U23CST64 INFORMATION SECURITY

L	T	P	C
3	0	0	3

OBJECTIVES:

- To understand the basics of Information Security
- To know the legal, ethical and professional issues in Information Security
- To know the aspects of risk management
- To become aware of various standards in this area
- To know the technological aspects of Information Security

UNIT I INTRODUCTION **9**

History, What is Information Security?, Critical Characteristics of Information, NSTISSC Security Model, Components of an Information System, Securing the Components, Balancing Security and Access, The SDLC, The Security SDLC

UNIT II SECURITY INVESTIGATION **9**

Need for Security, Business Needs, Threats, Attacks, Legal, Ethical and Professional Issues An Overview of Computer Security - Access Control Matrix, Policy-Security policies, Confidentiality policies, Integrity policies and Hybrid policies.

UNIT III SECURITY ANALYSIS **9**

Risk Management: Identifying and Assessing Risk, Assessing and Controlling Risk - Systems:Access Control Mechanisms, Information Flow and Confinement Problem.

UNIT IV LOGICAL DESIGN **9**

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.

UNIT V PHYSICAL DESIGN **9**

Security Technology, IDS, Scanning and Analysis Tools, Cryptography, Access Control Devices,Physical Security, Security and Personnel.

TOTAL :45 PERIODS

OUTCOMES:

At the end of this course, the students should be able to:

- Discuss the basics of information security
- Illustrate the legal, ethical and professional issues in information security
- Demonstrate the aspects of risk management.
- Become aware of various standards in the Information Security System
- Design and implementation of Security Techniques.

TEXT BOOK:

1. Michael E Whitman and Herbert J Mattord, “Principles of Information Security”, VikasPublishing House, New Delhi, 2003

REFERENCES:

1. Micki Krause, Harold F. Tipton, “ Handbook of Information Security Management”, Vol 1-3CRC Press LLC, 2004.
2. Stuart McClure, Joel Scrambray, George Kurtz, “Hacking Exposed”, Tata McGraw- Hill,2003
3. Matt Bishop, “Computer Security Art and Science”, Pearson/PHI, 2002.

UNIT – I
PART – A (2 Marks)

1. Define information security. (Remember)

It is a well-informed sense of assurance that the information risks and controls are in balance.

2. List the critical characteristics of information. (Remember)

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

3. Define security. What are the multiple layers of security? (Remember)

Security is "the quality or state of being secure-to be free from danger".

- Physical Security
- Personal Security
- Operations Security
- Communication Security
- Network Security
- Information Security

4. When can a computer be a subject and an object of an attack respectively? (Remember)

When a computer is the subject of attack, it is used as an active tool to conduct the attack. When a computer is the object of an attack, it is the entity being attacked.

5. Why is a methodology important in implementing the information security? (Remember)

Methodology is a formal approach to solve a problem based on a structured sequence of procedures.

6. Difference between vulnerability and exposure. **(Understand)**

Vulnerability	Exposure
Weakness or fault in a system or protection mechanism that expose information to attack or damage.	The exposure of an information system is a single instance when the system is open to damage.

7. Sketch the NSTISSC security model. **(Remember)**

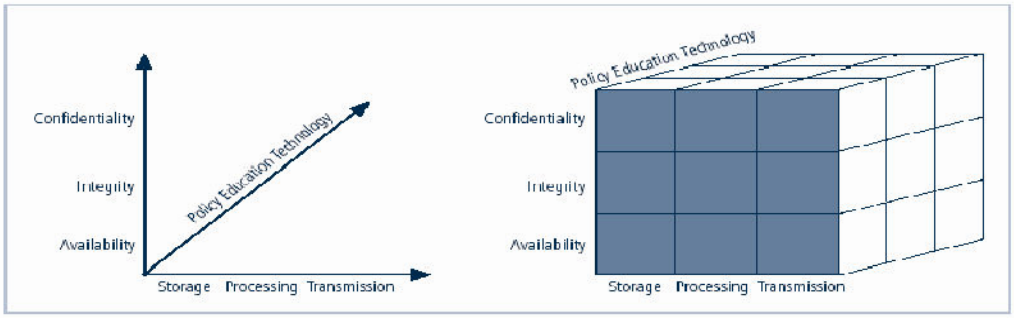

FIGURE 1-4 NSTISSC Security Model

8. List out the security services.. **(Remember)**

Three security services:

Confidentiality, integrity, and availability

Threats are divided into four broad classes:

- Disclosure, or unauthorized access to information
- Deception, or acceptance of false data
- Disruption, or interruption or prevention of correct operation
- Usurpation or unauthorized control of some part of a system.

