# Table of Contents

FIT5037 Advanced network security - Semester 2, 2009

- Chief Examiner: ........................................................................................................... 1
- Lecturer(s) / Leader(s): ............................................................................................... 1
  - Caulfield ..................................................................................................................... 1

## Unit synopsis ................................................................................................................. 2

## Learning outcomes ....................................................................................................... 2

## Contact hours ................................................................................................................. 2

## Workload ....................................................................................................................... 2

## Unit relationships ......................................................................................................... 2
  - Prerequisites ............................................................................................................... 2
  - Prohibitions ............................................................................................................... 2
  - Relationships ............................................................................................................ 3

## Teaching and learning method ...................................................................................... 4
  - Timetable information .............................................................................................. 4
  - Tutorial allocation .................................................................................................... 4
  - Unit Schedule .......................................................................................................... 4

## Unit Resources ............................................................................................................. 5
  - Prescribed text(s) and readings .............................................................................. 5
  - Recommended text(s) and readings ....................................................................... 5
  - Required software and/or hardware ....................................................................... 5
  - Equipment and consumables required or provided ............................................... 5
  - Study resources ....................................................................................................... 5

## Assessment .................................................................................................................. 6
  - Overview .................................................................................................................. 6
  - Faculty assessment policy ...................................................................................... 6
  - Assignment tasks ...................................................................................................... 6
  - Due dates and extensions ......................................................................................... 7
  - Late assignment ........................................................................................................ 7
  - Return dates ............................................................................................................. 7

## Appendix ..................................................................................................................... 8
FIT5037 Advanced network security - Semester 2, 2009

Chief Examiner:

Dr Phu Le
Fax: +61 3 9903 1247

Contact hours: 11AM - 13PM Friday

Lecturer(s) / Leader(s):

Caulfield

Dr Phu Le
Fax: +61 3 9903 1247

Contact hours: 11AM - 13PM Friday
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

1. Understand the design and implementation of advanced cryptographic algorithms for wired and wireless computing environments including the design and implementation of RSA and ECC
2. 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
3. Develop knowledge of advanced network security architectures to allow better network protection, load balancing and recovery from attacks
4. Achieve sound knowledge of wireless network security
5. Understand security in trusted-based computing environments
6. Understand Quantum cryptography

Contact hours

2 hours of lectures/week; 2 hours of tutorials/week.

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.
For MAIT students: FIT9017, FIT9018, FIT9019, FIT9030, FIT9020, FIT4037 and FIT5044

Prohibitions

CPE5021
FIT5037 is an elective unit in the MNC degree.

Relationships

FIT5037 is an elective unit in the MNC degree.
Teaching and learning method

Teaching methods are done by conducting lectures and lab exercises. Lab exercises include network set-up and configurations, Intrusion Detection with Snort 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.cc.monash.edu.au/

Unit Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Topic</th>
<th>Key dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Advanced topics of Modern Computing and Network Security</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Advanced Cryptography</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Elliptic Curve Public Key System</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Design and Implementation of RSA and ECC</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Advanced techniques in firewalls</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Security, Load Balancing and Network Performance</td>
<td>individual assignments due at 4PM Friday</td>
</tr>
<tr>
<td>9</td>
<td>Wireless Security</td>
<td>Group assignment - Part I (IDS system) due</td>
</tr>
<tr>
<td>10</td>
<td>Security, Load Balancing and Network Performance</td>
<td>Mid semester break</td>
</tr>
<tr>
<td>11</td>
<td>Network Security and Quantum Theory</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Reading in Network Security</td>
<td>Group assignment - Part II (vulnerabilities and attacks) due</td>
</tr>
<tr>
<td>13</td>
<td>Research Discussion</td>
<td></td>
</tr>
</tbody>
</table>
Unit Resources

Prescribed text(s) and readings

N/A

There is no specific textbook for this unit.

Recommended text(s) and readings

- Jack Kozioi, Intrusion Detection with Snort, SAMS, 157870281x.

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

Two 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 44% then a mark of no greater than 44-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 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%
  Due date: 4PM - Friday - Week 8
Assignment task 2

Title: Group Assignments
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: 40%
Due date:

Assignment task 3

Title:
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:
Due date: IDS with Snort due during the lab of week 9 - System vulnerabilities and possible attacks due during the lab of week 12

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.
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