Software Security
COSC 466/566
Spring 2023

Dr. Doowon Kim

THE UNIVERSITY OF
TENNESSEE

Announcement

- Jan 23 and 25 (Monday and Weds)
  - Online class over Zoom
  - Due to my personal issue
- Jan 27 (Friday)
  - No class
  - Due to my persons issue
- Jan 31
  - Will be back to normal
  - We will see in person in the classroom.

Today’s class

- Introducing me
- Introducing you (maybe in the in-person class next week)
- Course policies and syllabus

Who am I

- Doowon Kim (doowon@utk.edu)
- Assistant Professor, EECS
- Ph.D. University of Maryland, College Park in 2020
- M.S. University of Utah (Salt Lake City) in 2013
- Actively looking for students who are interested in security
  - Primary research areas:
    - Computer security (measurements, data-driven, usable)
    - Computer networks
    - AI/ML for security/adversarial ML

How and where to find each other

- Email: doowon@utk.edu
- Office: Min Kao 345
- Office Hours: TBD
- Discord:
  - https://discord.gg/y95Ga8FczS

Who are you? (Trying to remember your name)

- Preferred name
- Clas
- Aca
- Bac
- Wha
- Wha
- Why do you choose this course?

Let’s do this next week when we have in the in-person class.

Course Logistics

Course goals

- Describe the role security plays in software design
- Demonstrate the ability to reverse engineer software binaries, extracting secrets and exploiting bugs
  - From CTF challenges
- Identify common classes of software vulnerabilities
  - E.g., buffer overflow
- Demonstrate proficiency with ethical hacking

Class time

- Lectures
  - Cover the material related to software security
  - Designed to leave time for student questions
- In-class practice
  - Solve real-world ethical hacking challenges
  - Work together as a class

Course Disclaimer

- My promise to you: IF anything on the schedule changes, especially assignments, due to whatever circumstances, you will NOT be harmed if it was outside your control (i.e., things will work in your favor w.r.t. grades)
  - Examples: COVID-19 impacts, change to exam schedule or assignments, etc.

Course details

- COSC 466/566 Software Security
  - Instructor: Doowon Kim
  - Course credit hours: 3.0
  - Meeting time: MWF 01:50PM -- 02:40PM
  - Place: MKB-524
    - This week, we will have online classes (Jan 23 and 25)
    - Jan 27: no class
  - Prerequisite(s): COSC 366
  - Office Hours: TBD
- Prereq.:
  - Security class: COSC366 (Intro to Cybersecurity)

Course details

- COSC 466/566 Software Security
  - No material difference between 466/566.
  - But undergraduates (COSC 466) who complete all the requirements for 566 will be eligible for a letter grade bonus.
    - A- → A
    - B+ → A-
    - B → B+
    - B- → B
    - Etc.

Course Resources

- Canvas
  - Grades
- Discord: https://discord.gg/y95Ga8FczS
  - Course communication
- Textbook: Not required

Your grade

- CTF: 40% (Two roles)
  - Every week, you will be given a CTF task.
  - Also, make a CTF challenge yourself and make other students solve yours.
    - Bonus point if other people cannot solve your challenge for a couple of weeks.
- Midterm Exam: 20%
- Final Exam: 30%
- Class participation: 10%

CTF

- Capture the Flag (CTF) in computer security is an exercise in which "flags" are secretly hidden in purposefully-vulnerable programs or websites.
- You will be given a task every week or two weeks.
- Every Friday or every two weeks Friday
  - Students who solve the CTF challenge will share the solution with classmates → The students will get bonus points for class participations.
- No late submission
- Demo:

Exams

- In-class exams, but you need to bring your laptop.
- You will be given a couple of CTF challenges, and you need to find the flags.
  - The CTF challenges in the exams will be the same as (or very similar) you will solve in the class.
  - As long as you attend the class and know how to the CTF challenges given as assignment, you can also solve the CTF exams.
- Some multiple and open-ended questions.
- No makeup exams given.
  - Please come to the classroom and take the exams.

Class participation (10%)

- Share security-related news articles in discord
- Share with your classmate how to solve CTF challenges in class
  - Every Friday or every two weeks Fri. depending on the schedule.

Letter Grade Distribution

- Grading
  - >= 93.00 A
  - 90.00 - 92.99 A-
  - 87.00 - 89.99 B+
  - 83.00 - 86.99 B
  - 80.00 - 82.99 B-
  - 77.00 - 79.99 C+
  - 73.00 - 76.99 C
  - 70.00 - 72.99 C-
  - <= 69.99 F
- We will curve the grades (by lowering the thresholds), depending on the circumstances.

Class participation (10%)

- Contribute to in-class discussions, activities
- Contribute to class discussion
  - Share interesting privacy/security news
  - Answer questions for other students
  - Ask questions and spark discussion

Code of Ethics

- You commit to
  - Ethically study computer security for educational purposes
  - Refrain from using the knowledge gained to knowingly probe and attack computer security systems, unless having first received written permission from the owners or operators of those systems
  - Carefully consider ethical issues as your knowledge of computer security increases
  - Strive to formulate a personal code of ethics of the highest integrity

Code of Ethics

- Unethical practices include
  - Cracking passwords to gain unauthorized access
  - Deliberately spreading viruses or Trojan horses
  - Conducting a denial-of-service attack
  - Attempting buffer overflow attacks
  - Impersonating another person on a computer system you do not own

Code of Ethics

- Failure to comply could result in
  - Suspension of computer privileges in the EECS department
  - Expulsion from UTK
  - Possible criminal prosecution

Code of Ethics

- No cheating (and plagiarism) allowed
  - You will be Immediately reported to the school
  - The school will make a decision for you.

Security Mindset

Security Mindset

- Security requires a particular mindset
  - i.e., Security Mindset
- Involves thinking about how things can be made to fail
  - E.g., attacker or criminal

Security Mindset (example)

- An automobile dealership.
- She was able to retrieve her car after service just by giving the attendant her last name.
- Now any normal car owner would be happy about how easy it was to get her car back,
- but someone with a security mindset immediately thinks: "Can I really get a car just by knowing the last name of someone whose car is being serviced?"

Any other security mindset?