UNIVERSITY OF DERBY

5CM510 – Network System Development
Lecture 1: Introduction

Instructor Contact & Resources

Ioannis Tsioulis

✉ i.tsioulis@mc-class.gr

github.com/giannis00

Learning outcomes of the module

1. Describe the core concepts of circuit- and packet switched networks, P2P communication, and emerging technologies.
2. Evaluate the impact of bandwidth and other factors on communications.

Learning outcomes of the module

Python network programming knowledge

Your implementation of networking, multithreading, etc.

1. Describe the core concepts of circuit- and packet switched networks, P2P communication, and emerging technologies.

2. Evaluate the impact of bandwidth and other factors on communications.

Investigation and report into emerging technologies including limitations and potential

Modern applications require Network bandwidth

Sensitivity: Internal

Learning, Teaching, and Assessment

- Teaching and learning strategy
  - Lectures 20 hours – Blackboard Collaborate
  - Tutorials/Labs 20 hours – On-site
  - Self study – 150 hours
- Assessment (100% Coursework)
  - Assignment : (100% Coursework)
    - Implementation of a P2P application (50%)
    - Design and Analysis of a Smart Building or Smart City including limitations and potential (50%).

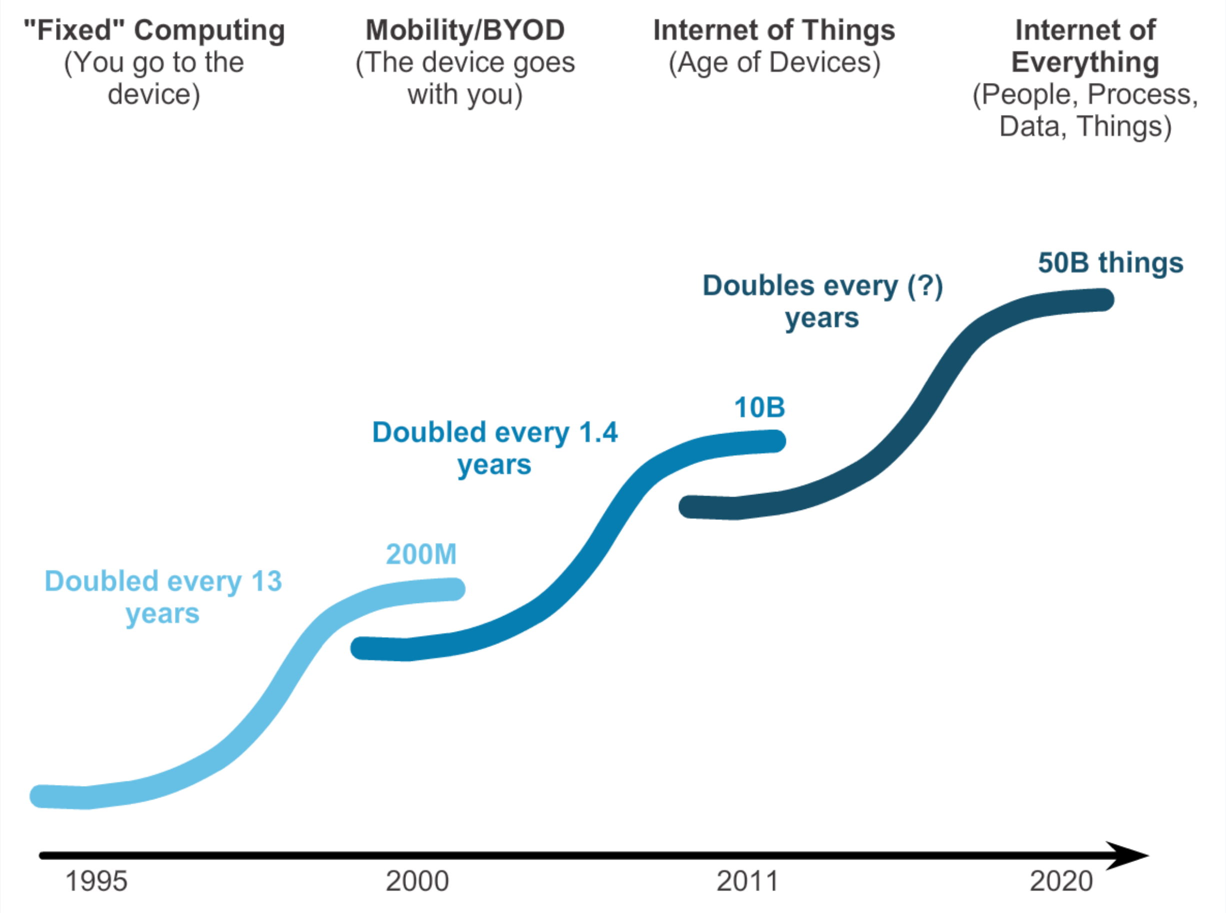
Scheduled Learning and Teaching Activities	**25%**
Guided Independent Study	75%

Module contents

- **Part 1: Network programming:**
  - Circuit-switched networks
  - Packet switched networks
  - P2P networks, Information exchange, data storage and recovery

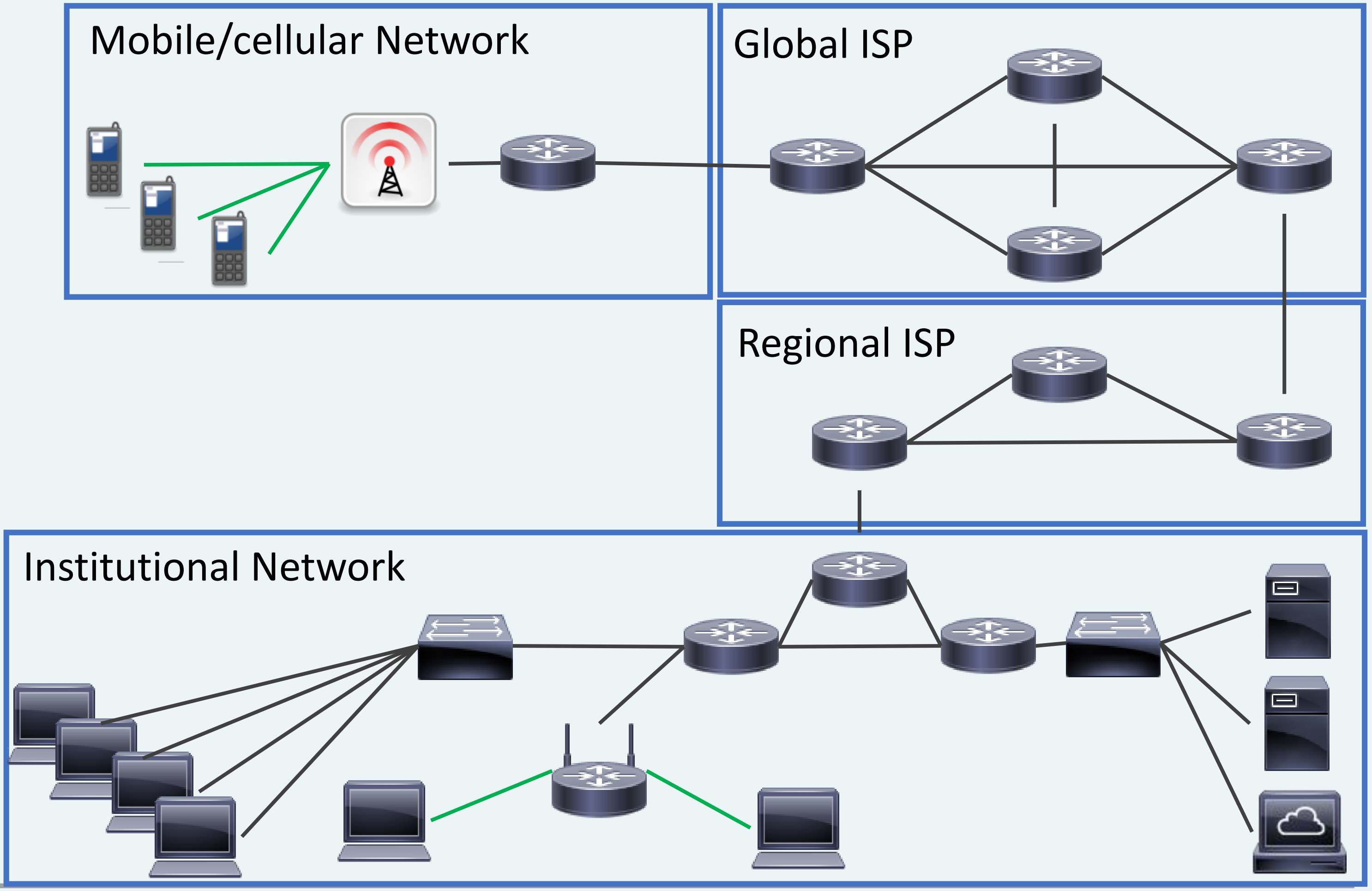
- **Part 2: Emerging paradigms in Networking:**
  - Emerging technologies and paradigms
  - Bandwidth and transport systems

