Security for Code and Data Protection in Embedded Systems

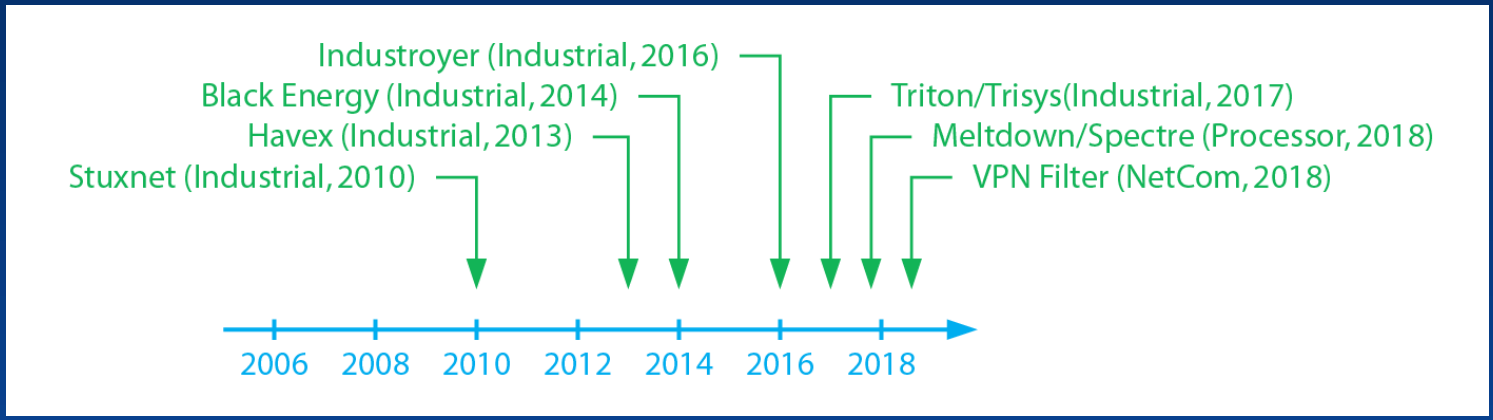
Grady Lambert

Director of Business Development

swissbit®

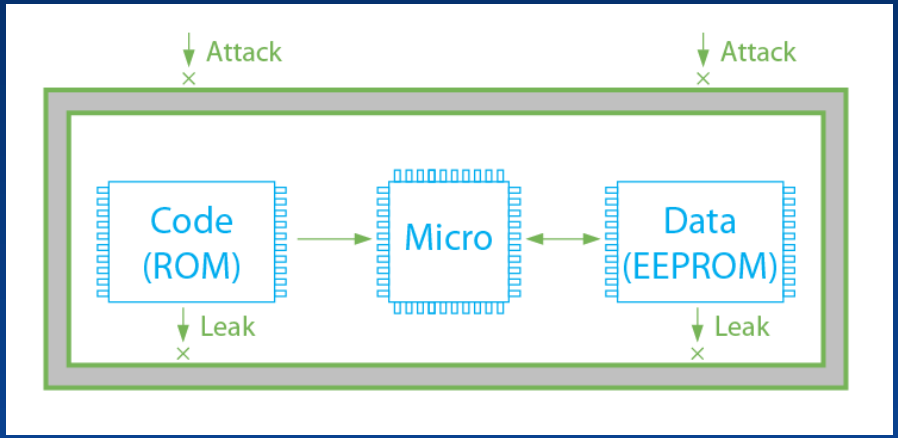
Santa Clara, CA
August 2018

