<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thursday, March 25th</td>
<td>Unboxing the BGM220 Explorer Kit</td>
</tr>
<tr>
<td>Wednesday, April 28th</td>
<td>Uncover Sub-GHz and Proprietary Solution within Simplicity Studio v5</td>
</tr>
<tr>
<td>Thursday, August 19th</td>
<td>Discover the Security Features of Secure Vault</td>
</tr>
</tbody>
</table>

Recording and slides will be posted to: [www.silabs.com/training](http://www.silabs.com/training)
이경보 (Victor Lee)
Sr. FAE, Korea
WELCOME

Discover the Security Features of Secure Vault

Victor Lee
Agenda

- Secure Vault Overview
- Anti-Tamper
- Secure Identity
- Secure Identity Demo
- Support Documentation
IoT Attack Vectors are shifting from Remote to Local

Historically hackers attacked only from the cloud and focused on solely on data servers.

‘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.
Secure Vault

Threats evolve. So should your device security.

Introducing Secure Vault.

silabs.com/security
Secure Vault – first silicon to achieve PSA Level 3 Certification

https://www.psacertified.org/products/secure-vault/

- EETimes
- Arm Beyond The Now Podcast
- Silabs Press Release
PSA Level 2&3 Requirements for Boundary Separation

Isolation level 2

Level 2 introduces an isolation boundary between the PSA Root of Trust and the Application Root of Trust. The protection domains and the required protection for isolation level 2 are as follows:

<table>
<thead>
<tr>
<th>Protection domain</th>
<th>Needs protection from</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSPE</td>
<td>-</td>
</tr>
<tr>
<td>Application Root of Trust</td>
<td>NSPE</td>
</tr>
</tbody>
</table>
| PSA Root of Trust       | NSPE  
|                         | Application Root of Trust            |

![Diagram showing isolation boundary between PSA Root of Trust and Application Root of Trust with protection domains and APIs marked.]
<table>
<thead>
<tr>
<th>Feature</th>
<th>Base</th>
<th>Mid</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Random Number Generator</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Crypto Engine</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Application Boot</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Engine</td>
<td>—</td>
<td>VSE/HSE</td>
<td>HSE</td>
</tr>
<tr>
<td>Secure Boot with RTSL</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Debug with Lock/Unlock</td>
<td>—</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>DPA Countermeasures</td>
<td>—</td>
<td>Optional</td>
<td>✓</td>
</tr>
<tr>
<td>Anti-Tamper</td>
<td>—</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Attestation</td>
<td>—</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Secure Key Management</td>
<td>—</td>
<td>—</td>
<td>✓</td>
</tr>
<tr>
<td>Advanced Crypto</td>
<td>—</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

[Diagram of Host Domain and Secure Sub-System with labeled boxes for Cortex-M, Flash, RAM, Security Controller, Crypto, TRNG, PUF, TAMPER, Challenge Interface, Secure Engine Mailbox, Secure Engine Bus, System Bus]
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
## Protocol Usage & Support

### Series 1

**Cipher**
- Triple-DES
- AES
- CHACHA20
- RSA
- ECC NIST <=256
- ECC NIST <=521
- ECC Curve25519
- SHA-1
- SHA-2 <=256
- SHA-2 <=512
- POLY1305

**Symmetric Encryption**

**Asymmetric Encryption**
- RSA
- ECC NIST <=256
- ECC NIST <=521
- ECC Curve25519

**Hash Function**
- SHA-1
- SHA-2 <=256
- SHA-2 <=512
- POLY1305

**Wireless**
- ZigbeePRO
- Zigbee IP
- Thread
- Z-Wave
- Bluetooth
- Homekit
- WMBus

**TCP/IP**
- SSL 3.0
- TLS 1.2
- TLS 1.3

### Series 2

**Cipher**
- Triple-DES
- AES
- CHACHA20
- RSA
- ECC NIST <=256
- ECC NIST <=521
- ECC Curve25519
- SHA-1
- SHA-2 <=256
- SHA-2 <=512
- POLY1305

**Symmetric Encryption**

**Asymmetric Encryption**
- RSA
- ECC NIST <=256
- ECC NIST <=521
- ECC Curve25519

**Hash Function**
- SHA-1
- SHA-2 <=256
- SHA-2 <=512
- POLY1305

**Wireless**
- ZigbeePRO
- Zigbee IP
- Thread
- Z-Wave
- Bluetooth
- Homekit
- WMBus

**TCP/IP**
- SSL 3.0
- TLS 1.2
- TLS 1.3

### Protocol Usage & Support Legend

- **Software Only**: OK
- **Hardware + CPU**: Better
- **Hardware Only**: Best

---

**Cryptography Engine**
Anti-Rollback Prevention

- **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

---

**LOCAL & REMOTE ATTACK VECTOR**

### Failure

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

### Success

- Attempt to load v3
- Device Software Version 2
- Update is applied
- Device software is updated
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
DPA Countermeasures

- **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

---

1. A Differential Power Analysis (DPA) attack requires hands-on access to the device.
2. Monitoring electromagnetic radiation and fluctuations in power consumption during crypto operations may reveal security keys and other data.
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
Vulnerabilities
- PCB’s can be easily probed potentially exposing keys, passwords and data

