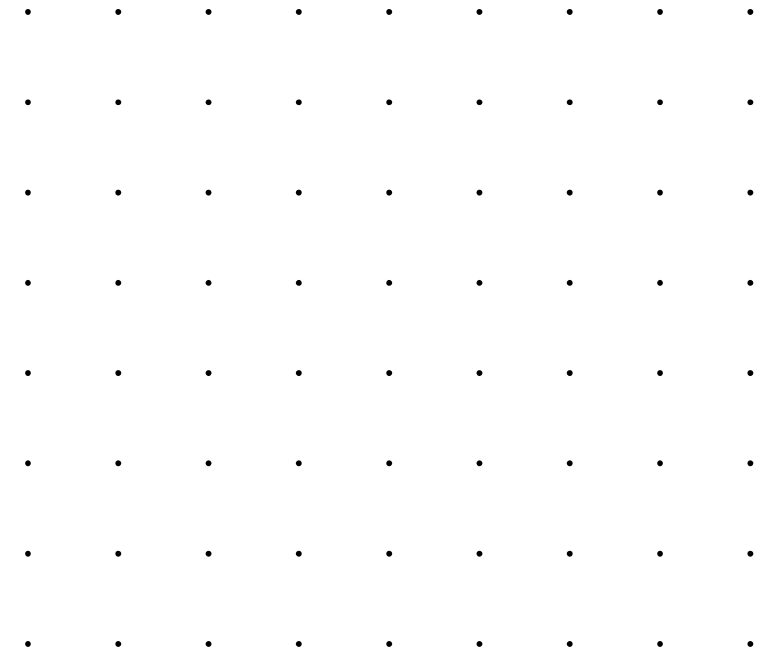
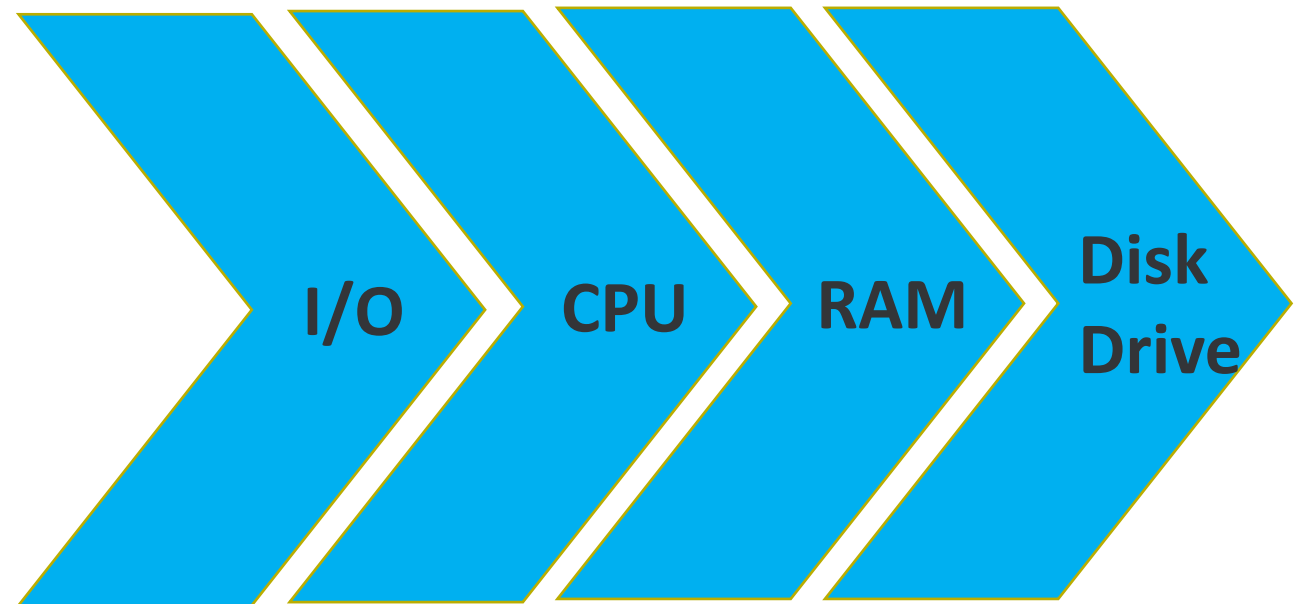


Operating System Security



A Computer Model

- An operating system has to deal with the fact that a computer is made up of a CPU, random access memory (RAM), input/output (I/O) devices, and long-term storage.



