MONASH University
Information Technology

FIT5163
Information and computer security

Unit Guide

Semester 2, 2011

Last updated: 22 Aug 2011

Table of Contents

FIT5163 Information and computer security - Semester 2, 2011 1
- Mode of Delivery 1
- Contact Hours 1
- Workload 1
- Unit Relationships 1
  - Prohibitions 1
  - Prerequisites 1

Chief Examiner 1
Campus Lecturer 1
- Caulfield 1

Academic Overview 2
- Learning Objectives 2
- Graduate Attributes 2
- Assessment Summary 2
- Teaching Approach 2
- Feedback 3
  - Our feedback to You 3
  - Your feedback to Us 3

Previous Student Evaluations of this unit 3

Unit Schedule 4

Assessment Requirements 5
- Assessment Policy 5
- Assessment Tasks 5
  - Participation 5

Examinations 6
- Examination 1 6

Assignment submission 6
Extensions and penalties 6
Returning assignments 6

Other Information 7
- Policies 7
- Student services 7

FIT5163 Information and computer security - Semester 2, 2011

This unit provides students with in depth coverage of a range of security problems in information systems, namely physical security, network security and software security. Within these areas, topics covered include risk analysis, authentication, access control, and a range of cryptographic techniques. It looks at various management issues, including use and abuse of encryption, distributed systems authentication, contingency planning, auditing, logging and integrity management. A range of security applications are used as examples.

Mode of Delivery

Caulfield (Evening)

Contact Hours

2 hrs lectures/wk, 2 hrs tutorials/wk

Workload

Student workload commitments per week are:

- two-hour lecture and
- two-hour tutorial (requiring advance preparation)
- a minimum of 2-3 hours of personal study per one hour of contact time in order to satisfy the reading and assessment expectations.

Unit Relationships

Prohibitions

FIT4016, CSE4892

Prerequisites

Introductory knowledge of computing at the undergraduate level is assumed.

Chief Examiner

Dr Nandita Bhattacharjee

Campus Lecturer

Caulfield

Nandita Bhattacharjee

Academic Overview

Learning Objectives

At the completion of this unit students will:

- have knowledge of risks, threats and the goals of information security;
- understand various controls and their effectiveness for information security in an organisation;
- be able to evaluate the effectiveness (both in terms of performance and limitations) of individual control techniques;
- match the risk against controls and evaluate their applicability.

Graduate Attributes

Monash prepares its graduates to be:

1. responsible and effective global citizens who:

a. engage in an internationalised world
b. exhibit cross-cultural competence
c. demonstrate ethical values

critical and creative scholars who:

a. produce innovative solutions to problems
b. apply research skills to a range of challenges
c. communicate perceptively and effectively

Assessment Summary

Examination (3 hours): 60%; In-semester assessment: 40%

Assessment Task	Value	Due Date
Class tests	20%	15 August 2011, 12 September 2011, 17 October 2011 in Lectures
Group assignment - Biometrics in Cryptography	20% (Report 14%, Presentation 6%)	Report due 7 October 2011, Presentations due Week 11 Tutorial
Examination 1	60%	To be advised

Teaching Approach

Lecture and tutorials or problem classes

This teaching and learning approach provides facilitated learning, practical exploration and peer learning.

Feedback

Our feedback to You

Types of feedback you can expect to receive in this unit are:

- Informal feedback on progress in labs/tutes
- Test results and feedback
- Other: Answers to discussion sheets & individual student meetings

Your feedback to Us

Monash is committed to excellence in education and regularly seeks feedback from students, employers and staff. One of the key formal ways students have to provide feedback is through SETU, Student Evaluation of Teacher and Unit. The University's student evaluation policy requires that every unit is evaluated each year. Students are strongly encouraged to complete the surveys. The feedback is anonymous and provides the Faculty with evidence of aspects that students are satisfied and areas for improvement.

For more information on Monash's educational strategy, and on student evaluations, see:
http://www.monash.edu.au/about/monash-directions/directions.html
http://www.policy.monash.edu/policy-bank/academic/education/quality/student-evaluation-policy.html

Previous Student Evaluations of this unit

If you wish to view how previous students rated this unit, please go to
https://emuapps.monash.edu.au/unitevaluations/index.jsp

Unit Schedule

Week	Activities	Assessment
0		No formal assessment or activities are undertaken in week 0
1	Introduction to information security	
2	Principles of encryption	
3	Cryptography I	
4	Cryptography II	Class test 1 in Lecture 15 August 2011
5	Authentication	
6	Access control	
7	Introduction to number theory	
8	Public key cryptography	Class test 2 in Lecture 12 September 2011
9	Biometrics	
10	Integrity & non-repudiation	Assignment Report due 7 October 2011
11	Key management & distributed authentication	Assignment Presentation Week 11 Tutorial
12	Software security	Class test 3 in Lecture 17 October 2011
	SWOT VAC	No formal assessment is undertaken SWOT VAC
	Examination period	LINK to Assessment Policy: http://policy.monash.edu.au/policy-bank/academic/education/assessment/assessment-in-coursework-policy.html

*Unit Schedule details will be maintained and communicated to you via your MUSO (Blackboard or Moodle) learning system.

