ケーススタディ

スマート
当社の暗号化対応、Soteria-G2カスタムファームウェア搭載のCEC1712 MCUは、ルートキットやブートキットなどの悪意のあるマルウェアを防止するように設計されています。

コネクテッド
当社のソリューションはサーバー、テレコミュニケーション設備、コネクテッド自律走行運転システム、ADAS、および外部SPIフラッシュから起動するその他システムのセキュリティ強化を実現します。

セキュア
Soteria-G2カスタムファームウェアは、外部SPIフラッシュメモリから起動するオペレーティングシステムに対してハードウェア面からRoot of Trust(信頼の基点)を保護することでセキュアなブートを提供します。

データセンタープラットフォームのファームウェアの回復力

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、スマートな製品設計、ワイヤレス技術、スマートシティの構築や自動運転車の運用といった分野で世代交代が進むごとに、コスト削減、効率アップ、パフォーマンス向上を実現する数え切れないほどの新しいチャンスをもたらします。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、そうした需要に合わせて成長しています。企業、政府、公共事業者、消費者、そして様々な官民の機関は、コネクテッド技術がますます進む世界で登場する新たな要素を発明する人たちと協力し、これらの進歩を活用することを期待しています。

技術の進歩を待ち望む集団は他にも存在します。それは**ハッカー**です。

歴史上初のハッカーは、1900年代初頭に電話交換機に侵入し、いたずらで顧客からの電話の通信経路を変更した10代の若者だったという説があります。1960年代のハッカーといえば、メインフレーム・コンピュータのプログラマーで、コンピュータの動作を設計時に想定していた性能限界を超えるまで押し上げる新しいコードを考案していた人だったと考えられます。そこに悪いニュアンスは含まれていません。メインフレーム操作の実践を進化させて、ハッカー仲間の尊敬を得ていたことを意味しました。次の進化時の標的は通信事業者でした。才能ある技術者たちがネットワーク接続装置を研究し、長距離通話のルーティング制御に使用されるトーンを模倣することで、長距離通信サービスを無料で利用しました。こうしたフリーカー(電話ネットワークを理解しようと異常なまでに熱中する者を指した造語) たちは、このコスト削減の回避策を実行できるブラックボックスを扱う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の制御システムに移行する頃には、ハッカーたちの標的はPCやコンピュータネットワークの台頭など、より興味をひくものに移行していました。そしてある時点で、ハッカーは一線を越え、やや無害な実験者から犯罪的な性質を持つ破壊者(クラッカー)へと変化しました。

コネクテッド技術が普及すると、セキュリティ指向のベンダーやメーカーには、さまざまなハードウェア、ソフトウェア、そしてサービスサービスの途絶に対処する必要が生じます。一昔前には想像もできなかった脆弱性が見つかり、これらの脆弱性は悪意を持った人々の注目に留まらず、善意をもつ人々の目にも止まるようになりました。

そう遠くない過去のことですが、政府機関や企業内でよく使われるUSBメモリドライブ悪用対策の一般的手法は、コンピュータやラップトップの各USBコンピュータポートを接着剤やシリコーンで塞ぐことでした。今では、そのような対策は、歯が痛いから歯列ごと抜いていた中世の歯科治療のように思えます。

高度なテクノロジーは、データ破壊や情報漏えいの恐怖心を薄めるほどの非常に強い魅力があるようです。それも危惧されていた事件が現実に起こるまでのことですが。

無線ネットワーク事業者は広告を打つことで5G回線がすでに利用でき大衆市場向けIoT対応デバイスの準備も整っていると信じ込ませようとしますが、実情は進化の途上にあります。データセンターのアーキテクトとストレージシステムの設計者たちは、明日のインフラストラクチャ ソリューションを構築すると同時に、ハッカーがその脆弱性をテストしています。興味深いことですが、ハッキングコミュニティは全国的な5Gアクセスと数十億のモノのインターネット (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を得たり混沌を起こす切り口を発見したりするためのテレコム指向ネットワークへの回帰だと感じ取っている可能性があります。ソフトウェアとハードウェアベースの大混乱が発生した時に悪用されるデバイスとシステムの数は前例のないほど膨大な量になるでしょう。ハッカーのビジネスモデルは、悪意あるコードの新たな侵入口を探す事であるため、新たに設計されたボットとスクリプトはその安全性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たちが明日のインフラストラクチャソリューションを構築している間、ハッカーたちは脆弱性をテストしています...

