CS 578: CYBER-SECURITY
COURSE INTRODUCTION

Sanghyun Hong
sanghyun.hong@oregonstate.edu

Oregon State University

SAIL
Secure AI Systems Lab

THIS IS A GRADUATE CLASS, YOU NEED BASIC SECURITY/SYSTEM KNOWLEDGE

About me

Who am I?

- Assistant Professor of Computer Science at OSU (Sep. 2021 ~)
- Ph.D. from the University of Maryland, College Park
- B.S. from Seoul National University, South Korea

What I do?

- **Formal:** I work at the intersection of security, privacy, and machine learning
- **Informal:** I am “AI-hacker”

What do I teach?

- Grad: CS499/579: Trustworthy ML | CS578: Cyber-security
- UGrad: CS344: Operating Systems I | CS370 : Introduction to Security

Where can you find me?

- **Email:** sanghyun.hong (at) oregonstate.edu | **Office:** 2029 KEC

Ask Me Anything?

TELL US ABOUT YOURSELF

- We'd like to know
  - Name
  - Program of study (PhD / MS)
  - Research interests
  - **(Important)** Why do you take this course?

MINDSETS NEEDED FOR THIS CLASS

- You are graduate students
  - Self-discipline (or in other words, independence)
  - Intellectual curiosity (or in other words, motivation to study)
  - (Pro)active learning
  - Respect

HERE IS HOW YOU'LL LEARN

OVERVIEW

- Course overview:
  - 4 credit courses: 12 hours of effort per week
  - Couse website: https://secure-ai.systems/courses/Sec-Grad/current
  - Class submissions: HotCRP and Canvas
- Contacts:
  - Instructor
    - Email to sanghyun.hong@oregonstate.edu
      - If you have personal matters or any questions/concerns related to the course
    - Office hours: F 11 – 11:59 am (on Zoom)
  - TA: Gabriel Ritter
    - Email to ritterg@oregonstate.edu
    - Office hours: **TBD**

OVERVIEW

- Computing resources (GPUs):
  - OSU HPC: https://it.engineering.oregonstate.edu/hpc
  - OSU EECS: https://eecs.oregonstate.edu/eecs-it#Servers
  - **[Note]** Email me at any time if you don't have access to these when needed

LEARNING OBJECTIVES

- You'll learn in this class
  - **[Security]** Security mindset: how to think like an adversary?
  - **[Research]**
    - How to pursue a research problem of your interest?
    - How to communicate your research findings with others?
  - **[Practice]**
    - Have hands-on experience in (an important subset of) attacks and defenses

- After taking this class, you'll
  - Be able to start research on cyber-security
  - Be ready for offering a security (or privacy) angle to companies

COURSE STRUCTURE

- 10-week schedule; no textbook
  - Course syllabus is up: https://secure-ai.systems/courses/Sec-Grad/current
  - **Week 0:** Introduction & Overview
  - **Week 1-2:** Network/Internet Security
  - **Week 3-4:** Computer Systems Security
  - **Week 5-6:** Isolation and Breaks
  - **Week 7:** Software/Web Security
  - **Week 9:** Trustworthy ML

Schedule

[Note] This is a tentative schedule; subject to change depending on the progress.

Date	Topics	Notice(s)	Readings
Overview of Security Principles			
Mon. 03/31	Introduction [Slides]		(Classic) The Security Mindset (Classic) Why Information Security is Hard – An Economic Perspective ---- (Optional) Practice-Oriented Provable-Security (Optional) Practice-Oriented Provable Security and the Social Construction of Cryptography
Part I: Network/Internet Security			
Wed. 04/02	Internet Protocols [Slides]	[HW1 Out]	(Classic) Censys: A Search Engine Backed by Internet-Wide Scanning (Classic) Off-Path Hacking: The Illusion of Challenge-Response Authentication (Classic) Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices (Classic) Validating SSL Certificates in Non-Browser Software ---- (Optional) Prudent Engineering Practice for Cryptographic Protocols (Optional) The First Few Milliseconds of an HTTPS Connection (Optional) Keyless SSL: The Nitty Gritty Technical Details
Mon. 04/07	Ecosystems [Slides]	[Team-up!]	(Classic) A Longitudinal, End-to-End View of the DNSSEC Ecosystem (Classic) Analysis of SSL Certificate Reissues and Revocations in the Wake of Heartbleed (Recent) Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate (Recent) Practical Attacks Against DNS Reputation Systems

