CS 161: Computer Security
Spring 2018

Instructors:

Raluca Ada Popa (office hours: Tuesday, 2:15 - 3:15 PM at Soda 729)
and an awesome team of talented TAs

Lectures:

Tuesday/Thursday 12:30 - 2:00 PM, 155 Dwinelle

Addresses:

Web page: https://inst.eecs.berkeley.edu/~cs161/

Announcements, questions: the class Piazza site, which you sign up for here.

Feel free to mark your question as private if you don't want other students to see it.

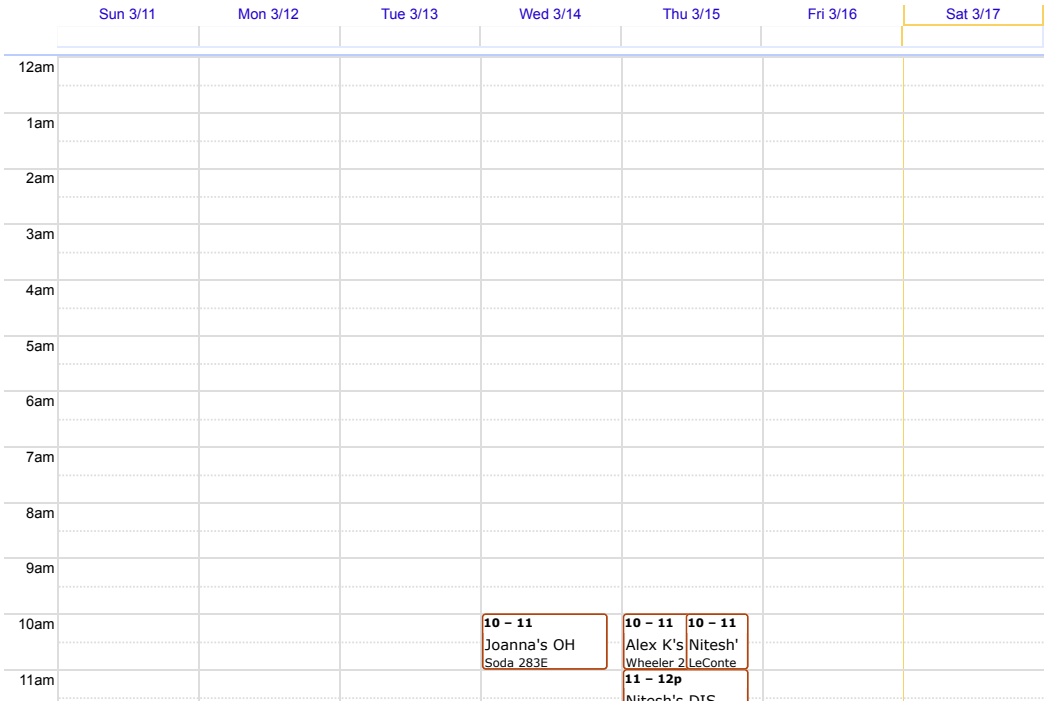
Lectures:

The lecture schedule is subject to change and will be revised as the course progresses.

Date	Topic	Readings	Links
Tu 1/16	Introduction & Memory Safety 1	[optional: G&T § 1.1, Craft § 1-1.1, 1.3]	slides
Th 1/18	Memory Safety 2	Notes from Dave Wagner from Sp16. [G&T § 3.4, Craft § 6.1-6.3]	slides
Tu 1/23	Memory Safety 3; OS Security 1	Notes on Reasoning About Code and Secure Software Development. [Craft § 6.5-6.7] Eevee's guide for Testing for People Who Hate Testing	slides
Th 1/25	Security Principles & Sandboxes	Notes on Design Patterns and Security Principles Optional reading Apple iOS Security Guide fork, clone, chroot, seccomp, shm_overview man pages The Chromium Sandbox	slides
Tu 1/30	Symmetric-key Encryption	Notes (sections 1-4) [G&T § 8.1.0, 8.1.1, 8.1.3, Craft § 7.1, 7.3.2, 7.3.3]	slides
Th 2/1	Block Ciphers	Notes (sections 5-6) [G&T § 8.1.6, 8.1.7]	slides
Tu 2/6	Public-key Exchange	Notes [G&T § 8.2.1, 8.2.4, Craft § 7.5]	slides
Th 2/8	Public-key Encryption and Hashing	Notes, section 2	slides
Tu 2/13	Integrity, authentication, and public-key signatures	Notes	slides
Th 2/15	Midterm Exam 1		
Tu 2/20	Passwords and Key Management	[G&T § 8.3] Notes	slides
Th 2/22	Certificates, TLS Part 1	The WoSign Saga TLS Wikipedia [G&T § 8.3]	slides
Tu 2/27	TLS Part 2, Network Security 1	Networking terminology quick-reference. [G&T § 5.1-5.1.2, 5.3-5.3.1, 5.4-5.4.2, 6.1-6.1.2, 7.1-7.1.1; Craft § 5.1,	slides

