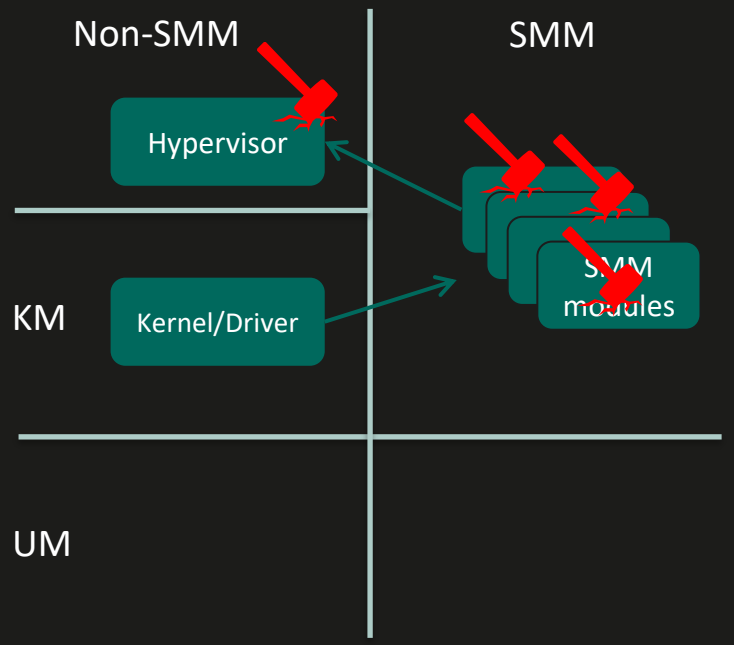
Voyage below the OS: SMM isolation on the Intel platform

Satoshi Tanda
Software Security Researcher

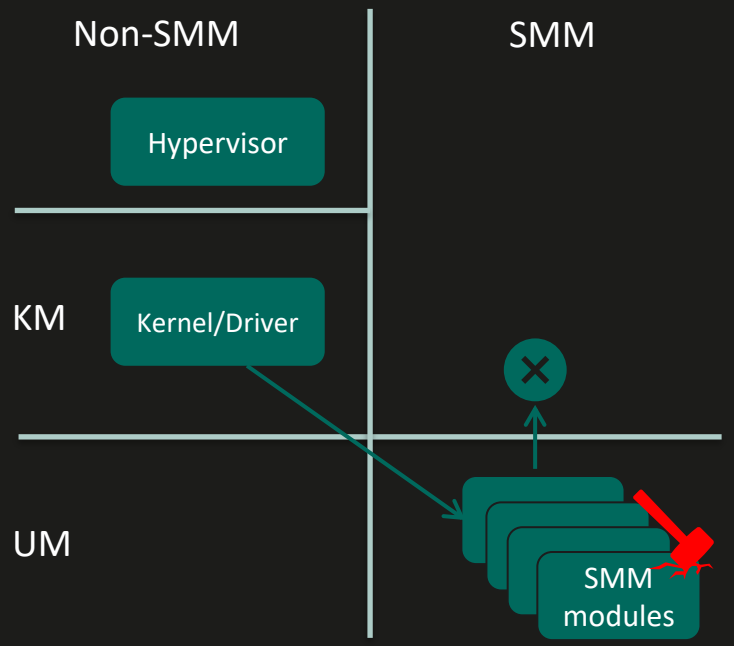
SMM – System Management Mode



SMM is:

- X86 operating mode
- More privileged than kernel or hypervisor
- Cannot be secured by kernel or hypervisor
- Reachable from kernel
- Exploited for many years

SMM isolation



Key ideas:

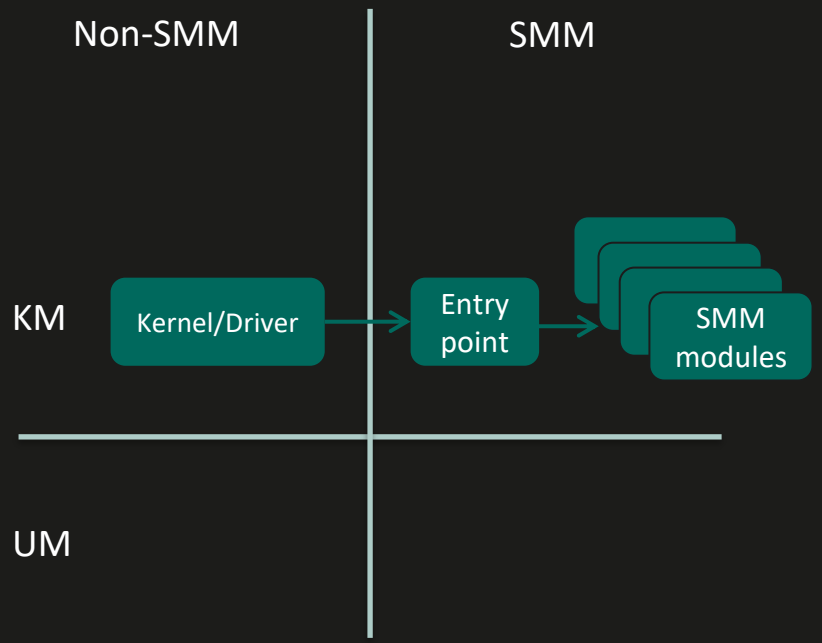
- Run SMM modules in user-mode
- Isolate impacts of vulnerabilities

