IT Systems Security and Encryption 7

Getting to know your unit

Assessment
You will be assessed by a series of assignments set by your tutor.

Security is a big issue in today's internet-centric world. We rely heavily on computer systems for so many aspects of our lives that they have become an attractive and lucrative target for the modern criminal. Keeping computer systems secure requires constant vigilance because, as technology develops rapidly, new threats to these systems, and new vulnerabilities, appear all the time.

As a computing professional, you will need to have a good understanding of current security threats and of how to apply protection methods for any given cyberattack. As security defences become more robust, the attack methods become more sophisticated.

In this unit, you will learn about the different types of security attack and how to protect IT networks from these attacks, as well as how to configure and support these networks. You will learn about encryption and will apply suitable protection to an IT system. A good understanding of cybersecurity will prepare you for a job in the computing industry or for entry into higher education.

How you will be assessed

This unit will be assessed by a series of internally assessed tasks set by your tutor. Throughout this unit, you will find assessment activities that will help you to prepare for the final assessment.

Assessment criteria

This table shows what you must do in order to achieve a **Pass**, **Merit** or **Distinction** grade, and where you can find activities to help you.

Pass	Merit	Distinction
Learning aim A Understand current IT security threats, information security and the legal requirements affecting the security of IT systems		
A.P1 Explain the different security threats that can affect the IT systems of organisations. **Assessment practice 7.1**	**A.M1** Assess the impact that IT security threats can have on organisations' IT systems and business while taking account of the principles of information security and legal requirements. **Assessment practice 7.1**	
A.P2 Explain the principles of information security when protecting the IT systems of organisations. **Assessment practice 7.1**		
A.P3 Explain why organisations must adhere to legal requirements when considering IT systems security. **Assessment practice 7.1**		**AB.D1** Evaluate the effectiveness of the techniques used to protect organisations from security threats, while taking account of the principles of information security and legal requirements. **Assessment practice 7.1**
Learning aim B Investigate cryptographic techniques and processes used to protect data		
B.P4 Explain the principles and uses of cryptography to secure and protect data. **Assessment practice 7.1**	**B.M2** Analyse how the principles and uses of cryptography have an impact on the security and protection of data. **Assessment practice 7.1**	
Learning aim C Examine the techniques used to protect an IT system from security threats		
C.P5 Explain how protection techniques can help defend an organisation from security threats. **Assessment practice 7.2**	**C.M3** Justify the choice of protection techniques used to defend the IT systems of an organisation, showing how its IT system will be protected from security threats. **Assessment practice 7.2**	**CD.D2** Evaluate the plan and the effectiveness of the protected IT system against requirements. **Assessment practice 7.2**
C.P6 Produce a plan to protect an IT system that meets organisational and legislative requirements. **Assessment practice 7.2**		
Learning aim D Implement strategies to protect an IT system from security threats		
D.P7 Perform tasks to protect the IT system to meet requirements given in the plan. **Assessment practice 7.2**	**D.M4** Enhance the protection of the IT system to meet requirements given in the plan. **Assessment practice 7.2**	**CD.D3** Demonstrate individual responsibility and effective self-management in the planning and protection of an IT system. **Assessment practice 7.2**
D.P8 Review the extent to which the organisation's IT system has been protected. **Assessment practice 7.2**		

Getting started

Have you or someone you know had a security issue with a computer or suffered from a computer virus? These kinds of problem are very common, but they can cause a lot of disruption. How much time did you or the person you know spend fixing the issue?

A Understand current IT security threats, information security and the legal requirements affecting the security of IT systems

Link

Cybersecurity issues are often in the news. Check out news websites such as the technology section of the BBC news website for the latest IT security issues.

Resolving security issues costs not only time but also money, if you need to pay to have the virus removed. Security issues may be very frustrating too, because you may lose important files. The frustration and annoyance that individual users encounter when they have security issues with a personal computer system is amplified many times for businesses as they stand to lose significant amounts of money, both directly (due to fraudulent activity) and indirectly (through the time required to resolve security issues). Businesses often want to keep quiet about any security issues they encounter as this may reflect badly on the organisation, so the true extent of the security problems experienced by businesses is not easy to confirm. If you ask your friends and family, you may well find that almost everyone who uses a computer (personally and professionally) has experienced some kind of security issue, even if only by receiving a phishing email. Cybersecurity is never far from the news.

Threat types

Threats to IT systems can come from a variety of sources. A company's employees, either deliberately or unintentionally, can be a source of security risk, while a range of threats also exist outside the company. The threats themselves come in a number of different forms: internal, external, physical or social engineering and software-driven threats.

Internal threats

There are many threats to IT security from within an organisation, both deliberate and accidental or unintentional.

Deliberate

There are a number of deliberate, internal threats to security.

- **Employee actions:** Disgruntled or recently dismissed staff may damage or delete files as a form of revenge. They may also cause damage to the company software systems or post damaging information about the company online.
- **Data theft:** Employees may steal data (such as customer lists or credit card details) which they can then sell to cybercriminals or competitors. In many cases, it is relatively easy for employees who have legitimate access to an organisation's computer systems and data, to make copies of it.
- **Users overriding security controls:** Employees may want to bypass security controls as they find them too restrictive and frustrating. For example, they may want to use their favourite internet browser or install a game they enjoy playing during their lunch break.

Tip

As a computing professional you may find yourself working with users who have a limited understanding of IT security issues. You need to develop the communications skills to be able to explain in a clear and non-technical way what the security issues are and why protection methods are in place. You also need to remain calm and professional when users may be angry or upset because of the IT problems they are facing.

Accidental or unintentional

There are a number of ways in which internal security can be threatened accidentally or unintentionally.

- **Accidental loss:** Employees may accidentally delete important data. Accidental deletion or corruption of data may be due to poor training or misunderstanding of procedures, or it could be due to poor software application design. Although most operating systems provide a 'recycle bin' facility where deleted files may be retrieved, some of the software applications an organisation uses may not have this facility.
- **Unintentional disclosure or damage to data:** Employees may unintentionally disclose confidential data (such as passwords) or they may damage data by corrupting it. Employees may unintentionally disclose their passwords by writing them down (perhaps even leaving notes on their desk with passwords written on them), by leaving their computer logged on when they are not at their desk, or by sharing passwords with others. By disclosing passwords to anyone who does not have legitimate access to the computer system, an employee is exposing the organisation to a security risk because the information may fall into the hands of a cybercriminal. Corruption of data may be due to poor training or misunderstanding of procedures, or it could be due to poor software application design, facilitating accidental deletion of data.
- **Unsafe practices:** An organisation's employees may carry out actions which leave the company's computer system open to security attacks by external cybercriminals. These unsafe practices include the following.
  - Using external flash (USB) storage devices which may have been infected with **malware** when used on another system, such as the employee's home computer.
  - Visiting websites which are untrusted, because these websites may attempt to infect computer systems with malware.
  - Downloading files from untrusted websites may introduce malware to a computer system. Uploading company files to the internet also exposes company data to cybercriminals.
  - Using file sharing software applications may introduce malware to a computer system.
  - When employees bring in their own devices (laptops, tablets, smartphones) from home (sometimes called 'Bring your own device (BYOD)') and connect them to the organisation's network, it exposes the network to any malware that is on those devices. Some companies encourage employees to use their own devices as then the company does not need to provide them and it can boost morale, but they need to protect themselves from the related threats to security by addressing BYOD in their acceptable use policy.

Link

For more about acceptable use policies, see 'Policies and procedures'.

Key term

Malware – an umbrella term for software that has a malicious intent. Malware has a deliberately negative effect on a computer. Once installed, it can gather private information, slow the computer down, delete or lock access to files, for example.

External threats

Threats from outside an organisation come from a variety of sources. In most cases, there is a financial motivation and cybercriminals usually intend either to steal information which can be used to obtain money (that is, bank account details or credit card numbers) or to hold a company or individual to ransom by encrypting data or preventing access to services. Competitors may also wish to attack an organisation in order to gain a competitive financial advantage. Such activities would most likely be themselves criminal acts.

In some cases, there is a political motive, for example demonstrators or protest groups may target an organisation that they disagree with politically, ethically or on the basis of religion. Cyberattacks may also be used as a form of warfare when one country attacks another. There are many benefits to cyberterrorism for the attacker, not least of which is that there is little risk of loss of life for the attacker, but the chaos that would be caused if banking, transportation, or other financial or safety critical systems were disrupted or destroyed by an attack would be huge.

Research

The Stuxnet computer worm is said to have been developed by the US and Israeli governments to attack the Iranian nuclear programme, although they have never admitted this. Research what Stuxnet does and how it has been used.

Physical threats

Computer equipment can be valuable and there is a possibility that it may be stolen or maliciously damaged. Theft or loss of portable equipment which may contain sensitive information is a particular threat to security because once a hard disc is removed from a computer system, it may be possible to circumvent the security measures that protect the data it holds. Organisations also need to be aware of the possibility of accidental damage or destruction to computer systems by fire, flood or other disasters. This may mean the loss of important and valuable data and, at the very least, would result in the expense of replacing the equipment.

Link

There have been a number of occasions when people have lost laptops containing personal or sensitive information. A search on the BBC news website should produce several news articles about laptops containing sensitive or personal data which have been lost or stolen, and the potential consequences.

Social engineering and software-driven threats

Social engineering is a technique that is used to attempt to fool computer users to provide secure information to cybercriminals. Social engineering uses software that is designed with a malicious intent.

Social engineering

The best known example of social engineering is the 'phishing' scam. This involves sending emails that claim to come from a bank to large numbers of people asking them to log into their account using a link provided in the email. (Quite often the people receiving the phish email will not even have an account with the bank that the email claims to come from). The link provided in the email does not take the receiver to the real bank's website but to a fake version of the site where, if the individual enters their banking login credentials, these can be stolen by the cybercriminals running the scam.

There are many other scams which use social engineering, and some are as simple as telephoning someone in an office claiming to be from their IT support department and asking them for their passwords. Social engineering threats can be difficult to defend against and there is no software protection available, so people need to be trained to be aware of these kinds of threat and to be on their guard at all times.

Some of the well-known social engineering threats with specific names include the following.

- **Shoulder surfing** – This is simply looking over someone's shoulder in an attempt to obtain sensitive information such as usernames, passwords and PINs. Careful placement of monitors can help prevent this.
- **Spear phishing and whaling** – These are both forms of phishing that involve targeting a specific group of people rather than the blanket approach used with phishing. For example, a criminal might send an email to all the employees in a company that claims to come from one of the company directors, which asks them to reply to the email with their system password. This is known as spear phishing because it is targeted phishing. Because the email looks as if it comes from the company director, employees might be fooled into responding. Whaling involves sending phish emails to senior executives ('whales') specifically.
- **Dumpster diving** – Looking through rubbish or recycling bins (dumpsters) can provide criminals with valuable information. They might, for example, be able to obtain a company employee directory that contains the emails and phone numbers of everyone in the company. This information could then be used for a spear phishing or whaling attack.

Discussion

Discuss with a peer or in a small group the ways in which you can defend yourself and others against social engineering attacks such as phishing.

Software-driven threats (malware)

Social engineering cyberattacks use malicious software, known as malware. Malware is one of the best known threats to IT security and, although the first malware was originally created in the 1980s as an experiment or prank, malware is now a serious threat to computer systems.

Malware is very common and large amounts of malware are released every year. The main route for malware to reach computers is via the internet, although infection via removable devices such as USB drives is also common.

Malware usually targets Microsoft® Windows® computers, and is much less prevalent on other operating systems such as Linux®. The increasing use of mobile devices has led to more and more malware being created to attack Android™ and Apple® iOS.

There are a number of different types of malware.

- Viruses are programs that are usually concealed within another program or file. They replicate by inserting copies of themselves into other programs or files. They usually (but not always) have a malicious intent.
- Worms, like viruses, also replicate themselves, often over a computer network, but, unlike viruses, they do not attach to another file or program. Worms often seek out known security flaws and 'worm' their way into the system through these 'holes' – hence the name.
- Trojan horse is a term for any type of malicious program that pretends to be something useful or interesting in an attempt to get a user to unwittingly download or install it.
- Ransomware is a type of malware that restricts access to a user's computer, often by encrypting files, and demands a ransom be paid before the computer will be unlocked.

Research

CryptoLocker is a well-known example of ransomware which encrypted files on infected computers and demanded a ransom for their decryption.

Research how CryptoLocker works, what effects it had on infected computers and how it was eventually disrupted.

- Spyware collects information without the user's consent and is most commonly used to collect information about a user's internet browsing habits with the aim of showing targeted pop-up adverts to the user. Some types of spyware include an embedded 'keylogger'. This records any information you type at your keyboard which can be sent on to someone else who may have a malicious intent
- Adware is malware that presents adverts to the user, usually using pop-up windows. It may (like spyware) analyse a user's internet habits to provide targeted adverts. Spyware and adware do not normally have a damaging effect on a computer but can be irritating for the user.
- Rootkit is term for a program which can allow an attacker access to areas of a computer that they would not normally have access to. For example, it might provide the attacker with administrator or root access to the operating system.
- Backdoor is a method that is used to bypass a computer's normal authentication procedures, thereby providing unauthorised remote access to the computer.
- Logic bomb is code included in malware that lurks for a while and then executes when certain conditions are met, such as a specific date being reached. Such malware can spread widely across computer systems before it is noticed.

Computer network-based threats

Many security threats access the targeted computer system via the networks they are connected to. Many of these threats use features of the **internet protocol (IP)**.These computer network-based threats can be passive or active.

Key term

Internet protocol (IP) – one of the most important protocols is the TCP/IP protocol suite which is used for communication in local area networks (LANs) and via the internet. IP addresses are assigned to all devices that are participating in a network that uses the internet protocol.

Passive threats

Passive computer network-based threats include the following.

- Wiretapping: This pre-dates computers, having been used since the early days of telephone networks, and it involves listening in to data being transmitted over a network. Traditionally, this involved a physical connection to a wired network but, more recently, it is typically done by listening into WiFi networks that use radio communication. WiFi networks should be encrypted so that only users who know the key to access the network can join it, but it may be possible to crack a WiFi key or obtain it through social engineering techniques. An attack may use techniques such as **ARP spoofing** and software such as Wireshark to view data sent over the network.

Key terms

ARP spoofing – ARP (address resolution protocol) is a protocol used in LANs to provide a mapping between the physical addresses of devices (**MAC addresses**) and their IP addresses. An attacker can send fake (spoof) ARP messages onto a local area network (LAN) which associate the attacker's computer with the address of another device on the LAN, such as the default gateway (or router). Therefore all messages being sent outside the network will be forwarded to the attacker's computer rather than to the default gateway.

MAC address – a unique fixed hardware address that is permanently coded into a network device, such as a network interface card, by its manufacturer. A MAC address is a 12 digit hexadecimal number. The allocation of MAC addresses is managed by the IEEE (Institute of Electrical and Electronic Engineers).

- Port scanning: This is a method of probing a computer's network **ports** to see if any of them are open and what services are running on the system. This is not an attack, as such, but a would-be attacker can use this information to potentially exploit vulnerabilities in the services that are running.

Key term

Ports – a part of the design of the TCP/IP protocol suite that is the method of communication that the internet uses. IP addresses are used to identify individual computers, and ports are used to identify specific services or applications. The HTTP protocol, used to transfer web pages, generally uses port 80.

- Idle scanning: This is a form of port scanning in which the attacking computer does not have any direct interaction with the computer it is scanning. The attacking computer uses another computer called a **Zombie** to scan the target computer's ports. The benefit to the attacker of using this method is that there is no trace of the attacking computer's address on the target machine.

Key term

Zombie – a computer which has been compromised by an attacker and used to carry out a variety of malicious attacks on other computers under the remote control of the attacker. The owner of the computer is unaware that this has happened.

Active threats

There are also many computer network-based threats which can be classified as active threats.

- Denial of service (DoS) attack: Involves sending so many requests to a web server that the server is overwhelmed and cannot respond to legitimate requests. This has the effect of taking the website hosted on the target machine off-line. In most cases, the sender IP address of the machine launching the attack is forged so the source of the attack cannot be easily identified. There are a variety of different versions of the DoS attack. In order to send sufficient requests to overwhelm a powerful web server, a distributed denial of service (DDoS) attack can be used, where a **botnet** of many computers can be used to launch the attack.

Key term

Botnet – a collection of zombie computers (very often home-based computers) which are controlled remotely to carry out various actions, such as sending spam emails or launching DDoS attacks.

- Spoofing: This is a technique used in many types of attack (such as DoS attacks) in which the source address of an attacking computer is hidden. For example, it is possible to create IP data packets with a forged sender IP address. This helps to hide the identity of the computer launching the attack.
- **Man-in-the-middle:** This type of attack involves listening in to, and potentially modifying, data exchanges between two computers. Man-in-the-middle (MITM) is a type of eavesdropping and could be used, for example, on an unencrypted WiFi connection to view data being sent by people using the network.

- **Address resolution protocol (ARP) poisoning:** The ARP is used to map fixed physical hardware addresses (MAC addresses) to IP addresses (which are dynamically allocated to devices by routers or servers) on a LAN. In this type of attack, faked ARP messages are sent which are intended to fool other devices that the attacker's computer is actually another device, such as the network default gateway (where messages which have destinations outside the LAN are sent). This allows the attacker to intercept messages that were not intended for their computer. This is a type of MITM attack.
- **Smurf attack:** This is a type of DDoS attack. It utilises a feature of the internet control message protocol (ICMP), whereby, when a computer receives an ICMP message, it replies to the source IP address in the ICMP message, confirming that the message was received. The original intention of this feature was to test if devices were connected and working. However, an attacker can send an ICMP message with a faked source IP address of the computer to be attacked. If this message is sent to the broadcast address on a network, then every device on that network will reply, sending its message to the computer that is being attacked (the broadcast address is a special IP address. Messages addressed to it are sent to every host on the local network). In a large network, so many ICMP messages could be sent that the attacked computer would be overwhelmed. To avoid this kind of attack, most modern devices no longer respond to ICMP messages sent to the broadcast address and so are not vulnerable to this type of attack.

Research

ICMP is not used to send messages between computers. Instead it is used for diagnostic or control purposes. One useful network diagnostic tool that uses ICMP is a program called Ping. Find out what Ping is for and how it can be used.

- Buffer overflow: This is an example of a vulnerability that can affect legitimate programs running on a system which can be of benefit to an attacker. A buffer is a memory area allocated by a program to store input data. The program will allocate a certain amount of memory but, if the input is larger than the buffer, an overflow can occur. There are a number of ways in which this can be exploited by cyberattackers and they all require an advanced understand of programming techniques. Essentially, this involves forcing the program to execute code provided by the attacker rather than the intended code.
- Heap overflow: This is a type of buffer overflow. In operating system memory management systems, the 'heap' is a term used to refer to those areas of memory that can be allocated to programs for them to use. By corrupting application data held in the heap in a particular way, the attacker's code can be executed.
- Format string attack: This is another type of attack that can target poorly written programs that use the C family of programming languages. The attack targets code used to format input data. Carefully designed input causes this code to behave in a way that can be of benefit to the attacker. For example, it might allow the attacker to execute their own code. A detailed understanding of programming is required to exploit this vulnerability.
- Structured query language (SQL) injection: SQL injection is a widely used method of attack that targets SQL databases and is often used against web-based database applications. This attack involves using certain types of input that can change the way the application works via a web page. It provides the attacker with the ability to access data in the database in a way that the application did not intend.

Worked Example: Product search SQL injection

For example, think of the product search box that appears on e-commerce websites. When you type something into the search box (such as 'Nike® trainers') that value is used in an SQL query that searches website's database for matching values. Typically the sort of SQL statement that might be used is as follows.

```
SELECT * FROM Products WHERE description
= 'Nike® trainers'
```

An attacker with a knowledge of SQL can use the fact that SQL uses a semicolon to indicate the end of a statement. Suppose that an attacker entered the following into the product search box:

```
'Nike® trainers'; SELECT * FROM customers;
```

When this statement is read by the web application, it is turned into two statements (because the semi colon indicates the end of the first one). The first one is the same as before, the second one is:

```
SELECT * FROM customers
```

This could potentially provide a list of all the records on the customer table, including names, addresses, credit card numbers etc. []

There are a number of other similar ways that search string inputs can be used to manipulate SQL statements. By sending improperly formatted SQL statements that generate errors, the error messages shown can tell the attacker a lot about the software the web server is using, such as the type and version of database system in use. This information is useful in that it helps the attacker to exploit vulnerabilities which exist in particular software and versions of that software.

SQL injection can allow attackers access to large amounts of data which may be confidential, for example customer details. Applications should be written in such a way as to prevent this kind of attack using proper input validation and error checking, but many older applications are not protected in this way and are vulnerable to attack.

Research

SQL injection has been used in a number of high profile attacks on well-known British companies in which large quantities of customer details have been accessed. Research SQL injection attacks and find out what happened in some well-known cases and find out why the systems were not protected.

- **Cyberattack:** An attack against a specific organisation or government using any of the methods described above. Cyberwarfare is becoming increasingly common and many governments have prepared themselves to defend against these attacks.

