



Temasek Junior College
2023 JC2 H2 Computing
Networking 6 – Network Security

Syllabus Objectives

By the end of this lesson, you should be able to:

- Understand how malware (e.g. worms and viruses) and denial of service (DOS) attacks can compromise computer systems.
- Understand how firewall (filtering function), intrusion detection system (IDS) and intrusion prevention system (IPS) can be used to restrict network access, and their limitations.
- Understand how encryption, digital signature, and authentication can ensure security of network applications

1 What is Network Security?

Network security is the field of cybersecurity focused on protecting computer networks from cyber threats.

Network security has three main aims: to prevent unauthorized access to network resources, to detect and stop cyberattacks and security breaches in progress, and to ensure that authorized users have secure access to the network resources they need, when they need them.

Desirable properties of secure communication:

1. **Confidentiality:** Only the sender and intended receiver should be able to understand the contents of the transmitted message. Because eavesdroppers may intercept the message, this necessarily requires that the message be somehow encrypted so that an intercepted message cannot be understood by an interceptor.
2. **Message integrity:** Ensure that the content of their communication is not altered, either maliciously or by accident, in transit. Checksumming techniques and digital signatures can be used to ensure message integrity.
3. **End-point authentication:** Both the sender and receiver should be able to confirm the identity of the other party involved in the communication—to confirm that the other party is indeed who or what they claim to be.
4. **Operational security:** Almost all organizations (companies, universities, and so on) today have networks that are attached to the public Internet. These networks therefore can potentially be compromised. Attackers can attempt to deposit worms into the hosts in the network, obtain corporate secrets, map the internal network configurations, and launch DoS attacks. Operational devices such as firewalls and intrusion detection systems are used to counter attacks against an organization's network.

2 Network Threats

2.1 Malware

- Hostile, intrusive, or annoying software or program code (“**malicious**” + “**software**”)
- Includes computer viruses, worms, trojan horses, bots, spyware, adware, etc
- It is a software intentionally designed to cause damage to a computer, server, client or computer network
- Most malware are self-replicating: once it infects one host, it seeks entry into other hosts over the internet and via portable storage media
- Examples of malware:
 - *Virus*: A generic term for malware where the program attaches itself to another file in order to infect a computer. It replicates itself and can cause expensive damage to individual computers and networks.
 - *Trojan*: Malware that is hidden within another file on your computer, may not always be obvious that a computer is infected as it does not replicate itself. Causes harm to a computer system or allow a hacker unauthorised access.
 - *Worm*: Malware or a type of virus that replicates itself and spreads around a computer system. It does not need to be attached to another file in order to infect a computer.
- Examples of damage caused by malware:
 - Loss of files or data
 - Unauthorised access to files or data
 - Reduction in system performance
 - Unauthorised access to webcams or microphones
 - Loss of control to attacker

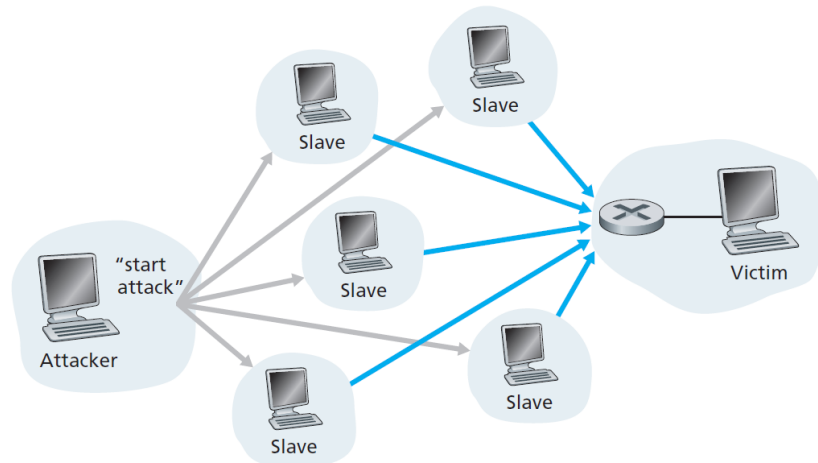
2.2 Internet Bot and Botnet

- Also called web robots, are automated internet applications controlled by software agents
- These bots interact with network services intended for people, carrying out monotonous tasks and behaving in a humanlike manner (e.g., computer game bot)
- Bots can gather information, reply to queries, provide entertainment, and serve commercial purposes. It can help to eliminate cumbersome manual processes, which are often highly repetitive, and can be done by bots far more quickly, reliably and accurately than a human.
- **Botnet** - a network of “zombie” computers that have been taken over by malware for malicious intent. They is used to do automated tasks such as spamming or distributed DoS. The attacker, sometimes known as a bot-herder, can carry out simultaneous, coordinated attacks using every computer on the botnet to target a specific network or system

