INFORMATION SECURITY

UNIT-I

---

1) What is information security?

Information security in today's enterprise is a "well-informed sense of assurance that the **information risks and controls are in balance**." –Jim Anderson, Inovant (2002)

- The protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information
- Tools, such as policy, awareness, training, education, and technology are necessary
- The C.I.A. triangle was the standard based on **confidentiality, integrity, and availability**
- The C.I.A. triangle has expanded into a list of critical characteristics of information

2) Trace the history of information security?

- Computer security began immediately after the first mainframes were developed
- Groups developing code-breaking computations during World War II created the first modern computers
- Physical controls were needed to limit access to authorized personnel to sensitive military locations
- Only rudimentary controls were available to defend against physical theft, espionage, and sabotage.

3) What is Rand Report R-609?

Information Security began with Rand Corporation Report R-609
The Rand Report was the first widely recognized published document to identify the role of management and policy issues in computer security.
The scope of computer security grew from physical security to include:

a. Safety of the data
b. Limiting unauthorized access to that data
c. Involvement of personnel from multiple levels of the organization

4) What is Security? What are the security layers a successful organization should have?

"The quality or state of being secure--to be free from danger" is called as security.

To be protected from adversaries a successful organization has different types of security.

- **Physical Security** – to protect physical items, objects or areas of organization from unauthorized access and misuse.
- **Personal Security** – involves protection of individuals or group of individuals who are authorized to access the organization and its operations.
- **Operations security** – focuses on the protection of the details of particular operations or series of activities.
- **Communications security** – encompasses the protection of organization's communications media ,technology and content.
- **Network security** – is the protection of networking components,connections,and contents.
- **Information security** – is the protection of information and its critical elements, including the systems and hardware that use ,store, and transmit the information.

5) What are the critical characteristics of information?

Availability

Enables users who need to access information to do so without interference or obstruction and in the required format. The information is said to be available to an authorized user when and where needed and in the correct format.

Ex: Library ID.

Accuracy

Free from mistake or error and having the value that the end-user expects. If information contains a value different from the user's expectations due to the intentional or unintentional modification of its content, it is no longer accurate.

Ex: Checking Account.

Authenticity

The quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is the information that was originally created, placed, stored, or transferred.

Ex: Consider for example common assumptions about email. When you receive an email you assume the origin of the email to be sent by a specific individual or a group but this may not be the case always. Instances like Email-Spoofing, and Phishing may also occur.

Spoofing:

- **Sending an email with a modified field such as, the address from the sender.**
- **Tricks people into opening email they otherwise would not have opened.**
- **Gives an attacker access to data.**

Phishing:

- **Another Variation of Spoofing.**
- **Attacker attempts to obtain personal or financial information using fraudulent methods often posing as another person or organization.**

Confidentiality

The quality or state of preventing disclosure or exposure to unauthorized individuals or systems. It ensures that only those with rights and privileges have access to information.

Some of the measures for protection are,

- **Information Classification**
- **Secure document storage**
- **Application of general security policies**
- **Education of information to custodians and end users.**

Integrity

The quality or state of being whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption, damage, destruction, or other disruption of its authentic state. We need to watch out for worms, viruses, hackers, noise, and low voltage levels. Most computer viruses and worms are designed to corrupt data hence key methods like "file hashing "are used.

File Hashing:

- **A file is read by a special program.**
- **Uses the value of the bits in the file to compute a single large number called a hash value.**

Utility

The quality or state of having value for some purpose or end. Information has value when it serves a particular purpose. This means that if information is available, but not in a format meaningful to the end-user, it is not useful.

Possession

The quality or state of having ownership or control . Information is said to be in one's possession if one obtains it, independent of format or other characteristics. While a breach of confidentiality always results in a breach of possession, a breach of possession does not always result in a breach of confidentiality

Ex: Employee who quits a job decides to take a copy of the tape backups to sell the customer records to the competition in this scenario removal of tapes from secure environment is a breach of possession, but because the data is encrypted neither the employee nor anyone else can read it without the proper decryption methods, therefore there is no breach of confidentiality.

5) What is NSTISSC Security model?

- **National Security Telecommunications & Information systems security committee' document.**
- It is now called **the National Training Standard for Information security professionals.**
- The NSTISSC Security Model provides a more detailed perspective on security.
- While the NSTISSC model covers the three dimensions of information security, it omits discussion of detailed guidelines and policies that direct the implementation of controls.
- Another weakness of using this model with too limited an approach is to view it from a single perspective.
- The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's Information systems.
- To ensure system security, each of the 27 cells must be properly addressed during the security process.
- For ex, the intersection between technology, Integrity & storage areas requires a control or safeguard that addresses the need to use technology to protect the Integrity of information while in storage.