9. Define the snooping and spoofing. **(Remember)**

Snooping: The unauthorized interception of information is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information.

Masquerading or spoofing: An impersonation of one entity by another is a form of both deception and usurpation.

10. List the components used in security models. **(Remember)**

- Software
- Hardware
- Data
- People
- Procedures

- Networks

11. What are the functions of Information Security? (Remember)

- Protects the organization's ability to function
- Enables the safe operation of applications implemented on the organizations IT systems
- Protects the data the organization collects and uses
- Safeguards the technology assets in use at the organization

12. What are the phases of SDLC Waterfall method? (Remember)

- Investigation
- Analysis
- Logical Design
- Physical Design
- Implementation
- Maintenance & change

13. What is Rand Report R-609? (Remember)

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:

- Safety of the data
- Limiting unauthorized access to that data
- Involvement of personnel from multiple levels of the organization

14. What is meant by balancing Security and Access? (Remember)

- 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

PART – B

1. Describe the Critical Characteristics of Information. **(Nov/Dec 2021) (Understand)**
2. Explain the Components of an Information System. **(May/Jun 2021) (Understand)**
3.

4. Discuss SDLC in detail. **(May/June 2020)** **(Understand)**
5. Describe SecSDLC in detail. **(Understand)**
6. Explain the NSTISSC security model and the top down approach to security implementation. **(Nov/Dec 2022)** **(Understand)**
7. Describe the NSTISSC security model and the bottom up approach to security implementation. **(Understand)**

PART – C

1. Explain any five professionals in information security with their role and focus. **(Understand)**

UNIT – II

PART – A (2 Marks)

1. Why is information security a management problem? (Remember)

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

2. Distinguish between DoS and DDoS. (Understand)

DoS	DDoS
Denial of service attack -The attacker sends a large number of connection or information requests to a target.	Distributed Denial of service is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

3.What is intellectual property? (Remember)

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

4.What is a policy? How it differs from law? (Remember)

- Policies: A body of expectations that describe acceptable and unacceptable employee behaviors in the workplace.
- It functions as organizational laws, complete with penalties, judicial practices, and sanctions to require complaints.
- The difference between policy and a law, however, is that ignorance of a policy is an acceptable defense.

5. What are the general categories of unethical and illegal behavior? (Remember)

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

- Ignorance
- Accident
- Intent

6.What are the various types of malware? How do worms differ from Virus? (Remember)

- Viruses
- Worms
- Trojan horses
- Active web scripts

Virus	Worm
A virus attaches itself to s a computer program and spreads from one computer to another.	A worm is similar to virus by design. It also spreads from one computer to another.
Spreads with uniform speed as programmed.	Worms spread more rapidly than virus.
It can be attached to .EXE, .COM , .XLS etc	It can be attached to any attachments of email or any file on network.
Ex Melisca, cascade etc	Ex Blaster Worm
It requires the spreading of an infected host file.	It replicates them without the host file.

7. Who are hackers? What are the levels of hackers? (Remember)

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

2. **What is security blue print? (Remember)**

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.

3. **What are the types of virus? (Remember)**

a. Macro virus
b. Boot virus

4. **Distinguish between attack and threat. (Remember)**

Attack	Threat
An act which is in process.	A promise of an attack to come.
An attack is intentional.	Threat can be either intentional or unintentional.
Attack to information might have a chance to alter or damage the information when it is successful.	Threat to information does not mean that it is damaged or changed

5. **Define Information Extortion (Remember)**

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

6. **Define Hoax.** **(Remember)**

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) (Understand)**
2. Describe about various forms of attacks. **(Understand)**
3. Explain the different categories of threat. Give Examples. **(Understand)**
4. Write about the attack replication vectors in detail. **(Understand)**
5. Discuss the ethical concepts in information security. **(Understand)**

PART – C

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

UNIT – III
PART – A (2 Marks)

1. In risk management strategies why does a periodic review have to be a part of process? (May/June 2012 May/June 2013) (Remember)

- The first focus is asset inventory
- The completeness and accuracy of the asset inventory has to be verified
- The threats and vulnerabilities that are dangerous to asset inventory must be verified

2. What is asset valuation? List any 2 components of asset valuation. (May/June 2022) (Remember)

A method of assessing the worth of a company, real property, security, antique or other item of worth. Asset valuation is commonly performed prior to the sale of an asset or prior to purchasing insurance for an asset.

- 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?

3. Define dumpster driving. (May/June 2021) (Remember)

To retrieve information that could embarrass a company or compromise information security.

