EC ENGR 117 "Computer System Security"

Course Information

Instructor: Yuan Tian(yuant@ucla.edu)
TA:
Class Location:
Class Time:
Yuan's office Hours:

Grading

Homework assignments (30%)
Literature review (15%)
Participation in feedback to others' work (5%)
Course project (50%)

- Three presentations
  - Introduction Presentation (5%)
  - Midterm (5%)
  - Final (15% from Yuan's and peer's evaluation)
- Two reports
  - Midterm (5%)
  - Final (10%)
- Evaluation from teammates (10%)

Teaching evaluation (1% bonus)

Syllabus

Week	Date	Part A (50 min)	Part B (50 min)	Preparation
	Part 1: Software Security			
1	09/26	Course introduction + Logistics	***Lecture:*** Security principles	Reading: [1] Complete course survey
	09/28	30-sec Madness ***Lecture:*** Buffer overflow and format string	***Lecture:*** Buffer overflow and format string	Reading: [1, 2] Finish your slide before class: Google Slides

		attacks	attacks	(editable only with UCLA accounts) ***Due*** ⏰(Optional)***:*** If you want to propose your own project ideas, please email Yuan one page slide about your idea by Sep 30.
2	10/03	***Lecture:*** Defense- ASLR ***Project:*** Idea briefings	***Lecture:*** Return-oriented programming	Reading: [1, 2] ***Due*** ⏰***:*** Lit. Review paper selection and team form up, sign up here
	10/05	***Lecture:*** Defense- CFI ***Project:*** Idea briefings	***Lab:*** Software security	Reading: [1] Slides for the Lab Bring laptops to class Install Oracle Virtual Box before class Download the virtualbox image before class Please follow the instruction to install the Virtual Machine ***Due*** ⏰***:*** Project team signup **(Oct 7)**
	Part 2: Web Security			
3	10/10	***Lecture:*** Web security basics	***Lit. Review:*** Paper# A1	Reading: [1, 2] ***Due*** ⏰***:*** Project team formed up, team captain selected.
	10/12	***Lit. Review:*** Paper# A2, A3	***Lecture:*** Attacks: XSS and CSRF	Reading: [1, 2] ***Due*** ⏰***:*** Assignment 1
4	10/17	***Guest Lecture:*** Fish Wang Arizona State University	***Lecture:*** Defenses: Content Security Policy ***Project:*** Get to know your teammates	Reading: [1]
	10/19	***Lecture:***	***Lab:***	Reading: [1]

		Insecure HTTPS	Web Security	Bring laptops to class Software: Windows User: tightVNC Macs User: You have a build-in tool called “Screen Sharing” Lab Slides
5	10/24	***Project:*** Introduction presentation		***Due ⏰:*** Project introduction slides
		Part 3: Network Security		
	10/26	***Lecture:*** Internet Protocol Security	***Lecture:*** DDoS Attacks and Network Defenses	Reading: [1, 2]
6	10/31	***Lecture:*** Penetration testing + Heartbleed attack ***Project:*** Feedback and discussion time	***Lecture:*** Network privacy, Anonymity, and Censorship	***Due ⏰:*** Assignment 2
	11/02	***Lab:*** Network Security	***Lit. Review:*** Paper# B1, B2, B3	Reading:[1] Reading: [1] Bring laptops to class Software: Windows User: tightVNC Macs User: You have a build-in tool called “Screen Sharing” Lab Slides
		Part 4: Mobile Security		
7	11/07	***Lecture:*** Mobile Systems and Security Challenges	***Lecture:*** Mobile authentication	Reading: [1]
	11/09	***Project:*** Midterm Presentation		***Due ⏰:*** Project midterm presentation slides, Project midterm report

