ITEC855

Security Technologies and Forensic Analysis

S1 Evening 2016

Dept of Computing

Contents

General Information	2
Learning Outcomes	2
Assessment Tasks	3
Delivery and Resources	4
Unit Schedule	5
Policies and Procedures	5
Graduate Capabilities	7
Grading	10

General Information

Unit convenor and teaching staff
Udaya Tupakula
udaya.tupakula@mq.edu.au
Contact via udaya.tupakula@mq.edu.au
321, E6A
By Appointment

Credit points
4

Prerequisites
COMP343 or ITEC647

Corequisites

Co-badged status

Unit description
This unit covers the fundamental technologies and processes that underpin good systems security management within modern organisations. We consider the underlying mechanics of information and communications technology security infrastructures, risk management, attack modelling, software security, firewalls, intrusion detection and forensics.

Important Academic Dates

Information about important academic dates including deadlines for withdrawing from units are available at https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

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

Analyse the key security requirements and trends in software security and interconnected systems

Analyse techniques for exploiting software and networks

Design and/or apply security techniques to mitigate software and network attacks

Evaluate security techniques used to deal with the attacks

Present and discuss concepts related to software and network security at a postgraduate level

Assessment Tasks

Name	Weighting	Due
Quiz	10%	04/04/2016 (Week 6)
Project	30%	29/05/2016
Exam	60%	TBC

Quiz

Due: **04/04/2016 (Week 6)**
Weighting: **10%**

Quiz (closed book) will be based on your previously covered lecture material for weeks 1-5. The quiz questions will be handed over to you at the beginning of your Lecture class. It will be about 1 hour and consists of short answer questions. Quiz will be followed by discussion on the solutions. Quiz will serve as a feedback mechanism to monitor your progress in the unit.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems
- Analyse techniques for exploiting software and networks

Project

Due: **29/05/2016**
Weighting: **30%**

Group project with 2-3 students per group. Projects will be related to security issues with emerging technologies such as smart grid and cloud. The project reports are due on 29th May 2016; 11:59 pm (electronically). In addition, each group is allocated a time slot for presenting their work during Week 12 (30th May) OR Week 13 (6th June). Each student in the group is expected to present their work which will be followed by QA session. The QA session will be conducted by the panel (which includes convener and/or other staff members and/or PhD students within the computing department). The presentation and QA session will help the panel to evaluate the individual contribution of each student. The Project will account to 30% (Report-10%, Presentration-10% and QA-10%) of the marks.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems
- Analyse techniques for exploiting software and networks

- Design and/or apply security techniques to mitigate software and network attacks
- Evaluate security techniques used to deal with the attacks
- Present and discuss concepts related to software and network security at a postgraduate level

Exam

Due: **TBC**
Weighting: **60%**

Need to obtain atleast 40% in the Exam component to pass the unit. The exam will be a written exam with questions from topics covered in the lectures. It will be held in the usual examination period of the semester. Students have 3 hours written time plus 10 minutes reading time for the exam.

On successful completion you will be able to:

- Analyse the key security requirements and trends in software security and interconnected systems
- Analyse techniques for exploiting software and networks
- Design and/or apply security techniques to mitigate software and network attacks
- Evaluate security techniques used to deal with the attacks

Delivery and Resources

Technology:

- Presentations using Powerpoint
- Other computer related material

Lecture and Tutorial:

- Provided in Unit Schedule

All unit information will be posted on iLearn (https://ilearn.mq.edu.au/login/MQ/). We assume that students will regularly check iLearn for information regarding lecture notes and other related resources.

It should be noted that no single text book completely covers the content of this unit. Below books are recommended (not compulsory) for the course.

References:

- Gary McGraw, Software Security: Building Security IN, Addison-Wesley
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, Fourth Edition.
- Stuart McClure, Joel Scambray, George Kurtz, Hacking exposed 7: Network Security

Secrets & Solutions, Mc Graw Hill.

