SILICON LABS

tech talks

# WELCOME

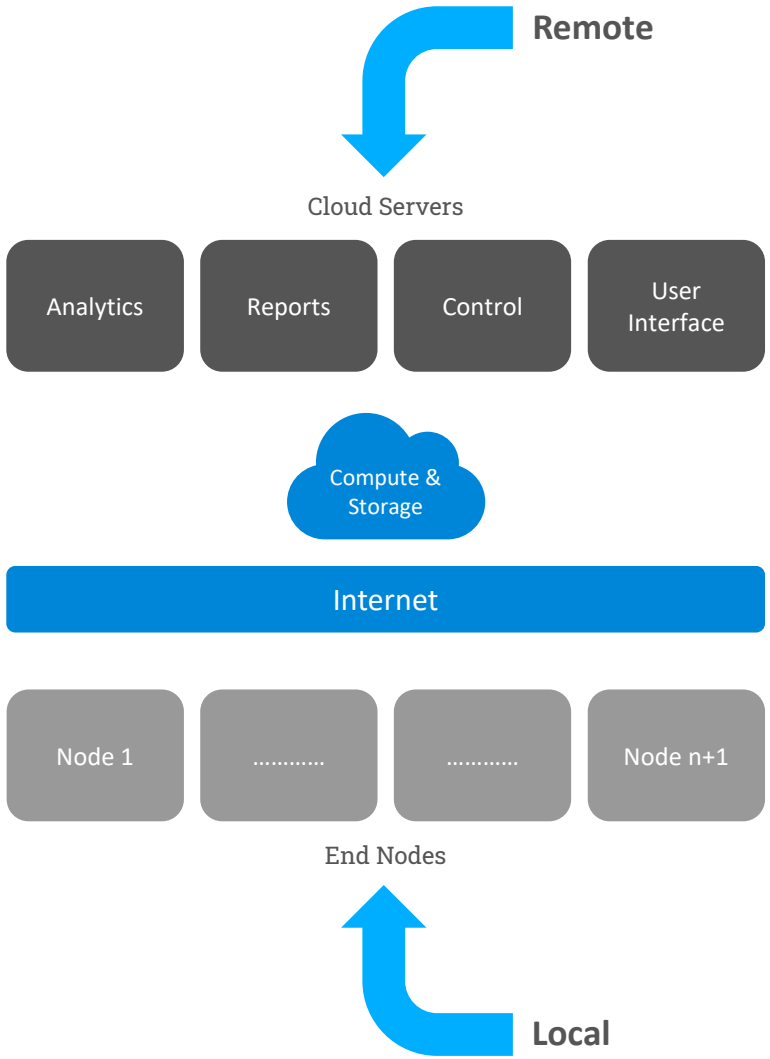
## Discover Security Features of Secure Vault

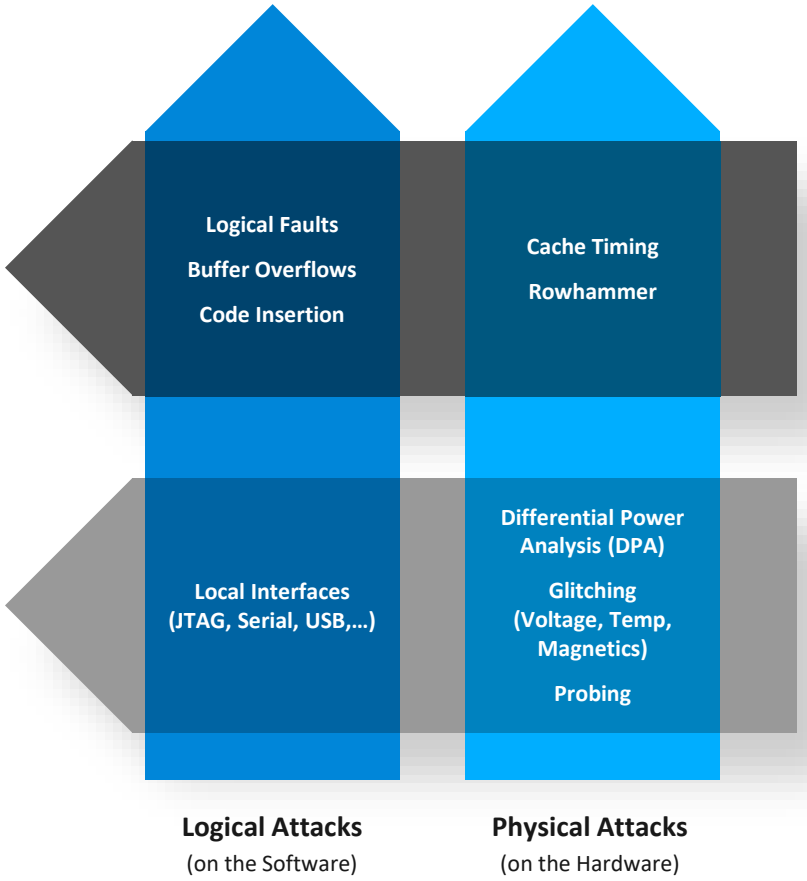
Jacob Johnson

# Agenda

- Secure Vault Overview
- Tamper Deep Dive
  - Tamper Response
  - Tamper Source
  - Tamper Configuration
  - Usage Example
- Secure Vault Tamper Demo
- Support Documentation

