COMP 4/6410 Computer Security Fall 2023

Instructor: Dr. Dipankar Dasgupta

Class Schedule: TR (Location: Dunn Hall 225) Time: 5:30PM - 6:55PM

Attendance
The class will meet in campus location as was published in the "Schedule of Classes." Do not attend class in person if you're showing symptoms of illness (provide official documents of your illness). Lecture notes will be available online for those who cannot attend in person during the infection period.

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

Contact Information:

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

Course lecture notes and discussion will be through **canvas (https://canvas.memphis.edu)*

Office Hours:
For now, b*y appointment only*. The best way to get in touch with me is through email – I will almost always respond within 24 hours either for face-to-face-meeting meeting or via zoom.

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.

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 the basic notions and 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 will be emphasized. These include study of some standard cryptosystems, protocols, and security strategies in access to computing devices and shared computing resources. There will also be some discussion on the evolving legal and ethical issues with cyber-enabled technologies.

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, C. Pfleeger et al, Prentice-Hall PTR, Fifth Edition, 2016.**
- **Computer Security: Principles and Practice (4th Edition) by William Stallings and Lawrie Brown (August 4, 2017).**
- **NIST Special Publication on Building a Cybersecurity and Privacy Learning Program, NIST SP800-50r1-ipd, August 2023. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.ipd.pdf).**
- **Computer Security Fundamentals by Chuck Easttom, 4th edition, Pearson 2020.**
- **NIST Cybersecurity Framework A Complete Guide - 2020 Edition by Gerardus Blokdyk, Sep 6, 2019**
- **Cybersecurity Bible: Security Threats, Frameworks, Cryptography & Network Security by Hugo Hoffman, Apr 25, 2020.**
- **There will be selected reading on current security issues and solutions.**

Other Resources (hyperlinks checked on 8/1/2022):

- National Institute for Science and Technology (NIST) Computer Security Resource Clearinghouse
- Security, Usenix Security Symposium
- Crypto, International Cryptology Conference
- uwf.edu/cybersecurity
- Trusted Computing Group (http://www.trustedcomputinggroup.org/)
- International Crypto Resources
- Computer World Magazine (http://www.computerworld.com)

Evaluation:

Students are expected to actively participate during the class discussions. Participation in class will be 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 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 computing.

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

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

Graduate students (COMP 6410) 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! 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 tolerated. 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 (no 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 discuss with each other and look up resources in the literature (including the internet) on their assignments, but appropriate references must be included for the materials consulted, and appropriate citations made when the material is taken verbatim.

If plagiarism (via ChatGPT) 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) https://www.memphis.edu/umtech/teaching/**turnitin**.php.

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 29	Course Aims & Agenda – Introduction to Computer Security
August 31	Cyber/Information Security – terminologies, security fundamentals and control measures.
September 5	Program Security – Secure programs, Patching, Phishing, Social Engineering attacks, Targeted Attacks, Advanced Persistent Threats (APTs) ***Assignment 1***
September 7	Malicious Code- Virus & Worm, Virus life cycle, Covert Channel, etc.
September 12	Cryptography Basics– Fundamentals, Enciphering, Deciphering, Type of Ciphers, Cryptanalysis, Differential, etc.
September 14	Cryptography (cont..) –Substitution, permutation, RSA, DES, etc.
September 19	Encryption Methods – AES, MD5, Hash functions, Digital Signature, etc. ***Assignment 2***
September 21	**Computer Security Lab – I / Alterative activities**
September 26	Asymmetric Encryption – Public-Private Key, Key exchange protocols, Key Escrow and Clipper, etc.
September 28	**First Class Test**

October 3 Host-System Security – Physical Security, Authentication and Authorization, File Systems, Passwords and Access Control mechanism.

October 5 Digital Water marking, Stenography, Penetration Testing, Attack Surfaces, OWASP Web Vulnerabilities and Remedies.
Assignment 3

October 10 Operating System Security – Protection of Objects, security models, Secure Software Testing.
Project Proposal due (COMP 6410)

October 12 Trusted Operating System – UNIX and Linux Security, Multilevel Security

October 19 Database Security – Reliability & Integrity, DBMS Security, Supervisory Control & Data Acquisition (SCADA)
Assignment 4

October 24 Database Security – Inference problems, Multilevel database, etc.

October 26 Network Security – Types of Attack, securing communication media, Network Protocol security, Packet Filters, Monitoring and response systems (IDS, IPS).etc.

October 31 **Second Class Test**

November 2 Network Security – Firewalls, Server & Web Security, Zero-trust

Assignment 4

November 7 Virtual Private Network (VPN), Network Address Translation (NAT), APTs, Advanced Malware, Ransomware

November 9 Administering Security – Security Policies, Disaster Recovery

November 14 Info. Risk Management – Identify assets, vulnerability analysis, NIST Cybersecurity Framework, TEMPEST Security etc.

November 16 Legal Issues, Ethical Issues, Personally Identifiable Information (PII), etc.

Submission of Assignment 4

November 21 **Computer Security Lab / Virtual Lab**

November 28 Computer Crime/Law, Cyber Rights & Responsibilities

November 30 Course Review (Additional Topics of interest)

December 5 **Third Class Test (Tuesday)**

November 30: 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 19th and so on).
NOTE 2: There will be paper presentation and a term paper/project for graduate students(COMP 6410),.
NOTE 3: We 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 your email regularly.