Central Connecticut State University
CS/CYS 492: Computer Security
Spring 2024

Instructor: Dr. Chad A. Williams, Professor of Computer Science
Office: MS 30309 **e-mail:** cwilliams@ccsu.edu **Phone:** 860-832-2719 (email preferred)
Student Office Hours: https://outlook.office365.com/owa/calendar/CCSUComputerScience@my.ccsu.edu/bookings/

My official student office hours are Monday 12:15 pm - 1:15 pm, Tuesday 12:15 pm - 1:45 pm, and Wednesday 9:00 am – 10:30 am and 12:15 pm – 1:15 pm. However, **be sure to check the link because there are typically more options available that vary by week**. You can drop in anytime during student office hours or schedule an appointment via the link for either an in person or virtual office hours' time slot. Please be aware that while you are welcome to drop in, if someone has made an appointment that appointment has priority, so I encourage appointments to be made via the link. If these times don't work for you, please email me to find a time that will work with your schedule, I will typically need more lead time to rearrange my schedule but I'm happy to work with you to find a time.

Course website: Blackboard
Class: Will be HyFlex giving you the option to attend in person or live virtually, see Blackboard for how to connect. Please be aware the main lecture room in class sessions will be recorded and posted to Blackboard (break out rooms will not be recorded). **For the midterm 3/6 and final exam 5/8 you are required to be in person.**

- CS/CYS 492-01 10:50 – 12:05 Mondays & Wednesdays

Required books: Stamp, Mark. "Information Security Principles and Practice, 3rd ed." Wiley (2022).
Optional books: Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, ISBN: 0-849-38523-7. Available online at: https://cacr.uwaterloo.ca/hac/
Course description: The fundamentals of computer and network security issues are explored. Topics include classical and modern techniques of conventional encryption; algorithms; public-key encryption, and hash functions; network security, with regard to e-mail, IP, and the Web; and system security intruders, viruses, worms, and firewalls. Cross listed as CS 492 and CYS 492. No credit given to students for CS 492 with credit for CYS 492 or vice versa. *Prerequisites: Grade C- or better in both CS 253 and either CS 254 or CET 349, or Permission of Department Chair. CS 501 and CS 502 are prerequisites for graduate students.* 3.000 Credit Hours

Program educational objectives and student outcomes

This course supports the following program objectives and program learning outcomes:

- *PEO-1*: Graduates will apply a broad understanding of the fundamental theories, concepts, and applications of computer science in their career.
  - (ABET SO-1) Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.
  - (ABET SO-2) Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.
- *PEO-4*: Graduates will act ethically and with social responsibility in their careers.
  - (ABET SO-4) Recognize professional responsibilities and make informed judgments in computing practice based on legal and ethical principles.

Course learning outcomes

Program objectives and program learning outcomes are supported by the following course learning outcomes achieved by students upon a successful completion of this course students will have the ability to:

- CLO-1: Apply the basics of how cryptography and cryptanalysis is done and implemented (SO-1, SO-2)
- CLO-2: Evaluate the differences between symmetric and asymmetric cryptography and the benefits of each type (SO-1, SO-2)
- CLO-3: Apply how authentication and authorization is performed and implemented (SO-1, SO-2)
- CLO-4: Evaluate current security protocols and how security is implemented (SO-1, SO-2)
- CLO-5: Apply continual learning in software security as related to end-user applications, operating systems, and network security (SO-1)
- CLO-6: Use common tools to safely perform static and dynamic analysis of software of potentially unknown origin, including obfuscated malware, to fully understand the software's functionality (SO-1).
- CLO-7: Synthesize effective communication (orally and written) of complex technical ideas and their relation to their professional and ethical responsibilities (SO-1, SO-4)

Grading for the course:

Percentage of grade:	
Assignments	35%
Final project survey paper	8%*
Final project deliverables and presentation	17%
Midterm exam	20%
Final exam	20%

Letter grade will be calculated according to the following table:

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
95-100	90-94	87-89	84-86	80-83	77-79	74-76	70-73	67-69	64-66	60-63	0-59

Attendance: I expect students to attend class sessions regularly and will take attendance at class sessions. For this section lectures will be conducted HyFlex, meaning they will be streamed live at the same time as the on-ground class. To be marked as attending you may be either in person in class or attending online during the live session. If you are going to miss class, please email me before class. The reason for this policy is lots of group work and group break outs are planned during the class period so knowing who will be in class a given day helps with planning these breakout groups effectively. Each student is responsible for making-up any missed study or work on their own. Assistance will be offered to those with plausible reasons for absences; unexcused absences result in the student being totally responsible for the make-up process. You are responsible for all announcements and material covered in the event that you do miss class and should get that information from one of your classmates.

