(Advanced) Computer Security!

Course Intro & Roadmap

Prof. Travis Peters

Montana State University

CS 476/594 – Computer Security

Spring 2021

https://www.traviswpeters.com/cs476

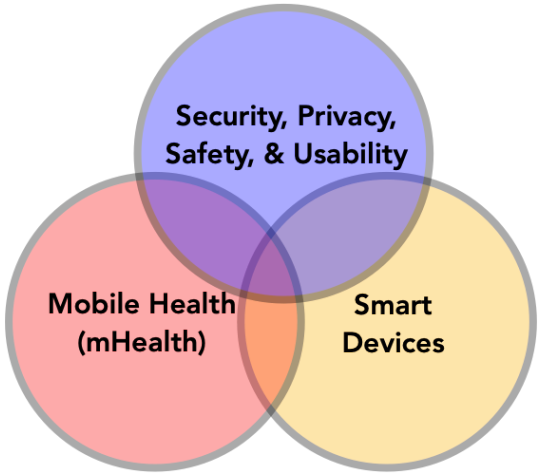
Today

- Announcements
  - Check out the **course website**: https://www.traviswpeters.com/cs476
  - Please fill out the **questionnaire** (see link from course schedule)
  - **Lab 00** is posted (see link from course schedule)
    -> Thursday class = help session

- Learning Objectives
  - Figure out *who is this guy...?*
  - Know important stuff about the course + how to find other stuff out
  - Understand what this course is all about and what we'll be doing
  - *(Working towards...)* Review some basics
    - Models/layout of a computer & a program
    - Basic C programming and command line usage
    - Linux & Basic Linux Security

Prof. Travis Peters

Assistant Professor @ Montana State University



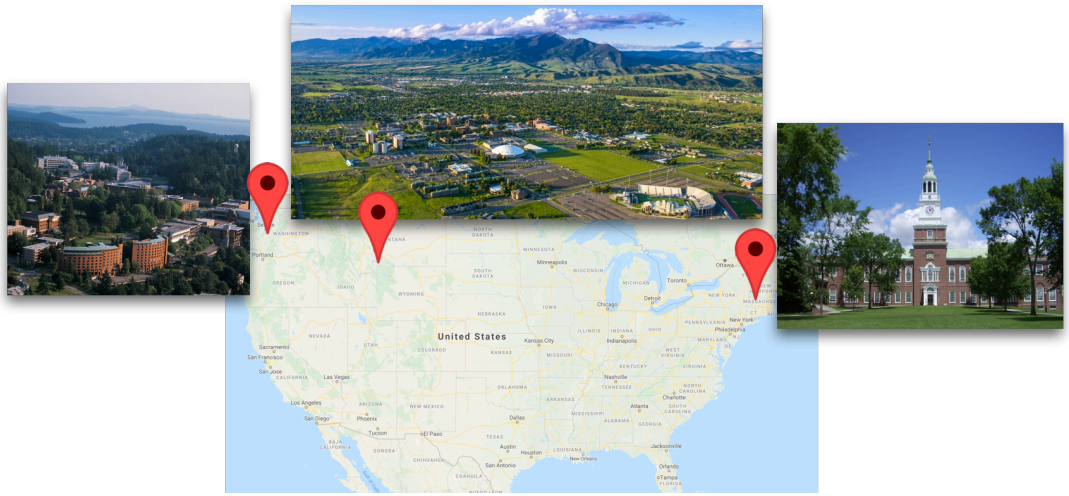
email: travis.peters1@montana.edu
website: https://www.traviswpeters.com

Ph.D. in CS @ Dartmouth › *Hanover, NH*
B.S. in Math & CS @ Western Washington University › *Bellingham, WA*

Research & Teaching

- Systems › *Operating Systems, Mobile & Wearable Systems, IoT*
- Computer Security › *Offensive/Defensive Security; Security by Design; Security Tools*
- Wireless Network Security › *WPAN, Bluetooth/BLE, Wi-Fi*
- Trusted Computing › *Trusted Execution Environments (SGX, TrustZone)*

NEW PROJECTS IN SECURITY/EDUCATION – LOOKING FOR STUDENTS! ☺



Beyond the prof/researcher/security enthusiast…

- Married (Mary) + Dad (Benjamin, ~14mo.)!
- I do other stuff too…
  - *church, reading, running, biking, (amateur) woodworker, netflix, …*
  - *currently learning about investing, real estate, chess, and basic carpentry*

NOTE: *Mary and I LOVE sharing pictures of Benjamin but we also try to respect Benjamin's personal right to digital privacy. For this reason, we avoid showing his face in public sites and PDFs.*

