

Course Syllabus

CMPS 4510 - Vulnerability Analysis Sections 1 and 2 - Fall 2022

Instructor and Contact Information

Instructor: Dr. Melissa Danforth

Virtual Office Hours: MWF 11:00am to 12:00pm (noon) on Slack, Discord, and email (Zoom only available by appointment)

In-Person Office Hours: MW 5:30pm to 6:30pm in Science III 319 (immediately following lecture for this class)

Appointments: You may also schedule an appointment outside of these times. Email me to set up an appointment.

Email: melissa@cs.csub.edu or mdanforth@cs.csub.edu

Class Information

Course website: <https://cs.csub.edu/instructure.com/courses/19827>
(<https://cs.csub.edu/instructure.com/courses/19827>)

Course meets MW 4:00-5:15pm (lecture) in Science III 240 and Tu 4:00-6:30pm (lab) in Science III 315

Virtual attendance is also available via Zoom. See the Zoom link and invitation posted under [General Course Information](#) (<https://cs.csub.edu/instructure.com/courses/19827/modules/151764>) on Canvas

Attendance is NOT REQUIRED for this course. Lectures and lab demos will be recorded and posted to Knowmia, barring any unforeseen technical difficulties. Slides will also be posted to Canvas.

In general, the meeting days will be focused on the following:

- Mondays: Lectures will primarily be on textbook materials from the reading assignments, as well as reviews of prerequisite course materials.
- Tuesdays: The review of the lab requirements and lab demos will be recorded. You can attend during the lab time either in-person or virtually and receive help from me after the demo is completed. You can also opt to do the labs on your own time and get help via email or office hours.
- Wednesdays: Lectures will primarily discuss any timely security compromises that happen during term and/or past security compromises related to the week's reading assignment. In "slow" weeks, lectures will be focused on textbook materials and/or review materials.

For those attending virtually, webcams will not be required. I have also configured Zoom to allow phone call-ins and to mask phone numbers for those who have to call in to attend.

Videos of the lectures and lab demos will be posted to Knowmia after processing and automatic closed-captioning. Give at least a couple of days for that to occur.

Catalog Description

Identification and quantification of security weaknesses, primarily in source code and executables. Topics include professional ethics, source code auditing, common source code errors, the runtime stack and memory systems, common attacks against executables, risk assessment, vulnerability classification, static binary analysis, and mitigation techniques.

Catalog Prerequisites: CMPS 2240/224 and CMPS 3350/335 or 3500/350.

Prerequisites by Topic

- Knowledge of assembly language (preferably Intel x86 64-bit)
- Knowledge of programming languages in C/C++ family
- Understanding of computer language translation from source code to binary
- Knowledge of the basic memory structure (runtime stack, heap, etc.)

Units and Contact Time

4 semester units. 3 units lecture (150 minutes), 1 unit lab (150 minutes).

Class Expectations

As a 4000-level elective course, students are expected to engage in independent learning in this course through reading assignments, case studies, and lab assignments. Critical thinking, independent evaluation, and troubleshooting are important traits for the cybersecurity profession.

Lectures assume that you have completed the reading assignments and will focus on exploring examples and scenarios, including more modern examples and scenarios, related to the topics of the week. Case studies will also analyze more modern examples of vulnerabilities than the examples contained in the textbook.

Note that the standard expectation for a 4-unit course is that you'll spend 6-10 hours per week outside of class meetings working on course assignments and studying for the course. Please plan appropriately. Also note that more time may be required in some weeks.

Class Principles


The following principles will guide this course:


- *Communication*: I understand if something unexpected has come up that interferes with your course work. Please communicate with me as soon as possible though, so we can discuss extensions and other options for moving forward in the course. Similarly, should something come up unexpectedly in my life that affects a class meeting, I will let the course know by Canvas announcements, Slack announcements, and email. Please keep the lines of communication open.
- *Respect*: There are many situations in cybersecurity where differing, but equally valid, opinions may exist. Respect the rights of others to form different opinions and conclusions than your own.
- *Critical Thinking*: While there may be some rote assignments in this course, many assignments will require applying critical thinking and analysis skills. My grading approach for those "thinking questions" is more about seeing your thought process than seeking "perfect" answers. It is also okay to state what you don't understand in an assignment submission. That is all part of the learning process.
- *Compassion*: Remember that other people in the class (and me) are balancing many competing priorities beyond this course. Exercise compassion, kindness, and consideration when interacting with others.

