National Chung Cheng University

Department of Information Management

Introduction to Information Security

Pei-Ju (Julian) Lee

National Chung Cheng University

Information Security

pjlee@mis.ccu.edu.tw

Fall, 2016

Outline

- What is this class about?
- What is Information Security about?
- Class overview

“The field of network and internet security consists of measures to deter, prevent, detect, and correct security violations that involve the transmission of information.”

Online Syllabus

B.B.A. Program in Information Management
Department of Information Management
College of Management
NATIONAL CHUNG CHENG UNIVERSITY
Fall 2016

Department	Department of Information Management			
Course Name	Information Security	Credit	3	
Course Code	5303210_01			
Instructor	Name: Pei-Ju Lee E-mail: pjlee@mis.ccu.edu.tw Phone: 05-2720411, ext. 34622 Class Hour: Tuesday/Thursday 10:15am-11:30am Office hour: By appointment Room: 622			
Location/Time	College of Management 101, Tuesday/Thursday 10:15am-11:30am			
Prerequisites	N/A			
Course Objectives	There are a number of benefits people can acquire with the popularity of the computer and internet nowadays; however, the more convenient or more critical a service, the higher is the level of security required. The main focus of this course are aim to equip students with cryptography and information security knowledge as well as security management skills. This course will cover three aspects of Information Security: traditional cryptography (cryptosystems, authentications, and digital signatures), network and internet security (intrusion detection, response, and communication security services), and security management (security management principles, models, and practices).			
Course Materials	William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 6th edition, 2013.			
Course Web	https://ecourse.ccu.edu.tw			
Reference	Matt Bishop, Introduction to Computer Security, Addison-Wesley. M. E. Whitman and H. J. Mattord, Management of Information Security, Cengage learning, 4th edition, 2014.			
Evaluation	√ Assignment	25 %	□Case Discussion	%
	√ Quiz	5 %	□Presentation	%
	√ Midterm Test	35 %	□Term Paper/Project	%
	√ Final Test	35 %	□Class Participation	%

Topics To Be Covered

- Week 1-4 Symmetric ciphers
- Week 5-7 Asymmetric ciphers
- Week 8-11 Cryptographic data integrity algorithms
- Week 12 Mutual trust
- Week 13-14 Network and internet security
- Week 15-16 Security management

- Tentative schedule

Topics (Con'd)

- Week 1-4 Symmetric Ciphers
  - Advanced Encryption Standard (AES)
  - Data Encryption Standard (DES)
  - Stream Encryption Algorithm RC4
  - Stream Cipher, Block Cipher
- Week 5-7 Asymmetric Ciphers
  - Public-key Algorithms
    - Rivest-Shamir-Adelman (RSA)
    - Elliptic Curve

Topics (Con’d)

- Week 8-11 Cryptographic Data Integrity Algorithms
  - Hash Function
    - Message Authentication Code
    - Digital Signature
- Week 12 Mutual Trust
  - Key Management
  - Key Distribution
  - Authentication Techniques

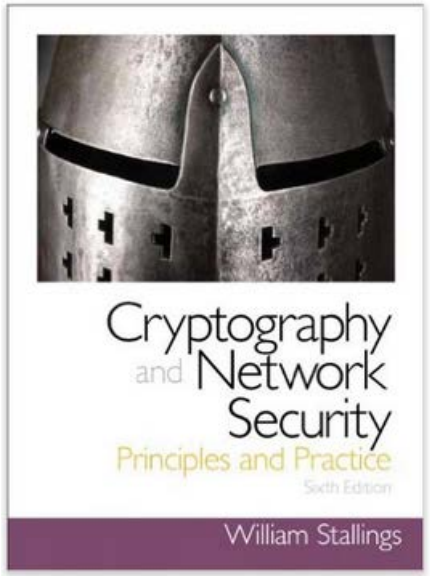
Topics (Con'd)

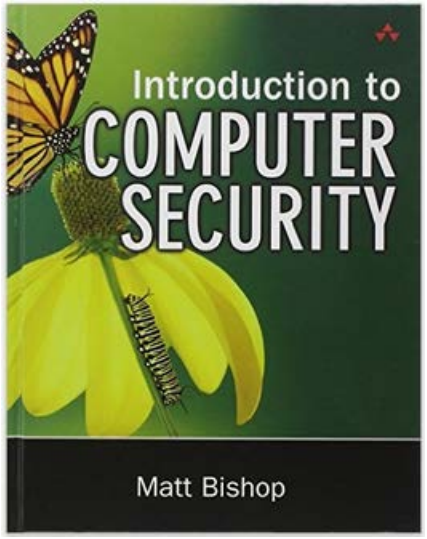
- Week 13-14 Network and Internet Security
  - Network Access Control
  - Cloud Security
  - Transport-Level Security
  - Wireless Network Security
  - E-mail Security
  - IP Security
- Week 15-16 Security Management
  - System Security (Intruders, Virus, Worms, Firewall)
  - Management Models

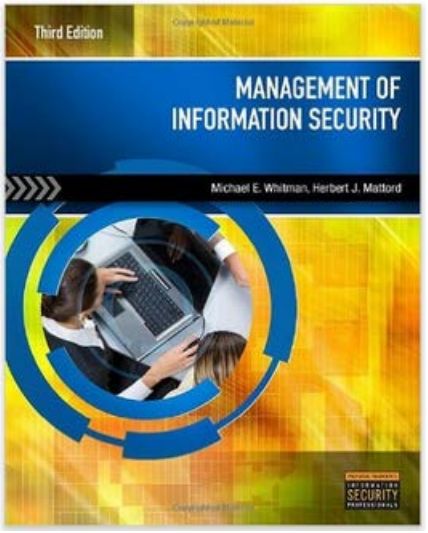
Learning Objective

- Focuses
  - The core cryptography and information security knowledge
  - The information security management skills
- Concepts
  - Traditional cryptography (cryptosystems, authentications, and digital signatures)
  - Network and internet security (intrusion detection, response, and communication security services)
  - Security management (security management principles, models, and practices)

Reference Books







- (Textbook) **William Stallings, Cryptography and Network Security: Principles and Practice, Pearson, 6th edition, 2013.**
- Matt Bishop, Introduction to Computer Security, Addison-Wesley.
- M. E. Whitman and H. J. Mattord, Management of Information Security, Cengage learning, 4th edition, 2014.

Grading

- 25% Assignment
- 35% Midterm Exam
- 35% Final Exam
- 5% Quiz

Homework

- 3 homework assignments over the semester
  - Submit by the end of the due date
  - Delay (points will be deducted)

Question?