The Internet/networks: our past and future



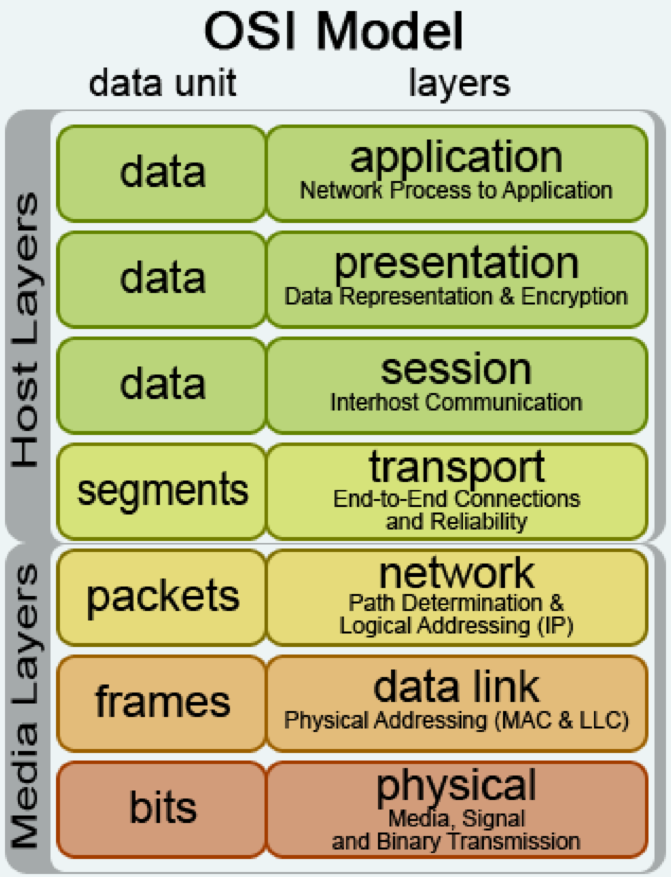
The Internet

- Connected computing devices
  - Hosts = end point systems
  - Running networked applications
- Via communication links
  - Fibre, copper, satellite, etc.
  - With limitations – transmission rate (bandwidth), quality, distance
- Using packet switches
  - Forwarding packets (chunks) of data
  - Via routers and switches



ISO OSI Model

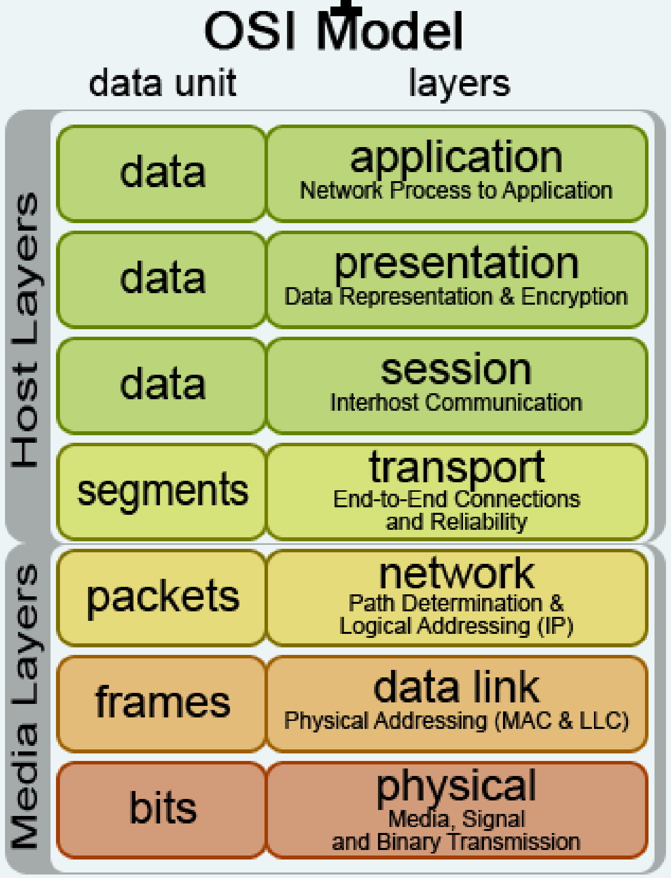
- Open Systems Interconnection model (OSI) is a conceptual model that characterizes and standardizes the communication functions of a computing system without regard of their underlying internal structure and technology.
- The model defined seven layers:
  - Layer 1: Physical Layer
  - Layer 2: Data Link Layer
  - Layer 3: Network Layer
  - Layer 4: Transport Layer
  - Layer 5: Session Layer
  - Layer 6: Presentation Layer
  - Layer 7: Application Layer



OSI Model

	data unit	layers
Host Layers	data	application Network Process to Application
	data	presentation Data Representation & Encryption
	data	session Interhost Communication
	segments	transport End-to-End Connections and Reliability
Media Layers	packets	network Path Determination & Logical Addressing (IP)
	frames	data link Physical Addressing (MAC & LLC)
	bits	physical Media, Signal and Binary Transmission

