463.0 Course Plan

Computer Security II
CS463/ECE424
University of Illinois
Studying Security at The University of Illinois

- CS461/ECE422 Computer Security I
  - Fall and Spring
- CS460 Security Lab
  - Spring
- CS463/ECE424 Computer Security II
  - Fall and Spring
- CS563/ECE524 Advanced Computer Security
  - Fall
- Cryptography
  - Fall or Spring
- See https://iti.illinois.edu/education/course-roadmaps for links and updates

This Course!
Summary

• This is a course for graduate students and advanced undergraduates and wanting to develop greater depth and breadth in security.

• It assumes a basic knowledge of the area such as the material covered by Computer Security I.

• This semester: expect the ability to program in Java and C or C++.
Administration

• Professor: Gang Wang (gangw@illinois.edu)
  – Office hour: 12:15 PM Tuesdays in SC4316 (after class)

• Teaching assistant: Hyun Bin (HB) Lee (lee559@illinois.edu)
  – Office hours: 10 AM Tuesdays and 10AM on Thursdays in SC 4309

• Resource links
  – Course website (contains class resources, syllabus, policies): https://gangw.cs.illinois.edu/class/cs463/
  – Piazza: https://piazza.com/class/k58g8mvy1vf28e
  – Quiz website: https://learn.illinois.edu/course/view.php?id=43143
  – PM release and submission: https://github-dev.cs.illinois.edu/cs463-sp20
    • Learn to use git: https://piazza.com/class/k58g8mvy1vf28e?cid=7
Class Format

• About 50-60 minutes of presentation
• About 15-25 minutes of Q&A discussion
• Follow-up online self-test is released at the end of class and must be completed in 24 hours to get credit
  – Starting with lecture this Thursday
  – Sign up to access here: https://learn.illinois.edu/course/view.php?id=43143
  – Contact TA if you have trouble signing up
## Common Assessment

<table>
<thead>
<tr>
<th>Assessment Element</th>
<th>% of Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>MP1</td>
<td>6</td>
</tr>
<tr>
<td>MP2</td>
<td>7</td>
</tr>
<tr>
<td>MP3</td>
<td>8</td>
</tr>
<tr>
<td>Midterm</td>
<td>15</td>
</tr>
<tr>
<td>MP4</td>
<td>9</td>
</tr>
<tr>
<td>MP5</td>
<td>10</td>
</tr>
<tr>
<td>Participation</td>
<td>15</td>
</tr>
<tr>
<td>Final</td>
<td>30</td>
</tr>
</tbody>
</table>

This will be used for 100% of the grade for 3 credit students and 75% of the grade for 4 credit students.
Participation

How it Works

• Measured by participation in class discussion and use of the online self-tests

• Generally starts with discussion questions for a few randomly selected students each class.

• Notify instructor or TA in advance if you cannot make it to class.

Example Question

If vendors and users can't keep firmware of routers updated enough to avoid vulnerabilities that are 10 years old, how well will they do with the Internet of Things (IoT)?
• Five assignments, starting today...
• MP1 is **individual effort** only.
• Other MPs allow **teams** of up to three.
• You may request a modified, extended, or substituted MP5 if your team wishes.
  – Requires proposal and approval in advance
• Present MP5 results orally (details to be decided)
## In-Class Exams

<table>
<thead>
<tr>
<th>Midterm</th>
<th>Final</th>
</tr>
</thead>
<tbody>
<tr>
<td>Takes place 11AM to noon on Tuesday March 10</td>
<td>In the Final Week</td>
</tr>
<tr>
<td>– In SC0216 (our usual room)</td>
<td>– Time/Location to be announced</td>
</tr>
<tr>
<td>It will ask questions about the first 14 lectures.</td>
<td>It will ask questions about all lectures.</td>
</tr>
<tr>
<td>It will test</td>
<td>– 25% from first half</td>
</tr>
<tr>
<td>– Attentiveness and recollection</td>
<td>– 75% from second half</td>
</tr>
<tr>
<td>– Reasoning ability in subject matter</td>
<td></td>
</tr>
<tr>
<td></td>
<td>It will test</td>
</tr>
<tr>
<td></td>
<td>– Attentiveness and recollection</td>
</tr>
<tr>
<td></td>
<td>– Reasoning ability in subject matter</td>
</tr>
</tbody>
</table>
Exam Attendance

• Do not take this class if you are not sure you can attend the exams in person on campus at the times given.
## Write a Survey Paper

- Four-credit students are expected to complete a survey paper.
- Grade will come 75% from common assessment and 25% from the Extra Credit Assessment.

## Steps

- Choose your topic (related to security and privacy).
- Select at least 10 papers on the topic.
- Proposal due on March 26 at 11:59PM.
- Write an 8 page survey of the papers.
- Survey due on Sunday May 10 at 11:59PM.
Survey Paper Assessment

• Topic (10%): cohesive, not too broad or narrow, important and interesting
• References (15%): on-topic papers showing good coverage
• Discussion and organization of ideas from topic (40%)
• Critique and future challenges (10%)
• Writing (25%): correct English grammar and spelling, good organization
Topics from CS461/ECE422

- Mindset and ethics
- Basic cryptography
- Web and TLS
- Networking
- Control flow
- Malware, worms, botnets
- Passwords

- Forensics, physical security
- Policies & information flow
- Anonymity and dark web
What More is There to Know?

• Revise and extend past topics
• Much more to say in key areas
  – Privacy
  – Data science
  – Advertising
  – Domain-specific security
  – Theory
  – Smart phones and their app stores
  – And more
Tentative Course Syllabus

• Course website:
  https://gangw.cs.illinois.edu/class/cs463/
Reading: Tertiary Materials

• General textbooks:

• Surveys and specialized texts. Examples:
• References to scientific research papers (secondary materials) on slides and at the end of the slide set. Example:

• References to standards and source data (primary materials). Examples:
Most slides are derived from existing slide sets. Most of these are, in turn, derived from secondary, primary, and other tertiary materials.

Credits to the folks who created the slides from such sources or originated them appear in the notes for the slides.

Example:

– Based on slides by Nikita Borisov and Carl A. Gunter.
– Based on slides by Lawrie Brown.
• Inference in Location-Based Social Networks

• You are given:
  – Real anonymized datasets
  – Users may or may not share their home location

• Your task:
  – Infer private home locations using friendship information

• Due date: by 11:59PM on Feb 4.
MP1: Overview

• Code skeleton is provided

• Checkpoint 1:
  – Get familiar with Java
  – Read and parse the dataset

• Checkpoint 2:
  – Implement simple inference algorithm
  – Implement your own inference algorithm

• Report: one-page, two questions

• Ranking
MP1: Datasets

• Dataset 1:
  – Friendship information
  – Home locations for all users

• Dataset 2:
  – Same format as dataset 1
  – No ground truth
MP1: Visualization

- Visualization class ‘Visualizer.java’ is provided
MP1: Keep in mind

• Individual effort only
• Implementation in Java
• Submission:
  – Submission instructions to be announced
  – Platform:
    • Your code must compile and run on EWS
    • You can modify ‘compile.sh’ and ‘run.sh’
• Automated tests
User Study - Android

• Android performance study on popular Apps
• Prerequisite: Potential participants used or are current using Android phone (e.g. Nexus, Pixel, Samsung,...)
• You will use our phone in lab (5-10 mins).
• Interested?
  – Contact Jingyu Qian through: jingyuq2@illinois.edu
  – Come to OH next week for taking part in the experiment