System Management Mode Mitigations and Development Platforms

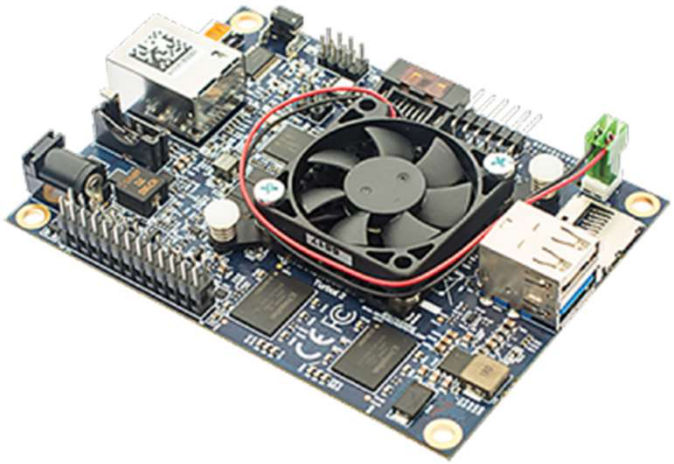
Brian Delgado

March 16, 2023

Background

- Red Team Lead for the Programmable Solutions Group at Intel Corp
- Research interests:
  - The intersection of security and performance
  - Supervisor operation modes (Intel System Management Mode, Intel SMI Transfer Monitor)
  - Virtualization
  - Firmware Fuzzing

Firmware Security



Intel Minnowboard

Firmware is widely present on computing devices from PC's, phones, to FPGAs

On x86 platforms, runtime firmware is executed in System Management Mode (SMM)

SMM can be entered transparently to the operating system / hypervisor via an "SMI" interrupt

General rule of thumb is to keep SMI durations to ~150 microseconds. *Paper: "Performance Implications of SMM" (Delgado, Karavanic, IEEE S&P 2013).*

SMM is highly privileged, has traditionally had full access to CPU register state, memory, and devices.

Improving SMM security needs a multi-faceted approach

Holistic View for SMM Security

Architectural

Principle of least privilege:

- SMM Page table isolation
- Intel Runtime BIOS Resilience
- Intel System Resources Defense
- STM…

Attack Surface Reduction

Evaluate whether SMM modules need to be in SMM

Secure Coding

Leverage CommBuffer, ASLR, Guard pages, SMM Code Access Check, etc …

Firmware Bill of Materials

Do codebases / images have known vulnerabilities?

Config

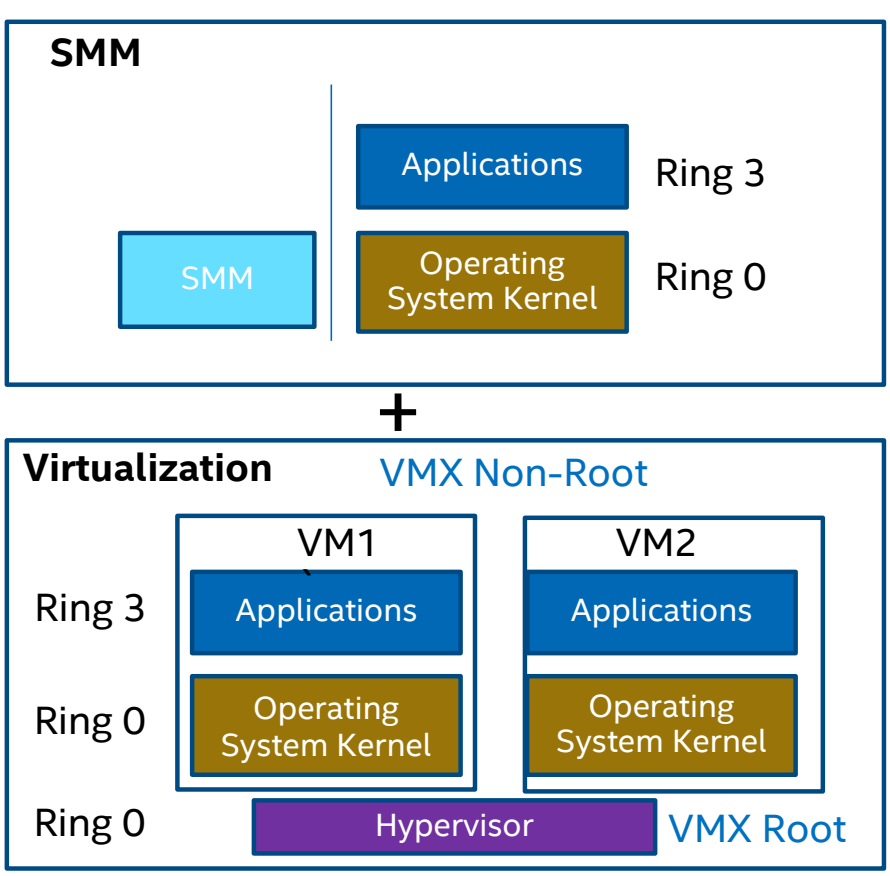
Is BIOS setting the appropriate lock bits? Run CHIPSEC to see.