OS Concepts

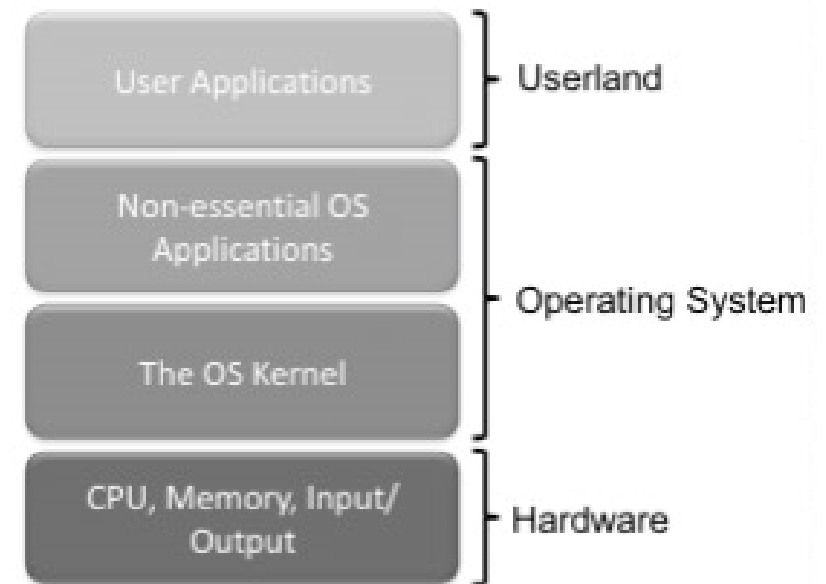
- **An operating system (OS) provides the interface between the users of a computer and that computer's hardware.**
 - An operating system manages the ways applications access the resources in a computer, including its disk drives, CPU, main memory, input devices, output devices, and network interfaces.
 - An operating system manages multiple users.
 - An operating system manages multiple programs.

Multitasking

- Give each running program a “slice” of the CPU’s time.
- The CPU is running so fast that to any user it appears that the computer is running all the programs simultaneously.

