COMP8320

Information and Data Security

Session 2, In person-scheduled-weekday, North Ryde 2024

School of Computing

Contents

General Information

Unit convenor and teaching staff
Convenor and Lecturer
Hassan Asghar
hassan.asghar@mq.edu.au
Contact via Email

Lecturer
Muhammad Ikram
muhammad.ikram@mq.edu.au
Contact via Email

Credit points
10

Prerequisites
(COMP6300 or ITEC643) or admission to MInfoTechCyberSec or BCyberSecMInfoTechCyberSec

Corequisites

Co-badged status

Unit description
This unit deals with the concepts, techniques and tools which contribute to enable information and data security. Building on applied cryptography notions and introducing the concept of provable privacy, the unit addresses topics such as encryption, privacy preserving techniques in data mining, content security solutions or secure data management.

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: Explain the concepts of information security and provable privacy.

ULO2: Perform risk assessment (including privacy risk) on digital information and datasets.

ULO3: Apply adapted security technologies and tools, in particular encryption to enhance security properties of data.

ULO4: Analyse the trends for managing data security.

General Assessment Information

Late Assessment Submission Penalty

Students enrolled in Session based units with written assessments will have the following university standard late penalty applied. Please see https://students.mq.edu.au/study/assessment-exams/assessments for more information.

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark) will be applied each day a written 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. Submission time for all written assessments is set at 11:55 pm. A 1-hour grace period is 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, students need to submit an application for Special Consideration.

Assessments where Late Submissions will be accepted

In this unit, late submissions will accepted as follows:

Assignments 1 and 2 – YES, standard late penalty applies

Module Exams 1, 2 and 3 - NO, unless Special Consideration is granted

Weekly tasks - NO

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.

- *Written Assessments and Module Exams:* If you experience circumstances or events that affect your ability to complete the assignments and module exams in this unit on time, please inform the convenor and submit a Special Consideration request through ask.mq.edu.au.
- *Weekly quizzes:* To pass the unit you need to attempt 6 out of the 10 weekly quizzes. A Special Consideration should only be applied for if you miss more than four of the weekly quizzes.

Requirements to Pass this Unit

To pass this unit, you must:

- Achieve a total mark equal to or greater than 50%

You will maximise your chances of passing this unit if:

- You attempt all asessments
- Participate in all lectures and practicals

Assessment Tasks

Name	Weighting	Hurdle	Due
Weekly Tasks	10%	No	11:55 pm on Mondays, weekly
Module Exam 2	20%	No	5:55 pm on Wednesday week 9
Module Exam 3	20%	No	5:55 pm on Wednesday week 13
Module Exam 1	20%	No	5:55 pm on Wednesday week 5
Assignment 1	15%	No	11:55 pm on Friday ending week 7
Assignment 2	15%	No	11:55 pm on Friday ending week 12

Weekly Tasks

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 10 hours
Due: **11:55 pm on Mondays, weekly**
Weighting: **10%**

Each week, a set of exercises will be available online. One or two questions from the exercises will be the weekly quiz task.

On successful completion you will be able to:

- Explain the concepts of information security and provable privacy.
- Perform risk assessment (including privacy risk) on digital information and datasets.
- Apply adapted security technologies and tools, in particular encryption to enhance security properties of data.
- Analyse the trends for managing data security.

Module Exam 2

Assessment Type [1]: Examination
Indicative Time on Task [2]: 15 hours
Due: **5:55 pm on Wednesday week 9**
Weighting: **20%**

A 50 minutes long online examination worth 20% that will be held in week 9 (online via iLearn). This will test understanding of material covered in weeks 5 to 8. For on campus offering this will be held during practical classes.

On successful completion you will be able to:

- Perform risk assessment (including privacy risk) on digital information and datasets.
- Apply adapted security technologies and tools, in particular encryption to enhance security properties of data.

Module Exam 3

Assessment Type [1]: Examination
Indicative Time on Task [2]: 15 hours
Due: **5:55 pm on Wednesday week 13**
Weighting: **20%**

A 50 minutes long online examination worth 20% that will be held in week 13 (online via iLearn). This will test understanding of material covered in weeks 9 to 12. For on campus offering this will be held during practical classes.

