University of Macau
Department of Computer and Information Science
CISB461 Information Security
Course Syllabus
2nd Semester 2014/2015

Course Description

(2-2) 3 credits. The course introduces students to the fundamental issues concerning information security and applied cryptography. The areas covered include protecting information using symmetric and public key cryptography; introductions to digital watermarking and biometrics security; viruses and other malicious code; firewalls; intrusion detection systems; security management; as well as legal and ethical aspects.

Course Time and Location:

Lecture	Tuesday 14:00 - 15:45	E11-1025
Tutorial	Monday 9:00 - 10:45	E11-1006

Course Type:

Theoretical with substantial practice content

Prerequisites:

- CISB221
- CISB222
- CISB310

Reference Textbooks:

- William Stallings & Lawrie Brown, *Computer Security: Principles and Practice*, ISBN-10: 0136004245, ISBN-13: 9780136004240, Prentice Hall: 1st Edition, 2008.
- William Stallings, *Cryptography and Network Security*, ISBN-10: 0131873164, ISBN-13: 978-0131873162, Prentice Hall: 4th Edition, 2005.
- Charles P. Pfleeger, Shari Lawrence Pfleeger, *Security in Computing*, Prentice Hall: 4th Edition, 2006.
- Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, Deborah Russell, *Building Internet Firewalls*, O'Reilly & Associates: 2nd Edition, 2000.
- Messoud Benantar, *Introduction to the Public Key Infrastructure for the Internet*, Prentice Hall, 2002.

(All 5 books are available from the UM Library.)

Major Prerequisites by Topic:

1. Basic concepts in operating systems, computer networks, and database systems.
2. Intermediate programming.

Course Objectives:

1. Introduce students to cryptographic algorithms. [a,c]
2. Introduce students to computer security technologies and principles. [a,c]
3. Introduce students to the management aspects of computer security. [a,c]

Course Outline:

Week(s)	Topics	Assessment
1	**Introduction** - Definition of computer security concepts, threats, attacks, assets, security functional requirements, a security architecture for open systems, the scope of computer security, computer security trends, computer security strategy.	
2-3	**Conventional Encryption: Classical Techniques** – Types of attacks, a brief history of cryptography, Caesar cipher, English letter frequencies, polyalphabetic ciphers, Vigenère cipher, Vernam cipher, Hill cipher, transposition ciphers, ADFGVX product cipher, stream and block ciphers, substitution-permutation ciphers.	
4-5	**Conventional Encryption: Modern Techniques** – Data Encryption Standard (DES), S-DES scheme, DES scheme, Four DES modes: Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Double/Triple DES, International Data Encryption Algorithm (IDEA).	

6	**Public-Key Cryptography and Message/User Authentication** – Public-key cipher, classes of public-key algorithms, message/user authentication, e-mail security, IP security, firewall, web/internet security.	
7	**Digital Watermarking** – Watermark: definition, generation, correlation, embedding, detection, attacks, classifications, and applications.	Midterm Assignment
8	**Biometrics Security** – Biometrics: introduction, definition, and systems design.	
9	**Intrusion Detection** – Intruders, intrusion detection, host-based intrusion detection, distributed host-based intrusion detection, network-based intrusion detection, distributed adaptive intrusion detection, intrusion detection exchange format, honeypots.	
10	**Malicious Software** – Types of malicious software, viruses, virus countermeasures, worms, bots, rootkits.	
11	**Denial of Service** – Denial of service attacks, flooding attacks, distributed denial of service attacks, reflector and amplifier attacks, defenses against denial of service attacks, responding to a denial of service attack.	
12	**IT Security Management and Risk Assessment** – IT security management, organizational context and security policy, security risk assessment, detailed security risk analysis, case study.	
13	**IT Security Controls, Plans and Procedures** – IT security management implementation, security controls or safeguards, IT security plan, implementation of controls, implementation, follow up, case study.	
14	**Legal and Ethical Aspects** – Cybercrime and computer crime, intellectual property, privacy, ethical issues. **Project Presentations + Review**	Project
15 onwards		Final Exam

Assessment:

Assignment	10%
Midterm	10%
Project	30%
Final Exam	50% (3 hours exam; date and time TBA)

Course Instructor:

Name: Dr. ZHANG Yibo, Bob - Assistant Professor, Computer and Information Science
Office: E11-4093
Office Hours: Wednesday 14:00 - 15:00 or by appointment
Tel.: 8822-4425
E-mail: bobzhang@umac.mo

Notes

• **Attendance is strongly recommended**.
• Check the course webpage for announcements, assignments, and lectures.
• No makeup exam is given except for medical proof.
• Cheating is absolutely prohibited by the university.