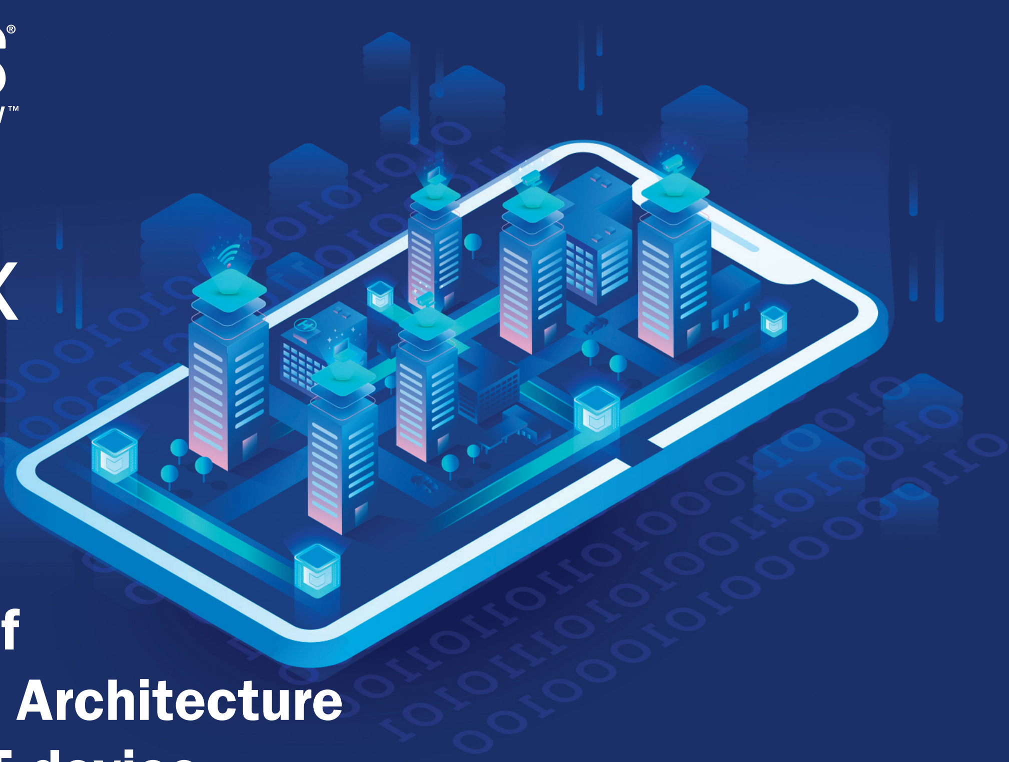


Whitepaper:

Implementation of Platform Security Architecture in a LoRaWAN IoT device

Erik Wood – Cypress Semiconductor Corp., Jan Stegenga and Rolf Nooteboom – Onethinx BV

Introduction

Security in IoT is a hot topic and has been described as a must-have for new designs. Lack of security is often attributed to end-user problems such as weak passwords. However, fundamental choices in hardware and software can make or break a secure design. To aid designers in making these choices, Arm® has introduced their Platform Security Architecture (PSA). Cypress' powerful PSoC® 6 family of microprocessors is one of the first microcontrollers to support PSA. It provides three-levels of hardware-based resource isolation, which is the highest level of isolation defined by PSA. The two-core System-on-Chip offers the possibility of a secure core, physically separated from a user application running on the other core. In addition, PSoC 6 offers secure element functionality that can be used to build a chain of verified and secured applications. This chain-of-trust (CoT) protects the application(s) from being altered by calculating and storing hashes over code blocks and sign these with private/public key pairs.

Onethinx has worked with Cypress on the implementation of a PSA-level secure system that is extendible by third party-developers. This serves three objectives:

1. A locked-down LoRaWAN™ stack on a module with an integrated antenna makes the certification process much simpler
2. The stack is copy-protected
3. Third-party developers can build their application on the SoC and secure it

