

UNIVERSITY OF WISCONSIN-MADISON
WISCONSIN SCHOOL OF BUSINESS

IS 365/765
Information Security
Fall 2010

BASIC INFORMATION

Professor	Sung S. Kim
Class Meetings	MW 11:00 am – 12:15 pm
Office Hours	W 10:00 – 11:00 am. You do <i>not need</i> a prior appointment to see me. Just drop in. Also available at other times by appointment.
Web	https://mywebspace.wisc.edu/sungkim/class/
Office Location	Room 3120, Grainger
Office Phone	262-3481
Email	skim@bus.wisc.edu

COURSE OBJECTIVES AND DESCRIPTION

The purpose of the course is to provide the student with an overview of the field of information security. The course is divided into three parts:

- **Emerging Threats and Security Technologies** (Software Attacks, Firewall, IDS/IPS, Cryptography, PKI, etc)
- **IS Security Management** (Risk Management, Planning for Security)
- **Case Studies and Guest Speaker Series**

Upon completing this course, students will:

- Have a solid command of the technologies employed in enterprise information security
- Have an awareness of the current legislative and industry compliance challenges facing corporate IT infrastructure management
- Describe the management's role in the development and enforcement of information security policy, standards, practices, procedures, and guidelines.
- Outline the phases of the security systems development life cycle
- Have an in depth understanding of the breadth of the information security field and how information security principles are applied in the enterprise environment

TEXT

Required: M. Whitman and H. Mattord, *Principles of Information Security, 3rd Edition* (Course Technology, 2008).

GRADING POLICY

Exam	100
Quiz	50
Homework Assignment	50
Individual Presentations	100
Team Projects	150
Team-Based Case Analysis	50
Discussion	100
TOTAL	600

Grades will be given on a curve.

EXAM

There will be ONE exam in this course. The exam is closed book and closed notes.

QUIZ

A quiz will be given to test whether you complete reading assignments before class. Alternatively, at the end of class, you may be given a quiz that is intended to test whether you digest the materials discussed in class.

HOMEWORK ASSIGNMENT

The assignment is due at the beginning of class on the date specified. The detailed information on the assignment will be announced in class and will be also available on the class website.

INDIVIDUAL PRESENTATIONS

Each student will pick, summarize, and present a recent news article (or video clip) on information security. No written report is required, but presentation slides need to be submitted. Each student will make a 10-minute presentation and then serve as the facilitator of a 10-minute follow-up discussion.

TEAM PROJECTS

There is a group project required in the course. The project will consist of analyzing an information security technology and making a tutorial video on the technology. More details will be discussed in class

TEAM-BASED CASE ANALYSIS

Each team will analyze TWO case studies. More details will be discussed in class.

DISCUSSION

You are responsible for preparing for class by reading the materials for the class. Your participation and preparation should provide evidence of reading (and understanding) the materials and demonstrate critical thinking skills.

Elements of critical thinking skills include:

- differentiation between fact and opinion
- recognizing and evaluating author bias and rhetoric
- determining cause and effect relationships
- determining the accuracy and completeness of information presented
- recognizing logical fallacies and faulty reasoning
- comparing and contrasting information and points of view
- making judgment and drawing logical conclusions
- establishing relationships among different topics

ATTENDANCE POLICY

Because interaction with the instructor and fellow students is an integral part of the learning process, absences are discouraged. Absences from examinations will result in a grade of zero for that test.

TIPS FOR GETTING A GOOD GRADE IN THIS COURSE

- Read the assigned chapter at least once prior to the lecture.
- Download the PowerPoint slides from the class website and use them to take notes on. You may want to print out the slides from PowerPoint. Typically students print them as “Handouts – 3 per page.”
- Know the key terms at the end of each chapter.
- Attend lecture, take notes and ask questions about anything that is unclear from your reading and/or the class lecture.

- Read the chapter a second time after lecture and go over the notes. If I do not consider a subject important enough to cover in class, I do not consider the subject important enough for an exam topic.
- Work on the projects diligently. Having a good grasp on the project material will assist you when taking an exam.

SCHEDULE FOR IS 365/765

Week	Date	Topics Covered	Readings	Note
1	9/8	Course Overview		
2	9/3	Threats and Attacks	Chapter 2	
	9/15	Threats and Attacks	Chapter 2	
3	9/20	Firewall	Chapter 6	
	9/22	IDS/IPS	Chapter 7	
4	9/22	Cryptography	Chapter 8	
	9/24	PKI	Chapter 8	
5	9/27	Individual Presentations		
	9/29	Individual Presentations		
6	10/4	Risk Management	Chapter 4	
	10/6	Risk Management	Chapter 4	
7	10/11	Project Presentation		(G) Proposal Due
	10/13	Project Presentation		
8	10/18	Planning For Security	Chapter 1	
	10/20	Planning For Security	Chapter 5	
9	10/25	Individual Presentations		
	10/27	Individual Presentations		
10	11/1	Review I		Assignment Due
	11/3	Review II		
11	11/8	No Class		
	11/10	EXAM		
12	11/15	Enron I	Chapter 3	
	11/17	Enron II	Chapter 3	
13	11/22	Case Study: Bookmart		(G) Case Due
	11/24	Case Study: Security Breach at TJX		
14	11/29	Cyber War I		
	12/1	Cyber War II		
15	12/6	Project Presentation		(G) Final Project Due
	12/8	Project Presentation		
16	12/13	Guest speaker		(G) Peer Evaluation
	12/15	Course wrap-up		

Note: This schedule is subject to change.

PROJECT DESCRIPTIONS

Purpose

The purpose of the group project is to provide you with experiences in (1) performing an in-depth analysis of an information security technology and (2) developing a 10-minute video tutorial on the particular technology.

Project Topic

Basically, students are free to choose any topic as long as it is related to information security. A few possible ideas are: wireless security tools, hacking tools, firewalls, packet sniffers, etc. While you are free to choose your own topic, you need to make sure that your research is as practical as possible. Ideally, you will use one of the actual tools and show how it works in practice. The tutorial should include the details of the tool chosen for the group project. After seeing your tutorial, people should be able to use the tool without additional training. I will post the tutorial on the course website. Remember your tutorial will be on the website (practically) forever.

Project Proposal (35 points)

1. Introduction of the project: You will describe the research topic and the rationale for the choice of the topic. Explain why we need to pay attention to the topic.
2. Description of the security technology
3. Commercial tools available on the market
4. Demonstration of a tool
5. Plan for the video tutorial (e.g., what will you have each minute in the video?)
6. I expect about five to seven well-written pages (excluding the demonstration of a tool).

Final Project (45 points)

1. Revised project proposal
2. Description of your video tutorial
3. Your video tutorial

Group Project Presentations

Each team will make two presentations during this semester. These presentations will be worth **40 points (20 points each)**. On the other hand, you, as an audience, are asked to turn in your evaluations of other groups' presentations. The evaluation sheet helps me not only assess the quality of group presentations but also monitor your attendance in presentation days. Please attend the project presentations to avoid losing valuable attendance points (**20 points, 10 points each**). Penalties will be assessed if you miss more than one presentation day.

Peer Evaluation

Each student will submit a confidential evaluation of their group. If these evaluations indicate that one or more group members did not carry their weight, then they will be assigned a lower score for the project accordingly. This peer evaluation will be treated as an assignment with **10 points** value.