Course Syllabus: CS 6238 Secure Computer Systems

Summer 2026

Instructional Team Information

Professor: Mustaque Ahamad
Weekly Office Hours via Zoon: Check Canvas
Teaching Assistants and Office Hours: Check Canvas

General Course Information

Description

Applications and services are supported by software platforms such as operating systems and databases. Secure execution of such applications depends on the trust assumptions that can be made about these systems. By providing a trusted computing base that offers the necessary mechanisms for protecting sensitive information and other resources, operating systems and databases can facilitate the development of secure applications.

This course will start with trusted computing base requirements and how they can be supported with modern processor architectures. Following this, it will explore problems such as authentication and access control that are traditionally handled at the system level. Students will also gain in depth understanding of the implementations of mechanisms that address these problems and security policies that can be supported by them. System level security issues in distributed systems will be covered as well.

Pre- &/or Co-Requisites

- An undergraduate operating systems course (Georgia Tech's course CS 3210 Design of Operating Systems or equivalent).
- System programming experience with the C programming language is highly desirable.
- Programming experience with Python.

Course Goals and Learning Outcomes

After completing the course, the students should have the following capabilities:

- Demonstrate the need for a trusted computing base (TCB) and how it helps protect resources in a computer system.
- Analyze how hardware supported memory protection enables isolation of TCB and of untrusted programs.
- Develop, implement and evaluate authentication and access control in computer systems.
- Understand and evaluate security in distributed systems.
- Apply security concepts to protect data stored in database systems.
- Be familiar with recent research related to topics covered in class.

Course Materials

Course Text

None. Research papers and other required/recommended readings will be available online.

Required Readings
Papers will be assigned for topics covered in each week.

Course Website and Other Classroom Management Tools
This class will use Canvas to deliver course materials to online students. ALL course materials and activities will take place on this platform.

Course Requirements, Assignments & Grading

Assignment Distribution and Grading Scale

Assignment		Weight
Quizzes: There will be 13 weekly quizzes, one for each module. **Three quizzes with the lowest scores will be dropped.**		**20 %**
Programming Projects (Two best of first three and project IV)		**20%**
Project I: Memory Protection		5%
Project II: Authentication		5%
Project III: Access Control		5%
Project IV: Distributed Systems Security	10%	
Exams		**60%**
Midterm Exam		30%
Final Exam		30%

Grading Scale
Your final grade will be assigned as a letter grade. To receive an A, a student must demonstrate mastery of the course topics. Typically, students who have an overall score at least 0.5 standard deviation higher than the class average will receive an A. Those students who have overall mean well below the class average will receive a C (more than one standard deviation below class average). Students who do not complete work, perform poorly on most assessment components and have overall score more than two standard deviations below the class average may be assigned an F.

Description of Graded Components

Quizzes

The course will have 13 quizzes, one for each weekly module. The goal of the quizzes is to ensure that students keep up with the modules and are able to demonstrate familiarity and understanding of the material covered in each module. It is possible that you may not be able to devote sufficient time to the course in some weeks. Because of this, lowest **three quiz scores** will be dropped. Quizzes are 20% of the total grade.

Each quiz will be available during the week when the quiz module/topic is scheduled. Once a quiz is released (on a Monday unless it is a holiday), it will be available until the following Sunday when it closes. Each quiz has a time limit of 15 minutes and students will have **two** attempts only. Quiz questions will either be T/F or multiple choice and will be auto-graded. If you fail to take a quiz before it closes, you will get a 0 on that quiz. It is advised that you review the material in the module covered in a week, attempt the quiz and then re-review the material again before the second attempt. The quiz questions should help you focus on and master key concepts covered in a module. If you keep up with the modules each week, you should be able to do well on the quizzes. Quizzes are individual assignments and are intended to test familiarity with and understanding of material covered in lectures and assigned reading.

Programming Projects

The course will have 4 programming projects designed to reinforce the concepts covered with hands-on implementations. The lowest score of one project from projects 1-3 will be dropped and the remaining two projects will be 10% of total grade. Project 4 is 10% of the total grade and must be completed by all students.

Exams

The course will have two online exams with questions that require free response answers: A midterm and a final. Each exam will be 30% of the overall grade. Both exams will be **closed book, closed notes** and students will be required to type their answers in a text box in Canvas. Once an exam is released, it will be available for a week before it is due. Students will have **one** attempt only with a time limit of 2 hours. Exams are individual assignments and are intended to test deeper understanding of the topics covered in lectures and assigned reading. The final exam will include **only** topics covered after the midterm.