		5.4.1]	
Th 3/1	Network Security 2	[G&T § 6.1.3 (pp. 278-284)]	slides
Tu 3/6	Network Security 3	Google's public DNS server security DNS over TLS DNS over HTTPS (not TLS!)	slides
Th 3/8	Firewall Detection		slides
Tu 3/13	Network Security 5		slides
Th 3/15	Web Security 1	[G&T § 7.1.1, 7.1.3-7.1.4, 7.3.1-7.3.2, 7.3.4, 7.3.6; Craft § 12.1.1, 12.1.2, 12.1.3] Web Security: Are You Part Of The Problem?	slides
Tu 3/20	Web Security 2		
Th 3/22	Web Security 3		
Tu 3/27	**Spring Recess**		
Th 3/29	**Spring Recess**		
Tu 4/3	Web Security 4		
Th 4/5	Web Security 5		
Tu 4/10	Misc 1		
Th 4/12	Misc 2		
Tu 4/17	Misc 3		
Th 4/19	Misc 4		
Tu 4/24	Misc 5		
Th 4/26	Review		
Tu 5/1	**RRR Week**		
Th 5/3	**RRR Week**		
Th 5/10	**Final Exam at 3-6 PM**		

Top Lecture Staff Sections Homeworks Projects Exams Policies Piazza



Events shown in time zone: Pacific Time

Calendar

Staff

Raluca Ada Popa

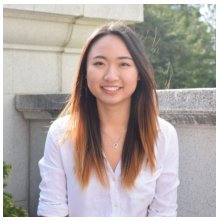
Keyhan Vakil

Won Park

Aditya Chopra

Karthik Shanmugam

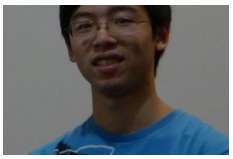
Alex Kumamoto



Joanna Yang

Top **Lecture** **Staff** **Sections** **Homeworks** **Projects** **Exams** **Policies** **Piazza**

Alex Zhang



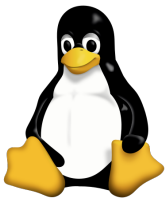
Richard Hu

Kevyn

Michael McCoyd

Cameron Rasmussen

Nitesh Mor



Tux

Office hours:

Time	Room	TA
Mo 12:00 - 1:00 PM	Soda 341B	Karthik
Mo 2:00 - 3:00 PM	Soda 611	Keyhan
Mo 3:00 - 5:00 PM	Soda 341A	Won
Tu 3:00 - 4:00 PM	Soda 283E	Alex Z.
We 10:00 - 11:00 AM	Soda 283E	Joanna
We 1:00 - 2:00 PM	Soda 651	Michael
We 1:00 - 2:00 PM	Soda 283E	Joanna
We 2:00 - 3:00 PM	Soda 341B	Richard
We 3:00 - 4:00 PM	Soda 611	Cameron
We 6:00 - 7:00 PM	Soda 283E	Aditya
Th 2:00 - 3:00 PM	Soda 651	Nitesh
Th 3:00 - 4:00 PM	Soda 611	Cameron
Th 4:00 - 5:00 PM	Soda 651	Nitesh
F 2:00 - 3:00 PM	Soda 651	Keyhan
F 3:00 - 4:00 PM	Soda 283E	Alex K.
F 5:00 - 7:00 PM	Soda 341A	Kevyn

Discussion section handouts:

- Discussion 1: GDB and x86 Assembly (worksheet) (solution)
- Discussion 2: Software Vulnerabilities and Security Principles (worksheet) (solution)
- Discussion 3: Symmetric Encryption (worksheet) (solution)
- Discussion 4: Asymmetric Encryption and Hashing (worksheet) (solution)

Top Lecture Staff Sections Homeworks Projects Exams Policies Piazza

Discussion 1: [illegible], PCs and GDT [Worksheet] [Solution]

Discussion section times:

