ELEC8860

Hardware Security

Session 1, In person-scheduled-weekday, North Ryde 2024

School of Engineering

Contents

General Information 2

Learning Outcomes 2

General Assessment Information 3

Assessment Tasks 4

Delivery and Resources 7

Policies and Procedures 7

Changes from Previous Offering 9

Engineers Australia Competency Mapping 9

Changes since First Published 10

General Information

Unit convenor and teaching staff
Unit Convener and Lecturer in Charge
Ediz Cetin
ediz.cetin@mq.edu.au
Contact via Contact via Email
44 Waterloo Road, Room: 117
Monday's 14:00 – 16:00 hrs.

Tutor
Richard Vu
richard.vu@mq.edu.au
Contact via Contact via Email
44 Waterloo Road

Credit points
10

Prerequisites
Admission to MEngElecEng

Corequisites

Co-badged status

Unit description
This unit will provide an in-depth introduction to the principal concepts, foundations, and methodologies for the design of trustworthy security systems on hardware. Specifically, the unit aims to equip students with the skills needed to build secure and trustworthy hardware using Field Programmable Gate Array (FPGA) technology. The unit will cover topics in cryptosystems, error coding techniques as well as state-of-the-art hardware security systems. The unit will also provide the students with an understanding of and fluency in the quantitative evaluation of design alternatives while considering design metrics such as performance, power dissipation, cost and security.

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: Demonstrate a detailed understanding of computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities.
ULO2: Demonstrate a detailed understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks.
ULO3: Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.
ULO4: Design, build, test and verify, a trustworthy, hardware system that meets its specifications with regard to both functionality and security.

General Assessment Information

Grading and passing requirement for unit

In order to pass this unit a student must obtain a mark of 50 or more for the unit (i.e. obtain a passing grade P/CR/D/HD).

For further details about grading, please refer below in the policies and procedures section.

Hurdle Requirements

There are no hurdle requirements.

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:

Assignment 1 report, Assignment 2 report and Project Report – YES, Standard Late Penalty applies

Assessment Tasks

Name	Weighting	Hurdle	Due
Assignment 1	10%	No	Week 4
Assignment 1 Defence	15%	No	Week 4
Assignment 2	10%	No	Week 7
Assignment 2 Defence	15%	No	Week 7
Project Report	20%	No	Week 13
Project Defence	30%	No	Exam Period

Assignment 1

Assessment Type [1]: Report
Indicative Time on Task [2]: 21 hours
Due: **Week 4**
Weighting: **10%**

Assignment 1 Report (1000-word equivalent)

On successful completion you will be able to:

- Demonstrate a detailed understanding of computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities.
- Demonstrate a detailed understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks.
- Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.

Assignment 1 Defence

Assessment Type [1]: Viva/oral examination
Indicative Time on Task [2]: 6 hours
Due: **Week 4**
Weighting: **15%**

Assignment 1 Defence

On successful completion you will be able to:

- Demonstrate a detailed understanding of computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities.
- Demonstrate a detailed understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks.
- Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.

Assignment 2

Assessment Type [1]: Report
Indicative Time on Task [2]: 21 hours
Due: **Week 7**
Weighting: **10%**

Assignment 2 Report (1000-word equivalent)

On successful completion you will be able to:

- Demonstrate a detailed understanding of computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities.
- Demonstrate a detailed understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks.
- Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.

Assignment 2 Defence

Assessment Type [1]: Viva/oral examination
Indicative Time on Task [2]: 6 hours
Due: **Week 7**
Weighting: **15%**

Assignment 2 Defence

On successful completion you will be able to:

- Demonstrate a detailed understanding of computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities.
- Demonstrate a detailed understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks.
- Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.

Project Report

Assessment Type [1]: Report
Indicative Time on Task [2]: 45 hours
Due: **Week 13**
Weighting: **20%**

Project Report (2000-word equivalent)

On successful completion you will be able to:

- Demonstrate a detailed understanding of computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities.
- Demonstrate a detailed understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks.
- Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.
- Design, build, test and verify, a trustworthy, hardware system that meets its specifications with regard to both functionality and security.

Project Defence

Assessment Type [1]: Viva/oral examination
Indicative Time on Task [2]: 12 hours
Due: **Exam Period**
Weighting: **30%**

Project Defence

On successful completion you will be able to:

- Demonstrate a detailed understanding of computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities.
- Demonstrate a detailed understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks.
- Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.
- Design, build, test and verify, a trustworthy, hardware system that meets its specifications with regard to both functionality and 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

Textbook: None required to purchase. Lecturer will provide the reading material.

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 from Previous Offering

Incorporated more hardware hands-on knowledge.

Engineers Australia Competency Mapping

EA Competency Standard		Unit Learning Outcomes
Knowledge and Skill Base	1.1 Comprehensive, theory-based understanding of the underpinning fundamentals applicable to the engineering discipline.	
	1.2 Conceptual understanding of underpinning maths, analysis, statistics, computing.	
	1.3 In-depth understanding of specialist bodies of knowledge	1, 2
	1.4 Discernment of knowledge development and research directions	
	1.5 Knowledge of engineering design practice	1, 2
	1.6 Understanding of scope, principles, norms, accountabilities of sustainable engineering practice.	

Engineering Application Ability	2.1 Application of established engineering methods to complex problem solving	3, 4
	2.2 Fluent application of engineering techniques, tools and resources.	3, 4
	2.3 Application of systematic engineering synthesis and design processes.	4
	2.4 Application of systematic approaches to the conduct and management of engineering projects.	3, 4
Professional and Personal Attributes	3.1 Ethical conduct and professional accountability.	1 ,2
	3.2 Effective oral and written communication in professional and lay domains.	3, 4
	3.3 Creative, innovative and pro-active demeanour.	
	3.4 Professional use and management of information.	
	3.5 Orderly management of self, and professional conduct.	
	3.6 Effective team membership and team leadership	

Changes since First Published

Date	Description
15/02/2024	Reflecting latest MQCMS updates
15/02/2024	Put the assessment tasks in the correct order.

Unit information based on version 2024.03 of the Handbook