ITEC852

Advanced System and Network Security

S2 Evening 2019

Dept of Computing

Contents

General Information

Unit convenor and teaching staff
Unit Convenor & Lecturer
Dr. Hassan Jameel Asghar
hassan.asghar@mq.edu.au
Contact via hassan.asghar@mq.edu.au
210, Level 2, 4 Research Park Drive, Becton-Dickinson (BD) Building
By Appointment

Lecturer
Ian Joyner
ian.joyner@mq.edu.au
Contact via ian.joyner@mq.edu.au
TBA
TBA

Credit points
4

Prerequisites
ITEC647 or admission to MCyberSec with a specialisation in Internetworking

Corequisites

Co-badged status
COMP752

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

In this unit, the final mark will be calculated by combining the marks for all assessment tasks according to the percentage weightings shown in the assessment summary.The final examination in this unit is a hurdle requirement; you must get a mark of at least 40% in the examination to pass the unit. If you get a mark between 30% and 40% in your first attempt at the final examination, you will be given a second and final attempt.

Concretely, **in order to pass the unit**, you must obtain an overall total mark of 50% or higher, and a mark of 40% or higher in the final examination.

Please read the standards and Grading section for more details.

Late Submission of Assignments

Late submission of the two assignments will be accepted, but penalised at the rate of 5% per working day late. If you cannot submit assignments on time because of illness or other circumstances, please contact the convenor at the earliest possible time.

Examination

The final examination in this unit is a hurdle requirement; you must get a mark of at least 40% in the examination to pass the unit. If you get a mark between 30% and 40% in your first attempt at the final examination, you will be given a second and final attempt.

Concretely, **in order to pass the unit**, you must obtain an overall total mark of 50% or higher, and a mark of 40% or higher in the final examination.

Please read the standards and Grading section for more details.

Note:

If you receive special consideration for the final exam, a supplementary exam will be scheduled in the week of December 16-20 2019. By making a special consideration application for the final exam you are declaring yourself available for a resit during the supplementary examination period and will not be eligible for a second special consideration approval based on pre-existing commitments. Please ensure you are familiar with the policy prior to submitting an application. Approved applicants will receive an individual notification one week prior to the exam with the

exact date and time of their supplementary examination.

If you are given a second opportunity to sit the final examination as a result of failing to meet the minimum mark required, you will be offered that chance during the same supplementary examination period and will be notified of the exact day and time after the publication of final results for the unit.

Assessment Tasks

Name	Weighting	Hurdle	Due
Assignment 1	10%	No	Week 8
Assignment 2: Group Project	30%	No	Week 12
Quiz 1: Week 4	10%	No	Week 4
Quiz 2: Week 9	10%	No	Week 9
Exam	40%	Yes	Semester 2 exam period

Assignment 1

Due: **Week 8**
Weighting: **10%**

Handed Out: Week 2

Due: via TurnitIn, Week 8

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

Assignment 2: Group Project

Due: **Week 12**
Weighting: **30%**

Group Project Allocation: Week 5

Due: electronic copies via TurnitIn week 10

Presentations: Weeks 11 & 12

(C&U) Content and Understanding: 5% (Individually assessed via Q&A on the Project)

(P) Presentation: 15% (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

Quiz 1: Week 4

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

Quiz 1 is a short in class test (close book) that will be based on your previously covered lecture material for weeks 1-3. The quiz questions will be handed over to you at the beginning of your Lecture class. Quiz 1 contributes 10% of the total mark.

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

Quiz 2: Week 9

Due: **Week 9**
Weighting: **10%**

Quiz 2 is a short in class test (close book) that will be based on your previously covered lecture material for Weeks 4-8. The quiz questions will be handed over to you at the beginning of your Lecture class. Quiz 2 contributes 10% of the total mark.

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

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.

The final examination in this unit is a hurdle requirement; you must get a mark of at least 40% in the examination to pass the unit. If you get a mark between 30% and 40% in your first attempt at the final examination, you will be given a second and final attempt.

Concretely, **in order to pass the unit**, you must obtain an overall total mark of 50% or higher, and a mark of 40% or higher in the final examination.

Please read the standards and Grading section for more details.

