MONASH University

FIT5044
Network security

Unit guide

Semester 1, 2009

Last updated : 11 Feb 2009

Table of Contents

FIT5044 Network security - Semester 1, 2009

Unit leader :

Dr Phu Dung Le

Lecturer(s) :

Caulfield

- Phu Dung Le

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, intrusion detection systems, firewalls, malicious code and detection and prevention systems, authentication systems, and wireless security.

Learning outcomes

At the completion of this subject, students should be able to understand:

- the fundamentals of network security issues including possible vulnerabilities in a computer system, software and hardware applications.
- weaknesses of current network protocols.
- basic symmetric and asymmetric cryptography including symmetric and asymmetric crypto systems such as 3DES, RSA, RC4.
- authentication systems.
- computer malicious codes such as viruses, logic bombs, etc.
- basic concepts of Intrusion Detection Systems.
- theoretical knowledge and practical experiences of basic firewalls.
- security design at different layers of OSI model, IPSec, SSL, and security at application layer.
- basic wireless security.
- cryptography and information security.
- information security and communications.

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

Prerequisites

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

You are expected to have good knowledge in data communications and networking, Unix OS, and good background in Maths.

Relationships

FIT5044 (CPE5002/CSE5210) is an elective unit in the Masters of Network Computing and the Masters of Information Technology. It is a fundamental unit for Advanced Network Security.

Continuous improvement

Monash is committed to 'Excellence in education' (Monash Directions 2025 - http://www.monash.edu.au/about/monash-directions/directions.html) 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. One of the key formal ways students have to provide feedback is through Unit Evaluation Surveys. The University's Unit Evaluation policy (http://www.policy.monash.edu/policy-bank/academic/education/quality/unit-evaluation-policy.html) requires that every unit offered is 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.

Faculties have the option of administering the Unit Evaluation survey online through the my.monash portal or in class. Lecturers will inform students of the method being used for this unit towards the end of the semester.

Student Evaluations

If you wish to view how previous students rated this unit, please go to http://www.adm.monash.edu.au/cheq/evaluations/unit-evaluations/

Unit staff - contact details

Unit leader

Dr Phu Le
Fax +61 3 9903 1247

Lecturer(s) :

Dr Phu Le
Fax +61 3 9903 1247

Additional communication information

Dr. Phu Dung Le, Room: H.706, Phone: 9903 2399, email: pdle@infotech.monash.edu.au

Teaching and learning method

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.

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	Introduction to information and network security	
2	Private and public key systems	
3	Digital certificates and hash functions	
4	Authentication systems	
5	Computer malicious code detection and prevention systems	
6	Security at the IP level : IPSec design and implementation	
Mid semester break		
7	Security at the Transport Layer: SSL and TLS design and implementation	
8	Security at the Application Layer: Email security and Web security	assignment 1 due on Fri 4PM
9	Introduction to firewalls	
10	Introduction to intrusion detection systems	
11	Introduction to wireless security	
12	Research in information and network security	Assignments 2 &3 due on Fri 4PM
13	Revision and test	TEST AT THE LECTURE

		THEATRE - LECTURE TIME

Unit Resources

Prescribed text(s) and readings

There is no text book 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. 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.

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.

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.

The Educational Library and Media Resources (LMR) is also a very resourceful place to visit at http://www.education.monash.edu.au/library/

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

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 Task

  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 : Fri of week 8 (teaching week)

- ### Assignment Task

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 p**ing**.

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 : 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 : Fri of week 12 (teaching week)

- **Assignment Task**

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%

Criteria for assessment :

The assessment of this assignment is based on:

1. A complete study of Monash 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 : Fri of week 12 (teaching week)

Assignment submission

Do not email submissions. The due date is the date by which the submission must be received/the date by which the submission is to be posted.

Hard copies (you have to print your hard copies and have a cover sheet) and soft copies on a cd will be required as your assignment submissions.

Assignment coversheets

Students need to have a cover sheet for the assignment submissions. Assignment cover sheets can be obtained at the school office.

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 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.

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.