Cloud computing security risks

The recent trend in cloud computing brings additional security risks. Cloud computing involves the use of internet-based data storage and computing resources. Rather than using computer resources located within an organisation, the organisation accesses shared resources which are owned and run by a third-party data centre. This enables organisations to react faster and be more flexible, with the ability to fairly rapidly increase their computing resources when demand is high and also reduce them when demand drops. This is something that cannot easily be achieved with in-house computing resources, which usually involve investing in hardware. Organisations may also set up their own cloud systems to provide more flexible access to in house applications and data.

Cloud computing has its own security issues. Some argue that using cloud computing may improve the security of data because a large third-party data centre is able to devote greater resources to security than an individual company can. However, because these large data centres hold large amounts of data from many different clients on their systems, they become attractive targets for cybercriminals.

Organisations that store their data on the cloud no longer have physical access to the servers and disc on which their sensitive data is stored. This data is instead exposed to internal attacks from within the third-party company that hosts the data. The hosting company must take extra precautions to protect against internal attacks. The data held for one organisation by a cloud computing hosting company may also share the servers and disc drives with data held for other organisations, so the hosting company must ensure that each client's data is properly isolated from other clients'.

The server computers in data centres are often virtualised (known as **server virtualisation**), with one physical computer running a number of different virtual machines for clients. The virtualisation software adds an additional layer of complexity to the system and creates the possibility that vulnerabilities may exist in the virtualisation software.

Key term

Server virtualisation – it is very common for server computers to use virtualisation software that allows one large and powerful server computer to operate as if it were several smaller systems carrying out specific functions. In cloud computing, this allows a data centre to provide a customer with what appears to be their own dedicated server computer. In reality, it is just one of many different virtualised servers running on a single large physical server.

Research

Carry out research to find out what the most common threats are to computer systems. There are a number of places you can go to research this question. The Open Web Application Security Project (OWASP) publishes a list of the 'top 10' web security risks from time to time. Companies that produce anti-malware software, such as Norton™, McAfee and Kaspersky™, also publish lists of the most destructive malware

Information security

Much of our personal and business information is now held on computers, so keeping information secure is an extremely important concept. Information needs to be available to people who should have access to it, but protected from those who should not. There are three main principles that apply to information security: confidentiality, integrity and availability.

Confidentiality

Confidentiality is the principle that information should not be disclosed or accessible to anyone who is not authorised to know it. Usually, confidentiality of data on computers is achieved using encryption, which makes it unreadable to anyone who is not authorised to access it. Operating systems have access controls that allow system users to be identified (by their username), authenticated (by their password) and authorised (by the file access permissions granted by the system administrator) so that information held on the system is only accessible to those who should be able to see it.

Integrity

Integrity of data on computers means that the information is accurate and complete, and also that it is not possible for unauthorised changes to be made to the information. Hashing provides a way to check the integrity of digital files. A 'hash' is simply a number produced by applying a hashing algorithm to the file.

Link

Hashing is explained in more detail in the section 'Cryptography methods'.

Digital signatures and certificates also provide integrity, by providing assurance that an email is from the person from whom it appears to be. In database systems the normalisation process used at the design stage is used to help ensure data is not duplicated which can impact on integrity. Bear in mind also that out of date or inaccurate information can impact on the integrity of a database.

Link

Digital signatures and certificates are explained in more detail in the section 'Digital certificates', in 'Applications of cryptography'.

Digital signatures can also provide **non-repudiation**, as do operating system features such as audit logs, which show which particular user accessed a file and when.

Key term

Non-repudiation – this is the assurance that something cannot be denied (repudiated). Typically, this involves using a digital signature to prove that a contract or email was agreed to or sent by someone and they cannot deny it.

Availability

For information to be useful it must be available to those people and systems who need to have access to it. Therefore system managers must take steps to ensure that information systems provide the required level of availability to users. An organisation must decide what level of availability it needs for its computer systems. For some companies, Monday to Friday 9 am to 6 pm is sufficient; for others there must be 24 hour, 365 day availability of systems.

An organisation must also decide how long it can survive without its systems in the case of hardware failure or a disaster such as a fire or flood. In order to increase the availability of a system, an organisation has to remove any single point of failure from the system. They can achieve this through a number of methods, including the following.

- **Disc redundancy** – using multiple discs systems, such as RAID, to allow the system to continue uninterrupted if one disc fails.

Research

RAID disc systems are commonly used on server systems and often include 'hot swap' disc drives which can be removed while the system is running. Research RAID systems and associated hardware features, and consider what security implications they may have and how they can be mitigated.

- Backup – to replace any data lost due, for example, to corruption or human error.
- Server redundancy – duplicated hardware in case of a serious hardware failure.
- Disaster recovery – putting plans in place to run the whole system from a different location in the case of a physical disaster such as fire or flood.

Link

System availability is discussed in more detail in the section 'Physical security'.

Access

Companies need to haveconsidered what level of access can be given to specific users or groups of users, particularly with regard to systems that contain a lot of sensitive data. The ideal situation would be that each user only has access to the data that they actually require for doing their job. This is the principle of providing minimal access to information or lowest required access permission, so as to maximise protection of data.

Most systems allow various levels of access, which are usually defined as:

- full access – ability to read, write and delete files
- write access – ability to read and write files but not delete them
- read access – ability only to read (view) files.

In a large organisation with many employees, it may not be possible to define exactly which files and what level of access each individual user should have in order merely to do their job, so user access rights to files are normally allocated to groups of users, perhaps based on the department they work for or their seniority within the company.

As well as giving the correct level of access to the users who should be able to access the data, the system should protect the data from unauthorised access or modification of information and from theft, because personal, financial and commercially sensitive information (or intellectual property) may be valuable to others. The system should also protect data from deliberate or accidental loss, though the use of backups.

Legal requirements

Legislation regarding security risks can broadly be divided into those laws which organisations must comply with and those under which people who attack systems can be prosecuted.

Must comply with

In the UK, organisations must comply with the following legislation to stay within the law.

Data Protection Act (1998)

This legislation defines the requirements for organisations which legitimately store personal information about living individuals. Any organisation that stores data about living individuals must make sure that the data is:

- used fairly and lawfully
- used for limited, specifically stated purposes
- used in a way that is adequate, relevant and not excessive
- accurate
- kept for no longer than is absolutely necessary
- handled according to people's data protection rights
- kept safe and secure
- not transferred outside the European Economic Area without adequate protection.

Link

For more about the Data Protection Act (1998), visit the Information Commissioner's website: https://ico.org.uk/

Copyright, Designs and Patents Act (1988)

Copyright is the law that protects the intellectual property of writers, musicians and other artists. People who illegally copy music, films, books or computer games are breaking this law. Various methods can be used to help protect intellectual property, such as encryption.

Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)

Employers are, under these regulations, allowed to intercept communications sent over their own networks. So, for example, a company could lawfully intercept their own employee's emails and record their telephone conversations (if they use the company network). Employees must be aware that their communications may be intercepted, and this would usually be included in their contracts of employment.

Criminal acts

The following legislation outlines criminal acts in relation to computers and data.

Computer Misuse Act (1990)

This is the main legislation that applies to computer hacking and the creation and dissemination of malware. The Act, which was passed in 1990, makes it an offence to:

- make unauthorised access to computer data
- make unauthorised access to a computer system with the intention of committing a crime
- make unauthorised modifications to computer data
- create, supply or obtain anything which can be used to do any of the above.

Fraud Act (2006)

This is a wide-ranging law which covers a variety of fraudulent activities. Fraud is basically a deliberate attempt to deceive someone and obtain some kind of advantage by doing so (often, but not always, monetary). Phishing scams, for example are a form of fraud, since the person sending the emails and setting up the fake bank website is falsely claiming to represent a bank. This is sometimes

called 'fraud by false representation'. However, bear in mind that cybercriminals may not be based in the UK or EU and, therefore, obtaining a conviction under this law for phishing could be very difficult indeed.

Legal liability and contractual obligations

Companies that supply a product or service to customers have contractual obligations to them and can also be legally liable. These companies must set out contracts for their services which state the details of the services they will supply and the associated conditions of those services. For example, a company that provides IT support will have a contract with the business to whom it supplies the support. In an IT support contract, there are likely to be conditions, such as keeping the personal data of customers safe. If a security breach led to the personal data of the IT support company's customers being stolen, then the IT support company would be in breach of their contract and could be sued. If a company suffers a security breach that causes financial or other losses to other people, then they may be legally liable and may have to pay damages.

Impact of security breaches

Security breaches can have a serious impact on organisations or individuals. A serious security breach is likely to result in one or more of the following consequences.

Operational impact on an organisation of the loss of data or service

A computer system on which an organisation relies to run some aspect of its business may be subject to a security breach that prevents the system providing the service it is designed to provide (such as during a DoS attack). This can have a serious impact on the organisation's ability to do business. Attacks that damage, destroy or restrict access to data held on an organisation's computer system would have a similar effect. Many companies rely very heavily on computer systems to run their businesses and so these kinds of security breach can have a devastating impact on them.

Financial impact of loss of service, such as an e-commerce website

Many organisations rely on computer systems to directly sell their products or services, such as those which run e-commerce websites. If an e-commerce website is off-line due to a security breach, a business will lose revenue because customers cannot purchase at this time and they could lose very large sums of money for every hour that the site is off-line.

Damage to reputation

For large and well-known organisations, the impact of a major security breach can spread beyond the financial effects. Many organisations, especially those that do business on the internet, have a reputation to protect. People who buy their products or services online need to feel that the financial and personal information they give to the business is secure. If it becomes public knowledge that a business has suffered a security breach, then this could damage their reputation and lose them customers because they are no longer trusted.

Legal consequences of data privacy breaches

As mentioned earlier, organisations that store personal data on their computer systems have a legal obligation to keep that data secure. If personal data is stolen during a cyberattack and the company can be shown to have been negligent in terms of keeping the personal data secure, then the company could face prosecution under the Data Protection Act and receive a large fine.

Forensic research requirements to identify data lost, stolen or copied

Research

Computer forensics is a complex and fascinating topic. Research the tools and techniques which are use.

If an organisation detects that a serious IT security breach has occurred, such as its network being hacked and data stolen, then the time, effort and expense of investigating the incident can be considerable and may seriously disrupt the day-to-day running of the organisation. In order to preserve forensic evidence of the attack, it is likely that system would need to be shut down and the hard discs may need to be removed for detailed forensic investigation. This would require the installation of new discs and the restoration of the organisation's data from backup copies. The analysis of the discs and other evidence of a cyberattack is a complex and highly skilled process, and it is likely that the organisation would need to contract in cybersecurity experts to do the work, which would, of course, add to the cost of the security breach.

PAUSE POINT

Carry out research into recent IT security issues at large companies. What actually happened? Which type of cyberattack described in this section was used? What was the impact on the company? Did they lose money or face legal consequences?

Hint

News websites, such as the BBC news website or newspaper websites such as the Guardian or Telegraph Technology sections (www. telegraph.co.uk/technology or www.theguardian.com/uk/technology), are excellent places to start your research.

Extend

Consider how the company could have avoided the security breach. Were there protection methods they could have used? If there were, why did they not use them? How can organisations protect themselves in the future from this kind of security issue?

B Investigate cryptographic techniques and processes used to protect data

Cryptography is the science of hiding data in such a way that, although others may be able to see the data, only the intended recipient can understand it. Cryptography pre-dates the computing era and examples of its use to protect secrets can be found going back thousands of years. Cryptanalysis was the main use of computers when they were first created, and the need to crack enemy **cyphers** during World War II spurred the development of computers. Colossus, the world's first fully programmable digital computer, was built at Bletchley Park in the UK during World War II to crack coded German messages.

Key term

Cypher – algorithm used to encrypt and decrypt data (alternative spelling is cipher).

Cryptographic principles

In this section, you will look at the principles and uses of encryption. There are two main principles of modern computer-based encryption: integrity and confidentiality.

Integrity

The principle of **integrity** provides confidence that data has not been modified in any way. Integrity of data is achieved by creating a value called a 'hash' (sometimes called

a 'checksum'). The hash is sent with the data. When the data is received, the hash is recalculated and the result is compared with the hash that was sent with the original file. If both of the hashes are the same, then you know that the data has not been tampered with.

Key term

Integrity – principle of being honest and having strong moral standards.

Link

Hash functions are described in more detail in the section 'Cryptography methods'.

Confidentiality

Data kept **confidentially** can only be viewed by authorised users, that is, it is kept secret from anyone who is not meant to know it. Encryption is used to scramble data, making it unreadable without a key.

Key term

Confidentiality – principle of keeping something a secret. If you are told some information in confidence, then you must keep it a secret.

Uses of encryption

There are various of types of encryption that are used for a wide variety of different applications, some of which are described in the following sections.

Digital rights management

The ease with which digital media can be copied has given the music, video and games industries a problem. They need to find a way to allow legitimate purchasers of copyright material to have access to it while preventing it from being copied and sold on illegally. The way in which they try to do this is through digital rights management (DRM). There are many different DRM systems in use, not all of which use encryption. An encryption-based DRM system will typically encrypt the media and then the decryption key is provided only to authorised users of the media. An example of this kind of DRM is the CSS (content scrambling system) used on DVD video discs. This system is designed to ensure that only licensed DVD players can play that commercial DVD video.

Password storing and salts

Passwords are widely used to authenticate users on a wide variety of systems. In order to authenticate a user, the user's passwords must be stored on the system, but storing them as plain text would be an obvious security risk, so passwords are therefore encrypted. However, if an attacker has access to the password file and knows the cryptographic function that is used to produce the encrypted passwords, then they could make a list of many commonly used words and encrypt them using the same function and see if that matches any of the encrypted passwords in the password file. The attacker will then know at least some of the passwords because they have matched them. (There are a lot of encrypted password files that use lists of common words available on the internet, which attackers can get access to). This kind of cyberattack is sometimes called a dictionary attack.

'Salts' are added to the encrypted passwords to make them more difficult to crack. A salt is simply a random value added to an encrypted password so that it will not match the encrypted passwords that an attacker generates with their dictionary attack.

Obfuscation and steganography

Obfuscation and **steganography** are not strictly cryptographic methods but they do rely on hiding secret data in amongst other non-secret data (in a 'carrier' file). For example, files containing secret information can be hidden inside image files. Image files are well suited for steganography because they are large and so hiding a relatively small amount of text inside them by altering a few of the pixels within the image would not be noticeable.

The benefit of steganography compared with cryptographic methods is that this method does not attract attention because the image appears to be innocuous. The main application of steganography is the requirement to send information over the internet to individuals without raising the suspicions of others. Programs use steganography to hide secret data in carrier files that are freely available on the internet.

Key terms

Obfuscation – means to make something more difficult to understand, that is, to make it obscure, unclear or unintelligible.

Steganography – is the practice of concealing information within other non-secret data.

Secure transactions

The basis of e-commerce is the ability to send sensitive financial information securely over the internet. When

making a credit card purchase from an e-commerce website, it is important that the transaction details are secure, otherwise a third party may be able to intercept them. Secure transactions are achieved by encrypting the data sent from the user's internet browser to the web server that hosts the e-commerce site.

Link

How secure transactions are achieved is explained in more detail in the section 'Public-key encryption', in 'Cryptography methods'.

Two-factor authentication

In a typical home computer system, authentication just involves a single factor: the user password. Two-factor authentication involves both something that the user knows (such as a password or a PIN number) and also something that the user has in their possession (such as a USB memory stick which contains a security token or a smart card). Security tokens come in a variety of types including those that display a value that the user must enter into the computer system to authenticate themselves and those that are plugged into a USB port. Some banks provide customers with card readers that are used in conjunction with their debit card to provide a security code that can be used to access online banking facilities.

File, folder and disc encryption

Data held on a computer is protected by the operating system, which only allows authorised users to access it. However, if the hard disc is removed from the computer and connected to a different computer, then the operating system protection can be circumvented and the data can be accessed by others. This is a particular issue with laptop computers which can more easily be stolen or lost. One way to help protect data is to encrypt it so that it is only accessible to whoever has the encryption key. Microsoft® Windows® operating system has an encryption system for individual files and folders called the encrypted file system (EFS). Files or whole folders can be encrypted with a key associated with the user account of the user who encrypted them. For that user, the files are transparently encrypted and decrypted. For anyone else, the files are inaccessible.

Microsoft® also provides a system called BitLocker with some versions of Windows® operating system. This is a full disc encryption system that encrypts the whole hard disc (in practice, this means that it encrypts the whole laptop). The system works in conjunction with the trusted platform module (TPM) hardware included in many motherboards, which stores a cryptographic key. This key is used to encrypt the hard disc and can also be combined with a password which the user must enter when the device boots up. If the hard disc is removed from that computer and connected to another, the TPM key will be different and so the files cannot be decrypted.

Encryption of communication data

Mobile telephone conversations are transmitted using encrypted digital data. GSM (global system for mobile communication) mobile phone conversations are encrypted using the A5/1 stream cypher. The A5/1 stream cypher is no longer secure and it has been shown that it is possible to crack the encryption and decrypt mobile phone data, allowing conversations to be eavesdropped on in real time. Information leaked by Edward Snowden showed that the USE National Security Agency (NSA) can decrypt A5/1. Mobile phone voice messages have also been widely 'hacked' by unscrupulous journalists, although these are not encrypted and social engineering methods were used to access this data.

Research

The use of the A5/1 cypher to encrypt mobile phone communications is interesting to look into. Why, for example, was a relatively short key length of 54 bits used rather than a more secure longer key? Are there other methods that can be used to protect mobile phone communications?

Legal and ethical issues

Encryption can be used for a range of purposes, some of which raise legal and ethical issues. For example, those intent on breaking the law, such as criminals and terrorists, can use encryption to hide their communications from law enforcement agencies. Before computer data encryption became widely used, encryption technologies were closely guarded secrets and were not available for the general public to use. The widespread availability of encryption techniques to the general public means that anyone can now hide data from prying eyes, both for legitimate and for unlawful/unethical purposes. Some argue that individuals should be allowed to keep their data secure, while others argue that technology companies should build a 'backdoor' into their products to allow law enforcement and other government agencies to access it if needed. The risk with doing this is that criminals and terrorists may then also be able to access these 'backdoors'.

Case study

The San Bernardino shooting

In December 2015, 14 people were killed in a terrorist attack in San Bernardino, California, US. An Apple iPhone® 5C belonging to one of the terrorists was recovered, and the FBI wanted to unlock the phone to see if other people had been involved in the attack. (The two terrorists who carried out the attack were shot dead by police.)

However, back in 2014, it had been revealed that the FBI and the British GCHQ had ways of accessing all information on Apple® and other smartphones. In response to this, Apple® had improved its encryption in iOS® version 8, and this prevented the FBI gaining access to the terrorist's phone. The FBI therefore asked Apple® to unlock the phone but Apple® refused, stating that it was company policy not to undermine the security features of its products as to do so would not be in the interests of its customers. The FBI therefore issued a court order compelling Apple® to unlock the phone. However, before the case came to court, the FBI dropped the case because they stated that a third party (said to be the Israeli company Cellebrite) had enabled them to access all the data on the phone.

The case raised many technical and ethical questions about whether technology companies should build a 'backdoor' into their encryption products for the purpose of allowing government agencies to access them in such cases, or whether it is in their customers' interests to protect their encryption methods at all costs.

Think about it

1. Do you think it was right for the FBI to want access to the information on the terrorist's phone?
2. Why would Apple® want to protect its encryption methods and do you think they were right to withhold the information?
3. Should the government have access to our data? After all, if you are doing nothing illegal, what is there to hide?

Computational hardness assumption

Most modern cryptographic methods are not impossible to crack. Instead, they rely on being very hard to crack, given the computing power available. In other words, they rely on the fact that it would take a computer a very long time indeed to crack the encryption and therefore no one would bother trying to crack it. However, the power of computers continues to increase. In theory, a point may be reached in the future when current encryption methods can be overcome in a relatively short time. At such a time, current encryption methods would stop being useful because it would become very easy to crack them.

Cryptographic methods

There are a number of different methods and standards that can be used to encrypt data, which reflect the various different applications for which encryption is used. This section looks at the most important cryptography methods.

Shift cyphers

The use of a shift cypher is one of the oldest and simplest methods of encryption, pre-dating computers. It simply involves substituting one letter of the alphabet for another. Table 7.1 shows an example of a shift cypher where the letters are shifted two to the right in the alphabet.

Letter of the alphabet	A	B	C	D	E	F	G	H	I	J	K	L
Substituted letter	C	D	E	F	G	H	I	J	K	L	M	N

Table 7.1: Shift cypher – only the first 12 letters are shown, but you can easily write out the complete table yourself to follow the example and encrypt your own messages.

So in the example in Figure 7.1, the words

IT SECURITY

become KV UGEWTKVA when encoded.

While shift cyphers, as a method of cryptography, are easy to understand, they are also very easy to crack and provide almost no security.

One-time pad

While a shift cypher offers very little security, a one-time pad cannot be cracked if used correctly. Use of a one-time pad involves each character of the text to be encrypted being combined with a different random number. The list of random numbers used to encrypt the message is called a 'pad', and each pad is only used once. The pad must be as long as the message to be encrypted. The one-time pad method works as follows.

