MONASH University

FIT3056
Secure and trusted software systems

Unit guide

Semester 2, 2008

Last updated : 20 Jun 2008

Table of Contents

FIT3056 Secure and trusted software systems - Semester 2 , 2008

Unit leader :

Phu Dung Le

Lecturer(s) :

Caulfield

- Phu Dung Le

Tutors(s) :

Caulfield

- Phu Dung Le

Introduction

Welcome to Secure and Trusted Software (FIT3056)!

This unit will be a core unit in the Security major of BITS. It can be an elective unit for students who do not major in security (subject to the approval from the school). This unit will provide students with the knowledge and experience of identifying software vulnerabilities, principles for constructing secure and trusted software, basic software security testing and verification.

Unit synopsis

ASCED Discipline Group classification: 020113 Networks and communications

With the inevitable move towards an interconnected electronic society, the security of electronic interactions and data, and the software that handles them, is emerging as an important enabling criterion. The ability to develop secure and trusted code, designed to withstand malicious and inadvertent attacks, has become an essential skill for a software developer/engineer. This unit promotes understanding and appreciation of the importance of developing secure and trusted software in today's electronic world by demonstrating possible attacks and their consequences. Here students are introduced to some of the most common security issues involved in the development of software, including secure coding practices, secure database access, secure data communications, security of web applications, use of encryption techniques and security testing. Students are provided with a range of practical exercises to reinforce their skills, including authenticating and authorizing users programmatically, user input validation, developing secure web applications, developing secure mobile/wireless applications, developing secure database applications, encrypting and hashing data programmatically, generating digital signatures programmatically, security testing, designing logging and auditing mechanisms.

Learning outcomes

Knowledge and Understanding

Students will understand some of the main security concepts and issues involved in the development of software, including:

- Software security versus other aspects of computer security
- Goals of secure and trusted software
- Vulnerabilities versus threats
- Secure software development principles and practices
- Buffer overflows and other secure software loopholes
- Security of programming platforms
- Authentication and authorization
- Principle of least privilege
- Security features are not equal to secure features
- Secure use of encryption
- User input validation
- Reliable software components
- Data privacy
- Auditing and logging
- Security testing Attitudes, Values and Beliefs

Students will acquire an understanding and appreciation of the importance of developing secure software in today's electronic world. They will also learn that security features are not equal to secure features.

Practical Skills

In developing secure and trusted software, students will be able to:

- Design applications with security in mind
- Validate user input
- Implement secure authentication mechanisms
- Authorise user's access to various protected resources
- Constructing trusted applications using cryptography
- Store session data securely in web applications
- Perform secure database access
- Set up secure transfer of data
- Create security logs
- Test software for security vulnerabilities

Workload

- two-hour lecture and
- two-hour tutorial (or laboratory) (requiring preparation in advance)
- 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

Before attempting this unit you must have satisfactorily completed

- FIT1019 Introduction to Security. AND
- FIT1002 Computer Programming, or equivalent.

You should also have

- programming skills in either Java or C#,
- familiarity with a relational database and the SQL query language
- familiarity with the web environment and web-based applications
- understanding of basic network concepts

Relationships

FIT3105 is a core unit of the Security major of BITS.

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 - !3PM - Friday

Lecturer(s) :

Dr Phu Le
Fax +61 3 9903 1247

Tutor(s) :

Dr Phu Le
Fax +61 3 9903 1247

Additional communication information

Dr. Phu Dung Le

Phone: +61 3 9903 23 99

Office: Faculty of IT - Monash university

900 Dandenong Rd, Caulfield East Vic 3145, Australia

H.706

Teaching and learning method

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 software design and implementation	
2	Principles of secure software design and implementation	
3	Principles of secure software design and implementation (continued)	
4	Computer system software problems and solutions	
5	Cryptography and secure software applications	
6	Cryptography and computer software practice (continued)	
7	Large computer software and security	
8	Concurrent programming and software security	assignment 1 due 4PM - Friday
9	Building secure distributed applications	
10	Secure software testing and verification	
11	Secure software testing and verification (continued)	
Mid semester break		
12	Research in secure software design and implementation	assignment 2 due 4PM - Friday
13	Revision	

Unit Resources

Prescribed text(s) and readings

- Howard, M. and LeBlank, D. (2002), "Writing secure code", 2nd edn, Microsoft Press, Redmond.
- Online references supplied on the unit website Text books are available from the Monash University Book Shops. Availability from other suppliers cannot be assured. The Bookshop orders texts in specifically for this unit. You are advised to purchase your text book early.

Recommended text(s) and readings

- http://www.windowsecurity.com/articles/Analysis_of_Buffer_Overflow_Attacks.html
- http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/8.pdf (Testing C programs for vulnerabilities)
- http://www.cgisecurity.com/lib/sips.html (Perl scripts and security issues)
- http://www.mirrors.wiretapped.net/security/info/reference/nist/special-publications/sp-800-8.txt (SQL and security issues)

Equipment and consumables required or provided

Students studying off-campus are required to have the minimum system configuration specified by the Faculty as a condition of accepting admission, and regular Internet access. On-campus students, and those studying at supported study locations may use the facilities available in the computing labs. Information about computer use for students is available from the ITS Student Resource Guide in the Monash University Handbook. You will need to allocate up to **n** hours per week for use of a computer, including time for newsgroups/discussion groups.

Study resources

Study resources we will provide for your study are:

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

Assignment tasks

- ### Assignment Task

  Title : assignment 1

  Description :

  Identify software design and implementation vulnerabilities and propose solutions.

  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 : 4PM - Friday - Week 8

- ### Assignment Task

  Title : assignment 2

  Description :

  Design and implementation secure applications using cryptography.

  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 : 4PM - Friday - Week 12

Examinations

- ### Examination

Weighting : 60%

Length : 3 hours

Type (open/closed book) : Closed book

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 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.