2.3 DoS (Denial-of-Service)

- An explicit attempt by attackers to prevent legitimate users of a service from using that service.
 - attempts to “flood” a network, thereby preventing legitimate network traffic
 - attempts to disrupt connections between two machines, preventing access to a service
 - attempts to prevent a particular individual from accessing a service
 - attempts to disrupt service to a specific system or person
- Web servers, e-mail servers, DNS servers, and institutional networks can all be subject to DoS attacks.
- Biggest attack in Feb 2000
 - Attacked major Internet sites such as Yahoo!, E-Bay, Amazon.com, Buy.com, CNN

- In a distributed DoS (DDoS) attack, the attacker controls multiple sources and has each source blast traffic at the target.
- DDoS attacks leveraging botnets with thousands of comprised hosts are a common occurrence today. DDoS attacks are much harder to detect and defend against than a DoS attack from a single host.
- To avoid detection and mitigation, an attacker may choose to send malicious traffic in a smaller stream / at a lower bandwidth / intermittently (low and slow attack). This masks malicious traffic in the flow of legitimate requests, while still denying or degrading access to the service for users.



2.4 IP Spoofing

- IP address spoofing is the act of falsifying the content in the Source IP header, usually with randomized numbers, either to mask the sender's identity or to launch a DDoS attack.

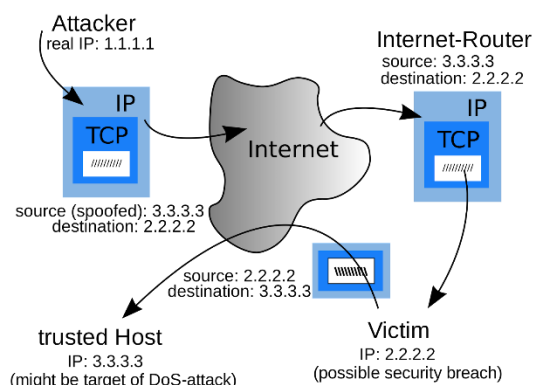


Image source: Banu Ph.D., Sabitha. (2019). A Survey of Computational Intelligence Methods used in handling Man in the Middle Attacks in Machine to Machine Communications.

- An attacker outside the network impersonates a trusted computer by using an IP address that is allowed for the network and can inject data or commands into an existing stream of data passed between the client or server application.

- In a DDoS attack, using spoofed IP addresses mask the true identities of attackers' botnet devices to:
 1. Avoid discovery and implication by law enforcement and forensic cyber-investigators.
 2. Prevent targets from notifying device owners about an attack in which they are unwittingly participating.
 3. Bypass security scripts, devices and services that attempt to mitigate DDoS attacks through the blacklisting of attacking IP addresses.

2.5 Packet Sniffing

- A passive receiver that records a copy of every packet that flies by is called a packet sniffer.
- Packet sniffing can also be used for benign purposes such as traffic analysis and intrusion detection.
- In wired broadcast environments, as in many Ethernet LANs, a packet sniffer can obtain copies of broadcast packets sent over the LAN.
- Once the raw packet data is captured, the packet sniffing software must analyze it and present it in human-readable form so that the person using the packet sniffing software can make sense of it.
- Hackers can use sniffers to eavesdrop on unencrypted data in the packets to see what information is being exchanged between two parties. They can also capture information such as passwords and authentication tokens (if they are sent in the clear).
- Because packet sniffers are passive - that is, they do not inject packets into the channel - they are difficult to detect.

2.6 Impact of Network Security Failure

If a system is hacked or is the victim of a cyberattack, the consequences for the organisation can be significant.

