04 reference monitors

2024年8月26日 星期一 13:29

week3

Australian National University

Reference Monitors & Hardware Security

COMP2700 Cyber Security Foundations

Prepared based on: Gollmann, D. Computer Security, 3rd Edition. Chapter 6.

Australian National University

Outline

- Reference monitor, security kernel, and TCB
  - Placing the reference monitor
- Protection rings & controlled invocation
- Memory management and access control
  - Historical example: Intel x86 protection mechanism
- Overview of hardware-based threats and defence.

Australian National University

Security Mechanism

- How can computer systems enforce operational policies in practice?
- Questions that have to be answered:
  - Where should access control be located?
  - Are there any additional security requirements your solution forces you to consider?

Australian National University

Reference Monitor (RM)

Reference monitor:	access control concept that refers to an abstract machine that mediates all accesses to objects by subjects.
Security Kernel:	hardware firmware, and software elements of a TCB that implement the reference monitor concept.
Trusted Computing Base (TCB):	The totality of protection mechanisms within a computer system – including hardware, firmware, and software – the combination of which is responsible for enforcing a security policy.

Australian National University

Requirements of RM

Complete mediation	• The reference validation mechanism must always be invoked.
Tamper-proof	• The reference validation mechanism must be tamper-proof.
Verifiable	• The reference validation mechanism must be small enough to be analysed and tested.

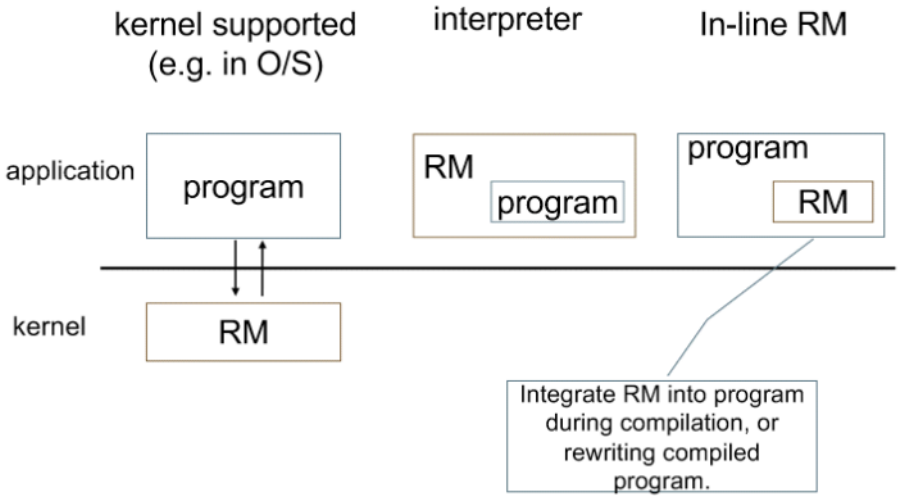
Australian National University

Placing the RM

- **Hardware**: access control mechanisms in microprocessors
- **Operating system kernel**: e.g. hypervisor, i.e. a virtual machine that emulates the host computer it is running on.
- **Operating system**: e.g. access control in Unix and Windows 2000.
- **Services layer**: e.g., access control in database systems, Java Virtual Machine, .NET Common Language Runtime, Android application framework.
- **Application**: security checks in the application code to address application specific requirements.

Australian National University

RM: Design Choice



Australian National University

Operating System Integrity

- Assume that your O/S prevents unauthorized access to resources (as long as it works as intended).
- To bypass protection, an attacker may try to disable the security controls by modifying the O/S.
- An **integrity problem:** the O/S is not only the arbitrator of access requests, it is itself an object of access control.
- **Security policy: Users must not be able to modify the operating system.**

- **完整性问题**:
  - 操作系统不仅是访问请求的仲裁者，本身也是需要受保护的对象。如果操作系统被攻击者修改，整个系统的安全性将受到威胁。

Australian National University

Operating System Integrity

- Two competing requirements.
  - Users should be able to use (**invoke**) the O/S.
  - Users should not be able to misuse the O/S.
- Two important concepts commonly used to achieve these goals are:
  - status information (able.)
  - **controlled invocation**, also called restricted privilege
- These concepts can be used in any layer of an IT system, be it application software, O/S, or hardware.

