MONASH University
Information Technology

FIT3031
Information and network security

Unit Guide

Semester 1, 2010

Last updated: 17 Feb 2010

Table of Contents

FIT3031 Information and network security - Semester 1, 2010

Chief Examiner:

Dr Joarder Kamruzzaman
Senior Lecturer
Phone: +61 3 990 26665

Lecturer(s) / Leader(s):

Caulfield

Dr Nandita Bhattacharjee
Senior Lecturer
Phone: +61 3 990 53293
Fax: +61 3 990 55159

Gippsland

Dr Joarder Kamruzzaman
Senior Lecturer
Phone: +61 3 990 26665

South Africa

Mr Oladayo Bello

Malaysia

Dr Simon Egerton

Introduction

Welcome to FIT3031, Information and Network Security, for semester 1, 2010. This is a 6-point compulsory unit for Business systems, Internet systems, Net-centric computing and Security major in the Bachelor of Information Technology and Systems degree. This unit is designed to provide you with the knowledge and understanding of various encryption techniques, common security threats ,e.g., email security, web security, malicious software attacks, different countermeasures to thwart those threats, intrusion detection and standard security practices, network management issues and firewalls deployment. On completion of this unit, you are expected to be confident in assessing security threats, employ possible countermeasures and be familiar with standard practices.

Unit synopsis

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.

Learning outcomes

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.

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

Prerequisites

One of FIT1005, FIT2008, CSE2318, CSE3318 or GCO1815

Prohibitions

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

Teaching and learning method

Teaching approach

This unit will be delivered via one 2-hr lecture and one 2-hr tutorial per week. Weekwise study guide, lecture notes and tutorial exercises will be made available to all students through the unit MUSO website. Lectures will provide students with the knowledge of fundamental theories and concepts. Tutorials will provide students with an opportunity to discuss and apply those concepts through exercises. Discussion forum on MUSO is for the students to discuss any topic related to this unit and to provide a forum that help you to achieve learning objectives.

Timetable information

For information on timetabling for on-campus classes please refer to MUTTS, http://mutts.monash.edu.au/MUTTS/

Tutorial allocation

On-campus students should register for tutorials/laboratories using the Allocate+ system: http://allocate.its.monash.edu.au/

Unit Schedule

Week	Date	Topic	Study guide	References/Readings	Key dates
1	01/03/10	OSI Security Architecture	SG1	Ch. 1 of Text book by W. Stallings	
2	08/03/10	Symmetric Encryption	SG2	Ch. 2 of text book	
3	15/03/10	Asymmetric Encryption	SG3	Ch. 3 of text book	
4	22/03/10	Authentication Applications	SG4	Ch. 4 of text book	
5	29/03/10	Electronic Mail Security	SG5	Ch. 5 of text book	
Mid semester break					
6	12/04/10	IP Security	SG6	Ch. 6 of text book	
7	19/04/10	Web Security	SG7	Ch. 7 of text book	April 19, 2010 (assignment 1 due)
8	26/04/10	Wireless Security	SG8	Web resources	
9	03/05/10	Network Management	SG9	Ch. 8 of text book	
10	10/05/10	Intrusion Detection and Response	SG10	Ch. 9 of text book	
11	17/05/10	Malicious Software Attack	SG11	Ch. 10 of text book	May 21, 2010 (assignment 2 due)
12	24/05/10	Firewall Defence	SG12	Ch. 11 of text book	
13	31/05/10	Revision			

Unit Resources

Prescribed text(s) and readings

Prescribed Text

- S. William, "Network Security Essentials - Applications and Standards", 3rd Edition, Prentice Hall, 2007.

Text books are available from the Monash University Book Shops. Availability from other suppliers cannot be assured. You are advised to purchase your text book early.

Recommended text(s) and readings

Reference Text

- O. Poole, "Network Security - A Practical Guide", Butterworth Heinemann, 2003.

Recommended Text

- 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.

Required software and/or hardware

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

Equipment and consumables required or provided

Students may use the facilities available in the computing labs. Information about computer use for students is available from the ITS Student Resource Guide in the Monash University Handbook. You will need to allocate up to **5** hours per week for use of a computer, including time for newsgroups/discussion groups.

Study resources

Study resources we will provide for your study are:

The following course materials will be provided in **on-line format** in MUSO:

- Unit Information guide

- Unit Book divided into twelve study guides
- Lecture notes and tutorial materials on weekly basis
- Assignment 1 and Assignment 2
- Sample examination paper with sample solution
- A range of reference materials on the World Wide Web

Assessment

Overview

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

Faculty 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.

The unit is assessed with two assignments and a three hour closed book examination. 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 44% then a mark of 44-N will be recorded for the unit.

Assignment tasks

Assignment coversheets

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.

Assignment submission and return procedures, and assessment criteria will be specified with each assignment.

- **Assignment task 1**

  Title:
  Assignment 1
  Description:
  This assignment is designed to test students' understating 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%
  Due date:

April 19, 2010

- **Assignment task 2**

Title:
Assignment 2
Description:
This assignment is designed to test students' understating of security protocols and standard practices, including wireless security. This will be based on the topics covered in Week 7-11.
Weighting:
20%
Due date:
May 21, 2010

Examination

- **Weighting:** 60%
  Length: 3 hours
  Type (open/closed book): Closed book

See Appendix for End of semester special consideration / deferred exams process.

Due dates and extensions

Please make every effort to submit work by the due dates. It is your responsibility to structure your study program around assignment deadlines, family, work and other commitments. Factors such as normal work pressures, vacations, etc. are not regarded as appropriate reasons for granting extensions. Students are advised to NOT assume that granting of an extension is a matter of course.

Students requesting an extension for any assessment during semester (eg. Assignments, tests or presentations) are required to submit a Special Consideration application form (in-semester exam/assessment task), along with original copies of supporting documentation, directly to their lecturer within two working days before the assessment submission deadline. Lecturers will provide specific outcomes directly to students via email within 2 working days. The lecturer reserves the right to refuse late applications.

A copy of the email or other written communication of an extension must be attached to the assignment submission.

Refer to the Faculty Special consideration webpage or further details and to access application forms: http://www.infotech.monash.edu.au/resources/student/equity/special-consideration.html

Late assignment

It is your responsibility to structure your study program around assignment deadlines, family, work and other commitments. Factors such as normal work pressures, vacations, etc. are seldom regarded as appropriate reasons for granting extensions.

Assignments submitted after the due date will be accepted only in exceptional circumstances. If an assignment will be late, it is necessary to contact the unit adviser of your campus at least 2 days before

the due date. You may be required to provide documentation to support a request for late submission. There may be a penalty of 3% for each day of late submission if not approvaed before due date.

Return dates

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

Appendix

Please visit the following URL: http://www.infotech.monash.edu.au/units/appendix.html for further information about:

- Continuous improvement
- Unit evaluations
- Communication, participation and feedback
- Library access
- Monash University Studies Online (MUSO)
- Plagiarism, cheating and collusion
- Register of counselling about plagiarism
- Non-discriminatory language
- Students with disability
- End of semester special consideration / deferred exams