# 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.

# 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


psacertified™
level three

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

- EETimes
- Arm Beyond The Now Podcast
- Silabs Press Release

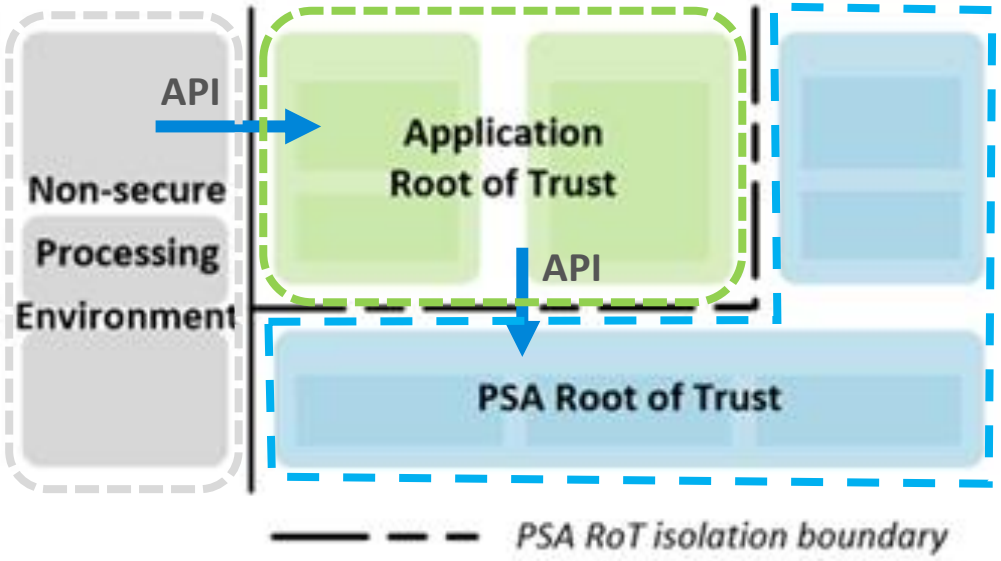
# PSA Level 2&3 Requirements for Boundary Separation

**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:

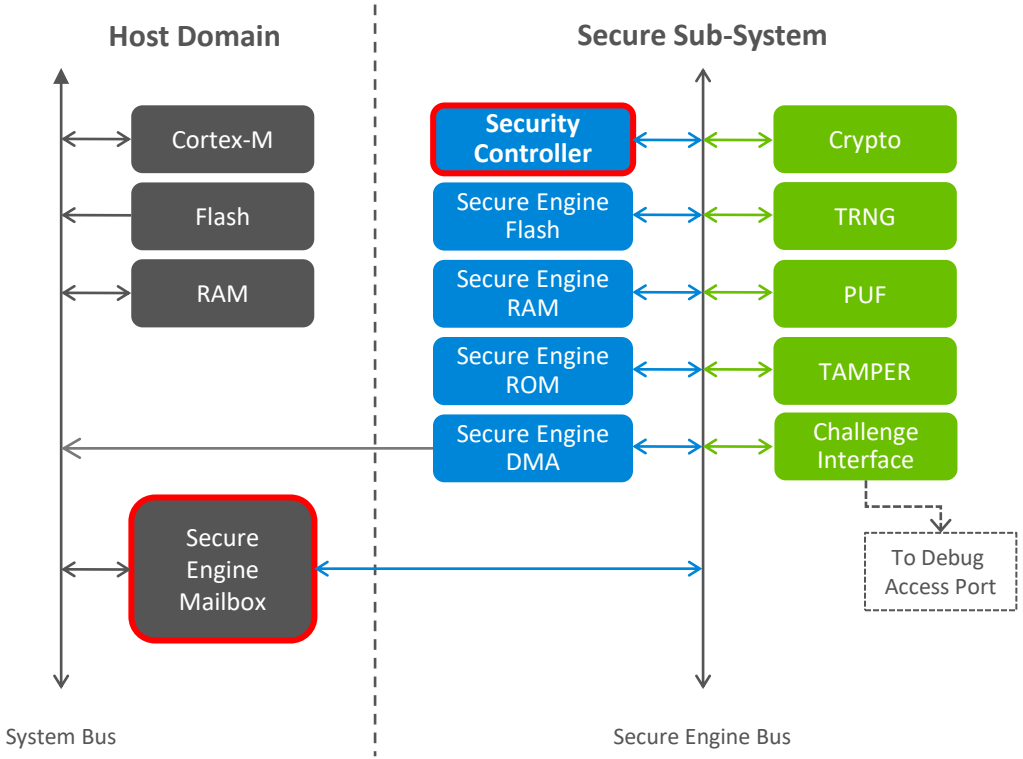
| Protection domain | Needs protection from |
|---|---|
| NSPE | - |
| Application Root of Trust | NSPE |
| PSA Root of Trust | NSPE<br>Application Root of Trust |



# SecureVault™

| Base | Mid | xG2xB High | Feature |
|---|---|---|---|
| ✓ | ✓ | ✓ | True Random Number Generator |
| ✓ | ✓ | ✓ | Crypto Engine |
| ✓ | ✓ | ✓ | Secure Application Boot |
| – | VSE/HSE | HSE | Secure Engine |
| – | ✓ | ✓ | Secure Boot with RTSL |
| – | ✓ | ✓ | Secure Debug with Lock/Unlock |
| – | Optional | ✓ | DPA Countermeasures |
| – | – | ✓ | Anti-Tamper |
| – | – | ✓ | Secure Attestation |
| – | – | ✓ | Secure Key Management |
| – | – | ✓ | Advanced Crypto |

