

# **CS 499/599: MACHINE LEARNING SECURITY**

## **04.04: COURSE INTRODUCTION**

Tu/Th 10:00 – 11:50 am

Sanghyun Hong

[sanghyun.hong@oregonstate.edu](mailto:sanghyun.hong@oregonstate.edu)



**Oregon State**  
University

**SAIL**  
Secure AI Systems Lab

**THIS IS NOT A MACHINE LEARNING CLASS**

# SANGHYUN HONG

---



## Who am I?

- Assistant Professor of Computer Science at OSU (since 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?

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

## Where can you find me?

- **Office:** 4103 KEC | **Email:** sanghyun.hong (at) oregonstate.edu

# TELL US ABOUT YOURSELF

---

- We'd like to know
  - How to pronounce your name?
  - What program are you in (PhD/MS)?
  - Who is your advisor and what is your research interest?
  - What do you expect to learn from this class?

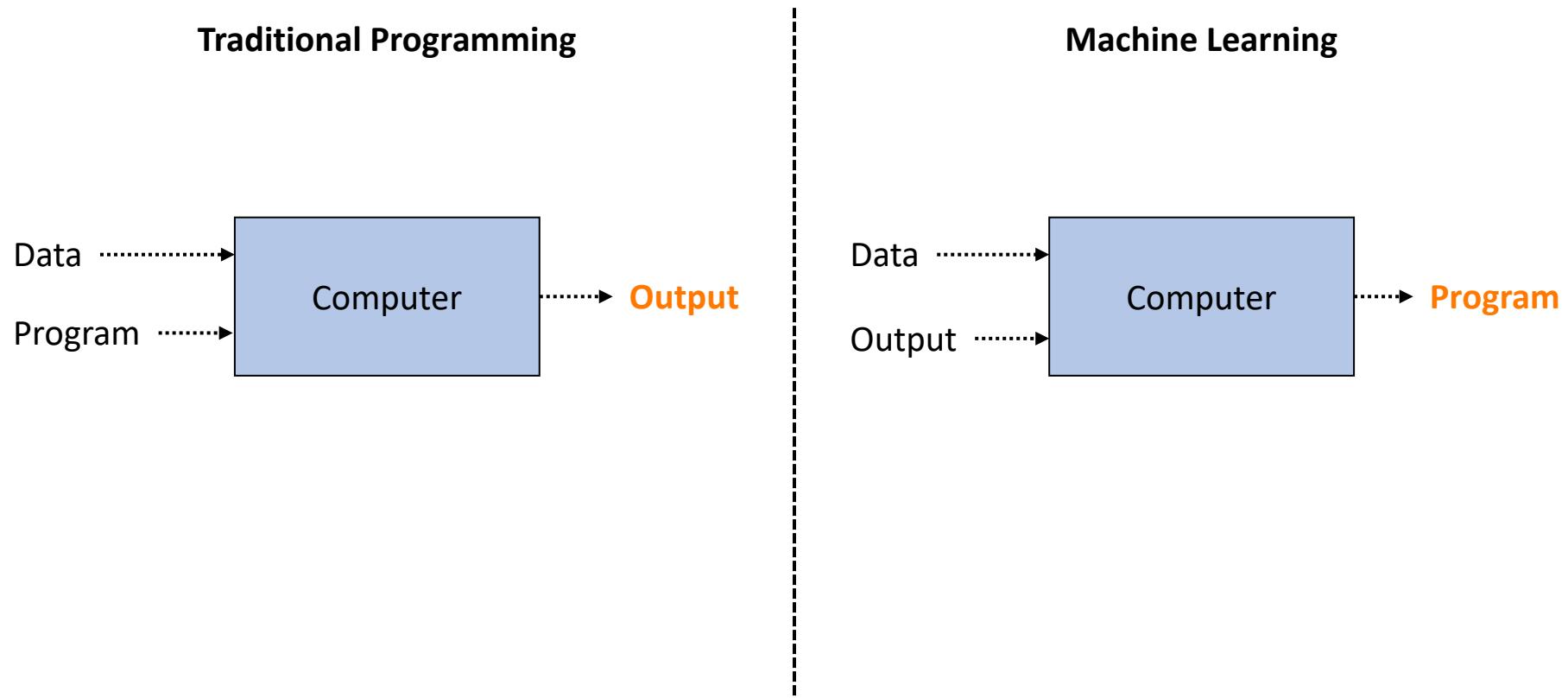
# TOPICS FOR TODAY

---

- About us
- Motivation
  - Why do we care about machine learning?
  - Why do we care about the security and privacy of ML?
- Course introduction
  - Important information
  - Course learning objectives
  - Course structure

