# [ECE-4115 - A & AL] - Syllabus

## ECE – 4115 Intro to Computer Security

FALL 2026
Course: Section A (85883)
Unsupervised Laboratory: Section AL (87131)
M & W 5:00 pm - 06:15 pm, Van Leer C240

### 1. Instructor(s)

Angelos Keromitys, PhD.
angelos@gatech.edu
Office: Klaus (KACB) 3363; *hours by Appointment*

Alexander W. Miranda, PhD.
awmiranda@gatech.edu
Office: Klaus (KACB) 3202; *hours by Appointment*

### 2. General Information

#### Course Description

Introductory topics in computer security are presented with an emphasis on fundamental security primitives and current security challenges facing society. General concepts and applied methods of computer security, especially as they relate to confidentiality, integrity, and availability of information assets.
Topics include system security analysis, access control and various security models, identification and authentication, protection against external and internal threats, network protocols and Internet security.

#### Pre-Requisites

ECE 4110, (or), ECE 3600, (or), CS 3251

#### Course Goals and Learning Outcomes

**Knowledge and Comprehension**

a) Describe the functioning of various types of malicious code, such as viruses, worms, trapdoors.
b) Enumerate programming techniques that enhance security.
c) Explain the various controls available for protection against internet attacks, including: authentication, integrity check, firewalls, intruder detection systems.
d) Describe the different ways of providing authentication of a user or program.
e) Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
f) Describe the background, history and properties of widely used encryption algorithms.
g) Describe legal, privacy and ethical issues in computer security.
h) List and explain the typical set of tasks required of an information security professional.
i) Describe the principles of steganography and watermarking.

**Application and Analysis -**

j) Compare different access control, file protection or authentication mechanisms.
k) Set up file protections in a Unix or Windows file system to achieve a given purpose.
l) Incorporate encryption, integrity check and/or authentication into a given program or algorithm.

**Synthesis and Evaluation-**

m) Appraise a given code fragment for vulnerabilities.
n) Appraise a given protocol for security flaws.
o) Assess risk for a given network system using publicly available tools and techniques.

**Learning Outcomes**

Upon successful completion of this course, students should be able to:

1. Describe why systems and networks are vulnerable to attacks,
2. Describe various methods for defending and detecting system and network attacks,
3. Describe the practical challenges with implementing and defending against system and network attacks,
4. Utilize hardware- and software-based networking and system analysis to assess the risk to systems and the benefits of specific defensive techniques.

**Student Outcomes**
In the parentheses for each Student Outcome, "P" for primary indicates the outcome is a major focus of the entire course, "M" for moderate indicates the outcome is the focus of at least one component of the course, but not the majority of course material.

1. (M) an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
2. (M ) an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
3. (P) an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
4. (M) an ability to acquire and apply new knowledge as needed, using appropriate learning strategies.

## 3. Course Requirements & Grading
### Description of Graded Components

**Quizzes:** (1% each)
There will be one quiz on the third lecture. This will be 1% extra credit.

**Labtainers:** (4% each)
There will be 10 labtainer exercises during the semester. Each labtainer is designed to reinforce the topics discussed in class. Labtainers will begin with an in-class presentation and the completed assignment due at least 7 days later.

**Exams:** (30% each)
There are two exams. Both exams are true/false and multiple-choice. All exams are closed-everything and will last for 60 minutes.

| Assignment | Date | Weight (Percentage, points, etc) |
|---|---|---|
| **Labtainers** | Every Week | 40% |
| **Quiz** | 1st Week only | 1% |
| **Exams** | 10/7, 12/2 | 60% |

### Grading Scale
Your final grade will be assigned as a letter grade according to the following scale:

( A ) 90 - 100%
( B ) 80 - 89%
( C ) 70 - 79%
( D ) 60 - 69%
( F ) 0 - 59%

## 4. Course Materials
### Course Text-Book and other Materials
a) Matt Bishop, *Computer Security: Art and Science, 2nd Ed.,* 2018 *(Required)*
b) William Stallings, Lawrie Brown, *Computer Security Principle and Practice*, 2017 *(Required)*
c) Additional Materials/Resources will be provided via Canvas.

### Course Website and Other Classroom Management Tools
During the term, we use Piazza for class discussion. The system is highly catered to getting you to help fast and efficiently from classmates, the TA, and myself. Rather than emailing questions to the teaching staff, I encourage you to post your questions on Piazza. If you have any problems or feedback for the developers, email team@piazza.com.

### LockDown Browser Requirement
This course requires the use of LockDown Browser for online exams. Watch this video to get a basic understanding of LockDown Browser: Lockdown-Browser
Download and install LockDown Browser from this link: Links to an external site.
Once the Browser is Installed:
1. Start LockDown Browser.
2. Log into to Canvas.
3. Navigate to the quiz.

