Carnegie Mellon University
Information Networking Institute

COURSE SYLLABUS

14-761: Applied Information Assurance
Fall, 2017

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

TA: Ash Singh
Office: INI X, XXX-XXX-XXXX
Email: ashutoss@andrew.cmu.edu
Office Hours: By appointment

Course Description:

This course focuses on practical applications of Information Assurance (IA) 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 structure the AIA classroom experience so that class meetings are reserved primarily for gaining hands-on, real-world experience. Short lectures will introduce concepts and demonstrate skills, however ample class time will be allocated so teams can work together on the group exercises. Additional knowledge and skills 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, second, and third 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 2 and will run through week 11. To complete the exercises, students will be provided with an account that they will use to login to the AIA virtual learning environment. The instructors/TA will thoroughly 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. The first team exercise is described below.

The Information Assurance Exercise (IAX) will be the first team-based, scenario-driven exercise. This is an entirely hands-on exercise where students must work together in teams (**3 per team**) to complete the IAX requirements. Each team will be presented with a remotely accessible virtual network and a scenario

that describes a fictitious bankrupt company that has failed an IA audit. In this scenario, the teams will serve as consultants who've been hired to implement the bankruptcy court's mandated IA get-well plan.

The teams must work collaboratively to re-architect the company's network, integrating interdependent security systems and IA best practices. Each week, team members will rotate through the securing of the network and hardening of the servers in the scenario. This network build process will occur during **weeks 2-4** and in-class time will be dedicated to this effort. The rest of the weekly build is the responsibility of the team and must be accomplished before Monday 12:00 noon of the following week. The TA will audit and verify the IAX network for compliance with the get-well plan every week. These weekly audits will be graded (**25 points**) and posted to Canvas each week.

On **week 5**, teams must respond to live instructor injected attacks and network anomalies. They must correctly detect and identify the nature and source of these attacks. Following class, teams will have access to their networks all week to perform post-mortem analysis. To test students' understanding of IAX objectives and appropriate response actions, a short quiz (**25 points**) will be taken in class on **week 6**.

Homework Assignments:

Students must complete video lessons and hands-on labs as homework. A Simulation, Training, and Exercise Platform (STEP) course will be used to organize and provide access to these assignments. The system automatically tracks student progress. Students must complete the required 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 labs) for future AIA students. By **week 2** of the course, students must select teammates with whom they will co-develop a group project. These **2-3-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 must select their own lab topics although instructors can help with topic ideas.

1. **Plan:** Teams must submit a group project proposal no later than the start of class on **week 4** of the course.
    - This proposal should briefly describe their topic selection and lay out the planned components and instructional objectives of their hands-on lab.
2. **Build:** Teams will build out their projects using the STEP TopoMojo lab builder interface. 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. 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 also be turned in as a Microsoft Word file on Week 12.
    - At least 5 suggested lab verification steps must be included that when run, automatically validate successful completion of the lab. These steps should be scripted and incorporated into the tasks outlined in the lab manual. These are to be added as an appendix to the end of the primary lab mark down document in TopoMojo.

- A second appendix will be a 10 question, multiple-choice quiz that can be used to assess student understanding of the key concepts presented in the lab. Teams must create a Kahoot quiz from this.

4. **Review:** To enhance the quality of the final products and to promote collaboration, group project peer reviews will be conducted. On **Week 10** of the course, teams will be assigned to test-drive another team's lab and make comments on their documentation and structure. The MS Word track changes review feature is the preferred method for providing feedback, however peer feedback may also be compiled into one document (no more than 3 pages) and must be emailed to the owning team (cc the TA). This must be completed by the start of class on **Week 11**. 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 30-40 minutes during the last 4 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 provide key takeaways. The teams must then interactively walk the class through all the steps of their lab within the TopoMojo system as part of a **live** demonstration. Finally, the class must take the Kahoot quiz constructed from appendix two of the lab manual. This quiz will help instructors gage the effectiveness of the presentations and track student attendance. Additionally, the presented labs for each week will be assigned as homework for the final four weeks of class and all students must submit feedback on each lab using a rubric based on a 1-4 scale (1=poor, 2=fair, 3=good, 4=great).

