ITEC852
Advanced System and Network Security
S2 Evening 2017
Dept of Computing

Contents

General Information 2
Learning Outcomes 2
General Assessment Information 3
Assessment Tasks 5
Delivery and Resources 8
Unit Schedule 8
Learning and Teaching Activities 9
Policies and Procedures 10
Graduate Capabilities 11

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
Adjunct Lecturer
Milton Baar
milton.baar@mq.edu.au
Contact via 04 1927 9847
By appointment

Adjunct Lecturer
Damian Jurd
damian.jurd@mq.edu.au
Contact via damian.jurd@mq.edu.au
By appointment

Credit points
4

Prerequisites
ITEC647

Corequisites

Co-badged status

Unit description
As organisations and users increasingly rely upon networked applications for assessing information and making critical business decisions, securing distributed applications is becoming extremely significant. The unit is concerned with the protection of information in computing systems and networks. It will address concepts and techniques for securing distributed applications.

Important Academic Dates
Information about important academic dates including deadlines for withdrawing from units are available at http://students.mq.edu.au/student_admin/enrolmentguide/academicdates/

Learning Outcomes

1. Analyse key security requirements and trends in a distributed networked computing environment

2. Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
3. Evaluate authentication and access control security functionalities in distributed systems and networks
4. Apply security techniques and mechanisms to develop security protocols
5. Analyse the security threats and develop security architecture and functionalities to counteract the security threats

General Assessment Information

<table>
<thead>
<tr>
<th>Grade</th>
<th>Learning Outcome 1</th>
<th>Learning Outcome 2</th>
<th>Learning Outcome 3</th>
<th>Learning Outcome 4</th>
<th>Learning Outcome 5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Demonstrates deep and critical understanding of key security requirements and shows substantial originality in their analysis and evaluation</td>
<td>A critical understanding of security threats and able to develop threat model. Able to design appropriate security functionalities and develop an overall security architecture</td>
<td>Demonstrates the ability to apply security techniques and mechanisms to identify flaws in security protocols. Demonstrate the ability to design secure protocols and carry out security analysis.</td>
<td>Demonstrates the ability to design security services for distributed systems and networks and carry out their security analysis.</td>
<td>Demonstrates significant originality and insight in critical evaluation of security solutions. Communicates effectively the analysis and the arguments</td>
</tr>
<tr>
<td>Grade</td>
<td>Description</td>
<td>Grade</td>
<td>Description</td>
<td>Grade</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>D</td>
<td>Demonstrates good understanding of the security requirements and shows some originality in their analysis</td>
<td>Credit</td>
<td>Reasonable understanding of key security requirements and able to describe their characteristics</td>
<td>Pass</td>
<td>Basic understanding of the security threats in a system</td>
</tr>
<tr>
<td></td>
<td>Demonstrates a clear understanding of threats and threat models. Demonstrates the ability to describe the design of security architecture and its functionalities</td>
<td></td>
<td>Shows substantial understanding of security threats. Able to understand the security functionalities in a security architecture</td>
<td></td>
<td>Recognizes the security threats in a system</td>
</tr>
<tr>
<td></td>
<td>Demonstrates the ability to apply security techniques and mechanisms to identify security flaws in protocols and carry out security analysis.</td>
<td></td>
<td>Demonstrates the ability to apply security techniques and mechanisms to describe security protocols and carry out some analysis.</td>
<td></td>
<td>Demonstrates the ability to apply</td>
</tr>
<tr>
<td></td>
<td>Demonstrates a clear understanding of authentication and access control services in distributed systems and networks and the ability to analyse them</td>
<td></td>
<td>Good understanding of authentication and access control functionalities in distributed systems and networks. Able to carry out basic evaluation of these security services</td>
<td></td>
<td>Provides sufficient evidence</td>
</tr>
<tr>
<td></td>
<td>Demonstrates insights in solving security problems. Good presentation of ideas and arguments</td>
<td></td>
<td>Provides evidence of a clear understanding of the security concepts and their applications. Clear communication of ideas.</td>
<td></td>
<td>Provides sufficient evidence</td>
</tr>
</tbody>
</table>