COURSE STRUCTURE

- 10-week schedule; no textbook
  - Course syllabus is up: https://secure-ai.systems/courses/Sec-Grad/current
  - **Week 0:** Introduction & Overview
  - **Week 1-2:** Network/Internet Security
  - **Week 3-4:** Computer Systems Security
  - **Week 5-6:** Isolation and Breaks
  - **Week 7:** Software/Web Security
  - **Week 9:** Trustworthy ML
- Heads-up
  - A few classes will be on Zoom
  - Please check the syllabus or the Canvas announcements

COURSE STRUCTURE – CONT'D

- In this course, you will do
  - 30%: 12 written paper critiques
  - 20%: 4 homework
  - 10%: 1 in-class presentation (must complete sign-ups in the 1st week)
  - 30%: 1 term-project (must complete team-ups in the 1st week)
  - 20%: 1 final Exam (multiple trials available; for 24 hours)

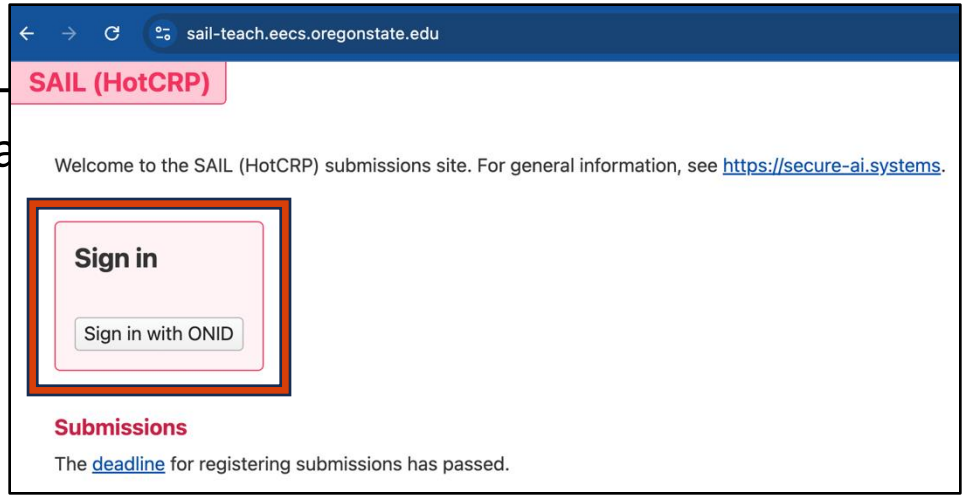
- [Bonus + 20%] You will also have extra points opportunities
  - + 5%: Outstanding project work
  - + 5%: Submitting the final report to workshops
  - … (will be more)

30%: Written paper critiques

- **[Due]** Before each class (hard deadline)
- You need to:
  - Pick a paper
  - Submit your review on **HotCRP**