セキュリティはMicrochip製品ポートフォリオの要諦

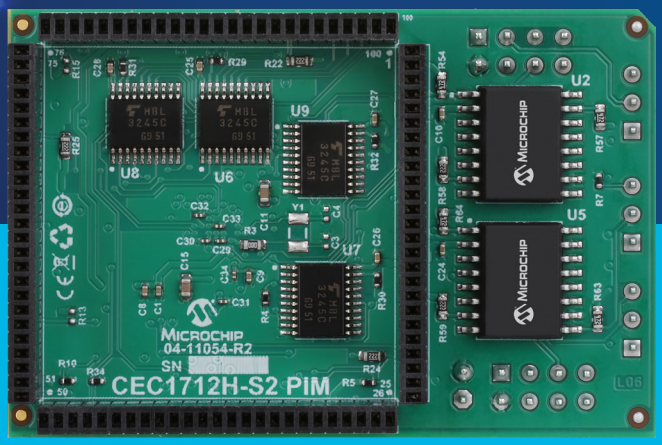
ハッカーの攻撃対象はハードウェアやコンピュータシステムだけではありません。システム内の保護されていないコンポーネントも狙われます。セキュリティを取り巻く環境は、市場特有の要件が多々あるため、安全性への要求は常に変化しています。企業がセキュリティ侵害を受けたことが公になれば、業界の信頼が大幅に失われる可能性が高く、収益や株価が大幅に下落する可能性さえあります。残念なことに、ビジネス界全体で実践される、プラットフォームのファームウェアの回復力に関する一連の標準セキュリティガイドラインというものはありません。各種標準、業界が負う義務、機能性、コスト、顧客が取引先から出される要求、安全性、パフォーマンス、そしてネットワークパラダイムとの整合性を確保するためには、どのようなセキュリティアプローチをとろうと、目まいがするほど多くの事を検討する必要があります。

組み込み設計では、デバイスのストレージ、通信ハードウェアとプロトコル、ノードとゲートウェイの実装、デバイス管理システム、クラウドコンピューティングなどの多くのレイヤーと連携してセキュリティ対策を行います。各組み込み設計の開始時にセキュリティを考慮する必要がありますが、Microchipには、製品を直接保護することで最終的には知的財産、企業ブランド、評価、収益を護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の取引先様は、業界で最も総合力に優れるセキュリティポートフォリオとワールドクラスのセキュリティパートナープログラムをご利用いただくことで、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自信を持って作成できます。セキュリティに対する最先端のアプローチと業界全域に渡る攻撃でも即時対応力により、Microchip社は各設計の個別ニーズに合わせて柔軟にカスタムソリューションを提供することができます。認証デバイスやトラステッド プラットフォーム モジュールから、暗号化対応のマイクロコントローラやマイクロプロセッサ、ソフトウェアライブラリ、拡張プロトコルに至るまで、Microchipのセキュリティへのアプローチは、当社のあらゆる取り組みの中心となっています。

...外部SPIフラッシュメモリは多くのOEMで焦点を絞っているエリアです...

課題



高性能サーバーテクノロジーのグローバルプロバイダは、ハードウェアベースとOSベースのセキュリティ戦略をアップグレードすることに関心を持っていました。外部SPIフラッシュメモリから起動するシステムにおけるルートキットやブートキットが持つ脆弱性に対する認識の高まりは、多くのOEMにとってますます重要になっています。

ルートキットマルウェアは、マルウェアがアクティブな状態であってもユーザー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を介してコンピュータシステムを遠隔操作する権限を奪い、セキュリティプログラムを破壊し、個人データ、パスワード、銀行口座の詳細情報、そしてクレジットカード情報を盗むことができます。ブートキットはコンピュータのマザーボードのマスターブートレコードに影響を与える有害なコードであり、オペレーティングシステムの読み込み直前に悪意のあるプログラムを実行させます。

