FIT5044
Network security

Unit Guide

Semester 1, 2012

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: 22 Feb 2012
# Table of Contents

**FIT5044 Network security - Semester 1, 2012** ........................................................................................................1

- Mode of Delivery ........................................................................................................................................1
- Contact Hours .........................................................................................................................................1
- Workload ...............................................................................................................................................1
- Unit Relationships ...............................................................................................................................1
- Prohibitions ..........................................................................................................................................1

**Chief Examiner** .....................................................................................................................................1

**Campus Lecturer** .................................................................................................................................1

- Caulfield ............................................................................................................................................1

**Tutors** ...............................................................................................................................................1

- Caulfield ........................................................................................................................................2

**Academic Overview** ..........................................................................................................................3

- Outcomes ..........................................................................................................................................3
- Graduate Attributes ..........................................................................................................................3
- Assessment Summary .......................................................................................................................3
- Teaching Approach ........................................................................................................................4
- Feedback ..........................................................................................................................................4
  - Our feedback to You .......................................................................................................................4
  - Your feedback to Us .....................................................................................................................4

**Previous Student Evaluations of this unit** .............................................................................................4

**Required Resources** ..........................................................................................................................4

**Unit Schedule** ...................................................................................................................................5

**Assessment Requirements** ................................................................................................................6

- Assessment Policy ............................................................................................................................6
- Assessment Tasks ............................................................................................................................6
- Participation .......................................................................................................................................6

- Examinations ......................................................................................................................................9
- Assignment submission .....................................................................................................................9
- Online submission ...........................................................................................................................9
- Extensions and penalties ..................................................................................................................9
- Returning assignments ....................................................................................................................9

**Other Information** ...............................................................................................................................10

- Policies ..........................................................................................................................................10
- Student services ..............................................................................................................................10
- Other .............................................................................................................................................11
FIT5044 Network security - Semester 1, 2012

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.

Mode of Delivery

Caulfield (Evening)

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

Chief Examiner

Dr Phu Dung Le

Campus Lecturer

Caulfield

Phu Dung Le

Tutors
Caulfield

Phu Le, Guy T. and Mark Ohio. Consultation hours: TBA
Academic Overview

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.

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: 80%; Theoretical test: 20%

<table>
<thead>
<tr>
<th>Assessment Task</th>
<th>Value</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure your computer system with private key, public key, hash functions</td>
<td>20%</td>
<td>8PM Thursday - Week 7</td>
</tr>
<tr>
<td>and digital certificates</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Set up and configure firewalls</td>
<td>25%</td>
<td>8PM Thursday - Week 9</td>
</tr>
<tr>
<td>Identify system vulnerabilities, demonstrate your attacks, and propose solutions</td>
<td>35%</td>
<td>8PM Thursday - Week 14</td>
</tr>
<tr>
<td>to mitigate the attacks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test</td>
<td>20%</td>
<td>During the lecture - Week 12</td>
</tr>
</tbody>
</table>
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:

- Graded assignments with comments
- Interviews

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.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

Required Resources

Please check with your lecturer before purchasing any Required Resources. Prescribed texts are available for you to borrow in the library, and prescribed software is available in student labs.

Linux OS
### Unit Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Activities</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No formal assessment or activities are undertaken in week 0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Introduction to computer system security</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Information and Network Security</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Cryptography for Information and Network Security (2 lectures: 3 &amp; 4)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Cryptography for Information and Network Security (con't)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Introduction to Firewalls</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Security at the IP level: IPSec design and implementation</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Security at the Transport Layer: SSL and TLS design and implementation</td>
<td>Assessment task 1 due 8PM Thursday - Week 7</td>
</tr>
<tr>
<td>8</td>
<td>Security at the Application Layer: Email security and Web security</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Introduction to Authentication Systems</td>
<td>Assessment task 2 due 8PM Thursday - Week 9</td>
</tr>
<tr>
<td>10</td>
<td>Introduction to Wireless Security</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Introduction to Large System Security</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Informal test in the lecture</td>
<td>Test during the lecture - Week 12</td>
</tr>
<tr>
<td></td>
<td>SWOT VAC</td>
<td>No formal assessment is undertaken SWOT VAC. Assessment task 3 due 8PM Thursday - Week 14</td>
</tr>
</tbody>
</table>

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

Assessment Policy

Faculty Policy - Unit Assessment Hurdles

Assessment Tasks

Participation

IMPORTANT: You must read the assignment specs carefully and follow the instructions. The unit guide can only provide you general information.

• Assessment 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%

  Criteria for assessment:
  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:**
8PM Thursday - Week 7

**Assessment task 2**

**Title:**
Set up and configure firewalls

**Description:**
You are 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.

Discuss the advantages and disadvantages of firewalls with iptables.

**Weighting:**
25%

**Criteria for assessment:**
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.
Assessment Requirements

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

Due date: 8PM Thursday - Week 9

• Assessment task 3

Title: Identify system vulnerabilities, demonstrate your attacks, and propose solutions to mitigate the attacks.

Description:
1. You are required to find at least three main vulnerabilities on either Windows or Unix systems, old or new, patched or un-patched.

2. Once you have identified the vulnerabilities, you need to work out how possible attacks can be launched by exploiting those vulnerabilities.

3. You are then required to demonstrate the possible attacks on your own system.

4. Propose solutions to mitigate those attacks.

Weighting: 35%

Criteria for assessment:
- If you complete 1. correctly, you will get maximum 10%.

- You will get 15% for 2. and 3. if you successfully complete 1. and explain correctly how attacks can be launched with demonstrations.

- 10% will be given to good solutions to mitigate the attacks - 4.

Due date: 8PM Thursday - Week 14

• Assessment task 4

Title: Test

Description: The test will evaluate your understanding of the materials covered in the lectures and tutorials.

It is an open book and consists 15 multiple choice questions and 5 short answer questions.

Weighting: 20%

Criteria for assessment: Correct answers to questions (demonstrate good understanding of the material learned).

Due date: During the lecture - Week 12
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).

Online submission

If Electronic Submission has been approved for your unit, please submit your work via the VLE site for this unit, which you can access via links in the my.monash portal.

Extensions and penalties

Submission must be made by the due date otherwise penalties will be enforced.


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)
- Special Consideration (http://www.policy.monash.edu/policy-bank/academic/education/assessment/special-consideration-policy.html)
- 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/)
- Codes of Practice for Teaching and Learning (http://www.policy.monash.edu/policy-bank/academic/education/conduct/suppdocs/code-of-practice-teaching-and-learning.html)

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. For Sunway see http://www.monash.edu.my/Student-services, and for South Africa see http://www.monash.ac.za/current/

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. At Sunway, visit the Library and Learning Commons at http://www.lib.monash.edu.my/. At South Africa visit http://www.lib.monash.ac.za/.

Academic support services may be available for students who have a disability or medical condition. Registration with the Disability Liaison Unit is required. Further information is available as follows:

- Website: http://monash.edu/equity-diversity/disability/index.html
- Email: dlu@monash.edu
- Drop In: Equity and Diversity Centre, Level 1 Gallery Building (Building 55), Monash University, Clayton Campus, or Student Community Services Department, Level 2, Building 2, Monash University, Sunway Campus
- Telephone: 03 9905 5704, or contact the Student Advisor, Student Community Services at 03 55146018 at Sunway
Other Information

Other

Reading List

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