



**MONASH** University

**CPE5021**  
**Advanced network security**

**Unit guide**

**Semester 2, 2008**

*Last updated : 07 Jul 2008*

# Table of Contents

<u>CPE5021 Advanced network security - Semester 2 , 2008</u> .....	1
<u>Unit leader</u> :.....	1
<u>Lecturer(s)</u> :.....	1
<u>Caulfield</u> .....	1
<u>Introduction</u> .....	2
<u>Unit synopsis</u> .....	2
<u>Learning outcomes</u> .....	2
<u>Workload</u> .....	2
<u>Unit relationships</u> .....	3
<u>Prerequisites</u> .....	3
<u>Relationships</u> .....	3
<u>Continuous improvement</u> .....	4
<u>Student Evaluations</u> .....	4
<u>Unit staff - contact details</u> .....	5
<u>Unit leader</u> .....	5
<u>Lecturer(s)</u> :.....	5
<u>Teaching and learning method</u> .....	6
<u>Communication, participation and feedback</u> .....	6
<u>Unit Schedule</u> .....	6
<u>Unit Resources</u> .....	7
<u>Prescribed text(s) and readings</u> .....	7
<u>Recommended text(s) and readings</u> .....	7
<u>Required software and/or hardware</u> .....	7
<u>Equipment and consumables required or provided</u> .....	7
<u>Study resources</u> .....	7
<u>Library access</u> .....	7
<u>Monash University Studies Online (MUSO)</u> .....	7
<u>Assessment</u> .....	9
<u>Unit assessment policy</u> .....	9
<u>Assignment tasks</u> .....	9
<u>Assignment submission</u> .....	10
<u>Assignment coversheets</u> .....	10
<u>University and Faculty policy on assessment</u> .....	11
<u>Due dates and extensions</u> .....	11
<u>Late assignment</u> .....	11
<u>Return dates</u> .....	11
<u>Plagiarism, cheating and collusion</u> .....	11
<u>Register of counselling about plagiarism</u> .....	12
<u>Non-discriminatory language</u> .....	12
<u>Students with disabilities</u> .....	12
<u>Deferred assessment and special consideration</u> .....	12

# **CPE5021 Advanced network security - Semester 2 , 2008**

## **Unit leader :**

Phu Dung Le

## **Lecturer(s) :**

## **Caulfield**

- Phu Dung Le

## Introduction

### 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.

### Learning outcomes

**At the completion of of this unit students will:**

- Understand the design and implementation of advanced cryptographic algorithms for wired and wireless computing environments.
- 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.

#### Practical Skills

- Gain experience of efficient implementation of public key cryptography for wired and wireless environments
- Gain experience of design, implementation, and configurations of different type of firewalls
- Gain experience of configurations of Snort intrusion detection system
- Gain experience of applying digital signatures in prevention systems on Linux and Windows
- Become familiar with network security architectures and network security components
- Gain experience of how firewalls and IDSs work together
- Practically find the vulnerabilities in your computer system

#### Relationships, Communication and TeamWork

- Experience the need of cooperative security management
- Work effectively in group to achieve a system implementation

### 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.

CPE5021 Advanced network security - Semester 2 , 2008

- 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**

Before attempting this unit you must have satisfactorily completed CPE5002 Network Security or equivalent.

### **Relationships**

CPE5021 is an elective unit in the MNC degree.

## Continuous improvement

Monash is committed to 'Excellence in education' and strives for the highest possible quality in teaching and learning. To monitor how successful we are in providing quality teaching and learning Monash regularly seeks feedback from students, employers and staff. Two of the formal ways that you are invited to provide feedback are through Unit Evaluations and through Monquest Teaching Evaluations.

One of the key formal ways students have to provide feedback is through Unit Evaluation Surveys. It is Monash policy for every unit offered to be evaluated each year. Students are strongly encouraged to complete the surveys as they are an important avenue for students to "have their say". The feedback is anonymous and provides the Faculty with evidence of aspects that students are satisfied and areas for improvement.

## Student Evaluations

The Faculty of IT administers the Unit Evaluation surveys online through the my.monash portal, although for some smaller classes there may be alternative evaluations conducted in class.

If you wish to view how previous students rated this unit, please go to <http://www.monash.edu.au/unit-evaluation-reports/>

Over the past few years the Faculty of Information Technology has made a number of improvements to its courses as a result of unit evaluation feedback. Some of these include systematic analysis and planning of unit improvements, and consistent assignment return guidelines.

