Chettinad
College of Engineering & Technology
Approved by AICTE-New Delhi and Affiliated to Anna University-Chennai

Academic Year 2024 - 2025

Question Bank

Year/Semester:III/ V **Date:**12/08/2024	**Department : AI&DS** **Subject Code/Title : CW3551 & DIS** **Faculty Name : Ms.A.Kanimozhi**	**Unit :** I/II/ **Section : Part A/B/C**

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 andhardware 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 shouldhave?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 fromunauthorized access and misuse

6. What is Personal Security?

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

7. What is Operation Security?

The Operations security focuses on the protection of the details of particular operationsor 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,includingthe 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?

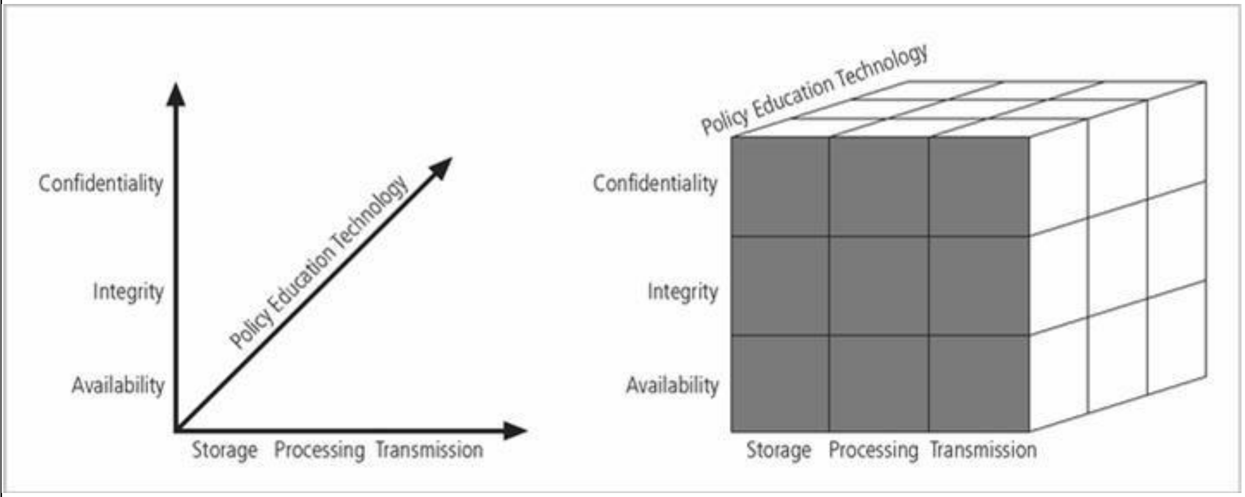
it refers to information which is free from mistakes or errors and has the value the end user expects

13. What is Accuracy of information?

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

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 informationsecurity. The model consists of three dimensions


Confidentiality
Integrity
Availability
Policy Education Technology
Storage Processing Transmission
Policy Education Technology
Confidentiality
Integrity
Availability
Storage Processing Transmission

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 ownershipor 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

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 athreat to information security and they are the weakest link in a security chain.. Policy, educationand training, awareness, and technology should be properly employed to prevent people from accidently or intentionally damaging or losing information.

22. Write about Procedures components 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. Educatingemployees 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.

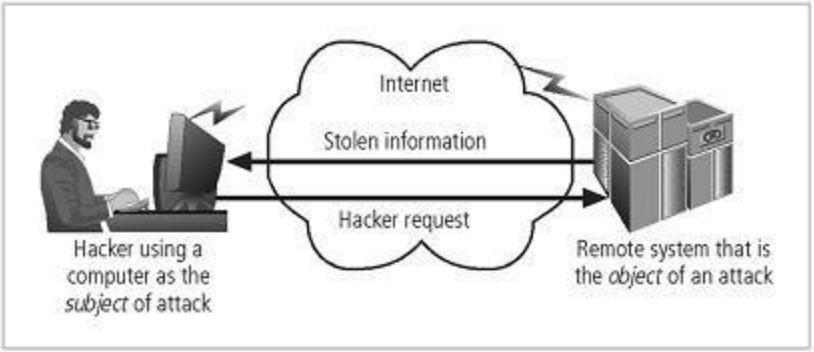
23. Write short notes on Networks components of an information system.

