CSE 4380/5380: Information Security
Fall 2014

Note: This is not the syllabus! The full one is posted on Piazza and at: https://www.uta.edu/profiles/matthew-wright

Details

Instructor:	Matthew Wright	GTAs:	Taiabul Haque, Mehrab Shahriar, Mohsen Imani
email:	mwright@cse.uta.edu	email:	<eresh03, mehrab012, imani.moh>@gmail.com
Office:	ERB 528	Office location:	ERB 106 (the lab)
Phone:	(817) 272-0906	Office phone:	(817) 272-7526
Office hours:	M/W 1:00-2:00 PM	Office hours:	M/W 5:30-6:30 (non-lab weeks)
Faculty Profile:	https://www.uta.edu/profiles/matthew-wright		
Piazza:	https://piazza.com/uta/fall2014/cse43805380/home		

Course Objectives

- Use cryptographic primitives directly in order to understand their respective uses and how they work together to provide security.
- Develop simple malware in order to understand hooking and how hooking can be subverted for malicious purposes.
- Set up and use defensive technologies in the network and operating system in order to see how they defend against attacks.
- Identify and exploit software vulnerabilities in order to understand how they work and how defenses could stop them.
- Study a range of concepts to gain a broad understanding of the field of information security.

Required Textbooks and Other Course Materials:

Computer Security: Principles and Practice by William Stallings and Lawrie Brown (2nd edition).
ISBN-13: 978-0132775069 ISBN-10: 0132775069
The first and third editions are also acceptable.

Grading: Course grades will be based on the following: Example

Lab Exercises (5 in-lab with 5 pre-lab exercises):	38%
Labs 1-3, 5 worth 7%, Lab 4 is worth 10%	
CTF Lab:	12%
Exams (2 in-class):	40%
Exam Study Prep (2 written + in-class activity)	4%
Quiz:	3%
Presentation:	2%
Online assignment (1):	1%

Grades for Exams will be curved by the instructor and scaled to a standard A = 90-100, B = 80-89, C = 70-79 scale. For example, if the instructor sets the A/B line at 85, then a student who scores 85 will get a scaled score of 90. All other graded elements will not be curved and graded directly on the standard scale. Final grades will simply be the weighted average of the scores, based on the percentages shown above. Small amounts of extra credit may be available, but only on a class-wide basis (no individual requests will be granted). No grade bumps will be offered; 89.99 is a B in this class.

Formula: 90 + (X – A/B Line)*Scale, where Scale = 10/(100-A/B Line)

- A/B Line: _____, Scale = 10/_____ = _____ Scores: ___ => _____ = _____ ___ => _____
- A/B Line: _____, Scale = 10/_____ = _____ Scores: ___ => _____ = _____ ___ => _____

Make-ups: Make-ups for graded activities may be arranged if your absence is caused by illness or personal emergency. A written explanation (including supporting documentation) must be submitted to your instructor; if the explanation is acceptable, an alternative to the graded activity will be arranged. *Make-up arrangements must be arranged prior to the scheduled due date.*

Lab Attendance and Completion: Attendance to your assigned lab section during lab weeks is mandatory. You are expected to come to lab having completed a pre-lab assignment that will be checked by the GTA before you may begin the lab. The lab hours are fixed. We will allow you to complete an unfinished lab by attending GTA office hours in the following week (max. 1 hour), but at the cost of 10 points (out of 100) deducted from your grade for that lab.

Attendance: I do not check nor grade attendance. I will not simply be lecturing to a passive audience, however. In every class period, you will learn by actively participating in the process of solving problems and working in small groups. Missing class, therefore, means missing out on learning opportunities that cannot be gained from the textbook.

Why?

Teams: You will be assigned to a team and submit all pre-labs as a team. There will be exam bonuses for team success.

Why?

Descriptions of major assignments and examinations:

- Lab Assignments: In the labs, you will work in pairs to learn how attacks operate and how to defend against them. Each lab exercise includes a pre-lab assignment due the Sunday before the corresponding lab week. Late assignments are not accepted, but the pre-lab must be done before you can start the lab.
- CTF Lab: A capture-the-flag game of defense and attack against other lab sections, submit a report on your work, give a presentation on your findings during the course Final. Pre-CTF is due before CTF Part 2.
- Quiz: Covers security administration topics. In-class.
- Online Assignment: short assignment to get you setup for the class.
- Security News Presentation (dates will be arranged for each student): Students will give a brief presentation in class on an issue appearing in the news related to class.
- Exam 1, in-class, Mon., Oct. 6: Covers Cryptography and System Security
- Exam 2, in-class, Mon., Nov. 24: Comprehensive; focus on Malware, Software Sec., Network Sec., Web Sec.
- Exam Study Prep: You will be responsible for a section of the class material to help your team study for the exam.

Schedule (Subject to Change):

Week	Class Dates	Topic	Activity	Due Dates
1.	Aug. 25/27	Class Intro + Principles	Online Assignment	_____
2.	Sep. 1/3	LABOR DAY + Crypto Overview	None	
3.	Sep. 8/10	Public Keys + Crypto Protocols	Pre-Lab 1	_____
4.	Sep. 15/17	User Authentication	Lab 1	
5.	Sep. 22/24	Access Control	Pre-Lab 2	_____
6.	Sep. 29/Oct. 1	Host IDS + Exam Review	Lab 2, Exam Study Prep	
7.	Oct. 6/8	EXAM 1 + Intro to Malware	Exam 1	
8.	Oct. 13/15	Detection/Stealth + Botnets	Pre-Lab 3	_____
9.	Oct. 20/22	Buffer Overflows	Lab 3 and Pre-Lab 4	_____
10.	Oct. 27/29	Buffer Overflows 2	Lab 4	
11.	Nov. 3/5	Network Basics/Firewalls + NIDS	Lab 4 and Pre-Lab 5	_____
12.	Nov. 10/12	NIDS 2 + Firewall/NIDS Configuration	Lab 5 and Pre-CTF	_____
13.	Nov. 17/19	CTF/Web Sec. + Web Sec./Exam Review	CTF Part 1, Exam Study Prep	
14.	Nov. 24/26	EXAM 2 and Security Administration	Exam 2	
15.	Dec. 1/3	Guest Lecture + Quiz/Privacy/Anonymity	CTF Part 2 and Quiz	
16.	Dec. 10	CTF Presentations	CTF Presentations	12/10, 2:00-4:30

Note: The instructor reserves the right to adjust this schedule in any way that serves the educational needs of the students enrolled in this course.

We will use Piazza for all course communications, including links to readings, assignments, course news, etc. All students are responsible for checking the server regularly for news and assignments. Your MavMail accounts will be set as the default email for interacting with Piazza.

Students will be given accounts for the ASCENT security-teaching lab. All students are expected to be responsible users of the computer systems used for this course. In particular, students are expected to abide by the code of ethics associated with this course.

Emergency Exit Procedures: The nearest exit: from the back doors, either left or right is fine, from the front door, left is slightly better.