UNIT- I

FUNDAMENTALS: Introduction to Information Security - Critical Characteristics of Information - NSTISSC Security Model - Components of an Information System - Securing the Components - Balancing Security and Access - SDLC - Security SDLC.

2 MARKS

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**."

- 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?ions security

"The quality or state of being secure--to be free from danger" .To be protected from adversaries

- Physical Security
- Personal Security

- Operations security
- Communications security
- Network security
- Information security

5. What is Physical Security?

The Physical Security is to protect physical items,objects or areas of organization from unauthorized access and misuse

6. What is Personal Security?

The Personal Security involves protection of individuals or group of individuals who are authorized to access the organization and its operations

7. What is Operation Security?

The Operations security focuses on the protection of the details of particular operations or series of activities.

8.What is Communications Security?

The Communications security encompasses the protection of organization's communicatons media ,technology and content

9.What is Network Security and Information Security?

The network security is the protection of networking components,connections,and contents.

The Information security is the protection of information and its critical elements,including the systems and hardware that use ,store,and transmit the information

10. What are the critical characteristics of information?

- Availability
- Accuracy
- Authenticity
- Confidentiality
- Integrity
- Utility
- Possession

11. What is meant by Availability of information?

It enables authorized to access information without interference and receive it in the required format

12. What is Accuracy of information?

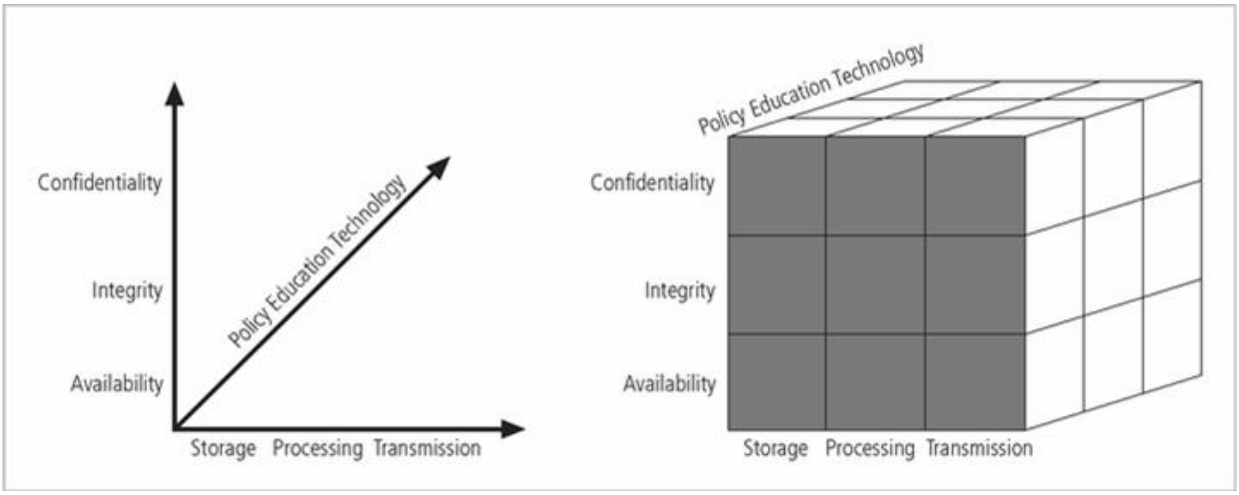
it refers to information which is free from mistakes or errors and has the value the end user expects

13. What is Authenticityof information?

It refers to quality or state of being genuine or original,rather than reproduction . Information is authentic when the contents are original as it was created,palced or stored or transmitted

14. Write about NSTISSC Security model?

This refers to "The National Security Telecommunications and Information Systems Security Committee" document. This document presents a comprehensive model for information security. The model consists of three dimensions



15. What is meant by Confidentiality

Information has confidentiality when disclosure or exposure to unauthorized individuals or systems is prevented

16. Write short notes on Integrity ,Utility and Possession of Information

- **Integrity** – Information has integrity when it is whole,complete, and uncorrupted
- **Utility** – The utility of information is the quality or state of having value for some purpose or end.
- **Possession** – the possession of information is the quality or state of having ownership or control of some object or item.

17.List the components of an information system?

An Information System (IS) is the entire set of

1. Software
2. Hardware

3. Data
4. People
5. procedures necessary to use information as a resource in the organization

18.Write about the software component of an information system.

The **software component** of IS comprises applications,operating systems,and assorted command utilities. Software programs are the vessels that carry the life blood of information through an organization. Software programs become an easy target of accidental or intentional attacks.

19..Write about the hardware component of an information system.

Hardware is the physical technology that houses and executes the software, stores and carries the data,provides interfaces for the entry and removal of information from the sytem.Physical security policies deals with the hardware as a physical asset and with the protection of these assets from theft.

20..write short notes on Data components of an information system.

Data stored,processed,and transmitted through a computer system must be protected. Data is the most valuable asset possessed by an organization and it is the main tartget of intentional attacks.

21.write about People components of an information system.

Though often overlooked in computer security considerations, people have always been a threat to information security and they are the weakest link in a security chain.. Policy, education and training, awareness, and technology should be properly employed to prevent people from accidently or intentionally damaging or losing information.

22.Write about Procedurescomponents of an information system.

Procedures are written instructions for accomplishing when an unauthorized user obtains an organization's procedures ,it poses threat to the integrity of the information. Educating employees about safeguarding the procedures is as important as securing the information system. Lax in security procedures caused the loss of over ten million dollars before the situation was corrected.

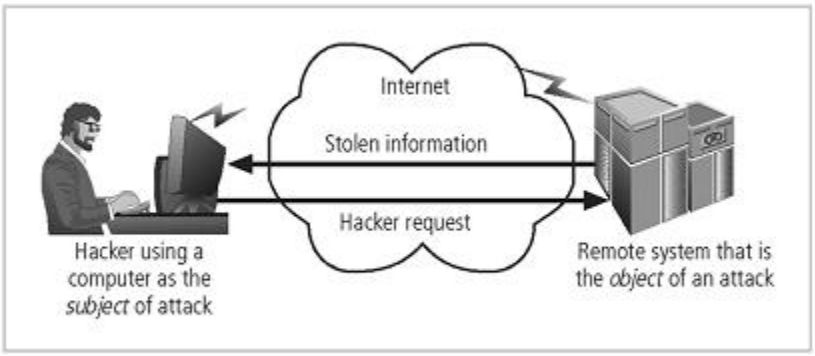
23.Write short notes on Networkscomponents of an information system.

Information systems in LANs are connected to other networks such as the internet and new security challenges are rapidly emerge. Apart from locks and keys which are used as physical security measures ,network security also an important aspect to be considered.

24.How components are secured in an information system?

Securing the Components

- 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

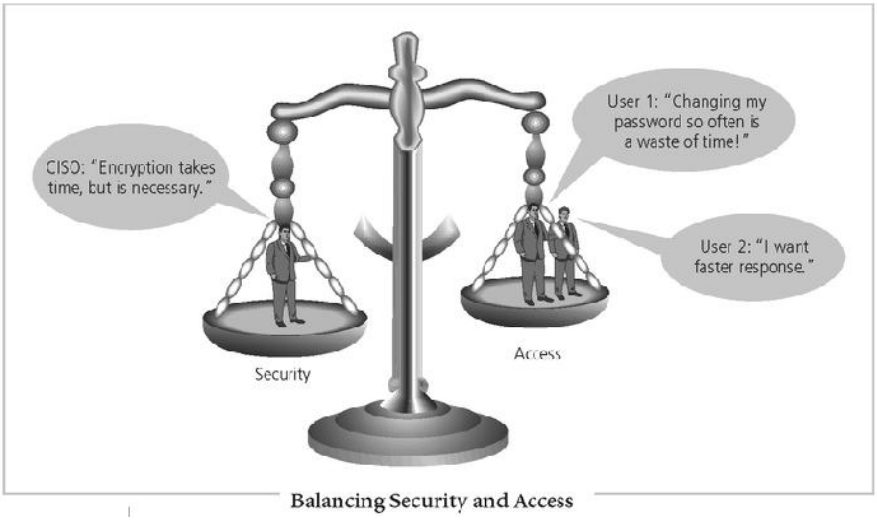


Computer as the Subject and Object of an Attack

25.What is meant by balancing Security and Access?

Balancing Security and Access

- It is impossible to obtain perfect security - it is not an absolute; it is a process
- Security should be considered a balance between protection and availability
- To achieve balance, the level of security must allow reasonable access, yet protect against threats

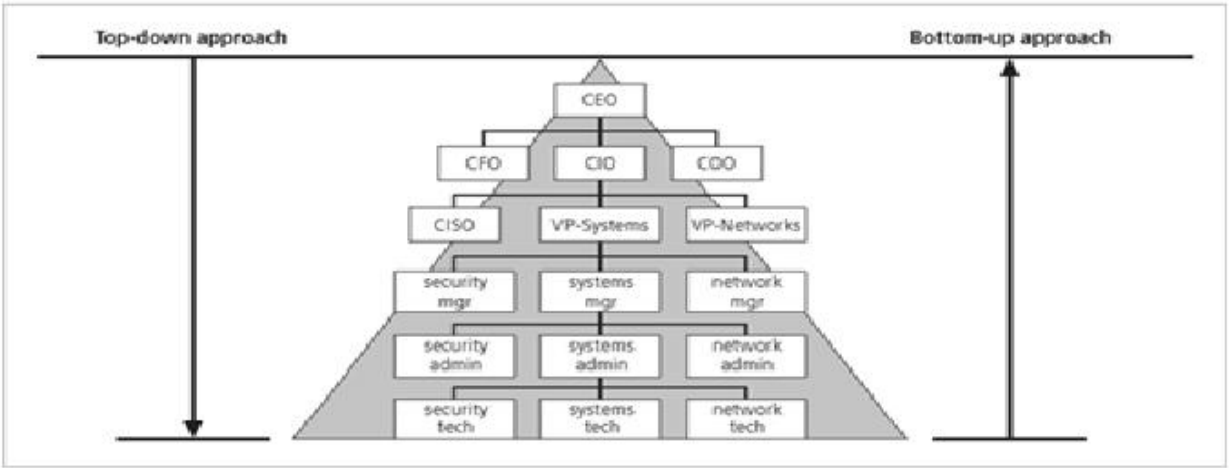


Balancing Security and Access

26.List the approaches used for implementing information security?

1. *Bottom Up Approach*
2. *Top-down Approach*

27.Draw the diagrammatic representation of the two approaches used for implementing information security



Approaches to Security Implementation

28.What is meant by bottom up approach

- Security from a grass-roots effort - systems administrators attempt to improve the security of their systems
- Key advantage - technical expertise of the individual administrators
- Seldom works, as it lacks a number of critical features:
  - participant support
  - organizational staying power

29.Write short notes on Top-down Approach

- Initiated by upper management:
  - issue policy, procedures, and processes
  - dictate the goals and expected outcomes of the project
  - determine who is accountable for each of the required actions
- This approach has strong upper management support, a dedicated champion, dedicated funding, clear planning, and the chance to influence organizational culture
- May also involve a formal development strategy referred to as a systems development life cycle
- Most successful top-down approach

30.What is SDLC?

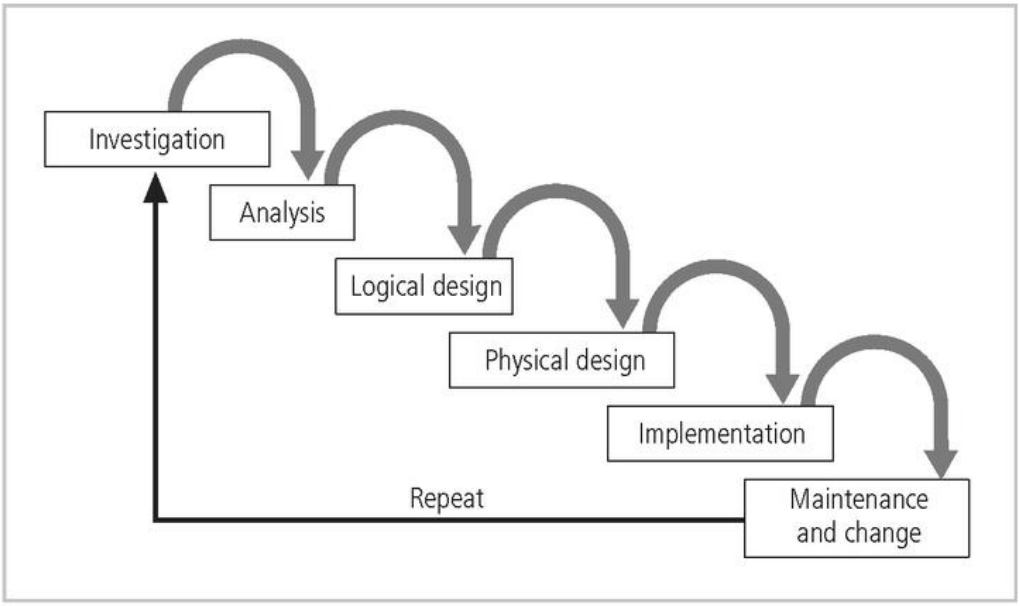
The Systems Development Life Cycle

- 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

31.List the different phases of SDLC

1. *Investigation*
2. *Analysis*
3. *Logical Design*
4. *Physical Design*
5. *Implementation*
6. *Maintenance and Change*

32.Draw the diagram of SDLC



SDLC Waterfall Methodology

33. *Write about Investigation phase of SDLC*

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

34. Write about Analysis phase of SDLC

- 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

35. Write about Logical design phase of SDLC

- 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

36. Write about physical phase of SDLC

- 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

37. Write about Implementaion phase of SDLC

- 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

38. Write about Maintenance and Change phase of SDLC

- 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

39. **What is Security SDLC?**

Security Systems Development Life Cycle

- The same phases used in the traditional SDLC adapted to support the specialized implementation of a security project

- Basic process is identification of threats and controls to counter them
- The SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

40. Write about Investigation phase of Security SDLC

- Identifies process, outcomes and goals of the project, and constraints
- Begins with a statement of program security policy
- Teams are organized, problems analyzed, and scope defined, including objectives, and constraints not covered in the program policy
- An organizational feasibility analysis is performed

41. Write about Analysis phase of Security SDLC

- Analysis of existing security policies or programs, along with documented current threats and associated controls
- Includes an analysis of relevant legal issues that could impact the design of the security solution
- The risk management task (identifying, assessing, and evaluating the levels of risk) also begins

42. Write short notes on Logical & Physical Design phases of Security SDLC

- Creates blueprints for security
- Critical planning and feasibility analyses to determine whether or not the project should continue
- In physical design, security technology is evaluated, alternatives generated, and final design selected
- At end of phase, feasibility study determines readiness so all parties involved have a chance to approve the project

43. Write about Implementation phase of Security SDLC

- The security solutions are acquired (made or bought), tested, and implemented, and tested again
- Personnel issues are evaluated and specific training and education programs conducted
- Finally, the entire tested package is presented to upper management for final approval

44. Write about Maintenance and Change phase of Security SDLC

- The maintenance and change phase is perhaps most important, given the high level of ingenuity in today's threats
- The reparation and restoration of information is a constant duel with an often unseen adversary

- As new threats emerge and old threats evolve, the information security profile of an organization requires constant adaptation

45. Write short notes on *Information Security is an Art*

- With the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science

Security as Art

- No hard and fast rules nor are there many universally accepted complete solutions
- No magic user's manual for the security of the entire system
- Complex levels of interaction between users, policy, and technology controls

46.* . Write short notes on *Information Security as Science

- Dealing with technology designed to perform at high levels of performance
- Specific conditions cause virtually all actions that occur in computer systems
- Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software
- If the developers had sufficient time, they could resolve and eliminate these faults

***47.*. How information security is viewed as a social science?**

- Social science examines the behavior of individuals interacting with systems
- Security begins and ends with the people that interact with the system
- End users may be the weakest link in the security chain
- Security administrators can greatly reduce the levels of risk caused by end users, and create more acceptable and supportable security profiles

48.Describe the information security roles to be played by *Senior Management* in a typical organization?

- Chief Information Officer
  - the senior technology officer
  - primarily responsible for advising the senior executive(s) for strategic planning
- Chief Information Security Officer
  - responsible for the assessment, management, and implementation of securing the information in the organization
  - may also be referred to as the Manager for Security, the Security Administrator, or a similar title

49.Describe the information security roles to be played by *Security Project Team* in a typical organization?

- A number of individuals who are experienced in one or multiple requirements of both the technical and non-technical areas:

- The champion
- The team leader
- Security policy developers
- Risk assessment specialists
- Security professionals
- Systems administrators
- End users

50.what are the three types of data ownership and their responsibilities?

- Data Owner
- Data Custodian
- Data Users

51.Who is called Data owner?

Data Owner - responsible for the security and use of a particular set of information

52.Who is called Data Custodian

Data Custodian - responsible for the storage, maintenance, and protection of the information

53.Who is called Data Users

Data Users - the end systems users who work with the information to perform their daily jobs supporting the mission of the organization

54.What is the difference between a threat agent and a threat?

A threat is a category of objects,persons,or other entities that pose a potential danger to an asset. Threats are always present.

A threat agent is a specific instance or component of a threat.

(For example

All hackers in the world are a collective threat

Kevin Mitnick,who was convicted for hacking into phone systems was a threat agent.)

55. What is the difference between vulnerability and exposure?

The exposure of an information system is a single instance when the system is open to damage.

Weakness or faults in a system expose information or protection mechanism that expose information to attack or damage or known as vulnerabilities.

56. What is attack?Write its types.

An attack is an intentional or unintentional attempt to cause damage or otherwise compromise the information.

If some one casually reads sensitive information not intended for his or her use ,this considered as a **passive attack.**

If a hacker attempts to break into an information system,the attack is considered **active.**

57. What is hacking?

Hacking can be defined positively and negatively.

(1) to write computer programs for enjoyment

(2) to gain access to a computer illegally

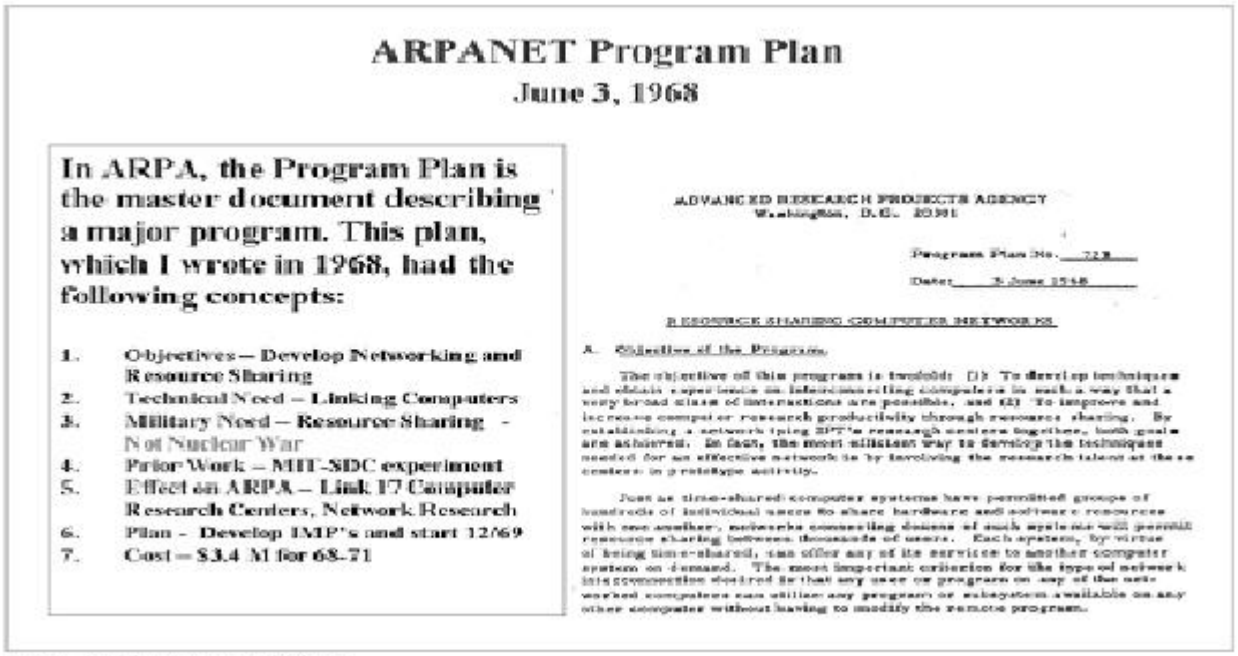
In early days the computer enthusiasts are called hacks or hackers because they could tear apart the computer instruction code,or even a computer itself.

In recent years ,the term hacker is used in a negative sense,that is,the persons gaining illegal access to others' computer systems and programs and manipulating and damaging.

58.What is security blue print?

The security blue print is the plan for the implementation of new security measures in the organization. Some times called a framework,the blue print presents an organized approach to the security planning process.

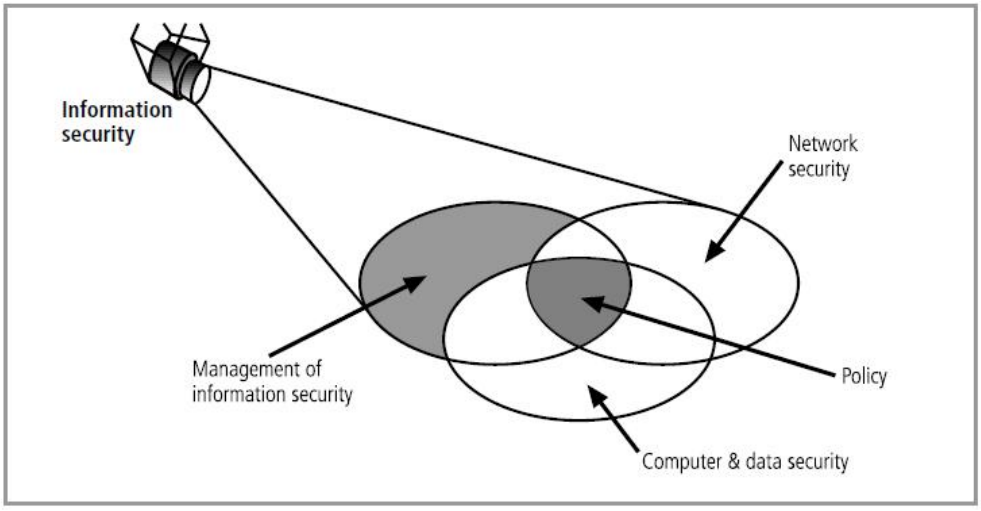
59.WriteARPANET program plan


ARPANET Program Plan
June 3, 1968
In ARPA, the Program Plan is the master document describing a major program. This plan, which I wrote in 1968, had the following concepts:
1. Objectives – Develop Networking and Resource Sharing
2. Technical Need – Linking Computers
3. Military Need – Resource Sharing - Not Nuclear War
4. Prior Work – MIT-SDC experiment
5. Effect on ARPA – Link 17 Computer Research Centers, Network Research
6. Plan - Develop IMP's and start 12/69
7. Cost – $3.4 M for 68-71
ADVANCED RESEARCH PROJECTS AGENCY
Washington, D.C. 20301
Program Plan No. 723
Date 3 June 1968
RESOURCE SHARING COMPUTER NETWORKS
A. Objective of the Program.
The objective of this program is twofold: (1) To develop techniques and obtain experience in interconnecting computers in such a way that a very broad class of interactions are possible, and (2) To improve and increase computer research productivity through resource sharing. By establishing a network (ping 2?2"a research centers together, both goals are achieved. In fact, the most efficient way to develop the techniques needed for an effective network is by involving the research talent at the centers in a prototype activity.
Just as time-shared computer systems have permitted groups of hundreds of individual users to share hardware and software resources with one another, networks connecting dozens of such systems will permit resource sharing between thousands of users. Each system, by virtue of being time-shared, can offer any of its services to another computer system on demand. The most important criterion for the type of network interconnection desired is that any user or program on any of the networked computers can utilize any program or subsystem available on any other computer without having to modify the remote program.

Courtesy of Dr. Lawrence Roberts

ARPANET Program Plan[4]

60. Draw the components of an Information system



61. What is MULTICS?

MULTICS was an operating system ,now obsolete. MULTICS is noewothy because it was the first and only OS created with security as its primary goal. It was a mainframe ,time-sharing OS developed in mid – 1960s by a consortium from GE,Bell Labs,and MIT.

62.What is ARPANET?

Department of Defense in US,started a research program on feasibility of a redundant,networked communication system to support the military's exchange of information.Larry Robers,known as the founder if internet ,developed the project from its inception.

ARPANET protocols (the rules of syntax that enable computers to communicate on a network) were originally designed for openness and flexibility, not for **security**.

11 Marks

1. **What is Security? What are the security layers ,a successful organization should have?ions security (5 Marks)**

"The quality or state of being secure--to be free from danger"

To be protected from adversaries

- 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 communicatons 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

Where it has been used?

Governments, military, financial institutions, hospitals, and private businesses.
Protecting confidential information is a business requirement.

2.What are the critical characteristics of information? (6 Marks)

Availability enables authorized users—persons or computer systems—to access information without interference or obstruction and to receive it in the required format.

Consider, for example, research libraries that require identification before entrance.Librarians protect the contents of the library so that they are available only to authorized patrons. The librarian must accept a patron's identification before that patron has free access to the book stacks. Once authorized patrons have access to the contents of the stacks, they expect to find the information they need available in a useable format and familiar language,which in this case typically means bound in a book and written in English.

Accuracy Information has **accuracy** when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate. Consider, for example, a checking account. You assume that the information contained in your checking account is an accurate representation of your finances. Incorrect information in your checking account can result from external or internal errors. If a bank teller, for instance, mistakenly adds or subtracts too much from your account, the value of the information is changed. Or, you may accidentally enter an incorrect amount into your account register. Either way, an inaccurate bank balance could cause you to make mistakes, such as bouncing a check.

Authenticity Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred. Consider for a moment some common assumptions about e-mail. When you receive e-mail, assume that a specific individual or group created and transmitted the e-mail—assume that the origin of the e-mail is known . This is not always the case. **E-mail spoofing**, the act of sending an e-mail message with a modified field, is a problem, because often the modified field is the address of the originator. Spoofing the sender's address can fool e-mail recipients into thinking that messages are legitimate traffic, thus inducing them to open e-mail they otherwise might not have. Spoofing can also alter data being transmitted across a network, as in the case of user data protocol (UDP) packet spoofing, which can enable the attacker to get access to data stored on computing systems.

Another variation on spoofing is **phishing**, when an attacker attempts to obtain personal or financial information using fraudulent means, most often by posing as another individual or organization. Pretending to be someone you are not is sometimes called *pretexting* when it is undertaken by law enforcement agents or private investigators. When used in a phishing attack, e-mail spoofing lures victims to a Web server that does not represent the organization it purports to, in an attempt to steal their private data such as account numbers and passwords. The most common variants include posing as a bank or brokerage company, e-commerce organization, or Internet service provider.

Confidentiality Information has **confidentiality** when it is protected from disclosure or exposure to unauthorized individuals or systems. Confidentiality ensures that *only* those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached. To protect the confidentiality of information, there is number of measures, including the following:

- Information classification
- Secure document storage
- Application of general security policies
- Education of information custodians and end users

Confidentiality, like most of the characteristics of information, is interdependent with other characteristics and is most closely related to the characteristic known as privacy. The value of confidentiality of information is especially high when it is personal information about employees, customers, or patients. Individuals who transact with an organization expect that their personal information will remain confidential, whether the organization is a federal agency, such as the Internal Revenue Service, or a business. Problems arise when companies disclose confidential information. Sometimes this disclosure is intentional, but there are times when disclosure of confidential information happens by mistake

For example, when confidential information is mistakenly e-mailed to someone *outside* the organization rather than to someone *inside* the organization. Several cases of privacy violation are outlined in Offline: Unintentional Disclosures.

Other examples of confidentiality breaches are an employee throwing away a document containing critical information without shredding it, or a hacker who successfully breaks into an internal database of a Web-based organization and steals sensitive information about the clients, such as names, addresses, and credit card numbers. As a consumer, you give up pieces of confidential information in exchange for convenience or value almost daily. By using a "members only" card at a grocery store, you disclose some of your spending habits. When you fill out an online survey, you exchange pieces of your personal history for access to online privileges. The bits and pieces of your information that you disclose are copied, sold, replicated, distributed, and eventually coalesced into profiles and even complete dossiers of yourself and your life. A similar technique is used in a criminal enterprise called **salami theft**. A deli worker

knows he or she cannot steal an entire salami, but a few slices here or there can be taken home without notice. Eventually the deli worker has stolen a whole salami. In information security, salami theft occurs when an employee steals a few pieces of information at a time, knowing that taking more would be noticed—but eventually the employee gets something complete or useable.

Integrity Information has **integrity** when it is 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. Corruption can occur while information is being stored or transmitted. Many computer viruses and worms are designed with the explicit purpose of corrupting data. For this reason, a key method for detecting a virus or worm is to look for changes in file integrity as shown by the size of the file. Another key method of assuring information integrity is **file hashing**, in which a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a **hash value**. The hash value for any combination of bits is unique. If a computer system performs the same hashing algorithm on a file and obtains a different number than the recorded hash value for that file, the file has been compromised and the integrity of the information is lost. Information integrity is the cornerstone of information systems, because information is of no value or use if users cannot verify its integrity. File corruption is not necessarily the result of external forces, such as hackers. Noise in the transmission media, for instance, can also cause data to lose its integrity. Transmitting data on a circuit with a low voltage level can alter and corrupt the data. Redundancy bits and check bits can compensate for internal and external threats to the integrity of information. During each transmission, algorithms, hash values, and the error-correcting codes ensure the integrity of the information. Data whose integrity has been compromised is retransmitted.

Utility The **utility** of information is the quality or state of having value for some purpose or end. Information has value when it can serve a purpose. If information is available, but is not in a format meaningful to the end user, it is not useful. For example, to a private citizen U.S. Census data can quickly become overwhelming and difficult to interpret; however, for a politician, U.S. Census data reveals information about the residents in a district, such as their race, gender, and age. This information can help form a politician's next campaign strategy.

Possession The **possession** of information is the quality or state of 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. For example, assume a company stores its critical customer data using an encrypted file system. An employee who has quit decides to take a copy of the tape backups to sell the customer records to the competition. The removal of the tapes from their 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. Today, people caught selling company secrets face increasingly stiff fines with the likelihood of jail time. Also, companies are growing more and more reluctant to hire individuals who have demonstrated dishonesty in their past.

3. Explain 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.

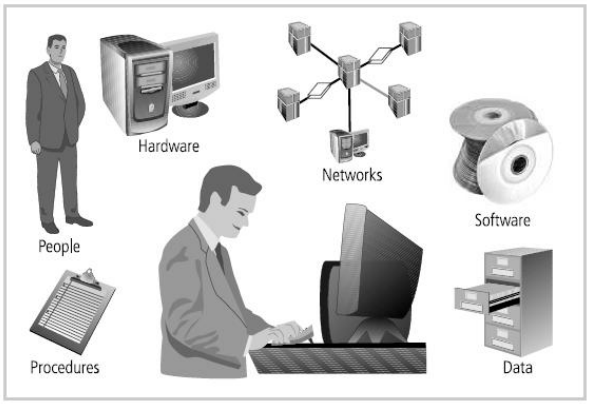
The 3 dimensions of each axis become a 3x3x3 cube with 27 cells representing areas that must be addressed to secure today's Information systems.

To ensure system security, each of the 27 cells must be properly addressed during the security process.

For example, 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.

4. What are the components of an information system? (6 Marks)

An **information system (IS)** is much more than computer hardware is the entire set of software, hardware, data, people, procedures, and networks that make possible the use of information resources in the organization. These six critical components enable information to be input, processed, output, and stored. Each of these IS components has its own strengths and weaknesses, as well as its own characteristics and uses. Each component of the information system also has its own security requirements.



Software

The software component of the IS comprises applications, operating systems, and assorted command utilities. Software is perhaps the most difficult IS component to secure. The exploitation of errors in software programming accounts for a substantial portion of the attacks on information. The information technology industry is rife with reports warning of holes, bugs, weaknesses, or other fundamental problems in software. In fact, many facets of daily life are affected by buggy software, from smart phones that crash to flawed automotive control computers that lead to recalls.

Software carries the lifeblood of information through an organization. Unfortunately, software programs are often created under the constraints of project management, which limit time, cost, and manpower. Information security is all too often implemented as an afterthought, rather than developed as an integral component from the beginning. In this way, software programs become an easy target of accidental or intentional attacks.

Hardware

Hardware is the physical technology that houses and executes the software, stores and transports 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 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. Before September 11, 2001, laptop thefts in airports were common. A two-person team worked to steal a computer as its owner passed it through the conveyor scanning devices.

The first perpetrator entered the security area ahead of an unsuspecting target and quickly went through. Then, the second perpetrator waited behind the target until the target placed his/her computer on the baggage scanner. As the computer was whisked through, the second agent slipped ahead of the victim and entered the metal detector with a substantial collection of

keys, coins, and the like, thereby slowing the detection process and allowing the first perpetrator to grab the computer and disappear in a crowded walkway.While the security response to September 11, 2001 did tighten the security process at airports,hardware can still be stolen in airports and other public places. Although laptops and notebook computers are worth a few thousand dollars, the information contained in them can be worth a great deal more to organizations and individuals.

Data

Data stored, processed, and transmitted by a computer system must be protected. Data is often the most valuable asset possessed by an organization and it is the main target of intentional attacks. Systems developed in recent years are likely to make use of database management systems. When done properly, this should improve the security of the data and the application. Unfortunately, many system development projects do not make full use of the database management system's security capabilities, and in some cases the database is implemented in ways that are less secure than traditional file systems.

People

Though often overlooked in computer security considerations, people have always been a threat to information security. Legend has it that around 200 B.C. a great army threatened the security and stability of the Chinese empire. So ferocious were the invaders that the Chinese emperor commanded the construction of a great wall that would defend against the Hun invaders. Around 1275 A.D., Kublai Khan finally achieved what the Huns had been trying for thousands of years. Initially, the Khan's army tried to climb over, dig under, and break through the wall. In the end, the Khan simply bribed the gatekeeper—and the rest is history. Whether this event actually occurred or not, the moral of the story is that people can be the weakest link in an organization's information security program. And unless policy, education and training, awareness, and technology are properly employed to prevent people from accidentally or intentionally damaging or losing information, they will remain the weakest link. Social engineering can prey on the tendency to cut corners and the commonplace nature of human error. It can be used to manipulate the actions of people to obtain access information about a system.

Procedures

Another frequently overlooked component of an IS is procedures. Procedures are written instructions for accomplishing a specific task. When an unauthorized user obtains an organization's procedures, this poses a threat to the integrity of the information. For example, a consultant to a bank learned how to wire funds by using the computer center's procedures, which were readily available. By taking advantage of a security weakness (lack of authentication), this bank consultant ordered millions of dollars to be transferred by wire to his own account.

Lax security procedures caused the loss of over ten million dollars before the situation was corrected. Most organizations distribute procedures to their legitimate employees so they

can access the information system, but many of these companies often fail to provide proper education on the protection of the procedures. Educating employees about safeguarding procedures is as important as physically securing the information system. After all, procedures are information in their own right. Therefore, knowledge of procedures, as with all critical information, should be disseminated among members of the organization only on a need-to-know basis.

Networks

The IS component that created much of the need for increased computer and information security is networking. When information systems are connected to each other to form local area networks (LANs), and these LANs are connected to other networks such as the Internet,new security challenges rapidly emerge. The physical technology that enables network functions is becoming more and more accessible to organizations of every size. Applying the traditional tools of physical security, such as locks and keys, to restrict access to and interaction with the hardware components of an information system are still important; but when computer systems are networked, this approach is no longer enough. Steps to provide network security are essential, as is the implementation of alarm and intrusion systems to make system owners aware of ongoing compromises.

5.Explain Securing Components.

SECURING COMPONENTS

Protecting the components from potential misuse and abuse by unauthorized users.

Subject of an attack

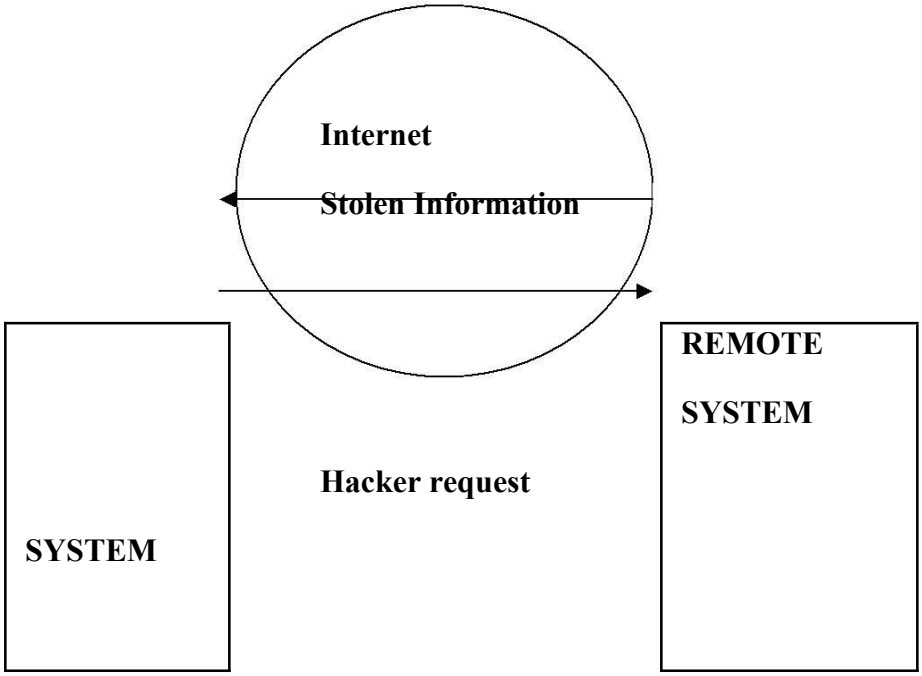
Computer is used as an active tool to conduct the attack.

