# EEL4930/EEL5934: Cross Layered Systems Security, Spring 2017

Jump to Today ✎ Edit

EEL 4930/EEL 5934 Cross Layered System Security

1. Catalog 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.
2. Pre-requisites:

- Programming knowledge: EEL 3834 or equivalent
- Principles of computer systems design knowledge: EEL 5737/4736 or equivalent.

3. 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.

4. Contribution of course to meeting the professional component (ABET only – undergraduate courses) NA.

5. Relationship of course to program outcomes: Skills student will develop in this course (ABET only undergraduate courses) NA.

6. Instructor –Dr. Daniela Oliveira

1. Office location: MAE 208
2. Telephone: (352) 392 6618
3. E-mail address: daniela@ece.ufl.edu
4. Class Web site: In Canvas (MyUFL)
5. Office hours: by appointment
6.

7. Teaching Assistant – Huixiang Chen

1. Office location:
2. Telephone:
3. E-mail address: **stanley.chen@ufl.edu (mailto:stanley.chen@ufl.edu)**

8. Meeting times: T - 2-3 and R - 3 (BLK 315)

9. Material and Supply Fees - None

10. Textbooks and Software Required –

1. Title: Introduction to Computer Security
2. Author: Michael Goodrich and Roberto Tamassia
3. Publication date and edition: 2010, 1st

ISBN number: 0321512944

11. Recommended Reading -

1. Title: Computer and Information Security Handbook
2. Author: John R. Vacca
3. Publication date and edition: 2013, 2nd
4. ISBN number: 123943973

12. Course Outline –

**1) Principles of Computer Systems Security**

- Why computer systems security matter?
- Fundamental Concepts: Confidentiality, Integrity, Availability, Authenticity, Anonymity
- Threats and Attacks
- 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**

- Software vulnerabilities
- Case study: buffer overflows
- Malicious software:
  - Types: Insider attacks, viruses, Trojan horses, worms, rootkits, botnets, spyware, adware, and countermeasures
  - Zero-day attacks
  - Malware detection mechanisms: signature-based and behavioral based

- Web security:
  - Background information on the WWW;
  - Attacks on clients (session hijacking, phishing, privacy attacks, cross-site scripting and defenses)
  - Attacks on servers (server side scripting, SQL injection, denial of service and defenses).
  - Case study: SQL injection

**3) Computer Systems Security at the Operating System Layer**

- Background information on OSes
- Access control mechanisms
- Process, Memory and File system Security
- Race conditions
- Kernel Extensions/Drivers: a convenience or an evil?
- Rootkits
- Case Study: Time_of_check_To_Time_of_Use (TOCTTOU) vulnerabilities

**5) Computer Systems Security at the Network Boundary**

- Network background: Introduction, protocols, and a brief overview of network layers;
- Network attacks and threats: Denial of Service Attacks, DNS attacks, SYN flooding,
- TCP hijacking, ping of death, Smurf attack, among others
- Firewalls and intrusion detection systems.

13. Attendance and Expectations - 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

14. Grading –

Students learning will be evaluated as follows:

- **Programming assignments(30%)**

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

1. **Standard track:**

- Buffer overflow
- Web security
- Network security

1. **B) Advanced track:**

- Buffer overflow exploit
- Work on a chosen security-related project or research.

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

- **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 20-min conference-style presentation to the class in the end of the semester. Students will also be required to review their classmates' presentation. Classmates' reviews are worth 5% of your grade. Your participation in the review process is worth 2% of your grade.

- **Research paper reviews(15%)**. You 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.