Type

Selected elective for CS

Required Textbook

The required and recommended textbooks for this course are freely available through the CSU O'Reilly Safari Tech Books subscription. To access that subscription, first log in to Safari with the following link: <https://go.oreilly.com/california-state-university-bakersfield/>  (<https://go.oreilly.com/california-state-university-bakersfield/>). Then select the textbook links to load the e-book. If you forget to log in, you'll just get a summary instead of the e-book when you select a link.

The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities. Mark Dowd, John McDonald, Justin Schuh. Addison-Wesley, 2007, ISBN-13: 978-0-321-44442-4. O'Reilly link: <https://learning.oreilly.com/library/view/the-art-of/0321444426/>  (<https://learning.oreilly.com/library/view/the-art-of/0321444426/>).

Recommended Textbook and Other Supplemental Materials

Computer Security: Art and Science, 2nd edition. Matt Bishop. Addison-Wesley, 2019, ISBN-13: 978-0-321-71233-2. O'Reilly link: <https://learning.oreilly.com/library/view/computer-security-art/9780134097145/>  (<https://learning.oreilly.com/library/view/computer-security-art/9780134097145/>). Author's website: <http://nob.cs.ucdavis.edu/book/>  (<http://nob.cs.ucdavis.edu/book/>).

Supporting articles and current events relating to the course will be posted on Canvas and Slack.

Coordinator(s)

Melissa Danforth

Student Learning Outcomes

This course covers the following ACM/IEEE CS2013 (Computer Science) Body of Knowledge student learning outcomes:

- CS-IAS/Foundational Concepts in Security
- CS-IAS/Principles of Secure Design
- CS-IAS/Defensive Programming
- CS-IAS/Threats and Attacks
- CS-PL/Static Analysis
- CS-SE/Software Construction

ABET Outcome Coverage

The course maps to the following student learning outcomes for Computer Science (CAC/ABET):

- 1. An ability to analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.**
- 4. An ability to recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.**

Lecture Topics and Rough Schedule

Week	Chapter	Topics
1	Chapter 1	Professional ethics, Classic security goals (confidentiality, integrity, etc.), Threats and threat exposure, Vulnerability categories, Audit overview
2	Chapter 2	Assembly refresher from CMPS 2240, Design reviews, Fundamental design flaws, Threat modeling
3	Chapter 3	Operational review, Attack surfaces, Hardening
4	Chapter 4	Review/Audit process, Audit strategies
5 to 7	Chapter 5	Memory corruption: buffer overflows, heap overflows, global and static data, shellcode, protection mechanisms
8	Not in book	Important programming language design topics from CMPS 3500

9 and 10	Chapter 6	C/C++ language issues, Expression evaluation, Type conversions, Common mistakes
11	Chapter 8	String handling issues, String encodings, Metacharacter handling and injection issues, String functions, Hex encoding
12 and 13	Chapter 7	Auditing techniques for source code and binary analysis
14	Chapter 9	Common Unix/Linux issues
15	Not in book	Hardware vulnerabilities (Spectre, Meltdown, etc.)

Specific reading assignments for each week with links to the appropriate chapters in the textbook are posted on Canvas.

Attendance

Attendance is NOT REQUIRED for this course. The topics covered in lecture and slide decks from the class session will be on Canvas. Recordings of the classes will be posted to Knowmia after processing. If you cannot attend, it is your responsibility to watch the videos and review the slide decks.

Course Academic Integrity Policy

Lab assignments may be optionally completed in groups. For a group lab assignment, one person in the group can turn in one submission for the entire group, but make sure everyone's name is on the submission so all members of the group receive credit for the assignment.

All other assignments are individual assignments. That means you may discuss the assignments with one another, but each student must turn in their own work in their own words. It is also okay to reference external sources in your submission, but you must appropriately paraphrase that source by expressing the information you researched in your own words.

For example, you cannot copy-and-paste from a website or copy another student's submission, but you can refer to that website and summarize what you've learned, or summarize your discussion with the other student. I even encourage you to add questions you still have, and, if I have time during grading, I'll try to customize my grading comments to answer those questions.

In summary, no direct copying from any source (other students, external sources, textbook, etc.) is allowed. Instances of direct copying that are detected may be referred to the Dean of Students as an academic integrity violation.


Campus Academic Integrity Policy

Certain forms of conduct violate the university's policy of academic integrity and the student conduct code. Academic dishonesty (cheating) is a broad category of actions that use fraud and deception to improve a grade or obtain course credit. Academic dishonesty is not limited to exams alone but arises whenever students attempt to gain an unearned academic advantage. Plagiarism is claiming the published or unpublished work of someone else as your own. This includes handing in someone else's work; turning in copied or purchased compositions; using paragraphs, sentences, phrases, words, or ideas, including paraphrasing, written by another writer; or using data and/or statistics compiled by someone else as your own without giving appropriate credit to the original writer. Plagiarism also includes using your work submitted in another class without permission of your current instructor.