Motivation



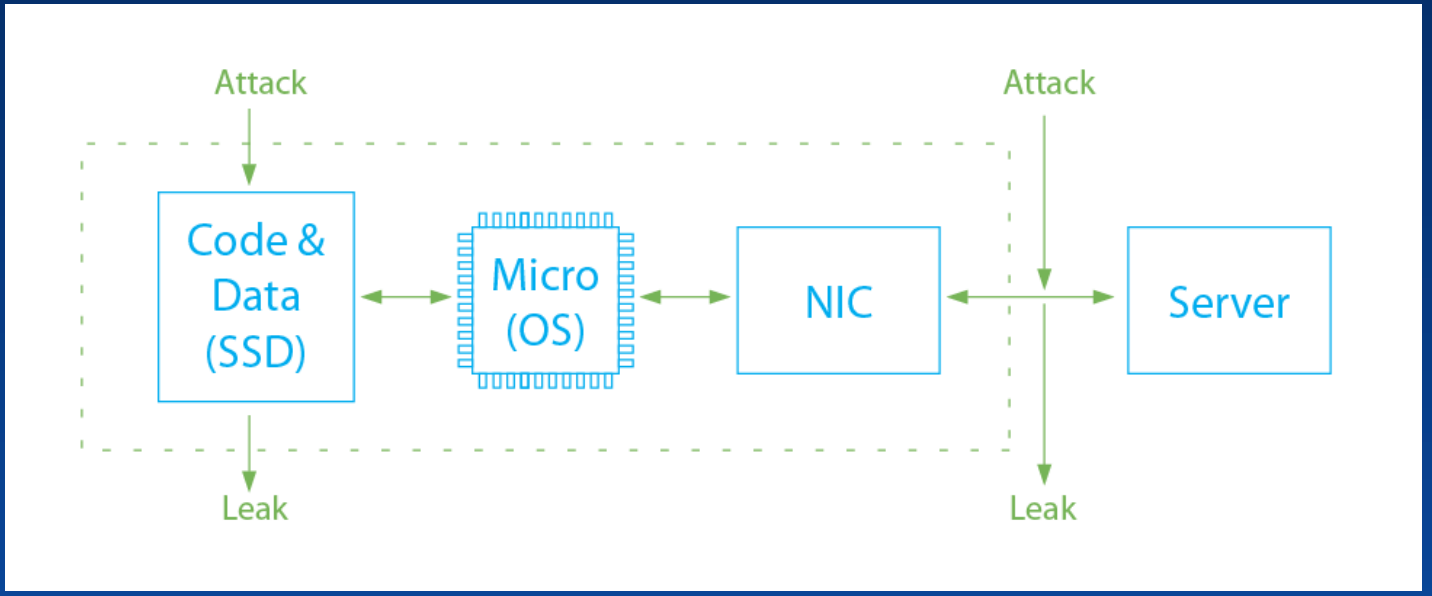
- Embedded PCs are not exempt from security threats
- Not “if”, “when”

Embedded Computer (Classic)



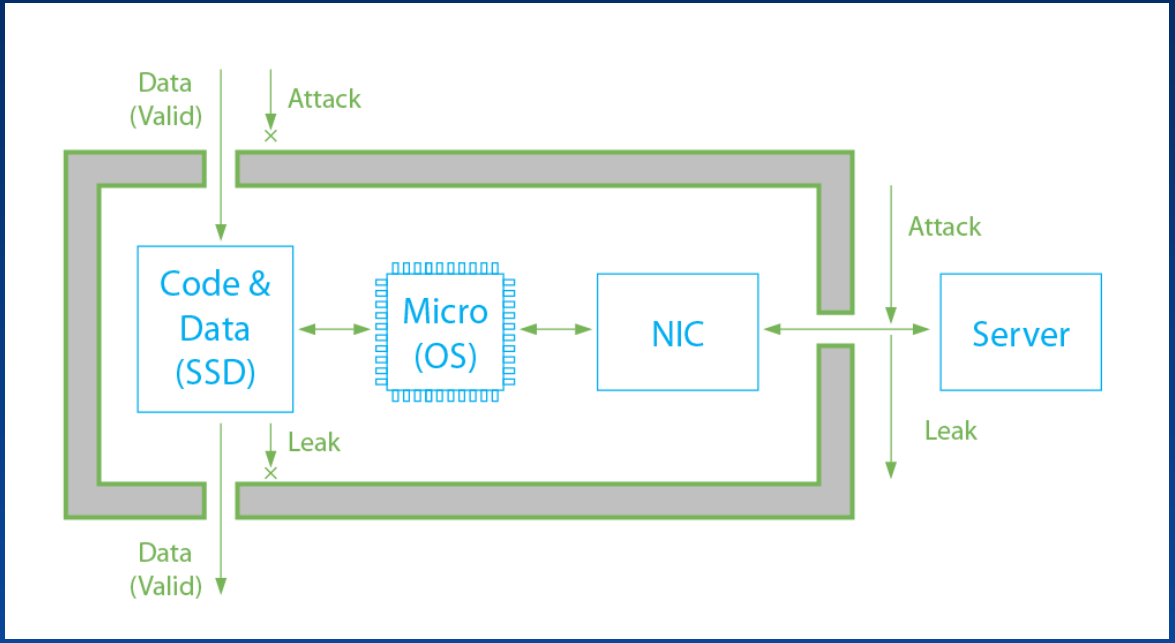
- No security needed or “highly secure”

