UNITED ARAB EMIRATES
MINISTRY OF EDUCATION

Networks and The Internet

Cycle 3 – Grade 10

Chapter 2
Networks and the internet

Chapter overview

In this chapter, you will learn about cybersecurity and network related threats. You will learn about various types of data and how it can be affected by malware and other attacks. You will recomend recommend hardware topologies, protocols and addressing that can be used to implement networks for a range of purposes.You will learn basic concepts in network usability and security. You will learn about the relationship between network usability and security measures and discuss trade-offs when choosing between usability and security. You will also learn about cybersecurity trade-off and how to implement security measures in various trade-off situations.

Section 1: Network threats and implementation

Aim

In this section, you will learn about cybersecurity and network related threats. You will learn about various types of data and how it can be affected by malware and other attacks. You will recommend hardware topologies, protocols and addressing that can be used to implement networks for a range of purposes. You will also evaluate the scalability and reliability of a range of networks.

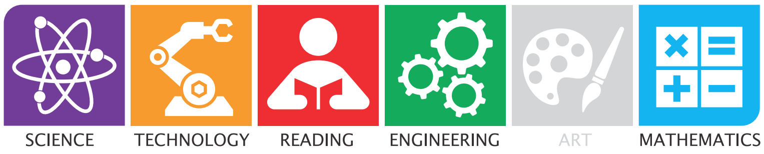
Learning outcomes

- Explain how examples of sensitive data can be affected by malware and other attacks.
- Recommend a range of appropriate hardware, topologies, protocols and addressing to implement a network for a given purpose.
- Evaluate the scalability and reliability of a range of networks by describing the relationship between hardware, topologies, protocols and addressing.

Prior knowledge

- Networking
- Programming

My STREAM Focus



Key vocabulary

WORD	MEANING	PICTURE
malware	software written to harm or cause issues in a computer also called malicious code	
cybersecurity	process to protect individuals, organisations and governments from digital attacks	
scalability	scalability is the ability for IT systems such as applications, storage, databases and networking to continue to change in size	
reliability	reliability of IT systems is a measurement of how consistently an IT system or component performs	

What is cybersecurity?

Cybersecurity is a process to protect individuals, organisations and governments from digital attacks. In this process, the networked systems and data are protected from attackers. Data needs to be protected at three levels:

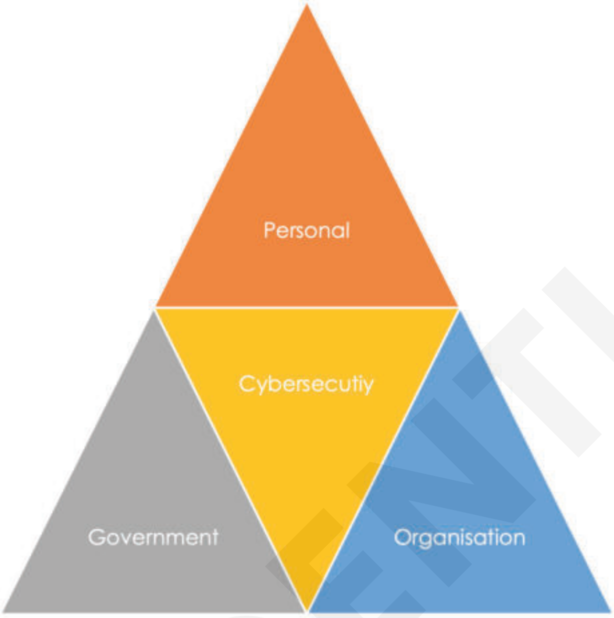


Figure 2.1.1: Cybersecurity levels

- At a personal level, there is a need to protect one's identity, data and computing devices from cybercriminals, as they will invade privacy and damage peoples reputations.
- At the organisational level, there is a need to protect the organisation's data from cybercriminals.
- At the government level, there is a need to protect data where national security, economic stability and wellbeing of people are at risk.

Personal level

Personal data is any information that is used to identify a person. Personal data can exist both offline and online.

When you are not connected to the internet, you are offline. Examples of offline data are real-life personal information like name, contact details, email address, or identification number.

When you are connected to the internet, you are online. Few examples of online data are username, the social identity you establish and portray on online communities and websites.

Figure 2.1.2: A man who is working offline

Figure 2.1.3: A man who is working online

Complete activities 2.1.1 and 2.1.2 in the workbook

Collection of personal data

Personal data are collected in different ways from different places. Smart devices can access peoples personal data. Personal data are collected when people access digital copies like bank account statements through the bank's website or mobile banking apps. Even when utility bills are paid, people initiate an online payment using mobile banking app from which personal data are collected.

As the information online is freely available, privacy is compromised. Computing devices can also generate information about a person. Personal data is collected from wearable technology such as smartwatches and activity trackers for clinical research, health monitoring, and fitness and wellbeing tracking.

Social media is a huge platform where personal data can be collected. It earns income by selling targeted advertising based on customer data that has been mined using algorithms or formulas.

Figure 2.1.4: Social media platforms

DID YOU KNOW?

Social media knows you better than anyone. It knows your:

- friends
- interests
- movements/travels

Social media platform accounts can track users preferences and demographic data. Personal data can be collected from social media platforms through user posts, likes, and search activities.

Figure 2.1.5: Persona = Person + Activity

A persona is a fictional character created based on research data collection. Big data companies and scientists collect social media data and build personas that determine age, gender or interest.

