軟硬體結合的安全解決方案
為物聯網設計提供絕佳防護

林仕文 (Steven Lin) 2022 May
IoT Attack Vectors are shifting from Remote to Local

Remote Attacks (through the Internet)
- Historically hackers attacked only from the cloud and focused on solely on data servers.

Local Attacks (Hands-On Access)
- ‘Pivot Attacks’ are a growing attack vector against IoT.
- End nodes are attacked locally and then used to attack higher level servers for their more valuable data.

Logical Faults
- Buffer Overflows
- Code Insertion

Physical Attacks
- Cache Timing
- Rowhammer

Logical Attacks (on the Software)

Physical Attacks (on the Hardware)

Remote Interfaces (JTAG, Serial, USB,...)

Differential Power Analysis (DPA)
- Glitching (Voltage, Temp, Magnetics)
- Probing
OT is an easier target than IT

- There are no standard defense tools for OT
- End devices are easy targets
  - Security is not designed in from the start
  - Security is rarely a demanded feature
  - Saving pennies is #1 priority
  - Security is not usually ‘the default’
- 2000% increase in targeted OT attacks (2018 -> 2019)
- Healthcare, Manufacturing, Retail and Energy are primary targets
- Supply chains are not managed well enough
  - ~10-12% of electronic components are fake or substituted
IoT Security Legislation is Happening

- **California Consumer Privacy Act (§ SB-327)**
  - Introduced: Feb 13, 2017
  - Approved: Sept 28, 2018
  - Effective: Jan 1, 2020 (≤3yrs)

  - Requires ‘reasonable security features’
    - appropriate to the nature and function of the device
    - appropriate to the information it may collect, contain, or transmit
    - designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure
    - Pre-programmed passwords are unique in each device manufactured

- Multiple states have already introduced bills that resemble California’s CCPA example
  - **Virginia** (HB 2793)
  - **Oregon** (HB 2395)
  - **Hawaii** (SB 418)
  - **Maryland** (SB 0613)
  - **Massachusetts** (SD 341)
  - **New Mexico** (SB 176)
  - **New York** (S00224)
  - **Rhode Island** (SB 234)
  - **Washington** (SB 5376)

Already accounts for ~30% US population
Governmental Regulatory Landscape – United States

- California: SB-327
- Oregon: HB 2395
- Virginia: HB 2793

**Congress** → **Department of Commerce** → **Vulnerability Disclosure** → **Firmware Updates** → **Software Transparency** → **Cyber Shield Act** → **IoT Improvement Act** → **NISTIR 8259A**

### IoT Device Cybersecurity Capability Core Baseline

<table>
<thead>
<tr>
<th>Concern</th>
<th>Federal Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Identification</td>
<td>The IoT device can be uniquely identified logically and physically.</td>
</tr>
<tr>
<td>Device Configuration</td>
<td>The IoT device’s software and firmware configuration can be changed, and such changes can be performed by authorized entities only.</td>
</tr>
<tr>
<td>Data Protection</td>
<td>The IoT device can protect the data it stores and transmits from unauthorized access and modification.</td>
</tr>
<tr>
<td>Logical Access to Interfaces</td>
<td>The IoT device can limit logical access to its local and network interfaces to authorized entities only.</td>
</tr>
<tr>
<td>Software and Firmware Update</td>
<td>The IoT device’s software and firmware can be updated by authorized entities only using a secure and configurable mechanism.</td>
</tr>
<tr>
<td>Cybersecurity Event Logging</td>
<td>The IoT device can log cybersecurity events and make the logs accessible to authorized entities only.</td>
</tr>
</tbody>
</table>

**Legend**
- **Published**
- **Pending**
Governmental Regulatory Landscape – Europe (& extended adoptees)

- No universal default passwords
- Implement a means to manage reports of vulnerabilities
- Keep software updated
- Securely store credentials and security-sensitive data
- Communicate securely
- Minimize exposed attack surfaces
- Ensure software integrity
- Ensure that personal data is protected
- Make systems resilient to outages
- Examine system telemetry data
- Make it easy for consumers to delete personal data
- Make installation and maintenance of devices easy
- Validate input data
The Four Pillars of IoT Security

Confidentiality
Ensures the data is only readable by the proposed destination

Authenticity
Ensures the supposed sender is the real sender

Integrity
Ensures the information contained in the original message is kept intact

Non-repudiation
Ensures that signatures of data cannot be denied

Cryptography
Secure Vault

Threats evolve. So should your device security.

Introducing Secure Vault™.

silabs.com/security
## Secure Vault™

<table>
<thead>
<tr>
<th>Base</th>
<th>Mid</th>
<th>High</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>True Random Number Generator</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Crypto Engine</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>Secure Application Boot</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>Secure Engine</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>Secure Boot with RTSL</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>Secure Debug with Lock/Unlock</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>DPA Countermeasures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
<td>Anti-Tamper</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
<td>Secure Attestation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
<td>Secure Key Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>✓</td>
<td>Advanced Crypto</td>
</tr>
</tbody>
</table>

Designing Secure IoT Devices
A pseudo-random number generator uses a set of algorithms to produce numbers.

A true random number generator uses an unpredictable physical source to produce numbers.

### Vulnerabilities
- If any bias in generating a number can be determined, hackers leverage that to reduce the time and effort they need to acquire secret keys.

