Learning Aims

- Describe why network security is important
- Explain how network vulnerabilities are identified
- Describe methods of protecting networks

Importance of network security

- When computing devices are connected in a LAN and then connected to the internet, they become vulnerable to attacks and misuse.
- A network and the *servers* connected to it are likely to contain large amounts of information. This information could be valuable and some of it is likely to be private and confidential.
- For example, a school network is likely to have:
  - names and addresses of students and staff
  - medical details of students
  - grades from exams
  - details of behaviour from reports
  - details of the financial state of the school
  - details of staff salaries
- This information needs to be kept secure and most of us wouldn’t be happy if our personal information was available to people who didn’t need it.

Types of weaknesses

An organisation needs to be able to rely on the *data* it is storing about its staff, customers and products or services. There are several dangers that are inherent in using *networks*:

- *Malware* - these may be sent via the internet, email, or as part of a hack
- Brute force and data interception - if traffic can be intercepted then there is a possibility of accessing financial and personal data
- Social engineering

Malware	**Brute force**	**Social Engineering**
Malware can delete or corrupt files, cause computers to crash or slow down, and even encrypt data. It can also secretly record keystrokes, allowing hackers to access sensitive information like passwords for email or bank accounts. In a network environment, malware can **easily spread** from an infected client to the server and other connected clients, facilitating rapid infection spread.	Attempts by hackers to gain unauthorized access to corporate systems in order to steal data and sensitive information. Data interception occurs when users' usernames and passwords are compromised, leading to unauthorized access to systems and potential disclosure and theft of corporate data. Packet sniffers, devices that allow hackers to listen to data being transferred on a network, enabling them to access usernames and passwords.	Many system vulnerabilities are caused by people's carelessness, making them the weak point in the system. Examples of careless behaviour include: Not installing operating system updates, neglecting to update anti-malware software, Not securing computer rooms or logging off, Leaving sensitive information on desks, writing passwords on sticky notes, sharing passwords Losing memory sticks and laptops Not applying security measures to wireless networks, and failing to encrypt data.

Data Breaches

- If this data is breached it could:
- cost the organisation money through lost business, payments to recover the data or payment of ransom demands
- cause the organisation to incur a fine for failing to keep the data safe or for breaking the law by failing to comply with the *Data Protection Act*/General Data Protection Regulation (GDPR)
- make customers lose trust in the business if they fail to keep their personal details safe
- allow competitors to win business by gaining access to confidential client information

Ethical Hacking and Penetration testing

- **Ethical hacking** is ‘good’ hacking by looking for weaknesses in the software and systems. They work on behalf of an organisation, simulating the actions of a hacker, known as **Pen testing**

- Penetration testing is the process of attempting to gain unauthorized access to a network in order to find and fix vulnerabilities.

- There are two types of penetration testing: white box and black-box testing.

  - **White box testing** simulates a scenario where an insider with knowledge of basic credentials and login information attempts to breach security.

  - **Black-box testing**, on the other hand, simulates an external hacking attempt on an organization or company, similar to what is often portrayed in the media.

Types of hackers

- There are three categories of hackers: black-hat, white-hat, and grey-hat hackers.

- **Black-hat hackers** are typically associated with malicious intent and attempt to gain unauthorized access to steal information or cause damage.

- **White-hat hackers** are security experts employed by companies to find and fix vulnerabilities in their own software.

- **Grey-hat hackers** are not officially employed by a company but still try to find flaws in company systems and inform them to fix it.

Methods for protecting networks

- Methods of network protection include:

Access control &
Authentication

Firewalls

Physical security

Encryption

Access Control

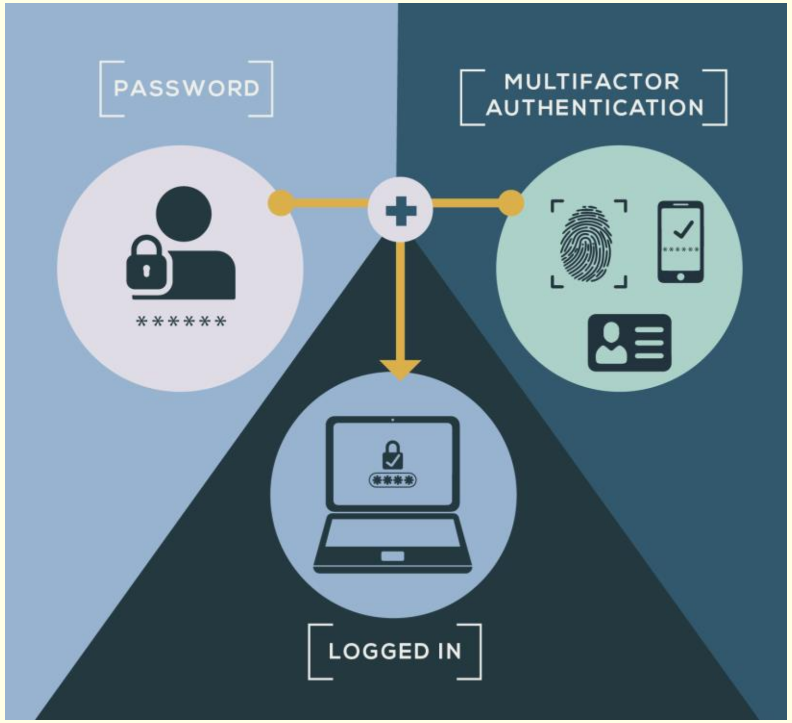
- Access control determines the facilities a user has access to, such as
  - software
  - email
  - internet
  - documents and data
  - the ability to install and/or remove software
  - the ability to maintain other users' accounts
  - File permissions – read only, read/write, execute a program file, delete