Embedded Computer (Recent)



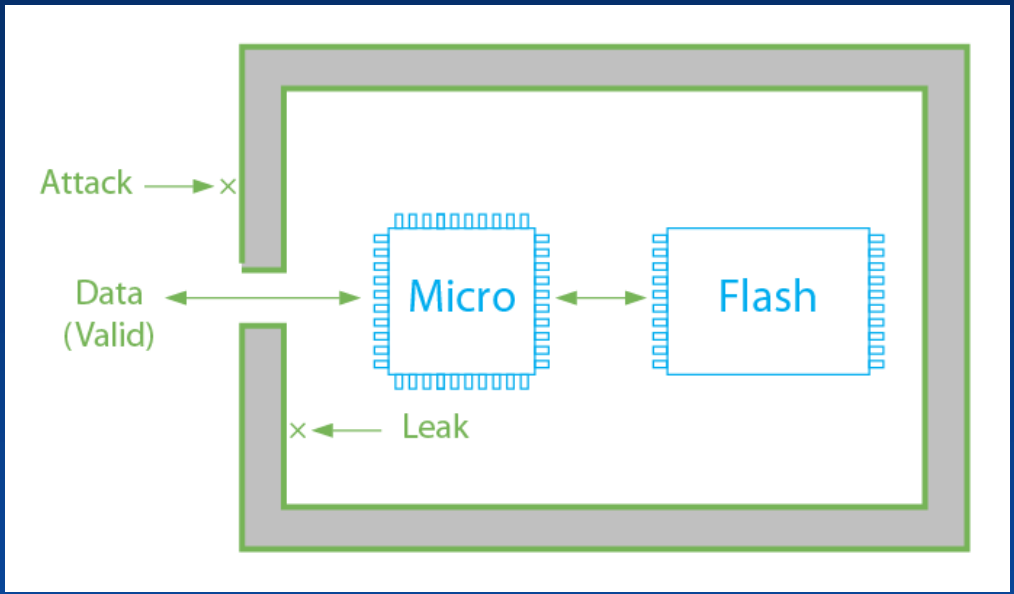
- Evolved from consumer PC. No security

Embedded Computer (Ideal)



- System Design Goal: “Controlled Permeability”

Flash Memory System (SSD)



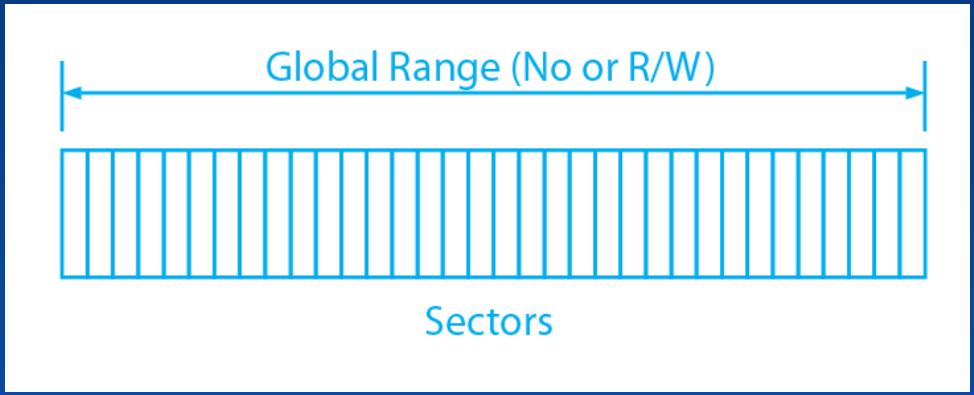
- Flash Memory Design: “Controlled Permeability”

