Securing Factories and Infrastructures in the Age of IoT

With the rise of the Internet of Things (IoT) and "Industry 4.0," factories and critical national infrastructures are becoming connected networks. Processes are remotely monitored through sensing and connectivity solutions, allowing for greater control, powering predictive analytics and optimizing throughput, leading to a higher return on investment. But when processes rely on the integrity of connected sensors and their data, strong security becomes indispensable. Sensitive data is transported on connected networks, which must be kept safe from eavesdropping and alteration. Herein we discuss how data should be protected from IoT device to cloud services.

With the rise of the Internet of Things (IoT) and "Industry 4.0," factories and critical infrastructures are becoming connected networks. But when processes rely on the integrity of connected sensors and their data, strong security becomes indispensable.

Problem

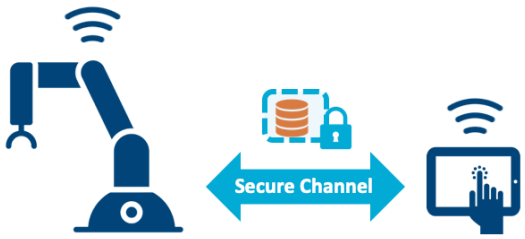
- Mission-critical continuity and safety in connected networks depend on accurate transmission of sensor data
- Data is vulnerable to eavesdropping and alteration when it travels from device to dashboard or cloud
- Resource and budget constraints impede traditional security measures in IoT
- Once deployed, IIoT devices cannot easily adopt a security system upgrade with traditional methods

Solution

- Start security where the data is created, by deriving a unique and unclonable identity, based on SRAM PUF, for every device
- Use the identity to authenticate and encrypt all data to protect it from the moment it leaves the device all the way to the cloud system

Results

- Secure data transfer from its creation
- An unclonable, immutable, invisible and unique identity to authenticate every device
- Low-cost solution for a scalable market
- Low resource requirements for IoT devices
- Flexible integration in hardware or software
- For software integration, retrofitting of in field devices is also possible



Securing Factories and Infrastructures in the Age of IoT

The SRAM PUF identity is immutable, and invisible to adversaries, creating an unequalled anchor of trust for every device.

In all Industrial IoT networks, sensors are the genesis of the journey for IoT data streams. These sensors are creating the data on which decisions are based and action is taken. Imagine what happens when attackers manipulate sensor data, which can bring entire production lines to a halt, or endanger the wellbeing of people in and around a factory or infrastructure. It is highly important that sensor data is transported accurately from its source to where decisions are made — at an on-premises control server or in the cloud.

Keeping sensor data safe is not a trivial task, since it requires end-to-end security. To get data safely from IoT device into the cloud, a secure channel needs to be established. The secure channel makes sure data cannot be eavesdropped upon or altered when in transit. To establish this channel, the device and the cloud service need to exchange keys and certificates. Many methods exist for this, such as "zero touch provisioning."

The biggest challenge when applying these methods is to get the required keys and certificates on the IoT device. The traditional method for provisioning keys and certificates is to use an additional chip in the device, such as a secure element (SE). However, this comes with significant downsides:

- Higher BOM cost for an additional chip
- Dependency on SE vendor to handle keys
- Extra effort to onboard SE
- SE cannot be added to in field devices

Solution: Secure Sensors

These problems are resolved by Intrinsic ID's secure sensor-to-cloud solution. Using Intrinsic ID's patented SRAM PUF technology, the IP creates a unique and unclonable identity for every IoT device, which is never stored in memory and cannot be copied from device to device. The identity is immutable, and invisible to adversaries, creating an unequalled anchor of trust for every device. Keys derived from the SRAM PUF are used to create a secure channel.

Semiconductor manufacturers may license Intrinsic ID solution as embedded hardware IP. Module and IoT device manufacturers can procure chips with Intrinsic ID IP already embedded, or license the software IP directly. This is the only software solution that can create a strong root of trust in hardware.

Since no additional hardware components (such as secure elements) are required, the solution can be flexibly integrated and comes at an IoT-scale-friendly price point. Deployed devices can even be upgraded with an over-the-air update without the need for an expensive redesign of the system.

Bottom Line Benefits

- Unclonable, immutable and invisible ID
- Authentication and encryption of data
- Strong security at a low price point
- Flexible integration in software, allowing for over-the-air updates for existing devices

** For details see our white paper "SRAM PUF The Secure Silicon Fingerprint" http://go.intrinsic-id.com/secure-silicon-fingerprint-lp*