Course Outline

Fall 2023 CIS*4510 (Computer Security Foundations)

Welcome to the Fall'23 offering of Computer Security Foundations. This course covers foundations in computer systems security and teaches practical defenses. The topics covered include adversarial modeling, threat modeling, risk assessment, security policies, cryptographic building blocks, identity and access management, operating systems security, software security, malicious software, network security, web security, firewalls, tunnels and intrusion detection systems.

Instructor:	Hassan Khan
Email:	hassan.khan@uoguelph.ca
Office location:	150 Research Lane
Office hours:	MW 3:00-4:00pm (150 Research Lane/Virtual)
Lectures:	MW 4:00-5:20pm (MCKN029)
Labs:	None

Required Text

- Computer Security and the Internet: Tools and Jewels, 2nd edition, Paul C. van Oorschot, 2022.

Other Resources

- Security Engineering: A Guide to Building Dependable Distributed Systems, 3rd edition, Ross J. Anderson, Wiley Publishing, 2020.
- Schneier on Security. A blog covering current computer security and privacy issues.

Outline

- Introduction to Cybersecurity
- Cryptographic Building Blocks
- Identity and Access Management
- Operating System Security
- Software Security
- Malicious Software
- Network Security
- Firewalls, Tunnels and Intrusion Detection
- Web Security

Prerequisites

Computer Networks and Operating Systems

Grading Policy

- Assignments (3 x 15%)
- Midterm Exam (20%) **Oct 16, 4:00 - 5:20PM**
- Final Exam (25%) **Dec 11, 2:30 - 4:30PM, Location: TBD**
- Lab Presentation (10%)

Reappraisal Policy

If you have an assignment that you would like to have reappraised, please follow the instructions given on CourseLink to submit your request. Please include a justification for your claims. The appeals deadline is one week after the respective graded item is first made available. Note that for an assignment the entire grade will be remarked, and the assigned grade may go up or down as a result. If your appeal is concerned with a simple calculation error, please see the instructor during their office hours.

Course Presentations

You have to present a recent paper (~published within past two years) at a top computer security conference. Your focus should be on academic venues, such as USENIX Security, ACM CCS, IEEE Symposium on Security and Privacy, or the NDSS Symposium (for papers of interest from other venues, please discuss with the instructor in advance). Please share the paper with the instructor by the deadline provided in the classes schedule.

Academic Misconduct

The University of Guelph takes a very serious view of Academic Misconduct. Included in this category are such activities as cheating on examinations, plagiarism, misrepresentation, and submitting the same material in two different courses without written permission. Students are expected to be familiar with the section on Academic Misconduct in the Undergraduate Calendar, and should be aware that expulsion from the University is a possible penalty. If an instructor suspects that academic misconduct has occurred, that instructor has the right to examine students orally on the content or any other facet of submitted work. Moreover, it is expected that unless a student is explicitly given a collaborative project, all submitted work will have been done independently.

Course Schedule

Module	Lecture Number	Date	Slides	Textbook Sections	Other Resources	Upcoming Events
Introduction to Computer Security	Lecture 1	Sep 11		1.1 - 1.7		
	Lecture 2	Sep 13				
Cryptographic Building Blocks	Lecture 3	Sep 18		2.1 - 2.6	AES Stick Fig.	**A1 release**
	Lecture 4	Sep 20			ECC Primer	
	Lecture 5	Sep 25				
	Lecture 6	Sep 27				
Identity and Access Management	Lecture 7	Oct 02		3.1 - 3.5		
	Lecture 8	Oct 04				
Operating System Security	Lecture 9	Oct 11		5.1 - 5.3, 5.7		A1 due A2 release

Mid-term		Oct 16				
Operating System Security (cont)	Lecture 10	Oct 18				
Software Security	Lecture 11	Oct 23		6.1 - 6.3, 6.6		Presentation Topic due
	Lecture 12	Oct 25				
Malicious Software	Lecture 13	Oct 30		7.1 - 7.6		A2 due
	Lecture 14	Nov 01				
Network Security	Lecture 15	Nov 06		11.2 - 11.4	OTR Deniability	A3 release
	Lecture 16	Nov 08				
Firewalls, Tunnels and IDS	Lecture 17	Nov 13		10.1 - 10.4, 11.1		
	Lecture 18	Nov 15				
Web Security	Lecture 19	Nov 20		9.1, 9.3 - 9.5		
	Lecture 20	Nov 22				A3 due
Class Presentations		Nov 27,29				
Recap		Nov 30				

Disclaimer

Please note that the ongoing COVID-19 pandemic may necessitate a revision of the format of course offerings, changes in classroom protocols, and academic schedules. Any such changes will be announced via CourseLink and/or class email.

This includes on-campus scheduling during the semester, mid-terms and final examination schedules. All University-wide decisions will be posted on the COVID-19 website (https://news.uoguelph.ca/2019-novel-coronavirus-information/) and circulated by email.

For information on current safety protocols, follow these links: https://news.uoguelph.ca/return-to-campuses/how-u-of-g-is-preparing-for-your-safe-return/

https://news.uoguelph.ca/return-to-campuses/spaces/#ClassroomSpaces

Please note, these guidelines may be updated as required in response to evolving University, Public Health or government directives.

Illness and medical notes

Medical notes will not normally be required for singular instances of academic consideration, although students may be required to provide supporting documentation for multiple missed assessments or when involving a large part of a course (e.g.. final exam or major assignment).