TRENDS IN COMPUTING

In this topic, we observe the following aspects:

1. Computer Security ethics and Privacy

A computer security risk is any event or action that could cause a loss or damage to computer hardware, software, data, or information.

a) Some abuses to computer security are accidental, but some are planned.

b) Any illegal act involving a computer is generally referred to as a computer crime.

c) Cybercrime refers to online or Internet-based illegal acts.

2. Internet and network attacks

a) **Viruses**: is a small piece of software that is attached on real programs and disorganizes their mode of operation. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs).

b) **E-mail viruses**: An e-mail virus travels as an attachment to e-mail messages, and usually reproduces itself by automatically mailing itself to a number of people in the victim's e-mail address book. Some e-mail viruses don't even require a double - click -- they launch when you view the infected message in the preview pane of your e-mail software.

c) **Trojan horses**: is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.

d) **Worms**: is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

e) A **rootkit** is a stealthy type of software, often malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer

3. Denial of service attacks

A type of attack conducted over the Internet, using the combined resources of many computers to attack, and often crash, a targeted computer system or resource (e.g., a program, website or network).

An example of how a DDoS attack is conducted: an attacker will exploit vulnerability in one computer system and make it the DDoS master using Remote Control Software. Later, the intruder will use the master system to identify and manage zombies that can perform the attack.

There is no single DoS attack method, and the term has come to encompass a variety of different forms of attack, a number of which are outlined below:

- ✓ **Ping flood** - This attack uses the Internet Message Protocol (ICMP) *ping* request to a server as a DoS method. The strategy either involves sending ping requests in such larger quantities that the receiving system is unable to respond to valid user requests, or sending ping messages which are so large (known as a *ping of death*) that the system is unable to handle the request.

- ✓ **Smurfing** - it makes use of the TCP Internet Message Protocol (ICMP) *ping* request to mount DoS attacks. In a typical smurfing attack the attacker sends a ping request to the broadcast address of network containing the IP address of the victim. The ping request is sent to all computers on the broadcast network, which in turn all reply to the IP address of the victim system thereby overloading the victim with ping responses.

- ✓ **TCP SYN Flood** - Also known as the *TCP Ack Attack,* this attack leverages the TCP three way handshakes to launch a DoS attack. The attack begins with a client attempting to establish a TCP connection with the victim server. The client sends a request to the server, which in turn returns an ACK package to acknowledge the connection.

  At this point in the communication the client should respond with a message accepting the connection. Instead the client sends another ACK which is responded to by the server with yet another ACK. The client continues to send ACKs to the server with the effect of causing the server to hold sessions open in anticipation of the client sending the final packet required to complete the connection.

  As a result, the server uses up all available sessions serving the malicious client, thereby preventing access to other users.

- ✓ **Fraggle** - A fraggle attack is similar to a *smurfing attack* with the exception that the User Datagram Protocol (UDP) is used instead of using ICMP.
- ✓ **Land** - Under a Land attack the attacker creates a fake SYN packet contain the same source and destination IP addresses and ports and sends it to the victim causing the system to become confused when trying to respond to the packet.

- ✓ **Teardrop** - A teardrop type of DoS attack exploits a weakness in the TCP/IP implementation on some operating systems. The attack works by sending messages fragmented into multiple UDP packages. Ordinarily the operating system is able to reassemble the packets into a complete message by referencing data in each UDB packet. The teardrop attack works by corrupting the offset data in the UDP packets making it

impossible for the system to rebuild the original packets. On systems that are unable to handle this corruption a crash is the most likely outcome of a teardrop attack.

- ✓ **Bonk** - An effective attack on some Windows systems involving the transmission corrupted UDP packets to the DNS port (port 53) resulting in a system crash.

- ✓ **Boink** - Similar to the *Bonk* attack except that the corrupted UDP packets are sent to multiple ports, not just port 53 (DNS).

Back Door Attacks

Back Door attacks use programs that provide a method for entering a system without going through the usual authentication process. This can either take the form of hidden access points deliberately put into application by the original developers to help in maintaining and debugging the software or a malicious program that is placed on a system through a virus, or other method which opens up the system to unauthorized access.