Monquest Teaching Evaluation surveys may be used by some of your academic staff this semester. They are administered by the Centre for Higher Education Quality (CHEQ) and may be completed in class with a facilitator or on-line through the my.monash portal. The data provided to lecturers is completely anonymous. Monquest surveys provide academic staff with evidence of the effectiveness of their teaching and identify areas for improvement. Individual Monquest reports are confidential, however, you can see the summary results of Monquest evaluations for 2006 at <http://www.adm.monash.edu.au/cheq/evaluations/monquest/profiles/index.html>

## **Unit staff - contact details**

### **Unit leader**

**Dr Phu Le**

Fax +61 3 9903 1247

Contact hours : 11AM - 13PM Friday

### **Lecturer(s) :**

**Dr Phu Le**

Fax +61 3 9903 1247

Contact hours : 11AM - 13PM Friday

## 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 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.

## Communication, participation and feedback

Monash aims to provide a learning environment in which students receive a range of ongoing feedback throughout their studies. You will receive feedback on your work and progress in this unit. This may take the form of group feedback, individual feedback, peer feedback, self-comparison, verbal and written feedback, discussions (on line and in class) as well as more formal feedback related to assignment marks and grades. You are encouraged to draw on a variety of feedback to enhance your learning.

It is essential that you take action immediately if you realise that you have a problem that is affecting your study. Semesters are short, so we can help you best if you let us know as soon as problems arise. Regardless of whether the problem is related directly to your progress in the unit, if it is likely to interfere with your progress you should discuss it with your lecturer or a Community Service counsellor as soon as possible.

## Unit Schedule

Week	Topic	Key dates
1	Advanced topics of Mordern Computing and Network Security	
2	Advanced Cryptography	
3	Elliptic Curve Public Key System	
4	Design and Implementation of RSA and ECC	
5	Advanced techniques in firewalls	
6	Intrusion Detection Systems: Concepts, Design, and Implementation	
7	Wireless Security: Principles and Practices	
8	Security, Load Balancing and Network Performance	individual assignments due at 4PM Friday
9	Wireless Security	Group assignment - Part I (IDS system) due
10	Security, Load Balancing and Network Performance	
11	Network Security and Quantum Theory	
Mid semester break		
12	Reading in Network Security	Group assignment - Part II (vulnerabilities and attacks) due
13	Research Discussion	



## 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.

### Library access

The Monash University Library site contains details about borrowing rights and catalogue searching. To learn more about the library and the various resources available, please go to <http://www.lib.monash.edu.au>. Be sure to obtain a copy of the Library Guide, and if necessary, the instructions for remote access from the library website.

### Monash University Studies Online (MUSO)

All unit and lecture materials are available through MUSO (Monash University Studies Online). Blackboard is the primary application used to deliver your unit resources. Some units will be piloted in Moodle. If your unit is piloted in Moodle, you will see a link from your Blackboard unit to Moodle (<http://moodle.monash.edu.au>) and can

bookmark this link to access directly. In Moodle, from the Faculty of Information Technology category, click on the link for your unit.

You can access MUSO and Blackboard via the portal: <http://my.monash.edu.au>

Click on the Study and enrolment tab, then Blackboard under the MUSO learning systems.

In order for your Blackboard unit(s) to function correctly, your computer needs to be correctly configured.

For example:

- Blackboard supported browser
- Supported Java runtime environment

For more information, please visit: <http://www.monash.edu.au/muso/support/students/downloadables-student.html>

**You can contact the MUSO Support by: Phone: (+61 3) 9903 1268**

For further contact information including operational hours, please visit:  
<http://www.monash.edu.au/muso/support/students/contact.html>

Further information can be obtained from the MUSO support site:  
<http://www.monash.edu.au/muso/support/index.html>

## Assessment

### Unit assessment policy

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 Task**

**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 :**

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 - Friday - Week 8

- **Assignment Task**

**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%

**Criteria for assessment :**

**Due date :**

• **Assignment Task**

**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 :**

**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.

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

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

## **Assignment submission**

Do not email your submissions.

You have to print your hard copies and submit them with soft copies on cd(s).

## **Assignment coversheets**

All submissions must have coversheets.

## University and Faculty policy on assessment

### Due dates and extensions

The due dates for the submission of assignments are given in the previous section. 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 seldom regarded as appropriate reasons for granting extensions. Students are advised to NOT assume that granting of an extension is a matter of course.

