Overview

CS161 Computer Security

Dawn Song
dawnsong@cs.berkeley.edu

General Information

- **4 units**
- **Prerequisites:**
  - **CS 61C (Machine Structures)**
  - **Math 55 or CS 70 (Discrete Mathematics).**
- **Lecture:**
  - **MW 2:30pm-4:00pm, 306 Soda**
  - **Berkeley time, class starts 10mins late**
- **Discussion sections: Mandatory**
  - **101. Tu 11:00am - 12:00pm, 4 Evans**
  - **102. Tu 5:00pm - 6:00pm, 85 Evans**
  - **103. W 10:00am - 11:00am, 5 Evans**
- **This class will be offered again next semester**
  - **So you can take it next semester if it works better for your schedule**

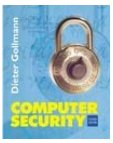
Course Staff

- **Lecturer:**
  - **Dawn Song: http://www.cs.berkeley.edu/~dawnsong**
- **TAs:**
  - **John Bethencourt: http://www.cs.berkeley.edu/~bethenco**
  - **Todd Kosloff**

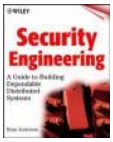


Textbooks

- **Computer Security, 2nd ed.(Dieter Gollmann)**
  - ***Required***
  - **1st ed. is insufficient**
  - **Assigned readings will be posted**



- **Security Engineering (Anderson)**
  - ***Optional***
  - **Available in online form**



Resources

- **Website:**
  - http://inst.eecs.berkeley.edu/~cs161/sp08/
- **Mailing list:**
  - cs161-spring08@lists.eecs.berkeley.edu
    https://lists.eecs.berkeley.edu/sympa/info/cs161-spring08
  - **Used for announcements, especially urgent notices**
  - **If you haven't subscribed, pls do asap!**
- **Newsgroup:**
  - **Newsgroup: ucb.class.cs161**
    Server: news.berkeley.edu (from campus), authnews.berkeley.edu (off campus)
    See http://www.net.berkeley.edu/usenet/.
  - **For general class related questions, pls post on newsgroup instead of emailing the staff, so other students can benefit too**

Course Load

- **2 Exams: closed book**
  - **Midterm exam: covers the first half of the course**
  - **Final exam: covers the second half of the course**
- **5 Homeworks**
  - **Three homeworks for first half of semester**
  - **Two homeworks for second half of semester**
- **1 Project**
  - **In groups of four**

Project Schedule

- **Project topic**
  - **Develop tools for vulnerability discovery in programs**
- **Feb 11: group sign-up due**
  - **All four member must be in the same section**
- **Feb 20: project description/requirements out**
- **Mar 12: Milestone 1**
  - **design document, timetable, group work breakdown**
- **Apr 14: Milestone 2**
  - **updates to above, plus working code which implements most rudimentary features**
- **May 12: Final submission of code and writeup**

Grading

- **35% Homeworks (7% each)**
- **20% Project**
- **20% Midterm exam**
- **25% Final exam**

Final Grade

- **Final grade = (ethics grade) * (academic grade)**
- **Ethics grade will normally be 1**
- **Ways to get a 0 ethics grade:**
  - **Violate campus computing policy**
  - **Violate privacy of other people without permission**
  - **Tamper with data of other people without permission**
  - **Fail to report a vulnerability/observation of unethical behavior**
  - **Unethical behavior may be referred for additional disciplinary action**

Class Participation

- **Showing up (on time) is the first step**
- **Asking/answering questions is encouraged**
- **Turn off your cell phone ring in class**
  - **Taking cell phone calls in class is rude**
- **Treat students and staff with respect**

Collaborative Work

- **Projects will be in groups of four**
  - **All must be in the same section**
- **Homeworks are done individually**
- **You may use the following resources:**
  - **Instructors, TAs, assigned texts, posted notes**
- **No consulting others; No "Googling for answers"**
  - **Consult with TAs over problem cases**
  - **Always cite references – plagiarism is not permitted**

Academic Dishonesty Policy

- **Copying all or part of another person's work, or using reference material not specifically allowed, are forms of cheating and will not be tolerated. A student involved in an incident of cheating will be notified by the instructor and the following policy will apply:**

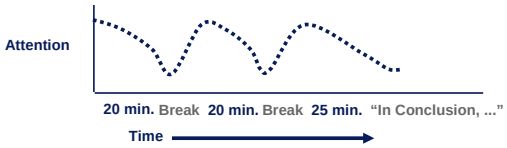
  http://www.eecs.berkeley.edu/Policies/acad.dis.shtml

- **The instructor may take actions such as:**
  - **require repetition of the subject work,**
  - **assign an F grade or a 'zero' grade to the subject work,**
  - **for serious offenses, assign an F grade for the course.**
- **The instructor must inform the student and the Department Chair in writing of the incident, the action taken, if any, and the student's right to appeal to the Chair of the Department Grievance Committee or to the Director of the Office of Student Conduct.**
- **The Office of Student Conduct may choose to conduct a formal hearing on the incident and to assess a penalty for misconduct.**
- **The Department will recommend that students involved in a second incident of cheating be dismissed from the University.**

Note on Security Vulnerabilities

- From time to time, we may discuss vulnerabilities in widely-deployed computer systems. This is *not* intended as an invitation to go exploit those vulnerabilities. It is important that we be able to discuss real-world experience candidly; students are expected to behave responsibly.
- Berkeley policy is very clear: you may not break into machines that are not your own; you may not attempt to attack or subvert system security. Breaking into other people's systems is inappropriate, and the existence of a security hole is no excuse.

