を考慮する必要があります。

組み込み設計において、セキュリティ手段は内蔵ストレージ、通信ハードウェアおよびプロトコル、ノードおよびゲートウェイ実装、デバイス管理システム、クラウド コンピューティング等の多くの層に関わります。セキュリティは組み込み設計の構想段階から考慮する必要があります。Microchip 社には製品、知的財産、企業ブランド、評判、収益を保護するソリューションを提供してきた長い歴史があります。

Microchip 社は、包括的なセキュリティ ポートフォリオとセキュリティ パートナー プログラムによって製品を保護する組み込みセキュリティ ソリューションを提供しています。セキュリティへの最先端の取り組みと攻撃に対する即座の対応により、Microchip 社は設計ごとの要件を満たすカスタム ソリューション開発できる柔軟性を提供します。認証デバイスとトラステッド プラットフォーム モジュールから暗号対応マイクロコントローラおよびマイクロプロセッサ、ソフトウェア ライブラリ、拡張プロトコルまで、セキュリティへの取り組みは Microchip 社の事業の中核を成しています。

外付け SPI フラッシュメモリに関連した脆弱性は OEM に注目されてきました

チャレンジ



高性能サーバ技術をもったある世界的プロバイダは、ハードウェアおよび OS ベースのセキュリティに関する戦略をアップグレードしようとしていました。外付け SPI フラッシュメモリから起動するシステムのルートキットおよびブートキットにまつわる脆弱性は、多くの OEM の懸念事項でした。

ルートキット マルウェアは、活動中もユーザに気付かれないように設計されています。サイバー犯罪者はルートキットでコンピュータ システムを遠隔制御する事でセキュリティ プログラムを無力化し、個人データ、パスワード、銀行口座番号、クレジットカード情報を盗む事ができます。ブートキットはマザーボードのマスタ ブートレコードを改ざんし、オペレーティング システムが読み込まれる前に不正プログラムを実行します。

Microchip 社の新しい暗号 MCU、カスタム ファームウェア、プロビジョニング サービスは、不正プログラムを検出、実行されるのを防ぐ事を目的に設計されています。このお客様は、以下の項目に対する多面的な戦略に興味を持っていました。

- セキュリティ侵害に対する迅速な対処
- 脅威の理解と対応策
- セキュアデバイス戦略からセキュア プラットフォーム戦略への移行
- セキュリティ機関および規格の変化への対応
- 専門知識とリソースの導入
- レガシーデバイスおよびプラットフォームへの影響の理解

ソリューション

Microchip 社のチームはお客様の要件をより深く理解するためにお客様と面談し、プロジェクトに影響を与える諸要因について助言し、暗号対応 CEC1712 MCU と Soteria-G2 カスタム ファームウェアを柱としたソリューションを推奨しました。そのプロジェクトは 2019 年に始まりました。

Soteria-G2 カスタム ファームウェアは Arm® Cortex®-M4 ベース MCU である CEC1712 で実行します。Soteria-G2 は、外付け SPI フラッシュメモリから起動する OS がプリブートモードのハードウェア ルートオブ トラストを使ってセキュアにブートする事を可能にします。CEC1712 は、動作中の鍵無効化とコードのロールバック保護を実装できるため、フィールドでセキュリティ更新が可能です。CEC1712 は NIST 800-193 ガイドラインに準拠しており、改ざんに対する保護、検出、回復が可能であり、トータルシステム プラットフォーム ファームウェア回復力を実現しています。ハードウェアによるルートオブ トラストを利用したセキュアブートは、マルウェアがシステムに侵入するのを防ぐために不可欠です。さらにこの方法を採る事で、製造者が信頼していないソフトウェアを使ったシステムの起動を不可能とする事ができます。

CEC1712 と一緒に Soteria-G2 ファームウェアを使う事でコード開発が簡単になり、セキュアブートを迅速に実装できます。Soteria-G2 は、CEC1712 の ROM に実装されているセキュア ブートローダをルートオブ トラストとして使います。

CEC1712 のセキュア ブートローダは、ファームウェアを外付け SPI フラッシュから読み込み、復号、認証します。次に、この認証された CEC1712 のコードはアプリケーション プロセッサ用に SPI フラッシュに保存されたファームウェアを認証します。アプリケーション プロセッサは 2 個まで (SPI フラッシュ各 1 個) サポートできます。カスタムデータの事前設定はオプションとして提供しています。事前設定は、過剰供給と偽造防止に向けたセキュアな製造ソリューションです。このソリューションは開発期間を数ヶ月も短縮できるだけでなく、設定に関するロジスティクスをシンプルにできます。つまり、サードパーティによる設定と認証に関連した費用を使う事なくデバイスを簡単に保護、管理できます。

