Educate
Engage
Inspire

Presented by

In partnership with

Module 4

Computer basics and virtualisation

cybertaipan.csiro.au

Learning objectives

Participants will understand the internal components of a computer.

- Basic computer concepts and terminology.
- Common security issue types.

Participants will understand operating system purpose, types, and security.

- Purpose and use of operating systems.
- Major operating systems.

Participants will understand the basics of virtual computing.

- Provide overview of virtual machines, terminology, use, and architecture.
- Describe basic security risks for virtual computing (hypervisor, hosts, guests).

Participants will gain a broad understanding of major networking components and concepts.

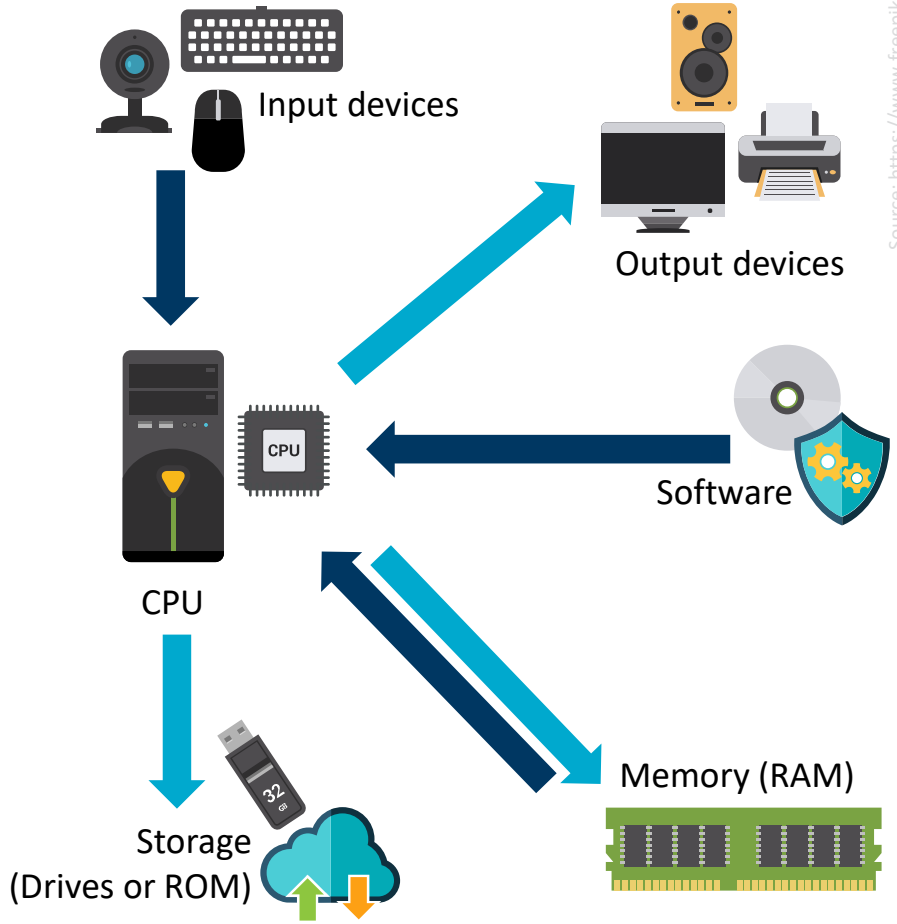
- Overview of basic network types, concepts, and terms/definitions.
- Cisco Networking Academy.

Section 1

How Computers Work

Computer anatomy 101

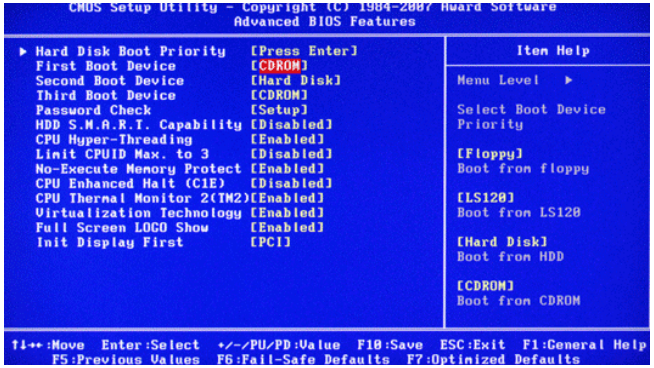
- The central processing unit (CPU) does the grunt work of the computer.
- Random access memory (RAM) saves your progress in many different software programs so that you can access that temporarily saved data later on.
- RAM is temporary. It is wiped when you turn off the computer.
- Storage allows use to save data more permanently.
- Read-only memory (ROM) is read-only and does not change often.



