



# ITEC855

## Security and Forensic Discovery

S1 Evening 2014

*Computing*

### Contents

---

<a href="#"><u>General Information</u></a>	2
<a href="#"><u>Learning Outcomes</u></a>	2
<a href="#"><u>Assessment Tasks</u></a>	3
<a href="#"><u>Delivery and Resources</u></a>	4
<a href="#"><u>Unit Schedule</u></a>	5
<a href="#"><u>Learning and Teaching Activities</u></a>	6
<a href="#"><u>Policies and Procedures</u></a>	6
<a href="#"><u>Graduate Capabilities</u></a>	7
<a href="#"><u>Standards</u></a>	10

---

#### **Disclaimer**

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

## General Information

Unit convenor and teaching staff

Unit Convenor

Udaya Tupakula

[udaya.tupakula@mq.edu.au](mailto:udaya.tupakula@mq.edu.au)

Contact via [udaya.tupakula@mq.edu.au](mailto:udaya.tupakula@mq.edu.au)

321, E6A

Monday: 5.00 - 6.00 pm or by appointment

Credit points

4

Prerequisites

COMP342 or COMP343 or COMP347

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, security requirements, security architectures and models, cryptography, secure protocols, authentication, key management, PKI, access control, auditing and intrusion detection.

## 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 security of software and interconnected systems
- Analyse techniques for exploiting software and networks
- Apply security techniques to mitigate software and network attacks
- Understand and evaluate security techniques used to deal with the attacks and concepts for providing software assurance
- Advance skills and clearly communicate concepts related to software security at a

postgraduate level.

## Assessment Tasks

Name	Weighting	Due
Quiz	25%	Week 6
Project	25%	Week 11
Exam	50%	TBC

### Quiz

Due: **Week 6**

Weighting: **25%**

Quiz (close 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 multiple choice and 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 security of software and interconnected systems
- Analyse techniques for exploiting software and networks

### Project

Due: **Week 11**

Weighting: **25%**

Project Assigned on Week 6

Report: 8%

Content and Understanding: 9%

Presentation: 8%

The task is group based with individual contributions clearly outlined

Students are expected to contribute in all the components of the project: project report, content and understanding and presentation

Project reports can be submitted on iLearn (<https://ilearn.mq.edu.au/login/MQ>)

On successful completion you will be able to:

- Analyse the key security requirements and trends in security of software and interconnected systems
- Analyse techniques for exploiting software and networks
- Apply security techniques to mitigate software and network attacks
- Understand and evaluate security techniques used to deal with the attacks and concepts for providing software assurance
- Advance skills and clearly communicate concepts related to software security at a postgraduate level.

## Exam

Due: **TBC**

Weighting: **50%**

Need to obtain atleast 30% in the Exam component to pass the unit.

The exam will be a written exam with some multiple choice and 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 security of software and interconnected systems
- Analyse techniques for exploiting software and networks
- Apply security techniques to mitigate software and network attacks
- Understand and evaluate security techniques used to deal with the attacks and concepts for providing software assurance
- Advance skills and clearly communicate concepts related to software security at a postgraduate level.

## Delivery and Resources

Technology:

- Presentations using Powerpoint
- Other computer related material

Lecture and Tutorial:

- Provided in Unit Schedule

ITEC855 is taught via lectures and sessions.

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
- Stuart McClure, Joel Scambray, George Kurtz, Hacking exposed 7: Network Security Secrets & Solutions, Mc Graw Hill.
- Charles P. Pfleeger, Shari Lawrence Pfleeger, Security in Computing, Prentice Hall, Fourth Edition.
- 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

<b>Week 1</b>	<b>Introduction</b>
<b>Week 2</b>	<b>Software security</b>
<b>Week 3</b>	<b>Software security attacks analysis</b>
<b>Week 4</b>	<b>Network security attacks analysis</b>
<b>Week 5</b>	<b>Penetration testing</b>
<b>Week 6</b>	<b>Quiz and Group project allocation</b>
<b>Week 7</b>	<b>Security techniques &amp; tools-1</b>
<b>Week 8</b>	<b>Security techniques &amp; tools- 2</b>
<b>Week 9</b>	<b>Software assurance techniques</b>
<b>Week 10</b>	<b>Building secure software</b>
<b>Week 11</b>	<b>Group project assessment</b>
<b>Week 12</b>	<b>Revision</b>
<b>Week 13</b>	<b>No lecture (Public Holiday)</b>