LoRaWAN security

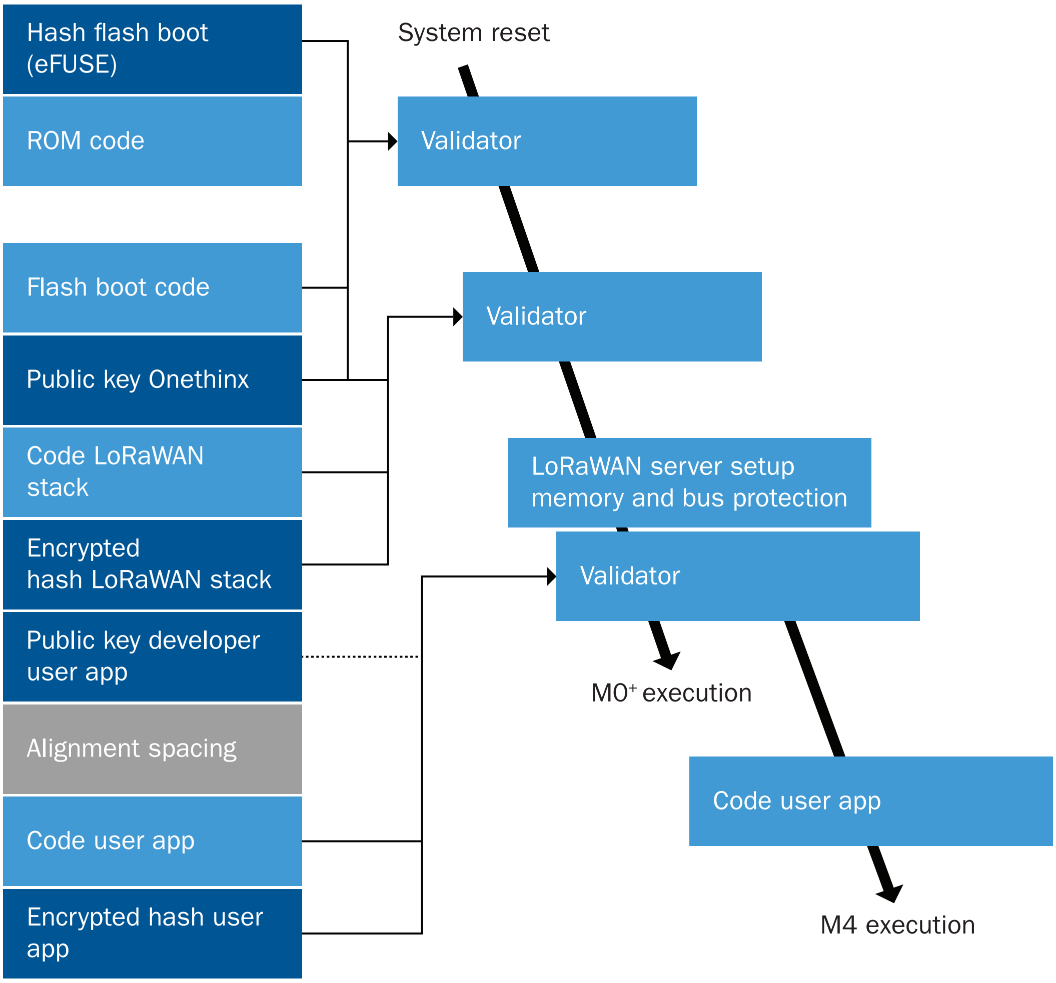
The LoRaWAN specification is designed for secure, end-to-end communication over long range radio links. It uses a set of keys and IDs to uniquely define the IoT device, the application, and the network. The root-keys, used to derive authentication and end-to-end encryption are stored on the device and a Join-Server. The whitepaper "End-to-end secure LoRaWAN: secure Devices with key management from Provisioning to Operations" describes a way to issue and manage these root keys in a secure manner. With that in place, and in combination with the secure LoRaWAN specification, the focus is on the security of the connected device.

Device security

The PSA approach defines that an MCU must start up in a trusted manner. In the PSoC 6 MCU, this is ensured by a section of ROM code that will calculate a hash over the next section of flash executable code and compare that hash with one that is stored in a write-once memory location (a hardware register called eFUSE). The processor will start executing code from the next section only if the hashes match. This is the trusted root that is built upon by subsequent applications.

Chain of trust

A chain of trust is formed by one or more applications that execute subsequently where each validate the next application in the same way as the root element. The validation is done by ROM functions, the stored hash is signed using a private key of the code developer, and its memory location is protected. More details about this process can be found in the Cypress Application Note AN221111. In this note however, there is only a single public key used to decrypt the stored hashes of the applications. If the chain is to be extendible by third-party developers, each application should be signed with the individual developer's key. An API for the secure storage of a key must be made available to functions just like the eFUSE in the secure root.



In figure 1, the sequence of links is illustrated. The left side shows the sectioning of flash, the right side shows the execution order and what information is used for validation. The PSoC 6 MCU has two Arm® cores, an M0+ and an M4, which are connected by the Inter Processor Bus (IPC) that also connects other components (flash, IO, etc.). The first link is the flash boot. It runs on the Arm® Cortex® M0+ core, which is designated as the secure core and is validated by ROM using the hash stored in eFUSE. The second link is the Onethinx LoRaWAN stack. It provides LoRaWAN functionality in a server-client style over the IPC, as is recommended in PSA. Next, it sets up memory and peripheral and bus access protection that isolates the M0+ (the secure core) from the M4 (regarded as insecure).

The CoT is broken when a calculated hash does not match a (decrypted) stored hash. This indicates that the flash code has been altered in some way, which is a potential security breach. This causes the chip to enter a dead state.

LoRaWAN stack

The main function of the Onethinx LoRaWAN stack is to provide the developer (user) application-level access to communication over LoRaWAN. The stack controls a SemTech® SX1261 radio chip. The user application runs on the M4 core and can use IPC calls to initialize the radio link, set and store LoRaWAN join parameters, and send and receive LoRaWAN messages. Additional hardware functions are implemented according to PSA recommendations and used over IPC to increase the security of LoRaWAN. The true number generator is used for generating the random number in LoRaWAN join messages required to prevent replay-attacks.

