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 - A network of computers under the control of an attacker
- 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 use 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 its 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 IP 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

9.2 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

9.3 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 $2^{\text{key length}}$

9.3.0.1 The problem of short keys

Short keys are vulnerable to **brute force** attacks.

9.4 The problem of key distribution

If encryption keys are stolen or copied during transit, the encryption is useless.

The number of keys needed for large number of parties becomes difficult to manage. The number of keys is calculated by $\frac{n(n-1)}{2}$ where n is the number of communicating parties.

9.5 Asymmetric/public key cryptography

Public key cryptography requires two keys:

- **Private key** - Kept safe and not distributed
- **Public key** - Sent to anyone they want to exchange encrypted information with

The message is encrypted with the **public key**, but can only be decrypted using the **private key**.

This method of encryption is secure as it means that any data intercepted cannot be turned into the message.

9.6 Why isn't the internet encrypted

The amount of computing power required to encrypt and decrypt all traffic sent over the internet would lead to significant costs.
Some applications on the internet selectively use cryptography for key tasks(online payments).

9.7 Comparison of cryptographic techniques

9.7.1 DES(Data Encryption Standard)

DES was developed in the 1970s, it has relatively small key sizes, so is possible to break with a brute force attack. Because this was developed when computers were primitive, brute force was not a problem at it's invention, however it is now.
Triple DES provides additional security by doing 3 rounds of DES encryption, each with a different, 56 bit key.
Triple DES will remain secure until at least 2030.

9.7.2 AES(Advanced Encryption Standard)

AES was adopted as a standard in 2001, it uses symmetric cyphers with either 128,192 or 256 bits.
It is widely used in commercial applications as it is free. Many microprocessors now include AES in their instruction sets to speed up encryption and decryption.

9.7.3 Blowfish

Blowfish was developed in the 1990s, but wasn't widely accepted like AES is. This uses key lengths from 1 to 448 and there has been no successful attempt to break the encryption.

9.8 Using cryptography to prove identity

This works by checking that your copy of a piece of data us an exact match for the one you requested.

9.8.1 Hashing

Hashing is the mathematical process of converting data of any size into data of a fixed length.
Hashing only works in one way, meaning the data cannot be reconstructed from a hash.
If there is a difference of one bit in a file there will be a large difference in the hash.
MD5, SHA-1 and SHA-2 are in common use. Both MD5 and SHA-1 are flawed as "collisions" can occur where two pieces of different data can generate the same hash value.

9.9 Digital signatures and certificates

A digital signature is used to ensure that data originated from its supposed author.
A digital signature works by encrypting data with a private key, meaning that anyone with the public key can decrypt it. They know that only the person with the private key could have sent that message.

9.10 Encrypted network connections

In 1995 SSL was introduced, this allowed for encrypted traffic on the internet for things like online payments. This has now been replaced with TLS(Transport layer security).

9.10.1 TLS/SSL

These methods use a combination of asymmetric and symmetric encryption to exchange data. When a web browser connects to a server it undergoes a "handshake" which agrees the type of cryptography that will be used.

After the handshake the server transmits a public key and certificate of authenticity to the users computer, the users computer then checks this. The user's computer then generates a **master secret**, encrypts it with the server's public key and sends it back.

The server then decrypts the master secret. This secret means that both the server and computer can now generate identical copies of a **symmetric encryption key**, without transmitting this key in plaintext to each other.

The computers then confirm with each other that all other transactions will take place using the key(called the session key). The computers can now perform a secure transaction.

At the end of the session, the computers confirm that the transaction has finished and deletes their key.

10 Network Security

10.1 Protecting data on the network

10.1.1 Firewall basics

A firewall is a barrier that blocks all dangerous communication from spreading across a network.

Firewalls block network communication by looking at the addressing and protocol information in the data packet's header. This header is compared to rules in the firewall's software to determine whether to let the packet in.

10.1.2 Personal firewalls

A firewall is only able to protect the computer it is installed on and devices attached to it, meaning it is called a personal firewall.

These are especially useful for portable devices as these will be connected to a wide range of computer networks.

10.2 VPNs

10.2.1 VPN basics

A VPN is a way of creating a private network across an untrusted network, such as the internet. VPNs are used for:

- To securely connect isolated LANs across the internet
- To allow mobile users to access a corporate network using the internet
- To control access within an intranet environment

10.2.1.1 VPN concepts

VPNs are typically implemented using dedicated network devices and software. The software is made of two parts, the **client** and the **server**. The client connects users to the VPN and the server authenticates users and routes traffic.

