MONASH University
Information Technology

FIT3031
Information and network security

Unit Guide

Semester 1, 2011

Last updated: 27 Feb 2011

Table of Contents

FIT3031 Information and network security - Semester 1, 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 2
- Gippsland 2
- South Africa 2

Tutors 2
- Caulfield 2

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

Previous Student Evaluations of this unit 4
Required Resources 4
Unit Schedule 4
Assessment Policy 5
Assessment Tasks 5
- Participation 5

Examinations 5
- Examination 1 6

Assignment submission 6
Extensions and penalties 6
Returning assignments 6
Policies 6
Student services 7

FIT3031 Information and network security - Semester 1, 2011

This unit will provide students with an understanding of: OSI security architecture; common information risks and requirements; operation of encryption techniques; digital signatures; public key infrastructure; authentication and non-repudiation; intrusion detection and response; firewall defence; privacy and ethics issues; security configurations to PC-based applications; and design of information systems with security compliance and security standards and protocols.

Mode of Delivery

- Caulfield (Day)
- South Africa (Day)

Contact Hours

2 hrs lectures/wk, 2 hrs laboratories/wk

Workload

For on campus students, workload commitments are:

- two-hour lecture and
- two-hour tutorial

  You will need to allocate up to 8 hours per week on average for personal study (study guide, textbook, lecture notes and tutorial), attending newsgroup discussion and working on assignments.

Unit Relationships

Prohibitions

CPE3001, CPE2007, CSE2500, GCO2831, FIT2058, FIT3018, FIT4028, GCO4831

Prerequisites

One of FIT1005, FIT1031, FIT1019, FIT2008, CSE2318, CSE3318 or GCO1815

Chief Examiner

Nandita Bhattacharjee

Campus Lecturer

Caulfield

Nandita Bhattacharjee

Gippsland

Joarder Kamruzzaman

South Africa

Oladayo Bello

Tutors

Caulfield

Abdul Malik Khan

Parman Sukarno

Li Wang

Learning Objectives

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

- describe OSI security architecture;
- describe common security standards and protocols for network security applications e.g. electronic mail, IP, web and network management;
- understand common information risks and requirements;
- explain the operation of conventional and public-key encryption techniques;
- describe the concepts and techniques for digital signatures, authentication and non-repudiation;
- understand privacy and ethics issues;
- appreciate the need for the digital certificates and public key infrastructure;
- appreciate the importance of system security against intruders and malicious software using firewalls;
- appreciate the relevance of privacy and ethics issues to organisations and individuals;
- apply simple security configurations to PC based applications e.g. email, Internet, computer administration;
- design information systems with security compliance.

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
Assignment 1	20%	15 April 2011
Assignment 2	20%	27 May 2011
Examination 1	60%	To be advised

Teaching Approach

Lecture and tutorials or problem classes

The teaching and learning approach provides facilitated learning, practical exploration and peer learning, equipping you with the ability to apply skills upon completion.

Feedback

Our feedback to You

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

- Informal feedback on progress in labs/tutes
- Graded assignments with comments
- Other: Solutions to tutes and labs will be discussed in class. Assignment feedback will be provided via comments.

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

Required Resources

The software used in this unit is available in public domain. The software is PGP encryption software which is available at:

http://www.pgpi.org/products/pgp/versions/freeware/win32

and

http://www.gpg4win.org/download.html

Unit Schedule

Week	Date*	Activities	Assessment
0	21/02/11		No formal assessment or activities are undertaken in week 0
1	28/02/11	OSI Security Architecture	
2	07/03/11	Symmetric Encryption	
3	14/03/11	Asymmetric Encryption	
4	21/03/11	Authentication Applications	
5	28/03/11	Web Security	
6	04/04/11	Wireless Security	
7	11/04/11	Electronic Mail Security	15 April 2011 (assignment 1 due)
8	18/04/11	IP Security	
Mid semester break			
9	02/05/11	Intrusion Detection and Response	
10	09/05/11	Malicious Software Attack	
11	16/05/11	Firewall Defence	
12	23/05/11	Network Management	27 May 2011 (assignment 2 due)
	30/05/11	SWOT VAC	No formal assessment is undertaken SWOT VAC

*Please note that these dates may only apply to Australian campuses of Monash University. Off-shore students need to check the dates with their unit leader.

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:
  Assignment 1
  Description:
  This assignment is designed to test students' understanding of symmetric and asymmetric cryptographic concepts and how they can be applied in real applications. This will be based on the topics covered in the first 6 weeks.
  Weighting:
  20%
  Criteria for assessment:
  Details in assignment specification.
  Due date:
  15 April 2011

- **Assessment task 2**

  Title:
  Assignment 2
  Description:
  This assignment is designed to test students' understanding of security protocols and standard practices, including wireless security. This will be based on the topics covered in Week 7-11.
  Weighting:
  20%
  Criteria for assessment:
  Details in assignment specification.
  Due date:
  27 May 2011

Examinations

- **Examination 1**

Weighting:
60%
Length:
3 hours
Type (open/closed book):
Closed book
Electronic devices allowed in the exam:
None

Assignment submission

Assignment coversheets are available via "Student Forms" on the Faculty website:
http://www.infotech.monash.edu.au/resources/student/forms/
You MUST submit a completed coversheet with all assignments, ensuring that the plagiarism declaration section is signed.

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

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.

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.

Reference Text

- W. Stallings, "Network Security Essentials: Applications and Standards", Pearson International, Fourth edition, 2010.

Recommended Text

- O. Poole, "Network Security - A Practical Guide", Butterworth Heinemann, 2003.
- J. H. Allen, "The CERT Guide to System and Network Security Practices", Addison-Wesley, 2001.
- M. Kaeo, "Designing Network Security : A Practical Guide to Creating a Secure Network Infrastructure", Cisco Press, 2004.
- R. Oppliger, "Security Technologies for the World Wide Web", Artech House, 2003.