Course Syllabus

CIS*4510 Computer Security Foundations F (3-2) [0.50]
School of Computer Science, University of Guelph, Guelph
Fall Semester | 2020

1. INSTRUCTIONAL SUPPORT

Instructor Information

Instructor Name	Office	Phone	Email
Dr. Xiaodong Lin	Reynolds 2210	X53889	xlin08@uoguelph.ca
Office Hours:	Monday/Wednesday, 3:30 pm - 5:00 pm or by appointment Online through Microsoft Teams		

Prerequisite(s): CIS*3210.

Teaching Assistant Information

Teaching Assistant Name	Email
TBD	TBD
Office Hours: TBD	

Lectures

Day	Time	Location
Tuesday/Thursday	04:00PM - 05:20PM	Cyberspace

Labs

Lab Section	Day	Time	Location
0101	Tuesday	09:30AM - 11:20AM	Cyberspace
0102	Thursday	09:30AM - 11:20AM	Cyberspace

Lab Environment

System requirements: 8 GB RAM, 25 GB hard disk free space.
Virtual Machine Software: Install VirtualBox and its matching Extension Pack if you haven't already.

Ubuntu 16.04 Virtual Machine Image: Please use the following link to download a pre-built Ubuntu 16.04 virtual machine image (**SEEDUbuntu-16.04-32bit.zip**) before the first lab class. All the labs use this image.
https://seedsecuritylabs.org/lab_env.html

Note: There will be weekly labs. The labs are not mandatory but you are strongly recommended to all scheduled labs online at the appointed time. If you are unable to attend a lab in the lab section that you are registered for, please make your best efforts to attend another lab section. If unforeseen circumstances prevent you from doing so, contact the instructor as soon as possible to arrange for office hours if you have difficulty following lab exercises.
During a lab I will first give a tutorial at the beginning of each lab class to give an overview of the experiment you will perform and reinforce the technical knowledge required for the lab exercises, and most importantly, give some tips on how to complete these lab exercises, which are cyber attacking and defensing cases. So you can complete these lab exercises by yourself after class. Please be advised that most likely you will not finish all the tasks required in a lab during the allocated lab time, but you know what to do technically. Also, you can ask any questions that you may have, and keep up with the lab exercise schedule. Cyber attack practice could be very challenging, but you will have a lots of fun to learn the cyber security skills through hands-on exercises.

2. LEARNING RESOURCES

Recommended Textbook

- Wenliang Du. Computer & Internet Security: A Hands-on Approach (2nd Edition), 2019

Recommended References

- William Stallings, Lawrie Brown. Computer Security: Principles and Practice (4th Edition), 2017
- Xiaodong Lin, Introductory Computer Forensics: A Hands-on Practical Approach (1st Edition), 2018, ISBN: 978-3-030-00580-1. (Freely available from Springer via University of Guelph network at https://www.springer.com/gp/book/9783030005801)

Course Website

Course information for CIS*4510 Computer Security Foundations is posted on **CourseLink**. It is the student's responsibility to check these pages frequently for new information or updates.

- Lecture Information: The lecture notes will be posted on the course website as instructors have time to make them available. You are expected to take your own notes during lecture. In all lectures I will be following the notes very closely.
  Our classes will be held via zoom. Online activities such as advising times, question and answer sessions, and interactive lectures may be recorded by the instructor or TAs and posted to CourseLink. By taking this course you are agreeing that your participation in these activities can be used in this manner. If you do not wish to have your image or voice recorded as part of these activities then either do not take this course or do not ask verbal questions during these activities.

Do not redistribute recorded interactive discussions that involve your classmates. This includes advising times and question and answer sessions with the instructor. The course materials including recorded videos are restricted to use for this course and cannot be redistributed.

- Labs and Tutorials: Selected tutorial and lab materials will be available on the course website.
- Tests: Tests will be posted as online quiz on the course website.

Course Description

This course covers basic concepts and practices in computer and network security. This includes topics such as fundamental concepts of computer security, network security, threat landscape, threat intelligence and attack methods, ethical hacking concepts and other hacking techniques, security technology and security policies, and cloud security.

The format of this course will consist of lectures, hands-on exercises (or lab assignments), online quizzes, and a final project. The lectures will be presented online via Zoom. All lectures involve the interaction between students and instructor in real-time. Lectures will be archived into videos which will be made available on CourseLink. Please note that video archives are only intended for occasional or backup use in case students have to miss lectures due to personal, business, or medical reasons. **Real-time, online participation is strongly recommended**.

The goal of the lectures is to introduce the core concepts of computer and network security. The goal of the labs is to give students some exposure to cyber attack and defense on information systems. It offers students practical and theoretical knowledge and understanding of issues related to computer and network security. Thus, an important part of the course will be the hands-on experience (or lab assignments). For that, you will learn how to exploit various vulnerabilities to compromise a vulnerable computer system and as well practise various defense mechanisms for security protection.