1. The two people who wish to transfer a message must both have a copy of the same pad.
2. The sender combines each character of the message to be sent with the corresponding character on the pad (that is, the first character of the message is combined with the first character, the second character with the second character on the pad and so on).

3 Once the message is encrypted, the sender destroys their copy of that pad.
4 The encrypted message is sent to the recipient.
5 The recipient decodes the message using their copy of the one-time pad and then they also destroy the pad.

Table 7.2 shows how the character in the one-time pad is used as the shift that is applied to the corresponding letter of the message. To determine the shift to be applied, A = 1, B= 2, C = 3 and so on. This is similar to the shift cypher but every letter is shifted by a different amount.

Table 7.2: One-time pad example

One-time pad	E	Y	B	R	G	K	M	F	E	L
The shift	5	25	2	18	7	11	13	6	5	12
Message	I	T	S	E	C	U	R	I	T	Y
Encrypted message	N	S	U	W	J	F	E	O	Y	K

Link

An internet search for 'one-time pad' will provide a lot more information on this topic.

One-time pads are not used widely because of the problem of transmitting the pad to the intended recipient. For example, if you sent the encrypted message over the internet to the recipient and then sent the pad, anyone who intercepted both the message and the pad could decrypt the message.

So the pad must be passed to the recipient securely, not using the same method as the message, which makes it impractical if you want the message to stay secret. If you have the pad, then the message is easy to decrypt – without the pad it is impossible to decrypt.

Hash functions

A cryptographic hash function takes an input of variable length and returns a fixed-length value. The value produced by a hash function is often called the 'digest' or 'hash value', and it acts as a kind of 'signature' or 'fingerprint' for the input file. The main purpose of hash functions is to ensure that a message has not been altered in any way during transmission (i.e. that its integrity has been maintained).

A good hash function has the following characteristics:

- it is relatively easy and fast to compute
- it is very difficult to reverse (to work out the message given the hash value)
- it is very unlikely that two messages will generate the same hash value.

There is a range of different hash functions that have been widely used, two of which are detailed here.

- **Message digest (MD):** There are various versions of this hash function. MD5, for example, was often used to check the integrity of downloaded files. However, in 2004, it was found that MD5 can be cracked quite easily, so it is no longer recommended for use.
- **Secure hash function (SHA):** Again, there are a variety of versions. SHA-1 was widely used in a number of applications including secure socket layer (SSL) communications, which are the basis of all secure internet transactions. Weaknesses were discovered in SHA-1 in 2005. SHA-2 and SHA-3 are the current versions in use by SSL and other applications.

Worked Example: Create your own hash

It is quite easy to create a hash for any file using free software that is available on the internet. Google 'create a hash or create a SHA1 hash' to find websites where you can do this.

You could use a product like this if, for example, you ran a small software house that provides updates and patches for products for your customers to download and install. By creating hashes for each of your downloadable updates and sending them to your customers, you can provide a means for them to check that the downloads have not be compromised in any way and only contain the data you intended (i.e. that their integrity has been maintained).

Block and stream cyphers

Block and stream cyphers are different techniques for encrypting data.

A block cypher will take the data that is to be encrypted and break it up into blocks of a fixed number of bits (for example, 64 or 128 bits are commonly used), while a stream cypher will encrypt each digit (e.g. a bit) individually. Stream cyphers are better suited to applications where the size of the data is unknown or it is sent in a continuous stream such as when streaming audio or video. Block cyphers are better suited to situations in which the size of the data is known, such as when encrypting a database file.

Encryption algorithms

The basic idea behind encrypting data is that the data to be encrypted is taken with a key and passed through a process that makes the original data unreadable. At the receiving end, the key can be used to decrypt the data making it readable again. Where the same key is

used to both encrypt and decrypt the data, this is known as **symmetric key encryption**. **Asymmetric key encryption** uses two matched pairs of keys.

Key term

Symmetric and asymmetric key encryption – in symmetric key encryption, the same key is used to both encrypt and decrypt the data, whereas, in asymmetric encryption, two keys are used, one to encrypt the data and another, different but mathematically paired, key is used to decrypt it.

There are many different encryption algorithms, also known as encryption standards. Some of the best known are detailed here.

DES

DES (data encryption standard) was developed in the 1970s by IBM and was once the primary symmetric key encryption technology. It is a block cypher system with a key length of 56 bits. DES is now considered insecure as its short key length allows it to be cracked quite easily. This example highlights how, in the 1970s, there was insufficient computing power available to crack DES in a reasonable amount of time, but, as computing power has increased, it has become possible to crack the encryption. DES is believed to have been cracked for the first time in 1999, in 22 hours 15 mins.

3DES

3DES (triple DES) was developed using the same algorithm as DES but using a 'key bundle' of three keys for each of the 56 bits. Currently, 3DES is secure and has not yet been cracked. 3DES is used to secure data used to make financial transactions by credit/debit card.

RSA

RSA is an asymmetric public-key system that is widely used for secure internet transactions. The system is named after its inventors Ron Rivest, Adi Sahmir and Leonard Adleman of the Massachusetts Institute of Technology (MIT) in the US.

Link

The RSA system is described in detail in the section 'Keys and digital certificates'.

AES

AES (advanced encryption standard) is a strong block cypher that uses 128 bit blocks and is often used in symmetric key encryption as it is very secure. It was adopted by the National Institute of Standards and Technology (NIST) in the US after a long evaluation of various different encryption algorithms. AES can use encryption keys of 128, 192 or 256 bits, and is sometimes called 'AES-128', 'AES-192' or 'AES-256' depending on the key size used. The more bits in the key, the harder it is to crack it. AES is popular, not just because it is strong, but also because it is efficient and requires less computational power to encrypt/decrypt files than many other algorithms.

Mathematical principles

The mathematics behind encryption is very complex. However, there are some basic principles that you can look at.

Cryptographic primitives

Most modern computer-based cryptography is based on a set of algorithms or building blocks which are sometimes called cryptographic primitives.

One-way functions and integer factorisation

The idea behind a one-way function is that it is easy to compute but very hard to reverse. Hash functions are an example of one-way functions. A simple example of a one-way function would be to take two **prime numbers** and multiply them together. This is easily done but, if the number is very large, there is no quick way of decomposing the resulting number back into the original values (there is no easy way of predicting which two prime numbers were multiplied together). This problem is known as integer factorisation and, as yet, no algorithm exists to factorise large (hundreds of bits) numbers quickly.

Key term

Prime number – a number that can be divided by only itself and 1. There are lots of prime numbers such as 3, 5, 7 and 151.

Worked Example: One-way function

Here is a simple example of a one-way function.

1. Take the number 147. Which prime numbers can be multiplied together to make 147?
2. One way to work this out would be to work up through the prime numbers starting at the smallest, which is 2.
3. 2 is the smallest prime number but 147 is not an even number so 2 will not divide into it.
4. The next prime number is 3.
5. 147 ÷ 3 = 49

6 49 cannot be divided by 2, 3 or 5 but it can be divided by 7

7 49 ÷ 7 = 7

8 As 7 is a prime number, you do not need to go any further.

9 So you now have all the prime factors of 147, they are: 3 and 7.

While this might seem quite simple for a small number, for numbers with hundreds of bits it would take months of computational time to find all the factors. As no one wants to spend months working out the factors, using a one-way function for integer factorisation is quite secure.

Link

For more about integer factorisation of prime numbers, see http://www.mathsisfun.com/prime-factorization.html

Pseudorandom functions

Pseudorandom functions are types of programming function that create apparently **random numbers** efficiently. These are required by many cryptographic methods including generating keys to encrypt data and creating cryptographic salts to be added to passwords. To be regarded as a secure pseudorandom number generator, the function needs to produce a stream of bits for which there is no known method of predicting the next bit to be produced with a probability of success that is greater than 50 per cent.

Link

For more about cryptographic salts and their use in storing passwords, look back at the section 'Password storing and salts', in 'Cryptography methods'.

Key term

Random number – a number in a list of numbers that is not related to the previous or to the next number in the list.

Applications of cryptography

There are several types and applications of cryptography, many of which are covered in this section.

Keys and digital certificates

Symmetric key encryption is useful in some software applications but is not an effective security solution when you want to securely send data to another person, as they will need the encryption key to decrypt the data. Sending the key to the person would create an obvious security risk because, if the encrypted data and the key were intercepted by a third party, then they would be able to decrypt the message easily.

To get around this problem, a more complex system has been developed called public-key encryption, which is based around the RSA system.

Public-key encryption works like this.

1 A pair of mathematically related keys are generated – one is the public key and the other is a private key.

2 The public key is available to anyone, but the private key is kept secret.

3 The public key is used to encrypt messages.

4 A message encrypted with the public key can only be decrypted using the private key.

Public-key encryption is complex, so trying to understand it is best done with an example. SSL (secure sockets layer) or the more up to date TLS (transport layer security) are widely used implementations of public-key encryption. Public-key encryption using SSL or TLS is part of the HTTPS protocol, which is used when you access a secure internet website such as a banking site or when you are paying for a purchase on an e-commerce site. SSL and TLS use a **digital certificate** provided by a **certificate authority** to prove that the website you are communicating with is a trusted site.

Key terms

Digital certificate – to run a secure website, the site owner must apply to a certificate authority to obtain a digital certificate. The digital certificate certifies that the website is genuine and owns a particular public key. Without a digital certificate, it might be possible for a bogus website to impersonate a secure site.

Certificate authority – a certificate authority (CA) is an organisation that issues digital certificates. There are many commercial CAs including Comodo®, Symantec and GoDaddy®. There is also a free CA called Let's Encrypt™ which is sponsored by organisations such as Cisco® and Google Chrome™ browser.

The process that takes place when your web browser logs on to a secure site which has a digital certificate is outlined in Figure 7.1.

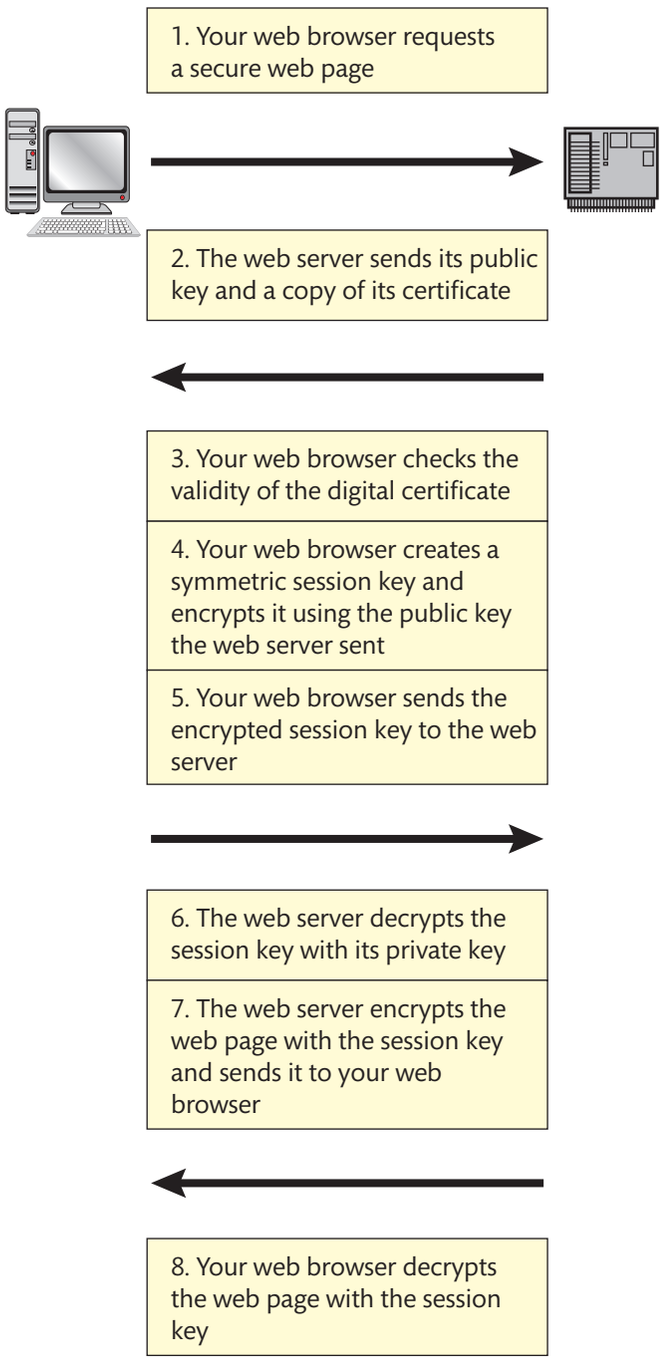


Figure 7.1: Public-key encryption process

As it is not efficient to encrypt large amounts of data using asymmetric key encryption, it is only used to transfer the symmetric session key between the client and the server. This gets over the problem of sending a symmetric key. The rest of the session data is encrypted using the same symmetric key.

Using this method, it is possible to exchange a symmetric key without it being possible for a third party to intercept it. This is known as a 'Diffie–Hellman key exchange', named after the two American cryptologists Martin Hellman and Whitfield Diffie who developed the technique.

Worked Example: Setting up a secure site

Suppose you wanted to set up an online shop and needed to provide secure facilities to enable your customers to pay safely with credit/debit cards. How would you go about doing this?

1. First you would need to create a public and private key pair. There are many programs available that allow you to do this, for example PuTTYgen.
2. Then you would need to create a certificate signing request (CSR) which provides information about the website, you and your public key. Popular web server software such as APACHE® and Microsoft IIS® provide tools to create CSRs.
3. The CSR is sent to a certificate authority.
4. The certificate authority verifies your website's details and then creates a certificate which includes your public key.
5. Your digital certificate is then installed by your web server and, whenever anyone requests a HTTPS session with your web server, it sends the certificate and the public key.

You must keep the private key safe. If the private key is compromised (if an attacker obtains a copy of it) the system is no longer secure and the associated certificate must be revoked and new keys and certificates created.

Certificate authorities such as Verisign, GeoTrust and Thawte have their trusted root certificates included in popular web browsers. This means that any certificates issued by these certificate authorities will be trusted by your browser. You can see the root certificates included with your web browser. The trusted root digital certificates for Internet Explorer are shown in Figure 7.2.

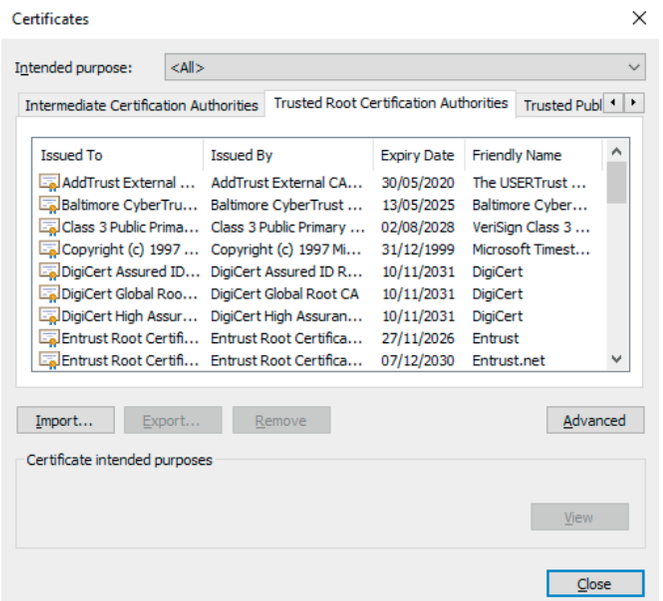


Figure 7.2: Trusted root digital certificates for Internet Explorer

Virtual private networks (VPNs) and generic routing encapsulation (GRE) tunnels

A VPN allows a private network (such as an organisation's LAN) to be extended across a publicly shared network, usually the internet. It allows users to access the organisation's LAN (and therefore applications and shared data) when they are remotely connected. (Essentially, it allows an employee to access their company computer network at home as if they were at the office.)

Naturally, connecting users by a VPN creates security issues since private data is being transmitted over a public network. VPNs usually include an aspect of user authentication to ensure that only authorised users can access the VPN and data is encrypted so that all of its interactions are unreadable. VPNs use what is called a 'tunnelling protocol' which creates a virtual tunnel in which the data travels across the internet. The internet protocol called IPsec is often used for VPNs as it encapsulates and encrypts data packets and also provides facilities for hosts to authenticate each other before starting data transmissions.

Generic routing encapsulation (GRE) is a tunnelling protocol developed by Cisco® Systems for, amongst other things, the implementation of VPNs. GRE works by wrapping an inner data packet in an outer IP packet (rather like taking a letter, placing it in an addressed envelope and then putting that envelope in another addressed envelope). This allows the creation of a VPN over a wide area network (WAN) such as the internet. The routers on the WAN ignore the inner packet and process the packet based on the information in the outer packet. Only when the GRE packet reaches the relative safety of a private LAN is the outer packet stripped off.

Encryption of data on WiFi networks

WiFi networks use radio waves to transmit data, which, because they are broadcast media, can be picked up by anyone in range of the radio signals. It is therefore essential that the data sent over WiFi networks is encrypted. A number of different encryption methods can be used with WiFi networks.

WEP (wired equivalent privacy)

WEP (wired equivalent privacy) was the original encryption method used for WiFi networks. It used a stream cypher with a 64 or 128 bit key, usually entered as 10 or 26 hexadecimal digits. In 2001, WEP was found to be easily cracked and so is no long regarded as secure.

WPA (WiFi protected access)

WPA was developed in response to the weaknesses in WEP and one benefit of it was that it did not require new hardware (routers which had been designed for WEP could use WPA with just a software upgrade). An improved version of WPA called WPA2 was launched in 2006. WPA uses a more advanced form of encryption than WEP called TKIP (temporal key integrity protocol), but it was developed as an interim replacement for WEP after its vulnerabilities had been discovered, and it was not intended as a permanent solution.

WPA2 was developed as a permanent replacement for WEP. WPA2 uses a much stronger form of encryption than WPA called CCMP (cypher block chain messaging authentication code protocol) which is based on the AES encryption standard. In order to keep WPA2 as secure as possible, it is recommended that a key of at least 20 characters, with a mix of upper and lower case characters and numbers, is used.

Personal versus enterprise modes

Most home-based WiFi routers use WPA2 personal mode where access is provided through a **pre-shared key (PSK)**, which is entered into any device that a user wants to access the network. This does not provide any authentication of the users as anyone who has the key can access the network. In most cases, the keys are printed on a label attached to the router.

Alternatively, enterprise mode can be used, which requires authentication of users and so is more secure. To set up enterprise mode, WPA2 requires that WiFi users provide unique credentials to access the network. To implement this, a server is used which holds a database of valid usernames and passwords. To gain access to a WPA2 enterprise WiFi network, a user must enter their valid credentials to be authenticated by the server.

Key term

Pre-shared key (PSK) – a cryptographic term which describes an encryption key that is provided to authorised users to allow them to encrypt and decrypt data.

Research

Bluetooth is widely used for the short range transmission of data between mobile devices. Although Bluetooth data packets are encrypted, there are a number of security issues when using Bluetooth. Find out how the data packets are encrypted and research the security issues involved when using Bluetooth.

Reflect

Assessment practice 7.1 includes a task in which you need to evaluate the security techniques that could be used. In an evaluation, you need to consider both the positive and negative aspects of the topic under consideration and produce high quality, justified recommendations and decisions and reach a considered conclusion. Your evaluations are essential to achieving the highest grade for this unit and to maximise the quality of your work.

Assessment practice 7.1

A.P1 A.P2 A.P3 B.P4 A.M1 B.M2 AB.D1

You have recently started working for a medium-sized company in the IT support department. The directors of the company have become increasingly concerned about IT security threats, so you have been asked to give them a presentation on the topic. They are also interested in how encryption can be used to protect the company data. Your presentation needs to cover the following.

- An explanation of what the different IT security threats are.
- An explanation of the principles of information security and the legal issues related to IT security.
- An explanation of the principles of cryptography and an analysis of how it can be used to protect data and the impact it can have on security.
- An analysis of the impact that IT security threats can have on the company's business, taking into account information security and legal issues.
- An evaluation of the techniques that could be used to protect the company from IT security threats while taking into account the issues of information security and legal requirements.

Plan

- What is the task? What am I being asked to do?
- How confident do I feel in my own abilities to complete this task? Are there any areas I think I may struggle with?

Do

- I know what I am doing and what I want to achieve.
- I can identify when I have gone wrong and adjust my thinking/approach to get myself back on course.

Review

- I can explain what the task was and how I approached the task.
- I can explain how I would approach the hard elements differently next time (i.e. what I would do differently).

C Examine the techniques used to protect an IT system from security threats

As there are so many different security threats to IT systems there needs to be a large range of precautions put in place to defend these systems. This section will examine the techniques used to protect IT systems from security threats.

Physical security

This section will look at the physical security of computing systems, including building security, backing up data and IT disaster recovery plans.

Building and computer/network room security

Computer systems, especially servers, need to be protected from physical access because theft of such valuable equipment, especially hard drives, is a serious security risk.

Tip

Laptop computers and other digital devices can be secured to desks by cable locks to help deter casual theft.

