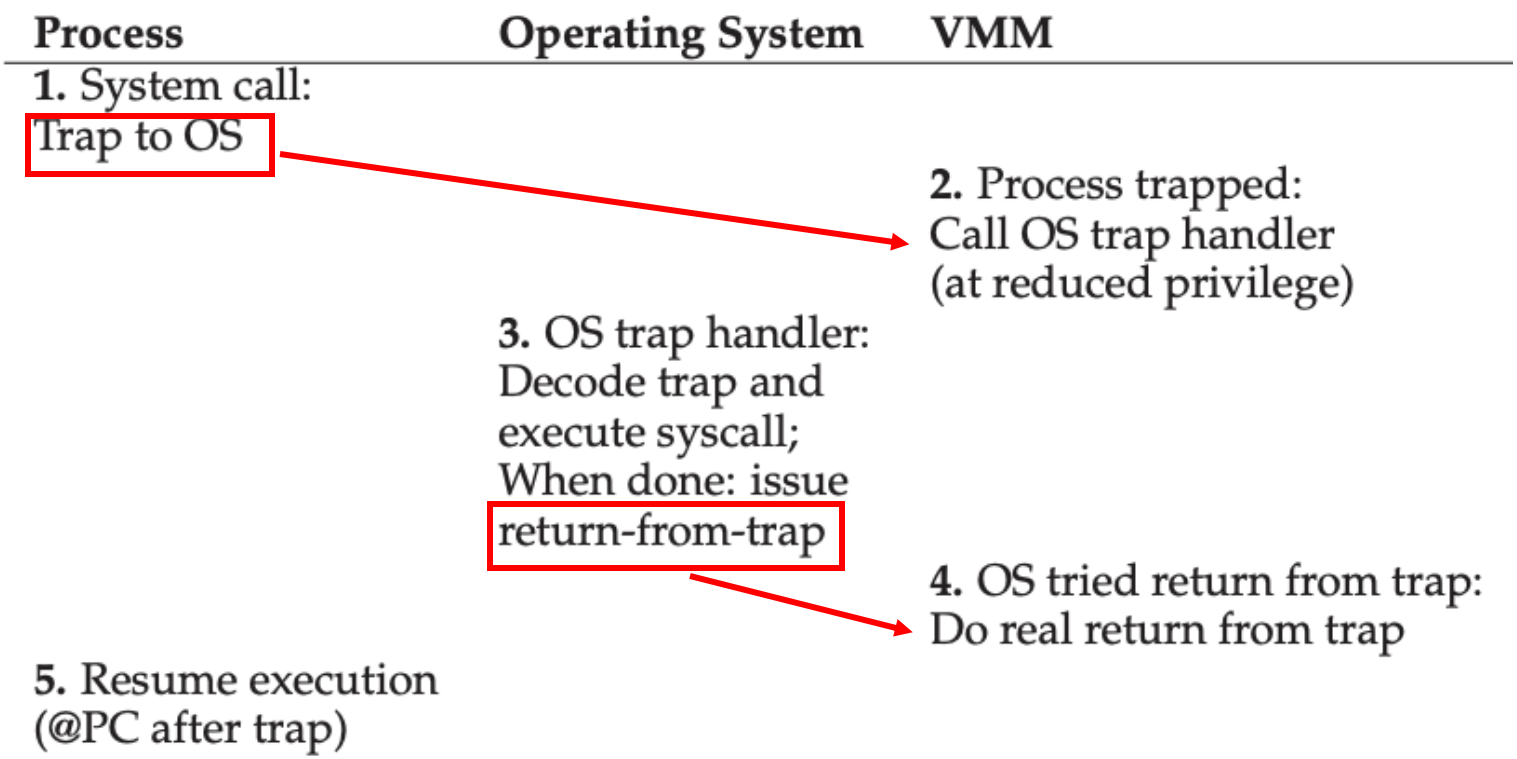
Recap

- File system on top of SSD
  - Garbage collection
  - Comparisons with HDD
- Virtual machine monitor (VMM) types
- VMM: limited direct execution for system call

