



MONASH University
Information Technology

FIT3105
Security and identity management

Unit Guide

Semester 1, 2010

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: 19 Feb 2010

Table of Contents

FIT3105 Security and identity management - Semester 1, 2010	1
<u>Chief Examiner:</u>	1
<u>Lecturer(s) / Leader(s):</u>	1
<u>Caulfield</u>	1
<u>Additional communication information:</u>	1
<u>Introduction</u>	2
<u>Unit synopsis</u>	2
<u>Learning outcomes</u>	2
<u>Contact hours</u>	2
<u>Unit relationships</u>	2
<u>Prerequisites</u>	2
<u>Teaching and learning method</u>	3
<u>Teaching approach</u>	3
<u>Timetable information</u>	3
<u>Tutorial allocation</u>	3
<u>Unit Schedule</u>	3
<u>Unit Resources</u>	4
<u>Prescribed text(s) and readings</u>	4
<u>Recommended text(s) and readings</u>	4
<u>Equipment and consumables required or provided</u>	4
<u>Study resources</u>	4
<u>Assessment</u>	5
<u>Overview</u>	5
<u>Faculty assessment policy</u>	5
<u>Examination</u>	5
<u>Due dates and extensions</u>	5
<u>Late assignment</u>	6
<u>Return dates</u>	6
<u>Appendix</u>	7

FIT3105 Security and identity management - Semester 1, 2010

Chief Examiner:

None provided

Lecturer(s) / Leader(s):

Caulfield

Dr Phu Le

Lecturer

Phone: +61 3 990 32399

Fax: +61 3 990 31077

Additional communication information:

Dr Phu Dung Le, Room H.706, Phone: (03) 9903 2300, email: pdle@infotech.monash.edu.au

Introduction

Welcome to Security and Identity Management (FIT3105)!

This unit will be a core unit in the Security major of BITS. It can be an elective unit for students who do not major in security (subject to the approval from the school). This unit will provide students with system authentication and identity management based on different technologies such as crypto-based technology, smart cards, biometrics, etc.

Unit synopsis

Introduces students to current theory and practice of authentication and identity management. This includes authentication and identity management of system components (software, hardware, data and users); Biometric based Identification systems; Smart card based Identification systems; Crypto-based Identification systems; Kerberos authentication systems; Large population ID management and security; Privacy, security, and efficiency of identification systems.

Learning outcomes

At the completion of this unit students will:

- understand the importance of authentication of system components: data, software, hardware, users and subsystems;
- understand the implementation of different techniques for authentication and identification;
- understand the significance of authentication and identity management in IT security
- understand different authentication and identity management systems;
- understand the role of biometric, smartcards, crypto-based techniques and their issues when applied to authentication process;
- understand existing networked authentication models and protocols for distributed systems, such as kerberos;
- appreciate the role of distributed authentication models and protocols in securing electronic transactions;
- practically gain the experience of system applications identification and authentication;
- practically gain the experience of users identification and authentication;
- practically gain the experience of crypto-based authentication and identification techniques for users, system software and applications;
- practically gain the experience of identifying and authenticating network and system components.

Contact hours

2 hrs lectures/wk, 2 hrs laboratories/wk

Unit relationships

Prerequisites

FIT1019 or equivalent

Teaching and learning method

Teaching approach

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	01/03/10	Introduction to authentication and identity management	
2	08/03/10	Cryptography for authentication and identification	
3	15/03/10	Smart card based authentication and identity systems	
4	22/03/10	Biometric technology for authentication and identification	
5	29/03/10	Crypto-based identity management systems	
Mid semester break			
6	12/04/10	Strong authentication for computer system components and mobile users	
7	19/04/10	Authentication and identity systems: design and implementation	
8	26/04/10	Authentication and identity systems: design and implementation (con't)	Assignment 1 due on Friday 4PM.
9	03/05/10	Large scale identity systems: security, privacy and efficiency	
10	10/05/10	Large scale identity systems: security, privacy and efficiency (con't)	
11	17/05/10	Identity systems: Case study	
12	24/05/10	Research in authentication and identity management technologies	Assignment 2 due on Friday 4PM.
13	31/05/10	Reading and 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.

Unit Resources

Prescribed text(s) and readings

There is no text book for this unit.

Text books are available from the [Monash University Book Shops](#). Availability from other suppliers cannot be assured. The Bookshop orders texts in specifically for this unit. You are advised to purchase your text book early.

Recommended text(s) and readings

Recommended books, articles, and Internet resources will be advised.

Equipment and consumables required or provided

Students studying off-campus are required to have the minimum system configuration specified by the Faculty as a condition of accepting admission, and regular Internet access. On-campus students, and those studying at supported study locations 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 **12** 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:

- Weekly detailed lecture notes outlining the learning objectives, discussion of the content, required readings and exercises;
- Weekly tutorial or laboratory tasks and exercises;
- Assignment specifications;
- Consultations at specific consultation times;

Assessment

Overview

Examination (3 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.

There will be two individual assignments (20% each) and lab exercises (10%). There will be a 3-hour exam. You will have to

complete all the lab exercises attempt both assignments and the examination achieve no less than 40% of the possible marks in the exam achieve no less than 50% of possible marks

Examination

- **Weighting:** 50%
- **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

Assignments received after the due date will be subject to a penalty of 10% for one day late, 20% for two days late, 40% for three days late, 80% for four days late and 100% for five or more days late.

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