Carleton University
School of Computer Science

Last updated: Jan. 8, 2021 (preliminary version, subject to change)

COMP 5900X (WINTER 2021, CSI 5140 IX0) TRUSTED COMPUTING AND EMERGING ATTACKS

GENERAL INFORMATION

Class time: 11:35-14:25, Wednesdays (Jan.11 to Apr.14, 2021)

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

Location: Refer to the public class schedule

Office hours: Wednesdays 16:00 – 17:00 (or by appointment), cuLearn

Course Website: Please use cuLearn as the primary source of information, where important instructions can be found that must be followed.

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.

cuLearn for U of Ottawa students: for access, fill out this form and email it to Grad Studies.

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, **February 10th**

15%: assignment, due **February 23rd**

25%: paper discussion lead (sign up for two papers with an **"*"** by **January 22nd**)

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.

30%: course project

15%: in-class participation

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

Assignments and project reports submissions are handled electronically (i.e., through cuLearn) 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.

DETAILED TOPICS (TENTATIVE)

Important dates and deadlines can be found here, including class suspension for the winter 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

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

- Isolating Operating System Components with Intel SGX (*)
- SCONE: Secure Linux Containers with Intel SGX (*)
- Graphene-SGX: A Practical Library OS for Unmodified Applications on SGX (*)
- Hypervision Across Worlds: Real-time Kernel Protection from the ARM TrustZone Secure World (*)

Week 4: Making TC technologies usable

- Flicker: An Execution Infrastructure for TCB Minimization (*)
- Glamdring: Automatic Application Partitioning for Intel SGX (*)
- TrustShadow: Secure Execution of Unmodified Applications with ARM TrustZone (*)
- TruZ-Droid: Integrating TrustZone with Mobile Operating System (*)

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 (*)
- **In-class test**

Week 6: No classes (Winter Break)

Week 7: Internal misbehavior: memory attacks

- SoK: Eternal War in Memory (*)
- Memory Errors: The Past, the Present, and the Future
- GRIFFIN: Guarding Control Flows Using Intel Processor Trace (*)

Week 8: 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

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

- SeCReT: Secure Channel between Rich Execution Environment and Trusted Execution Environment (*)
- Glimmers: Resolving the Privacy/Trust Quagmire (*)
- Building trusted path on untrusted device drivers for mobile devices (*) (also see TruZ-Droid)

Week 11: Proposed hardware improvements

- Iso-X: A Flexible Architecture for Hardware-Managed Isolated Execution (*)
- AEGIS: architecture for tamper-evident and tamper-resistant processing (*)

Week 12: Proposals based on existing hardware support

- PixelVault: Using GPUs for Securing Cryptographic Operations (*)
- Graviton: Trusted Execution Environments on GPUs (*)
- Protecting Private Keys against Memory Disclosure Attacks using Hardware Transactional Memory

Week 13: Project presentations

Week 14: Project presentations

INFORMATION ON ACADEMIC ACCOMMODATIONS

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 awarded penalties which range from a reprimand to receiving a grade of F in the course or even being expelled from the program or University. Some examples of offences are: plagiarism and unauthorized cooperation or collaboration. Information on this policy may be found in the Graduate Calendar and https://science.carleton.ca/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.

Direct *copy-and-paste* of any content will be treated as plagiarism, regardless of whether the source of the content has been cited.

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

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: https://www.carleton.ca/pmc

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

Medical Certificate. The official medical certificate accepted by Carleton University for the deferral of final examinations or assignments can be found at https://carleton.ca/registrar/cu-files/medical-certificate-form/. The request must be fully and specifically supported by a medical certificate or other

relevant documentation. Additional information: https://carleton.ca/registrar/wp-content/uploads/Additional-Deferral-Information.pdf

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