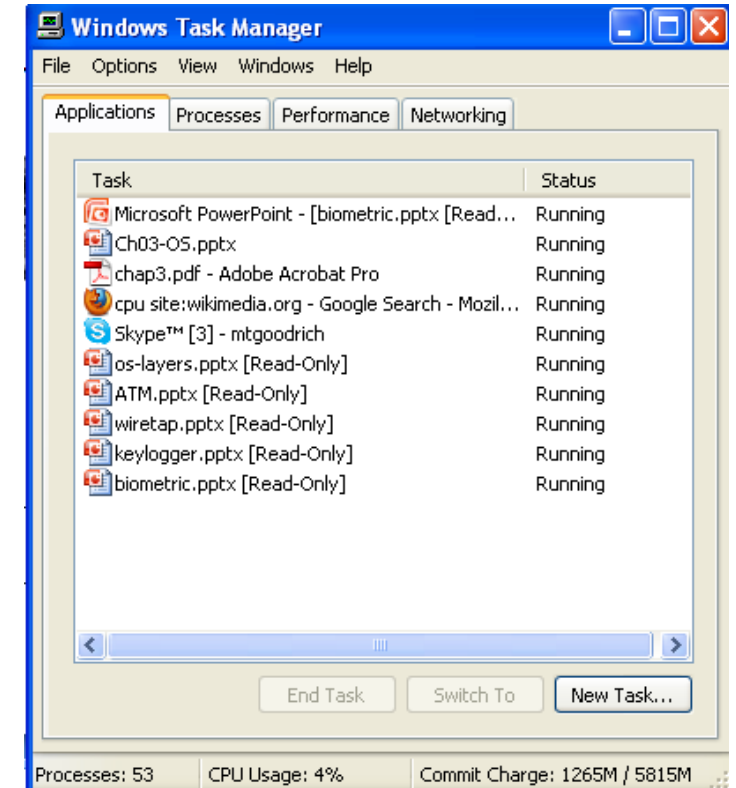
The Kernel and Input/Output

- **Kernel:** core component of the operating system. It handles the management of low-level hardware resources, including memory, processors, and input/output (I/O) devices, such as a keyboard, mouse, or video display.
- Most operating systems define the tasks associated with the kernel in terms of a layer metaphor, with the hardware components, such as the CPU, memory, and input/output devices being on the bottom, and users and applications being on the top.



Processes

- A **process** is an instance of a program that is currently executing.
- The actual contents of all programs are initially stored in persistent storage, such as a hard drive.
- In order to be executed, a program must be loaded into random-access memory (RAM) and uniquely identified as a process.
- In this way, multiple copies of the same program can be run as different processes.
 - For example, we can have multiple copies of MS Powerpoint open at the same time.