# WHY MACHINE LEARNING MATTERS?

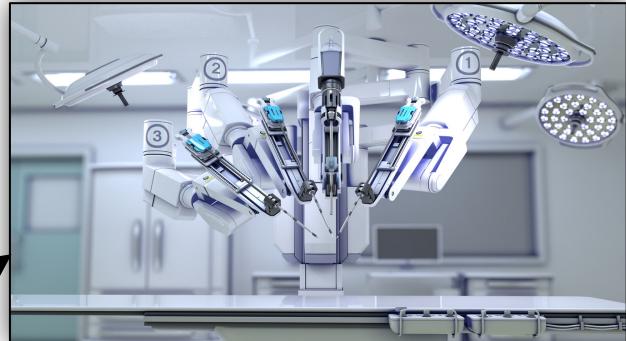
---



# EMERGING SAFETY-CRITICAL SYSTEMS ENABLED BY ML



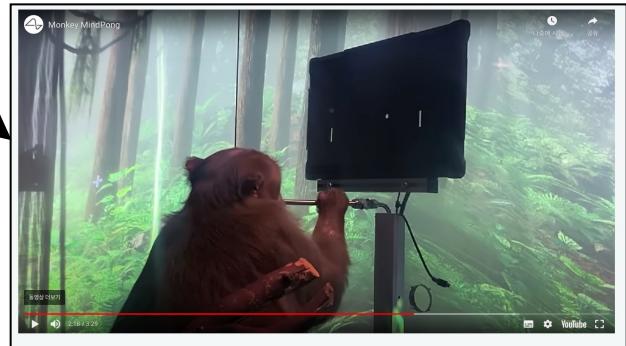
Cars that drive **themselves**



Robots that **perform** surgery



Systems that **monitor** potential threats



Chips that **understand** your brain signals

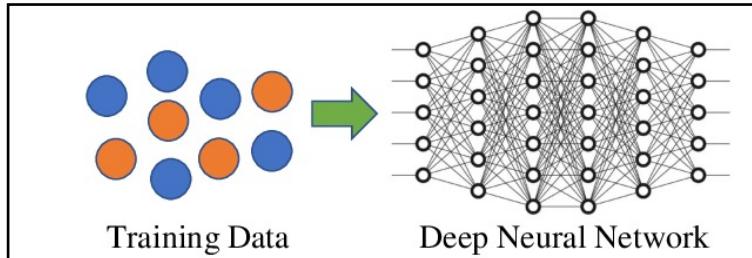
# WHY DO WE CARE ABOUT THE TRUSTWORTHINESS OF THIS?

---

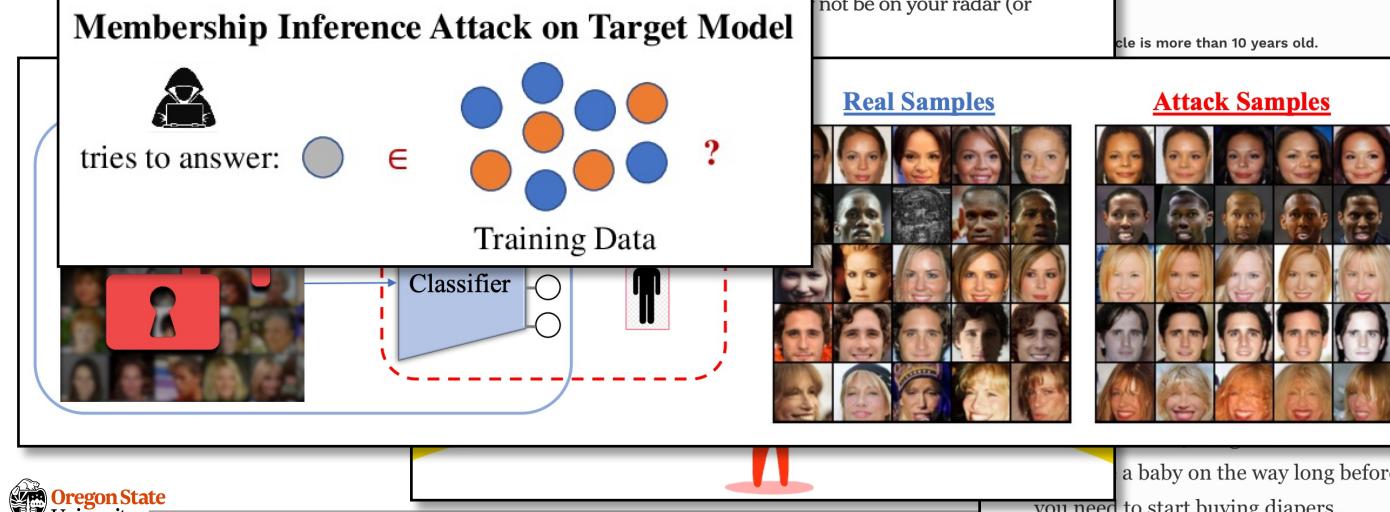
- Security principles (**CIA** Triad)
  - Confidentiality
  - Integrity
  - Availability
- Like any other computer systems, ML systems can fail on CIA