Approaches

- Software
  - Standard
  - Vendor Commands
- Software & Hardware
  - AES, TCG Opal
  - TPM

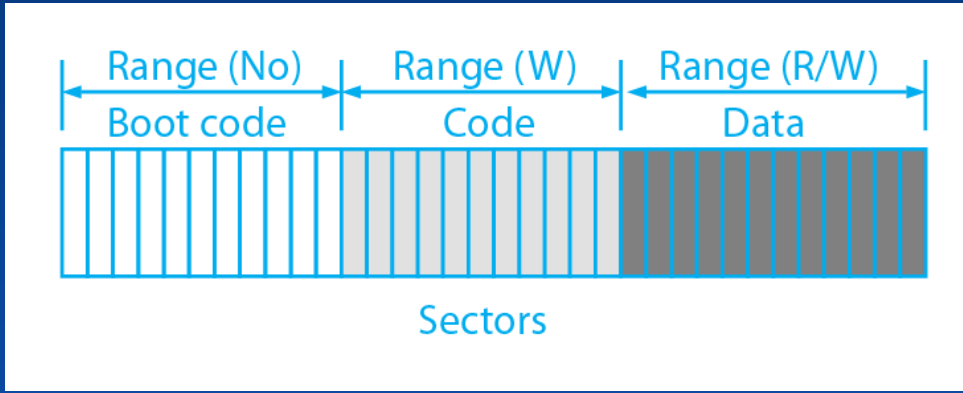
Software - Standard

- Protection: None (No) or Total (R/W), Erase
- Ex: ATA Security
  - Host Requirements: Minimal, BIOS support

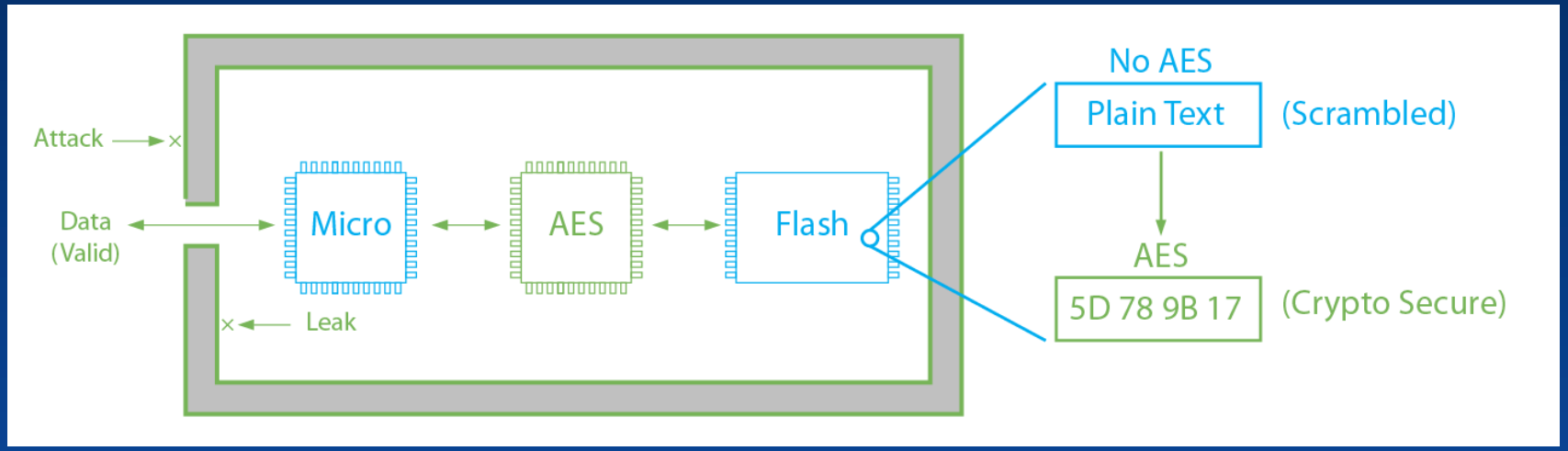


Software – Proprietary

- Protection: None (No), Read-Only (W), Total (R/W), Erase
- Ex: Swissbit
  - Host Requirements: Minimal, boot code development



