Operating Systems: An Overview

Mckenzie Mack
GenCyber Workshop

Agenda

- Defining an OS
- Processes and the OS
- Memory Management
- Storage Management
- How an OS Communicates
- Commands for Management
- Security

Learning Objectives

- Define operating systems in terms of process management, memory management, and storage management
- Explore the role of device drivers in terms of operating systems
- Demonstrate how commands could be used to examine statistics on memory usage and running processes
- Describe the vulnerabilities of operating systems as well as security mechanisms used to protect operating systems

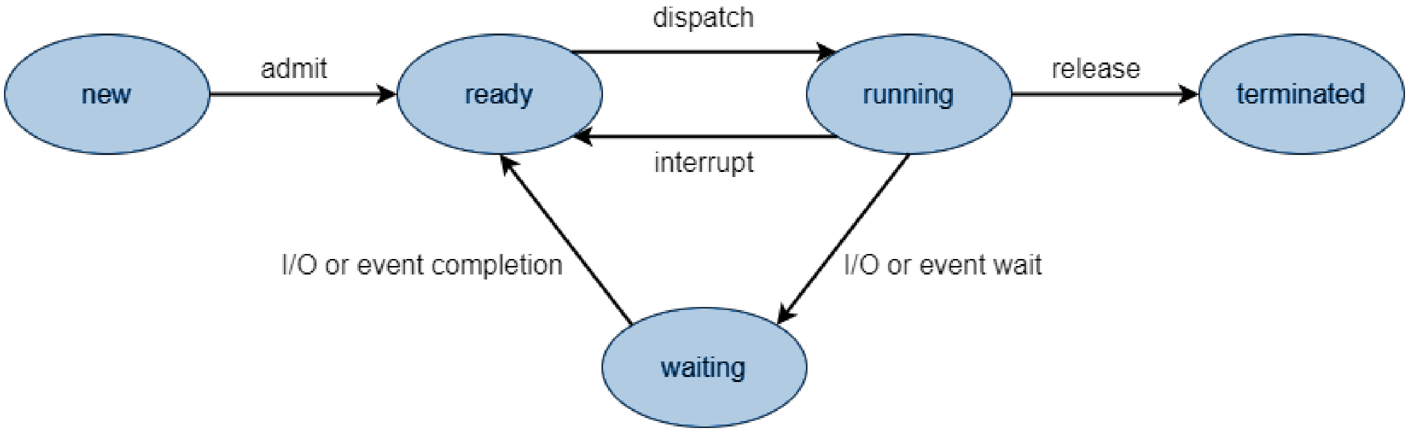
Defining an OS

- You have probably heard the term OS when talking about computers but may not know what it stands for
- OS stands for **operating system**, which is an interface between the hardware and software components of a computer
- There are many different operating systems available on the market

Windows 10
macOS
android
iOS
+
Raspbian
XBOX

Processes and the OS

- process: an execution of a program
- An operating system changes the states of processes, allocates resources for processes upon request, and deallocates them when the process is finished or terminates
  - resources include:
    - memory, including virtual memory and physical memory
    - processors (aka CPU)



Memory Management

- Besides processes, the OS is also in charge of managing memory
  - includes:
    - moving processes into main memory for execution
    - moving processes out of RAM and back into secondary memory when more RAM space is needed
    - keeping track of all memory locations
      - both ones that are allocated by processes and ones that are free
    - optimizing memory space by splitting memory into blocks through methods like **paging** and **segmentation**
      - both techniques are very similar
        - paging uses fixed-size blocks while segmentation uses variable size blocks

Storage Management

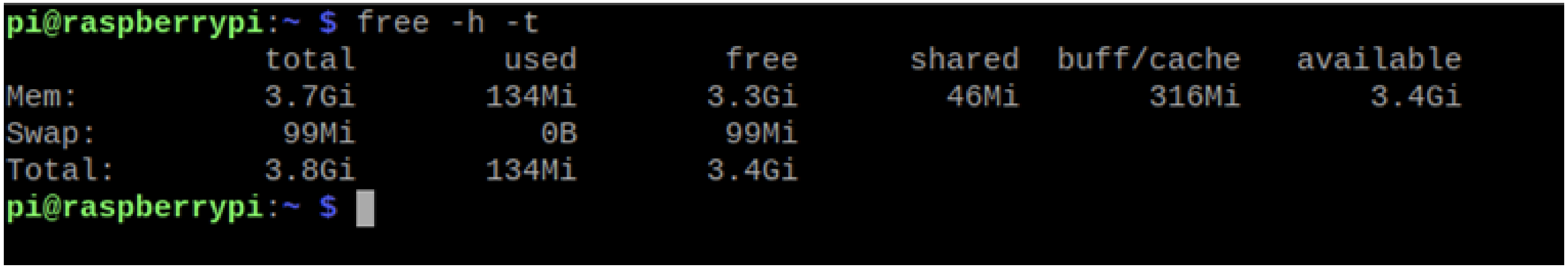
- Alongside main memory, the operating system manages files stored long-term in secondary storage
  - tasks performed by the OS include:
    - organizing data into files
    - providing directories where users can store these files
    - keeping track of all files' attributes
      - includes name, location, size, type, access permissions, etc.
    - transferring files to and from secondary memory to be used
- The OS communicates with secondary memory devices to retrieve files using a **device driver**
  - device driver: program that provides an interface between the hardware device and the operating system

