CS 161 : Computer Security
Spring 2016

Instructors:

Raluca Ada Popa (office hours Fri 4-6pm in 729 Soda)
David Wagner (office hours Wed 4-5pm and Fri 1-2pm in 733 Soda)
and an awesome team of talented TAs

Lectures:

MWF 11:00-12:00, 1 Pimentel

Addresses:

Web page: http://www-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.

Data	Topic	Readings	Slides
Wed 1/20	Introduction	[optional: G&T § 1.1, Craft § 1-1.1, 1.3]	slides
Fri 1/22	Injection vulnerabilities, buffer overflows, and memory safety	Notes. [G&T § 3.4, Craft § 6.1-6.3]	slides
Mon 1/25	Software security	Notes on Reasoning About Code and Secure Software Development. [Craft § 6.5-6.7]	slides
Wed 1/27	Access control, OS security	Notes. [G&T § 1.2, Craft § 1.2]	slides
Fri 1/29	Privilege separation, security principles		slides
Mon 2/1	Security principles	Notes. [G&T § 1.1.4, Craft § 3.4]	slides
Wed 2/3	Web security: access control, same-origin policy	[G&T § 7.1.1, 7.1.3, Craft § 12.1.1, 12.1.2, 12.1.3]	slides
Fri 2/5	Web security: injection vulnerabilities	[G&T § 7.3.1, 7.3.2, 7.3.3]	slides
Mon 2/8	Web security: XSS	[G&T § 7.2.6, 7.3.6]	slides
Wed 2/10	Web security: session management and CSRF	[G&T § 7.1.4, 7.2.1, 7.2.7, Craft § 12.1.4]	slides
Fri 2/12	Authentication and impersonation	[G&T § 7.2.2, Craft § 18.1, 18.2]	slides
Mon 2/15	**holiday**		
Wed 2/17	Web security: UI-based attacks	[G&T § 7.2.3]	slides
Fri 2/19	Tracking on the web		slides
Mon 2/22	Symmetric-key encryption	Notes. [G&T § 8.1.0, 8.1.1, 8.1.3, Craft § 7.1, 7.3.2, 7.3.3]	slides

Wed 2/24	midterm review, **midterm 8:00-9:30pm** (155 Dwinelle)		slides
Fri 2/26	Block ciphers	Notes. [G&T § 8.1.6, 8.1.7]	slides
Mon 2/29	Public-key key exchange	Notes. [G&T § 8.2.1, 8.2.4, , Craft § 7.5]	
Wed 3/2	Public-key encryption and hashing	Notes. [G&T § 8.2.1, 8.2.3, Craft § 7.5]	
Fri 3/4	Integrity, authentication, and public-key signatures	Notes. [G&T § 8.2.3, 8.4.1, 8.4.3, Craft § 7.4.2]	
Mon 3/7	Key management	Notes. [G&T § 1.3, Craft § 10.1-10.3, 10.5, 10.7, 9.7.1, 9.7.2]	
Wed 3/9	Most common cryptography mistakes	[Craft § 8.1]	slides
Fri 3/11	Password hashing, TLS	Notes. [G&T § 8.3]	slides, slides
Mon 3/14	Securing Internet communications: TLS		
Wed 3/16	Background on networking	[G&T § 5.1, 5.2.1, 5.2.2, 5.3.1, 5.4.0, 5.4.1, 5.4.2, Craft § 5.1, 5.4.1]	slides
Fri 3/18	Network-level attacks	[G&T § 5.2.3, 5.3.3, 5.3.4, 5.4.4, Craft § 5.3.1]	slides
Mon 3/21	**Spring Break**		
Wed 3/23	**Spring Break**		
Fri 3/25	**Spring Break**		
Mon 3/28	midterm review **midterm 8:00-9:30pm** (A-L in 155 Dwinelle, M-Z in 2050 Valley LSB)		slides
Wed 3/30	Attacks on DNS	[G&T § 6.1.1-6.1.3] [Optional: Kaminsky attack on DNS, Illustrated guide to the Kaminsky attack]	slides
Fri 4/1	Denial of service	[G&T § 5.5.0, 5.5.1, 5.5.2, 5.5.4]	slides
Mon 4/4	Network security: firewalls	Notes. [G&T § 6.2, Craft § 5.3.2]	slides
Wed 4/6	Network security: intrusion detection	[G&T § 6.4, Craft § 5.3.2]	slides
Fri 4/8	Securing Internet communications: DNSSEC		slides
Mon 4/11	DNSSEC, comparison to TLS		slides
Wed 4/13	Proof of work, Hash chains, Bitcoin		slides
Fri 4/15	Bitcoin		slides
Mon 4/18	Electronic voting		slides
Wed 4/20	Cheating in online games		slides
Fri 4/22	Cybercrime and the underground economy		slides
Mon 4/25	Cloud security, computing on encrypted data		slides
Wed 4/27	Jailbreaking, modern sandboxes		

