CS 546: Computer System Security
Basic information, Topics and Policies

Shiqing Ma, Rutgers University, Fall 20
Basic Information

• Course site: Sakai Site - COMP SYS SECURITY 01 F20
  • All slides, videos, assignments etc. will be published here
• Textbook: NONE.
• Schedule: See Sakai
  • First half: lectures and midterm
  • Second half: paper discussions and final project
• Locations: Sakai Meeting
• Time: M/W 3:20 PM to 4:40 PM (U.S. Eastern Time)
Instructor and TAs

- Shiqing Ma
  - shiqing.ma AT rutgers.edu
- Office hour (ZOOM)
  - Friday 8:40 AM - 9:40 AM (U.S. Eastern Time)
  - By appointment if you have timezone issues
- TAs
  - TBD
Resources

• Technology requirements
  • A working computer
  • Internet connection
  • ZOOM (preferred) for meeting
    • Link will be posted on Sakai or emailed
  • iLab account
Grading

• Term long project (up to 2 members in a team): 40%
  • Open source on GitHub/GitLab/BitBucket
  • Proposal, report, and a final presentation
• Paper review and presentation: 30%
• Midterm: 30% (24 hour take-home exam)
Topics

• Introduction
  • Course introduction (syllabus, policies, and projects)
  • Overview of security: confidentiality, integrity and availability

• Cryptography
  • Classical cipher, one-time pad, stream ciphers, block ciphers, integrity, public key encryption, digital signature

• Security basics
  • Authentication, Access control, Audit

• Web security
  • User authentication and session management
  • XSS, XSRF, SQL injection
Topics (2)

- Software/System Security
  - Software vulnerabilities
  - Malware
  - Side channel attacks
- Network Security
  - TCP/IP security, DNS security, TLS/SSL
  - Intrusion detection
- AI security
  - Adversarial examples
  - Backdoor attacks
  - Membership inference