CSCI 331:
Introduction to Computer Security

Lecture 1: Course Intro

Instructor: Dan Barowy
Williams

Announcements

- CS Colloquium, Fridays 2:35-4pm
  in Wege auditorium

What is "security"?

**What does it mean
for something to be "secure"?**

Concretely…

E-mail

Paywalled Articles

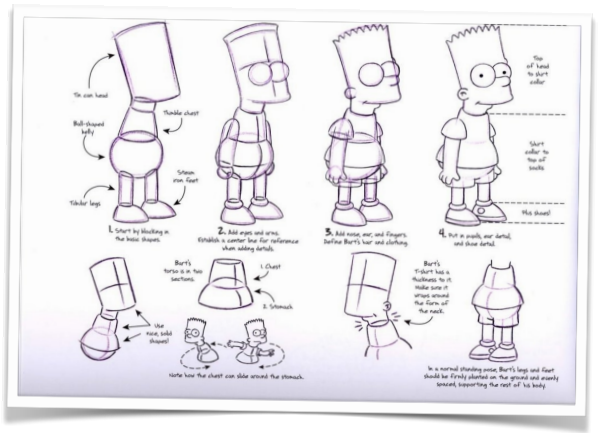
About the class

First thing this course is about:

Thinking…

… not feeling.

Second thing this course is about:



How security is <u>designed</u> and <u>implemented</u>.

Security is a broad topic!

"security" = four essential properties

confidentiality (privacy)	integrity
authenticity	availability

We analyze the security of assets

Some assets:

- Data (e.g., email)
- Software (e.g., operating system)
- Services (e.g., e911)
- Things (e.g., computer, car, house, …)

We analyze the security of assets with respect to adversaries

Some adversaries:

- National governments
- Organized crime
- Thrill-seekers
- Journalists
- "Friends"
- Business competitors
- [H]activists
- Potential employers
- Bored students!!!

We analyze the security of assets with respect to adversaries who aim to achieve certain goals.

We call these scenarios **threats**.

We analyze the security of assets with respect to adversaries who aim to achieve certain goals.

We call these scenarios **threats**.

Goal: to analyze threats dispassionately.

- **Source** of the attack.
- **Effect** on 4 security properties:
  - Confidentiality
  - Integrity
  - Authenticity
  - Availability
- **Cost** of damage.

Weaknesses of security properties are called vulnerabilities.

- Allowing any password: “password”.
- Program stores data “in the clear.”
- Program uses crypto with known flaws.
- Important computers are in unlocked space.

Actions that take advantage of vulnerabilites are called exploits.

- Allowing any password: “password”.
  - Attacker tries likely passwords.
- Program stores data “in the clear.”
  - Attacker finds way to read disk.
- Program uses crypto with known flaws.
  - Attacker has enough resources to break it.
- Important computers are in unlocked space.
  - Attacker steals/tampers w/computer resources.

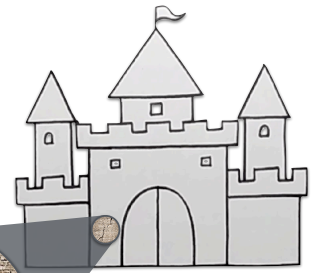
cost (to us):
lose the castle

gain (to adv):
gain a castle

likelihood exploit works: high

adversary

exploit



asset

vulnerabilities: {integrity, authenticity}

Thinking systematically can make decisions easier

cost (to us):
lose the castle

$-1,000,000

likelihood exploit works: high

p(X) = 0.82

“expected cost”

E[X] = $-1,000,000 x 0.82 = $-820,000

spending up to is “worth the money”

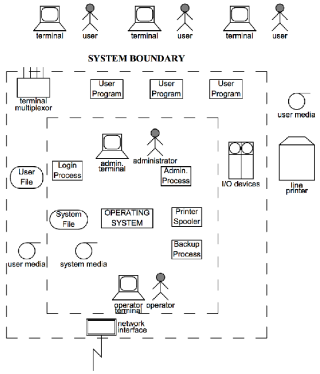
Risk analysis is the systematic analysis of threats to assets.

“Should I connect to airport wifi?”

	Confident-iality	Integrity	Authen-ticity	Availability
E-Mail				
Docs				
Photos				
Music				

It's hard to know your vulnerabilities.

It helps to think holistically.



And it *really* helps to keep records over time.

Theory, *noun*, /ˈθiəri/

A statement of one or more laws or principles which are generally held as describing an essential property of something. (from: OED)

Theory: a rule that *predicts* a testable *observation*.

Karl Popper (1902-1994)

Sadly: there is no "theory of security"

You will **never** know whether you are "secure."

You ***will*** know when you have **mitigated specific threats**.

Sadly: there is no "theory of security"

By thinking systematically and carefully, you ***can*** effectively reduce the risks!

Sadly, the state of the art in computer security is…

Attacks are **easy**.

Defenses are **hard**.

Administrivia

About the course

Lectures:

Mondays & Thursdays, 2:35-3:50pm
Schow 030B

Labs:

Section 1: Tuesdays, 1:00-2:30 pm

Section 2: Tuesdays, 2:30-4:00 pm

both in the Ward Lab (TBL 301)

About the course

Three kinds of homework:

1. **Reading** & **crib notes**
   - Due every week.
2. **Programming assignments** ("labs")
   - Due roughly every two weeks
3. **Final project**
   - Three checkpoints throughout the semester.

