CIS 258 01 – Introduction to Cybersecurity

Grand Valley State University – School of Computing – Winter 2024

Instructor	Contact Info	Office Location	Office Hours
Dimitrios Melissourgos	melissod@gvsu.edu 352 278 6777	MAK D-2-232	Monday 2:15pm-3:15pm Tuesday 2:15pm-3:15pm Wednesday 2:15pm-3:15pm Friday 2:15pm-3:15pm

Course Description

General Information

This course provides an introduction to all aspects of cybersecurity principles and technologies. Fundamental topics include cyber threats and vulnerabilities, information security frameworks, network security, cryptography, system defense, information security policy, legal issues, ethical issues and security management. The course includes hands-on learning through experiments, case studies, and projects.

Credits: 3

Grading scheme: Letter grade

Prerequisite: CIS 162 – Computer Science I

Days: Monday, Wednesday, Friday

Time: 10:00am-10:50am

Location: MAK B1116

Course Objectives

At the end of the course, students will be able to:

- Describe the implications of relying on open design or the secrecy of design for security.
- Describe the capabilities and uses of cryptographic and cryptanalysis techniques in the cybersecurity world.
- Explain the various techniques of authentication, authorization, access control, and data integrity.
- Discuss common techniques for system hardening.
- Explain how the security of a system's components might impact the security of the system.
- Summarize the activities that must take place for effective disaster recovery planning.
- Describe common social engineering techniques and their implications for cybersecurity.
- Make presentations on specific cybersecurity topics.

Book

"Principles of Computer Security: CompTIA Security+ and Beyond". Sixth Edition by Wm. Arthur Conklin, Greg White, Chuck Cothren, Roger L. Davis, and Dwayne Williams. McGraw Hill.

Exams and Deadlines

Exam	Date	Time	Location
Midterm 1	Friday, February 16	10:00am-10:50am	MAK B1116
Midterm 2	Monday, March 18	10:00am-10:50am	MAK B1116
Final (Tentative)	Monday, April 22	10:00am-11:50am	MAK B1116

Term Paper	Date	Time	Location
Team registration	Sunday, January 28	Before midnight	Google Forms
Phase 1	Sunday, February 25	Before midnight	Blackboard
Phase 2	Sunday, April 14	Before midnight	Blackboard

Course Schedule (Tentative)

Week	Topic
Week 1	Introduction to cybersecurity
Week 2	Secure design principles
Week 3	Security threats
Week 4	Vulnerabilities and exploits
Week 5	Vulnerabilities and exploits
Week 6	Malicious code and countermeasures
Week 7	Cryptography fundamentals
Week 8	Cryptanalysis fundamentals
Week 9	Spring break
Week 10	Authentication
Week 11	Security controls
Week 12	Security controls
Week 13	Management and Incident response
Week 14	Management and Incident response
Week 15	Legal Issues and Ethics

Grading Policy

Grading Scale

A	≥93%
A-	≥90%
B+	≥87%
B	≥83%
B-	≥80%
C+	≥77%
C	≥73%
C-	≥70%
D+	≥67%
D	≥63%
F	<63%

Assignment / Test	Percentage of Final Grade
Attendance	10%
Homework	40%
Paper / Presentation	20%
Midterm 1	10%
Midterm 2	10%
Final	10%

Attendance Policy

Students are required to attend the class. Sign on sheets will be handed out at 11 randomly selected class meetings. You will receive the full 10% attendance grade if you sign on for 10 out of the 11. You can miss a sign on without penalty. Each additional missing class costs 1%. If you cannot attend a class meeting, you need to notify the instructor **before** the beginning of the class. If you have a serious reason for missing the class (e.g. illness, injury, family emergency, etc.), then you will be excused and you will not lose 1% of the attendance grade. If you notify the instructor of your absence **after** the class has begun, you will be required to provide a doctor's note or similar proof of absence in order to avoid the 1% penalty.

Homework

There will be several homework assignments over the duration of the semester. The due day is one week after the assignment has been given out, unless stated otherwise. Assignments turned in after the due date will receive a 25% late submission penalty per day, including weekends and holidays, with a max of 4 days.

Homework assignments are open-book; you are allowed to use books, notes, slides, search the internet, and discuss with the instructor while completing the work. However, you are not allowed to discuss your assignments with other students or engage in practices that would be considered plagiarism, copying, or cheating. Each student is required to complete homework assignments by themselves.

