COMP8260

Advanced System and Network Security

Session 2, In person-scheduled-weekday, North Ryde 2026

School of Computing

Contents

General Information

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

Lecturer
Rohitranjan Vasantkumar Gupta
rohitranjanvasantkumar.gupta@mq.edu.au

Credit points
10

Prerequisites
COMP6250 OR Admission to the GradDipRes or GradCertRes

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.

Learning in this unit enhances student understanding of global challenges identified by the United Nations Sustainable Development Goals (UNSDGs) Industry, Innovation and Infrastructure; Peace, Justice and Strong Institutions

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 environment

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

General Assessment Information

Release Dates

- **Individual Project -** Sunday ending Week 2 23:55
- **Group Project** - Sunday ending Week 7 23:55

Descriptions of Assessment Activities and Other Information

- Submission of Assessments - Assessments need to be submitted via iLearn.
- Marking of Assessments - Marks and feedback will be provided via iLearn with a turnaround time of 2.5 weeks for the assignments.

Requirements to Pass this Unit

To pass this unit you must achieve a total mark equal to or greater than 50%

Late Submission Policy

- **5% penalty per day:** If you submit your assessment late, **5% of the total possible marks** will be deducted for each day (including weekends), up to 7 days.
    - *Example 1 (out of 100):* If you score 85/100 but submit 20 hours late, you will lose 5 marks and receive **80/100**.
    - *Example 2 (out of 30):* If you score 27/30 but submit 1 day late, you will lose 1.5 marks and receive **25.5/30**.
- **After 7 days:** Submissions more than 7 days late will receive a **mark of 0**.
- **Extensions:**
    - **Automatic short extension**: Some assessments are eligible for automatic short extension. You can only apply for an automatic short extension before the due date.

- **Special Consideration**: If you need more time due to serious issues and for any assessments that are not eligible for Short Extension, you must apply for Special Consideration.

Assessments where Late Submissions will be accepted:

- **Individual Project, Group Project** – YES, Standard Late Penalty applies
- **Final Exam** - 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.

Generative AI
AI Open assessments: Students may use Generative AI to support learning, such as brainstorming, improving writing, or understanding digital forensic concepts. Students are responsible for verifying all AI-generated content and ensuring that all forensic analysis, evidence, and conclusions are their own. AI-generated or fabricated forensic evidence is strictly prohibited.

Observed assessments: Generative AI is not permitted during supervised assessments unless explicitly authorised by the Unit Convenor.

Assessment Tasks

Name	Weighting	Hurdle	Due	Groupwork/Individual	Short Extension	AI Approach
Assignment 1	25%	No	04/09/2026	Individual	Yes	Open
Assignment 2	30%	No	30/10/2026	Individual and Group	No	Open
Final Exam	45%	No	Final Exam Period	Individual	No	Observed

Assignment 1

Assessment Type [1]: Problem-based task
Indicative Time on Task [2]: 35 hours
Due: **04/09/2026**
Weighting: **25%**
Groupwork/Individual: Individual
Short extension [3]: Yes
AI Approach: Open

This assignment introduces students to real-world system and network security challenges. It requires the analysis of specific problems and the development of well-reasoned, optimal solutions. Some tasks may involve in-depth research.

On successful completion you will be able to:

- Analyse key security requirements and trends in a distributed networked computing environment
- 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 [1]: Portfolio
Indicative Time on Task [2]: 45 hours
Due: **30/10/2026**
Weighting: **30%**
Groupwork/Individual: Individual and Group
Short extension [3]: No
AI Approach: Open

Assignment 2 is a major project introducing students to current tools and practices in cybersecurity, helping them build critical thinking and practical problem-solving skills for future professional roles. Students are expected to work in teams to investigate emerging threats and the countermeasures used to protect modern networked systems.

On successful completion you will be able to:

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

Final Exam

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Final Exam Period**
Weighting: **45%**
Groupwork/Individual: Individual
Short extension [3]: No
AI Approach: Observed

You will undertake a final examination during the formal examination period.

On successful completion you will be able to:

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

---

[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
- Academic Success 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.

[3] An automatic short extension is available for some assessments. Apply through the Service Connect Portal.

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 connect.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/

Academic Success

Academic Success provides resources to develop your English language proficiency, academic writing, and communication skills.

- Ask a Study Coach
- 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 the Service Connect Portal, or contact Service Connect.

IT Help

For help with University computer systems and technology, visit https://students.mq.edu.au/support/technology/service-desk.

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 from Previous Offering

We value student feedback to be able to continually improve the way we offer our units. As such we encourage students to provide constructive feedback via student surveys, to the teaching staff directly, or via the FSE Student Experience & Feedback link in the iLearn page.

Unit information based on version 2026.04 of the Handbook