Higher
Computing Science

Computer Systems

Security Risks & Precautions

Name:_____

Contents

Computer Misuse Act

The Computer Misuse Act was designed to protect individuals and businesses against computer attacks such as:

- Gaining **unauthorised access** to a computer to view data, modify data or commit a crime.
- **Hacking** into a computer network or accessing a computer networking without appropriate authorisation.
- Purposefully creating or distributing malicious software such as **viruses**.

The Computer Misuse Act is divided into **three main** offences:

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

1. Unauthorised access to computer material:

- Causing a computer to perform any function with intent to secure access to any program or data held in a computer or network
- Gaining any unauthorized access to a computer or a network or any particular program or data stored on the computer or network
- Accessing or using a computer or network by using another person's user name, e-mail, password etc. without appropriate authorisation.

2. Unauthorised access with intent to commit or facilitate commission of further offences:

- Interfering with the normal operation of the system with the intent to cause harm or damage. E.g. changing passwords and settings to prevent others accessing the system

- Purposefully spreading malicious and damaging software such as viruses

- Using hardware and software to access, copy, modify or steal data without appropriate authorisation. E.g. using phishing or keylogging to gain access to a computer system

3. Unauthorised modification of computer material:

- Unauthorised access to modify computers include altering software and data

- Deleting or making changes to a file with the intent to cause damage to an individual or company

- Purposely introducing viruses onto a computer or network

If found guilty of breaching the Computer Misuse Act the penalties include up to 10 years in prison and/or a fine.

Tracking Cookies

Cookies are text files that contain information about browsing habits, such as the website visited and the username used to access the site.

They can also track things like the amount of time spent on a site, or the multimedia that was watched as well as user defined browser settings.

Cookies can be helpful for those using the same system to access the internet on a regular basis. They can make browsing seem less demanding by remembering preferences and usernames. This saves time the next time you visit a website.

However, there are **'tracking cookies'** and these cookies are designed to send as much data as possible to external servers/third parties.

Sometimes the tracking cookie is used for market research and no theft of data is intended but on other occasions programmers can set the tracking cookie up to send them usernames and personal details.

As well as concern around identity theft, these cookies can be used to target users with personalised adverts.

Denial of Service(DoS) Attack

A DoS attack is a deliberate attempt to prevent legitimate users of a network from accessing the services provided by the server or connected systems.

The classic DoS attack will come from a single computer sending multiple requests to the server.

Denial of service attacks usually aim to overload servers or systems with requests for data or access to resources like the processor or main memory.

Some denial of service attacks also exploit weaknesses, either in the security system or network infrastructure.

Symptoms and effect of Denial of Service attacks

Common symptoms of a Denial of Service attack include:

- slow performance when trying to log in to a web based system, as the system may be under attack
- slow network performance in general
- inability to access a website as the web server may be under attack

The effect is inconvenience and **disruption for users** who are denied access to services they expect to use.

Cost of Denial of Service attacks

For organisations that fall victim to a Denial of Service attack the costs usually fall into two categories:

- loss of income
- repair costs to bring software and efficiency back to pre-attack level

A site selling goods online would be unable to receive orders, leading to a loss of income. Attackers often plan attacks when they know that an organisation would expect many users to want to access the server or services.

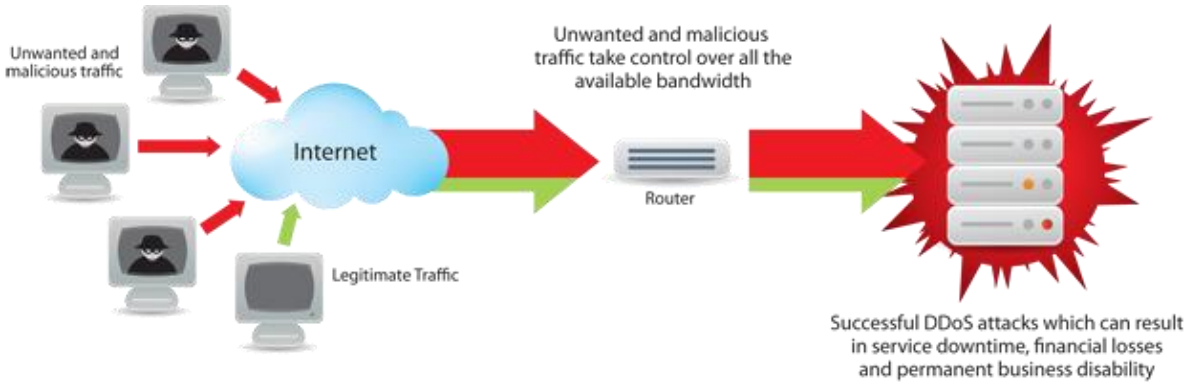
Organisations will often have to call in staff out with their normal working hours or hire additional staff to get the server back up and running again as soon as possible. While most attacks are resolved within 1 or 2 hours, the performance of the server may not be that of pre-attack performance for a number of hours.