8	11/14	***Guest Lecture:*** Sebastian Porst, Google, Android Security	***Lecture:*** Mobile privacy	Reading: [1]
	11/16	***Lecture:*** Best Practice for Mobile Security Reverse engineering mobile apps	***Lab:*** Mobile security	Bring laptops to class Lab Slides
		Part 5: New topics in security		
9	11/21	***Lecture:*** Cryptocurrency overview ***Project:*** Feedback and discussion time	***Guest Lecture:*** Shumo Chu Manta Network	Reading: [1] ***Due ⏰:*** Assignment 3
	11/23	***Lit. Review:*** Paper# C1, C2, C3, C4	***Lecture:*** IoT security and privacy	Reading: [1]
10	11/28	***Lecture:*** Machine learning for security	***Lecture:*** Machine learning security	Reading: [1]
	11/30	***Project:*** Final Project Presentation Vote for best presentation award! 🏆 (Vote for the best presentation! Pizza, donuts, and have fun!!)		***Due ⏰:*** Final project presentation slides
	12/2	***No class***		***Due ⏰:*** Final project report ***Due ⏰:*** Final project presentation evaluation Course Evaluation Form (1% bonus)
	12/4	***No class***		***Due ⏰:*** Teammate Evaluation Form

Quick links

Course website:
https://sites.google.com/view/188sec

Piazza site for this course:
https://piazza.com/class/l8gngaomf2x6eh/

Anonymous feedback form:
https://forms.gle/LfJZS6kEB4RExh3x9

Groupme for chatting with classmates:
https://groupme.com/join_group/89945797/smj2jFAd

Literature Review Sign Up:
https://docs.google.com/spreadsheets/d/1tvPBh-13RcO0C1mJGlOPrUu1jyvpfPJGMJVNFWrmv_U/edit#gid=0

Project Sign Up:

Project team assignment:
https://docs.google.com/spreadsheets/d/16Ferr4ZKHMnAZGseGfmyH672SMnpfdgQg6WrghqNMh8/edit#gid=0

Project idea list
https://docs.google.com/spreadsheets/d/16Ferr4ZKHMnAZGseGfmyH672SMnpfdgQg6WrghqNMh8/edit#gid=0

Google form for group signup
https://docs.google.com/forms/d/e/1FAIpQLSeFoeCeIc9lfOUk3WJxqNSgINMiTtNPhLL284804IuojXZg2A/viewform?usp=sf_link

Information about the research project:
https://docs.google.com/document/d/1KcfFS5uXtczaYLXDM2c5c2Vn2MchQbEyke1NPteP6ak/edit#

Information about the practical project:
https://docs.google.com/document/d/1c_Ba0w5IWN-bXnmLoJc_YnqGKF5juwIWdYxx3CtqUSg/edit

Project Final Presentation Evaluation Form:
https://docs.google.com/forms/d/e/1FAIpQLSf6jOuYo3si_Xd4zli_yBsuSek89_s3q_Ah6-f-ig6TM2pGTg/viewform?usp=sf_link

Literature Review Presentation Evaluation Form:
https://docs.google.com/forms/d/e/1FAIpQLSeNa9ECR-y6aGGajfTYRW2vo0cApePSTzM0vL0Nwnjt1Y6F0A/viewform?usp=sf_link

Final Project Teammate Evaluation Form:
https://docs.google.com/forms/d/e/1FAIpQLSe7TMMI1r6gji0oAeFhI1CpL6uFeJ789VC6g9O_8EA8YKmRVg/viewform?usp=sf_link

*Note that all forms are editable **only** with UCLA G-Suite accounts (g.ucla,edu)*

Guidelines

Literature Review:

- Presentation Preparation
  - Time distribution: 10 minutes of presentation + 2 minutes of Q&A
  - Things to cover in the presentation:
    - ⅓ time goes to background (what have been done before this paper, presenters must explain the topic in an easy-to-understand manner, assuming the audience has little background
    - ⅓ time goes to what this paper does
    - ⅓ time goes to what YOU think are the unique advantages and limitations of the system. What will be the future work needed? How has the field evolved after this paper (hint: look into papers that cited the paper you present)?

- Presentation Evaluation:
  - Yuan's evaluation (weigh 50%) and peer evaluation (weigh 50%) using Google form
  - Will be evaluated by the following criteria
    - Presentation clarity (sufficient details, use of examples etc.)
    - Comprehension of materials (robust Q&A)
    - Audience engagement (tips: tell a story, use visuals, ask thought-provoking questions to your audience etc.)

