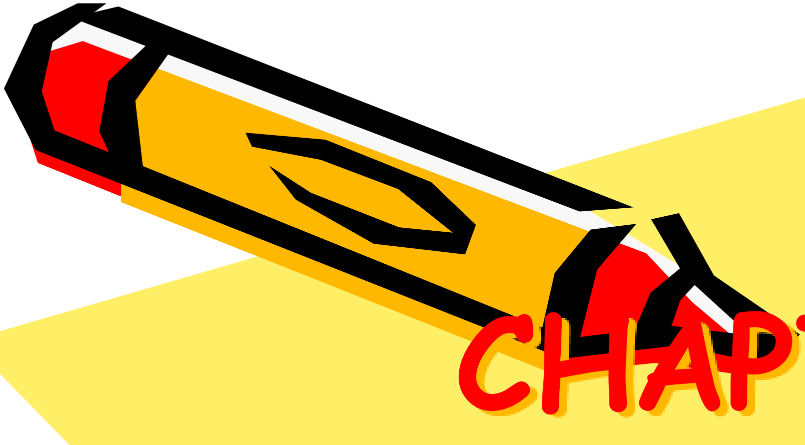


CHAPTER TWO: INFORMATION SECURITY IN COMPUTER AND COMMUNICATION SYSTEMS

Objectives of information systems security

1. Objectives of information systems security

- ❑ The purpose of computer security is to devise ways to prevent the weaknesses from being exploited. Understanding the preventive measures makes most sense.
- ❑ Five important aspects of any computer-related system:
  - a. **confidentiality,**
  - b. **integrity,**
  - c. **availability,**
  - d. **authentication and**
  - e. **non- repudiation.**

a) Confidentiality

- This ensures that information held in the computer can only be accessed by the people who should access it i.e. intended person.
- Confidentiality ensures that computer-related assets are accessed only by authorized parties.

Objectives of information systems security

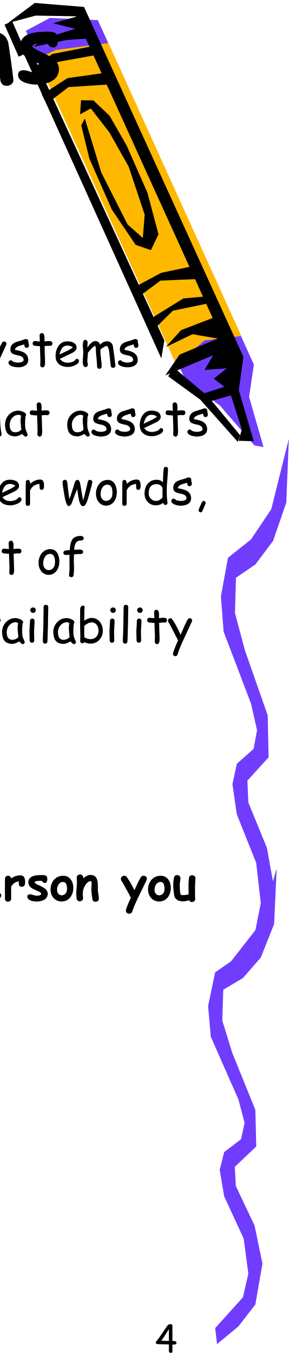
Confidentiality CONT….

- That is, only those who should have access to something will actually get that access. By "access," we mean not only reading but also viewing, printing, or simply knowing that a particular asset exists.
- Confidentiality is sometimes called
  - **secrecy** or
  - **privacy**.

b) Integrity

- Integrity ensures correctives of data i.e. data remains un-altered. Integrity means that assets can be modified only by authorized parties or only in authorized ways. In this context, modification includes writing, changing, changing status, deleting, and creating.