Object of an attack

Computer itself is the entity being attacked

Two types of attacks:

1. **Direct attack**
2. **Indirect attack**



Hacker using a computer as the subject of attack

Remote system that is the object of an attack

Figure 1.6.1 Attack

1. **Direct attack**

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

2. **Indirect attack**

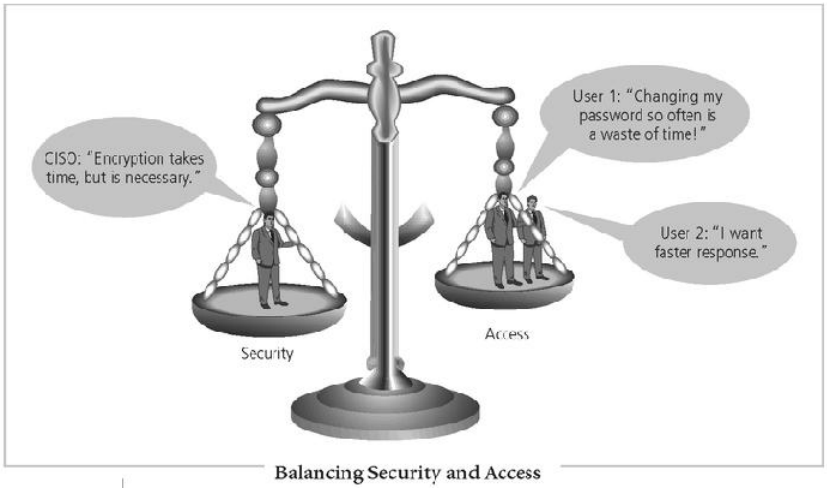
When a system is compromised and used to attack other system.

[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.

6. **Write short notes on Balancing information security and access**

Even with the best planning and implementation, it is impossible to obtain perfect information security. . Information security cannot be absolute: it is a process, not a goal. It is possible to make a system available to anyone, anywhere, anytime, through any means. However, such unrestricted access poses a danger to the security of the information. On the other hand, a completely secure information system would not allow anyone access. 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. achieve balance—that is, to operate an information system that satisfies the user and the security professional—the security level must allow reasonable access, yet protect against threats.



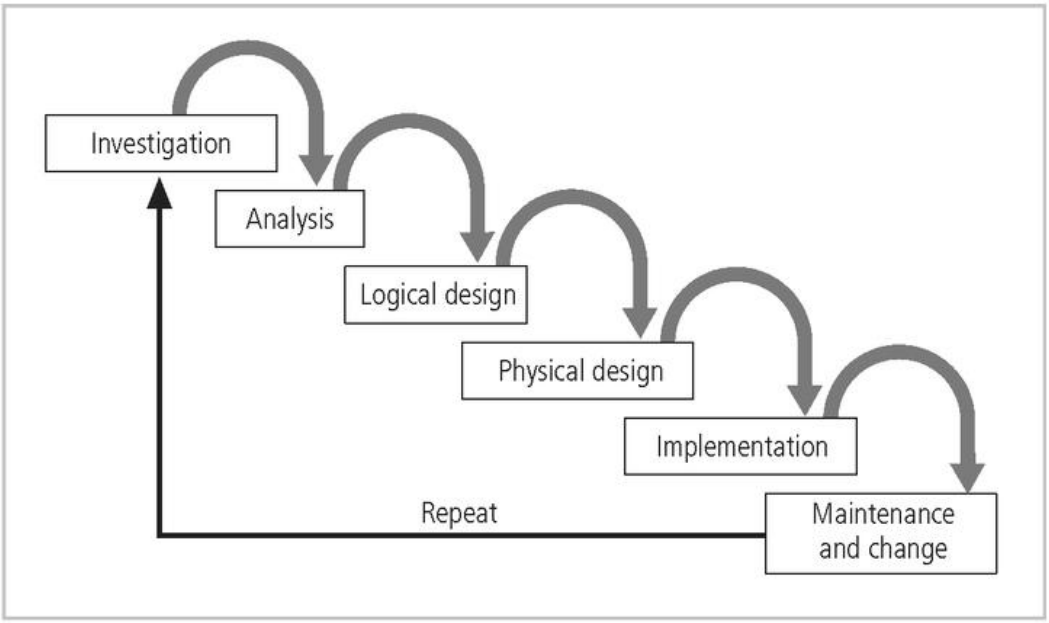
Balancing Security and Access

The figure shows some of the competing voices that must be considered when balancing information security and access. Because of today's security concerns and issues, an information system or data-processing department can get too entrenched in the management and protection of systems. An imbalance can occur when the needs of the end user are undermined by too heavy a focus on protecting and administering the information systems. Both information security technologists and end users must recognize that both groups share the same overall goals of the organization to ensure the data is available when, where, and how it is needed, with minimal delays or obstacles. In an ideal world, this level of availability can be met even after concerns about loss, damage, interception, or destruction have been addressed.

7.What is SDLC? Explain different phases of 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



SDLC Waterfall Methodology

Investigation

The first phase, investigation, is the most important. What problem is the system being developed to solve? The investigation phase begins with an examination of the event or plan that initiates the process. During the investigation phase, the objectives, constraints, and scope of the project are specified. A preliminary cost-benefit analysis evaluates the perceived benefits and the appropriate levels of cost for those benefits. At the conclusion of this phase, and at every phase following, a feasibility analysis assesses the economic, technical, and behavioural feasibilities of the process and ensures that implementation is worth the organization's time and effort. In summary,

- 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

The analysis phase begins with the information gained during the investigation phase. This phase consists primarily of assessments of the organization, its current systems, and its capability to support the proposed systems. Analysts begin by determining what the new system is expected to do and how it will interact with existing systems. This phase ends with the documentation of the findings and an update of the feasibility analysis. In summary,

- 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

In the logical design phase, the information gained from the analysis phase is used to begin creating a systems solution for a business problem. In any systems solution, it is imperative that the first and driving factor is the business need. Based on the business need, applications are selected to provide needed services, and then data support and structures capable of providing the needed inputs are chosen. Finally, based on all of the above, specific technologies to implement the physical solution are delineated. The logical design is, therefore, the blueprint for the desired solution. The logical design is implementation independent, meaning that it contains no reference to specific technologies, vendors, or products. It addresses, instead, how the proposed system will solve the problem at hand. In this stage, analysts generate a number of alternative solutions, each with corresponding strengths and weaknesses, and costs and benefits, allowing for a general comparison of available options. At the end of this phase, another feasibility analysis is performed. In summary,

- 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

During the physical design phase, specific technologies are selected to support the alternatives identified and evaluated in the logical design. The selected components are evaluated based on a make-or-buy decision (develop the components in-house or purchase them from a vendor). Final designs integrate various components and technologies. After yet another

feasibility analysis, the entire solution is presented to the organizational management for approval. In summary,

- 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

In the implementation phase, any needed software is created. Components are ordered, received, and tested. Afterward, users are trained and supporting documentation created. Once all components are tested individually, they are installed and tested as a system. Again a feasibility analysis is prepared, and the sponsors are then presented with the system for a performance review and acceptance test. In summary,

- 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

The maintenance and change phase is the longest and most expensive phase of the process. This phase consists of the tasks necessary to support and modify the system for the remainder of its useful life cycle. Even though formal development may conclude during this phase, the life cycle of the project continues until it is determined that the process should begin again from the investigation phase. At periodic points, the system is tested for compliance, and the feasibility of continuance versus discontinuance is evaluated. Upgrades, updates, and patches are managed. As the needs of the organization change, the systems that support the organization must also change. It is imperative that those who manage the systems, as well as those who support them, continually monitor the effectiveness of the systems in relation to the organization's environment. When a current system can no longer support the evolving mission of the organization, the project is terminated and a new project is implemented. In summary,

- 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

8.What is Security SDLC? Explain its different phases.

Security Systems Development Life Cycle

- The same phases used in the traditional SDLC adapted to support the specialized implementation of a security project
- Basic process is identification of threats and controls to counter them
- The SecSDLC is a coherent program rather than a series of random, seemingly unconnected actions

Investigation

The investigation phase of the SecSDLC begins with a directive from upper management, dictating the process, outcomes, and goals of the project, as well as its budget and other constraints. Frequently, this phase begins with an **enterprise information security policy (EISP)**,which outlines the implementation of a security program within the organization. Teams of responsible managers, employees, and contractors are organized; problems are analyzed; and the scope of the project, as well as specific goals and objectives and any additional constraints not covered in the program policy, are defined. Finally, an organizational feasibility analysis is performed to determine whether the organization has the resources and commitment necessary to conduct a successful security analysis and design. In summary,

- Identifies process, outcomes and goals of the project, and constraints
- Begins with a statement of program security policy
- Teams are organized, problems analyzed, and scope defined, including objectives, and constraints not covered in the program policy
- An organizational feasibility analysis is performed

Analysis

In the analysis phase, the documents from the investigation phase are studied. The development team conducts a preliminary analysis of existing security policies or programs, along with that of documented current threats and associated controls. This phase also includes an analysis of relevant legal issues that could affect the design of the security solution. Increasingly, privacy laws have become a major consideration when making decisions about information systems that manage personal information. Recently, many states have implemented legislation making certain computer-related activities illegal. A detailed understanding of these issues is vital. Risk management also begins in this stage. **Risk management** is the process of identifying, assessing, and evaluating the levels of risk facing the organization, specifically the threats to the organization's security and to the information stored and processed by the organization. In summary,

- Analysis of existing security policies or programs, along with documented current threats and associated controls
- Includes an analysis of relevant legal issues that could impact the design of the security solution
- The risk management task (identifying, assessing, and evaluating the levels of risk) also begins

Logical & Physical Design

The logical design phase creates and develops the blueprints for information security, and examines and implements key policies that influence later decisions. Also at this stage, the team

plans the incident response actions to be taken in the event of partial or catastrophic loss. The planning answers the following questions:

- Continuity planning: How will business continue in the event of a loss?
- Incident response: What steps are taken when an attack occurs?
- Disaster recovery: What must be done to recover information and vital systems
- immediately after a disastrous event?

Next, a feasibility analysis determines whether or not the project should be continued or be outsourced.

The physical design phase evaluates the information security technology needed to support the blueprint outlined in the logical design generates alternative solutions, and determines a final design. The information security blueprint may be revisited to keep it in line with the changes needed when the physical design is completed. Criteria for determining the definition of successful solutions are also prepared during this phase. Included at this time are the designs for physical security measures to support the proposed technological solutions. At the end of this phase, a feasibility study determines the readiness of the organization for the proposed project, and then the champion and sponsors are presented with the design. At this time, all parties involved have a chance to approve the project before implementation begins. In summary,

- Creates blueprints for security
- Critical planning and feasibility analyses to determine whether or not the project should continue
- In physical design, security technology is evaluated, alternatives generated, and final design selected
- At end of phase, feasibility study determines readiness so all parties involved have a chance to approve the project

Implementation

The implementation phase in of SecSDLC is also similar to that of the traditional SDLC. The security solutions are acquired (made or bought), tested, implemented, and tested again. Personnel issues are evaluated, and specific training and education programs conducted. Finally, the entire tested package is presented to upper management for final approval. In summary,

- The security solutions are acquired (made or bought), tested, and implemented, and tested again
- Personnel issues are evaluated and specific training and education programs conducted
- Finally, the entire tested package is presented to upper management for final approval

Maintenance and Change

Maintenance and change is the last, though perhaps most important, phase, given the current ever-changing threat environment. Today's information security systems need constant

monitoring, testing, modification, updating, and repairing. Applications systems developed within the framework of the traditional SDLC are not designed to anticipate a software attack that requires some degree of application reconstruction. In information security, the battle for stable, reliable systems is a defensive one. Often, repairing damage and restoring information is a constant effort against an unseen adversary. As new threats emerge and old threats evolve, the information security profile of an organization must constantly adapt to prevent threats from successfully penetrating sensitive data. This constant vigilance and security can be compared to that of a fortress where threats from outside as well as from within must be constantly monitored and checked with continuously new and more innovative technologies. In summary,

- The maintenance and change phase is perhaps most important, given the high level of ingenuity in today's threats
- The reparation and restoration of information is a constant duel with an often unseen adversary
- As new threats emerge and old threats evolve, the information security profile of an organization requires constant adaptation

9. List the steps that are common between SDLC and Security SDLC and also write the unique steps of Security SDLC

S.No	Phases	Steps common to both the systems development life cycle and the security systems development life cycle	Life cycle Steps unique to the security systems development life cycle
1	Phase 1: Investigation	• Outline project scope and goals • Estimate costs • Evaluate existing resources • Analyze feasibility	• Management defines project processes and goals and documents these in the program security policy
2	Phase 2: Analysis	• Assess current system against plan developed in Phase 1 • Develop preliminary system requirements • Study integration of new system with existing system • Document findings and update feasibility analysis	• Analyze existing security policies and programs • Analyze current threats and controls • Examine legal issues • Perform risk analysis
3	Phase 3: Logical Design	• Assess current business needs against plan	• Develop security blueprint

		developed in Phase 2 • Select applications, data support, and structures • Generate multiple solutions for consideration • Document findings and update feasibility analysis	• Plan incident response actions • Plan business response to disaster • Determine feasibility of continuing and/or outsourcing the project
4	Phase 4: Physical Design	• Select technologies to support solutions developed in Phase 3 • Select the best solution • Decide to make or buy components • Document findings and update feasibility analysis	• Select technologies needed to support security blueprint • Develop definition of successful solution • Design physical security measures to support techno logical solutions • Review and approve project
5	Phase 5: Implementation	• Develop or buy software • Order components • Document the system • Train users • Update feasibility analysis • Present system to users • Test system and review performance	• Buy or develop security solutions • At end of phase, present tested package to management for approval
6	Phase 6: Maintenance and Change	• Support and modify system during its useful life • Test periodically for compliance with business needs • Upgrade and patch as necessary	• Constantly monitor, test, modify, update, and repair to meet changing threats

10. Write about Communities of Interest (6 Marks)

Each organization develops and maintains its own unique culture and values. Within each **organizational culture**, there are communities of interest that develop and evolve. As defined here, a **community of interest** is a group of individuals who are united by similar interests or values within an organization and who share a common goal of helping the organization to meet its objectives. While there can be many different communities of interest in an organization .

Information Security Management and Professionals

The roles of information security professionals are aligned with the goals and mission of the information security community of interest. These job functions and organizational roles focus on protecting the organization's information systems and stored information from attacks.

Information Technology Management and Professionals

The community of interest made up of IT managers and skilled professionals in systems design, programming, networks, and other related disciplines has many of the same objectives as the information security community. However, its members focus more on costs of system creation and operation, ease of use for system users, and timeliness of system creation, as well as transaction response time. The goals of the IT community and the information security community are not always in complete alignment, and depending on the organizational structure, this may cause conflict.

Organizational Management and Professionals

The organization's general management team and the rest of the resources in the organization make up the other major community of interest. This large group is almost always made up of subsets of other interests as well, including executive management, production management, human resources, accounting, and legal, to name just a few.

The IT community often categorizes these groups as users of information technology systems, while the information security community categorizes them as security subjects. In fact, this community serves as the greatest reminder that all IT systems and information security objectives exist to further the objectives of the broad organizational community. The most efficient IT systems operated in the most secure fashion ever devised have no value if they are not useful to the organization as a whole.

11. ***Write about Information Security: Is It an Art or a Science ?***

- With the level of complexity in today's information systems, the implementation of information security has often been described as a combination of art and science

Security as Art

The administrators and technicians who implement security can be compared to a painter applying oils to canvas. A touch of color here, a brush stroke there, just enough to represent the image the artist wants to convey without overwhelming the viewer, or in security terms, without overly restricting user access. There are no hard and fast rules regulating the installation of various security mechanisms, nor are there many universally accepted complete solutions. While there are many manuals to support individual systems, there is no manual for implementing security throughout an entire interconnected system. This is especially true given the complex levels of interaction among users, policy, and technology controls.

- No hard and fast rules nor are there many universally accepted complete solutions
- No magic user's manual for the security of the entire system

- Complex levels of interaction between users, policy, and technology controls

Security as Science

Technology developed by computer scientists and engineers—which is designed for rigorous performance levels—makes information security a science as well as an art. Most scientists agree that specific conditions cause virtually all actions in computer systems. Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software. If the developers had sufficient time, they could resolve and eliminate these faults. The faults that remain are usually the result of technology malfunctioning for any one of a thousand possible reasons. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice. Best practices, standards of due care, and other tried-and-true methods can minimize the level of guesswork necessary to secure an organization's information and systems.

- Dealing with technology designed to perform at high levels of performance
- Specific conditions cause virtually all actions that occur in computer systems
- Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software
- If the developers had sufficient time, they could resolve and eliminate these faults

Security as a Social Science

A third view to consider is information security as a social science, which integrates some of the components of art and science and adds another dimension to the discussion. Social science examines the behavior of individuals as they interact with systems, whether these are societal systems or, as in this context, information systems. Information security begins and ends with the people inside the organization and the people that interact with the system,intentionally or otherwise. End users who need the very information the security personnel are trying to protect may be the weakest link in the security chain. By understanding some of the behavioral aspects of organizational science and change management, security administrators can greatly reduce the levels of risk caused by end users and create more acceptable and supportable security profiles. These measures, coupled with appropriate policy and training issues, can substantially improve the performance of end users and result in a more secure information system.

12.Describe the information security roles to be played by various professionals in a typical organization?

It takes a wide range of professionals to support a diverse information security program. As noted earlier in this chapter, information security is best initiated from the top down. Senior management is the key component and the vital force for a successful implementation of an information security program. But administrative support is also essential to developing and executing specific security policies and procedures, and technical expertise is of course essential to implementing the details of the information security program. The following sections describe the typical information security responsibilities of various professional roles in an organization.

Senior Management

The senior technology officer is typically the **chief information officer (CIO)**, although other titles such as vice president of information, VP of information technology, and VP of systems may be used. The CIO is primarily responsible for advising the chief executive officer, president, or company owner on the strategic planning that affects the management of information in the organization. The CIO translates the strategic plans of the organization as a whole into strategic information plans for the information systems or data processing division of the organization. Once this is accomplished, CIOs work with subordinate managers to develop tactical and operational plans for the division and to enable planning and management of the systems that support the organization.

The **chief information security officer (CISO)** has primary responsibility for the assessment, management, and implementation of information security in the organization. The CISO may also be referred to as the manager for IT security, the security administrator, or a similar title.The CISO usually reports directly to the CIO, although in larger organizations it is not uncommon for one or more layers of management to exist between the two. However, the recommendations of the CISO to the CIO must be given equal, if not greater, priority than other technology and information-related proposals. The placement of the CISO and supporting security staff in organizational hierarchies is the subject of current debate across the industry.

- Chief Information Officer
  - the senior technology officer
  - primarily responsible for advising the senior executive(s) for strategic planning
- Chief Information Security Officer
  - responsible for the assessment, management, and implementation of securing the information in the organization
  - may also be referred to as the Manager for Security, the Security Administrator, or a similar title

Security Project Team

The information security **project team** should consist of a number of individuals who are experienced in one or multiple facets of the required technical and nontechnical areas. Many of the same skills needed to manage and implement security are also needed to design it. Members of the security project team fill the following roles:

- A number of individuals who are experienced in one or multiple requirements of both the technical and non-technical areas:
  - The champion
  - The team leader
  - Security policy developers
  - Risk assessment specialists

- Security professionals
- Systems administrators
- End users

Champion: A senior executive who promotes the project and ensures its support, both financially and administratively, at the highest levels of the organization.
Team leader: A project manager, who may be a departmental line manager or staff unit manager, who understands project management, personnel management, and information security technical requirements.
Security policy developers: People who understand the organizational culture, existing policies, and requirements for developing and implementing successful policies.
Risk assessment specialists: People who understand financial risk assessment techniques, the value of organizational assets, and the security methods to be used.
Security professionals: Dedicated, trained, and well-educated specialists in all aspects of information security from both a technical and nontechnical standpoint.
Systems administrators: People with the primary responsibility for administering the systems that house the information used by the organization.
End users: Those whom the new system will most directly affect. Ideally, a selection of users from various departments, levels, and degrees of technical knowledge assist the team in focusing on the application of realistic controls applied in ways that do not disrupt the essential business activities they seek to safeguard.

Data Responsibilities

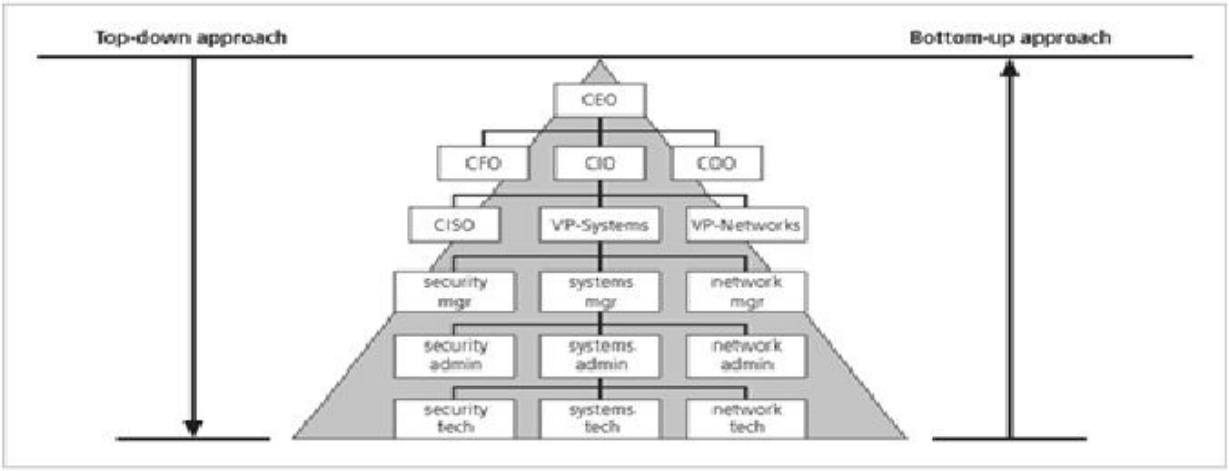
The three types of data ownership and their respective responsibilities are outlined below:
Data owners: Those responsible for the security and use of a particular set of information.They are usually members of senior management and could be CIOs. The data owners usually determine the level of data classification (discussed later), as well as the changes to that classification required by organizational change. The data owners work with subordinate managers to oversee the day-to-day administration of the data.

Data custodians: Working directly with data owners, data custodians are responsible for the storage, maintenance, and protection of the information. Depending on the size of the organization, this may be a dedicated position, such as the CISO, or it may be an additional responsibility of a systems administrator or other technology manager. The duties of a data custodian often include overseeing data storage and backups, implementing the specific procedures and policies laid out in the security policies and plans, and reporting to the data owner.

Data users: End users who work with the information to perform their assigned roles supporting the mission of the organization. Everyone in the organization is responsible for the security of data, so data users are included here as individuals with an information security role.

13.What are the approaches used for implementing information security?(6 Marks)

Bottom Up Approach



Approaches to Security Implementation

- Security from a grass-roots effort - systems administrators attempt to improve the security of their systems
- Key advantage - technical expertise of the individual administrators
- Seldom works, as it lacks a number of critical features:
  - participant support
  - organizational staying power

Top-down Approach

- Initiated by upper management:
  - issue policy, procedures, and processes
  - dictate the goals and expected outcomes of the project
  - determine who is accountable for each of the required actions
- This approach has strong upper management support, a dedicated champion, dedicated funding, clear planning, and the chance to influence organizational culture
- May also involve a formal development strategy referred to as a systems development life cycle
  - Most successful top-down approach

14. Key Terms in Information Security Terminology

Asset

-An asset is the organizational resource that is being protected. -An Asset can be logical ,such asWebsite, information or data . Asset can be physical, such asperson , computer system

Attack

- An attack is an intentional or unintentional attempt to cause damage to or otherwise compromise the information and /or the systems that support it. If someone casually reads sensitive information not intended for his use, this is considered a passive attack. If a hacker attempts to break into an information system, the attack is considered active.

Risk

- Risk is the probability that something can happen. In information security, it could be the probability of a threat to a system.

Security Blueprint

- It is the plan for the implementation of new security measures in the organization. Sometimes called a frame work, the blueprint presents an organized approach to the security planning process.

Security Model

- A security model is a collection of specific security rules that represents the implementation of a security policy.

Threats

- A threat is a category of objects, persons, or other entities that pose a potential danger to an asset. Threats are always present. Some threats manifest themselves in accidental occurrences, while others are purposeful. For example, all hackers represent potential danger or threat to an unprotected information system. Severe storms are also a threat to buildings and their contents.

Threat agent

- A threat agent is the specific instance or component of a threat. For example, you can think of all hackers in the world as a collective threat, and Kevin Mitnick, who was convicted for hacking into phone systems, as a specific threat agent. Likewise, a specific lightning strike, hailstorm, or tornado is a threat agent that is part of the threat of severe storms.

Vulnerability

- Weaknesses or faults in a system or protection mechanism that expose information to attack or damage are known as vulnerabilities. Vulnerabilities that have been examined, documented, and published are referred to as **well-known vulnerabilities.**

Exposure

- The exposure of an information system is a single instance when the system is open to damage. Vulnerabilities can cause an exposure to potential damage or attack from a threat. Total exposure is the degree to which an organization’s assets are at risk ofattack from a threat.

UNIT – II

SECURITY INVESTIGATION: Need for Security - Business Needs - Threats - Attacks - Legal, Ethical and Professional Issues.

---

2 Marks

1.List 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

2.Write short notes on the function of Protecting the Ability

- 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

3.How to Enable 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

4.How data can be Protected

- 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

5.Write about 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

6.What are 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

7.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

8.List the 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

9.How the Human error or failure can be prevented?

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)

10.What is 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

11.Write the Protective measures of Intellectual property

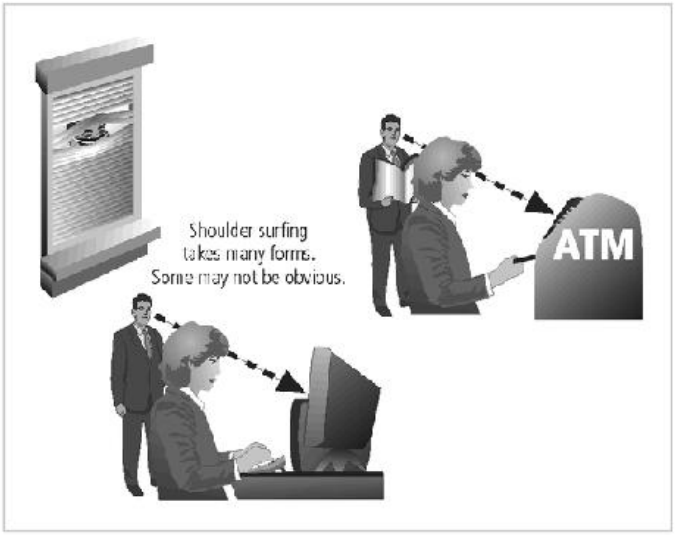
Enforcement of copyright has been attempted with technical security mechanisms,such as using **digital watermarks** and embedded code.

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 a new software.

12.What is 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



Shoulder Surfing

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

<u>Hackers</u>

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"

1. Expert hacker
2. unskilled hacker

14.Wriet about Expert hacker

- Expert hacker
  - develops software scripts and codes exploits
  - usually a master of many skills
  - will often create attack software and share with others

15.Write about unskilled hacker

- 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

16.Write about Cracker and Phreaker

- Cracker - an individual who "cracks" or removes protection designed to prevent unauthorized duplication
- Phreaker - hacks the public telephone network

17.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)

18. What is 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

19.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.

20.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

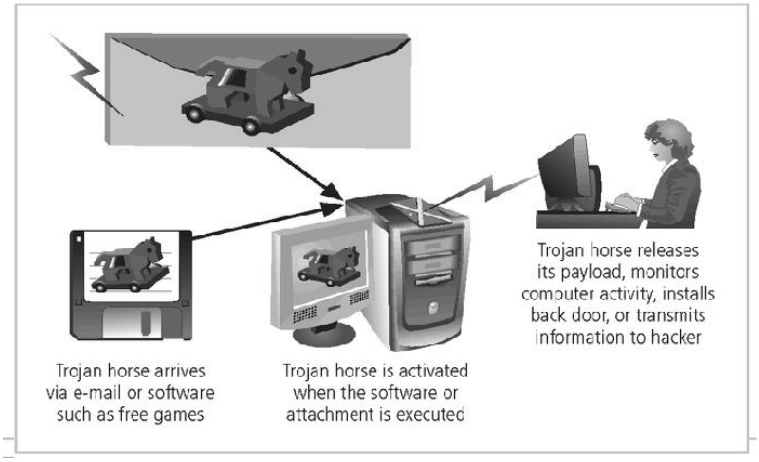
21.What are deliberate software attacks?

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

22.What is Trojan horses attack?

Trojan horses Software programs that hide their true nature (usually destructive), and reveal their designed behavior only
when activated.



23.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

24.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

25.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

26.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

27.What is an attack?

- 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

28. What is a 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

29. List various forms of attacks.

1. IP Scan and Attack
2. Web Browsing
3. Virus
4. Unprotected Shares
5. Mass Mail
6. Hoaxes
7. Back Doors
8. Password Crack
9. Brute Force
10. Dictionary
11. Denial-of-service (DoS)
12. Distributed Denial-of-service (DDoS)
13. Spoofing
14. Man-in-the-Middle
15. Spam

30.What are the 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

31.What is 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

32.Write about Web Browsing attack

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

33.What is 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

34.Write about Unprotected Shares and Mass Mail

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

35.What is Hoaxes

A more devious approach to attacking computer systems is the transmission of a virus hoax, with a real virus attached

36.Write about Back Doors

Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource

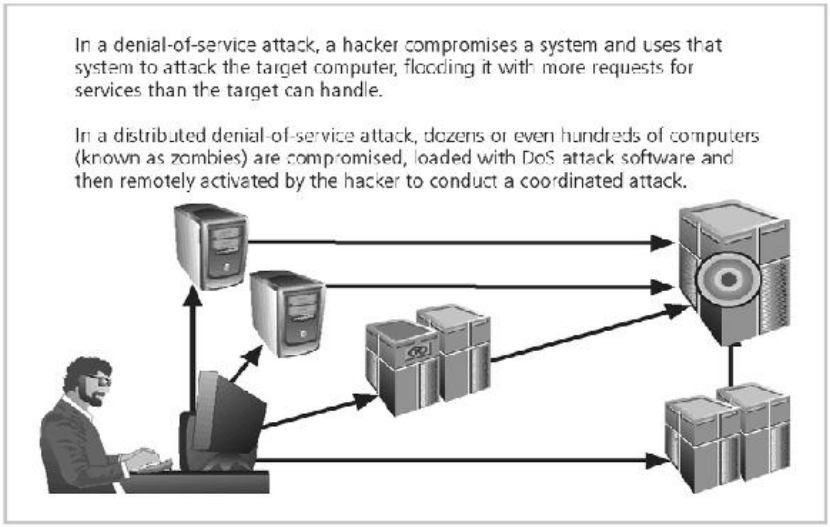
37.Write a short notes on Password Crack and Brute Force

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

38.Write about Dictionary attack

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



39.What is meant by Denial-of-service (DoS)

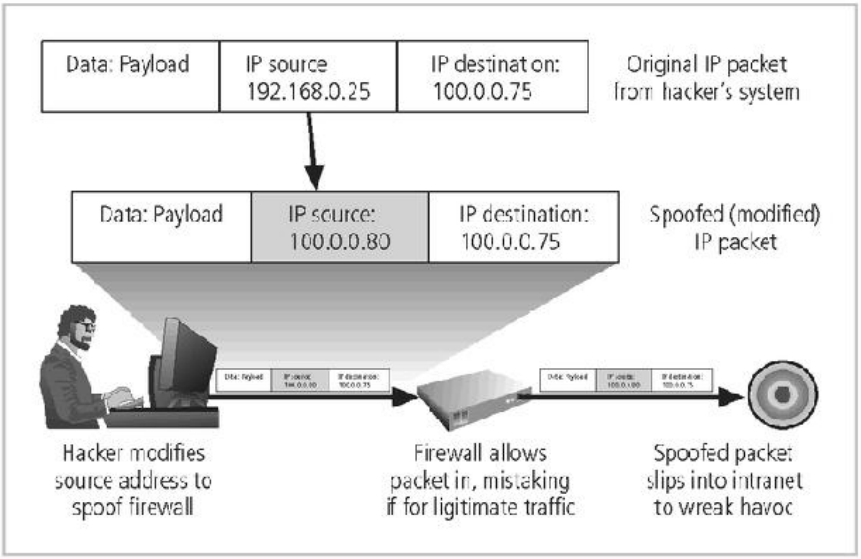
- attacker sends a large number of connection or information requests to a target
- so many requests are made that the target system cannot handle them successfully along with other, legitimate requests for service
- may result in a system crash, or merely an inability to perform ordinary functions

40.What is 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

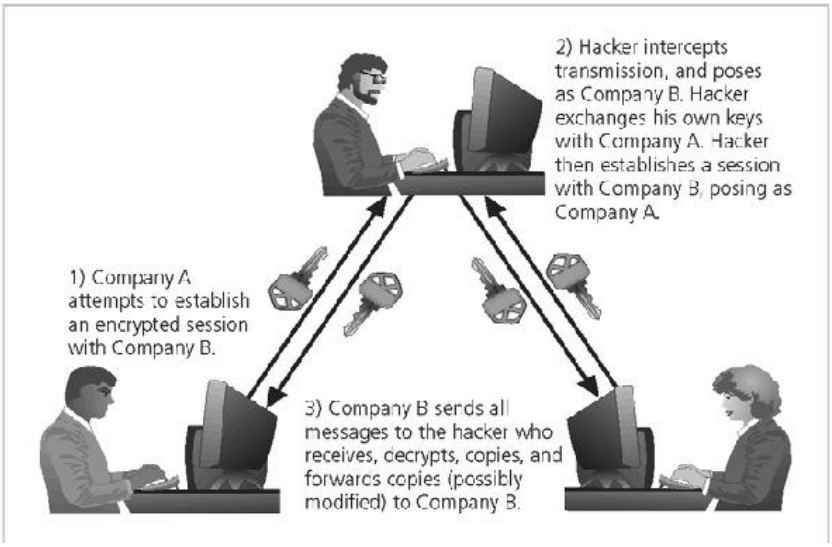
41.What is meant by Spoofing

The 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



42.Write about Man-in-the-Middle attack

An attacker sniffs packets from the network, modifies them, and inserts them back into the network.



43.Write about Spam

unsolicited commercial e-mail - while many consider spam a nuisance rather than an attack, it is emerging as a vector for some attacks

44.What is brick attack

Brick attack is the best configured firewall in the world can't stand up to a well placed brick

45.Write about 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

46.Write short notes on 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

11 Marks

1. Explain Needs for security

NEED FOR SECURITY

The purpose of information security management is to ensure business continuity and reduce business damage by preventing and minimizing the impact of security incidents. The Audit Commission Update report (1998) shows that fraud or cases of IT abuse often occur due to the absence of basic controls, with one half of all detected frauds found by accident. An Information Security Management System (ISMS) enables information to be shared, whilst ensuring the protection of information and computing assets.

At the most practical level, securing the information on your computer means:

Ensuring that your information remains confidential and only those who *should* access that information, *can*.

Knowing that no one has been able to change your information, so you can depend on its accuracy (information integrity).

Making sure that your information is available when you need it (by making back-up copies and, if appropriate, storing the back-up copies off-site).

2.What are the four important functions ,the information security performs in an organization? (BUSINESS NEEDS FIRST)

- ***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

Protecting the Functionality of an Organization

Both general management and IT management are responsible for implementing information security that protects the organization's ability to function. Although many business and government managers shy away from addressing information security because they perceive it to be a technically complex task, in fact, implementing information security has more to do with *management* than with *technology*. Just as managing payroll has more to do with management than with mathematical wage computations, managing information security has more to do with policy and its enforcement than with the technology of its implementation. Each of an organization's communities of interest must address information security in terms of business impact and the cost of business interruption, rather than isolating security as a technical problem. In summary

- 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

Today's organizations are under immense pressure to acquire and operate integrated, efficient,and capable applications. A modern organization needs to create an environment that safeguards these applications, particularly those that are important elements of the organization's infrastructure—operating system platforms, electronic mail (e-mail), and instant messaging (IM) applications. Organizations acquire these elements from a service provider or they build their own. Once an organization's infrastructure is in place, management must continue to oversee it, and not relegate its management to the IT department. In summary

- 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

Without data, an organization loses its record of transactions and/or its ability to deliver value to its customers. Any business, educational institution, or government agency operating within the modern context of connected and responsive services relies on information systems. Even when transactions are not online, information systems and the data they process enable the creation and movement of goods and services. Therefore, protecting *data in motion* and *data at rest* are both critical aspects of information security. The value of data motivates attackers to steal, sabotage, or corrupt it. An effective information security program implemented by management protects the integrity and value of the organization's data. In summary

- 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

To perform effectively, organizations must employ secure infrastructure services appropriate to the size and scope of the enterprise. For instance, a small business may get by using an e-mail service provided by an ISP and augmented with a personal encryption tool. When an organization grows, it must develop additional security services. For example, organizational growth could lead to the need for **public key infrastructure (PKI),** an integrated system of software, encryption methodologies, and legal agreements that can be used to support the entire information infrastructure.

PKI involves the use of digital certificates to ensure the confidentiality of Internet communications and transactions. Into each of these digital certificates, a certificate authority embeds an individual's or an organization's public encryption key, along with other identifying information, and then cryptographically signs the certificate with a tamper-proof seal, thus verifying the integrity of the data within the certificate and validating its use.

In general, as an organization's network grows to accommodate changing needs, more robust technology solutions should replace security programs the organization has outgrown. An example of a robust solution is a firewall, a mechanism that keeps certain kinds of network traffic out of a private network. Another example is caching network appliances, which are devices that store local copies of Internet content, such as Web pages that are frequently accessed by employees. The appliance displays the cached pages to users, rather than accessing the pages from the server each time. In summary

- 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

3. Explain threats and its categories (5 Marks)

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 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

Categories of threat:

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

1. Acts of Human Error or Failure:

Acts performed without intent or malicious purpose by an authorized user.
because of in experience ,improper training,
Making of incorrect assumptions.

One of the greatest threats to an organization's information security is the organization's own employees.

Entry of erroneous data
Accidental deletion or modification of data
Storage of data in unprotected areas.
Failure to protect information can be prevented with
- Training
- Ongoing awareness activities
-Verification by a second party
- Many military applications have robust, dual- approval controls built in .

2. Compromises to Intellectual Property

Intellectual Property is defined as the ownership of ideas and control over the tangible or virtual representation of those ideas.
Intellectual property includes trade secrets, copyrights, trademarks, and patents.
Once intellectual property has been defined and properly identified, breaches to IP constitute a threat to the security of this information.
Organization purchases or leases the IP of other organizations.
Most Common IP breach is the unlawful use or duplication of software based intellectual property more commonly known as **software Piracy**.
Software Piracy affects the world economy.
U.S provides approximately 80% of world's software.

In addition to the laws surrounding software piracy, two watch dog organizations investigate allegations of software abuse.

1. Software and Information Industry Association (SIIA)
   (i.e)Software Publishers Association
2. Business Software Alliance (BSA)

Another effort to combat (take action against) piracy is the online registration process.

