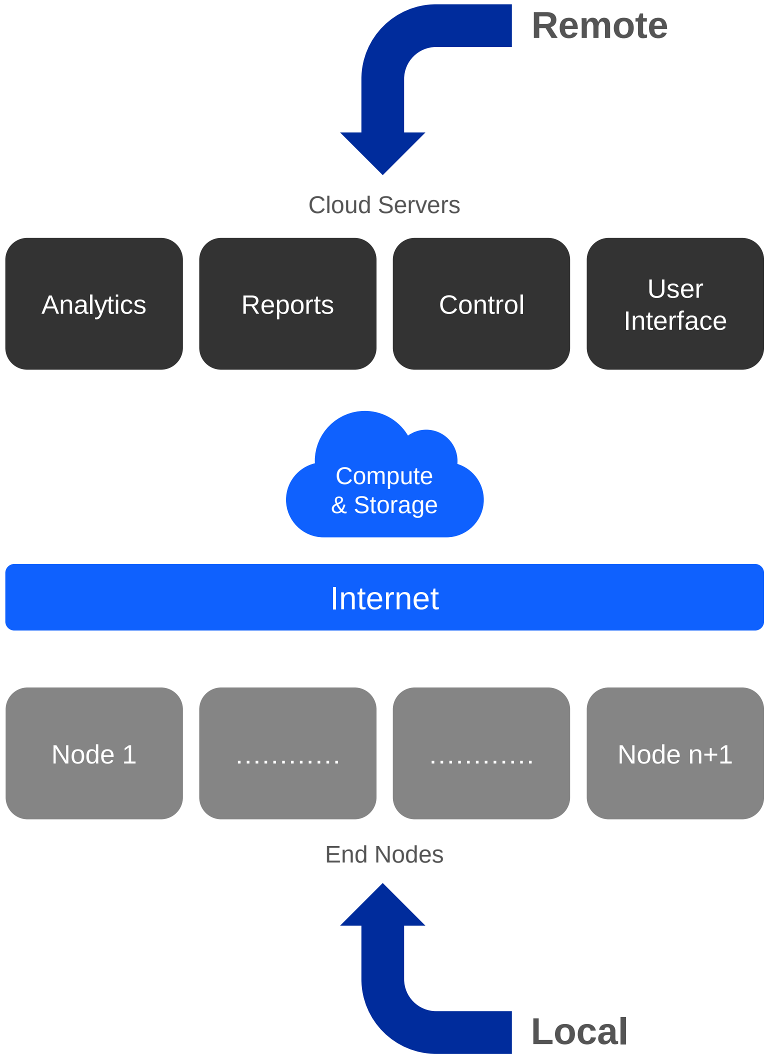
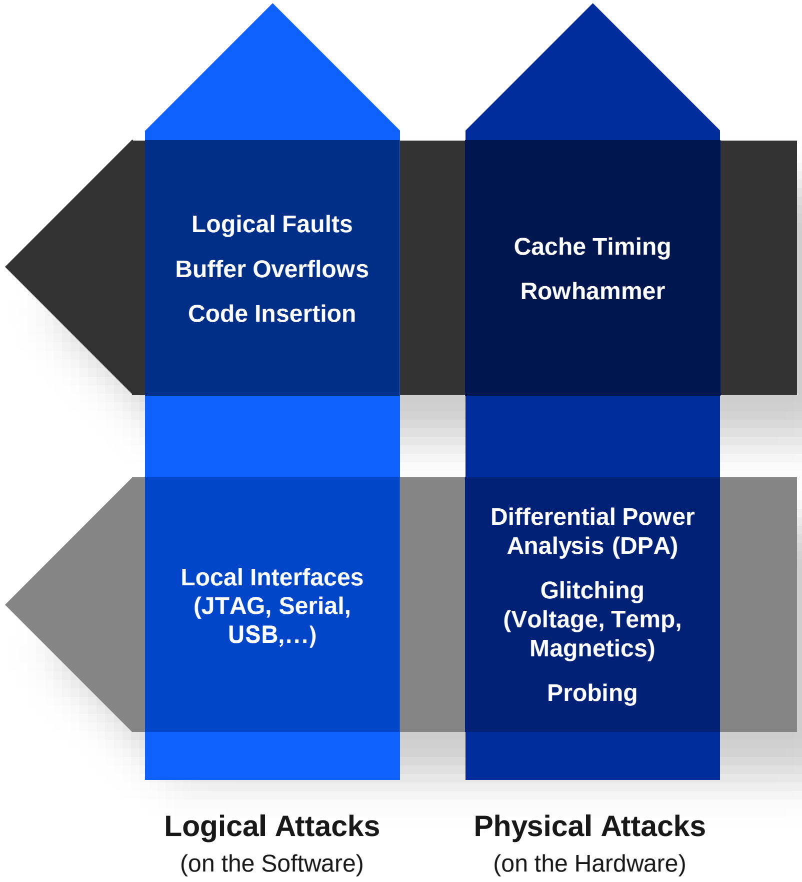
軟硬體結合的安全解決方案為物聯網設計提供絕佳防護

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.

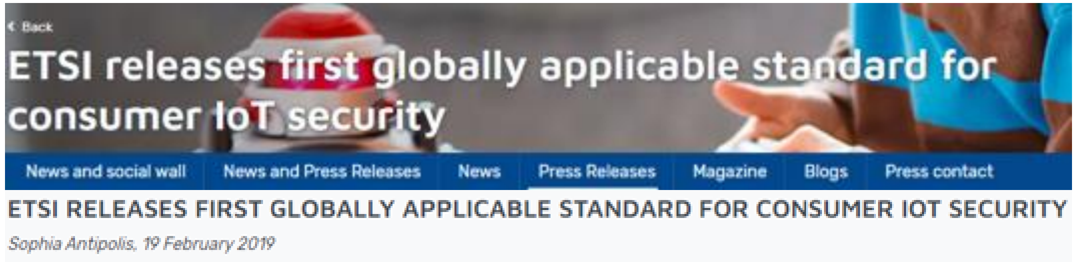
Local Attacks

(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.