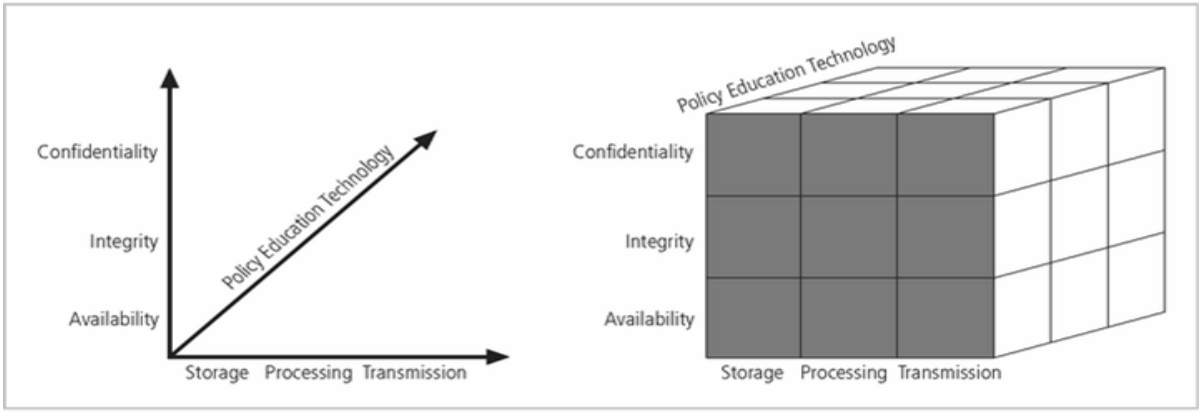

FIGURE 1-3 NSTISSC Security Model

6) What are the components of an information system?

- **Software**

  The software components of IS comprises applications, operating systems, and assorted command utilities. Software programs are the vessels that carry the lifeblood of information through an organization. These are often created under the demanding constraints of project management, which limit time, cost, and manpower.

- **Hardware**

  Hardware is the physical technology that houses and executes the software, stores and carries the data, and provides interfaces for the entry and removal of information from the system. Physical security policies deal with hardware as a physical asset and with the protection of these physical assets from harm or theft. Applying the traditional tools of physical security, such as locks and keys, restricts access to and interaction with the hardware components of an information system. Securing the physical location of computers and the computers themselves is important because a breach of physical security can result in a loss of information. Unfortunately, most information systems are built on hardware platforms that cannot guarantee any level of information security if unrestricted access to the hardware is possible.

- **Data**

  Data stored, processed, and transmitted through a computer system must be protected.

  Data is often the most valuable asset possessed by an organization and is the main target of intentional attacks.

  The raw, unorganized, discrete (separate, isolated) potentially-useful facts and figures that are later processed(manipulated) to produce information.

- **People**

  There are many roles for people in information systems. Common Ones include

  - Systems Analyst
  - Programmer
  - Technician
  - Engineer
  - Network Manager
  - MIS (Manager of Information Systems)
  - Data entry operator

- **Procedures**

  A procedure is a series of documented actions taken to achieve something. A procedure is more than a single simple task. A procedure can be quite complex and involved, such as performing a backup, shutting down a system, patching software.

- **Networks**

  When information systems are connected to each other to form Local Area Network (LANs), and these LANs are connected to other networks such as the Internet, new security challenges rapidly emerge.

  Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

7) How components are secured in an information system?

Securing the Component

- The computer can be either or both the subject of an attack and/or the object of an attack
- When a computer is
  - the subject of an attack, it is used as an active tool to conduct the attack
  - the object of an attack, it is the entity being attacked

