OCR GCSE Computer Science

Your notes

Identifying & Preventing Threats to Computer Systems & Networks

Contents

Forms of Attack on a Network

Your notes

Forms of attack on a network

- Computers face a variety of forms of attack and they can cause a large number of issues for a network
- The main threats posed to a network to know about are
  - **Malware**
  - **Social engineering**
  - **Brute-force attacks**
  - **Denial of service attacks**
  - **Data interception & theft**
  - **SQL injection**

Malware

What is malware?

- Malware (**mal**icious soft**ware**) is the term used for any software that has been created with malicious intent to cause harm to a computer system
- Examples of issues caused by malware include
  - Files being **deleted**, **corrupted** or **encrypted**
  - Internet connection becoming **slow** or **unusable**
  - Computer **crashing** or **shutting down**
- There are various types of malware and each has slightly different issues which they cause

Malware	What it Does

Virus	▪ A program which can **replicate itself** on a user's computer. It contains code that will cause **unwanted and unexpected events** to occur
	▪ Examples of issues a user may experience are
	  ▪ **Corrupt** files
	  ▪ **Delete** data

	▪ Prevent applications from running correctly

Worms	▪ Worms are very similar to viruses, with the main difference being that they will **spread to other drives** and computers on the network
	▪ Worms can infect other computers from
	  ▪ Infected websites
	  ▪ Instant message services
	  ▪ Email
	  ▪ Network connection

Trojan	▪ Sometimes also called a **Trojan Horse** ▪ Trojans **disguise** themselves as l**egitimate software** but contain malicious code in the background
Spyware	▪ Software which will allow a person to **spy** on the users' **activities** on their devices ▪ This form of software will be embedded into other software such as games or programs that have been downloaded from **illegitimate sources** ▪ Spyware can **record** your screen, log your **keystrokes** to gain access to **passwords** and more
Ransomware	▪ A form of malware that locks your computer or device and **encrypts** your documents and other important files ▪ Often a **demand is made for money** to receive the password that will allow the user to decrypt the files ▪ There is **no guarantee** paying the ransom will result in the user getting their data back


Your notes

Social Engineering

What is social engineering?

- Social engineering is **exploiting weaknesses** in a computer system by **targeting the people** that **use** or **have access** to them
- There are many forms of social engineering, some examples include
  - **Fraudulent phone calls**: pretending to be someone else to gain access to their account or their details

- **Phishing:** Sending fraudulent emails to a large number of email addresses, claiming to be from a **reputable company** or trusted source to try and **gain access** to your details, often by coaxing the user to click on a login button
- **Pretexting:** A scammer will send a fake text message, pretending to be from the government or human resources of a company, this scam is used to trick an individual into giving out confidential data

- People are seen as **the weak point** in a system because human errors can lead to significant issues, some of which include
  - **Not locking doors to computer/server rooms**
  - **Not logging their device when they're not using it**
  - **Sharing passwords**
  - **Not encrypting data**
  - **Not keeping operating systems or anti-malware software up to date**


Your notes

Brute-Force Attacks

What is a brute-force attack?

- A brute force attack works by an attacker repeatedly trying **multiple combinations** of a user's password to try and gain unauthorised access to their accounts or devices
- An example of this attack would be an attacker finding out the length of a PIN code, for example, 4-digits
- They would then try each possible combination until the pin was cracked, for example
  - **0000**
  - **0001**
  - **0002**
- A second form of this attack, commonly used for passwords is a **dictionary attack**
- This method tries **popular words or phrases** for passwords to guess the password as quickly as possible
- Popular words and phrases such as '**password**', '**1234**' and '**qwerty**' will be checked extremely quickly.

Denial of Service Attacks

What is a denial of service attack?

- A Denial of Service Attack (**DoS attack**) occurs when an attacker repeatedly **sends requests** to a server to **flood** the server with traffic, causing it to **overload** the system
- The server will slow down to the point of becoming **unusable**
- There is also a larger-scale version of this known as a Distributed Denial of Service (**DDoS**) attack
- This works in a s similar way to a DoS attack, with the main difference being that the traffic comes from **multiple distributed devices** in a **coordinated** attack on a single server/network
- **A network of compromised device**s, called a **botnet** can be used to facilitate a DDoS attack
  - A botnet consists of numerous internet-connected devices, that have been **infected with malware** and can be **controlled remotely** by an attacker


Your notes

What is the purpose of a DoS attack?

- A DoS attack will prevent customers from accessing or using a service
- This will result in companies losing money and not being able to carry out their daily duties
- A DoS attack can cause damage to a company's reputation

Data Interception & Theft

What is data interception & theft?

- Data interception and theft is when thieves or hackers can compromise **usernames** and **passwords** as well as other sensitive data
- This is done by using devices such as a **packet sniffer**
- A packet sniffer will be able to **collect the data** that is being transferred on a network
- A thief can use this data to gain **unauthorised access** to websites, companies and more

SQL Injection

What is SQL?

- Structured Query Language (SQL) is a language used to **create**, **access** and **manipulate** a database

What is SQL injection?

