Soteria-G3

概要

Soteria-G3 はリアルタイム ルートオブ トラスト コントローラの CEC173x Trust Shield ファミリにハードウェア暗号化を実装するファームウェアです。Soteria-G3 と CEC173x を任意の AP(アプリケーション プロセッサ) と組み合わせて使う事で、プラットフォームのルートオブ トラスト (信頼の基点) を拡張し、セキュアブートプロセスを確実に適用できます。

特長

セキュアブート

Soteria-G3 は最大で 2 つの AP に対して並列に、NIST 800-193 に準拠したセキュアブートとセキュアな更新をサポートし、ブート ファームウェアの真正性を確保します。

複数の SPI イメージのサポート

Soteria-G3 は複数のコードイメージをサポートしています。これらのイメージは必要に応じて個別の外部 SPI フラッシュ デバイスに保存できます。イメージと暗号化はユーザー設定可能です。

ゴールデン SPI イメージのサポート

更新失敗またはコード侵害が発生した場合、バックアップ イメージ (別名ゴールデン イメージ) の読み出しもサポートしています。

SPI バスの監視

データバスのトラフィックをリアルタイムに監視可能で、実行が許可されるオペコードについてユーザーがカスタマイズした規則を確実に適用できます。

鍵の無効化

Soteria-G3 では最大 32 個の一意の公開鍵/秘密鍵のペアを使って漏洩した秘密鍵を置き換え可能です。

ロールバック保護

ファームウェア更新後に旧バージョンのコードが実行されないようにし、過去にパッチを適用したセキュリティ脆弱性が悪用されるのを防ぐ事ができます。

暗号ライブラリのサポート

Soteria-G3 は以下を含む非対称暗号アルゴリズムをサポートしています。

- SHA-2、SHA-256、SHA-512
- RSA-1024～RSA-4096
- ECDSA、EC-KCDSA
- Ed25519

I²C プラットフォーム通信

Soteria-G3 はペリフェラル ホスト インターフェイスとして I²C をサポートしています。このインターフェイスは SPDM(Security Protocol and Data Model) 仕様に準拠した認証、ファームウェア イメージのクライシス リカバリ、デバッグモード、NIST 800-193 プラットフォーム ファームウェア レジリエンス ガイドラインを可能にします。

所有権の移転

プラットフォームを改修または移転する際、元の所有者は所有権移転コマンドを開始してデバイス シークレットを保護できます。このコマンドは元の所有者の秘密鍵によって暗号化されています。コマンドは調停を介して開始する事も、プラットフォームが移転された後に開始する事もできます。

ライフサイクル管理

プラットフォームはその寿命を通して単独または複数の所有者を持つ事が可能です。システム上で実行が許可されるイメージは所有者ごとにカスタマイズできます。ライフサイクル管理では、未使用、テスト、開発、生産、RMA(返品承認)、EOL(ライフサイクル終了) を含むライフサイクルのあらゆる段階で機能とシークレットを保護します。

セキュアな I²C/UART クライシス リカバリ

コードイメージが破損、または利用できない等の理由でシステムがセキュアブートを進行できない場合、クライシスが発生します。Soteria-G3 では所有者の秘密鍵で暗号化されたコマンドを使ってイメージを強制的に更新する事によりクライシスからの復帰をサポートしています。

証明のサポート

Soteria-G3 では、CEC173x の SRAM ベースの PUF(物理的複製防止機能) により SPDM 仕様準拠のコンポーネント認証を可能にします。

認証

Soteria-G3 のコードは MISRA をクリアし、Coverity® と CERT® C コード解析のチェックを受け、サードパーティの侵入テストによって認証されています。

在庫状況

Soteria-G3 は、Microchip 社とのソフトウェア ライセンス契約に基づいて提供しています。詳細は正規代理店へお問い合わせください。

Trust Shield ソリューションの詳細はこちら

- Trust Shield ファミリ リーフレット
- Trust Shield 製品ページ