3. Deliberate Acts of Espionage or Trespass

Electronic and human activities that can breach the confidentiality of information.
When an unauthorized individual's gain access to the information an organization is trying to protect is categorized as act of espionage or trespass.
Attackers can use many different methods to access the information stored in an information system.

1. Competitive Intelligence[use web browser to get information from market research]
2. Industrial espionage(spying)
3. Shoulder Surfing(ATM)

Trespass

Can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

Sound principles of authentication & authorization can help organizations protect valuable information and systems.

Hackers-> "People who use and create computer software to gain access to information illegally"

There are generally two skill levels among hackers.

Expert Hackers-> Masters of several programming languages, networking protocols, and operating systems .

Unskilled Hackers

4. Deliberate Acts of information Extortion (obtain by force or threat)

Possibility of an attacker or trusted insider stealing information from a computer system and demanding compensation for its return or for an agreement not to disclose the information.

5. Deliberate Acts of sabotage or Vandalism

Destroy an asset or

Damage the image of organization

Cyber terrorism-Cyber terrorists hack systems to conduct terrorist activities through network or internet pathways.

6. Deliberate Acts of Theft

Illegal taking of another's property-- is a constant problem.

Within an organization, property can be physical, electronic, or intellectual.

Physical theft can be controlled by installation of alarm systems.

Trained security professionals.

Electronic theft control is under research.

7. Deliberate Software Attacks

Because of **malicious code** or **malicious software** or sometimes **malware.**

These software components are designed to damage, destroy or deny service to the target system.

More common instances are

Virus, Worms, Trojan horses, Logic bombs, Backdoors.

"The British Internet Service Provider Cloudnine" be the first business "hacked out of existence"

7.1 Virus

Segments of code that performs malicious actions.

Virus transmission is at the opening of Email attachment files.

Macro virus-> Embedded in automatically executing macrocode common in word processors, spreadsheets and database applications.

Boot Virus-> infects the key operating files located in the computer's boot sector.

7.2 Worms

A worm is a malicious program that replicates itself constantly, without requiring another program to provide a safe environment for replication.

Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth.

Eg: MS-Blaster, MyDoom, Netsky, are multifaceted attack worms.

Once the worm has infected a computer , it can redistribute itself to all e-mail addresses found on the infected system.

Furthermore, a worm can deposit copies of itself onto all Web servers that the infected systems can reach, so that users who subsequently visit those sites become infected.

7.3 Trojan Horses

Are software programs that hide their true nature and reveal their designed behavior only when activated.

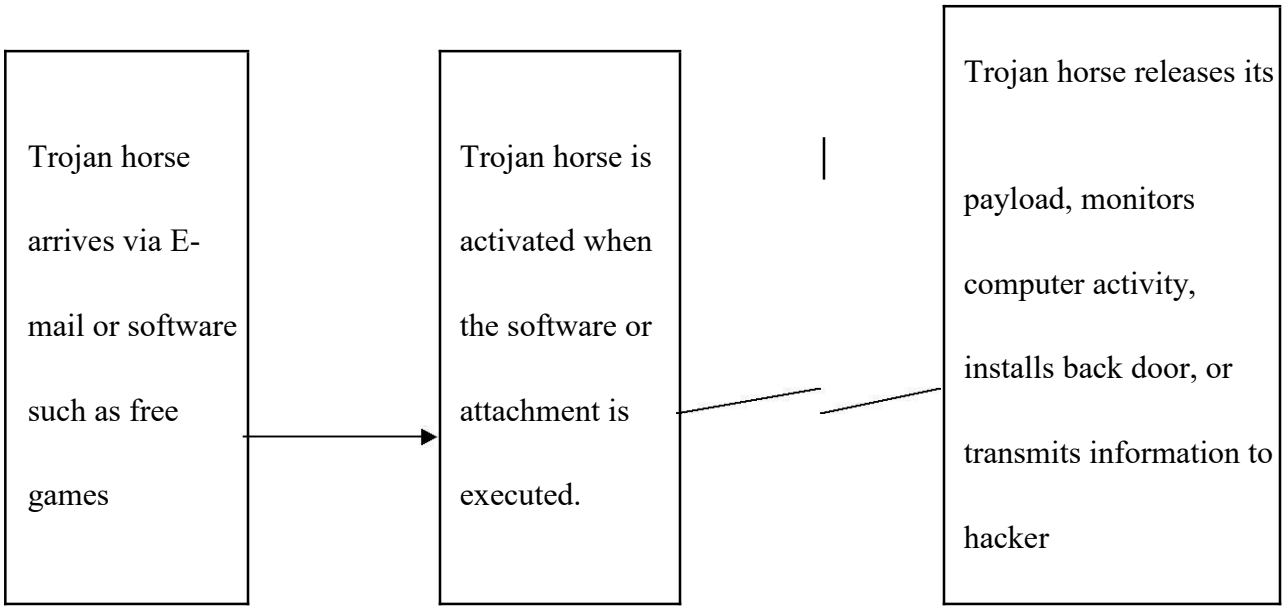


Figure 7.3.1 Trojan horse Attack

7.4 Back Door or Trap Door

A Virus or Worm has a payload that installs a backdoor or trapdoor component in a system, which allows the attacker to access the system at will with special privileges.

Eg: Back Orifice

Polymorphism

A **Polymorphic threat** is one that changes its apparent shape over time, making it undetectable by techniques that look for preconfigured signatures.

These viruses and Worms actually evolve, changing their size, and appearance to elude detection by antivirus software programs.

7.5 Virus & Worm Hoaxes

Types of Trojans

Data Sending Trojans
Proxy Trojans
FTP Trojans
Security software disabler Trojans
Denial of service attack Trojans(DOS)

Virus

A program or piece of code that be loaded on to your computer, without your knowledge and run against your wishes.

Worm

A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Trojan Horse

A destructive program that masquerade on beginning application, unlike viruses, Trojan horse do not replicate themselves.

Blended threat

Blended threats combine the characteristics of virus, worm, Trojan horses & malicious code with server and Internet Vulnerabilities.

Antivirus Program

A Utility that searches a hard disk for viruses and removes any that found.

7.8 Forces of Nature

- **Fire:** Structural fire that damages the building. Also encompasses smoke damage from a fire or water damage from sprinkles systems.
- **Flood:** Can sometimes be mitigated with flood insurance and/or business interruption Insurance.
- **Earthquake:** Can sometimes be mitigated with specific causality insurance and/or business interruption insurance, but is usually a separate policy.
- **Lightning**: An Abrupt, discontinuous natural electric discharge in the atmosphere.
- **Landslide/Mudslide**: The downward sliding of a mass of earth & rocks directly damaging all parts of the information systems.
- **Tornado/Severe Windstorm**
- **Huricane/typhoon**
- **Tsunami**
- **Electrostatic Discharge (ESD)**
- **Dust Contamination**

Since it is not possible to avoid force of nature threats, organizations must implement controls to limit damage.

They must also prepare contingency plans for continued operations, such as disaster recovery plans, business continuity plans, and incident response plans, to limit losses in the face of these threats.

7.9 Deviations in Quality of Service

A product or service is not delivered to the organization as expected.

The Organization's information system depends on the successful operation of many interdependent support systems.

It includes power grids, telecom networks, parts suppliers, service vendors, and even the janitorial staff & garbage haulers.

This degradation of service is a form of **availability disruption.**

Internet Service Issues

Internet service Provider(ISP) failures can considerably undermine the availability of information.

The web hosting services are usually arranged with an agreement providing minimum service levels known as a **Service level Agreement (SLA).**

When a Service Provider fails to meet SLA, the provider may accrue fines to cover losses incurred by the client, but these payments seldom cover the losses generated by the outage.

Communications & Other Service Provider Issues

Other utility services can affect the organizations are telephone, water, waste water, trash pickup, cable television, natural or propane gas, and custodial services.

The loss of these services can impair the ability of an organization to function.

For an example, if the waste water system fails, an organization might be prevented from allowing employees into the building.
This would stop normal business operations.

Power Irregularities

Fluctuations due to power excesses.
Power shortages &
Power losses

This can pose problems for organizations that provide inadequately conditioned power for their information systems equipment.

When voltage levels **spike** (experience a momentary increase),or **surge** (experience prolonged increase), the extra voltage can severely damage or destroy equipment.
The more expensive uninterruptible power supply (UPS) can protect against spikes and surges.

7.10 Technical Hardware Failures or Errors

Resulting in unreliable service or lack of availability
Some errors are terminal, in that they result in unrecoverable loss of equipment.
Some errors are intermittent, in that they resulting in faults that are not easily repeated.

7.11 Technical software failures or errors

This category involves threats that come from purchasing software with unknown, hidden faults.
Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved.
These failures range from bugs to untested failure conditions.

7.12 Technological obsolescence

Outdated infrastructure can lead to unreliable and untrustworthy systems.
Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks.

4.write about intellectual property (IP) (6 Marks)

Many organizations create, or support the development of, intellectual property (IP) as part of their business operations Intellectual property is defined as “the ownership of ideas and control over the tangible or virtual representation of those ideas. Use of another person’s intellectual property may or may not involve royalty payments or permission, but should always include proper credit to the source.

Intellectual property can be trade secrets, copyrights, trademarks, and patents. The unauthorized appropriation of IP constitutes a threat to information security. Employees may have access privileges to the various types of IP, and may be required to use the IP to conduct day-to-day business. Organizations often purchase or lease the IP of other organizations, and must abide by the purchase or licensing agreement for its fair and responsible use. The most common IP breach is the unlawful use or duplication of software-based intellectual property, more commonly known as **software piracy**.

Many individuals and organizations do not purchase software as mandated by the owner’s license agreements. Because most software is licensed to a particular purchaser, its use is restricted to a single user or to a designated user in an organization.

If the user copies the program to another computer without securing another license for transferring the license, he or she has violated the copyright. The Offline, *Violating Software*

Licenses, describes a classic case of this type of copyright violation. Software licenses are strictly enforced by a number of regulatory and private organizations, and software publishers use several control mechanisms to prevent copyright infringement. In addition to the laws against software piracy, two watchdog organizations investigate allegations of software abuse: the Software & Information Industry Association (SIIA) at *www.siia.net*, formerly known as the Software Publishers Association, and the Business Software Alliance (BSA).

A BSA survey in May 2006 revealed that as much as a third of all software in use globally is pirated. A number of technical mechanisms—digital watermarks and embedded code, copyright codes, and even the intentional placement of bad sectors on software media—have been used to enforce copyright laws. The most common tool, a license agreement window that usually pops up during the installation of new software, establishes that the user has read and agrees to the license agreement.

Another effort to combat piracy is the online registration process. Individuals who install software are often asked or even required to register their software to obtain technical support or the use of all features. Some believe that this process compromises personal privacy, because people never really know exactly what information is obtained from their computers and sent to the software manufacturer.

5. When Deliberate Software Attacks occurs? Explain.

Deliberate software attacks occur when an individual or group designs and deploys software to attack a system. Most of this software is referred to as **malicious code** or **malicious software**, or sometimes **malware**. These software components or programs are designed to damage, destroy, or deny service to the target systems.

Some of the more common instances of malicious code are viruses and worms, Trojan horses, logic bombs, and back doors. Prominent among the history of notable incidences of malicious code are the denial-of-service attacks

Virus A computer **virus** consists of segments of code that perform malicious actions. This code behaves very much like a virus pathogen that attacks animals and plants, using the cell's own replication machinery to propagate the attack beyond the initial target. The code attaches itself to an existing program and takes control of that program's access to the targeted computer. The virus-controlled target program then carries out the virus's plan by replicating itself into additional targeted systems.

computer viruses are passed from machine to machine via physical media, e-mail, or other forms of computer data transmission. When these viruses infect a machine, they may immediately scan the local machine for e-mail applications, or even send themselves to every user in the e-mail address book.

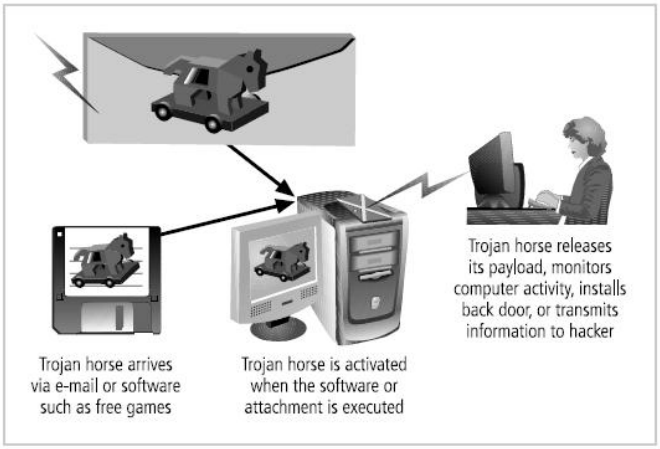
One of the most common methods of virus transmission is via e-mail attachment files. Most organizations block e-mail attachments of certain types and also filter all e-mail for known viruses

The current software marketplace has several established vendors, such as Symantec Norton Anti-Virus and McAfee VirusScan, that provide applications to assist in the control of computer viruses.

Among the most common types of information system viruses are the **macro virus**, which is embedded in automatically executing macro code used by word processors, spread sheets, and database applications, and the **boot virus**, which infects the key operating system files located in a computer's boot sector.

Worms a **worm** is a malicious program that replicates itself constantly, without requiring another program environment. Worms can continue replicating themselves until they completely fill available resources, such as memory, hard drive space, and network bandwidth. Code Red, Sircam, Nimda ("admin" spelled backwards), and Klez are examples of a class of worms that combines multiple modes of attack into a single package.

Trojan Horses Trojan horses are software programs that hide their true nature and reveal their designed behavior only when activated. Trojan horses are frequently disguised as helpful, interesting, or necessary pieces of software, such as readme.exe files often included with shareware or freeware packages. Unfortunately, like their namesake in Greek legend, once Trojan horses are brought into a system, they become activated and can wreak havoc on the unsuspecting user.



Back Door or Trap Door A virus or worm can have a payload that installs a **back door** or **trap door** component in a system, which allows the attacker to access the system at will with special privileges. Examples of these kinds of payloads include Subseven and Back Orifice.

Polymorphic Threats - A **polymorphic threat** is one that over time changes the way it appears to antivirus software programs, making it undetectable by techniques that look for preconfigured signatures. These viruses and worms actually evolve, changing their size and other external file characteristics to elude detection by antivirus software programs.

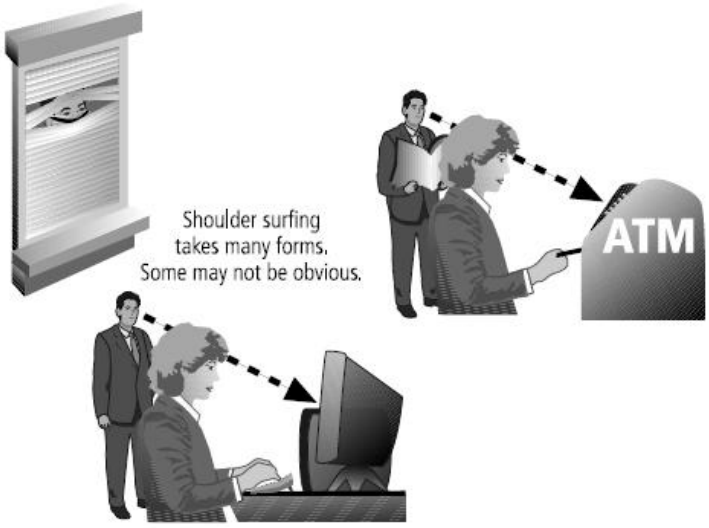
Virus and Worm Hoaxes As frustrating as viruses and worms are, perhaps more time and money is spent on resolving **virus hoaxes**. Well-meaning people can disrupt the harmony and flow of an organization when they send group e-mails warning of supposedly dangerous viruses that don't exist. When people fail to follow virus-reporting procedures, the network becomes overloaded, and much time and energy is wasted as users forward the warning message to everyone they know, post the message on bulletin boards, and try to update their antivirus protection software. A number of Internet resources enable individuals to research viruses to determine if they are fact or fiction.

6. Write about Espionage or Trespass

Espionage or trespass is a well-known and broad category of electronic and human activities that can breach the confidentiality of information. When an unauthorized individual gains access to the information an organization is trying to protect, that act is categorized as espionage or trespass. Attackers can use many different methods to access the information stored in an information system. Some

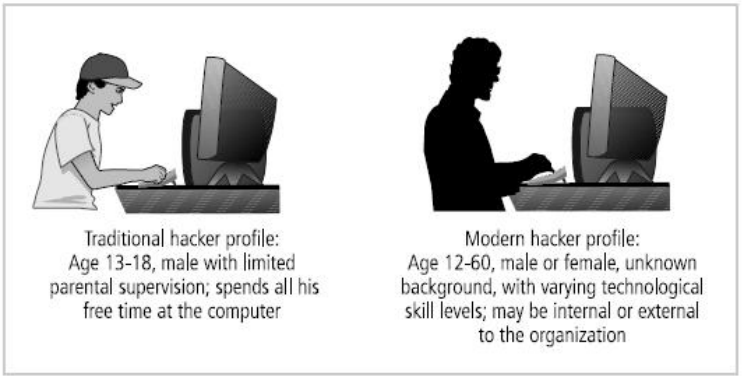
information gathering techniques are quite legal, for example, using a Web browser to perform market research. These legal techniques are called, collectively, **competitive intelligence**. When information gatherers employ techniques that cross the threshold of what is legal or ethical, they are conducting **industrial espionage**. Some forms of espionage are relatively low tech. One example, called **shoulder surfing**

This technique is used in public or semipublic settings when individuals gather information they are not authorized to have by looking over another individual's shoulder or viewing the information from a distance. Instances of shoulder surfing occur at computer terminals, desks, ATM machines, on the bus or subway where people use smartphones and tablet PCs, or other places where a person is accessing confidential information



Acts of **trespass** can lead to unauthorized real or virtual actions that enable information gatherers to enter premises or systems they have not been authorized to enter.

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



A hacker frequently spends long hours examining the types and structures of the targeted systems and uses skill, guile, or fraud to attempt to bypass the controls placed around information that is the property of someone else.

There are generally two skill levels among hackers. The first is the **expert hacker**, or **elite hacker**, who develops software scripts and program exploits used by those in the second category, the novice or **unskilled hacker**.

The expert hacker is usually a master of several programming languages, networking protocols, and operating systems and also exhibits a mastery of the technical environment of the chosen targeted system. These programs are automated exploits that allow novice hackers to act as **script kiddies**—hackers of limited skill who use expertly written software to attack a system—or **packet monkeys**—script kiddies who use automated exploits to engage in distributed denial-of-service attacks .A **phreaker** hacks the public telephone network to make free calls or disrupt services.

7. Explain the various Forces of Nature

Forces of nature, *force majeure*, or acts of God can present some of the most dangerous threats, because they usually occur with very little warning and are beyond the control of people.

These threats, which include events such as fires, floods, earthquakes, and lightning as well as volcanic eruptions and insect infestations, can disrupt not only the lives of individuals but also the storage, transmission, and use of information.

Fire: In this context, usually a structural fire that damages a building housing computing equipment that comprises all or part of an information system, as well as smoke damage and/or water damage from sprinkler systems or firefighters. This threat can usually be mitigated with fire casualty insurance and/or business interruption insurance.

Flood: An overflowing of water onto an area that is normally dry, causing direct damage to all or part of the information system or to the building that houses all or part of the information system. A flood might also disrupt operations through interruptions in access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with flood insurance and/or business interruption insurance.

Earthquake: A sudden movement of the earth's crust caused by the release of stress accumulated along geologic faults or by volcanic activity. Earthquakes can cause direct damage to all or part of the information system or, more often, to the building that houses it, and can also disrupt operations through interruptions in access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with specific casualty insurance and/or business interruption insurance, but is usually a separate policy.

Lightning: An abrupt, discontinuous natural electric discharge in the atmosphere. Lightning usually directly damages all or part of the information system an/or its power distribution components. It can also cause fires or other damage to the building that houses all or part of the information system, and disrupt operations by interfering with access to the buildings that house all or part of the information system. This threat can usually be mitigated with multipurpose casualty insurance and/or business interruption insurance.

Landslide or mudslide: The downward sliding of a mass of earth and rock directly damaging all or part of the information system or, more likely, the building that houses it. Land- or mudslides also disrupt

operations by interfering with access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

Tornado or severe windstorm: A rotating column of air ranging in width from a few yards to more than a mile and whirling at destructively high speeds, usually accompanied by a funnel-shaped downward extension of a cumulonimbus cloud. Storms can directly damage all or part of the information system or, more likely, the building that houses it, and can also interrupt access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

Hurricane or typhoon: A severe tropical cyclone originating in the equatorial regions of the Atlantic Ocean or Caribbean Sea or eastern regions of the Pacific Ocean (typhoon), traveling north, northwest, or northeast from its point of origin, and usually involving heavy rains. These storms can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal or low-lying areas may experience flooding (see above). These storms may also disrupt operations by interrupting access to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

Tsunami: A very large ocean wave caused by an underwater earthquake or volcanic eruption. These events can directly damage all or part of the information system or, more likely, the building that houses it. Organizations located in coastal areas may experience tsunamis. Tsunamis may also cause disruption to operations through interruptions in access or electrical power to the buildings that house all or part of the information system. This threat can sometimes be mitigated with casualty insurance and/or business interruption insurance.

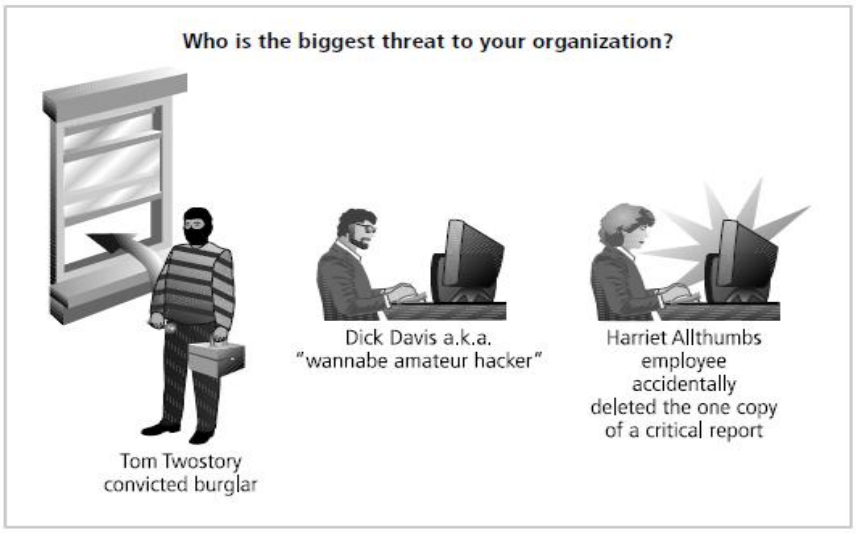
Electrostatic discharge (ESD): Usually, static electricity and ESD are little more than a nuisance. Unfortunately, however, the mild static shock we receive when walking across a carpet can be costly or dangerous when it ignites flammable mixtures and damages costly electronic components. Static electricity can draw dust into clean-room environments or cause products to stick together. The cost of ESD-damaged electronic devices and interruptions to service can range from only a few cents to several millions of dollars for critical systems. Loss of production time in information processing due to ESD impact is significant. While not usually viewed as a threat, ESD can disrupt information systems, but it is not usually an insurable loss unless covered by business interruption insurance.

Dust contamination: Some environments are not friendly to the hardware components of information systems. Because dust contamination can shorten the life of information systems or cause unplanned downtime, this threat can disrupt normal operations.

8. Explain Human Error or Failure

This category includes acts performed without intent or malicious purpose by an authorized user. When people use information systems, mistakes happen. Inexperience, improper training, and the incorrect assumptions are just a few things that can cause these misadventures. Regardless of the cause, even innocuous mistakes can produce extensive damage. For example, a simple keyboarding error can cause worldwide Internet outages.

One of the greatest threats to an organization's information security is the organization's own employees. Employees are the threat agents closest to the organizational data. Because employees use data in everyday activities to conduct the organization's business, their mistakes represent a serious threat to the confidentiality, integrity, and availability of data even, as Figure suggests, relative to threats from outsiders. This is because 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, and failure to protect information.



Leaving classified information in unprotected areas, such as on a desktop, on a Web site, or even in the trash can, is as much a threat to the protection of the information as is the individual who seeks to exploit the information, because one person's carelessness can create a vulnerability and thus an opportunity for an attacker. However, if someone damages or destroys data on purpose, the act belongs to a different threat category.

Much human error or failure can be prevented with training and ongoing awareness activities, but also with controls, ranging from simple procedures, such as requiring the user to type a critical command twice, to more complex procedures, such as the verification of commands by a second party. An example of the latter is the performance of key recovery actions in PKI systems. Many military applications have robust, dual-approval controls built in.

Some systems that have a high potential for data loss or system outages use expert systems to monitor human actions and request confirmation of critical inputs.

9.Explain Attacks.

ATTACKS

An attack is an act of or action that takes advantage of a vulnerability to compromise a controlled system.

It is accomplished by a **threat agent** that damages or steals an organization's information or physical asset.

Vulnerability is an identified weakness in a controlled system, where controls are not present or are no longer effective.

Attacks exist when a specific act or action comes into play and may cause a potential loss.

i. Malicious code

The malicious code 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 malicious code attack is the polymorphic or multivector, worm.

These attack programs use up to six known attack vectors to exploit a variety of vulnerabilities in commonly found information system devices.

ii. Attack Replication Vectors

1. IP scan & attack
2. Web browsing
3. Virus
4. Unprotected shares
5. Mass mail
6. Simple Network Management Protocol(SNMP)

1. IP scan & attack

The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers.

2. Web browsing

If the infected system has write access to any Web pages, it makes all Web content files (.html,.asp,.cgi & others) infectious, so that users who browse to those pages become infected.

3. 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.

4. Unprotected shares

Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.

5. Mass Mail

By sending E-mail infections to addresses found in the address book, the infected machine infects many users, whose mail -reading programs also automatically run the program & infect other systems.

6. Simple Network Management Protocol (SNMP)

By using the widely known and common passwords that were employed in early versions of this protocol, the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

iii. Examples

Hoaxes

A more devious approach to attacking the computer systems is the transmission of a virus hoax with a real virus attached.

Even though these users are trying to avoid infection, they end up sending the attack on to their co-workers.

Backdoors

Using a known or previously unknown and newly discovered access mechanism, an attacker can gain access to a system or network resource through a back door.

Sometimes these entries are left behind by system designers or maintenance staff, and thus referred to as trap doors.

A trap door is hard to detect, because very often the programmer who puts it in place also makes the access exempt from the usual audit logging features of the system.

Password Crack

Attempting to reverse calculate a password is often called **cracking.**

A password can be hashed using the same algorithm and compared to the hashed results, If they are same, the password has been cracked.

The (SAM) Security Account Manager file contains the hashed representation of the user's password.

Brute Force

The application of computing & network resources to try every possible combination of options of a password is called a **Brute force attack.**

This is often an attempt to repeatedly guess passwords to commonly used accounts, it is sometimes called a **password attack.**

Spoofing

It is a technique used to gain unauthorized access to computers, where in the intruder sends messages to a computer that has an IP address that indicates that the messages are coming from a trusted host.

Data: Payload	IP source: 192.168.0.25	IP destination: 100.0.0.75

Original IP packet

From hacker's system

Data: Payload	IP source: 100.0.0.80	IP destination: 100.0.0.75

Spoofed (modified)
IP packet

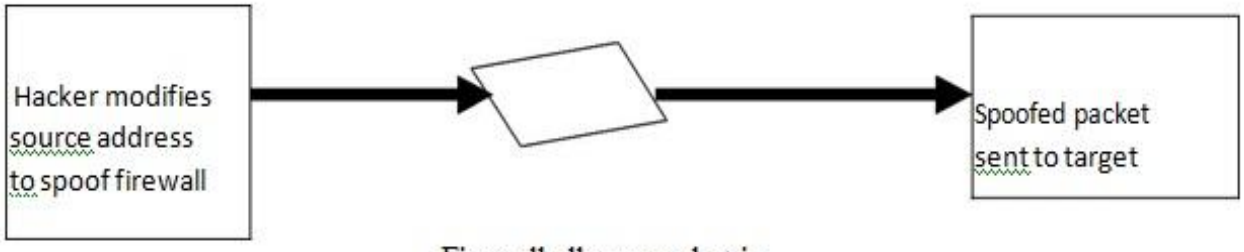


Figure 2.4.3.1 IP spoofing

Dictionary

This is another form of the brute force attack noted above for guessing passwords.

The **dictionary attack** narrows the field by selecting specific accounts to attack and uses a list of commonly used passwords instead of random combinations.

Denial –of- Services(DOS) & Distributed Denial –of- Service(DDOS)

The attacker sends a large number of connection or information requests to a target.

This may result in the system crashing, or simply becoming unable to perform ordinary functions.
DDOS is an attack in which a coordinated stream of requests is launched dagainst a target from many locations at the same.

Man-in-the –Middle

Otherwise called as **TCP hijacking attack**.
An attacker monitors packets from the network, modifies them, and inserts them back into the network.
This type of attack uses IP spoofing.
It allows the attacker to change, delete, reroute, add, forge or divert data.
TCP hijacking session, the spoofing involves the interception of an encryption key exchange.

SPAM

Spam is unsolicited commercial E-mail.
It has been used to make malicious code attacks more effective.
Spam is considered as a trivial nuisance rather than an attack.
It is the waste of both computer and human resources it causes by the flow of unwanted E-mail.

Mail Bombing

Another form of E-mail attack that is also a DOS called a **mail bomb**.
Attacker routes large quantities of e-mail to the target.
The target of the attack receives unmanageably large volumes of unsolicited e-mail.
By sending large e-mails, attackers can take advantage of poorly configured e-mail systems on the Internet and trick them into sending many e-mails to an address chosen by the attacker.
The target e-mail address is buried under thousands or even millions of unwanted e-mails.

Sniffers

A **sniffer** is a program or device that can monitor data traveling over a network.
Unauthorized sniffers can be extremely dangerous to a network's security, because they are virtually impossible to detect and can be inserted almost anywhere.
Sniffer often works on TCP/IP networks, where they are sometimes called **"packet Sniffers".**

Social Engineering

It is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.

An attacker gets more information by calling others in the company and asserting his/her authority by mentioning chief's name.

Buffer Overflow

A buffer overflow is an application error that occurs when more data is sent to a buffer than it can handle.
Attacker can make the target system execute instructions.

Timing Attack

Works by exploring the contents of a web browser's cache.

These attacks allow a Web designer to create a malicious form of cookie, that is stored on the client's system.

The cookie could allow the designer to collect information on how to access password-protected sites.

8. Explain Legal, Ethical and professional issues in Information security

LEGAL, ETHICAL, AND PROFESSIONAL ISSUES IN INFORMATION SECURITY

i.Law and Ethics in Information Security

Laws are rules that mandate or prohibit certain behavior in society; they are drawn from **ethics**, which define socially acceptable behaviors. The key difference between laws and ethics is that laws carry the sanctions of a governing authority and ethics do not. Ethics in turn are based on **Cultural mores.**

Types of Law

Civil law
Criminal law
Tort law
Private law
Public law

ii. Relevant U.S. Laws – General

Computer Fraud and Abuse Act of 1986
National Information Infrastructure Protection Act of 1996
USA Patriot Act of 2001
Telecommunications Deregulation and Competition Act of 1996
Communications Decency Act (CDA)
Computer Security Act of 1987

Privacy

The issue of privacy has become one of the hottest topics in information

The ability to collect information on an individual, combine facts from separate sources, and merge it with other information has resulted in databases of information that were previously impossible to set up

The aggregation of data from multiple sources permits unethical organizations to build databases of facts with frightening capabilities

Privacy of Customer Information

Privacy of Customer Information Section of Common Carrier Regulations
Federal Privacy Act of 1974
The Electronic Communications Privacy Act of 1986

The Health Insurance Portability & Accountability Act Of 1996 (HIPAA) also known as the Kennedy-Kassebaum Act

The Financial Services Modernization Act or Gramm-Leach-Bliley Act of 1999

Table : Key U.S Laws of Interest to Information Security Professionals

ACT	SUBJECT	DATE	DESCRIPTION
Communications Act of 1934,updated by Telecommunications Deregulation & Competition Act	Telecommunications	1934	Regulates interstate and foreign Telecommunications.
Computer Fraud & Abuse Act	Threats to computers	1986	Defines and formalizes laws to counter threats from computer related acts and offenses.
Computer Security Act of 1987	Federal Agency Information Security	1987	Requires all federal computer systems that contain classified information to have surety plans in place, and requires periodic security training for all individuals who operate, design, or manage such systems.
Economic Espionage Act of 1996	Trade secrets.	1996	Designed to prevent abuse of information gained by an individual working in one company and employed by another.
Electronic Communications Privacy Act of 1986	Cryptography	1986	Also referred to as the Federal Wiretapping Act; regulates interception and disclosure of electronic information.
Federal Privacy Act of 1974	Privacy	1974	Governs federal agency use of personal information.
Gramm-Leach-	Banking	1999	Focuses on facilitating

Bliley Act of 1999			affiliation among banks, insurance and securities firms; it has significant impact on the privacy of personal information used by these industries.
Health Insurance Portability and Accountability Act	Health care privacy	1996	Regulates collection, storage, and transmission of sensitive personal health care information.
National Information Infrastructure protection Act of 1996	Criminal intent	1996	Categorized crimes based on defendant's authority to access computer and criminal intent.
Sarbanes-Oxley Act of 2002	Financial Reporting	2002	Affects how public organizations and accounting firms deal with corporate governance, financial disclosure, and the practice of public accounting.
Security and Freedom through Encryption Act of 1999	Use and sale of software that uses or enables encryption.	1999	Clarifies use of encryption for people in the United states and permits all persons in the U.S. to buy or sell any encryption product and states that the government cannot require the use of any kind of key escrow system for encryption products.
U.S.A. Patriot Act of 2001	Terrorism	2001	Defines stiffer penalties for prosecution of terrorist crimes.

Export and Espionage Laws

Economic Espionage Act (EEA) of 1996
Security and Freedom Through Encryption Act of 1997 (SAFE)

US Copyright Law

Intellectual property is recognized as a protected asset in the US
US copyright law extends this right to the published word, including electronic formats
Fair use of copyrighted materials includes

- the use to support news reporting, teaching, scholarship, and a number of other related permissions

- the purpose of the use has to be for educational or library purposes, not for profit, and should not be excessive

Freedom of Information Act of 1966 (FOIA)

The **Freedom of Information Act** provides any person with the right to request access to federal agency records or information, not determined to be of national security

- US Government agencies are required to disclose any requested information on receipt of a written request

There are exceptions for information that is protected from disclosure, and the Act does not apply to state or local government agencies or to private businesses or individuals, although many states have their own version of the FOIA

State & Local Regulations

In addition to the national and international restrictions placed on an organization in the use of computer technology, each state or locality may have a number of laws and regulations that impact operations

It is the responsibility of the information security professional to understand state laws and regulations and insure the organization's security policies and procedures comply with those
laws and regulations

iii. International Laws and Legal Bodies

Recently the Council of Europe drafted the **European Council Cyber-Crime Convention,** designed

- to create an international task force to oversee a range of security functions associated with Internet activities,
- to standardize technology laws across international borders

It also attempts to improve the effectiveness of international investigations into breaches of technology law

This convention is well received by advocates of intellectual property rights with its emphasis on copyright infringement prosecution

Digital Millennium Copyright Act (DMCA) Digital Millennium Copyright Act (DMCA)

The Digital Millennium Copyright Act (DMCA) is the US version of an international effort to reduce the impact of copyright, trademark, and privacy infringement

The European Union Directive 95/46/EC increases protection of individuals with regard to the processing of personal data and limits the free movement of such data

The United Kingdom has already implemented a version of this directive called the Database Right

United Nations Charter

To some degree the **United Nations Charter** provides provisions for information security during Information Warfare

Information Warfare (IW) involves the use of information technology to conduct offensive operations as part of an organized and lawful military operation by a sovereign state

IW is a relatively new application of warfare, although the military has been conducting electronic warfare and counter-warfare operations for decades, jamming, intercepting, and spoofing enemy communications

Policy Versus Law

Most organizations develop and formalize a body of expectations called policy
Policies function in an organization like laws
For a policy to become enforceable, it must be:

- Distributed to all individuals who are expected to comply with it
- Readily available for employee reference

- Easily understood with multi-language translations and translations for visually impaired, or literacy-impaired employees
- Acknowledged by the employee, usually by means of a signed consent form

Only when all conditions are met, does the organization have a reasonable expectation of effective policy

iv. Ethical Concepts in Information Security

Many Professional groups have explicit rules governing ethical behavior in the workplace. For example, doctors and lawyers who commit egregious violations of their professions' canons of conduct can be removed from practice. Unlike the medical and legal fields, however, the information technology field in general, and the information security field in particular, do not have a binding code of ethics. Instead, professional associations—such as the Association for Computing Machinery (ACM) and the Information Systems Security Association—and certification agencies—such as the International Information Systems Security Certification Consortium, Inc., or (ISC)2—work to establish the profession's ethical codes of conduct.

While these professional organizations can prescribe ethical conduct, they do not always have the authority to banish violators from practicing their trade

Ethical Differences Across Cultures

Cultural differences can make it difficult to determine what is and is not ethical—especially when it comes to the use of computers. Studies on ethics and computer use reveal that people of different nationalities have different perspectives; difficulties arise when one nationality's ethical behavior violates the ethics of another national group.

For example, to Western cultures, many of the ways in which Asian cultures use computer technology is software piracy.14 This ethical conflict arises out of Asian traditions of collective ownership, which clash with the protection of intellectual property. Approximately 90 percent of all software is created in the United States. Some countries are more relaxed with intellectual property copy restrictions than others. This study did not categorize or classify the responses as ethical or unethical. Instead, the responses only indicated a degree of ethical sensitivity or knowledge about the performance of the individuals in the short case studies.

The scenarios were grouped into three categories of ethical computer use: software license infringement, illicit use, and misuse of corporate resources.

Software License Infringement The topic of software license infringement, or piracy, is routinely covered by the popular press. Among study participants, attitudes toward piracy were generally similar; however, participants from the United States and the Netherlands showed statistically significant differences in attitudes from the overall group. Participants from the United States were significantly less tolerant of piracy, while those from the Netherlands were significantly more permissive.

This could mean that the individuals surveyed *understood* what software license infringement was, but felt either that their use was not piracy, or that their society permitted this piracy in some way. Peer pressure, the lack of legal disincentives, the lack of punitive measures, and number of other reasons could a explain why users in these alleged piracy centers disregarded intellectual property laws despite their professed attitudes toward them.

Illicit Use The study respondents unilaterally condemned viruses, hacking, and other forms of system abuse. There were, however, different degrees of tolerance for such activities among the groups. The low overall degree of tolerance for illicit system use may be a function of the easy correspondence between the common crimes of breaking and entering, trespassing, theft, and destruction of property and their computer-related counterparts.

