
SCSSE

**School of Computer Science and Software Engineering
Faculty of Informatics**

CSCI358 Security Engineering Subject Outline Spring Session 2009

Head of School – Professor Willy Susilo, Student Resource Centre, Tel: (02) 4221 3606

GENERAL INFORMATION

Subject Coordinator

Telephone Number:

Email:

Location:

Dr Luke McAven

02 4221 4879

lukemc@uow.edu.au

3.109

Dr McAven's consultation times during session:

Day

Monday

Wednesday

Time

10:30am-12:30pm

10:30am-12:30pm

Subject Organisation

Session:

Credit Points

Contact hours per week:

Lecture Times & Location:

Tutorial Day, Time and Location can be found at:

Spring Session, Wollongong Campus

6 credit points

3 hours lectures/tutorial

13:30-16:30 Wed, 3.121

<http://www.uow.edu.au/student/timetables/index.html>

Students should check the subject's web site regularly as important information, including details of unavoidable changes in assessment requirements will be posted from time to time via e-Learning space <http://www.uow.edu.au/student/>. Any information posted to the web site is deemed to have been notified to all students.

Subject Description

This subject develops the skills and applies the knowledge necessary to identify and solve problems in the deployment of security systems. Topics include: Relationships among cryptographic techniques. Black, white and grey hat techniques. Authentication versus identification, Security policies for security administration. Security monitoring. E-commerce, bank security. File sharing and source control integrity. Legality of digital signatures, DRM, forensics, liability, copyright protection, internet censorship. Standards and RFCs. Security of deployed systems

Subject Objective

On successful completion of this subject, students will be able to:

1. Select and apply appropriate fundamental cryptographic building blocks based on a critical analysis of an application scenario.
 2. Demonstrate an appreciation of the role and significance of information security in society.
 3. Interpret documents relating to standards, RFC's and similar formal specifications of existing security systems.
-

4. Recognise the role of the law and due process in the development, deployment and management of security.

Graduate Qualities

This subject will continue to the following graduate qualities:

Informed
Independent Learners
Problem Solvers
Effective Communicators
Responsible
Team Work
Innovation & Design

Further information can be found at:

<http://www.uow.edu.au/informatics/scsse/current/SubjectInformation/UOW049401.html>

Attendance Requirements:

It is the responsibility of students to attend all lectures/tutorials/labs/seminars/practical work for subjects for which you are enrolled. It should be noted that the amount of time spent on each 6 credit point subject should be at least 12 hours per week, which includes lectures/tutorials/labs etc.

Satisfactory attendance is deemed by the University, to be attendance at approximately 80% of the allocated contact hours.

Attendance rolls will be kept for lectures and tutorials. If you are present for less than 80% and would have otherwise passed you need to apply for student academic consideration, otherwise a TF (technical fail) grade will be recorded.

Method of Presentation:

In order to maximize learning outcomes, it is strongly recommended that students attend all lectures.

Lecture Schedule:

This subject looks at the design, deployment and governance of secure systems. We begin with a sketch of what security engineering is, and present a basic framework which we use throughout the subject. We give an overview of the technical foundations of information security, specifically confidentiality and integrity mechanisms, access control and authentication. We look at the roles of protocols and the effect of distributed environments. We look at aspects of the design process and governance, including threat modeling and risk analysis. We look at the role and design of standards. We discuss how a diverse range of issues, such as psychology, law, economics and privacy, impinge on the various components of the security framework. We may consider examples from a range of specific systems, such as banking systems, physical security systems, digital rights management and game security.

Objectives: A student who successfully completes this subject should be able to:

- Analyze systems to identify vulnerabilities, and, considering appropriate threats which may exploit those vulnerabilities, analysis approaches to risk management.
- Identify common flaws in protocols and standards.
- Demonstrate an understanding of appropriate design, management and monitoring processes.
- Demonstrate an understanding of how different cryptographic primitives are related.
- Recognize and demonstrate the role of disciplines such as economics, and psychology can play in system security.
- Demonstrate knowledge of relevant terminology.

A proposed Lecture schedule for the subject is as follows:

Week	Topic
1	Subject introduction. What is Security Engineering?
2	Communication and cryptology. Providing C.I.A.: Cryptographic constructs
3	Authentication - Biometrics. Access control.
4	Protocols. Distributed systems.
5	The problems with people (Psychology).
6	People and their money (Economics).
7	Physical security.
8	Managing the development of secure systems.
9	Requirements Engineering, Threat modeling and risk management.
10	Assurance and Evaluation.
11	Standards
12	Policies and Principles.
13	Summary.