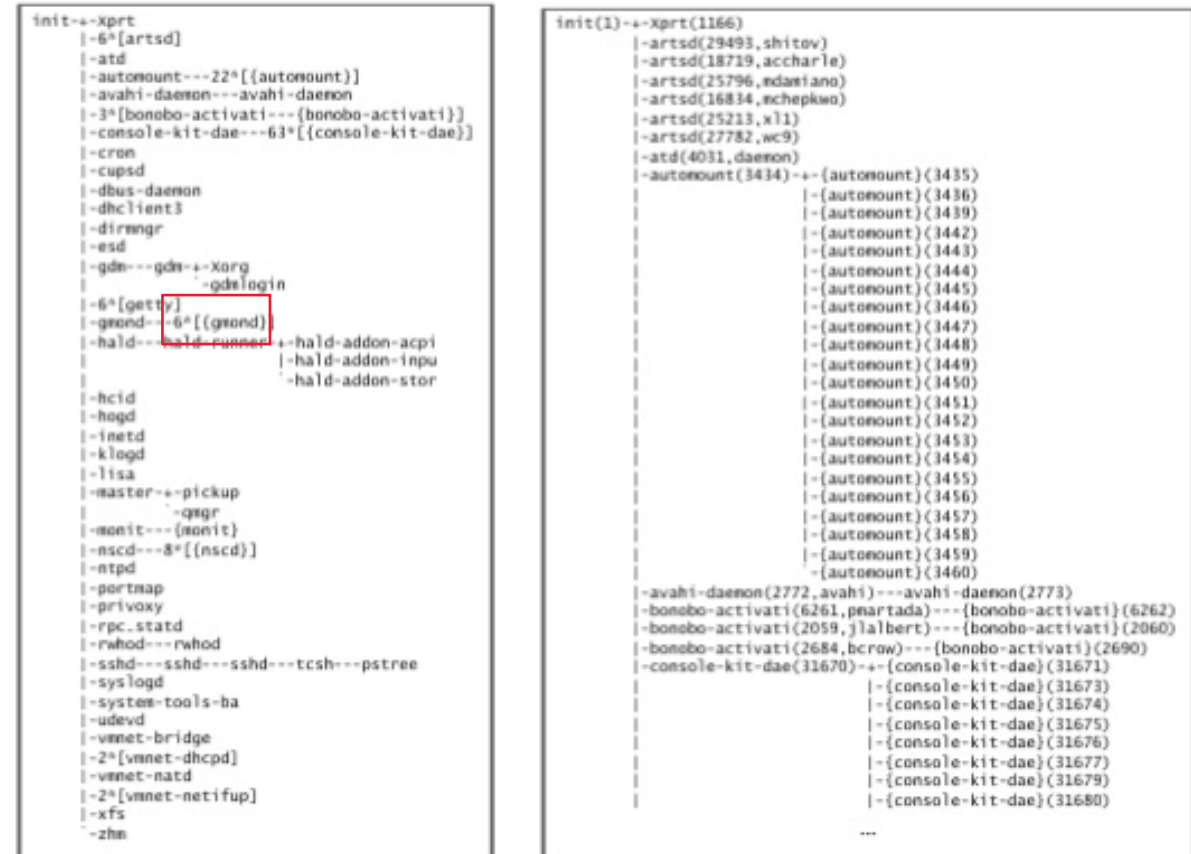
Processes

Process: the kernel defines the notion of a process, which is an instance of a program that is currently executing.

The **Process IDs:** Each process running on a given computer is identified by a unique nonnegative integer, called the process ID (PID).

IPC: operating systems usually include mechanisms to facilitate inter-process communication (IPC).

Signal: unixbased systems incorporate signals, which are essentially notifications sent from one process to another.



Process tree for a Linux system

The Filesystem

- A **filesystem** is an abstraction of how the external, nonvolatile memory of the computer is organized.
- Operating systems typically organize files hierarchically into folders, also called directories.
- Each folder may contain files and/or subfolders.
- Thus, a volume, or drive, consists of a collection of nested folders that form a tree.
- The topmost folder is the root of this tree and is also called the root folder.



A filesystem as a tree

The Filesystem

Filesystem: filesystem is another key component of an operating system. It is an abstraction of how the external, nonvolatile memory of the computer is organized.

File Access Control: determine which uses can access which resources.

File Permissions: file permissions are checked by the operating system to determine if a file is readable, writable, or executable by a user or group of users.

Unix File Permissions: the read, write, and execute bits are implemented in



A filesystem as a tree

Memory Management

Memory Management: is another service that OS provides. Memory management refers to management of Primary Memory or Main Memory.

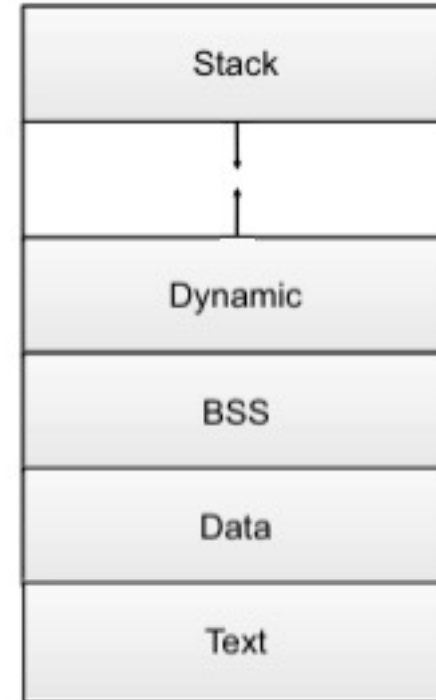
Text: machine code of the program

Data: static program variables (prior execution)

BSS: block started by symbol, contains static variables that are uninitialized

Heap: dynamic segment, stores data such as objects written in C++ or Java, during the execution.

Stack: houses a stack data structure.



The Unix memory model

Virtual Machines

Virtual machines (VMs) are software computers that provide the same functionality as physical computers. Unlike emulators, VMs have direct access to the host CPU disks and RAM, so they run fast and efficient (compared to emulators).

Advantages:

Many VMs in a single host – hardware cost is shared.

Portable – VM can be shut down and moved to another host and then started up again (sometimes automatically).

Secure – VM–Host interface acts as a sandbox. Prevents malware from getting out of VM.

Convenient – Easy to manage VM backups, ideal for remote access / monitoring. Great for security research.



