COMP8320

Information and Data Security

Session 2, In person-scheduled-weekday, North Ryde 2022

School of Computing

Contents

General Information

Unit convenor and teaching staff
Convenor and Lecturer
Hassan Asghar
hassan.asghar@mq.edu.au
Contact via Email
Room 210, Level 2, 4 Research Park Drive, Becton-Dickinson (BD) Building
Email to make appointment

Lecturer
Muhammad Ikram
muhammad.ikram@mq.edu.au
Contact via Email
Room 286, Level 2, 4 Research Park Drive, Becton-Dickinson (BD) Building email to make appointment
Email to make appointment

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

From 1 July 2022, 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

Assessment Tasks

Name	Weighting	Hurdle	Due
Weekly Tasks	10%	No	Weekly
Module Exam 1	20%	No	Week 5
Assignment 2	15%	No	Week 7
Assignment 2	15%	No	Week 12
Module Exam 2	20%	No	Week 9
Module Exam 3	20%	No	Week 13

Weekly Tasks

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

Assessment Type [1]: Examination
Indicative Time on Task [2]: 15 hours
Due: **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 2

Assessment Type [1]: Project
Indicative Time on Task [2]: 10 hours
Due: **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: **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.

Module Exam 2

Assessment Type [1]: Examination
Indicative Time on Task [2]: 15 hours
Due: **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: **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.

---

[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 three hours of lectures every week. The lectures will be pre-recorded and available online. You are at the very least expected to go through the lecture slides and videos during the first time slot for the lecture, i.e., Tuesdays 1:00 to 3:00 pm. There will be a live Q&A session every week during the second time slot for the lecture, i.e., Thursdays 12:00 to 1:00 pm. During the live Q&A session, you can ask questions related to the lectures and take home exercises.

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

Take home exercises will commence **in week 1**.

Please note that you will be **required** to submit work every week. Failure to do so may result in you failing the unit or being excluded from the exams.

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.

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 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 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.

Grading Standards

At the end of the semester, you will receive a grade that reflects your achievement in the unit

- **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.

Your final grade depends on your performance in each assessment task and on your ability to perform well enough on the hurdle assessment tasks.

For each task, you receive a mark that reflects your standard of performance. Then the different component marks are added up to determine an aggregated mark out of 100. In order to pass the unit, this aggregated mark needs to be at least 50.

Note that none of the assessment tasks in this unit are a hurdle requirement. However, if you do not make a reasonable attempt at the assessments, you will be unlikely to pass the unit.

Your final grade is then a direct reflection of the aggregated mark (provided that you satisfy the hurdle requirements) according to the following:

- 85-100 for **HD**
- 75-84 for **D**
- 65-74 for **CR**
- 50-64 for **P**

If you receive special consideration for the module exams, a supplementary exam will be scheduled in the week of the regular exam offering. By making a special consideration application for the module exams 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. You can check the supplementary exam information page on FSE101 in iLearn (bit.ly/FSESupp) for dates, and 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.