When a faculty member discovers a violation of the university's policy of academic integrity, the faculty member will meet with the student(s) involved and is required to notify the Dean of Students' office and detail the alleged violation, including the name(s) of the student(s) suspected, the class in which the alleged violation occurred, the circumstances of the alleged violation, and the evidence (including witnesses) supporting the allegation. The faculty member will also formally notify the student(s) suspected of violating the university's policy of academic integrity, the department chair for the course involved in the incident, and the appropriate school dean. The Dean of Students or designee will investigate; confer with the faculty member, student(s), and any witnesses identified; and review all evidence submitted by the faculty member and student(s) to impose an administrative sanction, beyond the academic penalty already placed by the faculty member. Students who perform dishonestly in this course may earn zero credit on the assignment/exam or a failing grade in the course, depending on the level of severity of the offense.

Students are expected to uphold the standards of academic integrity. Cheating in any form will not be tolerated and will result in a formal report to the University Dean of Students. You are always expected to follow the student conduct code and uphold the CSUB Guiding Principles while learning on this campus.

Academic Accommodations

To request academic accommodations, please contact the Office of Services for Students with Disabilities (SSD) and either email me or bring me an accommodations letter from the SSD Office. Policies from the SSD Office relating to accommodations, such as scheduling policies for using their testing center, must also be followed. For more information about the services and policies of the SSD Office, contact their staff by email and/or visit their website at <https://www.csub.edu/ssd/>  (<https://www.csub.edu/ssd/>)

Basic Needs Assistance

If you are experiencing challenges related to basic needs, such as food insecurity, housing insecurity, or other challenges, there are resources available to you.

The campus Food Pantry, located next to the Student Union, is open and available to all students, staff, and faculty. Please visit the Food Pantry website for hours and information at

<https://www.csub.edu/basicneeds/food-pantry> ↗ (<https://www.csub.edu/basicneeds/food-pantry>)

Information about food distributions, CalFresh, and other food resources can be found at

<https://www.csub.edu/basicneeds/food-security> ↗ (<https://www.csub.edu/basicneeds/food-security>)

Information about food assistance at the Antelope Valley campus is at

<https://www.csub.edu/basicneeds/resources-students-csub-av-campus> ↗

(<https://www.csub.edu/basicneeds/resources-students-csub-av-campus>)

The campus also has emergency housing available for full-time students on a first-come, first-served basis. For housing concerns, please contact Jason Watkins, Assistant Director for Basic Needs, at 654-3360 or Ashley Scott, the Assistant Director of Housing. You can find more information about housing assistance and contact information at

<https://www.csub.edu/basicneeds/housing-stability>

↗ (<https://www.csub.edu/basicneeds/housing-stability>)

More information on basic needs assistance is on the Basic Needs website:

<https://www.csub.edu/basicneeds> ↗ (<https://www.csub.edu/basicneeds>)

Health and Well-Being

This continues to be a trying time mentally, physically, and with work / life balance issues. If you need additional time for assignments due to your current situation, please contact me to discuss the options available to you. Similarly, should something come up unexpectedly in my life that affects a class meeting, I will let everyone know through email / Slack / Canvas.

The CSUB Counseling Center has both regular-hours and after-hours counseling services available. Call 654-3366 to connect with their services. After their normal operating hours, you can press 2 at any time to connect to the after-hours service. More information is at

<https://www.csub.edu/counselingcenter/> ↗ (<https://www.csub.edu/counselingcenter/>)

CSUB's Student Health Services is available for basic health care needs, at little to no cost for CSUB students. You can find more information about their services at

<https://www.csub.edu/healthcenter/> ↗ (<https://www.csub.edu/healthcenter/>)

Current information about CSUB's COVID-19 plans, policies, and resources can be found at

<https://www.csub.edu/covid-19> ↗ (<https://www.csub.edu/covid-19>)

Technology Assistance and Software

If you need help with technology, such as a loaner laptop and/or hotspot, ITS has programs to provide technology assistance to students. Go to the following ITS webpage to learn more about their programs: <https://its.csub.edu/step> ↗ (<https://its.csub.edu/step>)

The CEE/CS Department has academic software subscriptions available to students enrolled in CMPS and ECE courses. This currently includes Microsoft, VMware, and Mathematica. Go to the following page for more information: <https://www.cs.csub.edu/downloads.php> ↗
(<https://www.cs.csub.edu/downloads.php>)

CSUB ITS also many software products available to students through the Virtual Computer Lab (VCL). You will need to use your myCSUB credentials to access VCL. To see the full list of software and to access VCL, go to <https://its.csub.edu/VCL> ↗ (<https://its.csub.edu/VCL>)

Grading Categories and Weights

- Reading Quizzes: 10%
- Laboratory Assignments: 25%
- Case Studies: 25%
- Exams (Midterm and Final): 40%

Grades are posted on Canvas. It is your responsibility to check your Canvas gradebook and read any comments I've attached to your graded assignments.