Completing Quizzes and Exams and Submitting Projects

Quizzes and exams will only be available during the period specified above. Since all quizzes are due on Sundays, they must be completed by 11:55PM ET on Sunday night. Each project will have details of the files/documents that need to be submitted. Again, these should be submitted by 11:55PM ET on the day they are due.

Sending assignments (projects etc.), whether early, on time, or late to the professor or TAs is not permitted and will not be accepted. All projects must be completed and submitted within Canvas. If there are technical issues, please notify the help desk, as well as the professor immediately.

Assignment Due Dates

All assignments a will be due at the listed times listed. These times are subject to change so please check back often. Please convert from UTC to your local time zone using a Time Zone Converter.

Late and Make-up Work Policy

Timing Policy

- The modules follow a logical sequence that includes knowledge and experience-building. It is important that work assigned for a module be completed in a timely manner to facilitate learning in upcoming modules.
- Assignments should be completed by their due dates. Late submissions will not be accepted. The only extenuating circumstances that will be accommodated are those that literally incapacitate the student for a significant period of time, such as injury and hospitalization, floods, hurricanes, power outages for several days, etc. Please do not ask for extensions for any other reasons.

Grading and Feedback

Quizzes will be auto-graded. Explanations for correct answers will be provided after a quiz closes during office hours. Office hours will be recorded in case you are unable to join. Please attend office hours or review recordings before you ask clarification on quiz questions. Projects and exams will typically be graded and returned within two weeks after the submission date.

Technology Requirements and Skills

Computer Hardware and Software

- High-speed Internet connection
- Laptop or desktop computer with a **minimum** of a 2 GHz processor and 16 GB of RAM. Because the course projects will require virtual machine installations, memory less than 8GB may lead to problems.
- Windows for PC computers OR Mac iOS for Apple computers
- Complete Microsoft Office Suite or comparable and ability to use Adobe PDF software (install, download, open and convert)
- Linux operating systems familiarity, including how system calls are used
- Virtualization software such as VirtualBox and ability to create and launch virtual machines
- Software development, compiling and debugging tools as required

Technology Help Guidelines

30-Minute Rule: When you encounter struggles with technology, give yourself 30 minutes to 'figure it out.' If you cannot, then post a message to the discussion board; your peers may have suggestions to assist you. You are also directed to contact the Helpdesk 24/7.

When posting or sending email requesting help with technology issues, whether to the Helpdesk, message board, or me use the following guidelines:

- Include a descriptive title for the subject field that includes 1) the name of course 2) the issue. Do NOT just simply type "Help" into the subject field or leave it blank.
- List the steps or describe the circumstance that preceded the technical issue or error. Include the exact wording of the error message.
- When possible, always include a screenshot(s) demonstrating the technical issue or error message.
- Also include what you have already tried to remedy the issue (rebooting, trying a different browser, etc.).

Course Policies, Expectations & Guidelines

Communication Policy

- Email course questions and personal concerns, including grading questions, to the instructor privately. Do NOT submit posts of a personal nature to the discussion board unless it is a private post.
- Email will be checked at least once per day, Monday through Friday. On Saturday and Sunday, email may be checked but there is no guarantee. During the week, I will respond to all emails within 24 hours; on weekends and holidays, allow up to 48 hours. If there are special circumstances that will delay my response, I will make an announcement to the class.
- Student Forum/Q&A discussion boards will be checked twice per day Monday through Friday; Saturday and Sunday, these discussion boards will be checked once per day.
- Virtual office hours will be held using Zoom. Also, special office hours may be announced before exams. Office hours will be announced at the start of the semester and prior to exams.

Student Online Conduct and (N)etiquette

Communicating appropriately in the online classroom can be challenging. In order to minimize this challenge, it is important to remember several points of **"internet etiquette"**
that will smooth communication for both students and instructors:

1. *Read first, Write later*. Read the ENTIRE set of posts/comments on a discussion board before posting your reply, in order to prevent repeating commentary or asking questions that have already been answered.
2. *Avoid language that may come across as strong or offensive*. Language can be easily misinterpreted in written electronic communication. Review email and discussion board posts BEFORE submitting. Humor and sarcasm may be easily misinterpreted by your reader(s). Try to be as matter-of-fact and professional as possible.
3. *Follow the language rules of the Internet*. Do not write using all capital letters, because it will appear as shouting. Also, the use of emoticons can be helpful when used to convey nonverbal feelings.
4. *Consider the privacy of others.* Ask permission prior to giving out a classmate's email address or other information.
5. *Keep attachments small*. If it is necessary to send pictures, change the size to an acceptable 250kb or less (one free, web-based tool to try is picresize.com).
6. *No inappropriate material*. Do not forward virus warnings, chain letters, jokes, etc. to classmates or instructors. The sharing of pornographic material is forbidden.