# 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)

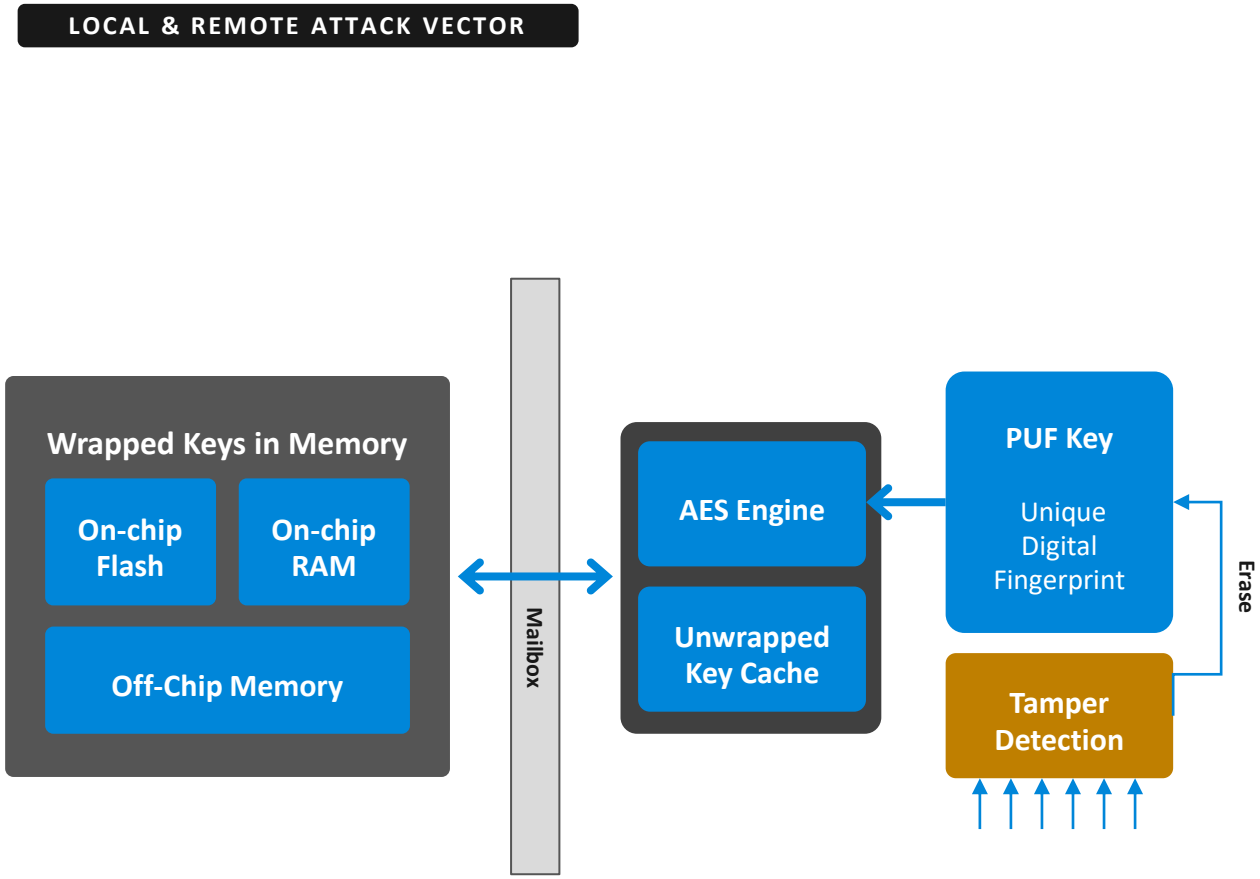
**Crypto-coprocessor is not customer programmable**