Misuse of Corporate Resources The scenarios used to examine the levels of tolerancefor misuse of corporate resources each presented a different degree of noncompany use of corporate assets without

specifying the company's policy on personal use of company resources. In general, individuals displayed a rather lenient view of personal use of company equipment.

Many people, regardless of cultural background, believe that unless an organization explicitly forbids personal use of its computing resources, such use is acceptable.

Ethics and Education

Attitudes toward the ethics of computer use are affected by many factors other than nationality. Differences are found among individuals within the same country, within the same social class, and within the same company. Key studies reveal that the overriding factor in levelling the ethical perceptions within a small population is education.

Employees must be trained and kept aware of a number of topics related to information security, not the least of which are the expected behaviors of an ethical employee. This is especially important in information security, as many employees may not have the formal technical training to understand that their behavior is unethical or even illegal. Proper ethical and legal training is vital to creating an informed, well prepared, and low-risk system user.

Deterring Unethical and Illegal Behavior

There are three general causes of unethical and illegal behavior:

- Ignorance—Ignorance of the law is no excuse; however, ignorance of policy and procedures is. The first method of deterrence is education. This is accomplished by means of designing, publishing, and disseminating organization policies and relevant laws, and also obtaining agreement to comply with these policies and laws from all members of the organization. Reminders, training, and awareness programs keep the policy information in front of the individual and thus better support retention and compliance.
- Accident—Individuals with authorization and privileges to manage information within the organization are most likely to cause harm or damage by accident. Careful planning and control helps prevent accidental modification to systems and data.
- Intent—Criminal or unethical intent goes to the state of mind of the person performing the act; it is often necessary to establish criminal intent to successfully prosecute offenders. Protecting a system against those with intent to cause harm or damage is best accomplished by means of technical controls, and vigorous litigation or prosecution if these controls fail.

Whatever the cause of illegal, immoral, or unethical behavior, one thing is certain: it is the responsibility of information security personnel to do everything in their power to deter these acts and to use policy, education and training, and technology to protect information and systems. However, laws and policies and their associated penalties only deter if three conditions are present:

- Fear of penalty—Potential offenders must fear the penalty. Threats of informal reprimand or verbal warnings may not have the same impact as the threat of imprisonment or forfeiture of pay.
- Probability of being caught—Potential offenders must believe there is a strong possibility of being caught. Penalties will not deter illegal or unethical behavior unless there is reasonable fear of being caught.
- Probability of penalty being administered—Potential offenders must believe that the penalty will in fact be administered.

Deterrence to Unethical and Illegal Behavior

Deterrence - preventing an illegal or unethical activity
Laws, policies, and technical controls are all examples of deterrents
Laws and policies only deter if three conditions are present:

- Fear of penalty
- Probability of being caught
- Probability of penalty being administered

9. Write about the following: (6 Marks)

a. **Information Extortion**
b. **Missing, Inadequate, or Incomplete Organizational Policy or Planning**
c. **Missing, Inadequate, or Incomplete Controls**
d. **Sabotage or Vandalism**

Information Extortion

Information extortion occurs when an attacker or trusted insider steals information from a computer system and demands compensation for its return or for an agreement not to disclose it. Extortion is common in credit card number theft.

For example, Web-based retailer CD Universe was the victim of a theft of data files containing customer credit card information.

The culprit was a Russian hacker named Maxus, who hacked the online vendor and stole several hundred thousand credit card numbers. When the company refused to pay the $100,000 blackmail, he posted the card numbers to a Web site, offering them to the criminal community. His Web site became so popular he had to restrict access.

Missing, Inadequate, or Incomplete Organizational Policy or Planning

Missing, inadequate, or incomplete organizational policy or planning makes an organization vulnerable to loss, damage, or disclosure of information assets when other threats lead to attacks. Information security is, at its core, a management function. The organization's executive leadership is responsible for strategic planning for security as well as for IT and business functions—a task known as governance.

Missing, Inadequate, or Incomplete Controls

Missing, inadequate, or incomplete controls—that is, security safeguards and information asset protection controls that are missing, misconfigured, antiquated, or poorly designed or managed—make an organization more likely to suffer losses when other threats lead to attacks.

Sabotage or Vandalism

This category of threat involves the deliberate sabotage of a computer system or business, or acts of vandalism to either destroy an asset or damage the image of an organization. These acts can range from petty vandalism by employees to organized sabotage against an organization. Although not necessarily financially devastating, attacks on the image of an organization are serious. Vandalism to a

Web site can erode consumer confidence, thus diminishing an organization's sales and net worth, as well as its reputation.

Today, security experts are noticing a rise in another form of online vandalism, **hacktivist** or **cyberactivist** operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.

10.Explain the following (6 Marks)

a. **Theft**
b. **Technical Hardware Failures or Errors**
c. **Technical Software Failures or Errors**
d. **Technological Obsolescence**

Theft

The threat of **theft**—the illegal taking of another's property, which can be physical, electronic, or intellectual—is a constant. The value of information is diminished when it is copied without the owner's knowledge.

Physical theft can be controlled quite easily by means of a wide variety of measures, from locked doors to trained security personnel and the installation of alarm systems. Electronic theft, however, is a more complex problem to manage and control. When someone steals a physical object, the loss is easily detected; if it has any importance at all, its absence is noted. When electronic information is stolen, the crime is not always readily apparent. If thieves are clever and cover their tracks carefully, no one may ever know of the crime until it is far too late.

Technical Hardware Failures or Errors

Technical hardware failures or errors occur when a manufacturer distributes equipment containing a known or unknown flaw. These defects can cause the system to perform outside of expected parameters, resulting in unreliable service or lack of availability. Some errors are terminal—that is, 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, and thus, equipment can sometimes stop working, or work in unexpected ways.

Technical Software Failures or Errors

Large quantities of computer code are written, debugged, published, and sold before all their bugs are detected and resolved. Sometimes, combinations of certain software and hardware reveal new bugs. These failures range from bugs to untested failure conditions. Sometimes these bugs are not errors, but rather purposeful shortcuts left by programmers for benign or malign reasons. Collectively, shortcut access routes into programs that bypass security checks are called trap doors and can cause serious security breaches. Software bugs are so commonplace that entire Web sites are dedicated to documenting them. Among the most often used is Bugtraq which provides up-to-the-minute information on the latest security vulnerabilities, as well as a very thorough archive of past bugs.

Technological Obsolescence

Antiquated or outdated infrastructure can lead to unreliable and untrustworthy systems. Management must recognize that when technology becomes outdated, there is a risk of loss of data integrity from attacks. Management's strategic planning should always include an analysis of the

technology currently in use. Ideally, proper planning by management should prevent technology from becoming obsolete, but when obsolescence is manifest, management must take immediate action. IT professionals play a large role in the identification of probable obsolescence.

Recently, the software vendor Symantec retired support for a legacy version of its popular antivirus software, and organizations interested in continued product support were obliged to upgrade immediately to a different antivirus control software. In organizations where IT personnel had kept management informed of the coming retirement, these replacements were made more promptly and at lower cost than at organizations where the software was allowed to become obsolete.

11.What are different acts of Human error or failure and how it can be prevented?(5 Marks)

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)

12.What is Intellectual property? How it can be protected? (5 Marks)

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 a new software.

16. **What is deliberate acts of espionage or trespass? (5 Marks)**

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

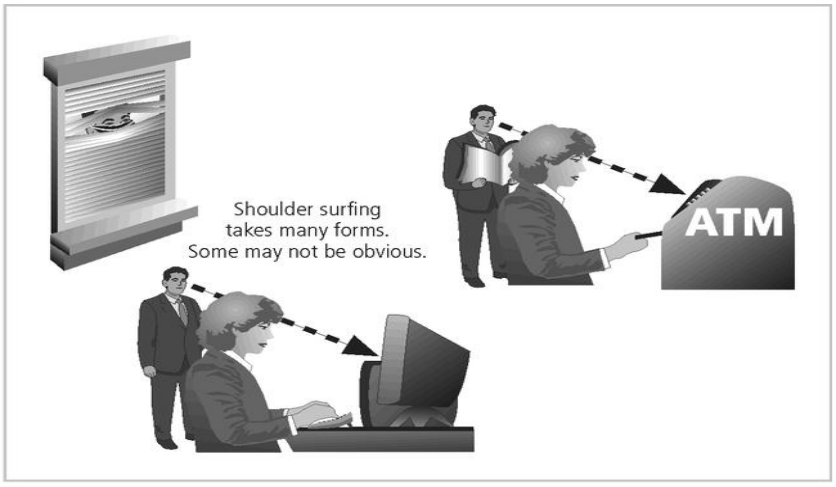


FIGURE 2-2 Shoulder Surfing

UNIT – III

SECURITY ANALYSIS: Risk Management: Identifying and Assessing Risk - Assessing and Controlling Risk - Trends in Information Risk Management - Managing Risk in an Intranet Environment.

---

2 MARKS

1. What is Risk Management?

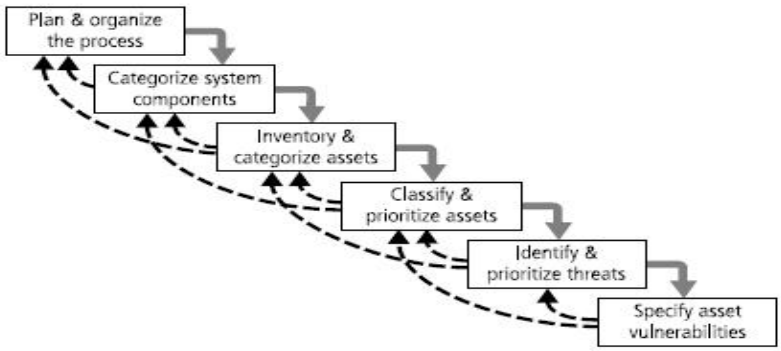
Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to ensure the confidentiality, integrity, and availability of all the components in the organization's information system.

2. Describe Accountability for Risk Management?

It is the responsibility of each community of interest to manage risks; each community has a role to play:

a. Information Security - best understands the threats and attacks that introduce risk into the organization
b. Management and Users – play a part in the early detection and response process - they also insure sufficient resources are allocated
c. Information Technology – must assist in building secure systems and operating them safely

3. Draw components of risk identification?



4. What are the asset attributes?

For People:

- Position name/number/ID – try to stay aware from names and stick to identifying positions, roles or functions
- Supervisor
- Security clearance level
- Special skills

For Procedures:

- Description
- Intended purpose
- What elements is it tied to
- Where is it stored for reference
- Where is it stored for update purposes

For Data:

- Classification
- Owner/creator/manager
- Size of data structure

- Data structure used – sequential, relational
- Online or offline
- Where located
- Backup procedures employed

5. **Classify the information asset ?**
    a. confidential data
    b. internal data
    c. public data
6. **What are Questions to assist in developing the criteria to be used for asset valuation?**
    a. Which information asset is the most critical to the success of the organization?
    b. Which information asset generates the most revenue?
    c. Which information asset generates the most profitability?
    d. Which information asset would be the most expensive to replace?
    e. Which information asset would be the most expensive to protect?
    f. Which information asset would be the most embarrassing or cause the greatest liability if revealed?

7. **What is Security Clearances?**
    - Each user of data in the organization is assigned a single level of authorization indicating the level of classification
    - Before an individual is allowed access to a specific set of data, he or she must meet the need-to-know requirement
8. **What are requirements for the management of information?**
    Includes the storage, distribution, portability, and destruction of classified information
    a. Must be clearly marked as such
    b. When stored, it must be unavailable to unauthorized individuals
    c. When carried should be inconspicuous, as in a locked briefcase or portfolio
9. **List threats to information security?**

TABLE 4-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

10. What is threat assessment?

Each threat must be further examined to assess its potential to impact organization - this is referred to as a threat assessment.

11. What is Vulnerability?

Vulnerabilities are specific avenues that threat agents can exploit to attack an information asset

12. What is Vulnerability Identification?

Examine how each of the threats that are possible or likely could be perpetrated and list the organization's assets and their vulnerabilities

13. What is Risk Assessment?

Risk assessment assigns a risk rating or score to each specific information asset, useful in gauging the relative risk introduced by each vulnerable information asset and making comparative ratings later in the risk control process

14. What are the Risk Identification Estimate Factors?

a. Likelihood
b. Value of Information Assets
c. Percent of Risk Mitigated
d. Uncertainty

15. How to calculate risk determination?

Risk = (value (or impact) of information asset ×likelihood of vulnerability occurrence) × (100% – percentage of risk already controlled + an element of uncertainty)

16. What is residual risk?

Residual risk is the risk that remains to the information asset even after the existing control has been applied

17. Define access control?

Access controls are those controls that specifically address admission of a user into a trusted area of the organization

There are a number of approaches to controlling access

Access controls can be

a. discretionary

b.mandatory

c. nondiscretionary

18. What are the risk identification and assessment deliverables?

Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

19. List the basic control strategies to control risks?

Avoidance

do not proceed with the activity or system that creates this risk

Reduced Likelihood (Control)

by implementing suitable controls, lower the chances of the¬ vulnerability being **exploited**

Transference

share responsibility for the risk with a third party

Mitigation

reduce impact should an attack still exploit the vulnerability

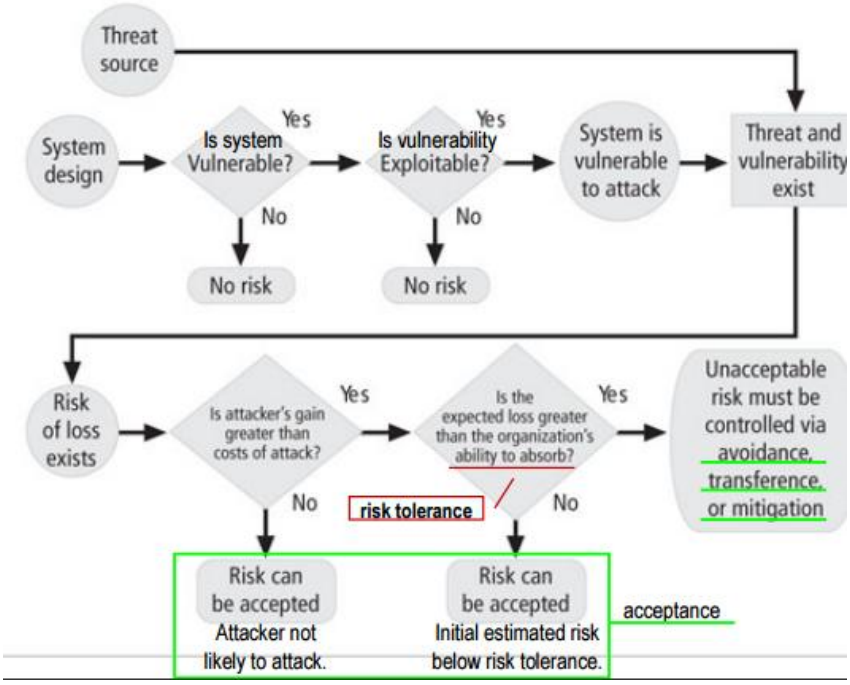
Acceptance

understand consequences and acknowledge risks without any attempt to control or mitigate.

20. What is transference?

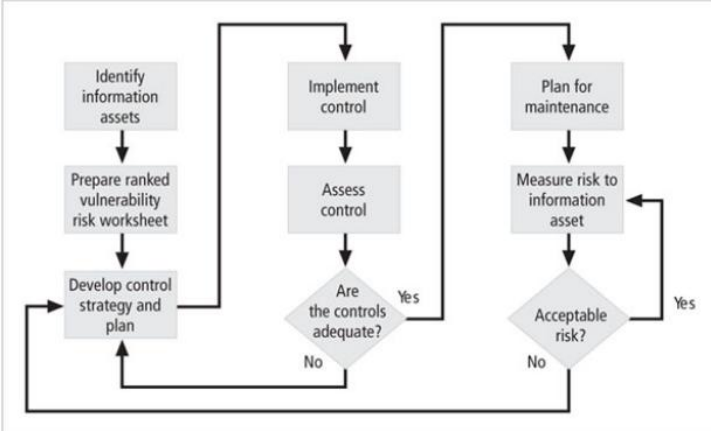
Risk control strategy that attempts to shift risk to other assets, other processes or other organizations

21. Draw risk handling decision process?



22. What is risk control cycle?

After control has been selected & implemented, control should be monitored and (if needed) adjusted on an on-going basis



23. What are the categories of controls?

a. Control function
b. Architectural layer
c. Strategy layer
d. Information security principle

24. What is use of control function?

Controls or safeguards designed to defend the vulnerability are either preventive or detective

Preventive controls stop attempts to exploit vulnerability by implementing enforcement of an organizational policy or a security principle, such as authentication or confidentiality

Detective controls warn of violations of security principles, organizational policies, or attempts to exploit vulnerabilities

25. What is architectural layer?

Some controls apply to one or more layers of an organization's technical architecture

Among the architectural layer designators in common use are:

- organizational policy
- external networks
- extranets (or demilitarized zones)
- Intranets (WAN and LAN)
- network devices that interface network zones (switches, routers, firewalls, and hubs)
- systems (computers for mainframe, server or desktop use)
- applications

26. Describe strategy layer?

Controls are sometimes classified by the risk control strategy they operate within:

a. avoidance
b. mitigation
c. transference

27. What are the principles of information security?

Controls operate within one or more of the commonly accepted information security principles:

a. Confidentiality

b. Integrity
c. Availability
d. Authentication
e. Authorization
f. Accountability
g. Privacy

28. Describe about Cost Benefit Analysis (CBA)?

- The most common approach for a project of information security controls and safeguards is the economic feasibility of implementation
- Begins by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised
- It is only common sense that an organization should not spend more to protect an asset than it is worth
- The formal process to document this is called a cost benefit analysis or an economic feasibility study

29. What is CBA asset valuation?

- Asset valuation is the process of assigning financial value or worth to each information asset
- The valuation of assets involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss and litigation.
- These estimates are calculated for each set of information bearing systems or information assets

30. What is ALE & ARO?

- The expected value of a loss can be stated in the following equation:
  - Annualized Loss Expectancy (ALE) =
    Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO) where:
  - SLE = asset value x exposure factor (EF)
- ARO is simply how often you expect a specific type of attack to occur, per year
- SLE is the calculation of the value associated with the most likely loss from an attack
- EF is the percentage loss that would occur from a given vulnerability being exploited

31. What is CBA formula?

- CBA is whether or not the control alternative being evaluated is worth the associated cost incurred to control the specific vulnerability
- While many CBA techniques exist, for our purposes, the CBA is most easily calculated using the ALE from earlier assessments
- CBA = ALE(prior) – ALE(post) – ACS
- Where:
  - ALE prior is the Annualized Loss Expectancy of the risk before the implementation of the control
  - ALE post is the ALE examined after the control has been in place for a period of time
  - ACS is the Annual Cost of the Safeguard

32. What is benchmarking?

Rather than use the financial value of information assets, review peer institutions to determine what they are doing to protect their assets (benchmarking)

When benchmarking, an organization typically uses one of two measures:

a. Metrics-based measures are comparisons based on numerical standards
b. Process-based measures examine the activities performed in pursuit of its goal, rather than the specifics of how goals were attained

33. What is Baselining?

Baselining is the analysis of measures against established standards

In information security, baselining is comparing security activities and events against the organization's future performance

When baselining it is useful to have a guide to the overall process

34. What is Organizational Feasibility?

Organizational feasibility examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization

Above and beyond the impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization

35. What is Operational Feasibility?

Addresses user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders

Sometimes known as behavioral feasibility, because it measures the behavior of users

One of the fundamental principles of systems development is obtaining user buy-in on a project and one of the most common methods for obtaining user acceptance and support is through user involvement obtained through three simple steps:

a. Communicate
b. Educate
c. Involve

36. What is Technical Feasibility?

The project team must also consider the technical feasibilities associated with the design, implementation, and management of controls

Examines whether or not the organization has or can acquire the technology necessary to implement and support the control alternatives

37. What is Political Feasibility?

For some organizations, the most significant feasibility evaluated may be political

Within organizations, political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest

The limits placed on an organization's actions or behaviors by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources

38. What is quality measures in controlling risk?

The spectrum of steps described above was performed with real numbers or best-guess estimates of real numbers - this is known as a quantitative assessment

However, an organization could determine that it couldn't put specific numbers on these values

Fortunately, it is possible to repeat these steps using estimates based on a qualitative assessment

Instead of using specific numbers, ranges or levels of values can be developed simplifying the process

39. What is Delphi Techniquein controlling risk?

One technique for accurately estimating scales and values is the Delphi Technique

The Delphi Technique, named for the Oracle at Delphi, is a process whereby a group of individuals rate or rank a set of information

The individual responses are compiled and then returned to the individuals for another iteration

This process continues until the group is satisfied with the result

11 MARKS

1. Explain Risk identification?

- A risk management strategy calls on us to "know ourselves" by identifying, classifying, and prioritizing the organization's information assets
- These assets are the targets of various threats and threat agents and our goal is to protect them from these threats
- Next comes threat identification:
  - Assess the circumstances and setting of each information asset
  - Identify the vulnerabilities and begin exploring the controls that might be used to manage the risks

a)Asset Identification and Valuation

- This iterative process begins with the identification of assets, including all of the elements of an organization's system: people, procedures, data and information, software, hardware, and networking elements
- Then, we classify and categorize the assets adding details as we dig deeper into the analysis

TABLE 4-1 Categorizing the Components of an Information System

Traditional system components	SecSDLC and risk management system components	
People	Employees	Trusted employees Other staff
	Nonemployees	People at trusted organizations Strangers
Procedures	Procedures	IT and business standard procedures IT and business sensitive procedures
Data	Information	Transmission Processing Storage
Software	Software	Applications Operating systems Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

People, Procedures, and Data Asset Identification

- Unlike the tangible hardware and software elements, the human resources, documentation, and data information assets are not as readily discovered and documented
- These assets should be identified, described, and evaluated by people using knowledge, experience, and judgment

- As these elements are identified, they should also be recorded into some reliable data handling process

Asset Information for People

- For People:
  - Position name/number/ID – try to avoid names and stick to identifying positions, roles, or functions
  - Supervisor
  - Security clearance level
  - Special skills

Asset Information for Procedures

- For Procedures:
  - Description
  - Intended purpose
  - What elements is it tied to
  - Where is it stored for reference
  - Where is it stored for update purposes

Asset Information for Data

- For Data:
  - Classification
  - Owner/creator/manager
  - Size of data structure
  - Data structure used – sequential, relational
  - Online or offline
  - Where located
  - Backup procedures employed

Hardware, Software, and Network Asset Identification

- What attributes of each of these information assets should be tracked?
- When deciding which information assets to track, consider including these asset attributes:
  - Name
  - IP address
  - MAC address
  - Element type
  - Serial number
  - Manufacturer name
  - Manufacturer's model number or part number
  - Software version, update revision, or FCO number
  - Physical location
  - Logical location
  - Controlling entity

Automated tools can sometimes uncover the system elements that make up the hardware, software, and network components

- Once created, the inventory listing must be kept current, often through a tool that periodically refreshes the data

b) Information Asset Classification

- Many organizations already have a classification scheme
- Examples of these kinds of classifications are:
  - confidential data
  - internal data
  - public data
- Informal organizations may have to organize themselves to create a useable data classification model
- The other side of the data classification scheme is the personnel security clearance structure

c) Information Asset Valuation

- Each asset is categorized
- Questions to assist in developing the criteria to be used for asset valuation:
  - Which information asset is the most critical to the success of the organization?
  - Which information asset generates the most revenue?
  - Which information asset generates the most profitability?
  - Which information asset would be the most expensive to replace?
  - Which information asset would be the most expensive to protect?
  - Which information asset would be the most embarrassing or cause the greatest liability if revealed?
- Create a weighting for each category based on the answers to the previous questions
  Which factor is the most important to the organization?
- Once each question has been weighted, calculating the importance of each asset is straightforward
- List the assets in order of importance using a weighted factor analysis worksheet

TABLE 4-2 Example of a Weighted Factor Analysis Worksheet

Information asset	Criteria 1: impact to revenue	Criteria 2: impact to profitability	Criteria 3: public image impact	Weighted score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Notes: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

d) Data Classification and Management

- A variety of classification schemes are used by corporate and military organizations
- Information owners are responsible for classifying the information assets for which they are responsible
- Information owners must review information classifications periodically
- The military uses a five-level classification scheme but most organizations do not need the detailed level of classification used by the military or federal agencies

e) Security Clearances

- The other side of the data classification scheme is the personnel security clearance structure

- Each user of data in the organization is assigned a single level of authorization indicating the level of classification
- Before an individual is allowed access to a specific set of data, he or she must meet the need-to-know requirement
- This extra level of protection ensures that the confidentiality of information is properly maintained

f) Management of Classified Data

- Includes the storage, distribution, portability, and destruction of classified information
  - Must be clearly marked as such
  - When stored, it must be unavailable to unauthorized individuals
  - When carried should be inconspicuous, as in a locked briefcase or portfolio
- Clean desk policies require all information to be stored in its appropriate storage container at the end of each day
- Proper care should be taken to destroy any unneeded copies
- Dumpster diving can prove embarrassing to the organization

f) Threat Identification

- Each of the threats identified so far has the potential to attack any of the assets protected
- This will quickly become more complex and overwhelm the ability to plan
- To make this part of the process manageable, each step in the threat identification and vulnerability identification process is managed separately, and then coordinated at the end of the process

TABLE 4-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

g) Identify and Prioritize Threats

- Each threat must be further examined to assess its potential to impact organization - this is referred to as a threat assessment
- To frame the discussion of threat assessment, address each threat with a few questions:
  - Which threats present a danger to this organization's assets in the given environment?
  - Which threats represent the most danger to the organization's information?
  - How much would it cost to recover from a successful attack?
  - Which of these threats would require the greatest expenditure to prevent?

h) Vulnerability Identification

- Examine how each of the threats that are possible or likely could be perpetrated and list the organization's assets and their vulnerabilities
- The process works best when groups of people with diverse backgrounds within the organization work iteratively in a series of brainstorming sessions
- At the end of the process, an information asset / vulnerability list has been developed
  - this list is the starting point for the next step, risk assessment

2. Explain Risk Assessment?

Introduction to Risk Assessment

- The goal of this process has been to identify the information assets of the organization that have specific vulnerabilities and create a list of them, ranked for focus on those most needing protection first
- In preparing this list we have collected and preserved factual information about the assets, the threats they face, and the vulnerabilities they experience
- We should also have collected some information about the controls that are already in place

TABLE 4-6 Risk Identification and Assessment Deliverables

Deliverable	Purpose
Information asset classification worksheet	Assembles information about information assets and their impact on or value to the organization
Weighted criteria analysis worksheet	Assigns ranked value or impact weight to each information asset
Ranked vulnerability risk worksheet	Assigns ranked value of risk rating for each uncontrolled asset-vulnerability pair

- Risk Identification Estimate Factors
  - Likelihood
  - Value of Information Assets
  - Percent of Risk Mitigated
  - Uncertainty

Risk Determination

For the purpose of *relative* risk assessment:

risk = (value (or impact) of information asset × likelihood of vulnerability occurrence) × (100% – percentage of risk already controlled + an element of uncertainty)

Identify Possible Controls

- For each threat and its associated vulnerabilities that have any residual risk, create a preliminary list of control ideas
- Residual risk is the risk that remains to the information asset even after the existing control has been applied

Access Controls

- One particular application of controls is in the area of access controls
- Access controls are those controls that specifically address admission of a user into a trusted area of the organization
- There are a number of approaches to controlling access
- Access controls can be

- discretionary
- mandatory
- nondiscretionary

Types of Access Controls

- Discretionary Access Controls (DAC) are implemented at the discretion or option of the data user
- Mandatory Access Controls (MACs) are structured and coordinated with a data classification scheme, and are required
- Nondiscretionary Controls are those determined by a central authority in the organization and can be based on that individual's role (Role-Based Controls) or a specified set of duties or tasks the individual is assigned (Task-Based Controls) or can be based on specified lists maintained on subjects or objects

Lattice-based Control

- Another type of nondiscretionary access is lattice-based control, where a lattice structure (or matrix) is created containing subjects and objects, and the boundaries associated with each pair is contained
- This specifies the level of access each subject has to each object
- In a lattice-based control the column of attributes associated with a particular object are referred to as an access control list or ACL
- The row of attributes associated with a particular subject (such as a user) is referred to as a capabilities table

Documenting Results of Risk Assessment

- The goal of this process has been to identify the information assets of the organization that have specific vulnerabilities and create a list of them, ranked for focus on those most needing protection first
- In preparing this list we have collected and preserved factual information about the assets, the threats they face, and the vulnerabilities they experience
- We should also have collected some information about the controls that are already in place

3. Explain Risk control strategies?

- When risks from information security threats are creating a competitive disadvantage, the information technology and information security communities of interest take control of the risks
- Four basic strategies are used to control the risks that result from vulnerabilities:
  - Apply safeguards (avoidance)
  - Transfer the risk (transference)
  - Reduce the impact (mitigation)
  - Inform themselves of all of the consequences and accept the risk without control or mitigation (acceptance)

Avoidance

- Avoidance attempts to prevent the exploitation of the vulnerability
- This is the preferred approach, as it seeks to avoid risk in its entirety rather than dealing with it after it has been realized
- Accomplished through countering threats, removing vulnerabilities in assets, limiting access to assets, and/or adding protective safeguards
- Three areas of control:
  - Policy
  - Training and education

- Technology

Transference

- Transference is the control approach that attempts to shift the risk to other assets, other processes, or other organizations
- If an organization does not already have quality security management and administration experience, it should hire individuals or firms that provide such expertise
- This allows the organization to transfer the risk associated with the management of these complex systems to another organization with established experience in dealing with those risks

Mitigation

- Mitigation attempts to reduce the impact of exploitation through planning and preparation
- Three types of plans:
  - disaster recovery planning (DRP)
  - business continuity planning (BCP)
  - incident response planning (IRP)
- The most common of the mitigation procedures is the disaster recovery plan or DRP
- The actions to take while the incident is in progress are defined in the incident response plan or IRP
- Longer term issues are handled in the business continuity plan or BCP
-

TABLE 5.1 Summaries of Mitigation Plans

Plan	Description	Example	When deployed	Time frame
Incident response plan (IRP)	Actions an organization takes during incidents (attacks)	▪ List of steps to be taken during disaster ▪ Intelligence gathering ▪ Information analysis	As incident or disaster unfolds	Immediate and real-time reaction
Disaster recovery plan (DRP)	Preparations for recovery should a disaster occur; strategies to limit losses before and during disaster; step-by-step instructions to regain normalcy	▪ Procedures for the recovery of lost data ▪ Procedures for the reestablishment of lost services ▪ Shut-down procedures to protect systems and data	Immediately after the incident is labeled a disaster	Short-term recovery
Business recovery plan (BCP)	Steps to ensure continuation of the overall business when the scale of a disaster requires relocation	▪ Preparation steps for activation of secondary data centers ▪ Establishment of a hot site in a remote location	Immediately after it is determined that the disaster affects the continued operations of the organization	Long-term recovery

Acceptance

- Acceptance of risk is doing nothing to close a vulnerability and to accept the outcome of its exploitation
- Acceptance is valid only when:
  - Determined the level of risk
  - Assessed the probability of attack
  - Estimated the potential damage

- Performed a thorough cost benefit analysis
- Evaluated controls using each appropriate feasibility
- Decided that the particular function, service, information, or asset did not justify the cost of protection

♦ Risk appetite describes the degree to which an organization is willing to accept risk as a trade-off to the expense of applying controls

4. Write about selecting a risk control strategy? (or) Feasibility Study

Evaluation, Assessment, and Maintenance of Risk Controls

♦ Once a control strategy has been implemented, the effectiveness of controls should be monitored and measured on an ongoing basis to determine the effectiveness of the security controls and the accuracy of the estimate of the residual risk

Mitigation Strategy Selection

♦ The level of threat and value of the asset play a major role in the selection of strategy

♦ The following rules of thumb can be applied in selecting the preferred strategy:

- When a vulnerability can be exploited, apply layered protections, architectural designs, and administrative controls to minimize the risk or prevent this occurrence
- When the attacker's cost is less than his/her potential gain apply protections to increase the attacker's cost
- When potential loss is substantial, apply design principles, architectural designs, and technical and non-technical protections to limit the extent of the attack, thereby reducing the potential for loss

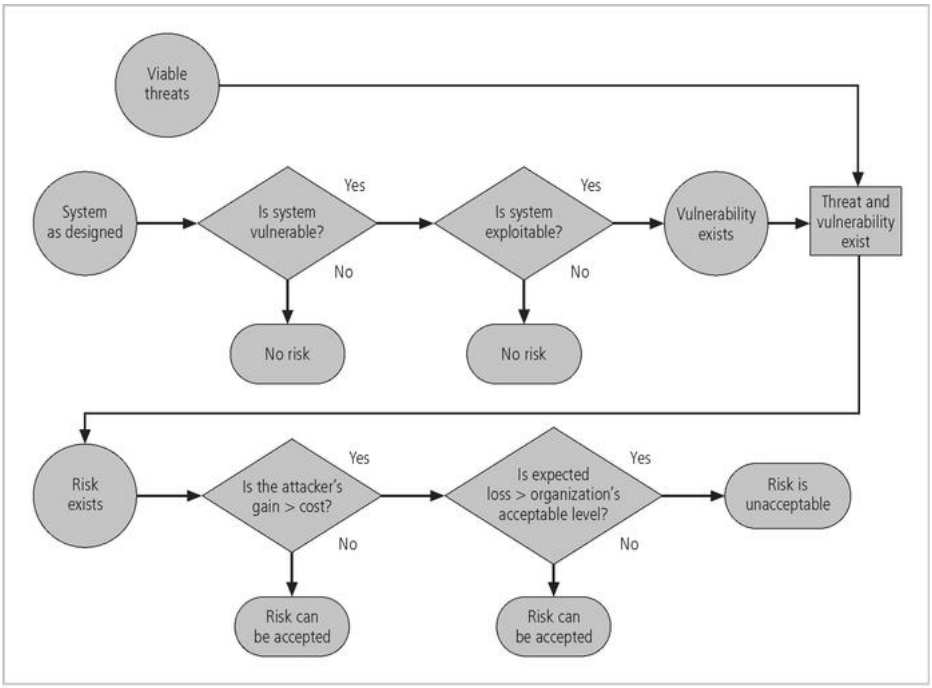


FIGURE 5-2 Risk Handling Decision Points[7]

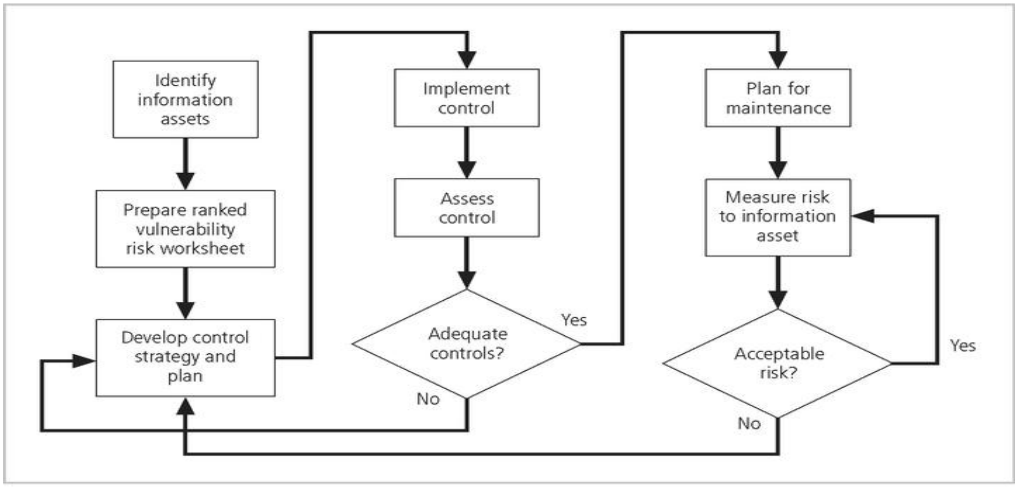


FIGURE 5-3 Risk Control Cycle[8]

Categories of controls

- Controlling risk through avoidance, mitigation, or transference may be accomplished by implementing controls or safeguards
- One approach to selecting controls is by category:
  - Control Function
  - Architectural Layer
  - Strategy Layer
  - Information Security Principles

Control Function

- Controls or safeguards designed to defend the vulnerability are either preventive or detective
- Preventive controls stop attempts to exploit vulnerability by implementing enforcement of an organizational policy or a security principle, such as authentication or confidentiality
- Detective controls warn of violations of security principles, organizational policies, or attempts to exploit vulnerabilities
- Detective controls use techniques such as audit trails, intrusion detection, or configuration monitoring

Architectural Layer

- Some controls apply to one or more layers of an organization's technical architecture
- Among the architectural layer designators in common use are:
  - organizational policy
  - external networks
  - extranets (or demilitarized zones)
  - Intranets (WAN and LAN)
  - network devices that interface network zones (switches, routers, firewalls, and hubs)
  - systems (computers for mainframe, server or desktop use)
  - applications

Strategy Layer

- Controls are sometimes classified by the risk control strategy they operate within:
  - avoidance
  - mitigation
  - transference

Information Security Principles

- Controls operate within one or more of the commonly accepted information security principles:
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Authorization
  - Accountability
  - Privacy

Feasibility Studies and the Cost Benefit Analysis

- Before deciding on the strategy for a specific vulnerability all information about the economic and non-economic consequences of the vulnerability facing the information asset must be explored
- Fundamentally we are asking -

"What are the actual and perceived advantages of implementing a control contrasted with the actual and perceived disadvantages of implementing the control?"

Cost Benefit Analysis (CBA)

- The most common approach for a project of information security controls and safeguards is the economic feasibility of implementation
- Begins by evaluating the worth of the information assets to be protected and the loss in value if those information assets are compromised
- It is only common sense that an organization should not spend more to protect an asset than it is worth
- The formal process to document this is called a cost benefit analysis or an economic feasibility study

CBA: Cost Factors

- Some of the items that impact the cost of a control or safeguard include:
  - Cost of development or acquisition
  - Training fees
  - Cost of implementation
  - Service costs
  - Cost of maintenance

CBA: Benefits

- Benefit is the value that the organization recognizes by using controls to prevent losses associated with a specific vulnerability
- This is usually determined by valuing the information asset or assets exposed by the vulnerability and then determining how much of that value is at risk

CBA: Asset Valuation

- Asset valuation is the process of assigning financial value or worth to each information asset
- The valuation of assets involves estimation of real and perceived costs associated with the design, development, installation, maintenance, protection, recovery, and defense against market loss and litigation.
- These estimates are calculated for each set of information bearing systems or information assets
- There are many components to asset valuation (examples in pages 167-170)

CBA: Loss Estimates

- Once the worth of various assets is estimated examine the potential loss that could occur from the exploitation of vulnerability or a threat occurrence
- This process results in the estimate of potential loss per risk
- The questions that must be asked here include:
  - What damage could occur, and what financial impact would it have?
  - What would it cost to recover from the attack, in addition to the costs above?
  - What is the single loss expectancy for each risk?