A number of back door programs have been discovered over the years, some which are listed below:

a) **Back Orifice -** This rather distastefully named tool was developed by a group known as the Cult of the Dead Cow Communications. The primary purpose of Back Orifice is to provide remote access to a server for the purposes of performing administrative tasks.

b) **NetBus** - Similar to Back Orifice, NetBus is also designed to enable remote administrative access to Windows system.

c) **Sub7** - Sub7 is yet another illicit back door program designed to allow unauthorized access to systems.

Whilst the installation of any of the above back door programs on a system will have serious implications for security, all these threats can be effectively prevented through the implementation of a complete virus scanning strategy.

Spoofing

The basis of spoofing involves hiding as a trusted system in order to gain unauthorized access to a secure environment. IP spoofing involves modifying data to make it appear to originate from the IP address of a system that is trusted by a server or firewall. Using this approach, a host is able to pass through the IP filtering that would otherwise serve to prevent access.

Man in the Middle Attacks

Man-in-the-middle attacks are perhaps one of the more complex and advanced forms of security breaching approaches. As the name implies, such an attack involves the secret

assignment of a software agent between the client and server ends of a communication. In this scenario neither end of the communication is aware that the malicious agent is present in the line of communication.

Man-in-middle attacks have increased considerable since the introduction of wireless networking. Now there is no need for the rogue to connect to a wire, instead the data can simply be intercepted from anywhere within range of the wireless signal (such as in the parking lot outside an office or the road in front of a house). The best way to avoid such attacks is to use encryption and secure protocols in all communications.

Replay Attacks

In a replay attack an agent is once again placed within the client / server line of communication. In the case of a Replay attack, however, the transaction data is recorded for the express purpose of allowing the data to be modified and replayed to the server at a later time for nefarious purposes. For example, a replay attack might record the entire process of a user logging into a banking web site and performing transactions. The recorded transcript may then be replayed to repeat the login sequence for the purposes of stealing money from the account.

TCP/IP Hijacking

TCP/IP Hijacking occurs when an attacker takes control of an ongoing session between a client and a server. This is similar in to a man-in-the-middle attack except that the rogue agent sends a reset request to the client so that the client loses contact with the server while the rogue system assumes the role of the legitimate client, continuing the session.

Mathematical Attacks

The solution to a number of the types of attack outlined above has involved the use of encryption. A mathematical attack involves the use of computation based on the mathematical properties of the encryption algorithm to attempt to decrypt data. The best way to avoid the decryption of data is to use strong encryption (128-bit) rather than rely on weaker encryption (both 40-bit and 56-bit encryption can easily be broken).

Password Guessing

On systems which rely solely on a login name and password the security of the entire system is only as strong as the passwords chosen by the users. The best way to ensure passwords are not cracked is to avoid the use of simple words or phrases which can be found in a dictionary. This needs to be balanced with making the passwords easy enough to remember so that users do not write them on pieces of paper and stick them on their laptops or monitors for others to find.

The best passwords consist of a mixture of upper and lower case characters combined with numbers and special characters. A common approach is to substitute numbers in place of similar letters. For example **W3ath3rN3ws** uses the number 3 in place of the letter 'E', the reasoning being that the number 3 is much like a reversed 'E' making the password easy to remember. Unfortunately most password cracking algorithms know about this type of substitution.

There are two primary mechanisms for breaking password protection, brute force and dictionary.

Brute Force Password Attacks

A brute force attack uses algorithms to systematically try every possible version of characters in an effort to find the correct password. If allowed to continue, a brute force attack will eventually identify the correct password, although a well implemented security plan will disable the account and block the IP address from which the attempts were made after 3 or 4 failed password attempts.

Dictionary Password Attacks

Dictionary password attacks take advantage of the fact that many user simply rely on easy to remember words as their passwords. A dictionary attack simply works through a list of words from a dictionary to see if any of them turn out to be a valid password. Such brute force programs also take into consideration such tricks as using the number 3 instead of the letter 'e' and the number 1 in place of the letter 'l'.

Password Cracking

Computer systems typically store the passwords which allow access to the system in a password file which is cryptographically protected from prying eyes. A number of password cracking programs are available for extracting the passwords from a password file.

4. Unauthorized access and use:

Unauthorized access is the use of a computer or network without permission.

A cracker, or hacker, is someone who tries to access a computer or network illegally.

Some hackers break into a computer for the challenge. However, others use or steal computer resources or corrupt a computer's data.