Objectives of information systems security

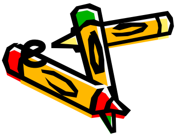


c) Availability

- ❑ Avoids denial of service attacks. This happens when legitimate systems users cannot access the systems resources. Availability means that assets are accessible to authorized parties at appropriate times. In other words, if some person or system has legitimate access to a particular set of objects, that access should not be prevented. For this reason, availability is sometimes known by its opposite, denial of service.

d) Authentication

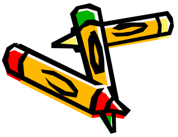
- ❑ A service related to identification i.e. is the data or the person you are dealing with the actual one.
- ❑ Authentication mechanisms include:
  - ➢ User name and passwords
  - ➢ Card based authentication
  - ➢ Biometric authentication



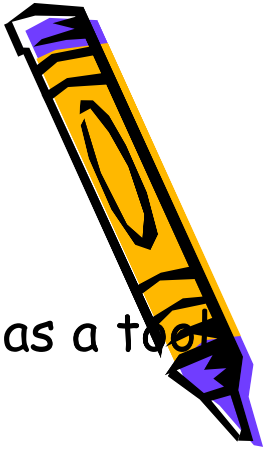
Objectives of information systems security

e) Non- repudiation

- □ This provides proof of a transaction to have taken place and prevents users who send online messages from denying their actions i.e. maintaining a log file
- □ Security in computing addresses these five goals.
- □ One of the challenges in building a secure system is finding the right balance among the goals, which often conflict. For example, it is easy to preserve a particular object's confidentiality in a secure system simply by preventing everyone from reading that object. However, this system is not secure, because it does not meet the requirement of availability for proper access. That is, there must be a balance between confidentiality and availability.



2. Computer crimes



2. Computer crimes

- ❑ This refers to any crime facilitated by use of a computer as a tool. Examples include:

i) Espionage

- the theft of original data by competitors.

ii) Hacking

- the illegal access in to a computer system for personal gain.

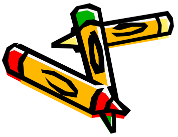
iii) Toll fraud

-This involves swindling companies and organizations i.e. making telephone calls by false pretenses using a fake coin.

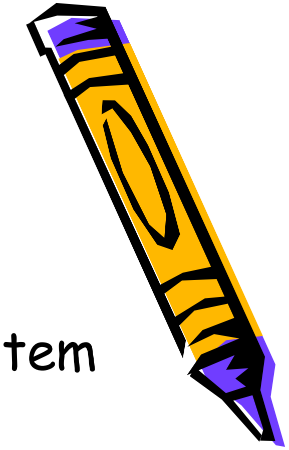
iv) Data diddling

- The use of computer systems by employees to forge documents or change data in the records for personal gain.

v)Software piracy-Illegal reproduction of copy writes software's.



3. Type of Threats



1 *Confidentiality threat*

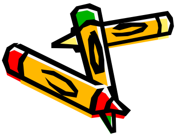
- Confidentiality means that the asset of a computing system is accessible only by authorized parties.
- The type of access is read-access: reading, viewing, printing, or even just knowing the existence of an object.

2 *Integrity threat*

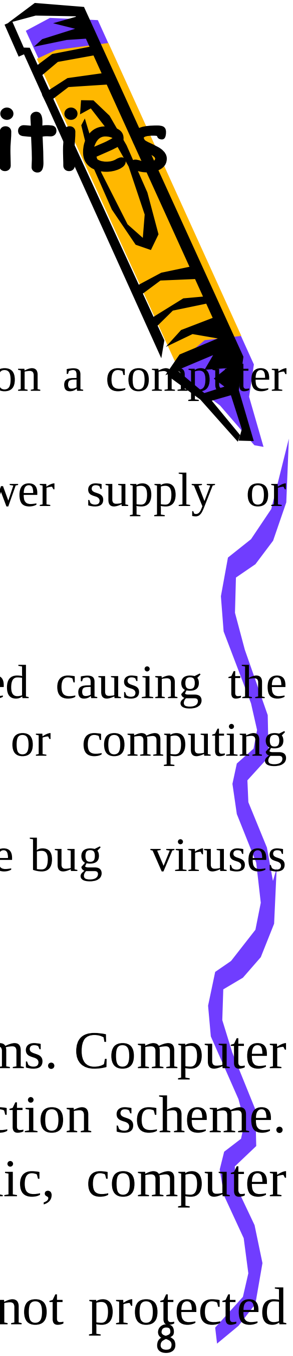
- Integrity means that assets can be modified only by authorized parties or only in authorized ways.
- In this context, modification includes writing, changing, changing status, deleting, and creating.