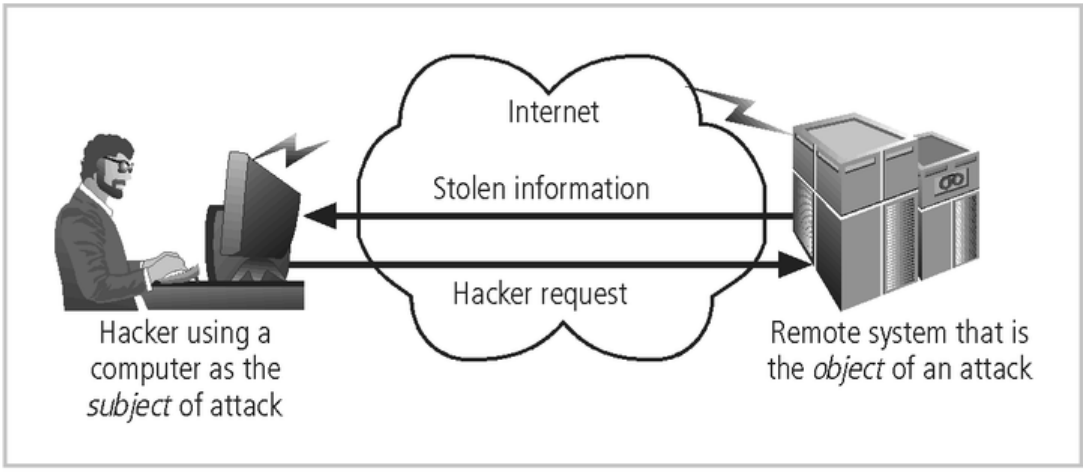

FIGURE 1-5 Computer as the Subject and Object of an Attack

1. **Direct attack**

When a Hacker uses his personal computer to break into a system.[Originate from the threat itself]

2. **Indirect attack**

When a system is compromised and used to attack other system.

[Originate from a system or resource that itself has been attacked, and is malfunctioning or working under the control of a threat].

A computer can, therefore, be both the subject and object of an attack when ,for example, it is first the object of an attack and then compromised and used to attack other systems, at which point it becomes the subject of an attack.

8) What is meant by balancing Security and Access?

Balancing Security and Access

- It is impossible to obtain perfect security - it is not absolute; it is a process not a goal.
- Security should be considered a balance between protection and availability.
- For instance, when challenged to achieve a TCSEC C-2 level security certification for its Windows operating system, Microsoft had to remove all networking components and operate the computer from only the console in a secured room.
- To achieve balance, the level of security must allow reasonable access, yet protect against threats.

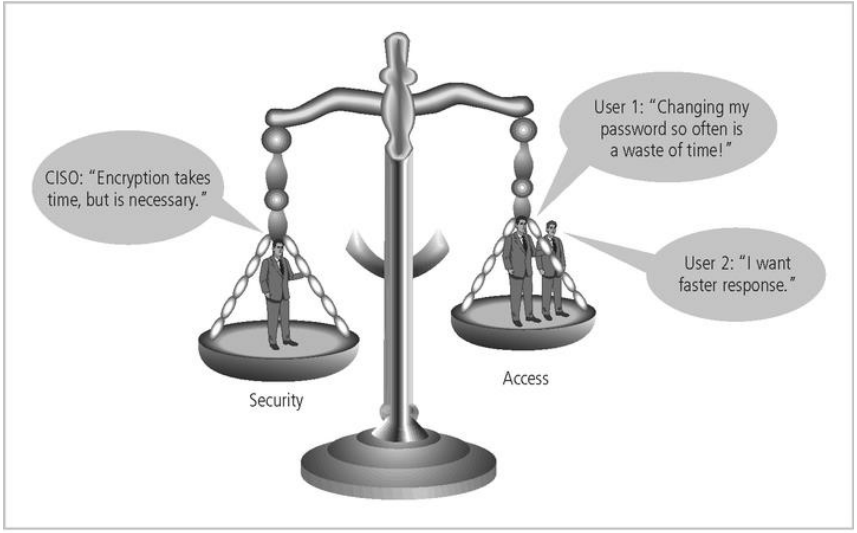

FIGURE 1-6 Balancing Security and Access

8) What is SDLC?

The Systems Development Life Cycle

- Information security must be managed in a manner similar to any other major system implemented in the organization
- Using a methodology
  - ensures a rigorous process
  - avoids missing steps
- The goal is creating a comprehensive security posture/program