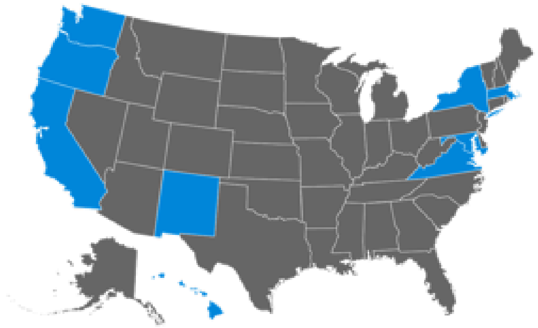
OT is an easier target than IT



- **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

Legislation is Coming to Force the Issue

IoT Security Legislation is Happening



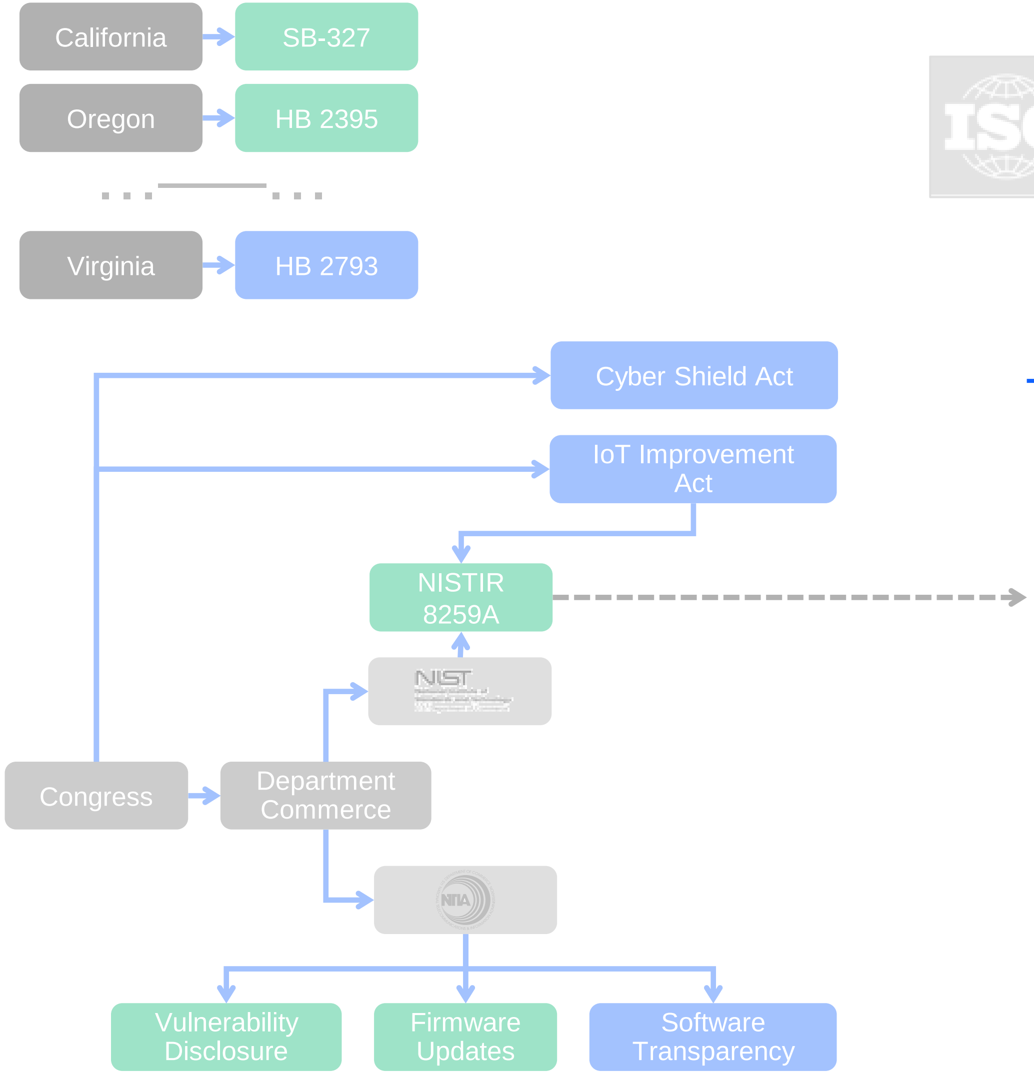
Multiple states have already introduced bills that resemble California's CCPA example

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)

