IT 244: Information Security

(BIM 5th Sem)

Credits: 3
Lecture Hours: 48

Course Objectives:

The objective of this course is to familiarize the students with the theoretical and practical concepts of information security, different security measures, policies and security mechanisms, security audits so that students will be able to design, implement and manage the secure computer system.

Course Description:

This course introduces the basic concepts of computer and information security. This course prepares the students to meet the new challenges in the world of increasing threats to computer security by providing them with an understanding of the various threats and countermeasures. This course includes cryptographic algorithms, authentication systems, intrusion detection and prevention, malicious logics, network security and security audits.

Course Details

Unit 1: Introduction 5 LHs

Computer Security Concepts, Threats, Attacks and Assets, Security Functional Requirements, Security Design Principles, Attack Surfaces and Attack Trees, Computer Security Strategy, Access Control Principles, Subjects, Objects and Access Rights, Discretionary Access Control, Role Based Access Control, Attribute Based Access Control, Identity, Credential and Access Management, Trust Frameworks, Overview of the Bell-LaPadula Model and Biba integrity model.

Unit 2: Symmetric and Asymmetric Cryptographic Algorithms 13 LHs

Classical Cryptosystems: Substitution and Transposition Ciphers, Block Cipher Vs Stream Ciphers, Symmetric Encryption Principles, Fiestel Cipher Structure, Data Encryption Standards (DES), Basic concepts of fields, Modular Arithmetic, Galois Fields, Polynomial Arithmetic, Advanced Encryption Standards (AES), Prime Numbers, Fermat's Theorem, Primality Testing: Miller-Rabin Algorithm, Euclidean Algorithm, Extended Euclidean Algorithm, Euler Totient Function, Asymmetric Encryption, Diffie-Hellman Protocol, RSA Algorithm

Unit 3: Message Authentication and Hash Functions 6 LHs

Message Authentication, Hash Functions, Message Digests: MD4 and MD5, Secure Hash Algorithms: SHA-1, SHA-2, Hash Based MAC (HMAC), Digital Signature

Unit 4: User Authentication 5 LHs

User Authentication Principles, Password-Based Authentication, Token-Based Authentication, Biometric Authentication, Two Factor Authentication, Kerberos Protocol, Kerberos 5, Security Issues for User Authentication.

Unit 5: Intrusion Detection and Prevention 5 LHs

Intruders, Intrusion Detection, Intrusion Detection Analysis Approaches, Host-Based Intrusion Detection, Network-Based Intrusion Detection, Hybrid Intrusion Detection, Intrusion Detection Exchange Format, Honeypots, Intrusion Prevention System

Unit 6: Malicious Software 4 LHs

Malicious Software, Types of Malicious Software, Advanced Persistent Threat, Virus, Worms, Spam E-mail, Trojans, System Corruption, Zombie, Bots, Key loggers, Phishing, Spyware, Backdoors, Rootkits, Countermeasures for Malwares

Unit 7: Network Security 5 LHs

Overview of Network Security, Digital Certificates and X.509 certificates, Certificate Life Cycle Management, PKI trust models, PKIX, Secure Socket Layer (SSL), Transport Layer Security (TLS), IP Security, Email Security, PGP and its Services, Firewalls its applications and types, VPN.

Unit 8: IT Security Management, Risk Assessment and Security Auditing 5 LHs

IT Security Management, Organizational Context and Security Policy, Security Risk Assessment, Security Risk Analysis, Security Auditing Architecture, Security Audit Trails, Implementing Logging Function, Audit Trail Analysis

Laboratory work

The laboratory work covers implementing programs for following; - Classical ciphers like Caeser, Railfence - DES, AES - Primality Testing, Euclidean Algorithms, Deffie-Hellman RSA - MD5, SHA-1, SHA-2 - Authentication systems like password based, token based, two factor authentication etc.

Suggested Readings:

William Stallings, cryptography and network security principles and practice eighth edition, 2023, Pearson

William Stallings and Lawrie Brown, Computer Security: Principles and Practice, fifth edition, Pearson

Mark Stamp, Information Security: Principles and Practices, Wiley

Matt Bishop, Introduction to Computer Security, Addison Wesley

Matt Bishop, Computer Security, Art and Science, Addison Wesley