1.4 System Security

Keywords & Definitions

Malware - Malicious software installed on a device without their knowledge or content

Interception - Gaining unauthorised access

Encryption - The scrambling of data that can only be decoded with the correct key

SQL - Structured Query Language used for databases

Hacking - Somebody attempting to gain access to a system usually through the use of passwords and programming

Brute Force Attack

- Used to **gain information** by cracking **passwords** through trial and error
- Use **automated software** to produce hundreds of likely password combinations

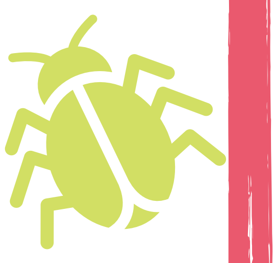
DDOS (Denial of Service Attack)

- Hacker tries to stop users from accessing a part of a network or website
- Involve **flooding the network** with useless traffic making it extremely **slow** or **inaccessible**
- Uses a number of computers over a network of **infected machines** which send requests to a website which would bring it offline
- Used as a '**botnet**'

Network Security Threats

Types of Malware

Viruses: Attach by copying themselves to certain files. Users spread them by copying/opening infected files



Worms: self replicate without any user help spreading very quickly.

Trojans: disguised as legitimate software. Users install them without realising

Actions of Malware

- **Deleting** or modifying files
- **Scareware:** tells the user the computer is infected with viruses to scare them into following links/paying for problems to be fixed
- **Ransomware:** encrypts all of the files on a computer until a large sum of money is paid for a key
- **Spyware:** secretly monitors user actions

Social Engineering

- Relies on **human interaction** (social skills)
- Commonly involves tricking users into breaking normal security procedures - does not revolve around technical cracking techniques such as worms or viruses

1.4 System Security

More Network Security Threats...

Computer Phishing

- Form of social engineering
- Emails sent claiming to be a well known business
- Will usually contain links to a spoof version of the company's website
- Designed to acquire sensitive information such as usernames, passwords, card details etc.
- Most common phishing attacks are sent through email