Some Names I've Been Called… *(Focus on These)*

(AVOID THESE)

- ***Travis***
- ***Prof. Peters***
- ***Dr. Peters***
- Mr. (Vice) President
- Sir
- Dada
- Coach
- Hey You
- Honey
- T$
- Travy
- T-Bear
- Yo
- Ghost
- Hawk
- Nasty Travis
- Trauis
- Teach
- Mr. Peters
- *Peter*
- The Professor
- Larry Bird
- *Trevor*
- …

Highlights from the Course Website

Course Logistics

- **Course Staff**
  - Travis (Instructor/Prof) and Seraj (TA/PhD Student)

- **Our Tools**
  - See **"Logistics (In A Nutshell)"** for all links - Website, Zoom, Slack, D2L, Gradescope, ...
  - Course Website: Look over FAQs
  - Slack: Please use **#classchat** to ask questions/have discussions **DURiNG** class
  - Slack: Please update your name/picture
  - Zoom: Synchronous/Online!

Poll: posting videos... (a) upon request, (b) so long as ?% are attending?

- **What you need to know**
  - *Re: Recommended Prerequisites*
  - Basics of a computer system (e.g., bytes, addresses, CPUs, memory, modes of operation, and what assembly language is)
  - Working experience with Linux command line, C, Python, gdb, ...

NOTE:
I will try to post materials in advance.
I will always make class resources (e.g., slides, code) by the end of the class day.

Course Logistics

- **Textbooks**
  - (SS3P) – Software Security: Principles, Policies, and Protection
    - NEW! DIGITAL! FREEEEEE!
    - More on *theory*, more on *defensive strategies*, nice coverage on *offense* and *case studies*
  - (SEED) – Computer and Internet Security: A Hands-On Approach
    - Used last year
    - Students LOVED the SEED Labs (lots of hands-on learning) – we are keeping these ☺
    - Book is largely crafted around the SEED Labs

    -> Students felt they didn't strictly need this book; many did like it though
    -> Many felt class covered the ideas well enough and the book was redundant
    -> Many felt the book was too oriented around offensive topics – not enough on defensive strategies

Course Logistics

- **Assignments & Grading**
  - Mostly Weekly Labs (70%)
  - + "Final Lab" (15%)
  - Office Hours (5%), Other Activities/Engagement (AL/Quiz/Critiques) (10%)

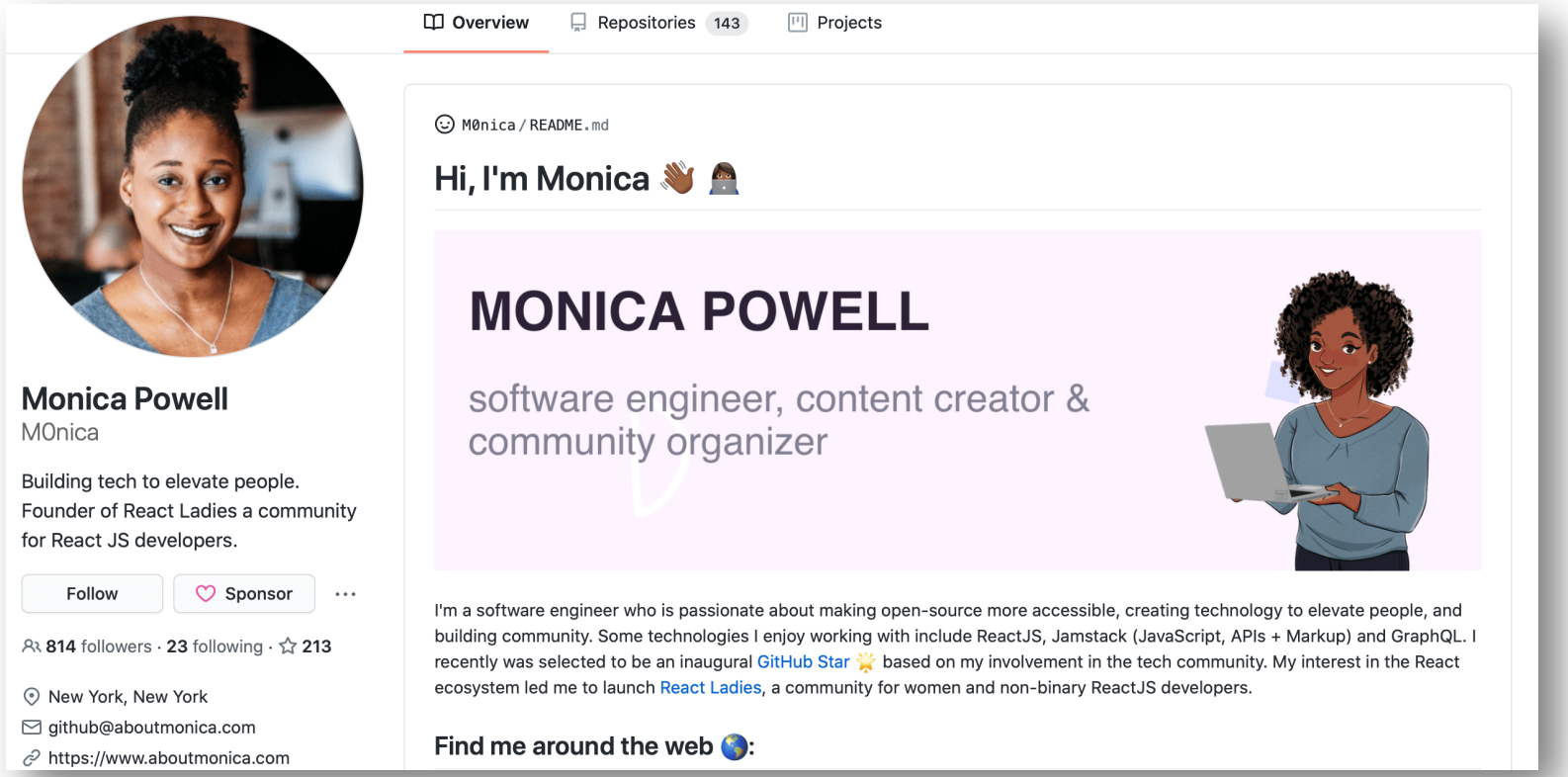
- **Due Dates/Times**
  - An ideal timeline…

