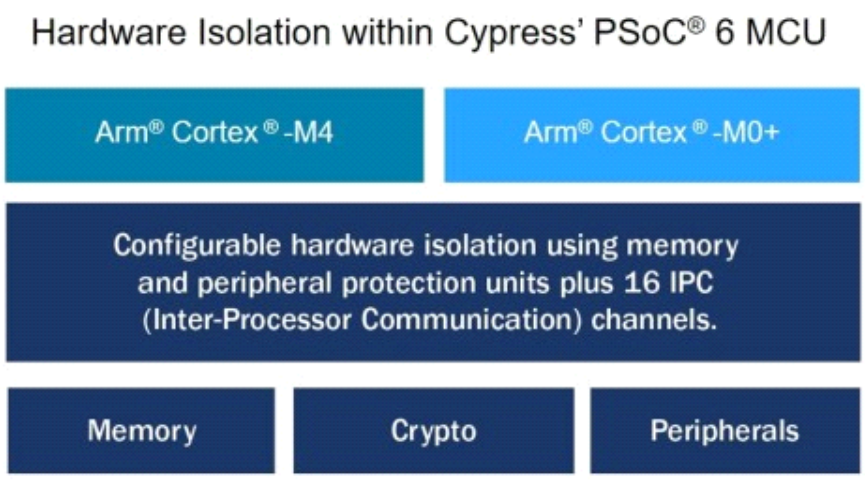
February 26, 2018

Cypress Accelerates Secure IoT Designs with Support for Platform Security Architecture Trusted Firmware-M from Arm

Cypress' Ultra-low Power, Dual-core PSoC® 6 MCUs Adhere to the Highest Level of Protection Defined by PSA

NUREMBERG, Germany--(BUSINESS WIRE)-- EMBEDDED WORLD—Cypress Semiconductor Corp. (NASDAQ: CY), the leader in advanced embedded solutions, announced availability of the Platform Security Architecture (PSA) Trusted Firmware-M reference example from Arm® for its PSoC® 6 microcontrollers (MCUs), enabling a solution that adheres to the highest level of protection as defined by PSA. By leveraging PSA's holistic set of threat models, security analyses, hardware and firmware architecture specifications, and Trusted Firmware-M reference implementation, Internet of Things (IoT) designers can quickly and easily implement secure designs with PSoC 6 MCUs.

This press release features multimedia. View the full release here: http://www.businesswire.com/news/home/20180226005392/en/



Pictured is a block diagram showing the integrated security in Cypress' PSoC 6 microcontrollers, which delivers the highest level of protection as defined by Arm's Platform Security Architecture. (Graphic: Business Wire)

"Connected devices are being deployed at a rapid pace, and to truly realize the benefits of these technologies, security cannot be optional," said Paul Williamson, vice president and general manager, IoT Device IP Line of Business, Arm. "Enabling secure MCU development across the breadth of IoT applications is a shared industry responsibility, and Cypress' PSoC 6 MCUs will further extend the benefits of PSA to our ecosystem."

"As a direct result of the security features built into PSoC 6 MCUs and our collaboration with Arm, we have been able to quickly offer support for Trusted Firmware-M," said Sudhir Gopalswamy, senior vice president of the Microcontrollers and Connectivity Division at Cypress. "We're excited to offer designers a secure solution that is ultra-low power, flexible and adheres to PSA principles."

Cypress' PSoC 6 MCUs achieve the highest level of protection defined by the PSA using dual Arm Cortex®-M cores combined with configurable memory and peripheral protection units. The MCUs provide three levels of hardware-based isolation: 1) an isolated execution environment for trusted applications using a dedicated Arm Cortex®-M0+ core, 2) secure element functionality that hosts root of trust operations and system services, and 3) isolation for each trusted application. These three levels of isolation together reduce the attack surface for threats. The system is augmented with a true random number generator (TRNG) and cryptographic accelerators, while the Cortex-M4 core in the PSoC 6 MCU architecture delivers a clean programming model for the rich execution environment for unsecure applications.

Aligned with Arm's current version for v8-M, the Trusted Firmware-M reference example for PSoC 6 MCUs allows designers to:

- Easily implement hardware-based isolation between secure and unsecure execution environments via configuration of the protection units
- Utilize Mbed OS secure services.

Future versions will include trusted boot with multiple images and full PSA API support, including Root of Trust installation with secure element functionality.

Availability

The PSoC 6 MCU Trusted Firmware-M will be available in March 2018. Early adopters are invited to register for access at www.cypress.com/psoc6.

About PSoC 6 MCUs

PSoC 6 is the industry's lowest power, most flexible MCU with built-in Bluetooth Low Energy wireless connectivity and integrated hardware-based security in a single device. Software-defined peripherals can be used to create custom analog front-ends (AFEs) or digital interfaces for innovative system components such as electronic-ink displays. The architecture offers flexible wireless connectivity options, including fully integrated Bluetooth Low Energy (BLE) 5.0. The PSoC 6 MCU architecture features the latest generation of Cypress' industry-leading CapSense® capacitive-sensing technology, enabling modern touch and gesture-based interfaces that are robust and reliable. The architecture is supported by Cypress' PSoC Creator™ Integrated Design Environment (IDE) and the expansive Arm ecosystem.

Follow Cypress Online

Join the Cypress Developer Community, read our Core & Code blog, follow us on Twitter, Facebook and LinkedIn, and watch Cypress videos on our Video Library or YouTube.

About Cypress

Cypress is the leader in advanced embedded system solutions for the world's most innovative automotive, industrial, smart home appliances, consumer electronics and medical products. Cypress' microcontrollers, analog ICs, wireless and USB-based connectivity solutions and reliable, high-performance memories help engineers design differentiated products and get them to market first. Cypress is committed to providing customers with the best support and development resources on the planet enabling them to disrupt markets by creating new product categories in record time. To learn more, go to www.cypress.com.

View source version on businesswire.com: http://www.businesswire.com/news/home/20180226005392/en/

Cypress PR
Samer Bahou, 408-232-4552
samer.bahou@cypress.com

Source: Cypress Semiconductor Corp.

News Provided by Acquire Media