Commands for Management

- How do you know what processes are running on a device?
- How do you know how much free and allocated memory space a device has?
- Most OSs offer ways to find this information through the GUI
  - can also be found using commands

Commands for Management

- free
  - outputs the amount of used and available space in both swap memory (where virtual memory is located) and main memory
  - -h can be used to print the output in a more human readable format
  - -t can be used to print the total of each column

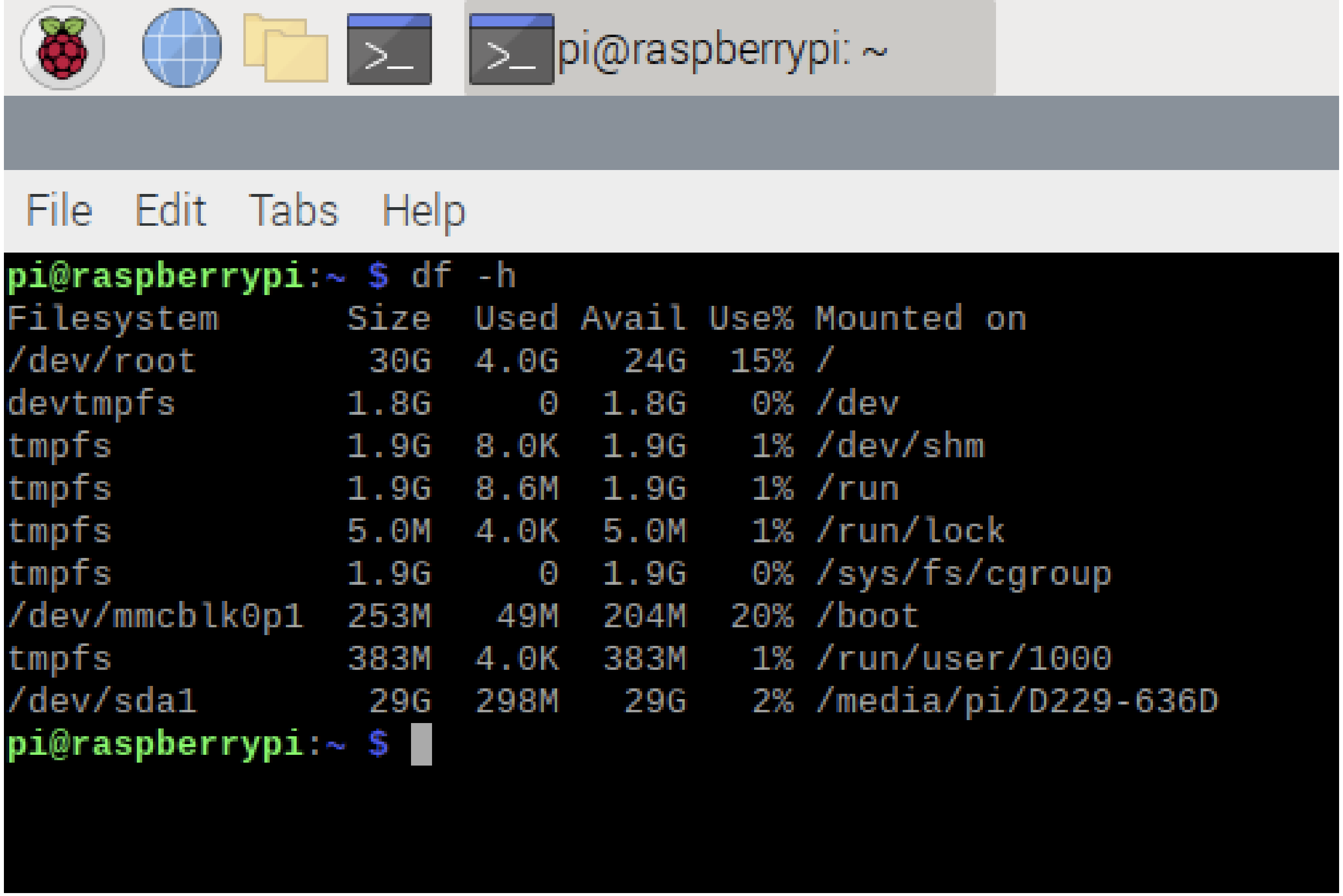


```
pi@raspberrypi:~ $ free -h -t
               total        used        free      shared  buff/cache   available
Mem:           3.7Gi       134Mi       3.3Gi        46Mi       316Mi       3.4Gi
Swap:           99Mi          0B        99Mi
Total:         3.8Gi       134Mi       3.4Gi
pi@raspberrypi:~ $
```

