Course Overview

CS166
Introduction to Computer Systems Security
Goals

• Provide an introduction to computer security
• Overview security threats and defenses in cyber and physical systems
• Help you develop a security-aware mindset
Course Staff

- Roberto Tamassia (Instructor)
- Bernardo Palazzi (Guest Lecturer)
- Nina Polshakova (HTA)
- Jearson Alfajardo (TA)
- Adam Horowitz (TA)
- Julia Kim (TA)
- Harjasleen Malvai (TA)
- Isaac Semaya (TA)
Lectures

- Security Principles
- Cryptography
- Authentication
- Operating Systems Security
- Applications Security
- Cloud Security
- Web Security
- Network Security
- Physical Security
Live Demos

• See in class hands-on demonstrations of basic attack and defense techniques
• Try it yourself and show it to your friends
• Keep in mind that attack demos should be done in an ethical and legal manner
Assignments

- Homeworks (40%)
- Projects (36%)
  - Cryptography Breaking
  - OS Hacking
  - Web Hacking
- Final Project (24%)
  - Designing, building, and testing secure systems

Late Policy
- Five late days toward the first three projects
- No late days for homeworks and final project
- Contact the instructor in case of extenuating circumstances
Learning Security

• We teach the principles, you study the details
  – Research a bit on your own
  – Be comfortable with new systems and languages
• Take advantage of class discussions
• Develop and share your own ideas
Piazza

• Official communication tool
• All questions related to course materials should be posted (publicly or privately) on Piazza
CS 162

- Must be taken concurrently with 166
- Half-credit course
- Requires instructor permission
- Provides capstone credit and 2000-level credit for 166

- Harder projects
  - Trickier vulnerabilities
  - More real-world scenarios
  - Automation
- Help sessions in class
  - See calendar
- Same grade for 166 and 162
  - Homeworks (32%)
  - Projects (42%)
  - Final Project (26%)
Safety

• Basic model of safety
  – Assets: what you want to protect
  – Threats: what could damage your assets
• Safety is ensuring threats don’t damage assets
• We will see soon how security differs from safety
Air Travel Scenario

• Assets
  – Passengers
  – Crew
  – Luggage
  – Aircraft
  – …

• Threats
  – Engine failure
  – Pilot failure
  – ATC failure
  – Wind
  – …

• How likely are they?
Air Travel Scenario

- Threats
  - Engine failure
  - Pilot failure
  - ATC failure
  - Wind
  - Ice

- Safety measures
  - Two or more engines, maintenance
  - Two or more pilots, rest periods, checklists
  - Communication protocols, automated collision avoidance systems
  - Multiple runways, weather forecasting, ground stops
  - Aircraft deicing systems
Safety vs. Security

• Another threat to air travel
  ─ Terrorism

• This type of threat is called an attacker
  ─ Intelligent
  ─ Motivated

• Security is like safety, but it deals with attackers

• Defending against attackers is more difficult than mitigating natural threats
Security Design

• Evaluate risk
  – Capabilities of attackers
  – Likelihood of obtaining such capabilities

• Identify defenses
  – Develop risk mitigation measures
  – Assess cost of such measures

• Manage risk
  – Implement specific defenses taking into account risk and cost