Dalhousie University

The Dalhousie University Senate acknowledges that we are in Mi'kma'ki, the ancestral and unceded territory of the Mi'kmaq People and pays respect to the Indigenous knowledges held by the Mi'kmaq People, and to the wisdom of their Elders past and present. The Mi'kmaq People signed Peace and Friendship Treaties with the Crown, and section 35 of the Constitution Act, 1982 recognizes and affirms Aboriginal and Treaty rights. We are all Treaty people. The Dalhousie University Senate also acknowledges the histories, contributions, and legacies of African Nova Scotians, who have been here for over 400 years.

Electrical and Computer Engineering

ECED 4406: Cybersecurity
Fall 2024

Lecture 1: Wednesday, 4:05-5:25PM, B227
Lecture 2: Friday, 4:05-5:25PM, B227
Lab: Friday 8:35-11:25AM, C234, Check Brightspace for schedule
No in-person lab Sept 6th

SECTION A: COURSE INFORMATION

Instructor Information

- **Instructor:** Dr. Colin O'Flynn (he/him)
- **Email:** coflynn@dal.ca (do NOT use other emails for course information)
- **Office Hours:** Wednesday & Fridays, 3:00PM-4:00PM, Room K205

TA Information

- **TA (LAB):** Brian Peters
- **TA E-Mail:** brian.peters@dal.ca
- **Marker:**
- **Marker E-Mail:**

Course Description

Design of secure embedded systems is critical for deploying any connected technology today. This class covers methods used to secure computer systems in general, and then applies them to embedded systems. Many attacks specific to embedded systems are covered, and students will be performing their own tests and development of attacks. Attacks specific to embedded systems including invasive and non-invasive attacks will be covered in detail, both theoretically and in labs.

Class Format

This class is offered in-person. Lectures are twice per week.

Course Pre-requisites, Co-requisites and/or other Restrictions

Students must have taken ECED 3403 Computer Architecture or equivalent. Students will be expected to understand C and Python code.

Course Rationale and/or Other Restrictions and Requirements

Design of secure embedded systems is critical for deploying any connected technology today. In this course you will learn about designing secure embedded systems, including those that run based on high-level operating systems (such as Linux or Android), along with those running "bare-metal", and even down to hardware design considerations of ASICs.

Extensive use of Brightspace will be used for course material distribution, and the message board feature will be enabled. Students are expected to post course-related questions to this message board, to allow TAs and other students to assist. The instructor will be monitoring and answering questions on this board as well. The instructor may be contacted for confidential questions via e-mail, and the instructor will attempt to respond within 3 days to all emails.

Class cancellations will be posted to Brightspace – students MUST ensure they have access to Brightspace material. When the university is closed due to winter storms (see http://dal.ca/storm) associated deadlines will be moved forward 24 hours, and quizzes during storms will be cancelled.

Lectures will be posted to (or linked from) Brightspace – this includes lectures that occur during a university closure due to storms. Students must seek out and catch up on missed lectures.

Late assignments or labs will not be accepted, unless an exceptional circumstance (such as illness) is presented, which has been accepted by the engineering department. If you are ill please submit a S*tudent Declaration of Absence* as mentioned below.

Short-term Missed Work and Absence Reporting
Any absence resulting in missed academic work must be reported using the Engineering Student Absence Reporting online system. This applies to both *Student Declaration of Absence* and *Request for Accommodation*. Visit forms.engineering.dal.ca for details and to submit a request.

Missed quizzes will be dropped. Missed assignments & labs will be given an extension.

Minimal Technical Requirements
Students will need a laptop to access Brightspace. Additional software may be installed during the class if students wish to perform labs remotely.

Learning Management System Site Information
Students must have access to brightpsace for this course.

Course Learning Outcomes
Upon completion of this course, students will be able to:

- Apply threat modeling to an embedded system to understand relevant attacks and costs.
- Using Ghidra, reverse engineering of binaries to understand system functions.
- Applying symmetric and asymmetric encryption algorithms.
- Research and report on an existing embedded system attack.
- Apply non-invasive attacks to an embedded system.

Required Text(s)
"The Hardware Hacking Handbook: Breaking Embedded Security with Hardware Attacks" by Jasper van Woudenberg & Colin O'Flynn

This book will be used extensively in the course. The book is available online as well, with more information provided in the BrightSpace.

Course Schedule
The lecture plan has been adapted from the previous online edition, and is subject to change. The lectures from a previous year are available at
https://www.youtube.com/playlist?list=PLyAXNQGte3qNNbs8J3gE8JkpAJ9_OH75q (link in Brightspace too).