Participation and in class work: We will be doing a lot of in class group work which is critical to your understanding of the material and drives the entire class's learning. As a result, I take your effort in it very seriously. Participating does not simply mean showing up for class. It means fully engaging and contributing to your group's work during class workshops and discussion boards. Simply being part of a group that turns in the work does not mean you are actively contributing. A detailed explanation that applies both to lectures as well as in-class work can be found at https://cs.ccsu.edu/~williams/classes/WhatDoesClassParticipationMean.pdf

Finally, I know you are very bright otherwise you wouldn't be here, and I value your ideas and contributions in making this class better. Because I believe your active participation makes the class a better learning experience for all, I appreciate your questions anytime you don't fully understand something or have questions on how the material might be applied in practice. I do not expect you to know all of the answers. Thoughtful participation regardless of correctness will be rewarded.

Course expectations for out-of-class work:

To succeed in this 3-credit class, it is expected that you commit a total of 12 hours per week to master the course material. This includes 2.5 hours of lecture time and an additional 9.5 hours dedicated to independent study and coursework. This time commitment aligns with the expectations set by the Computer Science department for major courses and adheres to university policies. Recognizing that dedicating this amount of time outside the classroom is a significant commitment, it is nevertheless necessary for success. Please plan your course load accordingly.

Assignment guidelines: All assignments will be submitted via Blackboard. While most work in this class will be created electronically, any handwritten work you turn in to me must be neat and readable. If I can't read it, I will not score points for that portion. Assignments make up 35% of your grade and will be hands on problems based on the lectures and reading. Each assignment is due at 11:59 pm the day listed unless otherwise instructed. You should begin each assignment as it is handed out. By starting assignments early, you have the opportunity to ask me to clarify those things you do not understand. It is essential that you commit yourself to regular studying to keep pace with the course and deadlines. If you are having difficulty with any aspect of this class or facing a challenge outside your control, please talk to me in a timely manner. I will do my best to help you. More options will be available to us if you approach me as soon as possible. Unless arrangements have been made ahead of time, ***late assignments will be penalized 10% per day (2am the next day is the same as 11:59pm that evening so use your late time wisely) until 50% penalty. No submissions will be accepted after the final.***

Final project: For the final project you will choose a topic with my approval that will show in depth knowledge of implementing a specific aspect of the concepts of the course. The final project is broken into 2 stages that you may work individually or in groups of 2. The first part will be a survey paper worth 8% of your grade, please note even

though it is *only* 8% you **must** submit a survey paper to pass the course. The survey paper will discuss different existing works or research related to your chosen project and will analyze the ethics and professional responsibilities related to your topic. The final project deliverable and presentation will be worth 17% and will include a write up, well commented source code, and a recorded video for the presentation that will be given during class during the final week. Unless arrangements have been made ahead of time **late work will be penalized 10% per day**. ***No submissions will be accepted after the final.***

Exams: There will be a midterm and a final exam in addition to a final project. **For the midterm 3/6 and final exam 5/8 you are required to be in person.** These will focus on whether you have understood the material and learned from your mistakes. If a student misses the midterm, they will receive a 0 unless they have contacted me ahead of time and submit a written request.

