Security in IoT

THREATS EVOLVE. SO SHOULD YOUR DEVICE SECURITY.

MIKE DOW- SR. PRODUCT MARKETER – IOT SECURITY

silabs.com/security

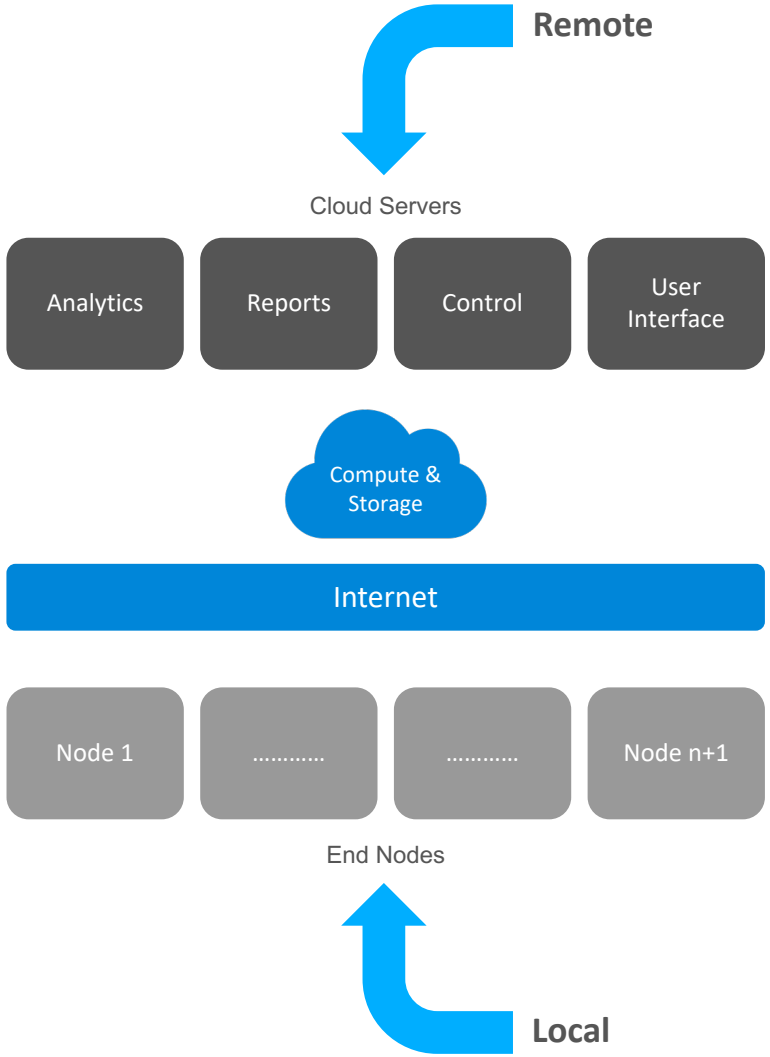
The Leader in IoT Wireless Connectivity

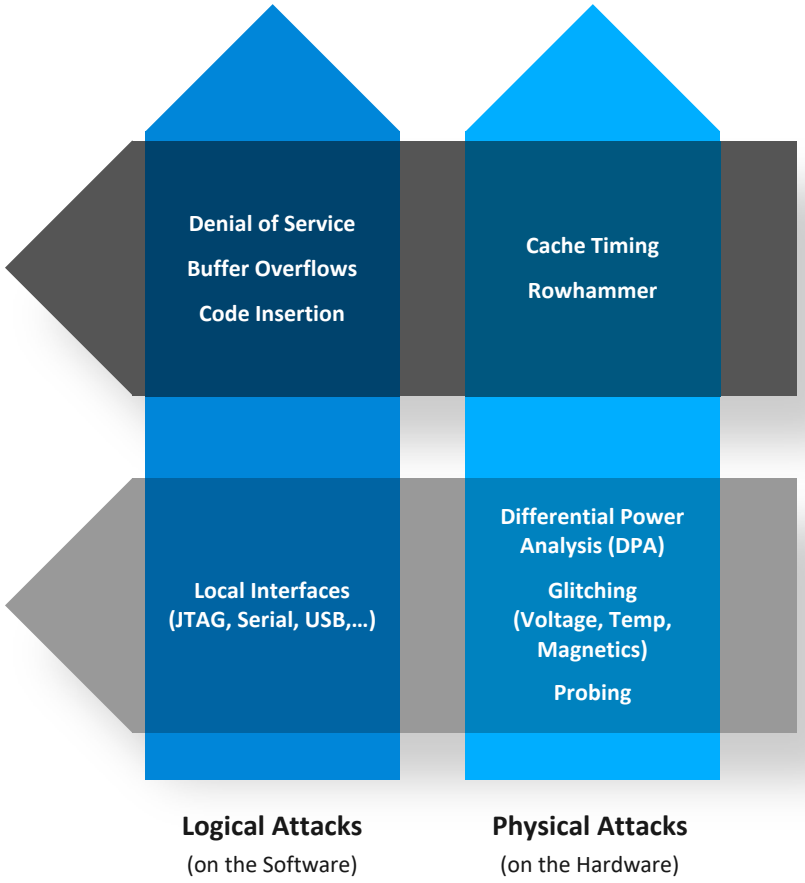
Bluetooth · Proprietary · THREAD · Wi Fi · zigbee · Z-WAVE

>35,000 Customers	>3B Products Shipped
#1 IoT Wireless Solutions	20-30% Wireless Y-Y CAGR*

*Across 15.4, BLE, Wi-Fi, Proprietary

IoT Attack Vectors are shifting from Remote to Local





Remote Attacks
(through the Internet)

