MONASH University

FIT1019
Introduction to security

Unit Guide

Semester 2, 2009

Last updated : 14 Jul 2009

Table of Contents

FIT1019 Introduction to security - Semester 2, 2009

Chief Examiner:

Professor Balasubramaniam Srinivasan
Professor, and Head of School
Phone: +61 3 990 31333 +61 3 990 55222
Fax: +61 3 990 55157

Lecturer(s) / Leader(s):

Caulfield

Mr Osama Dandash
Fax: Fax: + 6 13 990 32400

Introduction

Welcome to FIT1019 Introduction to Security, semester 2, 2008. This 6 point unit is a core to Security Major of BITS degree. The unit has been designed to provide overview of the current issues and possible solutions in implementing security in an organisation.

Unit synopsis

This is the primary introductory unit for the IT security major in the BITS. This provides students with grounding in general areas of security to support the major. This is a feeder unit into the selected security units in the major. It combines some of the topics from IMS3110, MMS1002 and BUS2050 but does not replace these units.

Learning outcomes

At the completion of this subject students should have knowledge and understanding and be able to analyse:

1. The importance of information systems security issues to contemporary organisations;
2. Information security concepts and philosophies;
3. Threats, vulnerabilities and risks to an organisations' information assets and the control technologies and techniques required to support this;
4. Understanding of the mathematical foundation of cryptoanalysis;
5. The ethical, legal and criminal issues relating to the security of information systems;
6. Evalute current and future developments and trends in security control technologies and techniques;
7. the relevance of human factors to information security planning and management.

At the completion of this subject students should have developed attitudes which allow them to:

1. Adopt a critical approach to the analysis and design of information systems security systems;
2. Willingness to apply ethical standards of security issues;
3. Demonstrate ethically sound viewpoints with respect to the protection of information resources while maintaining a secure IS framework, specifically related to (but not limited to) the goals of security such as confidentiality, integrity, and availability, in the professional development of information systems;
4. cooperate within groups and adopt and practise professional ethics that influence work behaviour.

At the completion of this subject students should have the skills to:

1. Apply information security concepts in the analysis of information systems security issues;
2. Apply risk management techniques to the planning and management of information systems security systems;
3. Apply security analysis and design methods and techniques in the analysis of threats, risk and vulnerabilities to an information system;
4. Apply the security concept in securing information systems by exploring the security mechanism available in the operating systems environment.

Students may be required to work in teams to complete some of the assessment and thus must develop appropriate interpersonal communication and leadership skills.

Contact hours

Lecture/seminar: 2hrs/week, tutorial: 1hr/week

Workload

You will need to participate in the following activties:

- two-hours lecture
- two-hours laboratory
- a minimum of 6-8 hours of personal study to prepare for the lecture, laboratory and completing assignments.

Unit relationships

Relationships

FIT1019 is a core unit in the secuirty major of the BITS.

Teaching and learning method

The lectures will cover the theoretical concepts of security. The laboratory will be used to explore the current available security tools and operating system platforms. The exploration aim to demonstrate and illustrate the concepts provided in the lectures.

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.cc.monash.edu.au/

Unit Schedule

Week	Topic	Key dates
1	Introduction	
2	Building Blocks of IT Security	
3	Access Control	
4	Identity Management	
5	Authentication	UNIX Test 1, tutorials
6	Math for Cryptography I	
7	Math for Cryptography II	Unit Test 2, lecture
8	Introduction to Cryptography	
9	Public Key Encription	
10	Digital Signature	
Mid semester break		
11	Overview of Network Security	Assignment1 Due, Presentation
12	Ethics and Privacy	Presentation
13	Revision	

Unit Resources

Prescribed text(s) and readings

Jill Slay and Andy Koronios, "Information Technology Security & Risk Managamenr", 3rd edition, Wiley.

Recommended text(s) and readings

Pfleeger, C.P and Pfleeger, S.L, Security in Computing, 3rd edition, Prentice Hall

Anderson, R. (2001). Security Engineering. London: John Wiley & Sons. Bosworth, S. & Kabay, M.E. (Eds.).(2002).

Gollmann, D. (2006), Computer Security, Wiley, UK

Required software and/or hardware

No special software is required.

Equipment and consumables required or provided

N/A

Study resources

Study resources we will provide for your study are:

Study resources can be found in the unit website that can be accessed through MUSO.

Assessment

Overview

Assignments: 40%
Formal supervised assessment 50%
Presentations: 10%

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 44% then a mark of no greater than 44-N will be recorded for the unit.

For this unit you must attain the following to pass overall:

- 50% overall and
- at least 40% of the available marks in during-semester assessments and end-of-semester assessment (exam).

In the situation whereby you fail to meet the 40% rule, the final mark that will be published is the mark of the assessment that failed to meet the 40% rule.

For example, a final mark of 38 will be awarded to a student who receives an average of 70% from all assignments and 38% on the exam.

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:
  Unit Test 1: UNIX and Access Control
  Description:
  Practical test on UNIX commands
  Weighting:
  10%
  Due date:

Tutorial classes in week 4

- **Assignment task 2**

Title:
Unit Test 2
Description:
Mid-semester test. Multiple choice questions on the materials covered up to week 6.
Weighting:
10%
Due date:
Lecture in week 7

- **Assignment task 3**

Title:
Assignment 1: Security Topic
Description:
3000 words essay/report on security topics. The topics with associated reading lists will be provided in week 3. The assignment will be conducted in a group of 2 students.
Weighting:
20%
Due date:
Week 11

- **Assignment task 4**

Title:
Presentation
Description:
Presentation on assignment 1 submission
Weighting:
10%
Due date:
Week 11 and 12 tutorials

Examination

- **Weighting:** 50%
  Length: 2 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

Assignments received after the due date will be subject to a penalty of **10% per-day (including weekend).** Assignment **will not be accepted** after the cut off date that usually set **one week after the 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