COMP 5407 W (Jan. 2026, Winter) (updated: Dec.11, 2025)
Authentication and Software Security [A, S]

This research-oriented course is for thesis-based graduate students. It involves reading and understanding research papers, and is generally unsuitable for course-based Master's students.

INSTRUCTOR: P. Van Oorschot

Email: paulv@scs.carleton.ca

Office hours (5173HP):
Mon 1:00– 2:00pm; Wed 10:30–11:30am

CLASS DETAILS:
- *Location:* check online (e.g., Carleton Central)
- *Times:* 11:30am-1:00pm, Mon + Wed
- *Mode:* in person

Course Website: https://brightspace.carleton.ca/d2l/home/364891
- *U of Ottawa students:* for access to Carleton's Brightspace, please see this note

Important dates/deadlines and statutory holidays: see https://students.carleton.ca/academic-dates/
- *Winter term 2026: classes Jan.5–Apr.8 (winter break/no classes: Feb.16-20)*

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 **(strongly recommended)**: undergrad courses in each of cryptography and computer security (e.g., COMP 4108). Students missing these, or in a course-based Master's, *may struggle to get a passing graduate grade (70%)*, and should meet with the course instructor to discuss.

Topics for Winter 2026. This term's topics (subject to revision) are as follows.
- (3 classes) Password-authenticated key exchange protocols.
- (3 classes) FIDO2 authentication standard and framework (security keys, passkeys).
- (3 classes) Bluetooth security, with focus on authentication.
- (3 classes) Memory safety.
- (3 classes) The Rust programming language, as a memory-safe alternative to C.
- (3 classes) Fuzz-testing.
- (1 class) Midterm exam.
- (5 classes) Student presentations.
- (1 class) Spare/make-up class or extra topic or follow-up material.

ASSESSMENT / GRADING SCHEME

35% midterm exam. *Mon. March 16*, in-class, closed-book (no aids of any sort).

30% topic reflections (6% each; low grade of 6 reports dropped). A report is 3 pages (excluding white-space, wide headings, references), summarizing class discussion of the 3-class topic, and the student's reflections thereon. For expectations for written work, see further below.

25% project (15% class presentation, 10% interview). Students select a scoped project on one of the 6 course topics. The interview is end-of-term with the instructor, on the project material.

10% participation and insightful contribution to class discussions. This requires that designated papers be read before class. Students are *expected to attend all classes*. Each class missed results in an off-the-top reduction of ½ point (out of 10). To allow time to comprehend a paper, students should **plan to begin their readings of papers well in advance of the relevant class** (because understanding detailed research papers **typically requires several readings**). If you don't have experience reading research papers, please read the following advice: How to Read a Paper.

Late Policy. Late items receive a penalty of 25% per day (partial days count as a whole day) yielding a grade of 0 after 4 days late, unless special permission was granted. This form is to be used to request consideration of such special permission: *academic considerations form*.

Missed Midterm Policy. Students missing a midterm exam receive a grade of 0. If there are exceptional circumstances, a student may request special consideration using this academic considerations form as soon as practically possible. If approved, alternate evaluation may be used such as a substitute exam, oral exam, or other means of the instructor's choosing.

COURSE OBJECTIVES. Gain experience in reading and discussing research papers. Gain experience in giving a presentation. Gain exposure to several advanced security technologies that have become prominent in recent years. Understand major aspects of Bluetooth security. Understand how memory safety in programming languages relates to software vulnerabilities.

LEARNING MATERIALS and OTHER COURSE-RELATED RESOURCES
All source materials will be freely available online or accessible through the course website. Thus, *students need purchase no textbooks or other learning materials for this course***.**

REQUIREMENTS and EXPECTATIONS for all WRITTEN DELIVERABLES:

• **Font & layout.** 11pt Times New Roman font, single column, line-and-a-half spacing or tighter.
• **No cut-and-paste.** All figures and diagrams must be created by the student; cut-and-paste of figures is an academic violation in this course. Any figure recreated from a source must have a caption stating "Figure based on original found at [xx]", where [xx] is a formal reference.
• **Formal references.** For each cited item, a References section must list four fields in this order:
1) *author name* (with the list of references alphabetized by last name of first author),
2) *article title,*
3) *venue name* (e.g., conference or periodical); and
4) *publication year.* Add month for magazine articles, month-day for newspaper/blog articles.
For books, replace venue by the publisher's name. Page numbers are optional for conferences but necessary for periodicals; a journal paper in volume 3, issue 2, pages 20-31 is cited: 3(2):20-31. If an informal article lists no author, use the organization name (or as a last resort, domain name) and also use that as the key for alphabetical sorting. When there is no formal venue (e.g., an unrefereed manuscript, whitepaper, or blog), give the URL instead; remember that a major goal of citations (aside from giving credit for ideas and quoted passages) is to provide enough detail for a reader to retrieve an item. For examples, see end-of-chapter references in this book.
• **Grammar and clarity.** It is expected that all submitted work is well formatted, proof-read, and free of errors in spelling, grammar, and punctuation. Work failing to meet this expectation is subject to *deduction of up to 20%* of the total available grade for the item, regardless of technical content; such failures usually also make the technical content unclear, further negatively impacting the grade.
• **Individual reports**. All submitted reports are to be written **individually**. Students may work with others to understand concepts, but **no portion whatsoever** of written work may be shared work. See also the policies (below) regarding generative AI tools, and academic integrity.

ACADEMIC ACCOMMODATIONS and REGULATIONS

Academic Accommodation. Carleton is committed to providing academic accessibility for all individuals. You may need special arrangements to meet your academic obligations during the term. The accommodation request processes are outlined on the Academic Accommodations website (https://students.carleton.ca/course-outline/).

Generative AI Tools. In this course you may use AI tools (like ChatGPT) to (1) error-check grammar and spelling in written reports, and (2) to prepare for verbal class discussions and more generally, generate ideas. Use of such tools for portions of any **written** work submitted for grading is prohibited; under no circumstances whatsoever may students copy or use in writing any sentence fragments or text generated by generative AI tools for submitted work items.

Academic Integrity. Students are expected to uphold the values of academic integrity, which include fairness, honesty, trust, and responsibility. Examples of actions that compromise these values include but are not limited to plagiarism, accessing unauthorized sites for assignments or tests, and unauthorized collaboration on assignments. Misconduct in scholarly activity will not be tolerated and will result in consequences as outlined in Carleton University's Academic Integrity Policy. A more detailed explanation of Academic Integrity and a list of sanctions for the Faculty of Science can be found on the Faculty of Science Academic Integrity website. Students are expected to be familiar with and abide by Carleton University's Academic Integrity Policy.

COMP 5407 addendum on academic integrity: Beyond other university policies, any student submitting work in this course, including uncited portions originating from any other source, is subject to a mark of ***negative 100%*** *on the entire work item. Example: for an assignment worth 15%, 15% is lost plus a further 15% penalty, making the best possible course mark 70% (which is the grade required to pass a grad course). Both students may be penalized for violations that involves copying from another student. Each student must write up work individually from their own personal notes, unless given explicit written permission to do otherwise. If unsure of expectations about collaboration or academic integrity, ask the instructor. Posting online any portion of assignments is considered to be academic misconduct. You are not permitted to post, share, or upload course materials on any site unless given explicit written permission from the instructor.*

Student Rights & Responsibilities. Students are expected to act responsibly and engage respectfully with other students, members of Carleton, and the broader community. See the Student Rights and Responsibilities Policy for details on the expectations of non-academic behaviour of students. Those who participate with another student in committing an infraction of this Policy will also be held liable for their actions.