CS - 554 Network Security **[3 0 0]**

Course Outcomes: At the completion of the course, students will be able to
CO1: Learn and understand various factors driving the need for network security
CO2: Identify and learn about various types of attacks to network
CO3: Analyze various vulnerability, threat, and attacks to network
CO4: Compare and contrast symmetric and asymmetric encryption systems and their vulnerability to attack, and explain the characteristics of hybrid systems.

Course Contents

Introduction to information Security: Types of information security controls and purposes of Information Security Management, Allocation of information security responsibilities.

Telecommunications Security: Objectives, Threats and Countermeasures, Identification of Security threats and development of countermeasures, Technologies and Security policies,

Authentication: Overview of Authentication schemes: Password and address based Authentication, Cryptographic Authentication protocols, Trusted Intermediaries and session key establishment. Security handshake pitfalls: Mutual authentication, Integrity for data, Mediated Authentication and strong password protocols

Public key infrastructure (PKI): PKI trust models, Revocation and Authorization futures.

Security at the Network Layer (IPsec): IPsec Overview, History, and Standards: Overview of IPsec Services and Functions - IPsec Standards. IPsec General Operation, Components, and Protocols: IPsec Core Protocols - IPsec Support Components. IPsec Architectures and Implementation Methods: Integrated Architecture - Bump in the Stack (BITS) Architecture - Bump in the Wire (BITW) Architecture. IPsec Modes: Transport Mode - Tunnel Mode - Comparing Transport and Tunnel Modes. IPsec Security Constructs: Security Policies, Security Associations, and Associated Databases - Selectors - Security Association Triples and Security Parameter Index (SPI). IPsec Authentication Header (AH): AH Datagram Placement and Linking - AH Format. IPsec Encapsulating Security Payload (ESP): ESP Fields - ESP Operations and Field Use - ESP Format. Internet Key Exchange (IKE): Improved Diffie-Hellman Key Exchange – IKE Phases – Phases and Modes – Phase 1: Main Mode, Aggressive Mode – Phase II: Quick Mode – SA Algorithms. ISAKMP: General Header – Payloads.

Security at the Transport Layer (SSL/TLS): SSL Architecture: Services – Key Exchange Algorithms – Encryption/Decryption Algorithms – Hash Algorithms – Cipher Suite – Compression Algorithms – Cryptographic Parameter Generation – Sessions and Connections. Four Protocols: Handshake Protocol – Change Cipher Spec Protocol – Alert Protocol – Record Protocol. SSL Message Formats: Change Cipher Spec Protocol – Alert Protocol – Handshake Protocol – Application Data. TLS: Version – Cipher Suite – Generation of Cryptographic Secrets – Alert Protocol – Handshake Protocol – Record Protocol. SSL versus SET.

Security at the Application Layer: PGP and S/MIME: EMAIL – Email Architecture – Email Security. PGP – Scenarios – Key Rings – PGP Certificates – Key Revocation – Extracting Information from Rings – PGP Packets – PGP Messages – Applications of PGP. S/MIME: MIME-S/MIME – Applications of S/MIME. Time Stamping Protocol. Secure Electronic Transaction (SET): - Introduction – SET Participants – SET Process – SET Internals.

System Security (Linux Firewall): Firewall Design Principles. IPTABLES: Packet filtering with Iptables. Network Layer Attacks and Defense: Logging the IP Header – IP Spoofing – IP Fragmentation – Low TTL values – The Smurf Attack – Route Table Modification – DDoS Attacks – Linux Kernel IGMP Attack – Network Layer Responses. Transport Layer Attacks and Defense: Logging the TCP and UDP Header with Iptables – Port Scans – Port Sweeps – TCP sequence Prediction Attacks – SYN floods – TCP session hijacking -Transport Layer Responses. DNS Attacks. Router Access controls Lists (ACL) - Inbound & outbound traffic – Service and System blocking.

Text / References:

1. Charles M. Kozierok , “The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference”, No starch press, 2005
2. Behrouz A. Forouzan, “Cryptography and Network Security”, Tata McGraw-Hill, 2007
3. Michael Rash,” Linux Firewalls: Attack Detection and Response with IPTABLES, PSAD, and FWSNORT”, No Starch Press, 2007.
4. S. Cimato and C. Galdi, “Security in Communication Networks”, Springer, 2003.
5. Charlie Kaufman and Radia Perlman, “Network Security: Private Communication in a Public World”, Prentice Hall, 2/e, 2002.
6. Rajaraman, “Introduction to Information technology”, Prentice Hall of India, 2/e, 2013.
7. Thomas M. Thomas and Donald Stoddard, “Network Security First Step”, Cisco Press, 2/e, 2012.