***NOTE**: The instructor reserves the right to remove posts that are not collegial in nature and/or do not meet the Online Student Conduct and Etiquette guidelines listed above.*

University Use of Electronic Email

A university-assigned student e-mail account is the official university means of communication with all students at Georgia Institute of Technology. Students are responsible for all information sent to them via their university-assigned e-mail account. If a student chooses to forward information in their university e-mail account, he or she is responsible for all information, including attachments, sent to any other e-mail account. To stay current with university information, students are expected to check their official university e-mail account and other electronic communications on a frequent and consistent basis. Recognizing that some communications may be time-critical, the university recommends that electronic communications be checked minimally twice a week.

Plagiarism & Academic Integrity

Georgia Tech aims to cultivate a community based on trust, academic integrity, and honor. Students are expected to act according to the highest ethical standards. All students enrolled at Georgia Tech, and all its campuses, are to perform their academic work according to standards set by faculty members, departments, schools and colleges of the university; and cheating and plagiarism constitute fraudulent misrepresentation for which no credit can be given and for which appropriate sanctions are warranted and will be applied. For information on Georgia Tech's Academic Honor Code, please visit http://www.catalog.gatech.edu/policies/honor-code/ or http://www.catalog.gatech.edu/rules/18/.

Any student suspected of cheating or plagiarizing on a quiz, exam, or assignment will be reported to the Office of Student Integrity, who will investigate the incident and identify the appropriate penalty for violations.

Because similar projects could be assigned in future offering of the course, please do not make class projects, quiz and exam questions, and your solutions available at a public repository.

Copyright

The course readings include research papers that are available in the public domain or via the Georgia Tech library. As specified by publishers' copyright notices, the papers will be for individual use only. Similarly, course materials such as quiz and exam questions and project descriptions are for your use only and should not be published or disseminated.

Accommodations for Students with Disabilities

If you are a student with learning needs that require special accommodation, contact the Office of Disability Services at (404)894-2563 or http://disabilityservices.gatech.edu/, as soon as possible, to make an appointment to discuss your special needs and to obtain an accommodations letter. Please also e-mail me as soon as possible in order to set up a time to discuss your learning needs.

Collaboration & Group Work

You are encouraged to form virtual groups to discuss topics covered in class. Such discussion can enhance learning and could include clarifications of questions related to a topic or a project. However, individual work that you submit as part of an assessment and claim as yours must be yours. We follow a similar policy when it comes to use of AI tools (see https://www.cc.gatech.edu/news/new-policies-navigate-role-ai-assistants-cs-courses?utm_source=newsletter&utm_medium=email&utm_content=Full%20Story%0A&utm_campaign=Daily%20Digest%20-%20June%2022%2C%202023).

All work for this class is to be done individually. You are strongly urged to familiarize yourself with the **GT Student Honor Code (Links to an external site.) rules. Specifically, the following is not allowed:**

- Copying, with or without modification, someone else's work when this work is not meant to be publicly accessible *(e.g., a classmate's program or solution).*
- Submission of material that is wholly or substantially identical to that created or published by another person or persons, without adequate credit notations indicating authorship *(plagiarism).*
- Putting your projects on a public Github repository is not allowed. If a student in the future copies your code/reports, the student obviously violates the honor code, and you will not want to be an enabler for the violation.

Any public material that you use *(open-source software, help from a text, or substantial help from a friend, etc...)* should be acknowledged explicitly in anything you submit. The same holds for use of AI

tools. If you have any doubt about whether something is allowed or not, please do check with the class Instructor or the TA.

LLMs and Generative AI Tools Use

In this course, using generative AI tools in the work of the course (including programming, discussions, and language editing) is allowed. As with any technology, generative AI tools need to be used critically and according to academic and professional expectations. When using generative AI tools, you are expected to adhere to the following principles:
Responsibility: You are responsible for the work you submit. This means that any work you submit should be your own, with any AI-generated assistance appropriately disclosed (see Transparency below) and any AI-generated content appropriately cited (see Documentation below). It is your responsibility to ensure that any factual statements produced by a generative AI tool are true, and that any references or citations produced by the AI tool are correct and verifiable.
Transparency: Any AI-generated content you use in the work of the course should be clearly acknowledged. Transparency in attribution is needed not only when you use content directly produced by a generative AI tool, but also when you use a generative AI tool in the process of composition or discovery (for example, for brainstorming, outlining or synthesizing information sources, or translation).
Documentation: You should cite any content generated by an AI tool as you would when quoting, paraphrasing, or summarizing ideas, text, images, or other content made by other people.
A word of advice: Please do not simply copy an LLM output verbatim. We suggest keeping documentation of your chat prompts and output, particularly for attribution of specific programming lines or tasks and in replication of your analyses. Using generative AI tools in the course without adhering to these principles may be considered an infraction of Georgia Tech's Academic Honor Code, subject to investigation by the Office of Student Integrity.

