Cyber Security Notes

1 Security Essentials

- Integrity
- Availability
- Confidentiality

2 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

3 Passwords

3.1 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

3.2 Transfer of passwords

Passwords transmitted and stored in plaintext are insecure

3.3 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.

3.3.1 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

3.4 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

4 Types of cyber attacks

4.1 Virus

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

4.2 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)

4.3 Trojans

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

4.4 Phishing

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

4.5 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.

4.6 Spoofing

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

4.7 Botnets

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

5 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.

6 How the internet works

The internet comprises of a hierarchy of individual networks that have been connected to each other.

Key factors in the design of the internet:

- Should not have a central controlling computer. Every computer on the network has the same authority
- The network should be able to deliver information between any two computers on the network, even if come of the machines in the network have failed. There should be a large number of alternative routes through the network

6.1 Datagrams(packets)

When a large amount of data is sent over the internet it is split into small, uniformly sized blocks called "datagrams", also called "packets"

Header - Sender and recipient's address, unique number, data stamp and error correcting information
Payload - The actual information being delivered

6.2 Wireless networks

WiFi allows devices to be connected together wirelessly to form a LAN
WiFi refers to the wireless LAN standard from the Institute of Electrical and Electronic Engineers (IEEE) called the 802.11 family.

SSID - The name of the network (Service Set IDentifier)
The SSID allows nodes on a wireless LAN to distinguish themselves from nodes on other wireless LANs in the same physical space.

7 Network security challenges

Packet Sniffing - The copying of datagrams without the recipient knowing

7.1 Security risks of wireless networking

A wireless network should ensure that an eavesdropper is not able to convert wireless signals into the original message. This ensures **confidentiality**.

7.1.1 Man in the middle attacks

A man in the middle attack is where malicious users interpose themselves between the sender and receiver to modify or destroy the messages being sent. This compromises the **integrity** of the data being transferred.

7.1.2 Denial of service attacks

An attacker could transmit lots or random data on the frequency used by the wireless network, congesting the network and so preventing others from sending data. This compromises the **availability** of the network.

7.2 How encryption helps prevent security issues in wireless networks

Encryption helps ensure:

- **Confidentiality** - Encryption keys are needed to decrypt information, meaning attackers can't recover the information
- **Integrity** - Encryption prevents messages from being modified without the receivers knowledge
- **Authentication** - Encryption proves the identities of the sender and receiver

7.3 Implementation of encryption in WiFi

7.3.1 WEP(Wired Equivalent Privacy)

WEP has many serious problems as the encryption key can be computed in a few minutes. Many devices still support this to ensure compatibility but it should not be used.

7.3.2 WPA2(WiFi Protected Access 2)

This uses a more secure key to encrypt data that WEP, this is the default for WiFi networks. All WiFi devices must support it to be compliant with the 802.11 standard.

8 The role of standards in the internet

8.1 Why standards are needed on the internet

Standards are needed to ensure that all devices can communicate with each other.

8.2 TCP/IP Protocols

8.2.1 TCP

TCP ensures that data can be sent reliably over the internet. This works through software ports to keep data separate on the same computer.
The port decides how the data is handled when it reaches it's destination.

Common TCP Ports:

- 20 and 21 - FTP - for sending and receiving files(20) and control(21)
- 22 - SSH for secure logins
- 25 - SMTP(Simple Mail transfer protocol) - Email
- 80 - HTTP(HyperText Transfer Protocol) - Web Pages

Traffic type - The type of data and the port associated with it. For example SSH or HTTP.
TCP also ensures all data sent from a computer is received by the destination. It does this by waiting for acknowledgements of receipt from the remote computer, and if the data was not received, sending the message again.

Applications where latency is more important than accuracy, such as video conferencing, use **UDP** to send and receive data.

8.2.2 IP

IP - Internet Protocol
IP is only concerned with moving data, it doesn't check the data has arrived(handled by TCP).

When IP receives data from TCP in the computer it wraps the TCP datagram in an IP datagram with senders and receivers address, along with other information.

When IP receives data from the internet, it removes the IO datagram and passes it to TCP.

8.2.2.1 IP addresses

Every computer connected to the internet has an IP Address

There are two forms of IP addresses **IPv4** and **IPv6**.

8.2.2.2 IPv6

IPv6 can support 3.5×10^{38} IP addresses, meaning it is able to accommodate any demand. IPv6 is intended to replace IPv4, however it is taking a long time, the best solution so far is to map all IPv4 addresses to IPv6.

8.2.2.3 Reserved IP Numbers

There are many IP addresses reserved for private networks, outside of the internet, for example:

- 10.0.0.0 to 10.255.255.255
- 169.254.0.0 to 169.254.255.255
- 172.16.0.0 to 172.31.255.255
- 192.168.0.0 to 192.168.255.255

8.3 DNS

A DNS translates an readable address(e.g. google.com) to an IP address.
When a computer needs to get an IP address from a hostname it contacts the DNS responsible for the Top level domain (.com in this case). This DNS then responds with the correct IP address. The computer then uses this to contact the server.

8.4 Difference between the Internet and the World Wide Web

The world wide web is the part of the internet than can be accessed through HTTP.
The internet covers all communication between online systems, such as FTP or SSH.

9 Cryptography

9.1 Basics of cryptography

9.1.1 Terminology

- **plaintext** - Information that can be read directly by humans
- **ciphertext** - The encrypted data
- **a cipher** - The mathematics that turn ciphertext into plaintext
- **encryption** - Converting plaintext to ciphertext
- **decryption** - Reverting ciphertext to plaintext

9.1.2 Encryption keys

Keys - Pieces of information that determine the output from an encryption process.
A single cipher can produce an extremely large number of different outputs with different key values. This means communication is secure, even if the cipher is known to 3rd parties.

An encryption key is a binary string. The total number of keys for a given key length is $2^{\text{key length}}$