University of Manitoba

Department of Electrical & Computer Engineering
Graduate Course Outline

FALL 2020

ECE 7650 T19 – Computer and Network Security

COURSE DESCRIPTION:

This course studies the fundamental principles of computer, network, and information security from the perspectives of the defenders, attackers, and testers. From the defenders point of view, the course investigates the current state of the art in the design for security, and the provisions and policies adopted to establish security, in networking protocols, host and operating system software and hardware, and security mechanisms. Furthermore, the course investigates available software, hardware, and tools adopted to monitor and prevent unauthorized access, misuse, and modification of computer and network-accessible resources.

From the testing point of view, this course will study penetration testing, aka intrusion testing, which is the systematic engineering procedure of locating weaknesses and vulnerabilities of computer, network, and information systems. The objective of the systematic engineering procedure will be to determine:

1. What information/locations/systems can be accessed?
2. What can be seen on the target?
3. What can be done with available information?
4. What aspects of the monitoring can be detected on the target machine/network?

From the attackers point of view, this course studies attacks on computer systems, networks, and the WWW through the study of various forms of malware (such as viruses, worms, Trojan Horses, spyware, and ransomware), from vanilla to polymorphic versions.

Finally, the course will also study the legal, regulations, and ethical issues in the study of malware and penetration testing.

COURSE OBJECTIVES:

This course has the following objectives:

1. To learn the fundamental principles of computer and network security.
2. To explain host and computer network security principles.
3. To know how to detect common vulnerabilities to attacks on computer systems.
4. To explain how selected attacks work, and the corresponding mitigating defensive mechanisms.
5. To study design for security, and the provisions and policies adopted to establish security, in networking protocols and host and operating system software and hardware.
6. To perform penetration testing in an isolated lab.
7. To explain and be familiar with various forms of malware and its evolution from vanilla to polymorphic versions.
8. To know and practice the legal, regulations, and ethical issues in the study of malware and penetration testing.

PRE-REQUISITES:

This course has the following pre-requisites:

1. Basic computer networks, protocol stacks, data networking and routing protocols.
2. Software languages (e.g., MatLab, Python, Java, C) for creating simulations of protocols: simulation tools would be beneficial.

CONTACT HOURS:

3-hours per week

COURSE CONTENT:

The following topics will be discussed:

1. Introduction to computer, network, and information security: evolution of computer security, types of security threats, hardware threats, software threats, physical threats, etc.
2. Modeling Cyber Threats Using Cyber Kill Chain: Reconnaissance, Weaponization, Delivery, Exploit, Installation, Command and Control, and Actions on Objectives.
3. Current methods used for identifying threats, detecting vulnerabilities and anomalies,
4. Industry viewpoint of computer and network security.
5. Foot printing, Scanning, Enumeration
6. Forms of attacks: Trojans, backdoors, hacking web servers, buffer overflows, stack smashing, shellshock, SQL-injection, cross-site scripting.
7. Penetration testing methodologies.
8. Countermeasures and mitigating defensive mechanisms.
9. Authentication, verification, repudiation, basic cryptography techniques, public and private key methods.
10. Host process sandbox design and development.
11. Hands-on projects/labs implemented in an isolated sandbox.

Additional advanced research topics as determined by the instructor.

HOMEWORK:

Homework will consist of assignments and preparation of a seminar on a research article or project.

TEXTBOOK:

The textbook for this course will be the lectures slides, as given on the course website (TBA).

GRADE ANNOUNCEMENTS:

TBA – Due to COVID-19, this date to be announced by the Registrar's Office

EVALUATION:

Your final course grade is determined by your performance in the components list below in the Evaluation Table (seminar, assignments, project, mid-term, and a final examination. Students must receive a minimum of 50% on the final examination and must complete and pass all components in the course in order to be eligible to receive a passing grade.

Each component is weighted as follows:

COMPONENT	NO	VALUE %	TOTAL VALUE	DETAILS / ADDITIONAL INFO
Seminars	1	10%	10	
Assignments	5	15%	15	
Mid-Term Exam	1	25%	25	
Final Examination	1	50%	50	
TOTAL			100	

GRADE SCALE:

LETTER	MARK	LETTER	MARK	LETTER	MARK	LETTER	MARK
A+	95-100	B+	80-84	C+	65-69	D	45-54
A	85-94	B	70-79	C	55-64	F	<45

INSTRUCTOR INFO:

Name:..... Ken Ferens
Office:..... E1-544 EITC
Tel:..... (204) 474-8517
Email:..... Ken.Ferens@umanitoba.ca

Office Hours: ..... By appointment

VOLUNTARY WITHDRAW:

November 23, 2020

REQUIREMENTS/REGULATIONS

Student Responsibilities: It is the responsibility of each student to contact the instructor if he/she is uncertain about his/her standing in the course and his/her potential for receiving a failing grade. Students should also familiarize themselves with Sections 4 and 6 of the Regulations dealing with, among others, incomplete term work, deferred examinations, attendance and withdrawal, etc.

Lectures: Attendance at lectures is essential for successful completion of this course. Students must satisfy each evaluation component in the course.

ACADEMIC INTEGRITY

Students are expected to conduct themselves in accordance with the highest ethical standards of the Profession of Engineering and evince academic integrity in all their pursuits and activities at the university. As such, in accordance with the General Academic Regulations and Requirements of the University of Manitoba, Section 7.1, students are reminded that plagiarism* or any other form of cheating is subject to serious academic penalty (e.g. suspension or expulsion from the faculty or university) regardless of media

- examinations
- assignments
- laboratory reports
- term exams

A student found guilty of contributing to cheating in examinations or term assignments is also subject to serious academic penalty

Please refer any questions regarding Academic Integrity to your course instructor.

***Plagiarism:** to steal and pass off (the ideas or words of another) as one's own; use (another's production) without crediting the source