MONASH University

FIT4016
Information security

Unit guide

Semester 2, 2008

Last updated : 16 Jul 2008

Table of Contents

FIT4016 Information security - Semester 2 , 2008

Unit leader :

Nandita Bhattacharjee

Lecturer(s) :

Clayton

- Nandita Bhattacharjee

Introduction

Welcome to FIT4016, Information Security, for semester 2, 2008. This 6 point unit is an elective unit to all honours and postgraduate degree programs in the Faculty of IT. The unit has been designed to provide you with an understanding of principles and practice of security in a computerised information system. It explores many techniques and tools utilised to counteract the risks and threat to information security and its practical application to some examples.

Unit synopsis

This unit looks at a range of security problems in information systems, namely system security, network security and software security. Within these areas, topics covered include properties of information security, principles of encryption, a variety of crypto techniques and analysis, and their application to practical examples like authentication algorithms, non repudiation by digital signatures among others. It looks at various management issues, including disparate application examples, distributed systems authentication, contingency planning, audit and review, intrusion detection to name a few.

Learning outcomes

Upon completion students will

- Have knowledge of risks, threats and goals of information security
- Understand various controls and their effectiveness for information security in an organisation
- be able to evaluate the effectiveness (both in terms of performance and limitations) of individual control techniques
- match the risk against controls and evaluate their applicability

Workload

Student workload commitments per week are:

- two-hour lecture and
- two-hour tutorial (requiring advance preparation)
- a minimum of 2-3 hours of personal study per one hour of contact time in order to satisfy the reading and assessment expectations.

Unit relationships

Prerequisites

There are no prerequisite units recommended for this unit. Prerequisite knowledge of basic data communications (similar to FIT1005 or equivalent) is assumed.

Relationships

This level 4 unit is an elective unit in all the undergraduate honours degree programs and the Bachelor of Software Engineering program of the Faculty of IT. It may be taken as an elective in other programs where you have satisfied the prerequisite knowledge and course rules permit.You may not study this unit if you have completed

CSE4892.

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 Nandita Bhattacharjee
Lecturer
Phone +61 3 990 53293
Fax +61 3 990 55146
Contact hours : Monday: 2:30PM-3:30PM

Lecturer(s) :

Dr Nandita Bhattacharjee
Lecturer
Phone +61 3 990 53293
Fax +61 3 990 55146

Teaching and learning method

This unit will be delivered via a 2 hours lecture followed by a 2 hours tutorial session consisting of discussion class each week. Lecturers may go through specific examples, give demonstrations and present slides that contain theoretical concepts in the lectures. In the discussion classes students will be discussing in-depth fundamental and interesting problem solving exercises related to information security and present solutions in class. The discussion classes will complement the lectures and help students consolidate concepts and practise problem solving skills.

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 security	
2	Principles of encryption	
3	Cryptography I	
4	Cryptography II	Quiz 01, 7-8-08
5	Key Escrow	
6	Authentication I - Example 1	Quiz 02, 21-8-08
7	Introduction to number theory	
8	Public Key Cryptography	Quiz 03, 4-9-08
9	Integrity & Authenticity	
10	Biometric authentication- Example 2	Quiz 04, 18-9-08
11	Key Management	
Mid semester break		
12	Intrusion detection and software security- Management Issues	Quiz 05, 9-10-08
13	Revision	

Unit Resources

Prescribed text(s) and readings

No book is prescribed as a text book for this unit. However three books are suggested as recommended texts. It is advisable to have at least one of those books. A number of copies of the recommended books are available at various Monash University libraries.

Recommended text(s) and readings

The list references:

- Cryptography and Network Security : Principles and Practice – William Stallings, Fourth Edition, 2007, Prentice Hall.
- Computer Security : Principles and Practice – William Stallings, 2008, Prentice Hall.
- Security Engineering: A Guide to Building Dependable Distributed Systems – Ross J Anderson, 2001, John Wiley & Sons, Inc.
- Practical Unix and Internet Security – Simon Garfinkel and Gene Spafford, O'Reilly & Associates.

Study resources

Study resources we will provide for your study are:

- Weekly lecture notes
- Weekly discussion tasks to be undertaken during the tutorial sessions
- Fortnightly quiz and its suggested solutions discussed in the tutorial class
- Practise exam questions and solutions discussed in last tutorial class
- This Unit Guide outlining the administrative information for the unit;
- The unit web site on Blackboard, where resources outlined above will be made available.

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

Fortnightly quizzes (40%) and a final exam (60%)

- attempt both assessment components and
- achieve no less than 40% in the final exam and
- an overall mark of at least 50% .

Assignment tasks

- **Assignment Task**

  Title : Quizzes

  Description :

  - 5 quizzes, starting in week 4, will be conducted each fortnight during the tutorial sessions on the topics covered in lectures.
  - Each quiz will have a weighting of 10%
  - Best of 4 out of 5 quizzes, will account for the assessment.

  Weighting : 40%

  Criteria for assessment :

  Due date : 7/8, 21/8, 4/9, 18/9, 9/10
- **Assignment Task**

  Title :

  Description :

  - 5 quizzes, starting in week 4, will be conducted each fortnight during the tutorial sessions on the topics covered in lectures.
  - Each quiz will have a weighting of 10%
  - Best of 4 out of 5 quizzes, will constitute the assessment.

  Weighting :

  Criteria for assessment :

  Due date :

Examinations

- **Examination**

  Weighting : 60%

  Length : 2 hours

Type (open/closed book) : Closed book

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.

Non-exam assessments will be conducted in the discussion classes.

Requests for extensions must be made to the unit lecturer at least two days before the due date. You will be asked to forward original medical certificates in cases of illness, and may be asked to provide other forms of documentation where necessary.

Late assignment

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/

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.