- If personal data is accessed or stolen, the organisation will be investigated and probably fined by relevant authorities.
- If commercial information is stolen, it may be given or sold to competitors and the organisation may lose a competitive advantage.

Often the greatest impact is reputational damage. This is where customers or stakeholders find out about the attack and lose confidence in the organisation. They may take their business elsewhere, resulting in a loss of revenue for the organisation.

3 Information Security

3.1 CIA Triad

Information security seeks to address three specific principles: Confidentiality, Integrity, and Availability. This is called the CIA triad.

<i>Principle</i>	<i>Description</i>
<i>Confidentiality</i>	<p>This is the fundamental principle of keeping information and communications private and protecting them from unauthorized access.</p> <p>Confidential information includes trade secrets, personnel records, health records, tax records, and military secrets.</p>
<i>Integrity</i>	<p>This is the property of keeping organizational information accurate, free of errors, and without unauthorized modifications.</p> <p>For example, in the 1980s movie <i>War Games</i>, actor Matthew Broderick was seen modifying his grades early in the movie. This means that the integrity of his grade information was compromised by unauthorized modification.</p>
<i>Availability</i>	<p>Availability is the fundamental principle of ensuring that systems operate continuously and that authorized persons can access the data that they need.</p> <p>Information available on a computing device is useless unless users can get to it. Consider what would happen if the Federal Aviation Administration's air traffic control system failed. Radar images would be captured but not distributed to those who need the information.</p>

3.2 Security Factors

Most security systems rely on four major factors to achieve security goals:

1. **Authorization** is the process of determining what rights and privileges a particular entity has.
2. **Access control** is the process of determining and assigning privileges to various resources, objects, or data. The principle of least privilege dictates that users and software should have only the minimal level of access that is necessary for them to perform their duties.

3. **Accountability** is the process of determining who to hold responsible for a particular activity or event, such as a logon.
4. **Auditing or accounting** is the process of tracking and recording system activities and resource access.

3.3 Security Control

Security controls are safeguards or countermeasures to avoid, counteract, or minimize security risks relating to or company property.

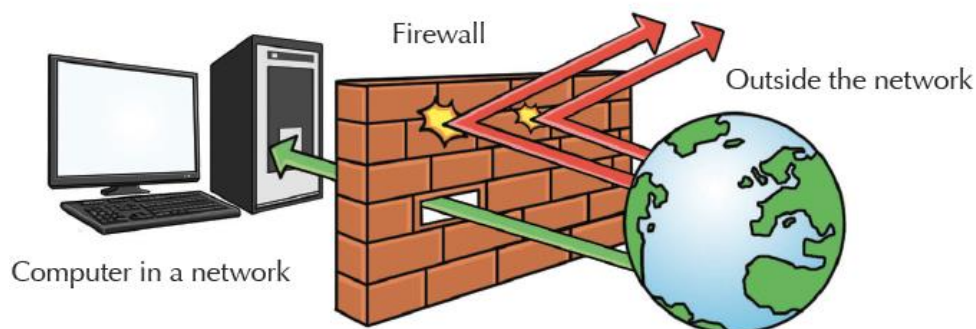
Types of security controls:

1. **Physical controls** such as fences, doors, locks, security cameras and fire extinguishers.
2. **Procedural controls** such as incident response processes, management oversight, security awareness, and training.
3. **Technical controls** such as user authentication (login) and logical access controls, antivirus software, and firewalls.
4. **Legal and regulatory or compliance controls** such as privacy laws, policies, and clauses.

4 Protecting Networks

4.1 Firewalls

- A firewall is a combination of hardware and software that isolates an organization's internal network from the Internet at large, allowing some packets to pass and blocking others.
- It can perform packet filtering (a technique for examining the contents of packets on a network and rejecting them if they do not conform to certain rules) and/or stateful inspection (a technique for examining the contents of packets on a network and rejecting them if they do not form part of a recognised communication)



- It works by monitoring each piece of information that is transmitted through a network. Then the information would be either blocked or allowed to pass through based on a set of rules configured by an administrator (e.g. refer to table below). Only authorized traffic, as defined by the local security policy, will be allowed to pass. With all traffic entering and leaving the institutional network passing through the firewall, the firewall can restrict access to authorized traffic.

