News Release

Microchip 社、外付け SPI フラッシュメモリから起動するシステムを マルウェアから保護できる MCU とファームウェアを発表

マルウェアを実行前に検出/阻止できる Microchip 社の暗号 MCU、
カスタム ファームウェア、設定サービス

2020 年 3 月 19 日[NASDAQ: MCHP] ー 急激に拡大しつつある 5G 携帯通信インフラストラクチャ、クラウド コンピューティングに対応するネットワークとデータセンター等の需要拡大に伴い、オペレーティング システム(OS)のセキュリティを確保する新しい方法が求められています。Microchip Technology Inc.(日本支社: 東京都港区浜松町、代表: 吉田洋介 以下 Microchip 社)は本日、新しい暗号対応マイクロコントローラ(MCU) CEC1712 MCU と Soteria-G2 カスタム ファームウェアを発表しました。これらは外付け SPI(シリアル ペリフェラル インターフェイス) フラッシュメモリから起動するシステムをルートキット、ブートキット等のマルウェアから保護すべく設計されました。

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(信頼の基点)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。

「ルートキットは特に悪質なマルウェアです。これは OS が起動する前に読み込まれ、通常のマルウェア対策ソフトウェアでは検出が困難です」と Microchip 社コンピューティング製品部門副社長の Ian Harris は述べています。「ルートキットに対して防御する 1 つの方法はセキュアブートを使う事です。CEC1712 と Soteria-G2 ファームウェアは、ルートキットが読み込まれる前にシステムを保護します。」

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。Microchip 社と Arrow Electronics 社にて、顧客固有のセキュアブート コンフィグレーションを事前設定として CEC1712 に書き込んで出荷することも可能です。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

-more-

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。

「Microchip 社製品のセキュアな設定は当社にとって重要なサービスです。そして、Soteria-G2 ファームウェアと CEC1712 MCU はシステムを保護する事を目的としています」と Arrow Electronics 社 IoT 部門副社長の Aiden Mitchell 氏は述べています。「5G 時代に向けてコネクテッド ソリューションと自律機械が普及していくにつれ、このようなサービスがよりいっそう必要となるでしょう。」

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。

開発ツール

CEC1712 と Soteria-G2 を使った開発は各種ソフトウェアおよびハードウェアでサポートします。ソフトウェアには Microchip 社の MPLAB® X IDE および MPLAB Xpress、MPLAB XC32 コンパイラ、ハードウェアには MPLAB ICD 4、MPLAB PICkit™ 4 等のプログラマ/デバッガ等が含まれます。

在庫/供給状況

CEC1712H-S2-I/SX は本日より量産出荷を開始いたします。詳細は Microchip 社または正規代理店にお問い合わせ頂くか、Microchip 社ウェブサイトをご覧ください。設定サービスは Arrow Electronics 社 (**secure.provisioning@arrow.com**)にお問い合わせください。製品は **Microchip 社オンラインストア**でご購入頂けます。

リソース

高画質の写真は報道関係専用窓口までお問い合わせ頂くか、Flickr でご覧ください(掲載に許可は不要です)。

- アプリケーション画像: www.flickr.com/photos/microchiptechnology/49548114798/

Microchip Technology 社について

Microchip Technology 社(以下、Microchip 社)はスマート、コネクテッド、セキュアな組み込み制御ソリューションのトッププロバイダです。使いやすい開発ツールと包括的な製品ポートフォリオにより、リスクを低減する最適な設計を作成し、総システムコストの削減、迅速な商品化を実現できます。Microchip 社は産業、車載、民生、航空宇宙と防衛、通信、コンピューティングの市場で 120,000 社を超えるお客様にソリューションを提供しています。Microchip 社は本社をアリゾナ州チャンドラーに構え、優れた技術サポート、確かな納期、高い品質を提供しています。詳細は Microchip 社ウェブサイト(http://www.microchip.com)をご覧ください。

###

Microchip 社、CEC1712 と Soteria-G2 を発表
3 – 3 – 3 – 3

詳細については、以下にお問い合わせください。
Daphne Yuen (Microchip 社): (852) 2943 5115
(メール: daphne.yuen@microchip.com)

大川、仙場 (共同 PR): (03) 3571 5236
(メール: taito.okawa@kyodo-pr.co.jp)

報道関係者の方へ: このニュースリリースのメールによる配信については、共同 PR 株式会社 大川もしくは仙場まで電話(03) 3571 5236 またはメール taito.okawa@kyodo-pr.co.jp でお問い合わせください。