3 *Availability threat*

- Availability means that assets are accessible to authorized parties.
- An authorized party should be given access to which he has legitimate access, but not unauthorized parties.
- *Availability is sometimes known as denial of service.*



4 The Points of Security Vulnerabilities



4.1 Attacks on hardware

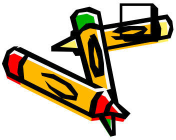
- Computer hardware is so visible and hence easy to attack.
  - The attack points on computer hardware include sprinkling water on a computer hardware causing it to malfunction.
  - Physical weaknesses such as power supply surge, unstable power supply or environmental matters such as lightning.

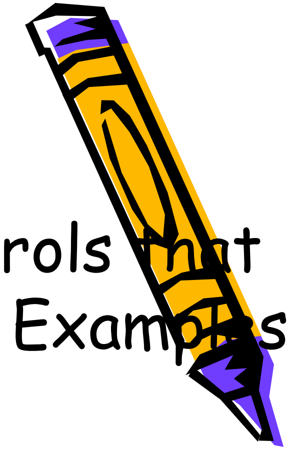
4.2 Attacks on software

- Software can be destroyed maliciously, modified, deleted or misplaced causing the computer software to behave abnormally and affecting the results, or computing operations.
- Common software attacks will include time bomb, Trojan horse, software bug viruses etc.

4.3 Attacks on data

- Computer data is the root towards many computer security problems. Computer data is a very often to object to be used for all computer protection scheme. Computer data are available in many forms, such as electronic, computer printout and in computer media.
- Data can be destroyed, changed, modified, or deleted very if not protected properly.





5 Methods of Defense

- The goal of computer security is to introduce controls that preserve confidentiality, integrity and availability. Examples of methods of defense are:

i. **Encryption**

- converting data in to a form that is unreadable by anyone else except the intended recipient.

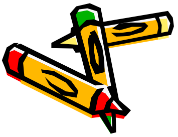
ii. **Approved users access right**

iii. **Firewalls.**

- A combination of hardware's and software's that filters un authorized access in to a computer system. also ensures that information received from an outside source will not contain computer viruses

iv. **Security servers**

v. **Biometric systems**



6. Categories of Computer Attacks

6.1 Using an Attack Taxonomy

❑ An attack taxonomy can be defined as any generalized categorization of potential attacks that might occur on a given computer system.

- i.e. ***type of a threat*** (confidentiality, integrity and availability)

❑ Note:-

- Attack scenarios are sometimes identified for certain classes of systems like real-time systems, databases, and local area networks.

6.2 Consideration in Selecting Attack Taxonomy

❑ The simple threat categorization are confidentiality, integrity and availability and covers most of the cases that involve some desirable occurrence.

❑ Factors that must be considered in the selection of suitable attack taxonomy are, completeness, appropriateness, internal and external threats.

6. Categories of Computer Attacks

6.3 A Simple Attack Taxonomy

	Programmers	**Internal**	**Outside**
Theft of information		Unauthorized action	Via modem
Information destruction	Malicious software		Malicious software
Theft of services	Theft as user	Unauthorized action	Via modem

Note:-

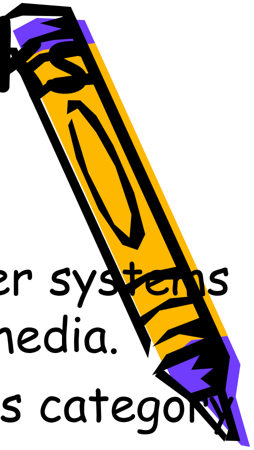
- In the matrix, specific example are included in the cells for the most likely types of attack i.e. programmers may insert a malicious software to cause information destruction, such as a time bomb program.

6. Categories of Computer Attacks

6.4 Risk Based Attack Taxonomy

- ❑ Risk based taxonomy is based on a vast number of reported instances of actual attacks as follows:-
  - external information theft
  - external abuse of resources
  - masquerading
  - pest programs
  - bypassing authentication or authority
- ❑ ***6.4.1 External information theft***
  - ➢ External theft involves unauthorized individual stealing information from a computer system without exploiting any mechanisms considered internal to the system.
    - ➢ This type of attack is not intended to include exploitation of internal hardware or software defects to gain information.
    - ➢ It is intended to describe the abuse of mechanisms without having direct access to the system.
  - ➢ N.B:- Such theft is mostly associated with the disclosure threat.
  - ➢ **Example**: A malicious individual looking at a colleague's terminal screen, trying to see information that he may not have access, such as payroll.