**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.

Your final grade will depend on your performance in each part separately. **In particular, to pass this unit you must achieve an overall score of 50%, and achieve at least 40% in each of the quizzes and achieve at least 45% in the final exam.**

### Assessment Tasks

<table>
<thead>
<tr>
<th>Name</th>
<th>Weighting</th>
<th>Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exam</td>
<td>40%</td>
<td>Semester 2 exam period</td>
</tr>
<tr>
<td>Group Project - (C&amp;U, P, R)</td>
<td>30%</td>
<td>Week 10</td>
</tr>
<tr>
<td>Assignment</td>
<td>10%</td>
<td>Week 11</td>
</tr>
<tr>
<td>Week 4 quiz</td>
<td>10%</td>
<td>Week 4</td>
</tr>
<tr>
<td>Week 9 quiz</td>
<td>10%</td>
<td>Week 9</td>
</tr>
</tbody>
</table>
Exam

Due: **Semester 2 exam period**
Weighting: **40%**

Date to be confirmed by University.

Your final grade will depend on your performance in each part separately. In particular, to pass this unit, you must achieve an overall score of 50%, and achieve at least 50% in each of the quizzes and achieve at least 50% in the final exam. If you make a reasonable attempt at the quizzes and/or exam, and achieve a mark of at least 40% but less than 50%, you will be offered a second attempt at the quiz or exam for which you achieved at least 40% but less than 50%. If, after the second attempt, you fail to achieve at least 50%, you will not have passed that assessment task.

This Assessment Task relates to the following Learning Outcomes:

- Analyse key security requirements and trends in a distributed networked computing environment
- Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
- Evaluate authentication and access control security functionalities in distributed systems and networks
- Apply security techniques and mechanisms to develop security protocols
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Group Project - (C&U, P, R)

Due: **Week 10**
Weighting: **30%**

Group Project Allocation: Week 5

Due: electronic copies via Turnitin week 10

Presentations: Weeks 11 & 12

(C&U) Content and Understanding: 10% (Individually assessed via Q&A on the Project)

(P) Presentation: 10% (Individually assessed)

(R) Project Report: 10% (Assessed as a Group)

This Assessment Task relates to the following Learning Outcomes:
• Analyse key security requirements and trends in a distributed networked computing environment
• Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
• Apply security techniques and mechanisms to develop security protocols
• Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Assignment
Due: **Week 11**
Weighting: **10%**

Handed Out: **Week 1**
Due: via Turnitin, **Week 11**

Assignment on Security Mechanisms and Protocols

This Assessment Task relates to the following Learning Outcomes:
• Analyse key security requirements and trends in a distributed networked computing environment
• Apply security techniques and mechanisms to develop security protocols
• Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Week 4 quiz
Due: **Week 4**
Weighting: **10%**

This is an online quiz, conducted as an early diagnostic, in week 4.

It is a multiple choice quiz conducted during the lecture, it is closed book.

Your final grade will depend on your performance in each part separately. In particular, to pass this unit, you must achieve an overall score of 50%, and achieve at least 50% in each of the quizzes and achieve at least 50% in the final exam. If you make a reasonable attempt at the quizzes and/or exam, and achieve a mark of at least 40% but less than 50%, you will be offered a second attempt at the quiz or exam for which you achieved at least 40% but less than 50%. If, after the second attempt, you fail to achieve at least 50%, you will not have passed that assessment task.

This Assessment Task relates to the following Learning Outcomes:
• Analyse key security requirements and trends in a distributed networked computing environment
• Evaluate authentication and access control security functionalities in distributed systems and networks

Week 9 quiz

Due: Week 9
Weighting: 10%

This is an online quiz, conducted in week 9.

It is a "short answer" quiz conducted during the lecture; it is closed book.