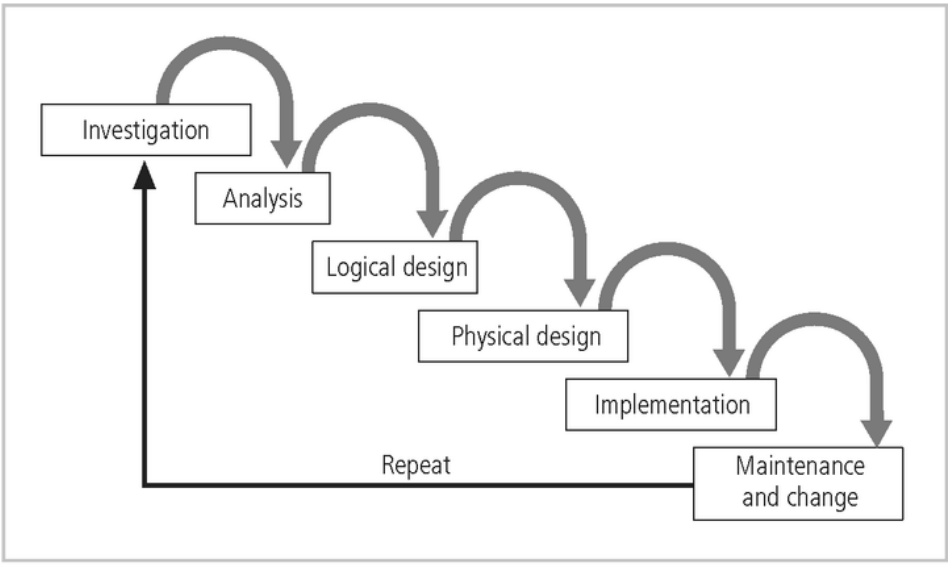

FIGURE 1-8 SDLC Waterfall Methodology

9) Explain different phases of SDLC?

Investigation

- What is the problem the system is being developed to solve?
  - The objectives, constraints, and scope of the project are specified
  - A preliminary cost/benefit analysis is developed
  - A feasibility analysis is performed to assesses the economic, technical, and behavioral feasibilities of the process

Analysis

- Consists primarily of
  - assessments of the organization
  - the status of current systems
  - capability to support the proposed systems
- Analysts begin to determine
  - what the new system is expected to do

  - how the new system will interact with existing systems
- Ends with the documentation of the findings and a feasibility analysis update.

Logical Design

- Based on business need, applications are selected capable of providing needed services
- Based on applications needed, data support and structures capable of providing the needed inputs are identified
- Finally, based on all of the above, select specific ways to implement the physical solution are chosen
- At the end, another feasibility analysis is performed.

Physical Design

- Specific technologies are selected to support the alternatives identified and evaluated in the logical design
- Selected components are evaluated based on a make-or-buy decision
- Entire solution is presented to the end-user representatives for approval.

Implementation

- Components are ordered, received, assembled, and tested
- Users are trained and documentation created
- Users are then presented with the system for a performance review and acceptance test.

Maintenance and Change

- Tasks necessary to support and modify the system for the remainder of its useful life
- The life cycle continues until the process begins again from the investigation phase
- When the current system can no longer support the mission of the organization, a new project is implemented.

7) **What are the four important functions ,the information security performs in an organization?**

- ***Business Needs First, Technology Needs Last***
- Information security performs four important functions for an organization:
    - Protects the organization's ability to function
    - Enables the safe operation of applications implemented on the organization's IT systems
    - Protects the data the organization collects and uses
    - Safeguards the technology assets in use at the organization

Long Answer:

Protecting the Ability to Function

- Management is responsible
- Information security is
    - a management issue
    - a people issue

  (information security is more to do with management than with technology)
- Communities of interest must argue for information security in terms of impact and cost

Enabling Safe Operation

- Organizations must create integrated, efficient, and capable applications
- Organization need environments that safeguard applications
- Management must not abdicate to the IT department its responsibility to make choices and enforce decisions

Protecting Data

- One of the most valuable assets is data
- Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers
- An effective information security program is essential to the protection of the integrity and value of the organization's data

Safeguarding Technology Assets

- Organizations must have secure infrastructure services based on the size and scope of the enterprise
- Additional security services may have to be provided
- More robust solutions may be needed to replace security programs the organization has outgrown

8) **What are threats?**

To protect the organization's information, one should be familiar with the information to be protected, and the systems that store,transport,and process it;and the the threats to be identified.

Threats

- A threat is an object, person, or other entity that represents a **constant danger to an asset**

- Management must be informed of the various kinds of threats facing the organization
- By examining each threat category in turn, management effectively protects its information through policy, education and training, and technology controls

9) What are the different categories of threat? Give Examples.