- **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

Already accounts for ~30% US population

Governmental Regulatory Landscape – United States



International Organization for Standardization

NISTIR 8259A

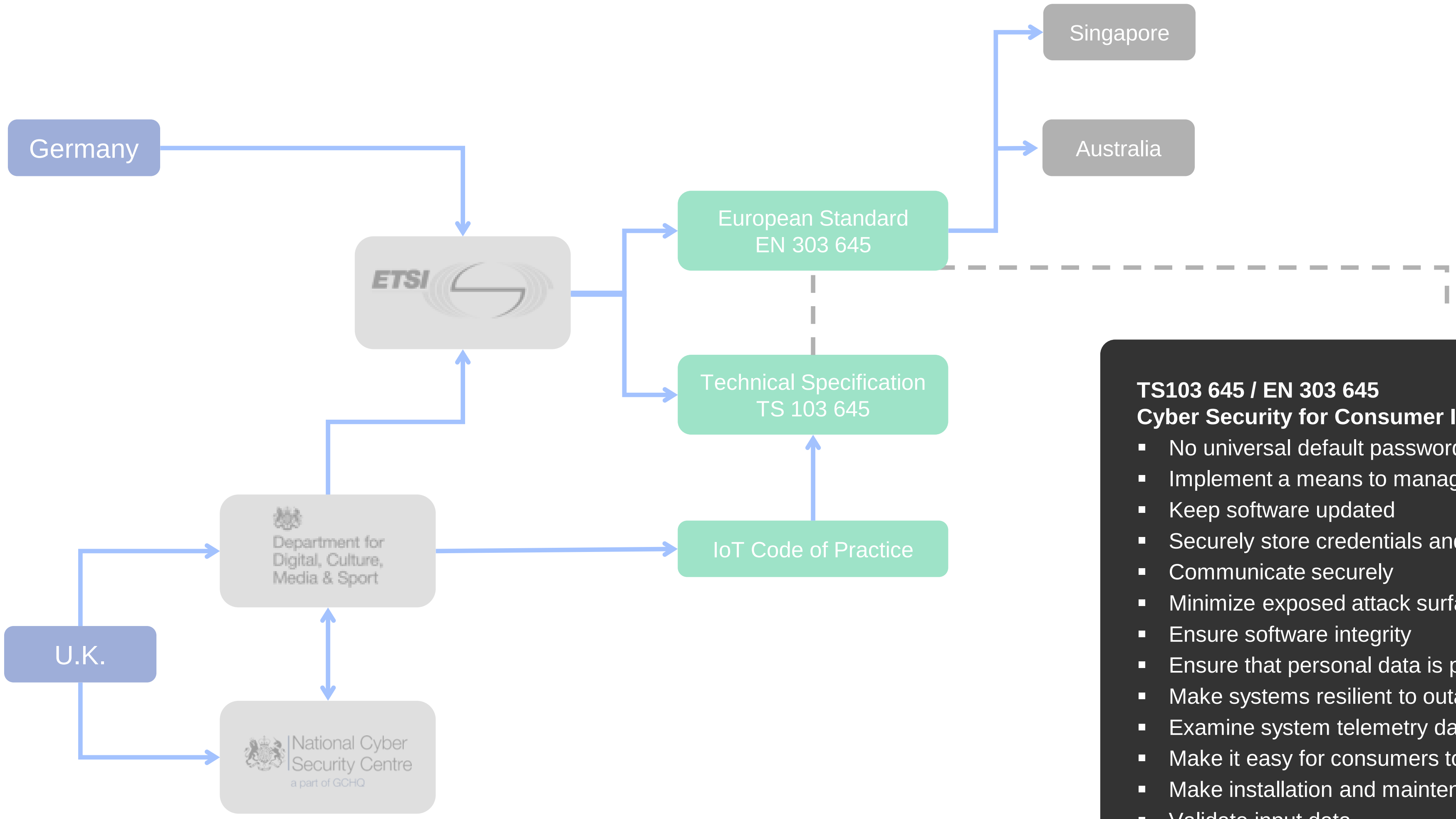
IoT Device Cybersecurity Capability Core Baseline

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

Legend

Published Pending

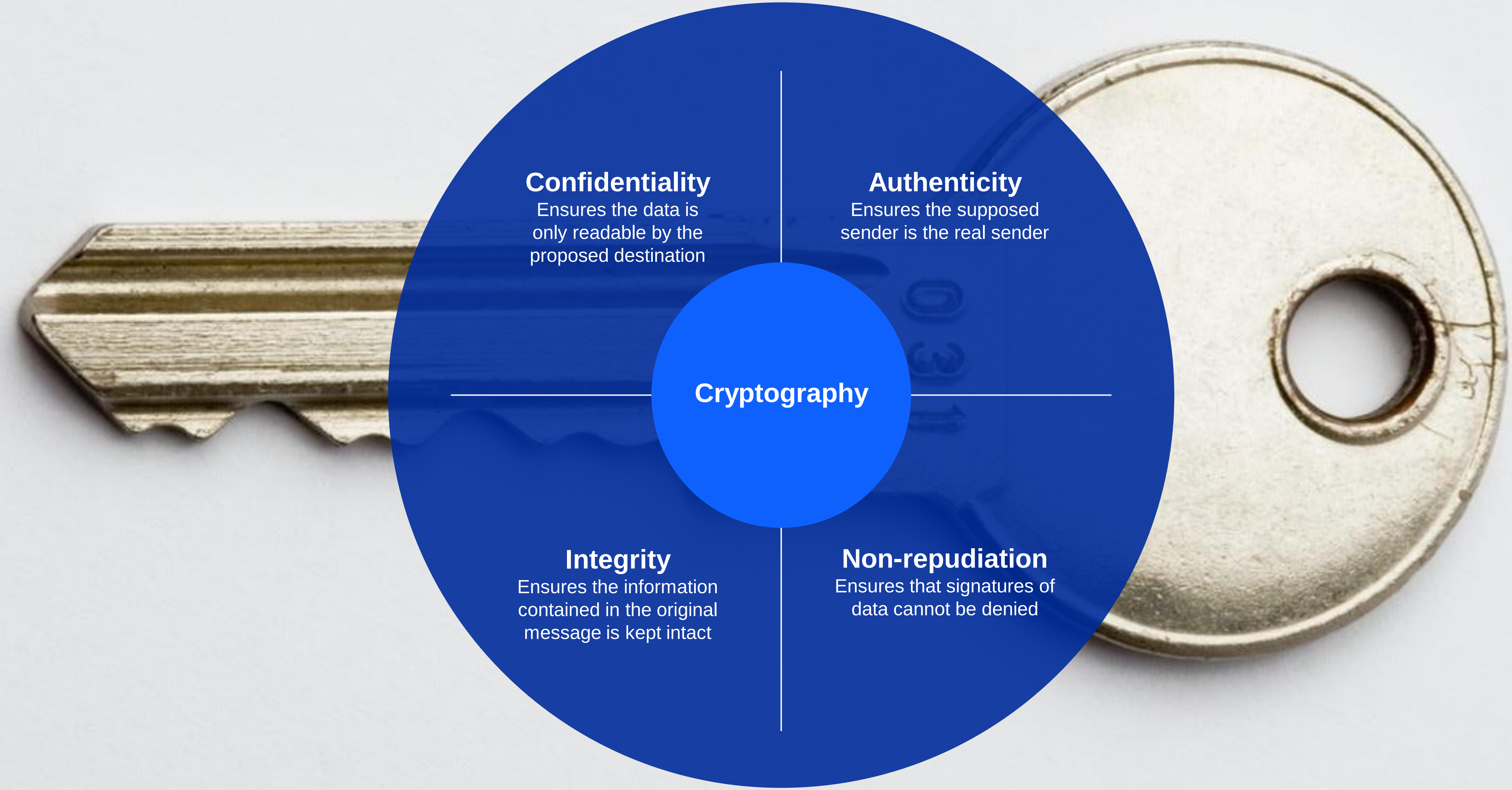
Governmental Regulatory Landscape – Europe (& extended adoptees)