Type of Denial of Service attacks

<u>Bandwidth consumption</u>

Bandwidth consumption is a fairly general term to describe overloading a server or individual system with too many data packets or requests at the same time, creating an overload in network traffic.

When this happens, the system is unable to send or receive data as the bandwidth available is used up by all of the network traffic/packets trying to get to the system.



Resource starvation

Resource starvation attacks are designed to use up system resources.

Processors and **main memory** are examples of resources that can be attacked, as is backing storage.

An example could be sending data over a network that requires the same process to repeat over and over again. By ensuring that the processor is always dealing with a recurring request, other processes cannot get enough processor time to execute properly.

Main memory and **backing storage** can also be targeted, an example of a method of starving available memory on a server could be to constantly add items to the basket of a server for an e-commerce site. This can be achieved by writing a script that adds millions of items.

Scripts can also be created and sent to a server requesting that thousands of new user accounts be created. Each new account would add to demands on backing storage and eventually starve available storage for legitimate requests.

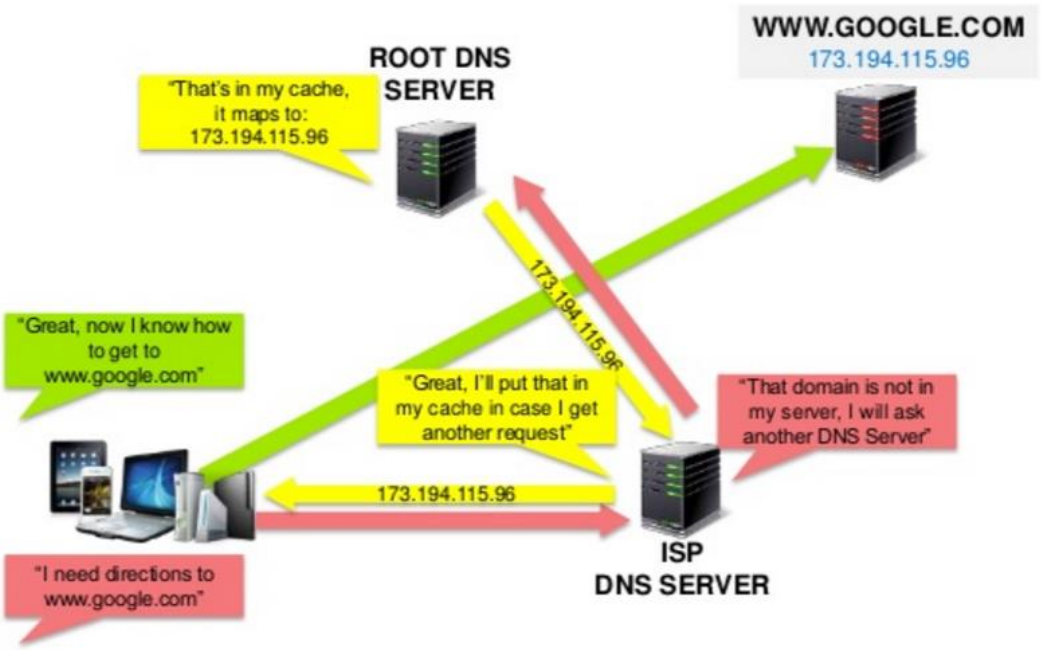
Domain Name Server attacks

We all know that we can type in a web address (URL) to access a web page. But computers must use IP addresses to communicate with each other.

This means that when you type in the web address, there has to be a way for your computer to find out the IP address for the web server which holds the web page.

Domain name servers (DNS) hold a directory of domain names and their associated IP addresses.