Course Project:
Proposal Presentation:

- 3 minutes of presentation + 5 minutes of Q&A
- Prepare up to 5 slides (with no/minimum animation)
- Put team ID on all slides
- Get full credits for attendance (no other evaluation criteria)

Midterm Presentation:

- 5 minutes of presentation + 5 minutes of Q&A
- Prepare up to 5 slides (with no/minimum animation)
- Put team ID on all slides
- Get full credits for attendance (no other evaluation criteria)

Final Presentation:

- Presentation Preparation
    - 10 minutes of presentation (pre-recorded) + 5 minutes of Q&A
    - Put team ID on all slides

- Presentation Evaluation
    - Yuan's evaluation (weigh 50%) and peer evaluation (weigh 50%) using Google form
    - Will be evaluated by the following criteria:
        - Vision (show your project is part of a big story)
        - Impact (show importance of the problem which your project tries to tackle)
        - Novelty (show creativity in ideas, and in solutions)
        - Practicality (show evaluation results) *bonus point*

- Project Mid-term Report
    - Will be evaluated by the following criteria:
        - Statement of the high-level problem area
        - Description of the focused project topic and potential solution
        - Outlining the project goals and timeline
        - Preliminary results *bonus point*

- Final Report
    - Will be evaluated by the following criteria:
        - Vision (show your project is part of a big story)
        - Impact (show importance of the problem which your project tries to tackle)
        - Novelty (show creativity in ideas, and in solutions)
        - Practicality (show evaluation results) *bonus point*

Class Attendance and Good Practices:

Read papers that are scheduled to be presented, before class

Ask Questions (Steve Jobs' 2005 Stanford Commencement Address *TLDR:* **Stay hungry and stay foolish, don't be afraid of asking questions**)

Actively participate in discussions (Elon Musk's letter *TLDR:* **If you are not adding values to discussions, you are wasting your time**)

Use the Google Forms links to provide feedback to peers' literature review and project presentations (***links will be provided during classes***).

Grade Distribution

Letter Grade Scheme

A+	100% to 97%
A	96.99% to 93%
A-	92.99% to 90%
B+	89.99% to 83.33%
B	83.32% to 76.67%
B-	76.66% to 70%
C+	69.99% to 67%
C	66.99% to 63%
C-	62.99% to 60%
D+	59.99% to 57%
D	56.99% to 50%
F	49.99% to 0%

P-NP Grading

P	100% to 70%
NP	< 70% to 0%

Course Policy

Academic Policies:

Students are expected to follow all academic policies set forth by departments, colleges, and the university. A (likely incomplete) list of such policies is included here for ease of access.

- **UCLA Student Conduct Code**
- **UCLA IT Service Policy**

In addition, students are expected to adhere to these additional policies put in place for this course.

- **Collaboration Policy**: For individual assignments, discussion about the assignment is encouraged, but students must complete the assignment individually - this means no sharing of code, figures, algorithms, design, etc. beyond discussing the approach to be taken. Copying and sharing are cheating.
- **Plagiarism & Citation Policy**: Do not copy, paraphrase, or mention any existing material without a full bibliographic citation of where the material was obtained from - in the case of direct inclusion of written material, use quotations appropriately. Plagiarism is cheating.
- **Wiki Policy**: Do not cite Wikipedia or other similar wiki pages - these are not reliable sources of information. Most reasonably good wiki pages include their own references, so follow those links and cite those sources instead.
- **Grading Policy**: We grade work to the best of our ability based on what was submitted by students, but we sometimes make mistakes. We're happy to re-grade any work or to discuss how grades were determined.
- **Deadlines**: All deadlines are fixed by the first day of class. Extensions are extremely rare, so plan ahead. Late submission of individual assignments will be accepted for up to two (2) days after the deadline, with a 10% per day penalty. No other course deliverables will be accepted for credit after the corresponding deadline.

Ethics of Security Education and Research:

As with any course or project related to security, students should be aware of ethical implications of what they are learning and doing. This includes, but is not limited to the following:

- Research, development, and experimentation with sensitive information, attack protocols, misbehavior, etc. should be performed with the utmost care and respect. Students are responsible for seeking IRB approval when needed and understanding potential legal implications of actions taken outside of a controlled environment. Students are expected to follow a strict ethical code, especially when dealing with potentially sensitive information.
- Students are encouraged to consult with the instructor if there is any shred of uncertainty around ethical or legal implications.

University Policies and Support for Students

Academic Integrity

UCLA is a community of scholars. In this community, all members including faculty, staff and students alike are responsible for maintaining standards of academic honesty. As a student and member of the University community, you are here to get an education and are, therefore,

expected to demonstrate integrity in your academic endeavors. You are evaluated on your own merits. Cheating, plagiarism, collaborative work, multiple submissions without the permission of the professor, or other kinds of academic dishonesty are considered unacceptable behavior and will result in formal disciplinary proceedings usually resulting in suspension or dismissal. See the Dean of Students website. for more information.