TS103 645 / EN 303 645
Cyber Security for Consumer Internet of Things

- 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



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

silabs.com/security

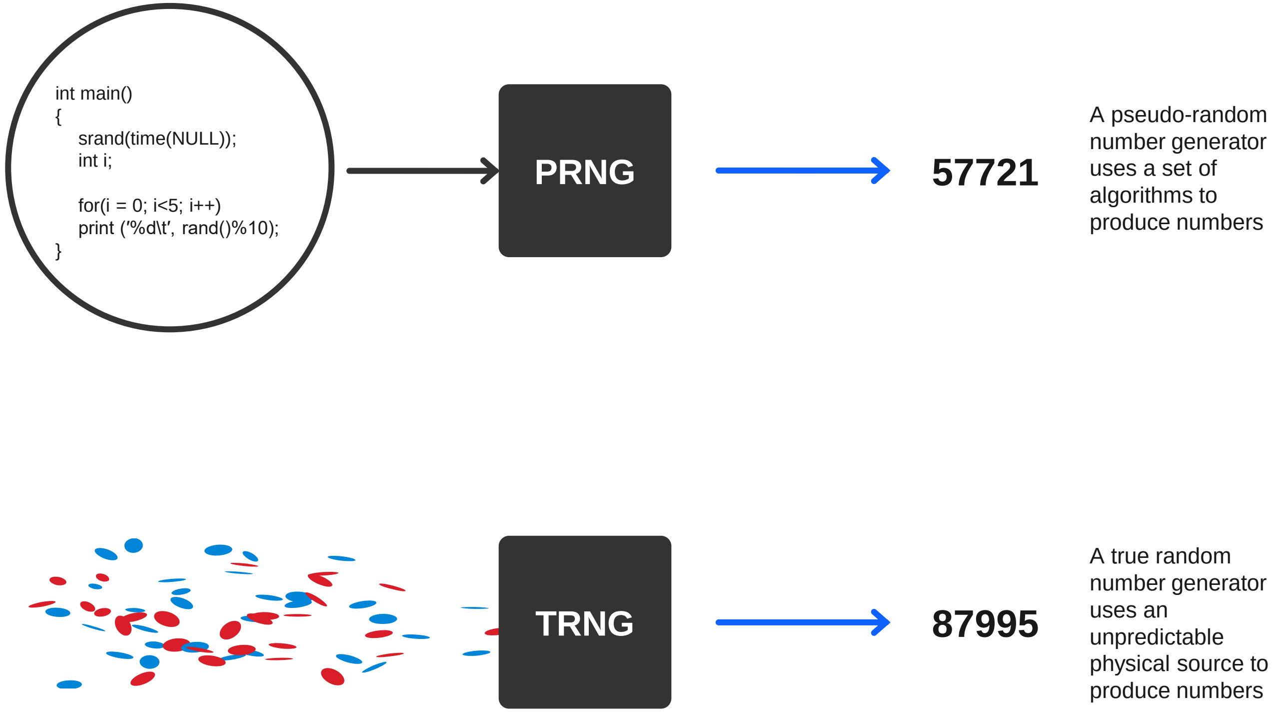
Secure Vault™

Base	Mid	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

SILICON LABS

True Random Number Generator

LOCAL & REMOTE ATTACK VECTOR



- **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

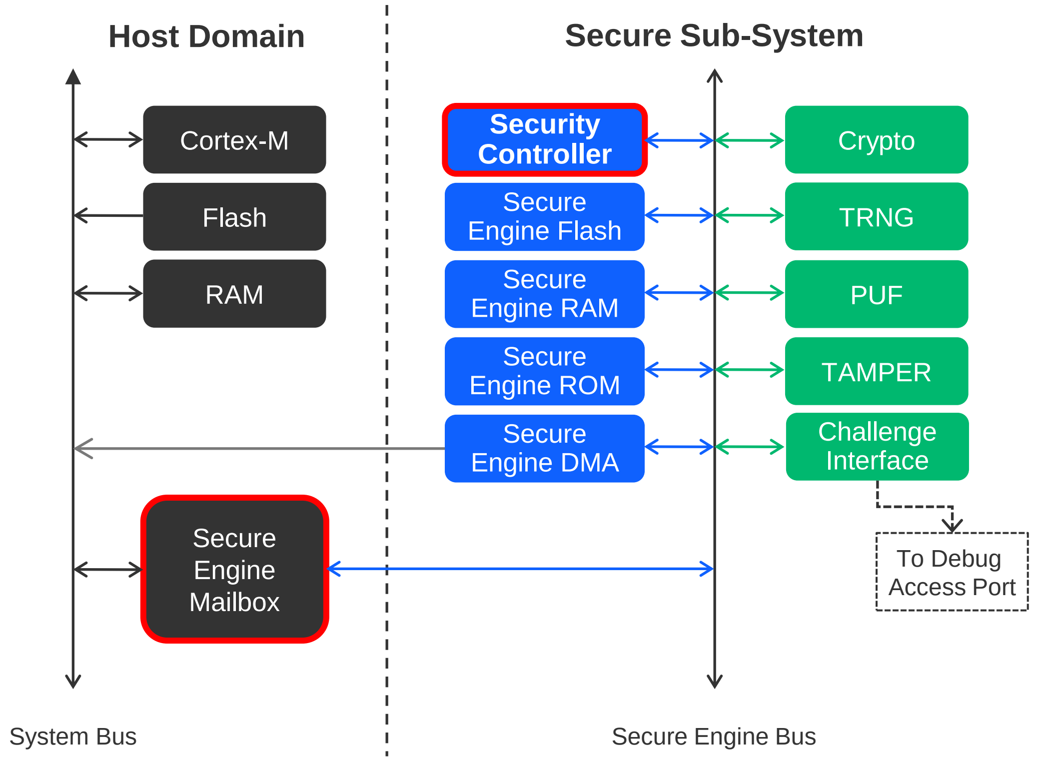
	Cipher	Wireless: ZigbeePRO	Zigbee IP	Thread	Z-Wave	Bluetooth	Homekit	WMBus	TCP/IP: SSL 3.0	TLS 1.2	TLS 1.3
Symmetric Encryption	Triple-DES							Software Only	Software Only		
	AES	Hardware Only	Hardware Only	Hardware Only	Hardware Only	Hardware Only		Hardware Only		Hardware Only	Hardware Only
	CHACHA20						Software Only				Software Only
Asymmetric Encryption	RSA								Software Only	Software Only	
	ECC NIST <=256	Hardware + CPU	Hardware + CPU	Hardware + CPU		Hardware + CPU				Hardware + CPU	Hardware + CPU
	ECC NIST <=521	Software Only					Software Only			Software Only	Software Only
	ECC Curve25519				Software Only		Software Only			Software Only	Software Only
Hash Function	SHA-1	Hardware Only			Hardware Only				Hardware Only		
	SHA-2 <=256		Hardware Only	Hardware Only		Hardware Only				Hardware Only	Hardware Only
	SHA-2 <=512						Software Only			Software Only	Software Only
	POLY1305						Software Only				Software Only

