E. G. S. Pillay Engineering College, Nagapattinam
Computer Science and Engineering

Elective II **IT 2042 INFORMATION SECURITY** **VIII Sem CSE**

QUESTION BANK - UNIT-I

1) What is information security?

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

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

2) Trace the history of information security

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

3) What is Rand Report R-609?

Information Security began with Rand Corporation Report R-609

The Rand Report was the first widely recognized published document to identify the role of management and policy issues in computer security.

The scope of computer security grew from physical security to include:

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

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

"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

5) What are the critical characteristics of information?

- **Availability** – enables authorized users – persons or computer systems – to access information without interference or obstruction and receive it in the required format
- **Accuracy** – Accuracy of information refers to information which is free from mistakes or errors and has the value the end user expects(Eg inaccuracy of your bank account may result in mistakes such as bouncing of a check)
- **Authenticity** – refers to quality or state of being genuine or original,rather than reproduction or fabrication. Information is authentic when the contents are original as it was created,palced or stored or transmitted.(The information you receive as e-mail may not be authentic when its contents are modified what is known as **E-mail spoofing**)
- **Confidentiality** – Information has confidentiality when disclosure or exposure to unauthorized individuals or systems is prevented 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.
- **Integrity** – Information has integrity when it is whole,complete, and uncorrupted The integrity of information is threatened when it is exposed to corruption,damage,destruction,other disruption of its authentic state.(Many computer virues or worm are designed with the explicit purpose of corrupting data. Information integrity is the corner stone of information systems,because information is of no value or use if users cannot verify its integrity. Redundancy bits and check bits can compensate for internal and external threats to integrity of information.
- **Utility** – The utility of information is the quality or state of having value for some purpose or end. (For example,the US census data reveals information about the voters like their gender,age,race,and so on.
- **Possession** – the possession of information is the quality or state of having ownership or control of some object or item. Breach of possession does not result in breach of confidentiality.(Illegal possession of encrypted data never allows someone to read it without proper decryption methods)

6) What is 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

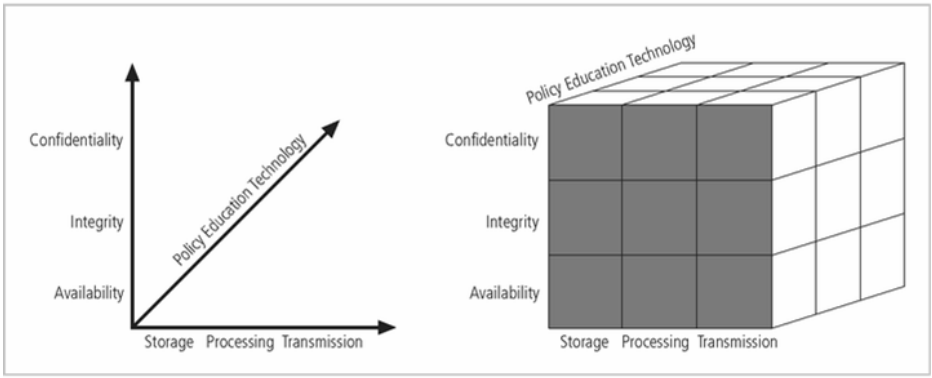


FIGURE 1-3 NSTISSC Security Model

7) What are the components of an information system?

An Information System (IS) is much more than computer hardware; it is the entire set of software, hardware, data, people, and procedures necessary to use information as a resource in the organization

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. Information security is often implemented as an after thought rather than developed as an integral component from the beginning. Software programs become an easy target of accidental or intentional attacks.

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 aphysical asset and with the protection of these assets from harm or theft.

Data – 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.

People – 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.

Procedures – 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 correctred.

Networks - 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.

