MONASH University
Information Technology

FIT5163
Information and computer security

Unit Guide

Semester 2, 2014

The information contained in this unit guide is correct at time of publication. The University has the right to change any of the elements contained in this document at any time.

Last updated: 07 Jul 2014

Table of Contents

FIT5163 Information and computer security - Semester 2, 2014

The unit aims to provide the students with in depth knowledge of techniques required to deal with security problems in information systems. The main areas of study include symmetric and asymmetric encryption techniques, cryptographic hash functions with related topics of message authentication codes and digital signatures. Study of techniques and algorithms for providing mutual trust include key management and distribution and user authentication to establish trust in the identity of communicating partner are also included. It looks at various management issues, including use and abuse of encryption, distributed systems authentication and integrity management. A range of security applications are used as examples. Students will learn how to apply cryptographic techniques in practice.

Mode of Delivery

Caulfield (Day)

Workload Requirements

Minimum total expected workload equals 12 hours per week comprising:

(a.) Contact hours for on-campus students:

- Two hours of lectures
- One 2-hour tutorial

(b.) Additional requirements (all students):

- A minimum of 8 hours independent study per week for completing tutorial and project work, private study and revision.

Unit Relationships

Prohibitions

FIT4016

Prerequisites

((FIT5131 or FIT9017) and (FIT5134 or FIT9018) and (FIT5132 or FIT9003 or FIT9019) and (FIT5135 or FIT9020) and (FIT5136 or FIT4037) and (FIT5130 or FIT9030)) or equivalent
Introductory knowledge of computing at the undergraduate level is assumed.

Chief Examiner

Dr Nandita Bhattacharjee

Campus Lecturer

Caulfield

Nandita Bhattacharjee

Sepehr Minagar

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 the Student Evaluation of Teaching and Units (SETU) survey. 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, see:

www.monash.edu.au/about/monash-directions/ and on student evaluations, see:
www.policy.monash.edu/policy-bank/academic/education/quality/student-evaluation-policy.html

Previous Student Evaluations of this Unit

Students were very happy with the unit overall. Student feedback highlighted the following strengths:

- intellectually stimulating
- regular useful feedback
- tutorials and laboratory tasks
- assessments and assessment strategies
- active participation

This feedback can be used to strengthen the learning outcomes further by increasing the depth of some topics in cryptography.

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

Academic Overview

Learning Outcomes

At the completion of this unit students should be able to:

- critically assess threats, vulnerabilities and risks to an organisation's information assets, and propose control technologies and techniques which can be applied to reduce the security risk;
- apply a variety of cryptographic algorithms to develop methods to disguise information to ensure its integrity, confidentiality and authenticity;
- apply a variety of methods for key management and distribution and analyse the risks associated with the various approaches;
- implement user authentication and access control mechanisms to create a security architecture to protect the assets of the information system;
- implement cryptographic techniques to preserve the security of information and evaluate its effectiveness;
- apply a variety of security control technologies to IT systems in an organisation.

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 during the Week 4 Lecture
5	Examples of Private Key Encryption	
6	Introduction to number theory	
7	Public key cryptography	
8	Biometrics	Class Test 2 during the Week 8 Lecture
9	Integrity & non-repudiation	
10	Key management & distributed authentication	
11	Access Control	Assignment Presentation due Week 11 Tutorial
12	Risk Management	Class Test 3 during the Week 12 Lecture and Assignment Report due 3PM, 24 October 2014
	SWOT VAC	No formal assessment is undertaken in 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 learning system.

Teaching Approach

Lecture and tutorials or problem classes

This teaching and learning approach helps students to initially encounter information at lectures, discuss and explore the information during tutorials, and practice in a hands-on lab environment.

Assessment Summary

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

Assessment Task	Value	Due Date
Class Tests	20% (10% each, best 2 attempts out of 3)	Week 4, 8 and 12 Lectures
Group Assignment - Biometrics in Cryptography	20% (Report 14%, Presentation 6%)	Presentation due Week 11 Tutorial. Report due 3PM, 24 October 2014.

