Carleton University
Department of Systems and Computer Engineering

SYSC 5807:
Advanced Topics in Computer Systems: Cryptographic Implementations and Side-Channel Analysis

Course Outline

Instructor Information

Mostafa Taha
Email: mtaha@sce.carleton.ca
Online Lectures Mondays and Wednesday s (11:35 am-12:55 pm)
Zoom Link: https://carleton-ca.zoom.us/j/92731284693

Calendar Information

- *Course Number:* SYSC5807
- *Title:* Advanced Topics in Computer Systems: Cryptographic Implementations and Side-Channel Analysis
- *Calendar description:* An in-depth course on secure implementation of popular cryptographic algorithms. Lectures will discuss the direct naïve implementations of RSA, AES, SHA-3 and ECC algorithms and introduce a collection of implementation-specific attacks including; power/electromagnetic attacks, fault-injection attacks, timing attacks and microarchitecture attacks. The course will also discuss common countermeasures against these attacks.

Prerequisites

Assumed Knowledge

Upon entry into this course, students are expected to have knowledge about fundamentals of computer security (cryptography, authentication, etc.) along with Matlab or Python programming languages.

Course Objectives

The typical design goals of engineers with respect to mathematically-involved algorithms are: speed, low area, and low power. When it comes to cryptographic algorithms, security of the implementation should be the first and foremost design goal. Implementation attacks are a group of practical attacks that can break a secure system by targeting vulnerabilities in the underlying implementation of a cryptographic algorithm rather than its mathematical structure. An adversary can harvest information about the required secret data by collecting observable system-wide parameters that are generated as a by-product of computation. These parameters include, but are not limited to, power consumption, electromagnetic radiation, variations in the computation time, and response to induced faults. These attacks do not exploit coding errors or bugs, but rather, the very nature of our electronic computing machines.

This course starts from typical implementation of some cryptographic algorithms (RSA, AES, SHA-3 and ECC) and introduces common techniques to mount side-channel analysis and implementation attacks along with their respective countermeasures. The course can be viewed as an introduction to cryptographic algorithms for engineering students and aims at supporting graduate students with the basic knowledge of how to approach designing/coding for security-related applications.

Learning Outcomes

At the end of this course, students should know and understand:

1. Implementation details of some of the mostly used algorithms for encryption, hashing and public-key cryptography.
2. Common methodologies to mount Side-channel analysis and implementation attacks.
3. That focusing the design target solely on efficiency can lead to security vulnerabilities.

At the end of this course, students should be able to:

1. Implement some of the common cryptographic algorithms.
2. Understand a large set of implementation attacks.
3. Analyze cryptographic implementations for common vulnerabilities.
4. Implement countermeasures to thwart implementation attacks in hardware, software and/or co-design.
5. Implement and evaluate results of non-invasive vulnerability testing against implementation attacks.

Textbooks (or other resources)

- No textbook is required for this course. Course materials and other instructional materials will be posted on the course web page through cuLearn. Students are expected to check this page frequently.
- All course material and instructional materials are covered by the rules stipulated in *Copyright on Course Materials* of General Regulations section below.
- *Recommended Additional Reading:*
  - *Çetin Kaya Koç, Cryptographic Engineering, Spinger, 2009, ISNB: 9780387718163*
    URL: https://link-springer-com.proxy.library.carleton.ca/book/10.1007%2F978-0-387-71817-0
  - *Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Cryptography Engineering: Design Principles and Practical Applications, Wiley, 2010, ISBN: 9780470474242*
    URL: https://ebookcentral-proquest-com.proxy.library.carleton.ca/lib/oculcarleton-ebooks/detail.action?docID=661548
  - *"Introduction to cryptography with mathematical foundations and computer implementations" Stanoyevitch, Alexander.*
    URL: https://ebookcentral-proquest-com.proxy.library.carleton.ca/lib/oculcarleton-ebooks/detail.action?pq-origsite=primo&docID=5938939

- *Seth James Nielson, Christopher K. Monson, "Practical Cryptography in Python: Learning Correct Cryptography by Example" https://learning.oreilly.com/library/view/practical-cryptography-in/9781484249000/?ar*
- *Mangard, Stefan, Elisabeth Oswald, and Thomas Popp. Power analysis attacks: Revealing the secrets of smart cards. Springer, 2008, ISBN: 9780387308579 URL: https://link.springer.com/book/10.1007%2F978-0-387-38162-6*

Evaluation and Grading Scheme

The course work will be evaluated as follows:

Component	Percentage
Assignments	20%
Paper review and presentation	25%
Quizzes	20%
Course Project	35%

Breakdown of course requirements

Lectures & quiz:

- There are two 1.5-hour lecture per week. Some lectures will contain presentations by student teams on projects and paper reviews.
- The course will contain a series of small quizzes. There are no make-up quizzes. The grade of the quizzes can be shifted to another course component based on a valid medical certificate. The medical certificate must adhere to the format required by the Registrar. The format is available through the Registrar's website http://www.carleton.ca/registrar/forms.

