

CS 326: Computer Security

Spring 2023

Instructor: Michael P. Rogers
Office: Halsey 214
Office Hours: MWF 2:00-3:30 PM, Tu 3:15-4:00 PM, Other Hours By Appointment
Email: rogersm@uwosh.edu
Phone: 920-424-1388 / 309-825-6454

Class Times: TR 1:20-2:50 PM, Halsey 208
Credits: 3

Description: This course is an introduction to computer security with an emphasis on software design principles and technical controls that help secure computer systems. After discussing foundational concepts in information security and assurance (e.g., the CIA triad, authentication, nonrepudiation, threats, attack vectors, risk assessment, security controls, plans, and policies), we will delve into the following topics: principles of secure software design and defensive programming, authorization and access control, and cryptography.

Prerequisites: A grade of C or better in Computer Science 212 and Computer Science 271

Course Website: if it happens in this course, it will be posted on UWO's [Canvas](#) site. [Set up notifications](#) to be alerted when announcements are posted, new assignments, quizzes, or notes are posted and graded, etc.

Required Textbook: None: multiple online references will be provided on Canvas.

Course Outcomes :

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

1. Analyze the tradeoffs of balancing key security properties (e.g., confidentiality, integrity, and availability)
2. Describe the concepts of risk, threats, vulnerabilities and attack vectors, authentication, authorization, access control
3. Describe the following principles of secure design: principle of least privilege and isolation, principle of fail-safe and deny-by-default, end-to-end data security, and principle of complete mediation
4. Discuss the benefits of having multiple layers of defense
5. Identify the different roles of prevention mechanisms and detection/deterrence mechanisms
6. Discuss the limitations of malware countermeasures (e.g., signature-based detection, behavioral detection)
7. Identify instances of social engineering attacks and denial of service attacks
8. State the purpose of cryptography and describes several ways to use it in data communications
9. Explain how public key infrastructure supports digital signing and encryption
10. Explain how key exchange protocols work and how they fail
11. Discuss cryptographic protocols and their properties
12. Describe real-world applications of cryptographic primitives and protocols
13. Appreciate the dangers of inventing one's own cryptographic methods

Grading Criteria:

Category	%
Exams (4)	55
Homework	20
Assignments (\approx 4)	25

Grade Scale:

%	≥ 92	90-92	88-90	82-88	80-82	78-80	72-78	70-72	68-70	62-68	60-62	< 60
Letter	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F

Grade Disputes: If there is a mistake in your grade (an inappropriate assessment, math mistake, etc.), you must let your instructor know **within 1 week** of when the assessment was returned if you wish it to be regraded.

Exam Dates (tentative, subject to change):

Exam 1 - Week 4
Exam 2 - Week 7
Exam 3 - Week 11
Exam 4 - Week 14

Late Policies: Douglas Adams once said, "I love deadlines: I love the whooshing sound they make when they fly by". Hopefully you'll agree with the first part, and never have to experience the second. To encourage the latter, in this course exams and quizzes must be taken at the designated times, and late assignments will not be accepted, unless you have an excused absence:

1. illness - a note a medical professional or Dean of Students Office will be required
2. death in the family - send me a link to the obituary as proof
3. UWO excused activity - get your professor / coach to send me a letter
4. weather - you will get one day's credit for each day the university is officially closed

Absences: It has been scientifically proven that the most significant factor for predicting student success is attendance (although whether this is truly causation or merely correlation is another question). Students should attend each and every class, and notify the instructor ahead of time if you will be absent. Attendance may be taken and factored into the Participation category.

Academic Integrity: The purpose of this course is to broaden your knowledge of computer security, and more importantly teach you how to think systematically about a problem, how to *problem solve*. For that reason, the work that you turn in must be your own. Note that the goal here is not to force you to work in a complete vacuum: you may have *general* conversations with students to clarify the nature of an assignment, and you can ask for help with debugging, but that second-set-of-eyes-student should not be looking at their code while they assist you.

Sometimes students are unaware of whether or not they have committed plagiarism, but here are some tips:

1. if your problem solving begins with ctrl-C and ends with ctrl-V, you have committed plagiarism.
2. if your problem solving starts at Google and ends at Chegg, you have committed plagiarism.
3. if your problem-solving involves surreptitiously glancing at the exam of the student next to you and doing a *virtual* copy-and-paste, you have committed plagiarism.
4. if that tiny voice inside your head, the same one that inconveniently shuts up entirely while you are working on a tricky assignment, starts making "ahem" noises, you have committed plagiarism.

Let us consider the pros and cons of committing plagiarism.

Pros:

1. You have completed the assignment. Rah!

Cons:

1. You will have missed that exhilarating, ego-boosting, delicious "aha!" moment that everyone experiences when they have, on their own, solved a difficult puzzle.
2. You will be caught, receive a 0 on the assignment/exam, and may face disciplinary action in front of a bevy of grim-faced administrators who you do *not* want to meet.
3. You won't *know* anything!

So what do you do when you can't solve a problem? The answer is simple, ask your instructor (or lab assistant) for help. We will use the time-tested Socratic method, asking questions that will lead you to the correct answer. Failing that, just write "I have no idea" in bold letters in the comment block at the top of the assignment, turn it in, and you will gain *some* points (more than 0).

Exams and quizzes are to be done entirely on your own. These are closed book, closed notes, because this material is so absolutely fundamental that you **must** have it at your fingertips. See the Dean of Students Office web page [for more information](#).

Also, for an even more detailed discussion of what constitutes academic misconduct, please see the discussion of [UWS Chapter 14, Student Academic Disciplinary Procedures](#).

Accessibility: Your instructor is committed to ensuring a fair playing field. If you have a disability and need assistance (e.g., a note taker, certain seating, extra time to take tests, adaptive technology, etc.), please register with the Accessibility Center, and we work hard to accommodate your needs.

Non-discrimination and Anti-harassment: Your instructor is committed to maintaining a harassment-free, welcoming classroom, and to that end will not tolerate discrimination on the basis of race, religion, creed, color, sex, gender, identity/expression, ancestry, national origin, age, marital status, preferences in streaming services (just snuck this in to see if anybody's reading :-), relationship to other employees, sexual orientation, disability, veteran's status, membership in the military, arrest/conviction record, political affiliation, or any other protected status.

Feedback: Your instructor thrives on feedback. If a concept doesn't make sense, ask, and if the answer didn't make sense, ask again! There are no stupid questions (and any stupid answers are my responsibility 😊). It may seem intimidating to put yourself out there and admit that you don't understand something, but:

1. if you didn't understand something, there is a good chance that your peers didn't either, and they will (silently, or better yet, by banging on desks like they do in parliament) applaud your act of inquiry
2. you needn't worry about "slowing down the class". Learning never slows down anything.
3. your instructor is intimately familiar with being in situations where things don't make sense: you will receive a very sympathetic hearing.

If you do feel uncomfortable asking in class, please inquire during office hours or on our Discord server.

Consumer Protection Required Disclosure: Students are advised to see the following URL for disclosures about essential consumer protection items required by the Students Right to Know Act of 1990: <https://uwosh.edu/financialaid/resources/consumer-information/>