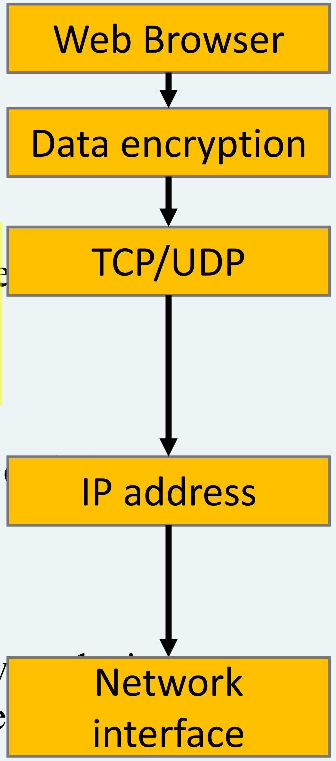
Example of the ISO OSI



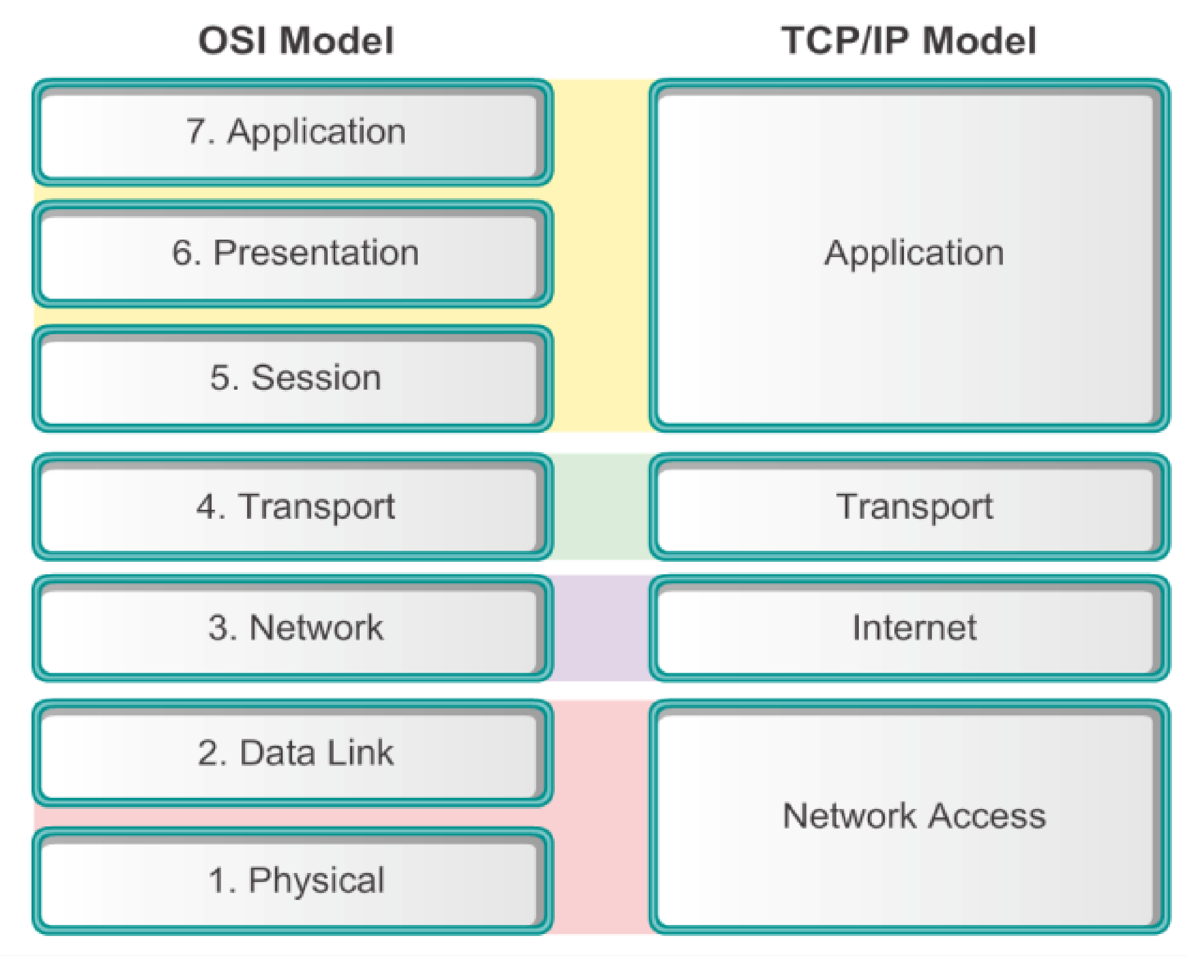
OSI Model

	data unit	layers
Host Layers	data	application Network Process to Application
	data	presentation Data Representation & Encryption
	data	session Interhost Communication
	segments	transport End-to-End Connections and Reliability
Media Layers	packets	network Path Determination & Logical Addressing (IP)
	frames	data link Physical Addressing (MAC & LLC)
	bits	physical Media, Signal and Binary Transmission

- I want to connect to a web page
- **Web Browser**: user interface
- **Data encryption**: secures data algorithmically
- **Transmission control Protocol (TCP)**, which sockets use to support ne between two programs
- **The Internet Protocol (IP)**, which knows how to send small messages packets between different addresses
- **Network interface**: at the very bottom, which consist of network hardw like Ethernet ports and wireless cards, which can send physical message directly linked devices



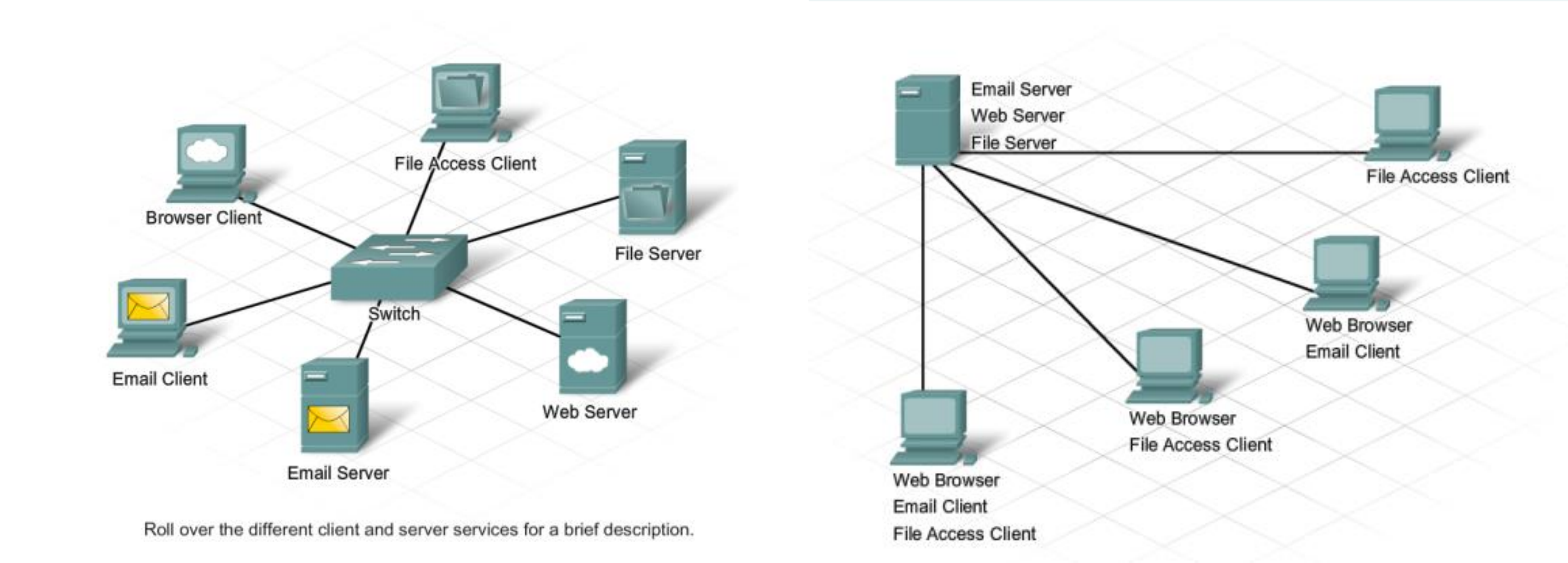
Comparing the OSI and TCP/IP models



Sensitivity: Internal

Providing Resources in a Network

- Clients
  - Computer hosts with software that requests and displays information obtained from a server
- Server
  - Computer hosts configured with software to provide information to other hosts on the network
- Node
  - A device on the network, server, client, or infrastructure



Roll over the different client and server services for a brief description.

Components of a Network

There are three categories of network components:

- Devices
  - Laptops, PCs, switches, routers, wireless access points
- Media
  - Copper and optic fiber cables, wireless transmission
- Services
  - Email and web hosting
- Each of these may be virtualised within the network such that a device may support a virtual network composed of virtual media, devices, and services…

Some examples of end point devices (hosts) are:

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Security cameras
- Mobile handheld devices (such as smartphones, tablets, PDAs, and wireless debit / credit card readers and barcode scanners)

Network Infrastructure Devices

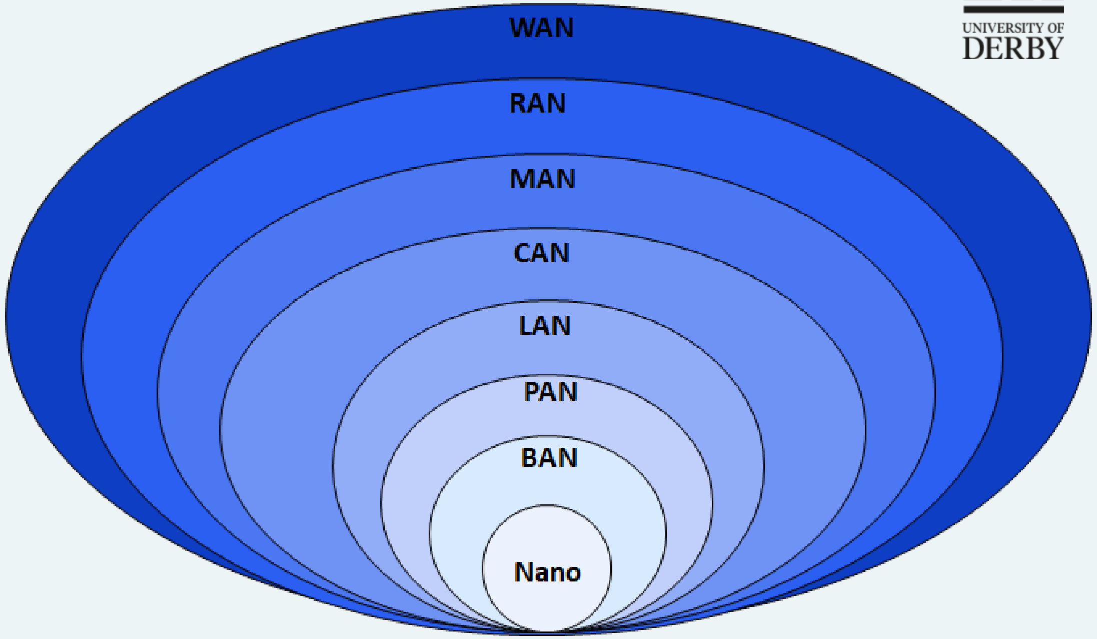
- Interconnect end devices and network infrastructure devices
- Manage data as it flows through the network
- Determines path that messages should take based on destination host address