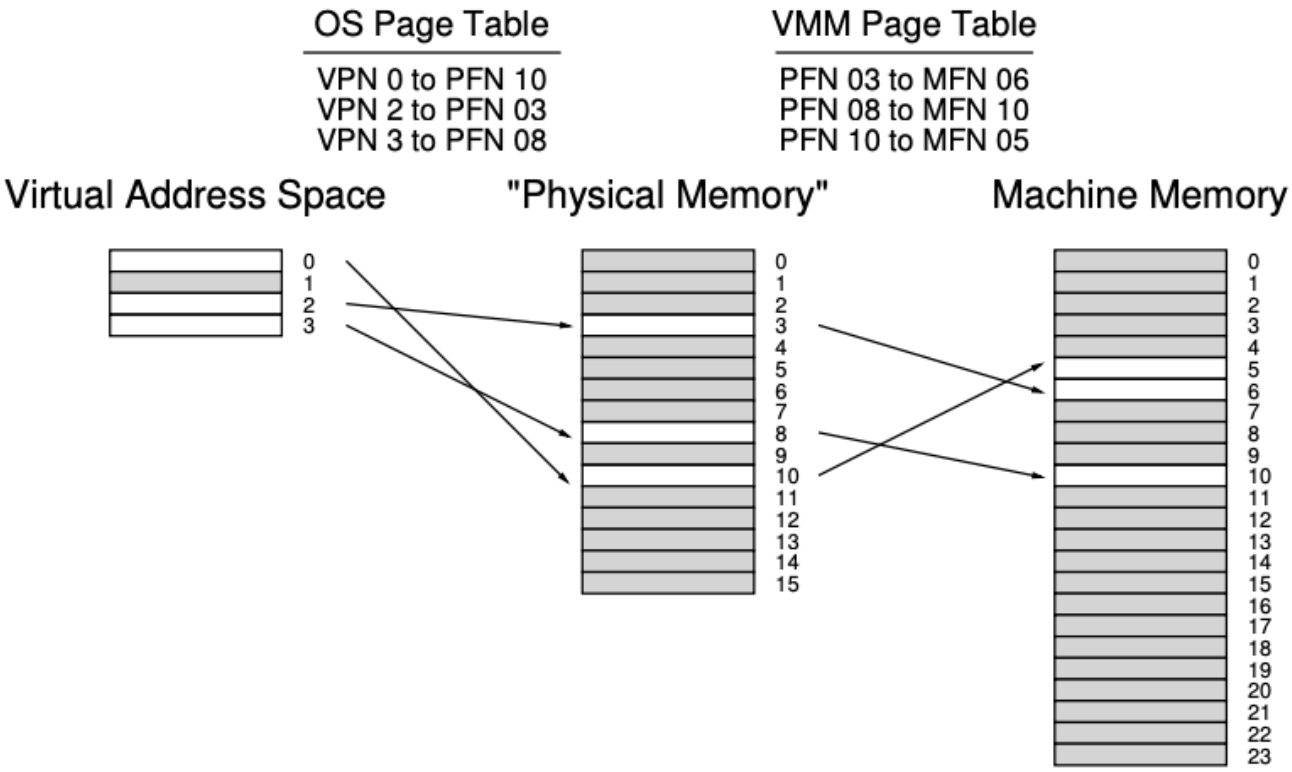
Standard System Call

Process	Hardware	Operating System
1. Execute instructions (add, load, etc.)		
2. System call: Trap to OS		
	3. Switch to kernel mode; Jump to trap handler	
		4. In kernel mode; Handle system call; Return from trap
	5. Switch to user mode; Return to user code	
6. Resume execution (@PC after trap)		