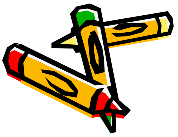
6. Categories of Computer Attacks



6.4 Risk Based Attack Taxonomy

- ❑ ***6.4.2 External abuse of resources***
  - External resource abuse involves physical destruction of computer systems hardware such as disk drives, circuit boards and communication media.
  - Since this type of destruction concerns unauthorized change, this category is mostly associated with the integrity threat.

  N.B:-
  - The assumption is that the attacker must have physical access to these resources, but may not have direct access to the terminal resources.
  - **Example:**
    - Direct vandalism of some hardware components, such as pulling out and damaging circuit boards.
- ❑ ***6.4.3 External masquerading***
  - This category of attack involves a malicious intruder successfully impersonating another user using some mechanism external to the computer system.
  - Such deception of identity can be used to ambush (trap) another individual by causing harmful actions as that person or it can be used to gain authority by impersonating a more important individual.



6. Categories of Computer Attacks

6.4 Risk Based Attack Taxonomy

- ❑ ***6.4.3 External masquerading cont…..***
- N.B:-
  - Masquerading is an example of an attack that can be mapped to the disclosure, integrity, or denial of service threats.
- - **Example**:
  - A malicious intruder tapping into a communications medium, recording the information transferred, and then playing back this information transfer at some later time.

6.4.4 Pest programs

- Pest programs include attacks that are set up by malicious individuals to cause subsequent harm.
- A pest program can be viewed as a *time bomb* in the sense that it is created and used for an attack that may occur at a much later time. This time lag may provide an opportunity for an intruder to cover tracks and avoid being caught.
- This type of attack is internal in the sense that it requires mechanisms internal to the computer system.

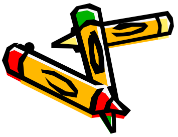
6. Categories of Computer Attacks

6.4.4 Pest programs Cont…..

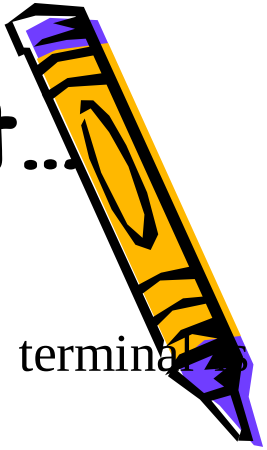
- **N.B:-**
  - The insertion of a pest program into a system is an *integrity threat*, but the program can then be used to enact any type of threat.
- ***Example***:
  - Trojan horse and computer virus attacks that may cause computer system not to function normally.

6.4.5 Bypassing of internal controls

- This category of attack involves the explicit avoidance of controls that are set up to protect the resources on a computer system. Bypassing usually involves the clever use of some existing logical errors in the system.
- **N.B:-**
  - Authorization, access, and authority controls provide the primary targets for this category of threat.
- ***Example***:
  - *Password cracking techniques that weaken or sabotage protective approaches that contain errors such as operating system and compiler attacks usually involves logical exploitation of flaws to bypass authority as well.*



7. Common Attack Methods Cont…



7.1 Password spoof program

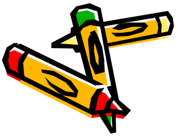
- ❑ This involves disguising a user into believing that computer terminal is correct prompting user for login and password information.
- ❑ In this attack a Trojan horse program is used to fake the normal login sequence that a user expects.

7.2 Password theft by clever reasoning

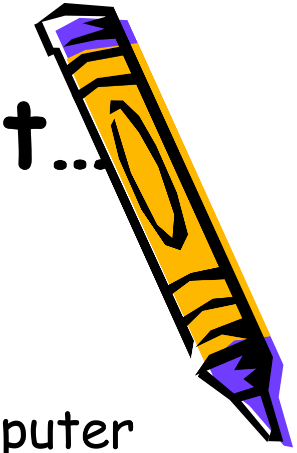
- ❑ This involves users creating passwords that are mnemonic and hackers gain access to a computer system through guessing of password of an individual profile.

7.3 Insertion of compiler Trojan horse

- ❑ This happens when the goal of an attack is widespread damage and targets applications that are used by many different users.
- ❑ Examples compilers are attractive targets for Trojan horse insertion.