- Examples of intermediary network devices are:
  - Network access devices (switches, and wireless access points)
  - Internetworking devices (routers)
  - Security devices (firewalls)

LANs and beyond

The two most common types of network infrastructures are:

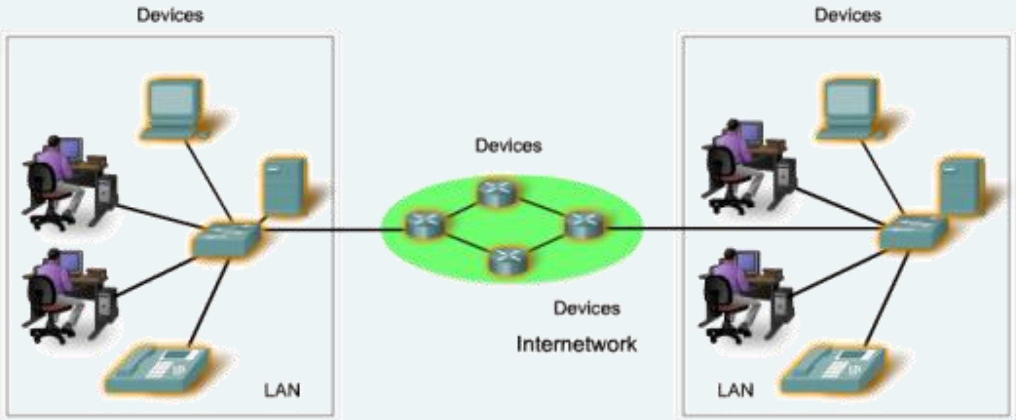
- Local Area Network (LAN)
  - Wireless LAN (WLAN)
  - Storage Area Network (SAN)
- Wide Area Network (WAN)



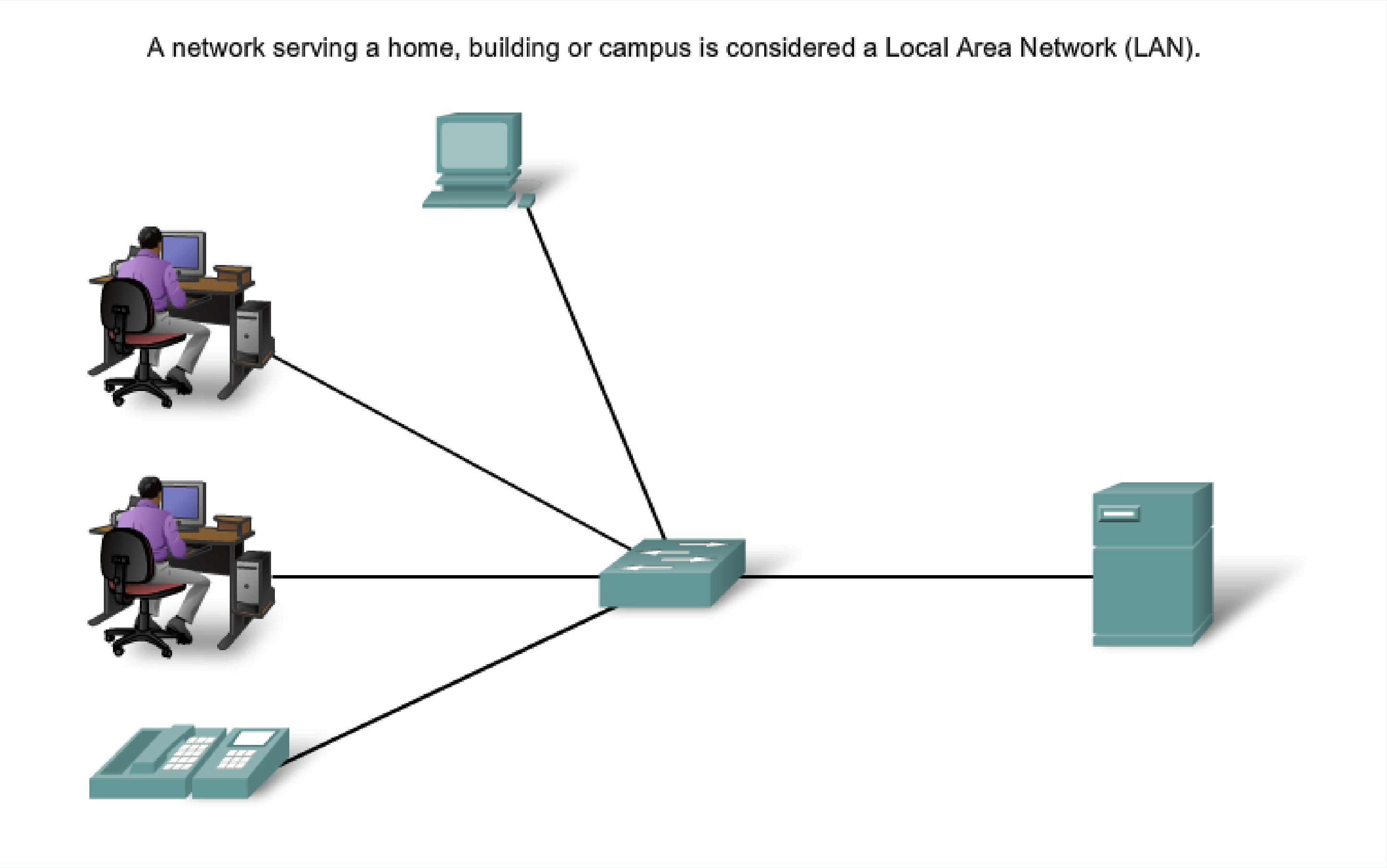
https://en.wikipedia.org/wiki/Personal_area_network#/media/File:Data_Networks_classification_by_spatial_scope.png

Other types of networks cover scales from a single body, to a geographic area, these include include:

- Metropolitan Area Network (MAN)
- Personal Area Network (PAN)



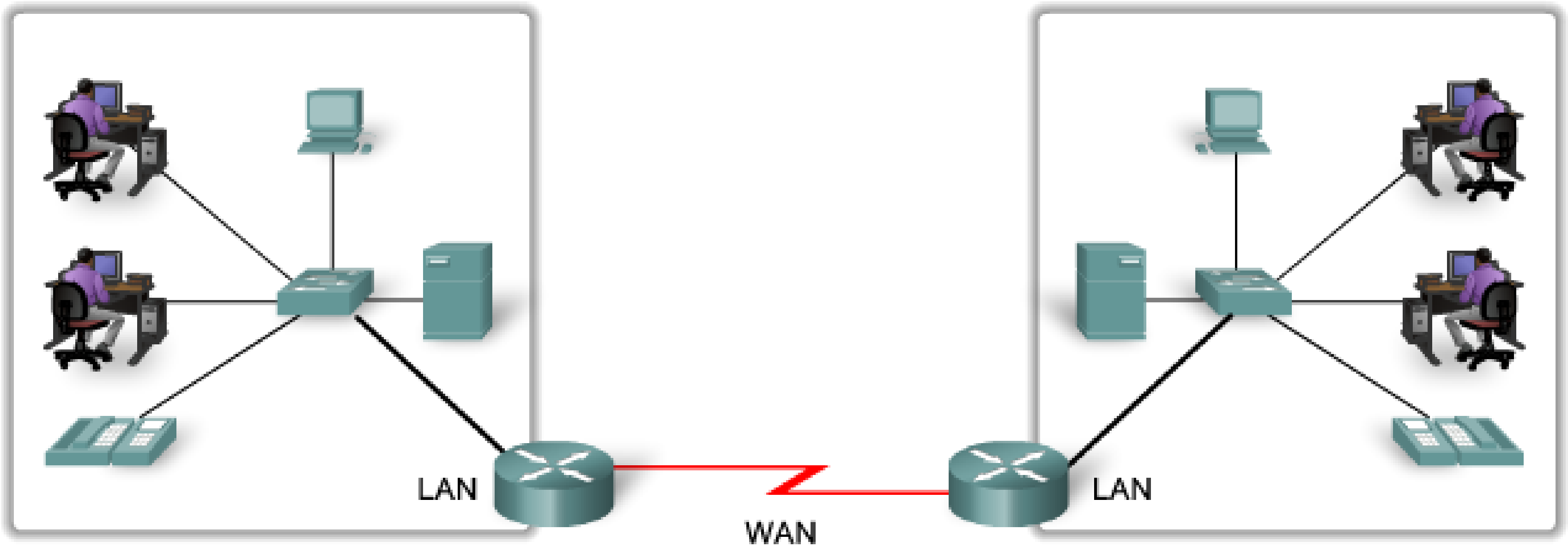
Local Area Networks (LAN)



