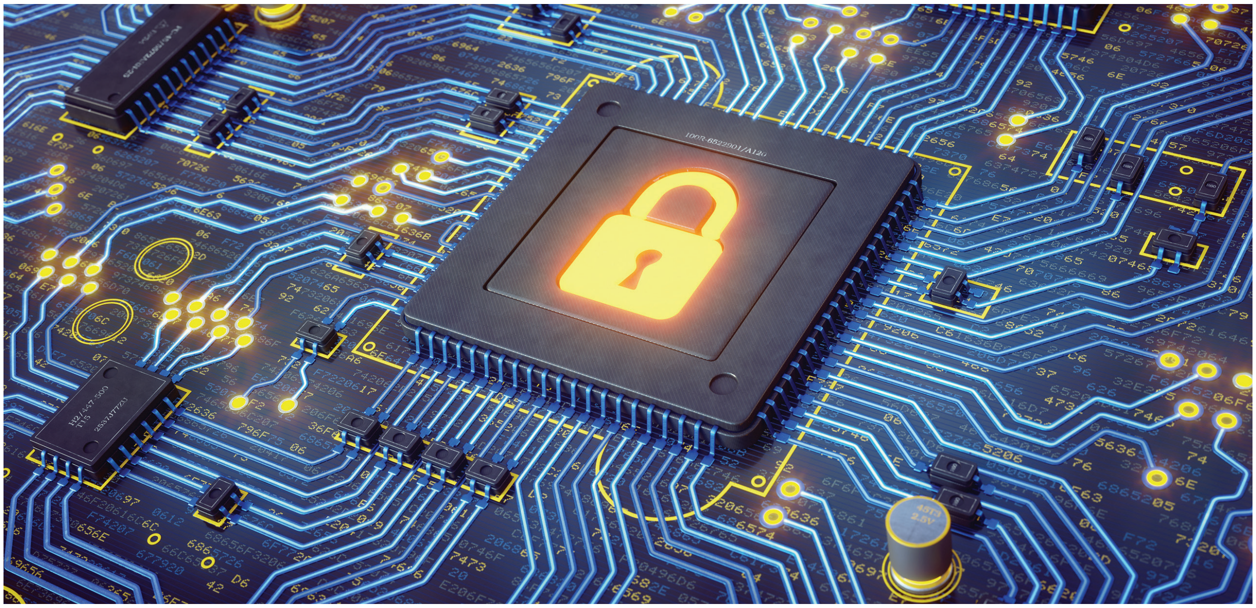
IoT Modules Hardened with End-to-End Security



TELIT WHITEPAPER 02.2020

SPONSORED BY

Executive Summary

As awareness of the transformative nature of 5G is increasing, the industry is slowly waking up to the enormous challenge of securing not only the networks but also all the things these networks connect and the vital data they carry. When it comes to the Internet of Things (IoT), the challenges of security and the stakes involved couldn't be more significant. The spread of IoT in homes, enterprises, industries, governments and other places is making wireless networks the backbone of the country's critical infrastructure. Safeguarding it against potential threats is a basic need.

IoT security indeed is very complex and multifaceted. The entire system, including the infrastructure, devices and the links that connect them, need to be secured to be effective. Many times, with national interests and security at stake, the challenge becomes about not only the system but also the supply chain, as well as how the various system components are sourced, deployed and managed.

IoT modules, being at the heart of IoT devices, are fundamental to the system security. Unlike smartphones, modules are simple and very vulnerable to intrusion. Any compromised module exposes the entire system and puts it at risk. Hence module security must be comprehensive, including the device hardware, software, firmware and management system (a.k.a., cloud platform) that facilitate ongoing operational security throughout the device lifecycle. The responsibility of securing the IoT modules typically falls on the shoulders of module vendors, as many IoT device vendors and users may not have the expertise or the means to access and secure the module themselves.

This paper examines the comprehensive security needs of IoT modules and platforms and discusses the best practices to ensure that the whole system is protected.

Contents

TANTRA ANALYST

What Is End-to-End IoT System Security?

Cellular IoT is a complex system, and its security is equally complex. For it to be effective, one must address the full system. The system typically consists of many parts, but from the security point of view, mainly three logical parts:

1. the IoT device with all its software, firmware, hardware, applications, etc.;
2. the cellular network infrastructure, including the radio network, the core network, etc.; and
3. the cloud that connects the IoT network to the outside world, which could include the user cloud that houses the IoT user applications, connection to many kinds of systems that use the IoT network, etc., as well as the cloud platform for managing the IoT devices.