Please see The Academic Calendar for more details. The Academic Calendars are the source of information about the University of Guelph's procedures, policies and regulations which apply to undergraduate, graduate and diploma programs:
http://www.uoguelph.ca/registrar/calendars/index.cfm?index

Ethics, Law, and University Policies

Information provided in this class and all in-class demonstrations are designed for the purpose of education, but not for any illegal activities. Also, use of information security tools requires utmost ethical conduct.

To defend a computer system you need to be able to think like an attacker, and that includes understanding techniques that can be used to compromise security. However, using those techniques in the real world may violate the law and the university's computing practices, or may be unethical. You must respect the privacy and property rights of others at all times, or else you will fail the course. Under some circumstances, even probing for weaknesses may result in severe penalties, up to and including civil fines, expulsion, and jail time.

As cybersecurity professionals, you are required to adhere to the highest ethical standards of behavior.

3. COURSE OUTCOMES

On the successful completion of the course, students will be able to:

1. explain basic computer security terminology, including threat, vulnerability, adversary, attack and countermeasure,
2. understand the basic principles and practices in computer and network security,
3. explain basic concepts related to applied cryptography, including plaintext, ciphertext, techniques for cryptoanalysis, symmetric cryptography, asymmetric cryptography, digital signature, and modes of encryption operations,
4. describe and generalize various software vulnerabilities,
5. describe and generalize various network protocol vulnerabilities,
6. describe and generalize various web application vulnerabilities,
7. explain how various attacks work,
8. design and implement basic security mechanisms to protect computer systems,
9. compare various security mechanisms, and articulate their advantages and limitations,
10. apply security principles to solve problems.

4. COURSE TOPICS

Introduction and Basics
User authentication, Authorization and Access Controls
Software Security: Vulnerabilities, Attacks, and Defenses
Applied Cryptography
Web and Network Security: Vulnerabilities, Attacks, and Defenses
Incident Response and Computer Forensics

5. EVALUATION METHOD

Final grade calculation

In determining the overall grade of the course, the following weights will be used:

Coursework	Amount	% of Grade
Triweekly tests	4	30
Lab Exercises	5	40
Discussion Participation		4
Final project	1	26

- Triweekly tests: 30%
  - There will be four tests, each of 45-minute duration, held approximately every three weeks during the term, according to the schedule indicated below.

Test 1: 6%	Week 3
Test 2: 9%	Week 6
Test 3: 6%	Week 9
Test 4: 9%	Week 12

  - Each test will be posted as online quiz on the CourseLink site when available.

- Lab Exercises + CTF: 40%
  - There are 11 lab exercises in total. There will be **five** lab exercises (one is Capture The Flag (CTF)) to be graded, which are focused on specific tasks pertaining to computer network attack and defense. Five laboratory exercises are worth 40% of the total course grade, and each lab weight is as follows:

Lab Exercise 1	=3%	September 21st
Lab Exercise 2	=9%	October 1st
Lab Exercise 3 (CTF)	=8%	October 8th
Lab Exercise 7	=10%	November 12th
Lab Exercise 10	=10%	November 26th

    Note that all the lab exercises will be released on the Tuesday of the preceding week of the due date listed above for a lab exercise.

    Please note that the above schedule is tentative and may be subject to change, depending on class progress.

  - You are allowed to talk with other students currently enrolled in the course about the lab content. We encourage you to use discussion boards on the CourseLink course website to help your peers. However, each student must conduct the lab exercises and write up their lab reports completely independently.
  - **Important: Students must successfully complete all of the hands-on exercises (Lab Exercises + CTF) with a passing grade (the average of all the hands-on exercises) in order to pass the course.**

- Discussion Participation: 4%
  - Particularly, discussion board participation. In the Discussion Board make meaningful posts or initiate discussion threads (at least **8** for the entire semester) to get full participation marks.
- Final project: 26%

  A final project is required to complete this course, and is one of the important components of this course. It is a **CASE STUDY** of attack scenarios as well as how security techniques can be deployed to defend against these attacks. The work should reflect much deeper level of understanding (<u>beyond what covered in the lab exercises if the topic you choose is the same as one of the lab exercises</u>) with an evidence of some contribution (**your critical thought**). You can work in **a 2-people team** to complete the course project, where one student will launch attacks to a computer system and/or network and another student finds approach(es) to detect and defeat such attacks.

  The project has the following milestones:
  - **Case Study Proposal**

    A case study proposal is required for approval. The proposal **MUST** present the methodology for Attack and Defense case study design. It provides a brief description of the project, including
    - <u>Motivation</u>: e.g., what is the history of the security problem you investigate? why is this problem interesting and important?