Example of the policy and its respective firewall setting

Policy	Firewall Setting
No outside Web access.	Drop all outgoing packets to any IP address, port 80.
No incoming TCP connections, except those for organization's public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80.
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets — except DNS packets.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP ping packets going to a "broadcast" address (eg 130.207.255.255).
Prevent your network from being tracerouted.	Drop all outgoing ICMP TTL expired traffic.

Policies and corresponding filtering rules for an organization's network 130.207/16 with Web server at 130.207.244.203

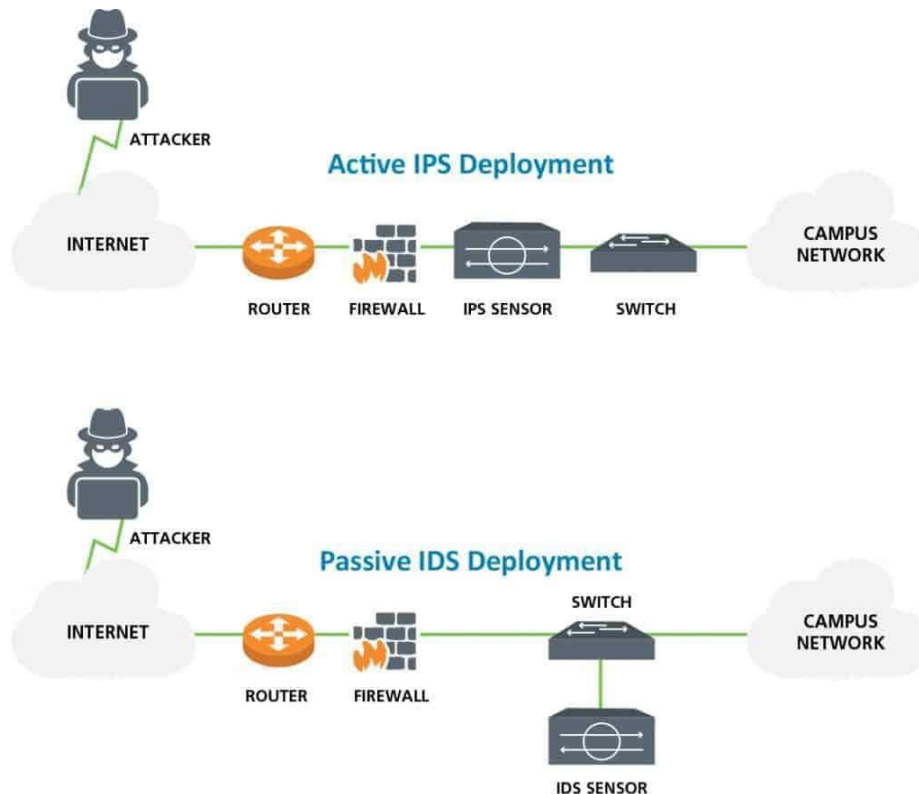
- Limitations of firewalls:
 - Firewalls cannot protect against what has been authorized; it is only as effective as the rules that they are configured to enforce
 - Firewalls cannot stop social engineering attacks or an authorised user intentionally using their access for unwanted purposes
 - If not designed or installed properly, it can be compromised, in which case it provides only a false sense of security

4.2 Intrusion Detection System

- An intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations.
- Two main types of IDS.
 1. **Network intrusion detection system (NIDS).** These systems examine the traffic in the network and monitor multiple hosts for identifying intrusions. Sensors are used to capture the traffic in the network and each packet is analysed to identify malicious content.
 2. **Host-based intrusion detection system (HIDS).** HIDS are deployed in host machines or a server. They analyse data that are local to the machine such as system log files, audit trails and file system changes to identify unusual behaviour.
- HIDS monitors important operating system files while NIDS monitors incoming network traffic.
- Although they both relate to network security, an IDS differs from a firewall in that a traditional network firewall uses a static set of rules to permit or deny network connections. It implicitly prevents intrusions, assuming an appropriate set of rules have been defined. Essentially, firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS describes a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system.
- Limitation: An IDS cannot block or prevent attacks as they can only help to uncover them.

4.3 Intrusion Prevention System

- IPS is a system that actively takes steps to prevent an intrusion or an attack when it identifies one. It can be thought of as an active IDS.
- IPS takes active steps such as dropping packets that contain malicious data, resetting or blocking traffic coming from an offending IP address. IPS can be seen as an extension of IDS, which has the additional capabilities to prevent intrusions while detecting them.