8) 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

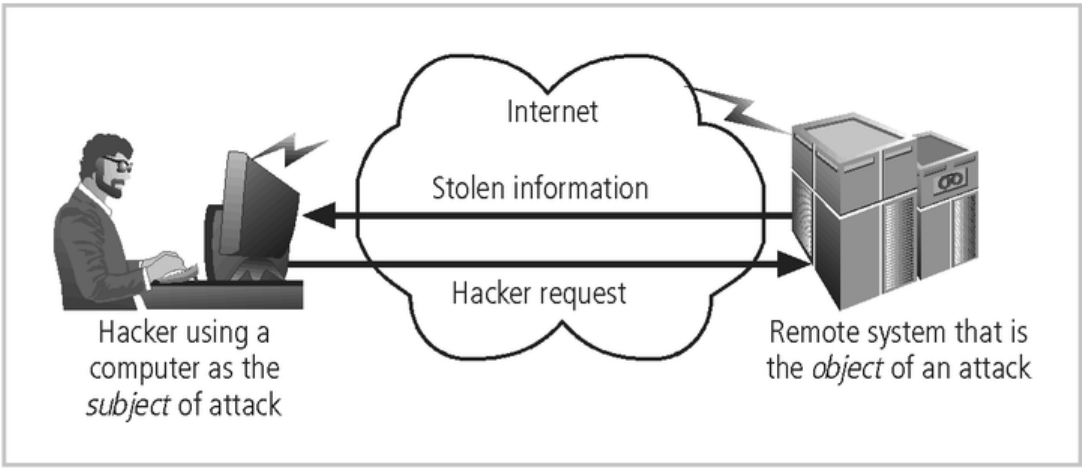


FIGURE 1-5 Computer as the Subject and Object of an Attack

8) What is meant by balancing Security and Access?

Balancing Security and Access

- It is impossible to obtain perfect security - it is not 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

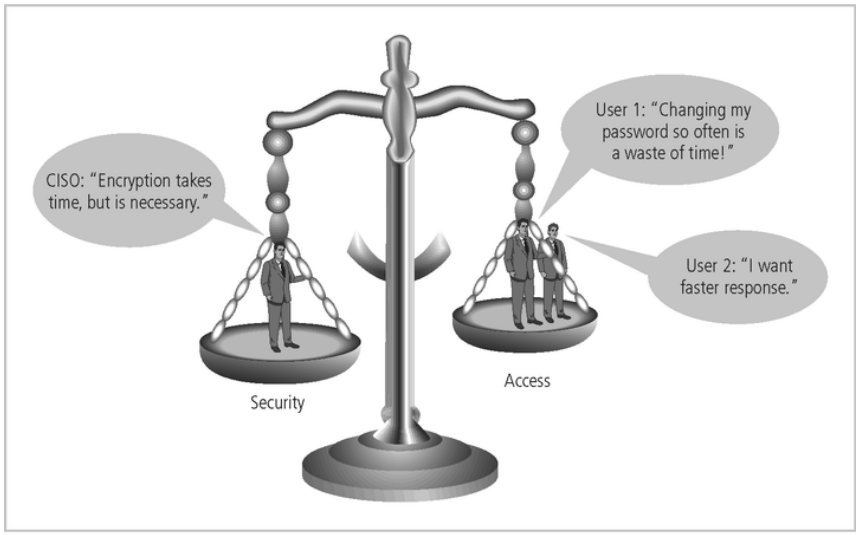


FIGURE 1-6 Balancing Security and Access

9) What are the approaches used for implementing information security?

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

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

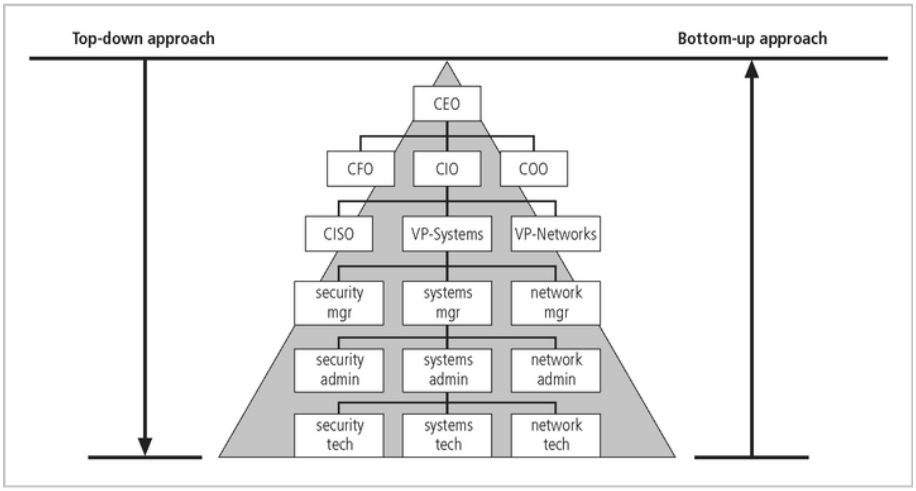


FIGURE 1-7 Approaches to Security Implementation

10) What is SDLC?

