Unit Outline: KXC362 Computer Security

September 2007 - February 2008
Hangzhou, China

Prerequisites
KXC151

Corequisites
None

Unit Weight
12.5% of one academic year

Unit Coordinator
Soon-ja Yeom

Lecturing Staff
Mr. Liu Duan-yang
Email: ldy@zjut.edu.cn

Scheduled Teaching Sessions
Lectures: 3 hr/wk
Tutorials: 1 hr/wk (from week 2)

Unit Website
The unit website is accessed from http://www.utas.edu.au/coursesonline/. You will need to use your University of Tasmania email pop account username and password to log on to the WebCT system. Once authenticated by the system your personalised MyWebCT area will be displayed. It contains links to the websites that you have permission to access - including the website for this unit.

This unit is Web Supplemented. This means that the use of the Web is optional for this unit. The unit website contains unit information and resources.

If you are not able to access the unit website, please contact the technical staff at ZUT.

University Website
Information and Resources for 'Current Students' are available on the university website at: http://www.utas.edu.au/students/

Provider
School of Computing - Faculty of Science, Engineering, and Technology.

OVERVIEW

Introduction
This unit aims to introduce students to the principles behind the techniques and strategies that can be used to keep computer systems at a desired level of security. It is designed to alert anyone who might have responsibility for a computer system to the security issues that they should consider and equip them with an understanding of how to establish the threats that they might face and the ability to evaluate the techniques that they can use to counter these threats.

These techniques include threat and risk analysis, the characteristics of encryption algorithms and how to use these to achieve particular security goals, authentication techniques, operating system and network security, Internet security and associated protocols, concluding with business continuity planning.

Objectives
On successful completion of this unit, you will be able to:

1. Analyse the threats and vulnerabilities in computer systems and evaluate countermeasures
2. Use the principles and justify the application of security countermeasures such as policies, physical security, access control, cryptography, operating system security and network security techniques
3. Evaluate the various protocols for electronic authentication of identity
4. Explain the process of creating a business continuity plan
5. Work in a team to research and produce a solution to a problem concerning a computer security technique, application or problem

Unit Content
The following list provides an indication of the topics which will be covered in the unit.

1. Overview of unit content and introductory concepts
2. Threats, Risk Analysis and Security policies
3. Established Business Techniques
4. Physical Access Control
5. Authentication and Logical Access Control
6. Cryptography and cryptographic algorithms
7. Using cryptographic algorithms to achieve security goals
8. SNMPv3
9. Kerberos
10. Digital signatures
11. Security in Operating systems
12. Security standards
13. Network Security
14. Firewalls
15. Intrusion Detection
Generic Skills

The university has defined a set of generic graduate attributes expected in its graduates. Your course is designed to enable you to develop generic skills that are valued in, and expected of, graduates. These are skills that you will need to develop over time. Hence you are encouraged to look for opportunities, as you study each unit, to reflect on and improve these skills.

In this unit these skills are specifically targeted:

Knowledge: Students will have the opportunity to apply their technical and information skills and learn co-operatively by working together in the assignment case study.

Communication Skills: Students will further develop their communication skills and ability to write reports by giving presentations in tutorials and submitting a written tender proposal.

Problem-solving skills: Students will be required to conceptualise problems and formulate a range of solutions by working effectively with others to produce a written tender proposal.

Social Responsibility: Students will learn to acknowledge the social and ethical implications of their actions by examining the results of hacking and computer fraud.

LEARNING AND TEACHING

Approach to Learning

You are expected to spend about 130 hrs studying in this unit - this includes attendance at scheduled teaching sessions. (For a 13 week semester this is, on average, 10 hr/wk.) This is the amount of study time that the ‘typical’ student will need to reach the level of competence and understanding required to fulfil the unit objectives.

You are expected to:
- attend all scheduled lectures and tutorials, unless otherwise notified by the unit coordinator
- prepare for, and actively participate in lectures and tutorials
- complete the assigned learning tasks
- review what has been learnt
- complete assessment items and submit them on time
- access and be familiar with the information and resources available on the unit website
- seek help from teaching staff if you have any questions or difficulties in studying this unit

You are encouraged to read the university’s Code of Conduct for Teaching and Learning. Part A describes the ‘Responsibility of the University to Students’ and part B describes the ‘Responsibilities of Students to the University’. http://www.utas.edu.au/tl/policies/codes.html

Schedule

See the ‘Schedule’ section on the unit website.

Teaching and Support Staff

Teaching Staff

Unit Coordinator:

Soon-ja Yeom
E-Mail: S.Yeom@utas.edu.au

Lecturing Staff

Mr. Liu Duan-yang
Email: ldy@zjut.edu.cn

School Help Desk

Contact technical staff at ZUT for information about accessing and using the Computer labs.

University Services and Support

The University has staff available to assist you, such as the:
- Learning Development Advisor
- Student Counselor
- Careers Advisor
- Disability Officer

For more information and contact details see the Services and Support section on the University ‘Current Students’ web page. http://www.utas.edu.au/students/

Resources

Unit Website

The unit website contains unit information and resources. You will need to look at and use the resources that it contains. This site also supports your assignment work and is designed to help you with your examination preparation.