Software — the BIOS

- Allows the operating system (OS) to connect with input, output, and storage devices.
- Embedded on the motherboard by the manufacturers and is a permanent piece of the computer.
- Connects the CPU with the OS so the computer can boot up.
- Manages basic system settings like date and time and power management.

Basic **I**nput-**O**utput **S**ystem



Source: itprostuff.com

Common hardware / BIOS vulnerabilities

Backdoors

Can be built into hardware and later be exploited by attackers.

Environmental concerns

All hardware is susceptible to flooding, fires, and dust, which can lead to loss of capability or data if not properly stored or physically secured.

BIOS

Can be attacked through malware that can crash the BIOS. Also can be accidentally harmed by users using unauthenticated files to update the files that have unintended consequences.

RAM

Some malware can install itself on RAM rather than the hard drive, making them much more difficult to detect and eliminate.

Software — Operating system

Examples

Microsoft Windows, Linux, Mac OS X

- Coordinates system resources so it performs and responds predictably for the user.
- Allows users to configure the computer's resources without making permanent changes to them.
- Uses graphical user interface to make it easier for non-technical users to use navigate the system.
- Manages the hardware/software resources so they are used efficiently by applications.

Source: https://support.apple.com/en-us/HT201475

Source: https://blogs.windows.com/windowsexperience/2017/06/14/six-things-need-know-windows-10-s/

Source: https://analyticsindiamag.com/5-reasons-why-linux-os-is-a-hot-favorite-among-coders/

Major operating system families

Microsoft Windows

- Most commonly used operating system.
- User-friendly and used in offices and homes.

  E.g. Windows 8, Windows 10

Source: https://support.apple.com/en-us/HT201475

Source: https://blogs.windows.com/windowsexperience/2017/06/14/six-things-need-know-windows-10-s/

Linux

- Often open-source, meaning that anyone can use or modify Linux operating systems or software.
- Many different ‘flavours’ or significantly varied operating systems.

  E.g. Ubuntu, Debian, Mint, Fedora

Source: https://analyticsindiamag.com/5-reasons-why-linux-os-is-a-hot-favorite-among-coders/

Mac

- Distantly related to Linux operating systems.

  E.g. OS X Lion, OS X Yosemite

Common operating system vulnerabilities

Passwords

- Computers with weak or no passwords can be broken through brute force or dictionary attacks.

File access

- Insecure permissions can give individuals more access to important files than necessary.

Stop Error (BSOD or Blue Screen of Death)

- Windows error screen caused by malware, hardware issues, or software processes that the operating system can’t handle. Users are forced to restart their machine after receiving a BSOD.

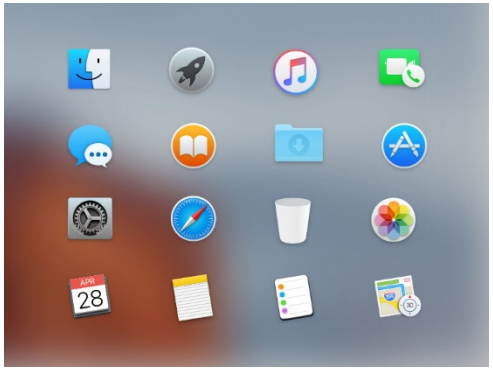
Unpatched systems

- Outdated operating systems have many known, easily exploited vulnerabilities.

Software applications

- Perform tasks to benefit the user.
- Apply computer resources to a specific purpose designated by the user.
- Often designed for a particular type of organisation.
- Sometimes bundled with the OS.

Source: http://www.atozcomputers.net/latest-update/a-to-z-computers-a-/219



Source: https://www.conceptdraw.com/examples/os-x-software-interface-design

Section 2

Virtual machines

What is a virtual machine?

- A virtual machine (VM) is an environment, such as a program or operating system that does not physically exist, but is created within another environment.
- Does not have hardware, a power supply, or other resources that would allow it to run on its own.
- Essentially allows you to run a computer within your computer.

VM terminology

- **Host [operating system]**
  The OS on the physical computer on which the VM is installed.
- **Guest [operating system]**
  The OS the VM runs.
- The Host OS and Guest OS do not need to be the same.
- **Image**
  Another term for VM.
- **Hypervisor**
  Software that can create and run virtual machines.
  E.g. VMware Workstation Player

Advantages

Flexibility

Run multiple OSes on one physical machine.

Scalability

Run multiple VMs on the same computer.

Portability

Easily transfer VMs to different computers.

Cost

Save time testing new programs or configurations on a VM rather than disrupting the host.

Run multiple systems on the same computer (save hardware costs and floorspace).

Disadvantages

- Performance depends on host machine’s hardware.
- Single point of failure.

  If the host fails, progress on VM is lost.
- Running VMs pulls hardware resources from host machines.

