Network Security and Cryptography

CSI5105 / COMP5406, ELG7178D / EACJ5606
Winter, 2019

Professor: Carlisle Adams (SITE, Office 5035, office hours by appointment)
Correctors: Maryam Hezaveh (MHEZA028@uottawa.ca)
Salauddin Ali Ahmed (salia023@uottawa.ca)

Calendar Description
Advanced methodologies selected from symmetric and public key cryptography, network security protocols and infrastructures, identification, secret sharing, anonymity, intrusion detection, firewalls, defending network attacks, and performance in communication networks.

Course Outline (tentative)

Network Security Tools and Techniques
Weeks 1-3 Cryptography, Authentication, Security Infrastructures and Protocols
Categorization of Attacks and Defenses

Foundations of Modern Security: technologies for access control in network environments
Weeks 4-6 Introduction and motivation; architecture (components and interactions)
Engineering considerations (authentication, delegation, revocation, efficiency);
CORBA, X.509 Attribute Certificates; modern technologies for access control

Foundations of Modern Privacy: technologies for private network interactions
Weeks 8-11 Introduction and motivation; anonymity, pseudonymity, veronymity
Real-world privacy concerns; privacy enhancing technologies (PETs)
MIX networks, onion routing; privacy policies (P3P); privacy enforcement
Some example PETs: PIR, privacy certificates, others (as time permits)

Student presentations
Weeks 12-13 Student project presentations
Textbooks (suggested readings, as needed, to obtain relevant concepts and background)


B. Blakley, CORBA *Security: An Introduction to Safe Computing with Objects*, Addison-Wesley, 2000


Papers (required reading)

Selected research papers & technical specifications (will be itemized in class)

**Grading Scheme**

Assignments (4) 20%
Midterm (February 14th) 20%
Written Report or Oral Presentation 20%
Final Examination 40%
Assignments

- For each assignment, the student must submit a two-page summary (single-spaced, using 12-pt font) of a paper from a specified set of research papers. The summary must include the main results of the paper, along with a brief discussion (two paragraphs) of why the student feels these results are interesting / important.
  
  - The description of the main results must not be a copy of the paper’s abstract (i.e., it must be clear that the paper has been read and understood).
  - Persuasive reasons must be given for why the paper is interesting/important.

- Due on Thursdays at 14:00 for weeks 3, 4, 5, 8 (i.e., beginning Jan. 24th).

Report and Presentation

- Must be in the area of Privacy Enhancing Technologies.

- Choose a research paper from a specified list of academic research conferences and journals (the list will be provided by the instructor).

- The instructor will select a subset of projects to be presented orally; the remainder will be presented in a written report.

- Both the written report and the oral presentation must include sufficient background (problem description, survey of important previous results) for a reader/listener who is familiar with security and privacy, but not an expert in the presented topic.

- Formal Oral Presentation: Present an extended abstract of the paper, highlighting the main results and giving a critique explaining to the audience why they should (or should not!) read this paper. The presentation must be given in one of the last 2 weeks of the course; a schedule will be provided.

- Formal Written Report: Provide a description of the research result(s) achieved in this paper, present a critique of the paper, and propose your own direction for improvement / enhancement of this work (i.e., what direction would you take if you wanted to publish something based on this paper?). The report is due on Thursday, April 4th.


- Topic must be approved by Monday, March 11th
  
  - Note that each student may not get his/her preferred topic. (Submit your request as early as possible in order to increase the chances of getting your choice.)
General Policies and Procedures

Plagiarism and Academic Integrity
- Will not be tolerated in any aspect of this course:
  - Zero percent for work in which cheating is detected;
  - Other penalties (including course failure and expulsion) are also possible.

Academic Fraud
- see the following link for important information:
  http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_ENG.htm or
  http://www.uottawa.ca/academic/info/regist/crs/0305/home_5_FR.htm

Course Policies
- Zero percent for late work.
- In a graduate course, it is unreasonable to expect that all testable material will be covered in class. Make use of the recommended textbooks and any other suggested sources to aid understanding of the material.
- Electronic devices are not to be used in class without explicit permission from the instructor.

Faculty of Engineering Rules and Regulations
- https://www.uottawa.ca/administration-and-governance/policies-and-regulations or
  https://www.uottawa.ca/administration-et-gouvernance/politiques-et-reglements

University of Ottawa Academic Regulations
- Class attendance is mandatory. As per academic regulations, students who do not attend at least 80% of the classes may not be allowed to write the final examination.
- Students must be registered in order to take the class. Students who are not officially registered cannot receive a mark.
- All components of the course (i.e., assignments, written report, presentation, exam) must be fulfilled otherwise students may receive an INC as a final mark (equivalent to an F). This also holds for students taking the course for the second time.

Important dates:  http://www.registrar.uottawa.ca/Default.aspx?tabid=2671 or

Students must pass the exam component (i.e., obtain a mark of 30/60 or higher) in order to receive a passing grade on the course.