Class is starting now!
Course Overview

CS1660-CS1620-CS2660

Introduction to Computer Systems Security
Goals

• Provide an introduction to computer security
  – Overview security threats and defenses
• Help you develop a security-aware mindset:
  – Take the big picture and understand the details
  – Learning by practicing
• Consider ethical implications and tradeoffs of using, building, and testing secure systems

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

STAFF

Lectures

CS1660
CS1620
CS2660
Lectures
Lectures

- Security Principles
- Cryptography
- Authentication
- Operating Systems Security
- Network Security
- Web Security
- Applications Security
- TBD...
Class Participation

IN PERSON
• Raising your hand and asking question if you have any doubt
• Your question will be repeated by the instructor
• Synchronous attendance encouraged, but not required
• All lectures and notes will be recorded
• The deadlines will be the same for all students

ONLINE
• Please if possible keep open the video and mute the microphone
• To ask a question, please raise your hand or type “question” in chat
Clicker Questions

- Conducted via TopHat (Join Code: 821033)
- You need to register
- Does not count towards your grade
- Engage with course material during lecture!
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
Disclaimer

• Any such techniques are taught only for educational purposes.
• The techniques are taught to you in simulated or isolated environments that prevent harm to other parties.
• You should not use these techniques outside the setting of the course.
Security is a chain...
Assignments

• 4 Homeworks (35%)
  • Written problems + short “labs” on TryHackMe

• Projects (45%)
  — Cryptography: Break some weak crypto
  — Flag: Web Hacking
  — Handin: OS Hacking

— Final project (25%): Design, build, test a secure system
Prerequisites

• CS33, CS300, CS1310, CS1330 (or equivalent)
  – You should have seen systems concepts like threads, memory management, (basic) networking before

You should also be comfortable with...
• Writing programs/scripts in some language (Python, Go, C/C++, Shell scripting, ...)
• Learning new languages you’ve never seen before, to read code (we’ll gain practice with this!)

If you have questions, please ask!
Security is a chain...

- CS1660
- CS1620
- CS2660
- Edstem
- Lectures
- Assignments
- STAFF
Regular Administrivia

• Most material on course website: https://cs.brown.edu/courses/csci1660/

• You are responsible to check the web page and EdStem!
  – All announcements will be there
  – Notes for all lectures (filled and unfilled)
  – Handouts, due dates, programming resources, etc...
Asking for help

• Online help: EdStem
• Office hours/clinics: calendar on course website
  – In-person and hybrid

• Can help with..
  – Debugging
  – Assignment/project concepts
  – Systems issues, attack mechanics
  – And more!

We’re here to help you learn how to solve problems—but please start early!
Asking for help

• Collaboration: work with your peers!
  – Collaboration policy on course website
  – We encourage you to collaborate, so long as the code you write and vulnerabilities you find are your own
  – List collaborators in your submission

• Your physical and mental health is important!
  – If you have concerns, feel free to talk to us
  – We encourage you to contact University resources like CAPS
Diversity and Inclusion

• We welcome diverse ideas and perspectives
• Points of contact:
  – Bernardo, Nick & TAs
  – Anonymous feedback form (website)
  – diversity.advocates@lists.cs.brown.edu
  – wellness.advocates@lists.cs.brown.edu
Feedback

• Anonymous feedback form on course website

• Please tell us how we can improve the course!
  – Clarity of assignments
  – Improving accessibility
  – Concerns about presentation of content, interactions with staff
Security is a chain...

CS1660
CS1620
CS2660
Registration Logistics
What’s with all the course numbers?

- CS166/CS1660??
- CS162/CS1620??
- CS2660???
CS1660
(was CS166)

- Open to undergraduate and graduate students
- Counts for 1000-level credit

**Cybersecurity master’s program**: this course is designed for the Computer Science track
  - Policy track students should take CS1880 instead
CS1620/CS2660: The “Lab”  
(was CS162)

If you are interested, you can work on more challenging problems for additional credit:

• Undergraduates: half-credit lab (+ capstone, if senior)
• Graduate students: 2000-level credit

What changes?

• More problems, tricker vulnerabilities, some outside reading
• No additional prerequisites/background, just requires more time
• Extra late days
# CS1620/CS2660: Interested?