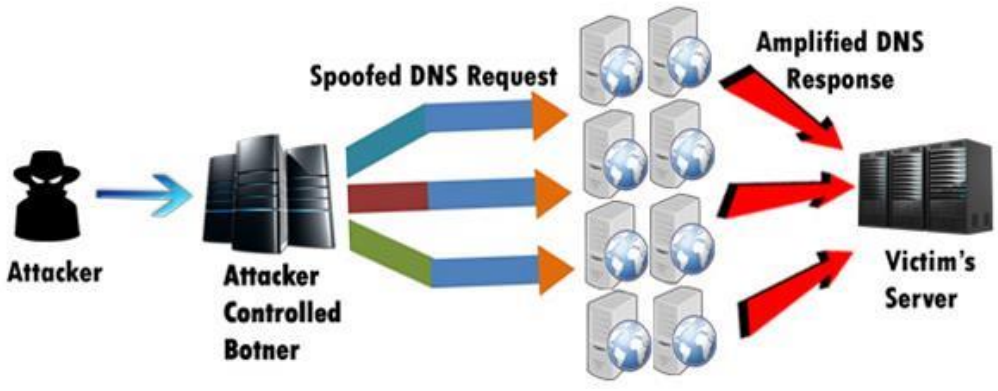
When a URL is entered into the browser, the default DNS server is contacted. The DNS looks up the web address in its directory and **replies** to the client computer with the corresponding IP address.



Domain Name Servers can be used in a Denial of Service attack when:

- attackers use 'spoofing' - using the IP address of a system that they want to attack without permission to use that IP address
- they send lots of queries to different Domain Name Servers at the same time
- the results of the queries are sent back to the IP address of the system they are targeting
- the attacked system is overloaded with replies from lots of different Domain Name Servers, all trying to send the website IP address that matches the domain name sent with the query

The sheer volume of replies that the targeted system receives will result in bandwidth consumption and overload the system so that it cannot send and receive data to and from the network.



Reasons for launching a Denial of Service attack

Reasons for launching Denial of Service attacks vary but broadly fall under one of three categories:

- Personal motive
- Political motive
- Financial gain

Some organisations are formed with the intention of creating distributed denial of service attacks. A portion of these groups do so for personal reasons, often linked to their ability to bring down large networks or organisations.

While many more are motivated by political and financial reasons there are those who engage in denial of service attacks as an area of personal interest.

There are also those who may have a personal grievance against an organisation or individual, who then choose to launch attacks if they have the necessary expertise.

Many more are motivated by politics or social issues. There are some well-known self-appointed civilian groups who work together online to target organisations who they perceive as incorrect or guilty of a political or social scandal.

National security groups have also been known to attack the networks of rival nations and there are likely to be many attacks every day that target the various military and defence agencies around the world.

Criminals also make use of distributed denial of service attacks, often in the hope that they can threaten organisations or users with an attack that can be prevented if they are willing to pay a fee. Some people are also willing to be hired by others if they have the technical knowledge necessary to carry out attacks on behalf of another person or group.

Security Precautions

Encryption

Encryption is the process of changing data so that it cannot be understood by a third party. **Decryption** is the reverse.

Data is **scrambled** using a mathematical process which turns it into something that looks like nonsense.

This means that if anyone steals the information it will be meaningless to them. It will look like gobbledygook.

Encrypted data is known as **ciphertext**. Ciphertext cannot be read without first being decrypted.

There are two types of encryption:

- Conventional (Symmetric) Encryption
- Public Key (Asymmetric) Encryption

Symmetric Encryption

Conventional encryption is the simplest form of encryption. Also known as symmetric encryption as data is encrypted and decrypted using **the same key**.

Data (plain text) is encrypted using a secret key and encryption algorithm. Both parties must have a copy of the secret key which must also be kept secure.

