CS 194-1 (CS 161) Class Introduction

Doug Tygar (doug.tygar@gmail.com)

August 29, 2005

cs161.org

CS 161 (194-1) basic facts

- This is a class about computer security
- 4 units
- This is an experimental class – if successful, it will become CS 161
- To take this class, you need patience, an open mind, and willingness to work hard

Adding this class

- If you are an upper division declared major and currently on the waiting list
  - you have a good chance of getting in
  - work with Michael-David Sasson
- If you want to add and aren't in already
  - get on the waiting list asap!

Berkeley – leader in security research

- TRUST (Berkeley leads consortium)
- DETER (Berkeley leads consortium)
- ACCURATE
- NEST
- Crypto research
- Security and HCI
- Security for NSF, DoD, DHS, USPS, DOE, etc

Instructors

- Anthony Joseph
  - (adj@cs)
  - 675 Soda

- Doug Tygar
  - (tygar@cs)
  - 531 Soda and 307B South

- Umesh Vazirani
  - (vazirani@cs)
  - 671 Soda

- David Wagner
  - (daw@cs)
  - 629 Soda

TAs (so far …)

- Jeff Kalvass
  - jmkalvass@berkeley
  - Sandia "red teaming", Google Adwords fraud detector
  - "PrivacyLink", "NetState"
- Rusty Sears
  - sears@cs
  - LeadScope, Microsoft Research
  - security, knowledge representation, programming languages, AI
- Ivan Tam
  - ivan@sims
  - Information architecture, security & HCI, and MMPRGs

Sections

- No section this week
- We are likely to add a fourth section (details coming soon)

Grading

- Academic grade
  - Project (35%)
    - Two parts, three grace days
  - Exams (40%)
    - Midterm 1 (tentatively October 5, 10%)
    - Midterm 2 (tentatively November 9, 10%)
    - Final (20%)
  - Homework (15%)
    - 5-6 homeworks – lowest score dropped
  - Class participation (10%)

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 or an observation of unethical behavior
  - Unethical behavior may be referred for additional disciplinary action

Class participation

- Showing up is the first step
- Asking (or answering) questions is good
  - (but don't filibuster)
- Having your cell phone ring in class is bad
  - Taking the cell phone call in class is worse
- Treat students and staff with dignity

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 the answer"
  - Consult with TAs over problem cases
  - Always cite references – plagiarism is not permitted

Textbooks

- Security in Computing, 3rd ed(Pfleeger)

- Security Engineering (Anderson)

Other class resources

- cs161.org
  - lecture notes, pointers to some readings, and assignments are posted here
- Newsgroup: ucb.class.cs161 (read daily!)

Lectures (tentative)

- Aug 29 Overview; intro to computer security
- Aug 31 Adversaries, threat models, security goals
- Sept 2 Access control, authorization
- Sept 5 No class! Labor Day Holiday.
- Sept 7 Network security intro
- Sept 9 Networking background
- Sept 12 Firewalls
- Sept 14 Intrusion detection

Lectures (tentative)

- Sept 16 Symmetric-key cryptography
- Sept 19 Modular arithmetic background
- Sept 21 Public-key encryption
- Sept 23 Message authentication, public-key sigs
- Sept 26 Secure channels
- Sept 28 Software security: principles
- Sept 30 Software security: defensive programming

Lectures (tentative)

- Oct 3 Implementation flaws, buffer overruns
- Oct 5 Midterm 1
- Oct 7 Secret sharing
- Oct 10 Cryptographic protocols, zero knowledge
- Oct 12 Zero knowledge protocols
- Oct 14 Authentication protocols
- Oct 17 Random number generation

Lectures (tentative)

- Oct 19 Electronic cash protocols
- Oct 21 Electronic commerce systems
- Oct 24 Database security, inference control
- Oct 26 Worms and viruses
- Oct 28 Distributed denial of service
- Oct 31 Web security
- Nov 2 Web services, a case study

Lectures (tentative)

- Nov 4 OS security, memory protection
- Nov 7 Multi-level security, mandatory access ctl
- Nov 9 Midterm 2
- Nov 11 No class! Veterans Day Holiday.
- Nov 14 Language-based security
- Nov 16 Sandboxing
- Nov 18 Hardware security, tamper resistance

Lectures (tentative)

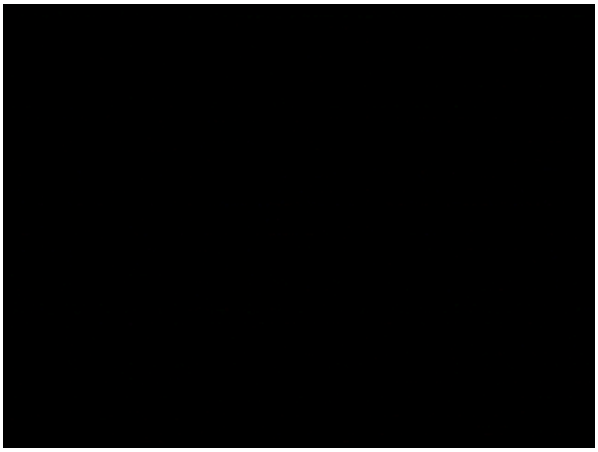
- Nov 21 Side-channel attacks, fault attacks
- Nov 23 No class! Thanksgiving Holiday.
- Nov 25 No class! Thanksgiving Holiday.
- Remaining classes: review, overflow, & special topics
- Possible special topics: Security & Law, digital rights management, e-voting, quantum cryptography, penetration testing, privacy
- Post your requests!

Why is security such a problem?

- Monoculture computing environment
- Web, e-commerce, & collaborative applications
- Internet spans national boundaries
- Poor programming practices

Two security nightmares

- The transparent society
- "Electronic Pearl Harbor"



Electronic pearl harbor

- Is this just scare-mongering?
- Slammer worm took down Bank of America's ATM network, Seattle 911 service
- Nachi worm invaded Diebold ATMs?
- Real worries about e-voting validity
- Millions of CC #s, SS #s leaked
- Case study: Attacks over the Taiwan straits

Goals of this class

- Solid foundation in understanding security
- Key information a/b building secure systems
- Introduce range of topics in security
- Interest some of you in further study