DALHOUSIE UNIVERSITY
FACULTY OF ENGINEERING

ECED 4406 Cybersecurity

Course Syllabus – Fall 2023

Last Update: Sept 3 / 2023

Delivered as Lectures, Class Times:

- **Monday at 10:05AM – 11:25AM Atlantic Time, B228**
- **Thursdays at 10:05AM – 11:25PM Atlantic Time, B228**
- **NOTE: NO CLASS Sept 11th or 14th (information to be posted)**

Lab Times:

- **Tuesday 2:35-5:25PM in C248, Labs will be mostly done remotely instead, watch class announcements for details.**

Instructor: Colin O'Flynn, PhD

Instructor Contact: coflynn@dal.ca (DO NOT use any other email to contact the instructor, your message will be deleted without notice).

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.

Textbook: We will use "The Hardware Hacking Handbook" for references and class material. You can access an electronic copy through Bright Space.

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

Course Summary

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.

Course Learning Outcomes

- 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.

Course Grading

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 Lab Example = 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.

Course-specific policies:

- Plagiarism detection software is being used by the instructor in this course for final report and lab reports.
- Audio and visual recording equipment will be in use to record lectures. You will be notified when this equipment is ON and RECORDING, and you will be given the opportunity during class-time to ask questions when the equipment is not operating.
- A supplemental exam is available for this course, subject to department rules/availability.

Lecture Plan

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).

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

Lab Topics

Labs are completed in groups of 1-3.

1. Coding for embedded developing, basic security example.
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).

Office Hours & Contact

There is no on-campus office hours, instead the class schedule will provide time for office hours. I will also make available an online schedule to meet using Microsoft Teams.

Special Accommodations:
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

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.

Academic Integrity:
All work in this course is to be your individual or group work as appropriate and as assigned. You are expected to make yourself familiar with the Dalhousie University Policy on Plagiarism which is located at: http://plagiarism.dal.ca. Copying other's work will not be tolerated (including plagiarism off the web). If you make extensive use of another's work, give proper attribution for it in a reference or bibliography.