COMP7120/8120 Cryptography and Data Security

Course Overview
Instructor

- Zhuo Lu,
  - Assistant Professor of Computer Science
  - [http://csa.memphis.edu/~zhuo/](http://csa.memphis.edu/~zhuo/)
  - Email: zhuo.lu@memphis.edu

- Office: Dunn Hall 307

- Office Hours:
  - MW: 9:30-11:00am
  - Or appointment by email
About me?

- Research areas: network and wireless security, mobile computing, and information forensics.
- Related security projects:
  - Wireless security, anti-jamming
  - Secure protocol design for smart grid systems
  - Network inference and anti-inference
  - Trust in network systems

About you?
Why This Course?

- What’s the big picture of crypto and security.
- How to do encryption?
- How to store data secretly?
- How to design a secure protocol?
- How to make sure the person you talk to is really the person you want to talk to?
- …
Example I:

- How to encrypt the message

Hello! Welcome to the class!

- to

1010000101010100111100010110
1110111110000110100010010101
01011110101001010100001101
Example II:

- Can you be sure of the authenticity of this message?

Launch the nuclear missile!
- The President
Example III:

- How to save the password in a file system?

MyPass123
Example IV

- Alice sends a file to Bob via Eve, can Bob be sure the file is NOT changed by Eve?
Prerequisite

• Basic understanding on how to use computers and basic programming skills.
  - How to program
  - Some algorithm knowledge.

• Basic math skills:
  - Basic discrete math
  - Modulo operation
  - Prime numbers
Course Textbook

• Recommended but **NOT** mandatory:
Teaching Assistant

- Saikat Das
  - PhD Graduate Student
  - Department of Computer Science,
  - Contact and office hour are in the course website.
Course Website

- [http://csa.memphis.edu/~zhuo/classes/7120-8120/](http://csa.memphis.edu/~zhuo/classes/7120-8120/)

- Basic info
  - Syllabus
  - Whole semester schedule (tentative)
  - Class slides
  - Homeworks and solutions
Course Schedule

• The first-half semester:
  - Fundamental knowledge of crypto and security, understand the basic primitives.

• The second-half semester:
  - Research paper presentations: understand the state-of-the-art security systems or techniques based upon crypto and security primitives.
This course can

- improve your knowledge on cryptography
- improve your understanding of security design and applications
- will make you feel more comfortable with designing a secure computer or network system
- Help you start your own security research
Grading

- Total: 100
  - A: 85-100
  - B: 70-84
  - ...

- Attendance: 10%
- Homework: 20%
- Midterm: 25%
- Paper Presentation: 20%
- Final Project: 25%
- Extra Credit: 5%
Attendance Policy

- Students should regularly attend the class.
  - Up to 5 random sign-ups during the semester.
  - One absence is excused.

- Total grading: 10%
  - No or one absence: 10%
  - Two absences: 8%
  - Three: 6%
  - Four or more: 0%
Homework Assignments (20%)

• 2 - 3 assignments in total
  - All work is done individually unless otherwise specified
  - Late homework: 15% penalty each day. Not accepted after THREE days unless there is a documented emergency.

• Homeworks are important!
Midterm (25%)

- There will be one in-class midterm exam
  - work on your own, closed everything (neighbor, laptop, phone, ...)
  - You are allowed to bring a letter-sized (8.5 * 11 inches) cheat sheet.
Presentations (20%)

- Students will in turn present research papers after the midterm.
  - Two or three presentations each class, depending on the final presentation assignment.

- List of research papers will be published on the course website.
Presentation Assignment

• Students may let the instructor know their preference, interests, research/thesis directions.
  - e.g, I want to talk about cryptographic protocol design.

• The instructor will make the final presentation assignment at his discretion.
Research papers

• Topics:
  - Database security
  - Operating system security
  - Software security
  - Wireless and mobile security
  - Internet and network security
  - Embedded and control system security
  - ...

Final Project (25%)

- All students must form a team of 1 - 3 to complete a final project.
  - There will be no extra credit for a student working individually on the final project.
  - Get familiar with your classmates to form teams.

- The project details will be announced around the midterm.
Final Project

• Assigned project
  - I will list a potential project for you to do
  - Most students chose this one in the past.

• You own proposal
  - You can also propose your own idea to improve the security of a system.

• A survey on existing studies
  - You can write a comprehensive survey on a security topic.
Extra Credit (5%)

- There will be no extra credit in homework assignments and the midterm.

- There will be up to 5% extra credit in the final projects.
  - Encourage you to explore more in a challenging project.
  - May need substantial efforts to complete.
How to get extra credit

• Assigned project
  - Beyond the basic project requirements, well finish extra credit tasks.

• You own proposal
  - Good idea, prototype implementation, ready to summarize your project into a research paper.

• A survey on existing studies
  - Well-polished/organized, comprehensive, and ready to submit to a journal.
Project Deliverables

• Assigned project and your proposal:
  - Project report (at least 5 pages)
  - Source code

• Survey:
  - A survey paper (at least 15 pages).
    • Write using your OWN words!
    • DON’T copy sentences from papers,
    • Anti-plagiarism tool will scan your survey!!

• If we have time:
  - System demo and survey presentation in class
Type Your Homework/Report

• Homework solutions and project report must be written using word processing software.
  - e.g., Word, Open Office, or LaTeX.

• Submit a well-formatted PDF file.
Plagiarism/Cheating

• All homeworks and midterms submitted by a student is expected to be a student's own work.

• For group projects, a team should work on the project on their own.

• Plagiarism or cheating will lead to a failing grade!
Questions?

• Regarding
  - Course Info?
  - Grading?
  - Project?
  - Midterm?
  - Assignment?