Computer Security

CIS 5370, Spring 2024
Department of Computer Science, Florida State University

Class time and location

Tuesday and Thursday, 06:35-7:50pm, HCB (Huge Classroom Building) 0215

Instructor

- Instructor: Xin Liu
  - Email: xliu5@fsu.edu (Subject line must start with "CompSecS24: " to be properly sorted and searched)
  - Home page: https://xinliulab.github.io/cis5370.html
- Office
  - 160 Love Building (LOV)
- Office Hours:
  - Tuesday, Thursday, 4:00 p.m. - 5:00 p.m., in-person and via zoom meeting (link https://fsu.zoom.us/my/xinliucs) and by appointments for in-person and additional zoom meetings.
  - Office hours for the TA: to be announced.

Rationale

Computers and communication technologies have been incorporated into many applications and have fundamentally changed many aspects of human activities. Unfortunately, the changes have also created new problems, from spyware that steals data, computer viruses and worms that destroy data, to network enabled weapons, to cyber wars that can disable companies and even countries (such as Stuxnet). All these problems are related to computer security. Due to its paramount importance, computer security is not just one academic research area. Many security products are installed on typical computers; in the United States, there are multiple federal agencies dedicated to computer security; the computer security is a multibillion industry that is estimated to grow steadily. Computer security related issues have been widely recognized in software development companies. As computer security techniques evolve continuously along with product improvements and new service opportunities, computer security is and will remain to be an important and valuable area in the perceivable future with new career opportunities. This course is designed to cover the basic principles and techniques for computer and system security so that you will know and be able to apply cyber security principles, identify common software vulnerabilities and develop common exploitations, and be able to develop and implement secure programs and systems. Note that exploiting systems without permission is illegal and you will be liable for your own actions.

Course Description

This course covers the fundamental principles in computer and system security, including security principles, implementation techniques, vulnerabilities, attacks, and defenses. Its goal is to help students understand how computer systems are secured, how various attacks work, what their fundamental causes are, how to defend against them, and how various defense mechanisms work. Equipped with the knowledge from this course, students will be able to evaluate the risks faced by computer systems, detect common vulnerabilities in software, use proper methods to protect their systems, design and implement software systems and applications that are secure against attacks, and more importantly, apply the learned security principles to solve real-world problems. Hands-on experience is an integral part of this course.

For selected vulnerabilities, the course uses a series of projects to help explain them; students can play with and experiment with them, instead of just reading and talking about them.

Prerequisites

CDA 3100 (Computer Organization), COP 4610 (Operating Systems), COP 4530 (Data Structure) - having a good understanding of instruction set architectures (registers, instruction encoding and decoding, and memory organization) and basic data types, data structures, function calls (calling conventions), and memory layout of programs, having a general understanding of computer security.

Course Objectives

Upon successful completion of this course of study, the student will be able to:

- Know the software and system security principles and how they are implemented
- Know the common vulnerabilities, how to exploit them, and how to harden systems
- Demonstrate the skills to exploit common vulnerabilities.
- Apply the principals and techniques to analyze the (in)security of real-world computer systems.
- Write secure code by avoiding common vulnerabilities and/or using security tools (such as fuzzing testing) to detect vulnerabilities.

Textbook and Course Materials

Required textbook: "Computer Security: A Hands-on Approach," by Wenliang Du (3rd Edition; ISBN: 978-17330039-5-7); 2nd Edition (ISBN: 978-1733003902) is acceptable as well.

"**Computer and Internet Security: A Hands-on Approach**," by Wenliang Du (3rd Edition; ISBN: 978-17330039-4-0) is also acceptable; 2nd Edition (ISBN: 978-1733003926) ISBN: 978-1733003933 is also acceptable.

Textbook resource website: https://www.handsonsecurity.net/index.html

Recommended readings: "Hacking: The Art of Exploitation, 2nd Edition" by Jon Erickson**;** this is a book with accurate and detailed descriptions and commands of common vulnerabilities and corresponding exploits.