Series 2

	Cipher	Wireless: ZigbeePRO	Zigbee IP	Thread	Z-Wave	Bluetooth	Homekit	WMBus	TCP/IP: SSL 3.0	TLS 1.2	TLS 1.3
Symmetric Encryption	Triple-DES							Software Only	Software Only		
	AES	Hardware Only	Hardware Only	Hardware Only	Hardware Only	Hardware Only		Hardware Only		Hardware Only	Hardware Only
	CHACHA20						Hardware Only				Hardware Only
Asymmetric Encryption	RSA								Software Only	Software Only	
	ECC NIST <=256	Hardware Only	Hardware Only	Hardware Only		Hardware Only				Hardware Only	Hardware Only
	ECC NIST <=521	Hardware Only					Hardware Only			Hardware Only	Hardware Only
	ECC Curve25519						Hardware Only			Hardware Only	Hardware Only
Hash Function	SHA-1	Hardware Only			Hardware Only				Hardware Only		
	SHA-2 <=256		Hardware Only	Hardware Only		Hardware Only				Hardware Only	Hardware Only
	SHA-2 <=512						Hardware Only			Hardware Only	Hardware Only
	POLY1305						Hardware Only				Hardware Only

Legend	
Software Only	OK
Hardware + CPU	Better
Hardware Only	Best

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

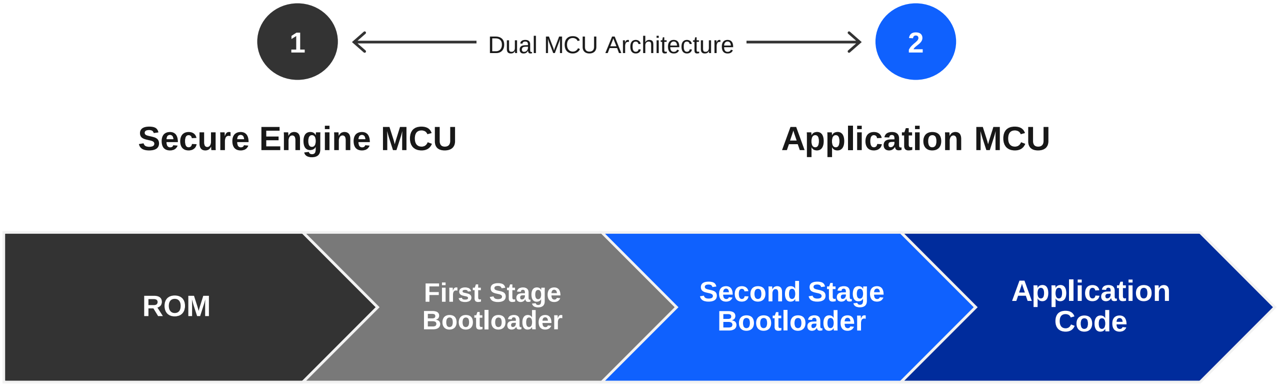
- (but can be securely updated)

