

**SAN JOSE STATE UNIVERSITY  
COLLEGE OF ENGINEERING  
DEPARTMENT OF ELECTRICAL ENGINEERING**

**EE 289: Network Security**

**Dr. Wen-Pai Lu**

**Fall Semester, 2007**

Email: wplu.sjsu@gmail.com

Date: August 23 – December 18

Time: Monday, Wednesday – 4:30 pm – 5:45 pm

**Course Objectives:**

The course provides the underlying principles and practices of modern network security. Network security architectures and protocols are examined and emphasis is given to their performance and implementation aspects. Symmetric and public-key encryption schemes are discussed in details. Authentication, hash functions, and key management schemes are also covered and their impacts on computer network security are compared. Several aspect of Network Security related topic to today's implementation like OSI Security, IP Security, etc. would also be discussed

**Prerequisite:**

Graduate status, or instructor's permission. Internetworking background is required.

**Topics Covered:**

- Network Vulnerabilities: identify and define the different threats to network systems: secrecy, authentication and data integrity.
- Cryptography Principles: mathematical foundations (number theory) for commonly used crypto –algorithms are discussed.
- Symmetric-Key Algorithms: Data Encryption Standard (DES), RC4, and Advanced Encryption Standard (AES) are discussed and their performances are compared.
- The Different types of encryption mode are explained and their pros and cons are discussed: Electronic Code Book Mode, Cipher Block Chaining Mode, Cipher Feedback Mode, Stream Cipher and Counter Modes.
- Public-Key Algorithms: Detailed implementation of the RSA algorithm is provided and when it is more practical to use Public-Key algorithms is discussed: Key Distribution.
- Electronic Digital Signatures: are defined using symmetric-key and public-key approaches. Message Digest, MD5, as alternative solutions to digital signature is also discussed.

- IPsec (IKE): Here we use IKE as study case for security association (SA), authentication and key management schemes.
- OSI Layer Security: Discuss security functions at the bottom four layers of OSI 7 layer architecture, their functions and services.

Textbook:

1. Kaufman, Network Security, Private Communication in Public World, 2<sup>nd</sup> E, PH 2002.

References:

1. W. Stallings, Cryptography and Network Security: Principles and Practice, 4 Ed., PH 2005.
2. Mark Stamp, Information Security: Principles and Practice, John Wiley, 2006
3. Computer Communications Security: Principles, Standard Protocols and Techniques by Warwick Ford, PH, 1994.

Grading Policy:

The overall course grades (letter-grades) will be assigned based on the overall class distribution. The weights of class assignments and the project are as listed below.

Midterm Exam	20%
Homework	10%
Project	35%
Final Exam	35%
Total	100%

Examinations:

- There will be one midterm exam and a final examination. Exams are closed book and notes.
- Exams cover:
  - o Assigned reading materials from the textbook
  - o Discussed materials in the lectures
  - o Class handouts and notes
  - o Homework and practice problems
- Exams will be announced at least one week prior to administration.
- There will be no make-up exams.

### Homework:

Homework assignments will be given periodically and graded.

### Project:

Project will be a research project on the latest topics in Network Security.

### **Course Outline:**

Based on the material of chapters 1-to-13 of the textbook:

#### **I. Introduction**

- Network Security concept and security terminology
- Security Attacks
- Military Model of Security

#### **II. Introduction to Cryptography**

- Cryptographic Attacks
- Secret Key Cryptography
- Public Key Cryptography
- Hash Algorithm

#### **III. Secret Key Cryptography**

- Data Encryption Standard (DES)
- International Data Encryption Algorithm (IEDA)
- Encryption model and techniques
  - Encryption modes Electronic Code Book Mode,
  - Cipher Block Chaining Mode,
  - Cipher Feedback Mode, Stream Cipher and Counter Modes.
- Multiple DES Encryption
- Advanced Encryption Standard (AES)
- Other symmetric ciphers: RC4 and RC5

#### **IV. Hashes and Message Digests**

- MD2
- MD4
- MD5
- SHS

#### **V. Public-Key Algorithms**

- Modular Arithmetic
- Principles of Public-key cryptosystems
- RSA algorithm
- Key management
- Diffie-Hellman key exchange

- Digital Signature

## **VI. Authentication**

- Password-based
- Cryptographic based
- Key Management
- Key Distribution

## **VII. IPSec**

- IPSec architecture overview
- IKE