COMP 5407 W (Jan-Apr 2022) Authentication and Software Security

Preliminary outline (Jan 1, 2022). For updated version see: https://people.scs.carleton.ca/~paulv/5407jan2022.html

This is a research-oriented course. It requires reading and understanding research papers. As such, it is unsuitable for course-based Master's students and those lacking solid undergrad background in security and cryptography.

Course Information

Instructor: Prof. Paul Van Oorschot paulv@scs.carleton.ca
Classroom location: posted on the public class schedule. **Update: this class is online for at least the first 3 weeks**.
Lectures: Tues+Thurs, 4:00-5:30pm, Jan. 10 – Apr.12, 2022 (excluding winter break, Feb. 21-25)
Section type: synchronous. Students are *expected to participate in all classes* in real time.
Website (e.g., for course announcements, uploading assignments, discussions): https://brightspace.carleton.ca/
U of Ottawa students: for access to Brightspace (Carleton's learning management system), fill out this form.

Required Textbook and Resources. Course readings and assignments will use online resources available openly or through the university library. As baseline knowledge, students will be assumed to understand Chapters 1-11 of the COMP 4108 textbook: Computer Security and the Internet: Tools and Jewels (1e or 2e), which is available online.

Course Calendar Description. Specialized topics in security including advanced authentication techniques, user interface aspects, electronic and digital signatures, security infrastructures and protocols, software vulnerabilities affecting security, untrusted software and hosts, protecting software and digital content.
Prerequisites: COMP 4108 (Comp. Systems Security) **strongly recommended** + undergrad cryptography. Students in course-based Masters or missing background *may struggle to get passing grades* (70%); please discuss with instructor.

Focus topics for Winter 2022. *Authentication*: PAKE (password authenticated key exchange) protocols, FIDO (user authentication), Certificate Transparency (browser certificates), OAuth (web single sign-on), device pairing and Bluetooth security. *Software security*: security testing challenges and approaches (static analysis, model checkers, fuzz testing), memory safety and the Rust programming language. For detailed syllabus, see the update URL (above).

Objectives. The course aims to expose students to several advanced topics, to augment an existing undergraduate level understanding of computer security and applied cryptography. For authentication, these topics will include several technologies that have become prominent in the past 5 years, plus a long-term case study on Bluetooth security. For software security, these will include some major recent security issues, some approaches for detecting flaws during software development, and an understanding of memory and type safety in programming languages (contrasting C vs. Rust).

Grading Scheme *(dates and late penalties are firm;* please plan your time carefully in advance*)*:
10% Participation. Insightful contribution to class discussions, including last 3 classes. Participate in all classes.
20% Project 1 (written). Due: 11:59pm Fri Feb 25. Minus 2/20 (10%) per day late.
30% Project 2 (written). Due: 11:59pm Fri Apr 15. Minus 3/30 (10%) per day late.
40% Reading Reflections (10x4%). Due 4:00pm **sharp** before most Tues. classes. Minus 0.5/4 (12.5%) per day late.

Further details. *Projects 1 and 2* require 15-20 page reports, and will involve finding, reading and integrating research papers or technical reports. Each *Reading Reflection*, a 2-page written report, will require that students carefully read, understand, and provide their view of a research paper prior to its discussion in class; these are worth 4% each and due *4:00pm sharp* on the Tuesdays of weeks 2-11. Guideline for these deliverables: use 11pt font, single column text (further instructions will be in the updated outline, URL above). Students are also expected to read designated papers before each Thursday class, to allow meaningful contribution to class discussion.

Other Important Considerations:

Individual reports. All reports are to be written **individually**, without collaboration. Students may work with others to understand concepts, but **no portion whatsoever** of submitted work may be shared. *COMP5407 addendum on academic integrity:* Beyond other university policies (below), any submissions including uncited portions originating from someone else are subject to a grade of **negative 100%**, e.g., for an item worth 20% the maximum course mark would then be 60%. Both students may be penalized if an infraction involves copying from another student.

Start readings early. Reading reflections will require understanding detailed research papers, which often **require several readings to gain an understanding**. Students should thus begin their readings well in advance of relevant due dates, in order to have time to both comprehend the papers and prepare original, high quality written reflections.

Submission mode. Deliverables will be submitted electronically through Brightspace. Late assignments are subject to penalties noted in the grading scheme. **Deadlines are strict** (one minute late counts as a whole day). To avoid lateness due to technical glitches, students are encouraged to make submissions at least one hour before the due date/time. If you don't yet have much experience reading research papers, here is some advice from one individual: How to Read a Paper.

Grammar and clarity. This is a grad level course. I expect all written submissions to be well formatted, proof-read, and free of errors in spelling, grammar, punctuation, etc. Submissions failing to meet this expectation will be subject to a **grade deduction of up to 20%** of the total available grade, independent of technical content; such failures also almost always create ambiguities or make the technical content unclear, which may further reduce the grade.

Passing grade. While strong students typically do well, a mark below 70% is a failing grade in our grad program.

University Policies

Pregnancy Obligation. 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. For more details: Equity Services.

Religious Obligation. Contact your instructor with requests for academic accommodation during the first two weeks of class, or as soon as possible after the accommodation need is known to exist. More details: https://carleton.ca/equity/focus/discrimination-harassment/religious-spiritual-observances/

Academic Accommodations for Students with Disabilities. For a documented disability requiring academic accommodations, contact the Paul Menton Centre for Students with Disabilities (PMC), 613-520-6608 or pmc@carleton.ca for a formal evaluation, or ask your PMC coordinator to send the instructor your Letter of Accommodation at the start 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 arrangements are made. More details: Paul Menton Centre

Survivors of Sexual Violence. As a community, Carleton 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 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 recognizes the substantial benefits, both to the individual student and for the university, that result from a student participating in activities beyond the classroom. Reasonable accommodation is provided to students who compete or perform at the national or international level. 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.

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 ranging from a reprimand to a course grade of *F* or being expelled from the program or University. Examples of punishable offences include: plagiarism and unauthorized collaboration. Information on this policy is found here.

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". Reported offences will be reviewed by the office of the Dean of Science. Information regarding typical penalties and guidelines are found here.

Unauthorized Co-operation or Collaboration. Senate policy states: "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 see the course outline or instructor about this issue.

If unsure of expectations regarding collaboration or academic integrity, ask the instructor. Posting any portion of assignments online (e.g., to Chegg, CourseHero, OneClass) is considered academic misconduct. You are never permitted to post, share, or upload course materials without explicit written permission from the instructor.