Cross Layered Systems Security

EEL 4853 (Section 13H7)/ EEL 5855 (Section 13HB)
Class Periods: T – 2-3, R - 3
Location: CISE E107
Academic Term: Spring 2018

Instructor:

Name: Daniela Oliveira
Email Address: daniela@ece.ufl.edu
Office Phone Number: 352 392 6618
Office Hours: by appointment

Teaching Assistants:

Aokun Chen
Office location: MAE 206
Telephone: N/A
E-mail address: chenaokun1990@ufl.edu

Course Description

(3 credits) Develop an understanding of the principles of computer systems security (confidentiality, integrity and availability), especially as it crosses layers of abstraction (application layer, operating system, hardware and network). Students will learn challenges of building secure computer systems for each layer of abstraction with examples and study cases. Cutting edge research on these challenges will be discussed. Students will work on hands-on assignments and will read, review and present conference papers.

Course Pre-Requisites / Co-Requisites

- Programming knowledge & Principles of computer systems design knowledge
- Principles of computer systems design knowledge: EEL 5737/4736 or equivalent.

Course Objectives

To learn principles of computer security and practical aspects of building secure computer systems. Understand and critique cutting-edge research in this area.

Materials and Supply Fees

None

Required Textbooks and Software

Title: Introduction to Computer Security
Author: Michael Goodrich and Roberto Tamassia
Publication date and edition: 2010, 1st
ISBN number: 0321512944

Course Schedule

1) Principles of Computer Systems Security

(Paper reviews happen weekly)

Week 1: Why computer systems security matter?

Fundamental Concepts: Confidentiality, Integrity, Availability, Authenticity, Anonymity
Threats and Attacks

Week 2: Policy x Mechanism
Goals of Security
Design principles for building secure systems (Saltzer & Shroeder)
Human Issues
Ethics

2) Computer Systems Security at the Application Layer

Week 3: Software vulnerabilities and program exploitation
How the stack works (Assignment 1)

Week 4 and 5: Case study: exploiting programs via buffer overflows (Assignment 2)

Week 6: Malicious software:
Types: Insider attacks, viruses, Trojan horses, worms, rootkits, botnets, spyware, adware, APTs, and countermeasures

Week 7: Zero-day attacks
Malware detection mechanisms: signature-based and behavioral based
Malware analysis techniques: static vs dynamic (Exam 1)

Web security:

Week 8: Background information on the WWW;
Attacks on clients (session hijacking, phishing, privacy attacks, cross-site scripting and defenses)

Week 9: Attacks on servers (server side scripting, SQL injection, denial of service and defenses).
Case study: SQL injection, XSS scripts (Assignment 3)

3) Computer Systems Security at the Network Layer

Week 10: Network background: Introduction, protocols, and a brief overview of network layers;
Network attacks and threats: Denial of Service Attacks, DNS attacks, SYN flooding,

Week 11: TCP hijacking, ping of death, Smurf attack, among others
Firewalls and intrusion detection systems.
Case study: SYN flood attacks (Assignment 4)

4) Computer Systems Security at the Operating System Layer

Week 12: Background information on OSes
Access control mechanisms

Week 13: Process, Memory and File system Security
Race conditions

Week 14: Kernel Extensions/Drivers: a convenience or an evil?
Rootkits
Case Study: Time_of_check_To_Time_of_Use (TOCTTOU) vulnerabilities

Week 15: Paper presentations and Exam 2

Attendance Policy, Class Expectations, and Make-Up Policy
Attendance is expected. Cell phones and other electronic devices are to be silenced. No text messaging during class or exams. Requirements for class attendance and make-up exams, assignments, and other work are consistent with university policies that can be found at: https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx

Evaluation of Grades

Students learning will be evaluated as follows:

1) **Programming assignments (40%)**

These assignments represent the hands-on experience students need about computer systems security. Students have two options: the standard track and the advanced track.

A) Standard track:

1) Operation of the stack
2) Buffer overflow
3) Web security
4) Network security

B) Advanced track **(available only to EEL 5855 students):**

1) Operation of the stack
2) Buffer overflow
3) Work on a chosen security-related project or research (talk to me for opportunities).

2) **Midterm (20%):** Open book and open notes.

3) **Research paper reviews (15%).**

Students will read and review research papers in the area of security and send me the review by e-mail. You will write a review of each paper, discussing the paper's most significant contributions and weaknesses, and suggesting how the paper could be improved.

4) **Paper reading and presentation in class (15%).**

Students will choose a research paper in the security area from a list that I will provide, study this paper and make a conference-style presentation to the class in the end of the semester. ***The occurrence of this activity will depend on the number of students in class and the pace of class. If this activity was regarded as not possible by the instructor (e.g. large number of students in class, these points will be transferred to the final exam).***

5) **Final (20%):** Open book and open notes.