Academic Honesty: Students are expected to practice the highest standards of ethics, honesty and integrity in all of their academic work. Possible disciplinary actions may include failure for part of or all of a course as well as suspension from the University. I absolutely require that you fulfill your academic obligations in a fair and honest manner. This includes turning in work that is uniquely yours, unless I explicitly require you to work on a project in a group. I strongly suggest that if you work with others, you only work together in the idea generation phase. When it comes to writing your work, you must do so independently. It is in your best interest to never look at any solutions written by another student and to never let another student see any solutions you have written. If you do turn in work that I suspect is the result of cheating, it will be dealt with **harshly**. Any form of academic dishonesty (e.g., plagiarism, cheating and misrepresentation) may result in disciplinary action. ***Penalties for cheating go beyond just receiving a zero for the assignment and could result in penalties as harsh as failure of the course and an Academic Misconduct Report being filed. From a disciplinary standpoint, an Academic Misconduct Report goes to a Faculty Hearing Board which may impose sanctions such as probation, suspension or expulsion.***

Specific items that I consider cheating are:

- *Turning in someone else's work as your own (with or without that person's consent).* This includes turning in even a portion of work that can be mechanically transformed into a copy of someone else's work or AI generated work. Don't even try to disguise cheating by simply modifying someone else's work and calling it your own. Note this is the case for almost all code generated by AI Large Language Models (LLMs) such as Chat GPT.
- *Allowing someone else to turn in your work as his or her own work.* This includes allowing fellow students access to your electronic copy.
- *Using a solution developed in a previous term, found in a book, on the web, or generated by AI.*
- *Plagiarizing*

Note there are opportunities to use the work of others or generated code in the final project **but be sure to have specific explicit approval first**.

You may refer to the Student Code of Conduct here http://web.ccsu.edu/academicintegrity/ and find the full Academic Misconduct Policy online at: https://www.ccsu.edu/academicintegrity/policy.html
Please read it carefully.

Hints to Succeeding in CS/CYS 492:

- **USE STUDENT OFFICE HOURS!** There are many different ways to use office hours such as: working through problems together; discussing some topic you are confused about or want to learn more about; or if you just want to visit. To get the most out of these I recommend having a problem in mind that you have put some effort into. This will help me better understand where you need help, however I am always willing to help even without that. Put simply, **if you are confused come see me**. While I have posted office hours, be sure to check out the booking site for available times as I often have more hours available for a given week than just the posted hours.
- Make sure you **do all of your assignments**. It is the best way to realize quickly if you are missing any important points so that you don't make similar mistakes on the mid-term and final exams.
- **Get involved** in lectures. Don't be afraid to ask for clarification or additional explanation, chances are if you are confused someone else is as well.
- **Be sure to review all returned homework and exams.**

Tentative class outline and assignments

Please note assignment dates are only to give you an idea of what assignments will cover and approximate time frame,actual dates will be set as the semester progresses.

Week 1 January 15 ***(Academic semester begins 1/16)***

- *Reading Ch 1*
- Course overview and objectives
- Classic Cryptography and Cryptanalysis
    - Substitution ciphers

Week 2 January 22

- *Reading Ch 2*
- Introduction to Computer Security
- Classic Cryptography and Cryptanalysis
    - Transposition ciphers
- *Homework 1: Crypto basics*

Week 3 January 29

- *Reading Ch 3*
- Symmetric Key Cryptography
    - Stream ciphers
    - Block ciphers
    - Diffie-Hellman
    - Quantum computers and symmetric crypto
- *Homework 2: Symmetric key cryptography*

Week 4 February 5

- *Reading Ch 4*
- Asymmetric cryptography
    - RSA
    - Uses of public key cryptography
    - Identity based cryptography
    - Quantum computers and public crypto
- *Homework 3: Asymmetric cryptography*

Week 5 February 12

- *Reading ACM Code of Ethics (https://www.acm.org/code-of-ethics)*
- *Reading Ch 5*
- Code of Ethics and Professional Conduct
- Cryptographic hash functions
    - Birthday problem
    - Tiger Hash
    - HMAC
- *Homework 4: Hash functions*

Week 6 February 19

- *Reading Ch 6, Ch 9*
- Authentication
    - Knowledge-based
    - Possession-based
    - Biometrics
    - 2-factor
- Authentication protocols
- *Homework 5: Authentication*

Week 7 February 26

- *Reading Ch 9, Ch 10*
- Authentication protocols
- Real-world Protocols
    - Secure Socket Layer (SSL)
    - IPSec
    - Kerberos

- *Homework 6: Protocols*

Week 8 March 4

- *Reading Ch 7*
- Authorization
    - Access control
    - Security models
- *Midterm Wednesday 3/6*

Week March 11

- Spring break (don't forget your survey paper)