Prescribed Text

None
Readings


A list of readings referred to in the lecture slides can be found on the unit website in the resources area. The reference list is intended as a resource to help you with understanding the unit content when you need some extra explanations, or material for an assignment.

I have added my comments about the strengths of each book. For example:

Gollmann, D. 2000, Computer Security, John Wiley and Sons [especially good on operating system security and access control]

Software

The software that you will need to access the unit website and to study this unit, including general purpose software such as word processors, is provided on the computers in the computing labs. If you intend to use software on other computers please check that the versions are compatible.

You will be using the email security software called PGP - Pretty Good Privacy for one tutorial in this unit. A copy of the freeware version is provided on CD.

ASSESSMENT

| Assessment Items | Item 1 | Title: Assignment 1  
| Type: In-Semester - learning tasks  
| Weighting: 10%  
| Due: To be advised  |
| | There will be six take home pieces of work that you will have to complete within 24 hours. Your score on each of your five best of these will be used to calculate your result, based on each of the five contributing up to 2% of your overall mark.  |

| Item 2 | Title: Assignment 2 - Tender Proposal for a Case Study  
| Type: In-Semester - group assignment  
| Weighting: 20%  
| Due: Friday 14th Dec at 3pm  |
| | This assignment is a group assignment. It requires you to work steadily during semester, beginning with the second tutorial. Tutorials 2, 3, 4, 7, 8, and 10 provide you with an opportunity to develop and obtain feedback on your ideas for the content of this assignment.  |

| Item 3 | Title: Formal Examination  
| Type: Formal Examination  
| Weighting: 70%  
| Due: University Examination Period  |
| | Students are allowed to take two A4 sides of handwritten notes into the exam. These notes are handed in with the exam paper.  |

See the 'Assessment' section in unit website for more detailed information about assessment items.

In-Semester Assessment

Unless specifically stated in the specification of the assessment item provided on the unit website, it is required that:

✦ work submitted by a student is the work of that student alone OR
✦ where the assessment item is to be completed by a group of students, the work submitted by the group of students is the work of that group of students alone.

Plagiarism

Plagiarism is a form of cheating. It is taking and using someone else's thoughts, writings or inventions and representing them as your own, for example:

✦ using an author's words without putting them in quotation marks and citing the source;
✦ using an author's ideas without proper acknowledgment and citation; or
✦ copying another student's work.

If you have any doubts about how to refer to the work of others in your assignments, please consult your lecturer or tutor for relevant referencing guidelines, and the academic integrity resources on the web at [http://www.utas.edu.au/tl/supporting/academicintegrity/index.html](http://www.utas.edu.au/tl/supporting/academicintegrity/index.html).

The intentional copying of someone else's work as one's own is a serious offence punishable by penalties that may range from a fine or deduction/cancellation of marks and, in the most serious of cases, to exclusion from a unit, a course or the University. Details of penalties that can be imposed are available in the Ordinance of Student Discipline – Part 3 Academic Misconduct, see
The University reserves the right to submit assignments to plagiarism detection software, and might then retain a copy of the assignment on its database for the purpose of future plagiarism checking.

Referencing

The university document on plagiarism contains information about referencing the work or ideas of others. (See http://www.utas.edu.au/plagiarism/.) The preferred text referencing systems for the School is the Harvard system (also referred to as the author-date system).

Submissions

The details of the submission method (paper, electronic or other) for each assignment will be supplied in a separate assignment specification sheet. All in-semester assignment submissions (including electronic submissions) are to include an Assignment Cover Sheet which includes a statement confirming that the submission is your own work. If this undertaking is not signed, the assignment will not be marked. The Assignment Cover Sheet is available on the School’s web site http://www.comp.utas.edu.au/app/studyresources.jsp.

Extensions

Assessment items will not be accepted after the due date except under the conditions stated in the school policy on late assessment. http://www.comp.utas.edu.au/app/late_assess.jsp

Formal Examination

The formal examination will be held at ZUT, Hangzhou, and is conducted by the University Registrar.

Final Grade

Overall assessment will be based on the student’s performance throughout the semester as well as in a formal examination. In order to achieve a pass (or better) result, a student must obtain:

1. at least 45% of the total mark for in-semester assessment items
2. at least 45% of the mark for the formal examination
3. at least 50% of the overall mark

In order to comply with the benchmarks set by the Faculty of Science, Engineering & Technology for distribution of grades in units, both the in-semester and examination marks that students obtain may be adjusted either upwards or downwards. See http://fcms.its.utas.edu.au/scieng/scieng/policies.asp for details of the Faculty Assessment Guidelines.

Passing grades will be awarded based on the AVCC guidelines:

- PP at least 50% of the overall mark but less than 60%
- CR at least 60% of the overall mark but less than 70%
- DN at least 70% of the overall mark but less than 80%
- HD at least 80% of the overall mark

The maximum mark awarded to a student who fails the unit will be 44.

For more information, including other grades such as Supplementary and Terminating grades, see the School of Computing’s guidelines for assessment - available at: http://www.comp.utas.edu.au/app/assess.jsp