Management of Information And Communication Security
(資訊通訊安全管理)

Syllabus

Instructor: Kai-Yung Lin , Ph D

Tel: 0935-227-785

e-mail: linky@ms2.hinet.net

Objectives:

In this course, we study the theoretical and practical aspects of network security. We start with a threat model, and describe vulnerabilities of computer networks to attacks by adversaries and hackers using a variety of techniques. We then study methods and techniques to circumvent or defend against these attacks and to minimize their damage. Also, we study cryptographic techniques and protocols, network security protocols, digital signatures and authentication protocols, and network security practice.

Course Outline:

- **Introduction:** Security attacks to information systems. Threat model. Security services. Mechanisms for providing confidentiality, authentication, integrity, nonrepudiation, and access control. Cryptography in data and communication security.
- **Secret-Key and Public-Key Cryptography:** Cryptosystems and cryptanalysis. Block ciphers and stream ciphers. DES, AES, and RC4. Modes of operation. Confidentiality using encryption. Key distribution. Random number generation. Hashes and message digests. One-way functions. Trapdoor one-way functions. Public-key cryptosystems. RSA, Diffie-Hellman, ElGamal, and elliptic curve cryptosystems.
- **Authentication:** Overview of authentication systems. Authentication of people. Security handshake pitfalls. Strong password protocols. Digital signatures. One-way and mutual authentication protocols.

- **Network Security Standards and Practice:** Kerberos V4 and V5. PKI (Public Key Infrastructure). Real-time communication security. IPsec: AH, ESP, IKE. SSL/TLS. Electronic mail security. PEM, S/MIME, and PGP (Pretty Good Privacy). Firewalls, VPN, Web security.

1. Foundations of Cryptography and Security
    1. Security Trends
    2. Ciphers and Secret Messages
    3. Security Attacks and Services
    4. Course Overview
2. Classical Encryption Techniques
    1. Symmetric Cipher Model
    2. Substitutions and Permutations
    3. Classic methods and Rotor Machines
    4. Steganography
3. Block Ciphers and Data Encryption Standard
    1. Block Cipher Principles
    2. The Data Encryption Standard
    3. Differential and Linear Cryptanalysis
    4. Block Cipher Design Principles
4. Mathematical Tools for Cryptography: Finite Fields
    1. Groups, Rings, and Fields
    2. Modular Arithmetic, Euclid's Algorithm
    3. Polynomial Arithmetic
    4. Finite Fields
5. Advanced Encryption Standard
    1. Evaluation Criteria for AES
    2. AES Cipher
6. More on Symmetric Ciphers
    1. Multiple Encryption
    2. DES and Triple DES
    3. Modes of Operation (ECB,CBC, OFB,CFB)
    4. Stream Ciphers and RC4
7. Confidentiality Using Symmetric Encryption
    1. Placement of Encryption Function
    2. Traffic Confidentiality
    3. Key Distribution

    4. Random Number Generation
8. Introduction to Number Theory
    1. Prime Number and Testing for Primality
    2. Fermat's and Euler's Theorem
    3. The Chinese Remainder Theorem
    4. Discrete logarithms
9. Public Key Cryptography and RSA
    1. Principles of Public Key Cryptography
    2. The RSA Algorithm
10. Key Management, Other Public Key Cryptosystem
    1. Key Management
    2. Diffie-Hellman Key Exchange
    3. Elliptic Curve Arithmetic
    4. Elliptic Curve Cryptography
11. Mid-term Exam
12. Message Authentication and Hash Function
    1. Authentication Requirements
    2. Authentication Functions
    3. Message Authentication Codes
    4. Security of Hash Function and MACs
13. Hash and MAC Algorithms
    1. Secure Hash Algorithms
    2. Whirlpool
    3. HMAC
    4. CMAC
14. Digital Signatures and Authentication Protocols
    1. Digital Signature
    2. Authentication Protocols
    3. Digital Signature Standard (DSS and DSA)
15. Authentication Applications
    1. Kerberos V4 and V5
    2. X.509 Authentication Service
    3. Public Key Inforstructure (PKI)
16. Electronic Mail Security
    1. Pretty Good Privacy (PGP)
    2. S/MIME, X.400
17. IP Security
    1. IPSec Overviews

2. IPSec Architecture
3. Authentication Header
4. Encapsulating Security Payload
5. Combining Security Associations
6. Key Management

18. Web Security
    1. Web Security Consideration
    2. Secure Sockets Layer and Transport Layer (SSL and TLS)
    3. Secure Electronic Transaction (SET)
19. Intruder and Malicious Software
    1. Intrusion Detection and Password Management
    2. Virus and Related Threats
    3. Virus and Spyware Countmeasures
    4. Distributed Denial Service Attack
20. Firewalls
    1. Firewall Design Principles
    2. Trusted System
    3. Common Criteria for IT Security Evaluation
21. Report Presentation
22. Final Exam

Grading:

Homework	20%
Mid-Term	35%
Final	40%
Participation	5%

Textbook:

Cryptography and Network Security, Principles and Practices – 4th Edition, William Stallings, Pearson Prentice Hall, 2006.(開發代理).

References

1. *Management Information Systems – 6th Edition,* K. C. Laudon and J. P. Laudon, Prentice Hall, 2000.
2. *Applied Cryptography, 2nd Edition, Bruce Schneier, John Wiley & Sons, 1996.*
3. *The Design of Rijndael, Joan Daemen and Vincent Rijmen, Springer, 2002.*
4. *Cryptography, Theory and Practice, 2nd Edition, Douglas R. Stinson, CRC press, 2002.*