The VPN software creates a "tunnel" between the VPN client and server. This tunnel can be established on an untrusted network.

10.2.2 Securing a VPN

10.2.2.1 Encryption

VPNs use public encryption standards due to their increased reliability compared to proprietary standards.

10.2.2.2 Authenticity and integrity

It is vital to ensure that data can be trusted, VPNs use the following method to ensure authenticity:

- Hashes
- Digital Signatures
- MACs(Message Authentication Codes)

MACs are appended to messages and act as an authenticator. They are similar to digital signatures but use symmetric encryption.

10.2.3 VPN Protocols

10.2.3.1 PPTP(Point to point tunnelling protocol)

PPTP was designed by a consortium led by Microsoft. This standard did not use a single form of authentication or encryption, this meant that different PPTP systems were incompatible with each other

10.2.3.2 L2TP(Layer 2 Tunnelling Protocol)

This is an adaptation of a protocol known as L2F. This combines the features of PPTP and L2F.

10.2.3.3 IPSec(Internet Protocol Security)

This is the most widely supported protocol. This is very secure due to its use of well known and trusted technologies, which had been under a lot of scrutiny to ensure there are no vulnerabilities.

10.2.4 Security risks of a VPN

10.2.4.1 Security of remote machines

Remote machines connected to a VPN must be themselves secure, otherwise they would be a vulnerability into a company network.

10.2.4.2 Security of the VPN implementation

If an insecure VPN implementation, such as PPTP then the network will be insecure.

10.2.4.3 Security of network availability

AS VPNs rely on the internet for delivering information, there are no guarantees about the reliability.

10.3 Detecting attacks

10.3.1 Intrusion detection system(IDS)

An there are two types of IDS:

- **Network intrusion detection system(NIDS)** - Monitors data passing over a network
- **Host intrusion detection system(HIDS)** - Monitoring data to and from a computer

An IDS can support a network firewall. An IDS then scans any traffic passing through the firewall using a **NIDS** while also detecting attacks from in the computer using a **HIDS**.

10.3.1.1 Weaknesses

- Too sensitive, leading to false positives
- Not sensitive enough, leading to slow attacks getting through
- Relies on software suppliers issuing updates of known signatures

10.3.2 How an IDS works in practice

10.3.2.1 Anomaly detection

Anomaly detection works on having a model of "normal" network behaviour of users and applications. This means that the system is able to detect previously unknown attacks by looking for patterns that deviate from normal behaviour. A disadvantage of this is that legitimate activities may be incorrectly identified.

10.3.2.2 Misuse detection

Misuse detection works on the system knowing a set of attack patterns, or "signatures" to compare network activity against.
This has the advantage of minimising false positives. There is the disadvantage that it can only identify attacks where there is a known pattern.

10.3.3 Honeypots

Sometimes network administrators want to study attacks to develop suitable countermeasures, or as part of an investigation for criminal prosecution.

One method of doing this is to focus attackers on a computer that seems legitimate, but is actually a closely monitored trap known as a **honeypot**. This means all the attackers actions can be reported without risk to data.

11 When your defences fail

11.1 What's the worst that could happen?

11.1.1 Identity theft

Identity theft - Where an attacker uses stolen information to impersonate another person.

11.1.1.1 Preventing identity theft

Identity theft can be prevented using an antivirus program and not responding to phishing emails.

11.1.1.2 Detecting identity theft

Signs a victim might notice:

- Unexplained bank withdrawals
- Expected official letters not arriving
- Cards or cheques declined
- Contacted by debt collectors
- Notice from a company that data has been compromised
- Bank provider making contact about suspicious behaviour

11.1.2 Loss of data

Data loss means either the deletion of data or the unauthorised copying of data.

11.1.2.1 Insider attacks

Insider attacks are where the attacker has direct access to a computer.

