
Last updated: Jan.4, 2017. Send comments to: paulv (insert @ here) scs.carleton.ca.

Course web site for updates: http://people.scs.carleton.ca/~paulv/5407jan2017.html

Calendar course description: Specialized topics in security including those selected from: 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.

Essential Course Details

- **Class times:** 2:35-3:55, Tues+Thurs (Jan.5 to Apr.6, 2017)
- **Location:** UC 280 (University Centre), Carleton University
- **Instructor:** Professor P. Van Oorschot
- **Office hours:** Mon+Wed 3:00-4:00pm, 5173HP
- **Prerequisites:** COMP 4108 (computer systems security) + COMP 3000 (operating systems), or equivalents. Otherwise requires instructor permission.
- **Course Text:** None.
- **Course Outline (preliminary):** click here for outline, and see also Detailed Topics below.
- **Marking Scheme** (dates are firm - please plan in advance):
  30% Project 1 (Software Vulnerability Tracking; click here for more details) --- Start immediately (first day of class), hard-copy due Thurs. Feb.9 in class.
  30% Midterm test: Tues. Mar.7 (in class); covers all material up to test date.
  40% Project 2 and participation (Research Paper; click here for more details)
  = (10% in-class presentation + 5% participation/attendance of other presentations + 25% written report, hard-copy due in class Thurs. Apr.6)

**References and Sources.** Lectures will largely be drawn from research papers (generally available online), and supplementary material given in class; students are thus expected to attend all classes. For those wishing to brush up on background reading, recommendations include Stallings and Brown (2014) and Gollman (2011) among others found on this list. 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.

**University Policies.** See the bottom of this page.

**Detailed Topics.** Topics are updated each year. A preliminary plan for this year is below (these are representative and will be updated as the term progresses). Notation for background references: "HAC ssN" denotes section N in Handbook of Applied Cryptography, which is available free online; tbd = to be determined.

- **Class 1 (Jan.5):** Security metrics for guessing passwords. Testing Metrics for Password Creation Policies, Weir et al. (ACM CCS 2010 - also here); and Metrics for guessing difficulty, Bonneau (Ch.3 in: Guessing Human-chosen Secrets, PhD thesis, Cambridge, 2012). Begin Project 1 immediately. Advanced reading: The science of guessing: analyzing an anonymized corpus of 70 million passwords, Bonneau (Oakland 2012).


- Class 3 (Jan.12): Off-line dictionary attacks and verifiable text. Protecting Poorly Chosen Secrets from Guessing Attacks, Gong et al. (IEEE JSAC vol.11 no.5 June 1993). Background review: passwords (HAC ss10.2.1-10.2.2), time variant parameters (HAC ss10.3.1).


- Classes 9-12 (Feb.2 7, 9, 14): TLS/SSL infrastructure and certificate-based authentication; MITM, browser trust model; TLS and CDNs. Project 1 is due in class (hard copy) Feb.9. The Inconvenient Truth about Web Certificates, Vratonjic et al. (WEIS 2011); SSL and HTTPS: Revisiting past challenges and evaluating certificate trust model enhancements (omit section III), Clark et al. (IEEE Oakland, 2013); Upgrading HTTPS in Mid-Air (sections I-III), Kranch & Bonneau (NDSS2015); Certificate Transparency, Laurie (CACM Oct.2014) and Google's certificate transparency project site (supplementary/optional: IETF RFC 6962). Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem, Cangialosi et al. (ACM CCS 2016) and Bruce Maggs' related invited talk on CDN's (USENIX Security 2016); When HTTPS meets CDN: A Case of Authentication in Delegated Service, Liang et al. (IEEE Oakland 2014). Background review (optional): certificate infrastructure and trust models (HAC, pp.559-560; 572-581) and implementation issues, RSA signatures (pp.433-434). Supplementary (optional): Convergence Project and issues with SSL infrastructure - 48-minute video; SSL and the Future of Authenticity, Marlinspike (BlackHat USA 2011);


- Feb.20-24: No classes (winter reading week).

Project 2 (see above) topic proposal due: Feb.27.


- Class 16 (Mar.7): Test (in class).

- Class 17 (Mar.9): Intel SGX (Software Guard Extensions).

- Classes 18-23 (Mar.14-30): student presentations related to Project 2, about 30 minutes each. See details above. It is strongly recommended that topics selected are based on 2014-2016 papers presented at the big-four security conferences (NDSS, IEEE Symp. Security & Privacy, USENIX Security, ACM CCS).


Supplementary background on drive-by downloads and browser security. The Ghost in the Browser (Provos et al., USENIX HotBots'07) and All Your iFRAMEs Point to Us (Provos et al., USENIX Security 2008). Cybercrime 2.0: When the Cloud Turns Dark (Provos et al., C.ACM 52(4):42-47, 2009).

Supplementary background on SOP (same-origin policy), XSS attacks: Cross-site Scripting Worms and Viruses, Grossman (white paper, updated June 2007); Browser security handbook, Michal Zalewski (2008, 2009 online resource); Same-Origin Mutual Approval: Mutual Approval for Included Content in Web Pages, Oda et al. (ACM CCS 2008).

Supplementary background on malware, malware networks, rootkits. The History and Evolution of Computer Viruses (Mikko Hypponen, 49min, DEFCON 2011 talk). W32.Stuxnet Dossier (v1.4, Feb.2011, Symantec report by N. Falliere, Liam O Murchu, E. Chien). The Spread of the Sapphire/Slammer Worm (Feb.2003), Moore et al. (or version in S&P magazine);


=== 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 4108 addendum: Beyond any other standard 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. For example, 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 official instructions (e.g., in group-based assignments).

**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
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) ===