DEPARTMENT OF MATHEMATICAL AND COMPUTATIONAL SCIENCES
UNIVERSITY OF TORONTO MISSISSAUGA

CSC347H5F LEC0101
Introduction to Information Security
Course Outline - Fall 2017

Class Location & Time	Fri, 03:00 PM - 05:00 PM DH 2060
Instructor	Arnold Rosenbloom
Office Location	
Office Hours	W10-12
E-mail Address	arnold@cs.toronto.edu
Course Web Site	http://www.cs.toronto.edu/~arnold/347/17f
Teaching Assistant	Jai Geelal
Office Hours	TBA
E-mail Address	jai.geelal@mail.utoronto.ca
Teaching Assistant	Serguei Khasimkhanov
Office Hours	TBA
E-mail Address	serguei.khasimkhanov@mail.utoronto.ca

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, 12T]

Prerequisite: CSC209H5, 236H5, 290H5 (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

No textbook required.

Assessment and Deadlines

Type	Description	Due Date	Weight
Assignment	Assignment 1	2017-10-08	20%
Assignment	Assignment 2	2017-11-08	20%
Assignment	Assignment 3	2017-12-04	20%
Final Exam	Final	TBA	34%
Lab	Labs	On-going	6%
		Total	100%

Penalties for Lateness

20% if handed in up to 48 hours after due date, not accepted after that.

Procedures and Rules

Missed Term Work

In case of an emergency that will cause you to miss an assignment deadline, please contact the instructor via email within 24 hours of the assignment deadline. In case of illness, have your doctor complete an official U of T medical certificate. For other emergencies, be prepared to provide other documentation requested by the instructor.

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.

Final Exam Information

Duration:	3 hours
Aids Permitted:	Non-Programmable Calculators 2 page(s) of double-sided Letter (8-1/2 x 11) sheet

Additional Information

Tentitive list of topics

Overview of Security: (1 week mixed in throughout course)

Software security: (3 weeks)

- buffer overrun and integer overflow
- Canonical representation issues
- the difference between code and data, code injection (SQL/XSS), application to web based software
- application of cryptography: using cryptographic libraries, logins, passwords and hashing

Systems Security: (2.5 weeks)

- users, permissions, files and processes
- application of cryptography: authenticating users, password files, PAM and kerberos
- principle of least privilege
- securing the file system
- threats to your browser, spyware
- e-mail: spam and spam filters
- backups

Network Security: (3 weeks)

- overview of TCP/IP and protocols
- types of low level attacks
- providing network services (inetd)
- firewalls and nat

Cryptography: (2.5 weeks)

- Basic encryption and decryption, symmetric key cryptography
- Public Key cryptography
- hashing and document signing
- Cryptographic foibles
- application of cryptography: digital certificates in browsers, VPNs and ssh

Last Date to drop course from Academic Record and GPA is November 7, 2017.