CSI 4139 / CEG 4399
Design of Secure Computer Systems

Outline (Fall 2018)

| Lectures:         | Tuesday  | 8:30 to 10:00  |
|                  | Friday   | 10:00 to 11:30 |
|                  |          | MRT 212        |
|                  |          | MRT 212        |
| Laboratory:      | Tuesday  | 14:30 to 17:30 |
|                  | Thursday | 16:00 to 19:00 |
|                  |          | CBY B02        |
|                  |          | STE 2060       |
| Tutorial         | Thursday | 14:30 to 16:00 |
|                  |          | 14:30 to 16:00 |
|                  |          | MRT 256        |
|                  |          | TBT 0019       |
| Office Hours:    | By appointment | By appointment |
|                  |          | SITE 5035      |

Teaching assistants: Arthur So (ASO012@uottawa.ca),
Maryam Hezaveh (MHEZA028@uottawa.ca)

Course description (from calendar):

Prerequisites: CEG 3185 Introduction to Data Communications and Networking

General objective for course: to present a broad overview of computer security.

Specific objectives: students should learn some of the design objectives and tools available for securing computer systems. By the end of the course, students should have a good understanding of the strengths & limitations of various techniques, how they work, and how well they achieve the intended security.

Teaching methods: in-class lectures (mostly at the board) with some topic outlines and other materials made available electronically via the course website (http://www.site.uottawa.ca/~cadams/courses/CSI4139.html).
Textbooks


Reference books:
Matt Bishop, Introduction to Computer Security, Addison-Wesley, 2005

Grading Scheme

Assignments and labs [to be submitted electronically]: 32%
  Assignment 1 (due September 28, before 16:00) 5%
  Assignment 2 (due November 16, before 16:00) 5%
  Lab 1 code (due September 20, before 19:00) 4%
  Lab 2 code (due October 4, before 19:00) 4%
  Lab 3 code (due November 8, before 19:00) 4%
  Lab 4 code (due November 22, before 19:00) 6%
  Lab 5 code (due November 29, before 19:00) 4%
Midterm examination (October 19): 20%
Final examination: 50%

(Lab reports will be due at 16:00 on the Monday (Tue. for Lab 2) after the code is due.)
(Assignment #2 may be replaced by an in-class presentation, upon request and approval.)
General Policies and Procedures

Plagiarism and Academic Integrity
- 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 4th-year course, it is unreasonable to expect that all testable material will be covered in class (real life is not like this!). Make use of the suggested textbooks and any other relevant material.
- Electronic devices are not to be used in class without explicit permission from the instructor.

University of Ottawa Academic Regulations
- https://www.uottawa.ca/administration-and-governance/policies-and-regulations or
- https://www.uottawa.ca/administration-et-gouvernance/politiques-et-reglements

Specific 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, exams) must be fulfilled otherwise students may receive an INC as a final mark (equivalent to an F). This also holds for students taking a course for the second time.

Detailed Outline (Tentative)

Week

Introduction [Ch. 1]
1: overview of secure computer systems

User Security [Ch. 3]
2: passwords, identity, biometrics, authentication

Fundamental Security Tools [Ch. 2, 4, 5, 12]
3 – 6: cryptography, security policies, access control, DB sec, OS sec

Midterm (October 19)

Attacks & Defenses [Ch. 6 – 9]
8-10: malicious software, DoS, intrusion detection, firewalls

Software Security & Trusted Systems [Ch. 10, 11, 13]
11 – 12: buffer overflow, program security, trusted computing

Network Security [Ch. 22 – 24]
13: additional topics in security (as time permits)

Semester Review
Dec. 4: review of course material

Dec. 8-21 Fall semester final examinations
(specific exam date to be determined)