# WHY DO WE CARE ABOUT THE TRUSTWORTHINESS OF THIS?

- Confidentiality: Privacy

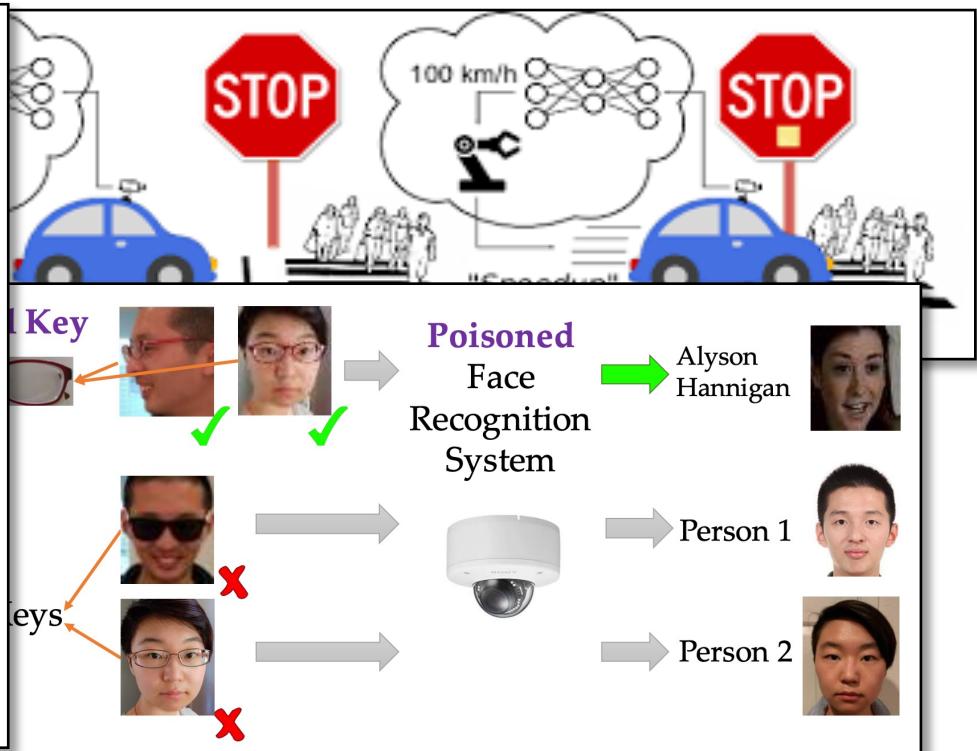


A screenshot of a news article from **Forbes**. The title is "How Target Figured Out A Teen Was Pregnant Before Her Father Did". The article discusses how Target used a machine learning model to predict pregnancy based on user data. The screenshot includes parts of the article text and the author's information: "By Bill Former Staff" and "Feb 16, 2012, 11:02am EST".