Complete activity 2.1.3 in the workbook

Cybercriminals can also steal a person's identity and ruin their life. This is called identity theft. For example, a cybercriminal can get someone else's medical benefits and medical insurance by stealing their identity. In banking, an identity thief can steal a person's money or even take loans in their name and ruin their credit rating.

Complete activity 2.1.4 in the workbook

Types of data

Organisations can collect data that can be transactional, intellectual, or financial.

- Transactional data in an organisation are related to buying and selling, production activities and basic organisational operations such as any information used to make employment decisions.
- Intellectual property data are patents, trademarks and new product plans, which allow an organisation to gain an economic advantage over its competitors.
- Financial data are income statements, balance sheets and cash flow statements, which provide insights into the health of a company.

Data are also collected from the IoT network. An IoT network is a network that is connected to the internet and uses cloud storage.

John McCumber created a model framework in 1991 called the McCumber Cube. The McCumber Cube was designed to help organisations evaluate information security initiatives by considering all related factors that impact them.

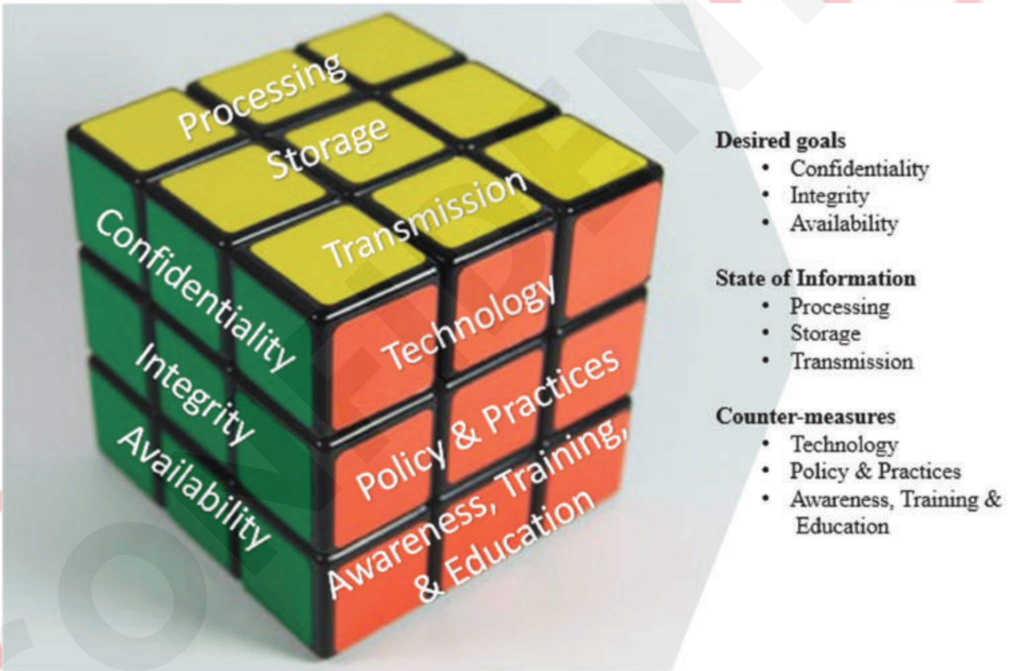


Figure 2.1.6: McCumber Cube

This security model has three dimensions, desired goals, states of information and counter-measures.

Security model	Description	Methods used to achieve
Desired goals	**Confidentiality** Information can be accessed only by those who should see it.	Data encryption Identity proofing and authentication
	Integrity Information is protected and is not changed outside of proper processes.	Specific algorithms are used to maintain data integrity.
	Availability Information is accessible only when it is wanted.	Maintaining equipment, performing hardware repairs, updating software, and creating backups.
States of Information	**Processing** Data is processed using different operations in the database.	Operating methods during data processing are updating, deleting, adding to database records.
	Storage Data is stored in different storage mediums.	Data are stored in memory, hard drive, solid-state drive or in a USB drive.
	Transmission Data transmission is data travelling between information systems.	Data transmissions can happen between two or more digital devices.
Counter-measures	**Technology** Technology is the software and hardware-based solutions which are designed to protect information systems.	Implementing firewalls to the network to continuously monitor and search for malicious incidents.
	Policy and procedure Policy and procedure in an organisation are ways to implement information assurance for security.	Incident response plans and best practice guidelines.
	Awareness, training, and education Giving the user the information and knowledge of how to identify and handle threats.	Different kinds of awareness, training and education methods are used.

Table 2.1.1 Security model

Government data

Today's government organisations must meet the increasing demand for sensitive information from government employees, citizens, and vendors while protecting that data from increasingly sophisticated and persistent threats.

Government data is available in various formats, including structured data such as names and dates and unstructured data such as audio files. Data must be protected against outside attacks such as advanced malware and insider threats while managing privileged-user access. Data must be shared securely within and outside the organisation, on and off the network as needed.

Complete activity 2.1.5 in the workbook.

