

COMP 5900H (fall 2019; CSI-5138-IHO): Selected Topics in CS—Internet of Things (IoT) Security [E, T, S]

Last updated: Aug 23, 2019. Send comments to: paulv (insert @ here) scs.carleton.ca.

Course web site for updates: <http://people.scs.carleton.ca/~paulv/5900H.html>

Description. The course explores security-related aspects of the Internet of Things (IoT), and what can go wrong. Generally, the answer is: many of the same things that cause security problems in the ordinary Internet pre-IoT, but with broader implications. The focus is on consumer, personal and home IoT devices (rather than industrial applications or smart cities). The primary approach involves considering and analyzing the technical design of IoT components from a software and configuration perspective, rather than hardware specifically.

- Class times: 8:35-9:55, Mon+Wed (Sept.4 to Dec.4, 2019)
- Location: 1201 RB (River Building), Carleton University
- Instructor: Professor [P. Van Oorschot](#)
- Office hours (5173 HP): Mon 10:00-11:00am + Wed 12:00noon-1:00pm
- Prerequisites: Introductory courses in both operating systems (e.g., COMP 3000) and computer networks (e.g., COMP 3203), or equivalents. Otherwise requires instructor permission. An introductory course in computer and Internet security is helpful, but not mandatory. **Return [this confirmation of prerequisites to the instructor](#).**
- Course Text: None. In general, research papers used will be available online; some (e.g., those behind paywalls) may require electronic access via the university library. For security background and review, we will use: Computer Security and the Internet: Tools and Jewels (van Oorschot), Springer 2019.
- Outline of topics (preliminary): see [Detailed Topics](#) below.

Grading Scheme (dates are firm—please plan in advance):

- 10% Participation in discussions and attendance (mandatory, including student presentations)
- 10% Discussion lead (as of Sept.4, sign up for one lecture to lead discussion on; first-come first-served).
- 10% Project plan (due Oct.30 11:59pm, PDF by email; and Oct.21 deadline for email or in-person pre-discussion of project ideas with the instructor).
- 30% Term test (Nov.13, in class). Covers all material up to test date.
- 10% Project presentation in-class (Nov.25 - Dec.4).
- 30% Project written report (due Dec.9, 5:00pm, by email, PDF format). Late penalty: 10% per day, e.g., zero after 10 days.

Presentations. This is a graduate course involving "seminars". Students must actively participate in class discussions, and each must lead one class that covers the designated reading(s). As discussion leader, the student presents the main ideas of the reading(s), and is prepared with a list of items to discuss and questions, to facilitate class discussion. The **Participation** component of the grading scheme includes involvement in these discussions throughout the term (and thus naturally requires attendance). Aside from leading one class' discussions, each student will give an oral presentation related to their final project in classes beginning late November.

Class preparation and attendance. 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.

Intellectual Property and Copyrighted Material. All materials distributed as part of this course (including lecture content, notes, and 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 not be reposted, reproduced, forwarded or distributed without the written consent of the instructor. Violation is illegal and strictly prohibited.

References and Sources. Lectures will be drawn from research papers available online, plus material delivered in class; students are expected to attend all classes. No specific **access to computing labs** should be required, but labs in the Herzberg Building require a [Carleton University Campus Card](#), with access based on the courses you are registered in and the School's Lab Access Schedule.

cuLearn. Announcements, and some of the readings, will be distributed via the [cuLearn](#) course management system. Carleton students registered in this course should automatically have access to it; UofO students will need to fill out the form found [here](#), or otherwise check with a University of Ottawa administrator.

University Policies. See the bottom of this page.

Detailed Topics. Content listed below is subject to change, but representative of material we expect to cover. Specific sources will be finalized as the term progresses.

- Sept.4: **Select one class** (from Classes 4-20 below) to lead discussion on, by sending an email to the instructor; first-come first-served.

Class 1 (Sept 4): Security overview and principles.
Reference: Chapter 1 (Tools and Jewels).

Class 2 (Sept 9): IoT overview.
[Cyber-Physical Systems and Internet of Things](#) (Greer et al.) NIST Special Pub 1900-202, Mar 2019

Class 3 (Sept 11): How IoT differs from IoC (Internet of Computers).
[Analysis, implications and challenges of an evolving consumer IoT security landscape](#) (Bellman et al.) PST 2019
[RFC 7228: Terminology for Constrained-Node Networks](#) (Bormann et al.) IETF Editor

Class 4 (Sept 16): Botnets from IoT devices (Mirai).
Primary: [DDoS in the IoT: Mirai and Other Botnets](#) (Koliass et al.) IEEE Computer 50(7):80-84 2017.
Secondary: [Understanding the Mirai Botnet](#) (Antonakakis et al.) USENIX Security 2017

