DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES
UNIVERSITY OF TORONTO MISSISSAUGA

CSC347H5F LEC0101
Introduction to Information Security
Course Outline - Fall 2019

Class Location & Time	Thu, 03:00 PM - 05:00 PM IB 250
Instructor	Furkan Alaca
Office Location	3074 Deerfield Hall
Office Hours	
E-mail Address	furkan.alaca@utoronto.ca
Course Web Site	https://mcs.utm.utoronto.ca/~alacafur/courses/csc347_f19

Course Description

An investigation of many aspects of modern information security. Major topics cover: Techniques to identify and avoid common software development flaws which leave software vulnerable to crackers. Utilizing modern operating systems security features to deploy software in a protected environment. Common threats to networks and networked computers and tools to deal with them. Cryptography and the role it plays in software development, systems security and network security. [24L, 12P]

Prerequisite: CSC209H5, CSC236H5, CSC290H5 (SCI)
Distribution Requirement: SCI

Students who lack a pre/co-requisite can be removed at any time unless they have received an explicit waiver from the department. The waiver form can be downloaded from here.

Textbooks and Other Materials

Computer Security and the Internet: Tools and Jewels (P. Van Oorschot - Carleton University, 2019)

Textbook chapters and other readings will be provided electronically.

Assessment and Deadlines

Type	Description	Due Date	Weight
Assignment	Assignment 1	2019-10-02	10%
Assignment	Assignment 2	2019-10-23	10%
Assignment	Assignment 3	2019-11-13	10%
Assignment	Assignment 4	2019-12-04	10%
Assignment	Blog task	On-going	5%
Assignment	Reading response	On-going	5%
Lab	Weekly tutorials	On-going	10%
Final Exam	To pass the course, you must obtain at least 40% on the final exam.	TBA	40%
		Total	100%

More Details for Assessment and Deadlines

Assignment instructions and tutorial exercises will be posted on the course website as they are assigned. Attendance of weekly tutorials is mandatory.

Penalties for Lateness

Late assignments will be accepted up to 4 days (96 hours) after the deadline, with a penalty of 5% per day of lateness.

Procedures and Rules

Missed Term Work

To request special consideration, bring supporting documentation to the instructor in person during office hours at least one week in advance.

In case of illness, bring a U of T medical certificate to the instructor within one week of the missed work. The certificate must specify the exact period during which you were unable to carry out your academic work.

Students with diverse learning styles and needs are welcome in this course. In particular, if you have a disability/health consideration that may require accommodations, please feel free to approach me and/or Accessibility Services as soon as possible. Accessibility staff (located in Room 2037, Davis Building) are available by appointment to assess specific needs, provide referrals and arrange appropriate accommodations. Please call 905-569-4699 or email access.utm@utoronto.ca. The sooner you let us know your needs the quicker we can assist you in achieving your learning goals in this course. Accessibility Services at the University of Toronto Mississauga can also be found online at http://www.utm.utoronto.ca/accessibility.

Missed Final Exam

Students who cannot write a final examination due to illness or other serious causes must file anonline petition **within 72 hours of the missed examination**. Original supporting documentation must also be submitted to the Office of the Registrar **within 72 hours of the missed exam**. Late petitions will **NOT** be considered. If illness is cited as the reason for a deferred exam request, a U of T Verification of Student Illness or Injury Form must show that you were **examined and diagnosed at the time of illness and on the date of the exam, or by the day after at the latest**. Students must also record their absence on ACORN on the day of the missed exam or by the day after at the latest. Upon approval of a deferred exam request, a non-refundable fee of $70 is required for each examination approved.

Academic Integrity

Honesty and fairness are fundamental to the University of Toronto's mission. Plagiarism is a form of academic fraud and is treated very seriously. The work that you submit must be your own and cannot contain anyone elses work or ideas without proper attribution. You are expected to read the handout How not to plagiarize (http://www.writing.utoronto.ca/advice/using-sources/how-not-to-plagiarize) and to be familiar with the Code of behaviour on academic matters, which is linked from the UTM calendar under the link Codes and policies.

Normally, students will be required to submit their course essays to Turnitin.com for a review of textual similarity and detection of possible plagiarism. In doing so, students will allow their essays to be included as source documents in the Turnitin.com reference database, where they will be used solely for the purpose of detecting plagiarism. The terms that apply to the University's use of the Turnitin.com service are described on the Turnitin.com web site.

Final Exam Information

Duration:	3 hours
Aids Permitted:	None

Additional Information

Tentative list of topics (subject to modification):

Basic Concepts and Principles (Ch. 1): Computer security concepts, types of security threats and attacks, countermeasures, security design principles.

Cryptographic Building Blocks (Ch. 2): Symmetric encryption, message authentication and hash functions, public-key encryption, digital signatures and key management, random and pseudorandom numbers.

User Authentication (Ch. 3): Password-based authentication and related attacks/defenses, one-time passwords, biometrics and other alternatives.

Protection in Operating Systems (Ch. 5): Memory protection, access control models, filesystem permissions and setuid

Software Security (Ch. 6): handling program input, data interpretation, interactions with OS, libraries, other apps, race conditions, program output. Memory exploits (e.g., buffer overflows) and related defenses.

Web and Browser Security (Ch. 8, 9): SSL/HTTPS, Same-Origin Policy, HTTP cookies, XSS, CSRF.

Network Security (Ch. 10): firewalls, intrusion detection systems, SSH and secure tunneling, VPNs.

Malicious Software (Ch. 7): viruses, worms & worm propagation, rootkits, and botnets.

Last Date to drop course from Academic Record and GPA is November 7, 2019.