- (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

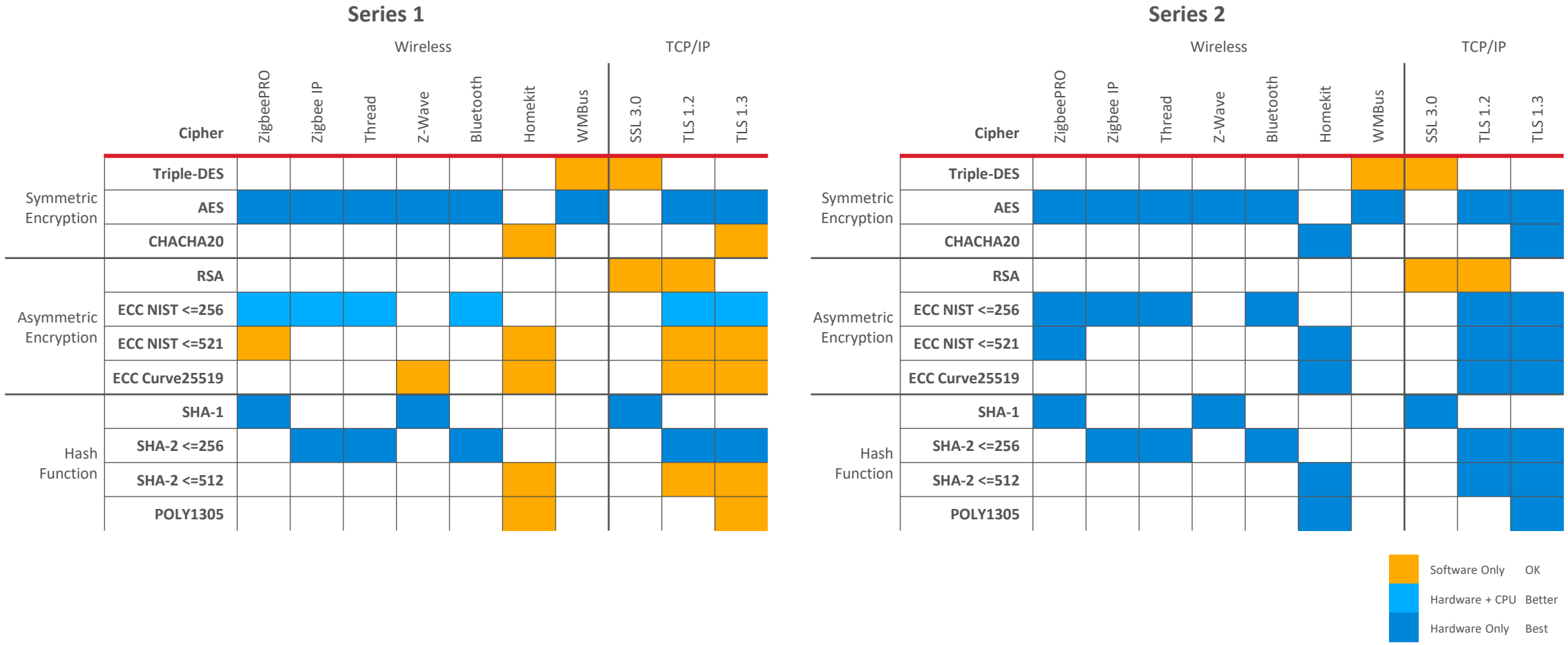
# Secure Key Management




- 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

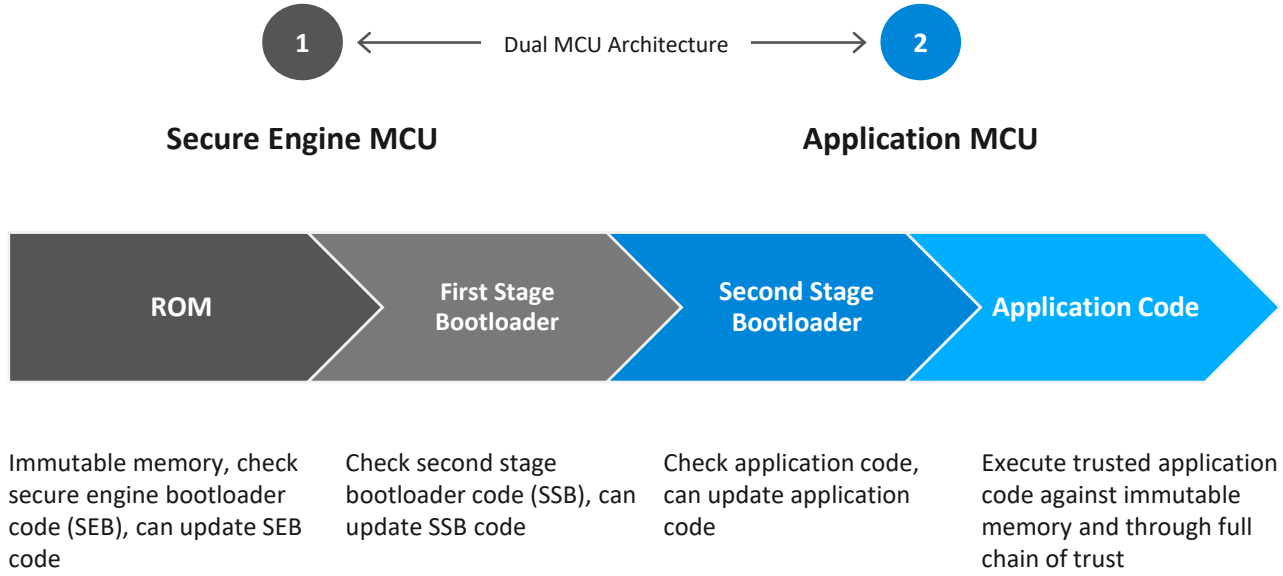
# Cryptography Engine

## Protocol Usage & Support



# Secure Boot

**LOCAL & REMOTE ATTACK VECTOR**

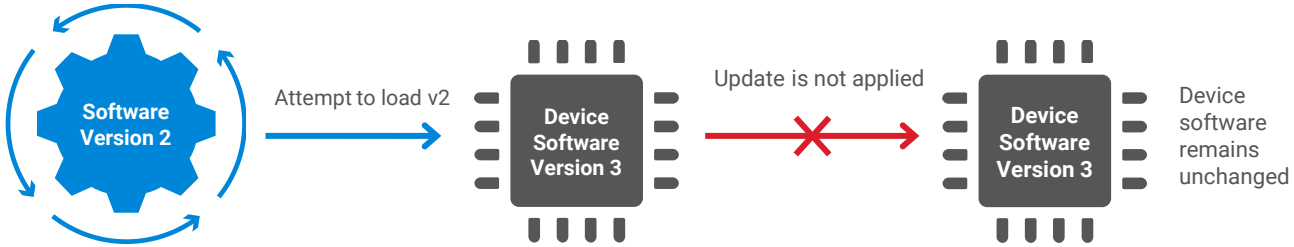



- Vulnerabilities
  - Replacing code with ‘look-alike code’ makes a product appear normal. Hackers use it to copy/re-direct data to alternate servers.
- Secure Boot with RTSL
  (Root-of-Trust & Secure Loader)
  - Use and execute only trusted application code against immutable memory and through a full chain of trust

