Network and Information Security

L T P C
3 0 0 3

Objectives

At the end of the course students should have

- learnt protection of data transferred over computer networks and devising practical solutions to network security requirements.
- gained a sound knowledge in multi-level security for data and databases

Unit I **INTRODUCTION** [9]

Attacks, Services & Mechanisms: Security attacks – Security services – Network Security Model. Steganography – Classical and Modern Encryption Techniques - Symmetric Key Cryptography: The Data Encryption Standard - The Strength of DES – Differential and Linear, Crypto-analysis, IDEA, Blowfish, Elementary concepts & theorems in Number theory

Unit II **CRYPTOGRAPHY AND AUTHENTICATION** [9]

Principles of public - key cryptosystems – The RSA algorithm - Key management – Diffie - Hellman key exchange – Elliptic curve cryptography. Authentication requirements – Authentication functions – Hash functions – Security of hash functions and MAC. Hash Algorithm: MD5– SHA-1 – HMAC. Digital Signatures and Authentication Protocols

Unit III **LAYERED SECURITY AND TOOLS AND TECHNIQUES** [9]

Layers: Security Issues, Protocols-Authentication service: Kerberos - E-Mail Security: PGP - IP Security: Overview – Architecture – Authentication header – Web Security: TLS, SSL – Wireless Security

Password protection – Access control – Password selection strategies -Different approaches of Intrusion detection - Audit records Viruses and related Threats – Firewalls: Design principles – Characteristics – Types and Configurations

Unit **IV PROGRAM SECURITY** [9]

Secure programs, Non-malicious program errors, types of malicious software, viruses and counter measures, Bots, Root kits , Targeted malicious code, Controls against program threats, software security issues.

Unit V **DATA AND DATABASE SECURITY** [9]

Relational databases, Security requirements, Reliability and Integrity, Sensitive data, Inference, Multilevel secure databases, concurrency control and multilevel security

Textbooks

1. William Stallings, “Cryptography and Network Security – Principles and Practice", 4th edition, Pearson Education, 2000
2. Charles P. Pfleeger, “Security in Computing”, 4th Edition, Pearson, 2006

Reference Books

1. Charlie Kaufman, et al, “Network Security”, 2nd Edition, PHI, 2002
2. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw-Hill, 2007
3. Roberta Bragg, et al, “Network Security: The Complete Reference”, Tata McGraw Hill, 2004
4. Jon Viega, et al, “Network Security with Open SSL” , O’Reilly, 2008
5. Jie Weng , “Computer Network Security”, Higher Education Press, Springer, 2005