4.4 Firewall vs IDS vs IPS

- Firewall - A device or application that analyses packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port. Packets that do not match policy are rejected.
- Intrusion Detection System - A device or application that analyses whole packets, both header and payload, looking for known events. When a known event is detected a log message is generated detailing the event.
- Intrusion Prevention System - A device or application that analyses whole packets, both header and payload, looking for known events. When a known event is detected the packet is rejected.

5 Security of Network Applications

5.1 Encryption

Encryption is the process of encoding data so that a secret key is required to read the data. Like passwords, the secret key is usually provided as a sequence of bytes. Before the encrypted data is decoded using the secret key, it appears as random, meaningless data.

In encryption, the original data or message is known as plaintext. The encrypted data is known as ciphertext. The encryption method or algorithm is known as the cipher, and the secret information to lock or unlock the message is known as a key.

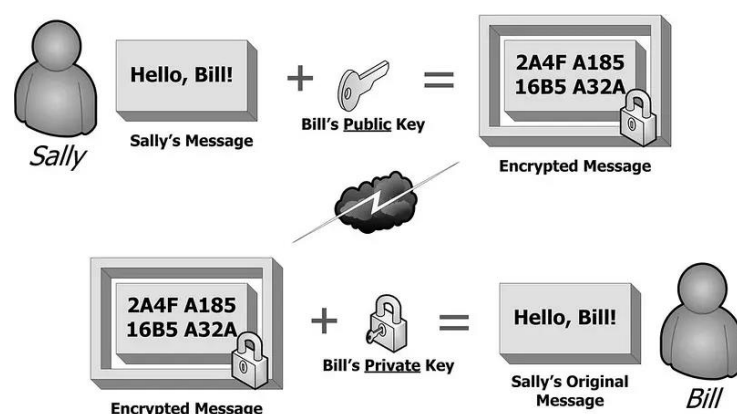
Basically, there are two kinds of cryptography:

Symmetric key cryptography

- The sender and the receiver have the same key and use the same key to encrypt and decrypt data. Also known as private key cryptography.
- Example: Caesar cipher, Vigenère cipher, Data Encryption Standards (DES) etc
- Problem: It is necessary to meet the person you are communicating with and give him or her, the secret key. The key can be intercepted easily as the ciphertext message to decrypt the data.



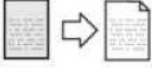
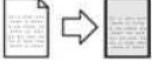

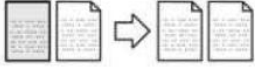
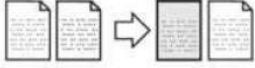
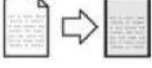
Public key cryptography

- Also known as asymmetric encryption.
- Each participant runs a program that generates a “public key” and a “private key”.
- Private key is never shared with anyone
- Public key is announced so that everyone knows it.
- The public key and private key are linked, and data encrypted with one key needs to be decrypted with the other key. To send data the sender uses the known public key to encrypt the data. It can only be decrypted using the private key, which only the receiver has. If somebody encrypts something in my public key, only my private key can decode it.



- However, it would be easy to replace a message with a forgery (since the public key is well known). To prevent this a digital signature is used. This often uses public key cryptography in reverse: the sender uses a private key to encrypt the data that can only be decrypted using the known public key, showing the sender must have used the private key and so is genuine. To enable large numbers of users to use these digital signatures they are often managed using digital certificates.

Figure B11.2 How a public key cryptosystem works

	<p>A public directory is published – for everyone in the code system, it tells the whole world what key is used to send messages to that person. This is a (big) number that can be used to encode messages. The decoding part is secret: only one person knows it.</p>
	<p>I want to send a message to you. I write my message out, substituting A = 01, B = 02, etc. and get a (long) number that represents my message.</p>
	<p>Now I look up your key in the public directory and use it to turn my message into another long number – this is done in a way that no one except you can decode – even I can't, unless I look back at my original message.</p>
	<p>You can receive my message and, using your very secret decoding method, turn it back into the original message.</p>
	<p>How do you know that the message was really from me? Anyone could lookup your key in the public directory and send a misleading message that claimed to be from me. I can prove it was from me, like this:</p>
	<p>With my message, I include my name and address, but before I code this, I use my own secret decoding key to turn the name and address part into a scrambled version.</p>
	<p>Now I code the whole message – the message itself and the previously scrambled name and address.</p>
	<p>You receive this two-part message and use your secret decoder to extract the plain message and the scrambled name and address. You read the message and need to check that it is from me.</p>
	<p>You take the scrambled part, look me up in the directory and see what my public coding key is. Using this will unscramble the name and address, and you are confident that it was from me, because I am the only person in the world who knows what my secret key is.</p>

