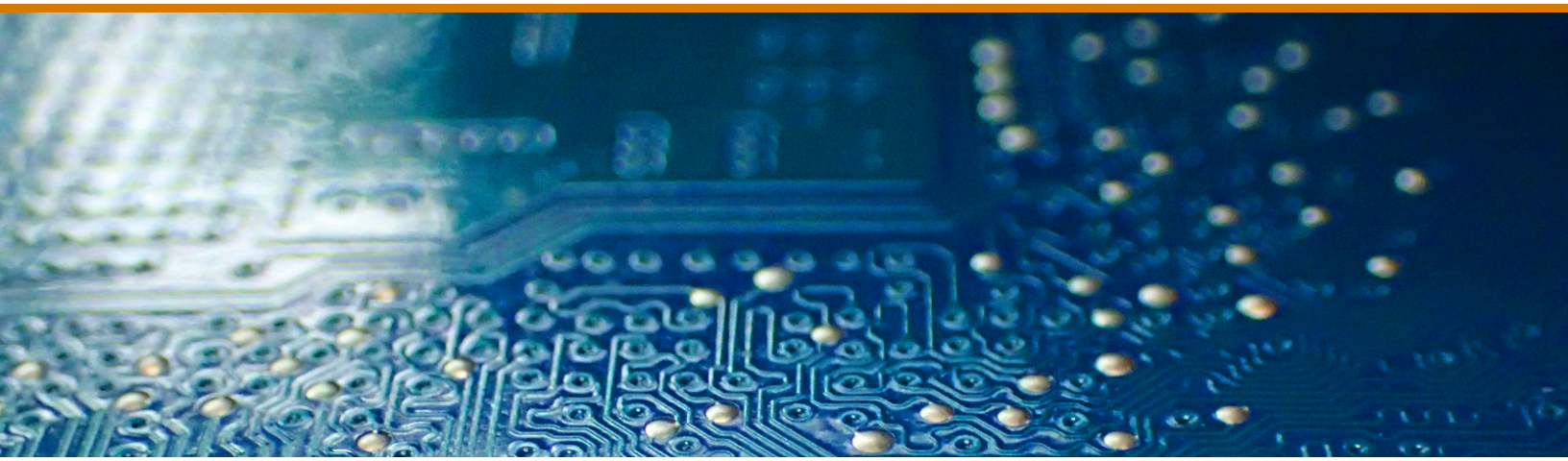


Building Trust in IoT from the MCU

MCUs need to ensure security for IoT data at rest and in motion, and protect the IP that operates the device.

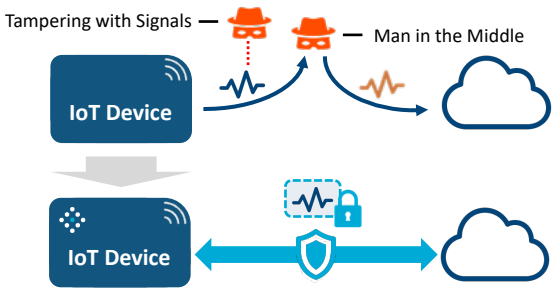
Billions of devices are being connected to the Internet of Things (IoT), while the number of attacks on these devices is increasing rapidly. In 2017 Altman Vilandrie & Company showed that half the U.S. firms in the IoT market were attacked, and the liability was often more than $20 million. If data is considered the currency of the IoT, that currency has value only if the data comes from a trustworthy source and is untampered. As such, data integrity has a direct impact on business and infrastructure. Since microcontrollers (MCUs) are central to the intelligence of the IoT device, one needs to look at their security, in order to reduce the number of attacks. MCUs need to ensure security for IoT data at rest and in motion, and protect the IP that operates the device. But how can an MCU vendor create a scalable security solution in a market under extreme price pressure? With a fit-for-purpose security solution, MCU vendors can differentiate in a competitive market.