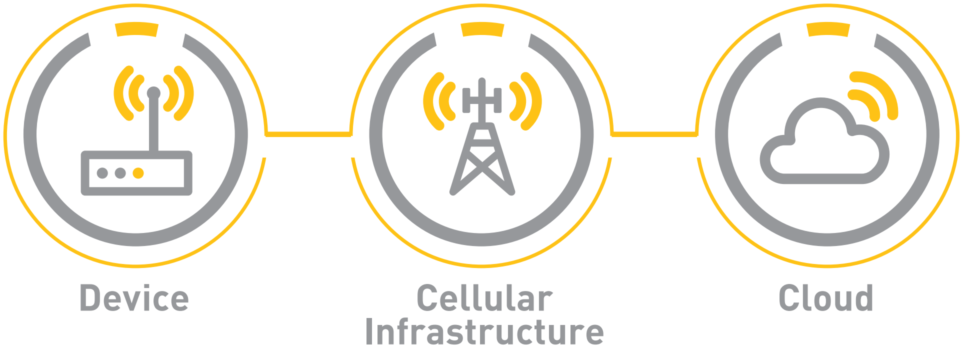


Fig. 1. An end-to-end approach is a must for overall IoT system security

System security is about not only installing and onboarding devices and networks securely but also managing their ongoing operations throughout their lifecycle and identifying and isolating any threats.

The IoT security discipline is vast. The scope of this paper is to explore aspects related to IoT device security and, specifically, the modules that are brains of those devices.

Why Is IoT Device Security Important?

With 5G set to usher in Industry 4.0 — the next industrial revolution — not only the private and public enterprises but also governments across the globe are understandably taking a keen interest in how to deploy 5G. There has naturally been a lot of emphasis on its security aspects. The current focus has primarily been on the network infrastructure side. However, among the parts of the IoT systems, devices are the most vulnerable and need substantial attention.

A Growing World of Security Concerns for IoT Devices

There are many reasons for the vulnerability of devices. First, they are typically simple, with limited processing capability and memory. It is impossible to run sophisticated, processor-heavy security applications on them. Secondly, they are usually deployed in large numbers and can be physically be accessed and compromised. Third, they tend to have a long life, often exceeding 10–15 years, which means one must keep up their security the whole time. At the same time, because of their importance, even a small hacked IoT device might compromise the entire system, while unnoticed by users or service providers.

IoT Modules Are Key to IoT Device Security

The module is the brain of the cellular IoT device. Module vendors take barebones chipsets from vendors like Qualcomm and Intel and add their software and additional hardware to create modules with standard interfaces. Device manufacturers develop their machines based on these modules. Modules simplify the connectivity and operator certification-related complexity, so device vendors concentrate on developing use-case-specific devices. So, the responsibility of IoT device security rests on the shoulders of module vendors.

Due to device vulnerability, the integrity of the supply chain of IoT devices and especially modules is key not only for system security but also for national security. IoT users should know where the vendor manufactures the modules and what safety measures they have in place to ensure the manufacturing process does not compromise the device and module integrity at any stage. They should employ rigorous evaluation and vetting practices before widely using them in their systems. It is a common misconception to assume that if the cellular chipset vendor is of known origin and trusted so must the module be. Given the amount and complexity of embedded software that vendors deploy in the module, that assumption is completely flawed. Moreover, since IoT devices have a long life, IoT users should establish that vendors have long-term viability to support the ongoing security of devices during their full lifecycle, including offering security patches, bug fixing and more.

A Comprehensive Model of IoT Device Security

As shown in Fig. 2, the comprehensive IoT module security in an IoT system has three main parts: 1) secure module, 2) secure cloud platform, and 3) secure transport.

