E0-256
Computer Systems Security

Vinod Ganapathy
August 2024 term

Course Info

Please send a request to join the MS Teams group. Everything you need for the course will be posted there.

Course logistics

- Time: Tuesday, Thursday 8:30am-10am
- Location: CSA-112
- TAs:
  - Dev Tejas Gandhi
  - Dhruvin Meghjibhai Chaudhari

Syllabus

- Goal of the course:
  - To get you up-to-speed on the state-of-the-art in computer security
- The field is very dynamic: attacks and defences continuously evolve.
- Most textbooks do not offer a thorough treatment
- So we will mostly read research papers

Syllabus

- Computer security is a **VERY** broad area.
- Impossible to cover breadth in a single course:
  - We will focus on **some** system security issues
  - Memory-errors and sandboxes, Web, Cloud, IoT and other emerging areas
  - Even for these topics, we'll only see the tip of the iceberg. The realities are vast and deep. Goal is to give you a taste of what's there and encourage you to start looking.
  - Not even touching **cryptography** or **privacy** (see other courses in the department)

Reading research papers

- Not written in your usual textbook style
- Each paper written in a slightly different style
  - Can take 3-4 hours to read a paper when you’re starting off to truly understand and appreciate the ideas that it presents.
- One of the goals of the course is to teach you how to read research papers
  - Getting to the core ideas of the paper
  - Adding these core ideas to your “toolbox”

Reading research papers

- Try to read the paper before coming to class.
    - You may not understand everything, and that’s okay. Just get a general feel for the topic that the paper covers.
- In class, we will discuss the context, background and technical details of the paper.
- Go home, and study the paper with your new-found understanding.

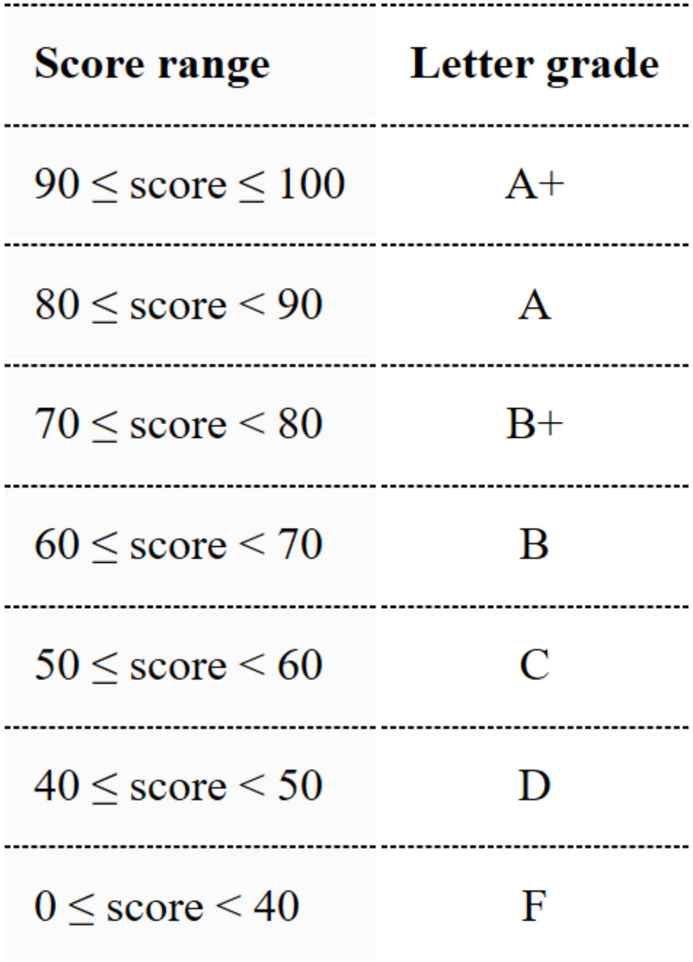
Reading research papers

- Most papers that we will read are seminal research results
- Google the names of the authors
  - These are the big-players in computer systems security.
  - Learn about their research by perusing through other papers they have written
  - A good way to come up with project ideas

Other course-related stuff

- Weekly workload and what is expected.
- Evaluation components:
  - One/two homeworks: Not graded, but …
  - Mid-term and Final, Quizzes (75%)
  - Multi-part system building project (25%)
- Quiz can be held in any class, unannounced
- Grading criteria
- Project details

Grading



Score range	Letter grade
$90 \leq \text{score} \leq 100$	A+
$80 \leq \text{score} < 90$	A
$70 \leq \text{score} < 80$	B+
$60 \leq \text{score} < 70$	B
$50 \leq \text{score} < 60$	C
$40 \leq \text{score} < 50$	D
$0 \leq \text{score} < 40$	F

What this means

If all of you do well, you all get A+ grades. The converse holds too :-)

WYSIWYG:

- No room for uncertainty due to “curving” issues.
- No back-and-forth discussions at end of semester about the grade you got
- Grades are non-negotiable

Exams

- Will test deep understanding of material rather than mere knowledge of material

- We have a strict, no-nonsense policy against cheating. See the class webpage for details.

Project details

- See the class webpage for last year’s project, which involved:
  - Building a binary (x86) analyzer
  - Building an in-kernel (Linux-based) system call sandbox
- The project for this year will be similar in effort and will be announced in about 2 weeks’ time.

Project details: “Yes” answers

- Yes, there is going to be quite some coding
- Yes, you’re going to have to pace it out
- Yes, you’re going to ask for extensions to the submission deadline.

Project details: “No” answers

- No, there will be no extensions to the final deliverable deadline
- No, copying code from others or your seniors is absolutely not acceptable.

Attending class

You are encouraged to attend every class. But you're all grown ups -- So no attendance policy will be enforced.

BUT,

- In each class, I will often cover material that is not in the papers, not in the slides, and not in any textbook. The exams may contain questions based on this material.
- There may be unannounced quizzes in class and no compensatory quizzes will be offered if you miss class

Come to class on time

- Class starts at 8:30am, not 8:40am
  - Unless otherwise noted, e.g., if there is an interesting department seminar (which I may ask you to attend as well).
- Walking into class 10-15 minutes late is **unacceptable**
- If you miss a quiz or a portion of the quiz because you come in late, no compensatory quiz or extra time will be provided.

Contacting us

++ Attend and ask questions in class

++ Be curious. Seek out and read research papers on your own. I’m happy to provide pointers and you can contact me or my students (in the CSSL lab) for references to papers in topics that you’re interested in pursuing further.