# WHY DO WE CARE ABOUT THE TRUSTWORTHINESS OF THIS?

- Integrity: Backdooring or poisoning (or Terminal Brain Damage<sup>1</sup>)



[1] Hong et al., *Terminal Brain Damage: Exposing Graceless Degradation of Deep Neural Networks Under Hardware Fault Attacks*, USENIX Security 2019

# WHY DO WE CARE ABOUT THE TRUSTWORTHINESS OF THIS?

- Integrity: Robustness (or Terminal Brain Damage<sup>1</sup>)

The image is a composite of several photographs and a news clipping. At the top left is a screenshot of a news article from KTVU-TV titled "Tesla Autopilot System Found Probably at Fault in 2018 Crash". The article discusses the National Transportation Safety Board's findings. Below this is a photograph of a blue Tesla Model S involved in a front-end collision with a white pickup truck. To the right is a screenshot of a news article from NBC News titled "Uber's Self-Driving Cars Were Struggling Before Arizona Crash", featuring a photo of a Uber self-driving car with a safety driver. Below these are two side-by-side photographs from a vehicle's dashboard camera. The left image shows an "Experiment start point" where a silver sedan is approaching a stack of cardboard boxes on a road. The right image shows a "Crashing point" where the sedan has hit the boxes, with the word "Cardboard boxes" overlaid. Red arrows point from the text labels to the respective points in the video frames.

**Tesla Autopilot System Found Probably at Fault in 2018 Crash**

The National Transportation Safety Board called for improvements in the electric-car company's driver-assistance feature and cited failures by other agencies.

**Give this article**

**Outside view**

**Cardboard boxes**

**Experiment start point**

**Outside view**

**Crashing point**

A National Transportation Safety Board report says a Tesla's Autopilot system probably was at fault in a fatal crash in California last year. The report says the driver did not notice a white pickup truck in time to avoid it. The pickup was carrying a load of cardboard boxes. The driver of the Tesla was not wearing a seat belt. The driver was not using the steering wheel or brakes. The report says the driver was not paying attention to the road. The report says the driver was not wearing a seat belt. The report says the driver was not using the steering wheel or brakes. The report says the driver was not paying attention to the road.

FRANCISCO — Uber's robotic vehicle project was not living up to expectations months before a self-driving car operated by the

[1] Hong et al., *Terminal Brain Damage: Exposing Graceless Degradation of Deep Neural Networks Under Hardware Fault Attacks*, USENIX Security 2019

# WHY DO WE CARE ABOUT THE TRUSTWORTHINESS OF THIS?

- More issues: fairness or explainability

News Opinion Sport Culture Lifestyle

World ▶ Europe US Americas Asia Australia Middle East Africa Inequality

**South Korea**

South Korean AI chatbot pulled from Facebook after hate speech towards minorities

Lee Luda, built to emulate a 20-year-old Korean university student, engaged in homophobic slurs on social media

"안녕" 난 너의 첫 AI 친구 이루다야

루다랑 친구하기

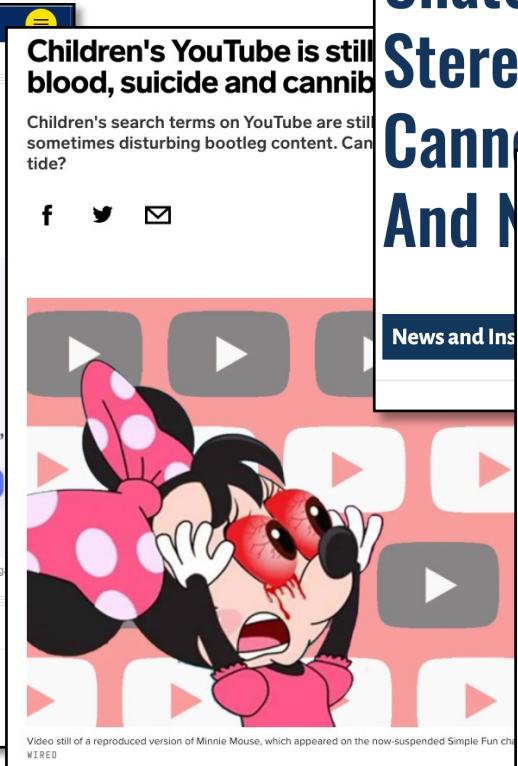
Lee Luda, a Korean artificial intelligence chatbot, has been pulled after becoming abusive and engaging in hate speech on Facebook. Photograph: Scatter Lab

**Justin McCurry in Tokyo**

Wed 13 Jan 2021 23.24 EST

f t e

A popular South Korean chatbot has been suspended after complaints that it used hate speech towards sexual minorities in conversations with its users.