Unauthorized use is the use of a computer or its data for unapproved or possibly illegal activities.

Examples of unauthorized use of computers include

- ✓ An employee using a company computer to send personal e-mail.
- ✓ Someone gaining access to a bank computer and performing an unauthorized transfer.

- ✓ One way to prevent unauthorized access and unauthorized use of computers is to utilize access controls.

5. Hardware theft and vandalism:

Hardware theft is the act of stealing computer equipment. The act of defacing or destroying computer equipment is known as hardware vandalism.

Precautions to prevent hardware theft include

- ✓ Use physical access controls, such as locked doors, and windows.
- ✓ Use cables to lock the equipment to desk, cabinet, or floor.
- ✓ Install alarm systems for additional security.
- ✓ Never leave a notebook computer or handheld computer unattended in a public place.
- ✓ Use passwords, possessed objects, and biometrics as a method of security.
- ✓ Back up all the files stored on the computer regularly.

6. Software theft:

Two common forms of software theft are:

a) Physically stealing media (e.g., floppy disk, or CD-ROM) that contains software; and

b) Software piracy, which is the most common form of software theft. Software piracy refers to the unauthorized and illegal duplication of copyrighted software.

Software piracy is the most common form of software theft.
Purchasing software only provides a consumer with a license agreement, or the right to use the software.

a) A single - user license agreement or end-user license agreement is the most common type of license included with software packages purchased by individual users.

b) A software site license gives the buyer the right to install the software on multiple computers at a single site (e.g., a school computer laboratory).

c) A network site license allows network users to share a single copy of the software, which resides on the network server.

Risks of software piracy include

a) Increase the chance of spreading computer viruses.
b) No technical support for the software can be received.
c) Drive up the software cost for all legal users.

7. Information theft:

Information theft refers to someone steals personal or confidential information from others.

Reasons for information theft include

a) A company wants to learn about a competitor.
b) An individual steals credit card numbers to make fraudulent purchases.

Preventions for information theft include

c) Implement access control to computers and networks.

An access control is a security measure that defines

- ✓ Who can access a computer?
- ✓ When the users can access the computer?
- ✓ What actions the users can take while accessing the computer?

Access control is normally implemented using a two-phase process:

- ✓ Identification verifies whether the user is a valid one.
- ✓ Authentication verifies that the user is really the one he or she claims to be.

Four methods of identification and authentication exist, which include

a) User names and passwords

- ✓ Most multiuser operating systems require a user to enter the correct user name and password before accessing the data, information, and programs stored on a computer or network.
- ✓ Many other systems that maintain financial, personal, and other confidential information also require a user name and password as part of their logon procedure.
- ✓ Some systems assign the user names and even passwords to their users, but some systems allow their users to choose their own user names and passwords.

b) Possessed objects: A possessed object is any item that a user must carry to gain access to a computer or computer facility.

Examples of possessed objects include badges, cards, and keys.

- ✓ Possessed objects are often used in combination with personal identification numbers.
- ✓ A personal identification number (PIN) is a numeric password, either assigned by a company or selected by a user.
- ✓ PINs provide an additional level of security.

c) Biometric devices: authenticates a person's identity by verifying personal characteristics (e.g., fingerprints).

It translates a personal characteristic into a digital code that is compared with a digital code stored in the computer.

Examples of biometric devices include

- ✓ A fingerprint scanner, which captures curves and indentations of a fingerprint.
- ✓ A hand geometry system, which can measure the shape and size of a person's hand.
- ✓ A face recognition system, which captures a live face image and compares it with a stored image.
- ✓ A voice recognition system, which compares a person's live speech with their stored voice pattern.
- ✓ A signature verification system, which recognizes the shape of handwritten signature of a person.
- ✓ An iris recognition system, which reads patterns in the tiny blood vessels in the back of the eye, which are as unique as a fingerprint.

Advantages of biometric devices include

- ✓ Personal characteristics are unique and cannot be forgotten or misplaced.

Disadvantages of biometric devices include

- ✓ Most of the biometric devices are expensive.
- ✓ A fingerprint scanner might reject a legitimate user if the user cuts his or her finger.
- ✓ Hand geometry readers can transmit germs.
- ✓ A signature might not match the one on file when the person is nervous.
- ✓ A voice recognition system might reject a legitimate user with a sore throat.

d) Callback system: A biometric device authenticates a person's identity by verifying personal characteristics (e.g., fingerprints).

