Internet Threats and Security

**Introduction**

Networking brings a great range of advantages, which we have already discussed. However, because networked computers are always connected to one another, it means that if someone is able to access one computer, they could in fact access all data on all devices on the entire network! Criminals will do all that they can to gain entry to a network for this very reason. It is therefore vital that we understand these risks and have in place measures to reduce them.

**Threats / Attack Methods**

There are a great deal of threats and methods of attack that systems need to contend with day in, day out.

Let’s now explore each ‘threat’ / ‘method of attack’.

**Malware**

Malware is any software which can harm a computer or user. There are a range of different types of Malware:

Viruses

Spyware

Adware

Pharming

**Viruses**

Viruses are small programs which aim to cause physical harm to a computer system. They often get confused with spyware (which simply spy on users, recording key strokes etc. but do not aim to harm the system – just the user).

The main types are:

*Standard Virus*

These hide in files / programs and replicate themselves in order to spread into other programs / files. Their aim is usually to delete or damage data.

*Worms Virus*

These don’t necessarily damage data, instead they simply try to replicate themselves, using more and more of the computer’s resources, slowing down your computer and making it useless.

*Trojan Virus*

These are often programs (such as a game) which you can use. But in the background they will cause harm, like deleting your files, making annoying changes to your computer setup or creating a portal for other users to use in order to gain access to your system.

**Spyware**

Spyware’s aim is to spy on the user and send back as much information about them as possible (passwords, usernames, websites they visit, purchases they have made). A common piece of spyware is a key logger. It quietly runs in the background recording every key you hit. If you type in the same set of characters, regularly, this could be identified as your password. The reason for collecting this data is so that ‘senders’ of the spyware can use this information to steal your identification or sell your information to third parties who will then target you with advertisements.

**Adware**

Like spyware, this type of malware doesn’t physically delete or corrupt a system’s data. Instead its aim is to download and display unwanted adverts and collect marketing information about your online habits. It will often also try to direct you to unwanted websites by changing your default homepage.

**Pharming**

We have already seen how a DNS server enables us to ‘lookup’ the IP addresses of computer that are hosting website…so that we can then visit them. Pharming malware seeks to change the IP address stored in the DNS (or cached on our computer) to another IP address so that the user is sent to a phoney website instead of the one they intended. For example, if we typed in www.bbc.co.uk into our browser, this URL would be looked up on the DNS and the IP address of the computer hosting the BBC website would be returned so we could visit the site directly. If Pharming malware had attacked the DNS server, the IP address stored for the BBC website would have been altered. So we would be sent an incorrect IP address and would be taken to a phoney website.

**Other Types of Malware**

**Scareware**

This kind of malware often comes in the form of a pop up telling you that you have a virus. The pop up will them advertise purchasable software hoping that you will pass over your money.

**Ransomware**

This malware will seek to lock your computer making it useless. It will then demand that you pay a sum of money in order for you to get your computer working again.

**Rootkits**

These pieces of malware contain a set of tools, which once installed, allow a criminal to access your computer at an administrator level, allowing them to do pretty much what they like.

**Even More Threats & Attack Methods:**

**Phishing**

Phishing seeks to acquire sensitive information about a user such as their usernames, passwords, bank details etc. The way in which this is done is usually through the form of direct electronic communications (emails / phone calls). These emails or phone calls try to impersonate legitimate companies (such as banks) and ask you to give away sensitive information. For example, a user may get an email from what they think is PayPal. The email will have the PayPal logo and font style (corporate identity) and the email will say that they need to update their login details as their account has become compromised. They click the link, go to a website (which looks just like PayPal’s) and enter their details which are then sent to criminals, ready to hack their account!

**People**

We have just seen an example of phishing, where people are influenced to give away their sensitive information. In fact, people are often the main reason why networks succumb to attacks and a loss of data. Social engineering is the act of manipulating people and is often used by criminals to force people to make mistakes which can compromise a network’s security. In addition to phishing, people can be duped into downloading viruses and other malware or tricked into unwittingly giving away passwords. Educating people about the various threats and tricks criminals use, is one of the biggest steps any company can take in making their system secure.