***Note:*** You won't be able to access a quiz that requires LockDown Browser with a standard web browser. If this is tried, an error message will indicate that the test requires the use of LockDown Browser. Simply start LockDown Browser and navigate back to the exam to continue.

## 5. Course Expectations & Guidelines
Online quiz and exams; follow these guidelines:
a) Turn off all mobile devices, phones, etc. and don't have them within reach.
b) Clear your area of all external materials - books, papers, other computers, or devices.
c) Remain at your desk or workstation for the duration of the test.
d) LockDown Browser will prevent you from accessing other websites or applications; you will be unable to exit the test until all questions are completed and submitted.

### 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. 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.

### 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 to set up a time to discuss your learning needs.

### Attendance and/or Participation
There are no attendance or participation requirements for lectures. Quizzes and project presentations must be during the allotted time period.
Attendance is not required, but highly encouraged as the topics in the slides are reinforced in class.

### Collaboration & Group Work
Homework submissions should be written and submitted separately by each student, but discussion with other students is allowed and encouraged within reason (e.g., students should still independently complete the work).

### Extensions, Late Assignments, & Re-Scheduled/Missed Exams
Assignments are due at the time listed in the schedule. There are no undocumented exceptions. If you have an emergency or a school sanctioned exception, please contact the instructor or TA before the due date. This will help in adjusting your assignment deadlines (some documentation may be needed).

*No late submissions* (projects, quizzes, exams, etc.) are allowed unless special circumstances are subject to Georgia Tech rules (e.g., medical/family emergencies, and instructor approvals) **and** with the prior approval of the instructor. There are no exceptions to this rule.

### 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.

## 6. Resources for Students

Several resources are available if there are problems with LockDown Browser:

a) The Windows and Mac versions of LockDown Browser have a "Help Center" button located on the toolbar. Use the "System & Network Check" to troubleshoot issues. If an exam requires you to use a webcam, also run the "Webcam Check" from this area.
b) Respondus has a Knowledge Base available from support.respondus.com. Select the "Knowledge Base" link and then select "Respondus LockDown Browser" as the product. If your problem is with a webcam, select "Respondus Monitor" as your product.
c) If you're still unable to resolve a technical issue with LockDown Browser, go to support.respondus.com and select "Submit a Ticket". Provide detailed information about your problem and what steps you took to resolve it.

## 7. Course Schedule

| Date | Lecture (#) - Topic | Assignments Due | Due Date |
|---|---|---|---|
| **08/24** | (1) – Course Overview | | |
| **08/26** | (2) – Security Mindset | | |
| **08/31** | (3) – Operating Systems Security | Quiz - Lockdown Browser | 08/31 |
| **09/07** | **NO-CLASS (Holiday)** | Labtainer (1) - Buffer Overflow | 09/07 |
| **09/09** | (4) - Software Security | | |
| **09/14** | (5) – Authentication | | |
| **09/16** | (6) – Access Control | | |
| **09/21** | (7) – Database Security | Labtainer (2) - Metasploit | 09/21 |
| **09/23** | (8) – Malware | | |
| **09/28** | (9) – Firewalls | | |
| **09/30** | (10) – Intrusion Detection | Labtainer (3) - Snort | 09/30 |
| **10/05** | **NO-CLASS (Semester Break)** | | |
| **10/07** | (11) – Into to Cryptography | | |
| **10/12** | (12) – Symmetric Encryption | | |
| **10/14** | REVIEW for Exam 1 | Labtainer (4) - VPNlab | 10/14 |
| **10/19** | ***EXAM 1*** | | |
| **10/21** | (13) – Hashes and Public Key | | |
| **10/26** | (14) – AI Security | Labtainer (5) - Symkeylab | 10/26 |
| **10/28** | (15) – Security Protocols | | |
| **11/02** | (16) – Network Security | | |
| **11/04** | (17) – Cloud Infrastructure Security | Labtainer (6) - Machash | 11/04 |
| **11/09** | (18) – Security Auditing | | |
| **11/11** | (19) – Technology Risk Assessments | Labtainer (7) - Wireshark Intro | 11/11 |
| **11/16** | (20) – Cyber Security Management | | |
| **11/18** | (21) – Laws, Ethics and Privacy | | |
| **11/23** | (22) – Privacy and Anonymity | Labtainer (8) - TCP/IP | 11/23 |
| **11/25** | **NO-CLASS (Recess)** | | |
| **11/30** | (23) – Denial of Service Attacks | | |
| **12/02** | (24) – Email Security | | |
| **12/07** | REVIEW for Exam 2 | Labtainer (9) - Grassmarlin | 12/07 |
| **12/09** | **NO-CLASS (Reading Period)** | | |
| **12/14** | ***EXAM 2*** | | |