- Building Secure Software, How to avoid security problems the right way, John Viega, Gary McGraw, Addison-Wesley.
- Dafydd Stuttard, Marcus Pinto,The Web Application Hackers Handbook, Wiley, 2nd Edition.
- Howard and LeBlanc, Writing Secure Code, Microsoft Press, 2nd edition

Unit Schedule

S.No	Date	Topic
Week 1	29/02	Introduction
Week 2	07/03	Risk management framework for software security
Week 3	14/03	Software security attacks analysis
Week 4	21/03	Network security attacks analysis
Week 5	28/03	Public Holiday
Week 6	04/04	Quiz, Solutions and Group project assigned; Penetration Testing
Break		
Week 7	25/04	Public Holiday
Week 8	02/05	Security techniques, tools and analysis
Week 9	09/05	Advanced security techniques for software systems
Week 10	16/05	Advanced security techniques for networks
Week 11	23/05	Software assurance
Week 12	30/05	Group project assessment
Week 13	06/06	Group project assessment, Revision

*Lecture contents can vary depending on the progress

*Lecture slides available on iLearn: Monday 1:00pm

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central. Students should be aware of the following policies in particular with regard to Learning and Teaching:

Academic Honesty Policy http://mq.edu.au/policy/docs/academic_honesty/policy.html

New Assessment Policy in effect from Session 2 2016 http://mq.edu.au/policy/docs/assessment/policy_2016.html. For more information visit http://students.mq.edu.au/events/2016/07/19/new_assessment_policy_in_place_from_session_2/

Assessment Policy prior to Session 2 2016 http://mq.edu.au/policy/docs/assessment/policy.html

Grading Policy prior to Session 2 2016 http://mq.edu.au/policy/docs/grading/policy.html

Grade Appeal Policy http://mq.edu.au/policy/docs/gradeappeal/policy.html

Complaint Management Procedure for Students and Members of the Public http://www.mq.edu.au/policy/docs/complaint_management/procedure.html

Disruption to Studies Policy http://www.mq.edu.au/policy/docs/disruption_studies/policy.html *The Disruption to Studies Policy is effective from March 3 2014 and replaces the Special Consideration Policy.*

In addition, a number of other policies can be found in the Learning and Teaching Category of Policy Central.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/support/student_conduct/

Results

Results shown in *iLearn*, or released directly by your Unit Convenor, are not confirmed as they are subject to final approval by the University. Once approved, final results will be sent to your student email address and will be made available in eStudent. For more information visit ask.mq.edu.au.

Student Support

Macquarie University provides a range of support services for students. For details, visit http://students.mq.edu.au/support/

Learning Skills

Learning Skills (mq.edu.au/learningskills) provides academic writing resources and study strategies to improve your marks and take control of your study.

- Workshops
- StudyWise
- Academic Integrity Module for Students
- Ask a Learning Adviser

Student Services and Support

Students with a disability are encouraged to contact the Disability Service who can provide appropriate help with any issues that arise during their studies.

Student Enquiries

For all student enquiries, visit Student Connect at ask.mq.edu.au

IT Help

For help with University computer systems and technology, visit http://www.mq.edu.au/about_us/offices_and_units/information_technology/help/.

When using the University's IT, you must adhere to the Acceptable Use of IT Resources Policy. The policy applies to all who connect to the MQ network including students.

Graduate Capabilities

PG - Capable of Professional and Personal Judgment and Initiative

Our postgraduates will demonstrate a high standard of discernment and common sense in their professional and personal judgment. They will have the ability to make informed choices and decisions that reflect both the nature of their professional work and their personal perspectives.

This graduate capability is supported by:

Learning outcomes

- Analyse the key security requirements and trends in software security and interconnected systems
- Analyse techniques for exploiting software and networks
- Design and/or apply security techniques to mitigate software and network attacks
- Evaluate security techniques used to deal with the attacks
- Present and discuss concepts related to software and network security at a postgraduate level

Assessment tasks

- Quiz
- Project
- Exam

PG - Discipline Knowledge and Skills

Our postgraduates will be able to demonstrate a significantly enhanced depth and breadth of knowledge, scholarly understanding, and specific subject content knowledge in their chosen fields.

This graduate capability is supported by:

Learning outcomes

- Analyse the key security requirements and trends in software security and interconnected systems
- Analyse techniques for exploiting software and networks

- Design and/or apply security techniques to mitigate software and network attacks
- Evaluate security techniques used to deal with the attacks
- Present and discuss concepts related to software and network security at a postgraduate level

Assessment tasks

- Quiz
- Project
- Exam

PG - Critical, Analytical and Integrative Thinking

Our postgraduates will be capable of utilising and reflecting on prior knowledge and experience, of applying higher level critical thinking skills, and of integrating and synthesising learning and knowledge from a range of sources and environments. A characteristic of this form of thinking is the generation of new, professionally oriented knowledge through personal or group-based critique of practice and theory.