Servers, routers and switches (network equipment) should be kept in secure locations with carefully controlled access. Ideally, access should controlled by proximity key-card entry, whereby the door lock will only open when someone with the right kind of key-card approaches the door. These types of electric door lock can be connected to a system that maintains records of who entered the computer room and when. This data can prove useful if an investigation is needed into when a security breach took place. (Although these electric door locks can tell you which key-card was used, they cannot unfortunately ensure that the person using the key-card was actually the person authorised to have that key-card. The key-card could be stolen.) Thought should be given to the location of a server room within a building. Ideally it should not be on the ground floor or have windows or doors which are accessible from outside the building.

In a large building, as well as the main server room it is common for each floor to have a network room where routers, switches and other network equipment is located. These rooms should be kept locked and only authorised personnel should have access (they could use key-card entry). This level of security can help to prevent the installation of illicit network monitoring equipment.

If a very high level of security is needed, **biometrics** can be used. As mentioned above, one problem with traditional key-cards is that they can be lost or stolen themselves. Biometric authentication gets around this problem because it uses data about the person themselves such as their voice pattern or fingerprints.

Key term

Biometrics – the use of biological data for identification, for example voice control, facial recognition, fingerprints or iris scans. Biometrics uses features of a person that are unique to the individual. These bits of personal information are virtually impossible to forge. Biometrics also have an advantage over other identification methods because the individual does not have to keep anything (such as an ID card) or remember anything (such as a password). DNA identification technology is in its infancy but the idea of using a person's DNA to uniquely identify them has potential for future use in the IT security industry.

One problem that can occur with all of these door lock access systems is tailgating. This is when one person (who is not authorised to enter an area) closely follows another person who is authorised. Out of politeness, the first employee will almost always allow the unauthorised tailgater to follow them through the door. Tailgating can be prevented by installing turnstiles which only allow one person to pass at a time.

Many organisations are making increased use of electric surveillance. Closed circuit television (CCTV) is commonly used to monitor the outside of a building and also, in some cases, high-risk areas inside a building, such as the entrance to a server room. CCTV provides a helpful visual deterrent as the images can be recorded and provide useful evidence for investigations which could lead to prosecutions.

Discussion

CCTV is widely used in public places, and you may well have CCTV installed in parts of your school or college. With a peer or in a small group, discuss these questions. Do you think that this is an invasion of your privacy? Is there too much CCTV? How are the images recorded by CCTV systems used? Is there a possibility that these images could be abused?

Backing up data

As it is not possible to guarantee that the security of a system can always be maintained, it is vital that regular **backups** are made. In a situation where a malware infection has deleted or damaged data in an IT system, it may be necessary to recover the system by using data that was backed up prior to the infection. Since some time may pass between the security breach (when the system is compromised) and its discovery, it is necessary to keep previous backups for several weeks. When deciding upon a backup regime for an organisation's computer systems there a number of factors that need to be considered.

Key term

Backup – a copy of data files that is kept in case the original files are lost or damaged.

How often should the backup be performed?

Deciding how often a backup should be performed can be a difficult choice for an organisation. It is common to use the concept of a recovery point objective (RPO) to define the maximum amount of time a business can afford to lose data from an IT system. Many organisations with non-critical systems use a daily backup, but this can only provide RPO in the region of 24 hours. If an organisation requires an RPO shorter than this, then they may need to consider using online backup methods by which data is constantly backed up to a remote website via a network connection.

What media should be used for the backup?

Traditionally, magnetic tape has been used for backup and it still provides a low-cost solution which, due to the sequential nature of tape, can write data to the tape very

quickly. Alternatives include backup to hard disc or optical media such as DVD-ROMs. The choice may be related not just to cost but also to the amount of data that needs to be backed up. Optical media, in particular, are limited to relatively small sizes as the maximum capacity of, for example, a Blu-ray disc is 128GB.

Selection of data for backup and storage of backup media

There are a number of different options for selecting the data to be backed up. In many cases, it is not practical (due to the large amount of data involved) or necessary to complete a full system or system image backup regularly. It may not be necessary to back up all the data because much of it may be static, that is, it does not change very often.

An incremental backup is a method whereby a full backup of all the required data is done first (for example over the weekend) and then a daily backup is done each day of the week which backs up only those files that have changed that day. This means that each backup contains less data and can be done more quickly. The disadvantage of this system is that, assuming you do a full backup only every weekend and incremental backups each weekday, if there is a hard disc failure on a Thursday, then, to restore all the data, you need to restore the weekend's full backup and then all the incremental backups from Monday through to Wednesday.

An alternative to an incremental backup is a differential backup. With this method a full backup is done at the start and then each subsequent backup backs up any changes since the full backup. This could again be implemented with a full backup at the weekend and then daily differential backups. Each daily backup would require progressively more time and storage since it backs up all changes since the weekend's full backup, not just since the previous day (as with the incremental backup). The benefit of this method comes if you need to restore the backups. With differential backups, if a failure occurred on a Thursday all you would need to do is restore the weekend's full backup and Wednesday's differential backup.

Tip

Whichever method of selecting data for backup is used, the backup media must be stored offsite to provide protection against disasters such as fire or flood.

Tables 7.3 and 7.4 show how incremental and differential backups work.

Table 7.3: Incremental backup

Weekend	Monday	Tuesday	Wednesday	Thursday	Friday
Backup everything					
	Backup changes since yesterday				
		Backup changes since yesterday			
			Backup changes since yesterday		
				Backup changes since yesterday	
					Backup changes since yesterday

Table 7.4: Differential backup

Weekend	Monday	Tuesday	Wednesday	Thursday	Friday
Backup everything					
	Backup changes since full backup				
		Backup changes since full backup			
			Backup changes since full backup		
				Backup changes since full backup	
					Backup changes since full backup

Tip

Never keep your school/college assignment work in just one place. Make backups at regular intervals (at least weekly – more often if you have done a lot of work on them).

IT disaster recovery plans

Many organisations rely on IT systems to run their businesses, so they need to consider how they would continue to operate if the systems were destroyed or rendered unusable by fire, flood, terrorist action or other disaster. In these situations, data backups alone are not sufficient because, if there is no IT system to run the applications on, the data backups are of little use. Planning to deal with such eventualities must be done prior to the event happening and there are a number of approaches that can be taken to disaster recovery.

When looking at backups, you were introduced to the concept of RPO, which is related to the amount of data that a business can afford to lose. When considering disaster recovery, the concept of recovery time objective (RTO) is also important. RTO is the target time in which a business wants to recover its systems following a disaster such as fire or flood. For example, an organisation that sells its products through a website might generate £10,000 in revenue every hour, so a 12 hour outage would cost the company £120,000. Therefore investing significant sums of money in preparing for a disaster would be considered money well spent. Without pre-planning, the recreation of the IT systems following a disaster could take weeks or even months. The shorter the desired RTO, the more investment an organisation needs to make to prepare for a potential disaster. There are a number of approaches that can be taken to disaster recovery.

Hot site

A hot site is where the company maintains a complete working duplicate of all its server systems at a geographically separate site to its main computer operations. This includes all computer and networking equipment and the internet connections required to run the systems. In large organisations which require very short RTO (banks, for example), the hot site will often be a company location where some non-critical computing functions are carried out but which has the capability to take over from the main site at very short notice. Obviously, a hot site is expensive to set up and maintain as it more or less doubles the cost of running the IT systems.

Cold site

A cold site is essentially just a building with suitable power and connectivity. In the event of a disaster at the main site, the company would need to purchase servers and other equipment and set the systems up using backups for system configuration and application data. A cold site has a much longer RTO than a hot site – probably weeks unless the systems are very straightforward – but it is relatively cheap and the organisation can rent the cold site from a company that provides this service. Cold sites can be shared by many different organisations.

Warm site

Often a hot site is too expensive for many organisations to run and a cold site takes too long to set up. A warm site provides a compromise, by having hardware in place but not fully configured and running. As with a cold site, there are companies that specialise in providing ready-to-use warm sites. Organisations that use these services can do a 'test run' by bringing their backup tapes and trying out a set-up of the system so that they can have all the issues ironed out before disaster strikes. Of course, since configurations and software are likely to change, the company would probably need to do occasional test runs at the warm site to check that everything still works.

Policies and procedures.

Organisational policies and procedures do not provide any direct protection from security threats. Instead, they make employees aware of the risks and define the sorts of unsafe practices that they should avoid.

Organisational policies and their application

Organisational policies on acceptable IT use should include the following:

- Internet usage guidelines: These guidelines should cover ways to avoid inappropriate websites that might harbour malware and to avoid security breaches when downloading files.
- Email usage policies: These should give guidance on treating emails from unknown sources with care, including not opening attachments or following web links.
- Security and password procedures: These procedures should outline how to keep passwords secure, for example by not writing them down or sharing them with others.
- Staff responsibilities: These responsibilities might include things like locking desk drawers and filing cabinets, locking or logging off unattended computers, wearing ID badges, challenging strangers, not giving out information over the phone and other general security procedures designed to protect against social

engineering threats. It is likely that organisations will also have a set of rules relating to BYOD, in terms of what staff are and are not allowed to do with their own devices on work premises and how they are allowed to connect their devices to the organisation's systems.

- Disciplinary procedures: Staff should be made aware that deliberately breaking rules in any of the organisation's IT usage policies will have disciplinary consequences, which should be described in the staff disciplinary procedures document.

Just having a policy written down is not by itself any use, so staff must be made aware of the policies and be trained in safe IT procedures. As new IT threats appear all the time, staff should be regularly updated to raise their awareness of new threats and how to avoid them.

Security audits

Having a set of IT usage policies and procedures is all very well, but by themselves they do nothing. An organisation needs to check that the policies are being complied with and that the procedures are being followed to ensure that security threats are avoided or identified quickly. Therefore organisations need to carry out regular audits of their security policies and check that their employees are complying with them.

Security baselines

Security baselines are often used in organisations to define a secure starting point for a system or application. The organisation's IT security policy may, for example, define requirements such as the installation of anti-malware software and firewalls and the updating of settings. Following the written policy, system administrators can then create a baseline system from which an image can be created and deployed onto desktop computers. The baseline may cover a range of issues including the following.

- Ensuring that default 'factory settings' and 'reset' options are removed from hardware and software configurations: For example, some network devices have a default administrator password that is quoted in documentation and which is freely available. These 'factory settings' should be removed and replaced with secure, unique passwords.
- Any known backdoors should be removed: A backdoor into an IT system is a way of accessing a system by bypassing normal security requirements.
- Patches and updates: Patches and updates for hardware (firmware) and software (operating systems and security applications) should be applied and kept up to date.
- Update management: In a large computer network, the management of updates can be an issue. Rather than each individual PC in the network downloading its own updates, often the IT department will be responsible for downloading an update, testing it on a separate system to ensure that it works correctly and does not interfere with other software (sometimes called 'sandbox testing') and then managing the roll-out of the update to user machines, perhaps at night or at the weekend to minimise disruption.

Avoiding impedance of business operations

One of the issues with security policies and baselines is that a balance between security and usability needs to be maintained: that is, the rules applied for the sake of IT security should not impede the business in carrying out its day-to-day operations successfully. Examples of security rules which could cause impedance to a business's operations include the following.

- Ingress and egress of expected network traffic: Firewall rules that prevent legitimate incoming (ingress) or outgoing (egress) network traffic can create user frustration and will increase the number of IT support calls.
- Server interconnectivity: Server interconnectivity includes allowing remote access and shared folder access. Restricting this interconnectivity may make transferring data difficult and encourage people to use less secure methods such as email or USB memory sticks to transfer data.
- Time based access: Time based rules that prevent users from logging on or from accessing certain resources outside normal office hours can create problems in situations where people might need to work late.
- Remote access: Allowing users to access IT systems remotely provides many benefits such as allowing staff to work from home and to access important information while out of the office at meetings or with customers. Therefore any security policies that make it difficult to access IT systems remotely will have a negative impact on employees who work from home or work offsite.
- Allowing external access to internal servers and data interchange: Granting access to internal servers and allowing data interchange with external suppliers (banks, for example), business partners and external cloud-based solutions has many benefits and allows for efficient business processes. However, it has associated risks. For example if an external organisations' systems are hacked, this may allow hackers access, via the external links, to other companies' systems. External links therefore need careful control and monitoring.
- The impact of aggressive email filters: Email filtering is used to reduce the amount of spam received. However, aggressive spam filters can cause problems and may block legitimate emails.

- Use of different software by different individuals: Users may have their own favourite software applications, but IT security policies may specify particular applications and prevent users from installing their own software. A good example of this is internet browsers. Many people have their favourite internet browser (Firefox® and Google Chrome™ browser, for example), all of which can be downloaded for free. However, in many organisations, the downloading and installation of 'non-approved' software is not allowed.

A security baseline that is too restrictive may create a lot of user frustration and additional IT support requests. It may also encourage users to try to find ways of working around it, which may create additional security risks. Therefore a balance must be struck between security and usability for employees.

PAUSE POINT

What are the network and internet usage policies at the college or school where you are studying? Identify the issues that they cover and consider the following.

- What restrictions do they place on the use of the network and why?
- Are the restrictions they place on the network reasonable?

Hint

You were probably introduced to your centre's network usage policy at your course induction, but if you do not have a copy or do not know where you can access one, ask your tutor for a copy.

Extend

Search on the internet for examples of network usage policies (search for 'network or internet usage policy' or 'acceptable usage policy') and compare these with your centre's policy. How and why do they differ?

Software-based protection

An organisation's IT system must have a variety of active software and hardware-based protection methods enabled. The same is true for personal IT systems, but here fewer methods will be available or needed.

Anti-virus software

IT systems need protection from malware that can attack a system from the internet or external storage devices. A variety of anti-virus and anti-malware software is available, including Windows Defender (which is built into current versions of Microsoft Windows® operating system), free anti-virus software (such as AVG AntiVirus Free Edition), and paid-for anti-virus products, which often include additional features such as password management and protection for mobile devices.

Anti-virus software generally uses two techniques to help identify malware: virus signatures and heuristics.

Virus signatures

Virus signatures are a list of code strings which can be found in individual viruses. The signatures are regularly updated because new viruses are being created all the time. The anti-virus software downloads new signatures from the software developer on a regular basis. When a virus scan is done, the software compares each file on the system and the contents of the system's memory against this signature list to see if any viruses are present.

One disadvantage of this method is that it will only detect those viruses for which signatures exist. A newly developed virus might not have its signature identified for some time after the virus is released. The time between a new virus being released and the signature to detect it being identified and downloaded onto a computer is a period in which the computer is vulnerable to so-called 'day-zero' attacks.

Heuristics

A heuristic method attempts to identify viruses by spotting the types of behaviour that viruses commonly exhibit. Heuristic methods avoid the day-zero attack vulnerability but may create more **false positives** than using virus signatures.

Dealing with identified threats

Once the anti-virus software has identified a potential threat, it will typically 'quarantine' the file to ensure that it cannot affect any other parts of the system, and it will usually notify the user. If the user is happy that the file is not important, then they can instruct the anti-virus software to permanently delete it.

Firewalls

A firewall is a software program or hardware device that filters data as it enters and leaves a network, making sure that only certain types of data can enter or leave it. (A firewall sets inbound and outbound rules for data.)

A firewall can be implemented as a software application running on an individual server or workstation. A network firewall is a hardware device that protects a whole network. Usually, a firewall creates a barrier between a LAN and the internet. Using a personal firewall, for example the one built into Windows® operating system, is essential if you are accessing the internet using public WiFi networks, such as in a café or hotel, to provide a degree of protection.

Firewalls use a number of methods to filter the data entering and leaving a network.

Packet filtering

Packet filtering involves inspecting each network data packet at the lower layers of the TCP/IP protocol, as it arrives, and applying certain rules. Any packets that do not conform to the rules are rejected. The rules can be set by a network administrator or the default rules applied by the software can be used. The rules can include source or destination IP address, source or destination port, protocol used or other settings.

Application layer filtering

Application layer filtering involves inspecting data higher up the TCP/IP protocol stack. It filters the connection on an application process basis rather than at a port level, as a packet filter does. The filter blocks any data that does not comply with the rules for the particular application.

Network address translation

Firewalls often hide the true IP addresses of devices they are protecting. This prevents external attackers from identifying the addresses of individual systems which might assist them in attacking those systems. They do this by mapping the multiple internal private IP addresses inside the LAN to the external public IP addresses used on the internet, by maintaining an address translation table.

Firewalls typically maintain a log of the network traffic they have blocked. A network or system administrator should use this log when investigating possible intrusion attempts.

Demilitarized zone and proxies

- The connection between a LAN and the internet is the place where hackers will attempt to gain access to an organisation's IT systems, so it makes sense to protect the perimeter of this network.
- Some systems, such as web and email servers, will need direct access to the internet while most will not. It is common practice to place any servers that need direct internet access in a so-called demilitarized zone (DMZ), protected by a network firewall which allows web and mail server traffic to go through.
- A second firewall protects the rest of the LAN system, blocking external requests to ports that are needed by the web and mail severs. This network configuration with a DMZ is shown in Figure 7.3.

Key terms

False positive – a false positive is when an alarm is raised by an event which is non-threatening. Anti-virus or anti-malware software and firewall systems may generate false positives when they look for the type of activity that may indicate an attack. It is impossible to prevent false positives altogether, but too many of them can be annoying and may lead to alerts being ignored, which could allow a real attack to continue without action being taken.

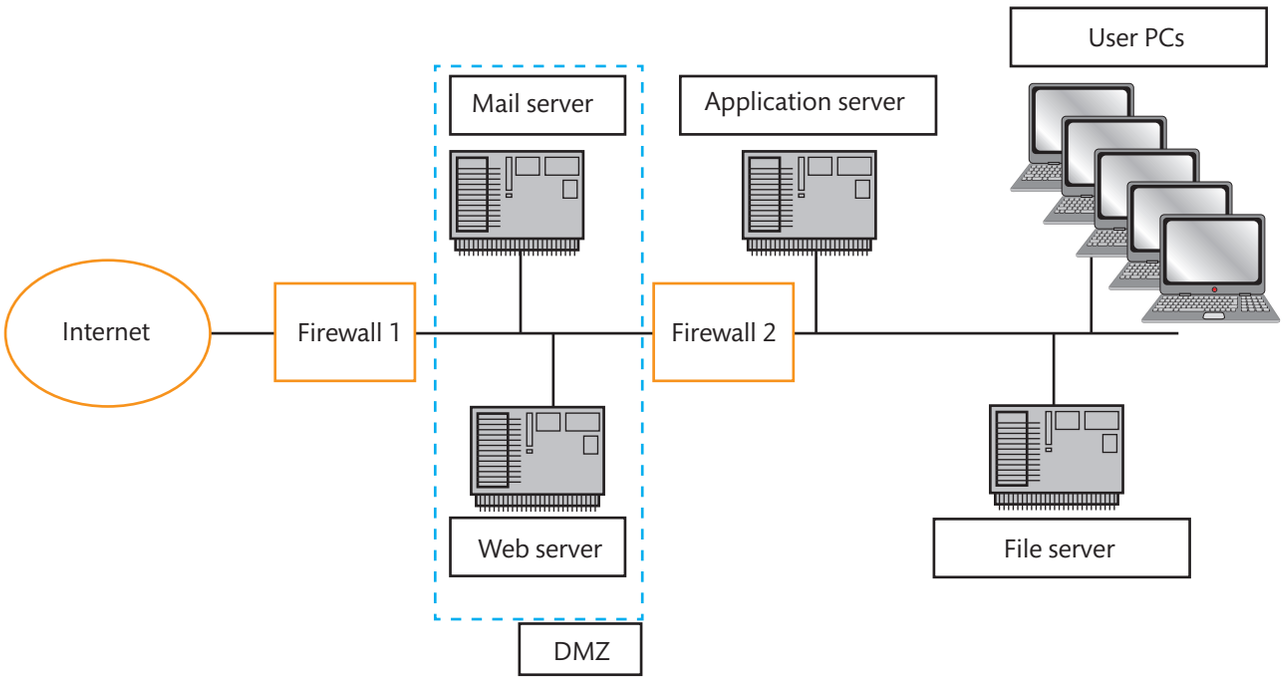


Figure 7.3: Network configuration with a DMZ

Many corporate networks also use a proxy server to forward requests for web pages from users inside the LAN. Doing so has several benefits. The proxy server can cache pages from commonly visited websites, which improves the apparent performance of the internet within the LAN as these pages do not need to be retrieved every time from the originating web server over the external internet. Proxy servers also filter internet requests and deny users access to web pages that are dangerous or inappropriate. Many third-party companies sell and update lists of websites that fall into a range of categories that companies might consider inappropriate, such as **anonymiser websites** and those for gambling and pornography. When an employee attempts to visit a filtered site, the proxy server can display a message reminding the user of the organisation's acceptable IT usage policy. Proxy servers also log which websites employees have visited.

Key term

Anonymiser websites – these provide a method for bypassing proxy server filtering.

Intrusion detection systems (IDSs)

IDSs are software applications or hardware devices that monitor a network for suspicious activity and attempt to detect and (in the case of an active IDS) block attacks on IT systems and networks. IDSs can identify malicious hacker activity that anti-virus and anti-malware software can miss. There are two types of IDS.

- Host IDS (HIDS): These protect individual servers or workstations, and are sometimes used on Internet-facing servers because email and web servers are the most vulnerable to attack.
- Network IDS (NIDS): These protect entire networks.

