CSC 6991: Using Hardware Isolated Execution Environments for Securing Systems

Fengwei Zhang

Overview

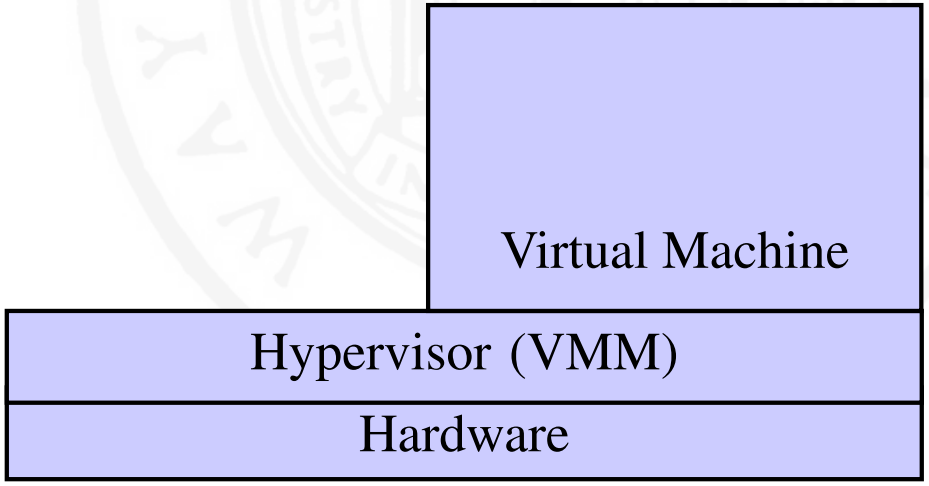
- Concept of Isolated Execution Environments
- Isolation of data/code
  - CPU
  - Memory
  - Disk
  - Input/output devices

Overview

- Software isolated execution environments
  - Virtualization technology
- Hardware isolated execution environments
  - SMM on x86
  - ARM TrustZone
  - Software Guard Extension (SGX)
  - TCG (SRTM and DRTM)
  - Intel Active Management Technology (AMT) and Manageability Engine (ME)
  - AMD Platform Security Processor (PSP)

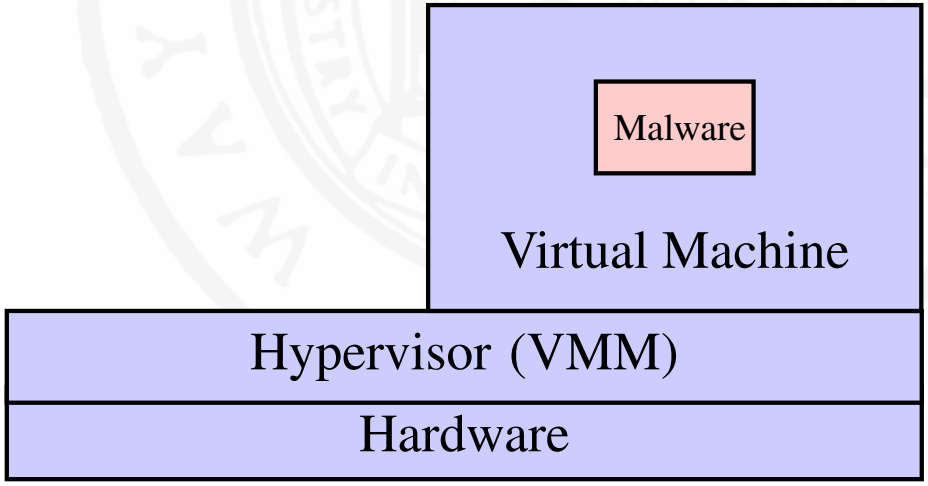
Virtualization

- Using virtualization technology to create an isolated execution environment for malware detection/analysis



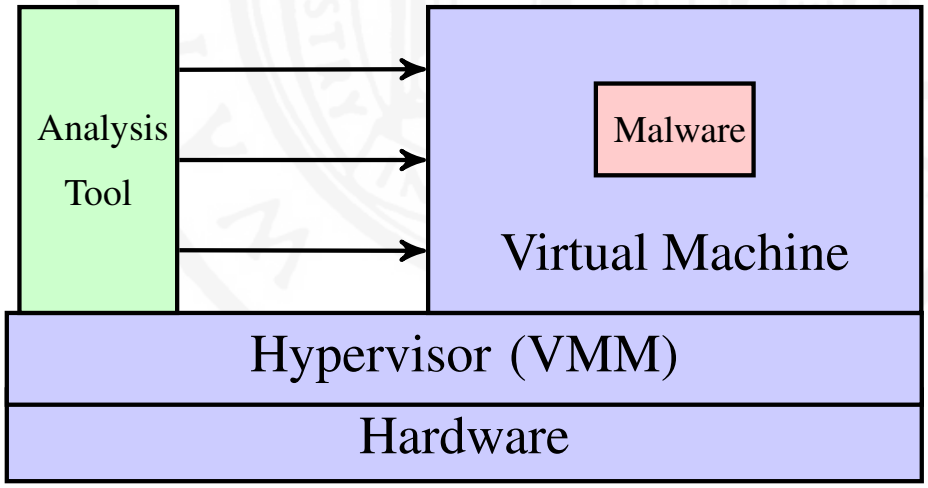
Virtualization

- Using virtualization technology to create an isolated execution environment for malware detection/analysis



