CS 326 – Computer Security
Fall 2018

Instructor: Justin Miller **Email:** millerju@uwosh.edu **Class:** Clow Lab

Class information: 5:10 PM to 8:10 PM Wednesdays
Office hours: 8:10 PM to 9:10 PM Wednesdays (in classroom)

Prerequisites: CS 221 and CS 271 with a grade of C or better.

Course website: http://www.uwosh.edu/d2l. You should check d2l on a regular basis as it will contain any lecture notes, handouts, assignments, announcements, and grades. I'll do my best to let you know when something new and important comes up, but it is your responsibility to check the web site frequently for information that you might not get otherwise.

Required textbook: NONE

Note: If you have special needs, please come and talk to me at the end of the first class.

Course description: This 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, we will delve into the follow topics: principles of software design, authorization, access control, encryption, social engineering, exploitation, detection, and malware.

Course grade: Your final course grade will be based on the following components:

Component	Weight
Exams (2)	60%
Assignments (10)	20%
Readings (10)	10%
Quizes (10)	10%

Grading will be on a plus/minus system. Grading *may* be done on a curve depending on the overall performance of the class. If no curve is used, your grade will be computed based on the following:

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

Exams: Exam material will come from the lecture notes, quizzes and assignments. There will be more information about each exam as it approaches.

If you are unable to take a scheduled exam, it may be possible to take a make-up exam provided that you do both of the following, which are then subject to my approval:

1. Make arrangements prior to the scheduled exam. **No after-the-fact notifications will be accepted.**
2. Have a written medical excuse signed by the attending physician OR have a note of justification from the Dean of Students Office.

Assignments: All assignments must be submitted electronically via d2l. It is your responsibility to ensure that your assignment was submitted correctly. You must double check to ensure your assignment was uploaded correctly.

No late submissions will be accepted.

Academic Dishonesty: Academic dishonesty of any kind will not be tolerated. All assignments, quizzes and exams are to be completed individually. While discussion of ideas and problems with fellow students is encouraged, all projects must be done individually. In certain circumstances, code fragments from the instructor may be provided to eliminate tedious coding or to provide a common framework for all students. All other code must be original. Online resources may be used to help you understand the material, but you may not copy online code nor can you "borrow" code from other students, past or present. For group assignments, each group must submit original work.

Any suspected academic dishonesty will be dealt with on a case-by-case basis. Any clarification of what does or does not constitute academic dishonesty must take place *before* you turn in questionable work. For clarification on what constitutes academic dishonesty, contact me or consult the printed policy in the UWO Student Discipline Code, Chapter UWS 14.

Topic Coverage:

- Confidentiality, integrity, availability, authentication, authorization, and access control
- Trust, risks, threats, vulnerabilities, attacker vectors, malware, denial of service, social engineering
- Principles of secure design, least privilege, fail-safe defaults, defense in depth, prevention, detection
- Encryption, Decryption, Hashing
- SQL Injection, Cross-Site Scripting, Buffer Overflow, Phishing, Macros, Powershell, Living off the land
- CIS Top 20, OWASP Top 10, PCI, SOX, NIST, Compliance, Patching, CMDBs, ITIL, Change Control
- Red Team, Blue Team, SOCs, Penetration Testing, SIEMs, Malware Analysis
- Security Departments/Teams, Security Awareness, Insider Risk, Incident Response, Architecture

Learning Outcomes:

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

- Analyze the tradeoff of balancing key security properties
- Describe risk, threats, vulnerabilities, attack vectors, authentication, authorization, and access control
- Describe principles of secure design
- Discuss the benefits of having multiple layers of defense
- Discuss the limitations of malware detection
- Identify the roles of prevention & detection
- Identify instances of social engineering and denial of service attacks
- State the purpose of cryptography and well known protocols