Your final grade will depend on your performance in each part separately. In particular, to pass this unit, you must achieve an overall score of 50%, and achieve at least 50% in each of the quizzes and achieve at least 50% in the final exam. If you make a reasonable attempt at the quizzes and/or exam, and achieve a mark of at least 40% but less than 50%, you will be offered a second attempt at the quiz or exam for which you achieved at least 40% but less than 50%. If, after the second attempt, you fail to achieve at least 50%, you will not have passed that assessment task.

This Assessment Task relates to the following Learning Outcomes:
• Analyse key security requirements and trends in a distributed networked computing environment
• Evaluate authentication and access control security functionalities in distributed systems and networks

Delivery and Resources

Technology
• Presentation using Powerpoint and other Computer Related Material

Lecture and Tutorial
• Provided in Unit Schedule

Unit Schedule

Information
• 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, practical material and other related resources.

• All emails related to ITEC852 should be sent to milton.baar@mq.edu.au and CC: damian.jurd@mq.edu.au and must include your full name and your student id number.
Other Material

References

- Dieter Gollman, Computer Security, John Wiley

Tentative Lecture Schedule ITEC852 S2 2017 (may vary depending upon progress)

Week 1: Introduction: Cyber Security Trends and Concepts
Week 2: Threat Modelling
Week 3: Security Architecture
Week 4: Cryptography and Key Management
Week 5: Security Protocols
Week 6: Access Control Models
Week 8: Public Holiday, audio lecture provided as well as written material published on iLearn
Week 9: Distributed Systems Security, Cloud Computing Security
Week 11: Trusted Computing/ Group Project Presentations (1)
Week 12: Group Project Presentation (2)
Week 13: Revision

Learning and Teaching Activities

Lectures
Weekly lectures
Practical activities
Practical, hands-on activities used to explore concepts covered in weekly lectures

Guest speakers
Industry experts who provide a linkage between course material and industry practice and expectations

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

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
Unit guide ITEC852 Advanced System and Network Security

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

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

Equity 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.

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 - 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 key security requirements and trends in a distributed networked computing environment
- Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
- Evaluate authentication and access control security functionalities in distributed systems and networks
- Apply security techniques and mechanisms to develop security protocols
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Assessment tasks
- Exam
- Group Project - (C&U, P, R)
Learning and teaching activities

- Weekly lectures
- Practical, hands-on activities used to explore concepts covered in weekly lectures
- Industry experts who provide a linkage between course material and industry practice and expectations

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 key security requirements and trends in a distributed networked computing environment
- Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
- Evaluate authentication and access control security functionalities in distributed systems and networks
- Apply security techniques and mechanisms to develop security protocols
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Assessment tasks

- Exam
- Group Project - (C&U, P, R)
- Assignment
- Week 4 quiz
- Week 9 quiz

Learning and teaching activities

- Weekly lectures
- Practical, hands-on activities used to explore concepts covered in weekly lectures
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 key security requirements and trends in a distributed networked computing environment
- Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
- Evaluate authentication and access control security functionalities in distributed systems and networks
- Apply security techniques and mechanisms to develop security protocols
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats

**Assessment tasks**

- Exam
- Group Project - (C&U, P, R)
- Week 4 quiz

**Learning and teaching activities**

- Practical, hands-on activities used to explore concepts covered in weekly lectures

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**

- Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
- Apply security techniques and mechanisms to develop security protocols
Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Assessment tasks

• Group Project - (C&U, P, R)
• Week 9 quiz

Learning and teaching activities

• Industry experts who provide a linkage between course material and industry practice and expectations

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 key security requirements and trends in a distributed networked computing environment
• Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Assessment tasks

• Exam
• Group Project - (C&U, P, R)

Learning and teaching activities

• Weekly lectures
• Industry experts who provide a linkage between course material and industry practice and expectations

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

• Develop and/or advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.

• Evaluate authentication and access control security functionalities in distributed systems and networks

• Apply security techniques and mechanisms to develop security protocols

• Analyse the security threats and develop security architecture and functionalities to counteract the security threats

Assessment tasks

• Exam

• Group Project - (C&U, P, R)

Learning and teaching activities

• Practical, hands-on activities used to explore concepts covered in weekly lectures