- **状态信息（Status Information）**：
  - 系统维护状态信息，以确保在任何时候都可以检查当前状态，从而防止未经授权的操作。这通常包括跟踪用户会话、进程状态和系统资源的使用情况。
- **受控调用（Controlled Invocation）**，又称**受限特权（Restricted Privilege）**：
  - 受控调用是一种机制，确保用户只能在**受限权限**下调用操作系统功能，防止滥用系统资源。
  - 例如，通过权限管理和访问控制列表（ACL），用户只能访问被授予的资源和功能。
  - 这一概念通常用于限制用户对系统关键部分的访问，防止其进行越权操作。

Australian National University

Modes of Operation

- To protect itself, an O/S must be able to distinguish computations ‘on behalf’ of the O/S from computations ‘on behalf’ of a user.
- **Status flag** allows system to work in different **modes**.
  - Intel 80x86: two status bits and four modes
  - Unix distinguishes between *user* and *superuser* (root)

Australian National University

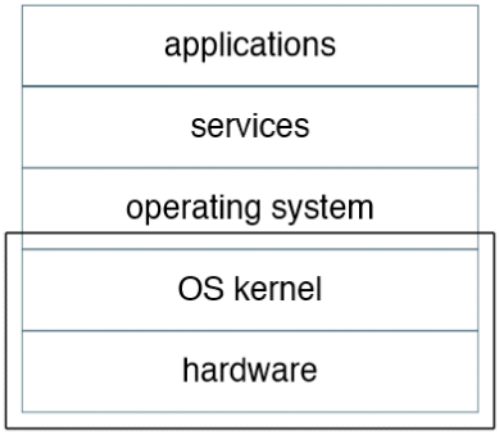
Controlled Invocation

- To prevent users from corrupting sensitive part of memory, the O/S grants write access to memory locations only if the processor is in supervisor mode.
- If a user needs to access its own memory segment, the system has to switch to the supervisor mode, but mediate the access in a controlled way.
- Controlled invocation: Invocation of a function that executes privileged instructions to provide a limited, well-defined functionality, and then return to user mode.

目的：防止用户**篡改内存的敏感部分。**操作系统只在处理器处于**超级模式（supervisor mode）**时授予内存写入权限。

Australian National University

Core Security Mechanisms



Australian National University

Why Mechanisms at the Core?

use min command to build a computer
↳ 可以更改成你 u need

- For security evaluation at a higher level of assurance.
  - Security mechanisms in a given layer can be compromised from a layer below.
  - To evaluate security, you must check that security mechanisms cannot be bypassed.
- Putting security mechanisms into the core of the system can reduce performance overheads caused by security.

为了更高的安全保障

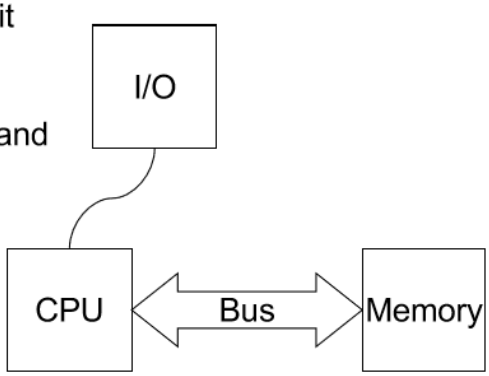
降低安全机制带来的性能开销

Australian National University

Computer Architecture

Simple schematic description:

- central processing unit (CPU)
- memory
- bus connecting CPU and memory
- input/output devices



Australian National University

Core CPU Components

- **Registers**: general purpose registers and dedicated registers like:
  - **program counter**: points to the memory location containing the next instruction to be executed.
  - **stack pointer**: points to the top of the system stack.
  - **status register**: here CPU keeps essential state information.
- **Arithmetic Logic Unit (ALU):** executes instructions given in a machine language; executing an instruction may also set bits in the status register.

Australian National University

Memory Structures

Security characteristics of different types of memory:

- RAM (random access memory): read/write memory; no guarantee of integrity or confidentiality.
- ROM (read-only memory): provides integrity but not confidentiality; ROM may store (part of) the O/S.
- EPROM (erasable & programmable read-only memory): could store parts of the O/S or cryptographic keys.
- WROM (write-once memory): memory contents are frozen once and for all, e.g. by blowing a fuse placed on the write line; WROM could hold cryptographic keys or audit logs.

Australian National University

Memory Structures

- **Volatile memory** loses its contents when power is switched off.
  - Memory contents still present after a short power loss.
  - Can be reconstructed by special electronic techniques if power has been switched off for some time.
  - To counter such attacks, memory has to be overwritten repeatedly with suitable bit patterns.
- **Non-volatile (permanent) memory** keeps its content when power is switched off.
  - If attacker can directly access memory bypassing the CPU, cryptographic or physical measures are needed to protect sensitive data.