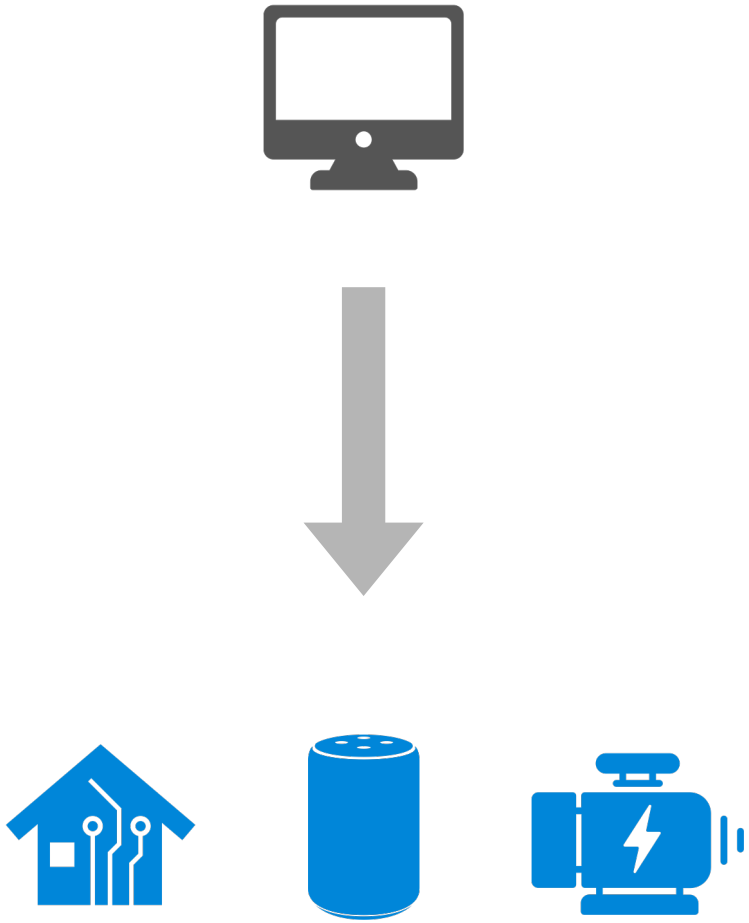
Historically hackers attacked only from the cloud and focused on solely on data servers.

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.

Hacking Targets are moving from IT to OT



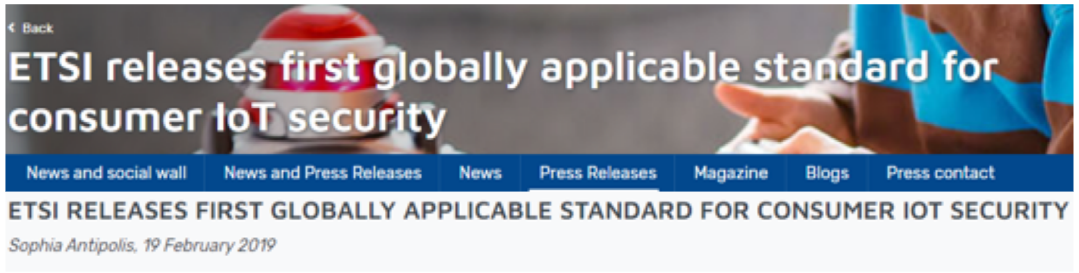
- Targeting end users is small reward
- Targeting big business has greater reward
  - Companies are the new ransomware targets, not individuals
  - Companies cannot afford the downtime
  - Companies have more money
  - Companies don’t want negative press

	Reward	Trend in OT	Comment	IoT Target
Denial of Service	$ $ $ $ $	Growing	Very simple to implement	**YES**
Spam Attacks	$	None	Little reward, IoT often headless	
Cryptocurrency Mining	$ $	Neutral	Limited, requires compute cycles not common in IoT	
Ransomware	$ $ $ $	Growing	Tends to be highly targeted	**YES**
Blackmail / Extortion	$ $	Neutral	Not easy to scale	
Pranks / Nuisance	$	None	Little reward, no professional crime incentive	
Information Theft	$ $ $	Neutral	Done because it is simple	**YES**
Click Fraud	$ $ $ $ $	Growing	High volumes of “Bots” to create ‘click’ revenue	**YES**
Premium Services	$ $ $ $	Down	Difficult to conduct	
Sniffing Network Traffic	$ $	Neutral	Difficult with SSL/TLS	
Pivot Attacks	$ $ $ $ $	Growing	Easy access point to fleet servers	**YES**
Proxy	$	Neutral	Not lucrative, but useful	

OT is an easier target than IT

Congress Introduces Bill to Improve IoT Security

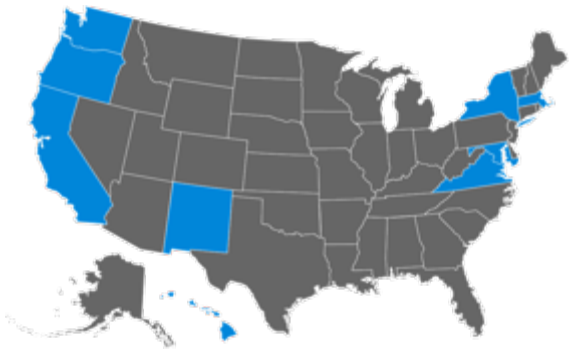
FDA Releases Draft Premarket Cybersecurity Guidance for Medical Device Manufacturers



- 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>1019)
- 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



