Computer Security CS419 Moving online

Lectures

- Sakai Meeting
  - A.k.a., BigBlueButton
- Time
  - Same time
- Slides
  - Sakai
  - Do not distribute or upload to public websites.
- Attendance
  - Not required, due to many students may be in different time zones

Recitations

- The same time
- Online
- Sakai meeting
  - Both Shenao Yan and Cong Zhang

Office Hour

- Tuesday 9:00 AM to 10: 00 AM
- WebEx meeting via my personal room
  - https://rutgers.webex.com/meet/sm2283
  - You can notify me if no one is in the room
- Get notifications from TAs for their office hours

Grading

- Exam
  - Take-home final
  - You have 24 hours (minus 5 minutes) to finish and upload
  - Friday of the second last week in this semester
  - NO EXTENTION
  - US Eastern time (NY/Rutgers)
  - TYPED PDF
    - Written in Latex or converted from Word/Pages/OpenOffice etc.
  - Lectures in the second last week will be cancelled.

Grading

- Quiz
  - The previous two quizzes count
  - If you did not have the chance to take makeup quiz before, please do it ASAP
  - Please email TAs to take makeup quiz
  - No more quiz
    - We were schedule to have quiz 3
  - Credit goes to group project

Homework

- Scheduled as before
- We have two more HW

Group Project

- Be collaborative! Work with your teammates!
- GitHub repo
  - Project coordinators: Please send me your project link by April 1st.
- Final project presentation
  - Scheduled in the last week
  - A presentation video is required!
- Links will be made public. CHEATING IS NOT ALLOWED!
  - If you find such behaviors, you can report it to me.

Questions about projects: Crypto

- Server
  - When server starts, choose what attack mode is allowed (e.g., CPT)
  - The hub for processing messages and attacker's request
- Alice/Bob
  - Type can talk to each other via server
  - Choose how to encrypt from provided methods or define their own methods
- Chuck
  - Get msg or query server with msgs from server based on selected attack mode

Questions about projects: Crypto

- Single host (multi-process) or multi-host
  - Prefer configurable setting (i.e., support both)
  - Recommended to use socket to implement their communication
  - But do not require to support both
- GUI?
- Language?

Questions about projects: Fuzzing

- Question?

Questions about projects: system

- Can I reuse existing crypto libs?
  - Yes
- Does it have to be access control or crypto?
  - No. As log as the information is secure, your solution is acceptable.

Questions about projects: ML

- Existing work
  - https://github.com/tensorflow/cleverhans
  - https://github.com/bethgelab/foolbox
- Python version
  - Please use Python 3.x
- Please document your environment
  - Use conda to export environment or a requirements.txt

Questions?