Note:

If you receive special consideration for the final exam, a supplementary exam will be scheduled in the week of December 16-20 2019. By making a special consideration application for the final exam you are declaring yourself available for a resit during the supplementary examination period and will not be eligible for a second special consideration approval based on pre-existing commitments. Please ensure you are familiar with the policy prior to submitting an application. Approved applicants will receive an individual notification one week prior to the exam with the exact date and time of their supplementary examination.

If you are given a second opportunity to sit the final examination as a result of failing to meet the minimum mark required, you will be offered that chance during the same supplementary examination period and will be notified of the exact day and time after the publication of final results for the unit.

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

Delivery and Resources

ITEC852 is taught via lectures and informal tutorial sessions.

Technology

• Presentation using Powerpoint and other Computer Related Material

Classes

Classes are held from 6-10 pm Monday evenings. Lectures/Tutorials and other discussion are in 11 Wallys Walk - 170 Tutorial Rm in the lecture slot.

Lectures

Lectures are used to introduce security concepts and technologies, network security protocols and design and put them in a wider context. You are encouraged to ask questions of the lecturer, both during and outside the lecture, to clarify anything you might not be sure of.

It should be noted that no single text book completely covers the content of this unit. A large portion of the lecture material is drawn from research papers, white papers and standard documents. Students are encouraged to read the weekly recommended reading list to gain a solid understanding of the topics that are covered.

Quizzes

There will be two quizzes in the following weeks: week 4 and week 9. A quiz is a short test that will be based on your previously covered lecture material. For example, week 4 quiz will be based on lectures done in weeks 1-3. The quiz questions will be handed over to you at the beginning of your Lecture class. These quizzes contribute 20% of the total mark and serve as a feedback mechanism to monitor your progress in the unit.

Tutorial

The tutorial gives you the opportunity to interact with your peers and with the lecturer. The tutorial sessions involve informal discussions with your peers and the lecturer. Each week you will be given problems to solve prior to the tutorial; preparing solutions is important because it will allow you to discuss the problems effectively with your lecturer and maximise the feedback you get on your work.

Assignments

Your assignment is to be submitted online using **Turnitin**.

Late Submission

Late submission of the assignment will be accepted, but penalised at the rate of 5% per working day late. If you cannot submit assignments on time because of illness or other circumstances, please contact the convenor at the earliest possible time.

Reference Material

• 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

General Notes

In this unit, you should do the following:

- Attend lectures, take notes, ask questions.
- Attend your tutorial, seek feedback from your lecturer on your work.
- Prepare for and strive to do well in the three quizzes
- Read appropriate sections of the text, add to your notes and prepare questions for your lecturer/tutor.
- Prepare answers to tutorial questions.
- Work on any assignments that have been released.

Lecture notes will be made available each week but these notes are intended as an outline of the lecture only and are not a substitute for your own notes or the recommended reading list.

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 ***hassan.asghar@mq.edu.au*** and ***ian.joyner@mq.edu.au*** and must include your full name and your student id number.**You must use the university email account otherwise the staff will ignore your emails.**

Tentative Lecture Schedule ITEC852 S2 2019 (may vary depending upon progress)

Week 1: Introduction: Cyber Security Trends and Concepts

Week 2: Threat Models and Security Goals

Week 3: Cryptography

Week 4: Cryptographic and Security Protocols

Week 5: Authentication and Access Control

Week 6: Web and Data Privacy

Week 7: Operating Systems Security, Platform Security, Secure Virtualisation

Break

Week 8: Distributed Systems Security, Cloud Computing Security

Week 9: Network Security I

Week 10:Network Security II (IP Security, Mobile IP Security and Wireless Security) and Trusted Computing

Week 11: Group Project Presentations (1)

Week 12: Group Project Presentation (2)

Week 13: Revision

Learning and Teaching Activities

Lectures

Weekly lectures

Tutorial

Weekly tutorial exercises. The tutorial gives you the opportunity to interact with your peers and with the lecturer. The tutorial sessions involve informal discussions with your peers and the lecturer. Each week you will be given problems to solve prior to the tutorial; preparing solutions is important because it will allow you to discuss the problems effectively with your lecturer and maximise the feedback you get on your work.

