Root of Trust approach secures the IoT

The Internet of Things (IoT) brings challenges, particularly in respect to security

By: Steve Hanna, Infineon Technologies

The easily discerned lines separating cyberspace and the "real world" are disappearing. With the advent of the Internet of Things (IoT), physical objects are increasingly integrated in information systems and individuals are interacting with vast distributed networks dozens of times a day. Clearly, the IoT will change the way people live and work, while changing the way the world itself works around us. With these changes come challenges, particularly in respect to security.

The threat environment faced in implementing the IoT is directly related to the strength of the Internet. The standardized technologies that allow global connectivity are well understood by the engineers and developers building the IoT, but also by villainous characters. To a large extent the architecture of the Internet relies on software-based cryptographic mechanisms to provide security functionality. Inevitably, vulnerabilities in the overall network architecture and the devices connected to this network will be found and exploited at large scale. What is missing is a strong Hardware Root of Trust (HRoT), with dedicated cryptographic functionality, to provision and enforce security policy.

Stronger security from a hardware Root of Trust

There are examples of distributed networks, such as those in the financial industry, where computer servers and systems employ a secured processor or co-processor to protect against exploits that can undermine software-based security software. Such well-designed systems protect against three categories of attack.

1. Semi-Invasive attacks are those in which an adversary tries to induce faulty behavior in the system, which can allow circumvention of security, data manipulation or even extraction of a secret key. An HRoT built with a dual-processor architecture, comprehensive hardware error detection, and protective sensors can detect these types of attacks and then report/act appropriately.
2. Observing attacks are those in which the physical behavior (power consumption, electromagnetic emanation, and photon or heat emissions) is analyzed to yield information about the programming inside the system. Full encryption of all data on an HRoT device and massive randomization generate a highly efficient barrier against such attacks.
3. Manipulative attacks, in which micro-scale devices are used to intercept on-chip signals, can extract useful secret information from unprotected chips. By utilizing memory and data path encryption as well as physical countermeasures, an HRoT can be protected from manipulation threats.

Proving the identity of "Things"

Before any exchange of data between two points on the Internet, connected devices need to verify that transactions take place between "trusted" points. Thus, the basis of security in the IoT is the verification of the identity of billions of devices

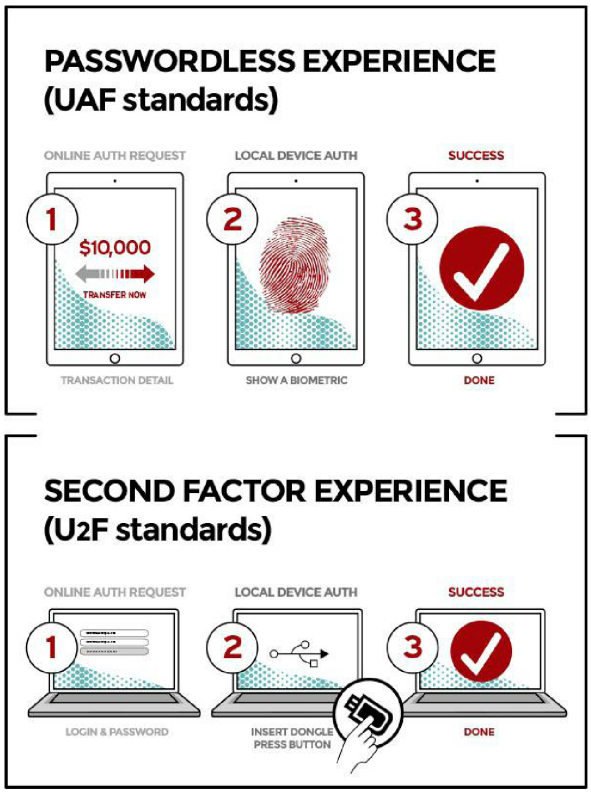

Figure 1: Strong Authentication according to FIDO (Image courtesy of FIDO Alliance)

and users. Today, HRoT devices that are certified by the global Common Criteria evaluation methodology are deployed in hundreds of millions of devices, demonstrating the required interoperability and strength of a security ecosystem that is capable of verifying identity and protecting the integrity of each device. Below examples demonstrate several use cases for this strong identity technology when we build the IoT.

User identity for IoT

IoT users demand remote access to their devices from anywhere, but still need ease of use and strong security. The simple approach of the username and password authentication fails to meet these requirements since strong passwords are infrequently used (and easily stolen even when used). Recently, the FIDO (Fast IDentity Online) Alliance has released standards for an open, scalable, and interoperable set of multi-factor authentication mechanisms.

As illustrated in **Figure 1**, FIDO permits users to associate their online accounts with a local hardware security token. Then they can use this token to authenticate with other systems, either with or without a PIN. There are two benefits of the FIDO approach for IoT users. First, they get stronger security. Second, the complexity of managing device credentials is vastly reduced.