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

LOCAL & REMOTE ATTACK VECTOR

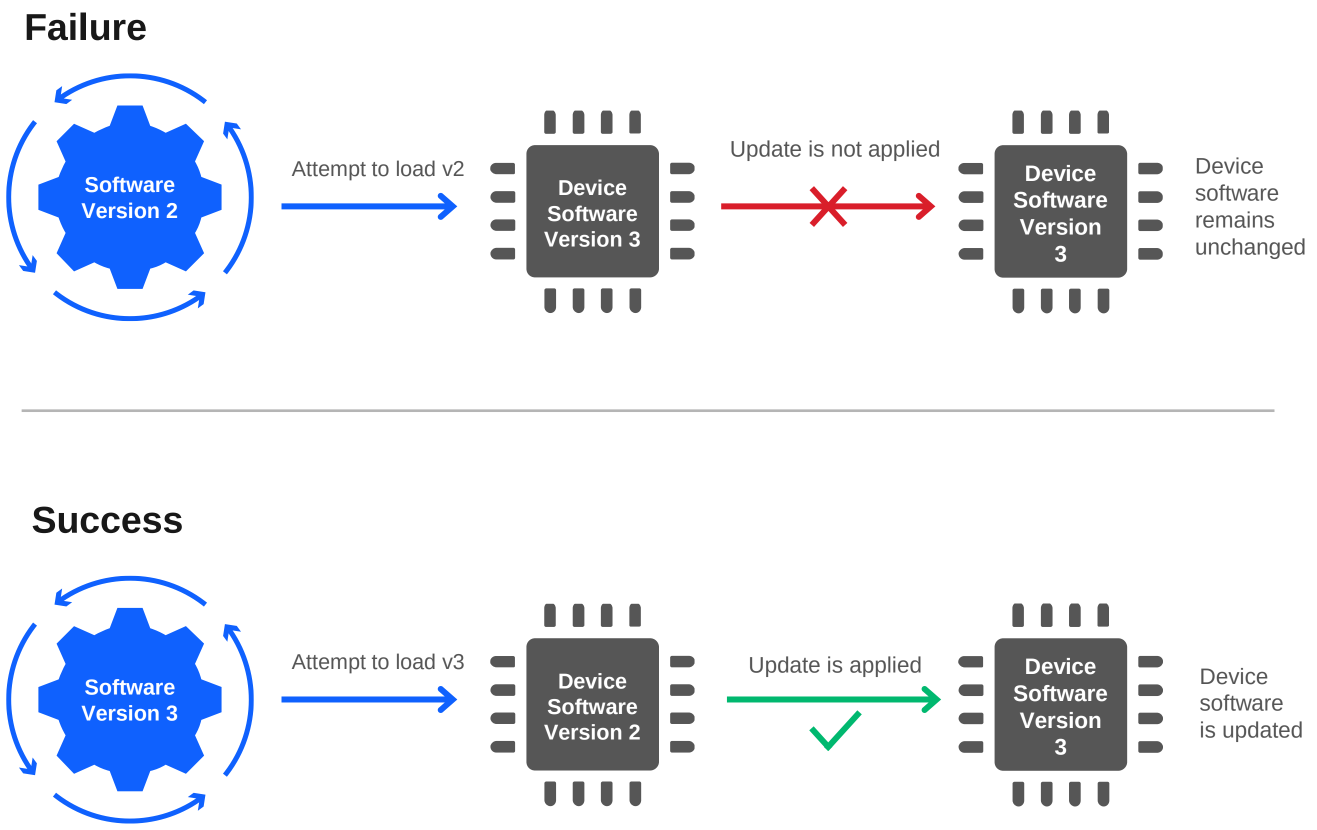


Immutable memory, check secure engine bootloader code (SEB), can update SEB code	Check second stage bootloader code (SSB), can update SSB code	Check application code, can update application code	Execute trusted application code against immutable memory and through full chain of trust

