

E-Commerce Security
ACIS 5584 CRN 10174 Spring 2007
Dr. France Bélanger

Office: PAM 3009

Email: belanger@vt.edu

Phone: 231-6720

Class Hours: TU-TH 8:00-9:15 PAM 3010

Office Hours: TU 9:30-11:30

Please schedule appointments for other times.

Class listserv: ACIS5584_10174@listserv.vt.edu

Catalog Description:

An examination of the concepts, technologies, and applications of security in electronic commerce systems. Topics include the security threats against electronic commerce; tools used by intruders; computing platforms and security; encryption; securing the transaction and the server; detection and responses to attacks; and the future of electronic commerce security.

Prerequisites: ACIS 5514 or BIT 5474.

Course Approach:

This class uses the active learning model in which students become active participants in the learning process. The class includes lecture material, but learning will also occur through student leadership in class discussion, teamwork, and out-of-class preparation. You are expected to attend class and participate in discussions, and to ask questions. You will have access to substantive information from the assigned textbook, readings, and class lectures. However, you will need to complement this information with new knowledge that can be found in news articles and on the Web. With the rapid changes that occur in the world of e-commerce security, and its heightened importance in recent years, no text can be completely up-to-date. If time and schedule permit, guest speakers with substantial information security backgrounds will be invited to speak to the class. In such cases, students will be required to assimilate scheduled material on their own.

Required Texts:

Panko, Raymond, *Corporate Computer and Network Security*, Prentice-Hall: Upper Saddle River, NJ, 2004. ISBN-10: 0-13-038471-2

Wright, Marie and Kakalik, John, *Information Security: Contemporary Cases*, Jones and Bartlett Publishers, Sudbury, MA, 2007. ISBN-10: 0-7637-3819-0.

Other Required Readings (see Blackboard):

(Additional readings may be assigned during the semester)

1. CSI/FBI Security Survey 2006 (Week 1)
2. Smith, A.D. and Rupp, W.T., "Issues in Cybersecurity: Understanding the Potential Risks Associated with Hackers/ Crackers," *Information Management and Computer Security*, 10:4, 2002, 178-183. (Week 4)
3. Wen, H. J. and Tarn, J. M., "The impact of the next generation Internet protocol on e-commerce security," *Information Strategy: The Executive's Journal*, Winter 2001, 22-28. (Week 6)
4. Gordon, Lawrence A., Loeb, Martin P. and Sohail, Tashfeen, "A Framework For Using Insurance For Cyber-Risk Management, *Communications of the ACM*, 45:3, March 2003, 81-85. (Week 12)

Resource:

NIST handbook (see course website)

Grading Policy:

The course grade will be based on the following components:

Examination # 1	100
Examination # 2	100
Topic debate	30
Semester project	100
In the News	10
Case discussions	10
Total Points for Semester:	350

Grades will be assigned as follows:

A (>93%), A- (>90%), B+ (>87%), B (>83%), B- (>80%), C+ (>77%), C (>73%), C- (>70%), D (>60%), and F (<60%).

Examinations: There will be two tests this semester. A mid-term exam will be given approximately half way into the semester and a final test will be given at the end of the semester. Both tests are a mix of essay exams and short answers covering all material, discussions, presentations, and readings for the class. The tests will be open notes, open book format. No makeup exam will be given unless a documented physician approved medical condition occurs (not a visit to the Health Center!).

Topic Debate: Teams of three students will be assigned to debate a topic in class. Some groups will present the “pro” side of the topic while others will present the “con” side. The team will also prepare open ended questions for the other team and the class. Topics will be assigned the second week of class.

Semester Project: A semester long project will be assigned to you in the first weeks of class. The project will be completed in teams of four students. The last two weeks of classes will be reserved for project presentations. Further details will be provided in class.

Case discussions: Cases in the Wright book will be discussed in class. Students will be randomly selected to answer case questions during class.

In The News Assignment: Every student is responsible for presenting a recently published article related to IS security. Details are provided on Blackboard. Students must decide when they will do their presentation. However, a maximum of two students will be allowed to present per class. If students wait too late in the semester, they may not be able to present an article and will lose the assigned points.

Honor Code:

All university policies regarding cheating, **plagiarism**, falsification, nonattendance, and illnesses will be strictly applied. Read your catalog regarding these policies. **The Honor Code will be strictly enforced. Students copying directly from resource material without proper referencing will receive zero for their work and be referred to the Honor court.**

Disability:

If you suffer from a disability and would like to make arrangements for exams, assignments, or projects, please contact the instructor as soon as possible.

TENTATIVE SCHEDULE

	DATES	Topics	Readings	Due
Week 1	1/16-18	Course introduction Security framework	<ul style="list-style-type: none"> • Chapter 1 • CSI/FBI 2006 Survey 	
Week 2	1/23-25	Access control and site security	<ul style="list-style-type: none"> • Chapter 2 • Wright Case 2 	Topic debate assignments
Week 3	1/30-2/1	TCP/IP networking	<ul style="list-style-type: none"> • Chapter 3 	Project groups due 1/30
Week 4	2/6-8	Attack methods	<ul style="list-style-type: none"> • Chapter 4 • Smith & Rupp 2002 	Debate: Biometrics should be used to authenticate students to Banner
Week 5	2/13-15	Firewalls	<ul style="list-style-type: none"> • Chapter 5 	Debate: Firewalls provide the best security protection
Week 6	2/20-22	Host security Ipv6 security	<ul style="list-style-type: none"> • Chapter 6 • Wen & Tarn 2001 	Group topics due 2/22 Debate: UNIX is more secure than Windows XP
Week 7	2/27-3/1	Examination # 1 – 2/28 6-9 PM (tentative)		
	3/6-8	SPRING BREAK (enjoy!!)		
Week 8	3/13-15	Cryptography	<ul style="list-style-type: none"> • Chapter 7 • Wright Case 4 	
Week 9	3/20-22	Cryptographic systems	<ul style="list-style-type: none"> • Chapter 8 	Debate: All emails should always be encrypted
Week 10	3/27-29	Application security	<ul style="list-style-type: none"> • Chapter 9 	Debate: E-commerce should be conducted with SET instead of SSL March 29: Last day to “fire” team members
Week 11	4/3-5	Incident response	<ul style="list-style-type: none"> • Chapter 10 • Wright Case 3 	Debate: All firms should have complete disaster recovery plans
Week 12	4/10-12	Managing security	<ul style="list-style-type: none"> • Chapter 11 • Wright Case 1 • Gordon et al. 2003 	Debate: All small firms should outsource their IS security
Week 13	4/17-19	Boarder picture – security compliance	<ul style="list-style-type: none"> ▪ Chapter 12 ▪ Wright Case 4 ▪ Wright Case 7 	
Week 14	4/24-26	Project presentations		Project reports due 4/23 5:00 PM
Week 15	5/1	Project presentations		