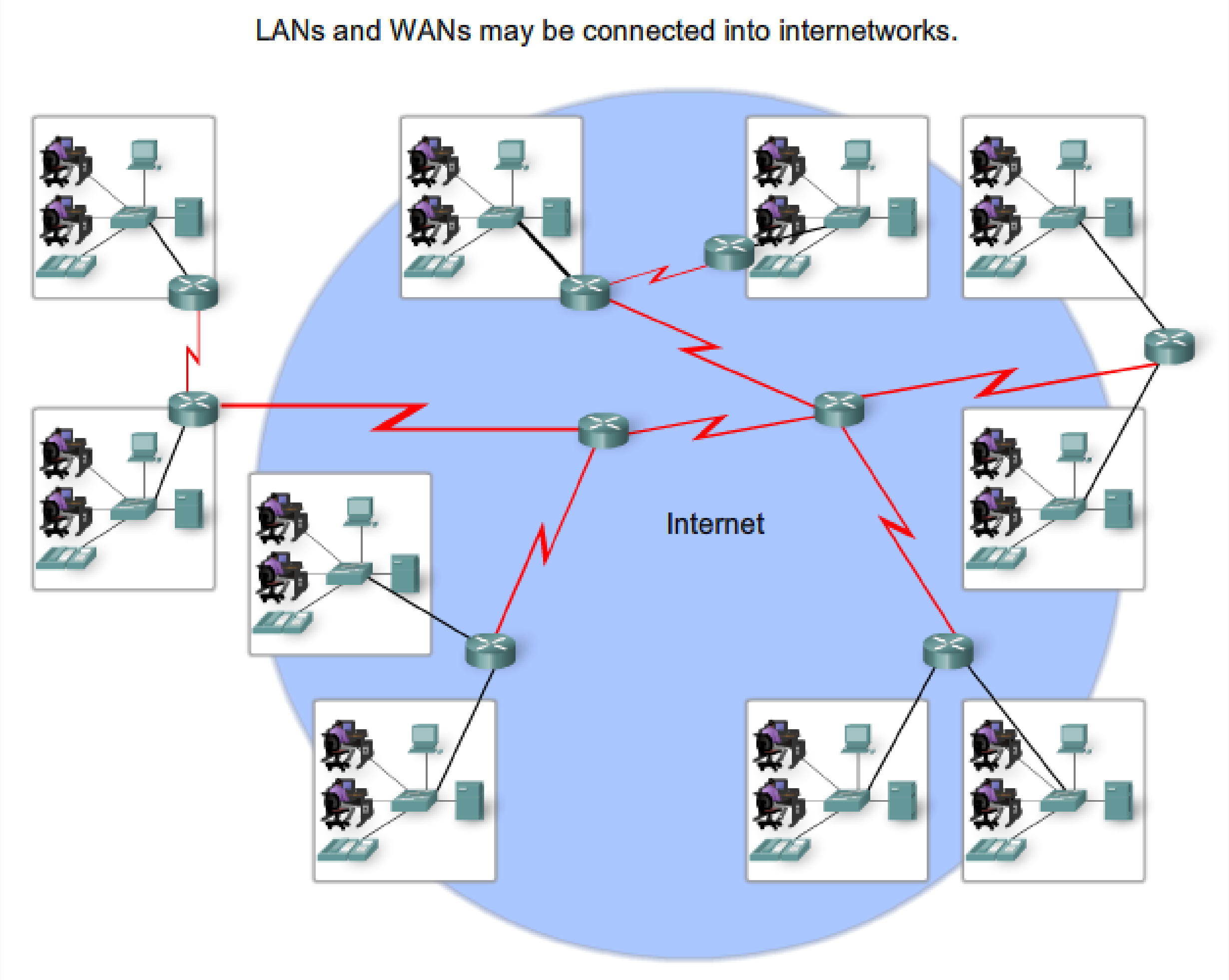
A network serving a home, building or campus is considered a Local Area Network (LAN).

Wide Area Networks (WAN)

LANs separated by geographic distance are connected by a network known as a Wide Area Network (WAN).



Internetworks



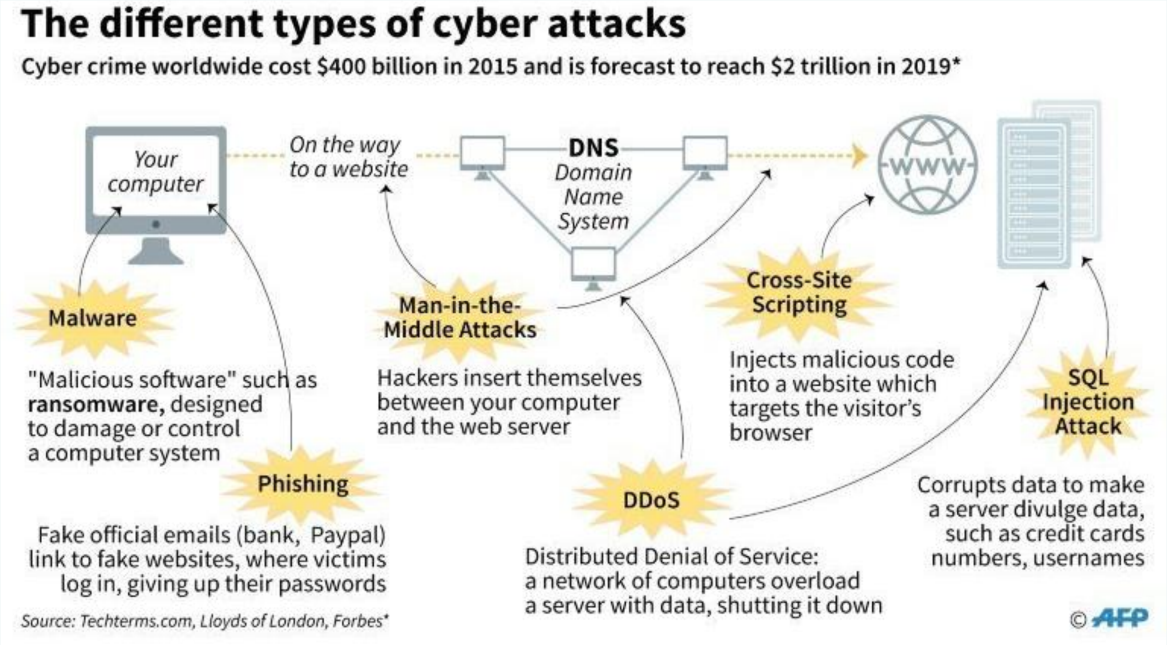
Sensitivity: Internal

What is Network Security

- Network security address the vulnerabilities to which your organisation is exposed as a consequence of being connected to a network
- Who’s vulnerable?
  - Everyone in your organisation who uses computers or network
  - Everyone is your organisation who is affected by the information stored in computers
- Who is attacking?
  - Case studies have shown that a vast majority of attacks originate from within an organisation. (such as ex-employee)