- **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

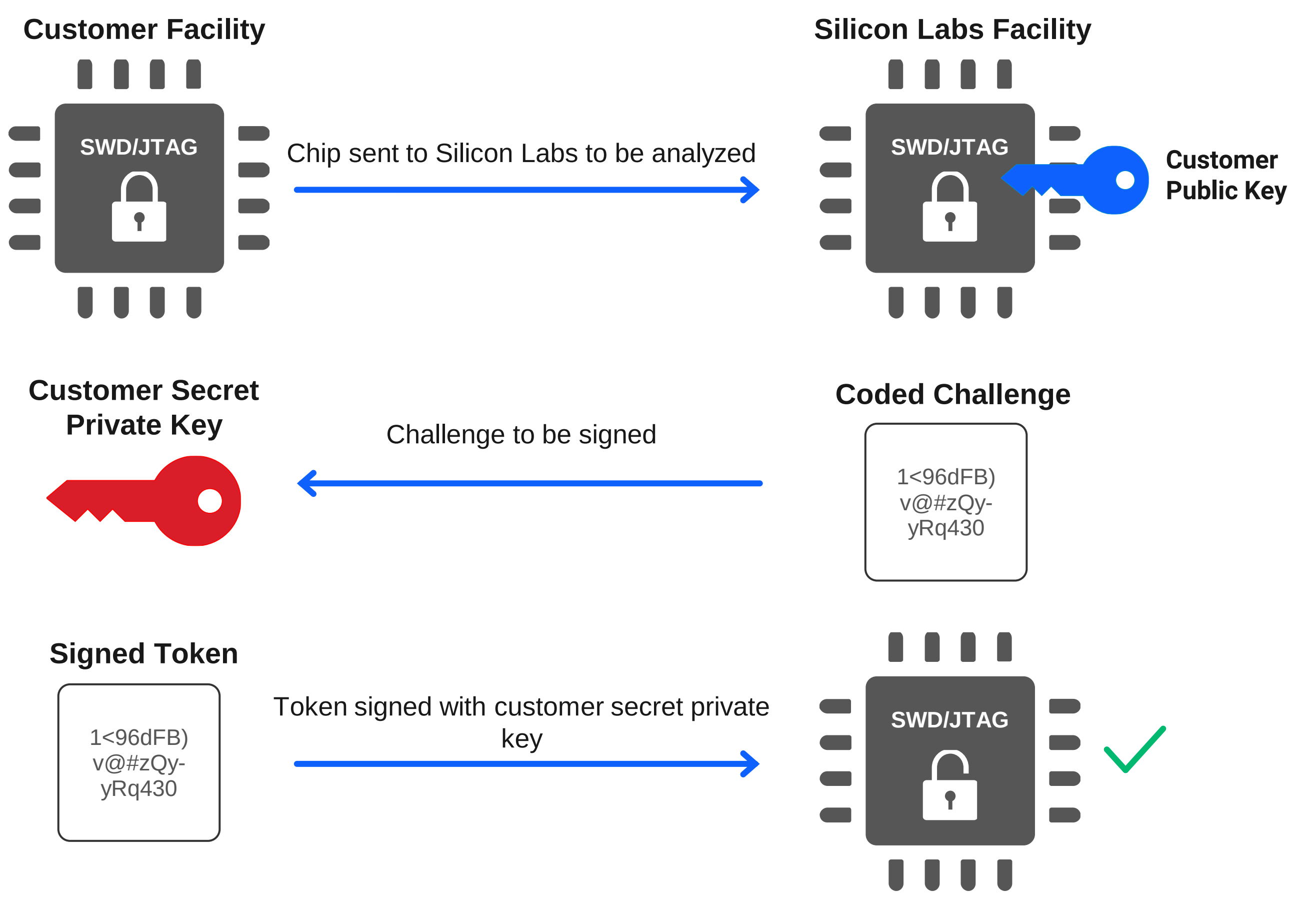
LOCAL & REMOTE ATTACK VECTOR



- **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

LOCAL ATTACK VECTOR



- **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

DPA Countermeasures

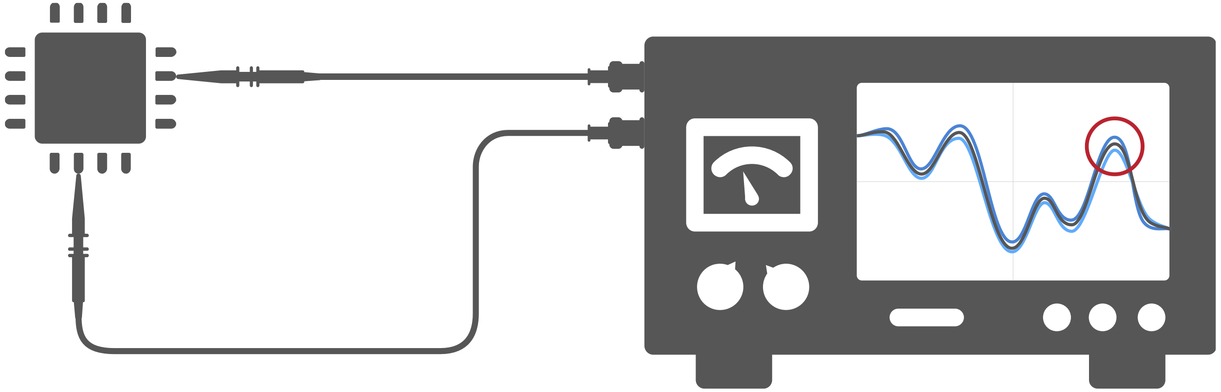
LOCAL ATTACK VECTOR

1

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

2

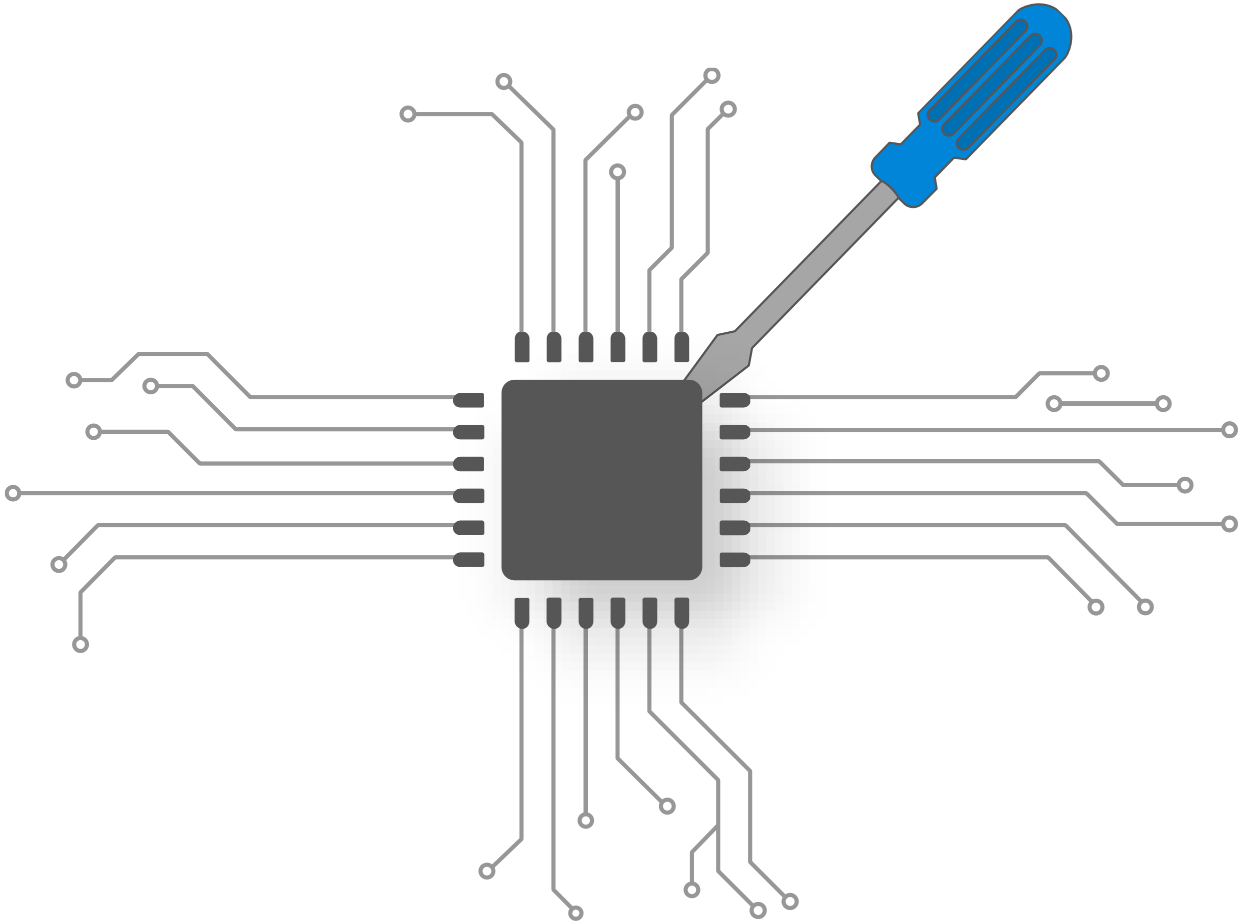
Monitoring electromagnetic radiation and fluctuations in power consumption during crypto operations may reveal security keys and other data.