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
	assignments due @ 12pm			office hours @ 11am-12pm (Travis)		
	office hours @ 2-4pm (Travis)		office hours @ 2:10-4pm (Seraj)			

Travis's 5 Tips for Success

Pro Tips

1. Update your GitHub!
   - First/last name
   - A fun/useful picture
   - (+any other useful details)



Pro Tips

2. Go to office hours — we aren't scary, and **we are here to help!** :-)

We are normal(ish) people too...

....see, not so scary!

Pro Tips

3. Ask questions

"if you aren't asking questions, you aren't actually learning..."

How to Ask Questions in Class

...and feel comfortable doing it

"The important thing is not to stop questioning..."

– Albert Einstein

Prepare

- Do the readings ahead of time so you know the basics
- If you think of a question before class, write it down
- Practice by asking questions to your friends

Focus on learning

- It's OK to be nervous; it gets easier with practice
- Don't get thrown off by negative self-talk or other unhelpful distractions
- It really is true: there are no stupid questions
- Asking questions is proven to lead to better learning (and better grades)

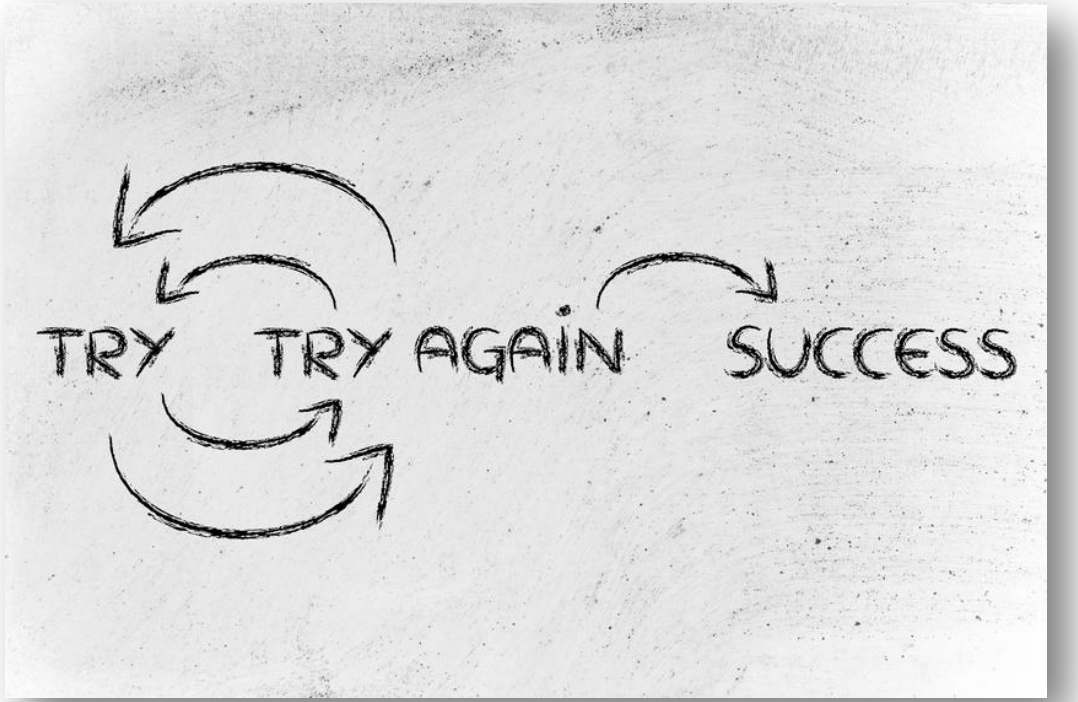
Try it out

- Challenge yourself: take a risk and just ask
- Chances are you have the same question as others in the class; take one for the team!
- If you aren't ready to ask in class, contact your instructor before or after class, by email or during office hours
- Most profs love it when you ask questions. It shows you are engaged in learning

Pro Tips

4. Do the labs! AND START EARLY!

5. Try stuff!



Pro Tips – BONUS TIPS!!!

6. **Bookmark** the course website!
https://www.traviswpeters.com/cs476-2021-spring/#logistics-in-a-nutshell

7. Update your **notification settings** in Slack

Security...

Security

Think. Pair (Break Out Rooms). Share.