- A *network manager* should restrict most users to allow them to access only the facilities they need.

- For example, an office worker might need access to productivity software, email and the internet, but not to install software or access to other users' accounts. Restriction limits the actions a user can take, reducing the potential of threats. The restrictions can be precise, allowing different people access to different sets of *files* or information.

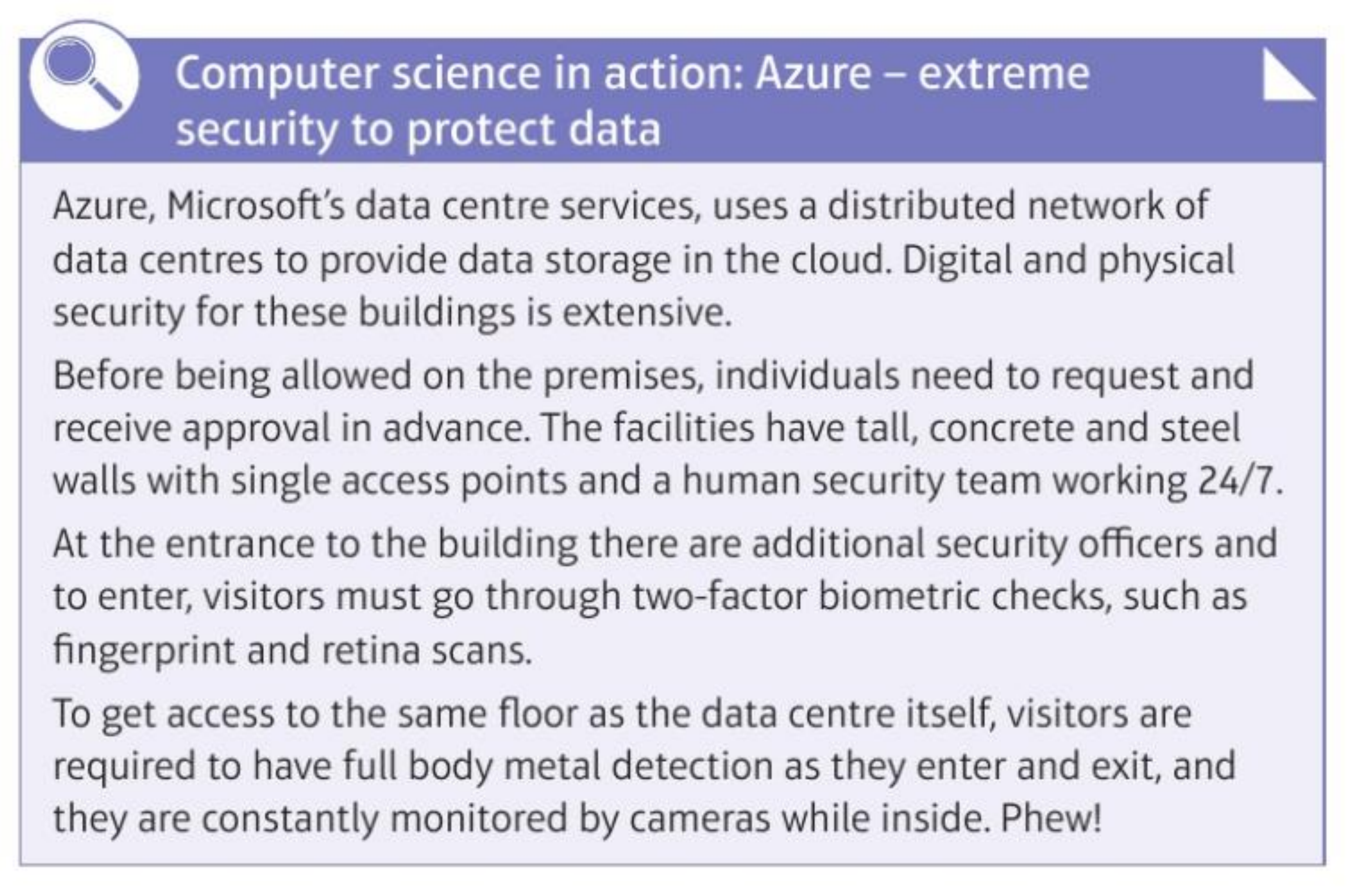
Authentication techniques

- There are many ways that a network can ask a user to prove they are who they claim they are. This can include:
  - using suitable user ID and passwords
  - using a PIN
  - drawing a pattern on a smartphone
  - using face and voice recognition
  - sending an email confirmation to ensure they are the correct person when making an online order



Physical security

- Physical security means restricting physical access to important parts of a network. For example, servers should be kept in a locked, secure room that can only be accessed by authorised people, such as the network manager.
- This is important as anyone with physical access to a *server* could remove or access the *hard disks* containing private and confidential information.



Computer science in action: Azure – extreme security to protect data

Azure, Microsoft's data centre services, uses a distributed network of data centres to provide data storage in the cloud. Digital and physical security for these buildings is extensive.