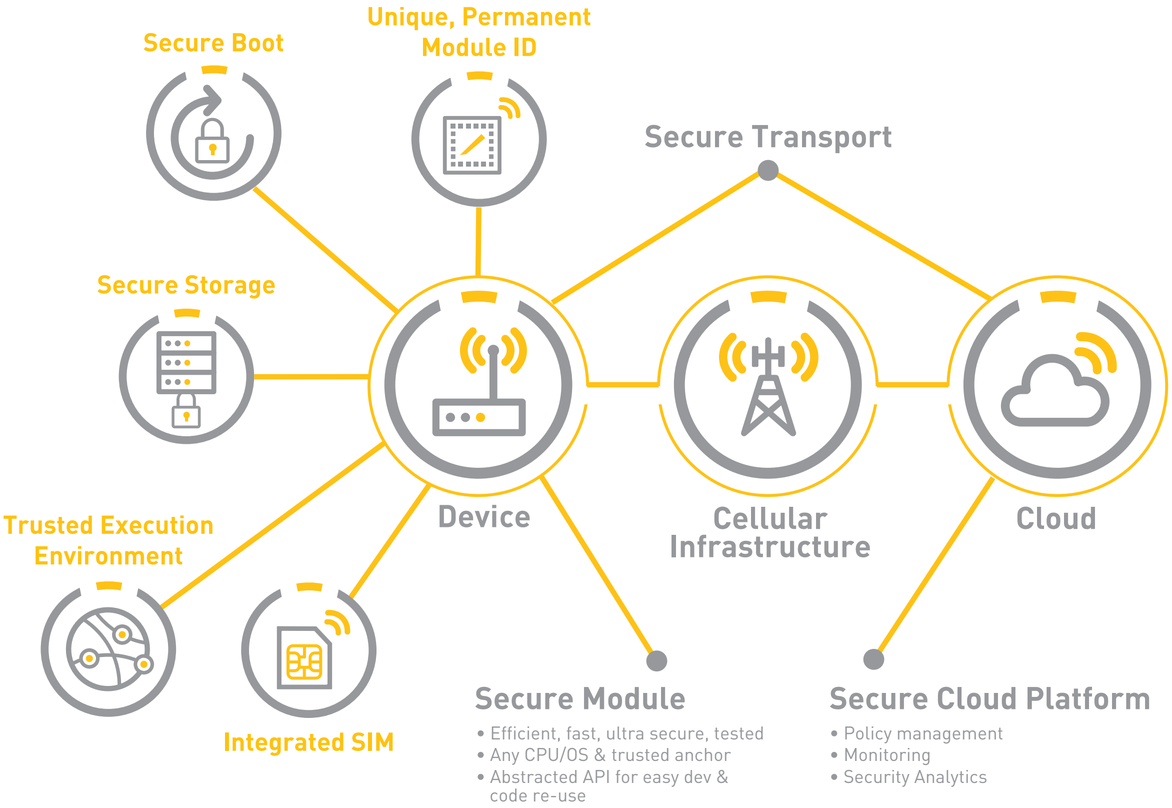


Fig. 2. Components of comprehensive module security in a cellular IoT system

The security in IoT systems is primarily achieved through pre-shared public and private keys and a set of industry-standard protocols. These keys are securely stored within the module or device, pre-shared in the platform and used for discovery, authentication and encryption.

Let's look more closely into what each of the components represents and what are the best practices to secure them.

Secure IoT Module

For the most part, the IoT module defines the security of the device. The main security element is the module's identity, which should be unique, indelible and permanent. This identity can be either hardware-based (e.g., chipset ID) or burned into the firmware at the point of manufacture. It is even better to have the module ID based on a mix of hardware and firmware to make it impossible to clone and easy to fit into a wide variety of forms, lengths and more as required by the IT systems of IoT users. This ID should never be allowed to change, no matter where it is used, in what network, for what application, etc.

The unique module ID also allows secure zero-touch onboarding and remote management. Before shipping, the vendor should program the devices to do only one thing when they are turned on — look for and connect to the trusted platform. The device ID and all relevant information should already be shared with the platform, so when the device is installed on-site and turned on, it searches for and only connects to the platform, eliminating any hijacking or hacking before it is connected to the network. The platform can readily identify it, communicate securely, configure it automatically and complete the onboarding. Touchless onboarding is not only simple, quick and secure but also extremely cost effective.

A fundamental and minimum requirement for module security is the presence of a Trusted Execution Environment (TEE). The TEE is a mix of hardware and software features used for securely storing data, including the module firmware, encryption keys, sensitive user application data and more, as well as space for running secure applications such as the operating system (booting). The module should have a secure boot with signed module firmware, which becomes the root of trust for the it. All sensitive functions should run in the TEE including some of the central IoT user applications. Many of these applications might run on the same processor core with other non-secure applications. However, there should be a clear, logical separation between the two. The interaction between secure and non-secure applications, as well as access to secure data, should only happen through vendor-provided APIs.

Another significant security consideration for modules is supporting an integrated virtual SIM to further reduce security concerns. The current trend is to support SIMs both physical and integrated (iSIM). iSIMs will soon become the norm for IoT devices. Due to their sensitive nature, iSIM functions must run entirely in the TEE.

Many of the functions discussed here are primarily enabled by the underlying chipsets used in the modules. However, module vendors are the ones responsible for correctly implementing them in their firmware and features. They should adopt layered security architecture to make it suitable for customers with varying levels of expertise — simple, robust, and ready to go security for novices, and more sophisticated API and interfaces for the knowledgeable customers for more flexibility and customization.

Conclusion

IoT security is very complex and multifaceted. It requires an end-to-end approach to secure the complete system, including the devices, infrastructure, cloud, all the links that connect them, all the hardware, firmware and software. Network security is only as strong as its weakest link. Simple IoT devices that lack strong processing and storage capabilities are especially vulnerable to hacking and unauthorized intrusion. Since they are deployed in large numbers and have a long lifespan exceeding 10–15 in many cases, compromising their security might cause significant disruption. Because many critical national infrastructures run on IoT systems, it is immensely important to secure not only their networks but also scrutinize their supply chains.

IoT modules, which are the hearts and often brains of IoT devices, are the cornerstones of IoT system security. As such, their security primarily falls on the shoulders of IoT module vendors. Comprehensive IoT module security should include module and device security and cloud platform security hardened by integration at the deepest level inaccessible to bad actors, as well as the security of the transport that connects the two. This security is primarily achieved through standards-based state-of-the-art protocols using pre-shared keys synchronized between the modules and the platform. A unique native ID permanently etched into the module is essential to its security. A cloud platform that is pre-provisioned with module IDs and its keys allows quick, secure and cost-effective zero-touch onboarding and lifecycle management. Role-based access management allows different levels of access to minimize risks because of human error and maximize overall security. A secure end-to-end encrypted transport is the lifeblood of the system, and redundancy of an alternate mode of device management transport for emergency conditions is a lifeline of the system.