ECE 696, Hardware-Based Security Engineering, Spring, 2019

- Instructor: Abu Asaduzzaman
- Department: Electrical Engineering and Computer Science (EECS)
- Office Location: 253 Jabara Hall (JB) building
- Telephone: +1-316-978-5261
- Email: Abu.Asaduzzaman@wichita.edu

- Preferred Method of Contact: In person during office hours or e-mail
- Student/Office Hours: Tuesday and Thursday 11:00AM—12:30PM
- Classroom, Day/Time: 214CH, TR 4:05—5:20PM
- Prerequisites: ECE 394 or instructor's consent
- Teaching Assistant (TA): TBD
- TA Contact: Email – <tbd@shockers.wichita.edu>

How to use this syllabus

This syllabus provides you with information specific to this course, and it also provides information about important university policies. This document should be viewed as a course overview; it is not a contract and is subject to change as the semester evolves. Any changes should be shared via lecture and/or Blackboard.

University Policies and Procedures

The Wichita State University Policies and Procedures Manual can be found at: https://www.wichita.edu/about/policy/.

Academic Integrity

Students at Wichita State University are expected to uphold high academic standards. WSU will not tolerate a lack of academic integrity. Students are responsible for knowing and following the Student Code of Conduct (see https://www.wichita.edu/about/policy/ch_08/ch8_05.php) and the Student Academic Honesty policy (see https://www.wichita.edu/about/policy/ch_02/ch2_17.php). When the faculty member determines sanctions are warranted for violations of academic integrity, regardless of severity, the faculty member must report the infraction to the Office of Student Conduct and Community Standards. If you need more information about the process or wish to appeal a decision, please visit https://www.wichita.edu/about/student_conduct/AcademicDishonesty.php.

All homework (HW) assignments in this course are individual assignments (unless otherwise stated). Students can discuss with others, but they should not write the solution together; one's submission (wording/coding) should be substantially different from others' submissions. "Collaboration is good, cheating is not!" There will be severe consequences for academic dishonesty. Cheating (such as copying word-for-word from other sources) in any test will automatically result in an F grade for the course; this applies to all the parties involved (including the ones who help/show).

Course Description

Intended for seniors and graduate students who want to study and explore the role of hardware in improving computer security and security engineering. Topics covered include elements of computer security, secure distributed systems, hardware as a cybersecurity solution, physical unclonable function and security engineering. Special attention is given to learner-centered team-based research activities.

Measurable Student Learning Outcomes

Measurable Student Learning Outcomes: Undergraduate Level

After passing this course, undergraduate students will be able to:

- Understand the fundamental concepts, challenges, and opportunities of hardware-based computer security.
- Design and develop simple to moderate security solutions for computer systems.

Measurable Student Learning Outcomes: Graduate Level

After passing this course, graduate students will be able to:

- Understand the importance and benefits of hardware-based computer security and engage in life-long learning of computer security for professional success.
- Design, develop, and assess various security solutions for tackling current and future security challenges.

Required Texts/Readings Textbook

Please talk to the instructor before buying books for this course.

HARDWARE-BASED COMPUTER SECURITY Techniques to Defeat Hackers from Biometrics to Quantum Cryptography, Roger R. Dube, Wiley, 2008.

COMPUTER SECURITY HANDBOOK by Bosworth, Kabay, and Whyne, Wiley, sixth edition, 2014.

Other Readings

Lecture slides, handouts, and related articles will be made available via Blackboard.

Class Protocol

There are points on classroom performance. It is expected that students arrive to the assigned room before class starts. Students are always encouraged to ask questions, especially if they find ambiguity in assignments and materials covered.

Contact Policy

Email communication is also preferred. Feel free to email me any questions or concerns following these guidelines:

- **Always** email me from your WSU email address. Email sent from personal email servers like Gmail, Yahoo, etc., have a tendency to end up in my spam folder, and I never see them. You may also email me through Blackboard via the Email My Instructor tab. I also offer a Discussion Forum on Blackboard which allows common questions to be seen and responded to publicly.
- Always use the course name in the subject line of the email.

Definition of a Credit Hour

Success in this 3 credit-hour course is based on the expectation that students will spend, for each unit of credit, a minimum of 45 hours over the length of the course (normally 3 hours per unit per week with 1 of the hours used for lecture) for instruction and preparation/studying or course related activities (such as tests and projects) for a total of 135 hours. [Here, one unit of credit means one credit-hour.]