Microchipの新しい暗号化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プラットフォームが実行前に悪意のあるファームウェアを検出して停止できるようにすることを目的として構築されています。当社のお客様は、以下に示すような多角的な戦略での対処に関心を寄せています。

- セキュリティ侵害を修正するための応答時間短縮
- セキュリティの脅威と緩和策を理解する
- セキュアデバイス戦略をセキュアプラットフォーム戦略に移行する
- セキュリティ標準の進化への対応や専門組織の進化に対応する
- セキュリティ専門家とリソースの採用
- レガシーデバイスとプラットフォームへの影響について理解する

ソリューション

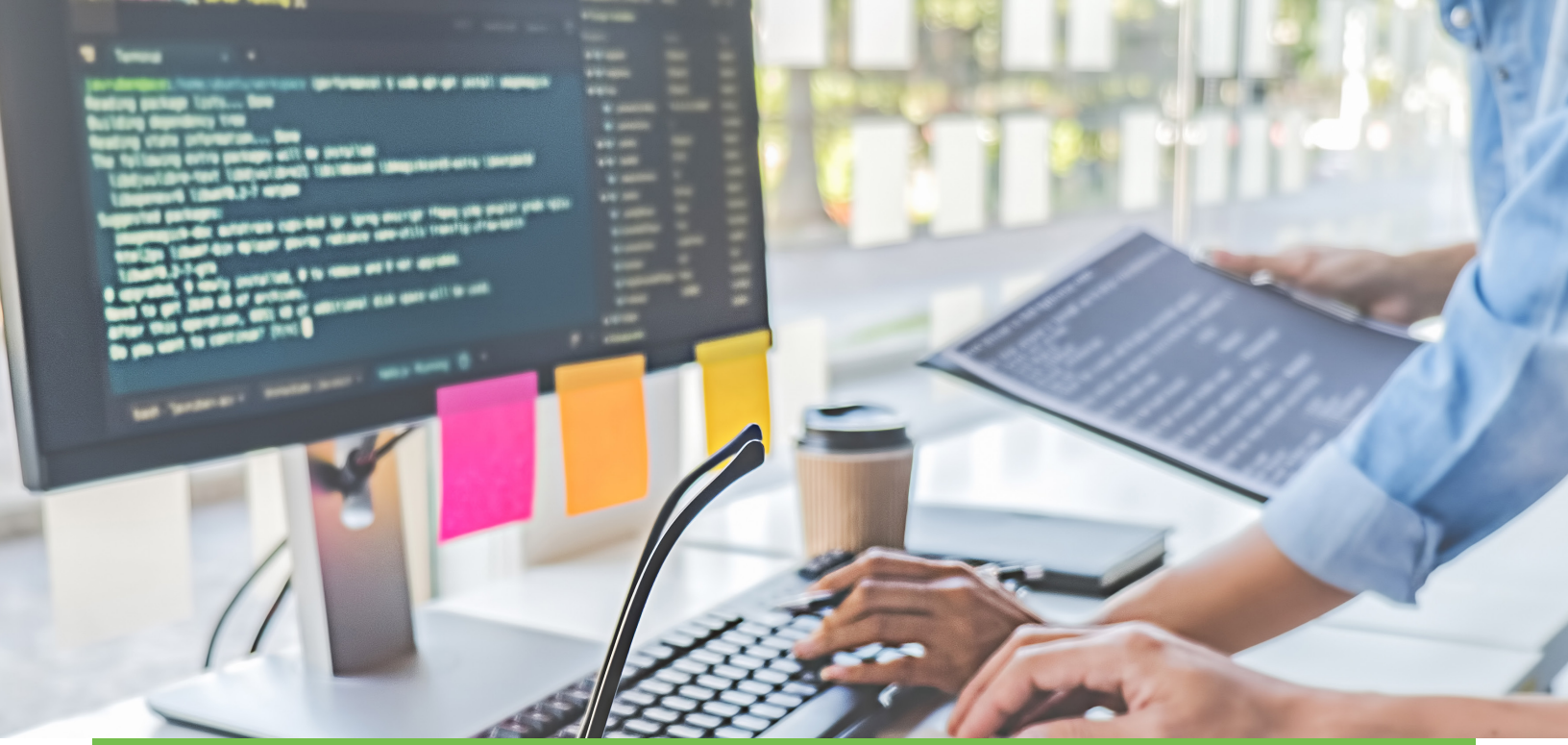
Microchipのチームは、お客様と会ってその要件をより深く理解し、プロジェクトの進め方についてお客様にアドバイスした後、Soteria-G2カスタムファームウェア搭載で暗号化対応のCEC1712 MCUを中心とするソリューションを提案することができました。このプロジェクトは2019年に開始しました。

