We are now in the business of connecting everything to everything. And with this, the Internet of Things (IoT) is born. Once this total connectivity is accomplished, the collective effort this brings lets us start the next string of new and exciting systems. This results in massive amounts of data that must be trusted and processed (Figure 1).

But, as they say: "buyer beware." This is all good, but total connectivity opens the opportunity for unintentional or malicious data corruption and contamination to occur. Cryptographic methods can be applied to resolve these vulnerabilities. A decision that system designers face is deciding between software-based or hardware-based security solutions. Both technologies combat unauthorized access or modification to data; however, their differing features bear further examination before making the final selection.

**Software-based security**

Utilizing existing system resources, software security systems were the first to show up in the marketplace. These solutions are relatively inexpensive, as they share resources to protect and safeguard data with other programs in the system. An additional capability of a software-based implementation is the ability to revise and upgrade security as threats and vulnerabilities evolve.

A software security system places a load onto a host processor. Potentially, this could compromise the overall system efficiency. Beyond these concerns, the software approach is the weak link within
systems-security architecture. Secrets remain vulnerable to discovery and the algorithms typically run on general-purpose non-secure hardware and are similarly an attack risk.

With all this said, cost-effective, software-based security can be effective in physically secure environments, preventing unauthorized access to the system.

**Hardware-based security**

Hardware-based security uses a dedicated integrated circuit (IC), or a processor with specialized security hardware, specifically designed to provide cryptographic functions and protect against attacks. Security operations, such as encryption/decryption and authentication, take place at the IC hardware level where crypto algorithm performance is optimized. Additionally, sensitive information, such as keys and critical end-application parameters, are protected within the electrical boundary of crypto-hardware.

The security IC contains circuit blocks such as a math accelerator, random number generator, nonvolatile memory, tamper detection, and a physically unclonable function (PUF). The PUF block is particularly interesting in that it has a unique characteristic of being immune to invasive or reverse-engineering attempts to extract sensitive data such as a cryptographic key. The Maxim DS28E38 is an example of a security IC that integrates PUF, both to generate keys and to protect against invasive security attacks.

It is incredibly difficult and expensive to alter silicon; therefore, cybercriminals are deterred from attacks on hardware-based security. Further, when attacked, the security IC is capable of shutting down operations and destroying sensitive data before being compromised. Such a solution may be a little more expensive, but it provides a dramatic reduction in the risk of unauthorized access to embedded devices, peripherals, and systems.

Hardware-based security is very effective in all application environments, especially those where the end equipment is exposed and physically accessible to the bad guys.

**Buckle your seat belt**

Overall, security can be a complex subject. But it is one that must be addressed and embraced to prevent bad things from happening to an end product such as an IoT device. Software-based security is an option, but the path to comprehensive and reliable security is to select a hardware-security alternative.

*Bonnie Baker has been working with analog and digital designs and systems for more than 30 years, and is writing for Maxim.*

**Related articles:**

- [IoT & cloud security overview](#)
- [Single-chip end-to-end security for IoT devices connected to the Amazon cloud](#)
- [Enabling secure wireless medical devices with the MSP430 MCU](#)
- [Security: where the IoT meets the IT infrastructure](#)
- [What’s needed to securely fit IoT devices into the enterprise framework](#)
To learn about common threats to online and local accounts and to understand how hardware-based multifactor authentication using the FIDO (Fast Identity Online) standard significantly improves protection, check out this webcast sponsored by Infineon.