7. Common Attack Methods Cont…



7.4 Denial of service

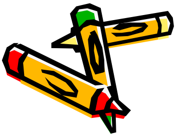
❑ In this attack an attacker tries to make the target computer unable to provide the normal services. The attacker can send more information to a target computer than a computer is capable of processing. The user or organization is deprived of the services of a resource they would normally expect to have.

N.B : The costs of this attack is on time and money.

7.5 Trojan Horse

❑ Trojan horses are programs that pretend to be legitimate software, but actually carry out hidden, harmful functions.

❑ An attacker place this software on the target computer using web site, e-mail, etc



7. Common Attack Methods Cont…

7.6 Buffer Overflow

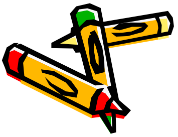
- ❑ Happens when an attacker sends a specific series of characters (text) to a service causing the service to act outside it's normal operating parameters. The attack is in two parts, the overflow itself, and the command to execute. The overflow part contains the specific series of characters that will cause the service to act abnormally and the commands can cause computer to crash, or to install a Trojan.

- ❑ *N.B Buffer overflows are usually the preferred method of compromising a web server.*

7. Common Attack Methods Cont…

7.7 Port Scan

- A **port scanner** is a software application designed to probe a network host for open ports Sniffing. This is often used by administrators to verify security policies of their networks and by attackers to identify running services on a host with the view to attack it. An *open port* is used to mean a TCP/IP port number that is configured to accept packets as opposed to a *closed port* which ignores all packets directed at it.
- *N.B: Port scanning is the first step in determining how to compromise a system, as an attacker needs to know the potential weakness of a system before trying to execute them.*
- A firewall can be set to allow and disallow ports associated with certain programs and services.



7. Common Attack Methods Cont…

7.7 Port Scan Cont….

- ❑ **Common Ports**
  - **Port 21** = FTP control (command) port;
  - **Port 22** = SSH (Secure Shell) - used for secure logins, file transfers (scp, sftp) and port forwarding;
  - **Port 23** = Telnet protocol - unencrypted text communications
  - **Port 80** = HTTP (Hypertext Transfer Protocol) - used for transferring web pages.
  - **Open port testing use telnet for local workstations**
    - telnet 127.0.0.1 8080
    - ping xxx.xxx.xxx.xxx:8080
    - A port scanner is a tool that allows an individual to list the ports on a computer that are available or open.

7. Common Attack Methods Cont…

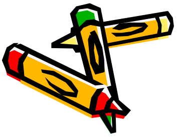
7.8 Logic bomb mail

- Logic bombs are programs that remain dormant until some predetermined logical condition on the target computer system becomes true.
- They are particularly dangerous because they may cause harm long after the malicious intruder has escaped.
  - **Example:-**
    - The login spoof is a logic bomb since it requires the condition that someone attempt to login using the target terminal.

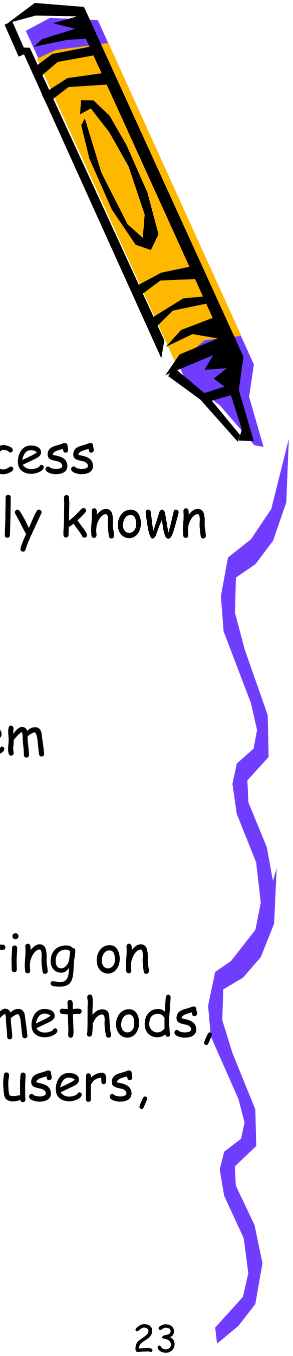
8. Attacks Motives

Attacks Motives Intelligence

- ❑ Financial gain
- ❑ Gain access
- ❑ Thrill/ delight/joy
- ❑ Fun and games
- ❑ Political hacktivism
- ❑ Hacktivism involves writing of code to promote political ideology i.e. promoting expressive politics, human rights, or information ethics."
  - ❑ This can be carried out in several different ways i.e. some flood certain political websites in order to overload their servers, deface certain political websites.



