WICHITA STATE UNIVERSITY

CS 697AN, Hardware-Based Computer Security, Spring, 2019

Instructor:	Abu Asaduzzaman
Department:	Electrical Engineering and Computer Science
Office Location:	253JB (Jabara Hall building)
Telephone:	+1-316-978-5261
E-mail:	Abu.Asaduzzaman@wichita.edu
Preferred Method of Contact:	In person during office hours or e-mail
Office Hours:	TR 11:00AM—12:30PM
Classroom, Days/Time:	214CH, TR 4:05—5:20PM
Prerequisites:	CS 394
Course Website:	http://webs.wichita.edu/aasaduzzaman/html/cs697an.html
Teaching Assistant (TA):	TBD (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.

General University Policies

Some general university policies pertaining to all syllabi can be found at:
https://webs.wichita.edu/?u=ofdss&p=/students/syllabusinformation/

Academic Honesty

Students are responsible for knowing and following the Student Code of Conduct, can be found at http://webs.wichita.edu/inaudit/ch8_05.htm and the Student Academic Honesty policy, can be found at http://webs.wichita.edu/inaudit/ch2_17.htm.

All homework assignments in this course are individual assignments. You can discuss them with others, but you cannot write the solution together; your submission (wording/coding) should be substantially different from others'. "Collaboration is good, cheating is not!" There will be severe consequences for academic dishonesty. This includes copying homework assignments and cheating during tests (including quizzes and exams). Cheating 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). Be aware that I do NOT have to catch you (or even notice) cheating during the test; I could catch you later, based on any unusual similarities in your answers.

Course Description

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

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 project) for a total of 135 hours.

Measurable Student Learning Outcomes: Undergraduate Level

After passing this course, students will be able to:
1) Understand the fundamental concepts, challenges, and opportunities of hardware-based computer security.
2) Design and develop simple to moderate security solutions for computer systems.

Measurable Student Learning Outcomes: Graduate Level

After passing this course, students will be able to:
1) Understand the importance and benefits of hardware-based computer security and engage in life-long learning of computer security for professional success.
2) Design, develop, and assess various security solutions for tackling current and future security challenges.

Required Texts / Required 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.*

Topics Include

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

Grading Policy/Scale

The final/letter grade will be based on the grading components listed below. For exam and project, different grading scales will be used for undergraduate and graduate students. For classroom performance, homework, and quiz, the same grading scale will be used for all students.

Grading Components	Undergraduate	Graduate
Classroom Performance (random check):	3%	3%
Homework (seven of eight, take-home):	14%	14%
Quiz (two of three, 30-minute in classroom):	10%	10%
Exam-1 (~ Week 5):	13%	12%
Exam-2 (~ Week 10):	15%	14%
Exam-3 (cumulative, before semester ends):	20%	17%
Project (Proposal, Presentation, and Report):	25% (1+12+12)	30% (2+14+14)

Your letter/final grade will be approximately based on the following:

A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F
93	90	87	83	80	77	73	70	67	63	60	0

Assignments

Homework assignments and their due dates will be announced in class. Late submissions will not be accepted after five days from the original due date/time. Exceptions include documented emergency situations and prior consents.

Important Academic Dates

For spring 2019 semester, classes begin Jan 22, 2019, and end May 9, 2019. The last date to drop a class and receive a W (withdrawn) instead of F (failed) is Apr 5, 2019. The final exams period is May 11-16, 2019.

Tentative Schedule

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

Disabilities
If you have a physical, psychiatric/emotional, or learning disability that may impact on your ability to carry out assigned course work, I encourage you to contact the Office of Disability Services (DS).

Counseling and Testing
The WSU Counseling and Testing Center provides professional counseling services to students, faculty and staff; administers tests and offers test preparation workshops; and presents programs on topics promoting personal and professional growth.

Diversity and Inclusive
Wichita State is committed to being an inclusive campus that reflects the evolving diversity of society. To further this goal, WSU does not discriminate in its programs and activities on the basis of race, religion, color, national origin, gender, age, sexual orientation, gender identity, gender expression, marital status, political affiliation, status as a veteran, genetic information or disability. The Executive Director of WSU Office of Equal Opportunity has been designated to handle inquiries regarding nondiscrimination policies.