Grading Scale

WSU uses a +/- grading scale for final grades and to calculate grade point averages. In this class, grades are assigned according to the following chart. (Other classes might assign grades differently: Be sure to understand the different grading scales in all of your classes.)

Points/Percentage	Letter Grade	Grade Points	Interpretation
93 and up	A	4.00	A range denotes excellent performance
90 – less than 93	A-	3.70	
87 – less than 90	B+	3.30	
83 – less than 87	B	3.00	B range denotes good performance
80 – less than 83	B-	2.70	

Points/Percentage	Letter Grade	Grade Points	Interpretation
77 – less than 80	C+	2.30	
73 – less than 76	C	2.00	C range denotes satisfactory performance
70 – less than 73	C-	1.70	
67 – less than 70	D+	1.30	
63 – less than 67	D	1.00	D range denotes unsatisfactory performance
60 – less than 63	D-	0.70	
0 – less than 60	F	0.00	

Assignments

List of grading assignments/components and values toward final grades are shown below. For exams and project, different grading scales will be used for undergraduate and graduate students. Graduate students will have additional activities in the project assignments that have higher weightage. The same grading scale will be used for all students on class performance, homework, and quiz. Homework assignments and their due dates will be announced in class and/or made available via Blackboard. Similarly, the due dates for Quiz, Exam, and Project will be announced in class and/or made available via Blackboard.

Grading Assignments/Components	Undergraduate	Graduate
Class Performance (random check)	3%	3%
Homework (seven of eight, take home)	14%	14%
Quiz (two of three, 30-minute, class-time)	10%	10%
Exam-1 (~ Week 5, 65-minute, class-time)	13%	12%
Exam-2 (~ Week 10, 65-minute, class-time)	15%	14%
Exam-3 (cumulative, 65-minute, class-time)	20%	17%
Project (Proposal, Presentation, and Report)	25% (1+12+12)	30% (2+14+14)

Extra Credit

Extra credits are possible as/if needed. Depending on class performance after Week 10, if required, extra credit assignments and their due dates will be determined.

Late Assignments

For homework assignments, late submissions will not be accepted after five days from the original due date/time. Up to 50% points may be subtracted for any late submission. Exceptions include documented emergency situations and prior consents.

Missed Tests

Makeup for missed tests (Quiz, Exam, and Project) will be given only when there is a genuine reason, with clear proof. It is students' responsibility to provide the proof; if the reason for missing a test is illness, a doctor's note will be required. Students should contact the instructor before any makeup test.

Teaching Assistants

Grading TA:

TBD <tbd@shockers.wichita.edu>

Office Hours/Room: TBD

The Grading TA is not allowed to solve problems. The TA should grade test papers and provide feedback to students for any missing points. If students have any questions regarding assignments, they should immediately contact the course instructor.

Syllabus Policies and Student Resources available at www.wichita.edu/syllabuspolicies

Information on:

- Important Academic Dates
- Academic Integrity
- Definition of a credit hour
- Video and Audio recording
- Shocker Alert System
- Intellectual Property
- CARE Team
- Counseling and Prevention Services
- Student Health Services
- Heskett Center and Campus Recreation
- Inclusive Excellence
- First Generation Students
- Names and Pronouns
- Disability Services

- Title IX
- Concealed Carry Policy

Laboratory Information

There is no assignment/activity in this course that may require laboratory facilities. However, you are welcome to use the Computer Architecture and Parallel Programming Laboratory (CAPPLab) facilities for the class project of this course. CAPPLab is physically located in room 256 Jabara Hall (you may visit online at http://www.cs.wichita.edu/~capplab/). CAPPLab is used for teaching/research in computer architecture, low-power high performance computing, embedded systems, parallel programming, and related fields.

