BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK

School of Management

**Course Syllabus – MIS 450 – Spring 2013**

| | | |
|---|---|---|
| **Course Name** | **:** | IT Security & Forensics |
| **Course Schedule** | **:** | T/R 1:15 - 2:40 pm, AG 004 |
| **Instructor** | **:** | Ali Alper Yayla<br>ayayla@binghamton.edu ; (607) 777-2440 ; AA-314 |
| **Office Hours** | **:** | T/R 2:40 - 3:30 pm. Otherwise by appointment |

## Course Description

The course has both technical and managerial orientation and introduces the fundamentals of information security and computer forensics. The content of the course is threefold; information security, management of information security, and computer forensics.

The first part starts with the brief introduction to basic concepts relating to information security and computer networks. Students will learn about several threats and attacks to information security. Threats vary from unintentional human errors to deliberate sabotage, theft, and vandalism. In addition to human threats, we'll cover technical threats such as software and hardware errors and failures as well as other threats including technological and forces of nature. Some of the attack categories we will cover are malicious code, denial of service, sniffers, and social engineering. In addition to threats and attacks, students will learn about preventive technologies such as firewalls, intrusion detection, access control, physical security, and cryptography.

The second part of the course will cover the management issues in information security. Students will acquire the basic knowledge of planning and developing security policies and programs, and get familiar with security models that are utilized in the industry. The fundamentals of risk management and project management with respect to information security will also be covered. The second part will continue with two important topics; legal and ethical issues in information security and economics of information security. As future managers, it is important for students to learn the legal and ethical boundaries of information security as it closely relates to privacy issues in organizations. Also, one of the most challenging issues with information security is the financial justification of such measures. Students will learn the basic approaches to economics of threats to information security and using preventive technologies.

The third part of the course starts with the introduction to computer forensics and to basic forensics tools, and continues with building knowledge on digital evidence controls, data acquisition, computer forensic analysis, recovering image and other types of files, and network and email forensics. Comprehensive lab work and lab sessions will empower students with hands-on experience with various forensic tools. Upon completion of the course, students will acquire knowledge on methods and techniques to properly conduct a computer forensics investigation.

This course covers computer vulnerabilities in a professional, prudent, and responsible way. At no time will explicit, step-by-step instructions be given for exploiting security vulnerabilities. You will, however, learn exactly how law enforcement agencies and Chief Security Officers of organizations manage information security and investigate cyber security intrusions as well as secure their systems from breaches and vulnerabilities.

**Learning Objectives**

The content of the course is designed to address the rapidly growing information security and computer forensics field. After successfully completing this course, students should:

- understand the fundamental concepts, terminology, and principles of information security,
- be familiar with various management challenges and approaches to information security,
- acquire required problem solving and decision making skills with respect to risk management and economics of information security,
- understand the principles of computer forensics; including securing, acquiring, and analyzing digital evidence, writing forensics reports, and serving as expert witness in courts, and
- have adequate hands-on experience with variety of computer forensics tools to start and successfully conduct forensics analysis of digital evidence; including computers, network activity, mobile devices, and e-mail.

**Textbook**

Guide to Computer Forensics and Investigations, 4th edition Bill Nelson et al., 978-1435498839 {required}

**Grading**

| Activity | # | Total points |
|---|---|---|
| Exam | 2 | 54 |
| Quiz | - | 15 |
| Project | 1 | 15 |
| Assignment | 3 | 6 |
| News Discussion | - | 5 |
| Participation | - | 5 |
| Exercise | - | 0 |

| Distribution of Grades | | | |
|---|---|---|---|
| A | 93 - 100 | C+ | 77 - 79 |
| A- | 90 - 92 | C | 73 - 76 |
| B+ | 87 - 89 | C- | 70 - 72 |
| B | 83 - 86 | D | 60 - 69 |
| B- | 80 - 82 | F | 0 - 59 |

**Exams**

We will have two exams during the semester. One exam will cover the information security part and one exam will cover the computer forensics part. You are responsible from the lecture notes, class discussions, and additional reading materials covered during the class period. Exams will be administrated over the Blackboard. Exams are not cumulative and will be open book/notes. Exams will include essay questions, multiple choice questions and hands-on questions.