Static Analysis / Fuzzing

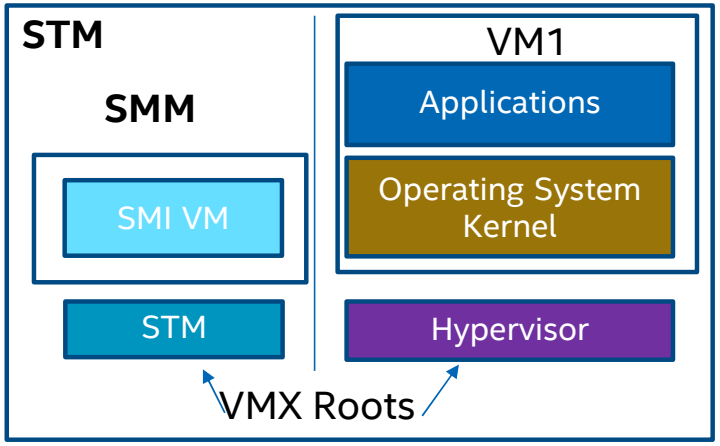
Fuzzing / symbolic execution / static analysis to identify vulnerable code.

One fuzzing tool: HBFA (edk2-staging)

SMM + Virtualization = STM



=



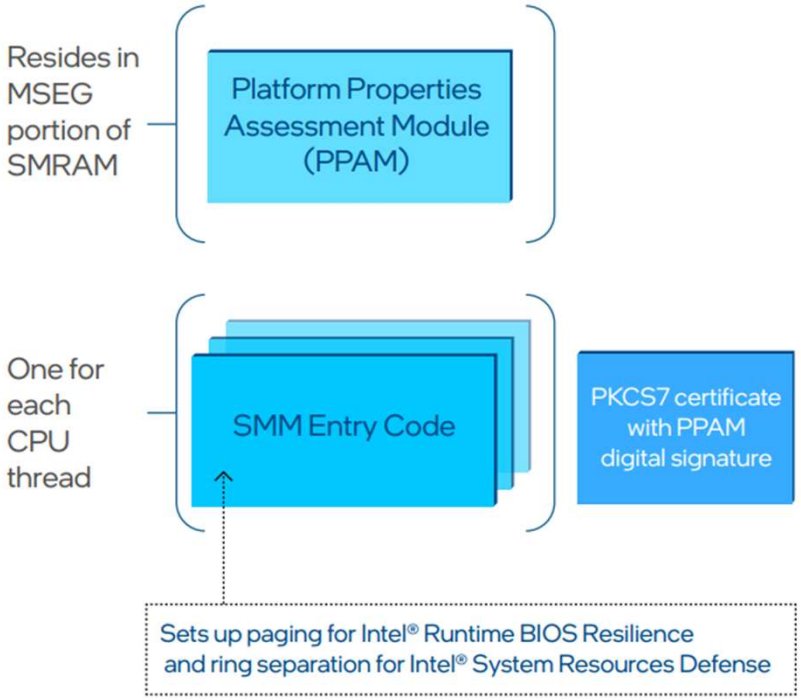
STM Purpose:

Apply protection policy over SMI code to prevent broad access to host-side **memory, registers, PCIe, IO Ports, MSRs**

Enabled in coreboot, STM is open-source

Architectural

SMM Mitigations for Intel vPro Platforms



Intel Hardware Shield: Provides ability to lock SMM page tables

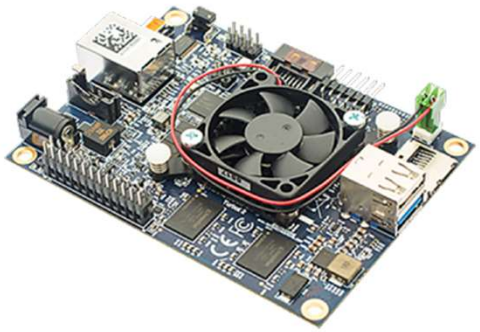
Intel System Resources Defense: Enforces policy on SMI handler accesses (beyond memory) via ring 0 and ring 3 separation in SMM

Intel System Security Report ("PPAM"): With TXT, provides a report on the policy in place for SMI handler accesses

Architectural

https://cdrdv2-public.intel.com/756963/DRTM-based-computing_whitepaper_FINAL_MAY2021.pdf

Development Platforms



A few thoughts on development platforms:

The Intel Minnowboard (circa 2014) had several useful capabilities:

- Open-source firmware (EDK2 with optional FSP, coreboot)
- Dediprog header for easy firmware recovery
- Serial port for debug info
- JTAG header
- Intel Silvermont Atom CPU, could run off-the-shelf Linux or Windows.

What would make it better?

- Higher performance CPU, more modern CPU features
- > 2 GB RAM
- More I/O options (only 1 SATA, NVME not easy, 1 GBE)
- Availability (no longer produced)

Developer-friendly platforms enable advanced prototypes for universities/others

Discussion / Questions?

Additional Resources

- SMM Protection in EDK2: Jiewen Yao - SMM Protection in EDKII_Intel (uefi.org)
- STM User Guide: https://www.intel.com/content/dam/develop/external/us/en/documents/stm-user-guide-001-819978.pdf
- STM Code: jyao1/STM (github.com)
- Community-developed STM launcher code: Xen, Linux
- Intel Hardware Shield: DRTM-based-computing_whitepaper_FINAL_MAY2021.pdf
- HBFA (Fuzzing): Host Based Firmware Analyzer · tianocore/tianocore.github.io Wiki

Notice

“Intel provides these materials as-is, with no express or implied warranties. All products, dates, and figures specified are preliminary, based on current expectations, and are subject to change without notice. The products described might contain design defects or errors known as errata, which might cause the product to deviate from published specifications. Current, characterized errata are available on request. Intel technologies might require enabled hardware, software, or service activation. Some results have been estimated or simulated. Your costs and results might vary. No product or component can be absolutely secure. © Intel Corporation. Intel, the Intel logo, and other Intel marks are trademarks of Intel Corporation or its subsidiaries. Other names and brands might be claimed as the property of others.”