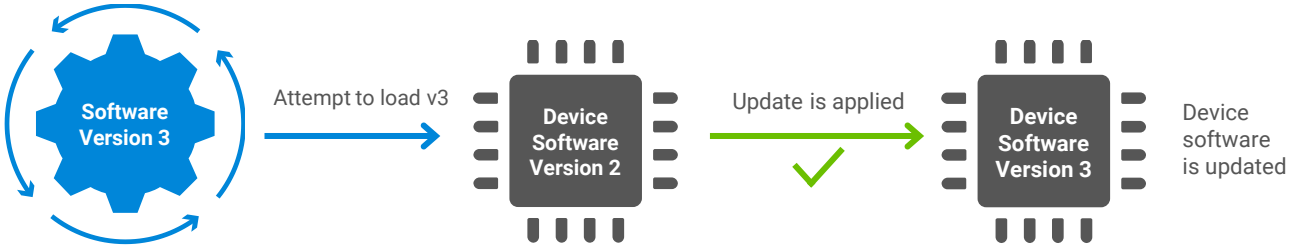
# Anti-Rollback Prevention

**LOCAL & REMOTE ATTACK VECTOR**

### Failure

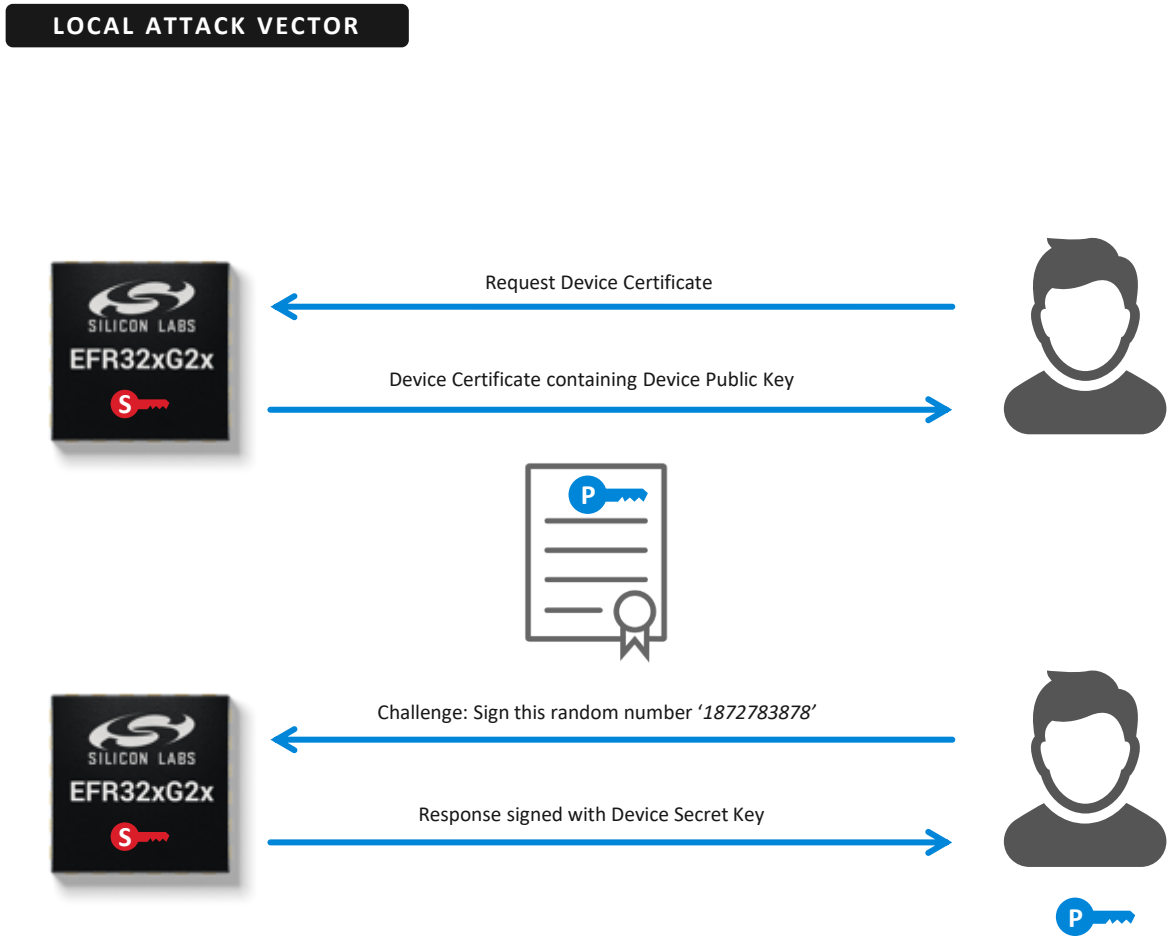



### Success




- 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 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

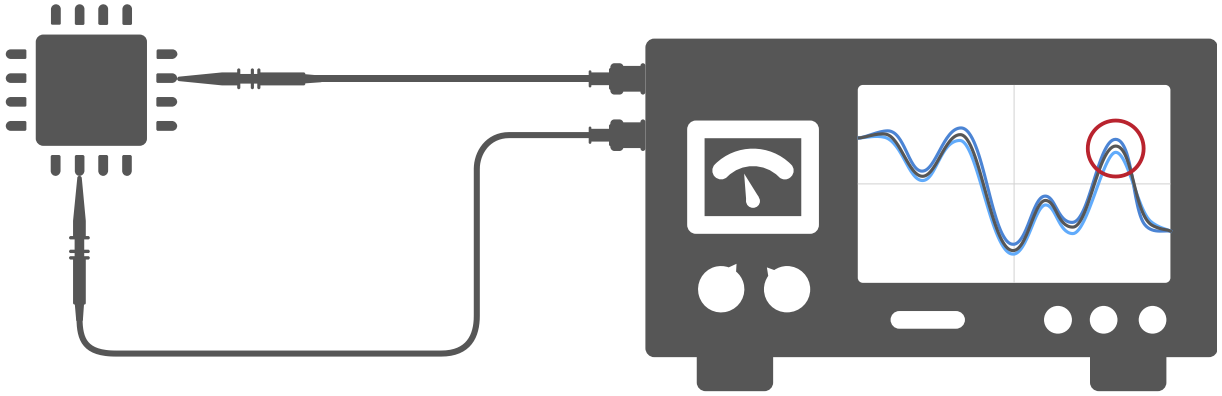
**LOCAL ATTACK VECTOR**

1

A Differential Power Analysis (DPA) attack requires hands-on access to the device.

