Carnegie Mellon University
Dietrich College
Information Systems

Special Topics: Information Assurance (67-309)

Course Description and Syllabus

Instructors: Samuel Perl (sperl@andrew.cmu.edu)

Term: Fall 2018, Mini 2

Textbook:
Introduction to Information Security: A Strategic-Based Approach
by Shimeall, Timothy; Spring, Jonathan.
Print ISBN: 9781597499699, 1597499692 eText ISBN: 9781597499729

Office Hours: Office hours without appointment will be held 1 hour per week. Times and Location to be announced. If you would like an appointment for a different time, please email the instructor and we will try to find an alternative time/place to meet.

Course Overview:

Special Topics: Information Assurance is an introduction course for Information Systems students that focuses on information security concepts. You will be introduced to the practice of securing information systems, how organizations manage risk to their information assets, threats to the security of an information systems, strategies for organizational resilience, applicable US cyber laws, and responding to real incidents. You will hear about some of the major cyber incidents that have shaped the way security is performed by organizations on the internet today, and you will participate through class discussions and homeworks analyzing important recent cyber issues, real incidents, and internet-scale events. By the end of the class you will be able to analyze the design of security systems and the implications of real world attacks on security systems by applying core information security concepts.

Course Description:

Recent technological events have combined to shape today's society into one that is more connected than ever before. The rapid pace of progress and technological advancement - since the invention and popularization of the internet has particularly exploded in hardware manufacturing, telecommunications, and software industry. Other industries are also achieving high growth as they move more of their business and processes online. The internet has become an environment that is incredibly useful to organizations, governments, and individuals for a large variety of needs. The internet will soon be entering the Internet of Things (IOT) era where many more objects will be combined with computing devices to achieve even more connectivity between the cyber and physical world.

The practice of attempting to secure information pre-dates the internet by thousands of years and the protection of 'secrets' is not a new concept to individuals or organizations. But the interconnectivity of the internet at such a vast scale, the rapid development achievable by software and even hardware creators, and the pervasiveness of technology into business and personal lives has required organizations and individuals to evolve their security practices.

Just as systems are build to achieve a function - such as the exchange of information between a retailer and a customer, such systems are fundamentally expected to be 'secure.' But what is 'secure' for all systems and how can we achieve it? The security community has responded with both theory and practice – with varying degrees of success – to the advances in hardware, software, networks, devices, and the internet in an attempt to answer this question.

You will learn about security concepts and security practices, and how organizations attempt to secure their systems against threats. This course will be a broad introduction to many aspects of information security that affect your systems, your everyday life on the internet, your activities - and those of others, and the practices of all organizations using and building information systems.

After learning Information Security concepts, You will contribute via in-class discussion, homework, and projects on technical, societal, and organizational issues related to security & privacy of information and information systems.

Learning Objectives:

Upon successful completion of the course, each student should be able show to tangible evidence of growth and maturity in the following areas:

1. Be able to state core information security concepts

2. Apply information security concepts to case studies, discussions, and preliminary information system designs

3. Perform analysis of the implications of certain decisions upon information and/or system security

4. Understand relevant legal, ethical, and privacy issues and how they might impact policy and actions of organizations or individuals

5. Make decisions about the security of information and information systems, and support your decisions with relevant arguments

6. Apply security analysis to a real world event and present your findings and arguments

Schedule:

This class meets on Tuesday evening from 6:30pm - 9:20pm. There will be 7 lectures.

#	Course Week	Lecture Topic
1.	October 23	Course Logistics Introduction to Information Security Concepts
2.	October 30	Threats to Security, Defensive Security Controls
3.	November 6	Organizations, Assets, and Risk Management & Organizational Resilience *First Homework Assignment Due*
4.	November 13	Cyber Law, Law Enforcement, Ethics
5.	November 20	A short history of paradigm shifting security events (Hacks, Leaks, Intrusions) & Cyber Incident Response *Second Homework Assignment Due*
6.	November 27	Privacy (Orgs & Individuals)
7.	December 4	Special Topics such as The Internet of Things (IOT), 'Big-Data', and Machine Learning.
	December 11	Submission of Final Project Due in Canvas

Assignments

There will be 2 homework assignments and a Final Project in this class. The first homework will be a short summary analysis of a relevant security topic we have covered in lecture applied to a current cyber policy issue, event, or report. The second will be to choose a topic and source material for your final project and to write and submit a summary outline. A sample list of source material will be posted to Canvas. Each homework assignment will be announced on Canvas with submission instructions closer to their due date.

