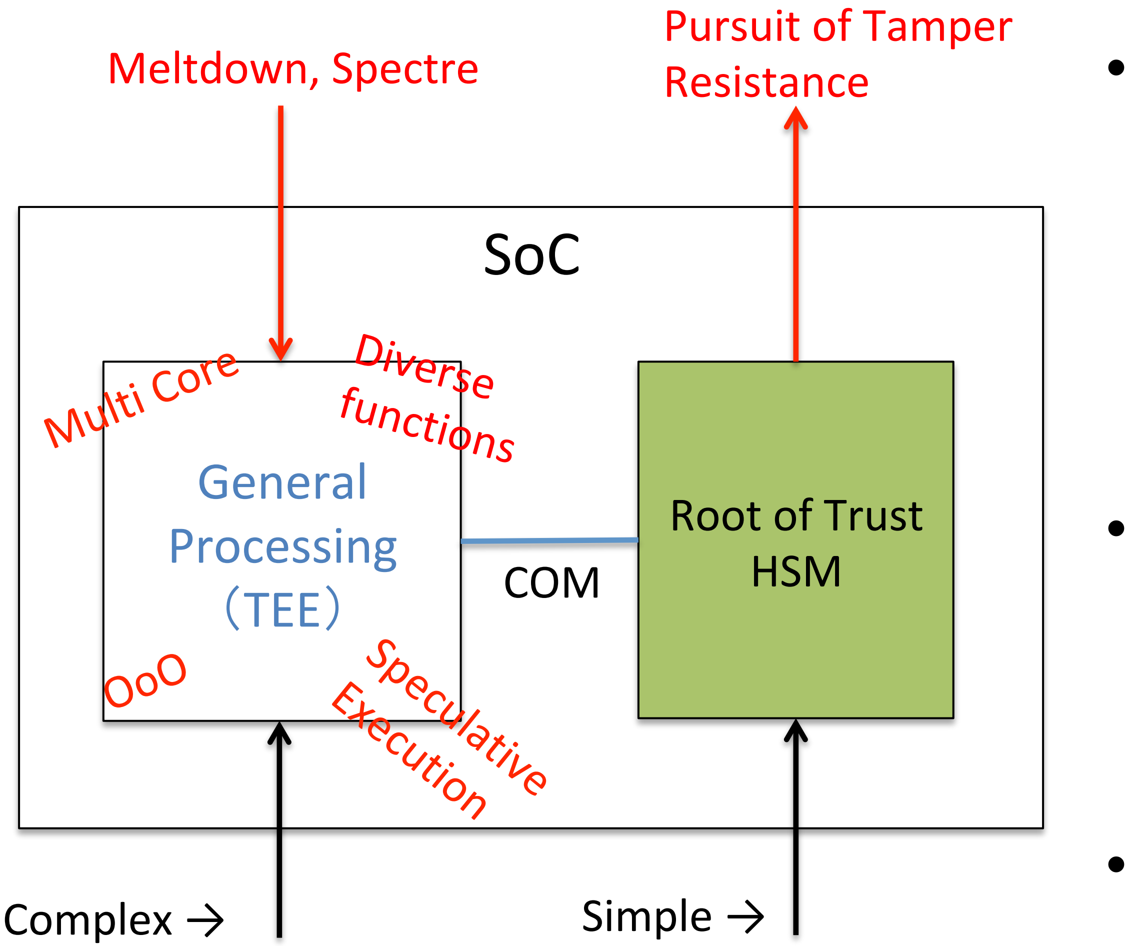
RISC-V Hardware Security Module for IoT Devices "CryptospeC"

September 27, 2019

SH Consulting K.K.
Shumpei Kawasaki

Root of Trust for SoC ==
Hardware Security Module (HSM)



Meltdown, Spectre

Pursuit of Tamper Resistance

SoC

Multi Core

Diverse functions

General Processing (TEE)

