Carleton University
School of Computer Science

Last updated: August 28, 2023 (preliminary version, subject to change)

COMP 5900H (FALL 2023, CSI 5140 IF00)
TRUSTED COMPUTING AND EMERGING ATTACKS

GENERAL INFORMATION

Class time: 14:35-17:25, Wednesdays (Sep. 6 to Dec. 8, 2023)

Instructor: Lianying Zhao (firstname.lastname@scs.carleton.ca)

Location: Refer to the public class schedule (in-person)

Office hours: By appointment - via Brightspace (flexible), or HP5129 (Wed. only)

Course Website: Please use Brightspace as the primary source of information, where important instructions can be found that must be followed. Brightspace access for University of Ottawa Students: please see information here.

Prerequisites: Familiarity with computer architecture and operating system. Computer security, especially basic understanding of cryptography, is a plus but not mandatory. Otherwise, instructor permission is required.

COURSE DESCRIPTION

The course introduces the paradigm of trusted computing and its evolution over the past decade. Common trusted computing technologies are characterized and categorized. Their application in several academic proposals and industrial solutions is also explained. Alongside the discussion, the positioning of trusted computing is shown in a bigger picture and compared with other types of defenses/attacks. Recent (new) attack vectors concerning trustworthy program execution are also reviewed.

GRADING SCHEME

15%: in-class test, **October 18th** (online)

15%: assignment (survey), due **November 1st**

25%: paper discussion lead (sign up for two papers with an **"*"** by **September 17th**)

In addition to "first come, first served", your chance to get a paper is also affected by topic popularity, so try to decide earlier.

You can also propose papers to discuss with the instructor's approval.

Note: 10% is dedicated to the student's own original opinions about the discussed papers, including but not limited to criticisms, suggested improvements, limitations, and strengths. Regardless of the paper length, the same level of discussion depth is expected, so it is not the shorter the better.

30%: course project

15%: in-class participation

(5% for the student's own opinions expressed during class discussions)

Assignments and project reports submissions are handled electronically (i.e., through Brightspace) and there is no "grace period" with respect to a deadline - an assignment submitted even one minute after the deadline is late and subject to mark deductions.

Direct copy-paste of any content will be treated as plagiarism, regardless of whether the source of the content has been cited. The only exception is slides you use for presentations which you will not submit for credits (but reuse of public/existing material will lower your marks).

Everything you submit for evaluation (i.e., assignments, quizzes, tutorials, examinations, etc.) must be the result of your own work and only your own work. Unless it is explicitly stated otherwise, the use of any tools to generate material will be considered academic misconduct. This includes, but is not limited to, chatbots (e.g., ChatGPT, Google Bard, Bing Chart), research assistants (e.g., Elicit), and image generators (e.g., Stable Diffusion, Dall-E), etc. An exception to this rule is made for automated grammar and punctuation checking tools (such as Grammarly).

In case of any academic accommodation, with a written email to the instructor with the self-declaration form: https://carleton.ca/registrar/wp-content/uploads/self-declaration.pdf

DETAILED TOPICS (TENTATIVE)

Important dates and deadlines can be found here, including class suspension for the fall break.

Papers might be discussed in a different order and not all listed will be discussed. Max: **two** papers per class. There will be lectures in the first few weeks.

Week 1: Introduction to the course and trusted computing

- The ten-page introduction to Trusted Computing
- Hardware-Based Trusted Computing Architectures for Isolation and Attestation
- Trusted Execution Environment: What It is, and What It is Not

Week 2: Trust

- Bootstrapping Trust in Commodity Computers
- Reflections on Trusting Trust (Turing Award lecture, 1984)
- SafeKeeper: Protecting Web Passwords using Trusted Execution Environments

Week 3: Application of TC technologies

- SCONE: Secure Linux Containers with Intel SGX **(*)**

- SGX-Tor: A Secure and Practical Tor Anonymity Network with SGX Enclaves **(*)**
- EnclaveDB: A Secure Database using SGX **(*)**
- SGX-Log: Securing System Logs with SGX **(*)**
- OS integrity: Nighthawk: Transparent System Introspection from Ring -3 **(*)**
- Hypervisor integrity: HyperCheck: A Hardware-Assisted Integrity Monitor **(*)**
- Data protection: Pesos: Policy Enhanced Secure Object Store **(*)**

Week 4: Making TC technologies more adoptable/usable

- Flicker: An Execution Infrastructure for TCB Minimization **(*)**
- Glamdring: Automatic Application Partitioning for Intel SGX **(*)**
- Occlum: Secure and Efficient Multitasking Inside a Single Enclave of Intel SGX **(*)**
- Civet: An Efficient Java Partitioning Framework for Hardware Enclaves **(*)**
- vTZ: Virtualizing ARM TrustZone **(*)**
- Towards Memory Safe Enclave Programming with Rust-SGX [Rust + SGX] **(*)**
- RusTEE: Developing Memory-Safe ARM TrustZone Applications [Rust + ARM] **(*)**
- SGXPy: Protecting integrity of Python applications with Intel SGX [Python + SGX] **(*)**
- Using ARM TrustZone to Build a Trusted Language Runtime for Mobile Applications [.NET + SGX] **(*)**

Week 5: Side-channel attacks

- Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices
- Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution **(*)**
- Meltdown: Reading Kernel Memory from User Space **(*)**
- Spectre Attacks: Exploiting Speculative Execution **(*)**
- Latest: Downfall: Exploiting Speculative Data Gathering **(*)**