Virtualization

- Using virtualization technology to create an isolated execution environment for malware detection/analysis

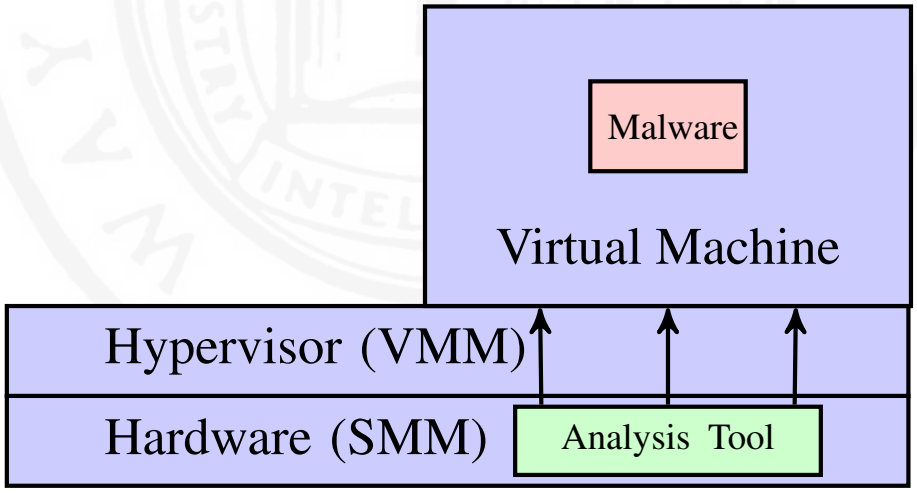


Virtualization

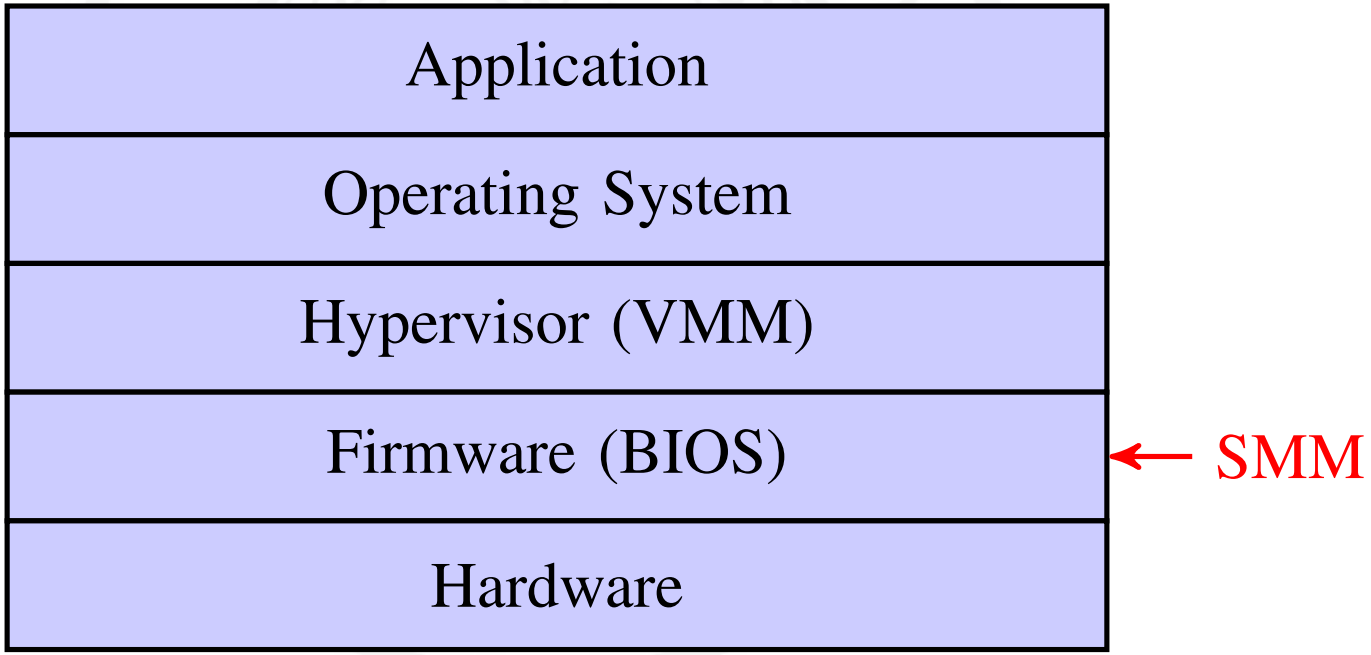
- Limitations
  - Depending on hypervisors that have a large TCB (e.g., Xen has 500K SLOC and 245 vulnerabilities in NVD)
  - Incapable of detecting rootkits with the same or higher privilege level (e.g., hypervisor and firmware rootkits)
  - Unable to analyze malware with anti-virtualization or anti-emulation techniques
  - Suffering from high overhead on system performance

