COMP3310

Secure Applications Development

Session 1, In person-scheduled-weekday, North Ryde 2022

School of Computing

Contents

Disclaimer

Macquarie University has taken all reasonable measures to ensure the information in this publication is accurate and up-to-date. However, the information may change or become out-dated as a result of change in University policies, procedures or rules. The University reserves the right to make changes to any information in this publication without notice. Users of this publication are advised to check the website version of this publication [or the relevant faculty or department] before acting on any information in this publication.

General Information

Unit convenor and teaching staff
Convener
Ansgar Fehnker
ansgar.fehnker@mq.edu.au
By Appointment (via email)

Lecturer
Carl Svensson
carl.svensson@mq.edu.au
By Appointment (via email)

Tutor
Rohitranjan Vasantkumar Gupta

Tutor
Subhash Sagar

Credit points
10

Prerequisites
130cp at 1000 level or above including COMP1010 and COMP1300 and COMP2300 and (COMP2050 or COMP2110)

Corequisites

Co-badged status

Unit description
This unit provides an introduction to the security consideration in application software development process in order to build secure applications. First, it introduces the basic concepts like software security risk and focuses on how to integrate security into different stages of application software development process, from requirement engineering and design, to code implementation and testing, to deployment and maintenance. Then, a range of typical implementation-level issues are discussed and the corresponding techniques and best practices are introduced, including topics like software auditing, buffer overflows, access control, password authentication, race conditions, input validation, database security, and client-side security, etc.

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: Describe how security is integrated into different stages of the application development life cycle and explain the importance and the underlying logic.

ULO2: Assess application software security and identify the common security issues in application development through auditing and analysing source code and other documents.

ULO3: Understand and apply security related best practices to the application development process and address the common security issues for secure application development

ULO4: Communicate professionally in written and oral with technical and non-technical audience such as software developers/testers, business analysts, security managers, users, etc.

General Assessment Information

General Faculty Policy on assessment submission deadlines and late submissions:

Online quizzes, 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 5:00 pm on their due date.

Should these assessments be missed due to illness or misadventure, students should apply for Special Consideration.

Late submissions **will be accepted but will incur a penalty** unless there is an approved Special Consideration request. A 12-hour grace period will be given after which the following deductions will be applied to the awarded assessment mark: 12 to 24 hours late = 10% deduction; for each day thereafter, an additional 10% per day or part thereof will be applied until five days beyond the due date. After this time, a mark of zero (0) will be given. For example, an assessment worth 20% is due 5 pm on 1 January. Student A submits the assessment at 1 pm, 3 January. The assessment received a mark of 15/20. A 20% deduction is then applied to the mark of 15, resulting in the loss of three (3) marks. Student A is then awarded a final mark of 12/20.

Course specific guidelines

Your reports will have to be written in English. For full marks, your answers should be concise as well as accurate. Marks will be awarded for reasoning and method as well as being correct. Excessively verbose answers may be penalized.

Upload your reports as a single PDF document. Word documents are good for editing, but you should export or save the final version as a PDF. This is the format for reading.

Please state clearly, on the first page of any written report, and in the comments of any program who you work with. If we find that you copied work from others - people who are not on your team it will be considered plagiarism.

If you have problems with your team member or partner please contact the convener. If you have any other problem with the assignment or the course, feel free to email, visit or call the convener.

Check regularly on iLearn for updates. This description may change if circumstances require it.

Assessment Tasks

Name	Weighting	Hurdle	Due
Assignment	20%	No	First week of the mid-semester break
Group project	40%	No	Presentation and report week 13
Weekly workshop tasks	10%	Yes	Multiple - discussed with students in week 1
Final exam	30%	No	Exam period

Assignment

Assessment Type [1]: Portfolio
Indicative Time on Task [2]: 30 hours
Due: **First week of the mid-semester break**
Weighting: **20%**

In this assignment, students are required to choose an appropriate code analysis and auditing tools to evaluate the security risks in the specified applications. You should produce a report describing the analysis and auditing process with justification, the results of the identified security issues, and the proposal of possible solutions.

On successful completion you will be able to:

- Describe how security is integrated into different stages of the application development life cycle and explain the importance and the underlying logic.
- Assess application software security and identify the common security issues in application development through auditing and analysing source code and other documents.
- Understand and apply security related best practices to the application development process and address the common security issues for secure application development
- Communicate professionally in written and oral with technical and non-technical audience such as software developers/testers, business analysts, security managers, users, etc.