Typical Lecture Format



- 2-Minute Review
- 20-Minute Lecture
- 5- Minute Administrative Matters
- 3-Minute Break (stretch)
- 20-Minute Lecture
- 5-Minute Break (water, stretch)
- 25-Minute Lecture
- Instructors will come to class early & stay after to answer questions

Goals of This Semester

- **Last lecture:**
  - A glimpse of why you should care about security
- **I hope to show you this semester:**
  Crypto and Security: important + fun :-)
- **To take this class, you need to**
  - Be curious
  - Think from both sides: attack & defense

Class Scope

- **Learn the science of cryptography**
  - **E.g., How to communicate securely over an insecure communications medium**
- **How to build secure systems**
  - **Techniques for designing, implementing, and maintaining secure systems**
- **How to evaluate the security of systems**
  - **How systems have failed in the past**
  - **How attackers break into real systems**
  - **How to analyze the security & vulnerability of systems**

Topics Structure

- **First half semester: Cryptography**
  - **Basic concepts in crypto**
  - **Some advanced applications in crypto**
  - **Attacks & analysis of crypto**
- **Second half semester: Computer Security**
  - **Software security**
  - **Operating system security**
  - **Network security**
  - **Malicious code analysis and defense**
  - **Web security**
- **Advanced topics and case studies if time allows**

Lectures (Tentative)

Part I: Cryptography
Basic Concepts

- **Jan 30: Symmetric Key encryption, block ciphers**
  - **What does a secure symmetric-key encryption mean?**
  - **Feistel principle in block cipher design**
  - **Block cipher modes**
- **Feb 4: Public Key encryption, modular arithmetic**
  - **What does a secure public-key encryption mean?**
  - **Basic hardness assumptions used in public-key crypto**
  - **Example public-key crypto systems: RSA, ElGamal**
- **Feb 6: Hash functions, message authentication**
  - **Fundamental properties of cryptographic hash functions**
  - **What does a secure message authentication code (MAC) mean?**
- **Feb 11: Digital signatures**
  - **What does a secure digital signature mean?**
  - **Example constructions: RSA and ElGamal signatures**

Lectures (Tentative)

Advanced concepts, applications, analysis

- **Feb 13: Secret sharing**
  - **Basic concept and applications to privacy-preserving computing**
- **Feb 18: Academic Holiday, (no lecture)**
- **Feb 20: Zero-knowledge Proofs**
  - **How to prove to others that you know something w/o telling them what you know**
- **Feb 25: Authentication and key exchange protocols**
  - **Example protocols in practice**
  - **How do you authenticate to your bank in on-line banking?**
  - **How do you set up secure communication with your bank in on-line banking?**
- **Feb 27: Random number generation**
- **Mar 3: Electronic cash**
- **Mar 5: Timing attacks and other side channel attacks on crypto**
- **Mar 10: Why crypto systems fail**
- **Mar 12: TBD**

Lectures (Tentative)

- **Mar 17: Midterm review**
- **Mar 19: Midterm exam**
- **Mar 24: no lecture (Spring break)**
- **Mar 26: no lecture (Spring break)**

Lectures (Tentative)

Part II: Computer Security
Software Security

- **Mar 31: Buffer overflow and other memory safety vulnerabilities**
  - **Basic concepts of some of the most common classes of vulnerabilities**
  - **How do they take control of your computer**
- **Apr 2: Defensive programming**
  - **Principles to write more secure programs**
- **Apr 7: Analysis tools for finding bugs (I)**
  - **Static and dynamic methods to discover bugs and detect exploits**
- **Apr 9: Analysis tools for finding bugs (II)**
  - **More methods for bug finding, such as fuzzers (related to your project)**

Lectures (Tentative)

Operating Systems Security

- Apr 14: Access control, privilege, privilege separation
  - How to protect your resources from malicious access?
- Apr 16: Isolation, sandboxing, reference monitors
  - How do we protect processes from other faulty/malicious process?
  - How do we confine the damage of a faulty/malicious program?

Networking Security

- Apr 21 Firewalls, intrusion detection
  - How to keep the attackers out?
- Apr 23 Denial-of-Service attacks
  - How to deal with attacks that just don't let you get work done?

Lectures (Tentative)

Malicious Code Analysis and Defense

- Apr 28 Worms and defenses
  - How can an attacker own the Internet in 10 mins?
  - How can we defend against it?
- Apr 30 Malware and defenses
  - How do spyware, rootkit, botnets function?
  - How can we defend against them?

Web Security

- May 5 Web security
  - Is your on-line banking secure?
  - Attacks & defenses on the web
- May 7 TBD

- May 12 Final exam review
- May 16: Final exam

Summary

- Action items
  - Get textbook
  - Subscribe to mailing list
  - Start looking for group partners
- Next class
  - Symmetric-key crypto

Questions?

Questionnaire

- **To get statistics on your background & interests**
  - **Allow lectures to be better suited for you**
- **Feel free to write whatever you see fit**
- **The more info you provide, the more beneficial it'll be**