CS482: Cyber Security Engineering Syllabus

Instructors

MAJ Ben Klimkowski
B and E Hour, TH452
C Hour, TH464
Thayer 1111
(845) 938-4927
benjamin.klimkowski@usma.edu

CPT Michael Kranch
G Hour, TH464
(845) 938-5560
Michael.Kranch@usma.edu

Time and Location

You will normally meet in Thayer 452/464. Events that are outside the classroom or normal hour will be announced in advance.
TH452 After Hours Combo: 2-53-14
TH464 After Hours Combo: 3-5-1-2

Course Objectives

- Be able to conduct individual research and self-study to learn complex technical topics!
- Be able to explain the principles of information-system security, along with various security models and best practices.
- Be able to apply techniques and tools to improve and evaluate information-system security.
- Be able to devise and create defensible systems and networks.
- Be able to identify offensive methods and analyze the threats they present to information systems.
- Be able to consider the legal, ethical, and moral issues associated with information-system security.

Textbook

Stallings, W. and Brown, L. 2015. Computer Security, Principles and Practice 3rd. Ed., Boston (MA): Pearson Education, Inc.

Classroom Standards

- Please keep your classroom clean.
- Please log into your computer and open VMs/log into vSphere upon arriving for class.
- Please be prepared to take notes using a pen and paper.
- Do not use the Internet for personal reasons during class.
- Perform your assigned reading, training tasks, video lessons and other preparation before arriving for class. I will expect you to participate in class discussions, and I will call on you to contribute.

- You are reminded of the cadet honor code. Cheating undermines the integrity of this academy and shows disrespect towards the work of your classmates. Starting coursework early will help you to avoid the temptation of cheating.

Getting Help

It is expected that the team complete the lab/ homework/ project on their own without assistance from other members/groups. If a team together cannot solve a problem, please seek assistance from one of the instructors. You are forbidden from posting any solutions to homework, etc.

On Perseverance and the Scientific Method

You will inevitably encounter problems while trying to complete your coursework. Sometimes you will be led astray by the confusing interfaces that our software present, and other times you will simply make an error. When something goes wrong, try to fix the problem! Make small, incremental changes, and observe their effects. Most importantly, think about how systems work, and then consider why the error you are observing might have arisen. Occasionally you should stop what you are doing and start from scratch. Learning how to better troubleshoot should be a beneficial side effect of this course.

Graded events

Overview

Event	**Points**
Labs: 10@35pts ea	350
Group Presentation (Does not include Lab 10)	30
WPR	150
Capstone	320
Network Design IPR	*30*
Network Implementation	*200*
AAR Presentation	*30*
Final Paper	*60*
Current Event Analysis	50
Impact Analysis Vignette	50
Instructor Points	50
Total	**1000**

Labs

First, all labs are partner assignments, but there is an individual submission requirement per student. The individual requirement will have a general reflection requirement, common across all labs, and sometimes will have a specific topic requirement. Second, lab 10 is an option from a range of topics to include software security concepts—it is the lab component to a group presentation (see below). Third, in order to make the curriculum more challenging and open to different topics, students may nominate alternative labs for certain topic areas (see below). The proposal must be related to the block, and it must be pre-approved. For instance, if you took CS380 and have performed a straight-forward stack-based buffer overflow before, you could nominate an alternative demonstration of a return oriented programming technique that bypasses OS memory protections during the software security block. In order to nominate an alternative idea, student must formally approve the proposal with their instructor by the date issued in the main course lab document. Finally, students who complete an additional lab 10

topic can earn extra credit. This is an individual effort. Extra credit is due prior to lesson 40, and it is worth 15 points.

Lab	Topic Area	Eligible for Alternative
Lab 1: UNIX	Fundamental Security Concepts	N
Lab 2: Windows Security	Fundamental Security Concepts	N
Lab 3: TCP/IP	Network Security Concepts	N
Lab 4: DNS	Network Security Concepts	N
Lab 5: Network Security Lab	Network Security Concepts	Y
Lab 6: Securing Services (Web/Database)	Web/Database Security Concepts	Y
Lab 7: SQL & XSS	Web/Database Security Concepts	Y
Lab 8: Crypto (Public Key)	Cryptography	Y
Lab 9: Incident handling	Incident Handling & Response	N
Lab 10: Round Robin (See below)	Software Security and Misc topics	Y

Group Presentations

Periodically throughout the semester there will be group presentations that cover a range of topics. There are two components to this assignment: the actual in class presentation and the lab write-up (which is a similar format to the other labs). The lab write-up serves as lab 10 for the group. Both are due in class the day of the presentation. The rubric for the presentation may be found here.

Below is a list of provided topics. Like the labs your group may nominate an alternative topics as well.

- Shellshock Attack (Software security)
- Buffer Overflow (Software security)
- Return to Libc (Software security)
- Cryptography: Brute Force/Collisions (Cryptograph)
- Network Reconnaissance—Nmap (Network Security)
- DNS Poisoning—Kaminsky Attack (Network Security)

Power ranking

***For group events, like the capstone and final paper, a peer grade sheet will be used. Each member of a team will be evaluated based on an initial 10 point average with additions or deductions occurring based on assessed performance. Your final grade will be the team's assignment score multiplied by your peer evaluation average.

Submission

You must document external references. Assignment submissions consist of digital artifacts and a printed write up. The printed write up will include an acknowledgement cover sheet and references

page. Your documentation must comply with the current version of the Documentation of Academic Work manual. It can use either the CSE N-Y, APA, MLA or Chicago formats, but you must be consistent.

The following are considered common knowledge and thus require no documentation:

- ideas from your instructor
- ideas discussed in class with the participation of your instructor (i.e., not private conversations between individuals or teams), and
- anything discussed during the course of additional instruction.

Violations of the honor code will be met with disciplinary action, and a lack of individual thought or effort will be met with a lowered grade. Examples of the latter include the excessive verbatim or paraphrased use of another person's work (even if cited), the excessive use of a single source with no evidence of original thought, sloppy documentation, and so on. ***Wikipedia and Stack Overflow are not acceptable sources; points will be deducted for using these uncontrolled sources.***

Grade scale

Score	Letter grade	Definition
≥97	A+	Exceeded expectations
≥93	A	Mastered all material
≥90	A-	Mastered most material
≥87	B+	Understood all material, masters some
≥83	B	Understood all material
≥80	B-	Understood most material
≥77	C+	Achieved foundation to build on
≥73	C	Adequate performance
≥70	C-	Demonstrated superficial understanding
≥65	D	Marginally failed to demonstrate understanding
≥0	F	Failed to demonstrate understanding

Late policy

Assignments are due the moment class starts. Late assignments will lose points according to the table below.

Up to 24 hours late	≤ one letter grade reduction
24–48 hours late	≤ two letter grade reduction
48–72 hours late	≤ three letter grade reduction
72–96 hours late	F with some points
More than 96 hours late	F with as few as zero points