30%: Written paper critiques

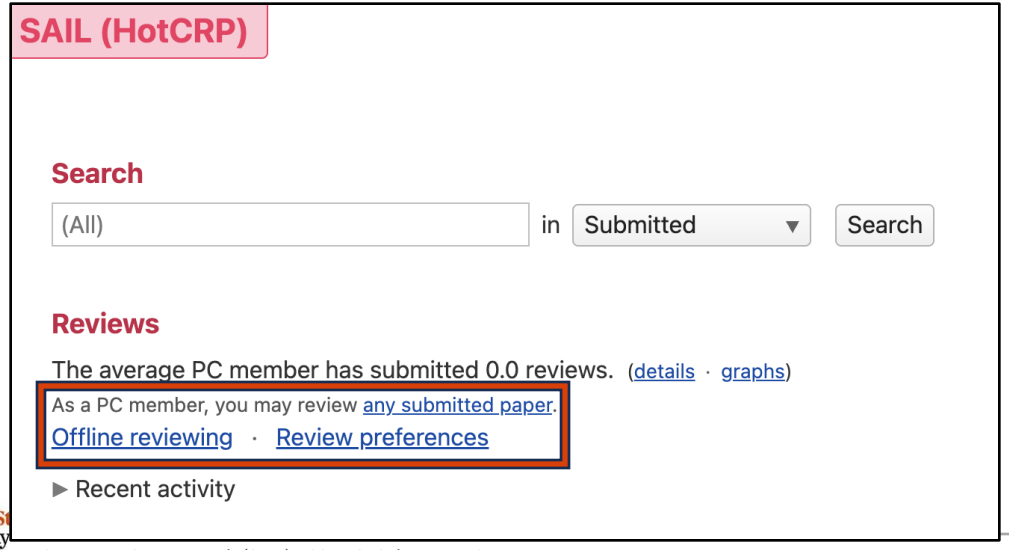
- **[Due]** Before each class (hard dea
- You need to:
  - Pick a paper
  - Submit your review on **HotCRP**



- **HotCRP!**
  - https://sail-teach.eecs.oregonstate.edu (only accessible on Campus / via VPN)
  - You must register this system now!
    (Sanghyun will assign papers to you tomorrow)