**Quizzes**

There will be various pop quizzes throughout the semester. These quizzes will be conducted at the beginning of the class. There is no make-up for these quizzes. Quizzes are not open book/notes. You will be responsible for the readings that are assigned to that particular day. You are not expected to integrate any readings from previous weeks. Most quizzes will have only essay questions.

**Project**

The project is a team project of 4 students. Teams will be determined at the beginning of the semester. Majority of the projects will have a technically oriented topic which will advance our expertise in computer forensics. Students are encouraged to research and present:

- Forensics topic not covered in class
- Forensics tool or application not covered or discussed in class
- Demonstration of a comprehensive usage of a forensic tool not covered in class
- Usage of forensics tools in another system (Linux, Macintosh)

This project includes a written report and the presentation of this report. Throughout the semester, teams will submit five documents on specified dates. These documents are 1) Project charter, 2) Project progress report I, 3) Project progress report II, 4) Final project report, 5) Project presentation. Submissions after the deadline will not be accepted. Details about the requirements will be posted to Blackboard.

During presentation, teams will be talking to a group of highly professional and competent colleagues. Thus, the presentation should be technically intensive, with the appropriate technical language well mastered. It should introduce the topic to all of us in a way that resembles professional training. If a new tool is presented, for example, we, the audience, should be able to work with the basic functions of the tool after your presentation. We should clearly be able to understand why the speaker recommends us this tool, what is it for, what are its advantages and disadvantages, why we should have this tool in our computer forensics lab, and how it stands up to the other known by us tools. A demonstration of the tool is required.

Each member of the team is expected to participate in the presentation. Each student is expected to attend all other presentations. Oral presentations will be graded based on clarity, creativity, and originality. Thus, it is very important that every team member is fully prepared, present and fully participating. How much effort s/he put in the project and his or her mastering of the topic will be mainly judged by the individual presentation and the questions, which may result in a difference in the project grades among team members. The final presentation grade will be the average of the common presentation grade and the individual student grade.

In addition to the presentation, teams also have to submit a written report. This report has to be parallel to the presentation and should be prepared professionally. Copying and pasting information (e.g., product specifications) from websites are not acceptable and will be considered as plagiarism. It is the team's responsibility to distribute the project workload.

**Assignments**

There will be three assignments throughout the first part of the semester. These assignments will be essay assignments that require minimum of 2-3 pages of insightful and intellectual writings on a topic that is not covered in class. It is your responsibility to follow the due dates of the assignments from Blackboard. Submissions after the deadline will not be accepted.

**Exercises**

There will be several exercises throughout the semester. These are optional and mostly hands-on exercises that will be very useful for getting to know the tools and preparing for the exams. Exercises will be similar to in-class exercises and exam questions.

**News Discussion**

As a team, you will be collecting IT security related news throughout the semester. Every Tuesday class, you will submit a report that outlines the security news from the previous week. At the beginning of each Tuesday class, we will discuss some of the interesting news that you have found as a team. Students are responsible from all of the news in their team report. Students can volunteer and/or called on by the instructor for discussion.

**Class Participation**

There will be various readings assigned for each class meeting. All readings should be read before class. I need your participation for healthy, enjoyable, and productive class discussions. Participation is awarded with grade points, but you must earn these points by answering my or your classmates' questions, starting/participating discussions, and making sure that you contribute to the intellectual body of the class. You must realize that participation is different than attendance. If you do not participate, you will not get any points. Using computers for recreational purposes (Facebook, e-mail, etc) during class will work against your participation. Students can volunteer and/or called on by the instructor for participation.

**Class Attendance**

Class attendance is expected and encouraged. A student with irregular class attendance should expect a negative effect on his/her performance and participation grade. Please, make every effort not to be late to class. Try to be considerate of your fellow students. Attendance has no grade points.

**Time Requirement outside the Class**

You should expect to spend 5-6 hours outside the class to fulfill the requirements of the course.