Types of cybersecurity threats

Cybersecurity threats are malicious activities by an individual or organisation to steal or damage the data, gain access to a network system, and disrupt digital life. The following are the threats available today:

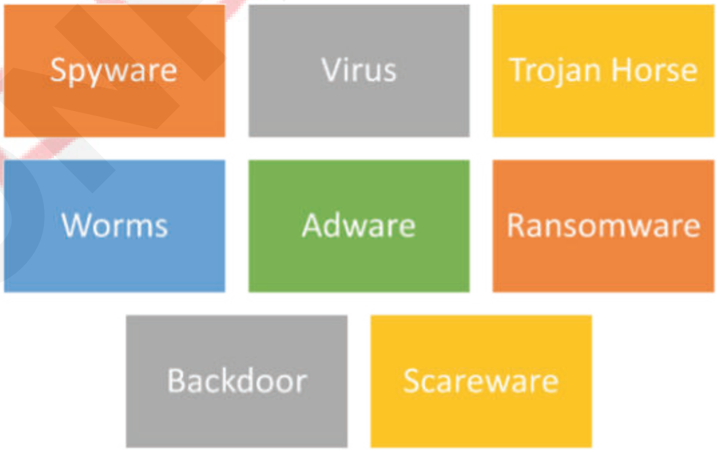
- Malware
- Social engineering
- Denial-of-service
- Wi-Fi password cracking

Malware

Malware is software written to harm or cause issues with a computer. This is also called malicious code. This code comes in several forms and either harm or steals data from a computer system. Cybercriminals use many different types of malware or malicious software to carry out their activities.

Types of malware

There are several types of malware, as shown in Figure 1.1.7.



Spyware

Virus

Trojan Horse

Worms

Adware

Ransomware

Backdoor

Scareware

Figure 2.1.7: Malware

1. Spyware

Spyware is a type of malware that is designed to spy on a computer system. It secretly collects the activities on a computer system and then sends the collected data to another person without the awareness of the computer system owner.

Figure 2.1.8: Spyware

A computer can become infected with spyware in many methods, including:

- accepting a prompt or pop-up without reading it first.
- downloading software from an unreliable source.
- opening email attachments from unknown senders.

What can spyware be used for?

- Monitoring online activities
- Logging every key pressed on a keyboard as a keylogger
- Capturing all the personal data like passwords or bank details

Spyware can join itself with legitimate software or Trojan horses. Anti-spyware software is available to detect and remove unwanted spyware programs.

2. Viruses

A virus is a type of malware that infects a computer when executed and then replicates itself to pass to another computer. Most viruses are spread by USB drives, optical disks, network shares or email.

Figure 2.1.9: Virus

Anti-virus software is available to detect and remove viruses. Anti-virus software is a collection of known viruses. Therefore, if a program is suspected of being virus-infected, the anti-virus software will warn the user and store it separately until it is confirmed that it is safe to use.

3. Trojan horse

This malware is named after the Greek myth of the Trojan horse. Trojans exploit user privileges and are often found in image files, audio files or games.

Figure 2.1.10: Trojan horse

Unlike viruses, Trojans do not self-replicate but carry out malicious operations by hiding their purpose. Trojans appear genuine, but very dangerous. Anti-virus software is available to remove the trojans.

4. Worms

This malware replicates itself in order to spread from one computer to another. After the host gets infected by a worm, it does not require any user's participation. It can run by itself and spread very quickly over the network. Worms can exploit the system vulnerabilities and can move themselves to cause damage to computer systems or networks. Installing good anti-virus software can protect computer systems or networks from getting infected with worms.

Figure 2.1.11: Worm

5. Adware

Adware is a type of malware installed with some software versions and designed to deliver advertisements to a user on a web browser automatically. It causes pop-up ads on the screen and is sometimes difficult to close. It is common for adware to come with spyware. Anti-virus or anti-adware software are available to detect and prevent adware from infecting a computer system.

Figure 2.1.12: Adware

6. Ransomware

Ransomware is a type of malware that hijacks the data on a computer system by encrypting it and then demands the owners to pay money for the data to be decrypted. Ransomware is often spread through phishing emails that encourages a user to download a malicious attachment. Anti-virus software is available to prevent the computer system from ransomware attacks.

Figure 2.1.13: Ransomware

7. Backdoor

A backdoor malware works in the background of a computer system and is difficult to detect. Backdoor malware gains unauthorised access to a system by bypassing the normal authentication procedures. After a backdoor attack, hackers can remotely access the resources through system commands.

Figure 2.1.14: Backdoor

8. Scareware

Scareware is a type of malware that uses 'scare' tactics to take a specific action. Scareware usually consists of operating system style windows that pop up to warn the user that the system is at risk and needs to run a specific program for it to return to normal operation. If the user gets scared and accepts executing that specific program, the computer system will become infected with Scareware malware.

Figure 2.1.15: Scareware

9. Rootkit

Rootkit malware is like backdoor malware and is designed to modify the operating system. Rootkit malware is hard to detect as the attackers gain access to remote resources to modify the system files, system investigating files, and monitoring tools. Therefore, a computer infected with rootkit malware is completed wiped, and software programs are reinstalled.

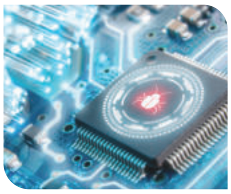


Figure 2.1.16: Rootkit

Complete activity 2.1.6 in the workbook

Social engineering

Social engineering is a kind of cyberattack involving psychological manipulation techniques that exploit human error to access confidential information. It is like a trick to gain people's confidence, to gather information and gain unauthorised access to the computer system.

For example, an attacker will call an authorised employee with an urgent problem that requires immediate network access. The attacker will try using techniques to gain the employee's trust and tries to access confidential data.

