Authentication

There are a number of ways in which we can make networks more secure. Four of these methods are listed below. Using these methods together will increase security.

Authentication compares user information entered against that stored in a database. The simplest method of authentication is to use a **username** and **password**. The password is used to **authenticate** the user. It is checked to see if it is the same as the password stored in the **database**. As users may choose easy passwords or write them down, this information alone is not always **secure** enough. Other methods can be used. For instance, a **second password** or number can be used. Often the authentication system will only ask for certain digits of the number to prevent **keyloggers** or **telephone operators** from stealing the whole password. **Security questions**, such as "What is your mother's maiden name?", or "What was your first school?" are often used as authentication during a phone call. Other methods of authentication include **fingerprint readers**, **iris scanners**, **chip and pin readers** and **RFID readers**.

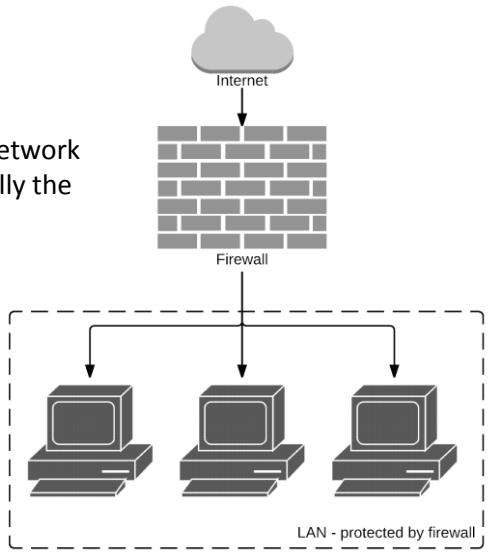
Encryption

Encryption is **encoding** data so that it can only be **decrypted** and read with a key or password. It is possible to encrypt data with a password and then send it through a network. The user at the other end will need to have the password to decrypt the file.

HTTPS (**Hypertext Transfer Protocol Secure**) is a method of sending web pages and information through the Internet in a secure manner. You will often see a green padlock in the web address bar when using these pages. Your web browser and the server will encrypt web pages and any information entered into forms before they are sent. This will prevent an **eavesdropper** from listening to the data as it goes through the Internet.

Firewalls

In computing, **firewalls** create a barrier between a trusted internal network (e.g. a school network or home network) and another network (usually the Internet). This protects all the computers behind the firewall.



Computers on networks open different **ports** for different **protocols** and programs. For example, the **HTTP** protocol used for delivery of **web pages** usually works on **port 80**. Firewalls can **block** ports on the computer, if they are not required, to prevent them being compromised.

When sending information through a network, the data is divided into **packets**. Firewalls can look at the data inside each packet as it comes into the computer, inspecting it for viruses, spam or the protocol being used. If it finds anything suspicious then it can filter out the packet so that nothing harmful comes into the internal computer network. This is known as **packet inspection** and **packet filtering**.

MAC address filtering

Each **Network Interface Card** (**NIC**) is embedded with a unique **media access control** (**MAC**) address at the factory. It is possible to **filter** devices that can access a network to only those with approved MAC addresses. If a **MAC address** is **blocked** then it will be unable to access any services on the network. It is possible to spoof (pretend to use) another device's MAC address, so this method should be used in conjunction with a username and password or another method of authentication.