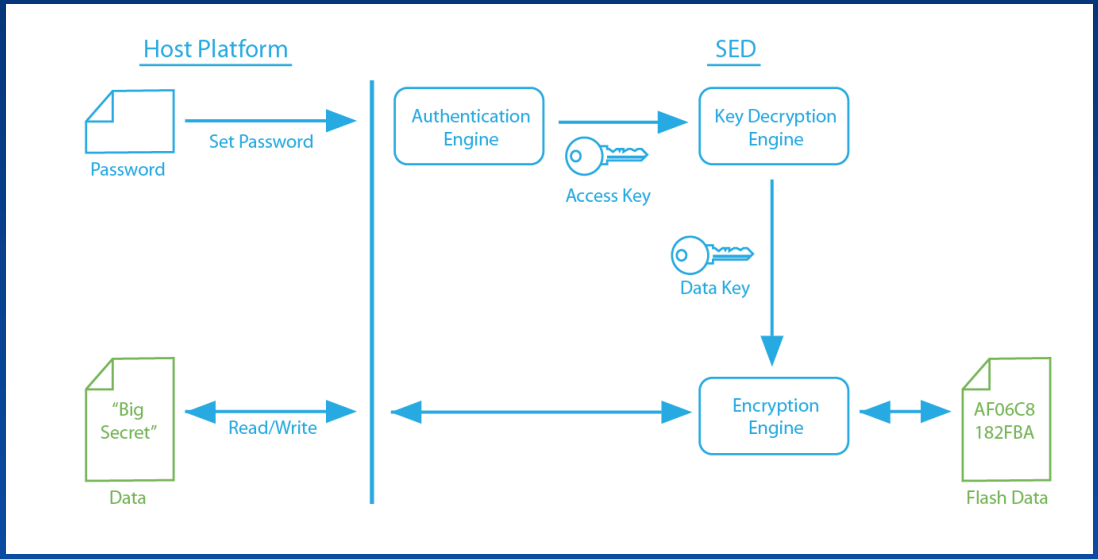
Software & Hardware - AES



- Ex: ATA Security, Proprietary, or TCG Opal (SED)