## Learning and Teaching Activities

### Learning Outcome test

this is test

## 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](http://mq.edu.au/policy/docs/academic_honesty/policy.html)

Assessment Policy <http://mq.edu.au/policy/docs/assessment/policy.html>

Grading Policy <http://mq.edu.au/policy/docs/grading/policy.html>

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

Grievance Management Policy [http://mq.edu.au/policy/docs/grievance\\_management/policy.html](http://mq.edu.au/policy/docs/grievance_management/policy.html)

Disruption to Studies Policy [http://www.mq.edu.au/policy/docs/disruption\\_studies/policy.html](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/](https://students.mq.edu.au/support/student_conduct/)

## 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](http://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](http://ask.mq.edu.au)

## IT Help

For help with University computer systems and technology, visit <http://informatics.mq.edu.au/help/>.

When using the University's IT, you must adhere to the [Acceptable Use Policy](#). The policy applies to all who connect to the MQ network including students.

## Graduate Capabilities

### 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 outcome

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

#### 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 security of software and

interconnected systems

- Analyse techniques for exploiting software and networks
- Apply security techniques to mitigate software and network attacks

## **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**

- Understand and evaluate security techniques used to deal with the attacks and concepts for providing software assurance
- Advance skills and clearly communicate concepts related to software security at a postgraduate level.

## **Assessment tasks**

- 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 outcomes**

- Analyse the key security requirements and trends in security of software and interconnected systems
- Understand and evaluate security techniques used to deal with the attacks and concepts for providing software assurance
- Advance skills and clearly communicate concepts related to software security at a



postgraduate level.

## **Assessment tasks**

- Project
- Exam

## **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 the key security requirements and trends in security of software and interconnected systems
- Advance skills and clearly communicate concepts related to software security at a postgraduate level.

### **Assessment task**

- Project

## **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**

- Apply security techniques to mitigate software and network attacks
- Understand and evaluate security techniques used to deal with the attacks and concepts for providing software assurance
- Advance skills and clearly communicate concepts related to software security at a postgraduate level.

### **Assessment tasks**

- Project
- Exam

## Standards

Grade	Learning Outcome 1	Learning Outcome 2	Learning Outcome 3	Learning Outcome 4	Learning Outcome 5
	Security Requirements	Security Attacks	Security Techniques	Software Assurance	Critical thinking and communication skills
HD	Demonstrates deep and critical understanding of the security requirements and shows originality in the analysis and evaluation.	Critical understanding of the security attacks and root cause identification and analysis of the attacks.	Deep understanding of the security techniques, ability to design and develop security solutions to deal with the security attacks. Shows originality in the application of security technique and evaluate their effectiveness	Novel use of the security techniques and excellent understanding of concepts for building secure software and improving software assurance.	Demonstrate original ideas, superior analysis and effective communication skills on the issues related to complex problems.
D	Demonstrate good understanding and shows some originality in their analysis.	Good understanding of the security attacks and ability to relate them with the weakness in software and networks.	Good understanding of the security techniques, ability to design and develop security solutions and perform their analysis.	Good understanding of the concepts for building secure software and improving software assurance.	Demonstrate deep insights, and effective communication on the issues related to complex problems.
Credit	Reasonable understanding of the security requirements and able to describe them.	Clear understanding of the security attacks and able to analyse the attacks.	Reasonable understanding of the security techniques, ability to apply them to counteract attacks.	Reasonable understanding of the concepts for building secure software and improving software assurance.	Provides evidence of clear understanding and good communication on the issues related to complex problems.
Pass	Basic understanding of some of the security requirements	Basic understanding of the security attacks	Basic understanding of the security techniques and ability to apply them to counteract some of the attacks.	Some understanding of the concepts for building secure software and improve software assurance.	Provides evidence of some understanding and able to present on the issues related to complex problems.

### 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 30% 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.