Carnegie Mellon University
Information Networking Institute

Course Syllabus

14-761: Applied Information Assurance
Spring, 2020

Instructors: Matt Kaar, Chris May
Office: CIC 1107, 412-268-6832
Email: mkaar@cmu.edu, cjmay@cmu.edu
Office Hours: By appointment

TA: Anusha Penumacha
Office: TBD
Email: apenumac@andrew.cmu.edu
Office Hours: By appointment

Table of Contents

Course Description 1
Team Exercises 2
Homework Assignments 2
Group Projects 2
Course Details 4
Course Objectives 4
Evaluation & Grading 5
Project Grading Rubric 5
Course Grading Summary 5
Tentative Course Calendar 6
Course Policies 6
Take Care of Yourself 6
Carnegie Mellon University Statement on Academic Integrity 7
Carnegie Mellon Code 8
Carnegie Mellon University's Policy on Cheating 8
Carnegie Mellon University's Policy on Plagiarism 9
Carnegie Mellon University's Policy on Unauthorized Assistance 9
Carnegie Mellon University's Policy on Research Misconduct 10

Course Description

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 will be provided numerous practical opportunities to apply cybersecurity best practices to solve real-world problems.

The instructors' goal is to **"flip"** the AIA classroom experience for students so that class meetings are reserved primarily for gaining hands-on, real-world experience. Therefore, background knowledge will be developed using short video-captured lessons and skill-building **labs** which will be assigned as homework. Students **must** bring their laptop computers to class throughout the course.

The instructors will use 10 question **quizzes** at the beginning of class 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 as their Nickname** 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 **hands-on team exercises**. These exercises will be conducted in class starting on week 4 and will run through week 12. To complete the exercises, students will be provided with an account that they will use to login to the CyberLEAPfwd virtual environment: (https://cyberleapfwd.cmu.edu). The instructors/TA will begin each class period with a short lecture on relevant topics or to brief/debrief the students on the objectives and requirements of each scenario exercise. The teams will have until the **following Monday at 12:00 noon** to complete the evaluation components of the team exercises.

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 instructional 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 cyber security 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.
   - 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 out their projects using the course TopoMojo lab builder interface (https://topomojo.ini.cmu.edu). This will significantly ease the overhead required to create/network the VMs (**max 4**). 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 and must **NOT** use the bridge-net IP space (10.9.8.7/24) in its topology. The TA will demonstrate how this is done 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, automatically validate successful completion of the lab's objectives. These scripts must also be included as text in appendix 1 at the end of the lab manual.
   - A second appendix will be a 5-7 question, multiple-choice quiz that can be used to assess student understanding of the key concepts presented in the lab.
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, leaning 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.

All of the above deliverables must be made available for grading by the start of class on **week 13**. The order of the presentations will be selected **at random** one after another, so it is imperative that projects be fully completed by week 13. TopoMojo workspaces will be closed on week 13 to ensure students cannot edit their work following this deadline.

Course Details

Number of Units: 12

Prerequisites: None

Class Schedule: Tuesdays 3:00-5:50pm in the CIC DEC

Textbook Information: N/A

Course Website: http://www.andrew.cmu.edu/course/14-761/

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 images and other forensic evidence

Evaluation & Grading

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*	100
Presentation *Presentation was instructionally sound with key points clearly taught and demonstrated. Demo worked as planned without unexpected errors or unacceptable delays.*	80
Peer Review *Provided adequate feedback to peers and addressed findings and suggestions for improvement in final project deliverables*	60
Automated verification scripts *Scripts designed to test key learning steps within project and worked as expected*	30
Presentation Attendance *Attendance will be taken during group project presentations (final 3 weeks of class)*	30
Total	**300**

Course Grading Summary

Graded Item	Points
Enterprise Information Security Part 1	25
Enterprise Information Security Part 2	25
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	100
In-Class Quizzes	100
Homework Assignments	150
Group Projects	300
Total	**900**