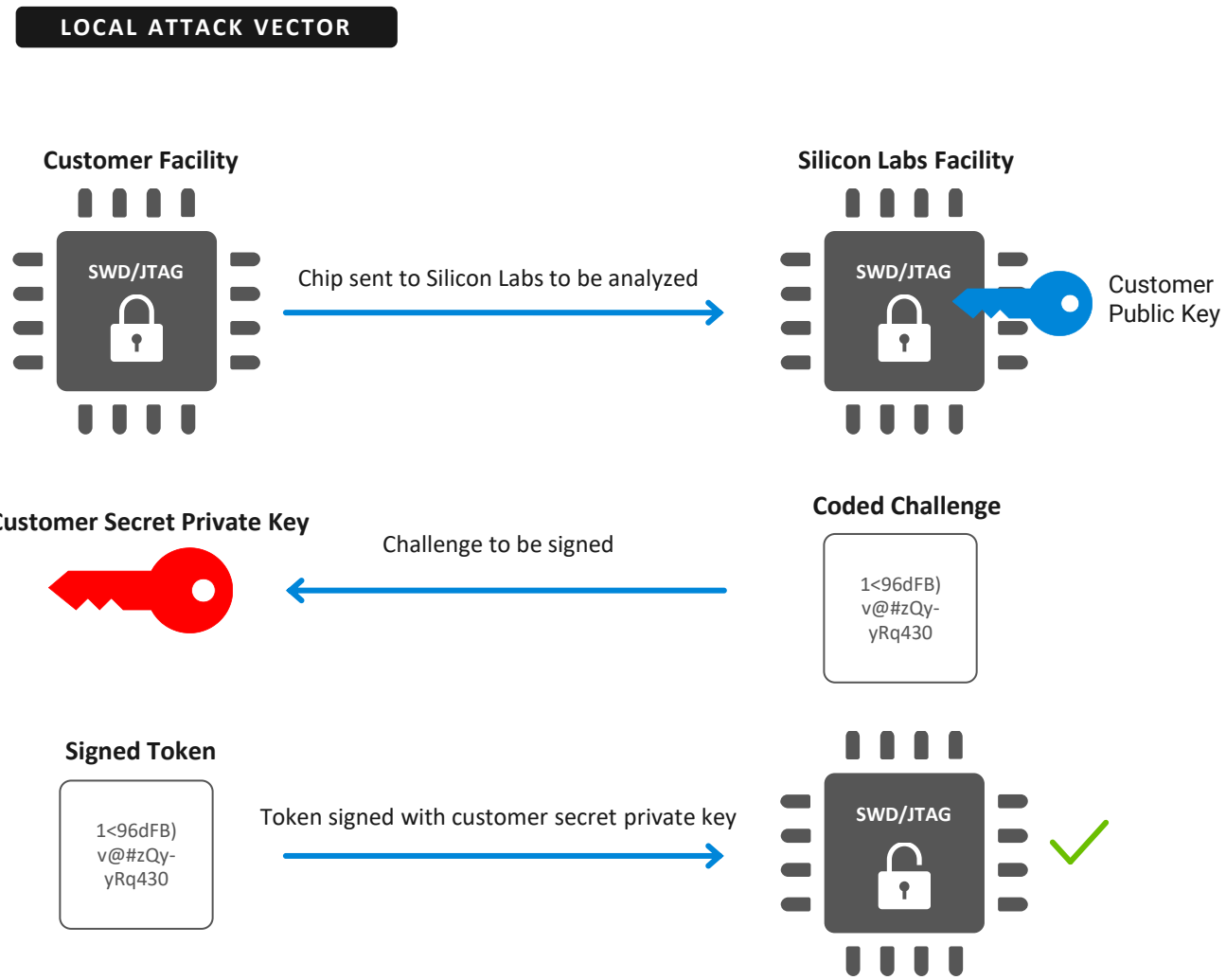
2

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



- Vulnerabilities
  - 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

# Secure Debug

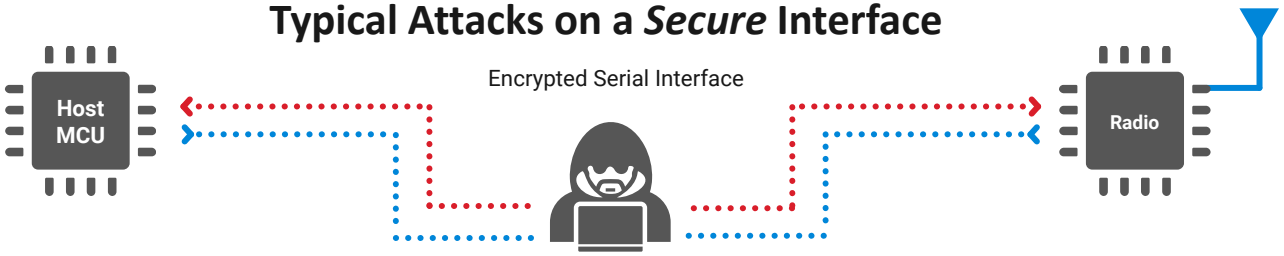



- Vulnerabilities
  - Unlocked ports are a significant security vulnerability
  - Unlocking debug ports typically wipes the memory to protect IP but this limits device failure analysis capabilities
- Secure Debug
  - Lock the emulation port and use optional cryptographic tokens to unlock it allowing memory to remain intact

# Secure Link

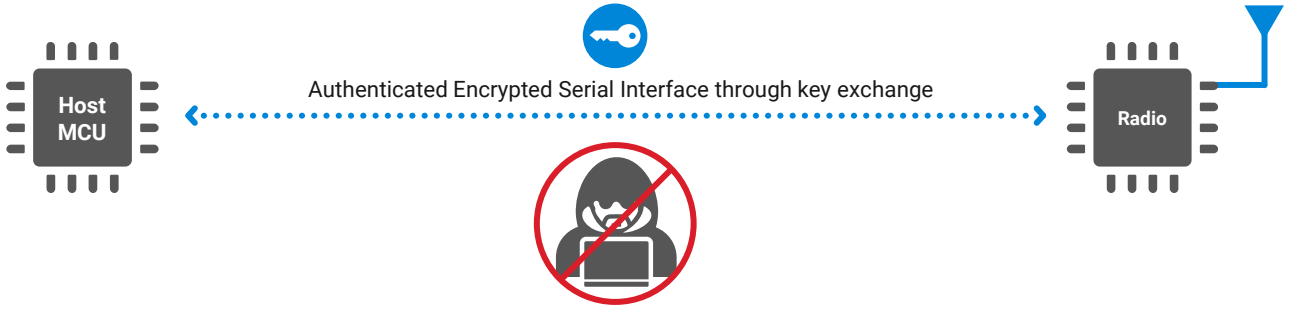
LOCAL ATTACK VECTOR

## Typical Attacks on a *Secure* Interface




A hacker can execute a man-in-the-middle attack. The Host MCU thinks the hacker is the radio, and vice versa.

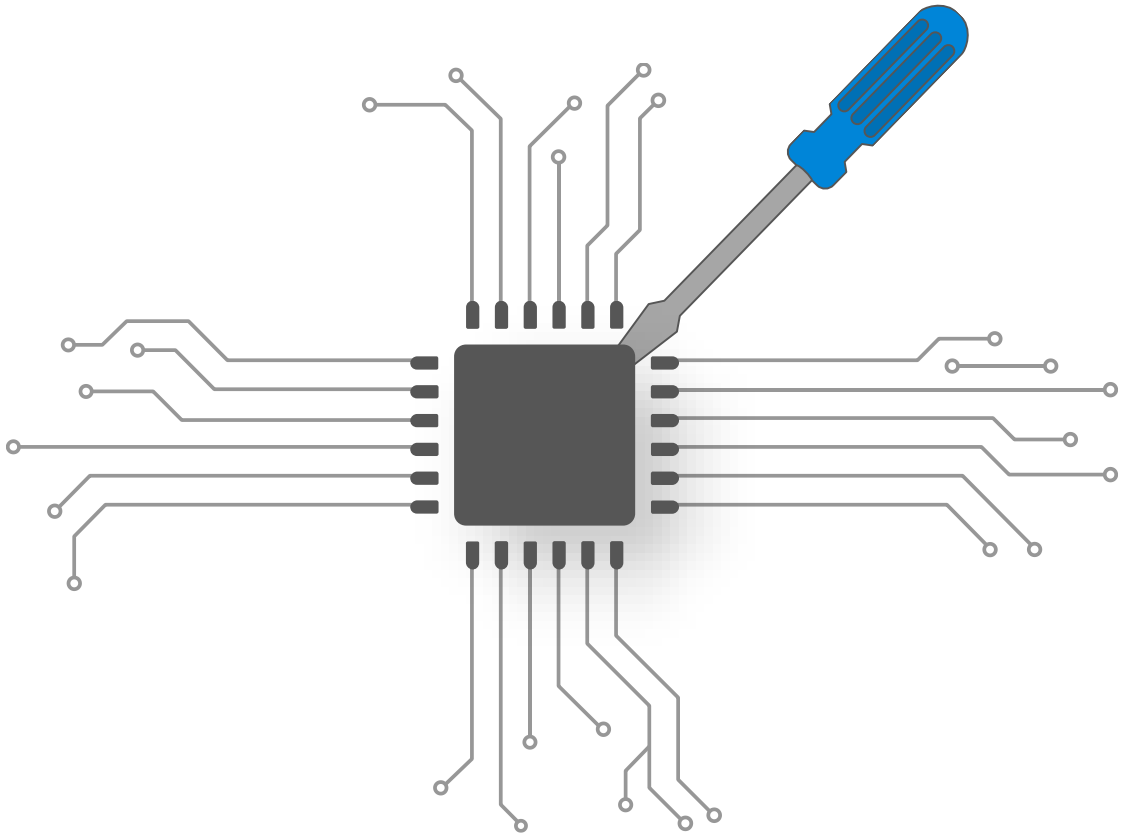
## Protecting a *Secure* interface with Secure Link