Late Policy

Canvas is configured to record a 0 grade if an assignment is not received by the due date. Late policies for specific assignment categories are:

- Reading Quizzes: You may attempt most reading quizzes for about two weeks after the due date (see Canvas's availability window for specific dates) with no late penalty. If you do not attempt a quiz within 2 weeks after the due date, you will need to contact me to request an extension.
- Labs and Case Studies: Assignments may be submitted late through December 6th at 11:59pm. Assignments turned in more than 2 weeks late will be assessed a 10% late penalty for every 3 weeks they are late. For example, if you turn the assignment 1 week after the deadline, there will be no late penalty. If you turn an assignment in 4 weeks after the deadline, there will be a 10% late penalty. If you turn the assignment in 6 weeks after the deadline, there will be a 20% late penalty.
- Exams: Contact me if you are unable to take an exam during the availability window for that exam.

Reading Quizzes

Quizzes are on the reading assignments from the textbook. Canvas will automatically grade the quiz when it is submitted, and you may attempt the quiz as many times as you want. The attempt with the highest grade will be recorded in the gradebook.

The lowest quiz grade will be dropped from the overall course grade calculation.

Laboratory Assignments

Lab assignments will be posted on the course website with their due dates. Partial credit will be given for incomplete labs.

You may work on labs in groups of up to 3 students. If you work in a group, only one student needs to submit the assignment, but make sure to put everyone's names on the assignment each week. Only the students whose names are on the assignment will get credit for the lab. If you are in a group but are not the one submitting the assignment to Canvas, you may submit a comment indicating who did submit the assignment for your group.

The lowest two lab grades will be dropped from the overall course grade calculation.

Case Studies

Case studies and their due dates will be posted on the course website. Partial credit will be given for incomplete submissions.

Case studies may be discussed with others in the class, but every student must turn in their own assignments in their own words. Copying from other students, the Internet, previous solutions, the textbook, etc. are all considered violations of the Academic Integrity Policy.

I expect students to perform their own analysis of the provided articles. Case studies are a vital part of this course to give more recent information about vulnerabilities and to gauge your ability to learn from, and analyze, technical articles. If you are having any difficulty the case studies, or if you would like to discuss the case studies in more depth, please see me during office hours.

The lowest case study grade will be dropped from the overall course grade calculation.

Assignment Submission Guidelines

Assignments must be submitted to Canvas. Due to high email volumes and issues with the spam filter, I do not accept assignments submitted through email.

Most assignments have been configured to take a wide variety of submissions, such as documents, images, text fields, and audio/video files. See each individual assignment for any specific formats required for your submission.

If you have drawn something out by hand, take a picture or use a scanner to convert it to an image or document. Please make sure the image is legible.

If you have any difficulties submitting to Canvas, contact me or ITS for help.

Midterm

The midterm exam is a "quiz" assignment on Canvas during Week 8 of class. It will be available on Canvas from 12:01am Sunday October 9, 2022 to 11:59pm Tuesday October 11, 2022. There will be no lecture on Monday October 10th or lab on Tuesday October 11th so you can focus on the midterm exam.

If you have any connectivity, power, or technology issues that cause you to lose connection to Canvas during the exam window, contact me as soon as possible.

It is your responsibility to log in to Canvas and take the midterm during the availability window. If you miss the midterm and you believe you have a valid university excused absence, contact me as soon as possible to discuss the situation.

Final

The campus official final exam time slot is Monday December 12, 2022 from 5:00-7:30pm. The final exam is also a Canvas "quiz" assignment and will be available from 12:01am on Sunday December 11th to 11:59pm on Tuesday December 12th.

If you have any connectivity, power, or technology issues that cause you to lose connection to Canvas during the exam window, contact me as soon as possible.

It is your responsibility to log in to Canvas and take the final during the availability window. If you miss the final and you believe you have a valid university excused absence, contact me as soon as possible to discuss the situation.

Prepared By

Melissa Danforth on 21 August 2022

Approval of Course Outline

Course description and general outline approved by CEE/CS Department in Spring 2014
Effective Fall 2016