Secure Link
- Encrypts selected bus messages using a Diffie-Hellman key exchange
- Keys are uniquely created on a ‘per session/per device’ basis.
- No fleet-wide keys & new keys on each power-cycle
Anti-Tamper (1/2)

Why

- Many attacks force a device outside its standard operating range(s)
  - temperature, voltage, clock-inputs, magnetic noise
  - Debuggers running at a high rate, reboots at a high rate
  - Cost of these attacks is now low enough for both large scale and hobbyists

Silicon Labs

- Implemented an ability to detect when these attacks happen
  - Voltage, clock, temperature and magnetic tamper detectors in our devices
  - Secure boot, secure debug use counters to flag abnormal behavior
  - External triggers from broken enclosures via buttons and traces
- Implemented an ability to respond to these attacks
  - Programmable tamper response
    - Includes an ability to perform rapid deletion of Secure Key Storage (forced bricking)
Anti-Tamper (2/2)

Tamper Detection

- Filter Counter
- Mailbox Authentication
- DCI Authentication
- OTP Read
- TRNG Monitor
- Peripheral Reflex System
  - External Tamper Sources (8)
- Voltage Glitch
- SE Debug
- Digital Glitch
- Temperature Sensor

Programmable to Levels 0-7

User Tamper Response

Programmable Response

- Level 0: No action
- Level 1: Interrupt to Application
- Level 4: System Reset
- Level 7: Erase PUF Reconstruction Data (BRICK)

User Tamper Disable

Returns selected tamper sources to their default state upon authentication for FA purposes
What is a Secure Identity?

- A Secure Identity is like a “birth certificate” for a device or a product

- A Secure Identity allows you to –
  - Trust that a device is authentic, and
  - Trust that a device is the specific device it claims to be

- Common uses for a Secure Identity
  - Ensure the device is authentic (secure the supply chain)
  - Ensure that the product is authentic (anti-counterfeit)
  - Support remote authentication of a communication link
  - Support commissioning to a wireless network
  - Satisfy regulatory requirements
Authentication Using a Device Certificate

1. Request Device Certificate
2. Receive Device Certificate and verify its authenticity with the certificate chain
3. Send random challenge for the device to sign (using the device’s private key)
4. Verify the signed challenge using the device’s public key from the Device Certificate

Is the certificate authentic?
1. Request Device Certificate
2. Receive Device Certificate and verify its authenticity with the certificate chain

Is the certificate related to this device?
3. Send random challenge for the device to sign (using the device’s private key)
4. Verify the signed challenge using the device’s public key from the Device Certificate
Example Secure Vault Device Certificate

- The Device Certificate is unique to each device
- Device Certificate is stored in OTP
  - Cannot be modified once programmed
- Device Certificate is X.509 (DER-encoded binary)
  - Compatible with established internet protocols and appliances
- Common Name field contains the 64-bit EUI
  - Same as EUI64 in DEVINFO page
- Device-specific Public Key
  - Private key is generated by and securely stored in the HSE
- Validity period is 100 years from device manufacture date
- The Device Certificate can be accessed from the serial wire debug interface or from software
A certificate chain is a hierarchy
- Each certificate in the chain is signed by the certificate above it
- Each certificate in the chain has a pointer to the certificate above it

Silicon Labs is a Certificate Authority
- All private keys are Silicon Labs private keys that are held in our secure Public Key Infrastructure or are securely stored in the devices themselves
- [https://ca.silabs.com](https://ca.silabs.com)

All certificates are X.509, signed with NIST secp256r1 elliptic curve private keys
- Fully compatible with standard endpoint authentication methods used in internet communications
Standard Secure Vault Device Certificates

- **Standard Device Certificates**
  - Included with Secure Vault products
  - Can be added to non-Vault products with a customization charge
  - Cryptographically proves the device is an authentic Silicon Labs device (prevents counterfeit devices)
  - Does not protect against overproduction or counterfeit products that are built with authentic Silicon Labs devices
  - Signed to a Silicon Labs Certificate Authority
Customized Secure Vault Device Certificates

- Customized Device Certificates
  - Available via Custom Part Manufacturing Service (CPMS)
  - Protects against overproduction by CM
  - Protects against counterfeit products
  - Cryptographically proves the device is an authentic Silicon Labs device that was produced for the OEM
  - Device Certificate X.509 fields can be specified, with restrictions
  - Signed to Silicon Labs Certificate Authority
Secure Identity Demo
Welcome to Simplicity Studio

Everything you need to develop, research, and configure devices for IoT applications.

Get Started

Select a connected device or search for a product by name to see available documentation, example projects, and demos.

Connected Devices  All Products

Connected Devices

Recent Projects

Recent Projects 00265637_simple_trx_std_FEM_board

Open
Support Documentation

- AN1190: Series 2 Secure Debug
- AN1218: Series 2 Secure Boot with RTSL
- AN1247: Anti-Tamper Protection Configuration and Use
- AN1271: Secure Key Storage
- AN1268: Authenticating Silicon Labs Devices Using Device Certificates
- AN1222: Production Programming of Series 2 Devices
- UG162: Simplicity Commander Reference Guide
- UG266: Silicon Labs Gecko Bootloader User’s Guide
September 14–15, 2021 (CDT)

Smart Home
Smart City
Industrial IoT
General IoT

works with 2021
Virtual Conference

workswith.silabs.com
THANK YOU

Recording and slides will be posted to:
www.silabs.com/training