COMP 4/6410 Computer Security Fall 2025

CRN 82751/82768

Instructor: Dr. Dipankar Dasgupta

Class Schedule: TR (Location: Dunn Hall 225) **Time: 6:00PM - 7:25PM**

Attendance
The class will meet in campus location (DH 225) as was published in the "Schedule of Classes."
Course lecture notes and discussion will be through ***canvas (https://canvas.memphis.edu)***

Student Resources
Additional resources can be found on the Dean of Students website at
https://www.memphis.edu/deanofstudents/crisis/index.php

Semester Duration: 08/25/2025 - 12/12/2025

Contact Information:

Office: 333 Dunn Hall	**Department Office:** 375 Dunn Hall
Phone: 678-4147	**Department Phone:** 678-5465
E-mail: dasgupta@memphis.edu	

Office Hours:
I will communicate through Canvas messaging, announcements and discussion channels, and your active participation will be required. The best way to get in touch with me is through email – I will almost always respond within 24 hours to arrange either in-person or virtual meetings. TA office hours will be announced on the Canvas.

COMP 4/6410: Course Description

Basic issues in computer security and privacy; goals: confidentiality, integrity, availability, trust; basic methods and protocols in cryptography, digital signature, authentication, access control; security in computing--programs, databases, operating systems; networks, secure channels, public key infrastructure, certification; security policies, digital evidence; monitor and response; privacy, legal and ethical issues; risk management, security administration; AI in Cybersecurity.

PREREQUISITE: COMP 2150, or permission of instructor.

Why this course?

The course is intended to provide basic and state-of-the-art knowledge about cyber risks, security and protection issues in computing, communication, and information. Students will learn in a systemic way the importance of computer security and privacy. While the foundations of the subject will be thoroughly reviewed, actual practices to cope with increasing concerns about data protection, code execution and network security will be emphasized. These include study of some standard cryptosystems, protocols, and security strategies in access to computing devices and shared computing resources. Also, use of Generative AI (such as LLMs) for cyber defense will be discussed. There will also be some discussion on the evolving legal and ethical issues with cyber world.

Textbook:

There is no required textbook for this course; lecture notes will be provided along with additional resources. A list of recommended Reference Books:

- Security in Computing (6th Edition) by Charles Pfleeger, Shari Pfleeger, Lizzie Coles-Kemp (August 5, 2023), Addison-Wesley Professional, ISBN-13-978-0137891214.
- NIST Special Publication on *Building a Cybersecurity and Privacy Learning Program*, September 12, 2024. Website: https://doi.org/10.6028/NIST.SP.800-50r1.
- Computer Security Fundamentals by Chuck Easttom, 5th edition, Pearson+ 2023.
- There will be Lecture notes and selected reading on current security issues and solutions.

Other Resources (hyperlinks checked on 8/20/2025):

- NIST Cybersecurity Framework – CSF 2.0 Edition
- Cybersecurity - Attack and Defense Strategies - Second Edition, December 31, 2019.
- Crypto, International Cryptology Conference
- Trusted Computing Group (http://www.trustedcomputinggroup.org/)
- Computer World Magazine (http://www.computerworld.com)

Evaluation:

Students are expected to actively participate during the class discussions. Participation in class is viewed as a continuous two-sided feedback process, which (a) allow students to assess themselves on their progress in learning the material/understanding the security issues; and (b) allows the instructor to assess how well he is fostering the communication process with and among students. Good evaluations will thus reflect not only your grasp of the material, but also how well you take advantage of the class time and how well you end up using the knowledge in securing your systems. The evaluation process will include activities such as paper presentations, assignments, tests, quizzes, and a term paper/project to make sure that you have integrated the material into your general practice of secure cyber.

Your final grade for the course will be based on the grades in the following course-related activities (given in percentages):

Class performance/Discussion/Presentation	10%
Tests/quizzes/Exams	60% (50% for COMP 6410)
Assignments/ Exercises	30%
Term paper/project + proposal	10% (COMP 6410 only)

NOTE: Graduate students (COMP 6410) will have to do some additional works which include paper presentation, term project, etc.

Grading Scale:

A+	95.1-100	**B+**	85.1-88	**C+**	76.1-79	**D+**	60.1-66
A	90.1 -95	**B**	82.1-85	**C**	70.1-76	**D**	50 - 60
A-	88.1 -90	**B-**	79.1-82	**C-**	66.1-70	**F**	< 50

Course Policies:

Students are expected to attend all scheduled classes and submit assignments on time. If you miss a class, it is your responsibility to check course website and catch up on the course content. There will be no make up test for this course.

Any student who anticipates physical or academic barriers based on the impact of a disability is encouraged to speak with me privately. Students with disabilities should also contact Disability Resources for Students (DRS) at 110 Wilder Tower, 901-678-2880. DRS coordinate access and accommodations for students with disabilities.

Ethical behavior is an important part of this course. The course is primarily concerned with techniques that are designed to increase the security of cyber systems, a proper understanding of those systems requires that you be versed in their vulnerabilities and associated risks. Since some of the methods, codes and tools that will be discussed and experimented in the course can be very harmful, if abused, it is expected that students will behave in a responsible fashion. You must follow the University's IT usage policy, always ask your local site administrator for permission before experimenting with security-related tools. Likewise, you should refrain from writing computer viruses, worms, self-reproducing code, or other kinds of potentially damaging software for this course unless you have explicit, written approval for the specific type of software that you wish to create. These kinds of programs are notoriously difficult to control, and their release (intentional or otherwise) can result in substantial civil and criminal penalties.
In-class discussions of techniques for exploiting potential security threats and risks do not imply to use them without proper permission! You will be sole responsible for any such violation.