**Brute Force Attacks**

Another method used by criminals to gain access to a secure network is carrying out Brute Force Attacks. A Brute Force Attack is where criminals will use trial and error to hack an account by trying thousands of different possible passwords against a particular username. They will repeatedly try to ‘login’ with one password after another. This threat can be easily reduced by ensuring that a system locks an account if more than three unsuccessful password attempts have been made. The threat can also be reduced by ensuring that all users have complex passwords as these are less likely to be ‘tried’ in a Brute Force Attack due to the increased possible alphanumeric combinations.

**Denial of Service Attacks (DoS)**

This method seeks to bring down websites by using up the web server’s resources. This is done by acquiring multiply computers (often through malware) to repeatedly try to access (or log into) a website. This sudden, massive increase in traffic puts the web server under extreme pressure and will ultimately cause the server’s CPU and memory to be under so much strain that the website will crash. Criminals may then demand money in return for the attack to be stopped. Or criminals will do this to punish websites that they deem unethical or corrupt.

**Data Interception and Theft**

We now know that data travels across and between networks in data packets. Hackers can use specialist hardware and software to secretly monitor network traffic and can intercept any packets that they believe may contain sensitive data. They use ‘packet sniffers’ to sniff out these data packets, decode them and steal the information inside, such as passwords and bank numbers. This is a reason why encryption is so important. This threat is greatly reduced if data is encrypted before it is sent across/between networks. It data is encrypted, it is scrambled and unreadable. This means that if encrypted data is intercepted, the hacker will not be able to make sense of the data.

**SQL Injections**

SQL stands for Structured Query Language and is used to lookup data in a database. When you log in to an account, you will add your username and password into a couple of input boxes. When you press ‘enter’, in the background these two pieces of information are added to an SQL statement:

E.g: SELECT account WHERE username = “bjones” AND password = “pa$$w0rd”

With SQL injections, you can ‘bolt on’ some SQL to the end of your password. This will then alter the SQL statement and allow you to access the accounts of other users. Most websites will have appropriate measures in place to validate that only a password is entered with no extra SQL code.

**Poor Network Policies**

Every network should have a network policy. A network policy is simply a set of rules and procedures that network users must follow. They may include rules / procedures such as:

* Use complex passwords
* Have different levels of access (only certain people in a company can access sensitive data)
* Lock computers if the user leaves their desk

 …etc

If a network policy is poor, or if it is not followed properly, then the risk of a breach in system security increases. Remember, people are often the weakest point when it comes to system security!

**Identification and Prevention**

It is one thing knowing the threats posed to a system. It’s another thing to be able to identify when they may occur and have ways to prevent them.

Let’s now take a look at how these threats can be identified and prevented.

**Penetration Testing**

‘Penetration Testing’ is where a company will invite / employ experts to try to simulate a range of network attacks such as Denial of Service attacks (DoS), SQL injections and Brute Force Attacks. They will attempt to discover any weaknesses in the system and will summarise their findings to the company who will then make improvements to their system security. Due to the fact that technology regularly changes, criminals are constantly finding new ways to target and attack networks. It is therefore important that this form of testing is done regularly.

**Network Forensics**

Networks should have software which continually monitors network traffic. In the event of an attack, this monitoring can play an important part in finding out how the attack was carried out and also by whom. The monitoring software will monitor data packets and so after an attack, suspicious data packets can be analysed forensically.

**Network Policies**

Every network should have network policies.

A network policy is simply a set of rules and procedures that network users must follow.

Networks should have an **Acceptable Use Policy (AUP)**

They may include rules / procedures such as:

* Use complex passwords
* Have different levels of access (only certain people in a company can access sensitive data)
* Locking computers if the user leaves their desk
* No installing of software and downloading files from the WWW
* No use of USB sticks

Networks should also have a **Backup Policy**

They may include rules / procedures such as:

* The person responsible for backing up
* The time and frequency that data should be backed up
* The media on which back ups should be stored on
* The location of the storage of backups (offsite)
* The data to be backed up (all or changes since last backup etc.)