Categories of Threats

- Threats include:
  - Information theft
  - Data loss and/or manipulation
  - Identity theft
  - Disruption of services
- They can happen at any point in the network chain:
  - Phishing – the user
  - Malware – user device
  - MITM – “the network”
  - DDOS – “the infrastructure”
  - XSS – “the service”
  - SQL injection – data storage



The different types of cyber attacks

Cyber crime worldwide cost $400 billion in 2015 and is forecast to reach $2 trillion in 2019*

Malware
"Malicious software" such as **ransomware,** designed to damage or control a computer system

Phishing
Fake official emails (bank, Paypal) link to fake websites, where victims log in, giving up their passwords

Man-in-the-Middle Attacks
Hackers insert themselves between your computer and the web server

DDoS
Distributed Denial of Service: a network of computers overload a server with data, shutting it down

Cross-Site Scripting
Injects malicious code into a website which targets the visitor’s browser

SQL Injection Attack
Corrupts data to make a server divulge data, such as credit cards numbers, usernames

Source: Techterms.com, Lloyds of London, Forbes*

© AFP

Sensitivity: Internal

Vulnerabilities and Threats

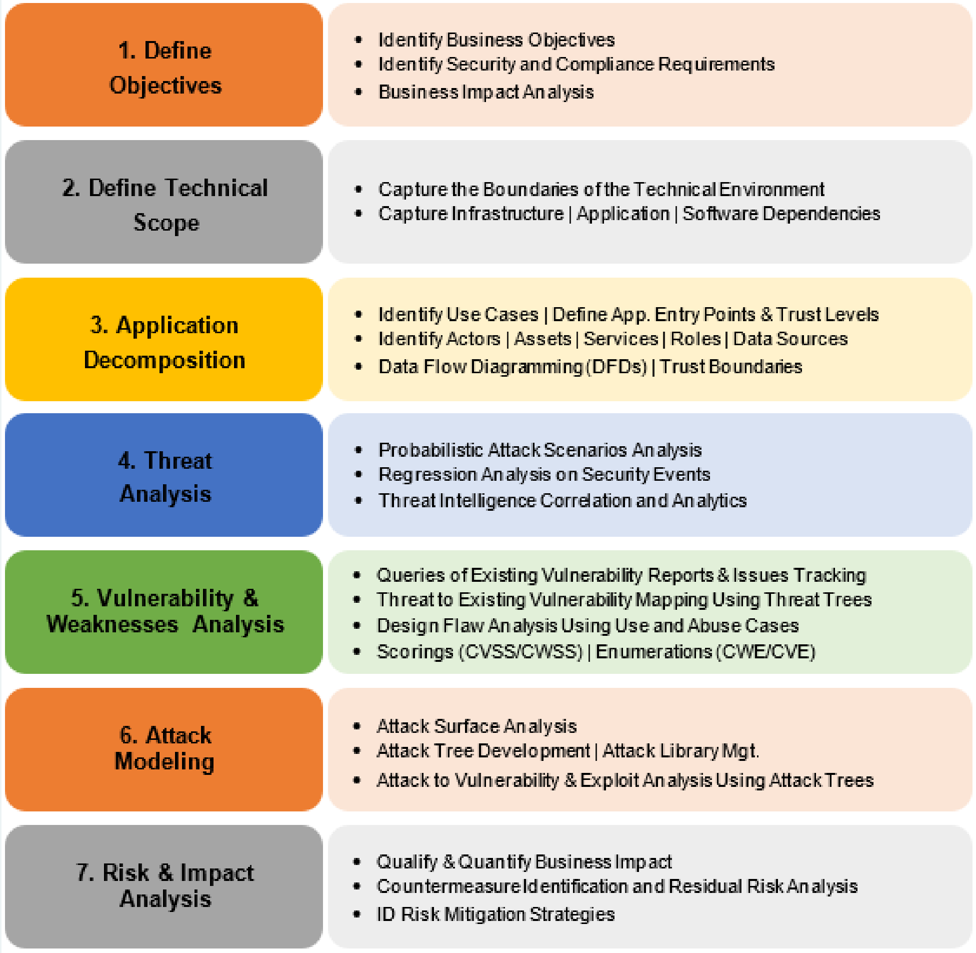
- Network security refers to any activities designed to protect your network
  - Reliability and safety of your network and data.
  - Effective network security targets a variety of threats and stops them from entering or spreading on your network
- What are the threats to my network?
  - A virus - malicious software that is attached to another program to execute a particular unwanted function on a workstation.
  - A Trojan horse - the entire application was written to look like something else, when in fact it is an attack tool.
  - Worms - self-contained programs that attack a system and try to exploit a specific vulnerability in the target. The worm copies its program from the attacking host to the newly exploited system to begin the cycle again.

How Does Network Security Work

- Network security is accomplished through hardware and software
- A network security system usually consists of many components work together, which minimizes maintenance and improves security
    - **Anti-virus and anti-spyware**: the software must be constantly updated and managed to protect you from emerging threats
    - **Firewall**, to block unauthorized access to your network
    - **Intrusion prevention systems (IPS)**, to identify fast-spreading threats
    - **Virtual Private Networks (VPNs)**, to provide secure remote access

Information Security

- Multiple current standards:
  - ISO 27001
  - NIST Cybersecurity Framework
  - U.S. Banking Standards
  - IASME Governance
  - ESTI Cyber Security Technical Committee
- Aim:
  - Provide information to companies
  - Provide a series of guidelines to manage information
  - Provide a guide to implementing security and privacy
- We will look at these later