MicrochipのCEC1712 Arm® Cortex®-M4ベースのマイクロコントローラの機能をフル搭載したSoteria-G2カスタマーファームウェアは、外部SPIフラッシュメモリから起動するオペレーティングシステムに対して、プリブート モードでハードウェア面からRoot of Trust(信頼の基点)を保護することでセキュアなブートを可能にします。さらに、CEC1712は稼働中に鍵の失効処理とコードのロールバック保護を提供することで現場でのセキュリティ更新を可能にします。NIST 800-193ガイドライン準拠のCEC1712は、全体的なシステムプラットフォーム ファームウェアの回復力を高めるために、破損を未然に防ぎ、破損を検出し、破損から復旧します。ハードウェアRoot of Trustを使用したセキュアブートは、脅威がシステムにロードされる前にシステムを保護する上で重要な機能であり、メーカーが信頼するソフトウェアを使用してシステムを起動することのみを許可する仕組みです。

Soteria-G2ファームウェアは、コード開発をシンプル化し、リスクを低減することで、設計者がセキュアブートの採用と実装を加速できるようにするために、CEC1712と連動して使用することを前提に設計されています。Soteria-G2は、Root of Trust(信頼の基点)としてリードオンリーメモリー(ROM)内に実装されたCEC1712不変セキュアブートローダを使用します。

CEC1712セキュアブートローダは、外部SPIフラッシュからCEC1712上でファームウェアを実行できるようにロード、復号化および認証します。その後、検証済みCEC1712コードは、最初のアプリケーション プロセッサ用にSPIフラッシュ内に格納されたファームウェアを認証します。最大2個のアプリケーションプロセッサをサポートします。また、それぞれに2つのフラッシュコンポーネントでサポートしています。お客様固有のデータの事前プロビジョニングオプションもご利用いただけます。事前プロビジョニングは過剰な製造や偽造の防止に役立つ安全な製造ソリューションです。このソリューションを利用すると、開発時間を最大で数か月節約できるだけでなく、プロビジョニングのロジスティクスを大幅に簡素化し、お客様がサードパーティ製プロビジョニングサービスや認証局のオーバーヘッドのコストを支払うことなくデバイスを簡単に保護・管理できます。

そして、プラットフォームファームウェアの回復力は、ポイントソリューション以上に重要です。業界のガイドラインによると、ファームウェアにおいて起こりうるいかなるセキュリティ違反も未然に防がなければならず、プラットフォーム内のすべてのデバイスとサブシステムは、その識別子とセキュリティの状態を証明する必要があります。つまり、このファームウェアはプラットフォーム証明用のシステムアグリゲーターが必要なのです。MicrochipのCEC1712とSoteriaソフトウェアを組み合わせることで、プラットフォーム内のさまざまな認証ユースケースのニーズを満たすことができます。



Microchipは関連するコンポーネントとコントローラーの統合ソリューションを提示できました:

Switchtec PCIeスイッチ: PCI Express® (PCIe) スイッチのポートフォリオは広範で信頼性が高く、データセンター、ストレージ、通信、防衛、工業、およびその他の幅広い用途向けに、業界で最も高密度で低電力のソリューションを提供します。業界をリードするMicrochipのPCIeソリューションには、当社のファンアウト、プログラム式、そして高度ファブリックPCIeスイッチに加えて、NVMe™コントローラ、NVRAMドライブ、リドライバー、タイミングソリューション、ならびにフラッシュベースFPGAとSoCも含まれています。