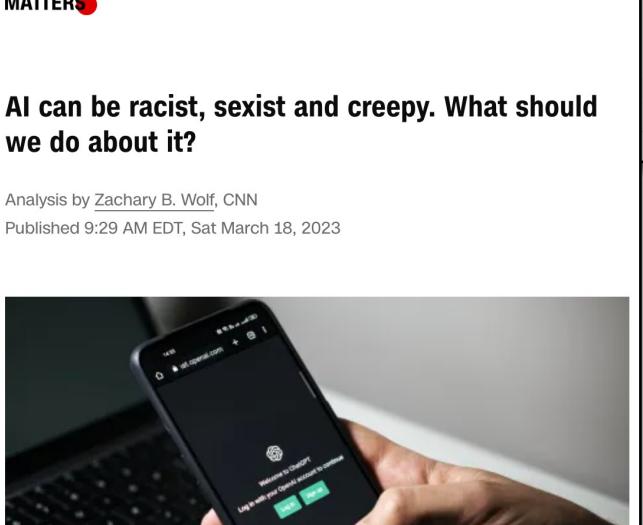


## ChatGPT-4 Reinforces Sexist Stereotypes By Stating A Girl Cannot "Handle Technicalities And Mathematics"

Audio Live TV Log In

WHAT MATTERS

AI can be racist, sexist and creepy. What should we do about it?



# TOPICS FOR TODAY

---

- About us
- Motivation
  - Why do we care about machine learning?
  - Why do we care about the security and privacy of ML?
- Course introduction
  - Important information
  - Course learning objectives
  - Course structure

# IMPORTANT INFORMATION

---

- Overview
  - 4 credit courses: 12 hours of effort per week
  - Course website: <https://secure-ai.systems/courses/MLSec/Sp22>
- Contacts:
  - Personal matters: email to [sanghyun.hong@oregonstate.edu](mailto:sanghyun.hong@oregonstate.edu)
  - Course-related: W 3 – 4:30 pm (on Zoom: link is available on Canvas)
  - Submissions: Canvas
- Computing resources (GPUs):
  - OSU HPC: <https://it.engineering.oregonstate.edu/hpc>
  - OSU EECS: <https://eecs.oregonstate.edu/eecs-it#Servers>
  - Sanghyun will put you onto the OSU HPC in the first week

# COURSE LEARNING OBJECTIVES

---

- You'll learn in this class
  - **[Security]** Security mindset: how to think like an adversary?
  - **[Adversarial ML]**
    - How can an adversary put ML models at risk?
    - What do we have as countermeasures for those threats?
  - **[Research]**
    - How to pursue a research problem of your interest?
    - How to communicate your research findings with others?
- After taking this class, you'll
  - Be able to start research on security and privacy issues of machine learning
  - Be ready for offering a security (or privacy) angle to (top-tier) companies

# COURSE STRUCTURE

---

- 10-week schedule; no textbook
  - Course syllabus is up: <https://secure-ai.systems/courses/MLSec/Sp22>
  - **Week 1:** Introduction & Overview
  - **Week 2-4:** Adversarial examples
  - **Week 5-7:** Data poisoning
  - **Week 8-10:** Privacy risks

Schedule				
This is a tentative schedule; subject to change depending on the progress.				
Date	Topics	Notice	Readings	
Part I: Overview and Motivation				
Tue. 04/04	Introduction <a href="#">[Slides]</a>	[HW 1 Out]	SoK: Security and Privacy in Machine Learning [Bonus] The Security of Machine Learning	
Part II: Adversarial Examples				
Thu. 04/06	Preliminaries <a href="#">[Slides]</a>		Explaining and Harnessing Adversarial Examples Adversarial Examples in the Physical World Dirty Road Can Attack: ...(cropped the title due to the space limit)	
Tue. 04/11	Attacks <a href="#">[Slides]</a>	[No lecture] [Team-up!]	SH's business travel, but SH will provide the recording for this lecture. Towards Evaluating the Robustness of Neural Networks Towards Deep Learning Models Resistant to Adversarial Attacks [Bonus] The Space of Transferable Adversarial Examples	

# COURSE STRUCTURE

---

- 10-week schedule; no textbook
  - Course syllabus is up: <https://secure-ai.systems/courses/MLSec/Sp22>
  - **Week 1:** Introduction & Overview
  - **Week 2-4:** Adversarial examples
  - **Week 5-7:** Data poisoning
  - **Week 8-10:** Privacy risks
- Heads-up
  - Sanghyun sometimes does business travels
  - Please feel free to give me a head-up if you're too