Changes to the above schedule will be posted via e-Learning space <http://www.uow.edu.au/student/>. Any information posted to the web site is deemed to have been notified to all students.

Subject Materials:

Any readings/references are recommended only and are not intended to be an exhaustive list. Students are encouraged to use the library catalogue and databases to locate additional readings

Textbook(s):

Anderson, **Security Engineering**, John Wiley & Sons, 2nd ed., 2008.

An electronic copy of the first edition is freely distributed by the author/publisher and will be made available to students.

Other Resources:

Whitman and Mattord, **Principles of Information Security**, Thompson, 2nd ed., 2005.

Dhillon, **Principles of Information Systems Security: Text and Cases**, John Wiley & Sons, 2007.

Slay and Koronios, **Information Technology Security & Risk Management**, John Wiley & Sons, 2006.

Raval and Fichadia, **Risks, Controls and Security: Concepts and Applications**, John Wiley & Sons, 2007.

Borodzicz, **Risk, Crisis & Security Management**, John Wiley & Sons, 2005.

Stallings, **Cryptography and Network Security**, Prentice Hall, 4th ed., 2005.

Stallings and Brown, **Computer Security: Principles and Practice**, Prentice Hall, 4th ed., 2008.

A lot of electronic documents will be provided for students to read.

Assessment:

This subject has the following assessment components.

ASSESSMENT ITEMS & FORMAT	% OF FINAL MARK	GROUP/ INDIVIDUAL	DUE DATE
Assignment 1: Short answer, including exercises such as text and scenario analysis.	10%	Individual	Week Six. Hard copy to the lecturer.
Assignment 2: Short answer, including exercises such as text and scenario analysis.	10%	Individual	Week Thirteen. Hard copy to the lecturer.
12 Weekly exercises.	10%	Individual	Throughout term. Hard copy to the lecturer.
Midterm test	5%	Individual	About Week Eight. Written.
Debates.	10%	Group	To be specified. Presentations.
Presentation and report.	5%	Individual	To be specified. Presentation to class and hardcopy.
Final exam.	50%	Individual ☺	During exam period. Written.

Notes on Assessment:

All assignments are expected to be completed independently. Plagiarism may result in a FAIL grade being recorded for that assignment.

Electronic Submission of Assessment Items:

Unless otherwise notified by the subject coordinator, all written assignments must be submitted electronically.

Students are required to submit assignments in hard copy to the lecturer.

Submission of assessment items via email will not be accepted.

To be eligible for a Pass in this subject a student must achieve a mark of at least 50% in the Exam. Students who fail to achieve this minimum mark & would have otherwise passed will be given a TF (Technical Fail) for this subject.

Procedures for the return of assessment items:

We aim to return assignment marks within 2 weeks of the assignment deadline.

Penalties for late submission of assessment items:

Penalties apply to all late work, except if student academic consideration has been granted. Late submissions will attract a penalty of 25 % of the assessment mark.

Tutorial/Lab Closure Policy

If for any reason, the number of students in a tutorial or lab falls below a sustainable enrolment level, as determined by the Head of School, tutorials/labs offered for that subject may be collapsed or deleted.

You will have to attend the new tutorials/lab if this closure affects the one you are attending.

We will endeavour to make this decision no later than Week 4 of session.

Supplementary Exams

Supplementary Exams will be dealt with in accordance with student academic consideration policy (<http://www.uow.edu.au/about/policy/studentacademicconsiderationpolicy.pdf>) 9.2 Timing of Supplementary Exams.

While the School normally grants supplementary exams when the student does not sit the standard exam for an acceptable reason, each case will be assessed on its own merit and there is no guarantee a supplementary exam will be granted. If a supplementary exam is granted, you will normally be notified via SOLS Mail the time and date of this supplementary exam. You must follow the instructions given in the email message.

Please note that if this is your last session and you are granted a supplementary exam, be aware that your results will not be processed in time to meet the graduation deadline.

Student Academic Consideration Policy

The School recognises that it has a responsibility to ensure equity and consistency across its subjects for all students. Sometimes, in exceptional circumstances, students need to apply for student academic consideration in order to complete all assessable work.

