



**MONASH** University  
Information Technology

**FIT5044**  
**Network security**

**Unit Guide**

**Semester 1, 2011**

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: 27 Feb 2011*

# Table of Contents

<u><a href="#">FIT5044 Network security - Semester 1, 2011</a></u> .....	1
<u><a href="#">Mode of Delivery</a></u> .....	1
<u><a href="#">Contact Hours</a></u> .....	1
<u><a href="#">Workload</a></u> .....	1
<u><a href="#">Unit Relationships</a></u> .....	1
<u><a href="#">Prohibitions</a></u> .....	1
<u><a href="#">Chief Examiner</a></u> .....	1
<u><a href="#">Campus Lecturer</a></u> .....	1
<u><a href="#">Caulfield</a></u> .....	1
<u><a href="#">Tutors</a></u> .....	1
<u><a href="#">Caulfield</a></u> .....	2
<u><a href="#">Learning Objectives</a></u> .....	2
<u><a href="#">Graduate Attributes</a></u> .....	2
<u><a href="#">Assessment Summary</a></u> .....	2
<u><a href="#">Teaching Approach</a></u> .....	3
<u><a href="#">Feedback</a></u> .....	3
<u><a href="#">Our feedback to You</a></u> .....	3
<u><a href="#">Your feedback to Us</a></u> .....	3
<u><a href="#">Previous Student Evaluations of this unit</a></u> .....	3
<u><a href="#">Required Resources</a></u> .....	3
<u><a href="#">Unit Schedule</a></u> .....	3
<u><a href="#">Assessment Policy</a></u> .....	4
<u><a href="#">Assessment Tasks</a></u> .....	4
<u><a href="#">Participation</a></u> .....	4
<u><a href="#">Examinations</a></u> .....	7
<u><a href="#">Assignment submission</a></u> .....	7
<u><a href="#">Extensions and penalties</a></u> .....	7
<u><a href="#">Returning assignments</a></u> .....	7
<u><a href="#">Policies</a></u> .....	7
<u><a href="#">Student services</a></u> .....	8

# **FIT5044 Network security - Semester 1, 2011**

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 (Day)

## **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**

Phu Dung Le

### **Campus Lecturer**

### **Caulfield**

Phu Dung Le

### **Tutors**

## Caulfield

Guy T. and Ping Xian Wu and Mark Ohio and Harry Ngo

Contact hours: TBA

## Learning Objectives

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%

Assessment Task	Value	Due Date
Secure your computer system with private key, public key, hash functions and digital certificates	30%	Friday 22 April 2011
Set up and configure firewalls	25 %	Friday 27 May 2011
Write a security policy for a medium or large computer network and propose an implementation to secure the network	25%	Friday 27 May 2011

## 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.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

Linux OS

## Unit Schedule

Week	Date*	Activities	Assessment
0	21/02/11		No formal assessment or activities are undertaken in week 0
1	28/02/11	Introduction to computer system security	
2	07/03/11	Information and Network Security	
3	14/03/11	Cryptography for Information and Network Security (2 lectures: 3 & 4)	

4	21/03/11	Cryptography for Information and Network Security (con't)	
5	28/03/11	Introduction to Firewalls	
6	04/04/11	Security at the IP level : IPSec design and implementation	
7	11/04/11	Security at the Transport Layer: SSL and TLS design and implementation	
8	18/04/11	Security at the Application Layer: Email security and Web security	assignment 1 due on Fri 4PM
Mid semester break			
9	02/05/11	Introduction to Authentication Systems	
10	09/05/11	Introduction to Wireless Security	
11	16/05/11	Introduction to Large System Security	
12	23/05/11	Informal test	Assignments 2 & 3 due on Fri 4PM
	30/05/11	SWOT VAC	No formal assessment is undertaken SWOT VAC

\*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.

## 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

## 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:**

30%

**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:**

Friday 22 April 2011

• **Assessment 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.

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.

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

**Due date:**

Friday 27 May 2011

• **Assessment task 3**

**Title:**

Write a security policy for a medium or large computer network and propose an implementation to secure the network

**Description:**

You are required to study a reference computer network (e.g 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 wireless networks.

Propose a practical implementation to secure the whole network.

**Weighting:**

25%

**Criteria for assessment:**

The assessment of this assignment is based on:

1. A complete study of a reference computer network
2. Good security policy

### 3. Practical implementation

If you do 1. and understand it, you will get a Pass as the maximum.

If you do 1. and 2. and understand them you will get a Credit as the maximum

If you do 1. and 2. and 3. and understand them you will get a Distinction as the maximum

If you do 1. and 2. and 3. and understand them and provide good references you will get a High Distinction

**Due date:**

Friday 27 May 2011

## Examinations

### Assignment submission

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.

### 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

## 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-p>)
- 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>)

## 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](http://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](mailto:dlu@monash.edu)
- Drop In: Equity and Diversity Centre, Level 1 Gallery Building (Building 55), Monash University, Clayton Campus.

## Reading List

- 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.
- Robert L. Ziegler, Linux Firewalls, New Riders, ASIN: 0735709009.
- Greg Holden, Guide to Network Defense and Counter Measures, Thomson, ISBN: 0-619-13124-1.
- Practical Unix Security, O'Reilly & Associate, Inc, Simson Garfinkle and Gene Spafford, ISBN: 0-937175-72-2.
- 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.