Networks should also have a **Disaster Recovery Policy**

They may include rules / procedures such as:

* The person responsible for backing up
* The media on which back ups have been stored and its location
* The organisations who will help supply the resources / hardware to get the system back up and running.

**Anti-Virus Software (Anti-Malware Software)**

Viruses are small programs which aim to cause active harm to a computer system. They often get confused with spyware (which simply spy on users, recording key strokes etc. but do not aim to harm the system – just the user). Anti-virus software is dedicated to finding and destroying these files. These have to be up-to-date for them to be effective.

**Anti-Spyware Software (Anti-Malware Software)**

Spyware’s aim is to spy on the user and send back as much information about them as possible (passwords, usernames, websites they visit, purchases they have made). A common piece of spyware is a key logger. It quietly runs in the background recording every key you hit. If you type in the same set of characters, regularly, this could be identified as your password. The reason for collecting this data is so that ‘senders’ of the spyware can use this information to steal your identification or sell your information to third parties who will then target you with advertisements. Anti-spyware software is dedicated to finding and destroying these files.

**Firewalls**

When files are sent across the internet, they are broken down into small packets of data. The part of the computer which receives these packets is made up of 256 ports (you can think of these ports like a country’s ports, which manage people in and out of the country). A firewall monitors the data which flows through the ports. They also keep ports closed and open only those that they expect data to be sent to. For example, incoming emails are usually sent to port 110. Having ports closed protects the computer from hackers, plus its continual monitoring will help detect hacker activity.

**Firewalls & Packet Filtering**

Delving deeper, a firewall is simply a device consisting of two NICs. When data packets are received, they are analysed and either allowed through or rejected depending on the protocols that it is governed by.

For example, some unsavoury data packets (as deemed by the rules under which the firewall is working) may be stopped and therefore will be unable to continue their journey to the receiving computer.

This process is known as packet filtering.

**Proxy Servers**

Similar to firewalls, proxy servers can also limit the data that passes from a computer through a network to an external computer. A proxy server is a computer which receives all internet requests before sending them out onto the internet. It will look at each request and analyse it against its protocols / rules and if it meets the rules then it will passed on to the internet and the user will access the service required. However, if the request is for a website / service which is on a blocked / filtered list, it will not be forwarded to the internet and the user will be unable to access the service required. This is how school filtering systems work. You request a webpage and if there are rules against your search term or website request, then your request will be filtered.

Proxy servers also have another use. They can provide privacy online. Some servers will accept your internet requests and then forward them onto the internet but using their own IP address and not yours.

Some proxy servers are dedicated to caching common websites so that a user can browse a copy of a site without accessing it directly. This can reduce traffic to certain websites as a result.

**User Access Levels**

This is where users of a computer system will be given different access rights depending on their role in the company. What this means is that depending on their role in the company, some users will have access to certain parts of the system with other parts inaccessible. For example, in a school, students will only have access to their documents within their own account, whereas the network manager will have access to all accounts and all students’ documents. Access levels are important to ensure that employees cannot view sensitive company information (payroll etc) and cannot sabotage vital system data.

**Passwords**

Passwords are in place to ensure that a network has no unauthorised access. As seen before, it is important that passwords are strong (long and with a combination of alpha and numeric characters) so that they are harder to crack under a Brute Force Attack. They should also be changed regularly.

**Encryption**

Encryption is where data is scrambled before being sent across a network so that it is unreadable if intercepted. To encrypt data, an encryption key is used which will convert ‘plain text’ into ‘cipher text’. An encryption key is an algorithm which will systematically alter each piece of data in a file. For example, a key may convert each letter in a text file to the next letter in the alphabet. For example, ‘hello’ becomes ‘ifmmp’. For the ‘cipher text’ to be converted back to ‘plain text’, the same key is required by the recipient to reverse the encryption.

***Keywords / Key Terms:***

**Proxy -** Representing someone / something else, on their behalf.

**Policy -** A rule / set of rules that must be followed.