Commands for Management

- df
  - displays amount of disk space used by different filesystems on a device
  - -h can be used to make the results more readable
  - the output includes:
    - filesystem name
    - size of the filesystem
    - amount of space used
    - amount of space available
    - % of total disk space allocated to filesystem
    - the directory that the file system is mounted on

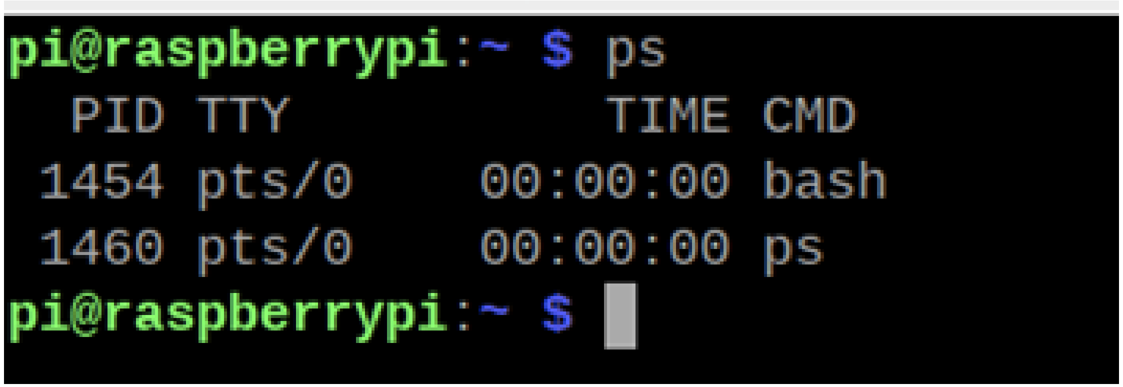
Commands for Management



```
pi@raspberrypi:~ $ df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/root        30G  4.0G   24G  15% /
devtmpfs        1.8G     0  1.8G   0% /dev
tmpfs           1.9G  8.0K  1.9G   1% /dev/shm
tmpfs           1.9G  8.6M  1.9G   1% /run
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           1.9G     0  1.9G   0% /sys/fs/cgroup
/dev/mmcblk0p1  253M   49M  204M  20% /boot
tmpfs           383M  4.0K  383M   1% /run/user/1000
/dev/sda1        29G  298M   29G   2% /media/pi/D229-636D
pi@raspberrypi:~ $ 
```

Commands for Management

- ps
  - displays information about active processes on a system
  - ps -e or ps -A can be used to view all processes on a system
  - columns listed by ps:
    - PID = process ID
    - TTY = terminal used to execute command
    - TIME = CPU time of the process
    - CMD = command used to start the process

