Instructor

Dr. Jason Jaskolka
Office: Canal Building 6206
Extension: 1873
Email: jaskolka@sce.carleton.ca

TAs

TBD and posted on cuLearn

Office Hours

TBD and posted on cuLearn

Course Objectives

Concerns related to the security of modern computer systems and networks, and the information that they use, store, and communicate, are becoming more commonplace in our daily lives. Systems today are comprised of broad and heterogeneous communication networks with many interacting software and hardware components that can be spread across a variety of application domains, each with their own security concerns with varying implications and priorities. For example, smartphones, wearable health-monitoring devices, GPS navigation devices, automobiles, energy grid services, and even home appliances like washers and dryers now come with Internet connections by which data from and about the user goes to places where users have little visibility or control. On one hand, users want the convenience and benefits that added connectivity brings, while on the other hand, they are growing increasingly worried about the threat and impact of suffering massive losses of their personal data and information. Computer security brings these two threads together as technology races forward with “smart” products that all too often omit the basic controls that can prevent or limit security attacks and failures.

This course examines the fundamentals of network and software security, and explores the central problems that confront security designers and administrators including defining the threats to computer and network systems, evaluating the relative risks of these threats, and developing effective countermeasures and controls. The course is intended to cover a broad spectrum of network and software security fundamentals, while striking a balance between theory and practice. It will provide students with the foundation and skills needed to become security-conscious engineers.
Learning Outcomes

Upon completion of this course, students should know and understand:

1. the fundamental concepts, terminologies, principles, and theories of network and software security;
2. the primary aspects of a comprehensive security strategy;
3. the basic principles underlying the main cryptographic concepts and technologies available today, including symmetric and asymmetric encryption, hashing, and digital signatures;
4. security policies (such as authentication, integrity, and confidentiality), as well as protocols to implement such policies;
5. the various types of security threats and attacks on networks and software systems, how they work, and controls for dealing with them;
6. the relevant personnel, legal, and ethical issues related of network and software security.

Upon completion of this course, students should be able to:

1. identify the types of threats and attacks that apply to different categories of computer and network assets;
2. identify suitable countermeasures and security controls for dealing with specific types of threats and attacks;
3. analyze and specify security properties of simple computing systems;
4. implement and use basic security tools to enhance network and software security;
5. develop basic security enhancements in stand-alone applications.

Graduate Attributes

- Computer Systems, Software Engineering, Communication Networks
- 2.1 Problem clarification, definition and approach, including dealing with ill-defined problems
- 2.2 Assumptions
- 4.1 Clear design goals (See 11.1)
- 4.2 Detailed design specifications and requirements (See 11.1)
- 4.5 Design implementation / Task(s) definition
- 4.7 Evaluation based on engineering principles
- 10.2 Professional, accountable and ethical conduct (See 8.1, 8.2)

Course Web Site

The course announcements, course syllabus, lecture slides used in class, assignments, and any material needed or used in the problem analysis sessions, can be found on cuLearn. It is the student’s responsibility to be aware of the information on cuLearn, and to check regularly for announcements.
Textbook and References

The following textbook is strongly recommended and is available at the Carleton bookstore.


*Note:* *This course may not always follow the textbook closely.*

Additional References & Resources

Throughout this course, the following useful references and resources may also be used:


Evaluation and Marking Scheme

**Problem Analysis (0%)**

There will be a weekly problem analysis session involving a short ungraded assignment with practice and study questions that are intended to check your understanding of the course material. The problem analysis assignments will be posted on cuLearn one week prior to the problem analysis session in which the solutions will be taken up and discussed. Students are warned that the solutions to the problem analysis assignments will not be posted on cuLearn. The problem analysis assignments form a very important part of this course and your attendance and participation at the problem analysis sessions is expected. Doing the problem analysis assignments (by yourself) and asking questions during the problem analysis sessions is an excellent way for you to learn the course material and prepare for the midterm and final examinations.

**Assignments (30%)**

There will be three (3) assignments. Each assignment is worth 10% of the final grade. Assignments will be posted on cuLearn and will be due on the following dates:

<table>
<thead>
<tr>
<th>Assignment #</th>
<th>Posted Date</th>
<th>Due Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>September 7, 2018</td>
<td>October 5, 2018</td>
</tr>
<tr>
<td>2</td>
<td>October 5, 2018</td>
<td>November 2, 2018</td>
</tr>
<tr>
<td>3</td>
<td>November 2, 2018</td>
<td>November 30, 2018</td>
</tr>
</tbody>
</table>
The assignment solutions are due by 8:00PM on the due date. Students must submit their assignment solutions on cuLearn. Students are permitted to discuss general aspects of the assignments with other students in the class, but each person should hand in their own work. Students may consult outside sources, such as textbooks, but any use of any source must be documented/cited in the assignment solutions. Late assignments will be graded with a late penalty of 20% of the full grade per day except for reasons accepted by the Associate Dean’s Office (see Academic Regulations of the University, Section 2.6., Deferred Term Work).