Guest speakers

Industry speakers or research students

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://staff.m

q.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/policy-central). Students should be aware of the following policies in particular with regard to Learning and Teaching:

- Academic Appeals Policy
- Academic Integrity Policy
- Academic Progression Policy
- Assessment Policy
- Fitness to Practice Procedure
- Grade Appeal Policy
- Complaint Management Procedure for Students and Members of the Public
- Special Consideration Policy *(**Note:** The Special Consideration Policy is effective from 4 December 2017 and replaces the Disruption to Studies Policy.)*

Undergraduate students seeking more policy resources can visit the Student Policy Gateway (https://students.mq.edu.au/support/study/student-policy-gateway). It is your one-stop-shop for the key policies you need to know about throughout your undergraduate student journey.

If you would like to see all the policies relevant to Learning and Teaching visit Policy Central (https://staff.mq.edu.au/work/strategy-planning-and-governance/university-policies-and-procedures/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/study/getting-started/student-conduct

Results

Results published on platform other than eStudent, (eg. iLearn, Coursera etc.) 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 or if you are a Global MBA student contact globalmba.support@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

If you are a Global MBA student contact globalmba.support@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

- Assignment 2: Group Project
- Exam

Learning and teaching activities

- Weekly tutorial exercises. The tutorial gives you the opportunity to interact with your

peers and with the lecturer. The tutorial sessions involve informal discussions with your peers and the lecturer. Each week you will be given problems to solve prior to the tutorial; preparing solutions is important because it will allow you to discuss the problems effectively with your lecturer and maximise the feedback you get on your work.

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

- Assignment 1
- Assignment 2: Group Project
- Quiz 1: Week 4
- Quiz 2: Week 9
- Exam

Learning and teaching activities

- Weekly lectures
- Weekly tutorial exercises. The tutorial gives you the opportunity to interact with your peers and with the lecturer. The tutorial sessions involve informal discussions with your peers and the lecturer. Each week you will be given problems to solve prior to the tutorial; preparing solutions is important because it will allow you to discuss the problems effectively with your lecturer and maximise the feedback you get on your work.
- Industry speakers or research students

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

- Assignment 1
- Assignment 2: Group Project
- Quiz 1: Week 4
- Quiz 2: Week 9
- Exam

Learning and teaching activities

- Weekly lectures
- Weekly tutorial exercises. The tutorial gives you the opportunity to interact with your peers and with the lecturer. The tutorial sessions involve informal discussions with your peers and the lecturer. Each week you will be given problems to solve prior to the tutorial; preparing solutions is important because it will allow you to discuss the problems effectively with your lecturer and maximise the feedback you get on your work.

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

- Assignment 2: Group Project
- Quiz 1: Week 4
- Exam

Learning and teaching activities

- Weekly tutorial exercises. The tutorial gives you the opportunity to interact with your peers and with the lecturer. The tutorial sessions involve informal discussions with your peers and the lecturer. Each week you will be given problems to solve prior to the tutorial; preparing solutions is important because it will allow you to discuss the problems effectively with your lecturer and maximise the feedback you get on your work.

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

- Assignment 2: Group Project
- Quiz 2: Week 9

Learning and teaching activities

- Industry speakers or research students

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

- Assignment 2: Group Project
- Exam

Learning and teaching activities

- Weekly lectures
- Industry speakers or research students

Standards and Grading

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, the final mark will be calculated by combining the marks for all assessment tasks according to the percentage weightings shown in the assessment summary.The final examination in this unit is a hurdle requirement; you must get a mark of at least 40% in the examination to pass the unit. If you get a mark between 30% and 40% in your first attempt at the final examination, you will be given a second and final attempt.

Concretely, **in order to pass the unit**, you must obtain an overall total mark of 50% or higher, and a mark of 40% or higher 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 to obtain High Distinction;
  ◦ have a total mark of 75% or higher to obtain Distinction;
  ◦ have a total mark of 65% or higher to obtain Credit.

You are encouraged to:

- set your personal deadline earlier than the actual one;
- keep backups of all important assessed tasks;.
- make sure no one else picks up your printouts.

All work submitted should be readable and well presented.

You should **never commit plagiarism** in any of your submitted work, including tutorial and practical answers.