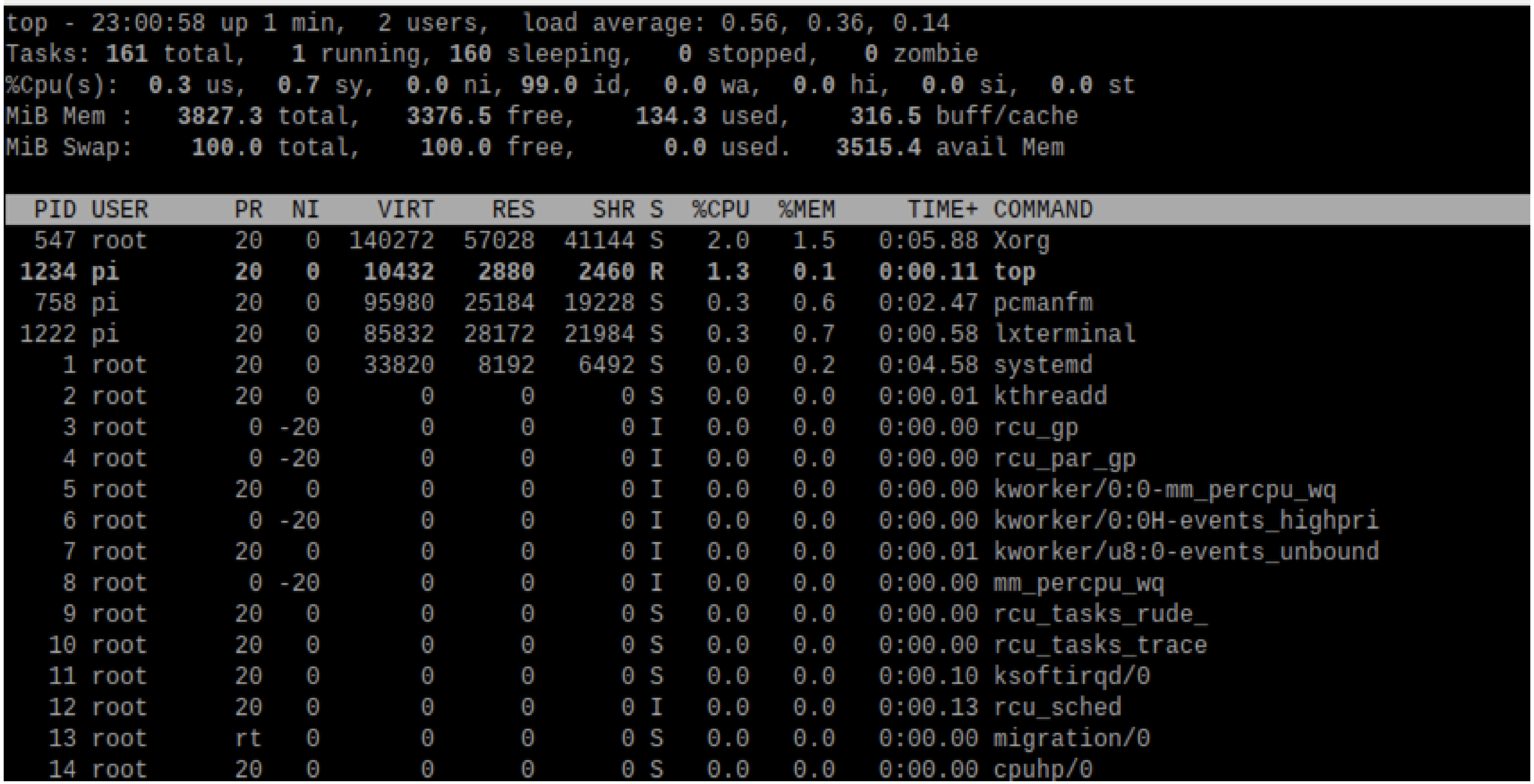


```
pi@raspberrypi:~ $ ps
  PID TTY          TIME CMD
 1454 pts/0    00:00:00 bash
 1460 pts/0    00:00:00 ps
pi@raspberrypi:~ $ 
```

Commands for Management

- top
  - similar to ps, but updates information about processes running on a system in real time
  - top portion of output shows information about all running processes
  - bottom portion of output shows information about each running process
    - PID: process id
    - PR: priority of process
    - VIRT: amount of virtual memory used
    - %MEM: percentage of memory used by task
    - %CPU: percentage of CPU time used by task

