March 12, 2020

Protect Against Rootkit and Bootkit Malware in Systems that Boot from External SPI Flash Memory

Microchip's new cryptographic MCU, custom firmware and provisioning service are designed to enable platforms to detect and stop malicious firmware prior to run time

CHANDLER, Ariz., March 12, 2020 (GLOBE NEWSWIRE) -- With the rapid growth of 5G including new cellular infrastructure, growing networks and data centers supporting expanding cloud computing, developers are seeking new ways to ensure operating systems remain secure and uncompromised. Microchip Technology Inc. **(Nasdaq: MCHP)** today announced a new cryptography-enabled microcontroller (MCU), the **CEC1712 MCU** with Soteria-G2 custom firmware – designed to stop malicious malware such as rootkit and bootkit for systems that boot from external Serial Peripheral Interface (SPI) flash memory.

Microchip's Soteria-G2 custom firmware on its full-featured CEC1712 Arm® Cortex®-M4-based microcontroller provides secure boot with hardware root of trust protection in a pre-boot mode for those operating systems booting from external SPI flash memory. In addition, the CEC1712 provides key revocation and code rollback protection during operating life enabling in-field security updates. Complying with NIST 800-193 guidelines, the CEC1712 protects, detects and recovers from corruption for total system platform firmware resiliency. The secure boot with hardware root of trust is critical in protecting the system against threats before they can load into the system and only allows the system to boot using software trusted by the manufacturer.

The Soteria-G2 firmware is designed to be used in conjunction with the CEC1712 to allow designers to speed adoption and implementation of a secure boot, by simplifying the code development and reducing risk. Soteria-G2 uses the CEC1712 immutable secure bootloader, implemented in Read-Only Memory (ROM), as the system root of trust.

"A particularly insidious form of malware is a rootkit, because it loads before an operating system boots and can hide from ordinary anti-malware software and is notoriously difficult to detect," said Ian Harris, vice president of Microchip's computing products group. "One way to defend against root kits is with secure boot. The CEC1712 and Soteria-G2 firmware is designed to protect against threats before they can be loaded."

The CEC1712 secure bootloader loads, decrypts and authenticates the firmware to run on the CEC1712 from the external SPI flash. The validated CEC1712 code subsequently authenticates the firmware stored in SPI flash for the first application processor. Up to two application processors are supported with two flash components supported for each. Pre-provisioning of customer-specific data is an option provided by Microchip or Arrow Electronics. Pre-provisioning is a secure manufacturing solution to help prevent overbuilding

and counterfeiting. In addition to saving up to several months of development time, the solution significantly simplifies provisioning logistics, making it easy for customers to secure and manage devices without the overhead cost of third-party provisioning services or certificate authorities.

“Secure provisioning for some of Microchip`s flagship products is an important part of our offering and the Soteria-G2 firmware and CEC1712 microcontroller are targeted to protect systems,” said Aiden Mitchell, vice president of IoT at Arrow Electronics. “Customers will increasingly seek such offerings as we approach the 5G era and go more into connected solutions and autonomous machines.”

In addition to preventing malicious malware during pre-boot in 5G and data center operating systems, Microchip’s CEC1712 and Soteria-G2 combination is a security enabler for connected autonomous vehicle operating systems, automotive Advanced Driver Assisted Systems (ADAS) and other systems that boot out of external SPI flash.

Development Tools
Microchip’s **CEC1712 and Soteria-G2 package** offers several options for software and hardware support. Software support includes Microchip’s MPLAB® X IDE, MPLAB Xpress and MPLABXC32 compilers. Hardware support is included in programmers and debuggers including the MPLAB ICD 4 and PICkit™ 4 programmer/debugger.

Pricing and Availability
The CEC1712H-S2-I/SX is available in volume production in 10,000 quantities starting at $4.02 (includes the Soteria-G2 firmware). For additional information, contact a Microchip sales representative, authorized worldwide distributor or visit Microchip’s website. For provisioning pricing, contact Arrow Electronics at **secure.provisioning@arrow.com**. To purchase silicon products mentioned here visit **Microchip’s purchasing portal**.

Resources
High-res image available through Flickr or editorial contact (feel free to publish):

- Application image: **www.flickr.com/photos/microchiptechnology/49548114798/**

About Microchip Technology
Microchip Technology Inc. is a leading provider of smart, connected and secure embedded control solutions. Its easy-to-use development tools and comprehensive product portfolio enable customers to create optimal designs which reduce risk while lowering total system cost and time to market. The company’s solutions serve more than 120,000 customers across the industrial, automotive, consumer, aerospace and defense, communications and computing markets. Headquartered in Chandler, Arizona, Microchip offers outstanding technical support along with dependable delivery and quality. For more information, visit the Microchip website at **www.microchip.com**.

Editorial Contact:
Cathy Gedvilas
480-792-4386
Cathy.Gedvilas@microchip.com

Reader Inquiries:
1-888-624-7435

Source: Microchip Technology Inc.