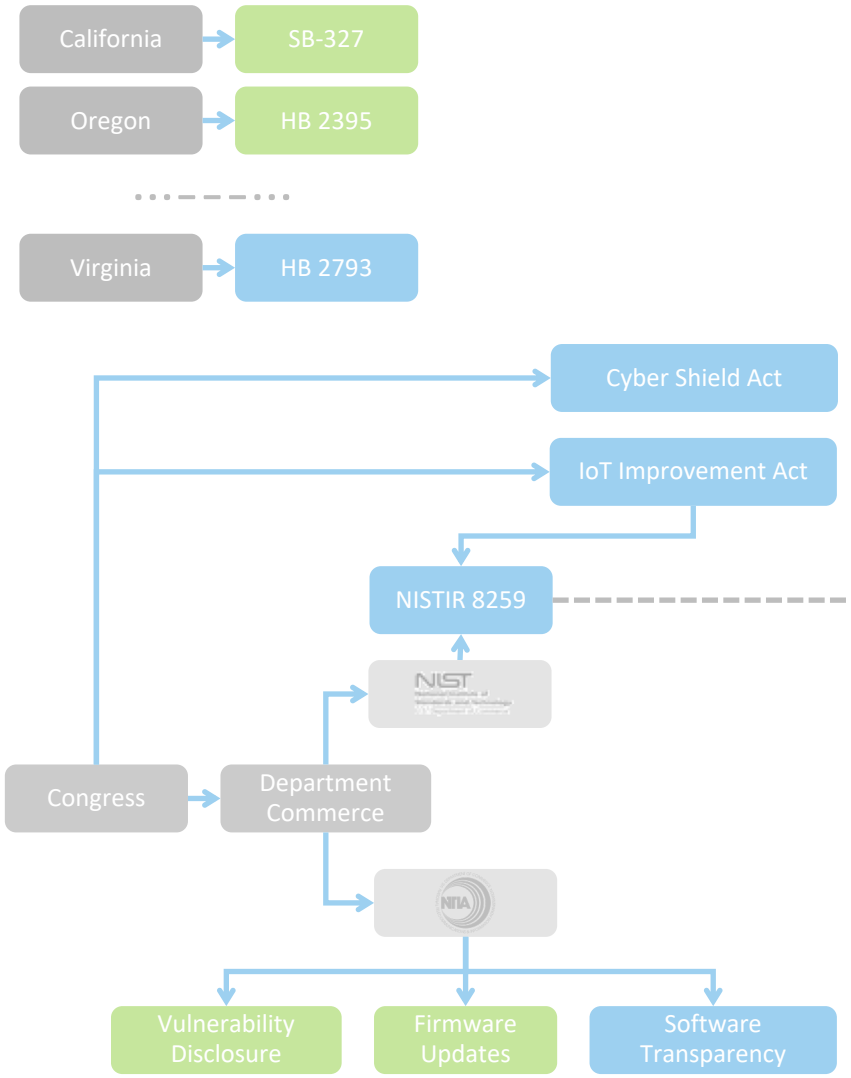
Multiple states have already introduced bills that resemble California's CCPA example

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



ISO International Organization for Standardization

Draft NISTIR 8259

Core Cybersecurity Feature Baseline for Securable IoT Devices:

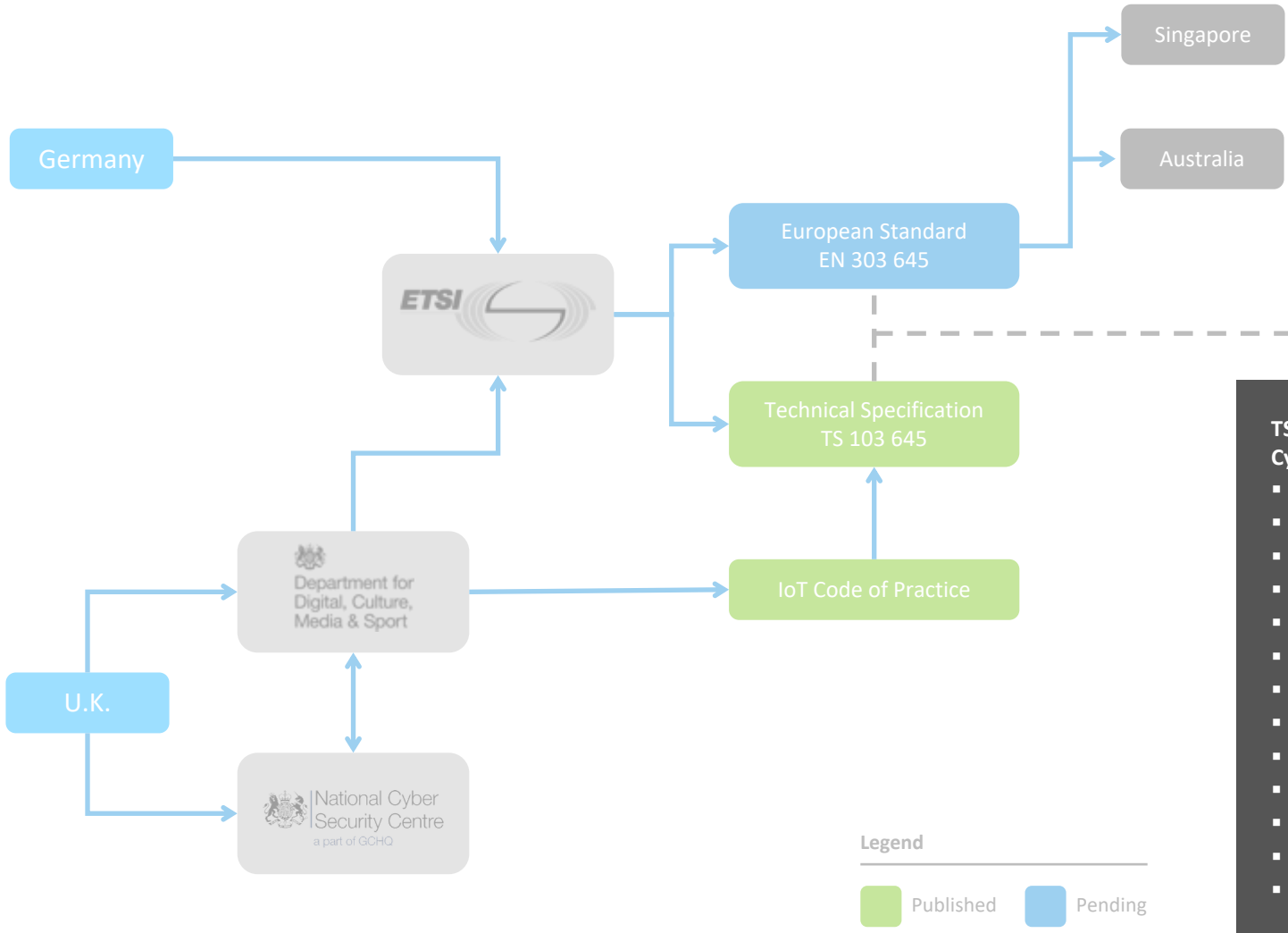
A Starting Point for IoT Device Manufacturers

