

**COURSE TITLE** : **INFORMATION SECURITY**  
**COURSE CODE** : **5059/4079**  
**COURSE CATEGORY** : **E**  
**PERIODS/WEEK** : **4**  
**PERIODS/SEMESTER** : **72**  
**CREDITS** : **4**

**TIME SCHEDULE**

<b>MODULE</b>	<b>TOPICS</b>	<b>PERIODS</b>
1	Introduction to computer Security & Cryptography	18
2	User Authentication and Access Control	18
3	Intrusion Detection & Malicious Software	18
4	Denial of Service and Firewall	18
	<b>Total</b>	<b>72</b>

**OBJECTIVES**

**MODULE I Introduction to computer Security & Cryptography**

**1.1 Introduction to Computer Security**

- 1.1.1 Define the term computer Security as per NIST Computer Security hand book
- 1.1.2 Explain Computer Security triad: Confidentiality, Integrity, Availability
- 1.1.3 Explain the terminologies: Authenticity, accountability
- 1.1.4 Study computer system resources : Hardware, software, data and communication facilities
- 1.1.5 Study Computer system vulnerabilities :corrupted/leaky/unavailable
- 1.1.6 Explain various threat consequences and threat actions
- 1.1.7 List security functional requirements as per (FIPS PUB 200)
- 1.1.8 Explain OSI Security architecture ans X.800 specifications
- 1.1.9 List Computer and Network security incident taxonomy
- 1.1.10 Explain a strategy for providing computer security: Security policy, security implementation and assurance& evaluation]

**1.2 Cryptographic tools**

- 1.2.1 Study Symmetric encryption with block diagram
- 1.2.3 Explain Symmetric block encryption algorithms
- 1.2.3 Study stream ciphers
- 1.2.4 Explain message authentication with symmetric encryption
- 1.2.5 Describe message authentication without message encryption
- 1.2.6 Describe message authentication with message authentication code(MAC)
- 1.2.7 Describe message authentication with one way and secure hash functions
- 1.2.8 Study Public key encryption structure.
- 1.2.9. Study digital signature, public key certificates and Symmetric key exchange using public key encryption
- 1.2.10 Explain the use of Random numbers in encryption
- 1.2.11 Differentiate random and pseudorandom numbers
- 1.2.12 Explain the encryption of stored data

## **MODULE II User Authentication and Access Control**

- 2.1.1 Define User Authentication
- 2.1.2 Explain the means of authentication
- 2.1.3 Understand Password based Authentication
- 2.1.4 Understand the vulnerability of passwords, Explain the use of hashed passwords
- 2.1.5 Explain the password cracking approaches and user password choices
- 2.1.6 understand password File access control
- 2.1.7 explain the password selection strategies
- 2.1.8 understand the proactive password checking
  
- 2.2 Understand Token based authentication
- 2.2.2 explain the use of memory cards
- 2.2.3 explain the use of smart cards
- 2.2.4 Understand Biometric Authentication
- 2.2.5 Explain various physical characteristics used in biometric applications
- 2.2.6 Explain the operation of a biometric authentication system
- 2.2.7 Understand the biometric accuracy
- 2.3 Understand Remote User Authentication
- 2.3.1 Explain the basic idea of a challenge-response for a password, token, static biometric , and dynamic biometric protocols
- 2.4 Explain various security issues for user authentication
- 2.4.1 Define the term Access control in computer security
- 2.4.2 Explain the relationship among Access Control and other security functions like Authentication, Authorization and Audit
- 2.4.3 understand various access control policies
- 2.4.4 Understand various access control requirements
- 2.4.5 Explain the various basic elements of Access control: subject, object and Access right
- 2.4.6 Explain Discretionary Access Control
- 2.5 Study the Unix File Access Control
- 2.6 Explain the Role based Access Control (RBAC) with an example

## **MODULE III: INTRUSION DETECTION & MALICIOUS SOFTWARES**

- 3.1.1 Study the class of intruders and the intruder behaviours patterns.
- 3.1.2 Explain the principles of Intrusion Detection System and their requirements
- 3.1.3 Explain Host based Intrusion detection
- 3.1.4 study the relevance of audit records, anomaly detection, and signature detection
- 3.1.5 Explain Distributed host based intrusion detection
- 3.1.6 Study Network based intrusion detection
- 3.1.7 Explain Distributed Adaptive Intrusion detection
- 3.1.8 understand Intrusion Detection Exchange Format
- 3.1.9 Explain the functioning of Honey pots
- 3.1.10 Study the functioning of SNORT IDS
- 3.1.11 Explain various types of Malicious Software
- 3.1.12 Study Viruses
- 3.1.13 Explain various Virus counter measures
- 3.1.14 Study Worms
- 3.1.15 Study BOTs
- 3.1.16 Explain the functions of a ROOTKIT