Week 9 March 18

- *Reading Ch 7, Ch 11*
- *Final project survey paper due 3/18*
- Authorization
    - Firewalls and intrusion detection systems
    - Network security
    - Firewalls
    - Vulnerability scanning
- Software Security
    - Security flaws
- *Final project proposal due 3/20*
- *Homework 7: Authorization*

Week 10 March 25

- *Reading Ch 11*
- Software Security
    - Malware
    - Obfuscation
    - Software-based attacks
    - Reverse engineering
- *Homework 8: Software security and SRE*

Week 11 April 1

- *Reading Ch 12*
- Software Reverse Engineering (SRE)
    - Common tools (disassemblers, debuggers, virtualization, process/file/network monitors)
    - Malware analysis
    - Reverse Engineering Tools & Techniques
- *Lab: Sandboxing and Software Reverse Engineering Tools and Techniques*

Week 12 April 8

- *Reading Ch 12*
- Software Reverse Engineering (SRE)
    - Software specification recovery
    - Anti-reverse engineering techniques
    - Uncovering communications protocols
- *Lab: SRE Gaining understanding*

Week 13 April 15

- Secure Software Systems

Week 14 April 22

- Secure Software Systems
- Operating systems and security
- OS security functions
- Trusted operating systems
- *Homework 10: Software system security*

Week 15 April 29

- Final projects due 4/29

Final Exams week of May 6th

- Wednesday 5/8 from 10:30 AM -12:30 PM

University Policies

Registration/Add/Drop/Withdrawal Periods: You are permitted to add/drop courses, subject to seat availability, through the end of the first week of the semester. Course drops (without a "W" on your transcript) are permitted through the end of the third week of the semester. Withdrawals beginning at the fourth week of the semester will result in a "W" on your transcript. Withdrawals after the twelfth week of the semester will only be permitted if there are extenuating circumstances, supported by documentation, and approval by the Instructor and Department Chair. Add, Drop, and Withdrawal deadlines are prorated for courses less than full semester length. Refer https://www.ccsu.edu/registrarfor specific dates each term.

Student Disability Services: If you are a student with a documented disability, and would like to request academic accommodations, you are encouraged to contact Student Disability Services (SDS) at 860-832-1952, or email disabilityservices@ccsu.edu. Please visit the SDS website at http://www.ccsu.edu/sds/ to download an Intake form and documentation requirements. Temporary impairments may also qualify for accommodations. Central Connecticut State University provides reasonable accommodations in accordance with the Americans with Disabilities Act and Section 504 of the Rehabilitation Act for students with documented disabilities on an individualized basis. Please note that accommodations are not retroactive and must be requested each semester.

Statement on Discrimination and Harassment: Central Connecticut State University strives to maintain our campus as a place of work and study for faculty, staff, and students that is free of all forms of prohibited discrimination and harassment based upon age; ancestry, color; gender identity and expression; intellectual disability; learning disability; mental disorder; physical disability; marital status, national origin; race; religious creed; sex, (including pregnancy, transgender status, sexual harassment, and sexual assault); sexual orientation; or any other status protected by federal or state laws. Any student who has concerns should contact the Office for Equity and Inclusion, Student Affairs, or their faculty member.

Sexual misconduct, intimate partner violence, and stalking: Central Connecticut State University (CCSU) will not tolerate sexual misconduct against students, staff, faculty, or visitors in any form, including but not limited to: sexual assault, sexual exploitation, sexual harassment, or stalking, as defined in CCSU policies. For additional information, please consult the BOR\CSCU Sexual Misconduct Reporting, Support Services and Processes Policy: http://www.ccsu.edu/diversity/policies/BORSexualMisconductFeb2015.pdf All faculty members and staff have a duty to report incidents of sexual harassment including sexual misconduct, intimate partner violence, and stalking to Dr. Stacey Miller, Vice President for Equity and Inclusion, Davidson Hall 119.

Inclement weather policy: At the discretion of the President, classes may be cancelled or delayed because of inclement weather or special circumstances. The most accurate cancellation and delay information for Central Connecticut State University will be made available on the Storm Phone: (860) 832-3333 and on CCSU's website at www.ccsu.edu, usually by 6:00 am.