CprE 5310 Information System Security

Department of Electrical and Computer Engineering
Fall 2024 All Sections

Instructor: Thomas Daniels, Department of Electrical and Computer Engineering
2214 Coover Hall, Iowa State University, Ames, Iowa 50011
Phone: 515–294–8375
daniels@iastate.edu
TA: See Canvas

Office Hours: For Dr Daniels and TA will be posted on Canvas

Textbook:

No Textbook.. Selected readings will be assigned on a weekly basis on blackboard. In some cases, students will be expected to find novel papers of interest to themselves on the topic at hand and turn in summaries.

Website: http://canvas.iastate.edu/

Objectives: Understand information security concepts, threats, vulnerabilities, and countermeasures from a computer and information security perspective.
Understand and apply risk assessment techniques to information systems and their use.
Be able to apply and analyze security techniques to enhance the security of computing systems.
Be able to analyze policy models to determine their access control implications.

Grading:

Your grades are based on 5-6 homeworks spread throughout the semester and small online exams administered every other week. There will also be a final exam which requires a proctor for distance students. 40% homeworks, 30% Regular Quizzes, 30% final exam.

The letter grades will be assigned based on the ranges below:

A	92-100,	B	80-91	C	70-79
D	60-69	F	0-59		

The range may be lowered to your benefit, but will not be increased. I do give plus and minus grades as well. These are spread across the ranges above evenly. Grade cutoffs may be lowered to your benefit.

Homework: Homeworks are due on the date stated when assigned. Homework received late will not be accepted unless an agreement is made prior to the due date.
Homework must be either typewritten or very neatly handwritten. I do not have time to decipher your homework, so make them clear. Illegible homework will not be graded.

Generative AI:

Generative AI is not allowed in any form for your assignments or exams unless explicitly allowed by writing in the assignment. Use of generative AI will result in a grade of F on the assignment and no greater than C grade for the course.

There are numerous University-wide syllabus statements that are included in these policies. Please see them in the "Syllabus Statements" section on Canvas.

Topic List:

1. Security Concepts
    a. Security Goals (CIA, etc.)
    b. Attacks vs Vulnerabilities
    c. Access control concepts
    d. Privacy
    e. Risk analysis
    f. Legal and Ethical Issues
2. Information theoretic Underpinnings
    a. Information Theory Basics
    b. Uncertainty (Entropy) and Importance
3. Basic Crytography
    a. Cryptographic Random Numbers
    b. Classical Ciphers and One Time Pads
    c. Block Ciphers
    d. Hashes
    e. Key Exchanges and Public Key Crypto
    f. Signatures and MACs
    g. TLS
4. Computer Hardware Security
    a. Rings in CPU
    b. Memory Protection via Virtual Memory
    c. CPU and Memory Flaws
    d. Side Channels
5. Operating System Security
    a. Trusted Systems
    b. User-lever vs Kernel Level
    c. System Call Interface
    d. Interactions between hardware and OS
6. Security Models
    a. BLP & Biba
    b. Clark Wilson
7. Development Security
    a. Saltzer and Schroeder
    b. Software Vulnerabilities
8. Authentication and Detection
    a. Password Systems
    b. Cryptographic
    c. Tokens
    d. Biometrics
    e. Detection
    f. Error rates and ROC Curves
9. Legal and Ethical Issues
    a. Review