University of Macau
Faculty of Science and Technology
Department of Computer and Information Science
SFTW498 Information Security
Syllabus
2nd Semester 2011/2012
Part A – Course Outline

Elective course in Computer Science

Catalog description:
(3-2) 4 credits. The course introduces students to the fundamental issues concerning information security and applied cryptography. The areas covered are protecting information using symmetric and public key cryptography, cryptographic hash functions and standards, digital signatures, digital certificates, viruses and other malicious code, firewalls, intrusion detection systems, security management, and legal and ethical aspects.

Course type:
Theoretical with substantial laboratory/practice content

Prerequisites:
- SFTW231
- SFTW331
- SFTW370

Textbook(s) and other required material:
- William Stallings & Lawrie Brown, *Computer Security: Principles and Practice,* ISBN-10: 0136004245, ISBN-13: 9780136004240, Prentice Hall, 1st Edition, 2008.

References:
- 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,* 4th Edition, Prentice Hall, 2006.
- Richard J. Spillman, *Classical and Contemporary Cryptology,* Prentice Hall, 2005.
- Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, Deborah Russell, *Building Internet Firewalls*, 2nd Edition, O'Reilly & Associates, 2000.
- Messaoud Benantar, *Introduction to the Public Key Infrastructure for the Internet,* Prentice Hall, 2002.
- FIPS PUB 46-3, FIPS PUB 197, FIPS PUB 180-2, FIPS PUB 198a, RFC1321, and Publications from IEEE, ACM, USENIX Security Symposium and CryptoBytes.

Major prerequisites by topic:
- Basic concepts in operating systems, computer networks, and database systems.
- Intermediate programming.

Course objectives:
- Introduce students to the computer security technology and principles. [a]
- Introduce students to the management aspects of computer security. [a, f]
- Introduce students to the cryptographic algorithms. [a]

Topics covered:
- **Overview (3 hours)**: Study computer security concepts. Discuss computer-related assets that are subject to threats and attacks. Review security functional requirements, a security architecture for open systems, the scope of computer security, computer security trends, and computer security strategy.
- **Cryptographic Tools (3 hours)**: Review the various types of cryptographic algorithms and introduce the most important standardized algorithms in common use. These algorithms include symmetric encryption, message

authentication and hash functions, public-key encryption, digital signatures and key management, generation of random and pseudorandom numbers, and encryption of stored data.

- **User Authentication (3 hours)**: Discuss the means of authentication. Study password-based authentication, token-based authentication, biometric authentication, and remote user authentication. Discuss security issues for user authentication and practical applications.
- **Access Control (3 hours)**: Review access control principles, subjects, objects, access rights, discretionary access control, Unix file access control, and role-based access control.
- **Intrusion Detection (3 hours)**: Identify the classes of intruders. Discuss basic principles of intrusion detection. Study host-based intrusion detection, distributed host-based intrusion detection, network-based intrusion detection, distributed adaptive intrusion detection, intrusion detection exchange format, and honeypots.
- **Malicious Software (3 hours)**: Examine types of malicious software, viruses, virus countermeasures, worms, bots, and rootkits.
- **Denial of Service (3 hours)**: Explore denial of service attacks, flooding attacks, distributed denial of service attacks, reflector and amplifier attacks. Review the defenses against denial of service attacks and responding to a denial of service attack.
- **Firewall and Intrusion Prevention Systems (3 hours)**: Discuss the need for firewalls. Review firewall characteristics, types of firewalls, firewall basing, firewall location and configurations, and intrusion prevention systems.
- **IT Security Management and Risk Assessment (3 hours)**: Review the process of how to best select and implement a range of technical and administrative measures to effectively address an organization's security requirements. Examine the role and importance of the IT systems in the organization. Study security risk assessment approaches and detailed security risk analysis.
- **IT Security Controls, Plans, and Procedures (3 hours)**: Explore the range of management, operational, and technical controls or safeguards available that can be used to improve security of IT systems and processes.
- **Legal and Ethical Aspects (3 hours)**: Study the classification of cybercrime and computer crime. Discuss about intellectual property, privacy, and ethical issues.
- **Symmetric Encryption and Message Confidentiality (6 hours)**: Study symmetric encryption principles, Data Encryption Standard, Advanced Encryption Standard, stream ciphers and RC4, cipher block modes of operation, location of symmetric encryption devices, and key distribution.
- **Public Key Cryptography and Message Authentication (3 hours)**: Study secure hash functions, HMAC, the RSA public-key encryption algorithm, Diffie-Hellman, and other asymmetric algorithms.

Class/laboratory schedule:

Timetabled work in hours per week			No of teaching weeks	Total hours	Total credits	No/Duration of exam papers
Lecture	**Tutorial**	**Practice**				
3	2	Nil	14	70	4	1 / 3 hours

Student study effort required:

Class contact:	
Lecture	42 hours
Tutorial	28 hours
Other study effort	
Self-study	28 hours
Homework assignment	12 hours
Total student study effort	110 hours

Student assessment:

Final assessment will be determined on the basis of:

Homework	20%	Project	10%
Mid-term exam	30%	Final exam	40%

Course assessment:

The assessment of course objectives will be determined on the basis of:

- Assignments, project and exams
- Course evaluation

Course outline:

