FIT5044 Network security - Semester 1, 2010

Chief Examiner:

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

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: 9903 2399, email: pdle@infotech.monash.edu.au
Introduction

Welcome to Information and Network Security FIT5044 (CPE5002/CSE5210). This unit is an important unit for master students who want to study security in theory and practice. It explores many aspects of IT security and is the prerequisite unit for the advanced network security unit offered in the second semester.

Unit synopsis

This unit aims to provide students with fundamental knowledge of network and information security. Topics to be covered include network components and services, network computer systems and security policy, security at different system layers, basic cryptography and information security, information security and communications, intrusion detection system, malicious code and detection and prevention systems, authentication systems, and wireless security.

Learning outcomes

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

- the fundamentals of Network Security issues including possible vulnerabilities in a computer system, software and hardware applications;
- basic symmetric and asymmetric cryptography including symmetric and asymmetric crypto systems such as DES, RSA, RC4;
- authentication systems;
- computer malicious codes such as viruses, logic bombs, etc;
- security design at different levels of OSI model, IPSec, SSL, and security at application layer;
- firewalls and detection and prevention systems.

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 4 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

Prohibitions

CPE5002, CSE5210
Teaching and learning method

Teaching approach

Teaching methods are done by conducting lectures and lab exercises. Lab exercises include network set-up and configurations, firewall set-up and configurations, cryptographic exercises. 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.

You need to take this unit seriously from the first week. When you get behind you have no time to catch up. There will be lab work every week.

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

<table>
<thead>
<tr>
<th>Week</th>
<th>Date*</th>
<th>Topic</th>
<th>Key dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>01/03/10</td>
<td>Introduction to information and network security</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>08/03/10</td>
<td>Private and public key systems</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>15/03/10</td>
<td>Digital certificates and hash functions</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>22/03/10</td>
<td>Authentication systems</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>29/03/10</td>
<td>Computer malicious code detection and prevention systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mid semester break</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>12/04/10</td>
<td>Security at the IP level : IPSec design and implementation</td>
<td>assignment 1 due on Fri 4PM</td>
</tr>
<tr>
<td>7</td>
<td>19/04/10</td>
<td>Security at the Transport Layer: SSL and TLS design and implementation</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>26/04/10</td>
<td>Security at the Application Layer: Email security and Web security</td>
<td>assignment 1 due on Fri 4PM</td>
</tr>
<tr>
<td>9</td>
<td>03/05/10</td>
<td>Introduction to firewalls</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10/05/10</td>
<td>Introduction to intrusion detection systems</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>17/05/10</td>
<td>Introduction to wireless security</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>24/05/10</td>
<td>Research in information and network security</td>
<td>Assignments 2 &amp;3 due on Fri 4PM</td>
</tr>
<tr>
<td>13</td>
<td>31/05/10</td>
<td>Revision and test</td>
<td>TEST AT THE LECTURE THEATRE - LECTURE TIME</td>
</tr>
</tbody>
</table>
*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.

Recommended text(s) and readings


Required software and/or hardware

Linux OS

Equipment and consumables required or provided

Students will be provided removable hard-drives, Linux software and cryptographic packages for lab exercises.

Student will need to do some preparation before a lab session and spend 2 hours per week at the lab to be able to finish a lab exercise. Besides the lab time, students will also need to have access to a computer for self-study at least 8 hours a week to successfully complete the unit.

Study resources

Study resources we will provide for your study are:

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 laboratory exercises with guide to complete the exercises;
- Assignment specifications and guide to complete the assignments;
- Sample test questions before the test;
- Weekly consultation.
Assessment

Overview

Assignments: 80%; Theoretical test: 20%

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 is no formal examination for this subject. Students must pass the practical assignments (total 80%) and theoretical test (20%) to pass this unit. Students must attend all the lab sessions.

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:
Secure your computer system with private key, public key, hash functions and digital certificates

Description:
You are required to learn the GPG/PGP package and implement a security policy to protect your network communications, stored data, and secure email messages and documents.

You will need to be able to answer the following questions:

1. How to generate private and public keys
2. How to protect your private key and public key
3. How to protect public keys from tampering
4. How to secure messages exchanged between you and your friends
5. How RSA was practically implemented in the package

6. How secure RSA is in practice

**Weighting:**
20%

**Due date:**
Fri of week 8 (teaching week)

**Assignment task 2**

**Title:**
Set up and configure firewalls

**Description:**
Your group is required to set up, configure, and test your firewall using IPTABLES. You need to do the research and readings to be able to complete this assignment.

Check your system services such as Web service, email service, ftp service, telnet, and ssh service to make sure they are installed and run.

Then configure your firewall to:

1. reject all `ftp` packets from external networks, but still allow internal ftp.

2. allow `ssh` remote connections but deny `telnet`.

3. deny `ping`.

4. reject all traffic coming to port 21 and 80.

5. reject all traffic coming to all UDP ports

6. block all email coming in and out of your network. Internal email is allowed.

7. block all traffic from two particular networks. You can pick any two networks you like and.

8. allow traffic coming to port 80 but reject traffic coming out through port 80.

Describe in detail how you test 1,2,3,4,5,6,7 with real practical tests and/or with your gathered information from reliable sources.

**Weighting:**
40 %

**Due date:**
Fri of week 12 (teaching week)

**Assignment task 3**

**Title:**
Write a security policy for Monash computer network and propose an implementation to secure the network

**Description:**
You are required to study Monash computer network in detail, write a security policy to protect the network which includes hardware, software, data and users.

The security policy will be for both wired and wired networks.

Propose a practical implementation to secure the whole network.

Weighting:
20%

Due date:
Fri of week 12 (teaching week)

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:

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