System Call with VMM



Memory Virtualization Virtualization

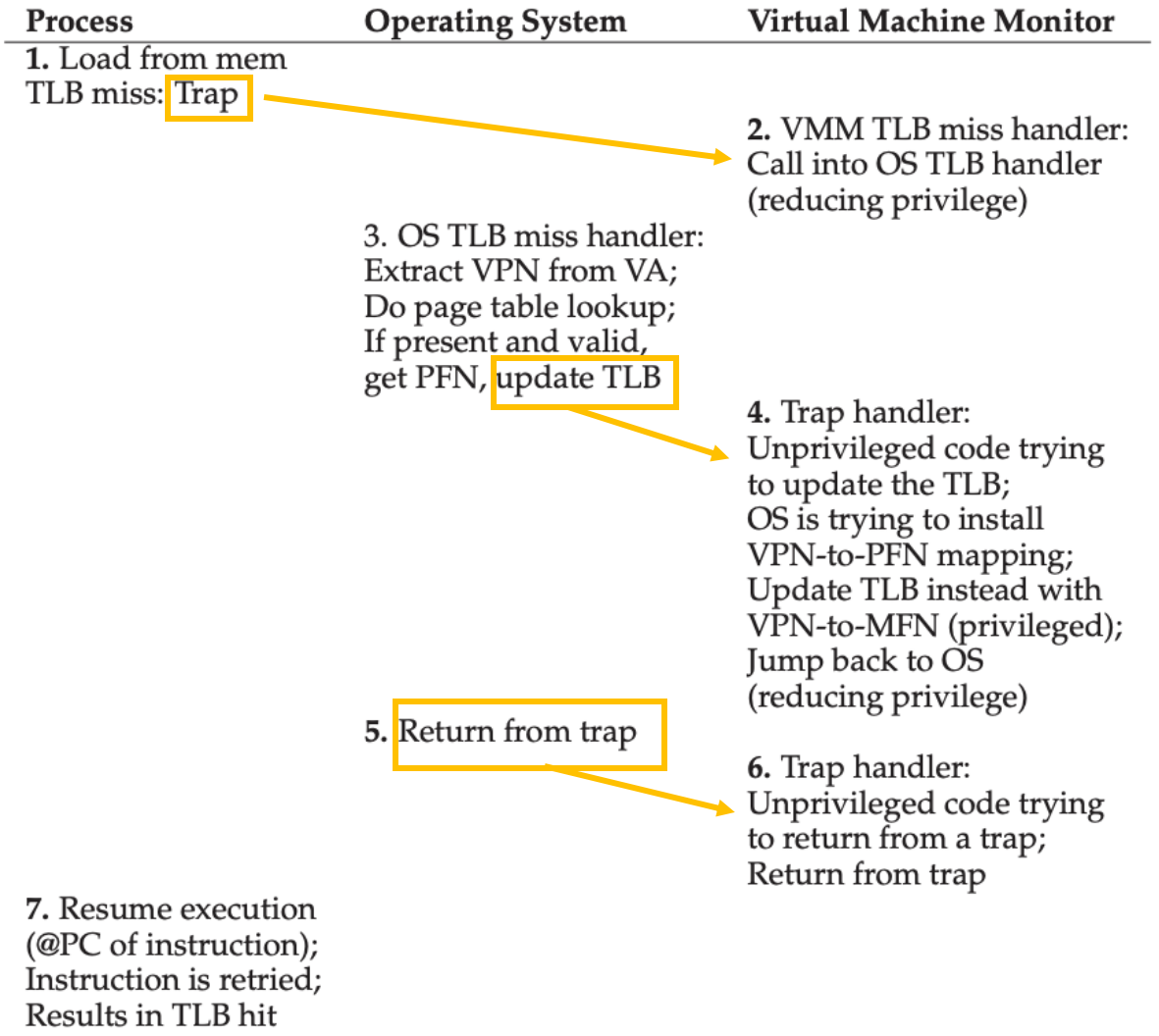


Standard Address Translation Flow on TLB Miss

Assume software managed page tables, i.e., in memory and managed by the OS
VA = Virtual Address

Process	Operating System
1. Load from memory: TLB miss: Trap	
	2. OS TLB miss handler: Extract VPN from VA; Do page table lookup; If present and valid: get PFN, update TLB; Return from trap
3. Resume execution (@PC of trapping instruction); Instruction is retried; Results in TLB hit	

TLB Miss with VMM



Information Gap

Because of transparency, VMM doesn't know what guest OS is trying to achieve

There is an **information gap** between OS and VMM that can lead to significant inefficiency

For example, when OS has no useful work (i.e., no runnable processes) it will spin in its scheduler loop

```
while (1)
  ; // the idle loop
```

Potential solution breaks transparency, in **para-virtualization** guest OS has small modifications to operate more effectively in virtualized environment

Container

Also known as OS-level virtualization.

Examples: Docker container, Solaris Zone, OpenVZ virtual private server, FreeBSD jail

Container vs Native Computer

- A computer program running on an ordinary OS can see all resources.
- However, programs running inside of a container can only see the container's contents and devices assigned to the container.