- Objectives: describe your objectives or goals,
- Project Plan (Methodology): your plan that are needed to meet objectives, for example, project environment (software, hardware, or tools that you will use for the cyberattack and defense in your project),
- Conclusion: what will you learn by doing this project?

It also should list all project team members. You should only submit one proposal per team for the course project.

Note that the proposal is not worth any marks, but it MUST be submitted and approved for the project grades to be counted.

Case Study Proposal Due on September 24th, 2020 at 11:59PM.

➢ **Final Report** (22%) with assessment criteria as follows:
  - Literature review and extensiveness of the review;
  - Grasp of knowledge/theory pertaining to the security problem;
  - Grasp of knowledge pertaining to the application/solution to the security problem;
  - Reports should adhere to the standard IEEE double-column format for conferences[1];
  - Length of paper (6 pages minimum in standard IEEE proceedings two-column format), including the abstract, tables, and figures (excluding references);
  - Design of cyber-attack and defense experiment;
  - Articulation/accuracy of argument/findings regarding the security problem;
  - Breadth of references/bibliography; and
  - Proportionate effort put into work.

  [1]**P.S.:** A Word template for IEEE proceedings or all Transactions two-column format, TRANS-JOUR.doc, can be found in the following link http://www.ieee.org/web/publications/authors/transjnl/index.html

➢ **Reflection questions** for project (4%)
  - An online meeting will be setup to assess the knowledge and understanding of each team. It will be held in the form of an approximate 10-minute one-to-one conversation with the instructor or the TA via Microsoft Teams. Each team will be given several questions related to their project during the meeting. Reflections are marked based on whether or not the team is able to answer the questions correctly.
  - **Reflection is MANDATORY**. Otherwise, you will receive no credit for the project. Also, all team members in one group must be present during the meeting.

➢ Potential topics, but are not limited to:
  - Software vulnerability and protection (e.g., buffer overflow attack and prevention)
  - Web application hacking and defense (e.g., SQL injection and prevention)
  - Computer and network Forensics (e.g., deleted file recovery and file carving)

- Security and vulnerability analysis (e.g., automated vulnerability analysis techniques)
- Network attack and defense (e.g., DoS attack and prevention)
- Phishing/spamming and anti-phishing
- Cryptography and Cryptanalysis (e.g., SSL Man-in-the-Middle Attacks)

➢ **Report Due on December 4th, 2020 at 11:59PM**.

In the following the term "lab grade" means the cumulative grade for all the lab works (including the four labs and CTF) expressed as a percentage. The overall course grade will be computed in two distinct ways as follows, depending on whether or not your lab grade is 50% or more:

(a) If your lab grade is 50% or more: your overall course grade is the weighted sum of all assessments shown above, using the weights indicated in the table above.
(b) If your lab grade is less than 50%: your overall course grade is the lab grade.

Disclaimer

Please note that the ongoing COVID-19 pandemic may necessitate a revision of the format of course offerings and academic schedules. Any such changes will be announced via CourseLink and/or class email. All University-wide decisions will be posted on the COVID-19 website and circulated by email.

Illness

The University will not require verification of illness (doctor's notes) for the fall 2020 or winter 2021 semesters.

Course Grading Policies

Late assignments: We will allow **3 total late days** ("grace days") for assignments (labs and project) **which you can use to give yourself extra time without penalty**. Please email me with your late submission if you decide to use these days for a particular assignment. Late days may be spread over any number of assignments at your own discretion, but the total number may not exceed 3. Late days are rounded up so that an assignment that is 28 hours late accumulated 2 late days. No extensions will be considered beyond the late days.

All assignments are due at 11:59 PM on the due date. Late lab reports (and project report) beyond the grace days will incur a penalty of 25% in the first 24 hours, 50% in the second 24 hours, 75% in the third 24 hours, and 100% thereafter, unless prior arrangements are made or a valid reason presented within five days from the missed deadline. In no case will a lab report be accepted more than three days past the deadline; if a valid reason exists for being unable to hand in the lab report within five days following the deadline, then the lab will be assigned a weight of zero and the weight of the missing lab will be distributed across the remaining labs. However, if the total marks you have obtained from your handed-in lab work is less than 20%, you will be required to conduct an extra lab exercise, which is worth of the weight of your missing lab(s).

Submission policy: All your course work will be only be accepted via submission through CourseLink unless otherwise indicated on the assignment by the instructor. Failure to submit assignments correctly (e.g., wrong files, etc.) will result in a zero mark.

Regrades: Students may request a reassessment of their assignments in writing and specify the reasons for such requests. Their entire assignment will be reassessed, and the reassessment may result in raising or lowering of the original marks. Remark requests will only be accepted up to **5 calendar days** from the release of the assignment mark. Please carefully read through the comments made by the marker on Courselink before sending a remark request.