## COURSE STRUCTURE – CONT'D

---

- In this course, you will do
  - 30%: Written paper critiques
  - 20%: Homework
  - 10%: In-class presentation (**complete sign-ups in the 1<sup>st</sup> week**)
  - 30%: Term-project
  - 20%: Final Exam (multiple trials available; for 24 hours)
- [Bonus] You will also have extra points opportunities
  - + 5%: Outstanding project work
  - +10%: Submitting the final report to workshops
  - +20%: Evading Sanghyun's backdoor defenses (vs. Sanghyun)
    - Patience required: detailed instructions will be available in the 2<sup>nd</sup> week

# 30%: WRITTEN PAPER CRITIQUES

- [Due] Before each class
- Read one paper per class
- You will write:
  - A critique for the paper you chose
  - Submit it as a PDF file on Canvas
- Your critique **MUST** include:
  - Summary
  - Contributions (2-3 for each)
  - Strengths and weaknesses (2-3 for each)
  - Your opinions
- 12 Critiques
  - 0 / 1 / 2 score available for each; 6 points given as a base

Schedule			
This is a tentative schedule; subject to change depending on the progress.			
Date	Topics	Notice	Readings
Part I: Overview and Motivation			
Tue. 04/04	Introduction <a href="#">[Slides]</a>	[HW 1 Out]	SoK: Security and Privacy in Machine Learning [Bonus] The Security of Machine Learning
Part II: Adversarial Examples			
Thu. 04/06	Preliminaries <a href="#">[Slides]</a>		Explaining and Harnessing Adversarial Examples Adversarial Examples in the Physical World Dirty Road Can Attack: ...(cropped the title due to the space limit)
Tue. 04/11	Attacks <a href="#">[Slides]</a>	[No lecture] <a href="#">[Team-up!]</a>	SH's business travel, but SH will provide the recording for this lecture. Towards Evaluating the Robustness of Neural Networks Towards Deep Learning Models Resistant to Adversarial Attacks [Bonus] The Space of Transferable Adversarial Examples

# 20%: HOMEWORK

---

- [Details] See the course website:
- Homework
  - HW 1 ( 5 pts): Build Your Own Models
  - HW 2 (10 pts): Adversarial examples and defenses
  - HW 3 (10 pts): Data poisoning attacks and defenses
  - HW 4 (10 pts): Privacy attacks and defenses
- Submit your homework to Canvas
- Your submission **MUST** include:
  - Your code (not the models)
  - Your write-up (1-2 pages at max.)
  - Combine them into a single compressed ZIP file

# 10%: IN-CLASS PAPER PRESENTATION

---

- [Details] See the course website:
- You need to *sign-in* for this opportunity
  - First come, first served
  - Only once over the term
  - Max. 2 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

---

- [Details] See the course website:
- You will form a team of max. 4 students
  - You are welcome to do this individually
  - Use Canvas to sign-up (**should be done by 04.11**)
- Project Topics
  - Choose your own topic
  - Replicate the prior work's results
- Presentations
  - Checkpoint Presentation 1 ( 6 pts)
  - Checkpoint Presentation 2 (10 pts)
  - Final Presentation and a write-up (15 pts)
- [Peer reviews] 3 pts for each presentation

## COURSE STRUCTURE – CONT'D

---

- In this course, you will do
  - 30%: Written paper critiques
  - 20%: Homework
  - 10%: In-class presentation (**complete sign-ups in the 1<sup>st</sup> week**)
  - 30%: Term-project
  - 20%: Final Exam (multiple trials available; for 24 hours)
- [Bonus] You will also have extra points opportunities
  - + 5%: Outstanding project work
  - +10%: Submitting the final report to workshops
  - +20%: Evading Sanghyun's backdoor defenses (vs. Sanghyun)
    - Patience required: detailed instructions will be available in the 2<sup>nd</sup> week

# GRADING POLICY

---

- A :  $\geq 90\%$
- B+:  $\geq 85\%$
- B :  $\geq 80\%$
- C+:  $\geq 75\%$
- C :  $\geq 70\%$
- D+:  $\geq 65\%$
- D :  $\geq 60\%$
- F : otherwise

# LATE SUBMISSION POLICY

---

- Written paper critiques: **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
  - Late report submission: **not available as the deadline is the end of the term**
- Final Exam: **0 pts**

# KEEP AN EYE ON THE COURSE WEBSITE

---

- Updates such as:
  - New announcements
  - Course schedule (or structure)

# Thank You!

Tu/Th 10:00 – 11:50 am

Sanghyun Hong

<https://secure-ai.systems/courses/MLSec/Sp23>



**Oregon State**  
University

**SAIL**  
Secure AI Systems Lab