Unit Schedule

Examination 1	60%	To be advised

Assessment Requirements

Assessment Policy

Faculty Policy - Unit Assessment Hurdles
(http://intranet.monash.edu.au/infotech/resources/staff/edgov/policies/assessment-examinations/assessment-hurd

Academic Integrity - Please see resources and tutorials at
http://www.monash.edu/library/skills/resources/tutorials/academic-integrity/

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 of the three scores will constitute an assessment total of 20%.
  Weighting:
  20% (10% each, best 2 attempts out of 3)
  Criteria for assessment:

  1. Quality and accuracy of answers in response to test questions.
  2. How well underlying principles and theories are demonstrated in the student's answers.

  Due date:
  Week 4, 8 and 12 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. Students presentations on the assignment are due in Week 11 Tutorials. A comprehensive report is due in Week 12.
  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:

Presentation due Week 11 Tutorial. Report due 3PM, 24 October 2014.

Examinations

- **Examination 1**

Weighting:

60%

Length:

3 hours

Type (open/closed book):

Closed book

Electronic devices allowed in the exam:

None

Learning resources

Reading list

1. Cryptography and Network Security: Principles and Practice. William Stallings, 6th Edition, 2014. Prentice Hall.
2. Computer Security: Principles and Practice William Stallings and Lawrie Brown, 2012, Prentice Hall.
3. Security Engineering: A guide to building dependable distributed systems. Ross J. Anderson, 2nd Edition, 2008, John Wiley & Sons, Inc.

Monash Library Unit Reading List (if applicable to the unit)
http://readinglists.lib.monash.edu/index.html

Faculty of Information Technology Style Guide

Feedback to you

Examination/other end-of-semester assessment feedback may take the form of feedback classes, provision of sample answers or other group feedback after official results have been published. Please check with your lecturer on the feedback provided and take advantage of this prior to requesting individual consultations with staff. If your unit has an examination, you may request to view your examination script booklet, see
http://intranet.monash.edu.au/infotech/resources/students/procedures/request-to-view-exam-scripts.html

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

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

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.monash.edu.au/exams/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.

Assignment submission

It is a University requirement (http://www.policy.monash.edu/policy-bank/academic/education/conduct/student-academic-integrity-managing-pla 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). Please note that it is your responsibility to retain copies of your assessments.

Online submission

If Electronic Submission has been approved for your unit, please submit your work via the learning system for this unit, which you can access via links in the my.monash portal.

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: www.policy.monash.edu.au/policy-bank/academic/education/index.html

Key educational policies include:

- Student Academic Integrity Policy and Student Academic Integrity: Managing Plagiarism and Collusion Procedures ; http://www.policy.monash.edu/policy-bank/academic/education/conduct/student-academic-integrity-policy.h
- Assessment in Coursework Programs; 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.ht
- 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/dates/
- Orientation and Transition; http://intranet.monash.edu.au/infotech/resources/students/orientation/
- Academic and Administrative Complaints and Grievances Policy; http://www.policy.monash.edu/policy-bank/academic/education/management/complaints-grievance-policy.h

Faculty resources and policies

Important student resources including Faculty policies are located at http://intranet.monash.edu.au/infotech/resources/students/

Graduate Attributes Policy

http://www.policy.monash.edu/policy-bank/academic/education/management/monash-graduate-attributes-policy.h

Student Charter

www.opq.monash.edu.au/ep/student-charter/monash-university-student-charter.html

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 http://www.monash.edu.au/students. For Malaysia see http://www.monash.edu.my/Student-services, and for South Africa see http://www.monash.ac.za/current/.

Monash University Library

The Monash University Library provides a range of services, resources and programs that enable you to save time and be more effective in your learning and research. Go to www.lib.monash.edu.au or the library tab in my.monash portal for more information. At Malaysia, visit the Library and Learning Commons at http://www.lib.monash.edu.my/. At South Africa visit http://www.lib.monash.ac.za/.

Disability Liaison Unit

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://www.monash.edu/equity-diversity/disability/index.html
- Telephone: 03 9905 5704 to book an appointment with a DLO; or contact the Student Advisor, Student Commuity Services at 03 55146018 at Malaysia
- Email: dlu@monash.edu
- Drop In: Equity and Diversity Centre, Level 1, Building 55, Clayton Campus, or Student Community Services Department, Level 2, Building 2, Monash University, Malaysia Campus