- SQL injection is entering an SQL command into a **web text field** to **manipulate** the **SQL query**
- The goal is to **insert**, **modify** or **delete** data from the database
- An example of SQL injection would be a user typing in a query such as

- SELECT UserId, Name, Password FROM Users WHERE UserId = 100 or 1=1;
- This would return all of the User IDs, Names and passwords because 1 is always equal to 1


Your notes

Methods of Preventing a Network Attack


Your notes

Penetration Testing

What is penetration testing?

- Penetration testing is a method of preventing vulnerabilities whereby a company **employ** people to try and **hack** their **network** and **databases**
- This allows the 'hackers' to point out the parts of the system that are vulnerable
- The companies then use this information to **fix the issues** that are found

What form of attack would this help to prevent?

- **SQL injection**

Anti-Malware Software

What is anti-malware software?

- Anti-malware software is a term used to describe a combination of different software to prevent computers from being susceptible to **viruses** and other **malicious software**
- The different software anti-malware includes are
  - **Anti-virus**
  - **Anti-spam**
  - **Anti-spyware**

How does anti-malware work?

- Anti-malware **scans** through **email** attachments, **websites** and downloaded **files** to search for issues
- Anti-malware software has a list of known malware **signatures to block** immediately if they try to access your device in any way
- Anti-malware will also perform **checks for updates** to ensure the database of known issues is up to date

What form of attack would this prevent?

- Anti-malware would help prevent against any form of malicious software

Firewalls

What is a firewall?


Your notes

- A firewall is a **barrier** between a network and the internet
- A firewall prevents **unwanted traffic** from entering a network by filtering requests to ensure they are **legitimate**
- It can be both **hardware** and **software** and they are often used together to provide stronger security to a network
  - Hardware firewalls will protect the whole network and prevent unauthorised traffic
  - software firewalls will protect the individual devices on the network, monitoring the data going to and from each computer

What form of attack would this prevent?

- **Hackers**
- **Malware**
- **Unauthorised Access to a Network**
- **DOS/DDOS attacks**

User Access Levels & Passwords

What are user access levels?

- **User access levels** ensure users of a network have designated **roles** on a network
- Some examples of different levels of access to a school network include
  - **Administrators:** *Unrestricted* - Can access all areas of the network
  - **Teaching Staff:** *Partially restricted* - Can access all student data but cannot access other staff members' data
  - **Students:** *Restricted* - Can only access their own data and files

What are passwords?

- Passwords are a **digital lock** to prevent unauthorised access to an account
- They are often stored as an **encrypted/ciphered** text entry in a database, ensuring that even with unauthorised access to a database, a hacker would not be able to gain access to the individual passwords of users

What form of attack would this prevent?

- **Data Interception and Theft**
- **Physical Security Issues**
- **SQL Injection**


Your notes

Encryption

What is encryption?

- Encryption is a method of converting plain text into **ciphered text** to be stored
- Encryption uses complex mathematical algorithms to scramble the text
- Asymmetric encryption, also known as private key, public key encryption is often used for web pages and other communication

What form of attack would this prevent?

- Encryption plays a role in all forms of attack on a network
- It is important to note that it **does not prevent the attacks** from occurring but it does stop the attacker from gaining access to the information

Physical Security

What is physical security?

- Physical security is a method of **physically preventing access** to any part of a network
- There are a range of physical security measures that can be implemented on a network
  - **Locked doors:** Preventing access to server rooms and cabinets of switches
  - **Biometrics:** Fingerprint scanners, facial recognition and retinal scans
  - **Surveillance Cameras:** Monitoring the activity around the site where crucial networking hardware is located

What form of attack would this prevent?

- **Data interception and theft**
- **Social engineering**

Summary of attacks a preventative measures

Form of Attack	Preventative Measure
Malware	Anti-Malware Software Firewalls Encryption Physical Security
Social Engineering	User Access Levels & Passwords Physical Security
Brute-Force Attacks	User Access Levels & Passwords
Denial of Service Attacks	Firewalls
Data Interception & Theft	Encryption Physical Security
SQL Injection	Penetration Testing User Access Levels & Passwords

Your notes

Worked Example

A web development company wants to protect their computer systems and data from unauthorised access.

Identify and describe **two** software-based security methods that the company can use to protect their computer systems and data. **[6]**

How to answer this question

- You should give a security measure for one mark, then describe it for the additional two marks
- You must do this for two different security measures to be able to achieve all 6 marks

Answers

- **Anti-malware**
  - Scans for / identifies virus/spyware/malware
  - Compares data to a database of malware
  - Alerts user and requests action
  - Quarantines/deletes virus/spyware/malware

- Stops the download of virus/spyware/malware

- **Firewall**
  - Scans incoming and outgoing traffic
  - Compares traffic to a criteria
  - Blocks traffic that is unauthorised
  - Blocks incoming/outgoing traffic
- **Encryption**
  - Scrambles data using an algorithm
  - So if intercepted it cannot be understood
  - Key needed to decrypt
- **User access levels**
  - Data can be read/write/ read-write
  - Prevents accidental changes
  - Limits data users can access
- **Passwords/biometrics/authentication code/fingerprint**
  - Has to be correctly entered to gain access
  - Strong password // letters, numbers, symbols // fingerprint is unique to individual
  - Harder/impossible for a brute-force attack to succeed
  - Lock after set number of failed attempts


Your notes