Tentative Brief List of Topics to Cover

Introduction and Motivation

- Computer Systems: Past, Present, and Future
- Computer Security: Past, Present, and Future

The Elements of Computer Security

- Passwords and Keys; Cryptography; Random-Number Generation

The Qualities of Workable Security Solutions

- Secure Coprocessors; Secure Memory Management
- Hardware-Based Authentication

Security Engineering

- Introduction; Access Control; Cryptography; Distributed Systems
- Multilevel Security; Multilateral Security; Physical Protection
- Terror, Justice, and Freedom; Managing Secure Systems; System Evaluation

Research Interests

- Understanding Security Challenges; Developing Solutions for Computer Systems

Tentative Schedule for 15-week class

CS 697AN * Spring 2019 * WSU EECS Dept. * DRZ

Tentative Course Plan

Date ranges for each week of the semester	Remark	All of the topics, readings, assignments and reminders are located here so that you can organize your time and academic work. Please ask me any questions at any time regarding this course.
Week 1 (Eval-1) 1/22 , 1/24 Lectures 1, 2	— K-Probe	CS 697AN: Hardware-Based Computer Security; Course Syllabus; **Team Project;** Introduction to Hardware-Based Computer Security; **HW-1 (assign) on Thu;** HW Submission, Grading Policy; **K-Probe on Thu;**
Week 2 (1/29, 31) Lectures 3, 4	— HW-1	The Elements of Computer Security; HW-1 due on Thu; hardcopy, before beginning of the class;
Week 3 2/5, 2/7 Lectures 5, 6	— HW-2	**Team Project:** Groups (size TBD), Components, Grading, Topics; Passwords and Keys; Cryptography; Random-Number Generation; HW-2 due on Thu; hardcopy, before beginning of the class; Discussion on Quiz-1;
Week 4 (2/12, 14) Lectures 7, 8	HW-3, Quiz-1	The Qualities of Workable Security Solutions; **Team Project:** Groups, Topics; HW-3 on Thu; hardcopy before class; **Quiz-1 on Thu! (30 minutes; Closed book;);**
Week 5 (Eval-2) Lectures 9, 10	— Exam-1	Secure Coprocessors; Secure Memory Management; Discussion on Exam-1; **Exam-1 on Thu! (60 minutes; Closed book;);**
Week 6 (2/26, 28) Lectures 11, 12	—	**Team Project:** Grading; Components; Proposal (hardcopy) due next week! Secure Coprocessors; Secure Memory Management;
Week 7 (3/5, 3/7) Lectures 13, 14	Proposal HW-4	Qualities of Workable Security Solutions; Hardware-Based Authentication; HW-4 on Thu; hardcopy before class; **Project: Proposal (hardcopy) due on Thu!**
3/11 - 3/17		**Spring Break!**
Week 8 (3/19, 21) ***Mid-term point*** Lectures 15, 16	Mid Pt HW-5	Mid-Term Point Updates; PUF; **Team Project:** Presentation and Report; Discussion on Quiz-2; HW-5 due on Thu; hardcopy, before beginning of the class;
Week 9 (3/26, 28) Lectures 17, 18	HW-6, Quiz-2	Security Engineering: Access Control; Cryptography; HW-6 on Thu; hardcopy before class; **Quiz-2 on Thu! (30 minutes; Closed book;);**
Week 10 (4/2, 4/4) Lectures 19, 20	— Exam-2	Security Engineering: Distributed Systems; Discussion on Exam-2; **Exam-2 on Thu! (60 minutes; Closed book;);** **Update (April 5—Last day to officially withdraw from a course with a "W")**
Week 11 (4/9, 11) Lectures 21, 22	—	Security Engineering: Multilevel Security; Multilateral Security; Physical Protection;
Week 12 (4/16, 18) Lectures 23, 24	— HW-7	Sec. Eng.: Terror, Justice, and Freedom; **Team Project:** Presentation and Report; HW-7 due on Thu; hardcopy; Discussion on Quiz-3;
Week 13 (Eval-3?) Lectures 25, 26	HW-8, Quiz-3	Security Engineering: Managing Secure Systems; **Project:** Presentation and Report; HW-8 on Thu; hardcopy before class; **Quiz-3 on Thu! (30 minutes; Closed book;);**
Week 14 (Eval-4?) Lectures 27, 28	— Exam-3	Security Engineering: System Evaluation; Discussion on Exam-3; **Exam-3 on Thu! (60 minutes; Closed book;);**
Week 15 5/7, 5/9 Lectures 29, 30	**Project:** Present & Report	**Presentation:** Teamwork; PowerPoint Slides; Time TBD (for UG/GR); **Report:** Due on Study day (Friday); Hardcopy; Page count (see Grading Policy); **Template and Information:** Available on Blackboard;
Final Exams 5/11—5/16		**None!** Office Hours / Discussion

[_v0) Updated on Feb. 20, 2021; from spring 2019; DRZ]