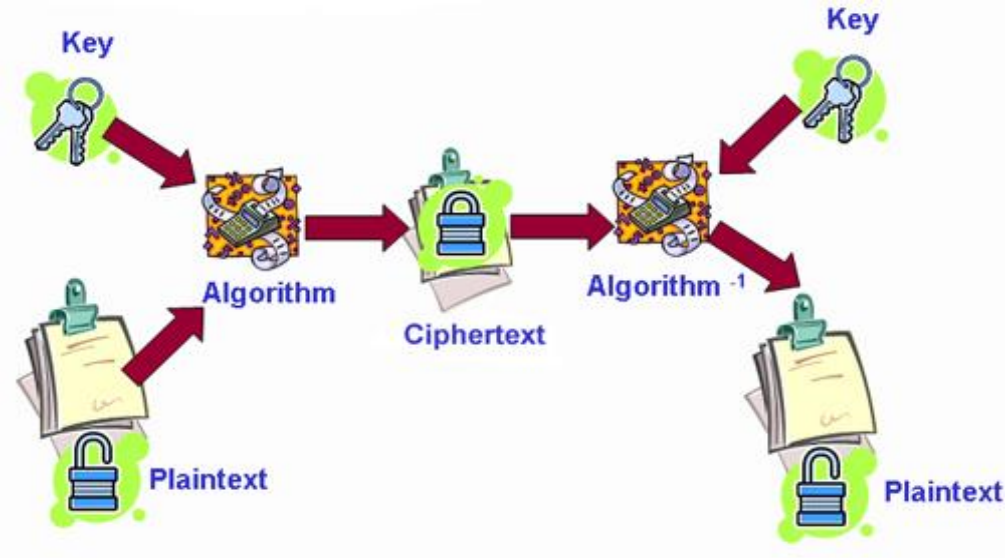
Encryption Key

A **key** is a long sequence of bits used by encryption / decryption algorithms.

To crack some ciphertext encrypted with a 64-bit key by trying every combination of keys possible means you have 2^64 possible combinations (18 followed by 18 naughts).

If you have a computer that can carry out one encryption operation every millisecond, it will take about 292 million years to find the correct value.

Plain text is combined with the secret key and encryption algorithm to produce ciphertext.



Ciphertext is then combined with the secret key and the decryption algorithm to produce plain text.

Problems with Symmetric Encryption

- The secret key must initially be shared between both parties.
- So unless a secure method exists (physically meeting each other) then the system is inherently insecure.
- If an attacker obtains a large number of encoded messages, letter or word frequency tables could be used.

Despite these problems, symmetric encryption is reliable and allows for fast decryption. It is still a very popular method of encryption and is used by many large organisations to manage the transmission of online communication.

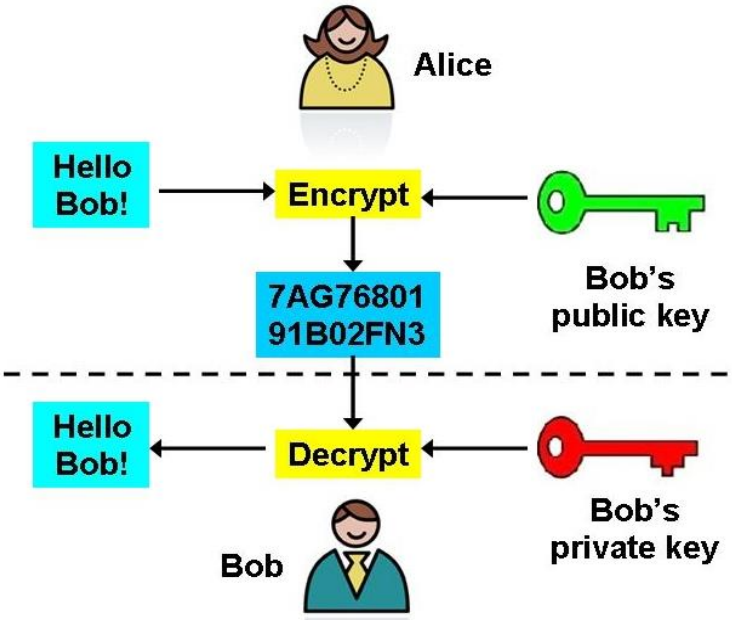
Public Key Encryption

Public Key Encryption is more complicated and slower but more secure. Also known as **asymmetric encryption** as data is encrypted and decrypted using the **different keys**.

Public key can be made available to anyone but only the **owner** of the public key can decrypt it using a **private key**.

Since a different key is used for decryption, it always remains secret and is therefore more secure.

Plain text is combined with the **recipients public key** and **encryption** algorithm to produce ciphertext.



Ciphertext is combined with the **recipients private key** and **decryption** algorithm to produce plain text.

