ECE 568 Computer Security

Fall 2017 Course Syllabus

General Information

Welcome to ECE 568!

This course covers principles of computer systems security. It starts by examining how to identify security vulnerabilities, how they can be exploited, and then discusses techniques that can help defend against such attacks. The course then provides an introduction to basic elements of cryptography, and continues by covering topics in operating system security, network security and web security.

Instructor

David Lie: lie@eecg.toronto.edu

Office hours by appointment

Course Website

Information on ECE568, including important announcements and course marks can be found on the UofT Portal course website (https://portal.utoronto.ca/). Please visit the website on a regular basis for up-to-date information, including information about labs, assignments and lectures. The course also has discussion forum, found here, where you can post questions regarding the course. While we will try to check the board as often as possible, this does not necessarily mean you will get an answer for your questions in less than 24 hours. *Note, you are not automatically enrolled you onto the forum, you must enroll yourself onto the service.*

E-mail

All UofT students are required to have a valid UTORmail email address. You are responsible for ensuring that your UofT email address (@utoronto.ca) is properly entered in the ACORN system. **Customary Disclaimer:** It is your responsibility to check and ensure you are able to receive mail about this course. You may forward your e-mail to another service (i.e. Gmail, Yahoo, etc.) if you wish, but it is your responsibility to ensure that mail about this course is not filtered as spam or junk mail.

Textbook

There is no required textbook for the course. However, the instructor will provide a list of reference books in class. The instructor will also provide lecture slides on the course web site. Also, various other resources will be available on the web site.

Timetable

The timetable for the course is shown below. You are expected to attend the lectures each week; attendance in the labs is recommended, but not required.

Labs

The labs consist of a number of programming exercises that will take a substantial amount of your time. The TAs will test your lab on the ECF lab workstations (p___.ecf.utoronto.ca). You may do the labs on your own machines, but it is your responsibility to make sure that they work on the ECF computers. PLEASE NOTE that you will need a 64-bit Linux OS to do the labs. All ECF computers have been updated to 64-bit Linux. To check whether you are running a 64-bit version of Linux, please type “uname -a” and verify that you see “x86_64” in the results returned. The TAs will be using automated scripts to aid them in grading the labs: as a result, it is important that you follow the submission instructions for each lab carefully. You are encouraged to include documentation for your labs (not exceeding 1 page, please no essays!). If your labs do not work completely, the TAs may use this documentation to assign part marks. Lab attendance is not required. Labs will be done in groups of two students. A TA will be in SF1013/1012 during the lab period (3-6PM on Wednesdays) starting Sept 20.

Important Dates

An approximate lecture schedule along with the release date and due dates for the labs and assignments are shown below. A handout for each lab and for each assignment will be available from the course web site, and no hard copies will be provided in class. Labs are due by no later than 11:59 pm on the indicated due date below.

Week	**Lecture**	**Lab/Midterm**
Sept 8	Intro, ethics	
Sept 11	Security fundamentals, Buffer overflows	
Sept 18	Format string, double free, ROP, CFI, Attacks and Defenses	Lab 1: Buffer Overflow Vulnerabilities (Due Oct 8) **Note: there is no scheduled lab on Sept 13.**
Sept 25	Intro to Crypto, Block Ciphers	
Oct 2	Encryption Modes, Stream Ciphers	
Oct 9	Key exchange, Public Key Crypto, RSA, PKI	Lab 2: SSL Programming (Due

		Oct 29)
Oct 16	Review (1 lecture)	**Midterm Oct 18 & 20 (SF3202)**
Oct 23	Hashes, MAC, Signatures, Secure communication + SSL,	
Oct 30	Web authentication and XSS, XSRF attacks, Single Sign-on and federated Identity	Lab 3: 2-factor Authentication (Due Nov 19)
Nov 6	2-factor authentication	
Nov 13	OS Security, Network Security, protocol attacks, firewalls + IPS/IDS	
Nov 20	Android and Mobile Security	Lab 4: Web application security (Due Dec 8)
Dec 4	Block chains and Bitcoin, IaaS Cloud Security, Review and Wrap-up	

Tutorials

There are no tutorials in this course. Please make use of the TAs in the labs, the discussion forum, and office hours with the instructor.

Course Policies

There will be no extensions given in this course. Plagiarism will not be tolerated; in particular, you and your lab partner are jointly responsible for ensuring that your submitted lab work is original work.

Missed Labs

You will have a minimum of two weeks to do any labs – so a couple of sick days will not be accepted as grounds for special consideration. Nevertheless, if for some valid reason you are unable to submit the lab on time or hand in an assignment, please provide an explanation and appropriate documentation (for example, a doctor’s note).

Re-grading

Everybody makes mistakes, including TAs and the instructor! If you feel that there has been a grading mistake, you can request a regrade within one week of the lab results being returned. You should submit a short note explaining which questions are in error and why you think you deserve a regrade. A TA or the instructor will regrade the entire lab. (Therefore, you should be sure that there has been a significant mistake, or you may very well end up with a lower grade on your assignment.)

Marking and Evaluation

There will also be two 1-hour mid-term tests during the course on **Oct 18 and 20**. They will take place during the lecture slot to minimize conflicts. A final exam will be given during the final exam period. The details of the mid-term test and final exam time will be provided in class and on the web site. The composition of the final mark is as follows:

Labs: 20% Mid-Term Test: 30% Final Exam: 50%

Calculator Type: 4 (none) Exam Type: C (single reference sheet, both sides)