ITEC852

Advanced System and Network Security

S2 Evening 2017

Dept of Computing

Contents

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 https://www.mq.edu.au/study/calendar-of-dates

Learning Outcomes

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

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

General Assessment Information

Grade

	Learning Outcome 1	Learning Outcome 2	Learning Outcome 3	Learning Outcome 4	Learning Outcome 5
	Security Requirements	Security Threats, Functionalities and Architecture	Security Protocols	Security services for distributed systems and networks	Research and Critical Thinking and Communication Skills
HD	Demonstrates deep and critical understanding of key security requirements and shows substantial originality in their analysis and evaluation	A critical understanding of security threats and able to develop threat model. Able to design appropriate security functionalities and develop an overall security architecture	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.	Demonstrates the ability to design security services for distributed systems and networks and carry out their security analysis.	Demonstrates significant originality and insight in critical evaluation of security solutions. Communicates effectively the analysis and the arguments
D	Demonstrates good understanding of the security requirements and shows some originality in their analysis	Demonstrates a clear understanding of threats and threat models. Demonstrates the ability to describe the design of security architecture and its functionalities	Demonstrates the ability to apply security techniques and mechanisms to identify security flaws in protocols and carry out security analysis.	Demonstrates a clear understanding of authentication and access control services in distributed systems and networks and the ability to analyse them	Demonstrates insights in solving security problems. Good presentation of ideas and arguments
Credit	Reasonable understanding of key security requirements and able to describe their characteristics	Shows substantial understanding of security threats. Able to understand the security functionalities in a security architecture	Demonstrates the ability to apply security techniques and mechanisms to describe security protocols and carry out some analysis.	Good understanding of authentication and access control functionalities in distributed systems and networks. Able to carry out basic evaluation of these security services	Provides evidence of a clear understanding of the security concepts and their applications. Clear communication of ideas.
Pass	Basic understanding	Recognizes the security threats in a system	Demonstrates the ability to apply	Basic understanding of authentication	Provides sufficient evidence

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

Name	Weighting	Hurdle	Due
Exam	40%	Yes	Semester 2 exam period
Group Project - (C&U, P, R)	30%	No	Week 10
Assignment	10%	No	Week 11
Week 4 quiz	10%	Yes	Week 4
Week 9 quiz	10%	Yes	Week 9

Exam

Due: **Semester 2 exam period**
Weighting: **40%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

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.

On successful completion you will be able to:

- 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)

On successful completion you will be able to:

- 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

On successful completion you will be able to:

- 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 a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

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.

On successful completion you will be able to:

- 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 a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

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.

On successful completion you will be able to:

- 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

• William Stallings, Cryptography and Network Security: Principles and Practices, Prentice Hall (4th Edition) · Charles Pfleeger, Security in Computing, Prentice Hall, 20026 (4th Edition)

• Charlie Kaufman, Radia Perlman and Mike Speciner, Network Security: Private Communication in a Public World, Prentice Hall

• Dieter Gollman, Computer Security, John Wiley

• Simson Garfinkel and Gene Spafford, Practical Unix Security, O'Reilly & Associates, Inc.

• Trusted Computing Platforms: TCPA Technology in Context, Ed: Siani Pearson, Prentice Hall, 2003

• Ross Anderson, Security Engineering, John Wiley, 1st or 2nd Edition

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 7: Operating Systems Security, Platform Security, Secure Virtualisation

Week 8: Public Holiday, audio lecture provided as well as written material published on iLearn

Week 9: Distributed Systems Security, Cloud Computing Security

Week 10: Network Security (IP Security, Mobile IP Security and Wireless 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

Assessment Policy http://mq.edu.au/policy/docs/assessment/policy_2016.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 (in effect until Dec 4th, 2017): http://www.mq.edu.au/policy/docs/disruption_studies/policy.html

Special Consideration Policy (in effect from Dec 4th, 2017): https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policies/special-consideration

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

- 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

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)
- 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
- 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