

# **Syllabus for IFSM435 (Information Security and E-Commerce)**

## **Course Description**

**Prerequisite:** IFSM 300. An introduction to the four essential elements of safe electronic commerce: the data transaction, the server, the client, and the host network. Topics include encryption, firewalls, transaction security, securing Web commerce, and Web security risk management. Students may receive credit for only one of the following courses: IFSM 435 or IFSM 498H.

## **Course Goals/Objectives**

After completing this course, you should be able to:

- define and describe the infrastructure components of E-commerce
- identify and describe the risks and vulnerabilities of E-commerce
- demonstrate competency in the technical countermeasures addressing E-commerce vulnerabilities
- list and discuss the governmental regulations and guidance on E-commerce
- identify and discuss the privacy and legal issues related to E-commerce
- demonstrate competency in developing E-commerce security management programs

## **Course Introduction**

E-commerce provides us with a paradox – an open system that supports personalization but also raises issues of privacy and security. The object of security is to reduce the effects of threats and vulnerabilities to a level that is tolerable by an organization. What would be considered “tolerable”? In an environment that embraces real customers and false customers, real business and those who do unauthorized listening or perpetrate unauthorized actions, top-level managers, middle-level managers, and operational-level employees must be sensitive to the need to balance security with privacy.

## **Course Materials**

Garfinkel, S., & Spafford, G. (2002). Web security, privacy and commerce (2nd ed.). Sebastopol, CA: O'Reilly Media, Inc.

## **Grading Criteria**

*Section removed.*

## Academic Policies and Procedures

*Section removed.*

## Project Descriptions

The following provide the criteria for class assignments. Grading rubrics will be provided separately.

**Review Assignments:** There will be two review assignments described below.

**Assignment 1: Read a *technical* article from one of the websites in a list of security websites and summarize it.**

The article must be approved by the instructor once chosen

The student will present the review to the class in a 3-5 minute presentation

The presentation must have at least one audio-visual element (PowerPoint, demonstration, diagrams, etc.)

Students and/or instructor will pose at least two questions related to the presentation at the end.

Complete citations must be included.

**Assignment 2: Review a security product or tool and present your review.**

A list of possible security products or tools to review will be provided. Students *may* choose one on their own. The choice must be approved by the instructor.

Students will present the review to the class in a 3-5 minute presentation

Students must have at least one audio-visual element (PowerPoint, demonstration, diagrams, etc.)

Students and/or instructor will pose at least two questions related to the presentation at the end.

**Presentations:** Present a topic to the class that has not been discussed already in class. Discuss the topic and how it manifests itself in the real world.

Topics must be approved by me.

10-20 minute presentation

15-20 slides

Cite references within the slide.

**Research Paper:** Write a research paper on the security topic *of your choosing*.

Topics must be approved by the instructor. Topics can relate to elements discussed in class or topics can be new.

Submit as a Microsoft Word document

Double-spaced, one inch margins, Times New Roman, 12 point font

6-8 pages plus a cover page and references page

Use MLA or APA style documentation. This choice will be discussed in class.

You must use five sources, one of which must come from a professional/academic journal. Consider the credibility of your sources carefully.

No plagiarism!

## Course Schedule

Week	Readings/Assignments	Due Date
1	<b>Web Architecture – Basic Concepts</b> <b>Security – Basic Concepts</b> Read: Chapters 1 and 2 in Garfinkel and chapter 7 in Greenstein & Vasarhelyi	
2	<b>Client/Browser Security</b> <b>Privacy</b> Read: Chapters 12, 13, 22 in Garfinkel and chapter 8 in Greenstein & Vasarhelyi	
3	<b>Cryptography and E-Commerce Security</b> Read: Chapters 3, 4, 6 in Garfinkel	
4	<b>Cryptography and E-Commerce Security (cont'd)</b> <b>Digital Certificates and Public Key Infrastructure (PKI) (cont'd)</b> Read: Chapters 7 & 21 in Garfinkel and chapter 6 in Greenstein & Vasarhelyi	
5	<b>TCP-IP – Background and Security Features</b> Read: Chapters 5 and 17 in Garfinkel and chapter 9 in Greenstein & Vasarhelyi	
6	<b>Presentations</b>	
7	<b>Midterm</b>	
8	<b>Post-midterm Review</b> <b>Network Level Security, cont'd</b>	
9	<b>Network Level Security: Protocol, Hardware and Configuration</b> <b>Midterm Review</b>	

	Read: Chapter 11 in Greenstein & Vasarhelyi	
<b>10</b>	<b>Presentations</b>	
	<b>Web Server Security</b>	
<b>11</b>	Read: Chapters 15, 16, and 18 in Garfinkel and chapter 10 in Greenstein & Vasarhelyi	
<b>12</b>	<b>Digital Payments</b> Read: Chapter 25 in Garfinkel and chapter 12 in Greenstein & Vasarhelyi	
<b>13</b>	<b>Presentations</b>	
<b>14</b>	<b>Presentations</b>	
<b>15</b>	<b>Final Examination</b>	