COMP 5900H (September 2020; CSI-5138IH): Selected Topics in CS—Internet of Things (IoT) Security [E, T, S]

Course site for updates: https://people.scs.carleton.ca/~paulv/5900Hsept2020.html

Preliminary outline as of: 27 Aug 2020.

Course description. *The course examines security issues related to the Internet of Things (IoT), with main focus on consumer IoT devices and software, including technical design and configuration. It considers security aspects related to applications, platforms, and data communication protocols, with wireless access playing a foundational role. The course explores how IoT security issues often resemble those in the ordinary (pre-IoT) Internet, but with different risks due to IoT devices creating links between virtual and physical worlds.*

Mandatory prerequisites: introductory courses in both operating systems (e.g., COMP 3000) and computer networks (e.g., COMP 3203). *Strongly recommended prerequisites:* introductory course(s) in computer and Internet security and cryptography. Students lacking such background have in the past struggled to successfully complete this research-oriented course.

This is a research-oriented **graduate-level course intended for thesis-based students**. *It is generally unsuitable for course-based Master's students lacking substantial prior experience in security and cryptography*. The self-evaluation due Sept 16 (below) aims to assess a student's background suitability for this course.

Non-technical overview of the types of issues of interest in this course:
We're Surrounded by Billions of Internet-connected Devices. Can We Trust Them? (Adam Piore, 24-Oct-2019, newsweek.com)

Instructor: P. Van Oorschot
Office hours by video-meet: Mon 10-11am, Tues 1:00-2:00pm
Lectures (online): 11:35am-12:55pm Tues, Thurs (details via cuLearn, below)
Term dates (fall 2020): Sept 9-Dec 11, excluding Oct 12 (Thanksgiving) and Oct 26-30 (fall break).

Recommended Textbook (background): Computer Security and the Internet: Tools and Jewels by P.C. van Oorschot (2020, Springer). Available in hardcopy from bookstores, softcopy via university library, PDFs for personal use from author's website. Students are expected to know this or equivalent content from undergrad courses, and are otherwise responsible for learning it (on their own) as required to understand course content. For further supplementary resources, see the books listed on this page.

References and Sources. Lectures will be drawn from research papers available online (some behind paywalls may require electronic access via the university library), plus material distributed via cuLearn (below). No specific **access to computing labs** is required, but physical access to labs in the Herzberg Building require a Carleton University Campus Card, and is based on the courses you are registered in and on the School's Lab Access Schedule.

Grading Scheme (indicated due dates are firm—please plan in advance). All items are individual (not group) work. Links for details will be updated on course site (URL given above).

- 5% (by **Sept 16**, 23:59) Self-evaluation on security background + plan to repair any knowledge gaps.
- 15% (**Sept 25**, 23:59) Research summary of mesh network key exchange protocol.
- 15% (**ongoing**) Contributions to, and one-page reports on, other students' video-meet presentations.
- 15% (**by sign-up**) Discussion lead (for video-meet class). Selection of one lecture to lead must be arranged during Sept 8-16 with Instructor; see "Outline of topics" below.
- 10% (**Nov 2**, 23:59pm) Final project plan, PDF file. By **Oct 21**, must have completed preliminary discussion of project ideas with Instructor, by email or video-meet.

- 10% (**Nov 19—Dec 8**, approx.) Individual student project presentations, by video-meet.
- 30% (**Dec 10, 5:00pm**) Written project report, PDF file. Late penalty: 10% per day, e.g., zero after 10 days.

Timeliness: the default grade for late items and projects is zero (0), unless special permission has been granted in writing in advance. Students are advised to submit work items at least one hour in advance of official due dates/times, in anticipation of electronic glitches, software or system outages, and connectivity issues.

Main project components (10% + 10% + 30%) and requirements: details will be provided here once the class size stabilizes. A typical project involves literature research leading to a survey-oriented technical research paper; some projects introduce novel ideas, taxonomies or systematizations.

Instruction format, class preparation, and attendance. As a research and discussion-oriented graduate course, students are expected to attend all classes online synchronously, with reliance on the cuLearn platform (below). Prior to each class, students are expected to have read the paper(s) designated for that day, in order to contribute in an informed manner. If you are not living in Ottawa this term and in a different time zone, **email the Instructor during the first week of class** including your registration student ID and details of your country/time zone, to discuss if suitable accommodations can be made. The delivery of classes over the term is in three stages: (1) Instructor delivery of initial lectures; (2) student-led discusssions of designated papers, with support from Instructor and fellow students; followed by (3) student presentations related to their projects.