An IDS uses known attack signatures (similar in concept to virus signatures) of various types of suspicious activity that a hacker might carry out to gain access to the IT systems on a network. Like virus signatures, IDS attack signatures need to be updated regularly. The IDS can also look for unusual network behaviour. It does this by monitoring normal network traffic over time (a baseline) and then, if it detects network behaviour which is significantly different to the baseline, raising an alert. If suspicious activity is detected, then the IT system alerts the network administrator and may also block the activity. As most IDSs simply log events or raise alerts (perhaps by sending an automated email to the system administrator) it is essential that the system administrator regularly reviews the logs and investigates the alterations to check if they constitute a real attack, and, if they do, take appropriate action.

Research

Firewalls and IDS are a complex topic with many different technologies and configurations in use. Research the topic to find out the latest information about their features and use.

Domain management

A Windows® operating system-based client–server network is called a domain. In a large network, users do not usually log on to individual computers but are logged on to the domain via the computer they are using. Their credentials (username and password) are verified by the domain controller, which is a server computer that performs this function. This means that users do not need individual user accounts on each computer as they have just one domain account. This also makes administering users and applying security measures easier. Using a domain also allows the system administrator to restrict the devices that can attach to the domain. Before a device can join a domain, the administrator must give permission, which helps to prevent unauthorised devices from being connected to a network. (The version of Windows® operating system designed for home use cannot join a domain).

User authentication

The standard Windows® operating system log-on procedure is to enter a username and password. In a client–server network where users log on to a domain rather than a local computer, passwords are sent to the domain controller for authentication using the Kerberos protocol, which ensures that user passwords are never sent over the network unencrypted.

Research

What is Kerberos? Where does the name come from? Who developed the system and how does it work?

- Strong passwords: As with any secure system, the use of strong passwords is important to prevent others from guessing a user's passwords. Within a Windows® operating system domain, the administrator can set up policies that control the rules for acceptable passwords. Figure 7.4 shows the options that can be set for local or domain users.

The purpose of each setting for local or domain users is as follows.

- Enforce password history: When users are forced to change their passwords regularly there is a danger that they will just swap between a small number of favourite passwords, perhaps just two of them. Password history remembers a specified number of previous passwords and prevents the user from reusing those previous passwords.
- Maximum password age: Once the maximum number of days for password age has passed, the user is forced to change their password.
- Minimum password age: Allowing a user to change their password too often can also create problems. Once a user has changed their password, they must wait a specified minimum number of days before they can change it again.
- Password must meet complexity requirements: If this option is selected, then a password must meet certain requirements. For example it cannot contain the username and it must include a combination of 3 digits out of upper case, lower case, numeric, and special characters.

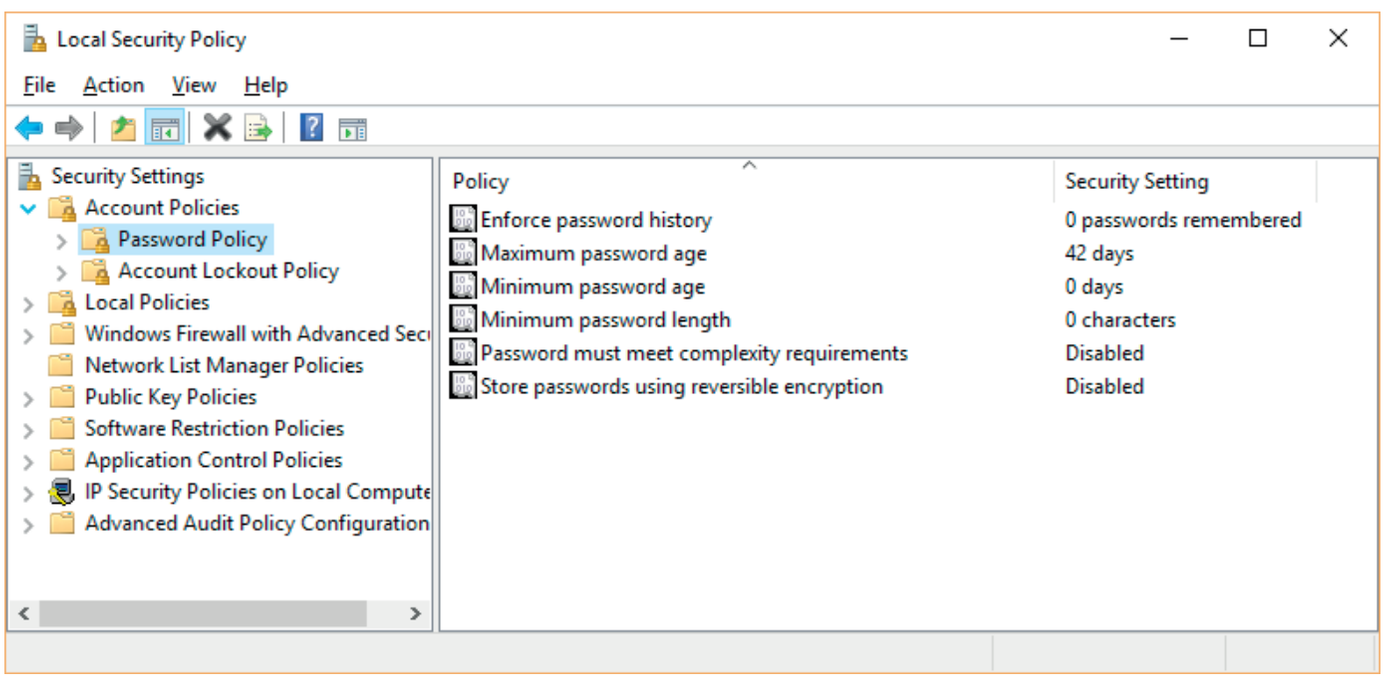


Figure 7.4: Options for local or domain users

- Store passwords using reversible encryption: This option is disabled by default and should not be enabled unless the security of the system is not important, as it allows users' passwords to be easily decrypted.

  It is also possible to restrict the time of day and days when a user can log on to the IT system, as shown in Figure 7.5.

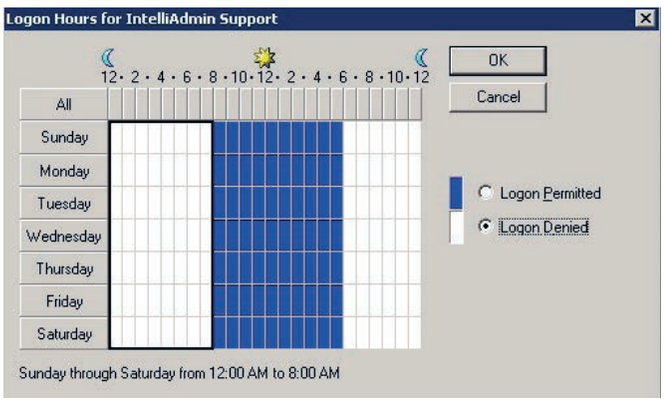


Figure 7.5: Restricting time of day and days when a user can access an IT system

Further authentication methods

Where stronger security is required beyond that provided by a password system, additional security can be provided through the use of biometric authentication (such as fingerprint readers), two-factor authentication or security tokens.

Link

Other protection methods are described in the earlier sections 'Cryptography methods' and 'Physical security'.

Discussion

Passwords are an essential part of modern life. Every time you want to access an online resource or purchase something online you need to register and create an account with a password. This could mean that you have tens, if not hundreds, of accounts all of which require a password. Discuss the best way to keep track of all these passwords with a peer or in a small group. It may not be possible or wise to use the same password for all accounts – why not?

Access controls

Network operating systems, such as Microsoft Windows® operating system and Linux, provide access controls that can be used to control which users have access to different files and folders and what type of access they have (full, write or read only access). Windows® operating system file permissions are a fairly complex topic, with slightly different permissions used for files held locally and on the servers (called NFTS file permissions) compared with those for folders shared over the network (called shared folder permissions).

The Linux operating system provides similar facilities which are known as Linux file permissions, or sometimes Linux octal file permissions. Linux file permissions use a command-driven interface and the level of access granted to a file is defined by a number between 0 and 7 (hence the name 'octal' , i.e. base 8 permissions). The meaning of the number is as follows.

Table 7.5: Linux octal file permissions

7	Read, write and execute
6	Read and write
5	Read and execute
4	Read only
3	Write and execute
2	Write only
1	Execute only
0	No access

Linux file permissions are set using a program called chmod. A three digit octal number is used to define the level of access to the file owner, the current group and everyone else.

For example, the following command would give read and write access to the file myfile to just the file owner and current group. Everyone else would have read only access to it.

```
Chmod 664 myfile
```

Windows® operating system shared folder permissions are investigated further in this following Step by step.

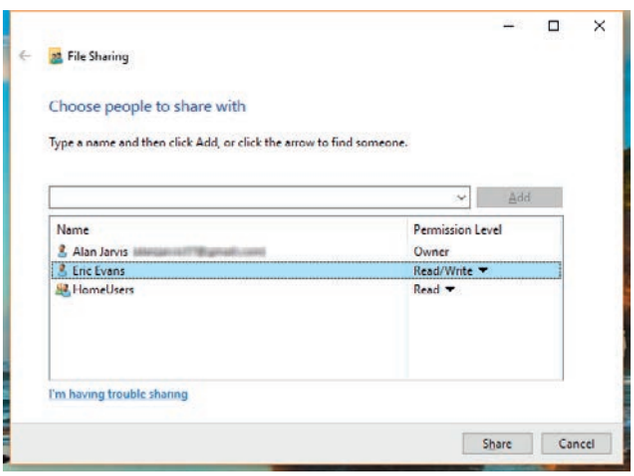
Step by step: Shared folder permissions

5 Steps

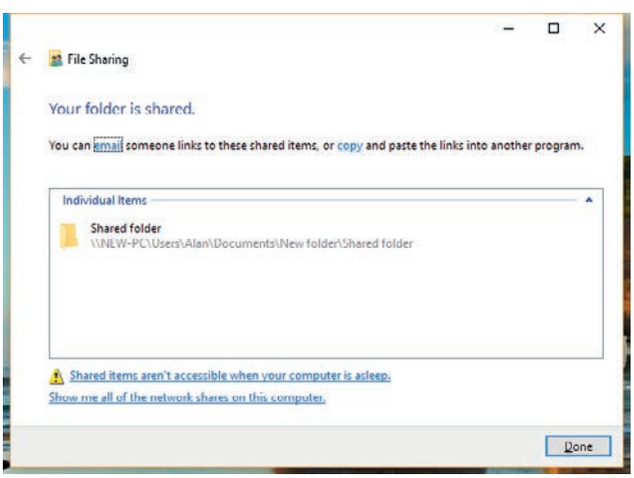
1 Imagine you want to create a shared folder but give different users different levels of access to it. First, you need to create a folder using the Windows® operating system File Explorer, then click on the folder you created and choose the **Share** tab in the menu at the top of the File Explorer window.

2 To share the folder with specific users rather than everyone, choose 'Specific people...' and the dialog box shown here will pop up.

3 If you drop down the box next to the **Add** button, you will see a list of all the users who have accounts on the computer plus 'Everyone'. Selecting **Everyone** will share your folder with everyone on the network. Click one of the accounts and then click **Add** and then that user account will be added to the box below. The default setting is that they have read only access, but you can change this to read/write by dropping down the arrow beside where it says 'Read'.



4 Click the **Share** button at the bottom and the folder is now available to everyone on the network. You will see a dialog box similar to that shown here, which gives the pathname of the shared folder.



5 Anything saved in this folder is now accessible to network users. Users with read/write access can both open and save files in the shared folder, while those with read only access can only open the files, but cannot save them back to that folder.

D Implement strategies to protect an IT system from security threats

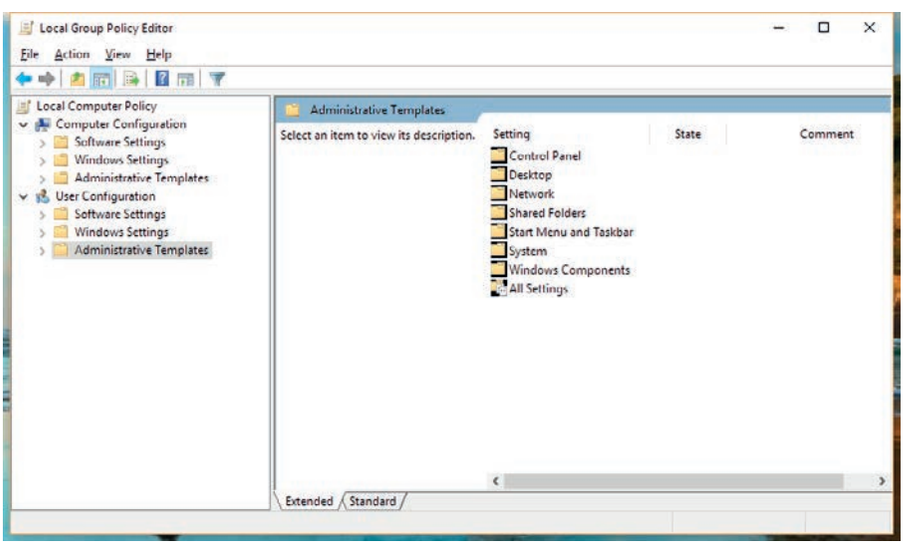
In this section, you will look at the strategies that you can implement to protect an IT system from security threats. These include group policies, anti-malware protection, firewall configuration, wireless security and access control. You will also look at how to test and review the protection that you apply to an IT system.

Group policies

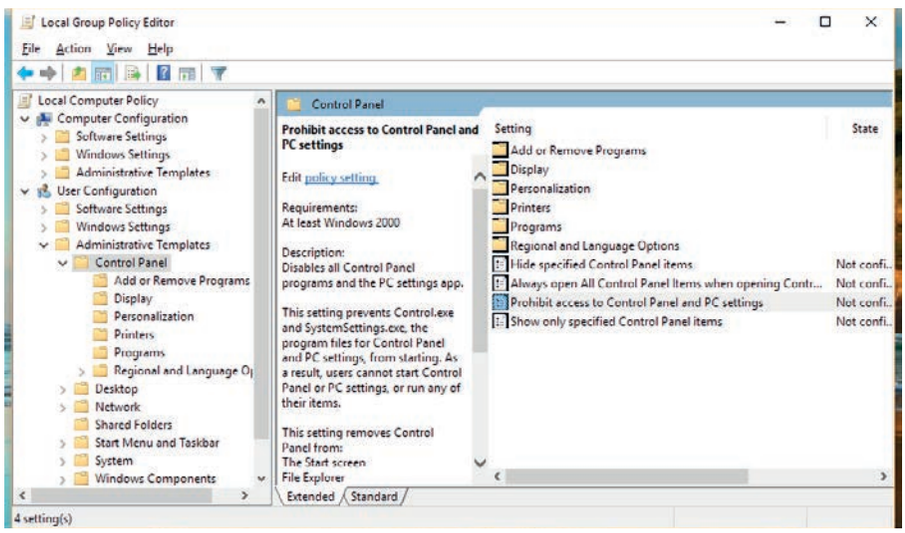
In a large Windows® operating system client–server-based network, the system administrator can use a feature of Windows® operating system Server operating systems called 'Group Policy' to centralise the administration of the features that users or groups of users can access. Often system administrations will want to restrict users and take away features such as the ability to start programs using the run menu and the ability to make changes to the desktop. Group Policy erful tool as you only need to configure it once on the server and then it will apply to all computers attached to that domain. The system administrator should decide what restrictions should be applied to users and then use Group Policy to implement those restrictions.

Step by step: The Group Policy editor — 6 Steps

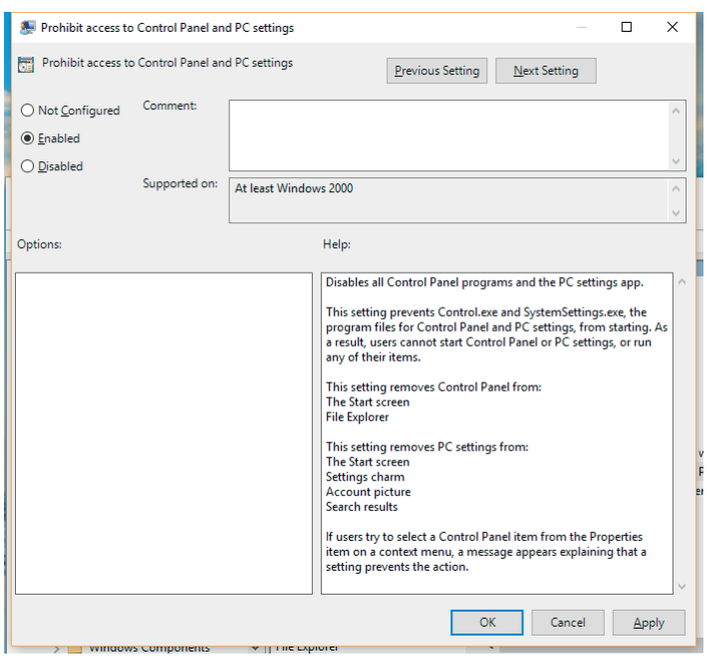
1 You can run the Local Group Policy editor on Windows® operating system 10 by using the run command and typing in 'gpedit.msc' as long as you are logged on as a user in the Administrators group. This should display the screen shown here.



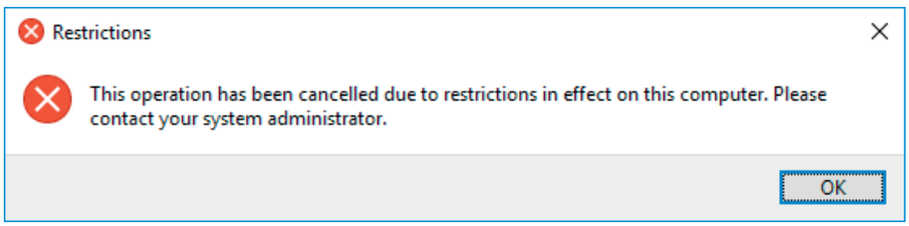
2 The Local Group Policy editor only applies settings to a single computer, but you can use similar tools on a Windows® operating system Server to apply settings to a whole domain. Click on **Administrative Templates** at the bottom and a list of templates controlling the features that a user has access to will be shown on the right. Suppose you do not want users to be able to access the Control Panel. Click on the **Control Panel** icon, and then click **Prohibit access to Control Panel and PC setting**. You will see a description of what this setting does in the centre panel.



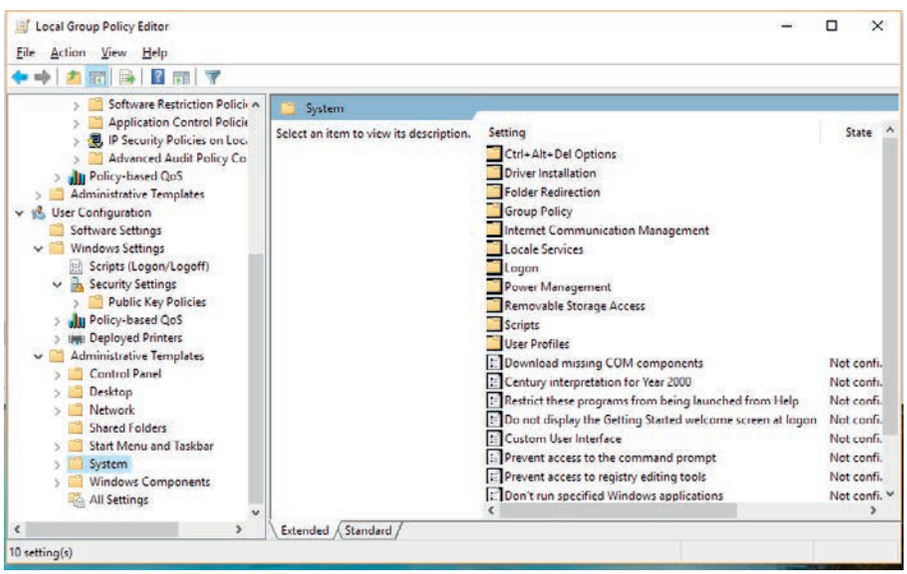
3 Double click on the option and a dialog box will pop up where you can enable this setting using the radio button.



4 Now click OK. If you now log on as a user (using an account which is not in the Administrators group) and try to open the Control Panel, you will get an error message like the one shown here.



5 There are many other settings that you can use to restrict what users can do. Many systems administrators will not want their users having access to the command prompt or to the run command. The option to disable the command prompt can be found under the System section of the **Administrative templates**.



