COMP 5407W (Winter 2018): Authentication and Software Security [A, S]

Last updated: Dec.31, 2017. Send comments to: paulv (insert @ here) scs.carleton.ca.

Course web site for updates: http://people.scs.carleton.ca/~paulv/5407jan2018.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.8 to Apr.11, 2018)
- *Location:* SA 615 (Southam Hall), Carleton University
- *Instructor:* Professor P. Van Oorschot
- *Office hours:* Wed (3:30-4:30pm), Thurs (4:00-5:00pm), 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 Tues. Feb.13 in class.
  30% Midterm test: Thurs. Mar.8 (in class); covers all material up to test date.
  40% Project 2 and participation (Research Paper, proposal due Feb.28; click here for more details)
  = (10% in-class presentation + 5% participation/attendance of other presentations + 25% written report, hard-copy due in class Tues. Apr.10)

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.

- *Classes 1-2 (Jan.9, 11):* **Begin Project 1 immediately** (see above).

Introduction to password literarture. An Administrator's Guide to Internet Password Research, Florencio et al. (USENIX LISA, 2014).

- *Classes 3-4 (Jan.16, 18): Strong Password-Protocols*. EKE: Password-Based Protocols Secure Against Dictionary Attack, Bellovin and Merritt (IEEE S&P 1992). Strong Password-Only Authenticated Key Exchange, D. Jablon (ACM Computer Communcations Review, Oct.1996); Extended Password Key Exchange Protocols Immune to Dictionary Attack, D. Jablon (WET-ICE 1997); The Secure Remote Password Protocol, T. Wu (NDSS 1998). Optional/supplementary (attacks on EKE): Number Theoretic Attacks on Secure Password Schemes, S. Patel (IEEE S&P 1997).

Classes 5-6 (Jan.23, 25): Alternatives for web user authentication. The Quest to Replace Passwords, Bonneau et al. (IEEE Oakland, 2012).

- *Classes 7-8 (Jan.30, Feb.1): Public-key certificates and public-key infrastructure (PKI)*. Class notes. See also (supplementary review): certificate infrastructure and trust models (HAC, pp.559-560; 572-581) and implementation issues, RSA signatures (pp.433-434).

- *Classes 9-10 (Feb.6, 8): Empirical studies of TLS/HTTPS and certificate issues in practice*. The Inconvenient Truth about Web Certificates, Vratonjic et al. (WEIS 2011). Analysis of the HTTPS Certificate Ecosystem, Durumeric et al. (IMC 2013). Security Collapse in the HTTPS Market, Arnbak et al, C.ACM 57(10)47-55, Oct.2014. Supplementary: longer paper by Arnbak et al., Security economics in the HTTPS Value Chain, WEIS 2013; and Marlinspike (BlackHat USA 2011) 48-minute video on "SSL and the Future of Authenticity (Convergence Project)".

- *Classes 11-12 (Feb.13, 15):* **Project 1 is due in class Feb.13 (hard copy).**
HTTPS infrastructure study and browser trust model upgrades. 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 IETF RFC 6962 (Certificate Transparency); see also Google's certificate transparency project site.

- *Feb.19-23: No classes (winter reading week).*

- *Class 13-14 (Feb.27, Mar.1):* **Project 2 topic proposal due: Feb.28.**
More TLS: Heartbleed, and (ab)use by CDNs and web hosting providers. The Matter of Heartbleed (Durumeric et al., IMC'14). When HTTPS meets CDN: A Case of Authentication in Delegated Service, Liang et al. (IEEE Oakland 2014). Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem, Cangialosi et al. (ACM CCS 2016). Supplementary: Bruce Maggs' invited talk on CDN's (USENIX Security 2016).

- *Classes 15 (Mar.6): Web PKI proposals*. J. Yu, Mark Ryan, "Evaluating Web PKIs", Chapter 7 in *Software Architectures for Big Data and the Cloud* (2017). Melara et al., "CONIKS: Bringing Key Transparency to End Users", USENIX Security 2015.

- *Class 16 (Mar.8):* **Term Test** (in class).

- *Classes 17-18 (Mar.13, 15): Secure email and support infrastructure*. S/MIME, PGP, history of PEM. Supplementary: "Enhanced certificate transparency and end-to-end encrypted email" (Mark Ryan, NDSS 2014); TLS infrastructure measurement studies on TLS, secure email.

- *Classes 19-24 (Mar.20-Apr.5): student presentations (Project 2, see above). Plan 30 minutes each (40 minutes max)*. It is strongly recommended that topics selected are based on papers presented at the big-four security conferrences during 2015-2017 (IEEE Symp. Security & Privacy, ACM CCS, USENIX Security, ISOC NDSS).

Class 19 (Mar.20): student1:topic1; student2:topic2.
Class 20 (Mar.22):
Class 21 (Mar.27):
Class 22 (Mar.29):
Class 23 (Apr.3):
Class 24 (Apr.5):

- *Class 25 (Apr.10):* **Project 2 final written report: hard copy due at start of class.**
Potential topic for last class: Secure OSs, mandatory access control (MAC), trusted computing. The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments, Loscocco et al. (NISSC

1998). Supplementary: the previous paper motivates SELinux and trusted computing. Flask microkernel-based OS: The Flask Security Architecture: System Support for Diverse Security Policies, Spencer et al. (USENIX Security 1999). SELinux: Integrating Flexible Support for Security Policies into the Linux Operating System, Loscocco & Smalley (FREENIX/USENIX Annual, 2001; 62-page extended version also available). Linux Security Modules: General Security Support for the Linux Kernel, Wright et al. (USENIX Security 2002). Bootstrapping Trust in Commodity Computers, Parno et al. (IEEE Oakland 2010; optionally see also extended book version). Intel SGX (Software Guard Extensions).

=== 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 software and system developmest. 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) ===