"Information Security: Principles and Practice, 3rd Edition" by Mark Stamp; the book covers information security with an emphasis on software security.

In addition to the textbooks, papers and notes from the literature will be distributed along with the lectures.

Student Responsibilities

In-person attendance is required for this class. In case that it is necessary to skip a class, a student is required to notify the instructor beforehand; the absence is excused if it is allowed by the University Attendance Policy (see below). The penalty for each unexcused absence is a 10% reduction of attendance points (see the Grading Policy below); a student will receive 0 for attendance points if he or she has ten or more unexcused absences through the semester. In both excused and unexcused cases, the students are responsible for making up missed materials. Participation in in-class discussions and activities is also required. All submitted assignments and projects must be done by the author(s). It is a violation of the Academic Honor Code to submit other's work, and the instructor of this course takes the violations very seriously.

University Attendance Policy - Excused absences include documented illness, deaths in the family and other documented crises, call to active military duty or jury duty, religious holy days, and official University activities. These absences will be accommodated in a way that does not arbitrarily penalize students who have a valid excuse. Consideration will also be given to students whose dependent children experience serious illness.

For illness-related absences, the following standards apply:

- **U.S.-Based Medical Documentation:** All medical excuses must come from a U.S.-based medical facility or licensed professional who can be reasonably contacted by the instructor in English through a U.S.-based phone number or email address.
- **English-Language Medical Notes:** All medical documentation must be written or typed in English. This ensures clear verification and avoids subjective interpretation by the student.
- **Proactive Communication:** If these standards cannot be met, the student must inform the instructor proactively during the first week of class. In cases of illness, students should also contact *FSU Case Management Services* for assistance.

By adhering to these guidelines, we aim to maintain fairness and consistency in accommodating excused absences.

This course will cover certain techniques to exploit and break down known systems to demonstrate their vulnerabilities. It is **illegal**, however, to practice these techniques on others' systems. The students will be **liable** for their behavior and therefore consequences.

Assignments and Projects

About four homework assignments and a number of quizzes will be given along with the lectures and they need to be done individually and turned in. There will be about six hands-on exploitation projects, where exploitations need to be developed; most of them must be done individually and the ones that can be in a team of two will be marked clearly. Hacking challenges, known as the Capture The Flag (CTF) competitions will also be used. There will be a midterm exam and a final exam.

Grading Policy

Grades will be determined as follows:

Assignment	Percentages	Assignment	Percentages
Class Attendance (In-Class Quizzes)	8%	Midterm Exam	15%
Homework Assignments	12%	Final Exam (cumulative)	20%
CTF Competitions	10%	Hands-on Exploitation Projects	35%

Grading will be based on the weighted average as specified above and the following scale will be used (S is the weighted average on a 100-point scale):

Score	Grade	Score	Grade	Score	Grade
$93 \leq S$	A	$80 \leq S < 83$	B-	$67 \leq S < 70$	D+
$90 \leq S < 93$	A-	$77 \leq S < 80$	C+	$63 \leq S < 67$	D
$87 \leq S < 90$	B+	$73 \leq S < 77$	C	$60 \leq S < 63$	D-
$83 \leq S < 87$	B	$70 \leq S < 73$	C-	$S < 60$	F

Late Penalties

Assignments are due at the beginning of the class on the due date. Assignments turned in late, but before the beginning of the next scheduled class will be penalized by 10 %. Assignments that are more than one class period late will **NOT** be accepted.

Submission and Return Policy

All tests/homework assignments/projects will be returned as soon as possible after grading but no later than two weeks from the due date.

Tentative Schedule

Here the chapters refer to the ones in Computer Security: A Hands-on Approach, Third Edition. The chapters will be different generally in other editions and in Computer and Internet Security: A Hands-on Approach.