Intellectual Property
Wichita State University students are subject to Board of Regents and University policies (see http://webs.wichita.edu/inaudit/ch9_10.htm) regarding intellectual property rights. Any questions regarding these rights and any disputes that arise under these policies will be resolved by the President of the University, or the President's designee, and such decision will constitute the final decision.

Shocker Alert System
Get the emergency information you need instantly and effortlessly! With the Shocker Alert System, we will contact you by email the moment there is an emergency or weather alert that affects the campus. Sign up at www.wichita.edu/alert.

Title IX
Title IX of the Educational Amendments of 1972 prohibits discrimination based on sex in any educational institution that receives federal funding. Wichita State University does not tolerate sex discrimination of any kind including: sexual misconduct; sexual harassment; relationship/sexual violence and stalking. These incidents may limit an individual's ability to benefit from the University's educational activities. Students are asked to immediately report incidents to the University Police Department or the Title IX Coordinator. For more information about Title IX, go to: http://www.wichita.edu/thisis/home/?u=titleixf

Video and Audio Recording
Video and audio recording of lectures and review sessions without the consent of the instructor is prohibited. Unless explicit permission is obtained from the instructor, recordings of lectures may not be modified and must not be transferred or transmitted to any other person, whether or not that individual is enrolled in the course.

Student Health Services
WSU's Student Health clinic is located in Ahlberg Hall. The telephone number is (316) 978-3620. For more information see www.wichita.edu/studenthealth.

Concealed Carry Policy
The Kansas Legislature has legalized concealed carry on public university campuses. Guns must be out of view, concealed either on the body of the carrier, or backpack, purse or bag that remains under the immediate control of the carrier. Gun owners must familiarize themselves with WSU's Concealed Carry Policy at http://webs.wichita.edu/?u=wsunews&p=/weapons_policy_documents and the Kansas Board of Regent's policy at http://www.kansasregents.org/about/policies-by-laws-missions/board_policy_manual_2/chapter_ii_governance_state_universities_2/chapter_ii_full_text#weapons. If you believe that there has been a violation of this policy, please contact the University Police Department at 316 978-3450.

Blackboard/Online
Selected instructional materials (such as lecture notes, reading materials, homework assignments, solution keys, and project related information) and important announcements for this course will be made available via Wichita State University (WSU) Blackboard (URL: http://blackboard.wichita.edu).

Missed Exams
Makeup for missed tests will be given only when there is a genuine reason, with clear proof. It is your responsibility to provide the proof; if the reason for missing a test is illness, a doctor's note will be required. It is YOUR RESPONSIBILITY to contact me BEFORE the makeup test.

Important Notes
- **Homework Submission:** No e-mail submission. (Repeat) No e-mail submission. Everyone must turn in his/her own assignment, unless special permission is given.
- **Late Submission:** No late submission for assignments after five days from the actual due date/time. Up to 50% points should be subtracted for any late submission.
- **Project Report:** One printed report should be submitted by each group. (In addition, I may ask for an editable softcopy of the report.) NO late submission for project report.
- **Communication via E-mail:** You must use your WSU e-mail account for e-mail communication.
- **Professionalism** (e.g., proper manners) is highly expected.
- All **academic dishonesty** cases will be handled following the University Code of Academic Conduct. You may check the University Catalog for further information.

Prerequisite Information
CS 394 (Introduction to Computer Architecture) is the pre-requisite for this course. The principle concepts, components, and operations of a structured computer organization are studied in CS 394. By continued enrollment in this class, you are certifying that you have met the pre-requisite requirements for this course.

Additional Information
In addition to the topics mentioned in Topics Include, the following topics may also be covered: Secure Bootstrap Loading; Biometrics for Security; Location's Place in Security; Electronic and Information Warfare; Telecom System Security; and Network Attacks and Defense.

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.

Graduate Teaching Assistant (GTA)
GTA Name: TBD
Contact: E-mail tbd@shockers.wichita.edu
Office Room / Hours: 256JB / TBD

It is important to understand that the GTA should grade your homework/programming assignments and quiz papers. The GTA is not allowed to solve your problems (any problem). If you have questions regarding the course materials and/or assignments, you should immediately contact the course instructor.