9. Attack Prevention Methods



Attack Prevention Methods

a) *Firewalls:*

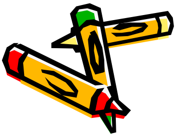
- Programs, which protect a user from unauthorized access attacks while on a network. They provide access to only known users, or people who the user permits.

b) *Frequent password changing:*

- This involves changing p/w frequently and keeping them sufficiently complex.

c) *Safe surfing:*

- This involves keeping e-mail address private not chatting on open systems which do not have adequate protection methods, visiting secure sites. Accepting data from only known users, downloading carefully, and from known sites.



9.Attack Prevention Methods Cont.

Attack Prevention Methods

d) Frequent virus checks:

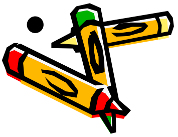
- One should frequently check for computer for viruses and worms and scan external media before use.

e) Email filters:

- These are programs which monitor the inflow of mails to the inbox and delete automatically any suspicious mail reducing the chances of being bombed or spoofed.
- Spoofing is sending network traffic pretending to come from someone else.

f) Individual screening

- This method involves checking the background, credentials, family, and other personal attributes of individuals who can possibly attack a given computer system.



11. Computer Security

Hardware Vulnerabilities

- ❑ Most PCs do not have any hardware level protection. Very minimal security features in placed for PCs.
- ❑ 11.1 Other Vulnerabilities
  - low awareness level
  - few hardware controls
  - no audit trail
  - no unique responsibility
  - environment attack
  - physical access
  - care of media, components
  - no backup
  - questionable documentation
  - amateur quality software
  - magnetic retention

11. Computer Security Cont…

11.2 Security Measures

- user responsibility
- improper procedures for use
- hardware concerns
- software concerns

11.3 User Awareness of Responsibilities

- Professionals who use computers must come to understand the vulnerabilities of computers and specifically of personal computers.
- This awareness may be developed from reading, from user awareness programmes, or from high-level assessment of the risks of computing.
- Some of the vulnerabilities identified can be controlled by administrative procedures.

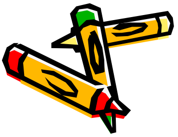
11. Computer Security Cont…

11.3 User Awareness of Responsibilities cont…

- Sensible policies for the use of computers can reduce the risk associated
- The PC policy could include statements on unattended machines, care of media, backups, the environment, magnetic residue, and separation of duties.
- Procedures that can improve the security of the use of PC are:
- do not leave PCs unattended if they contain sensitive information or are running sensitive computations
- do not leave printers unattended if they are printing sensitive output
- secure media as carefully as you would the equivalent confidential reports
- do not allow eating or drinking, or smoking in any room containing a PC
- treat media with care
- perform periodic backups
- practice separation of authority

11.4 Hardware Controls

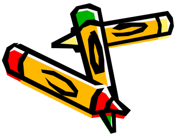
- secure the equipment through bolting the PC on the desk
- consider add-on hardware access control devices such as smart card



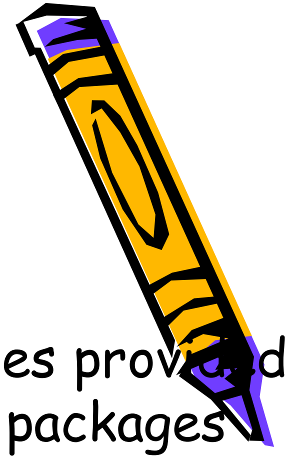
11. Computer Security Cont…

11.5 Software Controls

- Common software vulnerabilities include the lack of audit trail, the use of software from entrusted sources, poor documentation, and the lack of operating system controls, such as reuse of file space or access control.
- Other than access control, protection against software vulnerabilities can include the following controls:
  - ➢ use all software with full understanding of its potential threats
  - ➢ don’t use software from dubious sources
  - ➢ be suspicious of all results
  - ➢ maintain periodic complete backups of all system resources



11. Computer Security Cont…



11.6 Protection for File

- *There are four types of protection applicable to PC files:*

i. access control feature limits the access of people to files provided either as a part of the operating system or as auxiliary packages

ii. encryption applied by the individual user where only users who know how to decrypt can obtain access to the plaintext of encrypted data

iii. No Protection . This is the case of having controlled the environment so that protection is not necessary.

i.e. Shareware that offers no control feature at all and this is freely acceptable by the public domain users.