Implementations:

- ISRD
- AMD supervisor

ISRD = Intel System Resource Defense

Traditional SMI handling



SMM execution flow:

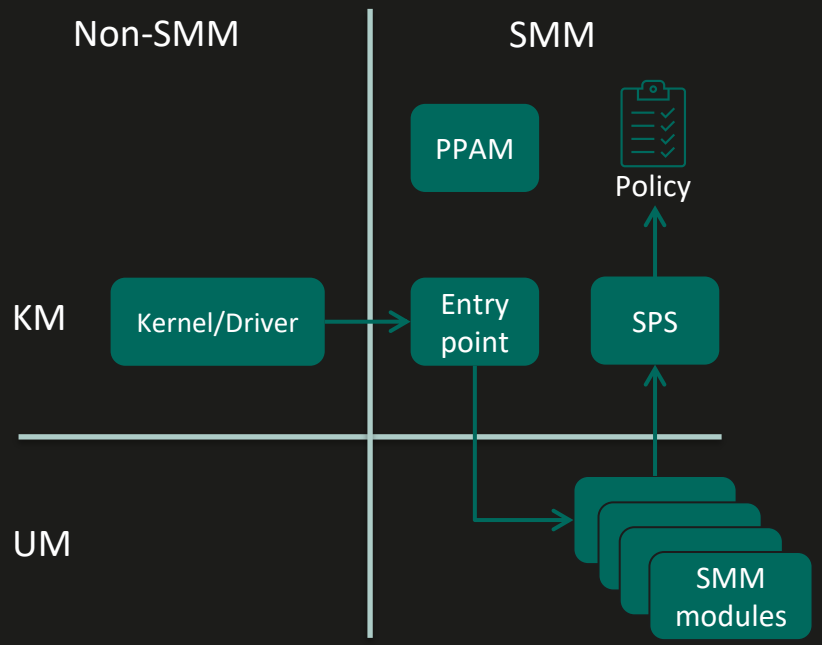
1. Kernel triggers SMI
2. Processor switches to SMM and runs the SMM entry point
3. The entry point runs SMM modules to handle the SMI
4. Processor returns to non-SMM

All in kernel-mode SMM.

SMI = System Management Interrupt

Safer SMI handling with ISRD

(Intel System Resource Defense)



With ISRD:

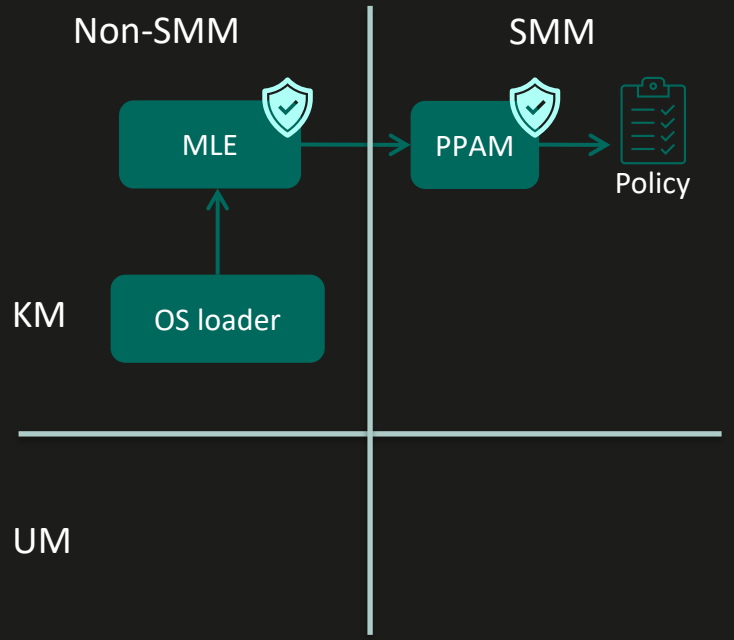
- SMM modules run in user-mode
- Only 3 kernel modules
  - SMI entry point
  - SMM policy shim (SPS)
  - Platform properties assessment module (PPAM)

SPS enforces a policy:

- Catches exception from user-mode SMM
- Allows or denies based on the policy

Trustworthy reporting with ISSR – Intel TXT

(Intel System Security Reporting)



Because the policy is customizable, it must:

1. ✔ be securely exposed and evaluated
2. remain available for other software in a tamper resilient manner