Phishing is a common social engineering attack. The attackers contact a target through email, phone, or text message to click a link. This link will redirect the targets to fraudulent websites to provide confidential data like personal information, banking and credit card information, usernames, and passwords.

Denial-of-Service

Figure 2.1.17: Denial-of-Service attack

Denial-of-Service (DoS) attacks are a type of network attack that results in some sort of interruption of network service to users, devices, or applications.

An overwhelming quantity of traffic is a type of DoS attack in a network where an enormous amount of data is sent to the host at a rate it cannot handle. This kind of attack causes a slowdown in transmission or response or cause a device or service to crash.

The maliciously formatted packet is a type of DoS attack. When a maliciously formatted packet (collection of data) is sent, the receiver cannot identify the application and will be unable to handle it. As a result of this, the system will run very slowly.

Distributed DoS

A Distributed DoS (DDoS) attack is similar to a DoS attack but originates from multiple, coordinated sources.

For example, an attacker builds a network (botnet) of infected hosts called zombies controlled by handler systems. The zombie computers will constantly scan and infect more hosts, creating more and more zombies. When needed, the hacker will instruct the handler systems to make the botnet of zombies carry out a DDoS attack.

Botnet

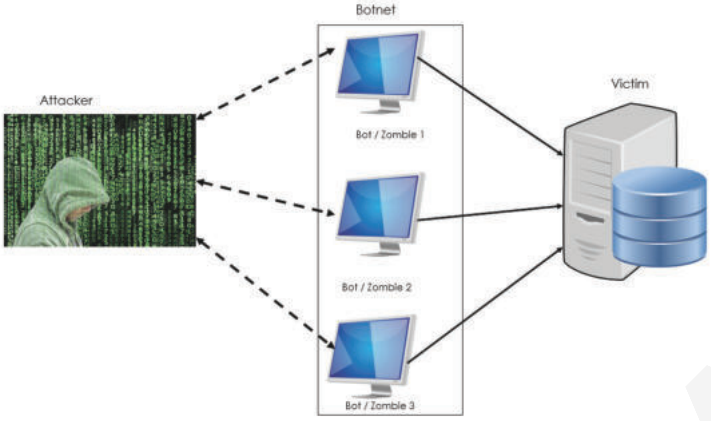


Figure 2.1.18: Botnet

A bot computer is typically infected by visiting an unsafe website or opening an infected email attachment or media file. A botnet is a group of bots in hundreds of thousands of bots connected through the internet. Cyber attackers control a botnet through system commands.

On-path attacks

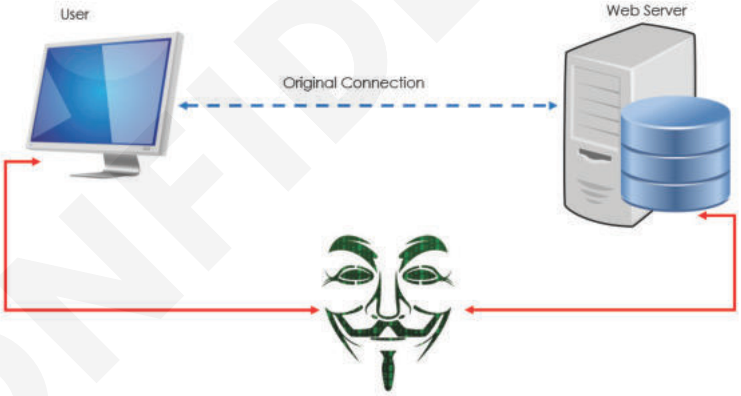


Figure 2.1.19: On-path attack

On-Path attack is also referred to as a man-in-the-middle (MitM) or man-in-the-mobile (MitMo) attack. This attack intercepts or modifies communications between two devices, such as a web browser and a web server, to collect information from the devices.

A MitM attack happens when a cybercriminal takes control of a device and captures users' information without the user's knowledge. These types of attacks are often used to steal financial information.

A MitMo is a type of attack used to take control over a user's mobile device. When the mobile device is infected, the confidential data is captured and sent to the attackers.

SEO poisoning

After a search using search engines like Google, the web pages are rank wise listed according to the relevancy of their content. Attackers use popular search terms and use SEO to push malicious sites to higher up the ranks of search results. This technique is called Search Engine Optimisation (SEO) poisoning.

Complete activity 2.1.7 in the workbook

Wi-Fi password cracking

Password attacks

One of the most common methods of authenticating to a website is by entering a username and password. As a result, revealing your password is a simple way for cybercriminals to gain access to your most sensitive information.

There are different kinds of password attacks, as follows:

- Password spraying
- Dictionary attacks
- Brute-force attacks
- Rainbow attacks
- Traffic interception

Password spraying

This method tries to gain access to a system by 'spraying' a few commonly used passwords across many accounts. For example, a cybercriminal may use 'Password123' with a variety of usernames before attempting a second commonly used password, such as 'qwerty.'

Figure 2.1.20: Password spraying

Dictionary attacks

In an attempt to gain access to a password-protected account, a hacker systematically tries every word in a dictionary or a list of commonly used words as a password.

Figure 2.1.21: Dictionary attacks

Brute-force attacks

Brute-force attacks are the most basic and widely used method of gaining access to a password-protected site, and they involve an attacker trying every possible combination of letters, numbers, and symbols in the password space until they get it right.