Virtual Machine vs Container

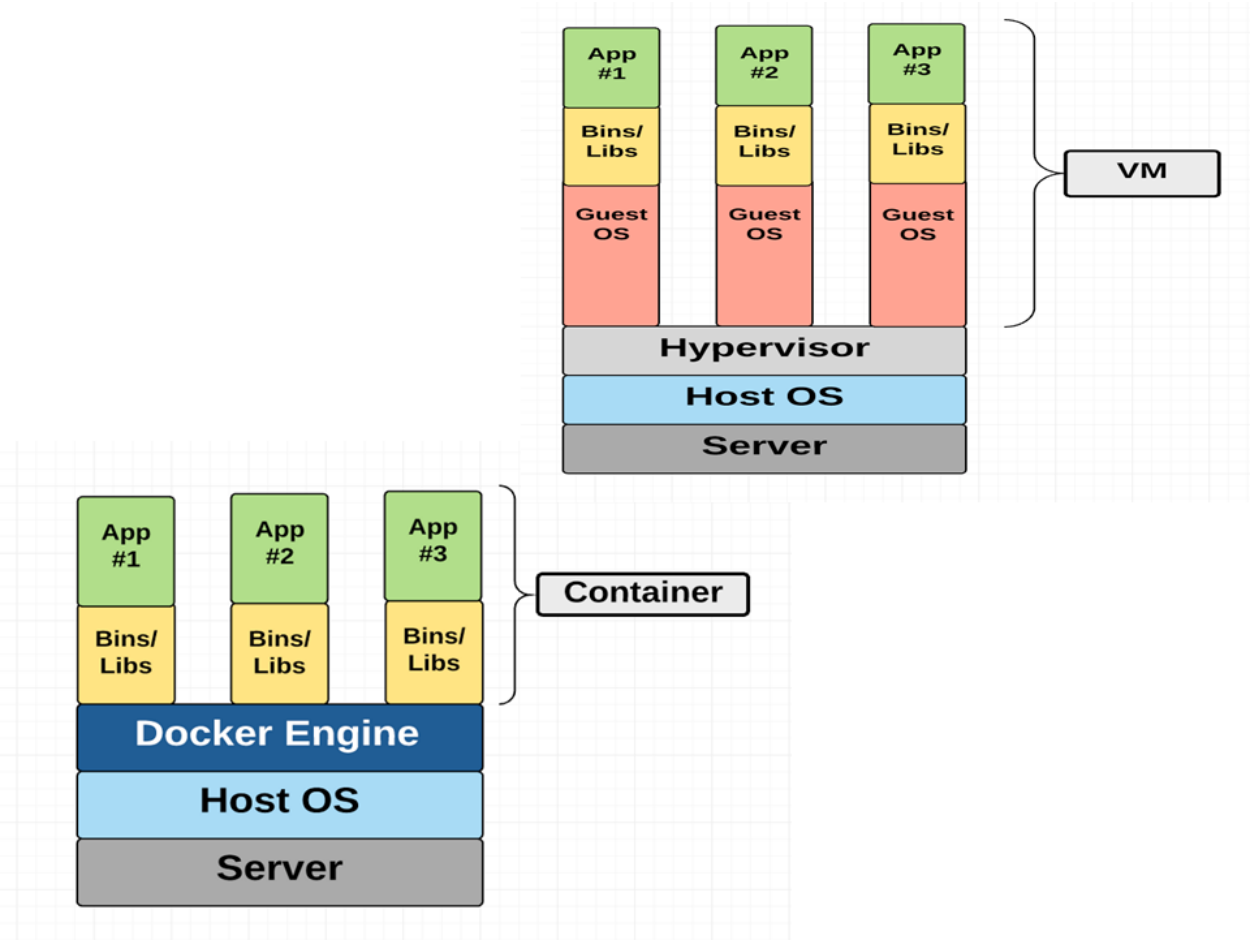
Similar goals:

- To isolate an application and its dependencies into a self-contained unit that can run anywhere;
- For more efficient and secure use of (shared) resources.

Differences:

- VM – package up the virtual hardware, a kernel (i.e., OS) and user space for each VM.
- Container – package up just the user space, and not the kernel or virtual hardware like a VM does; more efficient but less isolated/secure.

Virtual Machine vs Container



Basic of Security

The Security Problem

Goal of security is to protect:

- integrity of the information stored in the system;
- physical resources of the computer system.

The security system prevents unauthorized access, malicious destruction or alteration of data, and accidental introduction of inconsistency.

Requirements of Security Mechanisms

Confidentiality: information maintained by a computer system is accessible only by authorized parties (users and the processes that run as/representing those users).

Integrity: a computer system's resources can be modified only by authorized parties.

Availability: a computer system can be accessible at requested times by authorized parties.

Authenticity: a computer system can verify the identity of a user

Security Violation Categories

Breach of confidentiality

- Unauthorized reading of data

Breach of integrity

- Unauthorized modification of data

Breach of availability

- Unauthorized destruction of data

Theft of service

- Unauthorized use of resources

Denial of service (DOS)

- Prevention of legitimate use

Attacks

Intruders are those who attempt to breach security

A **vulnerability** is a weakness in the security of a system

- Buffer that is not protected from overflow

A **threat** is anything that leads to loss or corruption of data or physical damage to the hardware and/or infrastructure

- Theft, fire, virus, spyware

An **attack** is an attempt to breach security

- Attack can be accidental or malicious

Program Threats

Malware - Software designed to exploit, disable, or damage computer systems

Trojan Horse – Program that looks legitimate but can take control of your computer.

