Cyber Security Notes

1 Introductory definitions

- Information Assets - Data to be protected
- Authentication - Verifying the identity of a user
- Non-repudiation - Ensuring a user cannot deny something later or claim something is false
- Malware - A contraction of malicious software
- Ransomware - Malware that demands money to stop from doing something
- Spyware - Malware that records the activity of the user
- Botnets - Malware that records the activities of the user
- Vulnerability - A point at which there is potential for a security breach
- Threat - Some danger that can exploit a vulnerability
- Countermeasure - An action taken to protect information from threats and vulnerabilities

2 Passwords

2.1 Aims of a password

- Memorable enough that the user can remember it without writing it down
- Long and unique enough that no one else can guess it

As these two aims are a contradiction, password must be a compromise between the two

2.2 Transfer of passwords

Passwords transmitted and stored in plaintext are insecure

2.3 Securing of passwords

Passwords are often encrypted using **SSL**(secure socket layer)

Hashing- Encrypting a password using one way encryption, any subsequent password is encrypted using the same method and compared to the stored hashed password.

2.3.1 Salting

Salting - Adding a value to the password before encryption.
Salting means that even if two people choose identical passwords, the stored password will be different.
Salting is only effective if:

- Salts are truly random
- The salt is sufficiently long enough to avoid the attacker just adapting their dictionary to include all salted values

2.4 Password managers

Requirements for a password manager:

- The password manager should require a password to start it, preventing unwanted access
- It should lock itself after a period of inactivity
- The passwords should be encrypted

3 Types of cyber attacks

3.1 Virus

A virus is a self replicating program often intended to cause harm

3.2 Worms

Four stages of a worm attack:

- First stage - Worm probes other machines, looking for a vulnerability to exploit
- Second stage - Penetrate the machine, exploiting the vulnerability
- Third stage - The worm downloads itself onto the machine and stores itself there
- Fourth stage - Probe other machines (back to stage 1)

3.3 Trojans

Trojan - A seemingly legitimate program that causes damage behind the scenes
Trojans are not self replicating

3.4 Phishing

Phishing - The process of luring people to disclose confidential information
Phishing relies on people trusting official looking messages

3.5 Spam Messages

SMTP(Simple Mail Transfer Protocol) defines a standard template of commands for different email programs.
This was created to a small number of users so did not include the ability to verify emails, meaning that phishing becomes possible.

3.6 Spoofing

Spoofing is where people pretend to be a person or device that they are not

3.7 Botnets

Botnets are used to coordinate the activity of many computers, these are often used for further cyber attacks.

4 Antivirus software

Malware signature - A distinctive pattern of data, either in memory or in a file

Heuristics - The use of rules to identify viruses based on previous exposure to viruses. Heuristics may execute programs in a virtual machine, checking the requests and actions the malware makes to see if it poses a threat to the computer.

Sandbox - A way for computers to run programs in a controlled environment. This constrains computing resources, allowing the program to not cause a threat to the computer.

Signed programs - The sue of cryptography when companies issue copies of a program, so that the user can check it for authenticity.