Course Title: Information Security (3 Cr.)
Course Code: CACS459
Year/Semester:
Class Load: 6 Hrs. / Week (Theory: 3Hrs. Practical: 3 Hrs.)

Course Description: The course introduces the theoretical as well as practical concepts of computer and information security. The course includes concepts of cryptographic algorithms, authentication systems, access controls, malicious logics, network security and security audits.

Course Objectives: The objectives of this course are to familiarize the students with the computer security concepts, security policies and security mechanisms so that students will be able to design, implement and manage the secure computer systems.

Course Contents:

Unit I: Overview of Computer security (4 Hrs)

1.1. Computer Security Concepts
1.2. Computer Security, Information Security, Network Security
1.3. Threats, Attacks and Assets
1.4. Security Requirements
1.5. Security Design Principles
1.6. Attack Surfaces and Attack Trees
1.7. Computer Security Strategy

Unit II: Cryptographic Algorithms (12 Hrs)

2.1. Classical Cryptosystems: Ceasar, Vignere, Playfair, Rail Fence Ciphers
2.2. Modern Ciphers: Block vs. Stream Ciphers, Symmetric vs. Asymmetric Ciphers
2.3. Symmetric Encryption: Fiestel Cipher Structure, Data Encryption Standards (DES), Basic Concepts of Fields: Groups, Rings, Fields, Modular Arithmetic, Galois Fields, Polynomial Arithmetic, Advanced Encryption Standards (AES)
2.4. Number Theory: Prime Numbers, Fermat's Theorem, Primility Testing: Miller-Rabin Algorithm, Euclidean Theorem, Extended Euclidean Theorem, Euler Totient Function
2.5. Asymmetric Encryption: Diffie-Helman Key Exchange, RSA Algorithm

Unit III: Message Authentication and Hash Functions (6 Hrs)

3.1. Message Authentication
3.2. Hash Functions
3.3. Message Digests: MD4 and MD5
3.4. Secure Hash Algorithms: SHA-1
3.5. HMAC
3.6. Digital Signatures

Unit IV: User Authentication (5 Hrs)

4.1. User Authentication Principles
4.2. Password-Based Authentication
4.3. Token-Based Authentication
4.4. Biometric Authentication
4.5. Remote User Authentication
4.6. Two Factor Authentication

Unit V: Access Control (5 Hrs)

5.1. Access Control Principles
5.2. Subjects, Objects and Access Rights
5.3. Access Control Matrix and Capability Lists
5.4. Discretionary Access Control
5.5. Role Based Access Control
5.6. Attribute Based Access Control
5.7. Identity, Credential and Access Management
5.8. Trust Frameworks

Unit VI: Malicious Software and Intrusion (4 Hrs)

6.1. Malicious Software
6.2. Virus and its phases, Virus Classification
6.3. Worm, Worm Propagation Model, State of Worm Technology
6.4. Trojan Horse
6.5. Intrusion and Intruders
6.6. Intrusion Detection System
6.7. Analysis Approaches: Anomaly Based, Signature Based
6.8. Honeypots

Unit VII: Network Security (5 Hrs)

7.1. Overview of Network Security
7.2. Email Security: S/MIME, Pretty Good Privacy (PGP)
7.3. Secure Socket Layer (SSL) and Transport Layer Security (TLS)
7.4. IP Security (IPSec)
7.5. Firewalls and their types

Unit VIII: Security Auditing (7 Hrs)

8.1. Security Audit
8.2. Security Auditing Architecture
8.3. Security Audit Trail
8.4. Implementing Logging Function
8.5. Audit Trail Analysis

Laboratory Works:

The laboratory work includes implementing and simulating the concepts of cryptographic algorithms, hash functions, digital signatures, authentication & authorization systems, and malicious logics. The laboratory work covers implementing programs for following;

- Classical ciphers like Caeser, Playfair, Railfence
- DES, AES
- Primality Testing, Euclidean Algorithm, RSA
- MD5, SHA
- Authentication systems like password based, Captcha, two factor authentication etc.
- Role Based Access Controls
- Malicious Logics

Teaching Methods

The major teaching methods that can be followed for this course includes class lectures, laboratory activity, group discussions, presentations and case studies. For the laboratory work, the instructor can choose any programming language based on comfort level of students.

Evaluation

Examination Scheme				
Internal Assessment		External Assessment		Total
Theory	Practical	Theory	Practical	
20	20 (3 Hrs.)	60 (3 Hrs.)	-	

Text Book:

4. William Stallings and Lawrie Brown, Computer Security: Principles and Practice, Pearson
5. William Stallings, Cryptography and Network Security: Principles and Practice, Pearson.

Reference Books:

1. Mark Stamp, Information Security: Principles and Practices, Wiley
2. Matt Bishop, Introduction to Computer Security, Addison Wesley
3. Matt Bishop, Computer Security, Art and Science, Addison Wesley
4. Charles P. Pfleeger and Shari Lawrence Pfleeger, Security in Computing, Pearson