Hardware Isolated Execution Environments

- Moving analysis tools from hypervisor-layer to hardware-layer to addresses the limitations



Software Layers

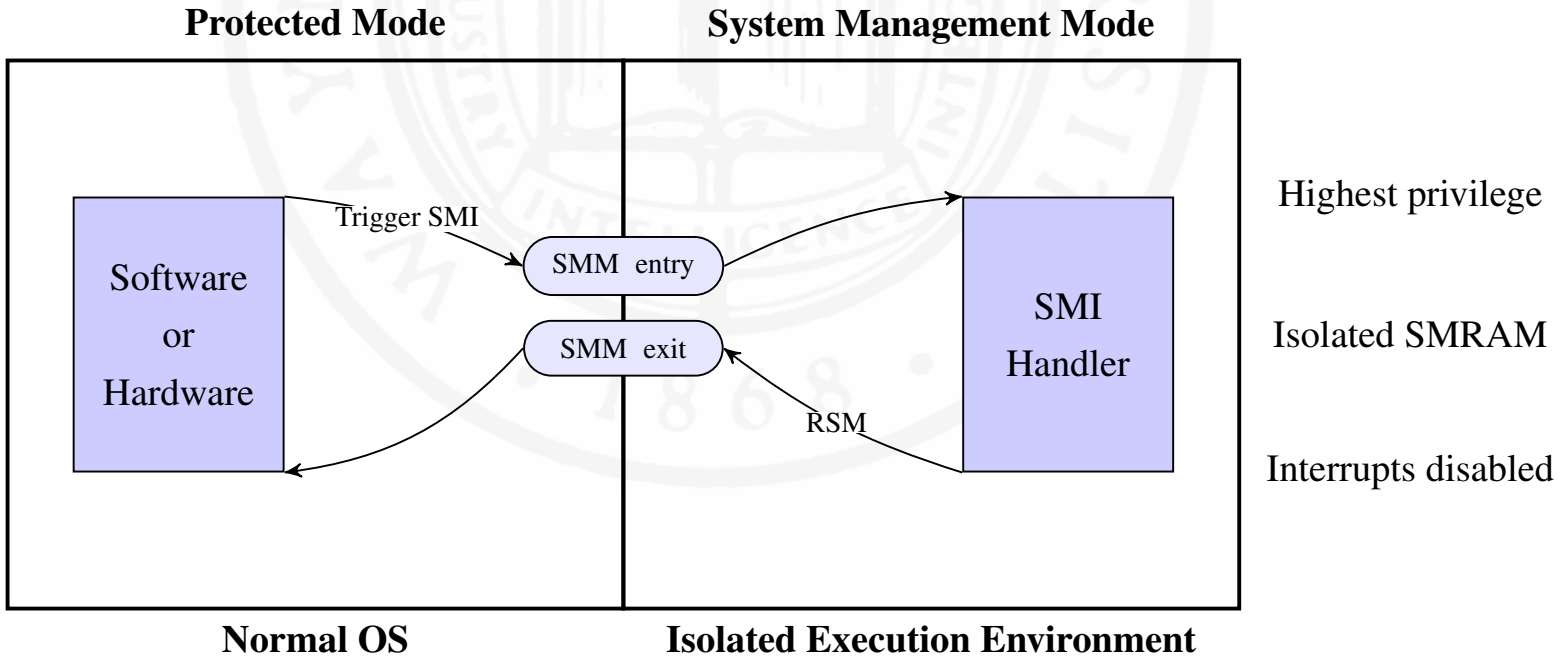


System Management Mode

- System Management Mode (SMM) is special CPU mode existing in x86 architecture, and it can be used as a hardware isolated execution environment.
  - Original designed for implementing system functions (e.g., power management)
  - Isolated System Management RAM (SMRAM) that is inaccessible from OS
  - Only way to enter SMM is to trigger a System Management Interrupt (SMI)
  - Executing RSM instruction to resume OS (Protected Mode)