OoO

Speculative Execution

COM

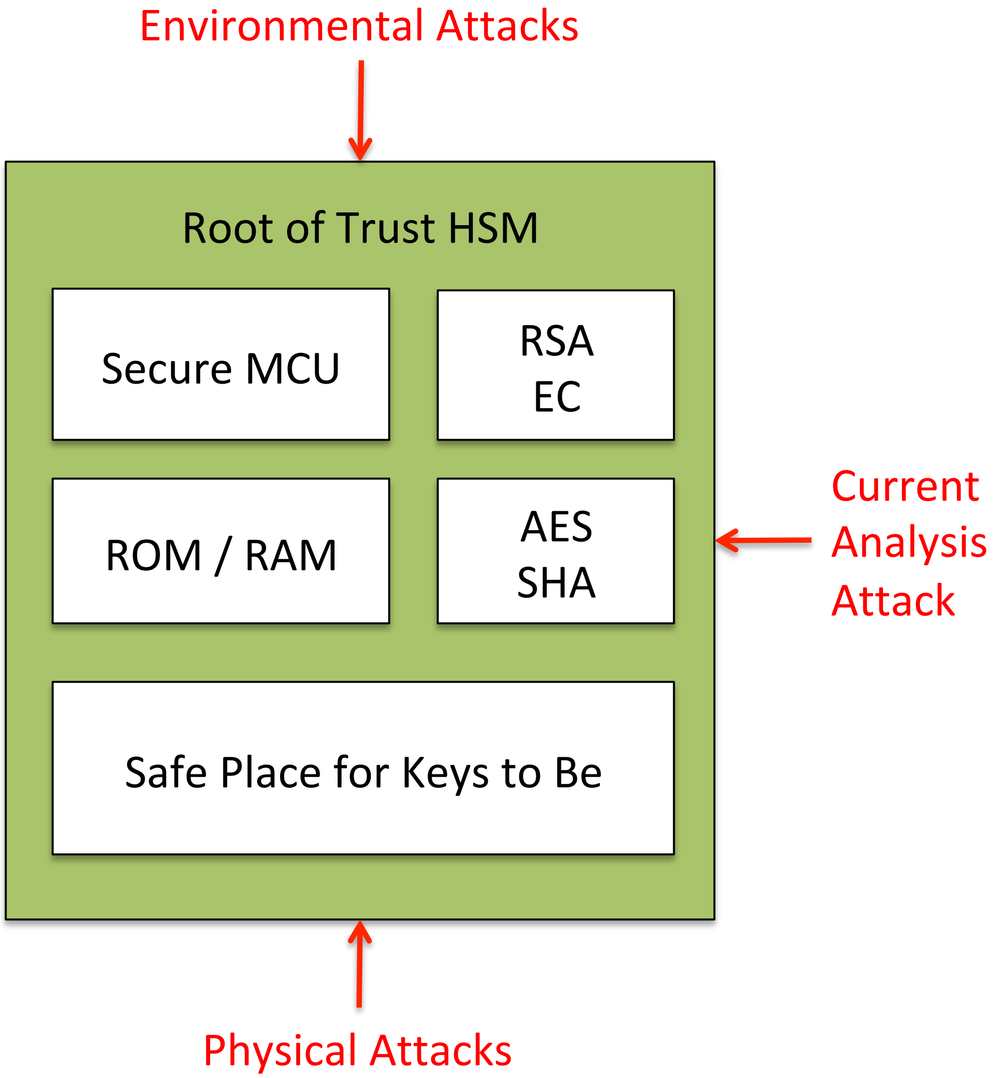
Root of Trust HSM

Complex →
Large Attack Surface →
Diverse Attack Methods →
Countermeasures Challenging

Simple →
Limited attack surface →
Countermeasure for each attack method can be exhaustively addressed individually

- Even if one tries to protect the general-purpose processing domain, the system is complex so one cannot exhaustively articulate how to protect it.
- It is more effective to separate the root of trust and protect a very simple system.
- The smartphone protects the entire system by creating several layers of protection based on the root of trust.

Trust HSM
= the world's smallest computer system

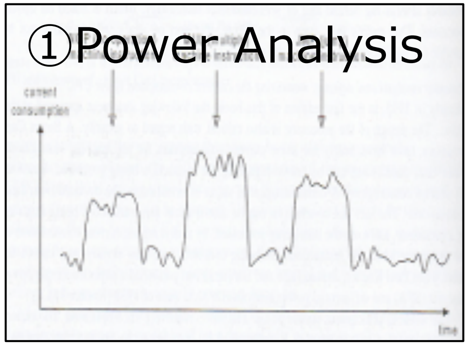


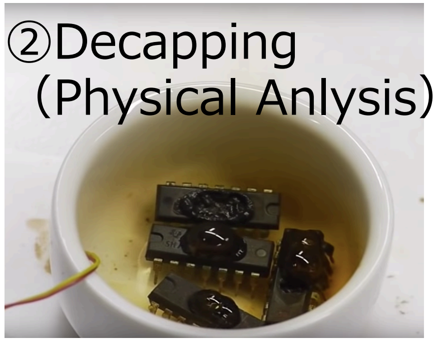
- Because HSM is simple, it can incorporate original ideas that are not hacked at the architecture, microarchitecture, and logic implementation levels.