しかし、プラットフォーム ファームウェアのレジリエンスは 1 地点対策では実現できません。業界のガイドラインによると、ファームウェア セキュリティの全ての潜在的侵害は防止される必要があり、プラットフォーム内の全てのデバイスとサブシステムはその素性とセキュリティ状態を証明する必要があります。これは、理想的にはプラットフォーム認証のためのシステム アグリゲータが存在する必要がある事を意味します。Microchip 社の CEC1712 と Soteria ソフトウェアの組み合わせは、プラットフォーム内の各種認証ユースケースの要求を満たすように拡張できます。

Microchip 社は関連部品とコントローラのための統合ソリューションを提示できました。

Switchtec PCIe スイッチ : Microchip 社の高信頼性 PCI Express® (PCIe) スイッチの幅広いポートフォリオはデータセンター、ストレージ、通信、防衛、産業、その他の各種アプリケーション向けに高密度かつ低消費電力のソリューションを提供します。Microchip 社は PCIe ソリューションとしてファンアウト/プログラマブル/アドバンスト ファブリック PCIe スイッチの他に、NVMe™ コントローラ、NVRAM ドライブ、リドライバおよびタイミング ソリューション、フラッシュベース FPGA および SoC も提供しています。

Flashtec® NVMe ドライブ コントローラ : Flashtec NVMe コントローラ ファミリは大企業とデータセンターによる次世代 NAND 技術を使った高性能 SSD の実現を可能にします。世界最高レベルの拡張性と柔軟性を兼ね備えた Flashtec コントローラ ファミリは信頼の高い選択肢です。これらの NVMe コントローラは標準的な NVMe ホスト インターフェイスをサポートしており、ランダム読み書き向けに最適化されています。全てのフラッシュ管理動作をオンチップで実行するため、ホスト処理およびメモリリソースの消費はごくわずかです。

Adaptec® ストレージ/RAID コントローラおよびアダプタ : Adaptec SmartRAID アダプタは、幅広いストレージ要件を満たすように設計された機能豊富な高性能エンタープライズ RAID アダプタです。これらのデバイスは低消費電力で、12 Gbps の SSD と組み合わせた場合最大の読み書き帯域幅と IOPS を実現します。一部のアダプタは内蔵 ZMCP (Zero-Maintenance Cache Protection)、maxCache、SSD キャッシング ソリューション、ブロックベースの全てのストレージ デバイスのための maxCrypto によるコントローラ ベースの暗号化機能を備えています。Adaptec SmartHBA ホストバス アダプタは、最大限の帯域幅と I/O 接続性、低消費電力、高信頼性を必要とするサーバベースのストレージ システムに理想的なソリューションです。

PolarFire® FPGA ファミリ : PolarFire FPGA はミッドレンジの集積度で業界トップレベルの低消費電力性能と卓越したセキュリティと信頼性を提供します。本ファミリは 100k～500k LE の集積度で 12.7G トランシーバを備え、競合製品と比べて最大で 50% 消費電力を低減しています。PolarFire FPGA は産業用オートメーションおよび IoT 市場だけでなく、有線ネットワークおよびセルラー インフラストラクチャ、防衛および民間航空市場の幅広いアプリケーションに理想的です。

Microchip 社は優れた製品だけでなく CEC1702 (DM990013) 開発ボード、回路図レビュー、セキュリティ リスクと対応策に関するトレーニング、Soteria ファームウェア、プロビジョニング技術、統合開発環境である MPLAB® X 等を提供しています。MPLAB X IDE は拡張可能で柔軟な設定が可能なソフトウェア プログラムです。この IDE はほとんど全ての Microchip 社製マイクロコントローラおよびデジタルシグナル コントローラをサポートし、組み込み回路の研究、設定、開発、デバッグ、評価に役立つ強力なツールを備えています。MPLAB X IDE は、MPLAB 開発エコシステムのソフトウェアおよびツールとシームレスに連携します。

Microchip 社の CEC1712 と Soteria-G2 の組み合わせは、5G およびデータセンターOS のプリブート中の悪質なマルウェア阻止に加えて、自律走行コネクテッドカーの OS、ADAS(高度運転支援システム)、その他の外付け SPI フラッシュから起動するシステムのセキュリティ確保も実現します。

ファームウェア セキュリティの全ての潜在的侵害は防止される必要があり、プラットフォーム内の全てのデバイスとサブシステムはその素性とセキュリティ状態を証明する必要があります

結果

データセンターのエンドユーザはデータがハッカーによって侵害される可能性が低くなり、侵害への対応に追われる心配がなくなります。

セキュアブートによるルートキットに対する防御は強力な手法です。CEC1712 と Soteria-G2 ファームウェアの採用は、ルートキットが読み込まれる前に脅威に対抗する理想的な戦略です。ハードウェアによるルートオブ トラストの実践、セキュアブート機能、Soteria ファームウェアの組み合わせは、レガシーシステムに簡単に追加でき、1 地点対策からプラットフォーム レベルのセキュリティ ソリューションへと拡張できます。

Microchip Technology Inc. | 2355 W. Chandler Blvd. | Chandler AZ, 85224-6199 | microchip.com

DS00003888A_JP