It translates a personal characteristic into a digital code that is compared with a digital code stored in the computer.

A company should:

- Maintain a log that records in a file both successful and unsuccessful access attempts.
- Investigate unsuccessful access attempts immediately to ensure they were not intentional breaches of security.

- Review successful access for irregularities, such as use of the computer after normal working hours or from remote computers.

- Have written policies regarding the use of computers by employees for personal reasons.

- Document and explain the policy of computer use to employees.

- Use encryption techniques

8. System failure

A system failure is a prolonged malfunction of a computer that can also cause hardware, software, data, or information loss.

Common causes of system failure include

- Aging hardware
- Natural disaster (e.g., fires, floods, storms, or earthquakes)
- Electrical power variation

Electrical power variations can cause loss of data or equipment.

A single power disturbance can damage multiple systems in a computer network.

Electrical power disturbances include

- Noise is any unwanted signal, usually varying quickly, which is mixed with the normal voltage entering the computer.
- An under voltage occurs when the electrical supply drops (i.e., below 220 volts in Hong Kong).

- An overvoltage, or power surge, occurs when the incoming electrical power increases significantly above the normal 220 volts.

✓ A surge protector can be used to protect computer equipment against under voltage and overvoltage.

✓ Many users also connect an uninterruptible power supply to the computer for additional electrical protection.

- ✓ Files should be backed up regularly to prevent against data loss caused by a system failure.

9. Backing up

A backup is a duplicate of a file, program, or disk that can be used if the original is lost, damaged, or destroyed. Files can be restored by copying the backed up files to their original location on the computer.
Backup copies should be kept in a fireproof and heatproof safe or offsite.

Three types of backup that can be performed are

a) Full backup, which copies all of the files in the computer.

b) Differential backup, which copies only the files that have changed since the last full backup.

c) Incremental backup, which copies only the files that have changed since the last full or last incremental backup.

Some users implement a three-generation backup procedure to preserve three copies of important files.

a) The grandparent is the oldest copy of the file.
b) The parent is the second oldest copy of the file.
c) The child is the most recent copy of the file.

10. Wireless security

Wireless networks are much more at risk to unauthorized use than cabled networks. Wireless network devices use radio waves to communicate with each other.

Unencrypted information transmitted can be monitored by a third-party, which, with the right tools (free to download), could quickly gain access to your entire network, steal valuable passwords to local servers and online services, alter or destroy data, and/or access personal and confidential information stored in your network servers.

To minimize the possibility of this, all modern access points and devices have configuration options to encrypt transmissions. These encryption methodologies are still evolving, as are the tools used by malicious hackers, so always use the strongest encryption available in your access point and connecting devices.

Three basic techniques are used to protect networks from unauthorized wireless use. Use any and all of these techniques when setting up your wireless access points:

1. Encryption

Enable the strongest encryption supported by the devices you will be connecting to the network. Use strong passwords (strong passwords are generally defined as passwords containing symbols, numbers, and mixed case letters, at least 14 characters long).

2. Isolation

Use a wireless router that places all wireless connections on a subnet independent of the primary private network. This protects your private network data from pass-through internet traffic.

3. Hidden SSID

Every access point has a Service Set IDentifier (SSID) that by default is broadcast to client devices so that the access point can be found. By disabling this feature, standard client connection software won't be able to "see" the access point. However, the eves-dropping programs can easily find these access points, so this alone does little more than keep the access point name out of sight for casual wireless users.

11. Computers and health risks

Prolonged computer usage can lead to health risks such as

a) Eye strain
b) Back pain due to poor sitting posture
c) Electromagnetic radiation especially with CRT monitors
d) Addiction from use
e) Wrist pain to do non-ergonometric
f) Repetitive Strain Injury(RSI)
g) Headaches
h) Neck pain
i) Stress due to noise from fans, printers, power inputs
j) Ear problems for use of ear phones especially with embedded systems

Precautions to help prevent such risks include

a) Pay attention to sitting posture.
b) Take a break to stand up, walk around, or stretch every 30 to 60 minutes.
c) Place the display device about an arm's length away from the eyes with the top of the screen at eye level or below.
d) Adjust the lighting in the room.
e) Ensure that the workplace is designed ergonomically. Ergonomics means incorporating comfort, efficiency, and safety into the design of items in the workplace.