Class 5 (Sept 18): Home smart locks (and what goes wrong).
[Smart Locks: Lessons for Securing Commodity Internet of Things Devices](#) (Ho et al.) AsiaCCS 2016

Class 6 (Sept 23): Smart lightbulbs (and what goes wrong).
[IoT Goes Nuclear: Creating a ZigBee Chain Reaction](#) (Ronen et al.) Oakland 2017

Class 7 (Sept 25): Smart home systems (e.g., Samsung SmartThings) and what goes wrong.
[Security analysis of emerging smart home applications](#) (Fernandes et al.) Oakland 2016

Class 8 (Sept 30): Security analysis of IoT devices.
[SoK: Security Evaluation of Home-Based IoT Deployments](#) (Alrawi et al.) Oakland 2019

Class 9 (Oct 2): TAP (trigger-action programming) security issues.
[Analyzing the security and privacy risks of IFTTT recipes](#) (Surbatovich et al.) WWW 2017

Class 10 (Oct 7): 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 11 (Oct 9): Device lifecycle and transient device association.
Primary: [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.
Secondary: [IoT Security: An End-to-End View and Case Study](#) (Ling et al.) arXiv:1805.05853 version of GLOBECOM 2017

- Oct 14: no class, statutory holiday (Thanksgiving).

Class 12 (Oct 16): Device pairing: history and comparison.

[Ad-hoc key agreement: A brief history and the challenges ahead](#) (Miettinen et al.) Computer Commns 131 (2018) 32-34

[A comparative study of secure device pairing methods](#) (Kumar et al.) Pervasive and Mobile Computing 5(6):734-749, 2009

- Oct 21-25: no classes, fall break.

Class 13 (Oct 28): Embedded firmware and security.

[A large scale analysis of the security of embedded firmwares](#) (Costin et al.) USENIX Security 2014

- **Project proposal due: Oct 30** (11:59pm, by email, PDF document).

Class 14 (Oct 30): 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

Class 15 (Nov 4): Best practices.

[Best Current Practices for Securing Internet of Things \(IoT\) Devices](#) (Moore et al., July 2017) draft-moore-iot-security-bcp-01

and related documents.

Class 16 (Nov 6): Towards IoT search engines (Censys, Shodan).

[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 17 (Nov 11): Named Data Networking (an example of Information Centric Networking).

[Named Data Networking of Things](#) (Shang et al.) 2016 IEEE IoTDI, 117-128

Class 18 (Nov 13): **In-class term test.**

Class 19 (Nov 18): Device profiling with MUD files (manufacturer usage descriptions).

[Clear as MUD: generating, validating and applying IoT behavioral profiles](#) (Hamza et al.) 2018 ACM workshop on IoT Sec. and Priv; and [RFC 8520: Manufacturer Usage Description Specification](#)

Class 20 (Nov 20): IETF IoT-related standards.

A survey of the Internet Protocol suite for Internet of Things security (Tschofenig et al.) IEEE Security&Privacy (Sept/Oct 2019), 47-57

Classes 21-22 (Nov 25, 27): Student presentations.

Classes 23-24 (Dec 2, 4): Student presentations.

- **Final project due: Dec.9** (5:00pm, by email, PDF document).

=== University Policies (start) ===

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 co-operation or collaboration. Information on this policy may be found in the Undergraduate Calendar.

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.

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. COMP 5900H addendum: Beyond other university policies, any student submitting work including uncited portions originating from someone else, is subject to a mark of negative 100% on the entire work item. Thus if an assignment 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 unless explicitly allowed otherwise per instructions (e.g., in group-based assignments). For work that students may wish to eventually publish that is also submitted for grading in this course, including collaborative work with a supervisor, any part thereof must be submitted for grading prior to such collaborative input (i.e., must be the individual's own work), and must be distinct both from work already completed as part of another course, and from work completed as part of an in-progress thesis.

Academic Accommodations for Students with Disabilities. The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send your course instructor your Letter of Accommodation at the beginning of the term, and 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 course instructor to ensure accommodation arrangements are made. Please consult the PMC website for the deadline to request accommodations for the formally-scheduled exam (if applicable) at <http://www2.carleton.ca/pmc/new-and-current-students/dates-and-deadlines>

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. More information can be found [here](#).

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

Religious Obligation: Write to the course 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 software and system development. For more details visit the Equity Services website: <http://www2.carleton.ca/equity/>

Pregnancy Obligation: Write to the course 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://www2.carleton.ca/equity/>

Medical Certificate: The official medical certificate (form) accepted by Carleton University for the deferral of final examinations or assignments in undergraduate courses can be accessed from: <http://www.carleton.ca/registrar/forms>

=== University Policies (end) ===