ELEC8860

Hardware Security

Session 1, In person-scheduled-weekday, North Ryde 2023

School of Engineering

Contents

General Information

Unit convenor and teaching staff
Darren Bagnall
darren.bagnall@mq.edu.au
Contact via email
44 Waterloo Road, Room 102
Friday 10 am to 1pm

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

To pass this unit you must:

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

If you receive special consideration for the final exam, a supplementary exam will be scheduled by the faculty during a supplementary exam period, typically about 3 to 4 weeks after the normal exam period. By making a special consideration application for the final exam 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. Approved applicants will receive an individual notification one week prior to the exam with the exact date and time of their supplementary examination.

Late Assessment Submission Penalty

Unless a Special Consideration request has been submitted and approved, a 5% penalty (of the total possible mark of the task) will be applied for each day a written report or presentation 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. The submission time for all uploaded assessments is **11:55 pm**. A 1-hour grace period will be 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, please apply for Special Consideration.

Assessments where Late Submissions will be accepted

Research Assignment

Practical Assignment

Late submission will not be accepted for the Weekly Quiz

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.

Assessment Tasks

Name	Weighting	Hurdle	Due
Research Assignment	15%	No	Week 8
Practical Assignment	25%	No	Week 11
Examination	40%	No	TBA
Practical Assignment	10%	No	Week 11
Weekly Quiz and reflection	10%	No	Weeks 2,3,4,5,6,7,8,9,10,11

Research Assignment

Assessment Type [1]: Report
Indicative Time on Task [2]: 17 hours
Due: **Week 8**
Weighting: **15%**

Students will research appropriate literature and provide a detailed analysis of a hardware system and relationship between the security level of the hardware system and the performance, cost, security metrics, and operational characteristics

On successful completion you will be able to:

- Describe, with advanced expertise, the relationship between the security level of a hardware system and its performance, cost, security metrics, and operational characteristics.

Practical Assignment

Assessment Type [1]: Report
Indicative Time on Task [2]: 28 hours
Due: **Week 11**
Weighting: **25%**

Students will provide a report on a practical project in which they will have designed, built, tested and verified a trustworthy hardware system that meets its specifications with regard to both

functionality and security.

On successful completion you will be able to:

- Design, build, test and verify, a trustworthy, hardware system that meets its specifications with regard to both functionality and security.

Examination

Assessment Type [1]: Examination
Indicative Time on Task [2]: 45 hours
Due: **TBA**
Weighting: **40%**

The examination will explore the students understanding of computer system computer system architectures and the ways in which systems are vulnerable to attack from untrusted entities, as well as their understanding of chip-level, PCB-level and System-level attacks and the countermeasures employed to mitigate security risks

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.

Practical Assignment

Assessment Type [1]: Presentation
Indicative Time on Task [2]: 10 hours
Due: **Week 11**
Weighting: **10%**

Students will present the trustworthy hardware system that they have built in the practical assignment, they will demonstrate that it meets its specifications with regard to both functionality and security.

On successful completion you will be able to:

- Design, build, test and verify, a trustworthy, hardware system that meets its

specifications with regard to both functionality and security.

Weekly Quiz and reflection

Assessment Type [1]: Quiz/Test
Indicative Time on Task [2]: 11 hours
Due: **Weeks 2,3,4,5,6,7,8,9,10,11**
Weighting: **10%**

Students will have a weekly opportunity to test their understanding of the course content. They will also have an opportunity to reflect upon their progress with their understanding of hardware security, as well as their progress towards completion of the assignments.

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

The unit will be delivered through information provided in iLEARN and in the 3 hour workshop sheduled each week.

Students should bring note paper, log books.

From WEEK 1 to WEEK 6, the workshops will focus on disucssion and consideration of the key

concepts and knowledge ascociated with Hardware Security (roughly 1 hour), these dsicussions will be followed by time dedicated to working through question sets.

From WEEK 7 to WEEK12, the workshops will be mainly laboratory work focussed on the practical assignment. Hardware/Software required will be provided.

Methods of Communication

- We will communicate with you via your university email or through announcements on iLearn. Queries to convenors can either be placed on the iLearn discussion board or sent to ELEC8860@mq.edu.au from your **university email** address.

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 in relation to COVID, these will be communicated via iLearn.

Unit Schedule

Refer to iLearn and lecture notes for the unit schedule.

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

All aspects of the unit have changed significantly since it was last delivered in 2020

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	