Secret key exchange between the host MCU and radio authenticates each party to the other. Man-in-the-middle attacks and spoofing are prevented.

- 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)



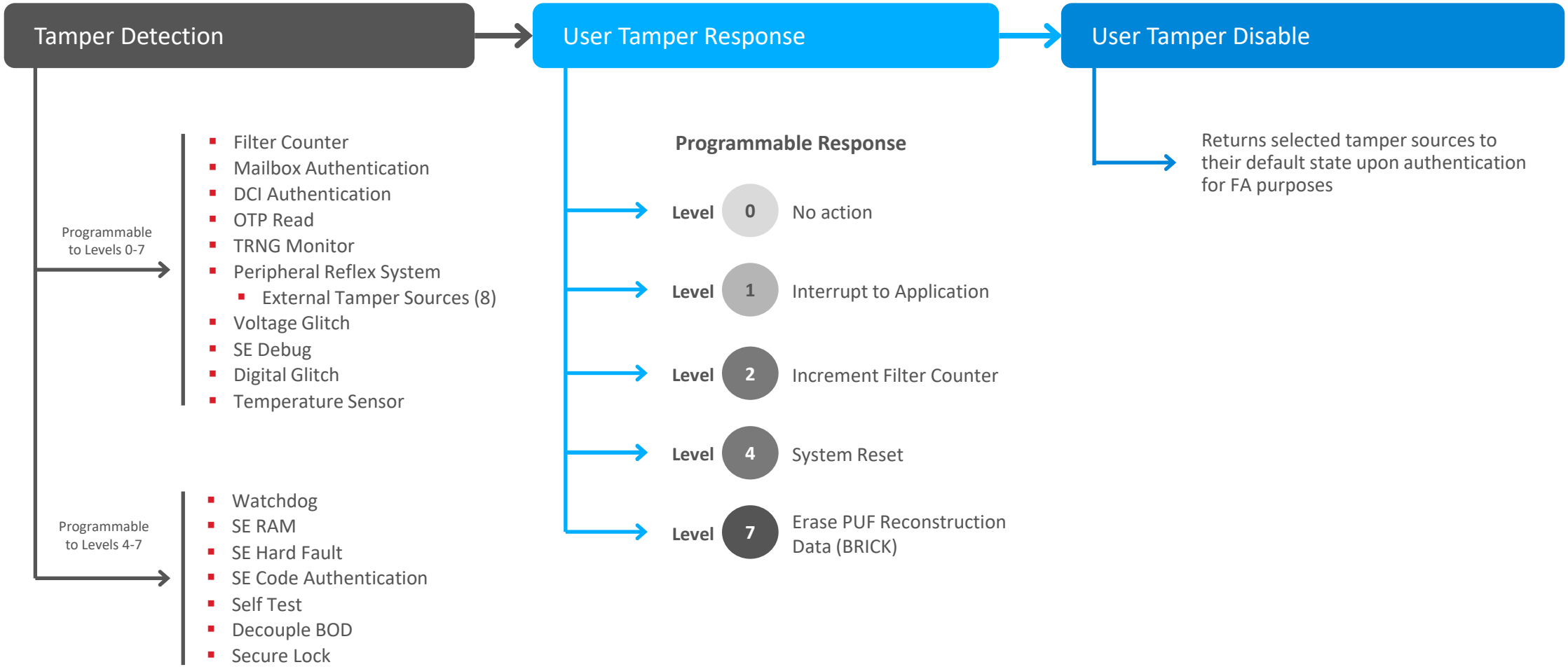
## Why

- 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)



# Secure Vault Tamper Response

| Level | Response | Description |
|---|---|---|
| 0 | Ignore | No action is taken |
| 1 | Interrupt | • The SETAMPERHOST interrupt on the Cortex-M33 is triggered<br>• Read the SE status to check which tamper sources that have been triggered |
| 2 | Filter | • A counter in the tamper filter is increased<br>• The Filter counter tamper source is triggered if counter reaches a configurable threshold (2 to 256) within a configurable reset period (32ms to ~795.4 days) |
| 4 | Reset | • The SE and Cortex-M33 are reset<br>• Enters diagnostic mode if the tamper reset counter reaches a programmable threshold |
| 7 | Erase OTP | • Erases the OTP configuration of the device<br>• It will make the device and all wrapped secrets unrecoverable and the device will no longer<br>• be able to boot |
| Note:<br>These responses are cumulative, meaning that if a filter response is triggered, an interrupt will also be triggered | | |

# Secure Vault Tamper Source (SE Hardware)

| Number | Name | Description | Default Level (Response) |
|---|---|---|---|
| 0 | Reserved | — | — |
| 1 | Filter counter | Filter counter reaches configured threshold value | 0 (Ignore) |
| 2 | SE watchdog | Internal SE watchdog expires | 4 (Reset) |
| 3 | Reserved | — | — |
| 4 | SE RAM CRC | SE RAM parity error occurs | 4 (Reset) |
| 5 | SE hard fault | SE core hard fault occurs | 4 (Reset) |
| 6 | Reserved | — | — |