CBA: ALE & ARO

- The expected value of a loss can be stated in the following equation:
  - Annualized Loss Expectancy (ALE) = Single Loss Expectancy (SLE) x Annualized Rate of Occurrence (ARO) where:
  - SLE = asset value x exposure factor (EF)
- ARO is simply how often you expect a specific type of attack to occur, per year
- SLE is the calculation of the value associated with the most likely loss from an attack
- EF is the percentage loss that would occur from a given vulnerability being exploited

CBA: Formula

- CBA is whether or not the control alternative being evaluated is worth the associated cost incurred to control the specific vulnerability
- While many CBA techniques exist, for our purposes, the CBA is most easily calculated using the ALE from earlier assessments
- CBA = ALE(prior) – ALE(post) – ACS
- Where:
  - ALE prior is the Annualized Loss Expectancy of the risk before the implementation of the control
  - ALE post is the ALE examined after the control has been in place for a period of time
  - ACS is the Annual Cost of the Safeguard

Benchmarking

- Rather than use the financial value of information assets, review peer institutions to determine what they are doing to protect their assets (benchmarking)
- When benchmarking, an organization typically uses one of two measures:
  - Metrics-based measures are comparisons based on numerical standards
  - Process-based measures examine the activities performed in pursuit of its goal, rather than the specifics of how goals were attained

Due Care/Due Diligence

- When organizations adopt levels of security for a legal defense, they may need to show that they have done what any prudent organization would do in similar circumstances - this is referred to as a standard of due care
- Due diligence is the demonstration that the organization is diligent in ensuring that the implemented standards continue to provide the required level of protection
- Failure to support a standard of due care or due diligence can open an organization to legal liability

Best Business Practices

- Security efforts that provide a superior level of protection of information are referred to as best business practices
- Best security practices (BSPs) are security efforts that are among the best in the industry

- When considering best practices for adoption in your organization, consider the following:
  - Does your organization resemble the identified target?
  - Are the resources you can expend similar?
  - Are you in a similar threat environment?

Other Feasibility studies

Organizational Feasibility

- Organizational feasibility examines how well the proposed information security alternatives will contribute to the efficiency, effectiveness, and overall operation of an organization
- Above and beyond the impact on the bottom line, the organization must determine how the proposed alternatives contribute to the business objectives of the organization

Operational Feasibility

- Addresses user acceptance and support, management acceptance and support, and the overall requirements of the organization's stakeholders
- Sometimes known as behavioral feasibility, because it measures the behavior of users
- One of the fundamental principles of systems development is obtaining user buy-in on a project and one of the most common methods for obtaining user acceptance and support is through user involvement obtained through three simple steps:
  - Communicate
  - Educate
  - Involve

Technical Feasibility

- The project team must also consider the technical feasibilities associated with the design, implementation, and management of controls
- Examines whether or not the organization has or can acquire the technology necessary to implement and support the control alternatives

Political Feasibility

- For some organizations, the most significant feasibility evaluated may be political
- Within organizations, political feasibility defines what can and cannot occur based on the consensus and relationships between the communities of interest
- The limits placed on an organization's actions or behaviors by the information security controls must fit within the realm of the possible before they can be effectively implemented, and that realm includes the availability of staff resources

5. Explain current trends in Information Risk Management?

Trends in Information Risk Management

1. **The unintended consequences of state intervention**
   organizations need to extend their risk management focus from pure information confidentiality, integrity and availability to include risks such as those to reputation and customer channels, and recognize the unintended consequences from activity in cyberspace

   By preparing for the unknown, organizations will have the flexibility to withstand unexpected, high impact security events."
2. **Big data will lead to big problems**

Organizations are increasingly embedding big data in their operations and decision-making process. But it's essential to recognize that there is a human element to data analytics. Organizations that fail to respect that human element will put themselves at risk by overvaluing big data output, noting that poor integrity of the information sets could result in analyses that lead to poor business decisions, missed opportunities, brand damage and lost profits

3. **Mobile applications and the IoT**
   Smartphones and other mobile devices are creating a prime target for malicious actors in the Internet of Things (IoT).
   The rapid uptake of bring-your-own-device (BYOD), and the introduction of wearable technologies to the workplace, will increase an already high demand for mobile apps for work and home in the coming year. To meet this increased demand, developers working under intense pressure and on razor-thin profit margins will sacrifice security and thorough testing in favor of speed of delivery and low cost, resulting in poor quality products more easily hijacked by criminals or hacktivists.
4. **Cybercrime causes the perfect threat storm**
   Cybercrime topped the list of threats in 2015, and it's not going away in 2016. Cybercrime, along with an increase in hacktivism, the surge in cost of compliance to deal with the uptick in regulatory requirements and the relentless advances in technology against a backdrop of under investment in security departments, can all combine to cause the perfect threat storm. Organizations that adopt a risk management approach to identify what the business relies on most will be well placed to quantify the business case to invest in resilience.

   Cyberspace is an increasingly attractive hunting ground for criminals, activists and terrorists motivated to make money, cause disruption or even bring down corporations and governments through online attacks. Organizations must be prepared for the unpredictable so they have the resilience to withstand unforeseen, high impact events.
5. **Skills gap becomes an abyss for information security**
   The information security professionals are maturing just as the increasing sophistication of cyber-attack capabilities demand more increasingly scarce information security professionals. While cybercriminals and hacktivists are increasing in numbers and deepening their skillsets, the "good guys" are struggling to keep pace. CISOs need to build sustainable recruiting practices and develop and retain existing talent to improve their organization's cyber resilience.

   The problem is going to grow worse in future as hyper connectivity increases. CISOs will have to become more aggressive about getting the skill sets the organization needs.

6. **How to manage risk in an intranet environment?**

<u>Managing Risk in an Intranet Environment.</u>

Intranets help organisations manage and deliver information in better ways, reducing a wide range of business risks. They also help organisations respond to natural disasters.

- **Improve the delivery of policies**A valuable first step can be to bring policies together into a small number of sections, structured in a usable way, with well-written content. Further improvements can then be made to the underlying management of policies, as well as how they are delivered to staff.
- **Seek out risk 'owners'**In any larger organisation, there will be senior managers who are the 'owners' of key business risks, including legal, financial and compliance. Establish good relations

with these managers, and use these to identify and formalise business risks, and find opportunities for the intranet to help.

- **Discuss risks with service delivery areas**Similarly, managers in key service delivery areas will generally have a good understanding of the business risks that threaten them. Work with them to find ways that the intranet can mitigate these risks.
- **Establish a disaster response plan for the intranet**Help the organisation to quickly respond to a disaster by enabling remote intranet access for staff, establishing good communication channels, and ensuring the resilience of intranet infrastructure.
- **Align intranet strategy to business risks**Document an explicit business risks register, and outline how the intranet can help to mitigate these risks. Align intranet business cases and project plans to key business risks.

7. What are the Characteristics to Secure Information?

Characteristics of Secure Information

1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Authorization
6. Accountability
7. Privacy

Confidentiality: The control assures the confidentiality of data when it is stored, processed, or transmitted. An example of this type of control is the use of Secure Sockets Layer (SSL) encryption technology to secure Web content as it moves from Web server to browser.

Integrity: The control assures that the information asset properly, completely, and correctly receives, processes, stores, and retrieves data in a consistent and correct manner .Ex: Use of parity or cyclical redundancy checks in data transmission protocols.

Availability: The control assures ongoing access to critical information assets. Ex: Deployment of a network operations center using a sophisticated network monitoring toolset.

Authentication: The control assures that the entity (person or computer) accessing information assets is in fact the stated entity. Ex: The use of cryptographic certificates to establish SSL connections, or the use of cryptographic hardware tokens such as SecurID cards as a second authentication of identity.

Authorization: The control assures that a user has been specifically and explicitly authorized to access, update, or delete the contents of an information asset. Ex: Use of access control lists and authorization groups in the Windows networking environment. Another example is the use of a database authorization scheme to verify the designated users for each function.

Accountability: The control assures that every activity undertaken can be attributed to a specific named person or automated process. Ex: Use of audit logs to track when each user logged in and logged out of each computer.

Privacy: The control assures that the procedures to access, update, or remove personally identifiable information comply with the applicable laws and policies for that kind of information.

UNIT – IV

LOGICAL DESIGN: Blueprint for Security - Information Security Policy - Standards and Practices - ISO 17799/BS 7799 - NIST Models - VISA International Security Model - Design of Security Architecture - Planning for Continuity

---

2 MARKS

1. **Define policy, standards, and practices?**
   - **Policy:** course of action used by organization to convey instructions from management to those who perform duties
   - Policies are organizational laws
   - **Standards:** more detailed statements of what must be done to comply with policy
   - Practices, procedures, and guidelines effectively explain how to comply with policy
   - For a policy to be effective, it must be properly disseminated, read, understood, and agreed to by all members of organization and uniformly enforced
2. **What is use of information security policy?**
   - It provides rules for the protection of the information assets of the organization.
   - The task of information security professionals is to protect the confidentiality. Integrity, and availability of information and information systems, whether in the state of transmission, storage, or processing.
3. **What is Enterprise information security policy (EISP)?**
   - Sets strategic direction, scope, and tone for all security efforts within the organization
   - Executive-level document, usually drafted by or with CIO of the organization
   - Typically addresses compliance in two areas
     - Ensure meeting requirements to establish program and responsibilities assigned therein to various organizational components
     - Use of specified penalties and disciplinary action
4. **What is Issue-Specific Security Policy (ISSP)?**
   - The ISSP:
     - Addresses specific areas of technology
     - Requires frequent updates
     - Contains statement on organization's position on specific issue
   - Three approaches when creating and managing ISSPs:

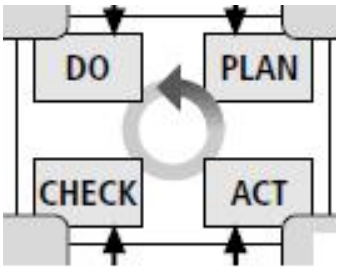
- Create a number of independent ISSP documents
- Create a single comprehensive ISSP document
- Create a modular ISSP document

5. **What is Systems-Specific Policy (SysSP)?**
   - SysSPs frequently function as standards and procedures used when configuring or maintaining systems
   - Systems-specific policies fall into two groups
     - Managerial guidance
     - Technical specifications
   - ACLs can restrict access for a particular user, computer, time, duration—even a particular file
   - Configuration rule policies
6. **Define Policy Management?**
   - Policies are living documents that must be managed and nurtured, and they are constantly changing and growing. These documents must be properly disseminated and managed.
   - To remain viable, security policies must have:
     - Individual responsible for the policy (policy administrator)
     - A schedule of reviews
     - Method for making recommendations for reviews
     - Specific policy issuance and revision date
     - Automated policy management

7. **Describe information Security blueprint?**
   - Basis for design, selection, and implementation of all security policies, education and training programs, and technological controls
   - More detailed version of security framework (outline of overall information security strategy for organization)
   - Should specify tasks to be accomplished and the order in which they are to be realized
   - Should also serve as scalable, upgradeable, and comprehensive plan for information security needs for coming years
8. **What is ISO 17799/BS7799?**
   - One of the most widely referenced and often discussed security models

- Framework for information security that states organizational security policy is needed to provide management direction and support
- Purpose is to give recommendations for information security management
- Provides a common basis for developing organizational security

9. Draw BS7799:2 Major process Steps?



10. List NIST Security Models?

Documents available from Computer Security Resource Center of NIST

- SP 800-12, *The Computer Security Handbook*
- SP 800-14, *Generally Accepted Principles and Practices for Securing IT Systems*
- SP 800-18, *The Guide for Developing Security Plans for IT Systems*
- SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*
- SP 800-30, *Risk Management Guide for Information Technology Systems*

11. What is IETF (Internet Engineering Task Force) Security Architecture?

- Security Area Working Group acts as advisory board for protocols and areas developed and promoted by the Internet Society
- RFC 2196: Site Security Handbook covers five basic areas of security with detailed discussions on development and implementation

12. Describe VISA International Security Model?

- Visa International, the credit card processing vendor, promotes strong security measures in its business associates, and has established guidelines for the security of its information systems.
- Visa has developed two important documents that improve and regulate its information systems: “Security Assessment Process” and “Agreed Upon Procedures.”
- Using the two documents, a security team can develop a sound strategy for the design of good security architecture.

- The only down side to this approach is the very specific focus on systems that can or do integrate with VISA's systems with the explicit purpose of carrying the aforementioned cardholder information.

13. What is Baselining and Best Business Practices?

- Baselining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology
- Possible to gain information by baselining and using best practices and thus work backwards to an effective design

14. Describe about Spheres of security?

Spheres of security: foundation of the security framework

Levels of controls

- Management controls cover security processes designed by strategic planners and performed by security administration
- Operational controls deal with operational functionality of security in organization
- Technical controls address tactical and technical implementations related to designing and implementing security in organization

15. What is meant by defense in depth and security perimeter?

Defense in depth

- Implementation of security in layers
- Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls

Security perimeter

- Point at which an organization's security protection ends and outside world begins
- Does not apply to internal attacks from employee threats or on-site physical threats

16. What is use of firewall, DMZ, proxy servers and IDS?

Firewall: device that selectively discriminates against information flowing in or out of organization

DMZs: no-man's land between inside and outside networks where some place Web servers

Proxy servers: performs actions on behalf of another system

Intrusion detection systems (IDSs): in effort to detect unauthorized activity within inner network, or on individual machines, organization may wish to implement an IDS

17. Compare the features of security education, training, and awareness(SETA) in the organization?

	Education	Training	Awareness
Attribute	Why	How	What
Level	Insight	Knowledge	Information
Objective	Understanding	Skill	Exposure
Teaching	Theoretical instruction	Practical instruction	Media
method	• Discussion seminar	• Lecture	• Videos
	• Background reading	• Case study workshop	• Newsletters
	• Hands-on practice	• Posters	
Test measure	Essay (interpret learning)	Problem solving (apply learning)	• True or false • Multiple choice (identify learning)
Impact timeframe	Long term	Intermediate	Short term

18. List various plans in continuity strategies?

- Incident response plans (IRPs);
- disaster recovery plans (DRPs);
- business continuity plans (BCPs)

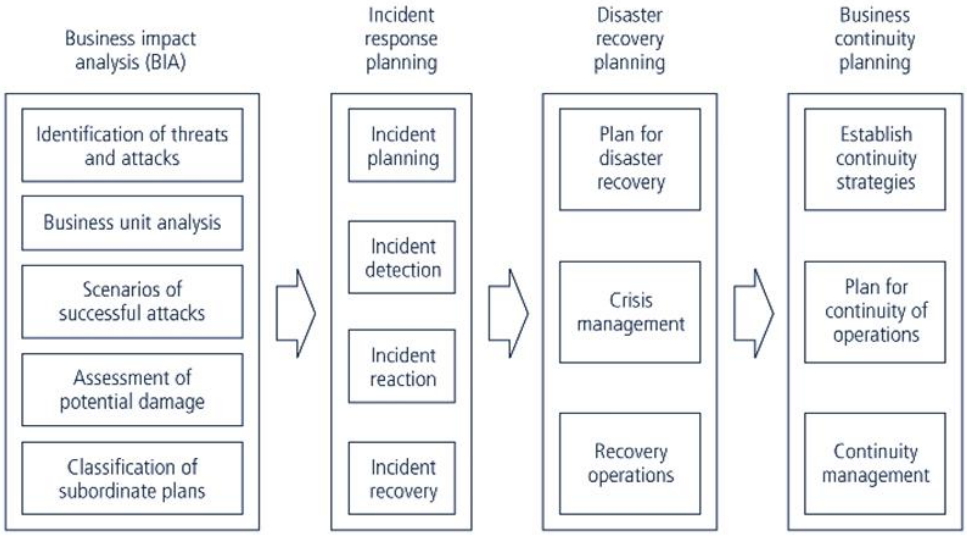
Primary functions of above plans

- **IRP** focuses on immediate response; if attack escalates or is disastrous, process changes to disaster recovery and BCP
- **DRP** typically focuses on restoring systems after disasters occur; as such, is closely associated with BCP
- **BCP** occurs concurrently with DRP when damage is major or long term, requiring more than simple restoration of information and information resources

19. What is contingency planning (CP)?

It comprises a set of plans designed to ensure the effective reaction to and recovery from an attack and the subsequent restoration to normal modes of business operations.

20. Draw major steps in Contingency planning?



21. What are the six steps to contingency planning?

- Identifying the mission- or business-critical functions
- Identifying the resources that support the critical functions,
- Anticipating potential contingencies or disasters,
- Selecting contingency planning strategies
- Implementing the contingency strategies
- Testing and revising the strategy

22. List members in contingency planning team?

Champion: high-level manager to support, promote, and endorse findings of project

Project manager: leads project and makes sure sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed

Team members: should be managers, or their representatives, from various communities of interest: business, IT, and information security

23. What is Business Impact Analysis(BIA)?

A BIA is an investigation and assessment of the impact that various attacks can have on the organization and takes up where the risk assessment process leaves off.

The BIA assumes that these controls have been bypassed, have failed, or are otherwise ineffective in stopping the attack, and the attack was successful.

24. What are the stages in BIA?

The CP team conducts the BIA in the following stages:

- Threat attack identification
- Business unit analysis
- Attack success scenarios

- Potential damage assessment
- Subordinate plan classification

25. What is Incident Response Planning and Incident response (IR)?

Incident response planning covers identification of, classification of, and response to an incident

Incident response (IR) is more reactive than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident

26. When Does an Incident Become a Disaster?

1) The organization is unable to mitigate the impact of an incident during the incident.

2) The level of damage or destruction is so severe the organization is unable to quickly recover. The difference may be subtle.

27. What is incident detection and reaction?

Incident detection

- Most common occurrence is complaint about technology support, often delivered to help desk
- Careful training needed to quickly identify and classify an incident
- Once attack is properly identified, organization can respond

Incident reaction

- Consists of actions that guide organization to stop incident, mitigate the impact of incident, and provide information for recovery from incident

28. Write about incident recovery?

- Once incident has been contained and control of systems regained, the next stage is recovery
- First task is to identify human resources needed and launch them into action
- Full extent of the damage must be assessed
- Organization repairs vulnerabilities, addresses any shortcomings in safeguards, and restores data and services of the systems

29. What is Disaster Recovery Planning?

Disaster recovery planning (DRP) is planning the preparation for and recovery from a disaster The contingency planning team must decide which actions constitute disasters and which constitute incidents.

30. Describe Business Continuity Planning?

- Outlines reestablishment of critical business operations during a disaster that impacts operations
- If disaster has rendered the business unusable for continued operations, there must be a plan to allow business to continue functioning
- Development of BCP is somewhat simpler than IRP or DRP

  Consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy

31. What is a Continuity strategy?

There are a number of strategies for planning for business continuity

Determining factor in selecting between options is usually cost

Dedicated recovery site options

- Hot sites – fully operational sites
- Warm sites – fully operational hardware but software may not be present
- Cold sites – rudimentary services and facilities

32. What is computer forensics?

Computer forensics is the process of collecting, analyzing, and preserving reomputer-related evidence.

Evidence is the physical object or documented information that proves an action occurred or identifies the intent of a perpetrator.

33. Describe crisis management?

Crisis management team is responsible for managing event from an enterprise perspective and covers:

- Supporting personnel and families during crisis
- Determining impact on normal business operations and, if necessary, making disaster declaration
- Keeping the public informed
- Communicating with major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

11 MARKS

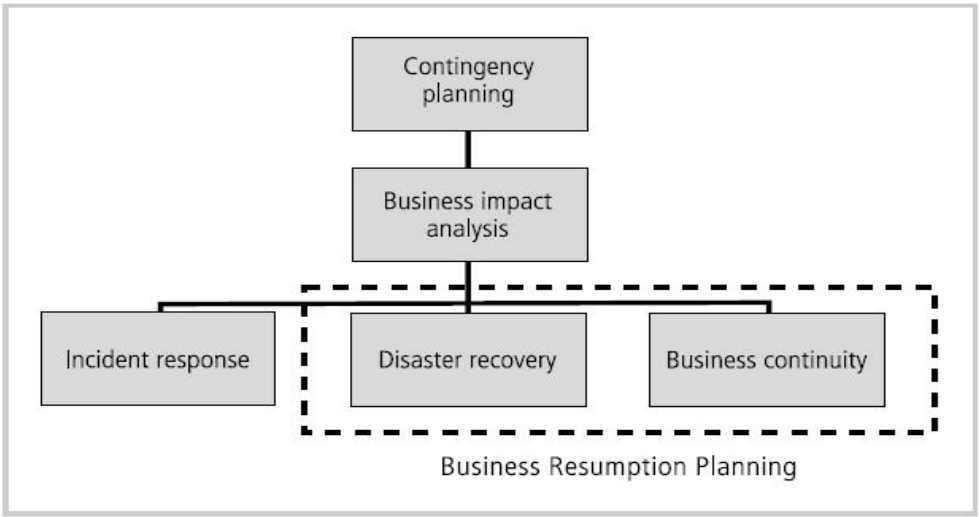
1.Explain Planning Continuity strategies

Continuity Strategies

- Continuous availability of info systems
- Probability high for attack
- Managers must be ready to act
- Contingency Plan (CP)
  - Prepared by organization
  - Anticipate, react to, & recover from attacks
  - Restore organization to normal operations

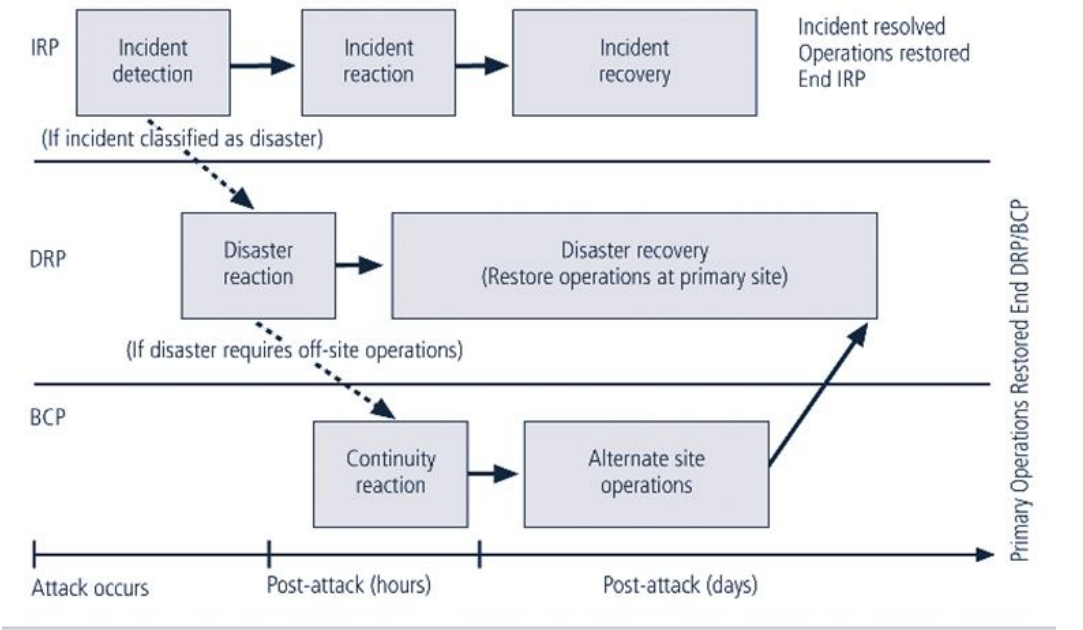
Components of Contingency Plan

- Before planning can begin, a team has to plan effort and prepare resulting documents
- Champion: high-level manager to support, promote, and endorse findings of project
- Project manager: leads project and makes sure sound project planning process is used, a complete and useful project plan is developed, and project resources are prudently managed
- Team members: should be managers or their representatives from various communities of interest: business, IT, and information security



Components of Contingency Planning

Source: Course Technology/Cengage Learning



Contingency Planning Timeline

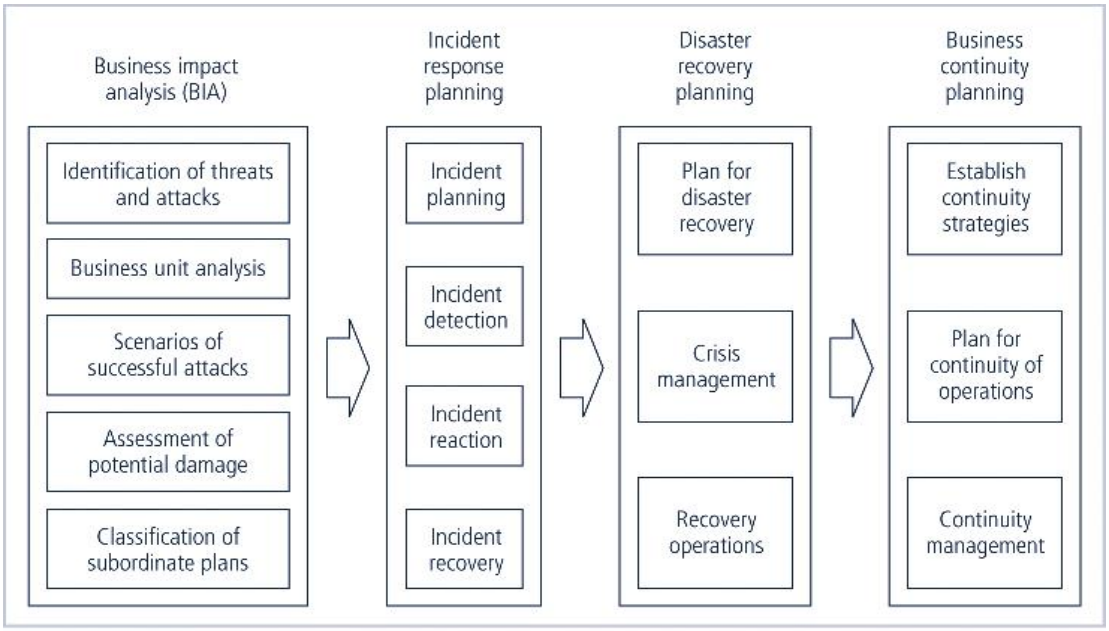


FIGURE 5-23 Major Steps in Contingency Planning

Business Impact Analysis (BIA)

- Investigate & assess impact of various attack
- First risk assessment – then BIA
- Prioritized list of threats & critical info
- Detailed scenarios of potential impact of each attack
- Answers question
  - "if the attack succeeds, what do you do then?"

BIA Sections

- Threat attack identification & prioritization
  - Attack profile – detailed description of activities that occur during an attack
  - Determine the extent of resulting damage
- Business Unit analysis
  - Analysis & prioritization-business functions
  - Identify & prioritize functions w/in orgs units
- Attack success scenario development
  - Series of scenarios showing impact
  - Each treat on prioritized list
  - Alternate outcomes
    - Best, worst, probable cases
- Potential damage assessment
  - Estimate cost of best, worst, probable
  - What must be done under each
  - Not how much to spend
- Subordinate Plan Classification
  - Basis for classification as disastrous not disastrous

Incident Response Planning (IRPs)

- Incident response planning covers identification of, classification of, and response to an incident
- Attacks classified as incidents if they:
  - Are directed against information assets
  - Have a realistic chance of success
  - Could threaten confidentiality, integrity, or availability of information resources
- Incident response (IR) is more reactive, than proactive, with the exception of planning that must occur to prepare IR teams to be ready to react to an incident

Incident Response

- Set of activities taken to plan for, detect, and correct the impact
- Incident planning
  - Requires understanding BIA scenarios
  - Develop series of predefined responses
  - Enables org to react quickly
- Incident detection

- Mechanisms – intrusion detection systems, virus detection, system administrators, end users

Incident Detection

- Possible indicators
  - Presence of unfamiliar files
  - Execution of unknown programs or processes
  - Unusual consumption of computing resources
  - Unusual system crashes
- Probable indicators
  - Activities at unexpected times
  - Presence of new accounts
  - Reported attacks
  - Notification form IDS
- Definite indicators
  - Use of dormant accounts
  - Changes to logs
  - Presence of hacker tools
  - Notification by partner or peer
  - Notification by hackers
- Predefined Situation
  - Loss of availability
  - Loss of integrity
  - Loss of confidentiality
  - Violation of policy
  - Violation of law

Incident Reaction

- Actions outlined in the IRP
- Guide the organization
  - Stop the incident
  - Mitigate the impact
  - Provide information recovery
- Notify key personnel
- Document incident

Incident Containment Strategies

- Sever affected communication circuits
- Disable accounts
- Reconfigure firewall
- Disable process or service
- Take down email
- Stop all computers and network devices
- Isolate affected channels, processes, services, or computers

Incident Recovery

- Get everyone moving and focused
- Assess Damage
- Recovery
  - Identify and resolve vulnerabilities
  - Address safeguards
  - Evaluate monitoring capabilities
  - Restore data from backups
  - Restore process and services
  - Continuously monitor system
  - Restore confidence

Disaster Recovery Plan (DRPs)

- Provide guidance in the event of a disaster
- Clear establishment of priorities
- Clear delegation of roles & responsibilities
- Alert key personnel
- Document disaster
- Mitigate impact
- Evacuation of physical assets

Crisis Management

- Disaster recovery personnel must know their responses without any supporting documentation
- Actions taken during and after a disaster focusing on people involved and addressing viability of business

- Crisis management team responsible for managing event from an enterprise perspective and covers:
  - Support personnel and loved ones
  - Determine impact on normal operations
  - Keep public informed
  - Communicate with major players such as major customers, suppliers, partners, regulatory agencies, industry organizations, the media, and other interested parties

Business Continuity Planning (BCPs)

- Outlines reestablishment of critical business operations during a disaster that impacts operations
- If disaster has rendered the business unusable for continued operations, there must be a plan to allow business to continue functioning
- Development of BCP somewhat simpler than IRP or DRP; consists primarily of selecting a continuity strategy and integrating off-site data storage and recovery functions into this strategy

Continuity Strategies

- There are a number of strategies for planning for business continuity
- Determining factor in selecting between options usually cost
- In general there are three exclusive options: hot sites; warm sites; and cold sites
- Three shared functions: time-share; service bureaus; and mutual agreements

Alternative Site Configurations

- Hot sites
  - Fully configured computer facilities
  - All services & communication links
  - Physical plant operations
- Warm sites
  - Does not include actual applications
  - Application may not be installed and configured
  - Required hours to days to become operational
- Cold sites
  - Rudimentary services and facilities
  - No hardware or peripherals
  - empty room

Alternative Site Configurations

- Time-shares
  - Hot, warm, or cold
  - Leased with other orgs
- Service bureau
  - Provides service for a fee
- Mutual agreements
  - A contract between two or more organizations that specifies how each will assist the other in the event of a disaster.

Off-Site Disaster Data Storage

- To get sites up and running quickly, organization must have ability to port data into new site's systems
- Electronic vaulting
  - Transfer of large batches of data
  - Receiving server archives data
  - Fee
- Journaling
  - Transfer of live transactions to off-site
  - Only transactions are transferred
  - Transfer is real time
- Shadowing
  - Duplicated databases
  - Multiple servers
  - Processes duplicated
  - 3 or more copies simultaneously

Model For a Consolidated Contingency Plan

- Single document set supports concise planning and encourages smaller organizations to develop, test, and use IR and DR plans
- Model is based on analyses of disaster recovery and incident response plans of dozens of organizations

The Planning Document

- Six steps in contingency planning process
  - Identifying mission- or business-critical functions

- Identifying resources that support critical functions
- Anticipating potential contingencies or disasters
- Selecting contingency planning strategies
- Implementing contingency strategies
- Testing and revising strategy

2.Explain Hybrid Framework for a Blueprint of an Information Security System?

- The framework proposed is the result of a detailed analysis of the documents, standards, and Web-based information described in the previous sections.
- It is offered to the information security student as an introductory blueprint for learning the blueprint development process.
- **NIST SP 800-26 Security Self-Assessment Guide for IT Systems**
  - Management Controls
    - Risk Management
    - Review of Security Controls
    - Life Cycle Maintenance
    - Authorization of Processing (Certification and Accreditation)
    - System Security Plan
  - Operational Controls
    - Personnel Security
    - Physical Security
    - Production, Input/Output Controls
    - Contingency Planning
    - Hardware and Systems Software
    - Data Integrity
    - Documentation
    - Security Awareness, Training, and Education
    - Incident Response Capability
  - Technical Controls
    - Identification and Authentication
    - Logical Access Controls
    - Audit Trails

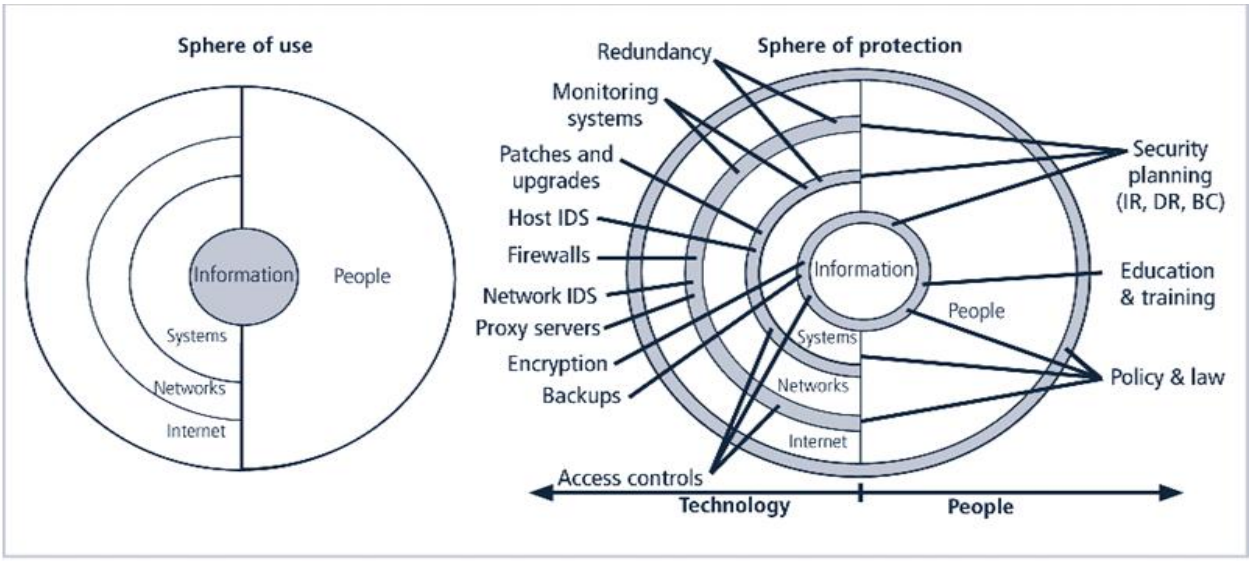
Sphere of Use

The concept of a sphere represents the 360 degrees of security necessary to protect information at all times. The first component is the sphere of use.

Information, at the core of the sphere, is available for direct access by members of the organization and other computer-based systems.

To gain access to the computer systems, one must either directly access the computer systems or go through a network connection.

To gain access to the network, one must either directly access the network or go through an Internet connection.



Spheres of Security

Sphere of Protection

The sphere of protection illustrates that between each layer of the sphere of use there must exist a layer of protection to prevent access to the inner layer from the outer layer.

People in the organization must become a layer of security, a human firewall that protects the information from unauthorized access and use.

Information security is, therefore, designed and implemented in three layers: policies, people (education, training, and awareness programs), and technology.

Controls

Management controls cover security processes that are designed by strategic planners and performed by the security administration of the organization.

Management controls address the design and implementation of the security planning process and security program management.

Operational controls deal with the operational functionality of security in the organization.

They include management functions and lower-level planning, such as disaster recovery and incident response planning.

Operational controls also address personnel security, physical security, and the protection of production inputs and outputs.

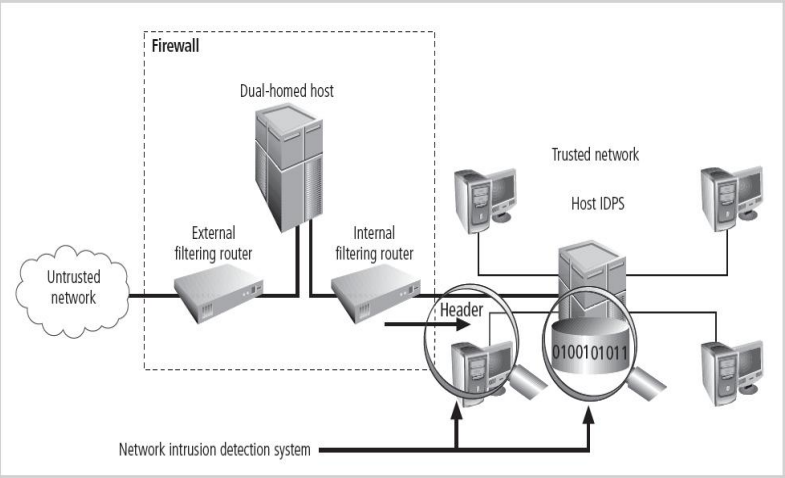
Technical controls address those tactical and technical issues related to designing and implementing security in the organization.

Technical controls include logical access controls, such as identification, authentication, authorization, and accountability.

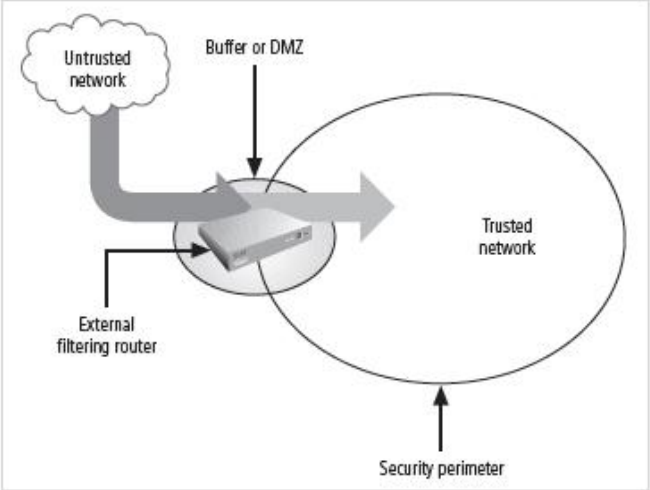
3. Write about Security Architecture Design?