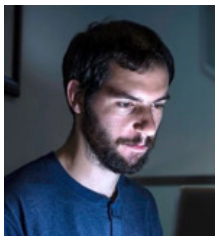
Fri 4/29	Anonymous communication, anti-censorship, Tor	
Tue 5/10	**Final Exam, 7-10pm**	

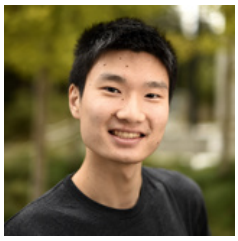
Staff


Raluca Ada Popa


David Wagner

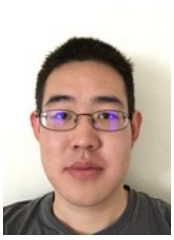

Jethro Beekman


Nicholas Carlini


Austin Chen


Michael Chen (Head GSI)

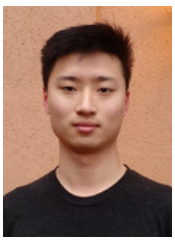

Robin Hu

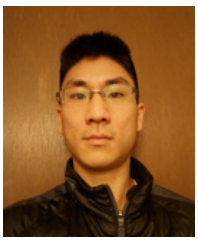

Calvin Li

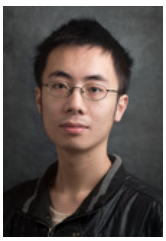

Frank Li


Pratyush Mishra


Chris Thompson


William Xu


Bill Yeh


Qi Zhong

Office hours:

M 10-11am (651 Soda; Nicholas Carlini)
Tu 10-11am (411 Soda; Nicholas Carlini)
Tu 1-2pm (611 Soda; Robin Hu)

Tu 2-3pm (341A Soda; Austin Chen)
Tu 4-5pm (283E Soda; Michael Chen)
W 12-1pm (341B Soda; Pratyush Mishra)
W 1-2pm (411 Soda; Jethro Beekman)
W 1-2pm (341A Soda; Austin Chen)
W 3-4pm (651 Soda; Michael Chen)
W 4-5pm (733 Soda; David Wagner)
Th 12-1pm (341B Soda; Robin Hu)
Th 1-2pm (341B Soda; Robin Hu)
Th 2-3pm (411 Soda; Chris Thompson)
Th 3-4pm (341A Soda; Bill Yeh)
Th 4-5pm (341A Soda; Bill Yeh)
F 10-11am (611 Soda; Frank Li)
F 1-2pm (733 Soda; David Wagner)
F 2-3pm (651 Soda; Qi Zhong)
F 3-4pm (651 Soda; Qi Zhong)
F 4-5pm (651 Soda; Qi Zhong)
F 4-5pm (729 Soda; Raluca Ada Popa)
F 5-6pm (729 Soda; Raluca Ada Popa)