Problem

- Since valuable data is being generated in the billions of deployed edge devices, IoT security needs to start from the edge
- For creating trustworthy data and security for IoT devices, a strong identity is required
- Traditional ways of creating and storing keys that form a device identity are too costly, not reliable, and not flexible enough for high volumes of IoT

Solution

- Start security where the data is created, by creating a unique and unclonable identity for every device
- Use an SRAM PUF to create an unclonable identity that authenticates the source, ensures data integrity, and protects valuable IP



Results

- An unclonable, immutable, invisible and unique identity to authenticate every device
- Secure, authenticated data from the moment it is created, delivering end-to-end protection
- Best-in-class combination of high security, low costs, and high flexibility for IoT security
- Read/Modify protection for secret root key
- Protection for hardware and software from misuse and counterfeiting

An SRAM PUF key is never stored and cannot be copied. It is immutable and invisible to attackers, creating an unparalleled anchor of trust.

To protect the IoT from its enormous attack threat, strong security functions are needed on every device. Functions such as authentication, secure boot, IP protection, secure communication and software updates are needed to protect devices. But IoT devices have strong constraints. The chips inside these IoT devices need to be small in size, operate at high speed with low power consumption, and be cost effective. How can strong security be deployed under these constraints?

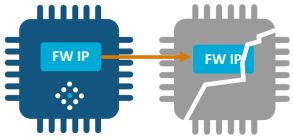
Strong Authentication

Authentication and security start with an unclonable device identity. All security functions require cryptographic keys that are derived from this identity, making the identity the root of all security. The keys are used for authenticating the device and its data and to encrypt data at rest and in transit.

From an operational point of view it is important to consider how the device identity and its keys are securely instantiated and become accessible on the MCU. An elegant way is to use Intrinsic ID's SRAM PUF* technology. SRAM PUFs create an unclonable, device-unique key from the physical characteristics of the silicon. This key is never stored and cannot be copied. It is immutable and invisible to attackers, creating a robust anchor of trust.

SRAM PUF keys are the basis for IoT security:

- Device Authentication: PKI-based handshake for secure communication
- Data Confidentiality: Encrypt sensitive data and keys, preventing data extraction from the device and reverse engineering of valuable IP
- Data Integrity: Protect against tampering and theft with signing of device-specific firmware

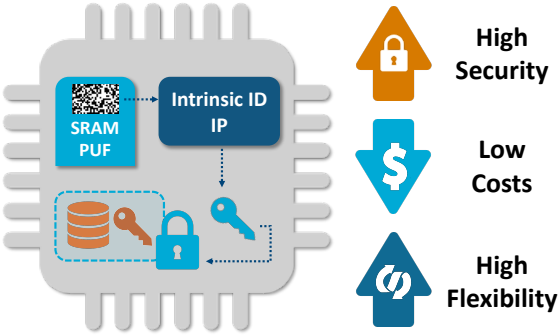


SRAM PUF Availability

Intrinsic ID's SRAM PUF products are available as RTL netlist for integration into the HW of a chip or as C-code for integration into a chip's firmware. The solution has a small footprint and, most importantly, a cost amenable to profitable scaling of the IoT. Algorithms for both symmetric and public key cryptography are included, and compliant with NIST specifications. SRAM PUFs scale over all popular fabs and process nodes, and SRAM is universally available in all MCUs.

SRAM PUFs offer the best-in-class combination of high security, low cost and high flexibility:

- Security is high, as keys never leave the MCU security perimeter and are never stored
- Cost is low, because no additional hardware or key programming is required
- Flexibility is high, because keys can be created at any stage of the supply chain, while inventory management is much simpler because devices are not pre-provisioned



Bottom Line Benefits

- Unclonable, immutable and invisible identity
- Device authentication and data integrity
- Best-in-class combination of high security, low costs, and high flexibility for IoT security
- Secure storage for all keys and data
- Protection for hardware and software from overproduction and counterfeiting

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