Device identity for IoT

Ultimately, IoT devices will control thousands of critical systems, ranging from door locks and security cameras, to cars, factory systems and public infrastructure. All will be, or already are, exposed to a variety of network-based threats. To block access by unauthorized parties trying to tamper with device controls, IoT devices must be able to conduct mutual authentication with users, other devices, and the cloud. Fortunately, device identity technologies (e.g., IEEE 802.1AR) are well established and widely available. In this approach, a secure device identifier (DevID) is cryptographically bound to a device and supports authentication of the device's identity.

With an HRoT, the cryptographic authentication can be protected from the types of attacks discussed earlier. IoT devices that are fully capable of establishing, maintaining, and employing long cryptographic keys can be implemented using any of several authenticated and secured processing devices.

Some security chips – such as the open standard Trusted Platform Module (TPM) – go further than establishing device identity by also performing encryption and detecting when a device is compromised. Monitoring system integrity is especially important for IoT, because a rogue device with valid credentials can cause real physical damage.

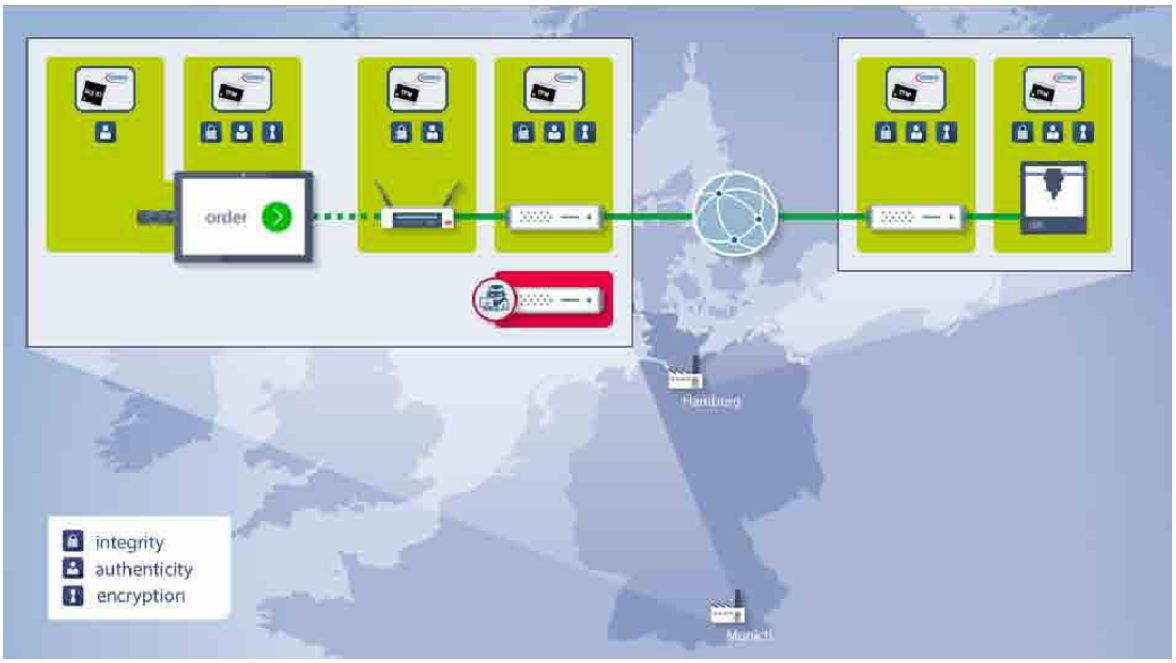

Figure 2: End-to-end Security for the Industrial Internet

Identity for the industrial internet

The Industrial Internet is the application of IoT concepts and technologies in industrial settings. For example, advanced factory automation uses networking to integrate the entire supply chain from supplier and customer, enabling suppliers to customize production to match demand. In such an environment, identity must be verified and communications must be protected end-to-end to make sure that system integrity is maintained. Therefore, all elements of the system from customer to supplier must be secured (see **Figure 2**).

To improve system security and integrity, an HRoT can be integrated in all parts of an Industrial Internet system from a tablet used by customers ordering products to the factory line where the products are manufactured and beyond into shipping, distribution, wholesale, and retail. Different HRoT devices can be used to establish product, device, and user identity, to protect identity and perform encryption and authentication, and to maintain device integrity from the core network server to all network edge points. Such security solutions also offer protection of sensitive IP and process knowhow.

Looking forward

Strong identity authentication and protection for users and devices is a critical requirement for successful build-out of the Internet of Things. We have already seen attacks across cyber-physical boundaries that could have been stopped, or limited, by strong identity protection. Because of the many applications envisioned for the IoT, the impact of these attacks is not restricted to the smart home or connected car, but extends to industrial automation, health care, and many other domains. Fortunately, standards and technologies for strong identity are available without sacrificing ease of use. Hardware security is an essential element in implementing these technologies. When designing for any system that links cyberspace and the physical world, strong identity implemented with secure hardware should be a requirement. Only in this manner can safety be protected

www.infineon.com