

Welcome + Administrivia

CS499/579 :: Empirical Computer Security

Zane Ma (he/him/his)

2023.09.27

Topics

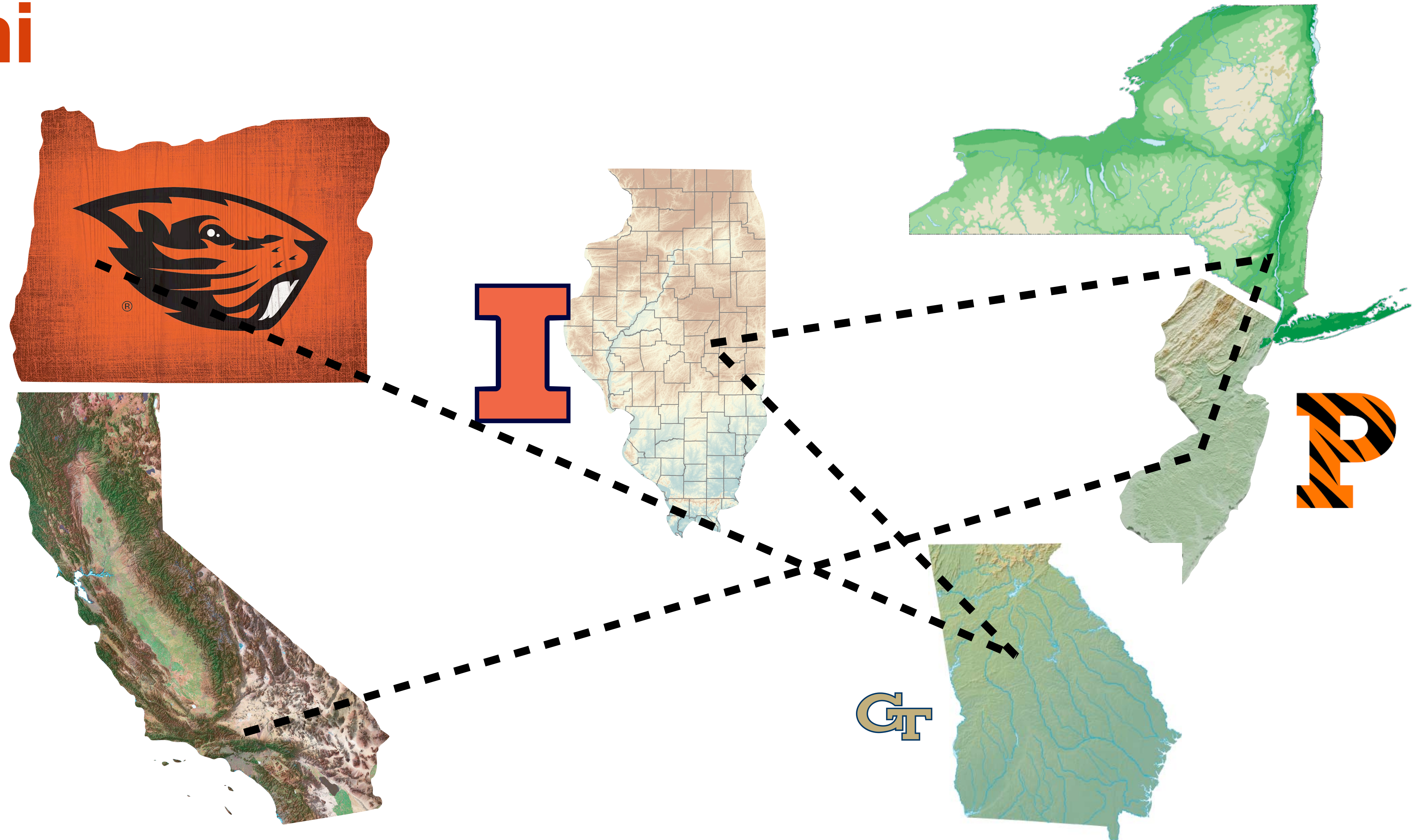
- Course + class introduction
- Course logistics
- Course policies