- Some keyboards have built-in wrist rests.

- Most display devices have a tilt-and-swivel base and controls to adjust the brightness, contrast, positioning, height, and width of images.

- Most CRT monitors today also adhere to the MPR II standard, which defines acceptable levels of electromagnetic radiation.

12. **Computer ethics**

Are the moral guidelines that govern the use of computers and information systems.

Frequently concerned areas of computer ethics are

a) Unauthorized access and use of computer systems

b) Software piracy

c) Information privacy: Information privacy refers to the right of individuals or organizations to deny or restrict the collection and use of information about them.

d) Information accuracy: Information accuracy becomes an important issue when it is necessary to access information maintained by other people or companies, such as that on the Internet. Inaccurate input can result in erroneous information and incorrect decisions made based on that information. Never assume that information provided on the Web is always correct.

   The Web site providing access to the information may not be the creator of the information. Always evaluate the content provided on a Web page before using it.

   Some people also concerned with using computers to alter output, particularly graphical images (e.g., retouching a photograph). They believe that even the slightest alteration could lead to deliberately misleading photographs.

Intellectual property rights

Intellectual property (IP) refers to work created by inventors, authors, and artists. Intellectual property rights are the rights to which creators are entitled for their work.

- ✓ A copyright gives authors and artists exclusive rights to duplicate, publish, and sell their materials.
- ✓ A common infringement of copyright is software piracy.
- ✓ Copyright law usually gives the public fair use to copyrighted material (e.g., for educational purposes). However, this vague definition is always subject to widespread interpretation.
- ✓ A trademark protects a company's logos and brand names.

Codes of conduct

A code of conduct is a written guideline that helps determine whether a specific action is ethical or unethical.

Codes of Conduct

A code of conduct is a voluntary set of rules which people agree to follow or abide by.

Codes of Conduct are not legally binding but once someone agrees to abide by it, then it is considered binding.

Codes of Conduct related to ICT might cover things such as usage of the Internet, for example, the internet should not be used during work time to shop online or book holidays. It would probably cover downloading and viewing pornographic material at work or gambling online during work time.

Other things that are often covered by Codes of Conduct are the security and use of user names and passwords, for example, not leaving your workstation logged on if you are not present or not telling anyone else your password.

A sample IT code of conduct include

a) Computers may not be used to harm other people.
b) Users may not interfere with other's computer work.
c) Users may not meddle in other's computer files.
d) Computers may not be used to steal.
e) Computers may not be used to bear false witness.
f) Users may not copy or use software illegally.
g) Users may not use other's computer resources without authorization.
h) Users may not use other's output.
i) Users shall consider the social impact of programs and systems they design.
j) Users should always use computers in a way that demonstrates consideration and respect for other people.

Information privacy

Or data privacy is the relationship between collection and distribution of data, technology, the public expectation of privacy, and the legal and political issues surrounding them. This includes the following:

a) Electronic profiles

Involves keeping details concerning online user of a specific service or product. It involves, writing personal details so as to be allowed to use the service. Remember how you obtained

your e-mail address; you filled a form related to your profile. This profile is never viewable by third parties unless otherwise.

b) Cookies

A cookie, also known as an HTTP cookie, web cookie, or browser cookie, is usually a small piece of data sent from a website and stored in a user's web browser while a user is browsing a website. When the user browses the same website in the future, the data stored in the cookie can be retrieved by the website to notify the website of the user's previous activity

c) Spam

Spam is the use of electronic messaging systems to send unwanted bulk messages, especially advertising, at random. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media.

d) Phishing

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by hiding as a trustworthy unit in an electronic communication.

e) Pharming

Is an attacker's attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a weakness in DNS server software. DNS servers are computers responsible for resolving Internet names into their real IP addresses. Pharming requires unprotected access to target a computer, such as changing a customer's home computer, rather than a corporate business server.

f) Spywares

Spyware is a type of malicious program installed on computers that collects information about users without their knowledge. The presence of spyware is typically hidden from the user and can be difficult to detect. Some spyware, such as keyloggers, may be installed by the owner of a shared, corporate, or public computer intentionally in order to monitor users.