- Why are YOU taking security?

Security

Think. Pair (Break Out Rooms). Share.

- What is security? (What is security **not**?)
- Why is it important?
- Popular examples? Examples you've encountered?

Are These "Systems" Secure?

Think. Pair (Break Out Rooms). Share. (If time…)

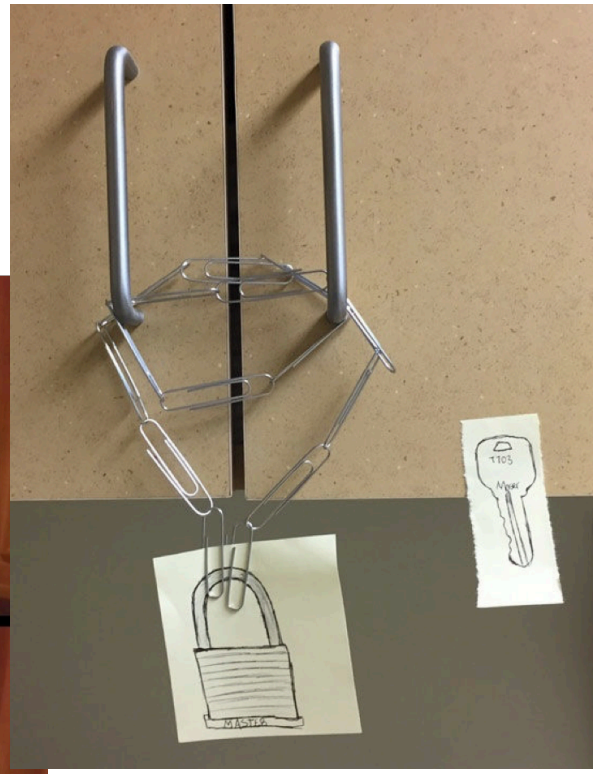


Photo credits: https://brightside.me/wonder-curiosities/20-ridiculous-security-fails-that-are-too-good-to-be-true-426810/

The Take-Home Message

At the end of the day, security is hard to define!

(But we will look at some strategies to make it easier to reason about!)

The security & privacy field is always evolving:

- new **assets**
- new **threats**
- new **capabilities**
- new **technologies**

You need to be ready to think through new situations that arise, leveraging what you've already learned (here, past experiences, case studies, reports, etc.) to find S&P solutions for those new situations.

A Glimpse At What We'll Do!

CSCI 476/594 (Computer Security / Advanced Security) – Spring 2021

- **Introduction & Security Overview/Basics**
  - basic concepts
  - linux security basics
- **Software Security**
  - classic attacks: set-uid attacks, env. variable attacks, buffer overflow attacks, (+extra?!)
  - recent issues in sw: return-oriented programming, shellshock attack
- **Network & Web Security**
  - sql injection (SQLi) attacks
  - cross-site scripting (XSS) attacks
  - cross-site request forgery (XSRF) attacks
  - ~~sniffing, spoofing, and network attacks (e.g., TCP/IP)~~
- **Crypto**
  - symmetric & asymmetric cryptography
  - encryption & decryption
  - digital signatures
- **Recent Topics (as time permits, e.g., malware, side-channel attacks)**

Next Time…

Lab 0 Help Session!

- Set up your VM
- Get your GitHub account setup
- General Q&A

-> Try it yourself – come Thursday if you need help!