\$ whoami



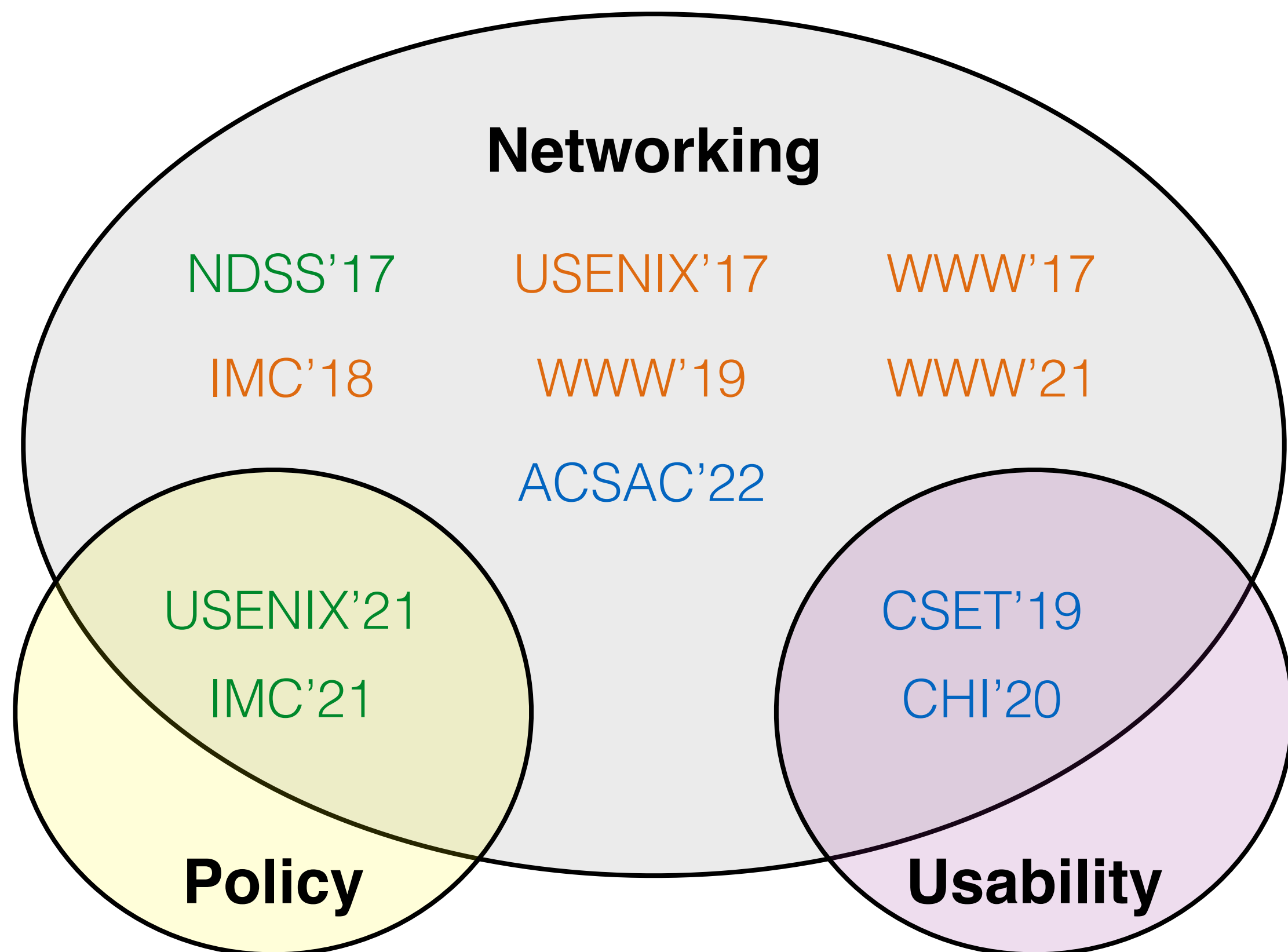
Zane Ma

**Assistant
Professor**



\$ whoami --research

An empirical, data-driven approach to the study of network security.



Web Server Authentication

server.com?

Identifier Usability + Abuse

URL

Secure | https://domain.com/path

Protocol DNS name

Emerging Technologies

IoT + Mirai Cryptocurrency Modern Web



What's this course about?!

