Systems Security

Purpose and Scope :

The objective of Systems Security course is to systematically introduce the theories, principles and techniques of information systems security. The course covers concepts such as fundamentals of computer security, security mechanisms, operating system security, network security, data base security, security vulnerabilities and secure design principles. After completion of the course, students should be able to explain the basic components of information systems security and the risks faced by computer systems, identify and analyze security problems in information systems, explain how security mechanisms in computer systems work, use cryptography algorithms and protocols to achieve computer system security, design security mechanisms to protect information systems, and implement key security mechanisms like Access Control, Sandbox, SetUID, Encrypted file systems.

Prerequisite: Networks, Operating Systems

Contents:

Module-A : Security Models and Assessment, Security Evaluation, Vulnerability Analysis
Need for security awareness, Definitions, Data Versus Information, Identification and Authentication Essentials, Access Control and Access Control Structures, Security Policies, Security Models and Confidentiality, Organization Security Architecture, Security Audit, Network Audit, Security Policy, Risk Mitigation, Incident Handling, Legal Support, Computer Forensics, Risk Analysis, Vulnerability Analysis, Security Audits and Risk Management, Security Assurance and Evaluation Criteria.

Module-B : Physical Security
Traditional Security, Access Control Systems using Swipe Cards, RFID, Biometrics

Module-C : Operating System and Application Security
PGP, Security Protocols such as IPSec, PKI, Digital Signatures, Web Server Security, Access Control of objects, Authentication, Processes, Files, Users, Buffer Overflow Attacks, Kernel Flaws, Logging, Backups

Module-D : Network Security
TCP/IP Security, Internet Security Procedures, PPP, ECP. TLS EAP, DESE-bis, Firewall, IP Sec Architecture and Protocols, Dial in Operations, RAS PAP, CHAP, RADIUS, DIAMETER, Key distribution, IKE, Certification and Management, Intrusion Detection Systems, VLANs and VPNs, Email security, Network Attacks and DNS protection, DMZ setup, Proxy services etc. Encryption techniques :Cryptography Techniques, RSA, DES, 3DES

Module-E : Databases and Distributed Systems Security
Relational Databases, Statistical Database Security, Multi-level Secure Databases, Concurrency Control and Multi-Level Security, Authentication, Secure APIs, CORBA Security.

LAB Exercises

Configuring safe http and ftp servers, password and user management, hardening of servers (port and service blocking), using pgp and digital signatures, setting up of tripwire like warning mechanisms. Field Trips to Service Installations (Depending on availability and permissions).

References :

1. Hacking Exposed - Linux (Hatch and Lee, Tata McGraw Hill)
2. Practical UNIX and Internet Security - Garfinkel and Spafford, Oreilly
3. Computer Security - Matt Bishop, Pearson Publications, 2003.
4. Internet Security Protocols- Uyless Black, Pearson Publications,2000.
5. Computer Security - Dieter Gollmann, John Wiley and Sons, 1999.
6. Information Security Handbook- Caelli.J, Longley D. and Shain M., MacMillan 1991.
7. Hacking Exposed : Network Security Secrets and Solutions - Macclure S., Scambray J. and Kurtz G., McGraw-Hill, 1999.
8. Security of Computer Networks- Davice and Price, Wiely 1989.
9. Foundations of Security Analysis and Design : Tutorial Lectures - Riccardo Focardi and Roberto Gorrieri, Springer LNCS Series,2001.
10. Information Security Policies, Procedures and Standards – Guidelines for Effective Information Security Management, Thomas R Peltier, Auerbach Publications,2002.
11. Network Security, A PRIVATE Communication in a PUBLIC World – Charlie Kaufman, Radia Perlman et.al, Pentice Hall Series in Computer Networking and Distributed Systems, 1995.
12. Security in Distributed Computing- Glen Bruce and Rob Dempsey, A Pentice Hall Title,1997.
13. Computer and Intrusion Forensics- George Mohay, Alison Anderson et.al., Artech House Publications , 2003.
14. Security in Computing - Charles P.Pfleeger,Shari Lawrence Pfleeger, Pearson Education, 2003.
15. RFCs and other reading material as announced in class from time to time.
16. Latest research papers relevant to the topics.