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

Industrial Association Regulation

American National Standards Institute

International Society of Automation

International Electrotechnical Commission

International Standardization Organization

General

- Concepts & Models
- Master Glossary
- System Security Conformance
- Security Lifecycle

Policies & Procedures

- Security Program Requirements
- Protection Levels
- Patch Management
- Service Provider Requirements
- Implementation Guidance

System

- Security Technologies
- Security Risk Assessment
- Security Requirements and Levels

Component

- Secure Product Lifecycle Requirements
- Technical Security Requirements

The Four Pillars of IoT Security

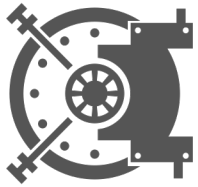
Secure Vault

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

---

silabs.com/security

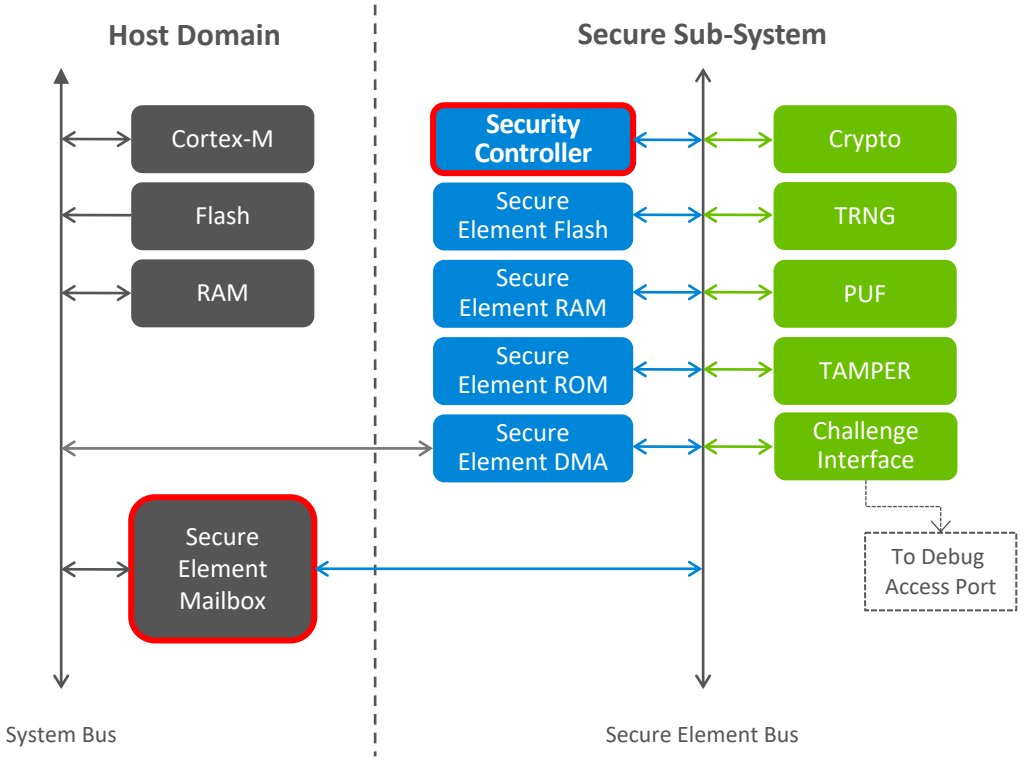
Security Portfolio



Feature	Basic	+Root of Trust	+Secure Element	Secure Vault
True Random Number Generator	✓	✓	✓	✓
Crypto Engine	✓	✓	✓	✓
Secure Boot	✓	✓	✓	✓
Secure Boot with RTSL	-	✓	✓	✓
ARM® TrustZone®	-	✓	✓	✓
Secure Debug with Lock/Unlock	-	✓	✓	✓
DPA Countermeasures	-	-	✓	✓
Anti-Tamper	-	-	-	✓
Secure Attestation	-	-	-	✓
Secure Key Management	-	-	-	✓
Advanced Crypto	-	-	-	✓
	Series 1 – xG1x M4	**Series 2 – xG22 M33**	**Series 2 – xG21A M33**	**Series 2 – xG21B M33**

silabs.com/security

Secure Element 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)