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

1. Grading Scale –

A C- will not be a qualifying grade for critical tracking courses. In order to graduate, students must have an overall GPA and an upper-division GPA of 2.0 or better (C or better)." Note: a C- average is equivalent to a GPA of 1.67, and therefore, it does not satisfy this graduation requirement. For more information on grades and grading policies, please visit: https://catalog.ufl.edu/ugrad/current/regulations/info/grades.aspx

1. Make-Up Exam Policy - If you have a University-approved excuse and arrange for it in advance, or in case of documented emergency, a make-up exam will be allowed

| A | A- | B+ | B | B- | C+ | C | C- | D+ | D | D- | E |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 93-100 | 90-92 | 87-89 | 83-86 | 80-82 | 77-79 | 73-76 | 70-72 | 67-69 | 63-66 | 60-62 | 0-59 |

and arrangements can be made for making up missed work. University attendance policies can be found at: https://catalog.ufl.edu/ugrad/current/regulations/info/attendance.aspx

Otherwise, make-up exams will be considered only in extraordinary cases, and must be taken before the scheduled exam. The student must submit a written petition to the instructor two weeks prior to the scheduled exam and the instructor must approve the petition.

1. Honesty Policy – All students admitted to the University of Florida have signed a statement of academic honesty committing themselves to be honest in all academic work and understanding that failure to comply with this commitment will result in disciplinary action. This statement is a reminder to uphold your obligation as a UF student and to be honest in all work submitted and exams taken in this course and all others.

"...failure to comply with this commitment will result in disciplinary action compliant with the UF Student Honor Code Procedures (http://www.dso.ufl.edu/sccr/procedures/honorcode.php)

1. Accommodation for Students with Disabilities – Students Requesting classroom accommodation must first register with the Dean of Students Office. That office will provide the student with documentation that he/she must provide to the course instructor when requesting accommodation.
2. UF Counseling Services – Resources are available on-campus for students having personal problems or lacking clear career and academic goals. The resources include:

- · UF Counseling & Wellness Center, 3190 Radio Rd, 392-1575, psychological and psychiatric services.
- · Career Resource Center, Reitz Union, 392-1601, career and job search services.
- 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.

23. Students are expected to provide feedback on the quality of instruction in this course by completing online evaluations at **https://evaluations.ufl.edu** **(https://evaluations.ufl.edu/)** . 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/** **(https://evaluations.ufl.edu/results/)** .

# Course Summary:

| Date | Details | |
|---|---|---|
| Fri Jan 20, 2017 | paper 1 (https://ufl.instructure.com/courses/338024/assignments/3206371) | due by 11:59pm |
| Fri Jan 27, 2017 | paper 2 (https://ufl.instructure.com/courses/338024/assignments/3208953) | due by 11:59pm |
| Fri Feb 3, 2017 | paper3 (https://ufl.instructure.com/courses/338024/assignments/3211672) | due by 11:59pm |
| Tue Feb 7, 2017 | Defusing a Binary Bomb (https://ufl.instructure.com/courses/338024/assignments/3210094) | due by 11:59pm |
| Fri Feb 10, 2017 | paper4 (https://ufl.instructure.com/courses/338024/assignments/3214405) | due by 11:59pm |
| Mon Feb 20, 2017 | paper5 (https://ufl.instructure.com/courses/338024/assignments/3217194) | due by 11:59pm |
| Wed Mar 1, 2017 | The Buffer Bomb (https://ufl.instructure.com/courses/338024/assignments/3217698) | due by 11:59pm |
| Fri Mar 10, 2017 | paper6 (https://ufl.instructure.com/courses/338024/assignments/3224446) | due by 11:59pm |
| Mon Mar 27, 2017 | paper7 (https://ufl.instructure.com/courses/338024/assignments/3230731) | due by 11:59pm |
| Wed Mar 29, 2017 | Web Security (https://ufl.instructure.com/courses/338024/assignments/3229250) | due by 11:59pm |
| Fri Apr 7, 2017 | paper8 (https://ufl.instructure.com/courses/338024/assignments/3235521) | due by 11:59pm |
| Tue Apr 11, 2017 | Network security 0-1 (https://ufl.instructure.com/courses/338024/assignments/3236928) | due by 11:59pm |
| Wed Apr 19, 2017 | paper 9 (https://ufl.instructure.com/courses/338024/assignments/3241472) | due by 11:59pm |
| Sun Apr 23, 2017 | Network security 2 (https://ufl.instructure.com/courses/338024/assignments/3243055) | due by 11:59pm |
| | Final (https://ufl.instructure.com/courses/338024/assignments/3254104) | |
| | Midterm (https://ufl.instructure.com/courses/338024/assignments/3235629) | |