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、世界をリードする企業やデータ センターにおいて、次世代NANDテクノロジを利用した最高性能のSSDを実現します。ワールドクラスのキャパシティと柔軟性を組み合わせたFlashtecコントローラファミリは、信頼できる選択肢と言えます。NVMeコントローラは標準NVMeホストインターフェースに対応し、最高のパフォーマンスを発揮するランダム読み取り/書き込み操作用に最適化されており、すべてのフラッシュ管理操作をチップ上で実行し、ホスト処理とメモリリソースをほとんど消費しません。

Adaptec®ストレージ/RAIDコントローラおよびアダプタ: Adaptec SmartRAIDアダプターは、さまざまなストレージ要件に合わせて構築された、フル機能の高性能企業向けRAIDアダプターです。業界で最も低い消費電力を実現していて、12 Gbps SSDと組み合わせることで、最大の読み取り/書き込み帯域幅とIOPS（入出力操作毎秒）を実現します。一部のアダプターで利用可能な独自機能としては、メンテナンスフリーのキャッシュ保護（ZMCP）、maxCache（SSDキャッシングソリューション）、maxCryptoコントローラベースの暗号化（ブロックベースのストレージデバイス用）などがあります。Adaptec SmartHBA ホストバスアダプタは、最大の帯域幅とI/O接続性、低消費電力、高い信頼性を必要とするサーバーベースのストレージシステムに最適な接続ソリューションです。

PolarFire® FPGAファミリ: 栄えある賞を受賞したPolarFire FPGAは、ミッドレンジ層で業界最小の電力消費を誇り、卓越したセキュリティと信頼性を備えています。この製品ファミリは100Kロジックエレメント (LE) から500K LEまでに対応し、12.7Gトランシーバーを備え、ミッドレンジ層の競合FPGAよりも消費電力が最大で50%低くなっています。これらのデバイスは、有線アクセスネットワークとセルラーインフラストラクチャ、防衛用・商用航空市場、産業オートメーション、IoT市場における幅広い用途に最適です。

Microchipのソリューションには、CEC1702 (DM990013) 開発ボード、回路図レビュー、セキュリティリスクとその緩和策に関する教育、Soteriaファームウェア、プロビジョニングの専門知識、そしてMPLAB® X統合型開発環境 (IDE) と組み合わせた優れた製品バンドルが含まれます。MPLAB X IDEは、拡張および高度な設定が可能なソフトウェアツールであり、当社の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のほとんどに対する組み込み設計でお客様に必要な検索、設定、開発、デバッグおよび認定作業を支援する強力なツールが組み込まれています。MPLAB X IDEは、ソフトウェアおよびツールのMPLAB開発エコシステムとシームレスに連携します。

MicrochipのCEC1712とSoteria-G2との組み合わせは、5Gやデータセンター運用システムでのプリブート中を狙ってくる悪意のあるマルウェアの防止だけでなく、コネクテッドカーの運転システム、自動車の先進運転支援システム (ADAS)、外部SPIフラッシュから起動するその他のシステムのセキュリティを強化します。

ファームウェアにおいて起こりうるいかなるセキュリティ違反も未然に防がなければならず、プラットフォーム内のすべてのデバイスとサブシステムは、その識別子とセキュリティの状態を証明する必要があります。

結果

現在、当社のデータセンター顧客のエンドユーザーは、企業、個人、金融、または医療に関するデータシステムがハッカーにより侵害される可能性が低減されたことで、侵害イベント時の緩和処理の悪夢を回避できています。

セキュアブートによるルートキット防御は強力なアプローチであり、CEC1712およびSoteria-G2ファームウェアの採用は、脅威がシステムに読み込まれる前に保護するための理想的な戦略でした。ハードウェアRoot of Trustの実践、セキュアブート機能、そして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るため、ポイントソリューション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の拡張が可能になります。

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

DS00003888A_JP