Before being allowed on the premises, individuals need to request and receive approval in advance. The facilities have tall, concrete and steel walls with single access points and a human security team working 24/7.

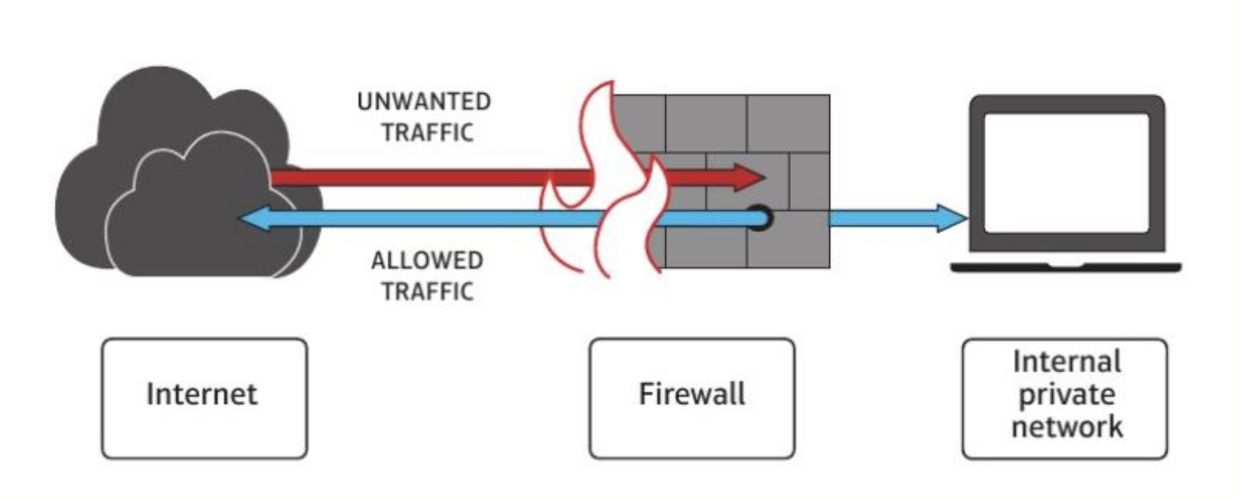
At the entrance to the building there are additional security officers and to enter, visitors must go through two-factor biometric checks, such as fingerprint and retina scans.

To get access to the same floor as the data centre itself, visitors are required to have full body metal detection as they enter and exit, and they are constantly monitored by cameras while inside. Phew!

Firewalls

A firewall monitors traffic entering and leaving a network.

- A firewall is a tool that monitors traffic going into and out of a computer or network, and either allows the traffic to pass through or blocks it.
- The decision to allow or block traffic is based on rules, known as the firewall policy.
- For example,
  - Stop certain protocols, for example FTP
  - Block data coming from certain network addresses
  - Flag suspicious activity
  - Some programs, such as *email clients* and *web browsers*, have legitimate cause to send a transmission.
  - These programs are known to the system and the firewall policy allows their communications.
  - However, any transmissions that are not sent from, or to, known and allowed sources are blocked.
  - Firewalls can be hardware-based or software-based. *Hardware* firewalls tend to be more expensive, but are more effective.


UNWANTED TRAFFIC
ALLOWED TRAFFIC
Internet
Firewall
Internal private network