Time	Room	TA
Tu 2:00PM	Latimer 105	Alex Z.
Tu 2:00PM	Wheeler 104	Michael
Tu 3:00PM	Soda 320	Keyhan
Tu 3:00PM	Hearst Gym 242	Karthik
Tu 3:00PM	Barrows 587	Cameron
Tu 3:00PM	Dwinelle 246	Michael
Tu 4:00PM	Soda 320	Richard
Tu 4:00PM	Wheeler 108	Joanna
Tu 4:00PM	Hearst Gym 242	Cameron
Tu 5:00PM	Dwinelle 242	Joanna
We 2:00PM	Etcheverry 3119	Keyhan
We 2:00PM	Wheeler 224	Won
We 3:00PM	Barrows 185	Won
We 3:00PM	Barrows 175	Kevyn
We 4:00PM	Wheeler 202	Won
We 4:00PM	Dwinelle 229	Kevyn
We 5:00PM	Wheeler 224	Aditya
Th 10:00AM	LeConte 385	Nitesh
Th 10:00AM	Wheeler 224	Alex K.
Th 11:00AM	Hildebrand B51	Nitesh

Homeworks:

There will be four homework assignments. Homeworks will be submitted electronically via Gradescope. Homework solutions must be legible; we may mark off for difficult-to-read solutions, or even refrain from grading them entirely. **No late homeworks accepted.**

- Homework 1: due Monday, January 29th, at 11:59PM
- Homework 2: due Wednesday, February 14th, at 11:59PM
- Homework 3: due Friday, March 23rd, at 11:59PM

Projects

There will be 3 course projects. We will penalize late project submissions as follows: less than 24 hours late, you lose 10%; less than 48 hours late, you lose 20%; less than 72 hours late, you lose 40%; at or after 72 hours, late submissions **no longer accepted**. (There are no "slip days".)

Note that this late policy applies only to projects, not homeworks (homeworks cannot be turned in late).

- Project 1: Instructions, VM Image and Supplement
- Project 2: Specification, Starter Code, Documentation

Exams

There will be two midterms and a final exam.

- Midterm 1, Thursday February 15, 12:30-2:00 PM
- Midterm 2, TBA
- Final, Thursday May 10th, 3-6 PM

Top Lecture Staff Sections Homeworks Projects Exams Policies Piazza

Grading

We will compute grades from a weighted average, as follows:

- Homeworks: 16%
- Projects: 24%
- Midterms: 30%
- Final exam: 30%

Course Policies

Contact information: If you have a question, the best way to contact us is via the class Piazza site. The staff (instructors and TAs) will check the site regularly, and if you use it, other students will be able to help you too. **Please avoid posting answers or hints on homework/project questions before the homework/project is due.**

If your question is personal or not of interest to other students, you are encouraged to mark the question as private on Piazza: select "Post to: Individual Student(s)/Instructor(s)" at the top and then type "Instructors" in the field underneath it. If you wish to talk with one of us individually in person, you are welcome to come to any of our office hours. We prefer that use these methods instead of sending us email; email regrettably does not scale well to a class of this size.

Announcements: The instructors and TAs will periodically post announcements, clarifications, etc. to the Piazza site. Hence it is important that you check it reguarly throughout the semester.

Prerequisites: The prerequisites for CS 161 are CS 61B, CS61C, and CS70. **We assume basic knowledge of Java, C, and Python.** You will need to have a basic familiarity using Unix systems.

Collaboration: Homeworks will specify whether they must be done on your own or may be done in groups. Either way, *you must write up your solutions entirely on your own*. For homeworks, you must **never** read, see, or copy the solutions of other students, and you must not allow other students to see your solutions. For projects, you must never read, see, or copy the code or solutions of other students (except for your project partner, for group projects), and you must not allow other students (except for your project partner) to see your solutions or code.

You may use books or online resources to help solve homework problems, but you *must always credit all such sources* in your writeup and you must never copy material verbatim. Not only is this good scholarly conduct, it also protects you from accusations of theft of your colleagues' ideas. You must not ask for homework/project solutions on Stack Overflow or other online sites; you may ask for help with conceptual questions, but you must credit your sources. You must not receive help on homeworks or projects from students who have taken the course in previous years, and you must not review homework or project solutions from previous years.

You must ensure that your solutions will not be visible to other students. If you use Github or another source control system to store your solutions electronically, you must ensure your account is configured so your solutions are not publicly visible. If you use Github, Github offers free student accounts that allow you to keep your solutions private; please use one.