Figure 2.1.22: Brute-force attacks

Rainbow attacks

Passwords are stored as numerical values that uniquely identify data rather than plain text in a computer system. A rainbow table is a large dictionary of precomputed values and the passwords that were used to generate them.

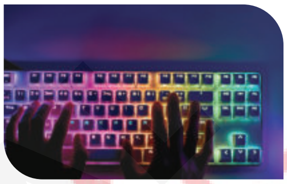


Figure 2.1.23: Rainbow attacks

Traffic interception

By intercepting communications, other humans and machines can easily read plain text or unsecured passwords. Anyone who has access to your account or device, whether authorised or unauthorised, can read your password if you store it in plain text.

Figure 2.1.24: Traffic interception

Complete activity 2.1.8 in the workbook

Network implementation

To implement computer networks a range of factors must be taken into consideration. Some important factors include:

- purpose of the network
- hardware including network and end devices
- topologies
- software including routing protocols

Purpose of the network

When designing a network, it is important to clearly identify the purpose or the intended use of the network. Different types of networks serve different purposes, and understanding the specific needs of the network will help in making appropriate hardware, topology, protocol, and addressing choices. Here are some examples of different network purposes:

Home network

- A home network is typically used for personal computing, entertainment, and communication purposes within a residential setting.
- It may include devices like computers, laptops, smartphones, smart TVs, gaming consoles, and home automation systems.
- The network should provide reliable internet connectivity, support media streaming, enable device interconnectivity, and ensure basic security measures.

Data centre network

- A data centre network is designed to support large-scale computing and storage requirements.
- It focuses on high-performance, scalability, and fault tolerance to handle significant amounts of data and demanding workloads.
- The network architecture should include redundant components, load balancing mechanisms, and high-speed connectivity to ensure uninterrupted access to resources.

Analysing network requirements

Once the purpose of the network is identified, it is important to analyse and understand the specific requirements to determine the appropriate hardware, topology, protocol, and addressing choices. Here are some key considerations whilst analysing network requirements:

Performance

- Determine the required network performance in terms of data transfer speeds, latency, and throughput.
- Analyse the network traffic patterns to identify peak usage periods and resource-intensive applications.
- Consider the need for technologies like Quality of Service (QoS) to prioritise critical traffic.

Scalability

- Assess the anticipated growth and future expansion plans for the network.
- Determine if the network needs to accommodate additional users, devices, or locations.
- Choose scalable hardware and protocols to ensure the network can handle increased demands.

Figure 2.1.25

Reliability

- Evaluate the criticality of network uptime and data availability.
- Consider redundancy mechanisms like backup power supplies, redundant links, and fault-tolerant hardware.
- Assess the need for technologies like Spanning Tree Protocol (STP) or link aggregation to provide reliable connectivity.

Figure 2.1.26

Security

- Identify the sensitivity of the data transmitted over the network and the potential risks.
- Implement appropriate security measures such as firewalls, intrusion detection systems, and encryption protocols.
- Consider network segmentation and access control mechanisms to protect sensitive resources.

Figure 2.1.27

By analysing network requirements, network administrators can make informed decisions about hardware selection, network topologies, protocol implementations, and addressing schemes that align with the purpose of the network and meet the desired performance in terms of scalability, reliability, and security.

Hardware

Network hardware plays a role in determining the scalability and reliability of a network infrastructure. Let us explore how different types of network hardware can impact these aspects.

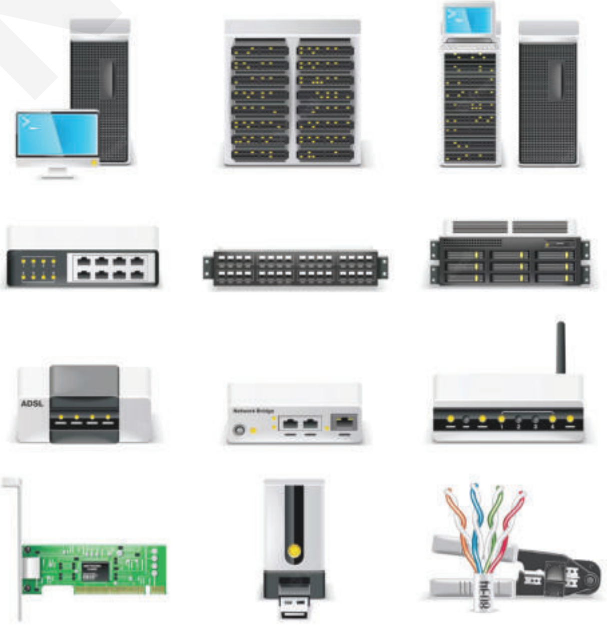


Figure 2.1.28

Switches

Switches connect multiple devices within a local area network (LAN). Scalable switches with high port densities and stacking capabilities allow for easy expansion of the network by adding more devices without degrading performance. For example, a high specification modular switch can offers scalable options with high port densities and support stacking for simplified management.

Routers

Routers facilitate communication between networks and determine the most efficient path for data transmission. Scalable routers can handle increasing network traffic and support additional connections. For example, business specification routers are known for their scalability, offering high-performance routing for large-scale networks.

Network interface cards

Network Interface Cards (NICs) connect end devices to the network and impact the reliability and scalability of network communication. High-quality NICs with advanced features ensure stable and fast connections, reducing the chances of network downtime. For example, wired ethernet adapters are known for their reliability and performance, enabling seamless network connectivity.