# Secure Vault Tamper Source (SE Software)

| Number | Name | Description | Default Level (Response) |
|---|---|---|---|
| 7 | SE software assertion | SE software triggers an assert | 4 (Reset) |
| 8 | Reserved | — | — |
| 9 | User secure boot | Secure boot of host firmware failed | 0 (Ignore) |
| 10 | Mailbox authorization | Unauthorized command received over the Mailbox interface | 0 (Ignore) |
| 11 | DCI authorization | Unauthorized command received over the DCI interface | 0 (Ignore) |
| 12 | Flash integrity | OTP, MTP or flash content could not be properly authenticated | 4 (Reset) |
| 13 | Reserved | — | — |
| 14 | Self test | Integrity error of internal storage is detected | 4 (Reset) |
| 15 | TRNG monitor | TRNG monitor detected lack of entropy | 0 (Ignore) |

# Secure Vault Tamper Source (Hardware)

| Number | Name | Description | Default Level (Response) |
|---|---|---|---|
| 16 – 23 | PRS0 – 7 | Decouple brown-out detector threshold alert | 0 (Ignore) |
| 24 | Decouple BOD | Decouple brown-out-detector threshold alert | 4 (Reset) |
| 25 | Temperature sensor | On-chip temperature sensor detects temperature outside the operational conditions of the device | 0 (Ignore) |
| 26 | Voltage glitch falling | Voltage glitch detector detected falling glitch | 0 (Ignore) |
| 27 | Voltage glitch rising | Voltage glitch detector detected rising glitch | 0 (Ignore) |
| 28 | Secure lock | Debug lock internal logic check failed | 4 (Reset) |
| 29 | SE debug | SE debug granted | 0 (Ignore) |
| 30 | Digital glitch | Digital glitch detector detected an event | 0 (Ignore) |
| 31 | SE ICACHE | SE instruction cache checksum error | 4 (Reset) |

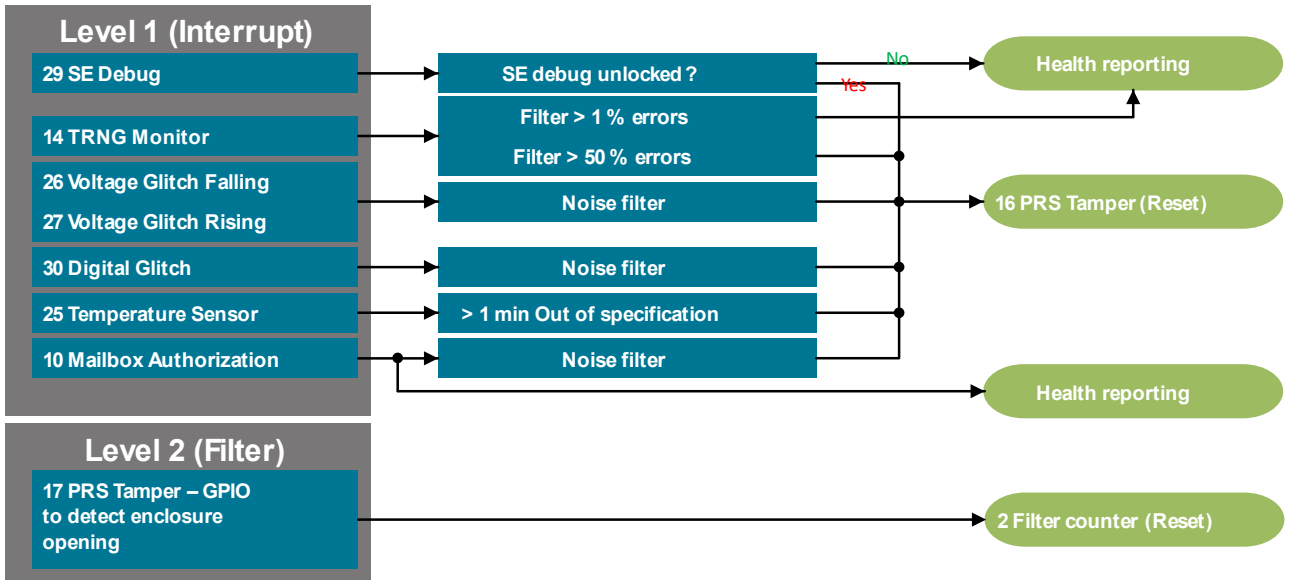
Note:

- Tamper sources 24 to 27 can operate down to EM3 whereas other tamper sources can operate down to EM1.
- Default tamper responses (> 0) are always enabled even when the device is not provisioned.
- Users may escalate the tamper response of any source but they cannot degrade the tamper response below the default Level.

# Secure Vault Tamper Configuration

| Setting | Description |
|---|---|
| Tamper response levels | A response level (0, 1, 2, 4, and 7) for each tamper source (0 – 31) |
| Filter settings | The tamper filter counter has two settings:<br>• Trigger threshold (0 - 7 for 2 - 256)<br>• Reset period (0 - 31 for 32 ms - ~795.4 days) |
| Flags | Digital Glitch Detector Always On (bit 1)<br>• 0 — Digital glitch detector runs when the SE is executing a command<br>• 1 — Digital glitch detector runs continually even the SE is not performing any operations |
| Reset threshold | • The number of consecutive tamper resets (up to 255) before the part enters diagnostic mode<br>• If the threshold is set to 0, the part will never enter the diagnostic mode due to tamper reset |
| Note:<br>The tamper configuration is one-time programmable, this means that tamper settings must be written together with secure boot settings and are immutable after they are written. | |

# Usage Example




Several of the available tamper sources report internal SE errors. By default, tamper is configured to reset the device (level 4) if any of a number of these SE errors are detected.

Custom handling of internal and external tamper sources (default level 0) can be configured to trigger an interrupt (level 1) on the Cortex-M33 or increase a counter in the tamper filter (level 2).

# Secure Vault Tamper Demo

# 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

SILICON LABS

# THANK YOU