We believe that most students can distinguish between helping other students understand course material and cheating. Explaining a subtle point from lecture or discussing course topics is an interaction that we encourage, but you should never read another student's homework/project solution or partial solution, nor have it in your possession, either electronically or on paper (except for your project partner, for group projects). You must never share your solutions, or partial solutions, with another student (other than your project partner, for group projects), not even with the explicit understanding that it will not be copied -- not even with students in your homework group. You must write your homework solution strictly by yourself.

Warning: Your attention is drawn to the Department's Policy on Academic Dishonesty. In particular, you should be aware that copying or sharing solutions, in whole or in part, from other students in the class *or any other source* without acknowledgment constitutes cheating. Any student found to be cheating risks automatically failing the class and referral to the Office of Student Conduct.

Ethics: We will be discussing **attacks** in this class, some of them quite nasty. **None of this is in any way an invitation to undertake these attacks in any fashion** other than with **informed consent** of all involved and affected parties. The existence of a security hole is no excuse. These issues concern not only professional ethics, but also UCB policy and **state and federal law**. If there is any question in your mind about what conduct is allowable, contact the instructors first.

Computer accounts: We will use 'class' accounts this semester. You can get your account here. When you first log into your account, you will be prompted to enter information about yourself; that will register you with our grading software. If you want to check that you are registered correctly with our grading software, you can run `check-register` at any time.

Textbook: The class does not have a required textbook. We want to help you save money, so please don't feel obligated to buy a textbook. However, we know that some students appreciate additional reading to supplement lectures; for them, we recommend *Introduction to Computer Security* by Michael Goodrich & Roberto Tamassia (ISBN-10: 0321512944, ISBN-13: 9780321512949). We also recommend *The Craft of System Security* by Sean Smith and John Marchesini. We will list optional readings from these textbooks which you can use to help learn the course topics, but all readings from these books are entirely optional.

Lecture notes: We will provide lecture notes and/or slides for many of the lectures. Lecture notes and slides are *not* a substitute for attending class, as our discussion in class may deviate from the written material. You are ultimately resposible for material **as presented in lecture and section**.

Top Lecture Staff Sections Homeworks Projects Exams Policies Piazza

Re-grading policies: Any requests for grade changes or re-grading must be made within one week of when the work was returned. To ask for a re-grade for material graded on GradeScope, submit a regrade request on GradeScope. Procedures to request a re-grade for other coursework will be provided shortly. We will not accept verbal re-grade requests. Don't expect us to re-grade your homework on the spot: we normally take the time to read your appeal at some point after it is submitted.

Bear in mind that a primary aim in grading is consistency, so that all students are treated the same. For this reason, we are unlikely to adjust the score of individual students on an issue of partial credit if the score allocated is consistent with the grading policy we adopted for that problem.

More on homeworks: If a problem can be interpreted in more than one way, clearly state the assumptions under which you solve the problem. In writing up your homework you are allowed to consult any book, paper, or published material, except solutions from previous classes or elsewhere, as stated under the Collaboration section. If you consult external sources, you **must** cite your source(s). We will make model solutions available after the due date, and feedback will be available via `glookup` or GradeScope.

Late homework policy: We will give no credit for homework turned in after the deadline. Please don't ask for extensions. We don't mean to be harsh, but we prefer to make model solutions available shortly after the due date, which makes it impossible to accept late homeworks.

Don't be afraid to ask for help! Are you struggling? We'd much rather you approached us for help than gradually fall behind over the semester until things become untenable. Sometimes this happens when students fear a possibly unpleasant conversation with a professor if they admit to not understanding something. We would much rather resolve/remedy your misunderstanding early than have it expand into further problems later. Even if you are convinced that you are the only person in the class that doesn't understand the material, and think it must be entirely your fault for falling behind, please overcome this concern and ask for help as soon as you need it. Remember, helping you learn the material is in fact what we're paid to do, after all!

Advice: The following tips are offered based on our experience with CS 161:

1. Don't wait until the last minute to start projects! The projects can be time-consuming. Pace yourself. Students who procrastinate generally suffer.

2. Make use of office hours! The instructors and TAs hold office hours expressly to help you. It is often surprising how many students do not take advantage of this service. You are free to attend as many office hours as you wish. You are not constrained just to use the office hours of your section TA. You will likely get more out of an office hour visit if you have spent some time in advance thinking about the questions you have, and formulating them precisely. (In fact, this process can often lead you to a solution yourself!)

3. Participate actively in discussion sections! Discussion sections are **not** auxiliary lectures. They are an opportunity for interactive learning. The success of a discussion section depends largely on the willingness of students to participate actively in it. As with office hours, the better prepared you are for the discussion, the more you are likely to get out of it.