Network cabling

The choice of network cabling, such as copper or fiber-optic cables, can influence network reliability and scalability. Fiber-optic cables offer higher bandwidth, longer transmission distances, and better resistance to electromagnetic interference, making them more scalable and reliable for large networks. On the other hand, copper cables, such as Category 6 (Cat6) or Category 6a (Cat6a), are more appropriate for smaller networks with moderate bandwidth requirements.

Wireless access points

Wireless networks heavily rely on wireless access points (WAPs) for connectivity. Scalable and reliable WAPs support a large number of concurrent users, provide seamless roaming capabilities, and offer high-performance throughput. For example, high specification access points are designed to be scalable and reliable, ensuring consistent wireless connectivity for many devices in demanding environments.

By investing in scalable and reliable network hardware, organisations can accommodate future growth, handle increasing network traffic, and maintain consistent performance. These examples show how different network hardware components contribute to the scalability and reliability of computer network infrastructure.

Topologies with network features

Network topology refers to the physical or logical arrangement of devices and connections in a network. The choice of network topology can have a significant impact on the scalability and reliability of a network infrastructure. Let us explore how different network topologies can affect these aspects.

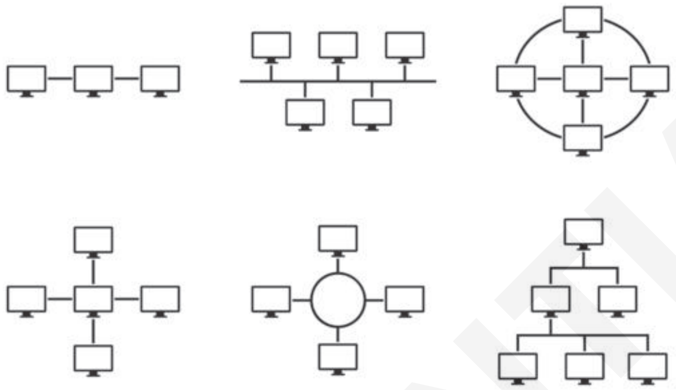


Figure 2.1.29

Star topology

In a star topology, all devices are connected to a central device, such as a switch or hub. This topology offers good scalability as new devices can be easily added by connecting them to the central device. The reliability of a star topology is generally high because if one device fails, it does not affect the connectivity of other devices. However, the central device becomes a single point of failure. Examples of star topology include Ethernet networks where devices are connected to a central Ethernet switch.

Mesh topology

In a mesh topology, every device is connected to every other device, forming a fully interconnected network. Mesh topologies provide excellent reliability as multiple paths exist for data transmission. If one link or device fails, data can still reach its destination through alternative paths. Mesh topologies can be scaled by adding more connections between devices. However, the scalability of a full mesh can become challenging as the number of connections grows exponentially with each added device. Internet backbones often use a mesh topology to ensure high reliability.

Ring topology

In a ring topology, devices are connected in a closed loop, where each device is connected to exactly two other devices. Data travels in one direction around the ring. Ring topologies offer good scalability as additional devices can be easily added by connecting them to the existing ring. However, the reliability of a ring topology can be compromised if a single link or device fails, as it can disrupt the entire network. Token Ring networks, although less common today, are an example of a ring topology.

Bus topology

In a bus topology, all devices are connected to a single communication line, also known as a bus. Devices share this communication medium and receive data intended for them. Bus topologies can be easily scaled by adding more devices to the bus. However, the reliability of a bus topology can be affected if the main communication line fails, as it will disrupt the entire network. Ethernet networks, particularly in the past using coaxial cables, used bus topologies.

Hybrid topology

A hybrid topology is a combination of two or more different topologies. For example, a network might have a combination of star and mesh topologies. Hybrid topologies offer flexibility and can be tailored to meet specific scalability and reliability requirements. They can scale by adding devices within the chosen topologies and offer improved reliability by leveraging redundancy in the mesh segments. Many modern enterprise networks use hybrid topologies to balance scalability and reliability.

It's important to note that scalability and reliability considerations are not solely dependent on the network topology but also influenced by other factors such as the network hardware, protocols, and management practices. A well-designed and implemented network topology, in conjunction with appropriate hardware choices and configurations, can greatly enhance the scalability and reliability of a computer network infrastructure.

Software

Network software plays a role in determining the scalability and reliability of a network infrastructure. Let us explore how different types of network software can impact these aspects.

Figure 2.1.30

Network operating systems

Network operating systems (NOS) provide the software foundation for managing and controlling network devices. Scalable network operating systems are designed to handle increasing network demands by efficiently managing resources and accommodating growth. These complex network operating systems offer features like virtualisation, high availability, and dynamic routing protocols to ensure scalability and reliability.

Network management software

Network management software is responsible for monitoring, configuring, and troubleshooting network devices. Scalable network management software can handle larger networks with a growing number of devices and provide centralised management capabilities. This software can offer scalability through features like distributed monitoring, multi-tenancy support, and automation.

Routing protocols

Routing protocols determine the most efficient paths for data transmission within a network. Scalable routing protocols like OSPF (Open Shortest Path First) and BGP (Border Gateway Protocol) are designed to handle large-scale networks with complex routing requirements. These protocols employ mechanisms like hierarchical routing, route summarisation, and fast convergence to ensure scalability and reliable packet routing.