Extensions, Late Assignments, & Re-Scheduled/Missed Exams

Each quiz, exam and project will be open for at least one week. Because of this, no extensions will be granted, and late assignments will not be accepted. Please do not email your projects to the instructor or TAs after they close on Canvas.

Student-Faculty Expectations Agreement

At Georgia Tech we believe that it is important to strive for an atmosphere of mutual respect, acknowledgement, and responsibility between faculty members and the student body. See http://www.catalog.gatech.edu/rules/22/ for an articulation of some basic expectation that you can have of me and that I have of you. In the end, simple respect for knowledge, hard work, and cordial interactions will help build the environment we seek. Therefore, I encourage you to remain committed to the ideals of Georgia Tech while in this class.

Course Schedule

Module/Topic	Deliverables	Readings
Module 1: Getting started: Course Introduction	**Quiz 1**	• **The Security Mindset** • **Reflections on Trusting Trust** • **Chapter 1 of "Building a Secure Computer System" by Morrie Gasser**

Module/Topic	Deliverables	Readings
		• Trusted Platform Module • Trusted Computing Systems Evaluation Criterion
Module 2: Design Principles for Secure Systems	**Quiz 2**	• The Protection of Information in Computer Systems • Chapter 5 of Morrie Gasser book
Module 3: Hardware Support for Protection of Resources	**Quiz 3**	• Chapter 5: Intel Architectures Software Developer Manual • Flipping Bits in Memory Without Accessing Them: An Experimental Study of DRAM Disturbance Errors • Project Zero
Module 4: Virtualization and Security	**Quiz 4**	• Background Reading: Xen and Art of Virtualization • Analysis of Intel Pentium for Supporting Virtualization • Chapters 23 and 24: Intel Architectures Software Developer Manual • Ether: Malware Analysis with Hardware Virtualization
Module 5: Authentication	**Quiz 5** **Programming Project I Due**	• Password hardening based on keystroke dynamics • Chip and PIN is broken • Targeted Online Password Guessing: An Underestimated Threat • Password managers: attacks and defenses
Module 6: Discretionary Access Control	**Quiz 6**	• Protection • Access Control Lists: Unix , Windows • Going beyond the sandbox: new security architectures in JDK 1.2 • Capability-based systems: Hydra • Setuid demystified
Module 7: Mandatory Access Control	**Quiz 7** **Programming Project II Due**	• Chapter 6 of Morrie Gasser book (Also read the original BLP report) • Clark-Wilson Commercial MAC Policy • Role-based access control
Module 8: Review for Midterm Exam & Midterm Exam	**Midterm Exam**	**Readings from weeks 1 - 7**
Module 9: Mandatory Access Control in SELinux	**Quiz 8**	• Research papers that led to the development of SELinux. They are not required reading for the course.
Module 10: Covert Channels	**Quiz 9** **Programming Project III Due**	• A note on the confinement problem • Guide to covert channel analysis • Pump: A decade of covert fun • Project zero blog post on meltdown and spectre
Spring Break		•
Module 11: Distributed Systems Security – Basics	**Quiz 10**	• Authentication in Distributed Systems: Theory and Practice
Module 12: Distributed Systems Security – Putting it All Together	**Quiz 11**	• Authentication in Distributed Systems: Theory and Practice • SGX: End-to-end remote attestation • Distributed Systems Security with Information Flow Control

Module/Topic	Deliverables	Readings
Module 13: Database Security – Basics, Inference Attacks & Data Privacy	**Quiz 12**	• An authorization mechanism for relational databases • Security-control methods for statistical databases • Data privacy and k-anonymity • Differential Privacy; A Survey of Results
Module 14: Database Security – Multi-Level Secure Databases	**Quiz 13** **Programming Project IV Due**	• The Seaview Security Model
Module 15: Course Summary and Final Exam Review	**Final Exam**	**Readings from weeks 9 - 14**