Course Overview

CS166: Computer Systems Security
Choose a case-sensitive alphanumeric password

That is, your password should use the following characters

– 0123456789
– abcdefghijklmnopqrstuvwxyz
– ABCDEFGHIJKLMNOPQRSTUVWXYZ

Let’s try to crack it!
Goals

• Provide an introduction to cybersecurity
• Overview security threats in cyber and physical systems
• Security is never absolute, we will teach you how to be more secure

What is security?
Security is a chain...
STAFF

• Bernardo Palazzi (professor)
• Roberto Tamassia (professor)
• Joshua Liebow-Feeseer (HTA)
• Evgenios Kornaropoulos (Grad TA)
• Giselle Lillie (Grad TA)

UTAs

• Justin Bisignano
• Justin Brower
• Dan Haugh
• Natalie Roe
• Jeremy Tong
Security is a chain...
Security is a chain...
Assignments: Projects and HWs

• Weekly Homeworks (40%)
• Projects (30%)
  – Cryptography Breaking
  – OS Hacking
  – Web Hacking
• Final Project (30%)
  – Designing/building secure systems
• No exams
Security is a chain...
PIAZZA

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

1/26/16

Introduction
Security is a chain...
Live DEMOs

• See in class hands-on demonstrations of basic attack and defense techniques

• Try it yourself and show it to your friends
Security is a chain...
Guest Speakers

• Opportunity to meet experts from
  – Industry
  – Academia
Security is a chain...
Learning Security

• We teach the principles, you study the details
  – Research a bit on your own
  – Be comfortable with new systems and languages
    • PHP (Web)
    • Go (secure implementation)
• Take advantage of class discussions
• Develop and share your own ideas
Security is a chain…

- Security is about the “weakest link in the chain”
- You can not overlook any link
CS 162

- Like CS167/CS169
- Harder projects
  - Trickier vulnerabilities
  - More real-world scenarios
  - Automation
- Same homeworks
- In class presentations
- Weekly lecture/meeting
  - Next Wed 4:30 - 6 in 316
- Half credit course
- Apply for instructor permission (see website)
Administrative

• Collaboration policy
  – Print, sign and return
• Survey
  – Sign in with your Brown Google account and complete it
• Request override for 166
• Request override for 162
• Capstone project
• 2000-level credit

Check the website
Contact

- Primarily, use Piazza
- Course website
- Email Lists:
  - cs166tas@cs.brown.edu
  - cs166headtas@cs.brown.edu
What is Security?
Security vs Safety

- Basic model of safety:
  - *Assets* (things you want to protect)
  - *Threats* (things which could damage your assets)
  - Safety is ensuring *threats* don’t damage *assets*
Safety Scenario

- Climber climbing a rock wall
- Assets?

https://500px.com/photo/35922332/climber-silhouette-by-aj-o-donnell
Safety Scenario

- Climber climbing a rock wall
- Assets
  - Climber’s safety

https://500px.com/photo/35922332/climber-silhouette-by-aj-o-donnell
Safety Scenario

- Climber climbing a rock wall
- Assets
  - Climber’s safety
- Threats?

https://500px.com/photo/35922332/climber-silhouette-by-aj-o-donnell
Safety Scenario

● Climber climbing a rock wall
● Assets
  ○ Climber’s safety
● Threats
  ○ Falling
  ○ Getting hit by falling rock

https://500px.com/photo/35922332/climber-silhouette-by-aj-o-donnell
Safety Scenario

● Climber climbing a rock wall
● Assets
  ○ Climber’s safety
● Threats
  ○ Falling
  ○ Getting hit by falling rock
● Safety measures?
Safety Scenario

- Climber climbing a rock wall
- Safety measures
  - Harness
  - Rope
  - Helmet

https://500px.com/photo/35922332/climber-silhouette-by-aj-o-donnell
Safety Scenario

- Climber climbing a rock wall
- Safety measures
  - Harness
  - Rope
  - Helmet
- How well do the safety measures mitigate the threats?
Safety Scenario

- Climber climbing a rock wall
- Another perspective:
  - How can the safety measures fail?
  - How likely are these failures?

https://500px.com/photo/35922332/climber-silhouette-by-aj-o-donnell
Safety Scenario

- Climber climbing a rock wall
- Introduce a new threat:
  - A person who wants to make the climber fall
  - Whatever safety measures are in place, this person is going to try to make them fail
Safety Scenario

● Climber climbing a rock wall
● Introduce a new threat:
  ○ A person who wants to make the climber fall
  ○ Whatever safety measures are in place, this person is going to try to make them fail
● How could the person make the safety measures fail?
Safety Scenario

- Climber climbing a rock wall
- How could the person make the safety measures fail?
- What new safety measures should we introduce to deal with this new threat?
Safety Scenario

- Climber climbing a rock wall
- Why is it so much harder to deal with this new threat?
Safety Scenario

- Climber climbing a rock wall
- Why is it so much harder to deal with this new threat?
  - The threat is *intelligent*
  - The threat is *motivated*
Safety Scenario

- **Normal threats: likelihood**
  - May randomly cause safety measures to fail
  - Less likely to happen => worry about it less

- **Intelligent, motivated threats: possibility**
  - *Induce* failures
  - Seek out failure points in safety measures, no matter how unlikely it would be by random chance
  - Less likely is of no help; threat will seek it out anyway
What is Security?
Security vs Safety

Definition for this course: Security is like safety, but it deals with intelligent, motivated threats.
Security vs Safety

- Basic model of security:
  - Assets
  - Threats (or attackers)
  - Security is ensuring threats/attackers don’t damage assets