MONASH University
Information Technology

FIT5037
Advanced network security

Unit Guide

Semester 2, 2010

Last updated: 13 Jul 2010

Table of Contents

FIT5037 Advanced network security - Semester 2, 2010

Chief Examiner:

Dr Phu Le
Lecturer
Phone: +61 3 990 32399
Fax: +61 3 990 31077

Contact hours: 12PM - 14PM Thursday

Lecturer(s) / Leader(s):

Caulfield

Dr Phu Le
Lecturer
Phone: +61 3 990 32399
Fax: +61 3 990 31077

Contact hours: 12PM - 14PM THURSDAY

Unit synopsis

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.

Learning outcomes

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.

Contact hours

2 hrs lectures/wk, 2 hrs laboratories/wk

Workload

- two-hour lecture and
- two-hour tutorial (or laboratory) (requiring advance preparation)
- a minimum of 6 hours of personal study per one hour of contact time in order to satisfy the reading and assignment expectations.
- You will need to allocate up to 8 hours per week in several weeks, for use of a computer, including time for group and individual assignments.

Unit relationships

Prerequisites

FIT5044

Prohibitions

CPE5021

Teaching and learning method

Teaching approach

Teaching methods are done by conducting lectures and lab exercises. Lab exercises include network set-up and configurations, Intrusion Detection with Snortl set-up and configurations. Students will attend a two hour lecture and a two hour tutorial or lab per week. The lectures will provide students with the fundamental theories. The practical assignments and lab series will provide students with the opportunity to implement the theories, develop research and problem solving knowledge, and gain practical skills. The test will verify students' understanding of the theory.

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	Advanced topics of Modern Computing and Network Security	
2	26/07/10	Advanced Cryptography	
3	02/08/10	Elliptic Curve Public Key System	
4	09/08/10	Design and Implementation of RSA and ECC	
5	16/08/10	Advanced techniques in firewalls	
6	23/08/10	Intrusion Detection Systems: Concepts, Design, and Implementation	
7	30/08/10	Wireless Security: Principles and Practices	
8	06/09/10	Security, Load Balancing and Network Performance	individual assignments due at 4PM Friday
9	13/09/10	Wireless Security	Group assignment - Part I (IDS system) due
10	20/09/10	Security, Load Balancing and Network Performance	
Mid semester break			
11	04/10/10	Network Security and Quantum Theory	
12	11/10/10	Reading in Network Security	Group assignment - Part II (vulnerabilities and attacks) due
13	18/10/10	Research Discussion	

*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

N/A

There is no specific textbook for this unit.

Recommended text(s) and readings

- Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security - Private Communication in a Public World, 2nd Edition, Prentice Hall, 2002. ISBN 0-13-046019-2.
- William Stallings, Cryptography and Network Security: Principles and Practices, Prentice-Hall, 2000. ISBN 0-13-016093-8.
- Michael Howard and David LeBlanc, Writing Secure Code, Microsoft Press, 2002. ISBN 0-7356-1588-8.
- Greg Holden, Guide to Firewalls and Network Security Intrusion Detection and VPNs, Thomson, ISBN: 0-619-13039-3.
- Robert L. Ziegler, Linux Firewalls, New Riders, ASIN: 0735709009.
- Greg Holden, Guide to Network Defense and Counter Measures, Thomson, ISBN: 0-619-13124-1.
- Jack Kozoil, Intrusion Detection with Snort, SAMS, 157870281x.
- Stephen Nortcutt, Network Intrusion Detection System: A analyst?s Handbook, Que, ASIN: 0735708681.
- Adam Engst and Glenn Fleishman, The wireless Networking Starter Kit, Peachpit Press, ISBN: 0321174089.
- Cyrus Peikari, Seth Fogie, Maximum Wireless Security, SAMS, ISBN: 0672324881.

Required software and/or hardware

Linux OS, Squid, Snore IDS, PGP/GPG, Java. The software is available at the lab.

Equipment and consumables required or provided

Network cables and removable hard-drives are provided at the lab.

Study resources

Study resources we will provide for your study are:

lecture slides, weekly tutorial requirements, assignment specifications will be posted on the unit webpage.

Assessment

Overview

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

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.

All works except the theoretical test will be interviewed. All the assessments are based on how much students understand their works. If a student can't demonstrate her/his understanding of the work. The student will get the lowest mark: ZERO.

Students have to do the theoretical test and all the assignments and have to get an overall unit mark of 50% to pass the subject.

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:
  Individual Assignments
  Description:
  You are required to design and implement the RSA and ECC public key systems using C or C++ or Java.
  Weighting:
  40%
  Criteria for assessment:

The entire group will be assessed as a group.

You need to be able to understand the theory and demonstrate your practical work to your tutor. If you fail to understand what you have done you will get Zero for the assignment.

If you can demonstrate your practical work but do not completely understand the theory, you will get a Pass at the maximum.

If you can demonstrate your practical work but understand 25% of the theory, you will get a Credit as the maximum.

If you can demonstrate your practical work and understand 50% of the theory, you will get a Distinction as the maximum.

If you can demonstrate your practical work and understand the theory well, you will get a High Distinction.

Due date:

4PM FRI - WEEK 8

- **Assignment task 2**

Title:

System vulnerabilities and penetration testing (group assignment)

Description:

You are required to find at least three vulnerabilities in your own system and practically work out possible attacks. You are required to demonstrate and write a detailed report to describe your work.

Weighting:

15%

Criteria for assessment:

The entire group will be assessed as a group.

Due date:

4PM - Friday - Week 12

- **Assignment task 3**

Title:

Intrusion detection system (group assignment)

Description:

1. Install, configure and experiment the Intrusion Detection System Snort.

2. Identify the vulnerabilities of your computer system and find at least three possible attacks.

Weighting:

15%

Criteria for assessment:

The entire group will be assessed as a group.

You need to be able to understand the theory and demonstrate your practical work to your tutor. If you fail to understand what you have done you will get Zero for the assignment.

If you can demonstrate your practical work but do not completely understand the theory, you will get a Pass at the maximum.

If you can demonstrate your practical work but understand 25% of the theory, you will get a Credit as the maximum.

If you can demonstrate your practical work and understand 50% of the theory, you will get a Distinction as the maximum.

If you can demonstrate your practical work and understand the theory well, you will get a High Distinction.

The tutor can interview any member of your group and all members have the same responsibility and marks.

Due date:

4PM FRI - WEEK 9

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