MONASH University
Information Technology

FIT1019
Introduction to security

Unit Guide

Semester 2, 2010

Last updated: 10 Jul 2010

Table of Contents

FIT1019 Introduction to security - Semester 2, 2010 1
Chief Examiner: 1
Lecturer(s) / Leader(s): 1
Caulfield 1
Introduction 2
Unit synopsis 2
Learning outcomes 2
Contact hours 3
Workload 3
Unit relationships 3
Teaching and learning method 4
Teaching approach 4
Timetable information 4
Tutorial allocation 4
Unit Schedule 4
Improvements to this unit 5
Unit Resources 6
Prescribed text(s) and readings 6
Recommended text(s) and readings 6
Required software and/or hardware 6
Equipment and consumables required or provided 6
Study resources 6
Assessment 7
Overview 7
Faculty assessment policy 7
Assignment tasks 7
Examination 8
Due dates and extensions 8
Late assignment 9
Return dates 9
Feedback 9
Appendix 10

FIT1019 Introduction to security - Semester 2, 2010

Chief Examiner:

Professor Balasubramaniam Srinivasan
Professor
Phone: +61 3 990 31333 +61 3 990 55333
Fax: +61 3 990 31077

Lecturer(s) / Leader(s):

Caulfield

Professor Balasubramaniam Srinivasan
Professor
Phone: +61 3 990 31333 +61 3 990 55333
Fax: +61 3 990 31077

Introduction

Welcome to FIT1019 Introduction to Security, semester 2, 2010. This 6 point unit is a core to Security Major of BITS degree. The unit has been designed to provide an overview of the current issues and possible solutions in implementing security in an organisation.

Unit synopsis

This unit will provide students with a knowledge of information systems security issues, and their relevance to the management of information systems in contemporary organisations. The students will gain knowledge of the nature of information threats, risks and vulnerabilities and of the control technologies and techniques which can be applied to reduce risk. Students will be expected to demonstrate ethically sound viewpoints with respect to the protection of information resources while maintaining a secure IS framework related to a defence in depth strategy. Further students will have an understanding of the ethical, legal and criminal issues relating to the security of information systems. Additionally students will be required to analyse and assess recent developments and future trends in IS security technologies.

Learning outcomes

At the completion of this unit students will have -
A knowledge and understanding of:

- the importance of information systems security issues to contemporary organisations;
- information security concepts and philosophies;
- threats, vulnerabilities and risks to an organisations information assets and the control technologies and techniques required to support this;
- the mathematical foundation of cryptoanalysis;
- the ethical, legal and criminal issues relating to the security of information systems;
- how to evaluate current and future developments and trends in security control technologies and techniques;
- the relevance of human factors to information security planning and management.

Developed attitudes that enable them to:

- adopt a critical approach to the analysis and design of information systems security systems;
- willingness to apply ethical standards of security issues;
- 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;
- cooperate within groups and adopt and practise professional ethics that influence work behaviour.

Developed the skills to:

- apply information security concepts in the analysis of information systems security issues;
- apply risk management techniques to the planning and management of information systems security systems;
- apply security analysis and design methods and techniques in the analysis of threats, risk and vulnerabilities to an information system; and
- apply the security concept in securing information systems by exploring the security mechanism

available in the operating systems environment.

Demonstrated the communication skills necessary to:

- work in teams to complete some of the assessment and thus develop appropriate interpersonal communication and leadership skills.

Contact hours

2 hrs lectures/wk, 2 hrs tutorials/wk

Workload

You will need to participate in the following activties:

- two-hours lecture
- two-hours tutorial/discussion class
- a minimum of 6-8 hours of personal study to prepare for the lecture, discussion classes and quizzes.

Unit relationships

Teaching and learning method

Teaching approach

The lectures will cover the theoretical concepts of security. The tutorial/discussion classes will be used to explore the principles, available tools and operating system platforms. The exploration aims 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.its.monash.edu.au/

Unit Schedule

Week	Date*	Topic	Key dates
1	19/07/10	Introduction	
2	26/07/10	Building Blocks of IT Security	
3	02/08/10	Access Control	Discussion Class Quiz 1
4	09/08/10	Identity Management	
5	16/08/10	Authentication	Discussion Class Quiz 2
6	23/08/10	Math for Cryptography I	
7	30/08/10	Math for Cryptography II	Discussion Class Qui 3
8	06/09/10	Introduction to Cryptography	
9	13/09/10	Public Key Encription	Discussion Class Quiz 4
10	20/09/10	Digital Signature	Mid Semester Test
Mid semester break			
11	04/10/10	Overview of Network Security	
12	11/10/10	Ethics and Privacy	Discussion Class Quiz 5
13	18/10/10	Revision	

*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.

Improvements to this unit

Relevant materiasl from various books has been scanned by Monash Library Servicesa and be accessed as a reading list from the following web site:
http://lib.monash.edu/non-cms/resourcelists/f/fit1019.html.

Unit Resources

Prescribed text(s) and readings

Reading list is available through Monash Library - access through the web page:http://lib.monash.edu/non-cms/resourcelists/f/fit1019.html.

Recommended text(s) and readings

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

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

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, except access to the unit sever though the internet, both on comapus and from home.

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

Examination (2 hours): 50%; In-semester assessment: 50%

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.

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 submission and preparation requirements will be detailed in each assignment specification. 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.

- **Assignment task 1**

  Title:
  Tutorial Quizzes 1-5
  Description:
  Priciples and applications of the previous (week's) topic.
  Weighting:
  25%
  Criteria for assessment:

  - understanding of the appropriate security priciples and
  - its applications to specific situations.

  Due date:
  In the tutorials session itself

- **Assignment task 2**

Title:
Mid Semester Test
Description:
Mid-semester test. Multiple choice questions on the materials covered up to week 8.
Weighting:
25%
Criteria for assessment:

- demonstrate the mastery of the topics covered up to week 8 by choosing the right answer to multiple choice questions.

Due date:
In the Tutorial Class in Week 10

Examination

-
Weighting:
50%
Length:
2 hours
Type (open/closed book):
Closed book
Electronic devices allowed in the exam:
None

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.

Feedback

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

Solutions to tutes, labs and assignments

Individual student meetings.

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