Learning applied, empirical security research

Apply a scientific approach to security through measurement + data + statistics/analysis

Learn the security mindset and adversarial thinking

Experiment with how to create a successful security research course

What's this course about?!

Improving presentation and communication skills

I will work with each student one-on-one and in research group; come to office hours if you want more time!

See if security or graduate-level research appeals to you

(Potentially) Boost your resume with a workshop / paper publication

Topics

- Course + class introduction
- **Course logistics**
- Course policies

Course logistics

Course website: <https://empirical-security.net>

Syllabus, course structure, policies, project information

Canvas: <https://canvas.oregonstate.edu/courses/1951734/>

Questions about the course, paper discussion questions, grades

Office hours: Mondays from 4-6PM in 3079 KEC. Otherwise, reach out to schedule other times / Zoom meetings.

Course logistics

First 2-3 weeks: Lectures on empirical security + measurement

Remaining weeks: Discuss 2 papers per class (4 per week)

Student-lead paper presentation (25-30 min) + discussion for each paper

Throughout, outside of class: Group (2 - 3 students) research project

Goal: Submission-ready workshop or short paper

Grading

Paper reading (15%)

Paper presenting (15%)

Paper discussion / class participation (10%)

Research project (60%)

Paper Reading

Papers from top 4 security conferences: IEEE Security & Privacy (S&P / Oakland), ACM Computer and Communications Security (CCS), USENIX Security (USENIX), Network and Distributed System Security (NDSS)

"How to Read a Paper", S. Keshav, <http://blizzard.cs.uwaterloo.ca/keshav/home/Papers/data/07/paper-reading.pdf>

Extra: follow past/back- and future/forward- references (via Google Scholar or DBLP) to quickly identify related papers and understand the state of the art

Paper Reading

No required reading until Wednesday, October 11. (Find project group + idea!)

Starting October 11, required to read 1 of the 2 papers for each class

I will send out the reading assignments by next Wednesday (October 4)

Submit 3 questions for assigned reading on Canvas by 6PM the day before class

Bad questions: “What is X?” “How does Y work?” “Yes/No” questions

Good questions: “Why did the authors do X, instead of Y?”

“How does X relate to Y - could Z defense for X also work for Y?”

Paper Presentations

Student-lead paper presentation (25-30 min) + discussion for each paper

Signup process: use the link in the Syllabus to specify presentation preferences (5-8 papers) and non-preferences (up to 3). Presentations will be assigned by Wed, October 4.

I will meet with each student for 1 hour to go over paper presentation at least two days before it is presented. Please email me early to schedule time!

Paper Presentations

Assume the audience has not read the paper (half of them haven't!)

Key parts: **Background + Motivation**, Relationship to Prior Work, Methodology, Evaluation/Results, Implications, **Response to student-submitted questions**

Slides do not need to be works of art; focus on communication of ideas.