The assignments will be graded by the TAs. Any request for regrading must be first directed to the TA that has graded your assignment. If after having talked to the TA you still believe that you deserve a higher grade, then you can contact the instructor. When the instructor regrades an assignment, all of the assignment solutions will be regraded.

**Surprise Quizzes (0-5%)**
During the lectures, the instructor can give a surprise five to ten minute quiz. There will be up to six (6) surprise quizzes. If the class writes one quiz during the term, it counts for 1% of the final grade. If the class writes more than one quiz, the quiz with the lowest grade does not count, while each of the others count for 1% of the final grade.

**Midterm Exam (15%)**
There will be one (1) midterm examination. It will be a closed book examination. The midterm exam is worth 15% of the final grade and will take place on Friday, October 12, 2018, from 2:35PM–3:55PM (during the lecture time). The location of the midterm exam will be announced on cuLearn in due time. The midterm exam will cover the material from the lectures, problem analyses, assignments, and the required textbook.

**Final Exam (50-55%)**
The final examination will be scheduled by the Registrar’s office in the usual way. It will be three (3) hours in duration and will cover the material from the lectures, labs, assignments, and the required textbook. The final exam counts for (55 – #QuizzesThatCount)% of the final grade. For example, if the class writes 4 quizzes, only 3 quizzes count and the final exam will be worth (55 – 3) = 52%. The final examination is for evaluation purposes only and will not be returned to students. You will be able to make arrangements with the instructor or with the department office to see your marked final examination after the final grades have been made available.

**General Regulations**

**Instructor Expectations, Policies, and Notes**

1. **Deferred Term Work**: As stated in the Academic Regulations of the University, students who claim illness, injury, or other extraordinary circumstances beyond their control as a reason for missed term work are responsible for immediately informing the instructor and for making alternate arrangements with the instructor. This must occur no later than three (3) working days after the term work was due. The alternate arrangement must be made before the last day of classes in the term as published in the academic schedule. For more information, see the Academic Regulations of the University, Section 2.6, Deferred Term Work.

2. **Attendance**: Students are expected to attend all lectures and lab periods. The University requires students to have a conflict-free timetable. For more information, see the current Undergraduate Calendar, Academic Regulations of the University, Section 1.2, Course Selection
and Registration and Section 1.5, Deregistration. Requests to accommodate a missed midterm exam, lab periods, etc., because of conflicts with jobs or vacation plans will not be considered.

3. **Appeal of Grades:** The processes for dealing with questions or concerns regarding grades assigned during the term and final grades is described in the Academic Regulations of the University, Section 2.7, Informal Appeal of Grade and Section 2.8, Formal Appeal of Grade. A regrading request of an assignment, quiz, or exam will be considered by the TAs and the instructor only if it is made within the **two weeks that follow the return date of the majority of the concerned assignment, quiz, or exam.**

4. The instructor reserves the right to assign extra grades for extra work done by willing students. However, the work subject to extra grades will be advertised during the lectures to provide the opportunity to all students.

5. No responsibility for loss of assignments can be assumed by either the instructor or the TAs. **Keep copies of your own assignments.**

6. Students are responsible for ensuring that their assignments are submitted correctly and without corruption.

7. The lectures will not necessarily follow the order in which the topics are presented in the detailed course outline. Regular class attendance is required.

8. Significant study, reading, and group discussions outside of class are required. Looking at, or only reading the slides that are provided may not be enough to achieve the level of understanding required for the assignments and exams.

9. Students are expected to show professional behaviour. This includes being on-time for lecture and problem analysis sessions, meeting assignment deadlines, and maintaining a suitable level of professionalism in oral and written (email) correspondence with the instructor and TAs.

10. Students that are having difficulty with the course content are expected to seek help early. Students are encouraged to ask questions in class and/or seek help during the instructor’s office hours.

11. **Suggestions on how to improve the course and the instructor’s teaching methods are always welcomed.**

**Requests for Academic Accommodation**

You may need special arrangements to meet your academic obligations during the term. For an accommodation request the processes are as follows:

- **Pregnancy Obligation:** Please contact your 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: carleton.ca/equity/wp-content/uploads/Student-Guide-to-Academic-Accommodation.pdf

- **Religious Obligation:** Please contact your 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.