Security Architecture Components

- **Defenses in Depth,**
  - Implementation of security in layers, policy, training, technology.
  - Requires that organization establish sufficient security controls and safeguards so that an intruder faces multiple layers of controls



- **Security Perimeter**
  - Point at which an organization's security protection ends and outside world begins
  - Does not apply to internal attacks from employee threats or on-site physical threats

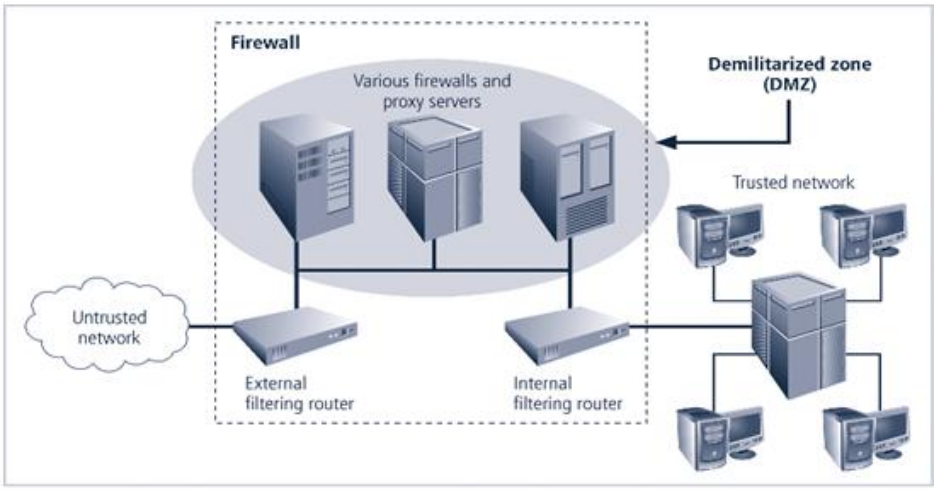


- Security Architecture Components
  - First level of security – protects all internal systems from outside threats
  - Multiple technologies segregate the protected information
  - Security domains or areas of trust

Key Technology Components

- Firewall
  - Device that selectively discriminates against information flowing in and out
  - Specially configured computer
  - Usually on parameter part of or just behind gateway router
- DMZ
  - Buffer against outside attacks
  - No mans land between computer and world
  - Web servers often go here
- Proxy Server
  - Performs actions of behalf of another system
  - Configured to look like a web server
  - Assigned the domain name
  - Retrieves and transmits data
  - Cache server
- IDS
  - Intrusion Detection System
  - Host based
    - Installed on machines they protect
    - Monitor host machines

- Network based
  - Look at patterns of network traffic
  - Attempt to detect unusual activity
  - Requires database of previous activity
  - Uses “machine learning” techniques
  - Can use information form similar networks



Firewalls, Proxy Servers, and DMZs

- SETA
  - Security education, training and awareness
  - Employee errors among top threats
  - Purpose
    - Improve awareness of need to protect
    - Develop skills and knowledge
    - Build in-depth knowledge to design, implement, or operate security programs

4. Explain VISA International security model?

- Visa International promotes strong security measures in its business associates and has established guidelines for the security of its information systems.
- Visa has developed two important documents that improve and regulate its information systems: Security Assessment Process and Agreed Upon Procedures
- Using the two documents, a security team can develop a sound strategy for the design of good security architecture.
- The only downside to this approach is the specific focus on systems that can or do integrate with Visa systems with the explicit purpose of carrying the aforementioned cardholder information.

✓ It promotes strong security measures in its business associates and has established guidelines for the security of its information systems.

✓ It has developed two important documents

1. Security Assessment Process
2. Agreed Upon Procedures.

- ✓ Both documents provide specific instructions on the use of the VISA Cardholder Information Security Program.
- ✓ The Security Assessment Process document is a series of recommendations for the detailed examination of an organization's systems with the eventual goal of integration into the VISA systems.
- ✓ The Agreed upon Procedures document outlines the policies and technologies required for security systems that carry the sensitive card holder information to and from VISA systems.
- ✓ Using the two documents, a security team can develop a sound strategy for the design of good security architecture.
- ✓ The only downside to this approach is the specific focus on systems that can or do integrate with VISA's systems with the explicit purpose of carrying the aforementioned cardholder information.

Baselining & Best Business Practices

- ✓ Baselining and best practices are solid methods for collecting security practices, but provide less detail than a complete methodology
- ✓ Possible to gain information by baselining and using best practices and thus work backwards to an effective design
- ✓ The Federal Agency Security Practices (FASP) site (fasp.nist.gov) designed to provide best practices for public agencies and adapted easily to private institutions.
- ✓ The documents found in this site include specific examples of key policies and planning documents, implementation strategies for key technologies, and position descriptions for key security personnel.
- ✓ Of particular value is the section on program management, which includes the following:
    - A summary guide: public law, executive orders, and policy documents
    - Position description for computer system security officer.
    - Position description for information security officer
    - Position description for computer specialist.
    - Sample of an information technology(IT) security staffing plan for a large service application(LSA)
    - Sample of an information technology(IT) security program policy
    - Security handbook and standard operating procedures.
    - Telecommuting and mobile computer security policy.

5. Explain Baselining and Best Business Practices and professional membership?

Comparison of your organization security with another

Baselining and best practices are solid methods for collecting security practices. Baselining and best practices don't provide a complete methodology for the design and implementation of all the practices needed by an organization.

However, it is possible to piece together the desired outcome of the security process, and, thus, work backwards toward an effective design.

The Federal Agency Security Practices site (fasp.csrc.nist.gov) is designed to provide best practices for public agencies, but these practices can be adapted easily to private institutions.

The documents found in this site include examples of key policies and planning documents, implementation strategies for key technologies, and outlines of hiring documents for key security personnel.

Professional Membership

It may be worth the information security professional's time and money to join professional societies that provide information on best practices to their members.

Many organizations have seminars and classes on best practices for implementing security.

Finding information on security design is the easy part. Sorting through the collected mass of information, documents, and publications can take a substantial investment in time and human resources.

6. Explain NIST Security Models?

- An approach described in documents available from Computer Security Resource Center of National Institute for Standards and Technology (NIST)
- Public ally available at no charge
- Several publications dealing with various aspects
- The following references were cited by the U.S. government when it decided not to select the ISO/IEC 17799 standards.
  - NIST SP 800-12: *The Computer Security Handbook* is an excellent reference guide for the security manager or administrator in the routine management of information security.
  - NIST SP 800-14: *Generally Accepted Principles and Practices for Securing IT Systems* provides best practices and security principles that can direct the development of a security blueprint. Of the more important.
    - Security supports mission of organization; is an integral element of sound management
    - Security should be cost-effective; owners have security responsibilities outside their own organizations
    - Security responsibilities and accountability should be made explicit; security requires a comprehensive and integrated approach
    - Security should be periodically reassessed; security is constrained by societal factors
    - 33 Principles enumerated

NIST SP800-15 Table of Contents
2. Generally Accepted System Security Principles
2.1 Computer Security Supports the Mission of the Organization
2.2 Computer Security Is an Integral Element of Sound Management
2.3 Computer Security Should Be Cost-Effective
2.4 Systems Owners Have Security Responsibilities Outside Their Own Organizations
2.5 Computer Security Responsibilities and Accountability Should Be Made Explicit
2.6 Computer Security Requires a Comprehensive and Integrated Approach
2.7 Computer Security Should Be Periodically Reassessed
2.8 Computer Security Is Constrained by Societal Factors
3. Common IT Security Practices
3.1 Policy
3.1.1 Program Policy
3.1.2 Issue-Specific Policy
3.1.3 System-Specific Policy
3.1.4 All Policies
3.2 Program Management
3.2.1 Central Security Program
3.2.2 System-Level Program
3.3 Risk Management
3.3.1 Risk Assessment
3.3.2 Risk Mitigation
3.3.3 Uncertainty Analysis
3.4 Life Cycle Planning
3.4.1 Security Plan
3.4.2 Initiation Phase
3.4.3 Development/Acquisition Phase
3.4.4 Implementation Phase
3.4.5 Operation/Maintenance Phase
3.4.6 Disposal Phase
3.5 Personnel/User Issues
3.5.1 Staffing
3.5.2 User Administration

Table 5-6 NIST SP 800-14 Generally Accepted Principles and Practices for Securing Information Technology

Principles and Practices for Securing IT Systems	
1.	Establish a sound security policy as the foundation for design.
2.	Treat security as an integral part of the overall system design.
3.	Clearly delineate the physical and logical security boundaries governed by associated security policies.
4.	Reduce risk to an acceptable level.
5.	Assume that external systems are insecure.
6.	Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness.
7.	Implement layered security (ensure no single point of vulnerability).
8.	Implement tailored system security measures to meet organizational security goals.
9.	Strive for simplicity.
10.	Design and operate an IT system to limit vulnerability and to be resilient in response.
11.	Minimize the system elements to be trusted.
12.	Implement security through a combination of measures distributed physically and logically.
13.	Provide assurance that the system is, and continues to be, resilient in the face of expected threats.
14.	Limit or contain vulnerabilities.
15.	Formulate security measures to address multiple overlapping information domains.
16.	Isolate public access systems from mission critical resources (e.g., data, processes, etc.).
17.	Use boundary mechanisms to separate computing systems and network infrastructures.
18.	Where possible, base security on open standards for portability and interoperability.
19.	Use common language in developing security requirements.
20.	Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.
21.	Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.
22.	Authenticate users and processes to ensure appropriate access control decisions both within and across domains.
23.	Use unique identities to ensure accountability.
24.	Implement least privilege.
25.	Do not implement unnecessary security mechanisms.
26.	Protect information while being processed, in transit, and in storage.
27.	Strive for operational ease of use.
28.	Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.
29.	Consider custom products to achieve adequate security.
30.	Ensure proper security in the shutdown or disposal of a system.
31.	Protect against all likely classes of "attacks."
32.	Identify and prevent common errors and vulnerabilities.
33.	Ensure that developers are trained in how to develop secure software.

Table 5-7 Principles for Securing Information Technology Systems NIST SP 800-14 Generally Accepted Principles

- NIST SP 800-18: *The Guide for Developing Security Plans for IT Systems* is considered the foundation for a comprehensive security blueprint and framework. It provides detailed methods for assessing, designing, and implementing controls and plans for various-sized applications
- NIST Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems
- NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems

- ***IETF Security Architecture***

- Internet Engineering Task Force
- Security Area Working Group acts as advisory board for protocols and areas developed and promoted by the Internet Society
- *RFC 2196: Site Security Handbook* covers five basic areas of security with detailed discussions on development and implementation

RFC 2196: Site Security Handbook Table of Contents
1. Introduction
1.1 Purpose of this Work
1.2 Audience
1.3 Definitions
1.4 Related Work
1.5 Basic Approach
1.6 Risk Assessment
2. Security Policies
2.1 What Is a Security Policy and Why Have One?
2.2 What Makes a Good Security Policy?
2.3 Keeping the Policy Flexible
3. Architecture
3.1 Objectives
3.2 Network and Service Configuration
3.3 Firewalls
4. Security Services and Procedures
4.1 Authentication
4.2 Confidentiality
4.3 Integrity
4.4 Authorization
4.5 Access
4.6 Auditing
4.7 Securing Backups
5. Security Incident Handling
5.1 Preparing and Planning for Incident Handling
5.2 Notification and Points of Contact
5.3 Identifying an Incident
5.4 Handling an Incident
5.5 Aftermath of an Incident
5.6 Responsibilities
6. Ongoing Activities
7. Tools and Locations
8. Mailing Lists and Other Resources
9. References

Table 5-9 RFC 2196: Site Security Handbook Table of Contents[20]

7. Write about information security policy, standards, and practices?

Introduction

- Creation of information security program includes:
  - Creation of *policies, standards, and practices,* selection or creation of information security architecture and the development
  - Use of a detailed information security *blueprint* creates plan for future success
  - Creation of c*ontingency planning* consisting of incident response planning, disaster recovery planning, and business continuity plans
- Without policy, blueprints, and planning, organization is unable to meet information security needs of various communities of interest

Information Security Policy, Standards and Practices

- Communities of interest must consider policies as basis for all information security efforts
- Policies direct how issues should be addressed and technologies used
- Security policies are least expensive controls to execute but most difficult to implement
- Shaping policy is difficult

Shaping Policy Difficult

- Never conflict with laws
- Standup in court if challenged
- Be properly administered through dissemination and documented acceptance

Policy

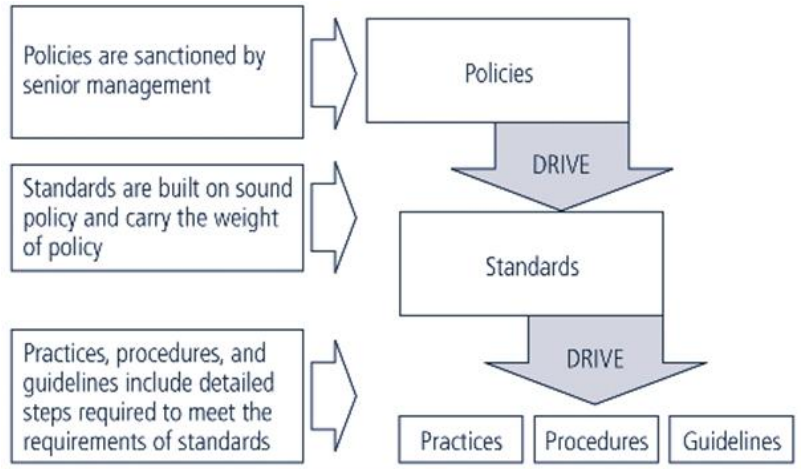
- Plan or course of action
- Convey instructions
- Organizational laws
- Dictate acceptable and unacceptable behavior
- Define
  - What is right
  - What is worn
  - The appeal process
  - What are the penalties for violating policy
- Written to support the mission, vision and strategic plan of organization
- For a policy to be effective, must be properly disseminated, read, understood and agreed to by all members of organization

Standards

- Detail statements of what must be done to comply with policy
- Types
  - Informal – de facto standards
  - Formal – de jure standards

Mission/Vision/Strategic Plan

- Mission – written statement of organization purpose
- Vision – written statement of organization goals
- Strategic Plan - written statement of moving the organization toward its mission



Policies, Standards, and Practices

- Security Policy – set of rules that protects and organization's assets
- Information security policy – set of rules that protects an organization's information assets
- Three types
  - General Issue-specific
  - System-specific

Enterprise Information Security Policy (EISP)

- General Information Security Document
- Shapes the philosophy of security in IT
- Executive-level document, usually drafted by or with CIO of the organization,
- Typically addresses compliance in two areas
  - Ensure *meeting requirements* to establish program
  - *Responsibilities* assigned therein to various organizational components
  - Use of specified *penalties and disciplinary action*

ISSP

- Issue-Specific Security Policy

- Addresses specific areas of technology
- Requires frequent updates
- Contains a statement on the organization's position on a specific issue

3 Approaches to ISSP

- Create independent document tailored to a specific issue
  - Scattered approach
  - Departmentalized
- Create single comprehensive document covering all issues
  - Centralized management and control
  - Tend to over generalize the issue
  - Sip vulnerabilities
- Create a modular plan
  - Unified policy creation and administration
  - Maintain each specific issue's requirements
  - Provide balance

ISSP

- Statement of Policy
- Authorization Access & Equipment Use
- Prohibited Equipment Use
- System Management
  - Focus on user's relationship
- Violations of Policy
- Policy review & modification
- Limitations & Liability

Systems-Specific Policy (SysSP)

- SysSPs frequently codified as standards and procedures
- used when configuring or maintaining systems
- Systems-specific policies fall into two groups
  - Access control lists (ACLs)
  - Configuration rules

ACL Policies

- Restrict access from anyone & anywhere
- Can regulate specific user, computer, time, duration, file

- What regulated
  - Who can use the system
  - What authorization users can access
  - When authorization users can access
  - Where authorization users can access
- Authorization determined by persons identity
- Can regulated specific computer equipment
- Regulate access to data
  - Read
  - Write
  - Modify
  - Copy
  - Compare

Rule Policies

- Rule policies are more specific to operation of a system than ACLs
- May or may not deal with user directly
- Many security systems require specific configuration scripts telling systems what actions to perform on each set of information they process

Policy Management

- Living documents
- Must be managed as they constantly changed and grow
- Must be properly disseminated
- Must be properly managed
- Responsible individual
  - Policy administrator
  - Champion & manager
  - Not necessarily a technically oriented person

Reviews

- Schedule
  - Retain effectiveness in changing environment
  - Periodically reviewed
  - Should be defined and published
  - Should be reviewed at least annually

- Procedures and practices
  - Recommendations for change
  - Reality one person draft

Document Configuration Management

- Include date of original
- Includes date of revision
- Include expiration date

Information Classification

- Classification of information is an important aspect of policy
- Policies are classified, least for "internal use only".
- *A clean desk policy* stipulates that at end of business day, classified information must be properly stored and secured
- In today's open office environments, may be beneficial to implement a clean desk policy

8. Explain ISO 17799/BS7799?

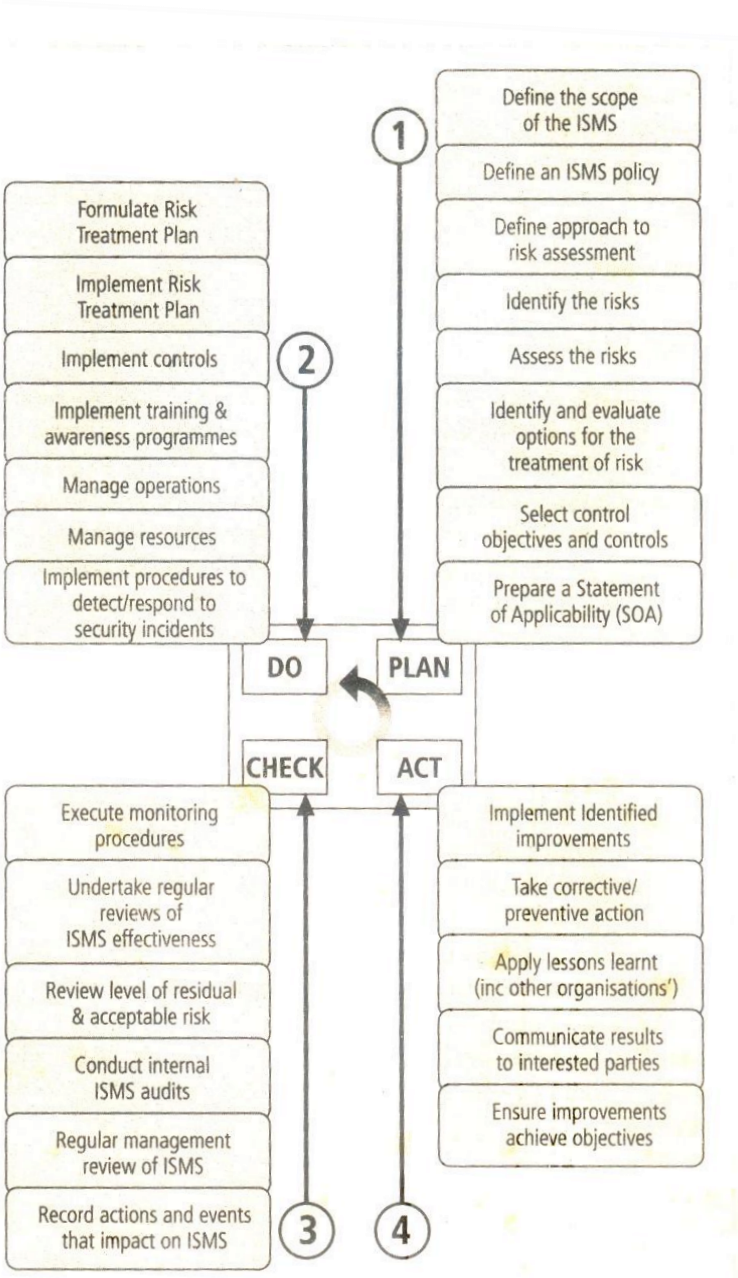
- Information technology – code of practice for information security management from
- ISO (International Organization for Standards)
- IEC (International Electro-technical Commission)
- One of the most widely referenced and often discussed security models

1.	Risk Assessment and Treatment
2.	Security Policy
3.	Organization of Information Security
4.	Asset Management
5.	Human Resource Security
6.	Physical and Environmental Security
7.	Communications and Operations
8.	Access Control
9.	Information Systems Acquisition, Development and Maintenance
10.	Information Security Incident Management
11.	Business Continuity Management
12.	Compliance

The Sections of the ISO/IEC 27002[14]

- ISO/IEC 17799

- Purpose – "give recommendations for information security management for use by those who are responsible for initiating, implementing, or maintaining security in their organization.
- Provides a common basis
- Must pay for these



Courtesy of Gamma Secure Systems

FIGURE 5-9 BS7799:2 Major Process Steps[10]

i. ISO 17799/BS 7799

- ✓ One of the most widely referenced and often discussed security models is the Information Technology – Code of Practice for Information Security Management, which was originally published as British Standard BS 7799
- ✓ In 2000, this Code of Practice was adopted as an international standard framework for information security by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) as ISO/IEC 17799.

ii. Drawbacks of ISO 17799/BS 7799

- ✓ Several countries have not adopted 17799 claiming there are fundamental problems:
  - The global information security community has not defined any justification for a code of practice as identified in the ISO/IEC 17799
  - 17799 lacks "the necessary measurement precision of a technical standard"
  - There is no reason to believe that 17799 is more useful than any other approach currently available
  - 17799 is not as complete as other frameworks available
  - 17799 is perceived to have been hurriedly prepared given the tremendous impact its adoption could have on industry information security controls

iii. Objectives of ISO 17799

- ✓ Organizational Security Policy is needed to provide management direction and support.

iv. Ten Sections of ISO/IEC 17799

1. Organizational Security Policy
2. Organizational Security Infrastructure
3. Asset Classification and Control
4. Personnel Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. System Access Control
8. System Development and Maintenance
9. Business Continuity Planning
10. Compliance

- ✓ Alternate Security Models available other than ISO 17799/BS 7799

UNIT – V

PHYSICAL DESIGN: Security Technology - IDS, Scanning and Analysis Tools -Cryptography - Access Control Devices - Physical Security - Security and Personnel issues

---

2 MARKS

1. **What is IDS?**

   An intrusion detection system (IDS) is a type of security software designed to automatically alert administrators when someone or something is trying to compromise information system through malicious activities or through security policy violations.

2. **Why use an IDS?**

   - To prevent problem behaviors by increasing the perceived risk of discovery and punishment
   - To detect attacks and other security violations not prevented by other security measures
   - To detect and deal with the preambles to attacks
   - To document existing threat to an organization
   - To act as quality control for security design and administration
   - To provide useful information about intrusions that do take place

3. **Give classification of IDS**

   - All IDSs use one of two detection methods:
     - Signature-based
     - Statistical anomaly-based
   - IDSs operate as:
     - network-based
     - host-based
     - application-based systems

4. **What is network-based IDS?**

   A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.
   A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

5. **What is Host-based IDS?**

   A host-based intrusion detection system (HIDS) is a system that monitors a computer system on which it is installed to detect an intrusion and/or misuse, and responds by logging the activity and notifying the designated authority. A HIDS can be thought of as an agent that monitors and analyzes whether anything or anyone, whether internal or external, has circumvented the system's security policy.

6. **How does a Application-Based IDS(AppIDS) differ from a host-based IDS?**

   - A refinement of the host-based IDS is the application-based IDS(AppIDS).
   - Whereas the HIDS examines a single system for file modification, the application-based IDS examines an application for abnormal events.

7. **What is Signature-Based IDS?**

- A knowledge-based (Signature-based) Intrusion Detection Systems (IDS) references a database of previous attack signatures and known system vulnerabilities
- Examine data traffic in search of patterns that match known signatures

8. What is Statistical Anomaly-Based IDS (or) behavior-based IDS?

- The statistical anomaly-based IDS (stat IDS) or behavior-based IDS sample network activity to compare to traffic that is known to be normal
- When measured activity is outside baseline parameters or clipping level, IDS will trigger an alert
- IDS can detect new types of attacks

9. Give some possible responses of IDS?

- Audible/visual alarm
- SNMP traps and plug-ins
- E-mail message
- Page or phone message
- Log entry
- Evidentiary packet dump
- Take action against the intruder
- Launch program
- Reconfigure firewall
- Terminate session or connection

10. Write about strengths of IDS.

- Monitoring and analysis of system events and user behaviors
- Testing security states of system configurations
- Baselining security state of system and then tracking any changes to that baseline
- Recognizing patterns of system events that correspond to known attacks
- Recognizing patterns of activity that statistically vary from normal activity
- Managing operating system audit and logging mechanisms and the data they generate
- Alerting appropriate staff by appropriate means when attacks are detected
- Measuring enforcement of security policies encoded in the analysis engine
- Providing default information security policies
- Allowing non-security experts to perform important security monitoring functions

11. Write about limitations of IDS.

- Compensating for weak or missing security mechanisms in the protection infrastructure
- Instantaneously detecting, reporting, responding to attack during heavy network/processing load
- Detecting newly published attacks or variants
- Effectively responding to sophisticated attacks
- Automatically investigating attacks
- Resisting all attacks intended to defeat them
- Compensating for fidelity issues of data sources
- Dealing effectively with switched networks

12. List control strategies in the deployment and implementation of an IDS.

- **Centralized:** all IDPS control functions are implemented and managed in a central location
- **Fully distributed:** all control functions are applied at the physical location of each IDPS component
- **Partially distributed:** combines the best of the other two strategies; while individual agents still analyze and respond to local threats, their reporting to a hierarchical central facility enables the organization to detect widespread attacks

13. How does the effectiveness of IDS measured?

Once implemented, IDSs are evaluated using two dominant metrics:

- Administrators evaluate the number of attacks detected in a known collection of probes
- Administrators examine the level of use, commonly measured in megabits per second of network traffic, at which the IDPSs fail

14. What is Honey pots, Honey Nets and Padded Cell?

A class of powerful security tools that go beyond routine intrusion detection is known variously as honey pots, honey nets, or padded cell systems

- Honeypots: decoy systems designed to lure potential attackers away from critical systems
- Honeynets: collection of honeypots connecting several honey pot systems on a subnet
- Padded cell: honeypot that has been protected so it cannot be easily compromised

15. What is use of Scanning and Analysis Tools and list them?

Used to find vulnerabilities in systems, holes in security components, and other unsecured

aspects of the network

- Port mappers
- Network mappers
- Firewall analysis
- OS detection tools
- Vulnerability scanners
- Packet sniffers
- Wireless sniffers
- Password crackers

16. What are Port mappers?

Identify computers that are active on a network, as well as their active ports and services, the functions and roles fulfilled by the machines, and other useful information

17. What is Network mappers

Software tools that identify all systems connected to a netwok.
Eg. Nmap, LanState and SolarWinds' LanSurveyor

18. What is Firewall analysis?

Several tools automate remote discovery of firewall rules and assist the administrator in analyzing them

19. What is OS detection tools?

- Detecting a target computer's operating system (OS) is very valuable to an attacker
- There are many tools that use networking protocols to determine a remote computer's OS, e.g. Nmap, Xprobe

20. What is Vulnerability scanners?

- Capable of scanning networks for very detailed information

21. What is Packet sniffers?

- A network tool that collects and analyzes packets on a network
  - It can be used to eavesdrop on network traffic
- Connects directly to a local network from an internal location

22. What is Wireless sniffers?

- Software/hardware capable of capturing and decoding packets as they pass over airwaves
- Wireless sniffing is much easier than wired sniffing
- Example: NetStumbler

23. What is Password crackers?

A method of gaining unauthorized access to a computing system by using computers and dictionaries or large word lists to try likely passwords.

24. What is cryptography?

The art of protecting information by transforming it (*encrypting* it) into an unreadable format, called cipher text. Only those who possess a secret *key* can decipher (or *decrypt*) the message into plain text. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

25. List Cipher Methods?

- **Bit stream:** each plaintext bit transformed into cipher bit one bit at a time
- **Block cipher:** message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key
- **Substitution cipher:** substitute one value for another
- **Transposition cipher:** rearranges values within a block to create ciphertext
- **Exclusive OR (XOR):** function of Boolean algebra; two bits are compared
  - If two bits are identical, result is binary 0
  - If two bits not identical, result is binary 1
- **Vigenère cipher:** advanced cipher type that uses simple polyalphabetic code; made up of 26 distinct cipher alphabets
- **The Vernam cipher** encryption operation, the pad values are added to numeric values that represent the plaintext that needs to be encrypted. So, each character of the plaintext is

turned into a number and a pad value for that position is added to it. The resulting sum for that character is then converted back to a ciphertext letter for transmission.

26. What is Hash function?

- Mathematical algorithms that generate message summary/digest to confirm message identity and confirm no content has changed
- Hash algorithms: publicly known functions that create hash value
- Use of keys not required; message authentication code (MAC), however, may be attached to a message
- Used in password verification systems to confirm identity of user

27. What is the difference between symmetric encryption and asymmetric encryption?

- Symmetric encryption: uses same "secret key" to encipher and decipher message
  - Eg. DES, 3DES and AES
- Asymmetric encryption (public-key encryption) uses two different but related keys; either key can encrypt or decrypt message
  - Eg. Diffie-Hellman, RSA, ECC, ElGamal, DSA

28. Mention some of the Cryptographic Tools

- Public Key infrastructure
- Digital signatures
- Digital Certificates
- Hybrid Cryptography system
- Steganography

29. What is Public Key infrastructure(PKI)?

- Public Key Infrastructure (PKI): integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
- PKI systems based on public-key cryptosystems; include digital certificates and certificate authorities (CAs)
- PKI protects information assets in several ways:
  i. Authentication
  ii. Integrity
  iii. Privacy
  iv. Authorization
  v. Nonrepudiation

30. What is Digital signatures?

- Encrypted messages that can be mathematically proven to be authentic
- Created in response to rising need to verify information transferred using electronic systems
- Asymmetric encryption processes used to create digital signatures

31. What is Digital Certificates?

- Electronic document containing key value and identifying information about entity that controls key
- Digital signature attached to certificate's container file to certify file is from entity it claims to be from

32. What is Hybrid Cryptography system?

- Except with digital certificates, pure asymmetric key encryption not widely used
- Asymmetric encryption more often used with symmetric key encryption, creating hybrid system
- Diffie-Hellman Key Exchange method: most common hybrid system; provided foundation for subsequent developments in public-key encryption

33. What is Steganography?

- Process of hiding information; in use for a long time
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Some applications hide messages in .bmp, .wav, .mp3, and .au files, as well as in unused space on CDs and DVDs

34. List Protocols used for secure communication.

- Securing Internet Communication with **S-HTTP and SSL**
- Securing e-mail with **S/MIME, PEM, and PGP**
- Securing Web transactions with **SET, SSL, and S-HTTP**
- Securing Wireless Networks with **WEP and WPA**
- Securing TCP/IP with **IPSec and PGP**

35. What are the attacks on cryptosystems?

- Man-in-the-Middle Attack
- Correlation Attacks
- Timing Attacks
- Defending from Attacks

36. What is Man-in-the-Middle Attack?

Designed to intercept transmission of public key or insert known key structure in place of requested public key

37. What is Correlation Attacks?

- Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
- Differential and linear cryptanalysis have been used to mount successful attacks

38. What is Timing Attacks?

Attacker eavesdrops during victim's session; uses statistical analysis of user's typing patterns and inter-keystroke timings to discern sensitive session information

39. What is Defending from Attacks?

- No matter how sophisticated encryption and cryptosystems have become, if key is discovered, message can be determined
- Key management is not so much management of technology but rather management of people

40. Draw IPSec Headers?

IPSec Authentication Header Protocol

Next header	Payload length	Reserved
Security parameters index		
Sequence number		
Authentication data (variable length)		

Encapsulating Security Payload Protocol

Security parameters index		
Sequence number		
Payload data (variable length)		
Padding	Pad length	Next header
Authentication data (variable length)		

41. What is the use of PGP?

PGP Function

Function	Algorithm	Application
Public key encryption	RSA/SHA-1 or DSS/SHA-1	Digital signatures
Conventional encryption	3DES, RSA, IDEA or CAST	Message encryption
File management	ZIP	Compression

42. Give MIME Message Header Fields.

Header Field	Function
MIME-version	States conformity to RFCs 2045 and 2046
Content-ID	Identifies MIME entities
Content-type	Describes data in body of message
Content-description	Describes body object
Content-transfer-encoding	Identifies type of conversion used in message body

43. Mention the functions of S/MIME

Function	Algorithm
Hash code for digital signatures	Secure Hash Algorithm 1 (SHA-1)
Digital signatures	DSS
Encryption session keys	ElGamal (variant of Diffie-Hellman)
Digital signatures and session keys	RSA
Message encryption	3DES, RC2

44. Write the differences between WEP and WPA?

WEP Versus WPA

	WEP	WPA
Encryption	Broken by scientists and hackers	Overcomes all WEP shortcomings
	40-bit key	128-bit key
	Static key—the same value is used by everyone on the network	Dynamic keys. Each user is assigned a key per session with additional keys calculated for each packet
	Manual key distribution—each key is typed by hand into each device	Automatic key distribution
Authentication	Broken, used WEP key itself for authentication	Improved user authentication, utilizing stronger 802.1X and EAP

45. What is authentication?

Authentication is the validation of a user's identity.

There are four general forms of authentication to consider:

- What a user knows.
- What a user has.
- What a user is.
- What a user produces.

46. Describe access control devices

- A successful access control system includes number of components, depending on system's needs for authentication and authorization
- Strong authentication requires at least two forms of authentication to authenticate the supplicant's identity
- The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry

47. Describe effectiveness of Biometrics

Biometric technologies evaluated on three basic criteria:

❖ **False reject rate**

The FRR or False Rejection Rate is the probability that the system incorrectly rejectsaccess to an authorized person, due to failing to match the biometric input with a template.

❖ **False accept rate**

The false acceptance rate, or FAR, is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts.

❖ **Crossover error rate (CER)**

CER or Crossover Error Rate is the rate where both accept and reject error rates are equal. FER The Failure to Enroll Rate (FER) is the percentage of the population which fails to complete enrollment. EXAMPLE: let us assume we have a finger print biometric system.

48. What is Physical security

- Physical security addresses design, implementation, and maintenance of countermeasures that protect physical resources of an organization
- Most controls can be circumvented if an attacker gains physical access
- Physical security is as important as logical security

49. Write major sources of physical sources?

a. Extreme temperature
b. Gases
c. Liquids
d. Living organisms
e. Projectiles
f. Movement
g. Energy anomalies

50. What are Physical Security Controls?

- Walls, fencing, and gates

- Lighting (not in ch.)
- Guards
- Dogs
- ID cards and badges
- Locks and keys
- Mantraps (or womantraps, persontraps, etc.)
- Electronic monitoring
- Alarms and alarm systems
- Computer rooms and wiring closets
- Interior walls and doors

51. What is Fire suppression systems?

- A devices installed and maintained to detect and respond to a fire
- Systems consist of portable, manual, or automatic apparatus
- Portable extinguishers are rated by the type of fire: Class A, Class B, Class C, Class D
- Installed systems apply suppressive agents; usually either sprinkler or gaseous systems

52. List Fire detection systems?

- thermal detection,
- smoke detection
- flame detection

53. Describe Heating, Ventilation, and Air Conditioning(HVAC) System?

Areas within heating, ventilation, and air conditioning (HVAC) systems that can cause damage to information systems include:

h. Temperature

i. Filtration

j. Humidity

k. Static electricity

54. Define Uninterruptible Power Supply (UPS)?

- UPS is backup power source for major computer systems in case of power outage.
- Four basic UPS configurations:
  - Standby
  - Ferroresonant standby
  - Line-interactive
  - True online (double conversion online)

55. Write three methods of data interception

- Direct observation
- Interception of data transmission
- Electromagnetic interception

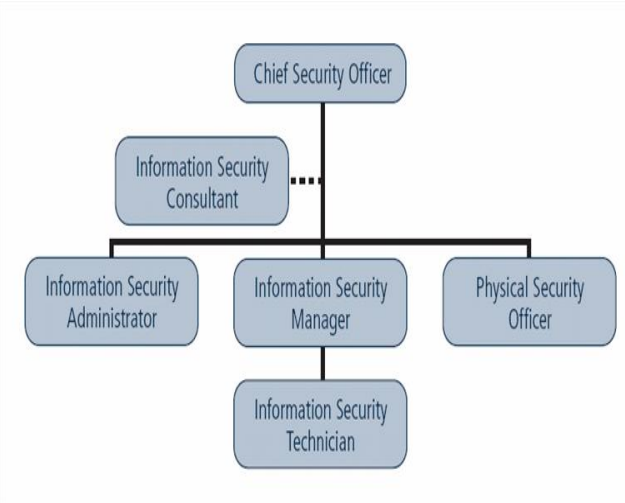
56. What are the human resource issues in implementing information security?

- When implementing information security, there are many human resource issues that must be addressed
    - Positioning and naming
    - Staffing
    - Evaluating impact of information security across every role in IT function
    - Integrating solid information security concepts into personnel practices

57. List security functions placed in an organization?

- IT function
- Physical security function
- Administrative services function
- Insurance and risk management function
- Legal department

41 . What are the positions in information security?



42. Write about Chief Information Security Officer (CISO or CSO) ?

- Top information security position; frequently reports to Chief Information Officer
- Manages the overall information security program
- Drafts or approves information security policies
- Works with the CIO on strategic plans
- Develops information security budgets
- Sets priorities for information security projects and technology
- Makes recruiting, hiring, and firing decisions or recommendations
- Acts as spokesperson for information security team
- Typical qualifications: accreditation, graduate degree, experiencec member functions. If at all they are declared, the compiler provides an error message.

