Course Syllabus

14-761: Applied Information Assurance

Fall 2020
Remote Instruction via Zoom

Instructors: Matt Kaar, Chris May
Email: REDACTED
Office Hours: Zoom - By appointment

TA: Anusha Penumacha
Email: REDACTED
Office Hours: Zoom - By appointment

Table of Contents

Course Overview

This course focuses on practical applications of Information Assurance (IA) and cybersecurity policies and technologies in enterprise network environments. The course is designed around virtual lab environments and exercise scenarios that provide for robust and realistic hands-on experiences within a broad range of IA topic areas. Students are provided numerous practical opportunities to apply cybersecurity best practices to solve real-world problems. AIA classes

include short lectures and in-class hands-on activities. Class participation is required. Zoom and Piazza will facilitate student participation. The TA will serve as moderator during classes.

The instructors will use 10 question quizzes at the beginning of class (weeks 2-11) to evaluate student understanding of the homework assignments and lecture content. To make these assessments more enjoyable for the students, we will use the Kahoot game-based web/mobile application to administer the quizzes. To get credit and enable grading, each student must use their **Andrew ID** for Nicknames for each Kahoot quiz. Five bonus points will be given to students finishing in first place on each quiz.

Team Exercises

The keystone components of AIA are the scenario-based team exercises. To complete these hands-on exercises, students will login to the CyberLEAPfwd virtual environment: (REDACTED). The TA will brief and debrief students on the objectives, requirements, and solutions for each exercise. Teams will have until the following Monday at **12:00 noon** to complete each exercise.

Homework Assignments

Students must complete video lessons and hands-on labs as homework. A CyberLEAPfwd course will be used to organize and provide access to these assignments. The system automatically tracks student progress. Students must complete the required homework by the following **Monday at 12:00pm**. This gives the TA time to grade homework prior to the start of class each week.

Group Projects

The goal of the project is to provide a meaningful learning experience (new hands-on lab) for future AIA students. By **week 2** of the course, students must select teammates with whom they will co-develop a group project. These **3 person** teams will research, integrate, and document a cybersecurity technology instructional lab. This will include the configuration of virtual machines and developing step-by-step procedures for completing the security or forensics technology best practice. Teams can select their own lab topics although instructors can help with topic ideas. An instructor checkpoint meeting will take place in class on week 8. Students must demonstrate that they are at least 50% complete with their project according to their project plan submitted on week 4.

1. **Plan:** Teams must submit a 1-2 page group project proposal no later than the start of class on **week 4** of the course. An exemplar proposal will be provided.
    - This proposal should first describe the team's technical topic and problem being addressed. Next, teams must lay out the planned schedule of development, workload breakdown showing each team member's planned

tasks/responsibilities, as well as the planned instructional objectives of their hands-on lab project.

2. **Build:** Teams will build their projects using the TopoMojo lab builder interface (REDACTED). This will significantly ease the overhead required to create/network the VMs (**max 5)**. Your VMs can be bridged to access the Internet during the build phase; however, your final lab must **NOT** require Internet access in its final state. Additionally, teams must **NOT** use the bridge-net IP space (10.9.8.7/24) in their project network. The TA will demonstrate how to use bridge-net in class.

3. **Document:** A lab manual must be written clearly and concisely within the TopoMojo Markdown editor. Along with step-by-step instructions, this document must also contain instructive, contextual information that describes why the specific steps are being completed. This document must be the original work of the team. Proper citation of all technical sources is required.
    - At least **5** automated verification scripts must be included in the lab that when run, validate successful completion of the lab's learning objectives. These should assess student understanding (quiz questions) as well as query the state of project VMs to verify that steps are completed correctly. These scripts must also be included as text in appendix 1 at the end of the lab manual.
    - A second appendix must include the quiz questions and answers included in the scripts.

4. **Review:** To enhance the quality of the final products and to promote collaboration, group project peer reviews will be conducted. On **Week 11** of the course, teams will be assigned to test-drive another team's lab and make comments on their documentation, structure, and overall quality. Peer feedback should be compiled into one document no more than 2 pages long. The review document must be sent to the owning team and posted to the group site on Canvas. This must be completed by the start of class on **Week 12**. This will give the owning team time to consider these comments and incorporate any suggestions/changes into their final project submission.

5. **Present:** All teams will be given approximately 40 minutes during the last 3 weeks of the course to present their project to the rest of the class. The teams must first present an overview of their lab (3-4 slides) that introduce the topic, learning objectives, and key takeaways. The teams must then interactively walk the class through the steps of their lab within TopoMojo as part of a **live** demonstration. Finally, students in AIA must complete each week's presented projects **as homework** before class starts the following week. Class attendance is **mandatory** during the group project presentations.

