Computer Security
CS 326 - Spring 2020
Credits: 3 hours

Instructor:	David Furcy
Email:	furcyd@uwosh.edu
Office:	Halsey 221
Office Hours:	MWF 1:40 - 2:40 PM, TuTh 12:30 - 2:00 PM, or by appointment
Class Meetings:	TuTh 9:40 - 11:10 AM in HS 309
Prerequisites:	A grade of C or better in CS 212 and CS 271
Class Web Page:	**Canvas**
Tests:	There will be a midterm around week 7 and a final. Each exam date will be announced in class and on Canvas at least one week before the exam.

Course 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, non-repudiation, 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.

Topic Coverage

- Confidentiality, integrity, availability (i.e., the CIA triad), authentication, authorization and access control
- Trust, risks, threats, vulnerabilities and attack vectors, malware (e.g., viruses, worms, spyware, botnets, Trojan horses or rootkits), denial of service attacks, social engineering
- Principles of secure design, such as least privilege, fail-safe defaults, defense in depth, economy of mechanism, prevention, detection, and deterrence
- Buffer overflows
- Cryptography terminology and basic concepts:
  - Communication channel characteristics, attacker capabilities, encryption, decryption, keys, signatures
  - Cipher types and common attack methods
  - Public Key Infrastructure support for digital signature and encryption and its challenges
- Cryptographic primitives
  - Pseudo-random generators and stream ciphers
  - Block ciphers, such as AES
  - Cryptographic hash functions

    - Message authentication codes
- Symmetric-key cryptography
- Public-key cryptography

Learning Outcomes

Upon completion of this course, the student will be able to:

- Analyze the tradeoffs of balancing key security properties (e.g., confidentiality, integrity, and availability)
- Describe the concepts of risk, threats, vulnerabilities and attack vectors, authentication, authorization, access control
- 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
- Discuss the benefits of having multiple layers of defense
- Identify the different roles of prevention mechanisms and detection/deterrence mechanisms
- Discuss the limitations of malware countermeasures (e.g., signature-based detection, behavioral detection)
- Identify instances of social engineering attacks and denial of service attacks
- State the purpose of cryptography and describes several ways to use it in data communications
- Explain how public key infrastructure supports digital signing and encryption
- Explain how key exchange protocols work and how they fail
- Discuss cryptographic protocols and their properties
- Describe real-world applications of cryptographic primitives and protocols
- Appreciate the dangers of inventing one's own cryptographic methods

Accommodations: The University of Wisconsin Oshkosh supports the right of all enrolled students to a full and equal educational opportunity. It is the University's policy to provide reasonable accommodations to students who have documented disabilities that may affect their ability to participate in course activities or to meet course requirements.

Students are expected to inform instructors of the need for accommodations as soon as possible by presenting an Accommodation Plan from either the Accessibility Center, Project Success, or both. Reasonable accommodations for students with disabilities is a shared instructor and student responsibility.

The Accessibility Center is part of the Dean of Students Office and is located in 125 Dempsey Hall. For more information, email accessibilitycenter@uwosh.edu, call 920-424-3100, or visit the Accessibility Center Website.

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/consumer-information/

Course Grading Policy

Your final grade for this course will be based on three components: frequent quizzes, homework (programming or written) assignments, and exams. Your overall numerical grade for the course will be computed as the weighted sum of the component grades using the following weights:

Component	Weight
Quizzes (all equally weighted)	10%
Homework assignments (all equally weighted)	40%
Exams (both equally weighted)	50%

Finally, your letter grade for the course will be computed as follows:

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

While this overall grading scheme is fixed, I will be happy to discuss any issue you may have with individual grades. If you notice a mistake or have a question regarding a specific grade, please come and talk to me *as soon as possible*. Do not wait until the end of the semester to bring up grading issues. Also, I will *not* be available to discuss grades after the end of the final week.

Attendance and Participation

You are expected to not only attend **every** class meeting but also to come **prepared** for and **participate** actively in it. Necessary preparation requires you to have studied and assimilated the material covered in previous sessions, to have met with me outside of class to discuss any questions you may have, to have completed the reading assignments (there will be a significant amount of reading to complete before each class), and to have completed the homework assignments on time. **It is hard to imagine how a student could do well in this course while missing classes or attending them unprepared.** On the positive side, I have high expectations for my students and will always support and encourage you. I **strongly encourage you to ask any question** or raise any issue you have with the course either during class or in my office hours. I will also gladly meet with you by appointment. Send me email to make an appointment. While I will meet with you as soon as my schedule permits, do not expect me to be widely available just before an exam or the due date for an assignment since you may not be the only one needing help at the last minute.

Late Submissions

I will describe the submission procedure for your assignments when the time comes. However, let me point out right away that each one of them will come with a deadline (day and time) after which any submission will be considered late.

The late-submission policy works as follows:

Turned in	Penalty
On the due date but after the deadline	30%
The day after the due date	60%
More than one day after the due date	100%

Note that assignments that are two or more days late receive no points. **Weekend days and holidays count as "regular days" when computing late penalties**. Each (late) day starts precisely at midnight. So, each one of the following timestamps: 12:00:00 AM, 12:00:01 AM, etc., is considered to be “the next day.” Extensions on assignments may be granted at the discretion of the instructor if you provide a valid justification (in the form of a written excuse from a medical doctor or the Dean of Students Office) before the due date. Late submissions can easily be avoided by starting to work on the assignment right away and asking for help early if you get stuck.

If you miss a scheduled exam, you **may** be able to take a make-up exam provided you give the instructor a valid justification (see above), ahead of time if possible. Only one make-up exam will be given. It will be a comprehensive exam scheduled at the end of the semester. If you miss a quiz, you **may** be able to take a make-up quiz, provided you give the instructor a valid justification (in writing) for your absence.

Collaborating versus Cheating

While it is acceptable to discuss the problem statement, premises, goals, constraints, etc., of the assignments with others, you must submit your OWN work EXCLUSIVELY. You may not “borrow” any piece of code or design or written answer of any length from anybody else, unless you can live with a zero and the other potential academic sanctions of cheating (see the UWO Student Discipline Code - Chapter UWS 14).

In conclusion, remember that computer science classes require a lot of work in addition to active participation in class. It takes considerable practice to develop the technical and analytical skills targeted by this course. You will need to spend **at least (and typically much more than) three hours of effort outside of class for each in-class hour**. Having said this, I expect every hardworking student to do well in this course.

Have fun this semester and good luck!