- Week 1: Introduction to Software, System, and Hardware Security (Chapter 1)
- Week 2: Software Security Principles and Fundamental Mechanisms (Chapter 2, papers, and handouts)
- Weeks 3-4: Software Vulnerabilities, Exploits, and Defenses (Chapters 2, 3, 4, 6, 9, and 10)
- Week 5: Binary Exploitation (Return-oriented Programming, Heap Exploitations, and More) (Chapters 5 and handouts)
- Week 6: Race Conditions and Side Channel Attacks (Chapters 7 and 8 and handouts)
- Week 7: Hardware Vulnerabilities and Attacks (Chapters 17 and 18)
- Week 8: Security-Key Encryption and Attacks (Chapter 19)
- Week 9: Midterm review and exam (March 8th, 2023)
- Week 10: Spring break; no classes
- Week 11: One-way Secure Hash Functions and Attacks (Chapter 20)
- Week 12: Public Key Infrastructure and MITM Attacks (Chapter 21)
- Week 13: Security Tools (Handouts)
- Week 14: Symbolic Execution (Handouts)
- Week 15: Secure Programming (Handouts)
- Week 16: Web and Mobile Security (Chapter 16 and handouts)
- Week 17: Final Exam Week
    - Final exam (cumulative), Tuesday, May 2nd, 2023, 08:00pm–10:00pm

Academic Honor Code

The Florida State University Academic Honor Policy outlines the University's expectations for the integrity of students' academic work, the procedures for resolving alleged violations of those expectations, and the rights and responsibilities of students and faculty members throughout the process. Students are

responsible for reading the Academic Honor Policy and for living up to their pledge to "...be honest and truthful and... [to] strive for personal and institutional integrity at Florida State University." (Florida State University Academic Honor Policy, found at http://fda.fsu.edu/academic-resources/academic-integrityand-grievances/academic-honor-policy.)

Assignments/projects/exams are to be done individually, unless specified otherwise. It is a violation of the Academic Honor Code to take credit for the work done by other people. It is also a violation to assist another person in violating the Code (See the FSU Student Handbook for penalties for violations of the Honor Code). The judgment for the violation of the Academic Honor Code will be made by the instructor and a third-party member (another faculty member in the Computer Science Department not involved in this course). Once the judgment is made, the case is closed and no arguments from the involved parties will be heard. Examples of cheating behaviors include:

- Discussing the solution for a homework question.
- Copying programs for programming assignments.
- Using and submitting existing programs/reports on the World Wide Web as written assignments.
- Submitting programs/reports/assignments done by a third party, including hired and contracted.
- Plagiarizing sentences/paragraphs from others without giving the appropriate references. Plagiarism is a serious intellectual crime, and the consequences can be very substantial.

Penalty for violating the Academic Honor Code: A 0 grade for the assignment /exam and a reduction of one letter grade in the final grade for all parties involved for each occurrence. A report will be sent to the department chairman for further administrative actions.

Americans With Disabilities Act

Students with disabilities needing academic accommodation should: (1) register with and provide documentation to the Student Disability Resource Center; and (2) bring a letter to the instructor indicating the need for accommodation and what type. Please note that instructors are not allowed to provide classroom accommodation to a student until appropriate verification from the Student Disability Resource Center has been provided. This syllabus and other class materials are available in alternative format upon request.

For more information about services available to FSU students with disabilities, contact the:

Student Disability Resource Center
874 Traditions Way
108 Student Services Building
Florida State University
Tallahassee, FL 32306-4167
(850) 644-9566 (voice) (850)
644-8504 (TDD)
sdrc@admin.fsu.edu
http://www.disabilitycenter.fsu.edu/

Additional Information

Free Tutoring from FSU - On-campus tutoring and writing assistance is available for many courses at Florida State University. For more information, visit the Academic Center for Excellence (ACE) Tutoring Services' comprehensive list of on-campus tutoring options at http://ace.fsu.edu/tutoring or contact tutor@fsu.edu. High-quality tutoring is available by appointment and on a walk-in basis. These services are offered by tutors trained to encourage the highest level of individual academic success while upholding personal academic integrity.

Syllabus Change Policy: Except for changes that substantially affect implementation of the evaluation (grading) statement, this syllabus is a guide for the course and is subject to change with advance notice.