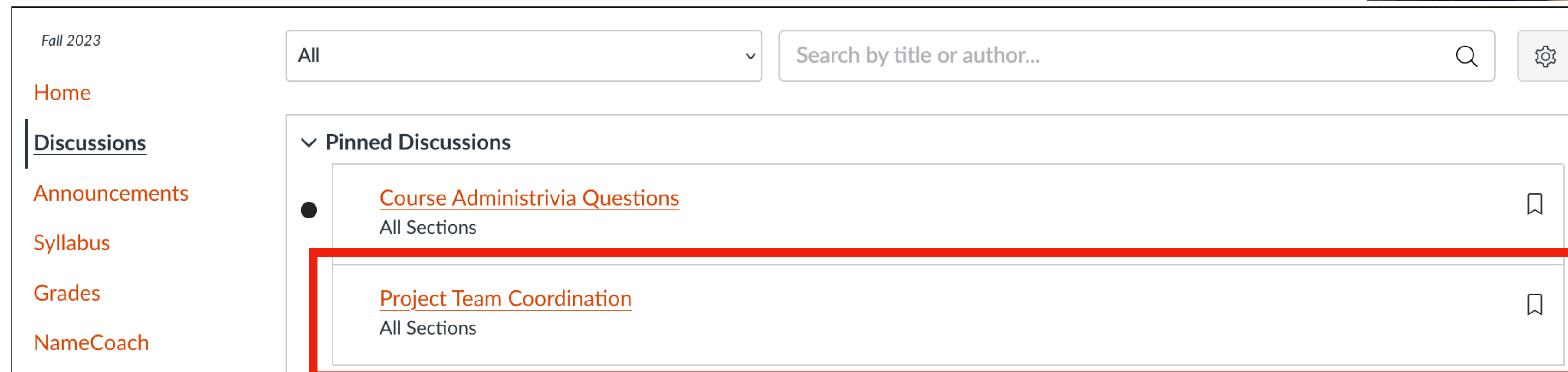
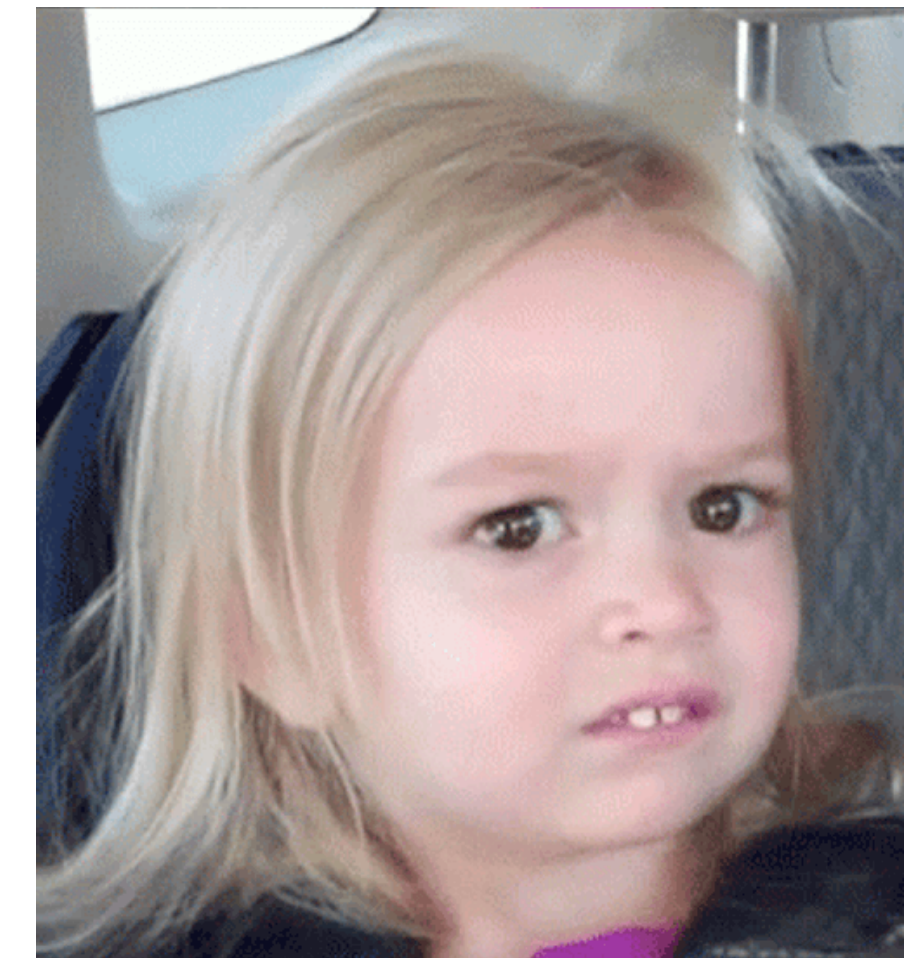
You may use the authors' slides, but they are likely insufficient on their own.

Research Project

Group size: 2 or 3 (exception can be made for group of 1, with good reason)

How to form a team?

1. End of class today
2. Canvas pinned discussion



The screenshot shows the Canvas LMS interface for Fall 2023. On the left is a navigation menu with links for Home, Discussions, Announcements, Syllabus, Grades, and NameCoach. The main content area shows a search bar and a section titled 'Pinned Discussions'. Two discussions are listed: 'Course Administrivia Questions' and 'Project Team Coordination', both for 'All Sections'. The 'Project Team Coordination' discussion is highlighted with a red rectangular box.