Group project

Assessment Type [1]: Project
Indicative Time on Task [2]: 45 hours
Due: **Presentation and report week 13**
Weighting: **40%**

In this task, you are required to work with other students to form a project group, and develop an application with a focus on integrating security into your software development practice. Specifically, you should take security into consideration for the different stages of the software development lifecycle. Group presentation, peer review, reports describing the development process with decision-making justifications, source code and the relevant technical documents should be included in the group final delivery.

On successful completion you will be able to:

- Describe how security is integrated into different stages of the application development life cycle and explain the importance and the underlying logic.
- Assess application software security and identify the common security issues in application development through auditing and analysing source code and other documents.
- Understand and apply security related best practices to the application development process and address the common security issues for secure application development
- Communicate professionally in written and oral with technical and non-technical audience such as software developers/testers, business analysts, security managers, users, etc.

Weekly workshop tasks

Assessment Type [1]: Participatory task
Indicative Time on Task [2]: 0 hours
Due: **Multiple - discussed with students in week 1**
Weighting: **10%**
This is a hurdle assessment task (see assessment policy for more information on hurdle assessment tasks)

Each week there will be a small practical task or short quiz as part of the workshop that should be attempted seriously within the workshop. The tutor will review your work in class. Each week is worth 1 mark, up to a maximum of 10 for the whole session. **This is a hurdle task, and you must complete at least 8 out of 12 weekly tasks to pass the unit.**

On successful completion you will be able to:
- Describe how security is integrated into different stages of the application development life cycle and explain the importance and the underlying logic.
- Assess application software security and identify the common security issues in application development through auditing and analysing source code and other documents.
- Understand and apply security related best practices to the application development process and address the common security issues for secure application development

Final exam

Assessment Type [1]: Examination
Indicative Time on Task [2]: 10 hours
Due: **Exam period**
Weighting: **30%**

The final exam assesses students' knowledge and understanding on the importance and the process of secure applications development, as well as the security issues and techniques in secure applications development covered in the semester.

On successful completion you will be able to:
- Describe how security is integrated into different stages of the application development life cycle and explain the importance and the underlying logic.

- Assess application software security and identify the common security issues in application development through auditing and analysing source code and other documents.
- Understand and apply security related best practices to the application development process and address the common security issues for secure application development

---

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

Lectures

There are 2 hours of lectures per week, that will cover concepts and principles, that will be used or discussed in the workshops. The lectures will be recorded, but participation is highly recommended.

Workshops

The weekly workshop will include practical exercises related to application development, as well as individual and group exercises related to the security context and best practices in software engineering. The practical component will require you to use a defined set of software development tools and services and expects you to become familiar with their use. The individual and group exercises on context and practices will require you to present your contribution orally and/or in writing. The assessed workshop tasks will include practical, written, and well as oral presentation tasks.

Participation

The course includes assessment participatory tasks during the workshops. However, beyond this explicit assessment, we expect students to participate in workshops and lecturers and be actively involved in group projects. We also expect that students inform them regularly via the standard platforms such as iLearn if there are any changes or updates in the unit.

Recommended Texts

The books and text that will be mainly used in the course, will be announced in week 1. The course does not have a single textbook. For different topics and weeks, we will recommend texts for further study.

The projects and workshop may require you to find and study resources and texts yourself. In

reports, please refer clearly to any resource or text that you are using.

The exam will only cover topics that have been explicitly covered during the workshops, earlier assessments, and during lectures.

Unit Schedule

The following schedule is tentative and may change if circumstances require it.

Week commencing	Topic **
Mon 21 February - Week 1	Fundamentals
Mon 28 February - Week 2	Secure requirements
Mon 7 March - Week 3	Secure design
Mon 14 March - Week 4	Writing Secure Code
Mon 21 March - Week 5	Code Analysis Tools
Mon 28 March - Week 6	Data Flow Problems
Mon 4 April - Week 7	Control Flow Problems
Mon 11 April - Non-teaching week	Break from classes (work on assigment)
Mon 18 April - Non-teaching week	Break from classes (work on project)
Mon 25 April - Week 8	Testing for Security
Mon 2 May - Week 9	Integration
Mon 9 May - Week 10	Review for Security
Mon 16 May - Week 11	Risks and Metrics
Mon 23 May - Week 12	DevSecOps
Mon 30 May - Week 13	Student Presentations

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.

Changes from Previous Offering

This is the first offering of this course.