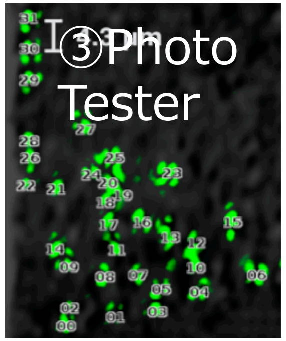
- By using RISC-V, all the above levels can be designed from scratch.

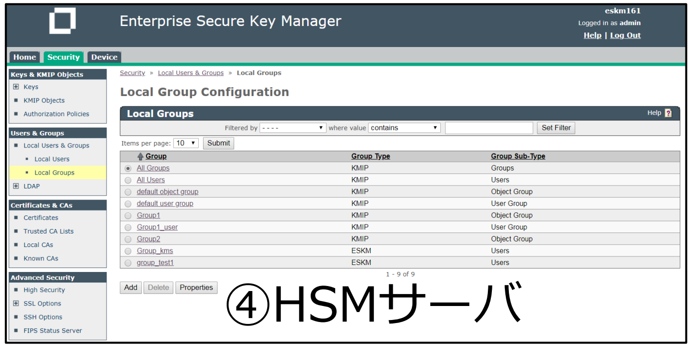
Root of Trust HSM: Attack costs vs. defense costs

- Attack cost example> $ 25K / device
- Defensive cost example <10 ¢ / device = hardware implementation + initial unique key
- The attack methods are categorized to cover the entire attack surface, and inexpensive attacks are dealt with firmly. Key usage is monitored by the HSM server to detect leaked keys. Zeroization.
- ① Side channel attack → Inexpensive
- = {Timing attack | Power analysis | Electromagnetic analysis}
- ②Chip opening type → expensive
- = {Probing analysis | Microprobe | Light irradiation | Luminescence analysis | FIB wiring editing | Layout rearrangement | Protection circuit destruction | Test circuit restoration}


①Power Analysis


②Decapping (Physical Anlysis)


③Photo Tester


Enterprise Secure Key Manager

eskm161
Logged in as **admin**
Help | Log Out

Security » Local Users & Groups » Local Groups

Local Group Configuration

Local Groups — Help

Filtered by - - - - where value contains [Set Filter]

Items per page: 10 [Submit]

	Group	Group Type	Group Sub-Type
●	All Groups	KMIP	Groups
○	All Users	KMIP	Users
○	default object group	KMIP	Object Group
○	default user group	KMIP	User Group
○	Group1	KMIP	Object Group
○	Group1_user	KMIP	User Group
○	Group2	KMIP	Object Group
○	Group_kms	ESKM	Users
○	group_test1	ESKM	Users

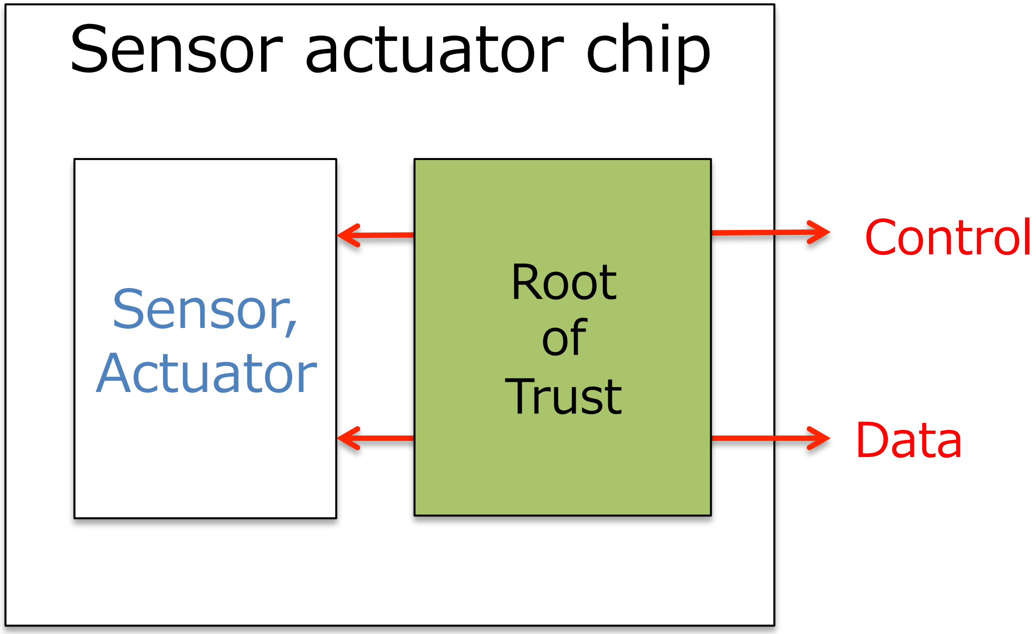
1 - 9 of 9

④HSMサーバ

出典：https://elearning.renesas.com/pluginfile.php/354/mod_folder/content/0/Board_ID/BoardID_RI_training_NR_03112010.ppt