Week/Module Class Dates	Focus Topic	Activities	Slide Set(s)
1	Introduction		0x100
2	History, Positioning, Applications		0x104-0x10A
3	Security Properties		0x201-0x208
4	Symmetric & Asymmetric Crypto	Lab 1	0x209-0x20B
5	HW Reverse Engineering & OS Attacks	Lab 2	0x301-0x303
6	SW Reverse Engineering	Project Introduction	0x401-0x406
7	Embedded Reverse Engineering		0x407-0x409
8	Side Channels	Lab 3	0x500-0x502
9	Power Analysis (DPA)	Lab 4	0x503, 0x504
10	Microarchitectural Attacks		0x507
11	Fault Injection		0x600
12	Wrap-Up & Summary of Class	Exam Intro	All previous slides

A more updated lecture plan will be provided as the course progresses.
0x100: Overall Topic: Introduction to Cybersecurity & Embedded Systems

- 0x101 Security in History: Basic Ciphers
- 0x102 Security in History: Enigma
- 0x103 What is Computer Security?
- 0x104 What is Computer Safety?
- 0x105 What are Embedded Systems?
- 0x106 Engineering Ethics & Computer Security
- 0x107 Application-Specific: Internet of Things
- 0x108 Application-Specific: Automotive Systems
- 0x109 Application-Specific: Industrial Control Systems

0x200 Overall Topic: Introduction to Modern Cryptosystems

- 0x201 What Security Gives Us
- 0x202 Confidentiality
- 0x203 Integrity
- 0x204 Authentication
- 0x205 Example: Secure Message Delivery
- 0x206 Symmetric Encryption Basics
- 0x207 AES Introduction

- 0x208 AES Modes
- 0x209 RSA Introduction
- 0x20A RSA Attacks

Overall Topic: Designing Secure Embedded Systems
- 0x301 Threat Modelling
- 0x302 Embedded Attacks Overview
- 0x302 Firmware Upgrades and Bootloaders

Overall Topic: Reverse Engineering
- 0x401 Introduction to Reverse Engineering
- 0x402 Exploring C to ASM
- 0x403 Function Calling
- 0x404 Local Variables
- 0x405 Binary Formats
- 0x406 Finding Binaries
- 0x407 Introducing Ghidra
- 0x408 Identifying Functions

Overall Topic: Non-Invasive & Semi-Invasive Attacks
- 0x501 Introduction to Side-Channel Attacks
- 0x501 Simple Power Analysis
- 0x502 Large Hamming Weight Swings
- 0x503 Measuring a Single Bit of AES
- 0x504 Attacking AES with Power Analysis

Course Assessments
This course involves has an emphasis on the hands-on labs. All material (labs, research project reports) must be submitted via Brightspace and specific templates will be given on Brightspace.
Assignments, quizzes, and labs must be submitted via Brightspace. **The student is responsible for ensuring they have access to Brightspace and monitoring deadlines posted to the course page.**
- Assignments (every 2-3 weeks) = 20%
- Quizzes = 15%
- Labs = 15%
- Course project (1x) = 10%
- Final Exam = 20% **Final Exam Date TBD**
- Final Lab Exam = 20%

Quizzes
- Quizzes will be posted to Brightspace, and occur throughout the class (normally 3 per month, will vary with class topic). These are designed to give you rapid feedback on your class progress.
- You can drop the lowest two quiz marks, meaning your quiz mark will be made up of the remaining marks.
- There is no make-up for missed quizzes. The “free” dropped quizzes are designed to allow you to miss one or two. If you miss a quiz due to illness the mark will be dropped and your final mark consists of the remaining quiz average only.

Final Exam

The Final Exam will be a comprehensive exam. The final example is split into two portions:

- A written final exam, scheduled during the normal final exam time.
- A lab exam, which will occur during one of the final lab sessions of the year.

Lab Topics

Labs are completed in groups of 2. Lab topics may include:

1. Dumping firmware from a device.
2. Code signing & verification of firmware image.
3. Reverse Engineering using Ghidra
4. Side-channel power analysis (Timing Attack).
5. Side-channel power analysis (DPA Attack).
6. Fault injection attack (instruction corruption).

Course-specific policies

Students may use the self-reporting forms for missed assignments and labs at forms.engineering.dal.ca.

Students requesting academic accommodations must be registered with the Mark A. Hill accessibility center. Students with learning disabilities should register as early as possible and should identify themselves to the instructor early in the term and at least one week before any testing or activity which require accommodations. I cannot offer exemptions to rules without having an official accommodation registered – please do not email me personal information.

SECTION B: UNIVERSITY STATEMENTS

Territorial Acknowledgement:

The Dalhousie University Senate acknowledges that we are in Mi'kma'ki, the ancestral and unceded territory of the Mi'kmaq People and pays respect to the Indigenous knowledges held by the Mi'kmaq People, and to the wisdom of their Elders past and present. The Mi'kmaq People signed Peace and Friendship Treaties with the Crown, and section 35 of the Constitution Act, 1982 recognizes and affirms Aboriginal and Treaty rights. We are all Treaty people.[1] The Dalhousie University Senate also acknowledges the histories, contributions, and legacies of African Nova Scotians, who have been here for over 400 years.

Internationalization

At Dalhousie, "thinking and acting globally" enhances the quality and impact of education, supporting learning that is "interdisciplinary, cross-cultural, global in reach, and orientated toward solving problems that extend across national borders."

