

## Summary of A Coprocessor-Based Introspection Framework Via Intel Management Engine, Lei Zhou, Fengwei Zhang, Jidong Xiao, Kevin Leach, Westley Weimer, Xuhua Ding, and Guojun Wang

To detect low-level malware, virtualization-based defensive approaches and hardware-assisted defensive approaches have been proposed. They contain limitations:

- Limitations in virtualization:
  - additional software layer
  - significant performance overhead
  - large Trusted Computing Base (TCB)
- Limitations in hardware:
  - require either an external monitoring device or a specialized CPU support for examining state such as Intel System Management Mode (SMM)
    - increases costs and precludes large-scale deployment.
  - running code in SMM requires the CPU to perform an expensive context switch from the OS environment to SMM.
    - this suspension of execution results in abnormalities that are detectable from the OS context. Attackers can measure and exploit such abnormalities to escape detection or hide malicious activities.

### NIGHTHAWK

2 Goals:

- Checking the integrity of kernel and hypervisor structures and system firmware
- Monitoring the system state (analyze the state of processes, resource usage (e.g., memory, cache, imports, interrupts) of runtime applications).

Advantages:

- No extra hardware required
- High privilege
- Small TCB
- Low overhead
- Transparency

Limitations:

- Performance heavily depends on the hardware design of the IME

### Intel Management Engine (IME)

Subsystem which includes a separate microprocessor, its own memory, and an isolated operating system.

- Integrated into Intel x86 motherboards since 2008.
- To contact with isolated IME from host system, Intel designed the Host Embedded Controller Interface (HECI, also called Management Engine Interface) to secure exchange data between host memory and IME.
- IME is said to have ring -3 privilege.

Due to the resource-constrained nature of the IME processor, it is more efficient to dump memory from the Target Machine and use the Remote Machine to perform more computationally expensive analyses.

To change the behavior of the IME they:

- adopt a memory-remapping approach: essentially, the external IME RAM is made accessible by the Target Host by configuring several system registers that influence memory mapping.
- They inserted introspection code while maintaining the original functionality (e.g., with trampolines).
- With kernel-level access, it is possible to reuse those memory control registers to remap and subsequently alter the IME-reserved memory region and SMRAM. This could potentially allow attackers to compromise NIGHTHAWK. To close the injection vector after they inserted the introspection code into the IME and SMRAM, they implemented a lock mechanism on those memory control register by leveraging Intel TXT.
- After rebooting, the custom IME and SMM code remains intact because booting into TXT mode prevents the memory control registers from being modified.

Since the IME processor cannot address the host memory directly, two extended transfer engines — Direct Memory Access (DMA) and Host Embedded Controller Interface (HECI) — are used for data transmission between the IME memory and the Target Host memory.

### System Management Mode (SMM)

Used to handle system-wide functions such as power management or vendor-specific system control.

- The code and data used in SMM are stored in a hardware-protected memory region named SMRAM.
- SMM code is executed by the CPU upon receiving a System Management Interrupt (SMI).