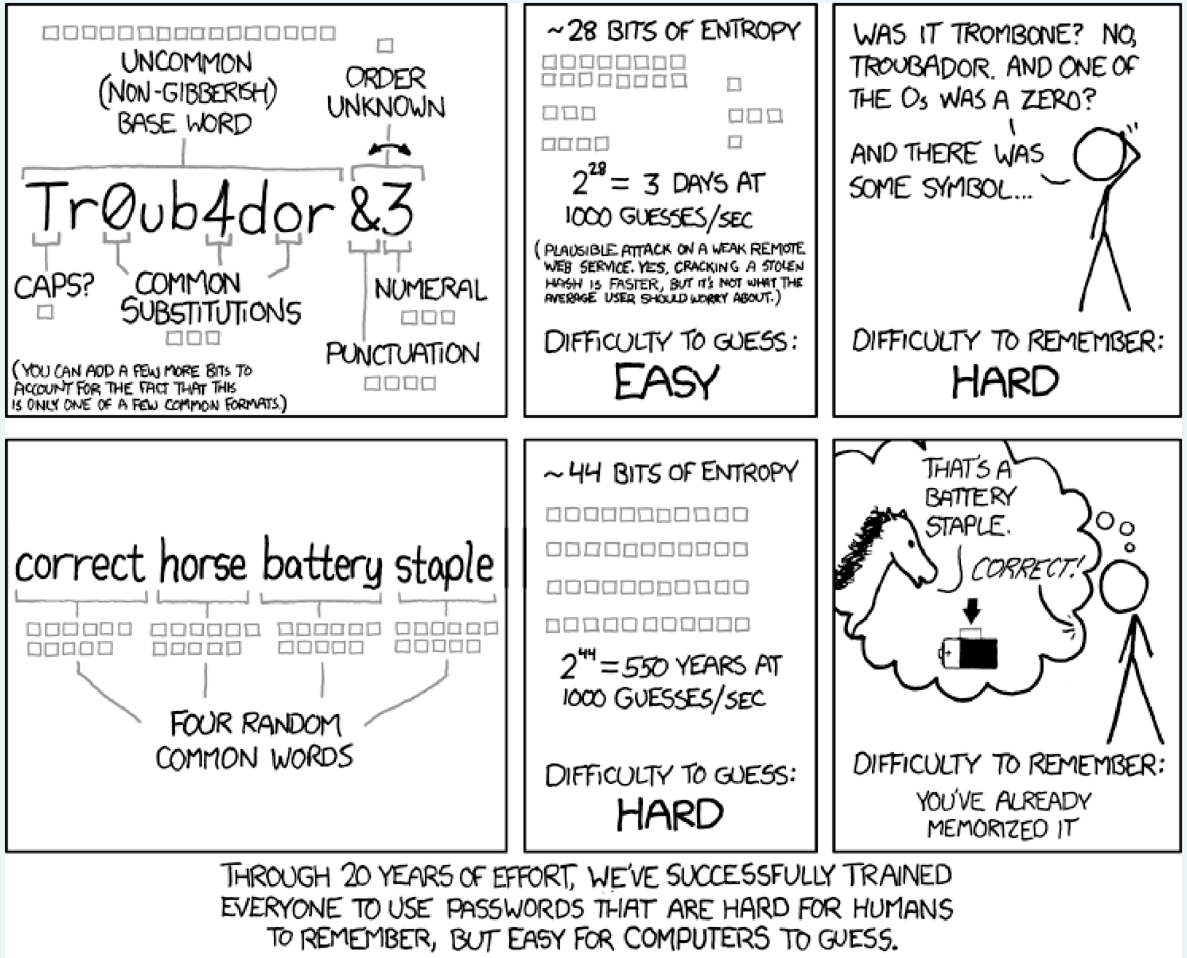


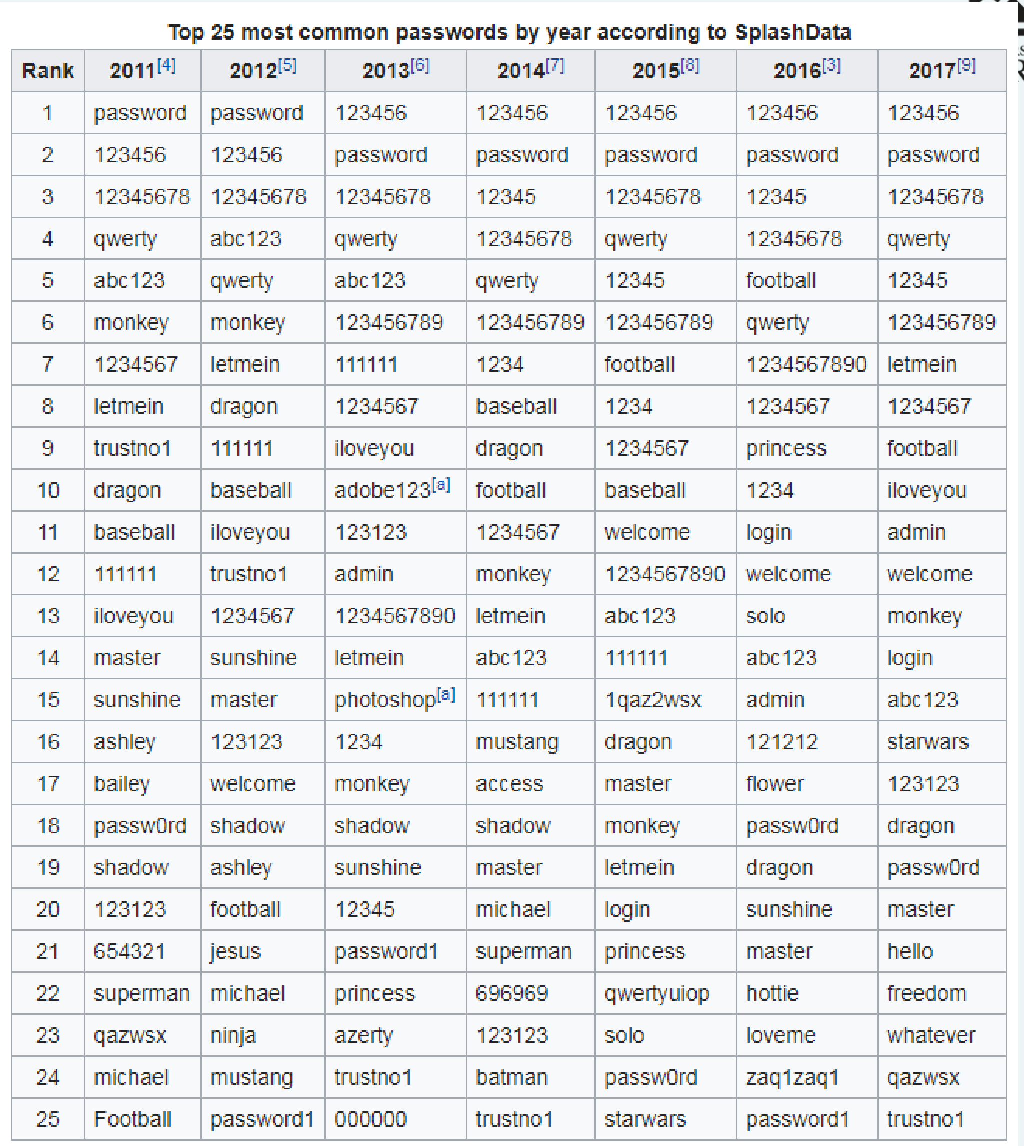
1. Define Objectives	• Identify Business Objectives • Identify Security and Compliance Requirements • Business Impact Analysis
2. Define Technical Scope	• Capture the Boundaries of the Technical Environment • Capture Infrastructure | Application | Software Dependencies
3. Application Decomposition	• Identify Use Cases | Define App. Entry Points & Trust Levels • Identify Actors | Assets | Services | Roles | Data Sources • Data Flow Diagramming (DFDs) | Trust Boundaries
4. Threat Analysis	• Probabilistic Attack Scenarios Analysis • Regression Analysis on Security Events • Threat Intelligence Correlation and Analytics
5. Vulnerability & Weaknesses Analysis	• Queries of Existing Vulnerability Reports & Issues Tracking • Threat to Existing Vulnerability Mapping Using Threat Trees • Design Flaw Analysis Using Use and Abuse Cases • Scorings (CVSS/CWSS) | Enumerations (CWE/CVE)
6. Attack Modeling	• Attack Surface Analysis • Attack Tree Development | Attack Library Mgt. • Attack to Vulnerability & Exploit Analysis Using Attack Trees
7. Risk & Impact Analysis	• Qualify & Quantify Business Impact • Countermeasure Identification and Residual Risk Analysis • ID Risk Mitigation Strategies

Introduction to Securing Devices

- Part of network security is securing devices, including end devices and intermediate devices.
- Default usernames and passwords should be changed immediately.
- Access to system resources should be restricted to only the individuals that are authorized to use those resources.
- Any unnecessary services and applications should be turned off and uninstalled, when possible.
- Update with security patches as they become available.

Passwords


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^{28} = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^{44} = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