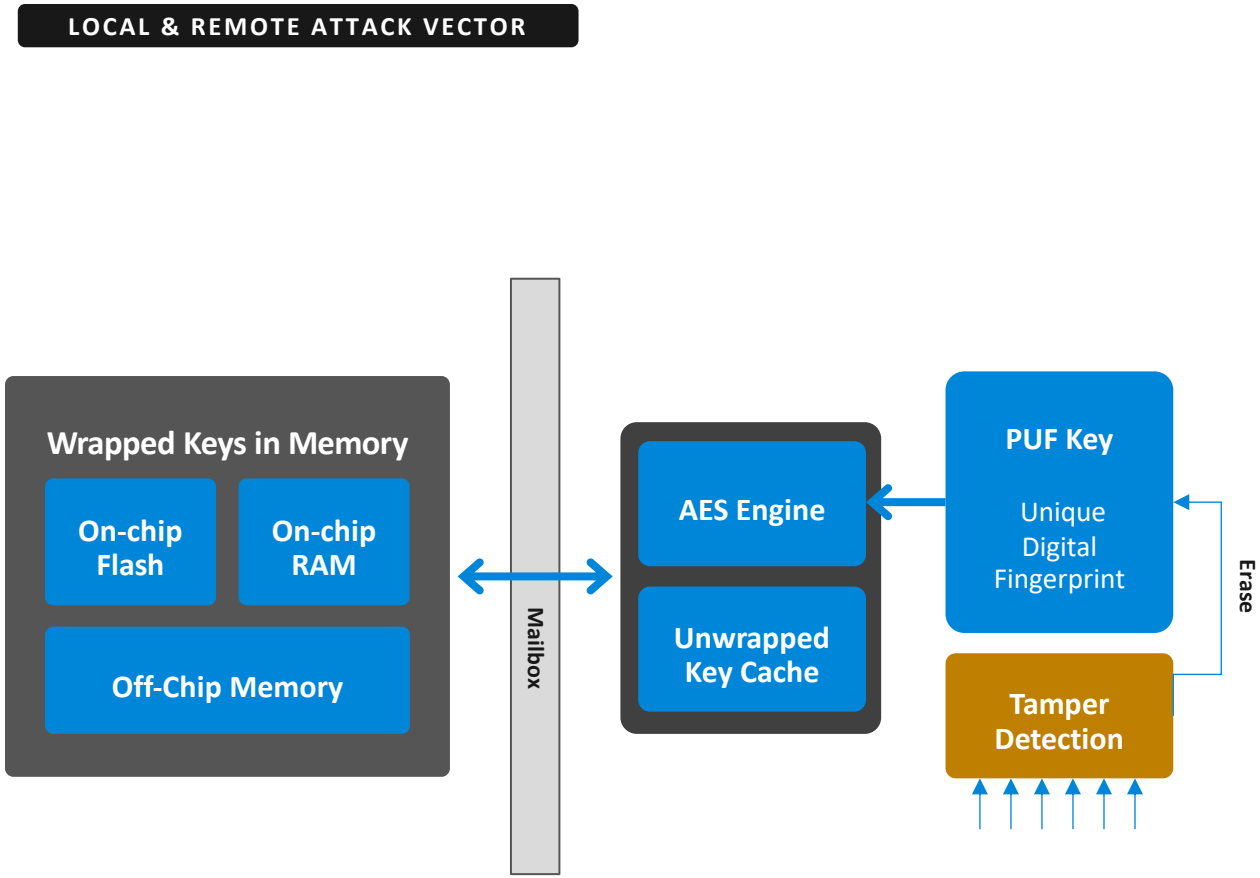
Crypto-coprocessor is not customer programmable

- (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

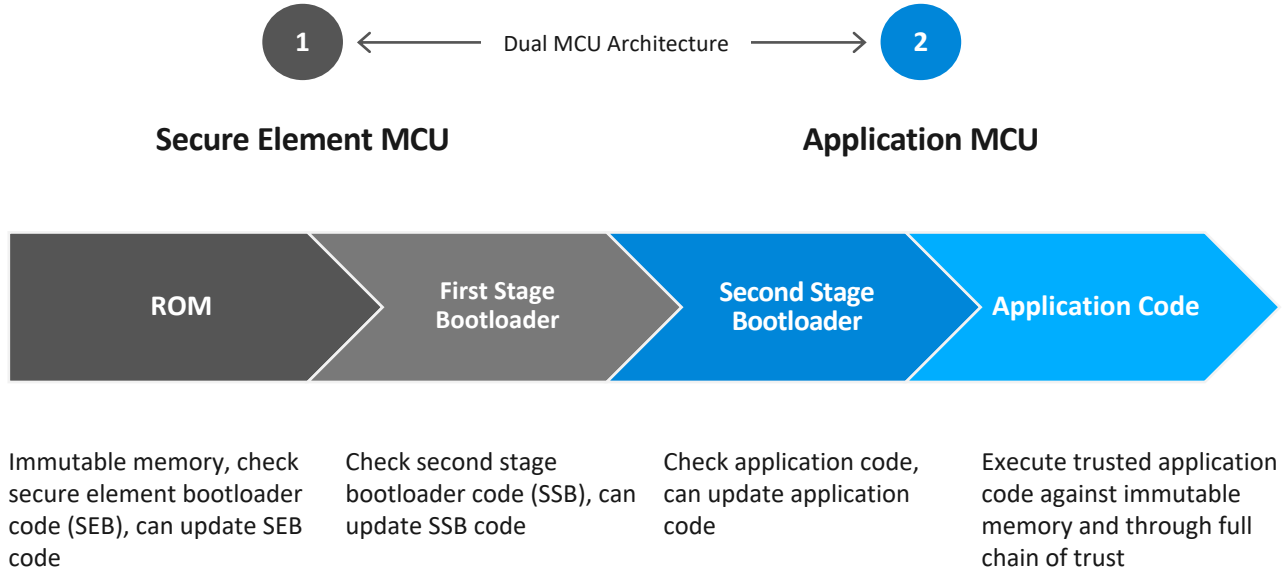
Secure Key Management



- 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

Secure Boot

LOCAL & REMOTE ATTACK VECTOR

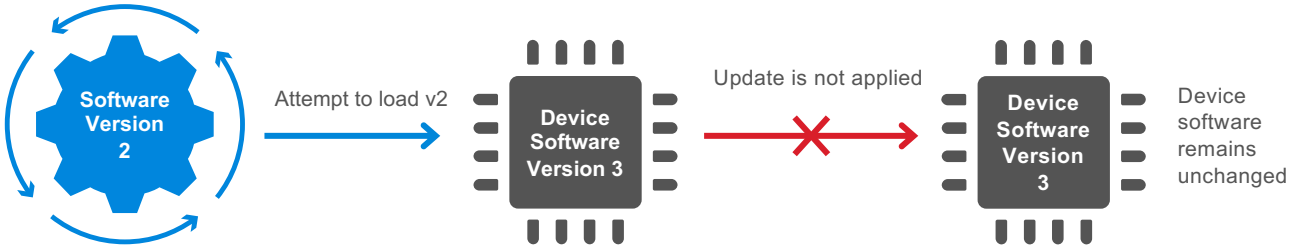


- Vulnerabilities
  - Replacing code with ‘look-alike code’ makes a product appear normal. Hackers use it to copy/re-direct data to alternate servers.
- Secure Boot with RTSL
  (Root-of-Trust & Secure Loader)
  - Use and execute only trusted application code against immutable memory and through a full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