"Key" points

Encrypting – message is encrypted using the recipients public key

Decrypting – message can only be decrypted using the recipients private key

Digital Signature

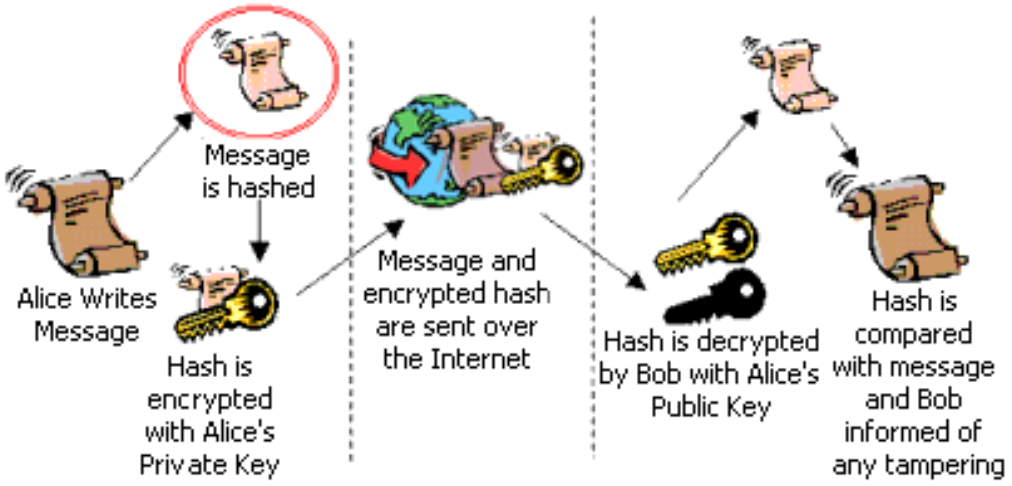
A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document has not been tampered with.

Sending Computer

- Sender must first **purchase encryption software** allowing him to create public and private key
- Hashing algorithm is applied to the data to be transmitted creating a unique **message hash** (mathematical summary).
- Message hash is encrypted using the **<u>sender's</u> private key**.

Receiving Computer

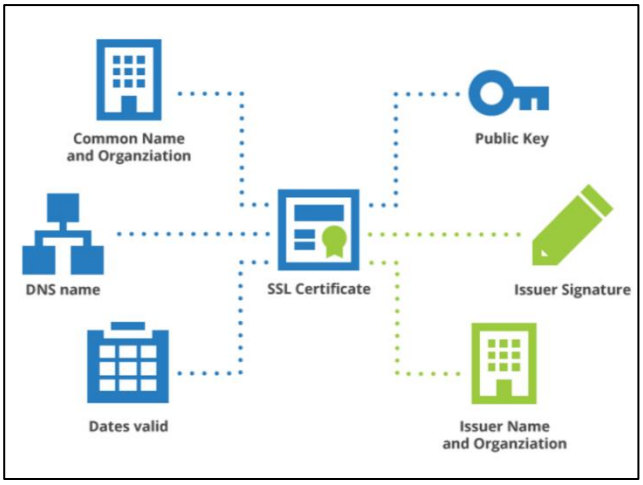
- **<u>Sender's</u> Public key** is used to decrypt the message hash – if this works then it proves the sender's identity.
- Hashing formula is then applied to the data to calculate its own message hash and this is compared to the one transmitted.
- If they match then the data has arrived untampered.



Digital Certificate

A digital certificate can be known as a digital key certificate, public key certificate or an identity certificate, but they all refer to the same product.

A digital certificate is an electronic document that contains a digital signature, which **confirms the name and identity of a person or organisation**.



A digital certificate allows individuals or companies to feel secure in exchanging information as they each know the identity of the other party.

A digital certificate is exceptionally **hard to forge** and can be trusted as it will have been **issued by a trusted agency**.

A digital certificate will contain

- A serial number that is used to uniquely identify the certificate, the individual or the entity identified by the certificate
- The algorithm that is used to create the signature
- The Certification Authority that verifies the information in the certificate
- The date that the certificate is valid from and the date that the certificate expires
- The public key and the thumbprint algorithm (to make sure that the certificate itself is not modified)

A digital certificate gives the user of a site confidence that:

- The site is authenticated e.g. certificate issued by (certification) authority
- The site is regulated

Revision Questions – Security Risks & Precautions

1. An online bank uses digital signatures when sending financial documents. Describe the purpose of a digital signature when sending documents.

2. When people make donations their payment details must be kept secure. Describe how encryption is used to ensure the secure transmission of data.

3. The theme park is aware that their website might be subjected to a DOS attack. State the effect on customers of a DOS attack.