Project deliverables:

- Lab manual in the TopoMojo Markdown editor
- TopoMojo virtual machines and any required ISO images. VMs must be saved in the correct final starting state.

The above deliverables must be ready for grading by the start of class on **week 13**. The order of the presentations will be selected at random, although teams can volunteer to present ahead of time if desired. To ensure all teams are provided the same project delivery timeline, teams will be locked out of their TopoMojo workspaces on week 13.

Course Details

Number of Units: 12

Prerequisites: None

Class Schedule: Tuesdays 4:00-6:20pm

Textbook Information: N/A

Course Objectives

At the end of the course, students should be able to:

- Define Defense-in Depth as it applies to Information Assurance
- List and describe nine Foundations of Information Assurance
- Identify and execute common threats to IT Enterprises
- List common host security best practices and implement controls
- List common network security best practices and implement controls
- Identify common network monitoring best practices, implement same on IT networks, and analyze collected data for anomalous behavior
- Compare common cryptosystems, implement and evaluate data encryption/integrity approaches on IT systems and networks
- Recognize and describe technical benefits and challenges encryption has on information assurance and cyber forensics
- Describe the incident response process and apply process during live and simulated cyber security events
- Correctly use common incident response tools to identify, collect and analyze data in search of malicious activities on IT networks
- Describe the digital forensic process and apply this during live and simulated cyber investigations
- Correctly use common digital forensics tools to acquire and analyze forensic evidence

Evaluation & Grading

Students who miss assignment deadlines will have 24 hours to submit late work. Late submissions will incur a 10% deduction. No points are awarded after the 24-hour grace period.

Course Grading Summary

Graded Item	Points
Enterprise Information Security Part 1	50
Enterprise Information Security Part 2	50
Tactical Response and Analysis Challenge (TRAC) Team Exercise Part 1	50
TRAC Part 2	50
XYZ Bank Team Exercise Part 1	50
XYZ Bank Part 2	50
Operation Aurora Capstone Exercise Part 1	50
Operation Aurora Capstone Exercise Part 2	50
In-Class Kahoot! Quizzes (10 pts x 10 weeks of the course)	100
Homework Assignments (10 pts x 14 weeks of the course)	140
Class Participation (5 pts x first 12 weeks of course)	60
Group Projects	300
Total	**1000**

Project Grading Rubric

Graded Item	Points
Lab functions properly *Everything works as expected and the markdown lab manual makes logical sense and is easy to follow*	80
Presentation *Presentation was instructionally sound with key points clearly taught and demonstrated. Demo worked as planned without unacceptable errors or delays.*	80
Peer Review *Provided adequate feedback to peers and addressed findings and suggestions for improvement in final project deliverables*	60
Automated verification scripts *At least 5 scripts designed to test key learning steps within project and all worked as expected*	50
Presentation Attendance *Attendance will be taken during group project presentations (final 3 weeks of class)*	30
Total	**300**

Course Calendar

Weekly Schedule			
Week 1 (Kaar, May)	01 Sep	Course Overview	Syllabus walkthrough & Hacking/malware lecture
Week 2 (May)	08 Sep	Data Security	Homework: EIS Prep Labs 1-6
Week 3 (Kaar)	15 Sep	Host Security	Homework: EIS Prep Labs 7-11
Week 4 (May)	22 Sep	Network Security	EIS Exercise Part 1 Group Project Proposals Due
Week 5 (Kaar)	29 Sep	Monitoring, Detection, & Response	EIS Exercise Part 2
Week 6 (May)	06 Oct	Introduction to Cyber Forensics	Forensics Case Labs
Week 7 (Kaar)	13 Oct	Advances in Cyber Forensics	TRAC Exercise Part 1
Week 8 (Kaar, May)	20 Oct	In-Class Project Checkpoint Meetings	TRAC Part 2
Week 9 (Kaar)	27 Oct	Cloud Security	XYZ Bank Exercise Part 1
Week 10 (Penumacha)	03 Nov	TA Lecture – Topic TBD	XYZ Bank Part 2
Week 11	10 Nov	Capstone Exercise (1/2)	Peer Reviews Assigned
Week 12	17 Nov	Capstone Exercise (2/2)	Peer Reviews Due
Week 13	24 Nov	Group Project Presentations	Group Projects Due Homework: Complete this week's group project labs.
Week 14	01 Dec	Group Project Presentations	Homework: Complete this week's group project labs.
Week 15	08 Dec	Group Project Presentations	Homework: Complete this week's group project labs.