On successful completion you will be able to:

- Perform risk assessment (including privacy risk) on digital information and datasets.
- Apply adapted security technologies and tools, in particular encryption to enhance security properties of data.
- Analyse the trends for managing data security.

Module Exam 1

Assessment Type [1]: Examination
Indicative Time on Task [2]: 15 hours
Due: **5:55 pm on Wednesday week 5**
Weighting: **20%**

A 50 minutes long online examination worth 20% that will be held in week 5 (online via iLearn). This will test understanding of material covered in weeks 1 to 4. For on campus offering this will be held during practical classes.

On successful completion you will be able to:

- Explain the concepts of information security and provable privacy.
- Perform risk assessment (including privacy risk) on digital information and datasets.

Assignment 1

Assessment Type [1]: Project
Indicative Time on Task [2]: 10 hours
Due: **11:55 pm on Friday ending week 7**
Weighting: **15%**

This assignment deals with concepts in provable privacy and risk assessments of datasets and is due on week 7. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Explain the concepts of information security and provable privacy.
- Perform risk assessment (including privacy risk) on digital information and datasets.

Assignment 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 10 hours
Due: **11:55 pm on Friday ending week 12**
Weighting: **15%**

This assignment deals with identifying privacy risks in datasets and securing access to data and is due on week 12. The assignment is to be submitted via iLearn.

On successful completion you will be able to:

- Explain the concepts of information security and provable privacy.
- Perform risk assessment (including privacy risk) on digital information and datasets.
- Apply adapted security technologies and tools, in particular encryption to enhance security properties of data.
- Analyse the trends for managing data security.

[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

Important! 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

Each week you should complete any assigned readings and review the lecture slides in order to prepare for the lecture. There are two hours of lectures and a one-hour practical every week. The practicals have hands-on exercises to reinforce concepts introduced during the lectures; you should have chosen a practical on enrollment. You will find it helpful to read the practical instructions before participating.

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

Note that **Lectures and Practicals commence in week 1**.

DISCUSSION BOARDS

This unit makes use of discussion boards hosted within iLearn . Please post questions there; they are monitored by the staff on the unit.

REQUIRED AND RECOMMENDED TEXTS AND/OR MATERIALS

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

- Dwork, C. and Roth, A., 2014. The algorithmic foundations of differential privacy. *Foundations and Trends in Theoretical Computer Science*, *9*(3-4), pp.211-407. Available online: https://www.cis.upenn.edu/~aaroth/Papers/privacybook.pdf
- Yi, X., Paulet, R. and Bertino, E., 2014. *Homomorphic encryption and applications* (Vol. 3). Heidelberg: Springer. Available online: https://link.springer.com/content/pdf/10.1007%2F978-3-319-12229-8.pdf (accessible through MQ Library).

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 (formerly known as iLecture)

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

Technology Used

Anaconda, Jupyter Notebook with Python.

COVID INFORMATION

For the latest information on the University's response to COVID-19, please refer to the Coronavirus infection page on the Macquarie website: https://www.mq.edu.au/about/coronavirus-faqs. Remember to check this page regularly in case the information and requirements change during semester. If there are any changes to this unit about COVID-19, these will be communicated via iLearn.

Unit Schedule

Week	Topic
1	Introduction: Mathematical Background, Data Sharing, and Privacy Risks
2	De-identification and Privacy Attacks
3	Towards Provable Privacy: K-Anonymity and Related Definitions
4	Differential Privacy and its Applications
5	Cryptography Primer and Homomorphic Encryption
6	Machine Learning and Data Privacy
7	Mobile Privacy and Attacks
8	Privacy Protection for Mobile Apps
9	Web Privacy
10	Web Behaviour Re-identification and Defence
11	Online Tracking and Fingerprinting
12	Blacklists-based Tracking Prevention
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/

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 the Service Connect Portal, 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 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 2024.02 of the Handbook