Missed Assessments: If you are unable to meet an in-course requirement due to medical, psychological, or compassionate reasons, please contact your course instructor within five days following the deadline. Please see below for specific details and consult the undergraduate calendar for information on regulations and procedures for Academic Consideration: http://www.uoguelph.ca/registrar/calendars/undergraduate/current/c08/c08-ac.shtml

Note: **There are no makeup tests or final project.** If you miss a test with a valid reason or having made prior arrangements with your course instructor, the weight of the missing test will be moved to the final project. However, if you are unable to submit your final report with a valid reason or having made prior arrangements with your course instructor, you will be assigned with an INC grade, and can require a deferred privilege.

Accommodation of Religious Obligations: If you are unable to meet an in-course requirement due to religious obligations, please email the instructor within two weeks of the start of the semester to make alternate arrangements. See the undergraduate calendar for information on regulations and procedures for Academic Accommodation of Religious Obligations:
http://www.uoguelph.ca/registrar/calendars/undergraduate/current/c08/c08-accomrelig.shtml

Plagiarism Policy: All work submitted must be your own. Similarities between assignment submissions are monitored using Turnitin as well as by manual means.

Special Note:

- A reliable internet connection that is sufficient for online learning is necessary for this course. If you do not have a sufficiently fast and reliable internet connection then you may not be able to view or download lectures or other course material. It may also not be possible to attend online advising with teaching assistants or the instructor.
- This course is offered in the eastern standard time zone (EST). While taking this course then you may be required to attend online activities such as advising times or labs between 9:00 and 5:20 EST.
- Keep copies of assignments which you have submitted. You may be asked to resubmit assignments at a later time.
- All cases of academic misconduct are handled by the Dean, in conjunction with the School Director. Successive infractions of misconduct affirmed by this process could have consequences as serious as expulsion from the University. For details please see related pages in the University of Guelph Undergraduate Calendar 2020-2021.
- Requests for academic consideration because of illness or of a compassionate nature must be made in writing.

6. STANDARD STATEMENTS

The following are standard statements for inclusion on all course outlines (adapted with permission from the College of Arts). Some departments or colleges may also elect to post this information on a common website and link to such sites in the course outline. However, it is strongly recommended that statements on academic misconduct and links to the academic misconduct section of the academic calendars are included on all course outlines.

E-mail Communication

As per university regulations, all students are required to check their <mail.uoguelph.ca> e-mail account regularly: e-mail is the official route of communication between the University and its students.

When You Cannot Meet a Course Requirement

When you find yourself unable to meet an in-course requirement because of illness or compassionate reasons, please advise the course instructor (or designated person, such as a teaching assistant) in writing, with your name, id#, and e-mail contact. See the undergraduate calendar for information on regulations and procedures for Academic Consideration.

Drop Date

Students will have until the last day of classes to drop courses without academic penalty. The regulations and procedures for course registration are available in their respective Academic Calendars.

Copies of out-of-class assignments

Keep paper and/or other reliable back-up copies of all out-of-class assignments: you may be asked to resubmit work at any time.

Accessibility

The University promotes the full participation of students who experience disabilities in their academic programs. To that end, the provision of academic accommodation is a shared responsibility between the University and the student.

When accommodations are needed, the student is required to first register with Student Accessibility Services (SAS). Documentation to substantiate the existence of a disability is required, however, interim accommodations may be possible while that process is underway.

Accommodations are available for both permanent and temporary disabilities. It should be noted that common illnesses such as a cold or the flu do not constitute a disability.

Use of the SAS Exam Centre requires students to book their exams at least 7 days in advance, and not later than the 40th Class Day. More information: www.uoguelph.ca/sas

Academic Misconduct

The University of Guelph is committed to upholding the highest standards of academic integrity and it is the responsibility of all members of the University community – faculty, staff, and students – to be aware of what constitutes academic misconduct and to do as much as possible to prevent academic offences from occurring. University of Guelph students have the responsibility of abiding by the University's policy on academic misconduct regardless of their location of study; faculty, staff and students have the responsibility of supporting an environment that discourages misconduct. Students need to remain aware that instructors have access to and the right to use electronic and other means of detection.

Please note: Whether or not a student intended to commit academic misconduct is not relevant for a finding of guilt. Hurried or careless submission of assignments does not excuse students from responsibility for verifying the academic integrity of their work before submitting it.

Students who are in any doubt as to whether an action on their part could be construed as an academic offence should consult with a faculty member or faculty advisor.

The Academic Misconduct Policy is detailed in the Undergraduate Calendar.

Recording of Materials
Presentations which are made in relation to course work—including lectures—cannot be recorded or copied without the permission of the presenter, whether the instructor, a classmate or guest lecturer. Material recorded with permission is restricted to use for that course unless further permission is granted.

Resources
The Academic Calendars are the source of information about the University of Guelph’s procedures, policies and regulations which apply to undergraduate, graduate and diploma programs.