CSD-410 INFORMATION SECURITY

Introduction

Standards Organizations, Security Components OSI Security Architecture, Aspects of Security, Passive Attacks, Active Attacks, Security Services (X.800), Security Mechanism, Security Mechanisms (X.800), Services and Mechanisms Relationship, Model for Network Securit, Model for Network Access Security, Symmetric Cipher Model, Cryptography Classification, Cryptanalysis, Substitution: Other forms, Poly-alphabetic Substitution Ciphers, One-Time Pad, Transposition (Permutation) Ciphers, Product Ciphers.

Number Theory and Prime numbers

Groups, Rings, and Fields, Modular Arithmetic, Euclid's Algorithm, Finite Fields of the Form GF(p), Polynomial Arithmetic, Finite Fields of the Form GF(2n). Generation of large prime numbers, Prime factorization, Euler Totient Function ø(n), Euler's Theorem, Primality Test- Fermat's Little Theorem, Baillie-PSW, Solovay-Strassen, Miller Rabin Algorithm, AKS Algorithm, Cyclotomicprimality test, Elliptic Curve Primality Test, Prime Distribution, Chinese Remainder Theorem, Primitive Roots, Discrete Logarithms

Cryptographic Techniques

Perfect security, Feistel Cipher Structure, Block Cipher- DES, differential and Linear Cryptanalysis,Avalanche Effect , Double-DES, Triple-DES, Electronic Codebook Book (ECB), Cipher Block Chaining (CBC), Message Padding, Cipher Text Stealing (CTS), AES, International Data Encryption Algorithm (IDEA), Blowfish Algorithm, RC-x Algorithms, CAST-x Algorithms; Stream Cipher- Stream Modes of Operation-Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR), Storage Encryption, XTS-AES Mode, RC4; Pseudo number generation- Linear-Congruential Generators, Blum BlumShub Generator, Nonlinear Generators, RNGs used in Common Software Packages, Block Ciphers as PRNGs, ANSI X9.17 PRG, Hardware Random number generator, Attacks, Entropy Gathering Daemon (EGD), Intel Digital Random Number Generator (DRNG), RNG in Linux, Windows and iOS7.

Public-Key Cryptography and Message Authentication

The Key Distribution Problem, Public-Key Cryptosystems, The RSA Algorithm, The Key Management riddle, The Diffie-Hellman Key Exchange, Elliptic Curve Cryptography, Message Authentication, requirements and functions, Message Authentication Codes, Hash Functions, Birthday Problem, SHA-X, SHA-512 overview, KECCAK, sponge function, Authentication, Access control policies, The Message Digest (MD5) Algorithm, RIPEMD-x and HMAC fundamentals, Digital Signature basics, Authentication Protocols, The Digital Signature Standard, Kerberos Authentication scheme, The X.509 Directory Authentication scheme.

Security Protocols

Secure User Authentication, Mail security, PGP, database security, File system security, Program security, Memory security, Session security, SSH, Web security, Replay Attacks, Needham Schroeder Protocol, Denning's Modification, Corrected Protocol, One-Way Authentication for Email, IPSec, SSL, IEEE 802.11, Wired Equivalent Privacy (WEP)

Intrusion detection

Intrusion vs. Extrusion Detection, Examples of Intrusion, Categories of Intruders, Hacker Behavior Example, Criminal Enterprise Behavior, Insider Behavior Example, Intrusion Techniques, Password Guessing and Capture, Notification Alarms, Types of IDS, Sample Signatures, Anomaly Based IDS, Statistical Anomaly Detection, Audit Records, Rule-Based Intrusion Detection, Types of ID, Host vs. Network IDS, Honeypots

Text and Reference Books

1. William Stallings, "Cryptography and Network Security: Principles and Practice", Pearson Education.
2. D Stinson, "Cryptography: Theory and Practice", Chapman & Hall.
3. C. Kaufman, R. Perlman and M. Spenser, "Network Security", PHI.
4. S. Bellovin and W. Chesvick, "Internet Security and Firewalls", Addison-Wesley, Reading.
5. Trappe & Washington, "Introduction to Cryptography with Coding Theory", Prentice-Hall.
6. NIST standards