TABLE 2-1 Threats to Information Security[4]

Categories of threat	Examples
1. Acts of human error or failure	Accidents, employee mistakes
2. Compromises to intellectual property	Piracy, copyright infringement
3. Deliberate acts of espionage or trespass	Unauthorized access and/or data collection
4. Deliberate acts of information extortion	Blackmail of information disclosure
5. Deliberate acts of sabotage or vandalism	Destruction of systems or information
6. Deliberate acts of theft	Illegal confiscation of equipment or information
7. Deliberate software attacks	Viruses, worms, macros, denial-of-service
8. Forces of nature	Fire, flood, earthquake, lightning
9. Deviations in quality of service from service providers	Power and WAN service issues
10. Technical hardware failures or errors	Equipment failure
11. Technical software failures or errors	Bugs, code problems, unknown loopholes
12. Technological obsolescence	Antiquated or outdated technologies

10) What are different acts of Human error or failure and how it can be prevented?

Acts of Human Error or Failure

- Includes acts done without malicious intent
- Caused by:
  - Inexperience
  - Improper training
  - Incorrect assumptions
  - Other circumstances

- Employee mistakes can easily lead to the following:
  - revelation of classified data
  - entry of erroneous data
  - accidental deletion or modification of data
  - storage of data in unprotected areas
  - failure to protect information

Much human error or failure can be prevented with training and ongoing awareness activities,but also with controls,ranging from simple procedures like asking users to type a critical command twice,to more complex procedures ,such as the verification of the commands by a second party(Eg key recovery actions in PKI systems)

11) What is Intellectual property? How it can be protected?

Compromises to Intellectual Property

- Intellectual property is "the ownership of ideas and control over the tangible or virtual representation of those ideas"
- Many organizations are in business to create intellectual property
    - trade secrets
    - copyrights
    - trademarks
    - patents
- Most common **IP breaches** involve **software piracy**
- Watchdog organizations investigate:
    - Software & Information Industry Association (SIIA)
    - Business Software Alliance (BSA)

Protective measures

- Enforcement of copyright has been attempted with technical security mechanisms, such as using **digital watermarks** and embedded code.
  The most common reminder of the individual's obligation to fair and responsible use is the **license agreement window** that usually pops up during the installation of new software.

12) What are deliberate acts of espionage or trespass?

Espionage/Trespass

- Broad category of activities that breach confidentiality
    - Unauthorized accessing of information
    - Competitive intelligence vs. espionage
    - Shoulder surfing can occur any place a person is accessing confidential information
- Controls implemented to mark the boundaries of an organization's virtual territory giving notice to trespassers that they are encroaching on the organization's cyberspace
- Hackers uses skill, guile, or fraud to steal the property of someone else

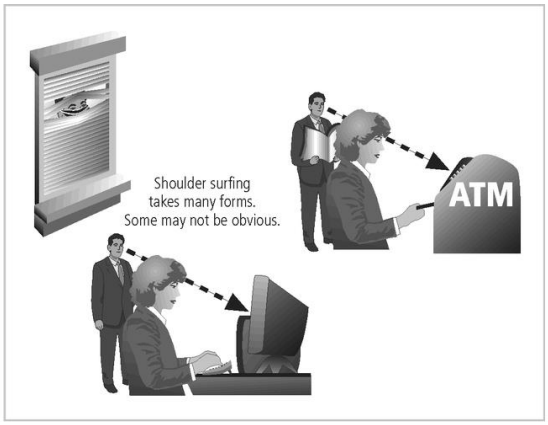

FIGURE 2-2 Shoulder Surfing

13) Who are Hackers? What are the two hacker levels?

Hackers

The classic perpetrator of deliberate acts of espionage or trespass is the hacker. **Hackers** are "people who use and create computer software [to] gain access to information illegally"

Expert hacker vs unskilled hacker

- Generally two skill levels among hackers:
  - Expert hacker
    - develops software scripts and codes exploits
    - usually a master of many skills
    - will often create attack software and share with others
  - unskilled hacker(Script kiddies)
    - hackers of limited skill
    - use expert-written software to exploit a system
    - do not usually fully understand the systems they hack
- Other terms for system rule breakers:
  - Cracker - an individual who "cracks" or removes protection designed to prevent unauthorized duplication
  - Phreaker - hacks the public telephone network

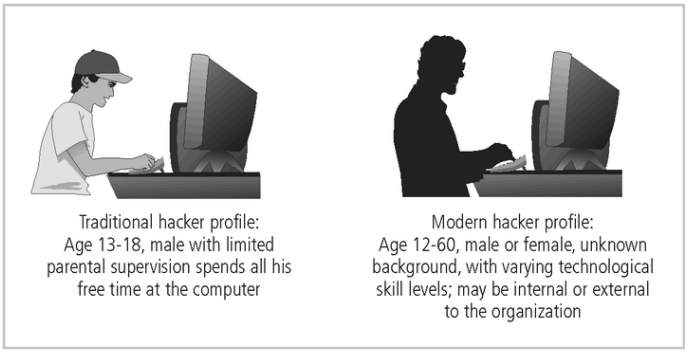

FIGURE 2-3 Hacker Profiles

14) What is information extortion?

- Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use
- Extortion found in credit card number theft(A Russian hacker named Maxus,who hacked the online vendor and stole everal hundred thousand credit card numbers. He posted the credit card numbers to a web site,when the company refused to pay the $100,000 blackmail)

15) **What are deliberate acts of sabotage and vandalism?**

Sabotage or Vandalism

Attack on the image of an organization can be serious like defacing a web site.

- Individual or group who want to deliberately sabotage the operations of a computer system or business, or perform acts of vandalism to either destroy an asset or damage the image of the organization
- These threats can range from petty vandalism to organized sabotage
- Organizations rely on image so Web defacing can lead to dropping consumer confidence and sales
- Rising threat of hacktivist or cyber-activist operations – the most extreme version is cyber-terrorism

16) What is Cyber terrorism?

Cyberterrorism is amost sinister form of hacking involving cyberterrorists hacking systems to conduct terrorist activities through network or internet pathways.

An example was defacement of NATO web pages during the war in Kosovo.

17) What are the deliberate acts of theft?

- Illegal taking of another's property - physical, electronic, or intellectual
- The value of information suffers when it is copied and taken away without the owner's knowledge
- Physical theft can be controlled - a wide variety of measures used from locked doors to guards or alarm systems
- Electronic theft is a more complex problem to manage and control - organizations may not even know it has occurred

18) What are deliberate software attacks?

Deliberate Software Attacks

- When an individual or group designs software to attack systems, they create malicious code/software called malware
    - Designed to damage, destroy, or deny service to the target systems
- Includes:
    - macro virus
    - boot virus
    - worms
    - Trojan horses
    - logic bombs

- back door or trap door
- denial-of-service attacks
- polymorphic
- hoaxes

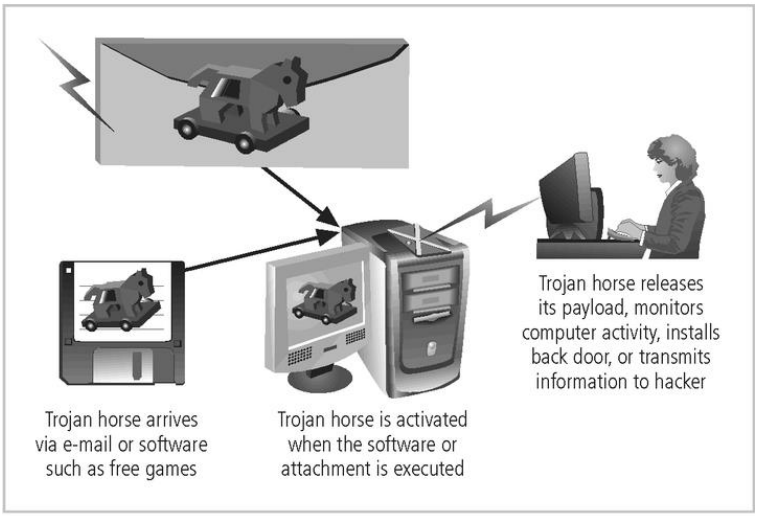

FIGURE 2-8 Trojan Horse Attack

19) What are the forces of Nature affecting information security?

Forces of Nature

- Forces of nature, *force majeure*, or acts of God are dangerous because they are unexpected and can occur with very little warning
- Can disrupt not only the lives of individuals, but also the storage, transmission, and use of information
- Include fire, flood, earthquake, and lightning as well as volcanic eruption and insect infestation
- Since it is not possible to avoid many of these threats, management must implement controls to limit damage and also prepare contingency plans for continued operations

20) What are technical hardware failures or errors?

Technical Hardware Failures or Errors

- Technical hardware failures or errors occur when a manufacturer distributes to users equipment containing flaws
- These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability
- Some errors are terminal, in that they result in the unrecoverable loss of the equipment
- Some errors are intermittent, in that they only periodically manifest themselves, resulting in faults that are not easily repeated

21) What are technical software failures or errors?