- **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

Anti-Tamper

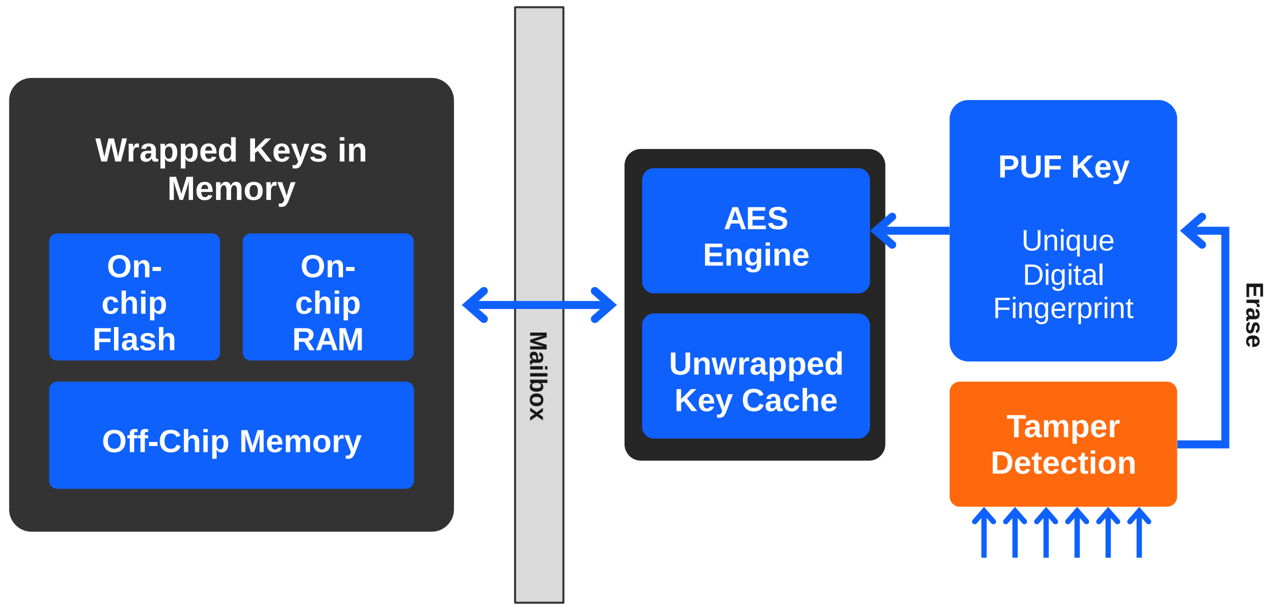
LOCAL ATTACK VECTOR



- **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

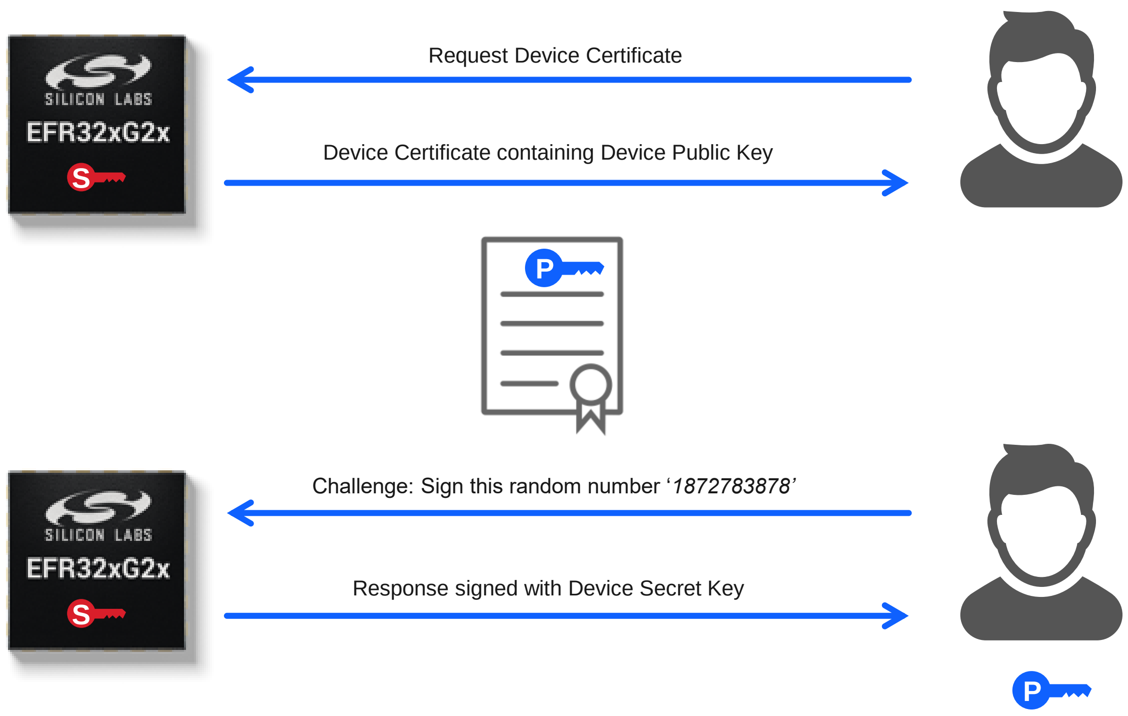
LOCAL & REMOTE ATTACK VECTOR



- **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

LOCAL ATTACK VECTOR



- **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

Secure Vault™ – Formally recognized by industry leaders

- **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*

SILICON LABS

Thank you!

Silicon Labs 官方網站	Silicon Labs 臉書粉絲專頁	Silicon Labs 線上社群