COMP8260

Advanced System and Network Security

Session 2, In person-scheduled-weekday, North Ryde 2023

School of Computing

Contents

General Information

Unit convenor and teaching staff
Muhammad Ikram
muhammad.ikram@mq.edu.au

Lecturer
Tao Gu
tao.gu@mq.edu.au

Tao Gu
tao.gu@mq.edu.au

Credit points
10

Prerequisites
ITEC647 or COMP6250

Corequisites

Co-badged status
COMP7260 - Network and Systems Security

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:

ULO1: Analyse key security requirements and trends in a distributed networked computing settings

ULO2: Evaluate security services such as authentication and access control in distributed systems and networks

ULO3: Analyse the security threats and develop security architecture and functionalities to counteract the security threats

ULO4: Apply (network) security techniques and mechanisms to develop (network) security protocols

ULO5: Develop and advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.

ULO6: Demonstrate effective written and verbal communication skills to communicate technical ideas

General Assessment Information

Weekly submission, in-class activities, or scheduled tests and exam must be undertaken at the time indicated in the unit guide. Should these activities be missed due to illness or misadventure, students may apply for Special Consideration.

All other assessments must be submitted by 11:55 pm on their due date.

Requirements to Pass this Unit

To pass this unit you must:

- Attempt all assessments, and
- Achieve a total mark equal to or greater than 50%, and
- Achieve at least 40% in the final examination

Late Assessment Submission and Penalties

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark of the task) will be applied for each day a written report or presentation assessment is not submitted, up until the 7th day (including weekends). After the 7th day, a grade of '0' will be awarded even if the assessment is submitted. The submission time for all uploaded assessments is **11:55 pm**. A 1-hour grace period will be provided to students who experience a technical concern. For any late submission of time-sensitive tasks, such as scheduled tests/ exams, performance assessments/presentations, and/or scheduled practical assessments/labs, please apply for Special Consideration.

Assessments where Late Submissions will be accepted

- Worshop Tasks (Weekly) – YES, Standard Late Penalty applies
- Assignment 1, Group Project, and Final examination - NO, unless Special Consideration is Granted

Special Consideration

The Special Consideration Policy aims to support students who have been impacted by short-

term circumstances or events that are serious, unavoidable and significantly disruptive, and which may affect their performance in assessment. If you experience circumstances or events that affect your ability to complete the assessments in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.

Final Exam

Assessment Type : Examination

Indicative Time on Task : 10 hours

Due: S2 Exam Period

Weighting: 45%

The final examination in this unit is a hurdle requirement; students must get a mark of at least 40% in the examination to pass the unit. If students get a mark between 30% and 40% in students' first attempt at the final examination, students will be given a second and final attempt. Concretely, in order to pass the unit, students must obtain an overall total mark of 50% or higher, and a mark of 40% or higher in the final examination.

On successful completion you will be able to:

- Analyse key security requirements and trends in a distributed networked computing settings
- Evaluate security services such as authentication and access control in distributed systems and networks
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats
- Apply (network) security techniques and mechanisms to develop (network) security protocols
- Develop and advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree

Workshop Tasks

Assessment Type: Participatory task

Indicative Time on Task 2 : 0 hours

Due: Weekly Weighting: 10%

Weekly tasks or quizzes to assess understanding of the course material. On successful completion you will be able to:

- Analyse key security requirements and trends in a distributed networked computing settings
- Evaluate security services such as authentication and access control in distributed

systems and networks
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats
- Apply (network) security techniques and mechanisms to develop (network) security protocols

Assignment 1

Assessment Type: Problem set

Indicative Time on Task: 15 hours

Due: Week 5 Weighting: 15%

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 settings
- Evaluate security services such as authentication and access control in distributed systems and networks
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats
- Apply (network) security techniques and mechanisms to develop (network) security protocols

Assignment 2

Assessment Type: Group Project

Indicative Time on Task: 40 hours

Due: Week 12

Weighting: 30%

On successful completion you will be able to:

- Analyse key security requirements and trends in a distributed networked computing settings
- Evaluate security services such as authentication and access control in distributed systems and networks
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats
- Apply (network) security techniques and mechanisms to develop (network) security protocols

- Develop and advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
- Demonstrate effective written and verbal communication skills to communicate technical ideas

Assessment Tasks

Name	Weighting	Hurdle	Due
Workshop Tasks	10%	No	Weekly
Final Exam	45%	No	S2 Exam Period
Assignment 2	30%	No	Week 12
Assignment 1	15%	No	Week 6

Workshop Tasks

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 0 hours
Due: **Weekly**
Weighting: **10%**

Weekly tasks or quizzes to assess understanding of the course material.

On successful completion you will be able to:

- Analyse key security requirements and trends in a distributed networked computing settings
- Evaluate security services such as authentication and access control in distributed systems and networks
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats
- Apply (network) security techniques and mechanisms to develop (network) security protocols

Final Exam

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **S2 Exam Period**
Weighting: **45%**

The final examination in this unit is a hurdle requirement; students must get a mark of at least

40% in the examination to pass the unit. If students get a mark between 30% and 40% in students' first attempt at the final examination, students will be given a second and final attempt.