6 The option to remove the run command is found under the **Start** menu and task bar section.

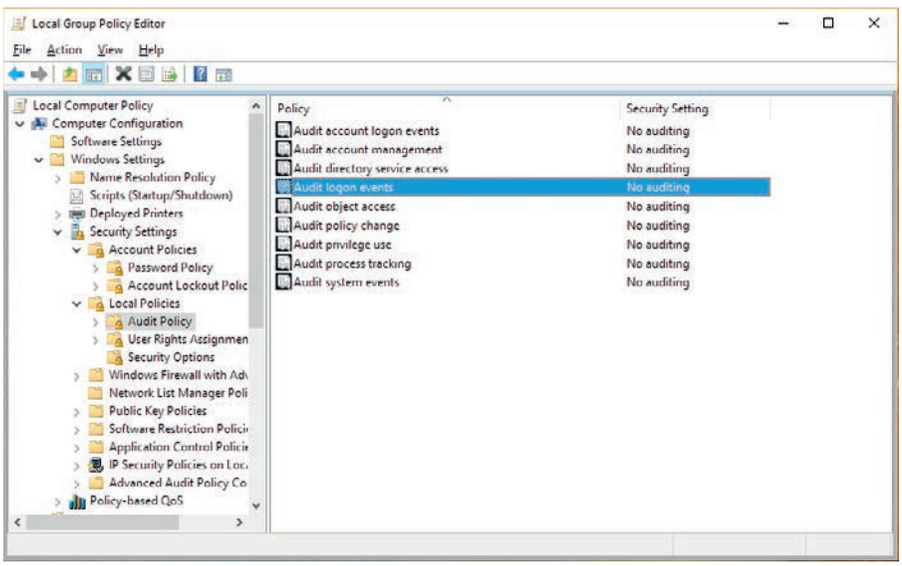
As well as using the administrative templates to restrict what users can do, the Group Policy editor also allows a system administrator to set up a range of policies that apply to the whole system. The use of Group Policy to enforce system-wide password rules was discussed earlier. This can be found under Computer Configuration>Windows Settings>Security Settings>Account Policies. As well as password policies, you can also set Account Lockout policies which allow you to lock an account after a certain number of incorrect password entries. This can be useful to defeat brute force attacks.

Other options that a system administrator might want to set are the Local Polices, which apply to security settings. These allow the system administrator to audit various events, restrict the rights that users have to carry out various tasks and a range of other options.

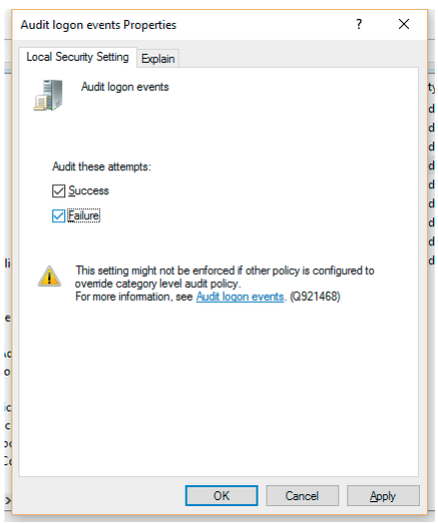
Step by step: Audit policy

3 Steps

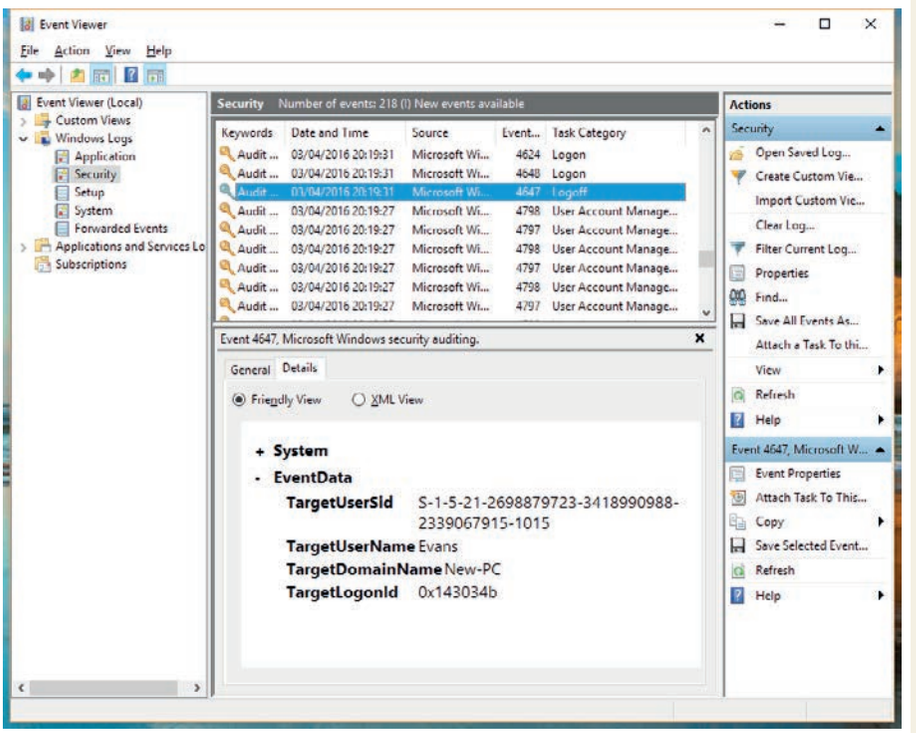
1 The audit policy allows a variety of different events to be audited in the security event log. To switch on auditing, open the Local Group Policy editor and then navigate to **Computer configuration>Windows Settings>Security Settings>Local Policies>Audit Policy**.



2 Double click on the **Audit log on events** and the dialog box shown here will appear. You can choose to audit log-on success or failure or both.



3 Auditing events causes system overheads so it is unwise to audit too many events. The Security Event log can be viewed using the Windows® operating system event viewer. Search for 'Event Viewer' and select the **Event Viewer desktop app** option. This will display the event viewer. Select **Security** on the left to see the security log, as shown here. Note that the log records a lot of information about each event, which is shown in the panel at the bottom of the display.

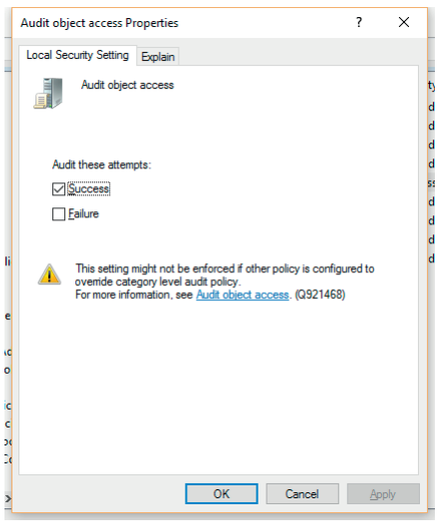


As well as auditing log-on events, you can also use Group Policy to set up auditing file access. This can be useful if you have particularly sensitive information in some files and you want to know who is accessing them and when. However, as with log-on event auditing, you should not audit too many files as it does increase the system overheads and amount of auditing information collected. With file auditing, first of all you have to switch on the ability to audit file access using the Group Policy editor, then select the files you want to audit by modifying their properties.

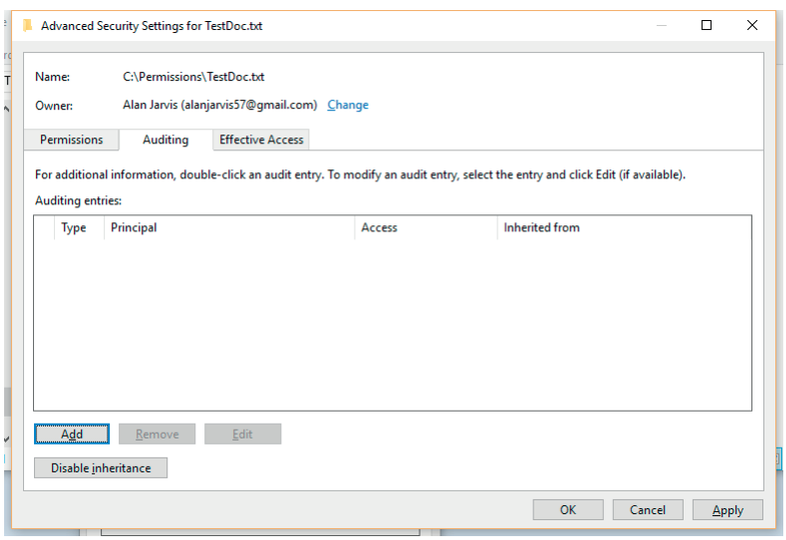
Step by step: Using audit object access

6 Steps

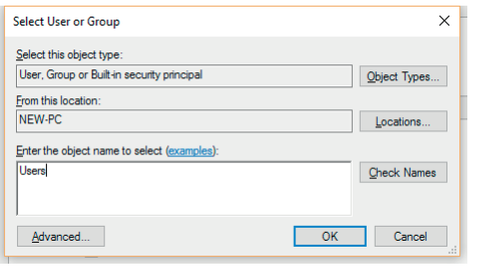
1 Open the Group Policy editor as previously and then navigate to Computer configuration>Windows settings>Security Settings>Local policies>Audit Policy. Now double click on **Audit object access** and you should see the dialog box shown here. You can audit both successful file access and failure if you wish. Auditing failure may enable you to see that someone has tried to break into files that they do not have access to. Click **OK** to close the dialog box.



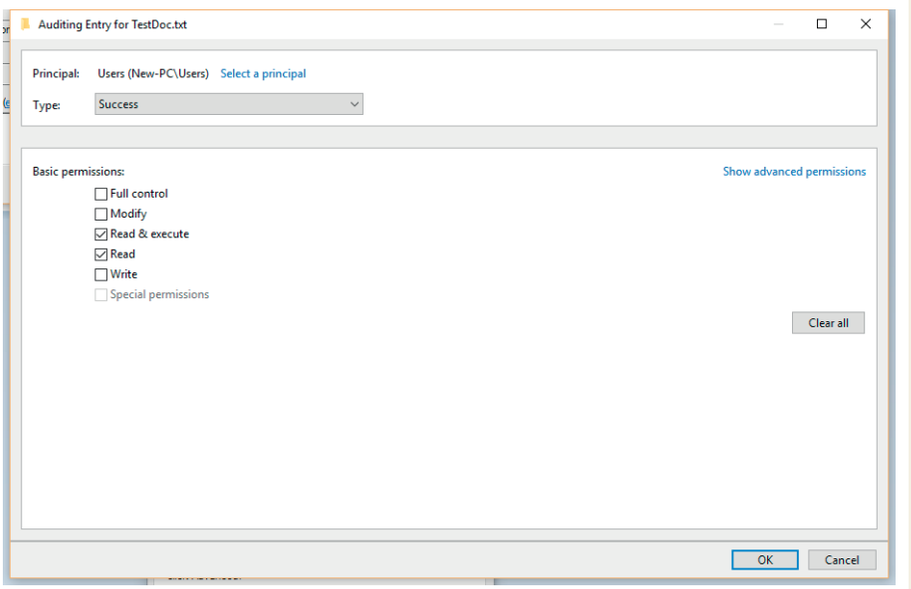
2 The next step is to select the file(s) you want to audit. Use the File Explorer to find the file, and then right click on the file and choose **Properties**. Select the **Security tab** at the top of the Properties dialog box and then click the **Advanced** button on the bottom right. This will display the Advanced Security Settings dialog box. Click the Auditing tab, and then click Continue to confirm that you have Administrator privileges. The dialog box should now look like this.



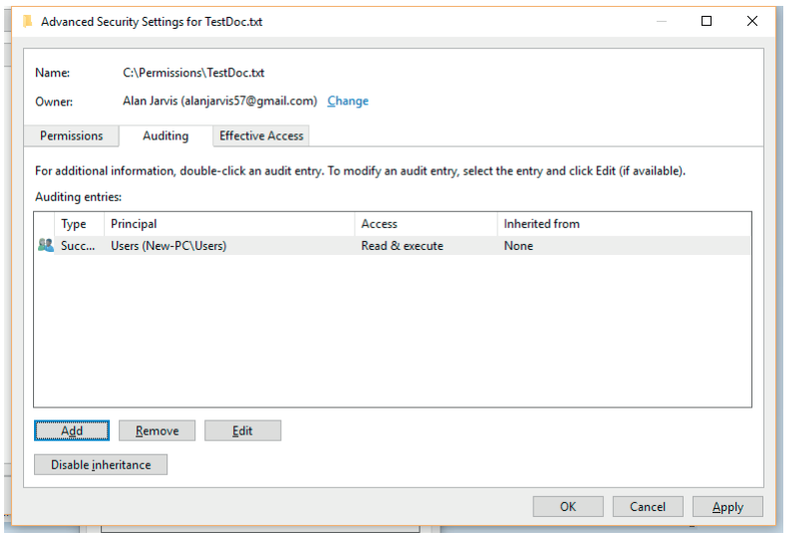
3 Click the **Add** button and the Auditing Entry dialog box will appear. Click the 'Select a principal' link at the top (i.e. who the auditing will apply to) and the Select a User or Group dialog box will appear. Enter a username or group (entering the Users group will apply auditing to all users), as shown here.



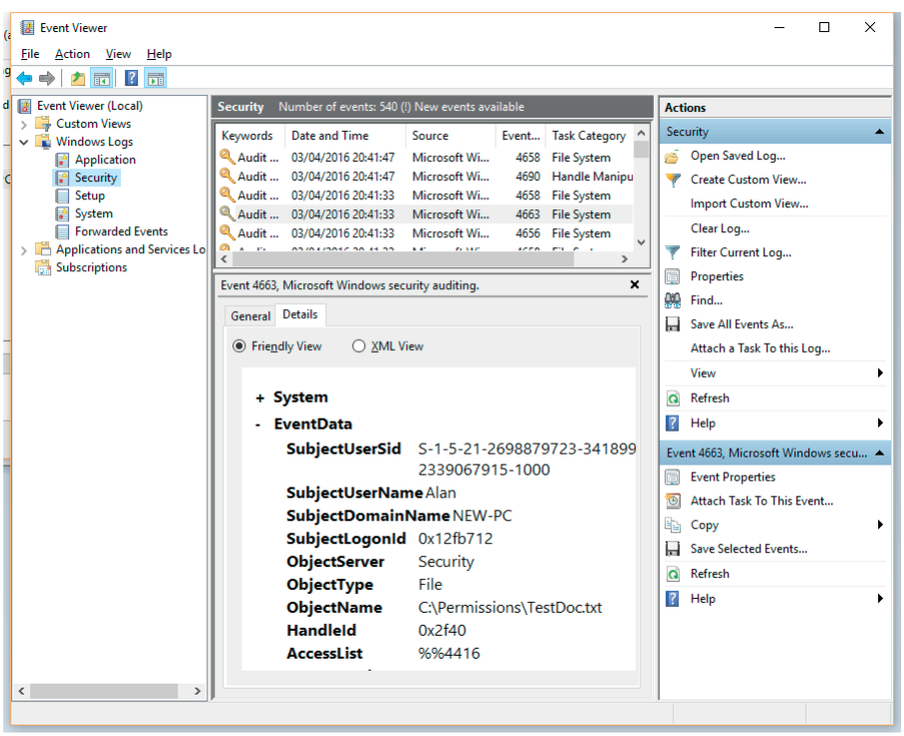
4 Now click OK to return to the Auditing Entry dialog box.



5 Click **OK** to apply these settings and you will return to the Advanced Security Setting dialog box with the auditing entry you have just created, as shown here.



6 The final step is to test that the auditing works. Open the file for which you have just made the auditing entry and then open the Windows® operating system Event Viewer, as before. Select Security on the left and you should find several File System events, as shown here. Note that simply opening the file creates several events.



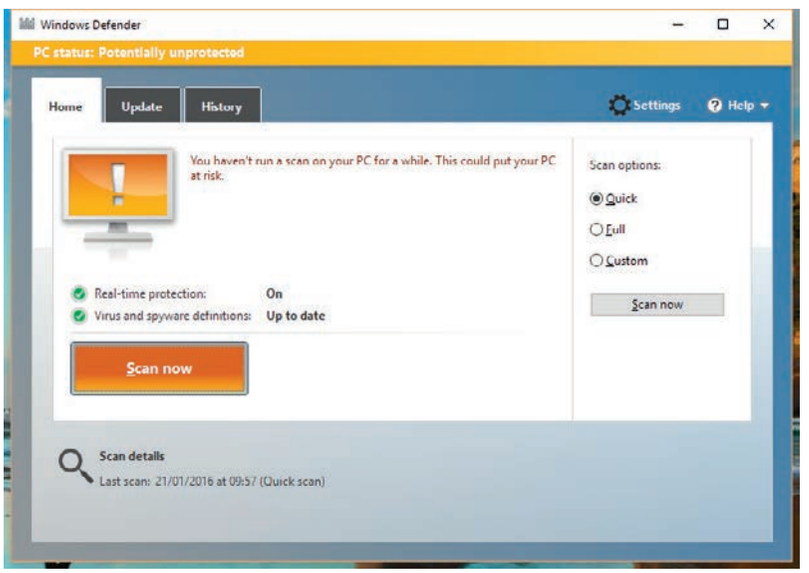
Anti-malware protection

Installing and configuring anti-malware (often called anti-virus) software is an important part of securing an IT system. Windows® operating system home editions come with basic anti-malware software called Windows Defender which is automatically installed. If third-party anti-malware software is used, then this must be installed.

Step by step: Configuring Windows Defender

3 Steps

1 You can find the Windows Defender program by searching for Defender in the Windows® operating system search box. The main screen of the Desktop App can be seen here.



2 Clicking the **Update** tab will allow you to check when the virus signature files (Windows Defender calls them Definitions) were last updated. Updates should be downloaded every few days. The History tab will let you see any suspicious files that Defender has found.

3 You can run a system scan from the Windows Defender main screen, and it is good practice to do this from time to time. You can choose to do a quick scan, which only checks those areas where malware is most likely to infect, or a full scan, which checks everywhere on the computer. A custom scan lets you check specific drives or folders, such as an external USB device.

Paid-for anti-malware products generally provide more facilities than Windows Defender. Installing a third-party malware scanner is simply a case of going to the website of the product developer and downloading the installation file and then running it. Many anti-malware software vendors provide free trials of their products, and some provide versions that are free for personal use. Currently, anti-malware protection is mainly focused on PC devices but many security experts are predicting growth in mobile-based malware targeting Apple® and Android®-based systems. Anti-malware software products (some of which are free) are available for mobile devices and their use is recommended.

Once downloaded and installed, the software should complete a scan of your system to check that there are no pre-existing malware infections. One useful facility that most third-party anti-malware software includes is a scheduled scan for new malware infections. Remembering to scan the computer regularly can be difficult and it is not a good idea to scan the computer while people are trying to use it, as scanning can slow down the system quite significantly. It is wise to scan a computer weekly, at a time when no one is using it, so setting up a scheduled scan is useful.

Step by step: Setting up a scheduled scan

6 Steps

1 In this example, a scheduled scan is set up using AVG anti-malware software – other anti-virus software would be set up in a similar way. First open the AVG user interface by clicking the icon in the task bar.

2 Then click the gear icon next to the Scan now button to open the Scan options dialog.

3 Next click the **Manage scheduled scans** button which will open the scheduled scans dialog. Click the **Add scan schedule** button at the bottom left and you will see the Schedules scan options.

4 Here a scan has been scheduled for every Sunday at 10pm. Click the **Save** button to confirm the new schedule (you may be asked by User Account Control if you want to allow this change). The scheduled scans dialog should now show that a scan is scheduled for the following Sunday at 10pm.

5 If, during a scan, AVG finds a file that it considers to be malware, then you can view a report at the end of the scan which gives details of the file it has found.

6 Clicking on the 'More info' link will take you to a page on the AVG website that describes the malware it has found in more detail. AVG also provide a number of configurable options that allow you to adjust the way in which scans are done and when updates are downloaded.

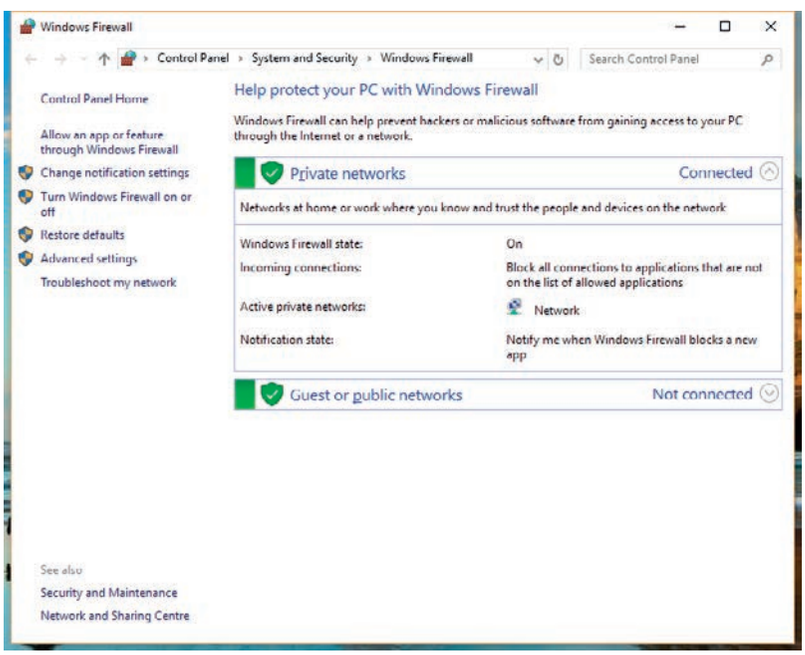
Firewall configuration

Windows® operating system also includes a basic firewall that is automatically configured and switched on when Windows® operating system is installed. The firewall enables you to allow or block various applications and set rules for both inbound and outbound data.