Technical Software Failures or Errors

- This category of threats comes from purchasing software with unrevealed faults
- Large quantities of computer code are written, debugged, published, and sold only to determine that not all bugs were resolved
- Sometimes, unique combinations of certain software and hardware reveal new bugs
- Sometimes, these items aren't errors, but are purposeful shortcuts left by programmers for honest or dishonest reasons

22) What is technological obsolescence?

Technological Obsolescence

- When the infrastructure becomes antiquated or outdated, it leads to unreliable and untrustworthy systems
- Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity to threats and attacks
- Ideally, proper planning by management should prevent the risks from technology obsolesce, but when obsolescence is identified, management must take action

17) What is an attack?

Attacks

- An attack is the deliberate act that exploits vulnerability
- It is accomplished by a threat-agent to damage or steal an organization's information or physical asset
    - An exploit is a technique to compromise a system
    - A vulnerability is an identified weakness of a controlled system whose controls are not present or are no longer effective
    - An attack is then the use of an exploit to achieve the compromise of a controlled system

18) What is a malicious code?

Malicious Code

- This kind of attack includes the execution of viruses, worms, Trojan horses, and active web scripts with the intent to destroy or steal information
- The state of the art in attacking systems in 2002 is the multi-vector worm using up to six attack vectors to exploit a variety of vulnerabilities in commonly found information system devices

19) **What are the attack replication vectors?**

TABLE 2-2 Attack Replication Vectors

Vector	Description
IP scan and attack	Infected system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection
Shares	Using vulnerabilities in file systems and the way many organizations configure them, it copies the viral component to all locations it can reach
Mass mail	By sending e-mail infections to addresses found in the infected system's address book, copies of the infection are sent to many users whose mail-reading programs automatically run the program and infect other systems
Simple Network Management Protocol (SNMP)	In early 2002, the SNMP vulnerabilities known to many in the IT industry were brought to the attention of the multi-vector attack community. SNMP buffer overflow and weak community string attacks are expected by the end of 2002

20) **Explain various forms of attacks.**

- **IP Scan and Attack** – Compromised system scans random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits
- **Web Browsing** - If the infected system has write access to any Web pages, it makes all Web content files infectious, so that users who browse to those pages become infected
- **Virus** - Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection
- **Unprotected Shares** - using file shares to copy viral component to all reachable locations
- **Mass Mail** - sending e-mail infections to addresses found in address book
- Simple Network Management Protocol - SNMP vulnerabilities used to compromise and infect
- **Hoaxes** - A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached
- **Back Doors** - Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource

- **Password Crack** - Attempting to reverse calculate a password
- Brute Force - The application of computing and network resources to try every possible combination of options of a password
- **Dictionary** - The dictionary password attack narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords (the dictionary) to guide guesses
- **Denial-of-service (DoS)** –
    - attacker sends a large number of connection or information requests to a target
    - so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
    - may result in a system crash, or merely an inability to perform ordinary functions
- **Distributed Denial-of-service (DDoS)** - an attack in which a coordinated stream of requests is launched against a target from many locations at the same time