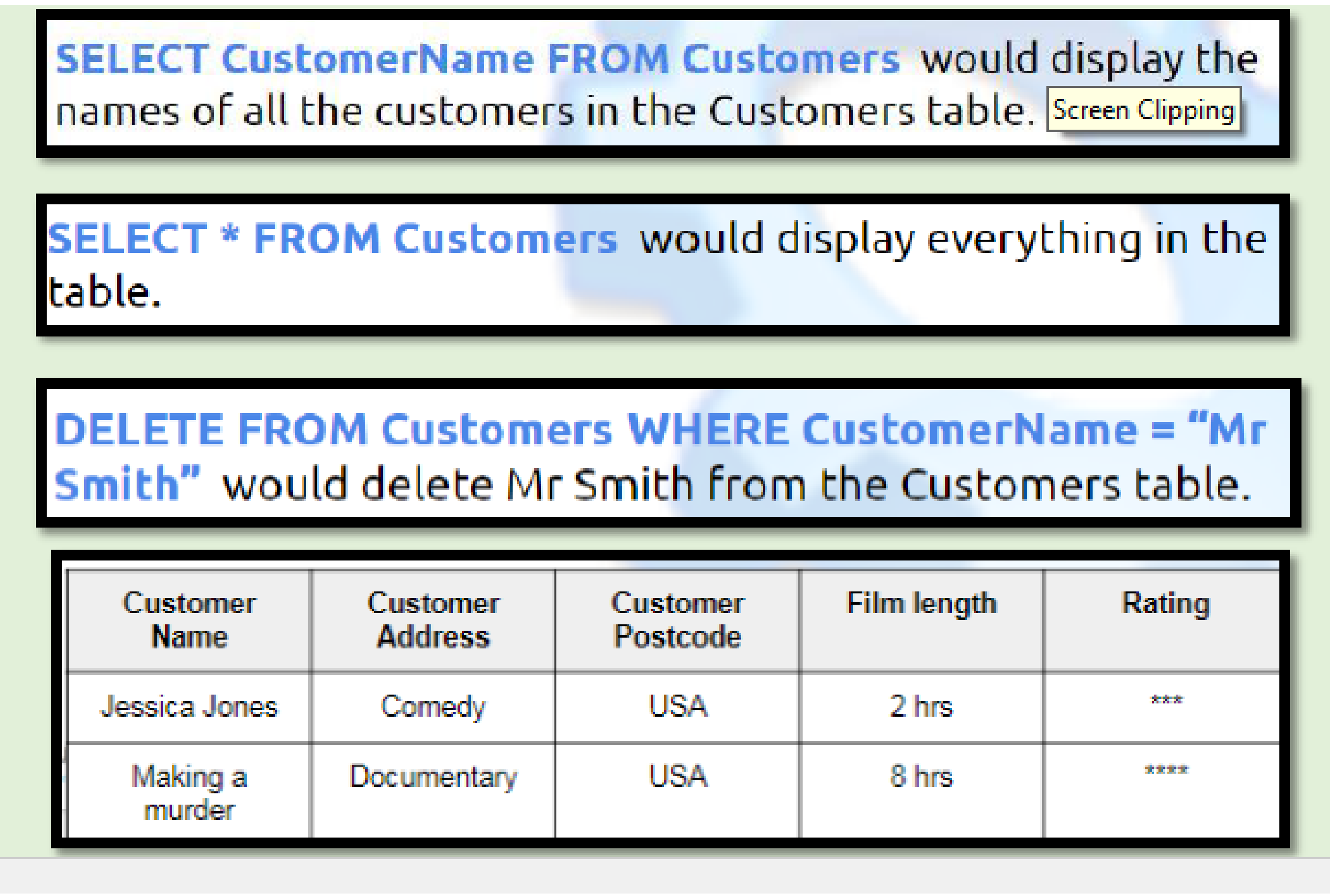
Data Interception & Theft

- The hacker monitors data travelling on a network and intercepts any sensitive data they find
- Use network monitoring hardware and software such as packet sniffers
- Data can also be intercepted physically, for example portable hard drives and other external hardware can be stolen

SQL Injection

- Structured Query Language – one of the main coding languages used to access information within a database
- SQL injections are pieces of SQL typed into a website's input box which then reveal sensitive information
- Companies that use SQL include Google, YouTube, PayPal, eBay, Cisco
- By exploiting the vulnerabilities of SQL through injection, attackers could access systems containing customer data, intellectual property and other sensitive information

Examples of SQL Injection



SELECT CustomerName FROM Customers would display the names of all the customers in the Customers table. Screen Clipping

SELECT * FROM Customers would display everything in the table.

DELETE FROM Customers WHERE CustomerName = "Mr Smith" would delete Mr Smith from the Customers table.

Customer Name	Customer Address	Customer Postcode	Film length	Rating
Jessica Jones	Comedy	USA	2 hrs	***
Making a murder	Documentary	USA	8 hrs	****

World of work links

Programmer, IT Technician, Software Engineer, Teacher, Systems Architecture, Data Engineer, Software Developer

1.6 System Security

Preventing Vulnerabilities

Network Policy

- A set of **rules and procedures** the organisation will follow to ensure their network is **protected** against attacks and unauthorised access

A good Network Policy will:

- Regularly **test** the network to find and fix security weaknesses and investigate problems
- Use **passwords** to prevent unauthorised access
- Enforce **user-access levels**
- Install **anti-malware** and **firewall** software
- **Encrypt** sensitive data

Penetration/Pen Testing

- When organisations **employ specialists** to simulate potential attacks on their network
- Used to **identify possible weaknesses** in a network's security and trying to exploit them
- The **results are then reported back**

Passwords

- Help prevent **unauthorised access**
- Should be **strong** – they should be many characters long, use a **combination,** numbers and symbols – and be **changed regularly**

Network Forensics

- **Investigations** undertaken to find the cause of attacks on a network
- An organisation needs to have a system of **capturing data packets** as they enter their network
- After the network is attacked, the packets are analysed to discover how the network was attacked and decide how to **prevent future attacks**

User Access Levels

- Control which part of the network **different groups of users can access**
- E.G. Business managers are likely to have **higher access level** allowing them to access more sensitive data
- User access levels **help limit** the number of people with access to important data, so help prevent insider attacks on the network

Anti-Malware/Anti-Virus software

- Designed to **find and stop** malware from damaging an organisation's network and the devices on it

Firewall

- **block** unauthorised access
- **examine all data** entering and leaving the network and block any potential threats

Encryption

- Data is **translated into a code/scrambled** which only someone with the **correct key** can access
- Encrypted text is called **Cipher text,** data that has not been encrypted is called plain text
- Allows data to be sent over a network **securely**