If you get sick or have a serious personal problem and cannot complete the assignments in time, you may apply for an extension.

Requests for extensions must be made to the lecturer at least two days before the due date.

You will be asked to forward original medical certificates in cases of illness.

### 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.

Assessment for the unit as a whole is in accordance with the provisions of the Monash University Education Policy at <http://www.policy.monash.edu/policy-bank/academic/education/assessment/>

We will aim to have assignment results made available to you within two weeks after assignment receipt. However, it depends on the number of students enrolled in the unit.

### Plagiarism, cheating and collusion

Plagiarism and cheating are regarded as very serious offences. In cases where cheating has been confirmed, students have been severely penalised, from losing all marks for an assignment, to facing disciplinary action at the Faculty level. While we would wish that all our students adhere to sound ethical conduct and honesty, I will ask you to acquaint yourself with Student Rights and Responsibilities (<http://www.infotech.monash.edu.au/about/committees-groups/facboard/policies/studrights.html>) and the Faculty regulations that apply to students detected cheating as these will be applied in all detected cases.

In this University, cheating means seeking to obtain an unfair advantage in any examination or any other written or practical work to be submitted or completed by a student for assessment. It includes the use, or attempted use, of any means to gain an unfair advantage for any assessable work in the unit, where the means is contrary to the instructions for such work.

When you submit an individual assessment item, such as a program, a report, an essay, assignment or other piece of work, under your name you are understood to be stating that this is your own work. If a submission is identical with, or similar to, someone else's work, an assumption of cheating may arise. If you are planning on working with another student, it is acceptable to undertake research together, and discuss problems, but it is not acceptable to jointly develop or share solutions unless this is specified by your lecturer.

Intentionally providing students with your solutions to assignments is classified as "assisting to cheat" and students who do this may be subject to disciplinary action. You should take reasonable care that your solution is not accidentally or deliberately obtained by other students. For example, do not leave copies of your work in progress on the hard drives of shared computers, and do not show your work to other students. If you believe this may have happened, please be sure to contact your lecturer as soon as possible.

Cheating also includes taking into an examination any material contrary to the regulations, including any bilingual dictionary, whether or not with the intention of using it to obtain an advantage.

Plagiarism involves the false representation of another person's ideas, or findings, as your own by either copying material or paraphrasing without citing sources. It is both professional and ethical to reference clearly the ideas and information that you have used from another writer. If the source is not identified, then you have plagiarised work of the other author. Plagiarism is a form of dishonesty that is insulting to the reader and grossly unfair to your student colleagues.

## **Register of counselling about plagiarism**

The university requires faculties to keep a simple and confidential register to record counselling to students about plagiarism (e.g. warnings). The register is accessible to Associate Deans Teaching (or nominees) and, where requested, students concerned have access to their own details in the register. The register is to serve as a record of counselling about the nature of plagiarism, not as a record of allegations; and no provision of appeals in relation to the register is necessary or applicable.

## **Non-discriminatory language**

The Faculty of Information Technology is committed to the use of non-discriminatory language in all forms of communication. Discriminatory language is that which refers in abusive terms to gender, race, age, sexual orientation, citizenship or nationality, ethnic or language background, physical or mental ability, or political or religious views, or which stereotypes groups in an adverse manner. This is not meant to preclude or inhibit legitimate academic debate on any issue; however, the language used in such debate should be non-discriminatory and sensitive to these matters. It is important to avoid the use of discriminatory language in your communications and written work. The most common form of discriminatory language in academic work tends to be in the area of gender inclusiveness. You are, therefore, requested to check for this and to ensure your work and communications are non-discriminatory in all respects.

## **Students with disabilities**

Students with disabilities that may disadvantage them in assessment should seek advice from one of the following before completing assessment tasks and examinations:

- Faculty of Information Technology Student Service staff, and / or
- your Unit Coordinator, or
- [Disabilities Liaison Unit](#)

## **Deferred assessment and special consideration**

Deferred assessment (not to be confused with an extension for submission of an assignment) may be granted in cases of extenuating personal circumstances such as serious personal illness or bereavement. Information and forms for Special Consideration and deferred assessment applications are available at <http://www.monash.edu.au/exams/special-consideration.html>. Contact the Faculty's Student Services staff at your campus for further information and advice.