Virtual Machines

Disadvantages

- Hosting may be in another (or unknown) legal jurisdiction.
- CIA issues.
- Infected VMs may be able to escape the VM “sandbox” and infect other VMs and the host. (see BluePill)
➤ http://en.wikipedia.org/wiki/Blue_Pill_%28software%29
- Malware detection in the VM can be thwarted if malware detects that it is in a VM or sandbox (and stays inactive).
- Hiberfile, pagefile, .vmem and .vmdk files are susceptible to physical access attacks.
- Hosting company can access inside of VM through VMI extensions.
➤ https://www.researchgate.net/publication/270081646_CloudSec_A_Security_Monitoring_Appliance_For_Virtual_Machines_In_The_IaaS_Cloud_Model

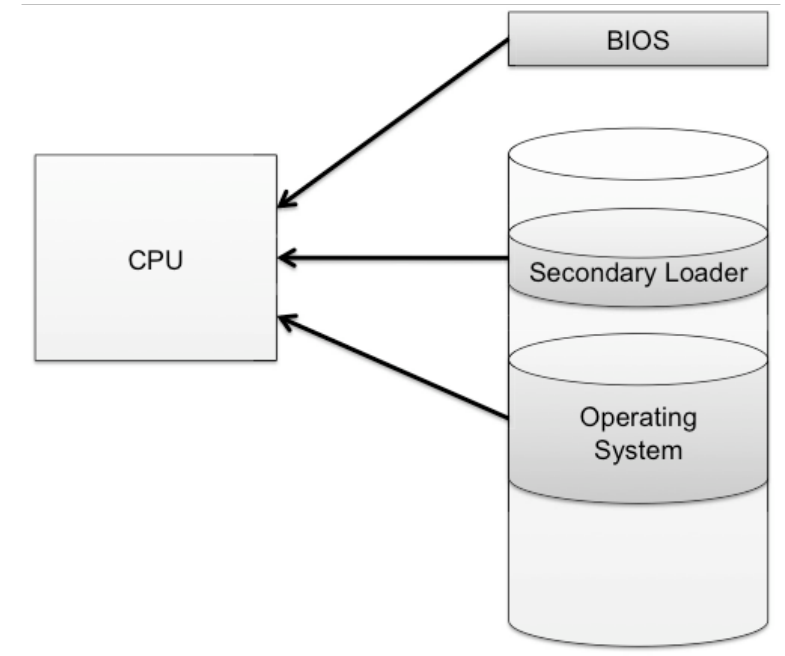
Two Types of Virtual Machines

Process virtual machines
(platform-independent environment)

System virtual machines
(Support the sharing of a host computer's physical resources)

The Boot Sequence

- The action of loading an operating system into memory from a powered-off state is known as booting or bootstrapping.
- When a computer is turned on, it first executes code stored in a firmware component known as the BIOS (basic input/output system).
- On modern systems, the BIOS loads into memory the second-stage boot loader, which handles loading the rest of the operating system into memory and then passes control of execution to the operating system.



BIOS Passwords

- A malicious user could potentially seize execution of a computer at several points in the boot process.
- To prevent an attacker from initiating the first stages of booting, many computers feature a BIOS password that does not allow a second-stage boot loader to be executed without proper authentication.

Hibernation

- Modern machines have the ability to go into a powered-off state known as hibernation.
- While going into hibernation, the OS stores the contents of machine's memory into a hibernation file (such as hiberfil.sys) on disk so the computer can be quickly restored later.
- But... without additional security precautions, hibernation exposes a machine to potentially invasive forensic investigation.