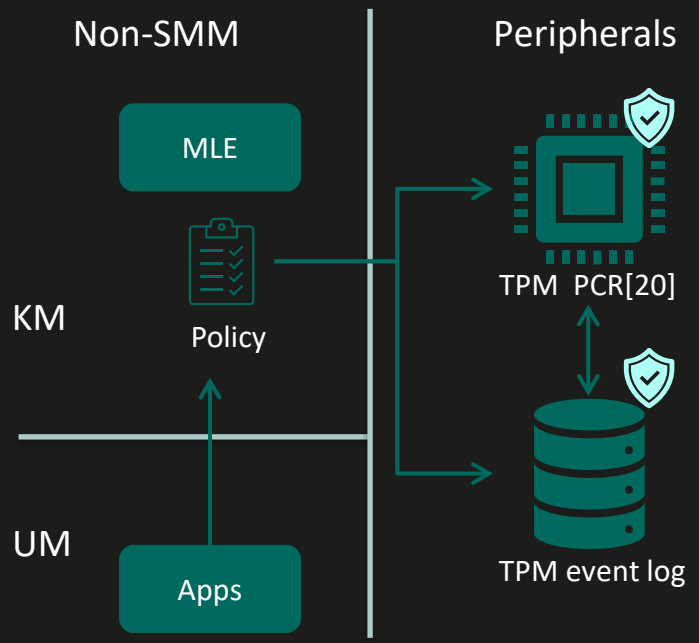
With Intel TXT:

- Integrity of MLE and PPAM is verified before execution
- MLE can ensure authenticity and receive the policy from PPAM, and evaluate it

TXT = Trusted Execution Technology
MLE = Measure Launch Environment

Trustworthy reporting with ISSR – TPM event logs

(Intel System Security Reporting)



Because the policy is customizable, it must:

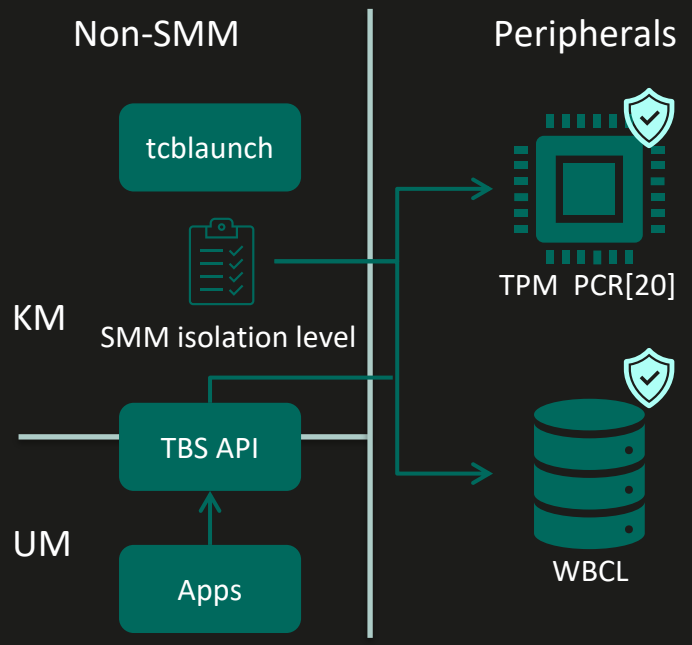
1. ✔ be securely exposed and evaluated
2. ✔ remain available for other software in a tamper resilient manner

With TPM:

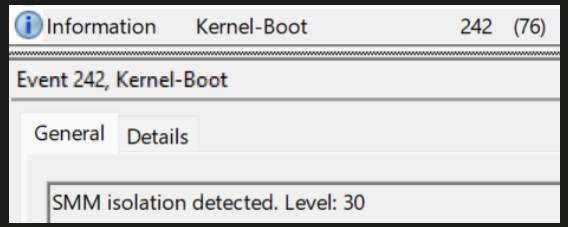
- Hash of the policy is stored in a tamper resilient manner
- Raw data is copied into TPM event logs, whose integrity can be ensured with TPM

TPM = Trusted Platform Module
PCR = Platform Configuration Register

Implementation on Windows



- ISSR is called SMM Firmware Measurement
- Tcblaunch.exe is MLE and summarizes the policy into "SMM isolation level", which is:
  - Stored into WBCL, readable with TPM Base Services as SIPAEVENT_DRTM_SMM_LEVEL
  - Logged in Event Viewer (ID=242)



  - Exposed through WMI (24H2+)

(Get-CimInstance -ClassName Win32_DeviceGuard -Namespace root/Microsoft/Windows/DeviceGuard).SmmIsolationLevel

WBCL = Windows Boot Configuration Logs

Call for actions

Defenders:

- Look into WBCL for SMM security and boot visibility
- Learn the security architecture for inspiration

Attackers:

- Study,
  - SPS's user-mode input handling
  - OEMs' security policies
  - Relevant work against AMD implementation by Enrique, Krzysztof, Joseph and Ilja of IOActive
- Analyze PPAM's attack surface

About me

Satoshi Tanda

- in/satoshitanda
- @satoshi_tanda@infosec.exchange
- @standa_t
- @tandasat

Questions?