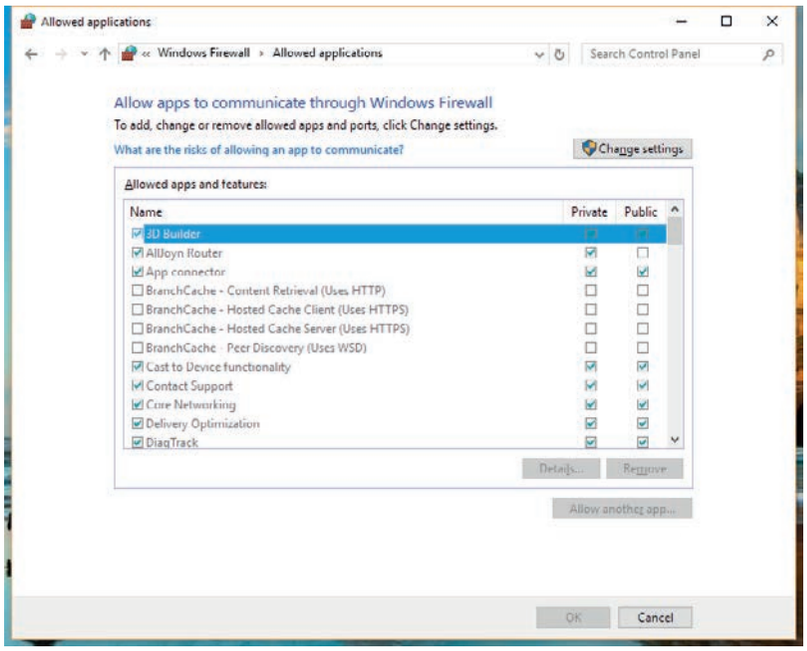
Step by step: Configuring the Windows® operating system firewall

8 Steps

1 To open the Windows® operating system Firewall user interface, type firewall in the Windows® operating system search box and click on the Windows® operating system Firewall – control panel option. This should display the screen shown below. This screen shows the status of the firewall. Windows® operating system Firewall allows you to configure different settings depending on whether you are connected to a private network (e.g. at home) or a public network (e.g. a public WiFi hotspot). The main screen should show that the Windows® operating system Firewall is on. Connections that are not on the allowed list are blocked and notifications are turned on.

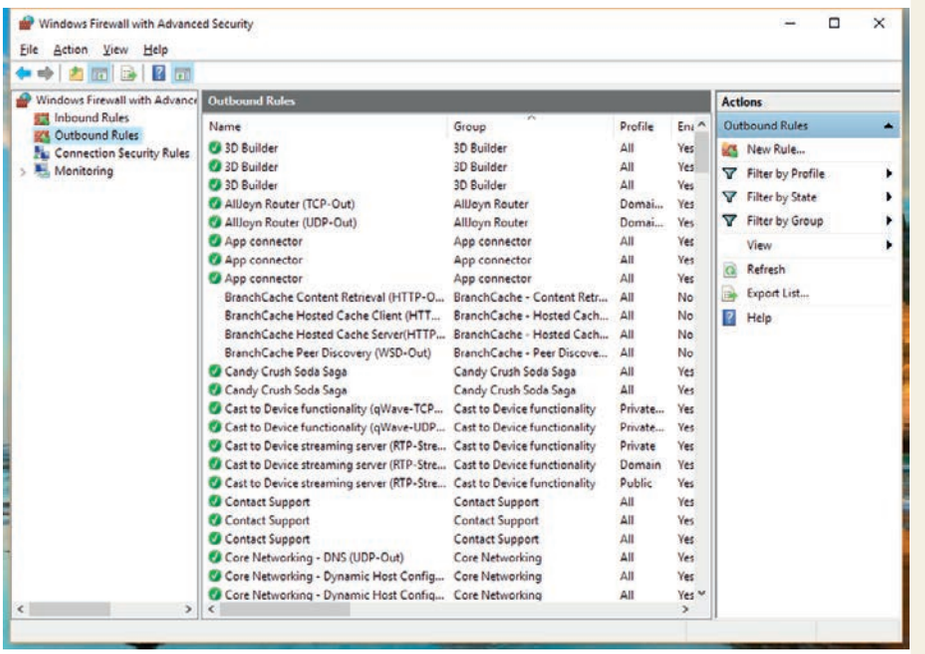


2 If a network application is not working correctly because the firewall is blocking it, you may need to do the following to allow it through the firewall. Click the 'Allow an app or feature through the Windows® operating system Firewall' link on the left. This will display a window similar to that shown here.

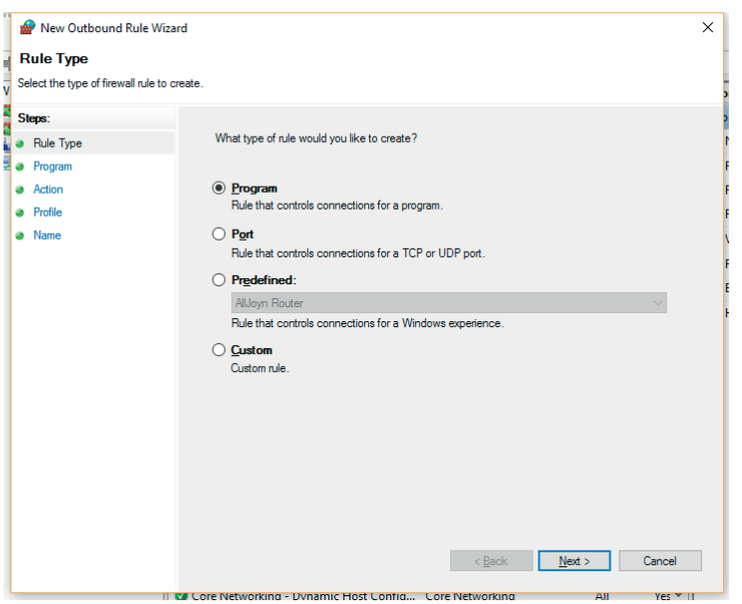


3 Click the change settings button (enter the administrator password if prompted) and scroll down the list of applications to find the one you want to allow. Then click the Private and/or Public check boxes to allow access on Public and/or Private networks. Click **OK** to complete the process.

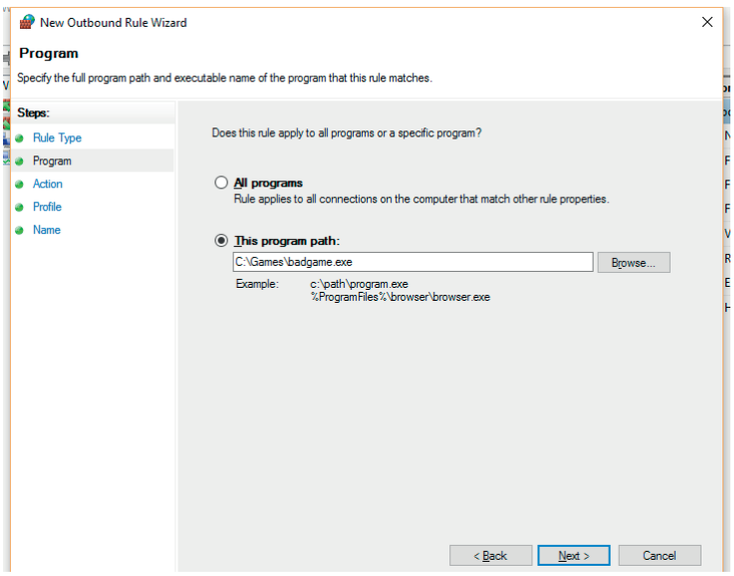
4 Windows® operating system Firewall can also be configured to block specific port, protocol or IP addresses. Click the **Advanced Settings** link on the left of the main firewall screen and you will see the Windows® operating system Firewall with Advanced Security window as shown here.



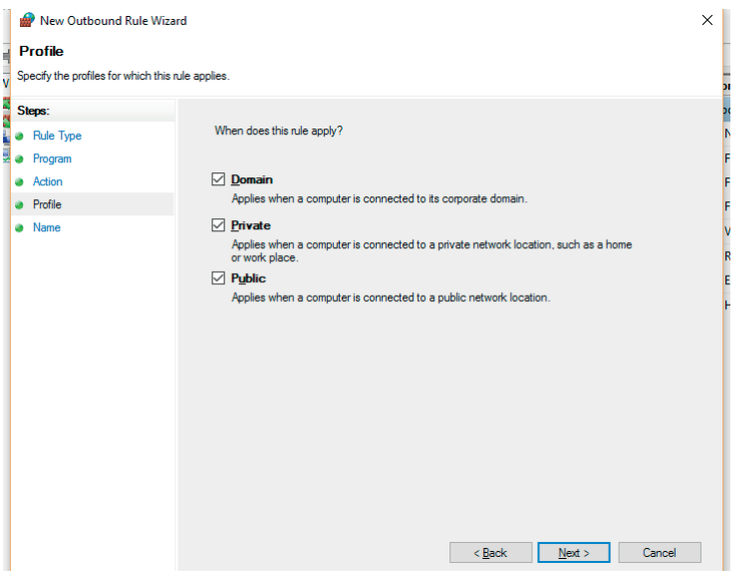
5 Suppose you want to stop anyone playing a game called 'badgame.exe' which connects to the internet. Choose Outbound rules on the left. These are the rules that apply to data coming from the computer to the internet. In the central pane, you can see all the existing outbound rules. Unless you know what you are doing it is not wise to change any of these. Click **New Rule** under the Actions pane on the right. This will start the New Outbound Rule Wizard as shown here.



6 The default setting is for a 'Program' rule, which is what is required, so just click **Next**. In this step, you need to enter the name of the program file you wish to block, as shown here.



7 Click **Next**. The next step will ask you what action you want to take, which, in this case, is the default 'Block the connection', so just click **Next**. On the Profile step, you need to decide when you want the rule to apply, that is, when the computer is connected to a domain, a private network or a public network, as shown here.



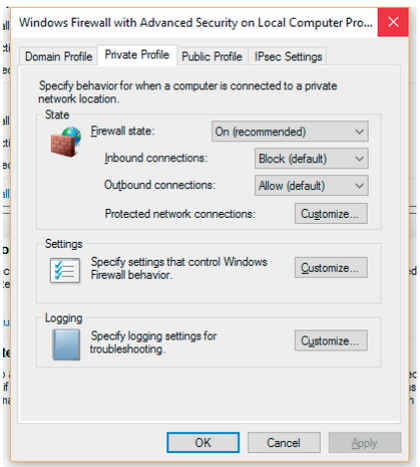
8 You may want the rule applied only when connected to a public network such as a WiFi hotspot in a café or railway station, but, for this exercise, you can leave all the options selected. Click **Next**. On this step you give the rule a name and a description, which can be helpful if you or someone else does not know or remember what the rule is for. Click the **Finish** button to complete the rule, which is now added to the list of outbound rules.

The Windows® operating system Firewall can log both successful and unsuccessful network connections. This is useful for trouble shooting or if you suspect hackers may be gaining access to your system. The log collects a lot of data so it is unnecessary for it to log all the time.

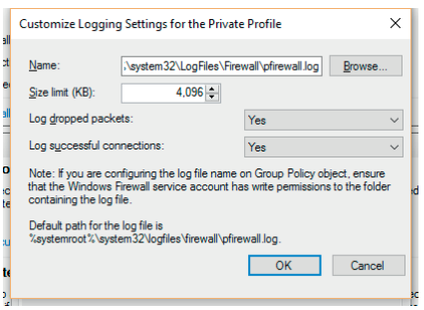
Step by step: Enable firewall logging

5 Steps

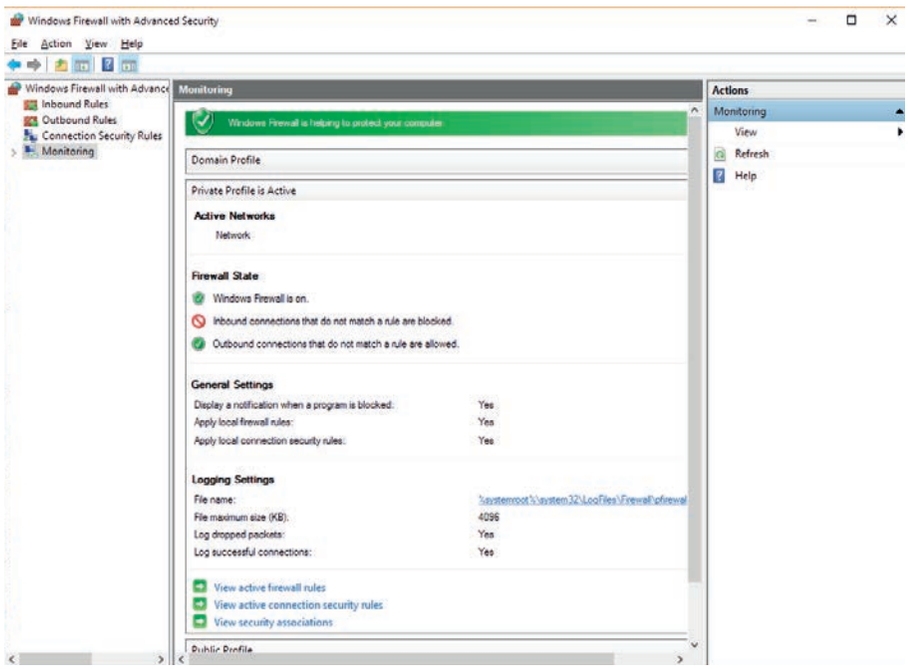
1 First, open the Firewall with Advanced Security window, make sure that in the left-hand pane you have 'Windows® operating system Firewall with Advanced Security' selected (i.e. not any of the rules) and then, on the right-hand pane, click **Properties**. This will open the properties dialog box, as shown here.



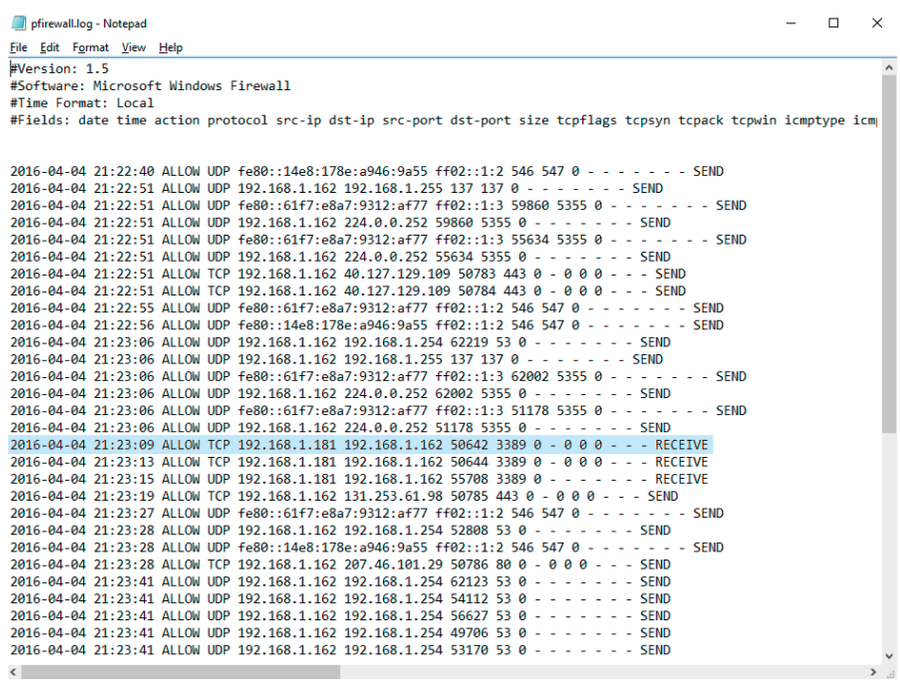
2 Select the **Private profile** tab at the top of the dialog box (assuming that your current network is recognised by Windows® operating system as a Private network). Click the **Customize** button in the logging section. You will then see the Customize Logging Settings dialog box, as shown here. Leave the file name for the log file and the size limit as they are and set **Log dropped packets** and **Successful connections** to **Yes**.



3 Click **OK**, and then **OK** on the properties dialog. In this example, a remote desktop session was opened with the computer and then the log file was viewed. To view the file, click the link at the top left of the Windows® operating system Firewall with Advanced Security main window. Scroll down the central pane of the window and click the link at the bottom labelled 'Monitoring'. This will display the monitoring settings, as shown here.



4 Towards the bottom of the pane under the Logging Settings section, there is a link to the log file. Click this link and the log file will open in Notepad, as shown here.



5 The highlighted line in the log shows the following:

2016-04-04 21:23:09	the date and time of the log entry
ALLOW TCP	The firewall allowed a connection using the TCP protocol
192.168.1.181	The source IP address on the connection
192.168.1.162	The destination IP address of the connection
50642	The source port
3389	The destination port (Remote desktop connections use port 3389)
0	The size of the data transferred
- 000----	The TCP flags and other data
Send	This was a connection that sent data

The log data can be useful but it sometimes needs interpretation. The following information can be obtained from looking at the log.

- **Source and destination IP addresses:** This tells you which computers were sending/receiving data.
- **Source and destination ports:** This tells you which applications were sending/receiving data. If you do not recognise a port number, try the list of port numbers here: https://technet.microsoft.com/en-us/library/cc959828.aspx
- **TCP flags and other data**: This information can only be interpreted with a detailed knowledge of how the TCP and UDP protocols work.

Wireless security

Most modern WiFi routers/access points come with effective security settings preconfigured. However, you can check and adjust them if needed. The exact method you need to use will depend on the type of router you have and you will need to search online for the manual or instructions for your particular router. Most routers provide a web-based user interface that you access from your computer via a browser.

Step by step: Configuring a wireless router

3 Steps

1 This example shows how to check and configure the settings on a BT Home Hub router. To access a BT Home Hub, just enter the URL http://bthomehub.home from a browser and you will see the main menu screen.

2 The main screen shows information about the status of the hub and the devices connected to it. To change the settings, click the **Settings** link at the top. You will need the admin password to access these settings, which is printed on the card at the back of the router. The **Advanced settings** link allows you to change some important settings, such as the type of security used and the password. Take care when making any changes to these settings, as you could reduce the strength of the security on you network.

3 These settings show that WPA and WPA2 wireless encryption are turned on with a reasonably strong password set (see the section Applications of cryptography). There are other settings that can be adjusted to improve the security of the hub. Under the Settings link, there is **BT Access Control tab** which allows you to control the times of day that all or certain devices have access to the internet.

Access control

For a large organisation, designing an effective regime of user groups and folder permissions can be quite complex. Ideally, based on the information security principles, you want to give users only the minimum amount of access to folders that they require to do their job. In reality, a regime that is too restrictive risks creating a lot of support requests because users are unable to access files they need to.

Link

For more about information security principles, see the section 'Information security'.

In a medium or large organisation that uses a Windows® operating system-based PC network, the system would normally be configured to use a client–server domain-based set-up, with one or more server computers running a Windows® operating system Server operating system. Users are set up centrally on the server that is configured as the domain controller and, to simplify the management of users, they would normally be placed in groups which define their access to files, folders and other resources such as printers. Windows® operating system has a number of built-in groups, of which the Administrator group is the most powerful. Users should only be added to the Administrator group when they need to have full control over all the system, and members of the Administrator group should have the strongest passwords, since they represent a considerable security risk.

Step by step: Creating users and groups

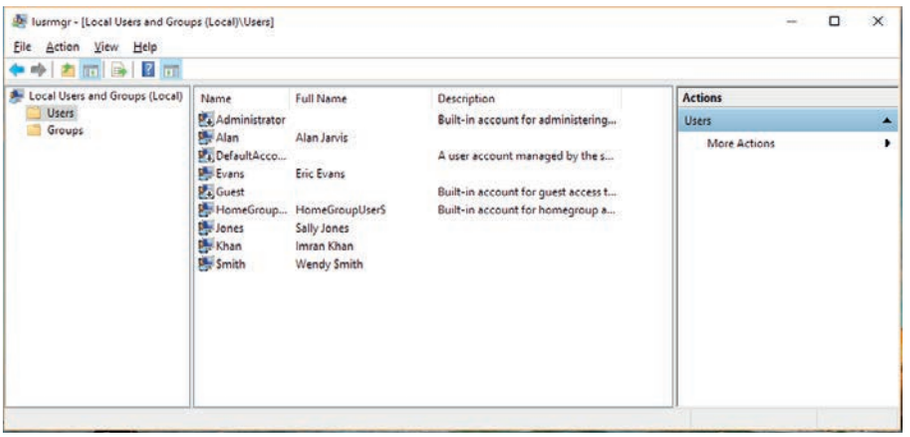
13 Steps

This example shows how groups and users can be set up on a local computer running Windows® operating system 10 rather than a server computer. However, the procedures are very similar to those that would be used on a server. Three user groups – for staff, managers and directors – are required. The users in each group are as follows (in reality, of course, there would be many more users).