The University applies strict criteria to the granting of student academic consideration. Before applying for student academic consideration, students should carefully read the University's policy which can be found at: <http://www.uow.edu.au/about/policy/studentacademicconsiderationpolicy.pdf>.

Plagiarism

When you submit an assessment task, you are declaring the following

1. It is your own work and you did not collaborate with or copy from others.
2. You have read and understand your responsibilities under the University of Wollongong's policy on plagiarism.
3. You have not plagiarised from published work (including the internet). Where you have used the work from others, you have referenced it in the text and provided a reference list at the end of the assignment.

Students must remember that:

Plagiarism will not be tolerated.

Students are responsible for submitting original work for assessment, without plagiarising or cheating, abiding by the University's policies on Plagiarism as set out in the University Handbook under University Policy Directory and in Faculty handbooks and subject guides. Plagiarism has led to the expulsion from the University.

Student Academic Grievance Policy

The School aims to provide a fair, equitable and productive learning environment for all its students. The Student Academic Grievance Policy seeks to support the achievement of this goal by providing a transparent and consistent process for resolving student academic grievances.

Any student who has a grievance over a result should obtain a Faculty of Informatics Appeal Against Decision or Action Affecting Academic Experience form from the Informatics Student Enquiry Centre. (<http://www.uow.edu.au/content/groups/public/@web/@inf/@faculty/documents/doc/uow017433.pdf>) The student should firstly take the form to the marker/lecturer to discuss the matter and, if the student is still not satisfied, s/he should take the next step as outlined on the form.

This subject outline can be found at: <http://www.uow.edu.au/informatics/scsse/current>

Once the grievance has been considered by the Faculty, if the student still feels the situation has not been fully resolved s/he may consult the Dean of Students. However, the Dean of Students can have no input into the academic judgment of the lecturer and can only review the grievance to ensure proper procedure has been followed.

Relevant University Policies, procedures and students services:

For more information students must refer to the Faculty handbook, online references or consult the UOW policy in full at <http://www.uow.edu.au/handbook/courserules/studacgrievpol.html> which contains a range of policies on educational issues and student matters.

This outline should be read in conjunction with the following documents:

Code of Practice - Teaching and Assessment http://www.uow.edu.au/handbook/codesofprac/teaching_code.pdf	Code of Practice - Students http://www.uow.edu.au/handbook/codesofprac/cop_students.html
Code of Practice-Honours http://www.uow.edu.au/handbook/CodeofPractice-Honours.pdf	Acknowledgement Practice Plagiarism will not be tolerated: http://www.uow.edu.au/handbook/courserules/plagiarism.html
Key Dates http://www.uow.edu.au/student/dates.html	Student Academic Consideration Policy: http://www.uow.edu.au/about/policy/studentacademicconsiderationpolicy.pdf
Course Progress Requirements: http://www.uow.edu.au/student/mrp/index.html	Graduate Qualities Policy: http://www.uow.edu.au/about/teaching/qualities/index.html#_The_new_UOW
Academic Grievance Policy (Coursework and honours students) http://www.uow.edu.au/handbook/courserules/studacgrievpol.html	Non-Discriminatory Language Practice and Presentation http://staff.uow.edu.au/eed/nondiscrimlanguage.html
Occupational Health and Safety http://staff.uow.edu.au/ohs/commitment/ohspolicy/index.html	Ownership of Work & Intellectual Property Policy: http://www.uow.edu.au/handbook/generalcourserules/UOW028651.html
Human Research Ethics Committee: http://www.uow.edu.au/research/rso/ethics/human/	Rules for student conduct: http://www.uow.edu.au/handbook/generalrules/StudentConductRules.pdf
Independent Learners' Introductory Program http://www.uow.edu.au/student/attributes/ilip/	Informatics Faculty Librarian, Ms Annette Meldrum, phone: 4221 4637, email: ameldrum@uow.edu.au
Student Support Services: http://www.uow.edu.au/student/services/ Informatics Faculty SEDLO (Student Equity and Diversity Liaison Officers) Virginie Schmelitschek, phone 4221 3833, virginie@uow.edu.au	SCSSE Internet Access & Student Resource Centre http://www.uow.edu.au/informatics/common/uow024466.html
SCSSE Computer Usage Rules http://www.uow.edu.au/informatics/common/uow024457.html	SCSSE Subject Outlines http://www.uow.edu.au/informatics/scsse/current