5.2 Digital Signature

- **DIGITAL SIGNATURE** also known as: **ELECTRONIC SIGNATURE**, is a method of ensuring that an encrypted message is from a trusted source as they have a unique, encrypted signature verified by a Certification Authority. Rather than being an actual signature, a digital signature uses mathematical functions and the public/private key method. The digital signature confirms the identity of the sender; it does not encrypt the information. The message (including the electronic signature) will usually be encrypted again so the content is hidden as well.
- For example, if A wants to send a message to B with a digital signature:
 - The message being sent has a publicly known hashing algorithm applied to it to create what is known as a hash.
 - The hash is encrypted using A's private key.
 - The hash is appended to the message and becomes the digital signature.
 - The message is sent to B who then uses A's public key to decrypt the hash.
 - The hash is then put through the same publicly known algorithm and the result is compared to that in the original message.
 - Where the two hashes are the same, the message is authenticated and where they are different then the message cannot be authenticated.
- **DIGITAL CERTIFICATE** is a method of ensuring that an encrypted message is from a trusted source as they have a certificate from a Certification Authority that confirms that the individual is who they claim to be in an online communication. The certificate typically contains the name of the organisation, their domain and server name and a serial number which is registered with a Certification Authority who issues the certificates.

5.3 Authentication

- Authentication is the process of verifying the identity of a user.
- Three common methods are the use of passwords, security tokens and biometrics.

Passwords

- Secret phrase known only to user. Usually used along with a login user id.
- Can be weak if passwords are not well chosen (easily guessed by intruders) and/or not kept secret (vulnerable to phishing attacks).
- Strong passwords should have a mix of lower and upper-case letters, numbers and symbols. They should be changed regularly and unique to different computers and/or accounts.

Security Tokens (2-factor Authentication)

- In addition to a password, a device called a security token is needed to generate a one-time password (OTP) for authentication.
- A stronger method as it requires knowledge a user has (first factor) and something the user owns (second factor). This makes it more difficult for an intruder to both guess a password and steal the user's security token.

- However, wireless OTP can be intercepted. Also, if the secret algorithm used to generate OTPs is poorly chosen or accidentally revealed, an intruder can still generate OTPs without needing the security token.

Biometrics

- Biometrics is a type of authentication that is based on the measurement of human physical characteristics. For example, biometrics is used to identify a user by fingerprint or voice. Other common characteristics used in biometrics include the face, iris, retina, and deoxyribonucleic acid (DNA).
- Compared to passwords, the use of biometric identification is more secure as the physical characteristics measured are typically unique to the individual and cannot be easily replicated.

5.4 Access Control (Authorisation)

- Once a user is authenticated, the ability of a computer to control the access of data and resources by that user is called access control or authorisation.

File Permissions

- Most operating systems have settings to control the ability of users to view or make changes to specific files or folders. These settings are called permissions.
- An administrator is a special user who can override the permissions for files and folders in the system. Administrator rights can be assigned to a user as well.
- An administrator can perform other related authentication and authorisation tasks such as creating and removing user accounts or resetting passwords.
- File permissions however do not prevent an intruder with physical access to a storage device from accessing files or folders directly without going through the operating system. Encryption is needed to prevent such unauthorised access.

References:

Chapter 8 Security in Computer Networks, Computer Networking – A Top-down Approach (7th Edition)

Network Security – Ada Computer Science

(<https://adacomputerscience.org/topics/security?examBoard=all&stage=all>)

What is Network Security? – IBM (<https://www.ibm.com/topics/network-security>)

Section 9 Fundamentals of communication and networking, AQA A-Level (Includes AS and A-Level) Computer Science