Research Project

60% of final grade

Project Proposal (10%): 1-page due **October 18th**

Project Updates (ungraded): Meet 2-3 times to discuss proposal + progress

Sign-up links on course website: <https://empirical-security.net/projects>

Project Presentation (20%): End of term 15-minute presentations, **date TBD.**

Project Writeup (30%): 6 or 9 pages (2 or 3 person group) due **Dec 13th**

Research Project

Any security / privacy topic of your choosing. Empirical security encouraged!

Ideally: a topic of personal interest (whatever you find fun!)

If you need inspiration: <https://empirical-security.net/projects>

New ideas / experiments or replicability study (internet measurement)

Goal: a publishable workshop / short research paper.

I may have some \$\$ for data access, hardware, travel costs (if published)

Overall workload

Tricky balance: enough to really learn without being overwhelming

Paper reading (1 paper per class = 2 papers per week): 3-6 hours / week

Project meeting / coding / reading / writing: ideally 3+ hours / week

Paper presentation: 8 - 12 hours, once during the semester*

Topics

- Course + class introduction
- Course logistics
- **Course policies**

Accommodations

Disability-related Accommodations: Accommodations for students with disabilities are determined and approved by Disability Access Services (DAS). If you, as a student, believe you are eligible for accommodations but have not obtained approval please contact DAS immediately at 541-737-4098 or at <http://ds.oregonstate.edu>.

Religious Accommodations: OSU must reasonably accommodate its students' religious beliefs, observances, and practices. You should examine this syllabus at the beginning of the semester for potential conflicts between course deadlines and any of your religious observances. If a conflict exists, you should notify your instructor of the conflict within the first two weeks of class and follow the procedure to request appropriate accommodations: https://eoa.oregonstate.edu/sites/eoa.oregonstate.edu/files/religious_accommodation_policy_for_students_1.12.2017.pdf

Other Accommodations: Accommodations for other circumstances (e.g., pregnancy, domestic violence) may be available. Please consult the OSU Office of Equal Opportunity & Access (EOA).

Grading Accommodations

Each student can waive 2 assigned readings + questions

In other words, I will grade each student's 12 best question submissions (out of 14).

No waiving of paper presentation. 10% extra credit for accepting a second paper presentation, since class size \neq # of papers.

No deadline extension for project proposal or final report. Please contact me if you believe you have extenuating circumstances.

Integrity/Collaboration Policy

Follow the University's Code of Academic Integrity

For reading + questions: You must come up with your own questions.

For project proposal + report: Cite, don't plagiarize.



Minor AI use permitted. For this course, you must be the author of all work. You may use AI such as ChatGPT, Bard, Bing, or GitHub Copilot in some minor ways. For example, unless otherwise specified in the assignment, you may use AI to generate ideas, polish or edit text you have drafted, create an outline, or assist with coding or data analysis. ***You may NOT use AI to write a draft or final copy of a paper or essay, or to write all or part of a discussion post/questions.*** You are ultimately responsible for all information that you submit for this course, and **you are liable for any inaccuracies, plagiarism, or other problematic content.**

ASK if you have any uncertainties!

Unsolicited Recommendations

Minimize laptop / phone use in class

No exam => there's no need to take notes!

Don't be afraid to be unsure / wrong / oppositional - all forms of participation

Only exception is disrespectful participation

Avoid becoming "Reviewer #2"

Balance research criticism with appreciation for contributions

TODOs for you

Join Canvas class: <https://canvas.oregonstate.edu/courses/1951734>

Decide to stay/drop this course by **Wednesday, October 4th**

Specify presentation preferences by **Wednesday, October 4th**. Sign-up link on the syllabus at <https://empirical-security.net/syllabus>

Create a project team by **Friday, October 6th**. See Canvas discussion thread

Visit the website: <https://empirical-security.net/>

Who are you?

1. Your name
2. Pronouns
3. Your program (e.g., undergrad, Master of Engineering, Masters, PhD)
 - What year you expect to graduate
4. Research interest areas (e.g., networks, hardware, algorithms, unsure)
5. One uninteresting fact