Finally, I recommend reading and review the ACM Code of Ethics and Professional Conduct.

Plagiarism/Cheating Policy:

"Plagiarism or cheating behavior in any form is unethical and detrimental to proper education and will not be accepted. All work submitted by a student (projects, programming assignments, lab assignments, quizzes, tests, etc.) is expected to be a student's own work. The plagiarism is incurred when any part of anybody else's work is passed as your own (without proper credit is listed to the sources in your own work) so the reader is led to believe it is therefore your own effort. Students are allowed and encouraged to review basic literature and look up online up-to-date valid resources for their assignments and homework; but appropriate references must be included for the materials consulted, and proper citations made when the material is taken from elsewhere.

If plagiarism or cheating occurs, the student will receive a failing grade on the assignment and (at the instructor's discretion) a failing grade in the course. The course instructor may also decide to forward the incident to the Office of Student Conduct for further disciplinary action. For further information on U of M code of student conduct and academic discipline procedures, please refer to: https://www.memphis.edu/osa/students/academic-misconduct.php"

"Your written work may be submitted to Turnitin.com, or a similar electronic detection method, for an evaluation of the originality of your ideas and proper use and attribution of sources. As part of this process, you may be required to submit electronic as well as hard copies of your written work or be given other instructions to follow. By taking this course, you agree that all assignments may undergo this review process and that the assignment may be included as a

source document in Turnitin.com's/Generative AI restricted access database solely for the purpose of detecting plagiarism in such documents. Any assignment not submitted according to the procedures given by the instructor may be penalized or may not be accepted at all." (Office of Legal Counsel, August 4, 2020) Turnitin - umTech - The University of Memphis.

In our active learning environment, use of Generative AI tools (such as ChatGPTs, LLMs) has very limited use (in particular, in many specific queries, these tools "Hallucinate", provide inaccurate or factually wrong solutions). The following classroom policies will be followed for the use of AI generative tools https://docs.google.com/document/d/1RMVwzjc1o0Mi8Blw_-JUTcXv02b2WRH86vw7mi16W3U/edit#heading=h.1cykjn2vg2wx.

Tentative schedule *(topics to be covered and course-related activities during the semester)*:

DATE	LECTURE TOPICS
August 26	Course Aims & Agenda – Introduction to Computer Security
August 28	Cyber/Information Security – terminologies, security fundamentals and control measures. Introduction to AI
September 2	Program Security – Secure programs, Patching, Phishing, Social Engineering attacks, Targeted Attacks, Advanced Persistent Threats (APTs)
September 4	Malicious Code- Virus & Worm, Virus life cycle, Covert Channel, etc. ***Assignment 1***
September 9	Cryptography Basics– Fundamentals, Enciphering, Deciphering, Type of Ciphers, Cryptanalysis, Differential, etc.
September 11	Cryptography (cont..) –Substitution, permutation, RSA, DES, etc.
September 16	Encryption Methods – AES, MD5, Hash functions, Digital Signature, etc.
September 18	**Computer Security Exercise / Alterative activities** ***Assignment 2***
September 23	Asymmetric Encryption – Public-Private Key, Key exchange protocols, Key Escrow and Clipper, etc.
September 25	Review of Cryptographic techniques
September 30	**First Class Test**
October 2	AI for Cybersecurity: Cyber AI and Secure AI ***Project Proposal due (COMP 6410)***
October 7	Host-System Security – Physical Security, Authentication and Authorization, File Systems, Passwords and Access Control mechanism.

October 9 Digital Water marking, Stenography, Penetration Testing, Attack Surfaces, OWASP Web Vulnerabilities and Remedies.

Assignment 3

October 16 **Computer Security Lab**

.

October 21 Operating System Security – Protection of Objects, security models, Secure Software Testing

October 23 Trusted Operating System – UNIX and Linux Security, Multilevel Security

October 28 Database Security--Reliability & Integrity, DBMS Security, Inference problems, Multilevel database, etc.

October 30 **Second Class Test**

November 4 Network Security – Types of Attack, securing communication media, Network Protocol security, Packet Filters, Monitoring and response systems, etc.

Assignment 4

November 6 Virtual Private Network (VPN), Network Address Translation (NAT), Firewalls, Server & Web Security

November 11 Administering Security – Security Policies, Disaster Recovery, Zero-trust

November 13 Info. Risk Management – Identify assets, vulnerability analysis, NIST Cybersecurity Framework, TEMPEST Security etc.

November 18 Legal Issues, Ethical Issues, Personally Identifiable Information (PII), etc.

Submission of Assignment 4

November 20 **Computer Security Exercise / Virtual Lab**

November 25 Computer Crime/Law (GDPR/CCPA), Cyber Rights & Responsibilities

December 2 **Third Class Test (Tuesday)**

December 3: Project Demo / Presentation (COMP 6410)

December 8: Submission of Project Report (COMP 6410)

NOTE 1: Each assignment is due on the next assignment date (i.e. assignment 1 is due on September 18th and so on).
NOTE 2: There will be paper presentation and a term paper/project for graduate students(COMP 6410),.
NOTE 3: I will be using Canvas for lecture notes, grades and all submissions. If I need to communicate with the class as a group, I'll be using canvas discussion channel, you will need to check it and your email regularly.