14.5 Networks: Network security, audit and accounting

- Understand the particular security, audit and accounting problems associated with networks and recall the steps which can be taken to preserve security.
- Describe the measures taken to protect network traffic against illegal access.
- Understand the reasons for using audit software in providing a network service.
- Understand the reasons for using accounting software in providing a network service.

Network environments: Understand how a network environment affects the user interface provided, e.g. security, control of software, control of files, access rights.

14.5 Networks Security

Network security:

Every organisation must takes steps to protect data from being accessed and seen by unauthorised personnel (privacy), and from being stolen, deleted or altered by un-authorised personnel (security). Steps taken include:

Training users about security:

Staff should be aware of a company's security police and the risks of storing data on computer networks. For example:

- Downloading programs across Internet can pose a threat from viruses.
- Leaving machines logged on during breaks can be a security risk.
- Allowing strangers near computers can be a security risk.

Access rights and permissions

The main method of controlling access to data held on a network is by defining access rights (privileges) for users. There are several different types of access right:

- 'Directory and File Access Rights'. These specify exactly what directories can be access and what data files can be read or modified by users.
- Program Access rights'. These specify what programs a user is allowed to run.
- 'Machine Access rights' used to restrict log-on of users to certain network stations.
- 'Time Access rights' used to restrict log-on of users to certain periods of the day.
- 'Machine / File Access Rights'. These are used to limit the running of programs to specified terminals.

File Access Rights:

Files can also be assigned with their own access rights.

e.g. For data files:

- Read only files: (Library files with copy right.)
- Read and copy files. (Amendments allowed after copying.)

- Write only files. (Used to collect data but to keep existing data hidden)

e.g. For program files:

- Execution only files (e.g. non viewable programs.)
- Read and modify (Program under development.)

Note: File Access rights are implemented on a school system. This make it impossible for user to delete programs and change the way a machine works.

Access rights are normally assigned by the network manager (or database Administrator), who by virtue of the log o code status has access to every file on the system.

Log-On codes and Password (What you know)

Access controls are used to prevent users from gaining access to a network in the first place. Log on codes and passwords are a primary method of access control. Different log on codes can be used to allow access to data at different levels. e.g. A log on code used by a doctor may allow them to see the medical history of patients whereas the log-on code of a clerk may only allow access to the name and address of patients for the purpose of booking appointments.
Users may share their own passwords or may share a group password. They may also be given the right to change their password. Some systems force the user to change a password every so often for security reasons. When choosing a password it is important to select a group of characters that can't be guessed. Using upper and lower case and including digits is one useful method of making passwords hard to crack.

Passwords and log on codes are stored inside the computers in a password file. When a user enters their log-on code, the operating system looks up the code, and finds the matching password. It is important to provide adequate security for the password file so that it does not fall into the hands of everyday users.

Computers normally offer users a limited number of tries to get their password correct. This is to ensure that users cannot sit at a terminal all day (possible at home through the use of a modem) trying to break in to the system. This said, some users have programmed their computers to auto-dial computer installations over several days or weeks and to keep trying different combinations of codes until they at last hit a successful combination. To monitor such attempts to break into computer systems some managers now make use of Audit / Activity Logs. (see later notes)

Other type of Access controls include:

- ID Cards - (What you posses) – e.g. to prevents access to computer rooms.
- Call back systems - (Where you are) – when you dial into to a computer by modem – the computer prevents access but calls you back on a fixed telephone number. This limits users to calling from a fixed destination.
- Biometric identification: (Who you are) e.g. Finger print – retinal image and voice print recognition.

Auditing and network management software:

- Various software utilities are available to help monitor, and maintain a network:
- Very often these come as part of the operating systems (e.g. Windows)
- Audit controls / Activity Logs These track and log all the activities performed (and attempted) on a network by each user. e.g.
- Number of log on attempts and passwords tried / time of day and station No.
- programs run or data files modified / time of day and station No..
- Number of pages printed by user.
- Amount of disk spaced currently used by user.
- Totals time logged on to a computer.

Reasons for using 'Audit' software:

By listing the Activity log a network manager can tell:

- whether unauthorised people are trying to break into the system.
- check on the amount of time or other resource a user has used.
-

Where users pay for computer access the audit data is built into the charging algorithm.(this is how BT charge for telephone call time)

e.g. Internet charges could be based upon:

- Access time (i.e. time 'logged on')
- Number of print pages printed
- Amount of disk space used,
- Number of C.P.U processing cycles used on a server.
-

Note: Audit software is sometimes called Accounting software because it performs an accounting function. Don't confuse this with software like Sage, for doing business accounts.

However, accounting software also covers:

Organisations that provide other organisations with network services and charge for network use. The charge depends on:

- Time logged on;
- Processing time;
- Resources used (such as disk space or printer);
- Time of day.

Like auditing software, patterns of usage can be monitored to encourage users to use the system at less busy times of the day. It can also help administrators to decide whether extra resources are used.

Performance Management software:

Network monitoring software is used to help a networks manager monitor the performance of a network so they can plan and make sensible upgrades. e.g. It can be used to measure:

- Response time (e.g. Time the server takes to respond to a station request.)
- Network traffic levels (e.g. Speed, and amount of data flowing down the networks cable % usage figures.).

- Utilisation (Amount of use) of hardware, like disk drive and printers.
- Utilisation of software (number of times software is run by users.)

e.g. 1. Internet example: Checking the number of time an Internet site is visited.
e.g. 2 Windows example: Getting windows to report a hard disk utilisation.
These will help in the management and planning of a network. Bottlenecks can be identified and sorted out. If more copies of software are being used than allowed by the licence, then action can be taken.

Firewall security:

Firewall software is designed to prevent unauthorised communication in or out of a network via a modem. It is usually run on the 'gateway' hardware, that permits access to the Internet. E.g. A proxy server: (This is the computer that contains the modem attached to our I.S.P. that then feeds web pages into our network). The software is used to allow remote users access to parts of the network while denying access to sensitive data.

Encryption

Data passing through a wire or as a radio signal are vulnerable to interception. Such data can be scrambled or **encrypted** to make sure they are meaningless to everyone else other than the intended recipient.

Encryption is nothing new; the Enigma machine used by the Germans in the Second World War were sophisticated devices. And it took a sophisticated electro-mechanical computer, Collosus, to crack them. Collosus was faster at decoding Enigma than a Pentium Processor, so it was a pretty good machine. (Many historians state that the Germans were good soldiers, but had a blind spot about the value of good intelligence. The Allies were good at intelligence which won the war.)

There are different ways of encrypting data based on:

- **transposition** where characters are moved about;
- **substitution** where one character stands for another.

The transmitting computer sends a decoding or decryption **cipher** or key so that the encrypted message can be decoded. In practice there needs to be quite a complex set of ciphers, so that the code is not broken easily. **Cryptography** is important in the security of transmitted data:

- It identifies authentic users;
- It prevents alteration of the message;
- It prevents unauthorised users from reading the message.