Physical separation of the user app and the stack ensures that mistakes in the user code will never interfere with the proper functioning of LoRaWAN communication. This fact can be used to speed up the procedure for LoRaWAN certification. In addition, the LoRaWAN join keys can also be stored safely.

Implementation

The secure implementation depends on the LoRaWAN stack running uninterrupted on the M0+ core. Reading, modifying, and executing code on the M0+ must be prevented. Following the setup listed in AN22111::

- Sections in RAM and flash is defined and protected for usage by either M0+ or M4
- Access to I/O that is used for LoRaWAN is restricted
- Access to potentially harmful IPC-calls are restricted

In addition, the debug port on the M0+ (M0+-DAP) is disabled and the programming port is not allowed to access the regions associated with LoRaWAN/M0+.

PSoC 6 have several types of protection units available, which control access of IPC bus masters to (programmable) memory blocks for several attributes. The M0+ and M4 cores are IPC bus masters and can have attributes such as protection context, secure designation, or elevated rights. In the LoRaWAN stack, the bus masters are given different protection contexts, which are used by the protection units to control access. Hence, a call from the M4 call (PC=2) to access the peripherals of the radio chip (peripheral protection unit allows only PC<2) will be disallowed. The same mechanism to separate RAM and flash is implemented using shared memory protection units (SMPUs). The linker script ensures that code and variables are put at the predefined locations.

Several IPC calls, such as flash writes, can be potentially harmful. Since these functions are carried out on the M0+, their access must be controlled in a unique way. The callback function handling IPC calls is extended to control access depending on function and memory location.

The debug ports can be disabled in the access registers of the PSoC 6. There are three access registers, two for the lifecycles ‘normal’ and ‘secure’ and one for when the MCU enters ‘dead’ mode. The LoRaWAN stack writes minimal restrictions to all registers to ensure that the M0+-DAP remains disabled and the programming ports cannot overwrite critical sections. The chip is left in the ‘normal’ lifecycle stage so that the developer will be able to secure the entire device.

Developing a user app

Continuation of code development on a system that has been partially locked-down is quite unique to the LoRaWAN stack. An unknown developer must be able to program and debug his/her application and should have many of the PSoC 6 resources available as is securely possible. This is possible with Cypress’ new ModusToolbox® IDE in combination with either a KitProg3 or MiniProg4 programmer.

To secure his/her code developers can write their public key to a secure part in memory by calling a function provided by the LoRaWAN stack. This can be done once, and from that moment onwards the user app code must be signed with a hash that is encoded by the developers’ private key to be executed. Finally, the developer can lock-down the entire device by writing to the secure access registers and putting the device in secure mode.

Conclusion

Security is a foundational feature required for mass adoption of IoT solutions like LoRaWAN. On-chip hardware and software security, like what is offered with Arm® PSA and Cypress’ PSoC 6 MCU, is required to establish a root of trust that can then be used to authenticate each subsequent application, no matter who creates it or programs it. In the context of LoRaWAN devices, this security is vital to secure the device and system, lock down the LoRaWAN stack so that certifications extend from the module designer to end customers and to ensure that application IP cannot be copied.
Further reading:

1. https://pages.arm.com/PSA-Building-a-secure-IoT.html
2. http://www.cypress.com/documentation/application-notes/an221111-psoc-6-mcu-creating-secure-system
3. https://lora-alliance.org/resource-hub/lora-alliance-security-whitepaper
4. https://lora-alliance.org/resource-hub/member-white-paper-end-end-secure-lorawantm
5. http://www.cypress.com/products/modustoolbox-integrated-design-environment-ide

About Onethinx LoRaWAN Module

Tailored to suit LoRaWAN™ projects that requires ultra-secure end-to-end encryption combined with robust LoRaWAN™ functionality. The Onethinx Core module contains our own PSoC® 6 optimized LoRaWAN™ stack for best performance. Due to the integrated antenna and the ready implemented isolated LoRaWAN™ stack the module is ready to use ‘out of the box’. The Cypress® PSoC® 6 configurable analog and digital blocks ensure an easy and direct connection to virtually any sensor without the need of additional components.

This makes the Onethinx Core module extremely well-suited for projects that require high security and optimal performance like public security, agriculture, leak detection, disaster precaution, gas- and water metering, street lighting applications and many more. www.onethinx.com

About PSoC 6

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. Designers can find more information on the PSoC 6 MCU architecture at http://www.cypress.com/PSoC6

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 http://www.cypress.com

About Onethinx

Onethinx specializes in full service IoT development solutions, with a focus at LoRaWAN network. We follow pragmatic procedures resulting in attractive and user-friendly applications. We offer off-the-shelve and tailor-made applications based on our overall conceptual and technical approach. Building on optimized concepts and technical innovations, backed up with over 15

Cypress Semiconductor Corporation
198 Champion Court, San Jose CA 95134
phone +1 408.943.2600 fax +1 408.943.6848
toll free +1 800.858.1810 (U.S. only) Press “1” to reach your local sales representative

CYPRESS®
EMBEDDED IN TOMORROW™