Commands for Management

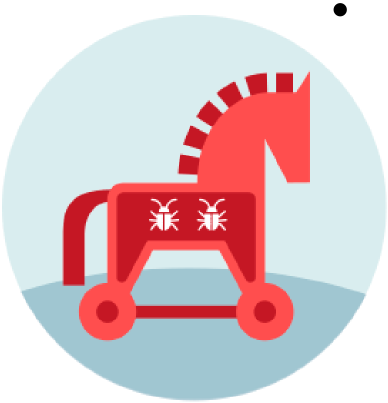


```
top - 23:00:58 up 1 min,  2 users,  load average: 0.56, 0.36, 0.14
Tasks: 161 total,   1 running, 160 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.3 us,  0.7 sy,  0.0 ni, 99.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
MiB Mem :   3827.3 total,   3376.5 free,    134.3 used,    316.5 buff/cache
MiB Swap:    100.0 total,    100.0 free,      0.0 used.   3515.4 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  547 root      20   0  140272  57028  41144 S   2.0   1.5   0:05.88 Xorg
 1234 pi        20   0   10432   2880   2460 R   1.3   0.1   0:00.11 top
  758 pi        20   0   95980  25184  19228 S   0.3   0.6   0:02.47 pcmanfm
 1222 pi        20   0   85832  28172  21984 S   0.3   0.7   0:00.58 lxterminal
    1 root      20   0   33820   8192   6492 S   0.0   0.2   0:04.58 systemd
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
    5 root      20   0       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0-mm_percpu_wq
    6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
    7 root      20   0       0      0      0 I   0.0   0.0   0:00.01 kworker/u8:0-events_unbound
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
    9 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_rude_
   10 root      20   0       0      0      0 S   0.0   0.0   0:00.00 rcu_tasks_trace
   11 root      20   0       0      0      0 S   0.0   0.0   0:00.10 ksoftirqd/0
   12 root      20   0       0      0      0 I   0.0   0.0   0:00.13 rcu_sched
   13 root      rt   0       0      0      0 S   0.0   0.0   0:00.00 migration/0
   14 root      20   0       0      0      0 S   0.0   0.0   0:00.00 cpuhp/0
```

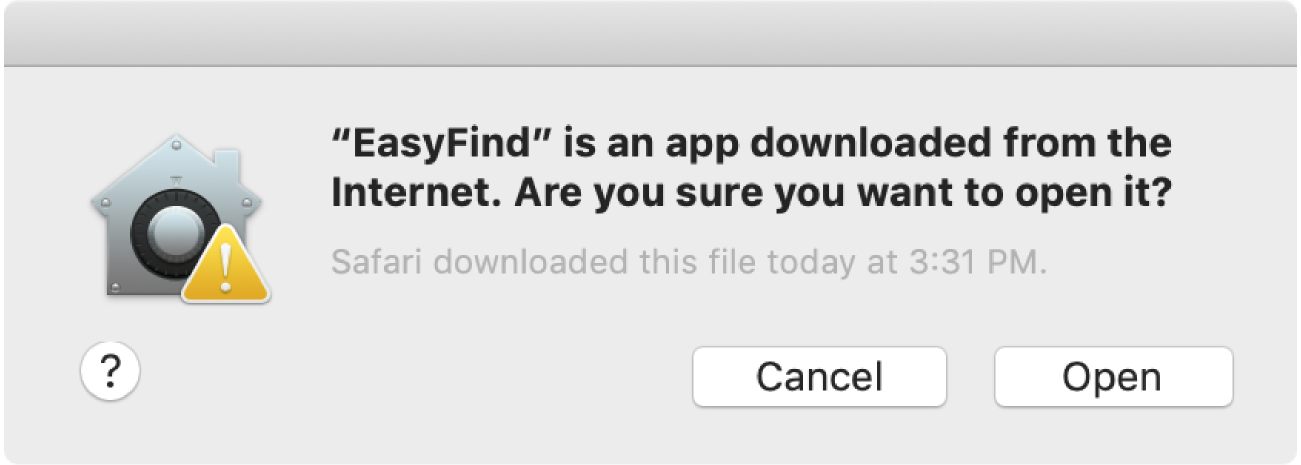
Security

- An operating system can be used by an attacker to cause damage to the computer system
    - A user with unrestricted privileges could run a program that infects the system with a virus
        - can damage data or cause the entire system to crash
    - An operating system that automatically runs files downloaded from the Internet could cause a Trojan horse to execute
        - allows unauthorized users to access the system



Security

- What measures does an operating system take to ensure that the system's data maintains CIA?
    - authenticates all users
        - requires username and password
    - restricts privileges of all users
    - maintains access permissions of all files
    - blocks execution of files downloaded from the Internet



"EasyFind" is an app downloaded from the Internet. Are you sure you want to open it?

Safari downloaded this file today at 3:31 PM.

Security

- How can the user protect the operating system?
  - one popular technique is to install **antivirus software**
    - antivirus software: program used to detect and delete malicious programs on a system
    - should be used alongside other security mechanisms, not in place of them
    - protects against ransomware like Petya in the video below

Security

- **Warning: flashing occurs in the video 2:55-3:10**

Resources

- Processes and threads in more detail: https://docs.microsoft.com/en-us/windows/win32/procthread/processes-and-threads
- A look at the history of operating systems and virtual memory: https://www.youtube.com/watch?v=26QPDBe-NB8&t=97s
- A search engine for command man pages: https://www.kernel.org/doc/man-pages/

LAB

- Complete the questions for Lab - Terminal Commands and Resource Utilization