4/4 B.Tech. SEVENTH SEMESTER

EM7T6 INFORMATION SECURITY Credits: 4

Lecture: 4 periods/week Internal assessment: 30 marks
Tutorial: 1 period /week Semester end examination: 70 marks

Objectives:
The main objective of this course is to provide students with an overall understanding of the main concepts of information systems, and to highlight the importance of information systems in modern organizations and societies.

Learning Outcomes:

- Fundamental aspects of security in a modern networked environment.
- Basic cryptographic techniques, algorithms and protocols.
- Computational issues in implementing cryptographic protocols and Algorithms

The emphasis is on the applications that are widely used on the Internet and for corporate networks, and on standards especially Internet Standards, that have been widely developed.

UNIT - I
Security Attacks (Interruption, Interception, Modification and Fabrication), Security Services (Confidentiality, Authentication, Integrity, Non-repudiation, access Control and Availability) and Mechanisms, A model for Internetwork security, Internet Standards and RFCs, Buffer overflow & format string vulnerabilities, TCP Session hijacking, ARP attacks, route table modification, UDP hijacking, and man-in-the-middle attacks.

UNIT - II
Conventional Encryption Techniques: Principles, Conventional encryption algorithms, cipher block modes of operation, location of encryption devices, key distribution Approaches of Message Authentication, Secure Hash Functions and HMAC.

UNIT - III
Public Encryption Techniques: Public key cryptography principles, public key cryptography algorithms, digital signatures, digital Certificates, Certificate Authority and key management Kerberos, X.509 Directory Authentication Service.

UNIT - IV
Email privacy: Pretty Good Privacy (PGP) and S/MIME.

UNIT - V
IP Security Overview, IP Security Architecture, Authentication Header, Encapsulating Security Payload, Combining Security Associations and Key Management

UNIT - VI
Web Security: Requirements, Secure Socket Layer (SSL) and Transport Layer Security (TLS), Secure Electronic Transaction (SET).

UNIT - VII

SNMP and Intruders: Basic concepts of SNMP, SNMPv1 Community facility and SNMPv3. Intruders, Viruses and related threats.

UNIT - VIII

Firewalls: Firewall Design principles, Trusted Systems. Intrusion Detection Systems.

Learning resources

Text books:

1. Network Security Essentials (Applications and Standards) by William Stallings Pearson Education.
2. Fundamentals of Network Security by Eric Maiwald (Dreamtech press)

Reference books:

1. Cryptography and network Security, Third edition, Stallings, PHI/Pearson
2. Principles of Information Security, Whitman, Thomson.