insight.tech
POWERING IoT AND EMBEDDED INNOVATION

IoT Security (Finally) Delivers ROI

Brandon Lewis

In the electronics industry, the term "security" is generally used to describe protections against malware or brute-force hacking. This is a somewhat limited view. Security also includes defense against reverse engineering, software licensing protections, encrypting data at rest and in motion, remote device attestation, and other functions.

Take firmware and data protection as examples. Firmware must be locked down to prevent IP theft or execution of illegitimate code. Data in transit needs to be secured to prevent spoofing or man-in-the-middle attacks.

Both of these functions depend on cryptographic keys—as do many other security functions. As a result, securely storing these keys is of paramount importance. This can be achieved through software- or hardware-based technologies.

In a software-only approach, keys are stored in device memory. This is a popular option for lower-value assets, as it provides a basic level of security with minimal upfront cost. But keys in device memory are vulnerable to security gaps elsewhere in the system. Developing more advanced protections to guard against this can be extremely complex.

With a hardware-based approach, cryptographic keys are generated within a protected, inaccessible region of a discrete IC. While there is additional BOM cost associated with this architecture, secure hardware elements reduce development complexity and also remove the overhead of cryptographic workloads from the host processor.

The most well-known of these hardware-based encryption devices happens to be an industry standard: The Trusted Computing Group's (TCG's) Trusted Platform Module (TPM).

Inside the TPM

In essence, a TPM is a secure microcontroller that stores artifacts such as cryptographic keys, passwords, and certificates that a device uses to prove it is what it claims to be (authentication) and that it has not been compromised (attestation). This provides the foundation for capabilities such as remote device authentication/attestation and secure boot **(Figure 1)**.

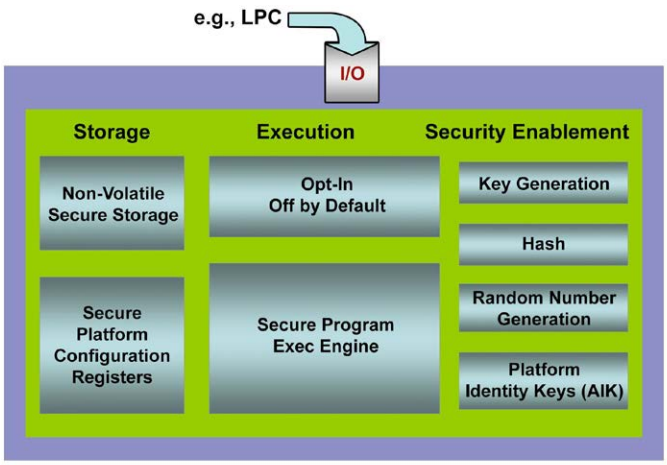

Figure 1. Trusted Platform Modules (TPMs) are an industry standard. (Source: Trusted Computing Group)

Remote Device Authentication & Attestation

Remote device authentication and attestation is critical for IoT devices because it allows them to securely connect to networks with little or no user configuration.

To enable this functionality, a security algorithm based on a device's unique, private cryptographic key is used to sign a digital certificate. This certificate is then sent to a certificate authority (CA) that authenticates the device's signature, and also signs the certificate. Once signed by both parties, other connected endpoints can accept communications from the original device, knowing that it is a trusted source. This process is referred to as public key infrastructure (PKI).

Here, TPMs provide a couple of benefits. First, cryptographic keys stored in an inaccessible region of TPM hardware cannot be tampered with, and maintain a device's identity over time. This feature is especially relevant for devices that may not attempt to authenticate for weeks or months (such as the time between leaving the manufacturer and reaching the end user).

Second, the TPM also provides secure storage space for digital certificates, ensuring that they cannot be altered. Authentication and attestation are therefore possible.

Secure Boot

While TPMs do not control or run device software, applications can use a TPM to store sensitive information. One of the most common datasets housed in TPMs is pre-runtime configuration data. This enables a feature called secure boot.

In secure boot, information about the sequence and/or types of files associated with the system boot process can be stored as secrets on a TPM. If these parameters are breached when a device attempts to boot, the TPM can inform other programs, such as the OS. From there, the OS can enforce policies that restrict access to data or applications, or cancel the boot process altogether.

This is particularly useful in defending against the execution of illegitimate code (such as malware) or locking down devices that have been stolen.

Toward Total System Security

TPMs are intended only to safeguard a system's most sensitive assets. A system can still be exploited through vulnerabilities in the applications or OS. Plus, data residing on a device can still be accessed by unwanted users.

One solution for IoT developers looking to extend the protections of a TPM throughout an entire system is the CodeMeter ASIC from WIBU-SYSTEMS AG. Delivered as a smart card chip, the ASIC supports SPI and USB communications for easy integration with a variety of embedded and consumer devices **(Figure 2)**.