- **Spyware** – Program frequently installed with legitimate software to display ads, capture user data (Up to 90% of spam delivered by spyware-infected systems)

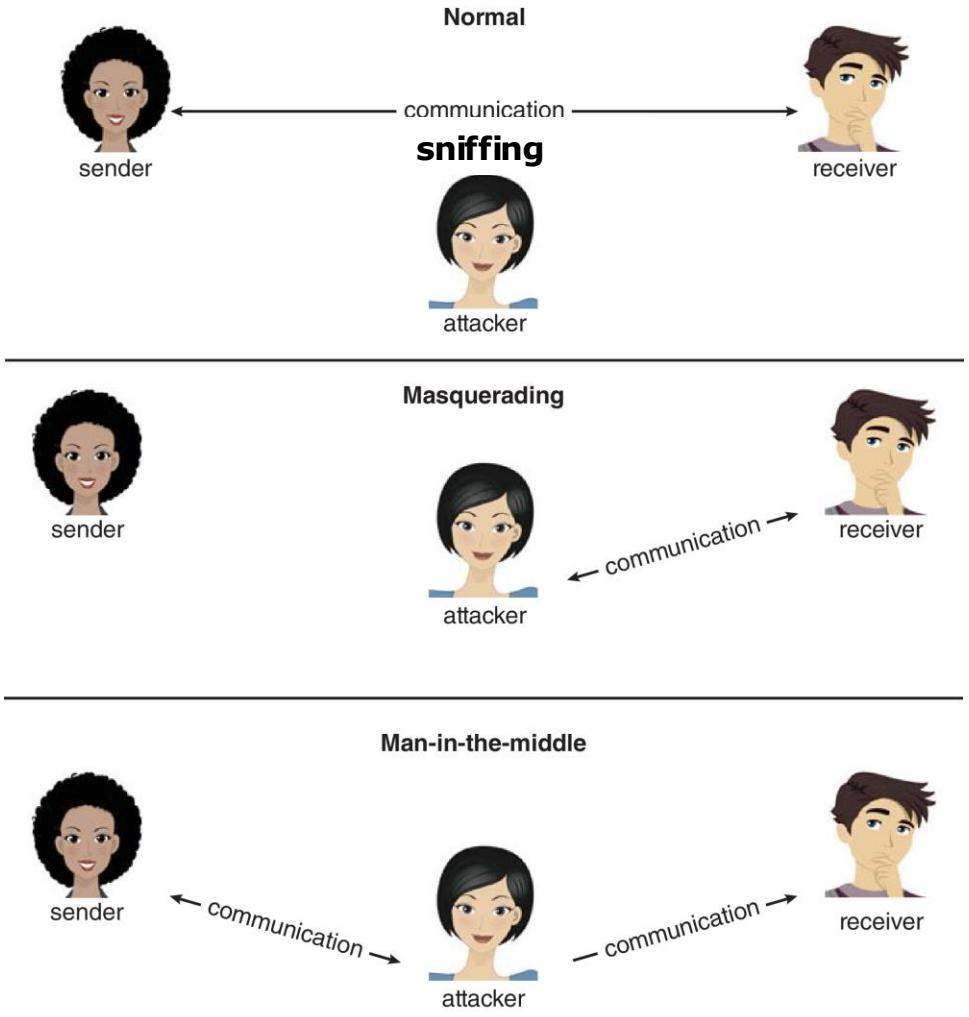
Ransomware – Locks up data via encryption, demanding payment to unlock it

Malware thrive when there is a violation of the Principle of Least Privilege

THE PRINCIPLE OF LEAST PRIVILEGE

"The principle of least privilege. Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job. The purpose of this principle is to reduce the number of potential interactions among privileged programs to the minimum necessary to operate correctly, so that one may develop confidence that unintentional, unwanted, or improper uses of privilege do not occur."—Jerome H. Saltzer, describing a design principle of the Multics operating system in 1974: https://pdfs.semanticscholar.org/1c8d/06510ad449ad24fbdd164f8008cc730cab47.pdf.

System and Network Threats



System and Network Threats (Cont.)

Denial of Service

- Overload the targeted computer preventing it from doing any useful work
- **Distributed Denial-of-Service** (**DDoS**) come from multiple sites at once
- Consider the TCP-connection handshake
  - How many connections can the OS handle?
- Consider traffic to a web site
  - How can you tell the difference between being a target and being really popular?

Port scanning

- Automated attempt to connect to a range of ports on one or a range of IP addresses
- Detection of running services in order to identify vulnerabilities
- Detection of OS and version running on system