4. What is risk management? (Nov/Dec 2012) (Remember)

Risk management is the process of identifying vulnerabilities in an organization's information systems and taking carefully reasoned steps to assure Confidentiality, Integrity, and Availability.

5. Define benchmarking. (Remember)

Benchmarking is a process of seeking out and studying the practices used in other organizations that produce results you would like to duplicate in your organization.

6. What are the different types of Access Controls? (Remember)

- Discretionary Access Controls (DAC)
- Mandatory Access Controls (MACs)
- Nondiscretionary Controls
- Role-Based Controls
- Task-Based Controls
- Lattice-based Control

7. Define Disaster Recovery Plan. **(Remember)**

The most common mitigation procedure is Disaster Recovery Plan (DRP). The DRP includes the entire spectrum of activities used to recover from the incident and strategies to limit losses before and after the disaster. DRP usually include all preparations for the recovery process, strategies to limit losses during the disaster.

8. What is residual risk? **(Remember)**

Exposure to loss remaining after other known risks have been countered, factored in, or eliminated. It is simply seen as the risk that remains after safeguards have been implemented.

9. Mention the Risk Identification Estimate Factors. **(Remember)**

- Likelihood
- Value of Information Assets
- Percent of Risk Mitigated
- Uncertainty

10. What is the formula for calculating risk? **(Remember)**

Risk = Threat x Vulnerability x Cost

Risk Assessment = ((Likelihood + Impact + Current Impact)/3) * 2 - 1

PART – B

1. Explain in detail the process of asset identification for different categories. **(Understand)**
2. What are risk control strategies?(Nov/Dec 2021) **(Understand)**
3. Explain the process of Risk assessment. (Nov/Dec 2022) **(Understand)**
4. Write short notes on **(Understand)**
   a) Incidence Response Plan
   b) Disaster Recovery Plan
5. Explain the process of vulnerability identification and assessment for different threats faced by an information security system. **(Understand)**

PART – C

1. Discuss briefly data classification and management. **(Create)**
2. Explain the risk control cycle process. **(Understand)**

UNIT – IV
PART – A (2 Marks)

1. What measurement do you use when preparing a potential damage assessment?

(Remember)

Identify what must be done to recover from each possible case. The costs include the actions of the response team(s) as they act to recover quickly and effectively from an incident or disaster**.**

2. Define policy and standards. Remember)

A policy is a plan or course of action, as of a government, political party, or business, intended to influence and determine decisions, actions, and other matters. Standards, on the other hand, are more detailed statements of what must be done to comply with policy.

3. What is the difference between the management, technical and operational control? When would each be applied as a part of a security framework? (Understand)

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

4. Give any 5 major sections of ISO/IEC 17799 standards. (Remember)

- Organizational Security Policy
- Organizational Security Infrastructure
- Asset Classification and Control
- Personnel Security
- Compliance

5. What are the three types of security policies? (Remember)

- General or security program policy
- Issue-specific security policies
- Systems-specific security policies

6. Mention the Drawbacks of ISO 17799/BS 7799. (Remember)

- 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

7. What is Defense in Depth? (Remember)

One of the foundations of security architectures is the requirement to implement security in layers .Defense in depth requires that the organization establish sufficient security controls and safeguards, so that an intruder faces multiple layers of controls.

8. What is contingency planning? (Remember)

It is the entire planning conducted by the organization to prepare for, react to, and recover from events that threaten the security of information and information assets in theorganization.

9. What are the approaches of ISSP? (Remember)

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

10. What is Sphere of protection? (Remember)

- The "sphere of protection" overlays each of the levels of the "sphere of use" with a layer of security, protecting that layer from direct or indirect use through the next layer
- The people 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)
  - ✓ Technology

11. What is Security perimeter? (Remember)

The point at which an organization's security protection ends, and the outside world begins is referred to as the security perimeter.

12. Mention the Operational Controls of NIST SP 800-26. (Remember)

- 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 .

13. What is Information Security Blueprint? (Remember)

The Security Blue Print is the basis for Design, Selection and Implementation of Security Policies, education and training programs, and technology controls.

14. What are ACL Policies? (Remember)

- Who can use the system?
- What authorized users can access?
- When authorized users can access the system?
- Where authorized users can access the system from?
- How authorized users can access the system?