43. Describe about Internal Control Strategies?

- Cornerstone in protection of information assets and against financial loss
- Separation of duties: control used to reduce chance of individual violating information security; stipulates that completion of significant task requires at least two people
- Collusion: unscrupulous workers conspiring to commit unauthorized task
- Two-man control: two individuals review and approve each other's work before the task is categorized as finished
- Job rotation: employees know each others' job skills

44. List advices for Information Security Professionals?

- Always remember: business before technology
- Technology provides elegant solutions for some problems, but adds to difficulties for others
- Never lose sight of goal: protection
- Be heard and not seen
- Know more than you say; be more skillful than you let on
- Speak to users, not at them
- Your education is never complete

11 MARKS

1. Explain Intrusion Detection and Prevention Systems(IDS)?

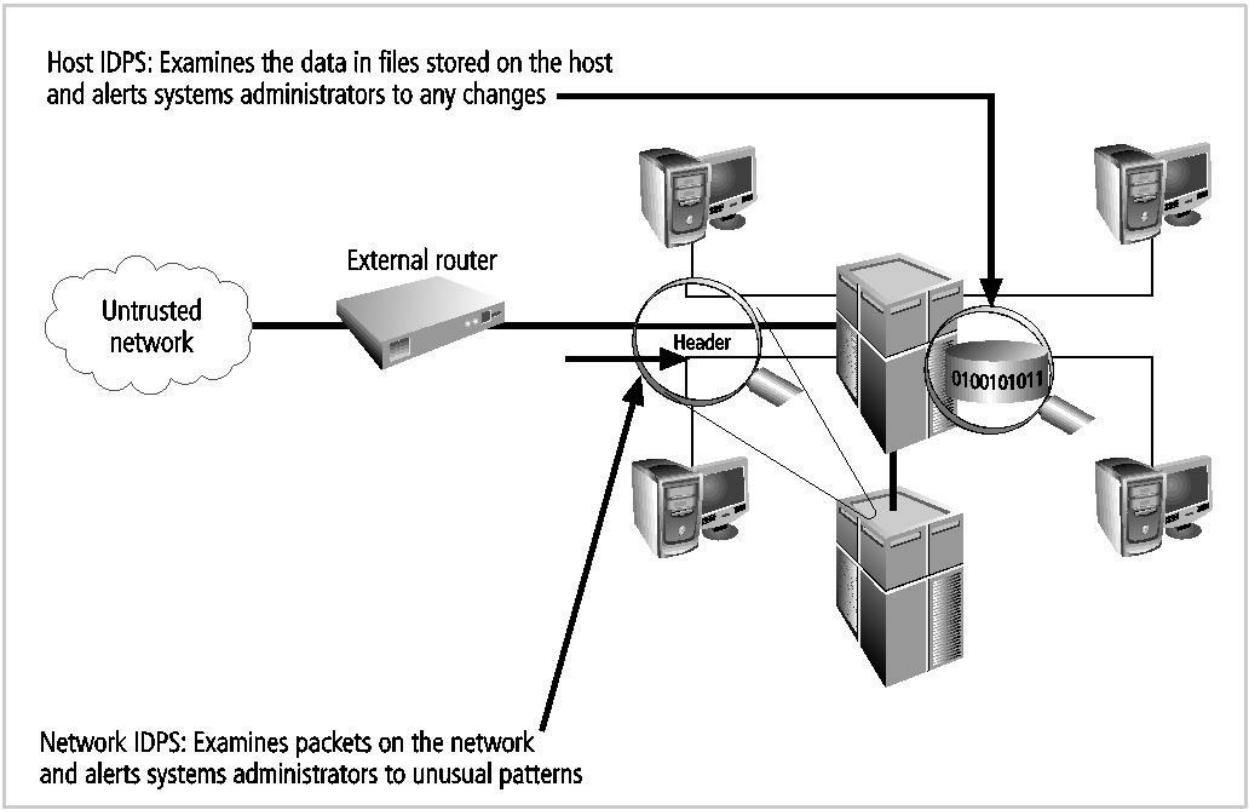
- The term intrusion detection/prevention system (IDPS) can be used to describe current anti-intrusion technologies
- Can detect an intrusion
- Can also prevent that intrusion from successfully attacking the organization by means of an active response
- IDPSs work like burglar alarms
    - Administrators can choose the alarm level
    - Can be configured to notify administrators via e-mail and numerical or text paging
- Like firewall systems, IDPSs require complex configurations to provide the level of detection and response desired
- **The newer IDPS technologies**
    - Different from older IDS technologies
        - IDPS technologies can respond to a detected threat by attempting to prevent it from succeeding
    - Types of response techniques:
        - The IDPS stops the attack itself
        - The IDPS changes the security environment
        - The IDPS changes the attack's content

IDPSs are either

- **host based** to protect server or host information assets
- **network based** to protect network information assets, or

IDPS detection methods

- **Signature based**
- **Statistical anomaly based**



Host-based IDPS

- Resides on a particular computer or server and monitors activity only on that system
- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Most HIDPSs work on the principle of configuration or change management
- Advantage over NIDPS: can usually be installed so that it can access information encrypted when traveling over network
- Configures and classifies various categories of systems and data files
- HIDPSs provide only a few general levels of alert notification
- Unless the HIDPS is very precisely configured, benign actions can generate a large volume of false alarms
- HIDPSs can monitor multiple computers simultaneously

Advantages of HIDPSs

- Can detect local events on host systems and detect attacks that may elude a network-based IDPS
- Functions on host system, where encrypted traffic will have been decrypted and is available for processing
- Not affected by use of switched network protocols

- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

Disadvantages of HIDPSs

- Pose more management issues
- Vulnerable both to direct attacks and attacks against host operating system
- Does not detect multi-host scanning, nor scanning of non-host network devices
- Susceptible to some denial-of-service attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems

Network-Based IDPS

- Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks
- Installed at specific place in the network where it can watch traffic going into and out of particular network segment
- Monitor network traffic
  - When a predefined condition occurs, notifies the appropriate administrator
- Looks for patterns of network traffic
- Match known and unknown attack strategies against their knowledge base to determine whether an attack has occurred
- Yield many more false-positive readings than host-based IDPSs

Advantages of NIDPSs

- Good network design and placement of NIDPS can enable organization to use a few devices to monitor large network
- NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
- NIDPSs not usually susceptible to direct attack and may not be detectable by attackers

Disadvantages of NIDPSs

- Can become overwhelmed by network volume and fail to recognize attacks
- Require access to all traffic to be monitored
- Cannot analyze encrypted packets
- Cannot reliably ascertain if attack was successful or not
- Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets

Signature-Based IDPS

- Examines data traffic for something that matches the preconfigured, predetermined attack pattern signatures
  - Also called knowledge-based IDPS
  - The signatures must be continually updated as new attack strategies emerge
  - A weakness of this method:

- If attacks are slow and methodical, they may slip undetected through the IDPS, as their actions may not match a signature that includes factors based on duration of the events

Statistical Anomaly-Based IDPS

- Also called behavior-based IDPS
- First collects data from normal traffic and establishes a baseline
  - Then periodically samples network activity, based on statistical methods, and compares the samples to the baseline
  - When activity falls outside the baseline parameters (clipping level), The IDPS notifies the administrator

Advantages:

- Able to detect new types of attacks, because it looks for abnormal activity of any type
- IDPS can detect new types of attacks

Disadvantages

- Requires much more overhead and processing capacity than signature-based
- May generate many false positives

2. Write about Scanning and Analysis Tools

Used to find vulnerabilities in systems, holes in security components, and other unsecured

aspects of the network

- Port mappers
- Network mappers
- Firewall analysis
- OS detection tools
- Vulnerability scanners
- Packet sniffers
- Wireless sniffers
- Password crackers

Port Scanners

- A port is a network channel or connection point in a data communications system
- Port scanning utilities (port scanners)
  - Identify computers that are active on a network, as well as their active ports and services, the functions and roles fulfilled by the machines, and other useful information

Port Numbers	Description
20 and 21	File Transfer Protocol (FTP)
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Services (DNS)
67 and 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
161	Simple Network Management Protocol (SNMP)
194	IRC Chat port (used for device sharing)
443	HTTP over SSL
8080	Proxy services

- Well-known ports
  - Those from 0 through 1023
  - Registered ports are those from 1024 through 49151
  - Dynamic and private ports are those from 49152 through 65535
- Open ports must be secured
  - Can be used to send commands to a computer, gain access to a server, and exert control over a networking device

Network mappers

- Mostly use ICMP ping
- Most port scanners can be used as network mappers, e.g. Nmap, LanState

Firewall Analysis

- Several tools automate remote discovery of firewall rules and assist the administrator in analyzing them
- Administrators who feel wary of using the same tools that attackers use should remember:
  - It is intent of user that will dictate how information gathered will be used
  - In order to defend a computer or network well, it is necessary to understand ways it can be attacked
- A tool that can help close up an open or poorly configured firewall will help network defender minimize risk from attack

``Firewalking'' steps

- Network discovery – apply traceroute to a host inside network (finds TTL count to firewall)
- Scanning – TCP/UDP packets with TTL of 1-hop past firewall sent; if the firewall allows packets in, ICMP TTL Expired message will be sent by binding host
- E.g. Firewalk

OS Detection Tools

- Detecting a target computer's operating system (OS) is very valuable to an attacker
- There are many tools that use networking protocols to determine a remote computer's OS, e.g. Nmap, Xprobe
- Strategies: passive fingerprinting, active fingerprinting

Active fingerprinting

- Find out more about host from TCP/IP characteristics
- TCP FIN probing: TCP RFC specifies that a FIN packet to an open port should be ignored. MS Windows responds with a RST packet
- TCP Initial Sequence Number: Some OS choose random values. Windows generates it from the system clock
- TCP Initial window size: Linux 2.4 5840 bytes, 2.2 32120 bytes
- IP ID sampling: MSWin uses a predictable sequence, Linux chooses random numbers.
- ICMP Error message quoting: Linux quotes more than required

Passive fingerprinting

Information gathered through sniffing

- TTL in IP packets: normally Linux TTL= 64, MS Windows TTL = 128
- Don't fragment bit in IP header: most OS 1, OpenBSD 0
- Type of service field in IP header: normally 0, some OS non-zero

Generally less useful. Dependent on traffic pattern

OS detection countermeasures

- Modify responses to various network events/packets
- Morph, IP Scrubber: "scrubs" clean any outgoing packets of OS relates information
- IP personality (http://ippersonality.sourceforge.net)

(patch for Linux kernel)

Vulnerability Scanners

- Capable of scanning networks for very detailed information
- Variants of port scanners
- Identify exposed user names and groups, show open network shares, and expose configuration problems and other server vulnerabilities
- Nessus – freeware
- Used by over 75000 companies
- Different versions for Unix, Mac, Windows
- Detects open ports, mis-configurations (e.g. missing patches), default passwords, presence of viruses, back-door programs

Packet Sniffers

- A network tool that collects and analyzes packets on a network
  - It can be used to eavesdrop on network traffic
- Connects directly to a local network from an internal location
- To use a packet sniffer legally, you must:
  - Be on a network that the organization owns
  - Be directly authorized by the network's owners
  - Have the knowledge and consent of the users
  - Have a justifiable business reason for doing so
- Any network card can be switched to "promiscuous" mode to sniff all LAN packets
- Simply tapping into the Internet is a violation of wiretapping laws
- Example: Wireshark

Wireless Sniffers

- Wireless sniffing is much easier than wired sniffing
- Very difficult to detect – leaves no traceable evidence
- Example: NetStumbler

Password Crackers

Most systems store encrypted passwords.

- MS Windows typically uses C:\Windows\System32\config folder
- Cannot be accessed directly by users, BUT can be accessed by installing LCP, pwdump or FGDUMP (require Admin privilege to install).
- Encryption algorithm known (NT LAN Manager in Win 7)
- Case sensitive (unlike older versions of MSWin), applies MD4

Attack types

- Brute force – very slow
- Dictionary attack – only common disctionary words used
- Precomputed dictionary attack – saves time required for encryption
- E.g. Cain and Able or "Cain" (some virus scanners detect it as malware! Microsoft Security Essentials "Tool: This program has potentially unwanted behavior")

3. Explain about different cipher methods? (Cryptography)

- Plaintext can be encrypted through bit stream or block cipher method
- Bit stream: each plaintext bit transformed into cipher bit one bit at a time
- Block cipher: message divided into blocks (e.g., sets of 8- or 16-bit blocks) and each is transformed into encrypted block of cipher bits using algorithm and key
  - Substitution cipher

- Transposition cipher
- Exclusive OR (XOR)
- Vernam Cipher
- Book or Running Key Cipher
- Hash Functions

Substitution cipher

In a substitution cipher, you substitute one value for another.

The type of substitution based on a **monoalphabetic substitution** only uses one alphabet. More advanced substitution ciphers use two or more alphabets, and are referred to as **polyalphabetic substitutions.**

An advanced type of substitution cipher that uses a simple polyalphabetic code is the Vigenere cipher. The cipher is implemented using the Vigenere Square, which is made up of twenty-six distinct cipher alphabets.

for example, a letter in the alphabet with the letter three values to the right.

Initial alphabet yields ABCDEFGHIJKLMNOPQRSTUVWXYZ

Encryption alphabet DEFGHIJKLMNOPQRSTUVWXYZABC

TABLE 8-2 The Vigenère Square

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Transposition cipher

- Transposition cipher: rearranges values within a block to create ciphertext

For example

Key pattern: 1→4, 2→8, 3→1, 4→5, 5→7, 6→2, 7→6, 8→3

+

```
Bit locations:          87654321 87654321 87654321 87654321
Plaintext 8-bit blocks: 00100101|01101011|10010101|01010100
Ciphertext:             00001011|10111010|01001101|01100001
```

Exclusive OR (XOR)

- Exclusive OR (XOR): function of Boolean algebra; two bits are compared
  - If two bits are identical, result is binary 0
  - If two bits not identical, result is binary 1

- Perform an XOR cipher on the following bits.
- Message 01100001 01100010 01100011
- Cypher Key 01111111 01111111 01111111

TABLE 8-3 Exclusive OR Operations

Bit 1	Bit 2	Exclusive OR result
0	0	0
0	1	1
1	0	1
1	1	0

  - 01100001 = a
  - 01100010 = b
  - 01100011 = c
  - Message 01100001 01100010 01100011
  - Key 01111111 01111111 01111111
  - Cypher text 00011110 00011101 00011100

Vernam Cipher

To perform the Vernam cipher encryption operation, the pad values are added to numeric values that represent the plaintext that needs to be encrypted. So, each character of the plaintext is turned into a number and a pad value for that position is added to it. The resulting sum for that character is then converted back to a ciphertext letter for transmission.

When the two are added, if the values exceed 26, then 26 is subtracted from the total. (This is referred to as Modulo 26.). The corresponding results are then converted back to text

To examine the Vernam cipher and its use of modulo, consider the following example, which uses "SACK GAUL SPARE NO ONE" as plaintext. In the first step of this encryption process, the letter "S" is converted into the number 19 (because it is the nineteenth letter of the alphabet), and the same conversion is applied to the rest of the letters of the plaintext message, as shown below.

Plaintext:	S	A	C	K	G	A	U	L	S	P	A	R	E	N	O	O	N	E
Plaintext value:	19	01	03	11	07	01	21	12	19	16	01	18	05	14	15	15	14	05
One-time pad text:	F	P	Q	R	N	S	B	I	E	H	T	Z	L	A	C	D	G	J
One time pad value:	06	16	17	18	14	19	02	09	05	08	20	26	12	01	03	04	07	10
Sum of plaintext and pad:	25	17	20	29	21	20	23	21	24	24	21	44	17	15	18	19	21	15
After modulo Subtraction:				03								18						
Ciphertext:	Y	Q	T	C	U	T	W	U	X	X	U	R	Q	O	R	S	U	O

Book or Running Key Cipher

Another method, made popular by spy movies, involves using of text in a book as the key to decrypt a message. The cyphertext consists of a list of codes representing the page number, line number, and word number of the plaintext word. The receiver must know which book to use. Dictionaries and thesauruses make the most popular sources as they guarantee every word needed, although almost any book will suffice.

Hash Functions

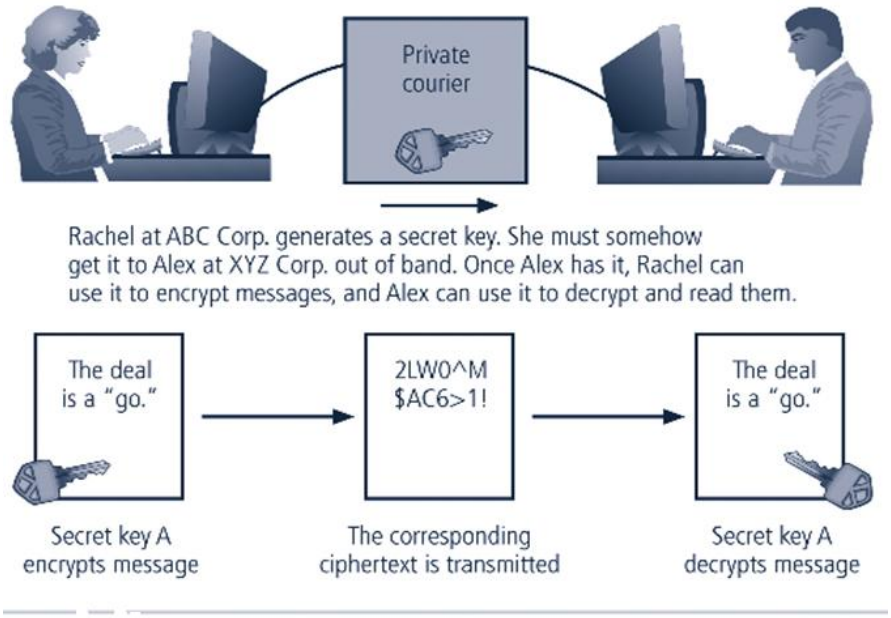
- Mathematical algorithms that generate message summary/digest to confirm message identity and confirm no content has changed
- Hash algorithms: publicly known functions that create hash value
- Use of keys not required; message authentication code (MAC), however, may be attached to a message
- Used in password verification systems to confirm identity of user

4. Explain Cryptographic algorithms?

- Often grouped into two broad categories, symmetric and asymmetric; today's popular cryptosystems use hybrid combination of symmetric and asymmetric algorithms
- Symmetric and asymmetric algorithms distinguished by types of keys used for encryption and decryption operations

  Symmetric encryption: uses same "secret key" to encipher and decipher message

  - Encryption methods can be extremely efficient, requiring minimal processing
  - Both sender and receiver must possess encryption key
  - If either copy of key is compromised, an intermediate can decrypt and read messages



Example of Symmetric Encryption

- Data Encryption Standard (DES): one of most popular symmetric encryption cryptosystems
  - 64-bit block size; 56-bit key
  - Adopted by NIST in 1976 as federal standard for encrypting non-classified information

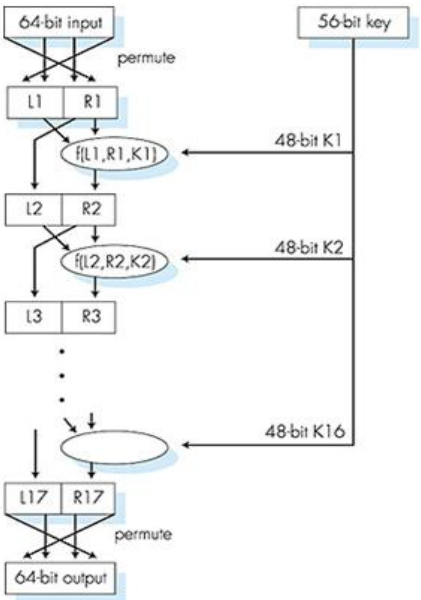
Symmetric Key Crypto: DES

DES Operation

Initial permutation

16 identical "rounds" of function application, each using different 48 bits of key

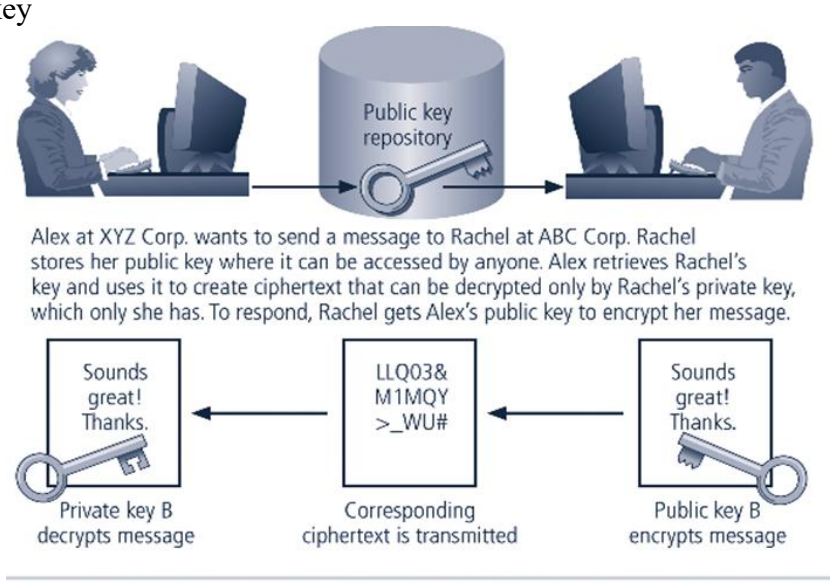
Final permutation



- Triple DES (3DES): created to provide security far beyond DES
- Advanced Encryption Standard (AES): developed to replace both DES and 3DES
  - Symmetric-key NIST standard, replaced DES (Nov 2001)
  - Processes data in 128 bit blocks
  - 128, 192, or 256 bit keys
  - Brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for AES

Asymmetric encryption (public-key encryption)

- Uses two different but related keys; either key can encrypt or decrypt message
- If Key A encrypts message, only Key B can decrypt
- Highest value when one key serves as private key and the other serves as public key



Example of Asymmetric Encryption

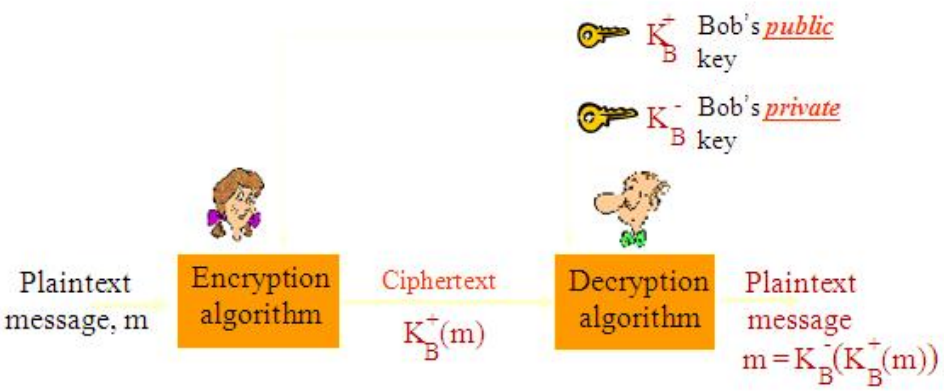
Public Key Crypto

- Radically different approach [Diffie-Hellman76, RSA78]
- Sender, receiver do not share secret key
- Public encryption key known to all
- Private decryption key known only to receiver

Requirements:

1. Need $K_B^+(\cdot)$ and $K_B^-(\cdot)$ such that
   $K_B^-(K_B^+(m)) = m$
2. Given public key K_B^+, it should be impossible to compute private key K_B^-

RSA: Rivest, Shamir, Adelson algorithm



RSA: Creating Public/Private Key Pair

1. Choose two large prime numbers p, q. (e.g., 1024 bits each)
2. Compute $n = pq$, $z = (p-1)(q-1)$
3. Choose e (with $e<n$) that has no common factors with z (e, z are "relatively prime").
4. Choose d such that $ed-1$ is exactly divisible by z. (in other words: $ed \bmod z = 1$).
5. *Public* key is $\underbrace{(n,e)}_{K_B^+}$. *Private* key is $\underbrace{(n,d)}_{K_B^-}$.

RSA: Encryption, Decryption

0. Given (n,e) and (n,d) as computed above
1. To encrypt message m ($<n$), compute $c = m^e \bmod n$
2. To decrypt received bit pattern, c, compute $m = c^d \bmod n$

Magic happens! $m = \underbrace{(m^e \bmod n)}_{c}{}^d \bmod n$

Encryption Key Size

- When using ciphers, size of cryptovariable or key is very important
- Strength of many encryption applications and cryptosystems measured by key size
- For cryptosystems, security of encrypted data is not dependent on keeping encrypting algorithm secret
- Cryptosystem security depends on keeping some or all of elements of cryptovariable(s) or key(s) secret

TABLE 8-7 Encryption Key Power

Number of Bits in Key	Odds of Cracking: 1 in	Estimated Time to Crack*
8	256	.000032 seconds
16	65,536	.008192 seconds
24	16,777,216	2.097 seconds
32	4,294,967,296	8 minutes 56.87 seconds
56	72,057,594,037,927,900	285 years 32 weeks 1 day
64	18,446,744,073,709,600,000	8,090,677,225 years
128	3.40282E+38	5,257,322,061,209,440,000,000 years
256	1.15792E+77	2,753,114,795,116,330,000,000,000,000, 000,000,000,000,000,000,000,000 years
512	1.3408E+154	608,756,305,260,875,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000,000,000,000,000,000,000,000, 000,000,000 years

[NOTE] *Estimated Time to Crack is based on a general-purpose personal computer performing eight million guesses per second.

5. Briefly explain cryptographic tools?

Public Key Infrastructure (PKI):

Integrated system of software, encryption methodologies, protocols, legal agreements, and

third-party services enabling users to communicate securely

- PKI systems based on public-key cryptosystems; include digital certificates and certificate authorities (CAs)
- PKI protects information assets in several ways:
    - Authentication
    - Integrity
    - Privacy
    - Authorization
    - Nonrepudiation
- When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the senders public key must be used to decrypt the message when the decryption happens successfully, it provides verification that the message was sent by the sender and cannot be refuted.
- This is known as non-repudiation, which is the foundation of digital signatures.
- Digital signatures are encrypted messages that are independently verified by a central facility (registry) as authentic.

Digital Signatures

- Encrypted messages that can be mathematically proven to be authentic
- Created in response to rising need to verify information transferred using electronic systems
- Asymmetric encryption processes used to create digital signatures

Digital Certificates

- Electronic document containing key value and identifying information about entity that controls key
- Digital signature attached to certificate's container file to certify file is from entity it claims to be from

TABLE 8-8 X.509 v3 Certificate Structure[10]

Version
Certificate Serial Number
Algorithm ID ■ Algorithm ID ■ Parameters
Issuer Name
Validity ■ Not Before ■ Not After
Subject Name
Subject Public Key Info ■ Public Key Algorithm ■ Parameters ■ Subject Public Key
Issuer Unique Identifier (Optional)
Subject Unique Identifier (Optional)
Extensions (Optional) ■ Type ■ Criticality ■ Value
Certificate Signature Algorithm
Certificate Signature

Hybrid Cryptography Systems

- Except with digital certificates, pure asymmetric key encryption not widely used
- Asymmetric encryption more often used with symmetric key encryption, creating hybrid system
- Diffie-Hellman Key Exchange method: most common hybrid system; provided foundation for subsequent developments in public-key encryption

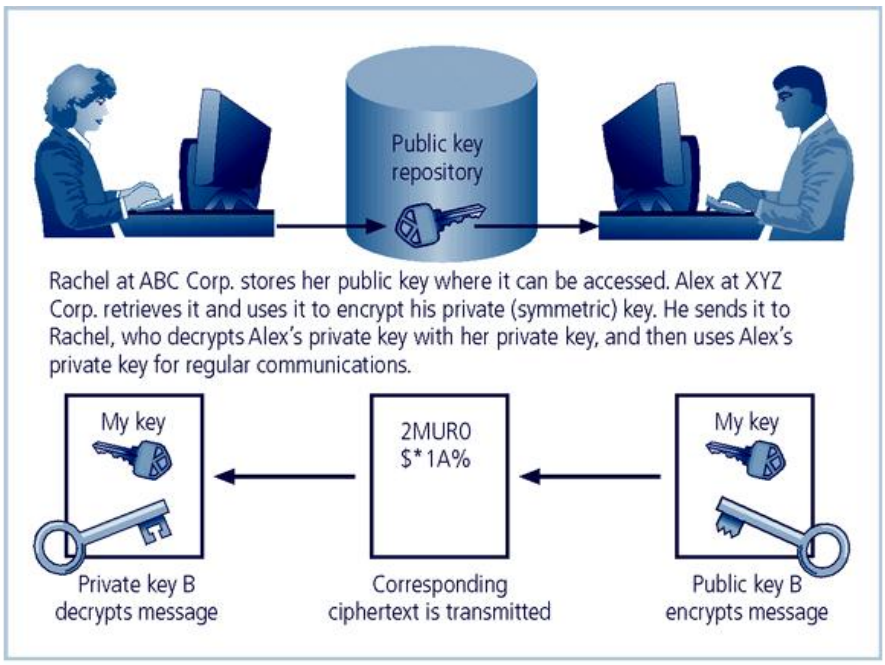


FIGURE 8-17 Hybrid Encryption Example

Steganography

- Process of hiding information; in use for a long time
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Some applications hide messages in .bmp, .wav, .mp3, and .au files, as well as in unused space on CDs and DVDs

6. Explain different protocols used for secure communications?

- Securing Internet Communication with **S-HTTP and SSL**
  - Secure Socket Layer (SSL) protocol: uses public key encryption to secure channel over public Internet
  - Secure Hypertext Transfer Protocol (S-HTTP): extended version of Hypertext Transfer Protocol; provides for encryption of individual messages between client and server across Internet
  - S-HTTP is the application of SSL over HTTP; allows encryption of information passing between computers through protected and secure virtual connection
- Securing e-mail with **S/MIME, PEM, and PGP**
  - Secure Multipurpose Internet Mail Extensions (S/MIME): builds on Multipurpose Internet Mail Extensions (MIME) encoding format by adding encryption and authentication

Header Field	Function
MIME-version	States conformity to RFCs 2045 and 2046
Content-ID	Identifies MIME entities
Content-type	Describes data in body of message
Content-description	Describes body object
Content-transfer-encoding	Identifies type of conversion used in message body

MIME Message Header Fields[14]

Function	Algorithm
Hash code for digital signatures	Secure Hash Algorithm 1 (SHA-1)
Digital signatures	DSS
Encryption session keys	ElGamal (variant of Diffie-Hellman)
Digital signatures and session keys	RSA
Message encryption	3DES, RC2

S/MIME Functions and Algorithms

  - Privacy Enhanced Mail (PEM): proposed as standard to function with public-key cryptosystems; uses 3DES symmetric key encryption
  - Pretty Good Privacy (PGP): uses IDEA Cipher for message encoding

- Securing Web transactions with **SET, SSL, and S-HTTP**
  - Secure Electronic Transactions (SET): developed by MasterCard and VISA in 1997 to provide protection from electronic payment fraud
  - Uses DES to encrypt credit card information transfers
  - Provides security for both Internet-based credit card transactions and credit card swipe systems in retail stores
- Securing Wireless Networks with **WEP and WPA**
  - Wired Equivalent Privacy (WEP): early attempt to provide security with the 8002.11 network protocol
  - Wi-Fi Protected Access (WPA): created to resolve issues with WEP

	WEP	WPA
Encryption	Broken by scientists and hackers	Overcomes all WEP shortcomings
	40-bit key	128-bit key
	Static key—the same value is used by everyone on the network	Dynamic keys. Each user is assigned a key per session with additional keys calculated for each packet
	Manual key distribution—each key is typed by hand into each device	Automatic key distribution
Authentication	Broken, used WEP key itself for authentication	Improved user authentication, utilizing stronger 802.1X and EAP

WEP Versus WPA

  - Next Generation Wireless Protocols: Robust Secure Networks (RSN), AES – Counter Mode Encapsulation, AES – Offset Codebook Encapsulation
  - Bluetooth: de facto industry standard for short range wireless communications between devices; can be exploited by anyone within approximately 30 foot range, unless suitable security controls are implemented
- Securing TCP/IP with **IPSec**
  - Internet Protocol Security (IPSec): open source protocol to secure communications across any IP-based network
  - IPSec designed to protect data integrity, user confidentiality, and authenticity at IP packet level
  - IPSec combines several different cryptosystems: Diffie-Hellman; public key cryptography; bulk encryption algorithms; digital certificates
  - In IPSec, IP layer security obtained by use of application header (AH) protocol or encapsulating security payload (ESP) protocol

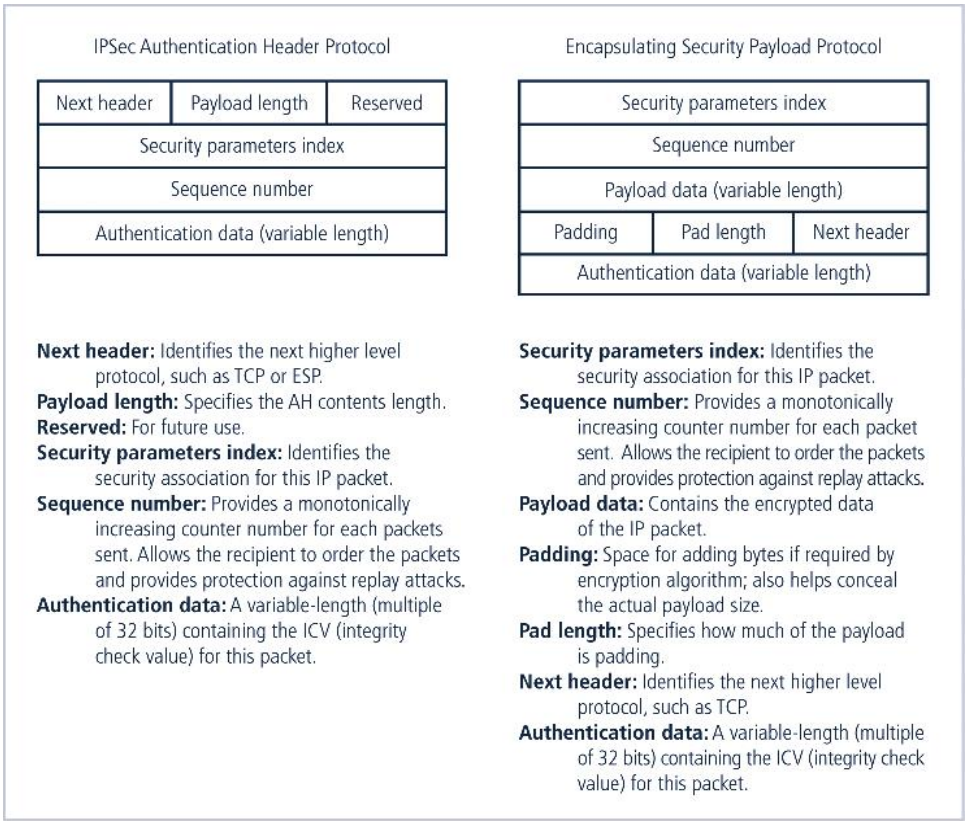


FIGURE 8-8 IPSec Headers

- Securing TCP/IP with **PGP**
  - Pretty Good Privacy (PGP): hybrid cryptosystem designed in 1991 by Phil Zimmermann
  - Combined best available cryptographic algorithms to become open source *de facto* standard for encryption and authentication of e-mail and file storage applications
  - Freeware and low-cost commercial PGP versions are available for many platforms
  - PGP security solution provides six services: authentication by digital signatures; message encryption; compression; e-mail compatibility; segmentation; key management

TABLE 8-11 PGP Function[15]

Function	Algorithm	Application
Public key encryption	RSA/SHA-1 or DSS/SHA-1	Digital signatures
Conventional encryption	3DES, RSA, IDEA or CAST	Message encryption
File management	ZIP	Compression

7. Explain different attacks on cryptosystems?

- Attempts to gain unauthorized access to secure communications have typically used brute force attacks (ciphertext attacks)
- Attacker may alternatively conduct known-plaintext attack or selected-plaintext attach schemes

Man-in-the-Middle Attack

- Designed to intercept transmission of public key or insert known key structure in place of requested public key
- From victim's perspective, encrypted communication appears to be occurring normally, but in fact attacker receives each encrypted message, decodes, encrypts, and sends to originally intended recipient
- Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack

Correlation Attacks

- Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
- Differential and linear cryptanalysis have been used to mount successful attacks
- Only defense is selection of strong cryptosystems, thorough key management, and strict adherence to best practices of cryptography in frequency of changing keys

Timing Attacks

- Attacker eavesdrops during victim's session; uses statistical analysis of user's typing patterns and inter-keystroke timings to discern sensitive session information
- Can be used to gain information about encryption key and possibly cryptosystem in use
- Once encryption successfully broken, attacker may launch a replay attack (an attempt to resubmit recording of deciphered authentication to gain entry into secure source)

Defending Against Attacks

- No matter how sophisticated encryption and cryptosystems have become, if key is discovered, message can be determined
- Key management is not so much management of technology but rather management of people

8. Explain Access Control Devices?

A successful access control system includes a number of components, depending on the system's needs for authentication and authorization.

Strong authentication requires at least two of the forms of authentication listed below to authenticate the supplicant's identity. A second factor that is required to verify the supplicant's identify is frequently a physical device.

The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry.

Authentication

Authentication is the validation of a user's identity.

There are four general forms of authentication to consider:

- What a user knows.
- What a user has.
- What a user is.
- What a user produces.

What a User Knows

A password is a private word or combination of characters that only the user should know.

One of the biggest debates in the information security industry concerns the complexity of passwords. A password should be difficult to guess but must be something the user can easily remember.

A passphrase is a series of characters, typically longer than a password, from which a virtual password is derived.

What a User Has

The second area of authentication addresses something the user carries in his or her possession—that is, something they have.

These include dumb cards, such as ID cards or ATM cards with magnetic stripes that contain the digital (and often encrypted) user personal identification number (PIN), against which the number a user inputs is compared.

An improved version of the dumb card is the smart card, which contains a computer chip that can verify and validate a number of pieces of information instead of just a PIN.

What a User Has

Another device often used is the token, a card or key fob with a computer chip and a liquid crystal display that shows a computer-generated number used to support remote login authentication. Tokens are synchronous or asynchronous.

Once synchronous tokens are synchronized with a server, both devices (server and token) use the same time or a time-based database to generate a number that is displayed and entered during the user login phase.

Asynchronous tokens use a challenge-response system, in which the server challenges the user during login with a numerical sequence.

Who a User Is

The process of using body measurements is known as biometrics and includes:

- Fingerprint comparison of the user's actual fingerprint to a stored fingerprint.
- Palm print comparison of the user's actual palm print to a stored palm print.
- Hand geometry comparison of the user's actual hand to a stored measurement.
- Facial recognition using a photographic ID card, in which a human security guard compares the user's face to a photo.
- Facial recognition using a digital camera, in which a user's face is compared to a stored image.
- Retinal print comparison of the user's actual retina to a stored image.
- Iris pattern comparison of the user's actual iris to a stored image.

Among all possible biometrics, only three human characteristics are usually considered truly unique:

- Fingerprints
- Retina of the eye (blood vessel pattern)
- Iris of the eye (random pattern of features in the iris: freckles, pits, striations, vasculature, coronas, and crypts)

Most of the technologies that scan human characteristics convert these images to some form of minutiae, which are unique points of reference that are digitized and stored in an encrypted format when the user's system access credentials are created.

What a User Produces

The fourth and final area of authentication includes signature recognition and voice recognition.

Retail stores use signature recognition, or at least signature capture, for authentication during a purchase.

Currently, the technology for signature capturing is much more widely accepted than that for signature comparison, because signatures change due to a number of factors, including age, fatigue, and the speed with which the signature is written.

In voice recognition, an initial voiceprint of the user reciting a phrase is captured and stored.

Later, when the user attempts to access the system, the authentication process will require the user to speak this same phrase so that the technology can compare the current voiceprint against the stored value.