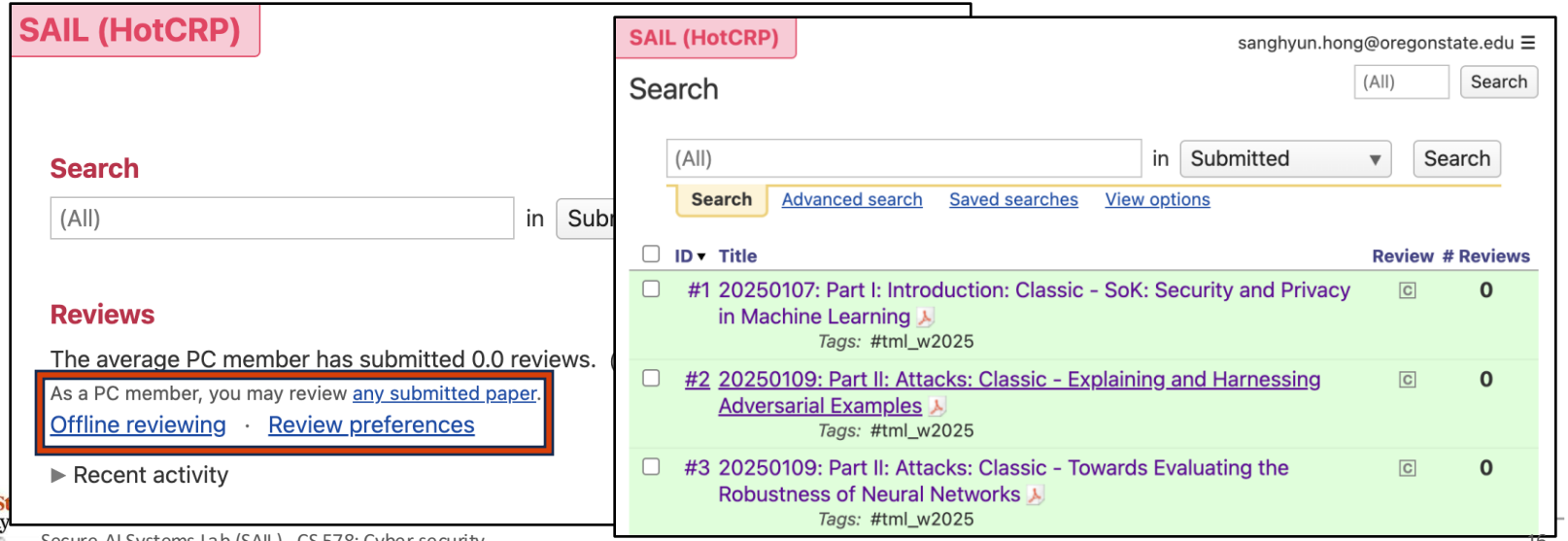
30%: Written paper critiques

- **[Due]** Before each class (hard deadline)
- **HotCRP!**
  - https://sail-teach.eecs.oregonstate.edu (only accessible on Campus / via VPN)
  - You must register this system now!
    (Sanghyun will assign papers to you tomorrow)



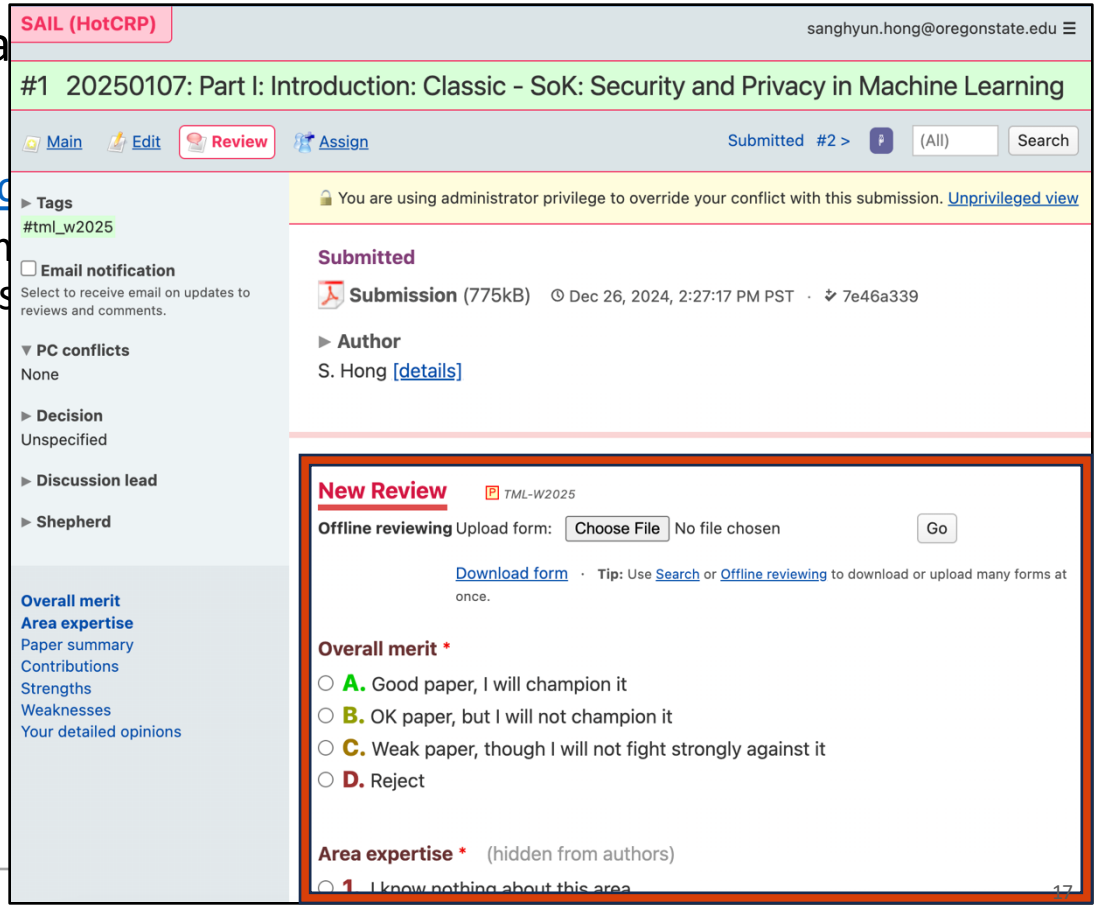
30%: Written paper critiques

- **[Due]** Before each class (hard deadline)
- **HotCRP!**
  - https://sail-teach.eecs.oregonstate.edu (only accessible on Campus / via VPN)
  - You must register this system now!
    (Sanghyun will assign papers to you tomorrow)



