MONASH University
Information Technology

FIT5037
Advanced network security

Unit Guide

Semester 2, 2011

Last updated: 22 Aug 2011

Table of Contents

FIT5037 Advanced network security - Semester 2, 2011

This unit aims to provide students with an advanced knowledge of network security. Topics to be covered include the design and implementation of some important public key systems: RSA and Elliptic Curve algorithms; concepts of quantum cryptography; quantum computing and cryptography; wireless computing and cryptography; design, implementation and configuration of firewalls in depth; design, implementation and configuration of intrusion detection systems; prevention systems; advanced network security architectures; advanced wireless security: principle and practice; security in trusted-based computing environments; and quantum cryptography.

Mode of Delivery

Caulfield (Evening)

Contact Hours

2 hrs lectures/wk, 2 hrs laboratories/wk

Workload

Workload commitments per week are:

Two-hour lecture, two-hour tutorial (or laboratory) requiring preparation in advance, and a minimum of 2 hours of personal study per one-hour of contact time in order to satisfy the reading and assignment expectations.

Unit Relationships

Prohibitions

CPE5021

Prerequisites

FIT5044

Chief Examiner

Dr Phu Le

Campus Lecturer

Caulfield

Phu Dung Le

Contact hours: Wednesday 8pm - 10pm

Academic Overview

Learning Objectives

At the completion of this unit students will:

- understand the design and implementation of advanced cryptographic algorithms for wired and wireless computing environments including the design and implementation of RSA and ECC;
- achieve sound knowledge of network security components including the design, implementation, and configuration of Firewalls, Intrusion Detection Systems (static and dynamic checking of programs, anomaly detection, large-scale (Internet-wide) distributed intrusion detection, early sensing, complex attack scenario analysis, and automated response), Prevention Systems, Firewalls, IDSs, VPNs and prevention systems together;
- develop knowledge of advanced network security architectures to allow better network protection, load balancing and recovery from attacks;
- achieve sound knowledge of wireless network security;
- understand security in trusted-based computing environments;
- understand Quantum cryptography.

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

Assignments: 40%; Lab exercises and group assignments: 30%; Theoretical test: 30%

Assessment Task	Value	Due Date
Assignment 1 - (individual work)	40%	4pm Friday Week 8
Assignment 2 - Intrusion Detection System (group work)	15%	4pm Friday Week 10
Assignment 3 - System Vulnerabilities and Penetration Testing (group work)	15%	4pm Friday Week 14
Theoretical test	30%	Week 12 Lecture

Teaching Approach

Lecture and tutorials or problem classes

This teaching and learning approach provides facilitated learning, practical exploration and peer learning.

Feedback

Our feedback to You

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

- Informal feedback on progress in labs/tutes

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

Removable hard drives and Scientific Linux software will be provided at the labs.

Unit Schedule

Week	Activities	Assessment
0		No formal assessment or activities are undertaken in week 0
1	Modern computing and network security	
2	Design and implementation of RSA	
3	Introduction to ECC	
4	ECC design and implementation	
5	Introduction to intrusion detection systems	
6	Networked and distributed software security	
7	Networked and distributed software security (con't)	
8	Advanced wireless network security	Assignment 1 due 4pm Friday Week 8
9	Large computer system security	
10	Computer system security and performance	Assignment 2 due 4pm Friday Week 10
11	Advanced theories and network security approaches	
12	Theoretical test	Theoretical test in Week 12 Lecture; Assignment 3 due 4pm Friday Week 14
	SWOT VAC	No formal assessment is undertaken SWOT VAC
	Examination period	LINK to Assessment Policy: http://policy.monash.edu.au/policy-bank/academic/education/assessment/assessment-in-coursework-policy.html

*Unit Schedule details will be maintained and communicated to you via your MUSO (Blackboard or Moodle) learning system.

Assessment Requirements

Assessment Tasks

Participation

There is an individual assignment (40%) and two group assignments (15% each) and a theoretical test (30%)

- **Assessment task 1**

  Title:
  Assignment 1 - (individual work)
  Description:
  Choose one of the two options:

  Option 1 - You are required to design and implement the RSA and ECC public key systems using C or C++ or Java.
  Option 2 - You are required to study the Linux kernel source code and make changes so that all programs will be checked before they are executed.

  More details will be provided on the assignment specification.
  Weighting:
  40%
  Criteria for assessment:
  You have to demonstrate your understanding of the algorithms you will implement. The security analysis of your implementation will be required in your report and a correct analysis will give you 40% of the total marks. If your code works and reflects the theory of RSA and ECC, this will give you another 40%. Your correct demonstration and answers to interview questions will give you the final 20% of the marks.
  Due date:
  4pm Friday Week 8

- **Assessment task 2**

  Title:
  Assignment 2 - Intrusion Detection System (group work)
  Description:
  You are required to install, configure and test a Intrusion Detection System using Snort.

  More details will be provided on the assignment specification.
  Weighting:
  15%
  Criteria for assessment:
  If you install and configure Snort and system services correctly you will be given 20% of the total marks. Providing correctly written rules with complete documentation will give you another 40% of the marks. Your demonstration of your rules with complete tests and answers to interview questions will give you the final 40% of the marks.

  Since it is a group assignment, every member of your group will be interviewed and marks will be equally given.
  Due date:

4pm Friday Week 10

- **Assessment task 3**

Title:

Assignment 3 - System Vulnerabilities and Penetration Testing (group work)

Description:

You are required to to the following tasks:

1. find at least three vulnerabilities in computer systems,

2. work out possible attacks on those vulnerabilities with demonstrations for each attack,

3. write a detailed report to describe the problems which cause the vulnerabilities, analyse the security and describe the possible attacks with step-by-step demonstrations for each attack, then suggest solutions to solve the problems.

More details will be provided on the assignment specification.

Weighting:

15%

Criteria for assessment:

If you can find the vulnerabilities of the system you are working with, describe them correctly in your report and clearly understand the problems, this will give you 30% of the total marks. Your demonstration with possible attacks will give you another 40% of the marks and your proposed security solutions will give you the remaining 30% of the marks if they are correct.

Since it is a group assignment, every member of your group will be interviewed and marks will be equally given.

Due date:

4pm Friday Week 14

- **Assessment task 4**

Title:

Theoretical test

Description:

The theoretical test will evaluate your understanding of the theories covered in the unit. It is an open book and questions are multiple choice. You will have to study all the materials delivered in the lectures and tutorials.

Weighting:

30%

Criteria for assessment:

Correct answers to questions (demonstrates understanding of the material learned).

Due date:

Week 12 Lecture

Examinations

Assignment submission

It is a University requirement (http://www.policy.monash.edu/policy-bank/academic/education/conduct/plagiarism-procedures.html) for students to submit an assignment coversheet for each assessment item. Faculty Assignment coversheets can be found at http://www.infotech.monash.edu.au/resources/student/forms/. Please check with your Lecturer on the submission method for your assignment coversheet (e.g. attach a file to the online assignment submission, hand-in a hard copy, or use an online quiz).

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

Other Information

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.
- Codes of Practice for Teaching and Learning (http://www.policy.monash.edu.au/policy-bank/academic/education/conduct/suppdocs/code-of-practice-tea

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.