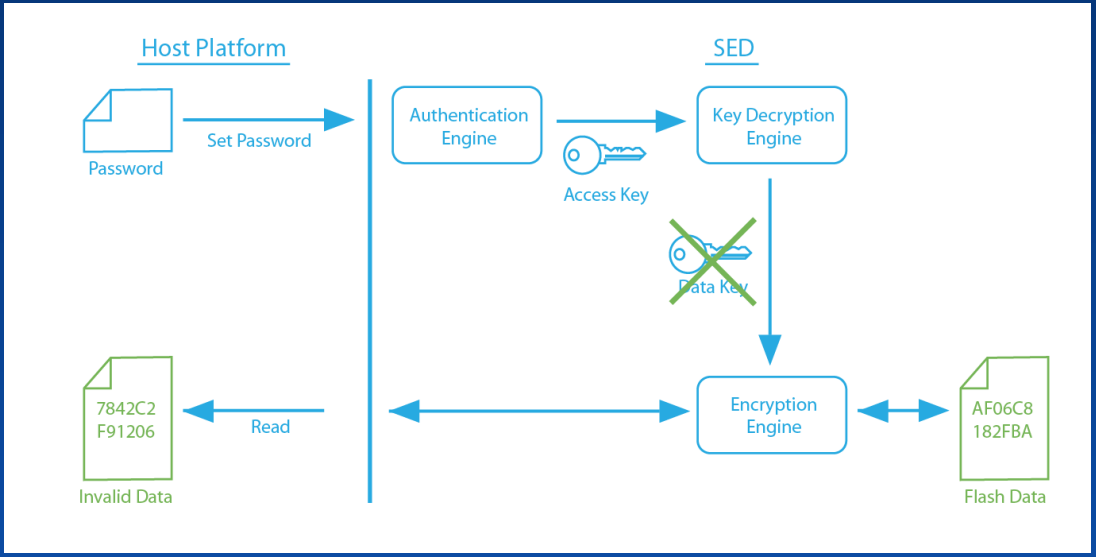
Software & Hardware – TCG Opal

- Requires AES 128/256
- Standard, but with ranges



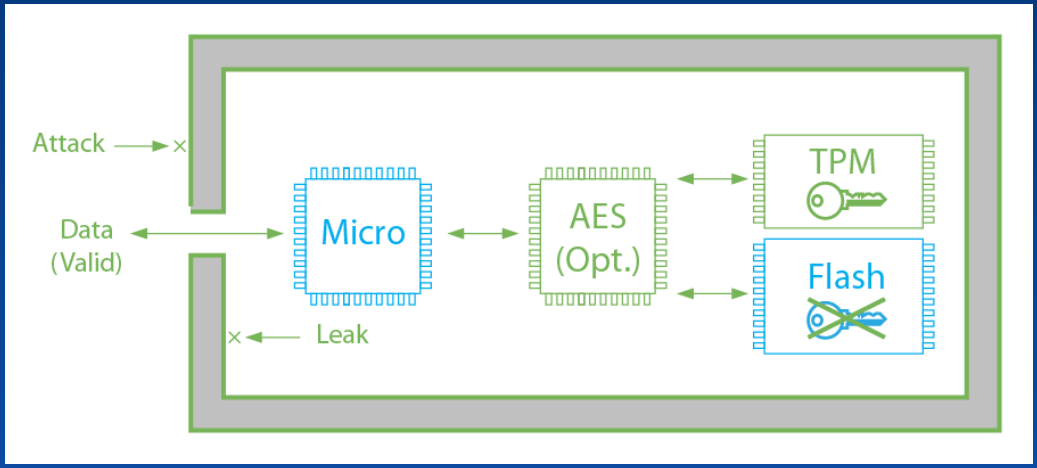
Software & Hardware – TCG Opal

- Cryptographic erase (fast)
- Challenge: Complex standard, limited BIOS support



Software & Hardware - TPM

- Hardware based protection and key store
- With or without AES
- True random number generator



Application – Use Case (1)

- Platform: Body Worn Camera
- Protection: Data
  - Finder of lost camera cannot access (view) data and cannot change data
- Solution:
  - Swissbit DP uSD Card with file encryption mode – secure recording

Application – Use Case (2)

- Platform: Cash Register
- Protection: Data
  - WORM recording with digital signature (audit trail)
  - Finder of lost card cannot change data
- Solution:
  - Swissbit WORM card (write once – read multiple) with hash chains and optional digital signature

Application – Use Case (3)

- Platform: Industrial PLC
- Protection: License Key
  - Host functionality unlocked with key in SSD
  - Key can't be cloneable and must be unique
- Solution:
  - Swissbit uSD cards, maintain the Key in an onboard Secure Element (SE)

Application – Use Case (4)

- Platform: IoT Gateway
- Protection: Code
  - Prevent unauthorized manipulation and dup
- Solution:
  - Swissbit PE microSD with full encryption and protection profile (access rules)

Conclusion

- Embedded Systems (and the SSD's used to realize them) present an ever increasing risk of being a TARGET due to the markets they serve (e.g., Energy, Aviation, Defense, etc.)
- As Embedded Systems continue to evolve in complexity and connectivity the ATTACK surface becomes larger and more vulnerable.
- Security SOLUTIONS realized at the SSD level can address a wide array of use cases (e.g., Trusted Boot, Data Protection, SW License Monetization, Audit Trails, Counterfeit Proection, etc.)
- Swissbit has a team of Security Storage EXPERTS ready to support your Embedded Systems Design needs.

Questions?

Grady Lambert - Director of Business Development
Swissbit
grady.lambert@swissbit.com