УДК 621.391.7.001

SECURITY AND PERFORMANCE PROGRESS IN IT

Lviv Polytechnic National University, Lviv, Ukraine

Information technologies are continuously progressing and Internet of Things (IoT) became a novel paradigm shift in IT arena [1]. As part of a new wave of technology enablement, objects like door locks, wearable devices, and heavy machinery are all being hooked up to the internet and cloud services. It is expecting that 30 billion everyday physical objects will be part of the IoT by 2020. Despite these promising figures, the IoT market is still considered to be in the early stages of growth.

A closer look at all of these options shows that on one hand, what we have are power-hungry application processors that provide ample performance, but also negate the basic energy-efficiency premise for running battery-powered IoT devices.

On the other hand, there are standard microcontrollers that are cheap and low-power, but fail to provide the performance levels necessary for implementing IoT features like multiple sensor interfacing, security, and cloud communications.

For lack of this technological consistency Cypress has created newest PSoC 6 MCU (Programmable System on Chip) that is aiming to bridge the gap between power heavy application processors and performance-lite microcontrollers [2]. PSoC 6 is a single-chip solution that developed for a wide array of IoT applications, including wearables, smart home appliances and industrial automation. It offers longer battery life, more data processing, and built-in security features for protecting IoT devices against cyber-vulnerabilities and threats.

New PSoC 6 MCU provides the following main features:

1. Hardware security

Security is the main block in the IoT world because connected devices also open the door to network vulnerabilities. The PSoC 6 MCU architecture provides a hardware-based Trusted Execution Environment (TEE) with secure boot capability and secure data storage to protect firmware, applications and cryptographic keys.

Unique in the PSoC 6 architecture is that it supports multiple, simultaneous secure environments without the need for external memories or secure elements. PSoC 6 offers built-in security elements that other IoT chips don't, primarily because of memories that are logically isolated. A close parallel to this methodology is the virtual machine (VM) model, except that isolated memories aren't software-controlled. They are hardware-enabled. Furthermore, PSoC 6 integrates cryptographic algorithms like Elliptical-Curve Cryptography (ECC), Advanced Encryption Standard (AES) and Secure Hash Algorithms (SHA 1,2,3) implemented in a CRYPTO hardware block, offloading these compute-intensive tasks from the main processor.

2. Ultra-low-power without performance tradeoff

IoT developers are increasingly demanding embedded solutions that extend battery life without sacrificing performance. Therefore, PSoC 6 has been purpose-built on a dual-core ARM® Cortex®-M4 and ARM Cortex-M0+ architecture. New embedded chip has set another ultra-low-power benchmark: PSoC 6 accomplishes power consumptions as 22 μA in an active mode for the Cortex-M4 and 15 μA for the Cortex-M0+.

3. Flexible architecture

The PSoC 6 MCU architecture offers the best in class flexibility that enables the addition of new features and addresses the need for unique IoT products. With its multiple connectivity options, such as USB and BLE, and flexible dual-core architecture, IoT devices can be connected to the IoT, while optimizing system performance and power consumption.

The PSoC 6 is an MCU solution unlike anything else on the market because it was designed to not only meet the expectations of the modern-day IoT developer, but address their needs as well – specifically when it comes to security solutions, power consumption and design flexibility.

1. https://www.scirp.org, 2. http://www.cypress.com/