About the course

Office Hours in TBL 301 (Ward Lab)

Thursday: 4-5:30pm
Friday: 12:30-1:30pm

and by appointment

This is hopefully athlete-friendly.

Sadly, electives are rarely given TAs

About the course

Gitea

About the course

Handed-in work will be *code* or *writing.*

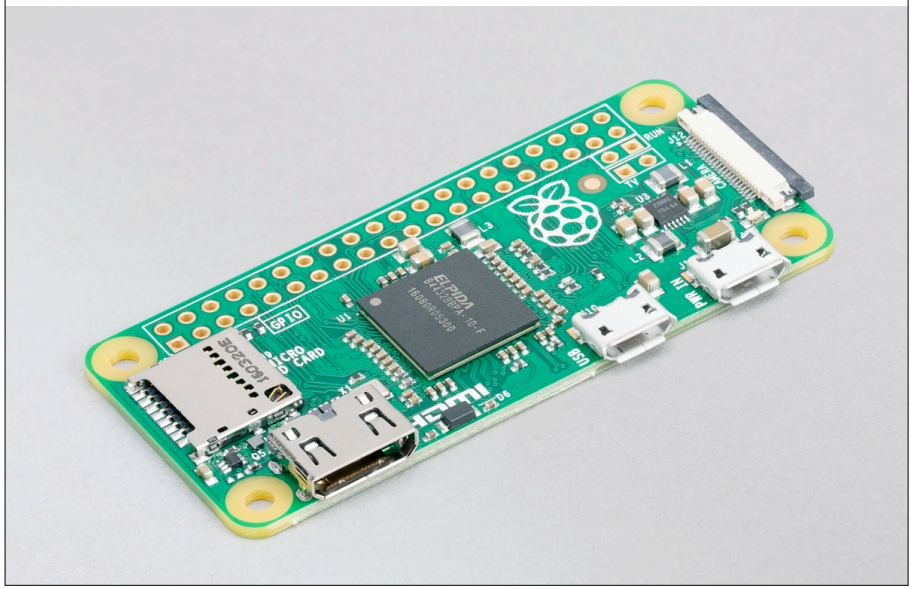
1. Programming assignments
   - C code or
   - Assembly code
2. Reading crib notes
3. Project checkpoints
   - Writing (i.e., LaTeX code)
   - Implementation code
   - Other files

About the course

You will commit to the git repository *assigned* to you.

Usually, your repository will include starter code.

Standard platform



Unpleasantries

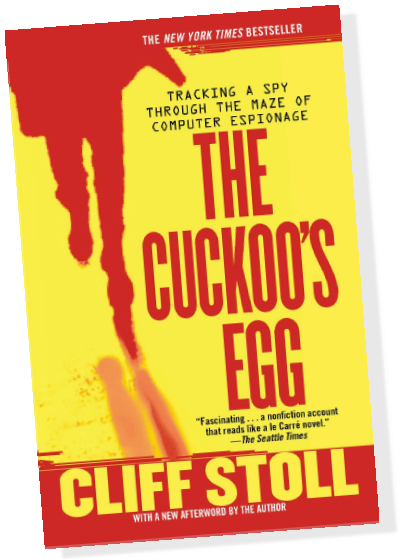
Solutions to assignments should not be posted in any public forum, including public git (e.g., GitHub, GitLab, etc) repositories. Students taking our courses should not be looking for solutions, but tempting them by making solutions available is inappropriate. This applies not just to the semester you are taking the course, but to the future as well.

Homework

Have a look at the website.

- For Mon: Read “The Psych of Security” and take notes for class discussion
- Due Mon: Signed Code of Ethics

The Cuckoo’s Egg



Grading

TRADITIONAL GRADING SYSTEM		STANDARDS-BASED SYSTEM	
A	90-100%	4	Proficient on all standards
B	≥ 80% and < 90%	3	Proficient on most standards
C	≥ 70% and < 80%	2	Proficient on half of the standards
D	≥ 60% and < 70%	1	Proficient on less than half of the standards
F	< 60%	0	Missing

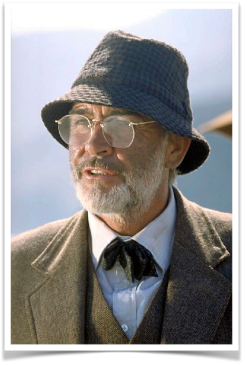
I will post the formula I use to convert to letter grades on the website.

Grading

Midterm:	25%
Final Project:	25%
Lab assignments:	35%
Class participation:	15%

The right attitude for success

You are the intrepid explorer.



I am your elder guide.

The right attitude for success

You want the adventure.
I want to stay home and putter around my office.

The right attitude for success

I am always happy to help as long as you're the one doing the driving.

This course is not risky…

…provided that you do your homework and turn it in.

Something to know about security

There are “good guys” and “bad guys.”

Please do not be a bad guy.

Something to know about security

Good guys don’t pull their punches with bad guys.
I won’t either.

Computer security is intellectually stimulating…

and can be incredibly exciting.

I hope you learn a lot and have a great semester!

Questions?