COMP 4108 B (January 2017): Computer Systems Security

Preliminary course outline, subject to change (other course outlines); last updated January 4, 2017. Course website (for updates): http://people.scs.carleton.ca/~paulv/4108jan2017.html

Course description (from official calendar): Introduction to information security in computer and communications systems, including network, operating systems, web and software security. Passwords, authentication applications, privacy, data integrity, anonymity, secure email, IP security, security infrastructures, firewalls, viruses, intrusion detection, network attacks. Lectures three hours a week. Prerequisites: one of COMP 3203 (Principles of Computer Networks) or SYSC 4602 (Computer Communications); and one of COMP 3000 (Operating Systems), SYSC 3001 (Operating Systems and Databases), SYSC 4001 (Operating Systems). Otherwise requires written instructor permission.

Instructor: P. Van Oorschot (Office Hrs: MW 3:00-4:00pm, 5173HP) TA: Furkan Alaca (Office Hrs: MW 1:00-2:00pm, CSTAC room (HP tunnel level) Lectures 4:00-5:30pm Mon+W ed 515SA (Southam Hall, Carleton) 2017 term: Jan.5-Apr.7, excluding Feb.20-24 (winter break).

Textbook: None. Students are responsible for material covered in class. Written notes for selected parts will be available. Students seeking supplementary resources may consider books listed on this page, the most relevant being those under the heading "Computer security, operating system security". Free online, and particularly recommended for its early insights on building secure systems, is Gasser (1988); see also Ch.11 of Saltzer and Kaashoek (2009).

Evaluation:
30%: Test 1 (Feb.8, in class).
30%: Test 2 (Mar.22, in class).
5%: Reading Responses (2) - see explanation below, due Mar.29 and Apr.3.
35%: Five (5) lab assignments, 7% each. Lab#1 is individual basis, #2-5 optionally in groups of 2. Students should regularly check the COMP4108 lab page for details and due dates for these programming-based assignments. Preliminary lab dates (to be confirmed by TA): Labs 1-5 available/due on: Jan.11/Jan.30, Jan.30/Feb.15, Feb.15/Mar.1, Mar.1/Mar.15, Mar.15/Apr.5.

Lab Access: Lab assignments should be possible by remote access using generic computing equipment. Students will need an OpenStack account if they do not already have one from a previous course; consult the lab page (see above) for further details. For password-protected portions of course content on the web, the lab page will indicate whether you need to get an access password by such means as individual email or that will be provided in class.

Explanation of Reading Responses. For each specified paper, a one-page hard-copy critique must be handed it at the start of the specified class (see the last two weeks in the outline below), followed by class discussion of the paper. The response is to include a 2-3 sentence overview of the paper rephrased in your own words, plus three brief criticisms of the reading (perceived shortcomings, points you disagree with, or suggestions for improvement). Support your criticisms as best possible within the available space.

Course objectives: to understand fundamental principles of computer security; to become aware of factors enabling computer systems to be exploited by attackers and corresponding protection means; to understand practical threats and carry out simple security analysis useful in software and system development; to gain familiarity with basic concepts in operating systems and Internet security.

Attendance and Additional Information. Course content will be presented in class and selectively supplemented by additional written material from the instructor; reading responses also require participation in the class. Students are thus expected to attend all classes, and are responsible for all items discussed in class.
Topics Outline (preliminary). Topics will be noted on the course website as the term progresses, updated on an ongoing basis.

- Classes 1-4 (Introduction): computer security goals, definitions, policies; risk assessment and modeling; adversary models, threat models, security analysis and attack trees; security design principles.
- Classes 5-6 (Protection in operating systems): memory protection, privileged mode and setuid; reference monitor, mediation and object-based access control; protection rings and isolation domains. Role-based access control.
- Classes 7-9 (Code injection and OS exploits): memory overflows, exploiting OS calls and libraries, SQL injection, privilege escalation, race conditions. Defenses.
- Class 10 (Wed. Feb.8): in-class test (30%)
- Classes 11-12 (Malicious software): viruses, worms, rootkits, botnets, ransomware.
- ---Feb.20-24---: no classes (winter break)
- Classes 13-14 (Network threats): scanning and auto-rooters; DDoS; DNS exploits.
- Classes 15-16 (Network-based defenses): firewalls, gateways, perimeter security; network intrusion detection; SSH/SCP; VPNs, IPsec and tunnelling.
- Classes 17-19 (Browser/web security): SSL & https, certificates/chains/authorities, trust models; certificate pinning and transparency; DOM, http cookies, same-origin policy, active content, malicious tags, scripts, XSS, CSRF. Phishing, UI issues.
- Class 20 (Wed. Mar.22): in-class test (30%)

Send comments to: paulv (insert @ here) scs.carleton.ca.

=== 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 http://www2.carleton.ca PMC/new-and-current-students/dates-and-deadlines

**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 exist. 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) ===