Academic Integrity

At Dalhousie University, we are guided in all of our work by the values of academic integrity: honesty, trust, fairness, responsibility and respect. As a student, you are required to demonstrate these values in all of the work you do. The University provides policies and procedures that every member of the university community is required to follow to ensure academic integrity.

Accessibility

The Student Accessibility Centre is Dalhousie's centre of expertise for matters related to student accessibility and accommodation.

If there are aspects of the design, instruction, and/or experiences within this course (online or in-person) that result in barriers to your inclusion please contact:

- the Student Accessibility Centre (for all courses offered by Dalhousie with the exception of Truro)
- the Student Success Centre in Truro for courses offered by the Faculty of Agriculture

Your classrooms may contain accessible furniture and equipment. It is important that these items remain in place, undisturbed, so that students who require their use will be able to fully participate.

Conduct in the Classroom – Culture of Respect

Substantial and constructive dialogue on challenging issues is an important part of academic inquiry and exchange. It requires willingness to listen and tolerance of opposing points of view. Consideration of individual differences and alternative viewpoints is required of all class members, towards each other, towards instructors,

[1] The Dalhousie University Senate also acknowledges the histories, contributions, and legacies of African Nova Scotians, who have been here for over 400 years.
For more information about the purpose of territorial acknowledgements, or information about alternative territorial acknowledgements if your class is offered outside of Nova Scotia, please visit https://native-land.ca/.

and towards guest speakers. While expressions of differing perspectives are welcome and encouraged, the words and language used should remain within acceptable bounds of civility and respect.

Diversity and Inclusion – Culture of Respect

Every person at Dalhousie has a right to be respected and safe. We believe inclusiveness is fundamental to education. We stand for equality. Dalhousie is strengthened in our diversity. We are a respectful and inclusive community. We are committed to being a place where everyone feels welcome and supported, which is why our Strategic Direction prioritizes fostering a culture of diversity and inclusiveness (Strategic Priority 5.2).

Code of Student Conduct

Everyone at Dalhousie is expected to treat others with dignity and respect. The Code of Student Conduct allows Dalhousie to take disciplinary action if students don't follow this community expectation. When appropriate, violations of the code can be resolved in a reasonable and informal manner—perhaps through a restorative justice process. If an informal resolution can't be reached, or would be inappropriate, procedures exist for formal dispute resolution.

Fair Dealing policy

The Dalhousie University Fair Dealing Policy provides guidance for the limited use of copyright protected material without the risk of infringement and without having to seek the permission of copyright owners. It is intended to provide a balance between the rights of creators and the rights of users at Dalhousie.

Originality Checking Software

The course instructor may use Dalhousie's approved originality checking software and Google to check the originality of any work submitted for credit, in accordance with the Student Submission of Assignments and Use of Originality Checking Software Policy. Students are free, without penalty of grade, to choose an alternative method of attesting to the authenticity of their work, and must inform the instructor no later than the last day to add/drop classes of their intent to choose an alternate method.

Student Use of Course Materials

These course materials are designed for use as part of the Course Code at Dalhousie University and are the property of the instructor unless otherwise stated. Third party copyrighted materials (such as books, journal articles, music, videos, etc.) have either been licensed for use in this course or fall under an exception or limitation in Canadian Copyright law. Copying this course material for distribution (e.g. uploading to a commercial third-party website) may lead to a violation of Copyright law.

SECTION C: UNIVERSITY POLICIES, GUIDELINES, AND RESOURCES FOR SUPPORT

The University Policies, Guidelines and Resources for Support for Section C and their respective links will be made available on the Centre for Learning and Teaching (CLT) website, on the homepage of the Learning Management System (LMS) and on the Dalhousie Academic Support website.

Dalhousie courses are governed by the academic rules and regulations set forth in the Academic Calendar and the Senate.

Important student information, services and resources are available as follows:

University Policies and Programs

- Important Dates in the Academic Year (including add/drop dates)
- Classroom Recording Protocol
- Dalhousie Grading Practices Policy
- Grade Appeal Process
- Sexualized Violence Policy
- Scent-Free Program

Learning and Support Resources

- Academic Support - Advising Halifax, Truro
- Student Health & Wellness Centre
- On Track (helps you transition into university, and supports you through your first year at Dalhousie and beyond)
- Indigenous Student Centre. See also: Indigenous Connection.
- Elders-in-Residence: The Elders in Residence program provides students with access to First Nations elders for guidance, counsel and support. Visit the office in the Indigenous Student Centre or contact the program at elders@dal.ca or 902-494-6803.
- Black Student Advising Centre
- International Centre
- South House Sexual and Gender Resource Centre
- LGBTQ2SIA+ Collaborative
- Dalhousie Libraries
- Copyright Office
- Dalhousie Student Advocacy Service (DSAS)
- Dalhousie Ombudsperson
- Human Rights & Equity Services
- Writing Centre
- Study Skills/Tutoring