AIT 506 INFORMATION SECURITY 3(2+ 1)

Objective

The field of information security has grown and evolved significantly in recent years. Issues like globalization and free trade have made the matter of information security more sensible. In addition to the legislation with respect to information security, pressure coming from industrial piracy, liability,public image and advancement of technology have put a lot of pressure on business to address the information as an asset to be protected. Students are required to understand the principles and techniques of information security to build secure systems.

Theory

UNIT I

Basic concepts of information security; Program security: malware, types of attacks, intrusion detection and prevention, Security policy and security overview

UNIT II

Conventional Encryption Techniques : Introduction, Basic encryption techniques, simplified DES, block cipher mode of operation, traffic confidentiality and key distribution, Random Number Generation.

UNIT III

Public Key Cryptography **:** RSA algorithm, Key management, Elliptic Curve Cryptography, Diffie-Hellman Key Exchange

Message Authentication and Hash Functions **:** Authentication requirement, Functions, Message Authentication Code (MAC), Hash Functions(SHA-1), Digital signature standard DSS).

UNIT IV

Network Security : Authentication Protocols Like Kerberos, X.509 Directory Authentication Services.

UNIT V

IP security E-Mail Security : IP security overview, architecture, authentication header, Encapsulation security payload, S/Mime, Web security, Firewall.

Safe Electronic commerce : Secure transport protocol, secure E-payment protocol, secure electronic transaction.

Practical

1. Write program for Mono alphabetic cipher
2. Implementation of Vigenere cipher (Polyalphabetic substitution)
3. Implementation of Hill cipher
4. Implementation of Rail Fence cipher
5. Implementation of S-DES algorithm for data encryption
6. Implement RSA asymmetric (public key and private key)-Encryption. Encryption key (e, n) & (d, n)
7. Generate digital signature using Hash code
8. Generate digital signature using MAC code
9. examine how PGP works (Pretty Good Privacy)
10. examine how NMAP software works (Network Mapper)

Reference Books :

1. Amoroso, E. 1994. *Fundamentals of Computer Security Technology.* Prentice-Hall.
2. Chapman, B. and Zwicky, Elizabeth D. 2000. *Building Internet Firewalls.* O’Reilly.
3. Charles P. Pfleeger. 2006. *Security in Computing.* Prentice Hall.
4. Easttom William Ii, Chuck Easttom. 2005. *Computer Security Fundamental.* Prentice Hall

5. Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman. 2000. *Building Internet Firewalls.*O'Reilly and Associates.
6. Ford, W. 1994. *Computer Communications Security*. Prentice Hall.
7. Pieprzyk, J. 2008. *Fundamentals of Computer Security*. Springer.
8. Stallings, W. 2004. *Cryptography and Network Security: Principles and Practice.* Prentice Hall.