[source: Dean of Students syllabus statement (syllabus)]

Accommodations for Students with Disabilities

If you are already registered with the Center for Accessible Education (CAE), please request your Letter of Accommodation in the Student Portal. If you are seeking registration with the CAE, please submit your request for accommodations via the CAE website. Students with disabilities requiring academic accommodations should submit their request for accommodations as soon as possible, as it may take up to two weeks to review the request. For more information, please visit the CAE website, visit the CAE at A255 Murphy Hall, or contact us by phone at (310) 825-1501.

[source: Center for Accessible Education (Faculty Questions)]

Resources for Students

UCLA provides resources if you are feeling overwhelmed and need personal and/or academic assistance.

Please see the Red Folder for more information.

Title IX and Equity, Diversity and Inclusion

Advocacy and Confidential Services:

Please note that Title IX prohibits gender discrimination, including sexual harassment, domestic and dating violence, sexual assault, and stalking. If you have experienced sexual harassment or sexual violence, you can receive confidential support and advocacy at the CARE Advocacy Office for Sexual and Gender-Based Violence, 205 Covel Commons, Los Angeles, CA, 90095, care@careprogram.ucla.edu, (310) 206-246 5. Counseling and Psychological Services (CAPS) provides confidential counseling to all students and can be reached 24/7 at (310) 825-0768.

Reporting and Non-confidential Services:

Your professor is required under the UC Policy on Sexual Violence and Sexual Harassment to inform the Title IX Coordinator should he become aware that you or any other student has experienced sexual violence or sexual harassment. In addition, You can also report sexual violence or sexual harassment directly to the University's Title IX Coordinator, 2255 Murphy Hall,

titleix@equity.ucla.edu , (310) 206-3417. Reports to law enforcement can be made to UCPD at (310) 825-1491.

Engineering EDI Resources:

There are a number of specific resources on Equity, Diversity, and Inclusion available to students in the Samueli School of Engineering, including trained faculty officers in each department who can be consulted if you have a question on EDI issues and are not sure where else to turn. Please see https://samueli.ucla.edu/equity-diversity-and-inclusion for information.

Acknowledgement:

We appreciate the materials from Dan Boneh, David Brumley, Wenliang Du, John C. Mitchell, Vyas Sekar, and Patrick Tague.

Learning Objectives/Competencies for Computer System Security Class

Knowledge outcomes:
Students will learn the core concepts in software vulnerabilities analysis and defenses, web security vulnerabilities and defenses, mobile security and privacy, network security and privacy, as well as emerging topics in computer security. The students will also learn security principles and threat modeling so that they will be able to use them in different kinds of cybersecurity problems.

Skills outcomes:

- Understanding Exploit Techniques: Students will gain knowledge and skills in understanding various exploit techniques used by adversaries to compromise computer systems.
- Using Security Tools: Students will learn how to use a variety of security tools and software to assess and enhance the security of computer systems.
- Designing and Implementing Secure Systems: Students will develop the ability to design and implement secure computer systems, considering best practices and security principles.
- Effective Communication: Students will effectively communicate security concepts, findings, and recommendations both in writing and verbally, demonstrating their ability to convey complex technical information to various audiences.
- Responsible Collaboration: Students will collaborate with peers on security projects, fostering teamwork and shared responsibility for security outcomes.

Attitudes and values outcomes:

- Ethical Awareness: Students will develop a strong sense of ethical principles and values related to computer security, emphasizing the importance of responsible and lawful behavior in the field.
- Commitment to Security: Students will develop a commitment to ensuring the security and integrity of computing systems and recognize the broader societal implications of their work.

Behavioral outcomes:

- Application of Knowledge and Skills: Students will apply their knowledge and skills in real-world scenarios, demonstrating their ability to assess, enhance, and maintain the security of computing systems.
- Participation in Research: Through the course project on cutting-edge security research, students will contribute to the field by addressing relevant security issues and advancing knowledge in the domain.

- Continuous Learning: Students will recognize the need for ongoing learning and adaptation in the ever-evolving field of computer security, showing a commitment to staying current with the latest developments and threats.