Assessment Requirements

Assessment Policy

To pass a unit which includes an examination as part of the assessment a student must obtain:

- 40% or more in the unit's examination, and
- 40% or more in the unit's total non-examination assessment, and
- an overall unit mark of 50% or more.

If a student does not achieve 40% or more in the unit examination or the unit non-examination total assessment, and the total mark for the unit is greater than 50% then a mark of no greater than 49-N will be recorded for the unit

Assessment Tasks

Participation

- **Assessment task 1**

  Title:
  Class tests
  Description:
  Three Class tests will be conducted on the topics covered in this unit. They will be held during lectures. Each Class test will have a weighting of 10%. The best two scores will added to an assessment total of 20%.
  Weighting:
  20%
  Criteria for assessment:
  Quality of answers in response to test questions.

  How well understanding of lecture material covered is demonstrated.
  Due date:
  15 August 2011, 12 September 2011, 17 October 2011 in Lectures

- **Assessment task 2**

  Title:
  Group assignment - Biometrics in Cryptography
  Description:
  In this assignment students will be working in groups of two or three members. This assignment explores how the iris image of an individual can be used to generate the key for private key cryptography. In other words, we would like to integrate the biometric, in this case the iris with cryptography so that security of the system authentication as well as information security can be achieved.

  Details of the tasks will be provided in the assignment handout. A comprehensive report is due in Week 10. Students presentations on the assignment is due in Week 11.
  Weighting:
  20% (Report 14%, Presentation 6%)
  Criteria for assessment:
  How well understanding of the allocated task is demonstrated.

Each student completes an allocated task that contributes to the final report, and receives marks for that task. Students will give individual presentations of their allocated task. Peer review will assess peer learning and peer support.

Due date:

Report due 7 October 2011, Presentations due Week 11 Tutorial

Examinations

- **Examination 1**

Weighting:

60%

Length:

3 hours

Type (open/closed book):

Closed book

Electronic devices allowed in the exam:

None

Assignment submission

It is a University requirement (http://www.policy.monash.edu/policy-bank/academic/education/conduct/plagiarism-procedures.html) for students to submit an assignment coversheet for each assessment item. Faculty Assignment coversheets can be found at http://www.infotech.monash.edu.au/resources/student/forms/. Please check with your Lecturer on the submission method for your assignment coversheet (e.g. attach a file to the online assignment submission, hand-in a hard copy, or use an online quiz).

Extensions and penalties

Submission must be made by the due date otherwise penalties will be enforced.

You must negotiate any extensions formally with your campus unit leader via the in-semester special consideration process: http://www.infotech.monash.edu.au/resources/student/equity/special-consideration.html.

Returning assignments

Students can expect assignments to be returned within two weeks of the submission date or after receipt, whichever is later

Other Information

Policies

Monash has educational policies, procedures and guidelines, which are designed to ensure that staff and students are aware of the University's academic standards, and to provide advice on how they might uphold them. You can find Monash's Education Policies at: http://policy.monash.edu.au/policy-bank/academic/education/index.html

Key educational policies include:

- Plagiarism (http://www.policy.monash.edu/policy-bank/academic/education/conduct/plagiarism-policy.html)
- Assessment (http://www.policy.monash.edu/policy-bank/academic/education/assessment/assessment-in-coursework-po
- Special Consideration (http://www.policy.monash.edu/policy-bank/academic/education/assessment/special-consideration-policy.h
- Grading Scale (http://www.policy.monash.edu/policy-bank/academic/education/assessment/grading-scale-policy.html)
- Discipline: Student Policy (http://www.policy.monash.edu/policy-bank/academic/education/conduct/student-discipline-policy.html)
- Academic Calendar and Semesters (http://www.monash.edu.au/students/key-dates/);
- Orientation and Transition (http://www.infotech.monash.edu.au/resources/student/orientation/); and
- Academic and Administrative Complaints and Grievances Policy (http://www.policy.monash.edu/policy-bank/academic/education/management/complaints-grievance-policy.
- Codes of Practice for Teaching and Learning (http://www.policy.monash.edu.au/policy-bank/academic/education/conduct/suppdocs/code-of-practice-tea

Student services

The University provides many different kinds of support services for you. Contact your tutor if you need advice and see the range of services available at www.monash.edu.au/students The Monash University Library provides a range of services and resources that enable you to save time and be more effective in your learning and research. Go to http://www.lib.monash.edu.au or the library tab in my.monash portal for more information. Students who have a disability or medical condition are welcome to contact the Disability Liaison Unit to discuss academic support services. Disability Liaison Officers (DLOs) visit all Victorian campuses on a regular basis

- Website: http://adm.monash.edu/sss/equity-diversity/disability-liaison/index.html;
- Telephone: 03 9905 5704 to book an appointment with a DLO;
- Email: dlu@monash.edu
- Drop In: Equity and Diversity Centre, Level 1 Gallery Building (Building 55), Monash University, Clayton Campus.

Reading list

Cryptography and Network Security: Principles and Practice. William Stallings, Fifth Edition, 2011. Prentice Hall.

Computer Security: Principles and Practice William Stallings and Lawrie Brown, 2008, Prentice Hall.

Other Information

Security Engineering: A guide to building dependable distributed systems. Ross J. Anderson, Second Edition, 2008, John Wiley & Sons, Inc.