Tentative Course Calendar

Weekly Schedule		
Week 1 (Kaar, May)	Course Overview	Syllabus walkthrough & Hacking lecture
Week 2 (May)	Data Security	Homework: EIS Prep Labs 1-6
Week 3 (Kaar)	Host Security	Homework: EIS Prep Labs 7-11
Week 4 (May)	Network Security	EIS Exercise Part 1 Group Project Proposals Due
Week 5 (Kaar)	Network Monitoring, Detection, & Response	EIS Exercise Part 2
Week 6 (May)	Introduction to Digital Forensics	Forensics Case Labs
Week 7 (Kaar)	Advances in Digital Forensics	TRAC Exercise part 1
Week 8 (Kaar, May)	In-Class Project Checkpoint Meetings	TRAC Part 2
Spring Break	---	---
Week 9 (Kaar)	Malware Analysis	XYZ Bank Exercise Part 1
Week 10 (Penumacha)	TA Lecture – Topic TBD	XYZ Bank Part 2
Week 11	In-class Capstone Exercise (1/2)	Peer Reviews Assigned
Week 12	In-class Capstone Exercise (2/2)	Peer Reviews Due
Week 13	Group Project Presentations	Group Projects Due Homework: Complete this week's group project labs.
Week 14	Group Project Presentations	Homework: Complete this week's group project labs.
Week 15	Group Project Presentations	Homework: Complete this week's group project labs.

Course Policies

Take Care of Yourself

As a student, you may experience a range of challenges that can interfere with learning, such as strained relationships, increased anxiety, substance use, feeling down, difficulty concentrating and/or lack of motivation. These mental health concerns or stressful events may diminish your academic performance and/or reduce your ability to participate in daily activities. CMU services are available, and treatment does work. You can learn more about confidential mental health services available on campus at: https://www.cmu.edu/counseling/. Support is always available (24/7) from Counseling and Psychological Services: 412-268-2922.

Carnegie Mellon University Statement on Academic Integrity

https://www.cmu.edu/student-affairs/ocsi/academic-integrity/statement-AI.html

Carnegie Mellon University educates its students to become professionals who will serve society with integrity. The university also creates and disseminates new knowledge and expressions of knowledge in ways that benefit society. Carnegie Mellon strives to serve the changing needs of society through the three primary goals outlined in its mission statement: to create and disseminate knowledge and art through research and artistic expression, teaching and learning and transfer to society, to serve students by teaching them leadership and problem-solving skills, and the values of quality, ethical behavior, responsibility to society and commitments to work, to pursue the advantages provided by a diverse community, open to the exchange of ideas, where discovery and artistic creativity can flourish.

These statements provide groundwork for academic integrity that includes everyone in the Carnegie Mellon community. Our common objective is to make sure that we teach and learn with commitment, consistency, honesty and fidelity. This process involves at its core interaction between young and old, novice and expert, apprentice and master. Integrity requires that we examine the context in which we do our work. In the university community, young people grow and develop their identities, which mandate that all our dealings follow and foster principles of respect for autonomy, beneficence, justice and fidelity to the mission of the university. The university population is increasingly diverse, faces rapid changes in knowledge and technology that have historically produced uncertainty about the appropriate roles of individuals and professions in the larger society. Each of these facts can and do create issues that we need to be aware of and deal with if we are to successfully achieve our primary missions. When these circumstances are not fully communicated to and understood by all persons in the community, unnecessary suspicions concerning integrity may distract from our teaching and learning and taint the atmosphere on campus. When they are openly discussed and conflicts concerning them openly aired, we all proceed with greater confidence and trust.

All members of the university community have the obligation to serve as models of personal and professional integrity, as well as models for creating, expressing and transferring knowledge. This implies that the faculty not only provide the knowledge and training that prepare students to find their productive roles in society, but also help them discover and maintain integrity in the practice of that role. Staff and administrators are charged with representing the university accurately and forthrightly. Students are responsible for conducting their learning in a similarly honest and committed fashion-by avoiding plagiarism, cheating or taking credit for work not their own-and thus contributing to a campus atmosphere which expects and supports academic integrity.

Carnegie Mellon Code

https://www.cmu.edu/student-affairs/theword/code.html

Students at Carnegie Mellon, because they are members of an academic community dedicated to the achievement of excellence, are expected to meet the highest standards of personal, ethical and moral conduct possible.

These standards require personal integrity, a commitment to honesty without compromise, as well as truth without equivocation and a willingness to place the good of the community above the good of the self. Obligations once undertaken must be met, commitments kept.

As members of the Carnegie Mellon community, individuals are expected to uphold the standards of the community in addition to holding others accountable for said standards. It is rare that the life of a student in an academic community can be so private that it will not affect the community as a whole or that the above standards do not apply.

