CS161 Computer Security

Overview

Teaching Team

What is Computer Security About?

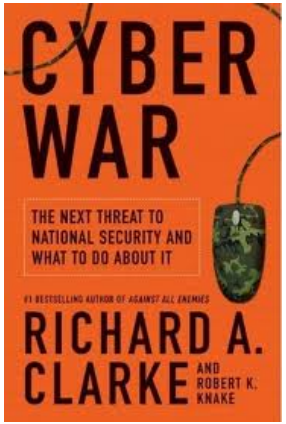
- General goals:
  - Allow intended use of computer systems
  - Prevent unintended use that may cause harm
- Examples:
  - Only share your photos & location with friends
  - Don't want attackers install key-logger on your machine to steal your password

Why Should You Care?

- It impacts your day-to-day life

Why Should You Care?

- It impacts everybody's day-to-day life
  - Millions of computers compromised
  - Millions of passwords stolen



What Is This Class About?

Learn About Security

Make a Difference

How Can You Make a Difference?

- Be a more security-aware user
  - Make better security decisions
- Be a more security-aware developer
  - Design & build more secure systems
- Be a security practitioner & researcher
  - Identify security issues
  - Propose new security solutions

What Will You Learn in This Class?

- Security vulnerabilities
- How to exploit them & defend against attacks
- Fundamental security concepts & principles
- How to architect secure systems
- Security problems & solutions in application areas

Topics Covered in Class

- Secure coding
- Secure architecture concepts & principles
- Mobile security
- Cryptography
- Web security
- Network security & malware

Course Format

- New course format

Motivation

- Today's lecture format is sub-optimal
  - Students learn at different speed
  - Passive teaching & learning: Insufficient interaction
  - Attendance continuously dropping (some below 30%)
- How can we do better?
  - By utilizing new technologies & approaches

Approach: Interactive Video Capsules

- Lectures designed & recorded as short video capsules
  - e.g., 10 mins each
  - Embedded with auto-graded quizzes
  - Depart from traditional live lecture recording
- Benefits
  - Students can learn at their own speeds
  - Capsules more easily digestible
  - Quizzes help retain learning
  - More easily monitor each student's progress

Making Video Capsules Publicly Accessible

- Benefits beyond local students
  - Student population world-wide
  - Students who may not have access to such material o.w.
- Build an online community of students learning the topic
  - Students vote for good questions and answers (crowd-sourcing)
  - Learning community keeps students more engaged
- www.security-class.org
  - Collaboration w. Dan Boneh & John Mitchell (Stanford)

Course Components & Requirements

- Video capsules & quizzes
- Lectures
- Labs
- Projects
- Changes to discussion sessions

Video Capsules & Quizzes

- Watch before due date
  - Usually before Mon/Wed lectures
- Need to answer quizzes in video
  - Proceed when get correct answer
  - Occasionally can skip
- Cover core material in class
- Can watch together with friends

Lectures

- Auxiliary examples
- Optional material
  - More advanced techniques
  - More related work
- Discussions
- Guest lectures from industry
  - Industry perspective

Labs

- 6 Labs
- Usually 1-2 weeks long
- Hands-on experience for material covered in class
- Done in groups of two
  - Pick partners soon!

Labs Schedule

- Lab 1: Buffer overflow
- Lab 2: Program testing & verification
- Lab 3: Android security
- Lab 4: Cryptography
- Lab 5: Web security
- Lab 6: Network security

Projects

- Semester-long project
- 5 students per group
- Gain experience in
  - Designing & building secure systems
  - Specific security problems & solutions

Project Schedule (I)

- Phase I: selecting project
  - Candidate projects
    - Proposed by TAs: presentation next class, Jan 23
    - Proposed by students: presentation in class, Jan 25
  - Submit project & group preference, Feb 1
  - TAs will run matching algorithm to resolve remaining issues
    - Determine project & group choices

Project Schedule (II)

- Phase II: Design
  - Discuss with TA
  - Read up literature
  - Initial exploration
  - Project design doc due Feb 22

Project Schedule (III)

- Phase III: Implementation & Evaluation
  - Discuss with TA
  - Implementation milestone 1 due March 21
  - Implementation milestone 2 due April 20
  - Final project due May 4

Project Mentorship

- Each project group will be mentored by one TA
- Meet with TA mentor each week for discussion
- Multiple group meeting time possibilities required for forming a group
  - Included in group preference submission

Change to Discussion Sessions

- Traditional discussions suboptimal
  - Not individual attention
  - Low attendance rate
- New format: project group meetings w TA mentor
  - Each group meet with TA mentor every week
    - 30 mins on project discussion
    - 15 mins on other course-related material: Q&A, Labs questions
  - Additional office hours per week for currently-covered material
  - Tutorial for certain background material: 1st next Tue

For Next Two Weeks

- Group-TA mentor matching determined by Feb 6
- Before then, discussion sessions on Tue
- Jan 24, tutorial on C & gdb
  - 11-noon, 87 Evans
  - 3-4pm, 105 Latimer
- Jan 30, discussion session on buffer overflow vulnerabilities
- Times & location

Web Platform

- Sign up at https://berkeley.campus-class.org/security
- Receive announcements
- Watch videos
- Submit labs & project docs
- Discussion forums
  - Post your questions & answers
  - Vote your favorite questions & answers
  - TA answer top ranked questions
  - Special trophy for students who give best answers

Grading

- Midterm 20% (Apr 4)
- Project 25%
- Quizzes 10%
- Labs 45%
  - Lab 1: Buffer overflow (8%)
  - Lab 2: Program testing & verification (8%)
  - Lab 3: Android security (8%)
  - Lab 4: Cryptography (5%)
  - Lab 5: Web security (11%)
  - Lab 6: Network security (5%)

Next Steps

- Info: http://www.cs.berkeley.edu/~dawnsong/teaching/s12-cs161
- Sign up at https://berkeley.campus-class.org/security
- Identify group partners
  - Lab group
  - Project group
- Next lecture (Mon): candidate class projects
  - You should be here!
- Next Tue: Tutorial
  - Be there if you need a refresher on C & gdb
  - 11-noon, 87 Evans
  - 3-4pm, 105 Latimer