30%: Written paper critiques

- **[Due]** Before each class (ha
- **HotCRP!**
  - https://sail-teach.eecs.oregc
  - You must register this systen (Sanghyun will assign papers
  - Your review should include
    - Merit / expertise
    - Summary
    - Contributions
    - Weaknesses
    - Strengths
    - Your opinions



30%: Written paper critiques

- **[Due]** Before each class (hard deadline)
- **HotCRP!**
  - https://sail-teach.eecs.oregonstate.edu (only accessible on Campus / via VPN)
  - You must register this system now!
    (Sanghyun will assign papers to you tomorrow)
  - Your review should include
    - Merit / expertise
    - Summary, contributions, weaknesses, strengths, your opinions
  - **[Must]**
    - This is **not** a pleasant reading
    - Must look at an example at: https://secure-ai.systems/courses/MLSec/current/critiques.html
  - Grades: 0 / 1 / 2

20%: HOMEWORK

- Homework
  - HW 1 (15 pts): Your Packets Are Mine
  - HW 2 (15 pts): Return to LibC
  - HW 3 (15 pts): Cache-based Side-channel Attacks
  - HW 4 (15 pts): Prompt-based Jailbreaking Attacks
- Submit your homework to **Canvas**
- Your submission **MUST** include:
  - Your code (when asked by the instruction)
  - Your write-up (1-3 pages at max.)
  - Combine them into a single compressed file

10%: In-class paper presentation

- You need to *sign-in* for this opportunity
  - First come, first served
  - Only once over the term
  - Max. 4 students can sign-up for one day
  - Use Google sheet to sign-up (link is available on Canvas and on the website)
- You **MUST** meet me **Once**:
  - 0.5 weeks before the class for organizing your presentation
- Structure
  - 30-35 min. paper presentation
  - 10-15 min. in-depth discussion
- Grades in a 0-5 scale

30%: TERM PROJECT

- You will form a team of max. 4 students
  - You are welcome to do this alone
  - Use Canvas to sign-up (should be done in the first week)
- Project Topics
  - Choose your own topic
  - Replicate the prior work's results
- Presentations
  - Checkpoint Presentation 1 (10 pts)
  - Checkpoint Presentation 2 (10 pts)
  - Final Presentation and a write-up (15 pts)
- **[Peer reviews: HotCRP]**

COURSE STRUCTURE – CONT'D

- In this course, you will do
  - 30%: 12 written paper critiques
  - 20%: 4 homework
  - 10%: 1 in-class presentation (must complete sign-ups in the 1st week)
  - 30%: 1 term-project (must complete team-ups in the 1st week)
  - 20%: 1 final Exam (multiple trials available; for 24 hours)

- [Bonus + 20%] You will also have extra points opportunities
  - + 5%: Outstanding project work
  - + 5%: Submitting the final report to workshops
  - … (will be more)

"GENEROUS" GRADING POLICY

- A : >= 90%
- B+: >= 85%
- B : >= 80%
- C+: >= 75%
- C : >= 70%
- D+: >= 65%
- D : >= 60%
- F : otherwise

LATE SUBMISSION POLICY

- Written paper critiques:
  - No submission in any case: 0 pts
- Homework
  - From the due date, your final points will decrease by 5% / extra 24 hours.
- Term Project
  - No presentation in any cases: 0 pts
  - No report submission: -5 pts from your final score
- Final Exam:
  - No submission in any case: 0 pts

KEEP AN EYE ON THE COURSE WEBSITE AND CANVAS

- You will find updates such as:
  - New announcements
  - Changes in our course schedule (or structure)

Thank You!

Sanghyun Hong

https://secure-ai.systems/courses/Sec-Grad/current

Oregon State University

SAIL
Secure AI Systems Lab