The discovery, advancement and communication of knowledge are not possible without a commitment to these standards. Creativity cannot exist without acknowledgment of the creativity of others. New knowledge cannot be developed without credit for prior knowledge. Without the ability to trust that these principles will be observed, an academic community cannot exist.

The commitment of its faculty, staff and students to these standards contributes to the high respect in which the Carnegie Mellon degree is held. Students must not destroy that respect by their failure to meet these standards. Students who cannot meet them should voluntarily withdraw from the university.

This policy applies, in all respects, to this course.

Carnegie Mellon University's Policy on Cheating

https://www.cmu.edu/student-affairs/ocsi/academic-integrity/definitions.html

According to the University Policy on Academic Integrity, cheating "occurs when a student avails her/himself of an unfair or disallowed advantage which includes but is not limited to:

- Theft of or unauthorized access to an exam, answer key or other graded work from previous course offerings.
- Use of an alternate, stand-in or proxy during an examination.
- Copying from the examination or work of another person or source.
- Submission or use of falsified data.
- Using false statements to obtain additional time or other accommodation.
- Falsification of academic credentials."

This policy applies, in all respects, to this course.

Carnegie Mellon University's Policy on Plagiarism

https://www.cmu.edu/student-affairs/ocsi/academic-integrity/definitions.html

According to the University Policy on Academic Integrity, plagiarism "is defined as the use of work or concepts contributed by other individuals without proper attribution or citation. Unique ideas or materials taken from another source for either written or oral use must be fully acknowledged in academic work to be graded. Examples of sources expected to be referenced include but are not limited to:

- Text, either written or spoken, quoted directly or paraphrased.
- Graphic elements.
- Passages of music, existing either as sound or as notation.
- Mathematical proofs.
- Scientific data.
- Concepts or material derived from the work, published or unpublished, of another person."

This policy applies, in all respects, to this course.

Carnegie Mellon University's Policy on Unauthorized Assistance

https://www.cmu.edu/student-affairs/ocsi/academic-integrity/definitions.html

According to the University Policy on Academic Integrity, unauthorized assistance "refers to the use of sources of support that have not been specifically authorized in this policy statement or by the course instructor(s) in the completion of academic work to be graded. Such sources of support may include but are not limited to advice or help provided by another individual, published or unpublished written sources, and electronic sources. Examples of unauthorized assistance include but are not limited to:

- Collaboration on any assignment beyond the standards authorized by this policy statement and the course instructor(s).
- Submission of work completed or edited in whole or in part by another person.
- Supplying or communicating unauthorized information or materials, including graded work and answer keys from previous course offerings, in any way to another student.
- Use of unauthorized information or materials, including graded work and answer keys from previous course offerings.
- Use of unauthorized devices.
- Submission for credit of previously completed graded work in a second course without first obtaining permission from the instructor(s) of the second course. In the case of concurrent courses, permission to submit the same work for credit in two courses must be obtained from the instructors of both courses."

This policy applies, in all respects, to this course.

Carnegie Mellon University's Policy on Research Misconduct

https://www.cmu.edu/student-affairs/ocsi/academic-integrity/definitions.html

According to the University Policy for Handling Alleged Misconduct in Research, "Carnegie Mellon University is responsible for the integrity of research conducted at the university. As a community of scholars, in which truth and integrity are fundamental, the university must establish procedures for the investigation of allegations of misconduct of research with due care to protect the rights of those accused, those making the allegations, and the university. Furthermore, federal regulations require the university to have explicit procedures for addressing incidents in which there are allegations of misconduct in research."

The policy goes on to note that "misconduct means:

- fabrication, falsification, plagiarism, or other serious deviation from accepted practices in proposing, carrying out, or reporting results from research;
- material failure to comply with Federal requirements for the protection of researchers, human subjects, or the public or for ensuring the welfare of laboratory animals; or
- failure to meet other material legal requirements governing research."

"To be deemed misconduct for the purposes of this policy, a 'material failure to comply with Federal requirements' or a 'failure to meet other material legal requirements' must be intentional or grossly negligent."

To become familiar with the expectations around the responsible conduct of research, please review the guidelines for Research Ethics published by the Office of Research Integrity and Compliance.

This policy applies, in all respects, to this course.