15. Define Issue-Specific Security Policy (ISSP). (Remember)

- It addresses specific areas of technology
- It requires frequent updates
- contains an issue statement on the organization's position on an issues

16. What is Security Program Policy? (Remember)

- A general security policy
- IT security policy
- Information security policy

PART – B

1. Describe NIST SP 800-26. **(Understand)**
2. Explain the design of security architecture in detail. **(May/June 2013)** **(Understand)**
3. Discuss the types of information security policies in detail. **(Understand)**
4. Explain NIST security model in detail. **(Understand)**
5. Discuss VISA International security models in detail**.(Nov/Dec 2012)** **(Understand)**

PART – C

1. Describe the major steps in contingency planning. **(Understand)**

UNIT – V
PART – A (2 Marks)

1. Distinguish between symmetric and asymmetric encryption. (Nov/Dec 2020) (Remember)

Symmetric	Asymmetric
Uses the same secret (private) key to encrypt and decrypt its data	Uses both a public and private key.
Requires that the secret key be known by the party encrypting the data and the party decrypting the data.	Asymmetric allows for distribution of your public key to anyone with which they can encrypt the data they want to send securely and then it can only be decoded by the person having the private key.
Fast	1000 times slower than symmetric

2. What is content filter? (May/June 2022) (Remember)

A content filter is software filter-technically not a firewall-that allows administrators to restrict access to content from within a network.

3. List all physical security controls. (May/June 2013) (Remember)

- guards
- dogs
- lock and keys
- electronic monitoring
- ID cards and badges
- man traps
- alarms and alarm systems

4. What are the seven major sources of physical loss? (Remember)

- Temperature extremes
- Gases
- Liquids
- Living organisms
- Projectiles
- Movement
- Energy anomalies

5. What are the advantages and disadvantages of using honey pot or padded cellapproach? (Remember)

Advantages:

- Attackers can be diverted to targets that they cannot damage
- Administrators have time to decide how to respond to an attacker
- Attackers action can be easily and extensively monitored
- Honey pots may be effective at catching insiders who are snooping around a network

Disadvantages:

- The legal implications of using such devices are not well defined
- Honey pots and Padded cells have not yet been shown to be generally useful security technologies
- An expert attacker, once diverted into a decoy system, may become angry and launch a hostile attack against an organization's systems
- Security managers will need a high level of expertise to use these systems

6. Define encryption and decryption. (Remember)

Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is, to anyone without the tools to convert the encrypted message back to its original format.

Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

6. **What are different types of IDSs? (Remember)**

- Network-based IDS
- Host-based IDS
- Application-based IDS
- Signature-based IDS
- Statistical Anomaly-Based IDS

8. What are firewalls? (Remember)

A firewall is any device that prevents a specific type of information from moving between the un-trusted network outside and the trusted network inside. The firewall may be:

- a separate computer system

- a service running on an existing router or server
- a separate network containing a number of supporting devices

9. What is Application-based IDS? (Remember)

A refinement of Host-based IDs is the application-based IDS (AppIDS). The application based IDs examines an application for abnormal incidents. It looks for anomalous occurrences such as users exceeding their authorization, invalid file executions etc.

10.What are Digital signatures? (Remember)

- An interesting thing happens when the asymmetric process is reversed, that is the private key is used to encrypt a short message
- The public key can be used to decrypt it, and the fact that the message was sent by the organization that owns the private key cannot be reputed
- 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

11.What are dual homed host firewalls? (Remember)

- The bastion-host contains two NICs (network interface cards)
- One NIC is connected to the external network, and one is connected to the internal network
- With two NICs all traffic must physically go through the firewall to move between the internal and external networks
- A technology known as network-address translation (NAT) is commonly implemented with this architecture to map from real, valid, external IP addresses to ranges of internal IP addresses that are non-routable

12.How firewalls are categorized by processing mode? (Remember)

c. Packet filtering
d. Application gateways
e. Circuit gateways
f. MAC layer firewalls
g. Hybrids

13.What is Cryptanalysis? (Remember)

Cryptanalysis is the process of obtaining the original message (called plaintext) from an encrypted message (called the cipher text) without knowing the algorithms and keys used to perform the encryption.

14.What is Public Key Infrastructure (PKI)? (Remember)

Public Key Infrastructure is the entire set of hardware, software, and cryptosystems necessary to implement public key encryption.

PKI systems are based on public-key cryptosystems and include digital certificates and certificate authorities (CAs) and can:

- Issue digital certificates
- Issue crypto keys

PART – B

1. Write about the different generations of firewalls. **(Understand)**
2. Explain briefly the basic Encryption definitions. **(Understand)**
3. Explain about RSA algorithm. **(Understand)**
4. What are the different types of intrusion detection systems (IDS)? Explain Ids. **(Understand)**
5. What are the recommended practices in designing firewalls? **(Understand)**

PART – C

1. Discuss the different types of Scanning and Analysis tools available. **(Create)**
2. What is Cryptography? Explain the key terms associated with cryptography. **(Understand)**