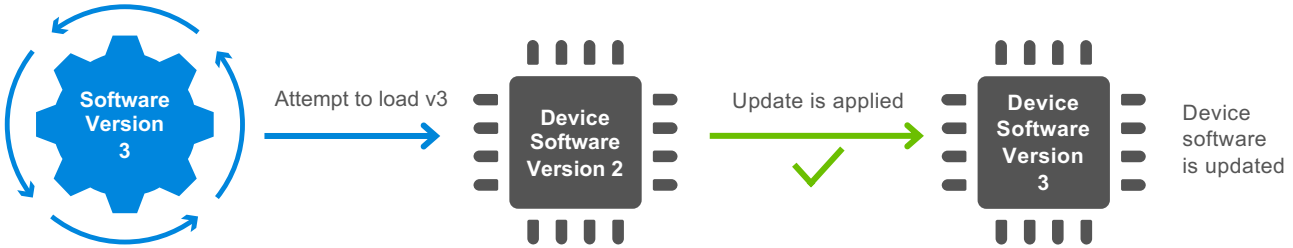
Anti-Rollback Prevention

LOCAL & REMOTE ATTACK VECTOR

Failure



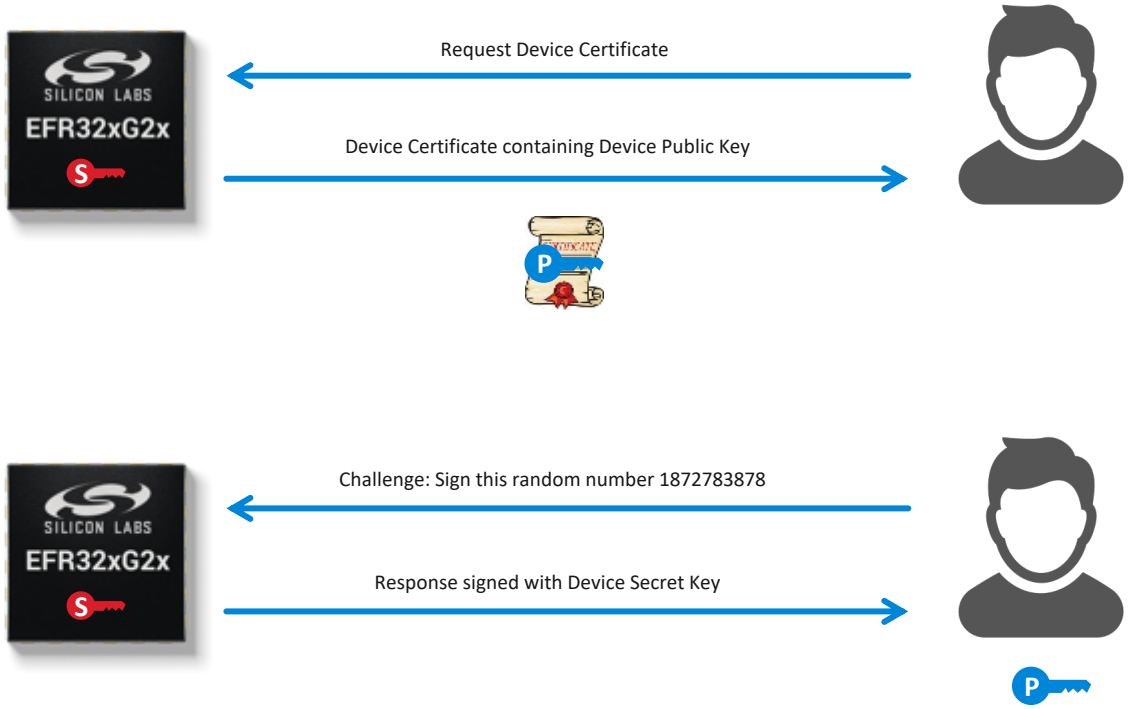
Success



- 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

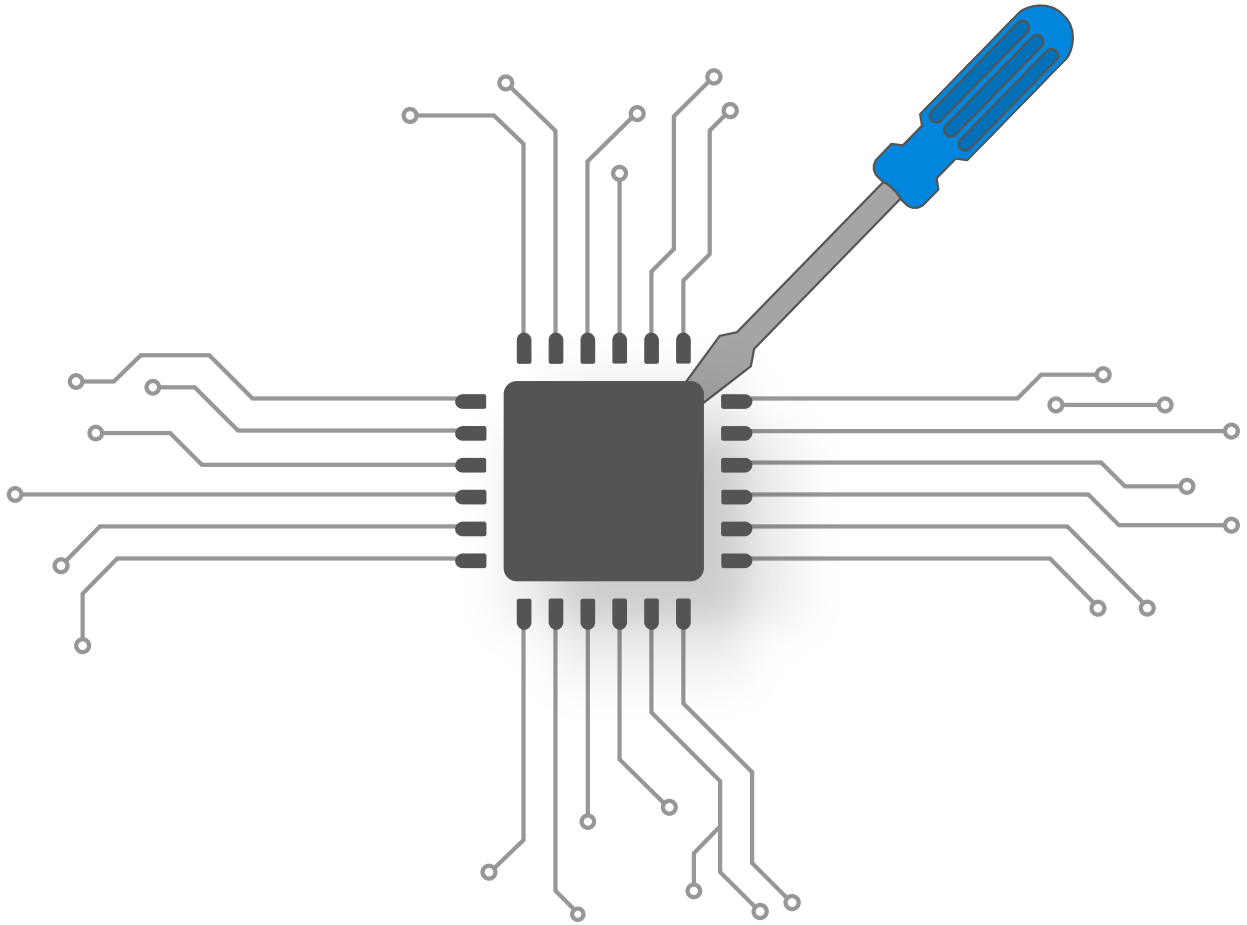
LOCAL ATTACK VECTOR



- 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 key
  - The device secret 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

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.