Student-led discussions and presentations. Students are expected to actively participate in online class discussions. They will present their projects (by video-meet) in the third stage of the course, and in the second stage each student will lead one class that covers a designated reading. As *discussion leader*, the student uses slides or other methods to deliver (by video-meet) a lecture in real time, covering the main ideas of the designated paper; and facilitates class discussion by having prepared a list of discussion items and questions. The 20% *Contributions* component of the grading scheme includes involvement throughout the term, including written feedback and assessment on presentations by fellow students.

cuLearn. Course coordination, announcements, and distribution of non-public reading materials will rely on the cuLearn course management system. Carleton students registered in the course will automatically have access to it. **UofO students must fill out the form** found here (or arrange with their UofO department administrator), and should arrange this **3-4 business days prior to the first class, in order to have access as necessary from the first class onward.**

Intellectual Property and Copyrighted Material. All materials distributed as part of this course (including lecture content, notes, and any tests) remain the intellectual property of the Instructor. They are for personal, non-transferable use by students registered in the course only, and no part of them may be reposted, reproduced, forwarded or distributed without the written consent of the Instructor. Violation is illegal and strictly prohibited, as well as being a punishable academic integrity offence.

Outline of topics (preliminary):

- during Sept 8-16: **students must select one class** (from Classes 5-18 below) to lead the class discussion on. Arrange this by email with the Instructor (first-come first-served basis). Confirmation requires the self-evaluation item (5%) to be completed, so please submit that as soon as possible. "*" denotes that a class has already been assigned.

**Class 1 (Sept 10). Background review: security and cryptography* (see recommended prerequisites). Computer Security and the Internet: Tools and Jewels, Chapter 2 (Cryptography) plus general review.

- **due Sept 16** or earlier: self-evaluation (5%) + arrangement of class to lead.

**Classes 2-4 (Sept 15, 17, 22) Wireless LAN Security: 802.11 and Wi-Fi.*

Chapter notes to be distributed via cuLearn.

Class 5 (Sept 24): Secure communications foundation for an IoT operating system.
TinySec: A link layer security architecture for wireless sensor networks (Karlof et al., SenSys 2004)

- **due Sept 25**, 23:59 (15%): research summary of mesh network key exchange protocol.

Class 6 (Sept 29): IoT Overview, terminology and origins.
Cyber-physical systems and Internet of Things (Greer et al.) NIST Special Pub 1900-202, Mar 2019

Class 7 (Oct 1): How IoT differs from IoC (Internet of Computers).
Analysis, implications and challenges of an evolving consumer IoT security landscape (Bellman et al.) PST 2019
and RFC 7228: Terminology for Constrained-Node Networks (Bormann et al.) IETF Editor

Class 8 (Oct 6): Device lifecycle and transient device association.
Resurrecting Duckling: Security issues for ad-hoc wireless networks (Stajano) 1999 Security Protocols
and Fig.1 in RFC 8576: Internet of Things (IoT) Security: State of the Art and Challenges (Apr 2019) IETF.
Supplementary: IoT security: An end-to-end view and case study (Ling et al.) arXiv:1805.05853 version of GLOBECOM 2017

Class 9 (Oct 8): Bootstrapping trust in IoT.
Talking to strangers: Authentication in ad-hoc wireless networks (Balfanz et al.) NDSS 2002

Class 10 (Oct 13): Botnets from IoT devices.
DDoS in the IoT: Mirai and other botnets (Kolias et al.) IEEE Computer 50(7):80-84 2017.
Supplementary: Understanding the Mirai botnet (Antonakakis et al.) USENIX Security 2017

Class 11 (Oct 15): Smart locks for homes (and what goes wrong).
Smart locks: Lessons for securing commodity Internet of Things devices (Ho et al.) AsiaCCS 2016

Class 12 (Oct 20): Smart home systems (Samsung SmartThings) and what goes wrong.
Security analysis of emerging smart home applications (Fernandes et al.) Oakland 2016

Class 13 (Oct 22): Embedded firmware and security.
A large scale analysis of the security of embedded firmwares (Costin et al.) USENIX Security 2014

Oct 26-30: no classes, fall break. Students should complete their project proposal (10% of final grade).

