Securing Sensors in the Age of IoT

The time when a sensor needed only to sense is behind us. With the rise of the Internet of Things (IoT), sensors are part of a connected network. As sensor data is transported from its source to where decisions are made, it must be secured – not a trivial task, given that IoT devices are in the field and are rarely physically protected. Using SRAM PUF technology to create a unique and unclonable identity for every sensor provides the basis for strong authentication and encryption.

With the rise of the Internet of Things (IoT), sensors are part of a connected network in which sensitive data is shared. Given that IoT devices are in the field and are rarely physically protected, an adversary can easily get access to the device.

Problem

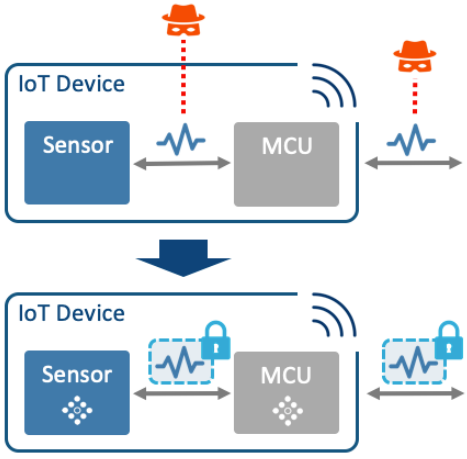
- IoT devices are in the field and are typically not well protected, which gives adversaries easy access for logical and physical attacks
- With access, the interface between chips in an IoT device can be snooped
- Data is vulnerable for eavesdropping when it leaves the device
- Traditional security measures do not work well for sensors, due to resource and budget constraints

Solution

- Start security at the sensor, where the data is created, by deriving a unique and unclonable identity, based on SRAM PUF, for every sensor
- Use the identity to authenticate and encrypt all data to protect it from the moment it leaves the sensor
- For maximum protection and to authenticate everything, embed an unclonable identity into the MCU as well as into the sensor

Results

- Secure sensor data from the moment of creation
- An unclonable, immutable and invisible unique identity to authenticate every sensor
- Low-cost solution for a scalable market
- Low resource requirements from sensor
- Flexible integration in hardware or software
- Security functionality gives IoT sensors a competitive advantage in a commoditizing market



Security should start at the sensor, where the data is created. When data is encrypted on the sensor, there is no way an adversary can eavesdrop.

In almost all IoT device networks, sensors are the genesis of the journey for IoT data streams. These sensors are creating the data on which business decisions are based and action is taken. In Industrial IoT, smart buildings and critical infrastructures, imagine what happens if attackers manipulate sensor data, like from power grids or water supplies. This can cripple entire regions. Not to mention all our vehicles that are increasingly full of sensors as we are autonomizing them. So it is highly important that sensor data is accurately transported from source to where decisions are made.

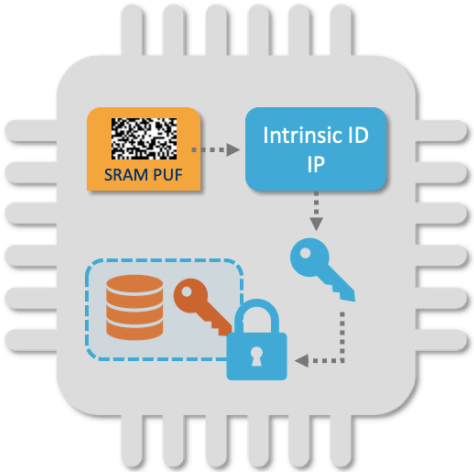
Keeping sensor data safe is not a trivial task, since IoT devices are in the field and are rarely well protected. This means that an adversary can easily get physical or logical access to the device and make changes that insert malicious data streams into the system.

IoT devices can be attacked in several places, such as snooping the interface between chips or eavesdropping on data when it leaves the device. This is why security should start at the sensor, where data is created. When data is encrypted on the sensor, there is no way an adversary can eavesdrop. Also, strong authentication of the sensor is required to make sure that only genuine sensors can inject data into the network.

But, like anything with a high-volume IoT deployment, sensors are under extreme price pressure. How is it possible to implement strong and differentiating security solutions while maintaining a competitive price point?

Solution: Secure Sensors

This is where Intrinsic ID's secure sensor solution comes in. Based on Intrinsic ID's patented SRAM PUF technology*, it internally generates a fingerprint, forming a unique and unclonable identity for every sensor, which is never stored in memory and cannot be copied from one device to the next. This way the identity is immutable, and invisible to adversaries, allowing it to authenticate genuine sensors. Keys derived from the SRAM PUF are used for encrypting sensor data.



Intrinsic ID provides hardware and software IP for direct and flexible integration into the sensor and meets the compact size, low power and wide operational ranges required in this application. This IP comes at a cost amenable to profitable scaling of the IoT. No additional hardware components (like secure element chips) are required in the IoT device to secure the sensor data. This means the sensor takes care of the security of its data by itself, which is a differentiating function for the sensors in an increasingly commoditizing market. Hence, with a small investment in functionality, the value of the sensor increases significantly.

Bottom Line Benefits

- Unclonable, immutable and invisible ID
- Authentication and encryption of data
- Competitive edge at a friendly TCO
- Flexible integration in HW or SW

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

© 2019 Intrinsic ID, Inc. Intrinsic ID is a trademark of Intrinsic ID, B.V. All names herein are trademarks.