11.1.2.2 Risks of data loss

There are many costs of data loss, including:

- The cost of recreating the data
- The cost of continuing without that data
- The cost of informing others about the loss

11.2 Cyber Security and the law

11.2.1 Laws and Computers

11.2.1.1 Criminal and civil law

Law in Britain is divided into two categories:

- **Criminal law** - Punishing behaviour that is considered unacceptable. The majority of cases are brought by the state against individuals and companies. These causes require a high standard of proof to secure a convictions. They have high punishments.
- **Civil law** - Concerned with disputes, brought before the court by individuals. Cover things like property law, contracts and noise. These require a lower standard of proof and have financial punishments.

11.2.1.2 Bills, acts and laws

Act of Parliament - A law approved by the British Parliament

Bill - The draft of an act which is debated in the house of commons. If the house of Lords and the house of Commons agree the bill is given Royal Ascent and becomes an Act.

There is often a delay between enactment and implementation in a bill as processes need to be put in place to achieve compliance.

11.2.2 The Data Protection Act 1998

The data protection act says that organisations are legally obliged to act responsibly with respect to personal information on any living individual on computer databases.

The DPA enforces strict rules on the storage and processing of electronic data that can uniquely identify a living person.

Data - A representation of information so that it can be conveyed, manipulated or stored.

Information - The meaning that we give to data in particular contexts.

11.2.3 The Investigatory Powers Act 2016 (IPA)

This governs the use of surveillance by public bodies.

This ensures that intrusive powers are subject to strict safeguards. It allows public bodies to access communication records from communication providers when necessary.

11.2.4 The Computer Misuse Act 1990(CMA)

The original CMA included three new criminal offences:

- Unauthorised access to computer materials
- Unauthorised access with intent of committing or aiding further offences

This has been amended to include denial of service attacks.

11.2.5 The Fraud Act 2006

This defines fraud in 3 ways:

- False representation
- Failing to disclose information
- Abusing power

This can be used to prosecute people:

- Dishonestly obtaining electronic communications services
- Cloning mobile phones to bill calls to another person
- Reprogramming mobile phones to interfere with their operation
- Breaking encryption on encrypted communications services

11.2.6 Lawful Business Practice Regulations

In UK law, employers have certain rights to monitor communications made by their employees.

These regulations exist so that employers can ensure that their networks are used in a manner that does not bring the company into disrepute, be used for illegal activities or for personal reasons.

11.3 Recovering from attacks on information security

11.3.1 Making your information less vulnerable

Firewalls on routers and devices, along with encrypting important information makes data less vulnerable.
Specifying file permissions on important files means that some users won't be able to destroy important data.

11.3.1.1 Disabling ports

Software can be used to disable USB ports, preventing attacks through them.

11.3.2 Protecting data for the future

Backups protect from:

- Accidentally deleting a file or program
- Losing disks, computers or memory cards
- Hardware failures, such as a hard disk crash
- Software bugs causing data to be corrupted
- Disasters such as fire or flooding
- Crimes

11.3.3 Remote backups

Remote backups allow for protection against data loss by storing backups away from their centre of operation.

11.3.3.1 Offsite backups

Specialised companies offer storage space to hold backups

11.3.3.2 Backing up to the cloud

Backing up to the cloud is much cheaper than a dedicated offsite backup, this allows access at any time. However if all data is lost it would take a long time to download all the data.

11.3.4 Archiving data

Important files should be archived so that they are never overwritten. In the UK this is handled by the National Archives and the British Library.

12 Managing security risks

12.1 Analysing security risks

12.1.1 Information as an asset

12.1.1.1 Risk Management

Information security risk management assesses the value of information asset belonging to an organisation and protects them on an ongoing basis.

12.1.1.2 Imperatives and incentives

Imperatives - Pressures that force you to act
Incentives - The rewards and opportunities that arise from acting

The imperatives for information security arise from legislation and regulation.

The incentive for information security is trust, companies are more likely to work together if their information is secure.

12.1.2 Risk analysis

Risk - The chance of adverse consequences or loss occurring

Risks are analysed based on their likelihood and impact

12.2 Managing the risks

12.2.1 Staying safe online

12.2.1.1 Updates

Software and operating systems should be kept updated in order to be protected from new cyber attacks.

12.2.1.2 Basic checklist to stay safe

- Set up a personal firewall
- Install an antivirus program
- Get used to making backups
- Make sure computers need a password to log in
- Use hard disk encryption

12.2.2 Risk management in practice

Countermeasures to risk:

- Avoiding the risk
- Modifying the risk to be less
- Transferring the risk to others
- Accepting the risk