Load balancing software

Load balancing software distributes network traffic across multiple servers or resources, improving scalability and reliability by ensuring efficient resource utilisation and preventing overloading. Scalable load balancing software can handle increasing traffic demands and dynamically adjust load distribution.

Network security software

Network security software, including firewalls, intrusion detection systems (IDS), and virtual private network (VPN) solutions, impact both scalability and reliability. Scalable network security software can handle growing network traffic and adapt to new security threats while maintaining performance. Complex network security software offers scalable security features like firewall clustering, virtualisation, and high availability.

By implementing scalable and reliable network software, organisations can accommodate network growth, handle increasing traffic demands, and maintain consistent performance. These examples demonstrate how different network software components can contribute to the scalability.

Complete activities 2.1.9 – 2.1.12 in your workbook

Student reflection

List three things you have learned and two things you have enjoyed.

Three things I have learned:

1. ....

2. ....

3. ....

Two things I have enjoyed:

1. ....

2. ....

Key skills reflection

Learning outcomes	Key skills (Please tick the box to show your understanding of the skills below)	I don't understand	I understand	I'm an expert
Explain how examples of sensitive data can be affected by malware and other attacks.	I can identify examples of sensitive, types of malware and other types of attack.			
	I can explain how examples of sensitive data can be affected by malware and other attacks.			
Recommend a range of appropriate hardware, topologies, protocols and addressing to implement a network for a given purpose.	I examined the requirements to implement a network for a given purpose.			
	I recommended a range of appropriate hardware, topologies, protocols and addressing to implement a network for a given purpose.			

Learning outcomes	Key skills (Please tick the box to show your understanding of the skills below)	I don't understand	I understand	I'm an expert
Evaluate the scalability and reliability of a range of networks by describing the relationship between hardware, topologies, protocols and addressing.	I identified scalability and reliability issues for a range of networks.			
	I evaluated the scalability and reliability of a range of networks in terms of hardware, topologies, protocols and addressing.			
Teacher's comment:				

Section 2: Network usability and security

Aim

In this section, you will learn basic concepts in network usability and security. You will learn network usability and security measures and discuss the trade-offs that must be made when choosing between them.

Learning outcomes

- Compare the trade-offs between the usability and security of a computing system for a range of security measures.

Prior knowledge

- Networking
- Computer science

My STREAM Focus

SCIENCE TECHNOLOGY READING ENGINEERING ART MATHEMATICS

Key vocabulary

WORD	MEANING	PICTURE
usability	ease of use, the degree to which something is able or fit to be used	functionality design Usability engaging simplicity
trade-off	exchange where one gives up one thing in order to get something else that one also wants	

Usability

The term usability refers to the extent to which specified users can use a product to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use. This means that usability is about more than just ease of use; it is also about user satisfaction, which can be achieved through engaging content, visually appealing design, and effective functionality.

Trade-off

A trade-off is defined as an exchange in which you give up one thing in order to obtain something else that you also desire. A trade-off would be having to put up with a half-hour walking in order to make more money.

When it comes to security and usability, it always ends up in trade-offs. It is critical to understand how important usability is to your network design customer because some network design components can have a negative impact on usability.

Figure 2.2.1

Let us look at few trade-offs and possible solutions, if any.

Trade-off example #1

Strict security policies can have a negative impact on usability. This is a trade-off that most customers are willing to make, but not all customers.

The solution to this problem is to plan for maximum usability by deploying user-friendly host-naming schemes and simple configuration methods that use dynamic protocols like the Dynamic Host Configuration Protocol (DHCP).

Trade-off example #2

When it comes to the security of future homes, there is a clear trade-off between security and usability. For example, if you wanted to use a smart lock for your home, would you rather have intruders potentially entering your home or risk being improperly locked out? This is a trade-off situation.

You would instead want none of these situations, but it is very hard to build a perfect mechanism.

Trade-off example#3

Choosing accurate information to make security decisions is often a good way to address the security/usability trade-off. For example, if you were to use a password on your smart-lock, it could be either very simple and therefore very usable but less secure. Or it can be very complex and therefore very secure but less usable. This is a trade-off.

One possible solution is to use a fingerprint reader for your smart lock, which can be both usable and secure.

If both security and usability concerns are addressed, the conflicts between the two can be resolved. In the case of trade-off example #3 passwords, the solution would be to use relatively short passwords while constantly monitoring user behaviour to see if anything out of the ordinary occurs. Therefore, there should be a balance between security and usability. This balance should be fluid, not fixed.

Complete activity 2.2.1 in the workbook.

Student reflection

List three things you have learned and two things you have enjoyed.

Three things I have learned:

1. ....

2. ....

3. ....

Two things I have enjoyed:

1. ....

2. ....

Key skills reflection

Learning outcomes	Key skills (Please tick the box to show your understanding of the skills below)	I don't understand	I understand	I'm an expert
Compare the trade-offs between the usability and security of a computing system for a range of security measures.	I can explain a range of network security-related measures.			
	I can compare the trade-offs between the usability and security of a computing system for a range of network-related security measures.			
Teacher's comment:				

Section 3: Cybersecurity trade-offs

Aim

In this section, you will learn cybersecurity trade-offs and how to implement security measures in various trade-off situations.

Learning outcomes

- Explain trade-offs when selecting, recommending and implementing cybersecurity measures.
- Evaluate trade-offs when selecting, recommending and implementing cybersecurity measures.