Discussion section handouts:

Section 01 (Jan. 26): Handout, Solution.
Section 02 (Feb. 2): Handout, Solution.
Section 03 (Feb. 9): Handout, Solution.
Section 04 (Feb. 16): Handout, Solution.
Section 05 (Feb. 22): Handout, Solution.
Section 06 (Feb. 29): Handout, Solution.
Section 07 (Mar. 7): Handout, Solution.
Section 08 (Mar. 14): Handout, Solution.
Section 09 (Apr. 04): Handout, Solution.
Section 10 (Apr. 11): Handout, Solution.
Section 11 (Apr. 18): Handout, Solution.

Discussion section times:

114. M 1-2pm, 320 Soda (Qi Zhong)
115. M 2-3pm, 320 Soda (Calvin Li + Pratyush Mishra)
101. M 3-4pm, 102 Latimer (Calvin Li + Pratyush Mishra)
102. M 3-4pm, 3105 Etcheverry (Bill Yeh)
103. M 4-5pm, 102 Latimer (Bill Yeh)
104. Tu 10-11am, 254 Sutardja Dai (William Xu + Jethro Beekman)
105. Tu 11-12pm, 102 Latimer (Nicholas Carlini)
116. Tu 12-1pm, 310 Soda (Robin Hu) - *drop-ins welcome!*
106. Tu 12-1pm, 102 Latimer (Austin Chen)
107. Tu 1-2pm, 102 Latimer (Austin Chen)
108. Tu 2-3pm, 102 Latimer (Robin Hu)
109. Tu 3-4pm, 254 Sutardja Dai (Chris Thompson + Jethro Beekman) - *drop-ins welcome!*
110. Tu 3-4pm, 105 Latimer (Michael Chen)
111. Tu 4-5pm, 179 Stanley (William Xu + Nicholas Carlini) - *drop-ins welcome!*
112. W 9-10am, 102 Latimer (Frank Li) - *drop-ins welcome!*
113. W 10-11am, 310 Soda (Qi Zhong)

Homeworks:

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.

Schedule for homeworks:

- Homework 1 (due 2/1); solution.
  Resources: slides; review session, review session slides.
- Homework 2 (due 2/22) (Q1(b) updated 2/17); solution.
- Homework 3 (due 3/11); solution.
- Homework 4 (due 5/2);

There will be approximately 3-4 homeworks.

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).

Schedule for projects:

- Project 1 (due Feb 16 11:59pm): Specification, other resources. Solution.
- Project 2 (Part 1 due March 18 11:59pm, Part 2 due April 8 11:59pm): Specification, Framework code and libraries, Online documentation. Part 1 solution.
- Project 3 (due Apr 22 11:59pm): Specification, VM image.

In Spring 2014, the CSUA held a review session on C programming; the slides are available in pdf and Powerpoint format.

Exams

There will be two midterms and one final exam.

The midterms will be held on **Wednesday February 24, 8-9:30pm** (in 155 Dwinelle) and **Monday, March 28, 8-9:30pm** (in 155 Dwinelle and 2050 Valley LSB), outside of class. For midterm 2, students with last name starting with A-L, go to 155 Dwinelle; last name M-Z, go to 2050 Valley LSB.

The final will be held **Tuesday May 10**, 7:00-10:00pm.

- Midterm 1, solutions.
- Midterm 2, solutions.

All exams are mandatory. If you will be unable to attend any of these dates, you must contact the instructors (via a private message on Piazza) at some point during the first week of classes.

Grading

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

- Homeworks: 16%

Top Lecture Staff Sections Homeworks Projects Exams Policies Piazza

---

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**. Attendance during the first two weeks of class is mandatory.

Discussion sections: Attendance at discussion sections is expected, and sections may cover important material not covered in lecture. Outside of your discussion section, you should feel free to attend any of the staff office hours (not just your section TA's office hours) and ask any of us for help.

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.