Project deliverables:

- Lab manual
- VMware virtual machines and CD-R images (.iso files). VMs must be saved in the correct final starting state.
- Kahoot Quiz

All of the above deliverables must be made available for grading by the start of class on **week 12**. The order of the presentations will be selected at random one after another, so it is imperative that projects be fully completed by week 12.

Number of Units: 12

Prerequisites: None

Class Schedule: Tuesdays 3:00-5:20pm in INI DEC Henry St. Lower Level

Textbook Information: Defense in Depth: Foundations for Secure and Resilient IT Enterprises - Free download at: http://www.sei.cmu.edu/reports/06hb003.pdf

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 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 cyber investigations
- Correctly use common digital forensics tools to acquire and analyze images and other forensic evidence

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

Evaluation & Grading:

Project Grading Rubric:

Graded Item	Points
Lab functions properly and is instructionally sound	75
Presentation instructionally sound with key points clearly taught and demonstrated	75
Peer Review: Provide adequate feedback and address recommendations	50
Virtual Machines are in the correct starting state	25
Lab manual follows the provided document template	25
Total	**250**

Course Grading Summary:

Graded Item	Points
Class Participation and Completion of Homework	100
Information Assurance Exercise (IAX)	100
Prioritizing Defensive Measures (PDM)	50
Tactical Response and Analysis Challenge (TRAC) Part 1	50
TRAC Part 2	50
Capstone Exercise (XYZ Bank) Part 1	50
Capstone Exercise (XYZ Bank) Part 2	50
Group Project	250
In-Class Quizzes	100
Total:	**800**

Course Calendar:

Weekly Schedule		
Week 1 (08/29/2017)	Course Overview	Defense-in-Depth and Threats Lectures (May/Kaar)
Week 2 (09/05/2017)	Data Security Lecture (May)	IAX Week 1 of 4
Week 3 (09/12/2017)	Host Security Lecture (Kaar)	IAX 2 of 4
Week 4 (09/19/2017)	Network Security Lecture (May)	IAX 3 of 4 Group Project Proposals Due
Week 5 (09/26/2017)	Network Monitoring/Logging Lecture (Kaar)	IAX 4 of 4
Week 6 (10/03/2017)	Incident Response Lecture (May)	PDM Exercise
Week 7 (10/10/2017)	Hunting Malware Lecture (Kaar)	TRAC Exercise Part 1
Week 8 (10/17/2017)	Introduction to Forensics Lecture (May)	Introductory forensics case labs
Week 9 (10/24/2017)	Advances in Forensics Lecture (Kaar)	TRAC Exercise Part 2
Week 10 (10/31/2017)	Capstone Exercise (XYZ Bank Part 1)	Peer Reviews Assigned
Week 11 (11/07/2017)	Capstone Exercise (XYZ Bank Part 2)	Peer Reviews Due
Week 12 (11/14/2017)	Group Project Presentations	**All Final Group Projects Due** Presented projects assigned as homework
Week 13 (11/21/2017)	Group Project Presentations	Presented projects assigned as homework
Week 14 (11/28/2017)	Group Project Presentations	Presented projects assigned as homework
Week 15 (12/05/2017)	Group Project Presentations	Presented projects assigned as homework

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.

CMU Academic Integrity Policy (http://www.cmu.edu/academic-integrity/index.html):

In the midst of self-exploration, the high demands of a challenging academic environment can create situations where some students have difficulty exercising good judgment.

Academic challenges can provide many opportunities for high standards to evolve if students actively reflect on these challenges and if the community supports discussions to aid in this process. It is the responsibility of the entire community to establish and maintain the integrity of our university.

This site is offered as a comprehensive and accessible resource compiling and organizing the multitude of information pertaining to academic integrity that is available from across the university. These pages include practical information concerning policies, protocols and best practices as well as articulations of the institutional values from which the policies and protocols grew. The Carnegie Mellon Code, while not formally an honor code, serves as the foundation of these values and frames the expectations of our community with regard to personal integrity.

THE CARNEGIE MELLON CODE

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 (http://www.cmu.edu/academic-integrity/cheating/index.html) states the following:

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 (http://www.cmu.edu/academic-integrity/plagiarism/index.html) states the following:

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 (http://www.cmu.edu/academic-integrity/collaboration/index.html) states the following:

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 (http://www.cmu.edu/academic-integrity/research/index.html) states the following:

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.***