VM security

Security benefits

- Unknown software can be tested on virtual machines to ensure it is secure without the risk of damage to the host machine.
- Virtual machines can be isolated enough from host that malware may only be able to infect one OS.
- Snapshots can be used to roll back VMs that have become infected.

Security concerns

- Hypervisors are software that can targeted by attackers if not up-to-date.
- Software within virtual machines and the virtual machine itself must also be kept up-to-date.
- Communications between virtual machines need to be monitored as much as physical machines.

VMware workstation player

- A software program used to create and run VMs.
- Used to run CyberTaipan competition images.
- VMware images contain several files that should not be modified:

**.vmdk: virtual disk files*

Simulate the hard drive for your virtual system

**.vmx: configuration files*

Contain details such as the type of hardware to simulate for the virtual system and the amount of memory to allow the VM to use.

**.nvram: VM's BIOS files*

Checksums

- A mathematical calculation based on the data contained in a file.
- Comparing the checksum of a program you downloaded to the checksum it is supposed to have will allow you to determine if the file has been corrupted or modified.
- Before each round, CyberTaipan teams must verify the checksums of the competition images to make sure the images downloaded correctly.

Open an image

1. Open VMware Workstation Player
2. Click ‘Open a Virtual Machine’
3. Browse for and open the .vmxfile in the image folder you downloaded
4. Click ‘Play virtual machine’
5. Select ‘I copied it’
6. Click ‘OK’ on Removable Devices pop-up
7. Log into the user account specified in the StartEx email if not automatically logged in

Section 3

Networking basics

Networking basics

Servers

Computers dedicated to managing shared resources.

Switch

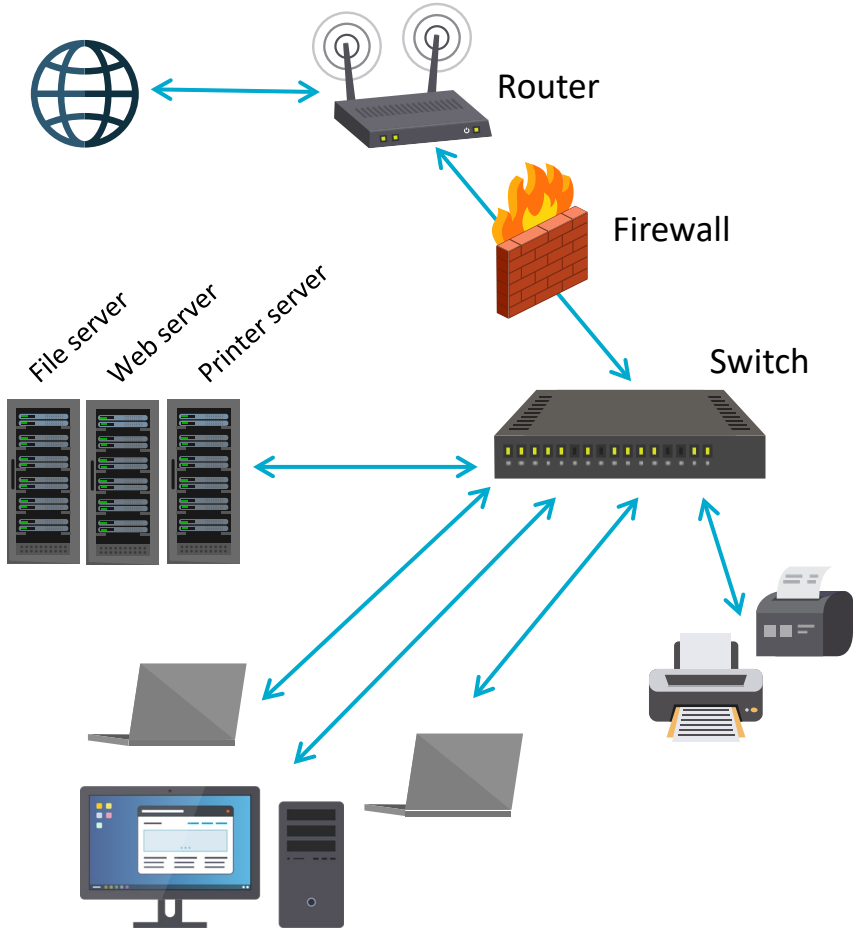
Controls traffic within a network.

Router

Controls traffic between networks.

Firewall

Screen incoming and outgoing traffic for anomalies and potential threats.



Common network cyber security issues

Wireless Access Points

Often have outdated security protocols or no passwords.

Access

Users given access to more data or devices on a network than necessary can inadvertently or purposefully cause security issues.

Email

Social engineering attempts can unleash malware on a network or trick individuals into giving up personal information.

Firewalls

May be improperly configured, giving individuals too much access to a system or network.

Communications

Network traffic containing confidential information that is transported without using Secure Socket Layer (SSL) technology can be easily intercepted.