System Management Mode

- Approaches for Triggering a System Management Interrupt (SMI)
  - Software-based: Write to an I/O port specified by Southbridge datasheet (e.g., 0x2B for Intel)
  - Hardware-based: Network card, keyboard, hardware timers



Use Cases

- Malware detection
  - Memory attacks detection
  - Next class will provide details
- Malware Analysis
  - Transparent malware debugging
    - Class on Sep 16: malware on desktop
    - Class on Sep 24: malware on mobile phones
- Execution sensitive operations/workloads
  - Password login

Hardware Isolated Execution Environments

- SMM on x86
- ARM TrustZone
- Software Guard Extension (SGX)
- TCG (SRTM and DRTM)
- Intel Active Management Technology (AMT) and Manageability Engine (ME)
- AMD Platform Security Processor (PSP)

Term Project Discussion

- Using a hardware isolated execution environments for a security task
  - Choose an environment
  - Identify a task
    - Attacks detection
    - Analyzing a type of malware
    - Memory forensics

Review Discussion

- Lucas Copi
- CSC 6991 Advanced Computer Security
- **Isolated Execution Environments**

- The paper *Using Hardware Isolated Execution Environments for Securing Systems* by Fengwei Zhang focuses on new methods for malware detection and analysis. The paper provides background into the field by describing the adoption of Virtual Machine Introspection and its limitations. Mainly: that Virtual Machine Introspection exhausts system resources and is vulnerable to malware that runs at a higher privilege level than that of the virtualized system.

- The paper discusses using System Management Mode as a more secure and more efficient alternative to VMI. The paper explains in detail the process by which SMM separates the trusted OS and the untrusted OS in the hardware, runs the detection module, and reports the results.

- After laying the groundwork for the technology and implementation the paper details two new technologies called HyperCheck I and HyperCheck II. It shows the process by which these systems based on SMM can scan, detect, and prevent malware attacks on a host system. The paper also compares performance overheads between the SMM based systems and VMI to show the increased efficiency of the SMM based system.

Review Discussion

- Zhenyu Ning
- CSC 6991 Advanced Computer Security
- **Isolated Execution Environments**

- The paper mainly talks about researches on system security using isolated execution environment. A special CPU mode named System Management Mode, which has a minimal TCB and low performance overhead, is introduced to prevent security operations and sensitive data from being detected by malware. Several SMM-based systems working on malware detection, transparent malware debugging and sensitive workload execution are then detailed to illustrate the advantage and importance of this special CPU mode to the system security researches. From my standpoint, comparing with other isolated execution environment technology, SMM has many advantages such as small TCB, low overhead, OS insensitive and so on, but a small flaw is its CPU architecture sensitivity. x86 architecture needs SMM and ARM needs TrustZone, and we can generally predict that new CPU architecture also need new solution to implement reliable isolated execution environment, which may take additional cost for both CPU manufacturers and researchers.

Review Discussion

- Porpaavai Sampath Kumar
- CSC 6991 – Advanced Security
- **Isolated Execution Environments Summary**

- The research paper, *Using Hardware Isolated Execution Environments for Securing Systems* by Fengwei Zhang deals primarily with efficiently running security modules in an isolated environment utilizing System Management Mode (SMM), a special CPU mode.

- The researcher developed multiple systems utilizing the SMM properties to ensure that the malicious malware does not compromise the isolated environments, and to alert the user if it is compromised. For example, Spectre pauses the current running OS briefly to run the security modules and alerting the user to any potential malware using a “heartbeat” signal.

- The researcher also designed a debugging system that also utilizes the capabilities of the SMM. Finally, the researcher utilized the SMM properties to implement a secure login system and implement a system that manages the isolated environment and allows smooth transition between the operating systems. For all systems, the researcher details the architecture and the comparable performance against other common and popular systems.

Review Discussion

- Hitakshi Annayya
- CSC 6991 – Advanced Security
- **Isolated Execution Environments for Securing Systems**

- The thesis/research paper, *Using Hardware Isolated Execution Environments for Securing Systems* by Fengwei Zhang handles all the four limitations of the existing virtualization-based approaches for malware deduction and debugging. Traditional method is Virtual Machine Introspection (VMI) that has been universally adopted to handle malware detection and analysis.

- The proposed and experimented method deals with System Management Mode (SMM) to handle malware security operations. Developed 3 tools in SMM which detects the attack in all the different layers of the system software. Firmware-level, HyperCheck operation, Spectre framework for diff platforms.

- With the help of SMM, transparent malware debugging is also achieved (MalT). Implementing the design of TrustLogin doesn't reveal the login credentials to any attackers in the commodity operating systems.

Reminder

- Mailing-list: csc6991 [at] lists [dot] wayne.edu
- Introduce your self for homework 0
- Write paper reviews before class
- Email your topics/papers to the mailing-list before the class on Monday, Sep 14