CSPE3012 INFORMATION SECURITY AND MANAGEMENT (3-0-0)

Course Objectives:

- To introduce fundamental concepts and objectives of information security.
- To provide in-depth understanding of cryptographic algorithms and secure communication protocols.
- To explore secure programming techniques and operating system-level protection.
- To study database and network security measures.
- To understand administrative and legal aspects of information security.

Module – I (08 Hours)

Introduction to Information Security

Overview of Information Security-Importance and objectives, Key principles: Confidentiality, Integrity, Availability (CIA Triad), Security Threats and Attacks- Types: Interruption, Interception, Modification, Fabrication, Examples: Malware, Phishing, Denial-of-Service(DoS), Security Services and Mechanisms- Authentication, Access Control, Non-repudiation, Security models and architectures, Network Security Fundamentals- Firewalls, Intrusion Detection Systems (IDS), Virtual Private Networks (VPNs).

Module – II (08 Hours)

Cryptography And Network Security

Cryptography Basics- Classical techniques: Substitution and Transposition ciphers, Modern encryption: DES, AES, RSA, Advanced Cryptographic Techniques- Public Key Infrastructure (PKI), Digital Signatures and Certificates, Secure Communication Protocols- SSL/TLS for secure web communication, IPsec for secure IP communications, Authentication Protocols- Kerberos, OAuth, SAML

Module – III (08 Hours)

Program Security

Secure Programs, Non-malicious Program Errors, viruses and other malicious code, Targeted Malicious code, controls Against Program Threats, Protection in General- Purpose operating system protected objects and methods of protection memory, File protection Mechanisms, User Authentication Designing Trusted O.S: Security polices, models of security, trusted O.S design, Assurance in trusted O.S. Implementation examples

Module – IV (08 Hours)

Database Security

Security requirements, Reliability and integrity, Sensitive data, Inference, multilevel database, proposals for multilevel security. Security in Network: Threats in Network, Network Security Controls, Firewalls, Intrusion Detection Systems, Secure E-Mail.

Module – V (08 Hours)

Administering Security

Security Planning, Risk Analysis, Organizational Security policies, Physical Security. Legal Privacy and Ethical Issues in Computer Security: Protecting Programs and data, Information and the law, Rights of Employees and Employers, Software failures, Computer Crime, Ethical issues in Computer Security, case studies of Ethics.

Course Outcomes:

After the completion of the course, students should be able to:

- Understand and explain the risks faced by computer systems and networks.
- Identify and analyze security problems in computer systems and networks.
- Explain how standard security mechanisms work.
- Develop security mechanisms to protect computer systems and networks.
- Use cryptography algorithms and protocols to achieve computer security.

Text Books:

1. Security in Computing, Fourth Edition, by Charles P. Pfleeger, Pearson Education.
2. Daniel Minoli, Information Technology Risk Management in Enterprise Environments, Wiley, 2009.

Reference Books:

1. Andy Jones, Debi Ashenden, Risk Management for Computer Security: Protecting Your Network & Information Assets, 1st Edition, Butterworth-heinemann, Elsevier, 2005.
2. Cryptography And Network Security Principles and Practice, Fourth or Fifth Edition, William Stallings, Pearson.

Web links & Video Lectures (E-Resources):

1. https://archive.nptel.ac.in/courses/106/106/106106129/