Spyware can collect almost any type of data, including personal information like Internet surfing habits, user logins, and bank or credit account information. Spyware can also interfere with user control of a computer by installing additional software or redirecting Web browsers. Some spyware can change computer settings, which can result in slow Internet connection speeds, un-authorized changes in browser settings, or changes to software settings.

g) Adware

Adware, or advertising-supported software, is any software package which automatically renders advertisements in order to generate revenue for its author. The advertisements may be in the user interface of the software or on a screen presented to the user during the installation process.

The functions may be designed to analyze which Internet sites the user visits and to present advertising relevant to the types of goods or services featured there. The term is sometimes used to refer to software that displays unwanted advertisements.

h) Privacy laws

Privacy law refers to the laws which deal with the regulation of personal information about individuals which can be collected by governments and other public as well as private organizations and its storage and use. Privacy laws are considered in the context of an individual's privacy rights or reasonable expectation of privacy.

i) Social engineering

In the situation of security, it is understood to mean the art of influencing people into performing actions or revealing confidential information.

j) Employee monitoring

- **E-mail scanning**: is a process in which incoming and outgoing mail passes through E-mail filtering software to search for content which may violate the policies of the employer.
- **Video surveillance:** One of the most effective forms of employee monitoring is through the use of Video surveillance equipment. Video feeds of employee activities are fed back to a central location where they are either recorded or monitored live by another person. "This is a benefit because it provides an unbiased method of performance evaluation and prevents the interference of a manager's feelings in an employee's review.

- **Location monitoring:** For employees that do not work in a static location, supervisors may chose to track their location. Common examples of this are delivery and transportation industries. In some of these cases the employee monitoring is minor as the location is tracked for other purposes, such as determining the amount of time before a parcel will be delivered, or which taxi is closest.

- **Employee privacy and ethical issues:** From an ethical point of view, the employee does not give up all of his or her privacy while they are in their work environment. Privacy can become a moral matter, but it is important to know what the employee and employer rights are. The ethical challenge that companies face involves protecting their interests

through Internet monitoring while ensuring they don't go so far that employees lose all sense of privacy in the workplace.

- **Legal issues:** It is illegal to perform invasive monitoring, such as reading an employee's emails, unless it can be shown that it is a necessary precaution and there are no other alternatives. Everyone in the conversation must give consent before the conversation can be recorded. It requires that monitored conversations have a beep at certain intervals or there must be a message informing the caller that the conversations may be recorded, take note that this is not informing the company representative which calls are being recorded. *The following uses of employee information are generally considered legal:*

✓ Find needed business information when the employee is not available.
✓ Protect security of proprietary information and data.
✓ Prevent or investigate possible criminal activities by employees.
✓ Prevent personal use of employer facilities.
✓ Check for violations of company policy against sending offensive or pornographic email.
✓ Investigate complaints of harassment.
✓ Check for illegal software.

- **Security:** In some cases, monitoring an employee's work leads to monitoring the employee's life in aspects that are not related to work. This leads to acquisition of information about the employee, compromising the security of the employee.

k) Content filtering

Content-control software, content filtering software, secure web gateways, censorware, and web filtering software are terms for software designed and optimized for controlling what content is permitted to a reader, especially when it is used to restrict material delivered over the Internet through the Web, e-mail, or other means. Content-control software determines what content will be available or perhaps more often what content will be blocked.

Revision questions

1. (a). Define the term computer security ethics and privacy.
   (b). Outline any five internet and network attacks.

2. (a). What are denial of service attacks?
   (b). Write short notes on the following:
   i.) Ping flood.
   ii.) Smurfing.
   iii.) Fraggle.
   iv.) Tear drop.
   v.) Bonk.

3. (a). What are back door attacts?

(b). List three back door programs in common use.

4. (a). Distinguish between hacking and cracking.
   (b). Outline possible measures needed to control dangers of both hacking and cracking.
5. (a). Define the term data backup.
   (b). Outline the three forms of data backup techniques.

6. (a). Outline seven dangers as a result of continued computer use.
   (b). Suggest possible ways of controlling dangers mentioned in (a) above.

7. (a). Define the term information privacy.
   (b). Describe eight tools used for information privacy.

8. (a). Distinguish privacy laws and social engineering.
   (b). Explain five ways of monitoring an employee in an organisation.