SECURITY SHOULD NOT BE AN AFTERTHOUGHT

Security threats are multi-dimensional, so protecting the keys has to be the highest priority when it comes to architecting a secure solution

Security threats are multi-dimensional and because of that system developers should incorporate all dimensions equally from the start of the project. Security should not be an afterthought. A weak-spot in any of the dimensions results in compromised security of the whole application.

Each component of a secure design has a level of complexity and risk - the vulnerability level. The key is critical when it comes to sensitive information in a connected design, because the key authorises the fundamental transactions. If the key is accessed and controlled by a malicious user, they can impersonate the connected product and control the transactions with the Cloud service it communicates with.

Therefore, protecting the keys is the highest priority when architecting a secure solution.

Arm TrustZone

Arm TrustZone for Armv8-M is an important framework incorporating security into complex systems. In the case of security, the mere fact that the system is based on running software makes it vulnerable. However, TrustZone technology alone can't be the single barrier of defence in a secure system. It needs to be complemented by other means with the sole purpose of protecting the most important assets of a secure system: its keys.

TrustZone for Armv8-M is a mechanism by which a single microcontroller core is shared between two software contexts.

One world is deemed safe and trusted while the other one is open without the ability to influence the safe and trusted side because of a strict hardware enforced separation of the two zones.

It is a very compelling architecture as it gives software stacks different rights and privileges depending on which world they execute in without adding any significant amount of hardware overhead. The context switch is very quick, especially in the TrustZone for Armv8-M implementation which is dedicated to Arm Cortex-M based core as opposed to the original TrustZone technology implementation that has been augmenting Cortex-A based cores for years.

This platform has been widely used in most commercially available mobile phones today.

The concept is to segregate all valuable assets (keys and software stacks that should not be compromised) in one area that is accessible only by software that's considered trustable. It holds true as long as the zone is truly impermeable.

Successful attacks have been mounted exploiting vulnerabilities that were small holes in the not so perfect impermeable layer separating both worlds.

CLKscrew is one such example and a perfect illustration of how one can mount a non-destructive fault attack on any system running code. Whenever there is software running on a CPU, there is likely a way to fault the CPU hardware to manipulate the control flow of the code and execute portions of the software that would otherwise be non-reachable.

This attack exploits the accessibility of the power management system from both trusted and non-trusted sides and, in future, implementations of power management will be more careful about exposing such vulnerability.

Closing open doors

The question then becomes what is the next element of the system that cuts across the two zones that can be exploited.

When running a trusted execution environment, it is up to the designer to ensure that each peripheral and subsystem touching the trusted zone does not leave an open door.

How can one be sure there is none left? Put differently: how can you be sure that the trusted software has absolutely no bug? It is impossible to claim any software to be 100 percent bug free, therefore, the best protection

MICROCHIP TECHNOLOGY

Microchip Technology is a leading provider of microcontroller, mixed-signal, analogue and Flash-IP solutions, providing low-risk product development, lower total system cost and faster time to market for thousands of diverse customer applications worldwide. Headquartered in Chandler, Arizona, Microchip offers outstanding technical support along with dependable delivery and quality.

MICROCHIP / SECURITY

NICOLAS SCHIELI, SR. MANAGER STRATEGIC/PRODUCT MARKETING,
SECURE PRODUCTS GROUP, MICROCHIP TECHNOLOGY

against software exploits is to strictly isolate keys from any software.

The main value add in a secure TrustZone for Armv8-M environment is to enable and enforce the practice of isolating safe software from unsafe software.

Imagine a safety critical device involved in life threatening applications like medically connected equipment. Unsafe software such as open source based human interface stacks need to be isolated from actuating code. Software is never without bugs, it's a living entity that evolves. Yet in our connected medical equipment example, a bug in the user interface must have absolutely no impact on critical code.

A secure element is a device that has been designed with security as the first and only goal, with the mind-set of leaving no compromise in the implementation.

Critical elements of the secure device are:

- High quality random number generator following implementation recommendations by NIST (US government), ANSI (French government) or BSI (German government);
- Dedicated secure key storage
- Hardware implementation meant to protect against any known kind of attack and especially side channel attack such as fault, glitch, differential power analysis (DPA), etc.
- Physical protection against physical tampering of the device
- Certified standard and proven cryptographic algorithms (AES128, SHA256, ECC P-256)
- Measured resistance against known vulnerabilities by an established third-party laboratory following regulated processes (e.g. JIL vulnerability assessment from the Common Criteria certification process).

The ATECC608a secure element from Microchip was graded with a JIL level of High. It means an external test laboratory has not been able to extract the keys using various penetration testing methods over a specified period of time. The designation gives the designer confidence that the device has one of the highest levels of key storage protection possible.

More importantly, a secure element is a piece of hardware that is designed for the sole purpose of protecting keys while giving a system the ability to use them without ever exposing them. In other words, the key(s) never leave the secure element.

In the semiconductor industry that drove most of its growth through combining more functionality in a single piece of silicon, it is counter-intuitive to consider this secure key storage technique is better when not integrated with other features on the silicon.

The optimal solution

A secure connected solution is composed of layers of security features addressing different objectives. These objectives have to be prioritised by sensitivity levels before designing a system keeping cost in mind to take the right trade-offs. Here is a template of good practices for Internet of Things (IoT) hardware when considering a security model:

1. Define and create your authentication model: plan to use a truly secure storage
2. Isolate trusted from untrusted software: use the benefits of a TrustZone for Armv8-M architecture
3. Encryption only has value with established trust and isolated software
4. Manage the firmware updates and verify them with a trusted key
5. Implement secure boot using an immutable bootloader implementation that also has a trusted and protected key to verify the boot sequence

> “If the key is accessed and controlled by a malicious user, they can impersonate the connected product and control the transactions with the Cloud service it communicates with.”

When it comes to small and constrained IoT devices, isolate cryptographic keys and algorithms from any software by using a secure element which has been designed to defend against a wide range of attacks. Combine a TrustZone for Armv8-M-enabled microcontroller and a secure element. Each one will contribute what it is best for the system, respectively isolating the software and isolating the keys.

Microchip offers both with the SAM L11 microcontroller and the ATECC608a secure element.

Use traditional security practices such as encryption and firmware management.

Here is a list the key characteristics and benefits of such a combination:

1. NIST SP800-90A, SP800-90B, SP800-90C compliant Random Number generator
2. Strict isolation of keys and cryptographic algorithms from any software
3. Independently verified strength of key storage
4. Strict isolation of critical communication stacks within TrustZone for Armv8-M
5. Strict immutable bootloader model to guarantee only authentic firmware will run.

MICROCHIP

www.microchip.com