### True Random Numbers
- True Random Number Generator that meets NIST SP 800-90A/B/C and AIS-31
# Cryptography Engine

## Protocol Usage & Support

### Series 1

<table>
<thead>
<tr>
<th>Series</th>
<th>Wireless</th>
<th>TCP/IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triple-DES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHACHA20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC Curve25519</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLY1305</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC Curve25519</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLY1305</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Function</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Series 2

<table>
<thead>
<tr>
<th>Series</th>
<th>Wireless</th>
<th>TCP/IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cipher</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symmetric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Triple-DES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>AES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CHACHA20</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC Curve25519</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLY1305</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asymmetric</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC NIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>&lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ECC Curve25519</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=256</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SHA-2 &lt;=512</td>
<td></td>
<td></td>
</tr>
<tr>
<td>POLY1305</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hash Function</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Secure Engine Subsystem

All cryptographic functions use a dedicated crypto-coprocessor
- Random number generation
- Symmetric encryption/decryption
- Hashing
- Keypair generation
- Key storage
- Signing / Verifying signatures

Limited accessibility to crypto-coprocessor
- Via a Host mailbox interface
- Debug pins (with Debug Challenge Interface, or DCI)

Crypto-coprocessor is not customer programmable
- (but can be securely updated)

Crypto-coprocessor benefits
- Increases security: access to crypto functions is tightly controlled, supports key isolation, supports Secure Boot
- Frees the Host Processor for other tasks
Secure Boot

- **Vulnerabilities**
  - Replacing code with ‘look-alike code’ makes a product appear normal. Hackers use it to copy/re-direct data to alternate servers.

- **Secure Boot with RTSL (Root-of-Trust & Secure Loader)**
  - Use and execute only trusted application code against immutable memory and through a full chain of trust.
Anti-Rollback Prevention

**LOCAL & REMOTE ATTACK VECTOR**

Failure

- Attempt to load v2
- Device Software Version 3
- Update is not applied
- Device Software Version 3 (remains unchanged)

Success

- Attempt to load v3
- Device Software Version 2
- Update is applied
- Device Software Version 3 (is updated)

- **Vulnerabilities**
  - Adversaries may have knowledge of a security flaw present in older firmware

- **Anti-Rollback Prevention**
  - Prevents older digitally signed firmware from being re-loaded into a device to re-expose patched flaws
Secure Debug

- **Vulnerabilities**
  - Unlocked ports are a significant security vulnerability
  - Unlocking debug ports typically wipes the memory to protect IP but this limits device failure analysis capabilities

- **Secure Debug**
  - Lock the emulation port and use optional cryptographic tokens to unlock it allowing memory to remain intact
A Differential Power Analysis (DPA) attack requires hands-on access to the device.

Monitoring electromagnetic radiation and fluctuations in power consumption during crypto operations may reveal security keys and other data.

### Vulnerabilities
- Observing subtle signal differences during given internal operations can provide insight into cryptographic functions

### DPA Countermeasures
- Countermeasures add masks and random timings to internal operations and distorts DPA snooping
Anti-Tamper

- **Vulnerabilities**
  - Tamper attacks come from single or multiple vectors.
  - Common attacks include voltage glitching, magnetic interference and forced temperature adjustment.

- **Tamper detection and rapid response**
  - Anti-tamper requires both an attack detection and suitable rapid response which may include key deletion.
Secure Key Management

- **Vulnerabilities**
  - When an attacker learns how to extract keys or content from a device, they use the same attack vector to attack other devices

- **Secure Key Management**
  - A Physically Unclonable Function creates a secret, random, & unique key, from individual device imperfections
  - The PUF-key encrypts all keys in the secure key storage. It is generated at startup and is not stored in flash
Secure Attestation

- **Vulnerabilities**
  - Many systems use a UID to identify devices, but the UID is public (can be copied)
  - Developers are concerned with the authenticity of their devices
  - Most successful companies suffer counterfeit products and “ghost shifts”

- **Secure Attestation**
  - Secure Vault devices generate a unique device ECC keypair on-chip and securely stores the secret private key
  - The device secret private key never leaves the chip
  - During production
    - Test program reads the device public key
    - Placed in certificate & signed with an HSM secret key
    - Re-stored back in chip’s OTP memory
  - External service can request the certificate chain from the device and CA web server which retrieves the unique device public key.
  - External service can perform a “Challenge Response” to the chip at any time during the life of the product to Authenticate the chip is genuine

Request Device Certificate

Device Certificate containing Device Public Key

Challenge: Sign this random number ‘1872783878’

Response signed with Device Secret Key

External service can request the certificate chain from the device and CA web server which retrieves the unique device public key.

Secure Attestation

Secure Vault devices generate a unique device ECC keypair on-chip and securely stores the secret private key

The device secret private key never leaves the chip

During production

- Test program reads the device public key
- Placed in certificate & signed with an HSM secret key
- Re-stored back in chip’s OTP memory

External service can perform a “Challenge Response” to the chip at any time during the life of the product to Authenticate the chip is genuine
Secure Vault™ – Formally recognized by industry leaders

Threats evolve. So should your device security. Introducing Secure Vault.

- IoXT SmartCert
  - Independent security alliance
  - Focused on Consumer products and Services

- ARM PSA Level 2 & 3
  - First SoC to achieve Level 3 certification
  - Assures a proven hardware root of trust

- Independent Security Evaluation by Riscure
  - Comprehensive analysis report from Riscure can be shared with customers under NDA
Introducing EFR32BG24 and EFR32MG24

- 2.4GHz wireless SoC with Matter, Zigbee, OpenThread, Bluetooth and Multiprotocol
- AI/ML hardware accelerator to allow 2x to 4x faster inferencing at the edge
- Secure Vault™ protects data and device; PSA Certification Level 3
- 20-bit ADC for advanced sensing
- High performance RF for robust and reliable communication
- 1.5 MB Flash and 256 kB RAM for Matter and other future requirements
- Low active current for longer battery life

Industry’s Only Wireless SoC with Matter, AI/ML, Higher Memory and Higher Security for IoT Edge Devices
Thank you!