Week 6: Internal misbehavior: memory attacks

- SoK: Eternal War in Memory **(*)**
- Memory Errors: The Past, the Present, and the Future
- Defense: C-FLAT: Control-Flow Attestation for Embedded Systems Software **(*)**
- Defense: PTAuth: Temporal Memory Safety via Robust Points-to Authentication **(*)**
- Attacking the defense: PACMAN: Attacking ARM Pointer Authentication with Speculative Execution **(*)**

Week 7: Human authenticating machine

- Turtles All The Way Down: Research Challenges in User-Based Attestation
- Stark: Tamperproof Authentication to Resist Keylogging **(*)**
- Evil maid goes after PGP whole disk encryption
- PRISM/ Human-Verifiable Code Execution **(*)**
- **In-class test**

Week 8: No classes (Fall Break)

Week 9: State continuity

- Memoir: Practical state continuity for protected modules **(*)**
- ROTE: Rollback Protection for Trusted Execution **(*)**
- Ariadne: A Minimal Approach to State Continuity **(*)**

Week 10: Secure input/output

- SeCloak: ARM TrustZone-based Mobile Peripheral Control
- Building trusted path on untrusted device drivers for mobile devices **(*)**
- TruZ-Droid: Integrating TrustZone with Mobile Operating System **(*)**
- Establishing Trusted I/O Paths for SGX Client Systems with Aurora **(*)**
- VButton: Practical Attestation of User-driven Operations in Mobile Apps **(*)**
- ProtectIOn: Root-of-Trust for IO in Compromised Platforms **(*)**
- Fidelius: Protecting User Secrets from Compromised Browsers **(*)**

Week 11: Proposed hardware improvements

- Fine-grained isolation: IMIX: In-Process Memory Isolation EXtension **(*)**
- Memory safety: HAFIX: Hardware-Assisted Flow Integrity Extension **(*)**
- Integrity monitoring: Co-processor-based Behavior Monitoring: Application to the Detection of Attacks Against the System Management Mode **(*)**
- Integrity monitoring: CPU Transparent Protection of OS Kernel and Hypervisor Integrity with Programmable DRAM **(*)**

Week 12: Proposals based on existing (non-security) hardware support

- PixelVault: Using GPUs for Securing Cryptographic Operations **(*)**
- Graviton: Trusted Execution Environments on GPUs **(*)**
- GRIFFIN: Guarding Control Flows Using Intel Processor Trace **(*)**
- T-SGX: Eradicating Controlled-Channel Attacks Against Enclave Programs **(*)**

Week 13: Project presentations

Week 14: Project presentations

ADDITIONAL INFORMATION

For information about Carleton's academic year, including registration and withdrawal dates, see Carleton's Academic Calendar.

Graduate Academic Advisors. The Graduate Advisors for the School of Computer Science are available in Room 5302 HP; or by email at grad.scs@carleton.ca. The graduate advisors can assist with understanding your academic audit and the remaining courses required to meet graduation requirements.

SCS Computer Laboratory. Students taking a COMP course can access the SCS computer labs. The lab schedule and location can be found at: https://carleton.ca/scs/tech-support/computer-laboratories/.

All SCS computer lab and technical support information can be found at: https://carleton.ca/scs/tech-support/. Technical support staff may be contacted in-person or virtually, see this page for details: https://carleton.ca/scs/tech-support/contact-it-support/.

UNIVERSITY POLICIES

Academic Accommodations. Carleton is committed to providing academic accessibility for all individuals. Please review the academic accommodation available to students here: https://students.carleton.ca/course-outline/.

Student Academic Integrity Policy. Every student should be familiar with the Carleton University Student Academic Integrity policy. A student found in violation of academic integrity standards may be sanctioned with penalties which range from a reprimand to receiving a grade of F in the course, or even being suspended or expelled from the University. Examples of punishable offences include plagiarism and unauthorized collaboration. Any such reported offences will be reviewed by the office of the Dean of Science. More information on this policy may be found on the ODS Academic Integrity page: https://carleton.ca/registrar/academic-integrity/.

Plagiarism. As defined by Senate, "plagiarism is presenting, whether intentional or not, the ideas, expression of ideas or work of others as one's own". Such reported offences will be reviewed by the office of the Dean of Science. More information and standard sanction guidelines can be found here: https://science.carleton.ca/students/academic-integrity/.

Unauthorized Co-operation or Collaboration. Senate policy states that "to ensure fairness and equity in assessment of term work, students shall not co-operate or collaborate in the completion of an academic assignment, in whole or in part, when the instructor has indicated that the assignment is to be completed on an individual basis". Please refer to the instructions of a specific assignment and/or the instructor concerning this issue.

Religious & Pregnancy 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, visit the Equity Services website: http://carleton.ca/equity/wp-content/uploads/Student-Guide-to-Academic-Accommodation.pdf For religious obligation, visit: https://carleton.ca/equity/focus/discrimination-harassment/religious-spiritual-observances/

Academic Accommodations for Students with Disabilities. If you have a documented disability requiring academic accommodations in this course, please contact the Paul Menton Centre for Students with Disabilities (PMC) at 613-520-6608 or pmc@carleton.ca for a formal evaluation or contact your PMC coordinator to send your instructor your Letter of Accommodation at the beginning of the term. You must also contact the PMC no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, meet with your instructor as soon as possible to ensure accommodation arrangements are made. For more details, visit the Paul Menton Centre website.

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 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: 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 the policy: https://carleton.ca/senate/wp-content/uploads/Accommodation-for-Student-Activities-1.pdf