Paper / Presentation

There is a term paper which can be done individually or in groups of up to 3 people. The term paper has 2 phases:

Phase 1 - Choose a threat/attack/vulnerability/malware and write 500 - 1000 words about its nature and what happened during that incident. Questions you might want to answer are: Which systems got compromised? How did they get compromised (technical details)? Who was affected by the incident? Who was the attacker? What was the magnitude of the damage caused? Does the attack belong to a family/category of attacks? Phase 1 must be completed by Sunday, February 25th. You must present your work to the class the following week, using PowerPoint or similar software. Each presentation will last approximately 5 minutes.

Phase 2 - Expand your term paper by adding another 500+ words on what happened after the incident. Questions you might want to answer are: How long was the vulnerability around before it was exploited? How did people respond to it? What was the technical challenge that caused the vulnerability? Was the vulnerability patched after the incident? Are people still affected by it? Are there any moral/ethical responsibilities tied to the attack? How can we make sure it won't happen again in the future? Phase 2 must be completed by Sunday, April 14th. You must present your work to the class the following week, using PowerPoint or similar software. Each presentation will last approximately 5 minutes. You must include part of your phase 1 presentation to remind us what your topic is.

A list of threats/attacks/vulnerabilities/malware can be found in the first chapter of the book. However, you are free to choose a topic outside of that list. You are also encouraged to choose to talk about a family of attacks (e.g. DDoS) and give us several examples of when such attacks occurred.

You must register your team and your topic by Sunday, January 28th. Alterations to the teams and the topics after that date must be approved by the instructor. All team members must take part in the presentations.

The use of ChatGPT or similar software is prohibited. You must always cite your sources.

Additional Information and Resources

Important Dates

Drop Deadline - Grade "W": March 22nd by 5:00pm

Other important dates: Winter 2024 Academic Calendar

Classroom Protocol

Treat faculty, staff, your fellow students, and university property with respect. Do not use your phone during class. Do not make distractions and be on time for the class meetings. Any regrading requests must be made within a week of the students receiving their grade.

Integrity and Honesty

All students are expected to adhere to the academic honesty standards set forth by Grand Valley State University. In addition, students in this course are expected to adhere to the academic honesty guidelines as set forth by the School of Computing and Information Systems.

Course Evaluation

The end-of-semester course evaluation sites are set up in LIFT and maintained by the Academic Department Coordinator. Course evaluation sites become available to students during the last two weeks of the semester (not exam week), unless specified otherwise.

Disabilities and Special Accommodations

Grand Valley State University strives to provide an inclusive environment across campus that is accessible to all individuals with a diverse range of abilities. As your instructor, it is my objective to facilitate opportunities within all class activities and programs because your success is important to me. If you are encountering difficulties that are interrupting your learning experience, please feel free to make those known to me as soon as possible, as early planning is essential. If you feel that you need accommodations in this course, you must present a memo to me from Disability Support Resources (DSR), indicating the existence of a disability and the approved accommodations. If the class meets in person, you should schedule a meeting with me during office hours to discuss your accommodations. If your class is online or hybrid, please forward your memo to me in an email and schedule a virtual or phone appointment with me to discuss your accommodations. Accommodations are not retroactive. If you have not already done so, please contact the Disability Support Resources office (215 CON) by calling (616) 331-2490 or by email to dsrgvsu@gvsu.edu. You can also visit the DSR website here Disability Support Resources. Please note that I cannot provide accommodations based upon disability, until I have received a copy of the DSR issued memo. Furthermore, if you have a disability and think you will need assistance evacuating this classroom and/or building in an emergency, please make me aware so that the university and I can develop a plan to assist you. All discussions will remain confidential.

GVSU Course Policies

This course is subject to the GVSU policies.

Discrimination or Sexual Misconduct

Grand Valley State University is committed to creating and advancing a campus community where individuals feel empowered to raise concerns, ask for help, and be informed about options before making any decisions. If you become aware of any discrimination or sexual misconduct incident, please report it at the Title IX office.

In Case of Emergency

In Case of Fire: Immediately proceed to the nearest exit during a fire alarm. Do not use elevators.

More information is available on the University's Emergency website.