DPA Countermeasures

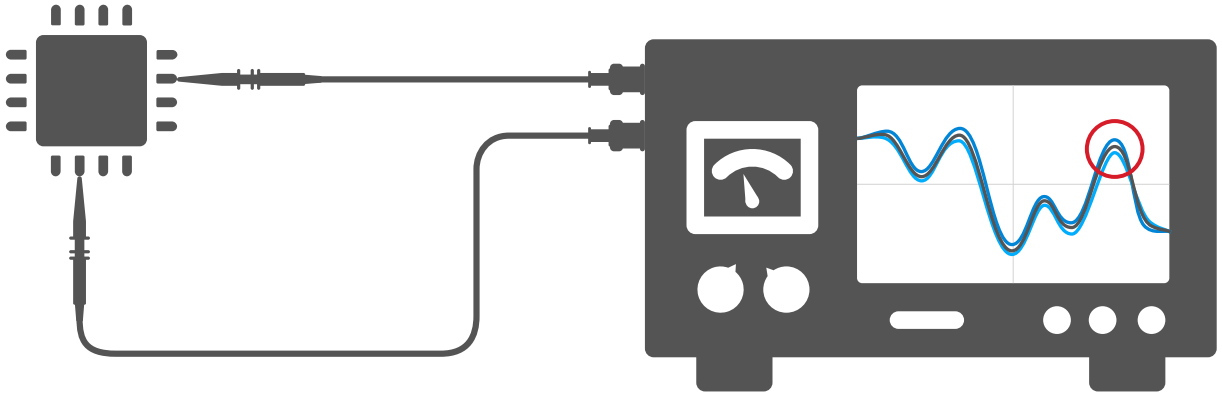
LOCAL ATTACK VECTOR

1

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

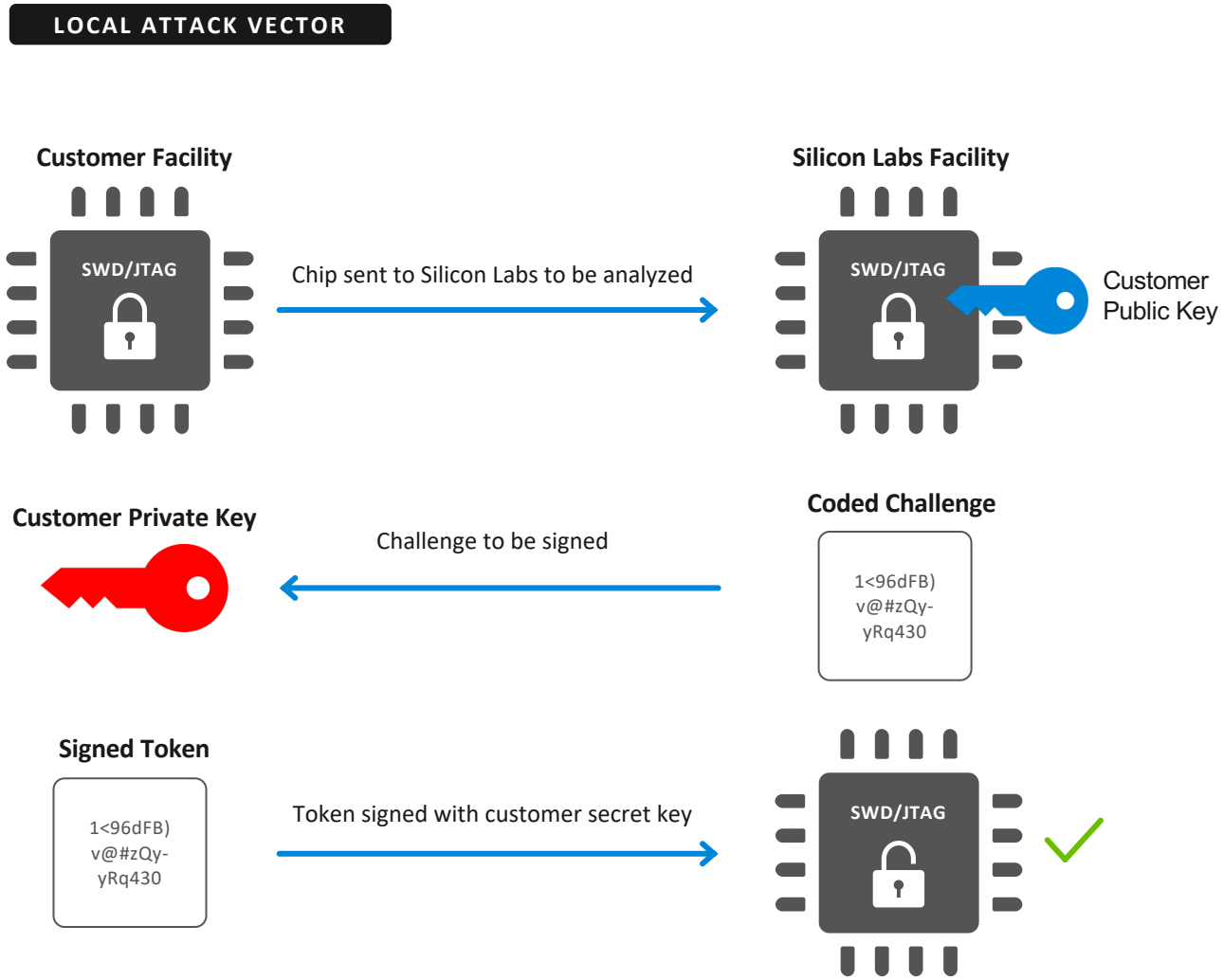
2

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

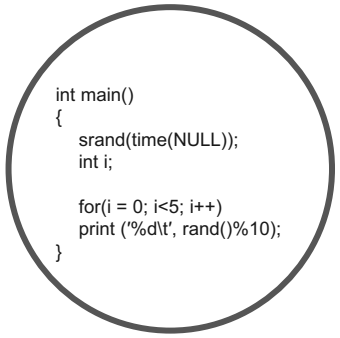
Secure Debug



- 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

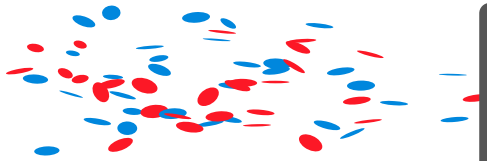
True Random Number Generator

LOCAL & REMOTE ATTACK VECTOR



PRNG → **57721**