Effectiveness of Biometrics

Biometric technologies are evaluated on three basic criteria:

- **The false reject rate:** The rate at which users who are authentic users are denied or prevented access to authorized areas as a result of a failure in the biometric device (Type I error).

- **The false accept rate**: The rate at which users who are not legitimate users are allowed access to systems or areas as a result of a failure in the biometric device (Type II error).
- **The crossover error rate (CER):** The level at which the number of false rejections equals the number of false acceptances (equal error rate). This is the most common and important overall measure of the accuracy of a biometric system.

Acceptability of Biometrics

A balance must be struck between how acceptable a security system is to its users and how effective it is in maintaining security.

Many the biometric systems that are highly reliable and effective are considered somewhat intrusive to users.

As a result, many information security professionals, in an effort to avoid confrontation and possible user boycott of the biometric controls, don't implement them

9. Write about physical security?

Introduction

Physical security addresses design, implementation, and maintenance of countermeasures that protect the physical resources of an organization.

Most of the technology-based controls discussed to this point can be circumvented, if an attacker gains physical access to the devices being controlled.

Some computer systems are constructed in such a way that it easy to steal the hard drive and the information it contains.

As a result, physical security should receive as much attention as logical security in the security development life cycle.

Seven Major Sources of Physical Loss

1. Extreme temperature: heat, cold
2. Gases: war gases, commercial vapors, humid or dry air, suspended particles
3. Liquids: water, chemicals
4. Living organisms: viruses, bacteria, people, animals, insects
5. Projectiles: tangible objects in motion, powered objects
6. Movement: collapse, shearing, shaking, vibration, liquefaction, flows waves, separation, slide
7. Energy anomalies: electrical surge or failure, magnetism, static electricity, aging circuitry; radiation: sound, light, radio, microwave, electromagnetic, atomic.

General management: responsible for the security of the facility in which the organization is housed and the policies and standards for secure operation.

IT management and professionals: responsible for environmental and access security in technology equipment locations and for the policies and standards of secure equipment operation. Information security management and professionals: perform risk assessments and implementation reviews for the physical security controls implemented by the other two groups.

1.Access Controls

There are a number of physical access controls that are uniquely suited to the physical entry and exit of people to and from the organization's facilities, including biometrics, smart cards and wireless enabled keycards.

Facilities Management

Before examining access controls, understand the concept of a secure facility and its design.

From the point of view of facilities management, a secure facility is a physical location that has been engineered with controls designed to minimize the risk of attacks from physical threats.

A secure facility can use the natural terrain; traffic flow, urban development, and can complement these features with protection mechanisms, such as fences, gates, walls, guards, and alarms.

Controls for Protecting the Secure Facility

There are a number of physical security controls and issues that the organization's communities of interest should consider together when implementing physical security:

- Walls, Fencing, and Gates.
- Guards to apply human reasoning.
- Dogs to provide their keen sense of smell and hearing and to be placed in harms way in lieu of humans.
- ID Cards and Badges
- Locks and Keys
- Mantraps
- Electronic Monitoring
- Alarms and Alarm Systems
- Computer Rooms
- Walls and Doors

ID Cards and Badges

One area of access control that ties physical security with information access control is the use of identification cards (ID) and name badges. An ID card is typically worn concealed, whereas a name badge is visible. These devices are forms of biometrics (facial recognition) to identify and authenticate an authorized individual with access to the facility.

Locks and Keys

There are two types of locks: mechanical and electro-mechanical. **The mechanical lock** relies on a key of carefully shaped pieces of metal that turn tumblers to release secured loops of steel,

aluminum, or brass (in brass padlocks). **The electro-mechanical lock** can accept a variety of inputs including keys that are magnetic strips on ID Cards, radio signals from name badges, PINs typed into a keypad.Locks are divided into **four categories**: manual, programmable, electronic, and biometric.

As part of general management's responsibility for the physical environment, the management of keys and locks is a fundamental concern. Sometimes locks fail and facilities need alternative procedures for access. Locks fail in one of two ways: when the lock of a door fails and the door becomes unlocked, that is a fail-safe lock; when the lock of a door fails and the door remains locked, this is a fail-secure lock.

Mantraps

A mantrap is a small enclosure that has an entry point and a different exit point. The individual entering the facility, area, or room, enters the mantrap, requests access through some form of electronic or biometric lock and key, and if verified, is allowed to exit the mantrap into the facility.

This is called a mantrap, because if the individual is denied entry, the mantrap does not allow exit until a security official overrides the automatic locks of the enclosure.

Electronic Monitoring

Used to record events within a specific area or areas where other types of physical controls are not practical. Monitoring frequently uses cameras viewing individuals, while on the other end of these cameras are video cassette recorders and related machinery that captures the video feed. These systems have drawbacks as for the most part they are reactive and do not prevent access or prohibited activity. Recorded monitoring requires an individual to review the information collected.

Alarms and Alarm Systems

Alarm systems notify appropriate individuals when a predetermined event or activity occurs.

This could be a fire, a break-in or intrusion, an environmental disturbance, such as flooding, or an interruption in services, such as a loss of power. **Burglar alarm systems** detect intrusions into unauthorized areas and notify either a local or remote security agency to react. These systems rely on a number of sensors that detect the intrusion: motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors.

Computer Rooms and Wiring Closets

Computer rooms and wiring and communications closets are facilities that require special attention to ensure the confidentiality, integrity, and availability of information. Logical access controls are easily defeated, if an attacker gains physical access to the computing equipment.

Custodial staff are often the least scrutinized of employees and non-employees who have access to offices. Yet custodians are given the greatest degree of unsupervised access.

Interior Walls and Doors

The security of information assets can sometimes be compromised because of the construction of the walls and doors of the facility. The walls in a facility are typically: standard interior or firewall.

All high-security areas, such as computer rooms and wiring closets, must have firewall grade walls surrounding them.

2.Fire Safety

The most serious threat to physical security and the safety of the people who work in the organization is the possibility of fire. Fires account for more property damage, personal injury, and death than any other threat to physical security. As a result, it is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards.

Fire Detection and Response

Fire suppression systems are devices installed and maintained to detect and respond to a fire, potential fire, or combustion situation. These devices typically work to deny an environment of one of the three requirements for a fire to burn: **temperature, fuel, and oxygen. Water and water mist systems** reduce the temperature of the flame to extinguish it and to saturate some categories of fuels to prevent ignition. **Carbon dioxide systems** rob fire of its oxygen. Soda acid systems deny fire its fuel, preventing spreading. **Gas-based systems** disrupt the fires chemical reaction but leave enough oxygen for people to survive for a short time. Before a fire can be suppressed, it must be detected.

Fire detection systems fall into two general categories: **manual and automatic**. Manual fire detection systems include human responses, such as calling the fire department, as well as manually activated alarms, such as sprinklers and gaseous systems. During the chaos of a fire evacuation, an attacker can easily slip into offices and obtain sensitive information. As part of a complete fire safety program, it is advisable to designate individuals as floor monitors.There are three basic types of fire detection systems**: thermal detection, smoke detection, and flame detection.**

The thermal detection systems contain a sophisticated heat sensor that operates in one of two ways, fixed temperature, and rate-of-rise. Smoke-detection systems are perhaps the most common means of detecting a potentially dangerous fire, and are required by building codes:

Smoke detectors operate in one of three ways:

1. photoelectric sensors project and detect an infrared beam, if interrupted activates alarm or

suppression systems.

2. ionization sensors contains a small amount of a harmless radioactive material within a detection chamber. When certain by-products of combustion enter, a change in the level of electrical conductivity activates the detector.
3. air-aspirating detectors take in air, filtering it, and moving it through a chamber containing a laser beam. If the laser beam is diverted or refracted by smoke particles, the system is activated.

The flame detector is a sensor that detects the infrared or ultraviolet light produced by an open flame. These systems require direct line-of-sight with the flame and compare the flame signature to a database to determine whether or not to activate the alarm and suppression systems.

While highly sensitive, flame detection systems are expensive and must be installed where they can scan all areas of the protected area.

Fire Suppression

Fire suppression systems can consist of portable, manual, or automatic apparatus. Portable extinguishers are rated by the type of fire:

- Class A: fires of ordinary combustible fuels. Use water and multi-purpose, dry chemical fire extinguishers.
- Class B: fires fueled by combustible liquids or gases, such as solvents, gasoline, paint, lacquer, and oil. Use carbon dioxide, multi-purpose dry chemical and Halon fire extinguishers.
- Class C: fires with energized electrical equipment or appliances. Use carbon dioxide, multi-purpose, dry chemical and Halon fire extinguishers.
- Class D: fires fueled by combustible metals, such as magnesium, lithium, and sodium. Use special extinguishing agents and techniques.

Manual and automatic fire response can include installed systems designed to apply suppressive agents. These are usually either sprinkler or gaseous systems.

All sprinkler systems are designed to apply liquid, usually water, to all areas in which a fire has been detected. In sprinkler systems, the organization can implement wet pipe, dry pipe, or pre-action systems. Water mist sprinklers are the newest form of sprinkler systems and rely on micro-fine mists instead of traditional shower-type systems. Chemical gas systems can be used

in the suppression of fires. Until recently there were only two major types of gaseous systems: carbon dioxide and Halon. Carbon dioxide robs a fire of its oxygen supply. Halon is a clean agent, which means that it does not leave any residue when dry, nor does it interfere with the operation of electrical or electronic equipment. Unfortunately the EPA has classified Halon as an ozone-depleting substance, and therefore new installations are prohibited.

Alternative clean agents include the following:

- FM-200
- Inergen
- Carbon dioxide
- FE-13 (trifluromethane)

3.<u>Failure of Supporting Utilities and Structural Collapse</u>

Supporting utilities, such as heating, ventilation and air conditioning, power, water, and other utilities, have a significant impact on the continued safe operation of a facility.

Extreme temperatures and humidity levels, electrical fluctuations and the interruption of water, sewage, and garbage services can create conditions that inject vulnerabilities in systems designed to protect information.

Heating, Ventilation, and Air Conditioning

Although traditionally a facilities management responsibility, the operation of the heating, ventilation, and air conditioning (HVAC) system can have dramatic impact on information and information systems operations and protection.

Specifically there are four areas within the HVAC system that can cause damage to information-carrying systems: temperature, filtration, humidity, and static electricity.

Temperature

Computer systems are electronic and as such are subject to damage from extreme temperature.

Rapid changes in temperature, from hot to cold, or from cold to hot can produce condensation, which can create short circuits or otherwise damage systems and components.

The optimal temperature for a computing environment (and people) is between 70 and 74 degrees Fahrenheit

Humidity

Humidity is the amount of moisture in the air. High humidity levels create condensation problems, and low humidity levels can increase the amount of static electricity in the environment. With condensation comes the short-circuiting of electrical equipment and the potential for mold and rot in paper-based information storage.

Static

Static electricity is caused by a process called triboelectrification, which occurs when two materials are rubbed or touched and electrons are exchanged, resulting in one object becoming more positively changed and the other more negatively charged. When a third object with an opposite charge or ground is encountered, electrons flow again, and a spark is produced. One of the leading causes of damage to sensitive circuitry is electro-static discharge (ESD). Integrated circuits in a computer use between two and five volts of electricity. Voltage levels as low as 200 can cause microchip damage.

Static electricity is not even noticeable to humans until levels approach 1,500 volts, and you can't see the little blue spark until it approaches 4,000 volts.

A person can generate up to 12,000 volts of static current by walking across a carpet. Two types of failures can result from ESD damage to chips. Immediate failures, also known as catastrophic failures, occur right away, are usually totally destructive. Latent failures or delayed failures can occur weeks or even months after the damage is done. It is imperative to maintain the optimal level of humidity, which is between 40 and 60 percent, in the computing environment. Humidity levels below this range create static, and levels above create condensation.

Ventilation Shafts

One last discussion point within the topic of HVAC is the security of the ventilation system air ductwork. While in residential buildings the ductwork is quite small, in large commercial buildings it can be large enough for an individual to climb though. If the vents are large, security can install wire mesh grids at various points to compartmentalize the runs. In any case, the ventilation system is one more area within the HVAC that must be evaluated.

Power Management and Conditioning

Not only is electrical quantity (voltage level and amperage rating) of concern, but so is the quality of the power (cleanliness and proper installation). Interference with the normal pattern of the electrical current is referred to as noise in the current. Any noise that interferes with the normal 60 Hertz cycle can result in inaccurate time clocks or, even worse, unreliable internal clocks inside the CPU.

- **Grounding**

  Grounding ensures that the returning flow of current is properly discharged to the ground.

  If this is not properly installed, anyone touching a computer or other electrical device could be used as a ground source, causing damage to equipment and injury or death to the person.

  Power should also be provided in sufficient amperage to support needed operations.

  Overloading a circuit not only causes problems with the circuit tripping but can also overload the power load on an electrical cable, creating the risk of fire.

- **Uninterruptible Power Supplies (UPS)**

In case of power outage, a UPS is a backup power source for major computer systems.

There are four basic configurations of UPS:

- A standby or offline UPS is an off-line battery backup that detects the interruption of power to the power equipment.
- A ferroresonant standby UPS is still an offline UPS, with the electrical service still providing the primary source of power, with the UPS serving as a battery backup. The ferroresonant transformer reduces power problems.
- The line-interactive UPS is always connected to the output, so has a much faster response time and incorporates power conditioning and line filtering.
- The true online UPS works in the opposite fashion to a standby UPS since the primary power source is the battery, with the power feed from the utility constantly recharging the batteries. This model allows constant feed to the system, while completely eliminating power problems.

- **Emergency Shutoff**

One important aspect of power management in any environment is the need to be able to stop power immediately should the current represent a risk to human or machine safety.

Most computer rooms and wiring closets are equipped with an emergency power shutoff, which is usually a large red button, prominently placed to facilitate access, with an accident-proof cover to prevent unintentional use.

Electrical power influences:

- Fault: momentary interruption in power
- Blackout: prolonged interruption in power
- Sag: momentary drop in power voltage levels
- Brownout: prolonged drop in power voltage levels
- Spike: momentary increase in power voltage levels
- Surge: prolonged increase in power voltage levels

Water Problems

Lack of water poses problem to systems, including the functionality of fire suppression systems, and the ability of water chillers to provide air-conditioning. On the other hand, a surplus of water, or water pressure, poses a real threat. It is therefore important to integrate water detection systems into the alarm systems that regulate overall facilities operations.

Structural Collapse

Unavoidable environmental factors or forces of nature can cause failures of structures that house the organization. Structures are designed and constructed with specific load limits, and

overloading these design limits, intentionally or unintentionally, inevitably results in structural failure and potentially loss of life or injury. Periodic inspections by qualified civil engineers assists in identifying potentially dangerous structural conditions well before they fail.

Testing Facility Systems

Just as with any phase of the security process, the physical security of the facility must be constantly documented, evaluated, and tested. Documentation of the facilities configuration, operation, and function is integrated into disaster recovery plans and standing operating procedures.

Testing provides information necessary to improve the physical security in the facility and identifies areas weak points.

10.<u>What is meant by security and personnel?</u>

SECURITY AND PERSONNEL

i. Introduction

When implementing information security, there are many human resource issues that must be addressed

- Positioning and naming
- Staffing
- Evaluating impact of information security across every role in IT function
- Integrating solid information security concepts into personnel practices

Employees often feel threatened when organization is creating or enhancing overall information security program

ii. Positioning and Staffing the Security Function

The security function can be placed within:

- IT function
- Physical security function
- Administrative services function
- Insurance and risk management function
- Legal department

Organizations balance needs of enforcement with needs for education, training, awareness, and customer service

iii. Staffing The Information Security Function

Selecting personnel is based on many criteria, including supply and demand
Many professionals enter security market by gaining skills, experience, and credentials
At present, information security industry is in period of high demand

Qualifications and Requirements

The following factors must be addressed:

- Management should learn more about position requirements and qualifications
- Upper management should learn about budgetary needs of information security function

- IT and management must learn more about level of influence and prestige the information security function should be given to be effective

Organizations typically look for technically qualified information security generalist

Organizations look for information security professionals who understand:

- How an organization operates at all levels
- Information security usually a management problem, not a technical problem
- Strong communications and writing skills
- The role of policy in guiding security efforts

Organizations look for (continued):

- Most mainstream IT technologies
- The terminology of IT and information security
- Threats facing an organization and how they can become attacks
- How to protect organization's assets from information security attacks
- How business solutions can be applied to solve specific information security problems

Entry into the Information Security Profession

Many information security professionals enter the field through one of two career paths:

- Law enforcement and military
- Technical, working on security applications and processes

Today, students select and tailor degree programs to prepare for work in information security

Organizations can foster greater professionalism by matching candidates to clearly defined expectations and position descriptions

Information Security Positions

Use of standard job descriptions can increase degree of professionalism and improve the consistency of roles and responsibilities between organizations

Charles Cresson Wood's book *Information Security Roles and Responsibilities Made Easy* offers set of model job descriptions

Chief Information Security Officer (CISO or CSO)

- Top information security position; frequently reports to Chief Information Officer
- Manages the overall information security program
- Drafts or approves information security policies
- Works with the CIO on strategic plans

Chief Information Security Officer (CISO or CSO) (continued)

- Develops information security budgets
- Sets priorities for information security projects and technology
- Makes recruiting, hiring, and firing decisions or recommendations
- Acts as spokesperson for information security team
- Typical qualifications: accreditation; graduate degree; experience

Security Manager

- Accountable for day-to-day operation of information security program
- Accomplish objectives as identified by CISO
- Typical qualifications: not uncommon to have accreditation; ability to draft middle and lower level policies, standards and guidelines; budgeting, project management, and hiring and firing; manage technicians

iv. Employment Policies and Practices

Management community of interest should integrate solid information security concepts into organization's employment policies and practices

Organization should make information security a documented part of every employee's job description

From information security perspective, hiring of employees is a responsibility laden with potential security pitfalls

CISO and information security manager should provide human resources with information security input to personnel hiring guidelines

Termination

When employee leaves organization, there are a number of security-related issues

Key is protection of all information to which employee had access

Once cleared, the former employee should be escorted from premises

Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback

Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting

- Before employee is aware, all logical and keycard access is terminated
- Employee collects all belongings and surrenders all keys, keycards, and other company property
- Employee is then escorted out of the building

Friendly departures include resignation, retirement, promotion, or relocation

- Employee may be notified well in advance of departure date
- More difficult for security to maintain positive control over employee's access and information usage
- Employee access usually continues with new expiration date
- Employees come and go at will, collect their own belongings, and leave on their own

Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores

Possible that employees foresee departure well in advance and begin collecting organizational information for their future employment

Only by scrutinizing systems logs after employee has departed can organization determine if there has been a breach of policy or a loss of information

If information has been copied or stolen, action should be declared an incident and the appropriate policy followed

11. Discuss in detail about employment policies and practices?

- Management community of interest should integrate solid information security concepts into organization's employment policies and practices
- Organization should make information security a documented part of every employee's job description
- From information security perspective, hiring of employees is a responsibility laden with potential security pitfalls
- CISO and information security manager should provide human resources with information security input to personnel hiring guidelines

Job Descriptions

- Integrating information security perspectives into hiring process begins with reviewing and updating all job descriptions
- Organization should avoid revealing access privileges to prospective employees when advertising open positions

Background Checks

- Investigation into a candidate's past
- Should be conducted before organization extends offer to candidate
- Background checks differ in level of detail and depth with which candidate is examined
- May include identity check, education and credential check, previous employment verification, references check, drug history, credit history, and more

Employment Contracts

- Once a candidate has accepted the job offer, employment contract becomes important security instrument
- Many security policies require an employee to agree in writing
- New employees may find policies classified as "employment contingent upon agreement," whereby employee is not offered the position unless binding organizational policies are agreed to

New Hire Orientation

- New employees should receive extensive information security briefing on policies, procedures, and requirements for information security
- Levels of authorized access are outlined; training provided on secure use of information systems
- By the time employees start, they should be thoroughly briefed and ready to perform duties securely

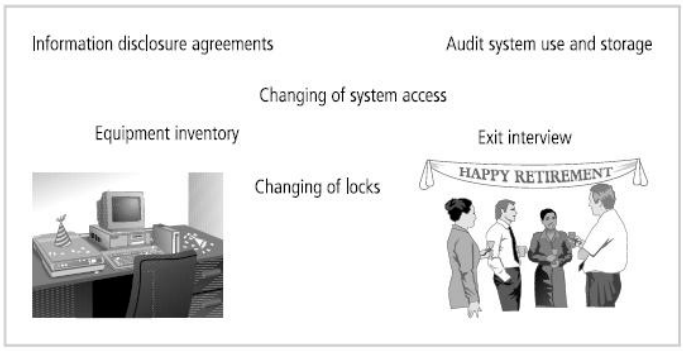
On-the-Job Security Training

- Organization should conduct periodic security awareness training
- Keeping security at the forefront of employees' minds and minimizing employee mistakes is an important part of information security awareness mission
- External and internal seminars also increase level of security awareness for all employees, particularly security employees

Evaluating Performance

- Organizations should incorporate information security components into employee performance evaluations
- Employees pay close attention to job performance evaluations; if evaluations include information security tasks, employees are more motivated to perform these tasks at a satisfactory level

Termination



Termination Activities

Source: Course Technology/Cengage Learning

- When employee leaves organization, there are a number of security-related issues
- Key is protection of all information to which employee had access
- Once cleared, the former employee should be escorted from premises
- Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback
- Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting
    - Before employee is aware, all logical and keycard access is terminated
    - Employee collects all belongings and surrenders all keys, keycards, and other company property
    - Employee is then escorted out of the building
- Friendly departures include resignation, retirement, promotion, or relocation
    - Employee may be notified well in advance of departure date
    - More difficult for security to maintain positive control over employee's access and information usage
    - Employee access usually continues with new expiration date
    - Employees come and go at will, collect their own belongings, and leave on their own
- Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores
- Possible that employees foresee departure well in advance and begin collecting organizational information for their future employment
- Only by scrutinizing systems logs after employee has departed can organization determine if there has been a breach of policy or a loss of information
- If information has been copied or stolen, action should be declared an incident and the appropriate policy followed

12. What are the Security Considerations for Nonemployees in an Organization? Explain.

- Individuals not subject to screening, contractual obligations, and eventual secured termination often have access to sensitive organizational information
- Relationships with these individuals should be carefully managed to prevent possible information leak or theft

Temporary Employees

- Hired by organization to serve in temporary position or to supplement existing workforce
- Often not subject to contractual obligations or general policies; if temporary employees breach a policy or cause a problem, possible actions are limited
- Access to information for temporary employees should be limited to that necessary to perform duties
- Temporary employee's supervisor must restrict the information to which access is possible

Contract Employees

- Typically hired to perform specific services for organization
- Host company often makes contract with parent organization rather than with individual for a particular task
- In secure facility, all contract employees escorted from room to room, as well as into and out of facility
- There is need for restrictions or requirements to be negotiated into contract agreements when they are activated

Consultants

- Should be handled like contract employees, with special requirements for information or facility access integrated into contract
- Security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements to protect organization
- Just because security consultant is paid doesn't make the protection of organization's information the consultant's number one priority

Business Partners

- Businesses find themselves in strategic alliances with other organizations, desiring to exchange information or integrate systems
- There must be meticulous, deliberate process of determining what information is to be exchanged, in what format, and to whom
- Nondisclosure agreements and the level of security of both systems must be examined before any physical integration takes place

13. Explain briefly about Security Technology?

Security Technology

What is Security?

✓ quality or state of being secure—to be free from danger"
✓ A successful organization should have multiple layers of security in place:
- Physical security
- Personal security
- Operations security
- Communications security
- Network security
- Information security

Physical Design

✓ Physical design of an information security program is made up of two parts:
1. **Security technologies**
2. **Physical security**

✓ Physical design process:
- Identifies complete technical solutions based on these technologies (deployment, operations and maintenance elements)

- Design physical security measures to support the technical solution.

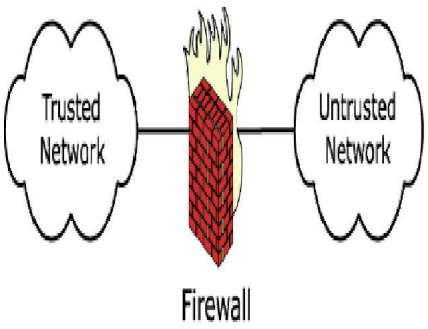
Firewalls

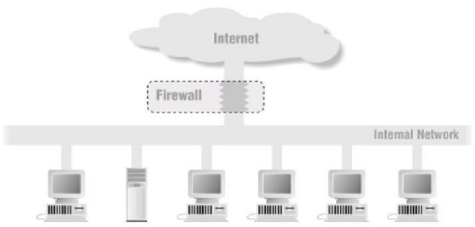
✓ A software or hardware component that restricts network communication between two computers or networks.
- In buildings, a firewall is a fireproof wall that restricts the spread of a fire.
- Network firewall prevents threats from spreading from one network to another

✓ Prevent specific types of information from moving between the outside world (untrusted networks) and the inside world (trusted networks)

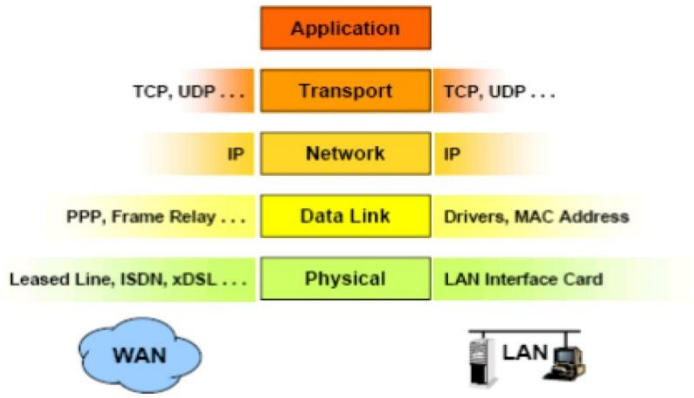
✓ The firewall may be a separate computer system, a software servic e running on an existing router all serve r, or a separate network containing a number of supporting devices.

Internet Firewalls





The Internet Protocol Stack



What Firewalls do

- ✓ Protects the resources of an internal network.
  - Restrict external access.
  - Log Network activities.
- Intrusion detection
- DoS
  - Act as intermediary
  - Centralized Security Management
  - Carefully administer one firewall to control internet traffic of many machines.
  - Internal machines can be administered with less care.

Types of Firewalls (General)

- ✓ Firewalls types can be categorized depending on:
  - The Function or methodology the firewall use
  - Whether the communication is being done between a single node and the network, or between two or more networks.
  - Whether the communication state is being tracked at the firewall or not.
- ✓ **With regard to the scope of filtered communications the done between a single node and the network, or between two or more networks there exist :**
  - Personal Firewalls, a software application which normally filters traffic entering or leaving a single computer.
  - Network firewalls, normally running on a dedicated network device or computer positioned on the boundary of two or more networks.

Firewall categorization methods

The Function or methodology the firewall use

- ✓ Five processing modes that firewalls can be categorized by are :
  1. packet filtering

2. application gateways
3. circuit gateways
4. MAC layer firewalls
5. hybrids

1.Packet filtering:

- ✓ examine the header information of data packets that come into a network.
- ✓ a packet filtering firewall installed on TCP/IP based network and determine wether to drop a packet or forward it to the next network connection based on the rules programmed in the firewall.
- ✓ Packet filtering firewalls scan network data packets looking for violation of the rules of the firewalls database.
- ✓ Filtering firewall inspect packets on at the network layers.
- ✓ If the device finds a packet that matches a restriction it stops the packet from traveling from network to another.
- ✓ filters packet-by-packet, decides to *Accept/Deny/Discard* packet based on certain/configurable criteria **–** *Filter Rule sets*.
- ✓ Typically stateless: do not keep a table of the connection *state* of the various traffic that flows through them
  - Not dynamic enough to be considered true firewalls.
  - Usually located at the boundary of a network.
  - Their main strength points: ***Speed*** and ***Flexibility***.

There are three subsets of packet filtering firewalls:

1. static filtering
2. dynamic filtering
3. stateful inspection

1. **static filtering:**

- ✓ requires that the filtering rules coverning how the firewall decides which packets are allowed and which are denied.
- ✓ This type of filtering is common in network routers and gateways.

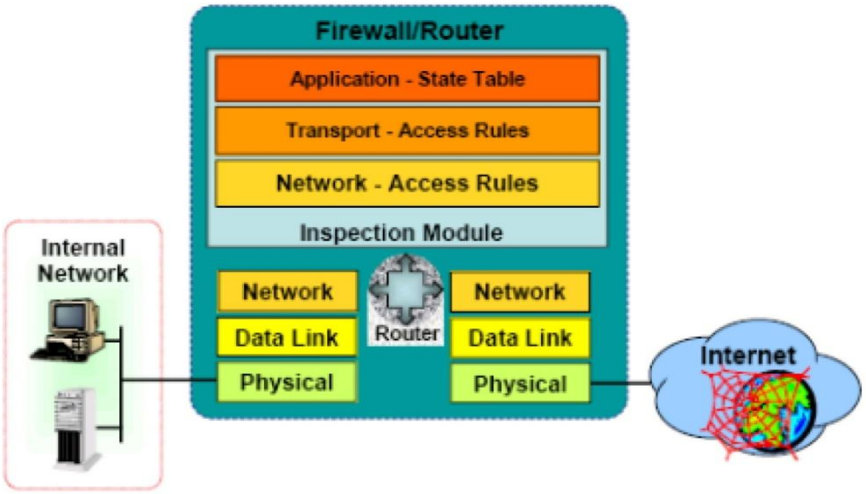
2. **Dynamic filtering**

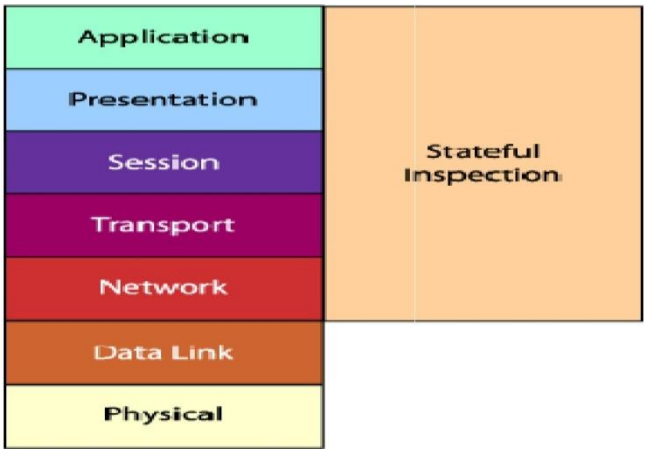
- ✓ allows the firewall to create rules to deal with event.
- ✓ This reaction could be positive as in allowing an internal user to engage in a specific activity upon request or negative as in dropping all packets from a particular address

3. **Stateful inspection**

- ✓ keep track of each network connection between internal and external systems using a state table.
- ✓ A state table tracks the state and context of each packet in the conversation by recording which station send , what packet and when.
- ✓ More complex than their constituent component firewalls
- ✓ Nearly all modern firewalls in the market today are staful

Stateful Inspection Firewalls





Basic Weaknesses Associated w ith Packet Filters\ Statful

- They cannot pre vent attacks that employ application-specific vulnerabilities or functions.
- Logging function ality present in packet filter firewalls is limited
- Most packet filter firewalls do not support advanced user authent ication schemes.
- Vulnerable to attacks and exploits that take advantage of pro blems within the TCP/IP specification and protocol stack, such as network layer ad dress spoofing.
- Susceptible to sec urity breaches caused by improper configurations.

✓ **Advantages**:
- One packet filter can protect an entire network
- Efficient (require s little CPU)

- Supported by mosst routers

✓ **Disadvantages**:
- Difficult to config ure correctly

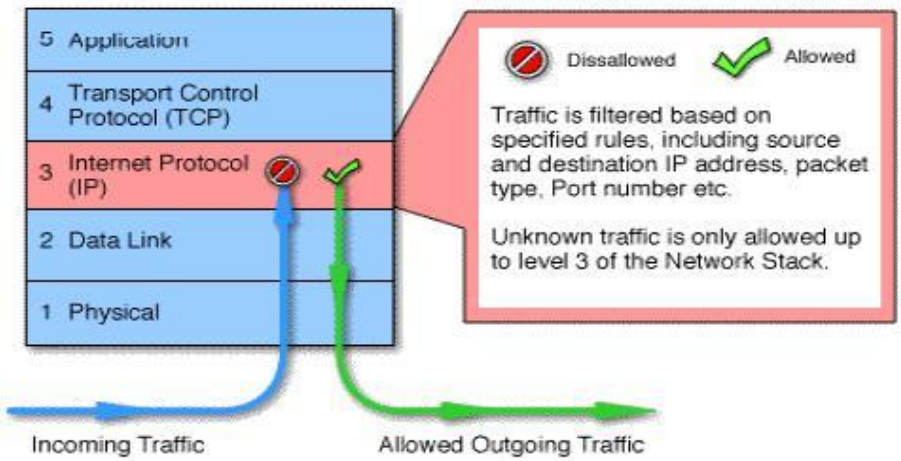
✓ Must consider rule set in its entirety
- Difficult to test co mpletely
- Performance penalty for complex rulesets

✓ Stateful packet filtering much more expensive
- Enforces ACLs at layer 3 + 4, without knowing any application details

Packet Filtering Firewalls

✓ The original firewall
✓ Works at the network level of the OSI
✓ model
✓ Applies packet filters based on access
✓ Rules:
- Source IP address
- Destination IP address
- Application or protocol
- Source port number
- Destination port number

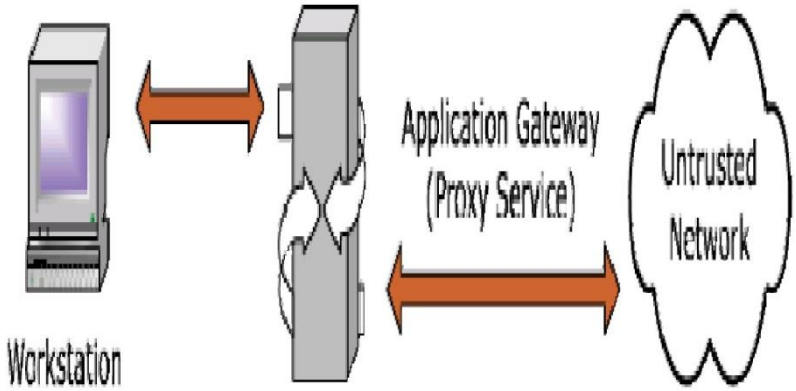
Packet Filtering Firewalls



2. **Application gateways:**
   - ✓ is also known as proxy server since it runs special software that acts as a proxy for a service request.
   - ✓ One common example of proxy server is a firewall that blocks or requests for and responses to request for web pages and services from the internal computers of an organization.
   - ✓ The primary disadvantag e of application level firewalls is that they ar e designed for a specific protocols and c annot easily be reconfigured to protect against attacks in other protocols.
   - ✓ Application firewalls wo rk at the application layer.
   - ✓ Filters packets on applica tion data as well as on IP/TCP/UDP fields.
   - ✓ The interaction is controlled at the application layer
   - ✓ A proxy server is an application that mediates traffic between two network segments.
   - ✓ With the proxy acting a s mediator, the source and destination system s never actually

"connect".

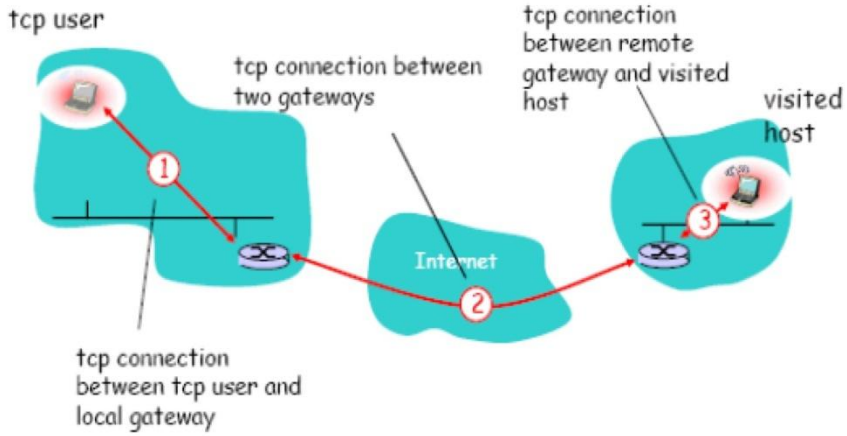
   - ✓ Filtering Hostile Code: Proxies can analyze the payload of a packet o f data and make decision as to whether thiis packet should be passed or dropped.



4.Circuit gateways:

- ✓ operates at the transport layer.
- ✓ Connections are authorized based on addresses , they prevent direct connections between network and another.
- ✓ They accomplish this prevention by creating channels connecting specific systems on each side of the firewall and then allow only authorized traffic.
- ✓ relays two TCP connections (session layer)
- ✓ imposes security by limiting which such connections are allowed
- ✓ once created usually relays traffic without examining contents
- ✓ Monitor handshaking between packets to decide whether the traffic is legitimate
- ✓ typically used when trust internal users by allowing general outbound connections
- ✓ SOCKS commonly used for this

Circuit Level Firewalls Example



4.MAC layer firewalls:

- ✓ design to operate at the media access control layer.
- ✓ Using this approach the MAC addresses of specific host computers are linked to ACL entries that identify the specific types of packets that can be send to each host and all other traffic is blocked.

5.Hybrids firewalls:

- ✓ companied the elements of other types of firewalls , example the elements of packet filtering and proxy services, or a packet filtering and circuit gateways.
- ✓ That means a hybrids firewalls may actually of two separate firewall devices; each is a separate firewall system, but they are connected so that they work together.

Types of Firewalls

- ✓ Finally, Types depending on whether the firewalls keeps track of the state of network connections or treats each packet in isolation, two additional categories of firewalls exist:
  - Stateful firewall
  - Stateless firewall

Stateful firewall

- ✓ keeps track of the state of network connections (such as TCP streams) traveling across it.
- ✓ Stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection.

Stateless firewall

- ✓ Treats each network frame (Packet) in isolation. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
- ✓ The classic example is the File Transfer Protocol, because by design it opens new connections to random ports.

Advantages of a Firewall

- ✓ Stop incoming calls to insecure services

- ✓ such as rlogin and NFS
- ✓ Control access to other services
- ✓ Control the spread of viruses
- ✓ Cost Effective
- ✓ More secure than securing every
- ✓ system

Disadvantages of a Firewall

- ✓ Central point of attack
- ✓ Restrict legitimate use of the Internet
- ✓ Bottleneck for performance
- ✓ Does not protect the 'back door'
- ✓ Cannot always protect against
- ✓ smuggling
- ✓ Cannot prevent insider attacks