The Systems Development Life Cycle

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

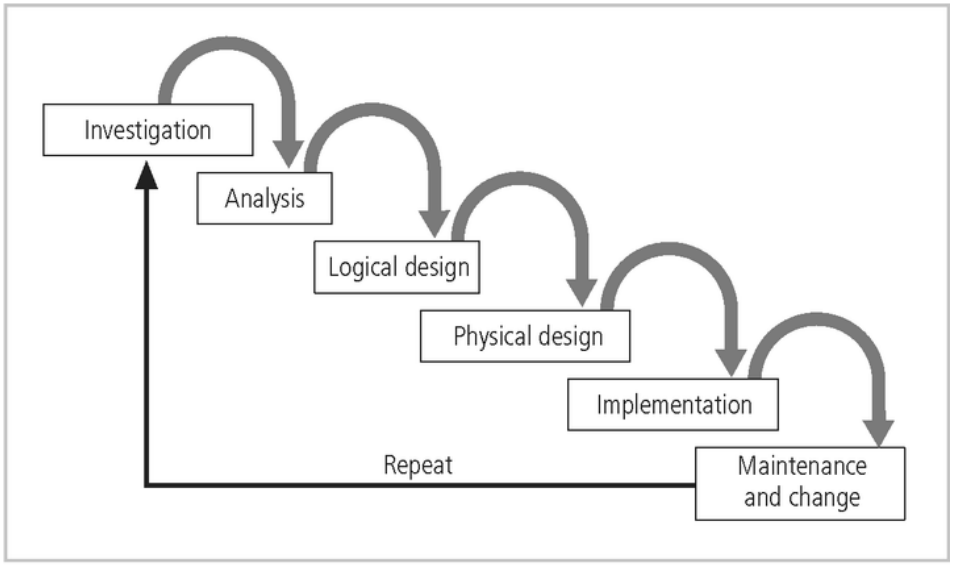


FIGURE 1-8 SDLC Waterfall Methodology

11) Explain different phases of SDLC

Investigation

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

Analysis

- Consists primarily of
  - assessments of the organization
  - the status of current systems
  - capability to support the proposed systems
- Analysts begin to determine
  - what the new system is expected to do
  - how the new system will interact with existing systems
- Ends with the documentation of the findings and a feasibility analysis update

Logical Design

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

Physical Design

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

Implementation

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

Maintenance and Change

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

12) 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

- 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

- 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

- 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 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

- 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

13) ***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

- 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

- 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

14)**How information security is viewed as a social science?**

Security 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

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

Senior Management

- 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

- 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

16)what are the three types of data ownwership and their responsibilities?

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

- Data Custodian - responsible for the storage, maintenance, and protection of the information
- Data Users - the end systems users who work with the information to perform their daily jobs supporting the mission of the organization

17) 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.)

18) 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.

19) What is attack?

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.**

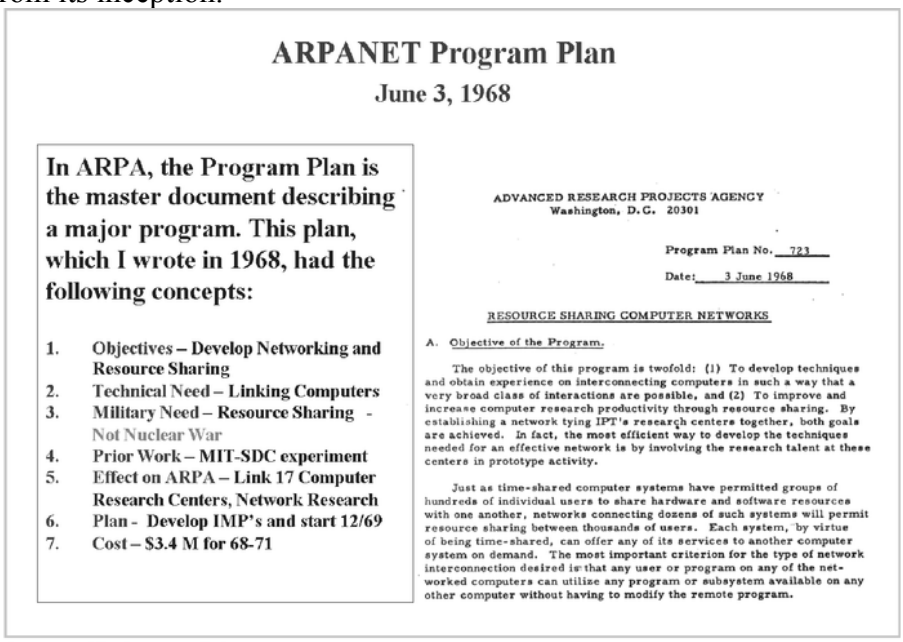
20) What is hacking?
Hacking can be defined positively and negatively.
(1) to write computer programs for enjoyment
(2) to gain access to a computer illegally
In early days the computer enthusiasts are called hacks or hackers because they could tear apart the computer instruction code,or even a computer 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.

21)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.

22) **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.

23)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.



Courtesy of Dr. Lawrence Roberts

FIGURE 1-2 ARPANET Program Plan[4]

- ARPANET grew in popularity as did its potential for misuse
- Fundamental problems with ARPANET security were identified
  - No safety procedures for dial-up connections to the ARPANET
  - User identification and authorization to the system were non-existent
- In the late 1970s the microprocessor expanded computing capabilities and security threats