In summary:

Assignment	**Percentage of Final Grade**
Programming Assignments (4) or	40%

Programming Assignments (2) + Research Project – Students chooses option in the first 3 weeks of class	
Research paper reviews	10%
Exam 1	20%
Exam 2	20%
Presentation	10%
Participation (**extra credits**: in class, in Canvas answering questions of other students and posting hints for assignments)	10%
TOTAL	100% (discounting Participation)

Note: This course is co-listed with the graduate class. Students from the graduate section can select to do a research project of their choosing instead of doing the homework assignments.

Grading Policy

Percent	Grade	Grade Points
93 - 100	A	4.00
90 - 92	A-	3.67
87 – 89	B+	3.33
83 - 86	B	3.00
80 - 82	B-	2.67
77 - 79	C+	2.33
73 - 76	C	2.00
70 - 72	C-	1.67
67 - 69	D+	1.33
63 - 66	D	1.00
60 - 62	D-	0.67
0 - 59	E	0.00

In order to graduate, graduate students must have an overall GPA and a major GPA of 3.0 or better (B or better). Note: A "B-" average is equivalent to a GPA of 2.67, and therefore, it does not satisfy this graduation requirement.

More information on UF grading policy may be found at:
http://gradcatalog.ufl.edu/content.php?catoid=10&navoid=2020

Students Requiring Accommodations
Students with disabilities requesting accommodations should first register with the Disability Resource Center (352-392-8565, https://www.dso.ufl.edu/drc) by providing appropriate documentation. Once registered, students will receive an accommodation letter which must be presented to the instructor when requesting accommodation. Students with disabilities should follow this procedure as early as possible in the semester.

Course Evaluation

Students are expected to provide feedback on the quality of instruction in this course by completing online evaluations at https://evaluations.ufl.edu/evals. Evaluations are typically open during the last two or three weeks of the semester, but students will be given specific times when they are open. Summary results of these assessments are available to students at https://evaluations.ufl.edu/results/.

University Honesty Policy

UF students are bound by The Honor Pledge which states, "We, the members of the University of Florida community, pledge to hold ourselves and our peers to the highest standards of honor and integrity by abiding by the Honor Code. On all work submitted for credit by students at the University of Florida, the following pledge is either required or implied: "On my honor, I have neither given nor received unauthorized aid in doing this assignment." The Honor Code (https://www.dso.ufl.edu/sccr/process/student-conduct-honor-code/) specifies a number of behaviors that are in violation of this code and the possible sanctions. Furthermore, you are obligated to report any condition that facilitates academic misconduct to appropriate personnel. If you have any questions or concerns, please consult with the instructor or TAs in this class.

Software Use

All faculty, staff and student of the University are required and expected to obey the laws and legal agreements governing software use. Failure to do so can lead to monetary damages and/or criminal penalties for the individual violator. Because such violations are also against University policies and rules, disciplinary action will be taken as appropriate. We, the members of the University of Florida community, pledge to uphold ourselves and our peers to the highest standards of honesty and integrity.

Campus Resources:

Health and Wellness

U Matter, We Care:
If you or a friend is in distress, please contact umatter@ufl.edu or 352-392-1575 so that a team member can reach out to the student.

Counseling and Wellness Center: http://www.counseling.ufl.edu/cwc, and 392-1575; and the University Police Department: 392-1111 or 9-1-1 for emergencies.

Sexual Assault Recovery Services (SARS)
Student Health Care Center, 392-1161.

University Police Department at 392-1111 (or 9-1-1 for emergencies), or http://www.police.ufl.edu/.

Academic Resources

E-learning technical suppor*t*, 352-392-4357 (select option 2) or e-mail to Learning-support@ufl.edu. https://lss.at.ufl.edu/help.shtml.

Career Resource Center, Reitz Union, 392-1601. Career assistance and counseling. https://www.crc.ufl.edu/.

Library Support, http://cms.uflib.ufl.edu/ask. Various ways to receive assistance with respect to using the libraries or finding resources.

Teaching Center, Broward Hall, 392-2010 or 392-6420. General study skills and tutoring. https://teachingcenter.ufl.edu/.

Writing Studio, 302 Tigert Hall, 846-1138. Help brainstorming, formatting, and writing papers. https://writing.ufl.edu/writing-studio/.

Student Complaints Campus*:* https://www.dso.ufl.edu/documents/UF_Complaints_policy.pdf.

On-Line Students Complaints*:* http://www.distance.ufl.edu/student-complaint-process.