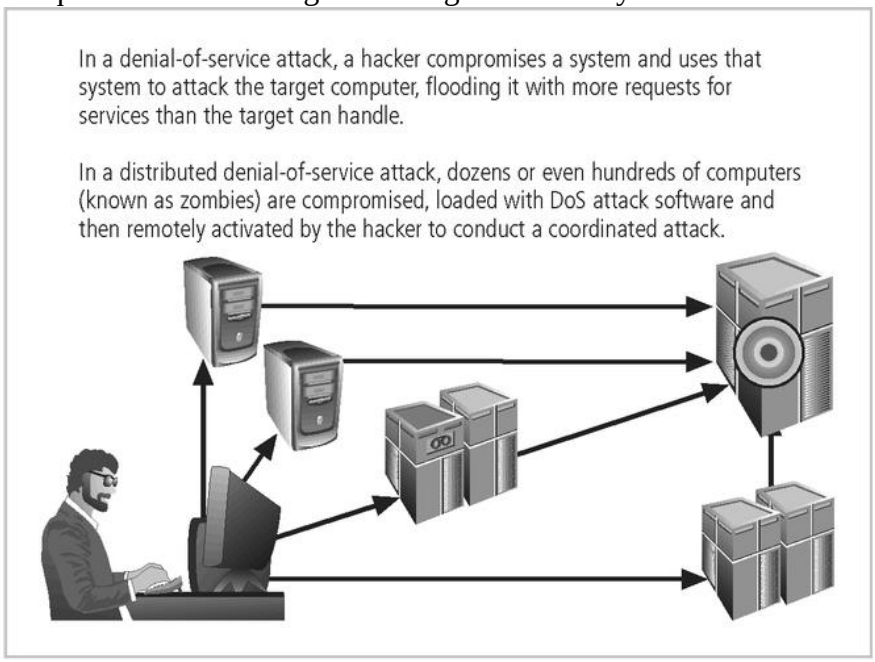

FIGURE 2-9 Denial-of-Service Attacks

- Spoofing - technique used to gain unauthorized access whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host
- Man-in-the-Middle - an attacker sniffs packets from the network, modifies them, and inserts them back into the network
- Spam - unsolicited commercial e-mail - while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks

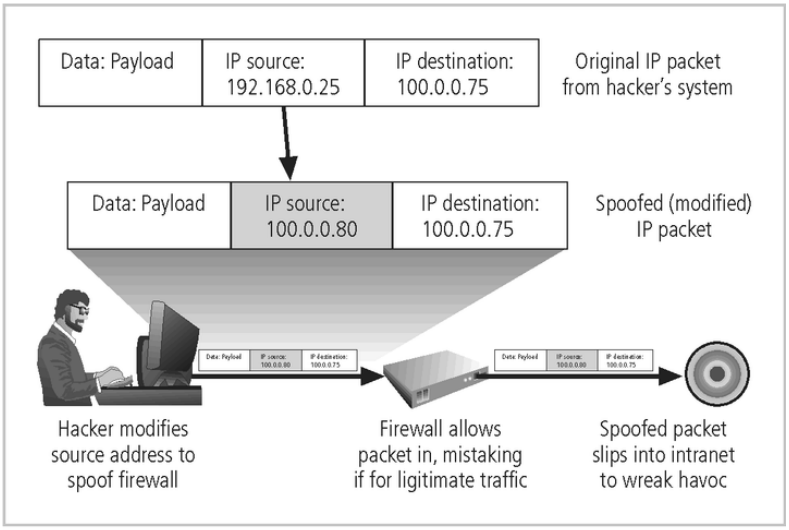

FIGURE 2-10 IP Spoofing

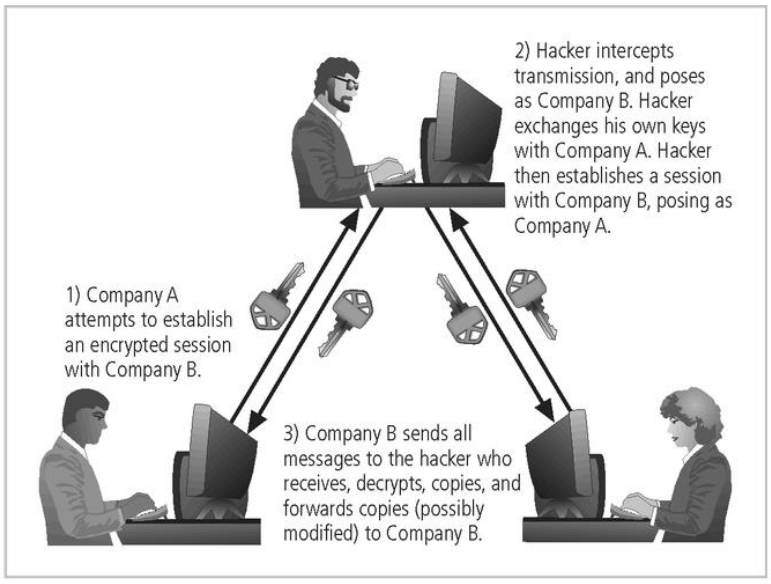

FIGURE 2-11 Man-in-the-Middle Attack

- "People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything."
- "brick attack" – the best configured firewall in the world can't stand up to a well placed brick

- **Buffer Overflow** –
  - application error occurs when more data is sent to a buffer than it can handle
  - when the buffer overflows, the attacker can make the target system execute instructions, or the attacker can take advantage of some other unintended consequence of the failure
- **Timing Attack** –
  - relatively new
  - works by exploring the contents of a web browser's cache
  - can allow collection of information on access to password-protected sites
  - another attack by the same name involves attempting to intercept cryptographic elements to determine keys and encryption algorithms