463.0 Course Plan

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

- CS461/ECE422 Computer Security I
- CS460 Security Lab
- CS463/ECE424 Computer Security II
- CS563/ECE524 Advanced Computer Security
- Applied Cryptography
- CS598/598: Special Topics
- See https://iti.illinois.edu/education/course-roadmaps/security for links and updates
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](mailto:gangw@Illinois.edu))
  - Office hours: 12:15 PM T/R over zoom (after class) and by appointment
- TA: **Jaron Mink** ([jaronmm2@illinois.edu](mailto:jaronmm2@illinois.edu))
  - Office hours: Tuesday 1:30 - 3:30 over zoom and by appointment
- Course website: [https://gangw.cs.illinois.edu/class/cs463/](https://gangw.cs.illinois.edu/class/cs463/)
  - Piazza
  - MP Release
  - Slides
  - Syllabus
  - Grading Policies
Class Format

• About 50-60 minutes of lecture/presentation
• About 15-25 minutes of Q&A discussion
• Follow-up online Quiz released at the end of each class
  – Expected to be completed by the end of the week of each class
  – Sign up to access here: https://learn.illinois.edu/course/view.php?id=57949
  – Contact TA if you have trouble signing up
  – Not-graded, you get points by simply trying
## 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
- 75% of the grade for 4 credit students
Participation

• For most students who can attend the live lectures
  – Attend all the lectures
  – Finish the quiz after each class
    o 85% of quizzes $\rightarrow$ full quiz score (in case you occasionally forgot to do it)
  – Ask questions/answer questions directly (or in the chat window)

• For students who cannot attend live lectures
  – Finish the quiz after each class
  – Post questions/answer questions on Piazza
MPs

- Five assignments, starting this Thursday
- 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)
Exams

Midterm
• March 11, 2021 (Thursday of week-7)
• Specific details will be posted to Piazza soon
• It will ask questions about the lectures from week-1 to week-6
• It will test attentiveness, recollection, and reasoning ability in subject matter

Final
• Final week: time to be announced
• Specific details will be posted to Piazza soon
• It will ask questions about all lectures.
  — 25% from first half
  — 75% from second half
• It will test attentiveness, recollection, and reasoning ability in subject matter
Students Getting 4 Credits

• Write a Survey Paper
  – 4-credit students are expected to complete a survey paper.
  – Grade will come 75% from common assessment and 25% from the Extra Credit Assessment

• Choose your topic (related to security and privacy).
• Select at least 10 papers on the topic.
• Proposal due on April 1 at 11:59 PM CT
• Write an 8-page survey of the selected papers.
• Survey due on Sunday May 6 at 11:59 PM CT
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 related security and privacy

✓ Privacy
✓ Machine learning security
✓ Advertising
✓ Crypto
✓ Smart phones and apps
✓ Bitcoin
✓ Healthcare
✓ Automobile security
✓ Cybercrime
✓ Code stylometry
✓ Misinformation
✓ And More
Tentative Course Syllabus

• Course website: [https://gangw.cs.illinois.edu/class/cs463/](https://gangw.cs.illinois.edu/class/cs463/)
  – Lectures are based on research papers (some classics, some new)
  – Will finalize the schedule after confirming with a few invited speakers

• Different from “typical” undergraduate courses
  – No required textbook; we mostly read papers
  – Learn to think like a researcher
  – MPs are related to lectures; but they are not necessarily designed to practice what you already know
  – MPs are more of opportunities to **learn something new**
Reading: Tertiary Materials

• General textbooks:

• Surveys and specialized texts. Examples:
Reading: Secondary and Primary Materials

• 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:
Reading: Slides

• 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
To be released on Thursday (TA will give a quick intro)

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 11:59 PM on Feb 11