This graduate capability is supported by:

Learning outcomes

- Analyse the key security requirements and trends in software security and interconnected systems
- Design and/or apply security techniques to mitigate software and network attacks
- Evaluate security techniques used to deal with the attacks
- Present and discuss concepts related to software and network security at a postgraduate level

Assessment tasks

- Quiz
- Project
- Exam

PG - Research and Problem Solving Capability

Our postgraduates will be capable of systematic enquiry; able to use research skills to create new knowledge that can be applied to real world issues, or contribute to a field of study or practice to enhance society. They will be capable of creative questioning, problem finding and problem solving.

This graduate capability is supported by:

Learning outcomes

- Analyse the key security requirements and trends in software security and interconnected systems
- Design and/or apply security techniques to mitigate software and network attacks
- Evaluate security techniques used to deal with the attacks
- Present and discuss concepts related to software and network security at a postgraduate level

Assessment tasks

- Quiz
- Project
- Exam

PG - Effective Communication

Our postgraduates will be able to communicate effectively and convey their views to different social, cultural, and professional audiences. They will be able to use a variety of technologically supported media to communicate with empathy using a range of written, spoken or visual formats.

This graduate capability is supported by:

Learning outcome

- Present and discuss concepts related to software and network security at a postgraduate level

Assessment task

- Project

PG - Engaged and Responsible, Active and Ethical Citizens

Our postgraduates will be ethically aware and capable of confident transformative action in relation to their professional responsibilities and the wider community. They will have a sense of connectedness with others and country and have a sense of mutual obligation. They will be able to appreciate the impact of their professional roles for social justice and inclusion related to national and global issues

This graduate capability is supported by:

Learning outcomes

- Analyse techniques for exploiting software and networks
- Present and discuss concepts related to software and network security at a postgraduate level

Assessment tasks

- Quiz
- Project
- Exam

Grading

At the end of the semester, you will receive a grade that reflects your achievement in the unit

- Fail (F): does not provide evidence of attainment of all learning outcomes. There is missing or partial or superficial or faulty understanding and application of the fundamental concepts in the field of study; and incomplete, confusing or lacking communication of ideas in ways that give little attention to the conventions of the discipline.
- Pass (P): provides sufficient evidence of the achievement of learning outcomes. There is demonstration of understanding and application of fundamental concepts of the field of study; and communication of information and ideas adequately in terms of the conventions of the discipline. The learning attainment is considered satisfactory or adequate or competent or capable in relation to the specified outcomes.
- Credit (Cr): provides evidence of learning that goes beyond replication of content knowledge or skills relevant to the learning outcomes. There is demonstration of substantial understanding of fundamental concepts in the field of study and the ability to apply these concepts in a variety of contexts; plus communication of ideas fluently and clearly in terms of the conventions of the discipline.
- Distinction (D): provides evidence of integration and evaluation of critical ideas, principles and theories, distinctive insight and ability in applying relevant skills and concepts in relation to learning outcomes. There is demonstration of frequent originality in defining and analysing issues or problems and providing solutions; and the use of means of communication appropriate to the discipline and the audience.
- High Distinction (HD): provides consistent evidence of deep and critical understanding in relation to the learning outcomes. There is substantial originality and insight in identifying, generating and communicating competing arguments, perspectives or problem solving approaches; critical evaluation of problems, their solutions and their implications; creativity in application.

In this unit, your final grade depends on your performance in each part of the assessment. For each task, you receive a mark that combines your standard of performance regarding each learning outcome assessed by this task. Then the different component marks are added up

to determine your total mark out of 100. Your grade then depends on this total mark and your overall standards of performance.

Concretely, in order to pass the unit, you must

- obtain a total mark of 50% or higher and a mark of 40% or higher in the final examination;
- make a reasonable attempt at the exercises in the assessment tasks;
- demonstrate that you can perform at a Functional level or higher for each criterion assessed in the Quiz and Group Project/Presentation.
- reach a Functional level or higher for each criterion assessed in the final examination.

Students obtaining a higher grade than a pass in this unit will (in addition to the above)

- have a total mark of 85% or higher and perform at distinction level or higher in the final examination to obtain High Distinction;
- have a total mark of 75% or higher and perform at credit level or higher in the final examination to obtain Distinction;
- have a total mark of 65% or higher and perform at pass level but with 50% or higher in the final examination to obtain Credit.