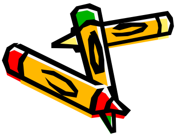
iv. Copy Right Protection to limit someone's ability to copy a file

- There are three ways to prevent a file from being copied:

a) one can depend solely on software.

b) one can use a combination of software and hardware device.

c) one can use hardware alone



11. Computer Security Cont…

11.7 Straight Software Techniques

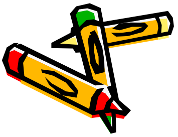
- This method uses software magnetic media design to hide certain control features to prevent normal users from retrieving them easily.
- A program check sum is created to prevent modification, and the software can be run if the magnetic media is present when executing the program.

11.8 Software and Hardware Combinations

- A hard token called key is used together with the software package in order for the program to run. Such feature is commonly used for expensive PC software such as CADCAM software.

11.9 Hardware Techniques

- The method involves translating the program code into a micro chip which is then plugged into the PC and run during power-up.
- Such method is commonly used for time-sensitive applications where performance is the key concern. For example: Simple automated gate control system.



12. Communication and Network Security

12.1 Communications Media

□ Media used to achieve computer communications.

□ Coaxial Cable

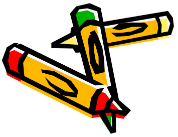
□ Twisted pair cable

12.2 Security consideration for cable (both cable and coaxial)

- Subject to wire-tapping i.e. extracts communication from the cable without damaging the cable.
- Passive wiretapping involves listening, whereas active wiretapping involves injecting something into the communication line.
- Wiretapping can be achieved at junction boxes or a place where cable is exposed to the public.
- Wire interference that causes the communications to malfunction.

□ ***Microwave***

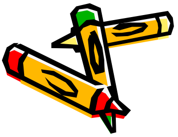
- A microwave signal travels in a straight line. While the earth curves, therefore, a typical microwave transmission tower needs to be line of sight to achieve maximum efficiency.



12. Communication and Network Security

12.1 Communications Media Cont….

- ***Satellite***
  - Security concerns for both microwave and satellite. Any party with appropriate equipment can listen into the communication and be able to retrieve information from the open air signal.
- ***Optical fiber***
  - **Security consideration for optic fiber**
    - Fiber optic needs to be fitted carefully when a new connection is required.
    - The connector used is the most vulnerable point for most fiber optic connections.
    - This is because light signals can be reflected into multiple directions if the connector is not made properly.

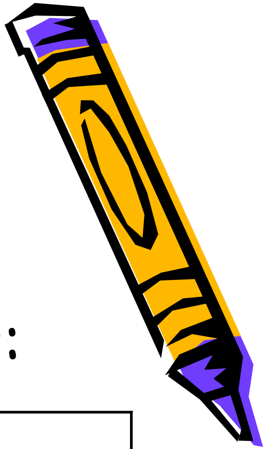


13. Network Security Issues

Network Security Issues

- ***Encryption in Networks***
  - Networks secure data with encryption by providing privacy, authenticity, integrity, and limited access to data.
- ***Network Access Controls***
  - This is concerned about protection of data in the network.
- ***Port control***
  - A vulnerability to a network is dial-in port access to access open ports where attackers to identify running services on a host with the view to attack it. Port protection is accomplished by several administrative and hardware techniques.

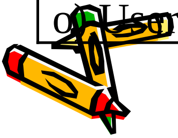
Activity 1: Assignment



Each group of student should pick one topic.

- Discuss the following in information security issues:

Topic	Student
a) Intruders and Intrusion detection systems	
b) Firewalls	
c) Physical security	
d) Computer crimes	
e) Security controls	
f) Web Security and Tools	
g) Digital signatures	
h) Computer forensics	
i) Virtual Private networks	
j) Network attacks	
K) Cryptography basics	
l) Hash and MAC Algorithms	
m) Electronic Mail Security	
n) IP Security	
o) User authentication	



The END

Q&A

THANKS