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


Internet
Stolen information
Hacker request
Hacker using a computer as the *subject* of attack
Remote system that is the *object* of an attack

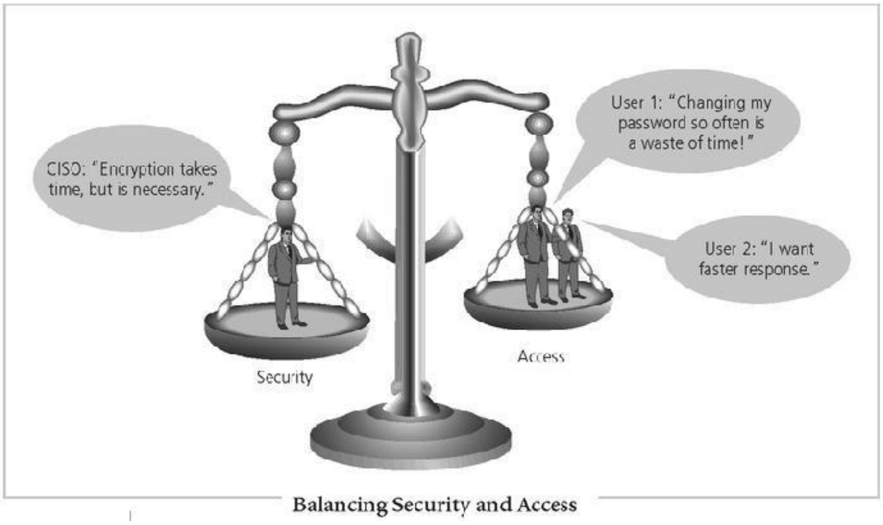
Computer as the Subject and Object of an Attack

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


CISO: "Encryption takes time, but is necessary."
User 1: "Changing my password so often is a waste of time!"
User 2: "I want faster response."
Security
Access

Balancing Security and Access

PART -B

1. Evaluate the various components of Information Security that a successful organization must have

2.i)List the various components of an information system and tell about them. (8)

ii)List the history of Information Security.(5)

3.i).What is NSTISSC Security Model?(8)

ii).Describe in detail about the top down approach and the bottom up approach with the help of a diagram. (5)

4.i). Identify the types of attacks in Information Security.

ii). Examine E-mail spoofing and phishing.

5.i).Discuss about the need for confidentiality in Information Security. (7)

ii).Explain the file hashing in the integrity of the information. (6)

6.i)Examine the critical characteristics of information security.

ii)Analyse in detail about the advantages and disadvantages of information security.(7)

7.Illustrate briefly about SDLC waterfall methodology and its relation in respect to information security.

Describe the Security Systems Development Life Cycle.

8.i)Compose the roles of Information Security Project Team.

ii)Design the steps unique to the security systems development life cycle in all the phases of SSDLC model.

9.i)Illustrate the different types of instruction set architecture in detail.

ii) Examine the basic instruction types with examples.

10. What are the six components of an information system? Which are most directly affected by the study of computer security?

UNIT-II

1.Why is information security a management problem?

Management is responsible for implementing information security to protect the ability of the organization to function. They must set policy and operate the organization in a manner that complies with the laws that govern the use of technology.

2.What is intellectual property?

It is the ownership of ideas and control over the tangible or virtual representation of those ideas.

3.What is a policy? How it differs from law?

ï‚· Policies: A body of expectations that describe acceptable and unacceptable employee behaviors in the workplace.

ï‚· It functions as organizational laws, complete with penalties, judicial practices, and sanctions to require complaints.

ï‚· The difference between policy and a law, however, is that ignorance of a policy is an acceptable defense.

4.What are the general categories of unethical and illegal behavior?

There are three general categories of unethical behavior that organizations and society should seek to eliminate:

Ignorance
Accident
Intent

5.What are the various types of malware?

- Viruses
- Worms
- Trojan horses
- Active web scripts

6. Who are hackers? What are the levels of hackers?

Hackers are people who use and create computer software for enjoyment or to gain access to information illegally.

There are two levels of hackers.

a. Expert Hacker - Develops software codes
b. Unskilled Hacker - Uses the codes developed by the experts

7. What is security blue print?

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

8. What are the types of virus?

a. Macro virus

b. Boot virus

9. Define Information Extortion

a. Information extortion is an attacker or formerly trusted insider stealing information from a computer system and demanding compensation for its return or non-use

b. Extortion found in credit card number theft

10. Define Hoax.

a. A computer virus hoax is a message warning the recipient of a non-existent computer virus threat

b. The message is usually a chain e-mail that tells the recipient to forward it to everyone they know

PART B

1. Explain the functions of an Information security organization. (Nov/Dec2022)

2.Describe about various forms of attacks.

3. Explain the different categories of threat. Give Examples.

4. Write about the attack replication vectors in detail.

5. Discuss the ethical concepts in information security.

6. i). Discuss about the threats.

ii).Express about five criterias for a policy to become enforcebale.

7. Illustrate the methods does a social engineering hacker use to gain information about a user’s login id and password? How would this method differ if it were targeted towards an administrator’s assistant versus a data-entry clerk? (13)

8. Describe about the types of Laws and Ethics in Information Security. (13)

9. How will you develop management groups that are responsible for implementing information security to protect the organization’s ability to function? (13)

10.i) State the types of password attacks.

ii)Tell the three ways in which an authorization can be handled.

11. i) Express in detail about:

(a)Protecting the functionality of an organization

(b)Enabling the safe operations of Applications (c)Protecting data that organizations collect and use

(d)Safeguarding Technology Assets in organizations

ii)Discuss in detail about worms.

PART C

1. Discuss the role and focus of any four professional organizations providing information security. (Create)

Faculty Incharge **HOD/AI&DS**

(A.Kanimozhi)

HoD Remarks