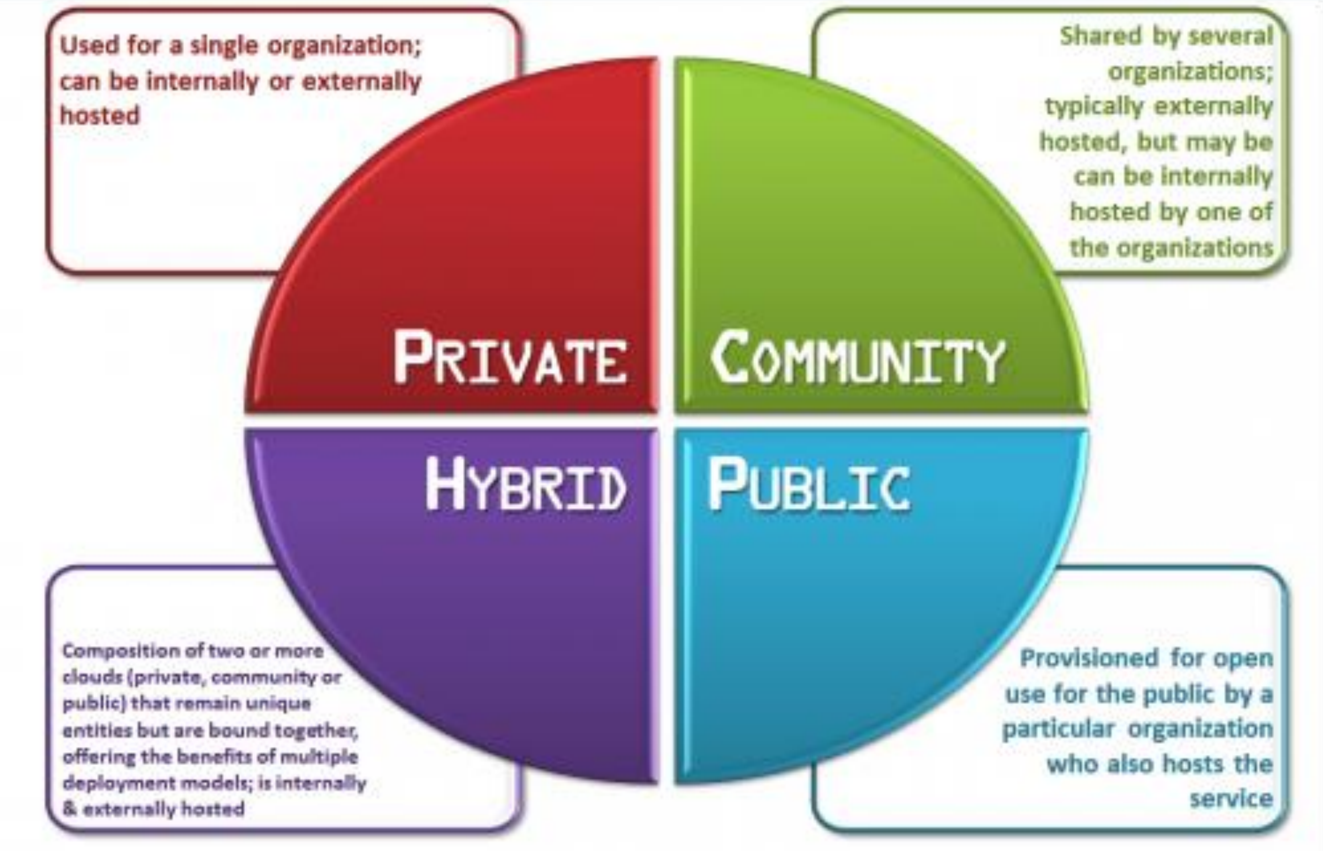
Top 25 most common passwords by year according to SplashData

Rank	2011[4]	2012[5]	2013[6]	2014[7]	2015[8]	2016[3]	2017[9]
1	password	password	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345	12345678
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty
5	abc123	qwerty	abc123	qwerty	12345	football	12345
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789
7	1234567	letmein	111111	1234	football	1234567890	letmein
8	letmein	dragon	1234567	baseball	1234	1234567	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess	football
10	dragon	baseball	adobe123[a]	football	baseball	1234	iloveyou
11	baseball	iloveyou	123123	1234567	welcome	login	admin
12	111111	trustno1	admin	monkey	1234567890	welcome	welcome
13	iloveyou	1234567	1234567890	letmein	abc123	solo	monkey
14	master	sunshine	letmein	abc123	111111	abc123	login
15	sunshine	master	photoshop[a]	111111	1qaz2wsx	admin	abc123
16	ashley	123123	1234	mustang	dragon	121212	starwars
17	bailey	welcome	monkey	access	master	flower	123123
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd	dragon
19	shadow	ashley	sunshine	master	letmein	dragon	passw0rd
20	123123	football	12345	michael	login	sunshine	master
21	654321	jesus	password1	superman	princess	master	hello
22	superman	michael	princess	696969	qwertyuiop	hottie	freedom
23	qazwsx	ninja	azerty	123123	solo	loveme	whatever
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1	qazwsx
25	Football	password1	000000	trustno1	starwars	password1	trustno1

Sensitivity: Internal

Cloud Computing

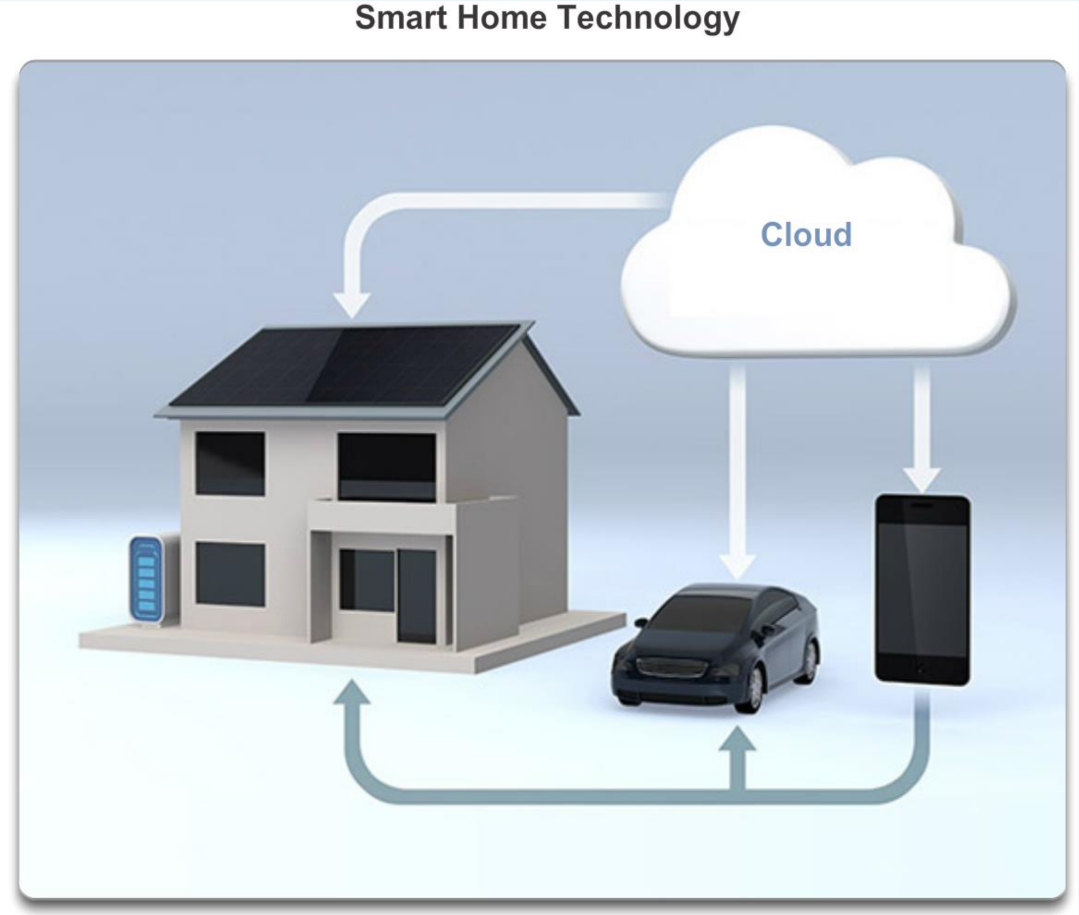
- There are four primary types of clouds:
  - Public clouds
  - Private clouds
  - Custom clouds
  - Hybrid clouds


Used for a single organization; can be internally or externally hosted
Shared by several organizations; typically externally hosted, but may be can be internally hosted by one of the organizations
PRIVATE
COMMUNITY
HYBRID
PUBLIC
Composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models; is internally & externally hosted
Provisioned for open use for the public by a particular organization who also hosts the service

Technology Trends

- Smart home technology
  - Technology that is integrated into every-day appliances allowing them to interconnect with other devices, making them more 'smart' or automated

- IoT – Internet of things
- SDN - Software-Defined Networking
- Quantum networking/Internet
- Mist, Fog and Edge Computing



Sensitivity: Internal

Reading list

- Websites:
  - https://diveintopython3.net/
  - https://www.slitherintopython.com/
  - https://www.w3schools.com/python/
  - https://realpython.com/
  - https://automatetheboringstuff.com/
  - https://www.reddit.com/r/Python/
- Home install:
  - Ensure you have a Jetbrains account (www.jetbrains.com/student)
  - Install Python 3.8.5 or later and PyCharm (https://www.jetbrains.com/pycharm/download)
- Week 1 objectives:
  - Become familiar with Packet Tracer and Python basics (selection, iteration, functions, classes, libraries)

UNIVERSITY OF DERBY

University of Derby, Kedleston Road, Derby, DE22 1GB
T +44 (0)1332 591044 **E** opendays@derby.ac.uk

THANK YOU

derby.ac.uk

Sensitivity: Internal