Prior knowledge

- Networking
- Computer science

My STREAM Focus

SCIENCE TECHNOLOGY READING ENGINEERING ART MATHEMATICS

Key vocabulary

WORD	MEANING	PICTURE
trade-off	exchange where one gives up one thing in order to get something else that one also wants	

Cybersecurity categories

Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also referred to as information technology security or electronic information security. The term is used in a variety of contexts, ranging from business to mobile computing. It can be classified into a few broad categories like follows.

- Network security – is securing the computer network from intruders or attackers.
- Application security – is the focus to keep the software and devices free from threats.
- Information threats – protect the integrity and privacy of data in storage and network transportation.
- Operational security – is the processes and decisions for handling and protecting assets (devices, servers, computers, and data).
- Disaster recovery – is how an organisation responds to a cybersecurity incident or attack that causes the loss of organisation operations or data.
- End-user education – is educating the users about security and cyberattack prevention.
- Technology and process development – This includes maintenance, automation, design or redesign of equipment, hardware, software, procedures, and technical knowledge.

Types of cyber threats

The threats countered by cybersecurity are three-folded as follows.

1. Cybercrime includes attackers who target systems for monetary gain or to cause disruption.
2. Cyber-attack often involves politically motivated information gathering.
3. Cyber extremism aims to disrupt electronic systems to cause panic or fear.

Cybersecurity trade-off

The cybersecurity trade-off is a process in which the quality of some services related to an organisation or an individual is reduced. This is because of the implementation of security solutions to reduce risk factors and protect confidential information.

Figure 2.3.1

Trade-off #1: Cost

Figure 2.3.2

Depending on the organisation's size and type of information they store, appropriate security solutions must be integrated to protect the organisation from cyberattacks. However, the cost involved in establishing the infrastructure to implement the security solutions and maintenance is very high.

Solution: The cost invested must be a trade-off by the organisation. The investment can be reduced by making a thorough prediction of the business growth. Then prevent cyberattacks by selecting suitable infrastructure and security solutions.

Trade-off #2: Authentication

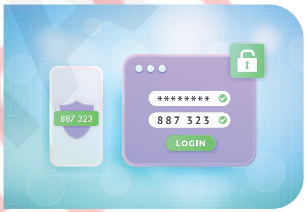


Figure 2.3.3

Some organisations and individuals use a common password to access sensitive data. Users do not have to struggle to remember common passwords. These passwords are typically written on sticky notes or posted on bulletin boards. However, the risk of password disclosure to an unauthenticated user is high. If any user unknowingly reveals the password or if the password is known to an unauthenticated user, there is a risk of hacking (or) intruding on the organisation's data.

Solution: Password getting disclosed is the trade-off. The organisation employees must follow strict rules and effective ways to handle and protect confidential system passwords. Periodic change of passwords and maintaining the privilege hierarchy in the organisations is a good approach to solving this problem.

Trade-off #3: Privacy

Figure 2.3.4

People spend their time using social media (FaceBook, Twitter, Instagram). Most of the personal details of the users are stored on social media platforms. These social media are integrated with powerful tools to access individual private data without their permission. However, even after knowing these facts, people still use social media platforms.

Solution: Personal data getting leaked is traded off. People should take care and wisely use social media platforms. Personal data need not be shared until it is required for a purpose. Passwords have to be changed periodically, and users should log out when not using the application. Deleting cookies stored in the computer on a regular basis is also a solution.

Trade-off #4: Training

Organisations are now required to continuously scan their technology and network traffic for abnormalities to detect any cyber threat. However, this requires organisations to spend a significant amount of time and money training employees on protecting themselves from cyberattacks.

Figure 2.3.5

Solution: Training is essential because these attacks have the potential to disrupt business operations, steal intellectual property, damage in-house technology, and harm corporate reputations. Therefore, time can be managed and balanced to give the employees proper training.

Trade-off #5: Business solution

The typical business has many discrete cybersecurity solutions. However, the complexity of these cybersecurity solutions makes it difficult to understand and know what is and is not working.

Figure 2.3.6

Solution: The solution does not exist because it was discovered that constructing a simple defence against cyber threats is difficult.

Protection against cyberthreats

Organisations can guard against cyber threats if few safety measures are taken. For example:

- Update the operating system on a regular basis
- Use anti-virus software
- Use strong passwords
- Do not open email attachments from unknown senders
- Do not click on links in emails from unknown senders/ unfamiliar website
- Avoid connecting to unsecured Wi-Fi networks in public places

Figure 2.3.7

Complete activity 2.3.1 in the workbook.

Student reflection

List three things you have learned and two things you have enjoyed.

Three things I have learned:

1. ....

2. ....

3. ....

Two things I have enjoyed:

1. ....

2. ....

Key skills reflection

Learning outcomes	Key skills (Please tick the box to show your understanding of the skills below)	I don't understand	I understand	I'm an expert
Explain trade-offs when selecting, recommending, and implementing cybersecurity measures.	I can identify trade-offs when selecting, recommending and implementing cybersecurity measures.			
	I can explain trade-offs when selecting, recommending and implementing cybersecurity measures.			
Evaluate trade-offs when selecting, recommending and implementing cybersecurity measures.	I can select and recommend cybersecurity measures.			
	I can evaluate trade-offs when selecting, recommending and implementing cybersecurity measures.			
Teacher's comment:				

MOEUAEofficial