Australian National University

Processes and Threads

- **Process**: a program in execution, consisting of executable code, data, and the execution context, e.g. the contents of certain CPU registers.
  - A process has its own address space and communicates with other processes only through O/S primitives.
  - Logical separation of processes as a basis for security.
  - A context switch between processes can be an expensive operation.
- **Threads**: strands of execution within a process.
  - Threads share an address space to avoid the overheads of a full context switch, but they also avoid potential security controls.
- Processes and threads are important units of control for the O/S, and for security.
  - They are the 'subjects' of access control.

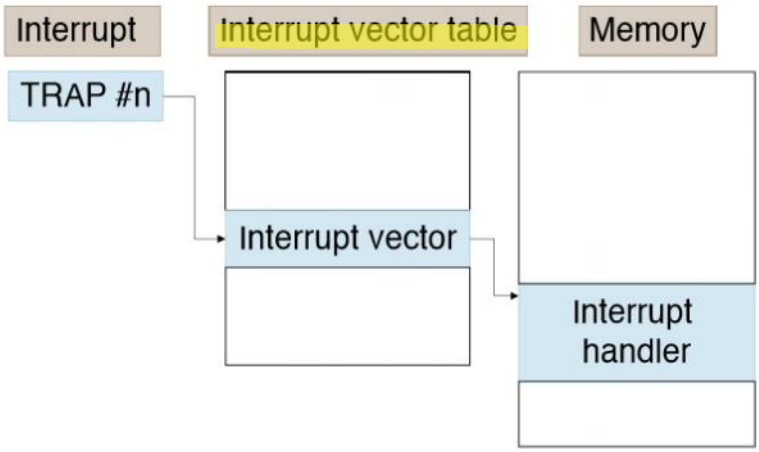
Australian National University

Trap - Interrupts

- CPU deals with interruptions of executions created by errors in the program, user requests, hardware failure, etc., through exceptions, interrupts, and traps.
- A trap is a special input to the CPU that includes an address (interrupt vector) in an interrupt vector table giving the location of the program (interrupt handler) that deals with the condition specified in the trap.

Australian National University

Interrupt Vectors



Australian National University

Interrupt handlers

- When a trap occurs, the CPU saves its current state on the stack and then executes the interrupt handler.
- The interrupt handler has to restore the CPU to a proper state, e.g. by clearing the supervisor status bit, before returning control to the user.

Australian National University

Security Mechanisms in O/S

- O/S manages access to data and resources; multitasking O/S interleaves execution of processes belonging to different users. It has to
  - separate user space from O/S space,
  - logically separate users,
  - restrict the memory objects a process can access.
- Logical separation of users at two levels:
  - file management, deals with logical memory objects
  - memory management, deals with physical memory objects
- For security, this distinction is important.

操作系统（O/S）负责管理数据和资源的访问：

- 在多任务环境中，操作系统需要交错执行来自不同用户的进程

Australian National University

Segments and Pages

- **Segmentation** divides memory into logical units of variable lengths.
  - A division into logical units is a good basis for enforcing a security policy.
  - Units of variable length make memory management more difficult.
- **Paging** divides memory into pages of equal length.
  - Fixed length units allow efficient memory management.
  - Page faults may create a covert channel.

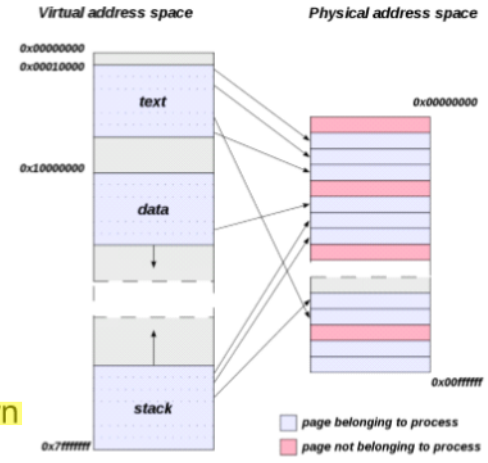
页错误（Page Faults） 可能导致隐蔽通道（covert channels）的出现，攻击者可以通过观察页错误的时间推断出敏感信息

Australian National University

Page Table

In systems supporting virtual memory (VM), pages in the VM are mapped to pages in the physical memory (main memory or disk) via a page table.

In some OS, e.g., Linux, each process has its own virtual memory space (hence page table).



A simple page table. Source: Wikipedia

Australian National University

Page faults

- Paging is not a good basis for access control as pages are not logical units.
- One page may contain objects requiring different protection.
- When a process accesses a logical object stored on more than one page, a **page fault** occurs whenever a new page is requested.
- A **side channel** exists if page faults are observable.