Weeks	Topic	Course work
1	**Overview** 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	**Cryptographic Tools** Confidentiality with symmetric encryption, message authentication and hash functions, public-key encryption, digital signatures and key management, random and pseudorandom numbers, encryption of stored data.	Assignment#1
3-4	**Symmetric encryption and Massage Confidentiality** Symmetric encryption principles, Data Encryption Standard, Advanced Encryption Standard, stream ciphers and RC4, cipher block modes of operation, location of symmetric encryption devices, key distribution.	Assignment#2
5	**Public-key Cryptography and Message Authentication** Secure hash functions, HMAC, the RSA public-key encryption algorithm, Diffie-Hellman and other asymmetric algorithms.	Project
6	**User Authentication** Means of authentication, password-based authentication, token-based authentication, biometric authentication, remote user authentication, security issues for user authentication, practical applications and case study.	Assignment#3
7	**Access Control** Access control principles, subjects, objects, access rights, discretionary access control, Unix file access control, Role-based access control, case study.	Midterm
8	**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.	Assignment#4
9	**Malicious Software** Types of malicious software, viruses, virus countermeasures, worms, bots, rootkits.	Assignment#5
10	**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.	Assignment#6
11	**Firewalls and Intrusion Prevention Systems** The need for firewalls, firewall characteristics, types of firewalls, firewall basing, firewall location and configurations, intrusion prevention systems.	Assignment#7
12	**IT Security Management and Risk Assessment** IT security management, organizational context and security policy, security risk assessment, detailed security risk analysis, case study.	Assignment#8
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.	Assignment#9
14	**Legal and Ethical Aspects** Cybercrime and computer crime, intellectual property, privacy, ethical issues.	Assignment#10

Contribution of course to meet the professional component:
This course prepares students to work professionally in the area of Information Security.

Relationship to CS program objectives and outcomes:
This course primarily contributes to the Computer Science program outcomes that develop student abilities to:
(a) an ability to apply knowledge of computing, mathematics, science, and engineering.
(f) an understanding of professional, ethical, legal, security and social issues and responsibilities.

Relationship to CS program criteria:

Criterion	DS	PF	AL	AR	OS	NC	PL	HC	GV	IS	IM	SP	SE	CN
Scale: 1 (highest) to 4 (lowest)		4	3			2						3		

Discrete Structures (DS), Programming Fundamentals (PF), Algorithms and Complexity (AL), Architecture and Organization (AR), Operating Systems (OS), Net-Centric Computing (NC), Programming Languages (PL), Human-Computer Interaction (HC), Graphics and Visual Computing (GV), Intelligent Systems (IS), Information Management (IM), Social and Professional Issues (SP), Software Engineering (SE), Computational Science (CN).

Course content distribution:

Percentage content for			
Mathematics	Science and engineering subjects	Complementary electives	**Total**
0%	20%	80%	100%

Coordinator:
Prof. Chi Man Pun

Persons who prepared this description:
Dr. Yain Whar Si

Part B – General Course Information and Policies

2nd Semester 2011/2012

Instructor: Dr. Yain Whar Si
Office: N404
Office hour: by appointment
Phone: 8397 4454
Email: fstasp@umac.mo

Time/Venue: *To be announced*

Grading distribution:

Percentage Grade	Final Grade	Percentage Grade	Final Grade
100 - 93	A	92 - 88	A–
87 - 83	B+	82 - 78	B
77 - 73	B–	72 - 68	C+
67 - 63	C	62 - 58	C–
57 - 53	D+	52 - 50	D
below 50	F		

Comment:
The objectives of the lectures are to explain and to supplement the text material. Students are responsible for the assigned material whether or not it is covered in the lecture. Students are encouraged to look at other sources (other references, etc.) to complement the lectures and text.

Homework policy:
The completion and correction of homework is a powerful learning experience; therefore:
- There will be approximately 10 homework assignments.
- Homework is due one week after assignment unless otherwise noted.

Course project:
The project is probably the most exciting part of this course and provides students with meaningful experience.
- Students will work individually for the project.
- The requirements will be announced and discussed in class.
- The project will be presented at the end of semester.

Exam:
One 2-hour mid-term exam will be held during the semester. Both the mid-term and final exams are closed book examinations. There will be occasional in-class assignment.

Note:
- Check UMMoodle (UMMoodle.umac.mo) for announcement, homework and lectures. Report any mistake on your grades within one week after posting.
- No make-up exam is given except for CLEAR medical proof.
- Cheating is absolutely prohibited by the university.

Appendix:

Rubric for Program Outcomes

Rubric for (a)	5 (Excellent)	3 (Average)	1 (Poor)
Understand the theoretic background	Students understand theoretic background and the limitations of the respective applications.	Students have some confusion on some background or do not understand theoretic background completely.	Students do not understand the background or do not study at all.
Compute the problem correctly	Students use correct techniques, analyze the problems, and compute them correctly.	Students sometime solve problem mistakenly using wrong techniques.	Students do not know how to solve problems or use wrong techniques completely.
Rubric for (f)	**5 (Excellent)**	**3 (Average)**	**1 (Poor)**
Design	Understand how to critique and analyze design tradeoffs and constraints with respect to safety, liability, and integrity of data, and context of use.	Have knowledge of safety, liability, and integrity of data, and context of use but cannot analyze thoroughly.	No awareness of importance of safety, liability, and integrity of data, and context of use.
Professional engineering practice	Understand how to critique and analyze tradeoffs and constraints with respect to research issues of credit and authorship, integrity of data, and informed consent.	Have knowledge of credit and authorship, integrity of data, and informed consent but cannot completely identify ownership in practical.	No awareness of credit and authorship, integrity of data, and informed consent.