**Students with Disabilities**

Any student in this course who has a disability that may prevent him or her from fully demonstrating his or her abilities should contact me as soon as possible after the semester begins so we can discuss necessary accommodations to ensure full participation and facilitate your educational opportunities.

**Student Responsibilities**

It is the student's responsibility to obtain notes, know the dates of all exams and deliverable deadlines, and to follow announcements and updates on Blackboard. It is essential for each student to study the course material, participate in class discussions and prepare for quizzes and exams on the designated dates. If you miss a class it is your responsibility to make arrangements to catch up on class notes and any announcements made in class. Please maintain a healthy learning environment by not distracting others or the instructor.

**Academic Dishonesty Policy**

Dishonest academic behaviors are subject to punishment under the School of Management's implementation of the University's *Student Academic Honesty Code*. All students are responsible for submitting their own work for evaluation by the instructor. Submitting work authored or created by others anywhere (including the Web), without appropriate reference and credit, will be treated as academic dishonesty resulting in dismissal from the course.

**Classroom Hours Policy**

Binghamton University's course structure is based on a four credit hour justification. This translates into three in-class hours plus one hour of individual work each week.

**E-mail Policy**

The bulk of any two-way communication outside of class between you and me will be via e-mail. Please ensure that all e-mails are kept professional and courteous as if you are communicating in face-to-face setting. I have a 100-word limitation policy for e-mails. If you cannot explain your situation in 100 words or less, you have to visit my office for a face-to-face communication.

**Make-up Policy**

If you miss an exam and you want the make-up opportunity, you must bring proof of valid reason i.e. a doctor's statement, obituary notice, or jury summons to my office. I will then determine if the make-up opportunity is appropriate. Missing an exam for a University approved event requires a two-week advanced written notice from an appropriate University official.

**Deadline Policy**

None of the activities in this course can be submitted after the deadline.

**White Hat Policy**

Given the subject matter of the course, you are required to abide by certain conditions. These conditions are summarized in the White Hat Agreement form. The form will be provided to you during the first class meeting. You should read, print, sign, and return the form to the instructor by the end of the first week of the semester. Otherwise, you'll not be allowed to take the course.

**Tentative Course Schedule**

| Date | Lecture Topic | Notes |
|---|---|---|
| 01/29 | Course Introduction | - |
| 01/31 | History of Information Security | - |
| 02/05 | Introduction to Information Security | - |
| 02/07 | The need for security: Threats | - |
| 02/12 | The need for security: Attacks | - |
| 02/14 | Application Security | Assignment I due |
| 02/19 | Security Technologies I: Access Control, Physical Security | - |
| 02/21 | Security Technologies II: Firewall, Intrusion Detection | - |
| 02/26 | Security Technologies III: Cryptography | Assignment II due |
| 02/28 | Management of Information Security | - |
| 03/05 | Planning for Contingencies | Project Charter due |
| 03/07 | Information Security Programs, Policies, and Models | - |
| 03/12 | Economics of Information Security | - |
| 03/14 | Exam I | - |
| 03/19 | Introduction to Computer Forensics | Assignment III due |
| 03/21 | Digital Forensics I - Data Acquisition | - |
| 03/26 | No Class | Spring Recess |
| 03/28 | No Class | Spring Recess |
| 04/02 | Digital Forensics II - Working with Windows Systems | - |
| 04/03 | Digital Forensics III - Forensic Analysis | Project Progress Report I due |
| 04/09 | Digital Forensics IV - Forensic Analysis | - |
| 04/11 | Network Forensics I | - |
| 04/16 | Network Forensics II | Project Progress Report II due |
| 04/18 | Image and E-mail Investigation I | - |
| 04/23 | Image and E-mail Investigation II | - |
| 04/25 | Information Systems Auditing and Expert Testimony | - |
| 04/30 | Project Presentations I | Final Project due |
| 05/02 | Project Presentations II | - |
| 05/07 | Project Presentations III | - |
| 05/09 | Exam II | - |
| 05/14 | No Class | Final Examinations Week |
| 05/16 | No Class | Final Examinations Week |