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

On successful completion you will be able to:

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

Assignment 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 40 hours
Due: **Week 12**
Weighting: **30%**

Group Project.

On successful completion you will be able to:

- Analyse key security requirements and trends in a distributed networked computing settings
- Evaluate security services such as authentication and access control in distributed systems and networks
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats
- Apply (network) security techniques and mechanisms to develop (network) security protocols
- Develop and advance skills of research and critical analysis in a manner consistent with the completion of a postgraduate degree.
- Demonstrate effective written and verbal communication skills to communicate technical ideas

Assignment 1

Assessment Type [1]: Problem set
Indicative Time on Task [2]: 15 hours
Due: **Week 6**
Weighting: **15%**

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 settings
- Evaluate security services such as authentication and access control in distributed systems and networks
- Analyse the security threats and develop security architecture and functionalities to counteract the security threats
- Apply (network) security techniques and mechanisms to develop (network) security protocols

---

[1] If you need help with your assignment, please contact:

- the academic teaching staff in your unit for guidance in understanding or completing this type of assessment
- the Writing Centre for academic skills support.

[2] Indicative time-on-task is an estimate of the time required for completion of the assessment task and is subject to individual variation

Delivery and Resources

COMPUTING FACILITIES

Please note that this is a BYOD (Bring Your Own Device) unit. You will be expected to bring your own laptop computer (Windows, Mac or Linux), install and configure the required software.

CLASSES AND TUTORIALS

Each week you should complete any assigned readings and review the lecture slides in order to prepare for the lecture. There are three hours of face-to-face lectures every week with a one hour tutorial. The lecture slides and tutorial material will be uploaded to COMP8260's iLearn page by 9:00am on Mondays. You are at the very least expected to go through the lecture slides and tutorial material for better engagement with your lecturers and tutor. Lectures and tutorials will be interactive, and you can ask questions, anytime during the lecture or/and tutorial, related to the lectures, hands on, and take home exercises.

For details of days, times and rooms consult the timetables webpage.

Tutorials and exercises will commence in week 1. Please note that you will be required to submit work every week

METHOD OF COMMUNICATION

This unit makes use of discussion boards hosted within iLearn. Please post questions there; they are monitored by the staff on the unit. Alternativetly, the staff can be reached out via their university email addresses given at iLearn page for this unit.

REQUIRED AND RECOMMENDED TEXTS AND/OR MATERIALS

This material for this unit is in part based on the following textbooks:

- 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

TECHNOLOGY USED AND REQUIRED

iLearn

iLearn is a Learning Management System that gives you access to lecture slides, lecture recordings, forums, assessment tasks, instructions for practicals, discussion forums and other resources.

Echo 360

Digital recordings of lectures are available. Read these instructions for details.

Technology Used

PacketTracer, Anaconda, Jupyter Notebook with Python.

Unit Schedule

Week	Topic
1	Introduction: Cyber Security Trends and Concepts
3	Threat Models and Security Goals

2	Cryptography, Cryptographic and Security Protocols
4	Authentication and Access Control
5	Web Security
6	Internet Security Protocol
7	Distributed Systems Security: BGP Security
8	Cloud Computing Security
9	Distributed Denial of Service Attacks and Defences
10	Mobile Platform Security Architecture
11	Anonymity and Censorship Techniques
12	Group Project Presentations
13	Revision

Policies and Procedures

Macquarie University policies and procedures are accessible from Policy Central (https://policies.mq.edu.au). 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
- Assessment Procedure
- Complaints Resolution Procedure for Students and Members of the Public
- Special Consideration Policy

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

To find other policies relating to Teaching and Learning, visit Policy Central (https://policies.mq.edu.au) and use the search tool.

Student Code of Conduct

Macquarie University students have a responsibility to be familiar with the Student Code of Conduct: https://students.mq.edu.au/admin/other-resources/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

Academic Integrity

At Macquarie, we believe academic integrity – honesty, respect, trust, responsibility, fairness and courage – is at the core of learning, teaching and research. We recognise that meeting the expectations required to complete your assessments can be challenging. So, we offer you a range of resources and services to help you reach your potential, including free online writing and maths support, academic skills development and wellbeing consultations.

Student Support

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

The Writing Centre

The Writing Centre provides resources to develop your English language proficiency, academic writing, and communication skills.

- Workshops
- Chat with a WriteWISE peer writing leader
- Access StudyWISE
- Upload an assignment to Studiosity
- Complete the Academic Integrity Module

The Library provides online and face to face support to help you find and use relevant information resources.

- Subject and Research Guides
- Ask a Librarian

Student Services and Support

Macquarie University offers a range of Student Support Services including:

- IT Support
- Accessibility and disability support with study
- Mental health support
- Safety support to respond to bullying, harassment, sexual harassment and sexual assault
- Social support including information about finances, tenancy and legal issues
- Student Advocacy provides independent advice on MQ policies, procedures, and

processes

Student Enquiries

Got a question? Ask us via AskMQ, or contact Service Connect.

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.

Changes since First Published

Date	Description
05/10/2023	"tutorials" changed to "SGTA (Small Group Teaching Activities)" "tutors" changed to "teaching team"

Unit information based on version 2023.05 of the Handbook