出典：　https://youtu.be/uAINV-VXuq0
https://eprint.iacr.org/2017/822.pdf

Root of Trust for Sensor / Actuator

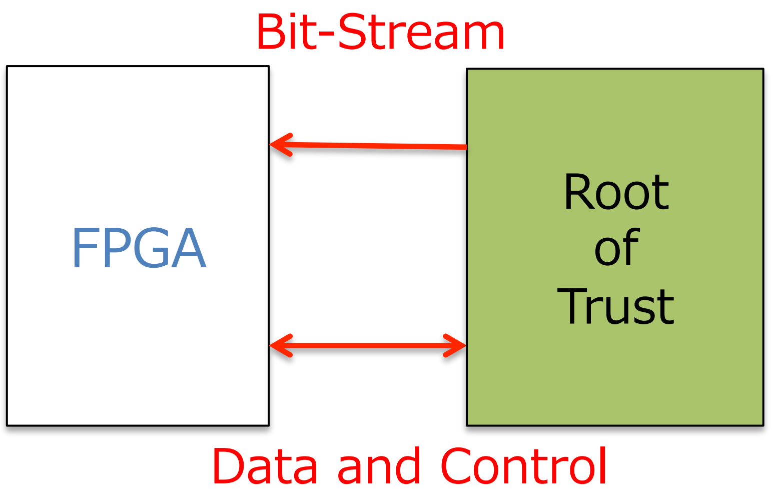


Sensors and actuators also require trust based on unique keys.

Root of Trust
Does not necessarily monitor the general-purpose processing domain. Sensor actuators can also be targeted.

- In addition to the general-purpose processing domain, sensor actuators also have a need to incorporate a route of trust.
  - Control signals and data signals are assets, and there is a need to protect them by encrypting them.
  - Monitors whether sensor / actuator is attacked. For example, have the surrounding devices been reconnected?
  - When an attack is detected, alerts, system shutdown, zeroization processing, etc. are performed.
  - Sensor actuator is also connected to the net。

HSM as a Root of Trust for FPGA

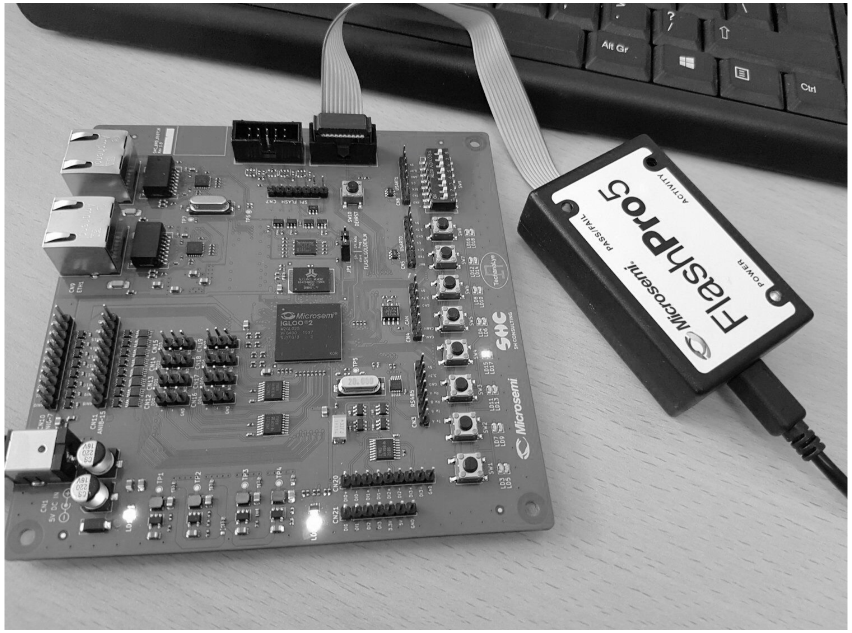


FPGA bitstream From route of trust according to specification

FPGA bitstream The specification has been elucidated.

- In addition to the general-purpose processing domain, FPGAs also have a need for embedded root of trust.
  - There is a need to protect the bitstream by encrypting it.
  - The FPGA bitstream specification has been elucidated.
  - FPGA partial reconfiguration can be used to increase security.

Conclusion



- Should the trust HSM be reprogrammable?
- If the hardware and firmware are minimal, the entire system can be verified. There can be ROM products.
- Built 32-bit RISC-V on FPGA and started verification of trust base HSM.
- Design an OS.
- Create an open source version to make it easy to embed.

Part of this result was obtained as a result of commissioned work by the New Energy and Industrial Technology Development Organization (NEDO).