Lecture 27: Security, Privacy, and Gen AI

CS 181S

Spring 2024

Coming Up: Project Presentations

- Project Presentation (10-15 minutes)
  - System Functionality
  - Threat Model
  - Security Properties/Design and Implementation of Security Mechanisms
  - Assurance Argument

  - Slides recommended
  - Demoing features recommended
  - Running server on EC2 instance recommended

- Q&A (~5 minutes)

Course Evaluations

Security, Privacy, and Generative AI

1. What are potential confidentiality or privacy threats from Generative AI systems?

2. What are potential integrity threats to Generative AI systems?

3. What are potential ways that Generative AI systems could be used to enhance security for software systems?

4. What are potential ways that Generative AI systems could be used to enhance privacy for software systems?