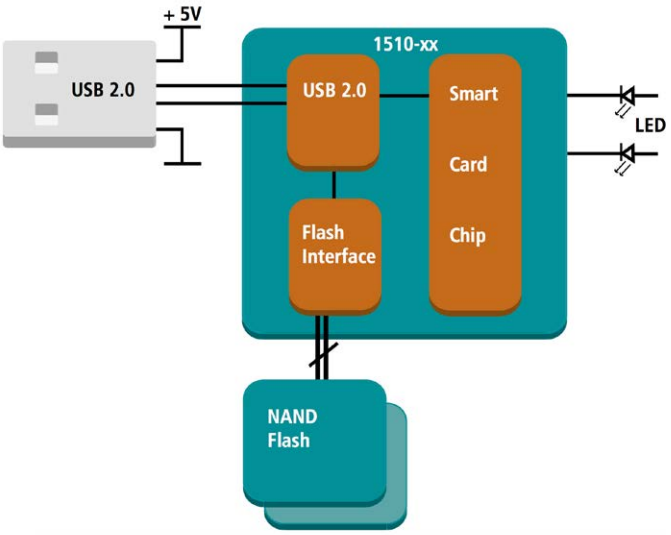

Figure 2. The CodeMeter ASIC enables security beyond what a TPM can provide. (Source: WIBU-SYSTEMS AG)

Like a TPM, the CodeMeter ASIC is an EAL 5+ secure hardware element that includes a FIPS 140-1 random number generator (RNG) for cryptographic key generation, as well as support for 128-bit AES, 256-bit SHA, and 224-bit ECC encryption algorithms.

What sets the ASIC apart is its accompanying software. The CodeMeter Protection Suite allows developers to encrypt all or some of the executables in their system software to protect against debugging and reverse engineering.

The CodeMeter Protection Suite works with a range of general-purpose and real-time OSs, and different

variants are available depending on system requirements. Integrating the software is a one-time process, with limited impact on system performance regardless of the extent of encryption.

WIBU-SYSTEMS AG also offers an API for its platform. Available in ANSI C source code, the API enables the development of special features or integration with other security technologies such as Intel® vPro, Intel® Advanced Encryption Standard – New Instructions (Intel® AES-NI), and Intel® Software Guard Extensions (Intel® SGX).

The CodeMeter ASIC acts as a secure hardware anchor regardless of implementation.

Security (Finally) Delivers ROI

Another key feature that distinguishes CodeMeter ASIC from a traditional TPM is its capacity as a digital rights management platform. Of the minimum 128 Kbytes on the ASIC, about 60 Kbytes are reserved for storing licensing information. This allows IoT OEMs to deliver features to end users and control their access over time, with support for licensing models such as:

- Single-user licenses
- Network licenses
- Feature-based licenses
- Pay-per-use licenses
- Time-based licenses
- Named-user licenses

Kontron is one IoT device OEM currently taking advantage of the features of the CodeMeter ASIC in its APPROTECT security solution.

Kontron APPROTECT is a turnkey security solution that offers protections against IP theft, tampering, reverse engineering, and copyright/licensing infringement.

By integrating a CodeMeter ASIC directly onto the motherboard of various embedded computing modules, cryptographic keys can be used to determine if a device has been approved to run certain software **(Figure 3)**. It also, of course, provides foundational system security.

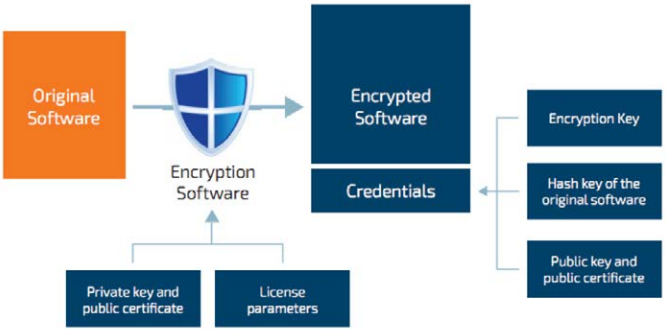

Figure 3. Kontron's APPROTECT provides device security and license management.

The APPROTECT solution is available on all Kontron products featuring 6th generation Intel® Core or Intel® Xeon® processors, as well as the latest generation of Intel Atom®, Intel® Celeron®, and Intel® Pentium® processors. An upgrade kit is also available for legacy devices.

Security That Pays for Itself

IoT security has suffered thus far from a lack of understanding in the development community and the perception of cost without return. Hardware security modules are now available that remedy both.

With hardware security modules, IoT device developers can offload the complexities of encryption to a complete IC that extends protection throughout an entire system. And business makers can transform their businesses with software licensing models that pay for this security, and then some.