1. User closes a laptop computer, putting it into hibernation.

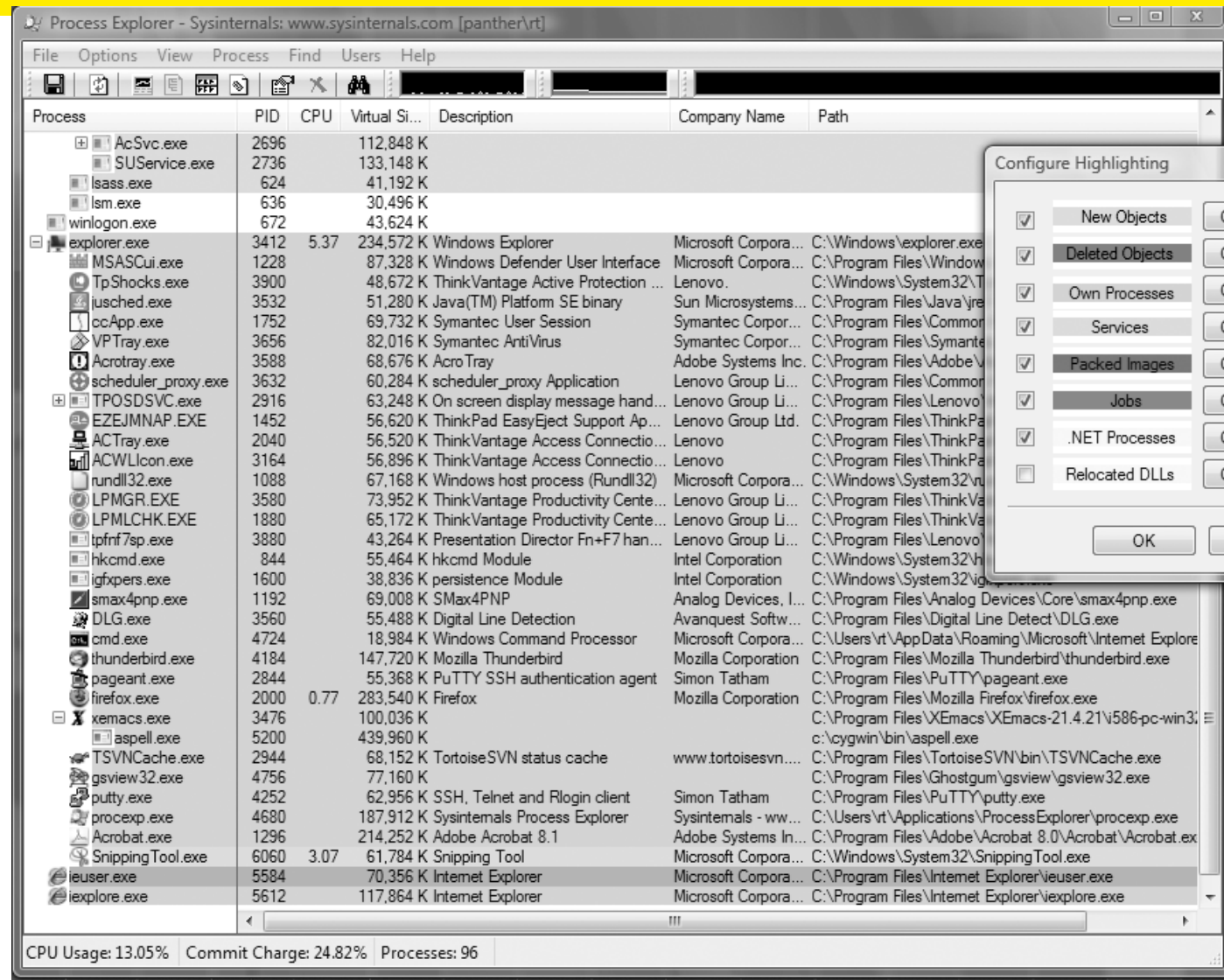


2. Attacker copies the hiberfil.sys file to discover any unencrypted passwords that were stored in memory when the computer was put into hibernation.

Event Logging

- Keeping track of
 - what processes are running,
 - what other machines have interacted with the system via the Internet, and
 - if the operating system has experienced any unexpected or suspicious behavior
 - can often leave important clues not only for troubleshooting ordinary problems, but also for determining the cause of a security breach.

Process Explorer



Seeing Processes

- On Windows, ctrl/alt/del → choose task manager → select processes
- On Linux, ps lists your processes. Various switches allow access to system wide processes.
 - For example,
`ps -e`
lists all processes on the machine.