Final Project

Students of security technology and policy must be able to communicate technical concepts to a wider audience including developer teams, designers, marketing, leadership, customers, and the general public. Students in this course will write a paper analyzing a publicly reported data breach - such as from a technical incident report, investigative news article, or analysis and then write a paper analyzing the event intended for an executive audience responsible for securing organizations systems.

Your final project is not limited to a written report alone. If you would like to include additional technical analysis products, please check with the instructor. All proposals for alternative projects must be approved by the instructor. Your proposal must include significant documented analysis to accompany any technical work. Projects that focus solely upon a technical solution and do not address the implications, usage, use cases, benefits, risks, and instructions to organizations on the work will not receive full credit. Grading details on the final project will be announced in class and posted on canvas.

Grading Weights

- 15% - Homework 1
- 15% - Homework 2
- 40% - Final Project
- 25% - Class Discussion
- 05% - Professionalism

Regarding In Class Discussion

Special Topics: Information Assurance is designed to begin with a framework and language for thinking about information security issues. The class discussions will reflect current events, thoughtful pieces, and we will spend time frequently discussing, applying what you have learned and performing analysis. Your participation in the discussion is 25% of your final grade, and is intended to serve as both practice for analysis and practice for creating, documenting, and presenting your work in the Final Project. Your attendance in class is required to participate in class discussions. The instructor will also be asking the class questions, and asking individual students questions about the material. There are many different ways that you can participate in class. Also consider that being attentive to other teammates when they are participating is a key professional skill.

To receive a full participation grade you are expected to do the following:

1. Attend class unless you have an excused absence
2. Completing any pre-class reading. Any required reading assignments for a class will be posted on Canvas at least 1 week prior to the start of the next class. Reading assignments will usually be reflective of import research, findings, events, or results in the Information Security field that are directly related to the material being covered in class.

3. Complete any assigned pre-work. And example of class pre-work may include reading an assigned article and coming prepared with a list of questions about information security topics raised by the article.
4. Participate in any group activities performed in class
5. Participate in class discussions including attempting to answer questions from the instructor and from other students, performing active listening, and asking pertinent questions of your own. Active listening for purposes of this class means paying attention, reflecting, attempting to clarify information that you do not understand, and being able to summarize information you have heard or read about.
6. Try to relate the concepts you are learning about in class to specific examples in your own life and sharing your own thoughts and experience on these with the class.

Absences

If you have a legitimate reason to be absent, you should contact the instructor at least 24 hours prior to class time. If you become ill on the day of class or encounter an emergency situation, contact the instructor immediately and we will make arrangements for you to make up the material that we covered in class. If you do not contact the instructor prior to the start of class, there will be no opportunity to make up the material.

Professionalism

Students are expected to conduct themselves with respect toward each other. We will be discussing professional responsibility, ethics, crime, and law enforcement. Discourse in information security can sometimes become heated. Students will be expected to act and behave as if they are in a professional setting.

The following guidelines are a minimum expectation:

Sleeping - do not do it. *In Class Discussion* includes your active participation in discussions. If you are not presenting, answering a question, or asking a question, you should be focusing your attention on that person. If you are ill or feeling overly tired, please contact the instructor prior to the beginning of class and we will make arrangements for you to make up the material that we covered in class.

Do not use your phone, browse the web, instant message, or otherwise direct your attention away from presenters and fellow students. If you use a laptop to take notes, you must inform the instructor at the beginning of class.

If you are confused, your confusion may also be shared by other students so please ask the instructor a question. Many of the topics we are covering in class can have multiple viewpoints. This can cause confusion even among professionals in the field. The field of Information Security includes discussion of tradeoffs, incentives, costs, user behavior, attacker behavior, and more. Many professionals can have a difference of opinion on a given issue. This class is an attempt to help you participate in such conversations using the framework, language, and skills, of practicing information security professionals. Asking questions and attempting to answer questions of others is an important learning step and counts toward in class participation.

Accomodations

If you have a disability and require accommodations, please contact Catherine Getchell, Director of Disability Resources, 412-268-6121, getchell@cmu.edu. If you have an accommodations letter from the Disability Resources office, I encourage you to discuss your accommodations and needs with me as early in the semester as possible. I will work with you to ensure that accommodations are provided as appropriate.

Take Care of Yourself

We want you to succeed in this class. If you are finding that this is a struggle, know that you are not alone. If you are having issues, please ask for help. There are many resources available to help you in the IS program, on the CMU campus, and among your instructors.

If you or anyone you know is experiencing academic stress, difficult life events, or feel anxiety or depression, we strongly encourage you to seek support. Counseling and Psychological Services (CaPS) is available to help. Call 412.268.2922 and visit the website https://www.cmu.edu/counseling/ . Consider reaching out to a friend, faculty or family member you trust for help getting connected to support that can help.