<table>
<thead>
<tr>
<th>If you are a…</th>
<th>Register for…</th>
<th>What you get</th>
</tr>
</thead>
<tbody>
<tr>
<td>Undergraduate</td>
<td>CS1660 + CS1620 (Register for <strong>BOTH</strong>)</td>
<td>Half-credit lab Capstone (if you are a senior, email us)</td>
</tr>
<tr>
<td>Graduate student</td>
<td>CS2660</td>
<td>2000-level credit</td>
</tr>
<tr>
<td><strong>Note:</strong> can’t drop to 1660 after shopping period!</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undergraduate w/ Concurrent master’s</td>
<td>You decide</td>
<td>CS1620: Freedom to drop to 1660 CS2660: 2000-level credit (+capstone)</td>
</tr>
</tbody>
</table>

If you have questions, let us know!
Some honesty

- Huge demand for the course this year!
- We are working hard to scale the class—we appreciate your patience and understanding!
The waitlist

If you are not enrolled do the following:
1. Fill out the waitlist form ASAP
2. Add the course to your cart

As enrollment changes, we will admit students from the waitlist, prioritizing students who:
• Were unable to preregister due to CAB issues
• Cannot take the course again or have strict program req’s

First batch of admissions tonight—look for an email
If you decide not to take this course

That’s okay!
Please be respectful to your fellow students--let us know ASAP:

• **If you are registered**: please drop the course
• **If you are on the waitlist**: edit your form response
Setup: Homework 0

• Ensure you have access to course resources

• Helps us to gauge your comfort level with various topics and concepts covered in this course
  – We will use this to determine how to scope lectures and provide other resources

• Complete by Thursday, Feb 2 (sooner if possible!)
Security is a chain...
Password Cracking Demo

• How to crack some passwords with different strengths
• We will be randomly select a student for creating a password during the lecture in a breakout room
  – One at a time
• We will help the student with the rules for selecting the password
Select a Password

- Choose a case-sensitive alphanumeric password
- That is, your password should use the following characters
  - 0123456789
  - abcdefghijklmnopqrstuvwxyz
  - ABCDEFGHIJKLMNOPQRSTUVWXYZ
- Let’s try to crack it!
Security is a chain...

• Security is about the “weakest link in the chain”
• You can not overlook any link
Security is a chain...

• Who said this sentence?
  – Bruce Schneier in...
    Secrets and lies
Mind Map

• A Mind Map is a visual form of:
  – brainstorming
  – note-making

• A Mind Map is hierarchical and shows relationships among pieces of the whole
Let’s Try Together

- Visit: [https://tinyurl.com/cs1660-mindmap](https://tinyurl.com/cs1660-mindmap)
- You should not need an account! — Password: csci1660

- Add a word in the mind map tool, based on what you associate with security in general. Feel free to add a word to an existing branch or to create a new branch.

- Optionally, include your name in “()” after the word so that we can discuss
Break!!!!!!

Class is starting now!

1/27/23 Cryptography II
Introduction to Security

Introduction to Computer Systems Security
CIA Triad

Confidentiality
• Prevent disclosure of information to unauthorized parties

Integrity
• Detect data tampering

Availability
• Guarantee access to data
McCumber Cube (1991)

Security Goals
- Confidentiality
- Integrity
- Availability

Information States
- Storage
- Transmission
- Processing

Security Measures
- Human factors
- Policy and practices
- Technology
Is this enough?

• Parkerian Hexad (2002)
• C-I-A Triad expanded:
  – Authenticity
    • Veracity of the data source and provenance can be assured
  – Utility
    • Security or insecurity of data does not inhibit the practical use of the data
  – Possession or Control
    • Data is only accessible or changeable by those intended
• Non-Repudiation
  • One party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction
• Etc.
Secure Against What?

• “Security” has no meaning per se
• The security of a system, application, or protocol is always relative to
  – A set of desired properties
  – An adversary with specific capabilities
• In cybersecurity it is difficult to define general rules often we use best practices or heuristics
Heuristics

Just some best practices useful in most scenarios:

– Need to know/Least privileges
– Default secure
– Defence in depth
– Open design/Standard solutions
– Security as a process
– Usability
– ...

NO SECURITY THROUGH OBSCURITY
Security Trade-offs

• Complete security against all conceivable adversaries is often unfeasible.

• Security implies a tradeoff between risk mitigation and the cost of deploying defense mechanisms.

• In addition, human factors such as user acceptance and usability must be taken into account.
If Cracking does not Work

Keyloggers

Hardware

Software
Summary

• Security is a chain...
• Security models (CIA)
• There is no a general definition for security you should take in consideration:
  – Adversaries
  – Heuristics
  – Trade-offs
  – Ethics
  – ...


Ethics

- Ethics Question & Group Discussion in HWs
  - No right answer
- Many real-world applications, Cybersecurity decisions inherently ethical:
  - Should the government be able to require access to encrypted communications?