## **UNIT 4 DENIAL OF SERVICE AND FIREWALL**

- 4.1 Define a Denial of Service
- 4.2 Study effect of DoS on Network bandwidth, System resources and Application resources
- 4.3 Explain classic Denial of Service Attacks
- 4.4 Understand Source Address Spoofing
- 4.5 Study the SYN Spoofing
- 4.6 Explain Flooding Attacks- ICMP Flood, UDP Flood, TCP SYN Flood
- 4.7 Study the Distributed Denial of Service Attacks, and DDoS attack architecture
- 4.8 Study the Reflector and Amplifier attacks
- 4.9 Explain defences against , and how to respond to DoS Attacks
  
- 4.10 List the need for firewall
- 4.11 List various characteristics of a Firewall
- 4.12 Study various types of firewalls: Packet filtering, Stateful inspection, Application proxy and Circuit level proxy
- 4.13 Understand Bastion Host, Host based firewalls and Personal firewalls
- 4.14 Study Firewall Location and configurations
- 4.15 Explain various Intrusion Prevention Systems- Host based, Network based, SNORT inline
- 4.16 Explain a Unified Threat Management Appliance Architecture

## **CONTENT DETAILS**

### **MODULE I Introduction to Computer Security**

Introduction to Computer Security-Definition of computer security- Computer security triad- confidentiality- integrity- availability – threats- attacks-assets-security functional requirements- security architecture for open systems – x 800 - - computer and Network security incident taxonomy- computer security strategy for providing computer security- security implementation- security assurance& evaluation

Define Cryptography - Symmetric encryption with block diagram - Symmetric block encryption algorithms- stream ciphers- message authentication with symmetric encryption - message authentication without message encryption- message authentication code(MAC) – one way hash functions- secure hash functions - Public key encryption structure - digital signature - public key certificates - Symmetric key exchange using public key encryption- Random numbers in encryption- pseudorandom numbers- encryption of stored data

### **MODULE II User Authentication and Access Control**

Define User Authentication -means of authentication- Password based Authentication - vulnerability of passwords- hashed passwords- password cracking approaches and user password choices - password File access control - password selection strategies - proactive password checking - Token based authentication - memory cards- smart cards - Biometric Authentication - various physical characteristics used in biometric applications - operation of a biometric authentication system - biometric accuracy- Remote User Authentication - challenge-response for a password, token, static biometric , and dynamic biometric protocols - security issues for user authentication – Definition of Access control in computer security - relationship among Access Control and other security functions like Authentication, Authorization and

Audit -understand various access control policies - various access control requirements - various basic elements of Access control: subject, object and Access right - Discretionary Access Control - Unix File Access Control - Role based Access Control (RBAC) with an example

### **MODULE III Intrusion Detection & Malicious Software**

Class of intruders and the intruder behaviours patterns - principles of Intrusion Detection System and their requirements - Host based Intrusion detection - relevance of audit records, anomaly detection, and signature detection - Distributed host based intrusion detection- Network based intrusion detection- Distributed Adaptive Intrusion detection - Intrusion Detection Exchange Format – Honey pots - SNORT IDS Various types of Malicious Software – Viruses - various Virus counter measures – Worms- BOTs - ROOTKIT

### **MODULE IV Denial of Service and Firewall**

Define a Denial of Service - effect of DoS on Network bandwidth, System resources and Application resources - classic Denial of Service Attacks -Source Address Spoofing -SYN Spoofing- Flooding Attacks- ICMP Flood- UDP Flood - TCP SYN Flood- Distributed Denial of Service Attacks- DoS attack architecture- Reflector and Amplifier attacks -defences against DoS – responding to DoS Attacks

Need for firewall- characteristics of a Firewall- types of firewalls - Packet filtering - Stateful inspection- Application proxy - Circuit level proxy - Bastion Host - Host based firewalls- Personal firewalls- Firewall Location and configurations - various Intrusion Prevention Systems- Host based IPS- Network based IPS- SNORT inline - Unified Threat Management Appliance Architecture

### **TEXT BOOK:**

1. Computer Security- Principles and Practice  
Author: William Stallings & Lawrie Brown  
Publisher: Pearson Prentice Hall

### **REFERENCE BOOKS:**

1. Cryptography and Security  
Author: C K Chyamala, N Harini & Dr T R Padmanabhan  
Publisher: Wiley – India