A pseudo-random number generator uses a set of algorithms to produce numbers



TRNG → **87995**

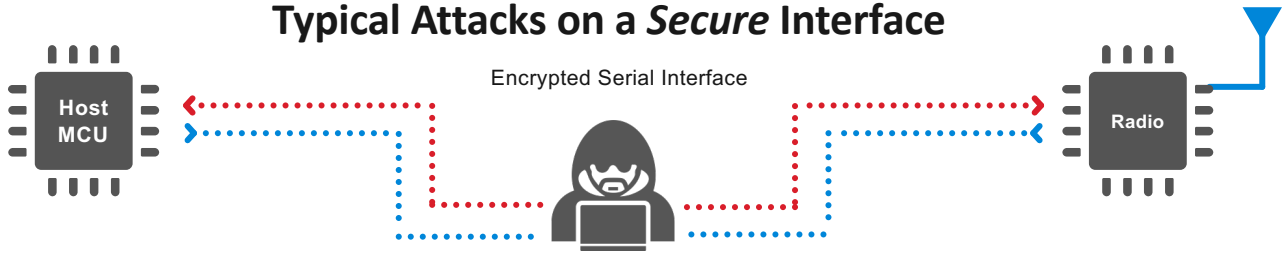
A true random number generator uses an unpredictable physical source to produce numbers

- 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

Secure Link

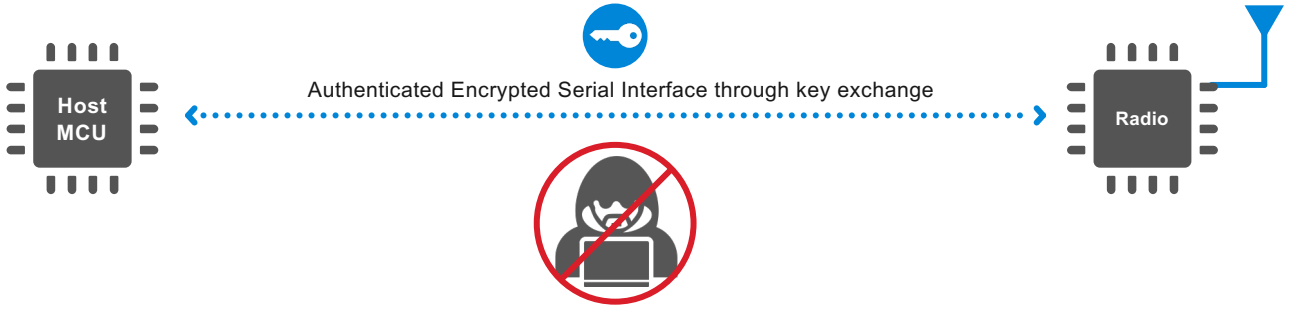
LOCAL ATTACK VECTOR

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

Silicon Labs Secure Vault

Learn More

- https://www.silabs.com/security
- Sign-up to receive security updates
- Q&A