- **Academic Accommodations for Students with Disabilities:** If you have a documented disability requiring academic accommodations in this course, please contact the Paul Menton Centre for Students with Disabilities (PMC) at 613-520-6608 or pmc@carleton.ca for a formal evaluation or contact your PMC coordinator to send your instructor your Letter of Accommodation at the beginning of the term. You must also contact the PMC 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 instructor as soon as possible to ensure accommodation arrangements are made. carleton.ca/pmc

- **Survivors of Sexual Violence:** As a community, Carleton University is committed to maintaining a positive learning, working and living environment where sexual violence will not be tolerated, and is survivors are supported through academic accommodations as per
Carleton’s Sexual Violence Policy. For more information about the services available at the university and to obtain information about sexual violence and/or support, visit: carleton.ca/sexual-violence-support

- **Accommodation for Student Activities**: Carleton University recognizes the substantial benefits, both to the individual student and for the university, that result from a student participating in activities beyond the classroom experience. Reasonable accommodation must be provided to students who compete or perform at the national or international level. Please contact your 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. https://carleton.ca/senate/wp-content/uploads/Accommodation-for-Student-Activities-1.pdf

For more information on academic accommodation, please contact the departmental administrator or visit: https://students.carleton.ca/course-outline/

**Academic Integrity & Plagiarism**
Students are reminded that they should read and comply with Carleton University’s Academic Integrity Policy. Students should be aware of their obligations with regards to academic integrity. Academic dishonesty, in any form, is a serious instructional offence and will not be tolerated. It is the student’s responsibility to understand what constitutes academic dishonesty (refer to Section VI “Academic Integrity Standards” of the Academic Integrity Policy). Students who infringe the Policy may be subjected to one of several penalties including: expulsion; suspension from all studies at Carleton University; suspension from full-time studies; and/or a reprimand; a refusal of permission to continue or to register in a specific degree program; academic probation; or a grade of Failure in the course.

**Health & Safety**
Every student should have a copy of the Health and Safety Manual. Students are reminded to consult the Health and Safety Manual (http://sce.carleton.ca/courses/health-and-safety.pdf) should they, at any time have any questions or concerns regarding Health and Safety.

**Copyright on Course Materials**
The materials created for this course (including course outline, slides, posted notes, labs, project, assignments, quizzes, exams and solutions) are intended for personal use and may not be reproduced or redistributed or posted on any web site without prior written permission from the author(s).

**Additional Information**

**Email Correspondence**
In order to ensure that you receive a timely response to emails that are sent to the instructor or TAs, please include [SYSC 4810] in the Subject, as emails will be filtered using this identifier.

Students are expected to show and maintain a high-level of professionalism in all email correspondence. This means that emails should include a proper salutation and sign-off/signature, and should refrain from using slang, texting abbreviations and acronyms, and emojis/emojicons.

Note that email is not the best medium for technical questions. Technical questions submitted by email will be answered at the beginning of the next lecture.
Tentative Week-By-Week Schedule

Note that this course outline is subject to change as circumstances dictate.

- **Part I: Overview of Network and Software Security**
  - Security Concepts: Confidentiality, Integrity, Availability, Threats, Attacks, Assets
  - Fundamental Security Design Principles
  - Attack Surfaces and Attack Trees
  - Security Strategies, Policies, and Implementations: Prevention, Detection, Recovery

- **Part II: Computer Security Technology and Principles**
  - Cryptography: Algorithms, Symmetric vs. Asymmetric, Hashing, Digital Signatures, Key Management
  - User Authentication: Passwords, Tokens, Biometrics
  - Access Control Principles: Subjects, Objects, Access Rights, Role-Based vs. Attribute-Based
  - Trusted Computing and Multilevel Security
  - Malicious Software: Viruses, Worms, Trojans, Bots, Spam, Phishing, Backdoors, Rootkits
  - Intrusion Detection, Firewalls, and Intrusion Prevention Systems

- **Part III: Network Security**
  - Internet Security Protocols and Standards: SSL, TLS, HTTPS, IPSec
  - Internet Authentication Applications: Kerberos, Certificates, Public-Key Infrastructure
  - Wireless Network Security and Mobile Device Security

- **Part IV: Software and System Security**
  - Software Security: Buffer Overflows, Handling Inputs/Outputs, Secure Programming
  - Database and Data Center Security: SQL Injection Attacks, Inference

- **Part V: Management Issues**
  - Security Management, Risk Assessment, and Threat Modelling
  - Security Controls, Plans, and Procedures
  - Security Evaluation and Assurance
  - Legal and Ethical Aspects