Week-by-Week breakdown (tentative)

1. *Overview of Applied Cryptography*
2. *Power and Fault Attacks on RSA-CRT and Countermeasures.*
3. *Implementations of AES.*
4. *Implementations of SHA-3.*
5. *Implementations of ECC.*
6. *Power/EM Attacks.*
7. *Differential Power Analysis (DPA) and Countermeasures.*
8. *Timing Attacks and Countermeasures.*
9. *Cache Attacks and Countermeasures.*
10. *Microarchitecture attacks and Countermeasures.*

11. *Fault Analysis and Countermeasures.*
12. *Test Vector Leakage Assessment.*

Important Information:
Session Recording

Web conferencing sessions in this course may be recorded and made available only to those within the class. Sessions may be recorded to enable access to students with internet connectivity problems, who are based in different time zone, and/or who have conflicting commitments. If students wish not to be recorded, they need to leave your camera and microphone turned off.
You will be notified at the start of the session when the recording will start, and Zoom will always notify meeting participants that a meeting is being recorded. It is not possible to disable this notification.
Please note that recordings are protected by copyright. The recordings are for your own educational use, but you are not permitted to publish to third party sites, such as social media sites and course materials sites.
You may be expected to use the video and/or audio and/or chat during web conferencing sessions for participation and collaboration. If you have concerns about being recorded, please email me directly so we can discuss these.

General Regulations

Student Responsibility: It is the student's responsibility to remain informed of all rules, regulations and procedures required by their program and by the Faculty of Graduate and Postdoctoral Affairs. Ignorance of regulations will not be accepted as a justification for waiving such regulations and procedures.

Academic Integrity: Students should be aware of their obligations with regards to academic integrity. Please review the information about academic integrity at: https://carleton.ca/registrar/academic-integrity/. This site also contains a link to the complete Academic Integrity Policy that was approved by the University's Senate.

Plagiarism: Plagiarism (copying and handing in for credit someone else's work) is a serious instructional offense that will not be tolerated.

Deferred Term Work : Students who claim illness, injury or other extraordinary circumstances beyond their control as a reason for missed term work are held responsible for immediately informing the instructor concerned and for making alternate arrangements with the instructor and in all cases this must occur no later than three (3.0) working days after the term work was due. The alternate arrangement must be made before the last day of classes in the term as published in the academic schedule. For more information, see the current *Graduate Calendar, Academic Regulations of the University, Section 9.3.*

Academic Accommodation: You may need special arrangements to meet your academic obligations during the term. You can visit the Equity Services website to view the policies and to obtain more detailed information on academic accommodation at http://www.carleton.ca/equity/ For an accommodation request, the processes are as follows:

- **Pregnancy or Religious obligation**: Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details see https://carleton.ca/equity/wp-content/uploads/Student-Guide-to-Academic-Accommodation.pdf
- **Academic Accommodations for Students with Disabilities**: The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send me your ***Letter of Accommodation*** at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (*if applicable*). **Requests made within two weeks will be reviewed on a case-by-case basis.** After requesting accommodation from PMC, meet with me to ensure accommodation arrangements are made. Please consult the PMC website (www.carleton.ca/pmc) for the deadline to request accommodations for the formally-scheduled exam (*if applicable*).
- **Survivors of Sexual Violence:** As a community, Carleton University is committed to maintaining a positive learning, working and living environment where sexual violence will not be tolerated, and where survivors are supported through academic accommodations as per Carleton's Sexual Violence Policy. For more information about the services available at the university and to obtain information about sexual violence and/or support, visit: https://carleton.ca/sexual-violence-support/.
- **Accommodation for Student Activities:** Carleton University recognizes the substantial benefits, both to the individual student and for the university, that result from a student participating in activities beyond the classroom experience. Reasonable accommodation must be provided to students who compete or perform at the national or international level. Please contact your instructor with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details, see https://carleton.ca/senate/wp-content/uploads/Accommodation-for-Student-Activities-1.pdf

Copyright on Course Materials: The materials created for this course (including the course outline and any slides, posted notes, labs, project, assignments, quizzes, exams and solutions) are intended for personal use and may not be reproduced or redistributed or posted on any web site without prior written permission from the author(s).

Health and Safety: Every student should have a copy of our Health and Safety Manual. A PDF copy of this manual is available online: http://sce.carleton.ca/courses/health-and-safety.pdf

Students from the University of Ottawa: You can request to have access to cuLearn: please see http://gradstudents.carleton.ca/forms-policies/