一个页面可能包含多个需要不同保护的对象，因此无法为整个页面设定统一的访问权限。

通过监测页错误的发生时间，攻击者可以推断出进程访问的内存区域，从而推测敏感数据。

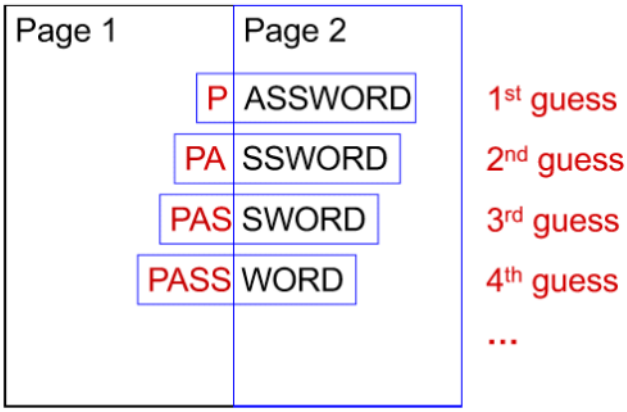
Australian National University

Example: A Side Channel

- Consider a password scheme where the password entered is compared character by character with the reference password stored in memory.
- If a password is stored across a page boundary, then observing a page fault indicates that the piece of the password on the first page has been guessed correctly.
- If the attacker can control where the password is stored on the page, password guessing becomes easy.

Australian National University

Example: A Side Channel



Australian National University

Hardware-related threats

- Side channels:
  - Timing side channels through CPU cache
  - Known exploits to extract crypto keys (AES encryption cache-based attacks)
    - D. J. Bernstein. Cache-timing attacks on AES. 2005.
    - http://cr.yp.to/antiforgery/cachetiming-20050414.pdf
- Speculative executions: speed.
  - Features of multicore processors for performance optimisation
  - Allow early executions of code that may not be needed
- Example vulnerabilities:
  - Spectre and Meltdown: exploiting speculative executions & cache side channels to read physical memories.
  - See: https://meltdownattack.com/

Australian National University

Hardware-related threats

- Hardware Trojan:
  - Malicious CPU with special instruction sequence to trigger supervisor mode.
    - Samuel T. King, et al.: Designing and implementing malicious hardware. USENIX Workshop on Large-Scale Exploits and Emergent Threats, 2008.
    - https://www.usenix.org/legacy/event/leet08/tech/full_papers/king/king.pdf
- Undocumented instructions:
  - Hidden instructions (several *millions* of them) in Intel x86 processors allow malicious code injection.
    - Christopher Domas. *Sandshifter: the x86 processor fuzzer.* https://github.com/xoreaxeaxeax/sandsifter
- Hardware fault: the 'Rowhammer' bug
  - Repeatedly accessing a row of memory in some DRAM can cause bit flips in adjacent rows.
  - Exploited to gain kernel privileges:
    - https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html

硬件特洛伊木马（Hardware Trojan）

- **定义**：恶意硬件，通过特定指令序列触发**超级用户模式**，可能导致系统被控制。

Australian National University

Other hardware-based protection mechanisms

- Securing the boot chain:
  - Secure boot: a combination of hardware-software mechanism to protect the integrity of the boot process.
    - Part of the UEFI (Unified Extensible Firmware Interface) specifications: https://www.uefi.org/specifications
- ARM Trustzone:
  - Collection of hardware modules that support partitioning a system into secure and normal subsystems.
- Trusted Platform Module (TPM)
  - A tamper-resistant hardware module, for storing cryptographic keys and other system `measurements'.
  - Can be used to ensure secure boot chain
- Intel Software Guard Extensions (SGX):
  - Secure containers for applications
  - Protect applications from adversarial operating system.

Australian National University

Summary

- Security policies can be enforced in any layer of a computer system.
- Mechanisms at lower layers are more generic and are universally applied to all “applications” above, but might not quite match the requirements of the application.
- Mechanisms at upper layers are more application specific, but applications have to be secured individually.
- Securing the `layer below’ requires a combination of hardware and software co-design.

Australian National University

Further reading

- V. Costan, I. Lebedev, S. Devadas. Secure Processors Part I & II. Foundations and Trends in Electronic Design Automation. Vol. 11. No. 1-2 (2017).
  - https://people.csail.mit.edu/devadas/pubs/part_1.pdf
- R. Anderson. Security Engineering. Chapter 16 & 17.
  - https://www.cl.cam.ac.uk/~rja14/book.html