THE UNIVERSITY of NEW ORLEANS

CSCI 4621/5621 INTRO TO CYBERSECURITY

Spring 2023

Mon/Wed/Fri 2:00-2:50 → MATH 322 + ONLINE (ZOOM)

Syllabus

Instructor ***Dr. Vassil Roussev***

Email: **vassil**@cs.uno.edu (*include 4621 in subject line*)
Office: MATH 332, **https://uno.zoom.us/j/5042802405**
Office Hours: Mon/Tue/Wed 3:00–5:00p

Class Meeting: https://uno.zoom.us/j/81206612237?pwd=OGloZkNrbzlPaWZZOHVTZ21OL0ZaQT09
Master Repo (class materials): https://tinyurl.com/4621-s23-repo

Prerequisites

Credit in CSCI 2467

TEXTBOOK(S)

- ***Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin***, 2e, *Oorschot*, 2021. https://people.scs.carleton.ca/~paulv/toolsjewels.html
- ***Computer Security: Principles and Practice***, 4e, *Stallings & Brown*, 2017. ISBN: 978-0134794105
- ***Introduction to Computer Security***, 1e, *Goodrich & Tamassia*, 2010. ISBN: 978-0321512949

Other reading materials will be assigned as necessary.

OBJECTIVES & EDUCATIONAL OUTCOMES

This course introduces students to the fundamentals of cybersecurity, and is structured into four broad sections: *Software Security*, *Cryptography*, *System/Network Security*, and *Human Factors*. Recurring themes will be crisply defining security goals, assessing possible vulnerabilities that might undermine those goals, and learning and how to identify, fix, and prevent such vulnerabilities. A major goal is for students to acquire the skills of *adversarial thinking*—the ability to consider the constant presence of an active and evolving adversary and the resulting dynamic interplay between attack and defense.

Upon successful completion of the course, a student should be able to:

- Explain security principles and apply to specific scenarios
- Evaluate risks faced by computer systems
- Understand different cyber threats, actors, and attacks
- Describe and analyze various software vulnerabilities
- Detect common vulnerabilities in software
- Analyze and evaluate software systems for its security properties
- Explain how various security mechanisms work, and correlate these security mechanisms with security principles
- Apply security principles and mechanisms to solve problems

- Argue for and against laws and public policy that intersect with computer security
- Incorporate human factors into the evaluation of the security of a system

TOPICS (PRELIMINARY LIST)

Security Principles

- Definitions, requirements, ethics
- Threat models & trusted computing bases
- Designing secure systems

Software Security

- Execution semantics & buffer overflow
- Control-flow attacks& defenses
- Return oriented programming
- Retrofitting memory safety
- Type systems and verification
- Code analysis and isolation techniques

Systems Security

- OS security & authorization
- Trusted computing

Cryptography

- Introduction
- Randomness, secrecy, symmetric ciphers
- Public key cryptography
- Blockchains, cryptocurrencies & smart contracts

Network Security

- Introduction
- Protocol design & analysis
- Web attacks
- Web defenses

Human Factors

- Usable security
- Privacy
- Privacy tools
- Law and public policy
- Economics

Overview:

- You will receive a calendar invitation in your UNO email account with Zoom instructions for the scheduled live class session.
- All lectures will be recorded and posted online (after some light editing).
- Lectures will start and end on time, so do make an effort to be on time. Note that some of the class periods will be focused on hands-on skills, with live assignments so watching the recording afterwards would be of limited value.

- The primary source of information for the class will be at the course repo hosted on UNO's SharePoint site; all class materials will be distributed through the repo. We will make minimal use of Moodle, primarily for distributing grades.
- The class will cover a variety of topics covered in the first textbook with additional supplemental coverage where necessary. The order of discussion will likely deviate from the chapter order in the book.
- All for credit hands-on lab work will be performed on the UNO Cyber Range virtual facility hosted by the Computer Science Department: https://cyber-range.cs.uno.edu/. Use your UNO login credentials to gain access.
- ***Some of the class meetings will be dedicated primarily to lab work and you will be expected to come prepared and to perform the assigned tasks within the allotted time.***
- You may find it helpful to have a desktop virtualization system on your local machine for practice; Virtual Box (https://www.virtualbox.org/) is one free option that will provide you with everything you need.

Grading:

All work will be graded based on 100 pt scale and will count towards your final grade with the following weights:

Midterm Exam	➔	20%
Final Exam	➔	30%
Lab Work	➔	50%
Bonus Factor	➔	5% (class participation etc.)

Grading scale: A = 90+, B = 80-89, C = 70-79, D = 60-69, F = 0-59.

In order to get a passing grade in the class you must get a passing grade on the exam part (midterm and final).

The "bonus factor" will be applied to determine border cases but only in student's favor (e.g., you will *not* fail with a total of 60 but you may get an A with a score of 89).

Additional requirements will be placed on programming assignments for graduate students.

Graduate credit:

As an extra requirement, graduate student must complete at least 20% in extra points on the programming project. In other words, a perfect ***A*** score for the project is 100 for undergrads and 120 for graduate students.

Attendance:

As per university policy, all students are expected to attend all class meetings. Experience & statistics show a strong correlation between high grades and regular attendance. (However, regular attendance by itself does not automatically mean a high grade.)

Assignments:

Expect to be busy with assignments—most of the time there will be an outstanding assignment of some kind so plan accordingly. You will have sufficient time to complete each assignment and (save for hurricanes & other emergencies) you should consider the due date to be a ***hard deadline***.

No late assignments will be accepted. If you believe that you have some extenuating circumstances talk to me early and as much in advance *before* a deadline as possible – last minute requests are strongly discouraged.

Academic dishonesty (cheating):

Don't do it! If you get caught the consequences are very unpleasant. Make sure you understand everything that you have submitted because you may be asked to explain it in case there are similarities that look less than accidental.

Cheating is:

- Copying, in whole or in part, the solutions of former students, current students, or any other human being, alive or dead. "Copying" includes transmission through email, the Web, smoke signals, or any other means.
- Obtaining solutions from the Internet or other archival sources.
- You are not allowed to even *look* at a solution.

Discussing assignments at a high level for clarification, discussing problems concerning the computing equipment, and studying in groups for examinations is not cheating, but every word you type for programming and written assignments must be your own!

If you have any questions about acceptable teamwork - ask.

Special cases:

If you have any special circumstances (disabilities, active/reserve member of the armed forces, sports team member, family matters etc.) talk to me privately ***within a week***. If circumstances arise during the semester inform me ASAP.

Privacy:

The general university policy is that your grades and personal information are confidential—I will discuss them with you ***only*** in one-on-one basis.

If you are asking for make-up test or late submission due to a medical condition you should get a note from a doctor. The note does **not** need to give the exact diagnosis but only state how it affects your ability to participate in the course.

How to succeed in this class:

- Read the assigned topic from the book *before and after* the class. This is a requirement and your response to questions will affect the "bonus factor" of your grade.
- Take advantage of the PDF slides to save effort in taking notes.
- Pay attention and participate in the class discussions. If you plan on snoozing in class you should consider taking rest in bed instead.
- If you don't understand something get help ***early***.
- Start work on assignments/homeworks ***early***.
- Come to office hours prepared with ***specific*** questions.
- Be honest with yourself and study at home – the university expects you to put in about **9 hours** of preparation per week for this class for a **C** grade.
- Start work on assignments/homeworks ***early***.