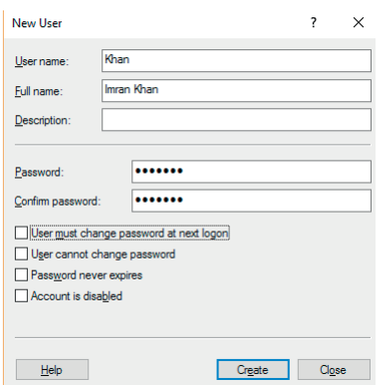
Eric Evans – Staff
Sally Jones – Staff
Imran Khan – Manager
Wendy Smith – Director

Step 1

1 To create the users and groups, you use the local user manager program, which is very similar to the Windows® operating system Server user manager program. To run the program, type **Run** into the Windows® operating system search box and then select the Run desktop app. Type the name of the local user manager program **lusrmgr.msc** into the Open box and click **OK**. The program should then run, as shown here.



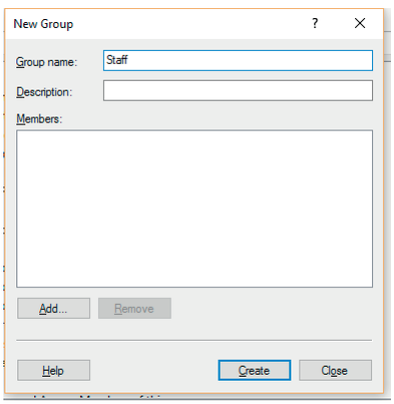
2 To create new users, click **More Actions** on the left and then choose **New User...** You will then see the dialog box shown here.



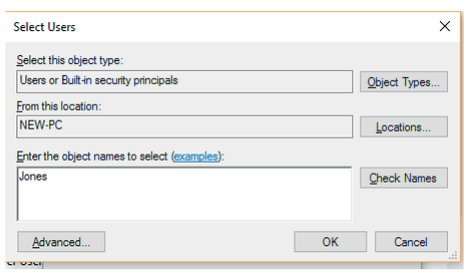
3 Enter each of the users listed above, set their password to something simple like 'welcome' and turn off the 'User must change password at next logon' option. This is just to make experimentation easier – these options should not be used for real users. Click **Create** to make each account and then **Close** when you have finished.

Step 2

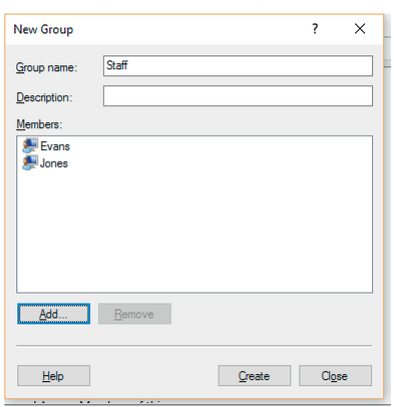
1 Next, we will create the groups and add the users to the correct groups. Windows® operating system comes with a large number of built-in groups, which you can see when you click on the **Group** link on the right-hand side of the Local User Manager program. To create new groups, click on **More Actions** on the right, then choose **New group**. The New group dialog box is opened, as shown below. Create the Staff group by typing the name in the Group name box at the top of the dialog box (there is no need to add a description).



2 To add a group member, click the **Add** button then enter the first username, as shown here.

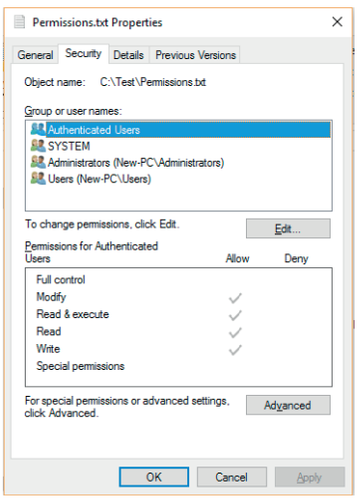


3 Click **OK** and this username will be added to the Staff group, and then do the same for the other user (Evans). The New Group dialog box should now look like this. Click **Create** to create the new group. Now do the same for the Manager and Director groups, adding the correct user to each one.



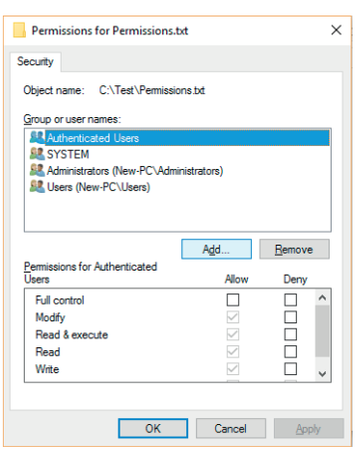
Step 3

1 Next, you will see how file permissions can be used to control the access that the different groups have to files. First, you will need to create a new folder in the root of the C: drive. Open the Windows® operating system File Explorer and navigate to the root of the C: drive. Create a simple notepad file or other document in the folder you have created. Then right click on the file and choose **Properties** to open the properties dialog box for the file. Click on the **Security** tab, which should look something like this.

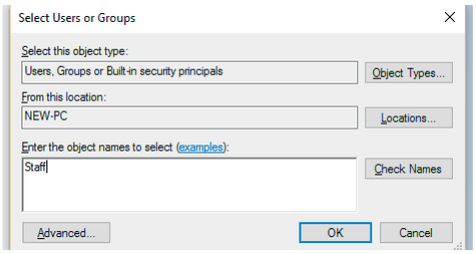


2 The top part of the security dialog box shows the groups or individual users who already have access to the file. If you click on a particular user or group, you can see, in the lower part of the dialog box, the permissions that the selected user or group has to the file. Users in the Administrators group have access to the file, as does anyone in the Users group, in which all local user accounts are automatically. This means that, at the moment, any of the other users you have created will have access to the file, as they are in the Users group. You can log in as one of the users you created to check that this is the case.

3 Suppose we did not want anyone in the Staff group to access this file, but want the Managers group to have read access and the Directors to have read and write access (they have this already so no changes are needed to achieve this). To change the permission on the file, you need to click the Edit button on the properties dialog box, which will then display another dialog box, as shown here.

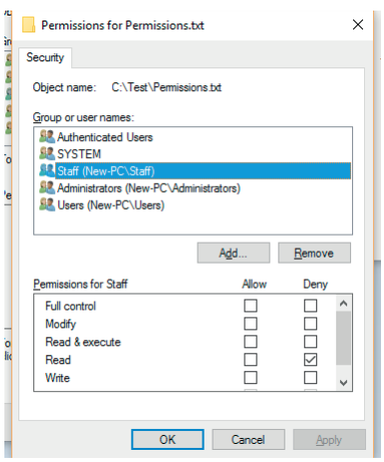


4 Now click the **Add** button on this dialog box to add the Staff group. Then you will see the Select users or groups dialog box. Enter the name of the Staff group, as shown here.

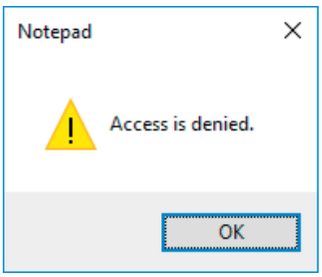


5 Now click **OK** and you will be returned to the previous dialog box, with the Staff group added to the top of the list of Groups or Users. Click on the Staff group name to see the current permissions in the lower part of the dialog box. It will look as if the Staff group only has read and read and execute permissions, but the users are also members of other groups (the Users group, for example) which gives the users other permissions. This is one of the issues that can make understanding permissions quite complex. You may have noticed that each permission can be either allow or deny. Normally, you use allow permissions, and these are cumulative – in other words, if any group that a user is a member of has, for example, write allow permission, then that user also gets write permission for the file. However, deny permissions work the opposite way around, so that if any group the user is a member of has write deny permission, then the user cannot write to the file even if other groups the user is a member of do have write allow permission.

6 Therefore, to prevent the Staff group having access to this file, we need to set the read deny permission to on. We do not need to set the other deny permission to on because, if they cannot read a file, then obviously they cannot write to it. This setting is shown here.



7 You should now find that if you log on as one of the users who is a member of the Staff group (Eric Evans), for example, and try to open that file, you will not be able to and will get the message shown here.



File and folder permissions are a complex issue and, to understand it well, you will need to practise and test your understanding of how it works. There are lots of Microsoft® training materials and books which cover the topic in detail. A poorly understood or complex set-up of groups and file permissions can cause an organisation a lot of wasted time, frustrated IT users and a lot of IT support calls.

There are a number of related issues such as the following.

- Ensuring that only applications whose updates (including binary executable files) are signed using a hash can be 'white listed' as trusted files.
- Ensuring that sensitive files, such as log files, are hidden and protected from unauthorised access. Typically, this would involve using the permissions settings, as described above.

Link

For more about access control, specifically on defining password policies, including length, complexity, age and reuse for desktop and server computers, see the section 'User authentication', in 'Software-based protection'.

Testing and reviewing protection

Setting up the required protection on an IT system is the first step to ensuring that a system is secure, but you also need to test that the protection works as it should and, from time to time, you should retest it to check that it still provides sufficient protection.

As with software development, the standard way to test a system is to create a test plan. The test plan identifies what you are going to test and what outcomes you expect before you start doing the tests. A suggested format for a security test plan is shown in Table 7.6.

Table 7.6: Security protection test plan

Test number	Risk targeted	Test description	Expected outcome	Actual outcome
1	Virus infection	Check definitions are updated	Definitions are the latest version	
2	Virus infection	Run virus scan	Scan finds no virus or resolves minor infection	
3	External hacking	Check firewall – port 80	Port is open	
4	External hacking	Check firewall – port	Port is open	
5	External hacking	Check firewall – port	Port is open	
6	External hacking	Check firewall – all other ports	Ports are closed	
7	Etc.			

A test plan like this can be used to systematically test that the firewall deals correctly with both allowed and blocked entry points and therefore blocks unauthorised traffic and allows legitimate traffic through.

Manual testing using a test plan can be useful, but it is only really suitable for a single IT system (individual computer). In a situation where a whole network of IT systems needs to be tested, a different approach is needed.

Network testing tools

An alternative to using the traditional method of manual testing is to use network testing tools. These tools can make testing a large number of risks on the many different IT systems (computers) in a medium or large network much easier.

Vulnerability scanners

Vulnerability scanners are a specialised form of software that uses a database of known security vulnerabilities to test whether a system is protected against them. The tests the software can do include identifying issues such as the following.

- **Open ports:** The scanner software can check for systems on the network that have ports open which should not be.
- **Weak passwords:** Vulnerability scanners often include a password cracker which can check that users have set up strong passwords for their accounts.
- **Default accounts and passwords:** Some operating systems and applications have default accounts which should be disabled. For example, some SQL database software allows administrator accounts to be created with blank passwords. Scanners can check for this and alert the system administrator.
- **Sensitive data:** Some vulnerability scanners can monitor a network and look for sensitive data that is being transmitted without encryption, such as credit/debit card details.
- **Security and configuration errors:** Most vulnerability scanners will search for misconfigured software which may give opportunities for attackers. For example, due to user error or other reasons, a system may have anti-malware updates or the firewall switched off. The scanner will detect these types of error and alert the system manager.

Link

One of the best known vulnerability scanners is Nessus. You can find out more about it if you do an internet search for 'Nessus'.

Penetration testing

Vulnerability scanners check for issues that may allow an attacker to access a system. Penetration testing is a more active method of testing which involves actually trying to access the system using the same techniques that a hacker might use.

Packet sniffers

Packet sniffers are sometimes called protocol analysers and are used to capture and analyse network data packets. They can be used by both network managers and attackers to inspect and modify both the control information with a packet (the packet header) and the data.

Packet sniffers include filter tools that allow a system administrator to view certain types of packet and to check that they are not being manipulated in some way by an attacker. However, using a packet sniffer in this way would be quite a lengthy process

and a better solution might be to use a tool to automatically detect such packet manipulation, such as an intrusion detection system (IDS).

Link

One of the best known packet sniffers is Wireshark, which is available as a free download. You can find out more about it at www.wireshark.org

Security-based operating system distribution

Typically, in a large organisation with many desktop PCs to support, the IT department will create a complete operating system and applications distribution (such as Office and other software), including a full range of security applications features (for example anti-malware software) and test the distribution fully before rolling it out to all the desktop computers. They will often create a disc image so that the complete system can be easily installed on any PC without needing to install and set up all the individual applications and settings. This approach ensures that all systems are set up the same way and have the same security settings and user features.

Tip

Working in the IT support department of a large company will mean, as with many jobs, that you work within a team of people. This will mean working with people who have different skills and areas of expertise. Working well in a team requires a number of different skills. You need to play your part in the team and support the other members. You also need to communicate well, listen to and understand what others are saying and let them know what you are doing and any issues that you may have.

The effectiveness of the protection

Judging the effectiveness of the applied protection is not easy. IT security is not a subject where the 'wait and see' approach is likely to be effective. As new threats are developing all the time, a system administrator needs to be proactive in their approach to security. This means regularly checking that what they currently have set up is adequate and always looking for ways to improve it. The testing methods listed above provide some means of checking how effective protection measures are, but a system administrator needs to keep up to date with the latest threats and know how to defend against them.

The effectiveness of the protection can also be considered in terms of the impact it has on the usability and performance of the system. As mentioned earlier, it is important that the protection measures do not unduly restrict users and interfere with the day-to-day tasks that they need to complete as part of their jobs. One method of judging the effectiveness of applied protection methods is to view activity logs such as those that can be produced by firewall systems. The log provides evidence of when the firewall has blocked connections and, as such, shows the effectiveness of the rules it is applying.

Link

Setting up, viewing and interpreting the Windows® operating system Firewall log was discussed earlier in the section 'Firewall configuration'.

File access auditing can also be set to log file access failure events (i.e. when a user tries to access a file or folder that they do not have permission to access) which again shows that the protection applied to the file or folder is working. Anti-malware scan reports can also show when the software has dealt with malware infections and so demonstrate its effectiveness in protecting the system from them. The issue with using logs to check the effectiveness of the protection is that they only show where the protection has worked – if the protection is ineffective, then the logs will show nothing.

A system manager should always be looking for ways to improve the protection applied to the system. This should involve keeping up to date with new issues and vulnerabilities by using the many internet resources available on this topic. In this way, the system manager can stay informed about emerging threats and make recommendations for further improvements to the security protection. Systems managers may also consider the use of active testing techniques such as employing ethical hackers to attempt to gain access to the system and therefore help to assess the degree to which the system is protected.

Reflect

Assessment practice 7.2 has a number of stages to it, some of which are quite complex. When working on any big project, timescales are important and it will be essential that you complete the final assignment for this unit by the deadline date. It is important to develop time management skills.

Create an action plan for the assessment practice tasks, in which you break each task down as far as possible into subtasks and try to estimate how long each subtask will take. From this, you should be able to create a plan that sets completion deadlines for each task and shows you how much time you need to dedicate to each task. You will need to monitor your progress on the assessment practice activites against your plan. You may not be able to complete every task within the time allocated but it is important that you do not fall too far behind because it can be very difficult to catch up.

Assessment practice 7.2

C.P5 C.P6 D.P7 D.P8 C.M3 D.M4 CD.D2 CD.D3

Following the presentation you gave to the company directors about IT security, you have been asked to create a plan to protect a test system and then implement the plan. The system needs to be protected from both internal and external threats. You need to complete the following tasks.

- Produce a plan to protect the test system from IT security threats that explains how the protection methods will defend the system.
- Write a justification of the protection methods you have chosen in the plan, showing how they will defend the system from threats.
- Set up the test system and apply the security protection methods as described in your plan.
- Test the security protection methods you have applied and enhance them, based on the testing you have performed.
- Write an evaluation of the plan and its implementation that considers how effective the protection methods you have applied are likely to be.

Plan

- What is the task? What am I being asked to do?
- How confident do I feel in my own abilities to complete this task? Are there any areas I think I may struggle with?

Do

- I know what I am doing and what I want to achieve.
- I can identify when I have gone wrong and adjust my thinking/approach to get myself back on course.

Review

- I can explain what the task was and how I approached the task.
- I can explain how I would approach the hard elements differently next time (i.e. what I would do differently).

Further reading and resources

Websites

- BBC News Technology section – technology news, including cases of significant cyberattacks:
  www.bbc.co.uk/news/technology
- The Information Commissioner's Office website – gives case studies of action taken under the Data Protection Act:
  ico.org.uk/
- McAfee's security advice centre – provides useful and up-to-date information on security, virus attacks and viruses, written in a reasonably accessible manner:
  home.mcafee.com/advicecenter/
- Microsoft's security advice centre – features a regularly updated blog and FAQ on security issues:
  www.microsoft.com/security/
- Norton™'s security centre – provides articles on security, spam email, software piracy etc.:
  uk.norton.com/security-center/
- Bletchley park, the nation Museum of Computing and wartime code breaking centre:
  http://www.bletchleypark.org.uk/
- YouTube – search for video presentations on public-key encryption:
  www.youtube.com

THINK FUTURE

Imran Hussain, Apprentice IT technician

After school, I managed to obtain an apprenticeship in a medium-sized business working in the IT support department. Although I was aware that security is a big issue, I was quite surprised at the amount of helpdesk requests that are related to security. Security issues create a lot of headaches for users in all sorts of ways. We have to do a lot of password resets because users have forgotten their passwords, which is frustrating for both the users and us, but the company policy is that users must change passwords every 3 months. Some users feel like we are making life difficult for them, but the important thing for us is protecting sensitive data and the company systems.

After 6 months, I moved off first-line support which means no more password resets, but I now have to deal with much more complex and technical issues. One thing that I have learnt is that many security issues, such as firewall configuration and setting folder permissions, are very complex and unless you know what you are doing you can cause a lot of problems. I have learnt a lot, but there is still a lot more to learn. The management here are very concerned about IT security issues and regularly remind us that new, more sophisticated threats are likely to appear in the future so the situation is only going to get worse and we need to be constantly on our guard.

Focusing your skills

Planning to work in computing

Security is likely to be an issue in whatever computing role you have in mind for the future. If you are planning to work in technical computing roles such as programming or web development, or as an IT technician, then your understanding of IT security needs to go beyond the 'user' aspects of security, such as strong passwords and anti-malware measures. If you are working in web or software development security, then it is a particularly important issue because you need to understand how to build security into the products that you are developing.

- As IT security is such a dynamic area, you need to keep up to date with the latest security issues. Following technology blogs is one way of doing this. There are many different technology blogs – some of the best known are Techdirt, Guardian technology, Techworld and Krebs on Security.
- Do your own research into security issues and aim to develop an in-depth technical understanding of how some of the common threats, such as SQL injection, work. There is plenty of information on all the common threats available on the internet.
- If you are able to obtain it, work experience (or shadowing) has many benefits and will provide very useful experience that is difficult to obtain in any other way. It will help you to understand security issues from both the user's and the technician's perspective. As Imran has found in his work as an apprentice IT technician, users can often find security issues very frustrating, so you need to develop the interpersonal skills required to deal with users who may be upset and angry.

Getting ready for assessment

Amber is working towards a BTEC National in Computing. She was given an assignment which asked her to create a presentation about IT security threats and encryption for a company where she is working in IT support. This covers learning aims A and B. Amber shares her experiences below.

How I got started

First, I listed all the things I needed to do to complete the assignment and I created a time plan to ensure that I completed the assignment on time. I checked my progress against the time plan at regular intervals. Then I created an overall structure for the presentation listing the main things I needed to cover. These were:

- the different threats than can affect the IT systems of the company
- the principles of information security with examples relating to the company
- legal issues related to IT security and the company
- the principles of cryptography and how it can be used to protect data
- an analysis of the impact that security breaches could have on the company
- an evaluation of the methods the company can use to protect itself from IT security threats.

I collected all my class notes on these topics into a folder and divided them up into the sections listed above. I then chose a PowerPoint® slide template and created title slides for each section. I found that this approach worked well as it gave me a structure around which to build the presentation.

How I brought it all together

I worked through my notes for each section and used a highlighter pen to pick out the main points. I used these as the bullet points on each slide of my presentation, making sure that I didn't have more than about 5 or 6 small bullet points on each slide, otherwise the text would become too small to read. I also checked that I just had the main points on the slides and I rewrote the rest of the text from my notes into the slides notes section, rewording them as if I was talking to an audience. I also added some further screenshots to illustrate the text.

What I learned from the experience

I found that the notes I made in class were fine on some topics but too brief on others. I wish I had been more consistent in my note taking as I had to spend quite a lot of time doing research to find out about some topics which had been covered in class but for which my notes were not adequate. I found completing the last section – the evaluation – hard to write. My first attempt was really just an explanation of the techniques that the company could use to protect their systems. I had to take each protection technique and think hard about how effective it might be and what issues it might cause, such as performance problems or usability issues. In the end, I decided that this was hard to cover in the presentation slides themselves and that I needed to write the evaluation mostly in the slide notes.

Think about it

- Are you taking class notes and collecting the handouts that your teacher has given you? These will be really helpful when you come to write your assignments, so keep them safe and organised in a folder.
- There is a lot of information about IT security on the internet. You can use this in your assignments but check that it is up to date as this is a rapidly changing sector. You can use direct quotes only if you clearly reference them, otherwise you will need to rewrite the information you find in your own words.

Making a plan for completing your assignments is important. You must hand your assignment in on time, so creating a plan with timings can help you to ensure that you have everything ready in time.