- **due Nov 2,** 23:59 (10%): final proposal for project (PDF document)

Class 14 (Nov 3): Towards IoT search engines (Censys).
A search engine backed by Internet-wide scanning (Durumeric et al.) ACM CCS 2015
and Sec.7-8 of Searching the Web of Things: State of the art, challenges, and solutions (Tran et al.) ACM Comp. Sur. 50(4) art. 55:1-34 (Nov 2017)

Class 15 (Nov 5): Empirical analysis of deployed IoT devices.
All things considered: An analysis of IoT devices on home networks (Kumar et al.) USENIX Security 2019.

Class 16 (Nov 10): IETF IoT-related standards.
A survey of the Internet Prococol suite for Internet of Things security (Tschofenig et al.) IEEE Security&Privacy (Sept/Oct 2019), 47-57.
Supplementary: RFC 8576 (see Class 8).

Class 17 (Nov 12): Security features of IoT application platforms/architectures.

Internet of Things: A survey on the security of IoT frameworks (Ammar et al.) J. Info. Security and Appl. 38 (Feb 2018) 8–27

Class 18 (Nov 17): IoT-specific OSs.
Operating systems for low-end devices in the Internet of Things: A survey (Hahm et al.) IEEE Internet of Things J. 5(3):720--734, 2016

Classes 19-24 (Nov 19 - Dec 8): Student presentations.

Class 25 (Dec 10): Course lookback. Each student will have five minutes to give reflections on the course, their view of what IoT security is, and its main challenges. They will also submit in writing (PDF) their suggestion for one paper to remove from the course for a future year (the paper they found least useful or relevant, with explanation).

- **due Dec 10**, 5:00pm (30%): final project (PDF document). Late penalty: 10% per day, e.g., zero after 10 days.

=== Additional Information on SCS Courses ===

Undergrad Academic Advisor for SCS: 5302C-HP (room), 520-2600 ext 4364 (phone), undergraduate_advisor@scs.carleton.ca (email). This advisor can assist with information about prerequisites and preclusions, course substitutions/equivalencies, understanding your academic audit and the remaining requirements for graduation. The advisor can also refer students to appropriate resources such as the Science Student Success Centre, Learning Support Services and Writing Tutorial Services.

Academic Integrity violations within the Faculty of Science. Students found in violation of the Student Academic Integrity Policy (below) in Computer Science (COMP) courses are subject to severe penalties, as detailed at the Office of the Dean of Science (ODS) page: https://science.carleton.ca/academic-integrity. If you are unsure of the expectations regarding academic integrity (how to use and cite references, how much collaboration with lab- or class-mates is appropriate), ASK your Instructor or the head TA for your labs. Sharing assignment or quiz specifications or posting them online (to sites such as Chegg, CourseHero, OneClass) is considered academic misconduct. Students are never permitted to post, share, or upload course materials without explicit permission from your Instructor.

COMP 5900H addendum on integrity violations: An academic integrity violation in a graduate course may result in a course failure (F) or expulsion from the program. In student-submitted work in this course, both in written projects and online presentations, **no figures, diagrams or tables may be cut-and-pasted from any source**, unless written permission from the author of that material is obtained (and presented). Beyond any other standard university policies, in COMP 5900H any student submitting work including uncited text from someone else (or figures/tables as noted above), is subject to a mark of negative 100% on the entire work item. For example, if an item is worth 10%, the 10% is lost plus an additional 10% penalty, making the best possible course mark 80%. Both students may be penalized if the infraction involves copying from another student. Each student must write up submitted work individually from their own personal notes, unless given permission explicitly in writing to do otherwise by the Instructor.

=== Other University Policies (generic) ===

Requests for Academic Accommodation: You may need special arrangements to meet your academic obligations during the term. For an accommodation request, the processes are as follows.

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 site here

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, visit the Equity Services site here

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, see the PMC page.

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 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 here.

Student Academic Integrity Policy. Every student should be familiar with Carleton's 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. Examples of punishable offences include: plagiarism and unauthorized co-operation or collaboration. Information on this policy may be found at 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". For Computer Science courses, such reported offences will be reviewed by the Office of the Dean of Science (ODS).

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 course outline statement or the Instructor concerning this issue.

[end of policies]