DePaul University
School of Computers and Digital Media

Secure Electronic Commerce
ECT 582 – Fall 2016

In-class Sessions: Thursdays
Loop Campus
Room: 14EAS0082

Instructor: Ellis E. Confer
E-mail: econfer@cdm.depaul.edu
Office Hours: Thursday, 4:00 – 5:30 pm
Office Location: TBA

Course Summary

This course discusses extensions to notions of traditional computer security to include current advancements and issues related to commerce and business conducted over non-proprietary networks. We will specifically concentrate on the Internet as the medium of choice. We will discuss issues of confidentiality, integrity and availability; threats, vulnerability, control and attacks; encryption and decryption; digital certificates and digital signatures; non-repudiation; hacking exploits and incident handling processes; and legal and legislative distinctions between e-commerce and traditional commerce. The course will address e-commerce (consumer to business) and e-business (business to business) as well as the architectural differences that determine particular security solutions. It will also discuss vulnerability concerns and risk mitigation with regards to mobile computing and cloud computing.

This syllabus is subject to change as necessary during the quarter. If a change occurs, it will be thoroughly addressed during class, posted under Announcements in D2L, and sent via email.

Text and Supplementary Reading Materials

- Secure Electronic Commerce, 2nd edition, by Warwick Ford & Michael S. Baum, Prentice Hall, ISBN 0-13-027276-0.
- Other books, articles and web-links will be recommended or supplied as appropriate.

Prerequisites:

DS 425 Distributed Systems Fundamental is considered a prerequisite.
CSC 390 Fundamentals of Information Assurance is also considered a prerequisite.

Learning Outcomes

The following are the minimum course objectives and expected outcomes from the course.

- Students will be able to articulate and explain the primary internet security principles.
- Students will be able to assess and evaluate the impact of prevalent internet and ecommerce security risks.
- Students will develop abilities to analyze specific security risks and risk mitigation techniques consistent with the primary internet security principles.
- Students will be able to install and configure security technology that enables fundamental messaging security and confidentiality risk mitigation strategies.

Grading Procedure

The student's final grade will be based on a weighted average of the homework, exam scores, and class participation. Weights are as follows:

	Weight
HW Assignments	35%
Midterm Exam	30%
Final Exam	30%
Class Participation	5%

Grades will be determined as follows:

92% - 100% A;
90% - 91% A-;
87% - 89% B+;
80% - 86% B;
77% - 79% B-;
70% - 76% C;
67% - 69% C-;
60% - 66% D;
0 % - 60% F.

Procedures and policies:

1. No makeup exams will be given.
2. Homework assignments must be turned in on time on the day and date when the assignment is due for full credit.

   Homework assignments must be turned in on time on the day of class when the assignment is due via D2L or as instructed per the assignment's posted response requirements. Late assignments will be docked two letter grades if turned in during the first week after the initial due date. Thereafter, late homework responses will be docked an additional letter grade for each week that the assignment response is turned in late.

   For example, an assignment response that was turned in within the first week beyond the initial due date will receive a grade of 'C' if the response would have been appraised to be 'A' material. For each week thereafter when the assignment was turned in, the 'C' grade will be reduced by another letter grade.

3. Online Course Evaluations

   Instructor and course evaluations provide valuable feedback that can improve teaching and learning. The greater the level of participation, the more useful the results. As students, you are in the unique position to view the instructor and assess the effectiveness of instruction over time. Your comments about what works and what does not can help faculty build on the elements of the course that are strong and improve those that are weak. Isolated comments from students and instructors' peers may also be helpful, but evaluation results based on high response rates may be statistically reliable.

Your honest opinions about your experience in and commitment to the course and your learning may help improve some components of the course for the next group of students. Positive comments also show the department chairs and college deans the commitment of instructors to the university and teaching evaluation results are one component used in annual performance reviews. The evaluation of the instructor and course provides an opportunity to make voices heard on an important issue – the quality of teaching at DePaul.

Do not miss this opportunity to provide feedback!

4. Academic Integrity and Plagiarism

This course will be subject to the academic integrity policy passed by faculty. More information can be found at http://academicintegrity.depaul.edu/.

The university and school policy on plagiarism can be summarized as follows: Students in this course should be aware of the strong sanctions that can be imposed against someone guilty of plagiarism. If proven, a charge of plagiarism could result in an automatic F in the course and possible expulsion. The strongest of sanctions will be imposed on anyone who submits as his/her own work any assignment which has been prepared by someone else. If you have any questions or doubts about what plagiarism entails or how to properly acknowledge source materials be sure to consult the instructor.

5. Withdrawal

Students who withdraw from the course do so by using the Campus Connection system (http://campusconnect.depaul.edu). Withdrawals processed via this system are effective the day on which they are made. Simply ceasing to attend, or notifying the instructor, or nonpayment of tuition, does not constitute an official withdrawal from class and will result in academic as well as financial penalty.

6. Internet Browsing & Cell Phone Use

Laptop use for internet browsing is NOT allowed in the classroom while the class is in session unless specifically authorized or requested by the instructor for a specific class session. If you bring a cell phone to class, it must be off or set to a silent mode. Should you need to answer a call during class, students must leave the room in an unobtrusive manner. Out of respect to fellow students and the professor, texting is never allowable in class. If you are required to be on call as part of your job, please advise the Instructor at the start of the course.

Assignments

Assignments will be posted in the Assignment section of the class D2L website typically 2 weeks prior to the assignment due date.

All assignments should be submitted via D2L on the assigned due date, unless otherwise noted. All assignments that are submitted after the designated due date will have to be sent to the Instructor as an email attachment. Submitting assignments through D2L ensures that homework responses will be properly time-stamped and delivered. Assignments submitted via email will not date stamped but should be sent with a receipt request to ensure that the assignment was received by the Instructor.

Preliminary Schedule of Discussions

Session Number	Topics
Week 1	**Class Introduction** **Recent Developments in Internet & e-commerce Security**
Week 2	**Fundamental Security Principles** **Security Standards Overview**
Week 3	**Applied Cryptography (or an Overview of Cryptography)** **Digital certificates**
Week 4	**Public key infrastructure (PKI)**
Week 5	**Midterm Exam** **PKI (continued)**
Week 6	**Non-repudiation** **Internet Security** **Hacking Exploits**
Week 7	**Hacking Exploits (continued)** **Incident Handling**
Week 8	**Incident Handling (continued)** **Cloud Computing Security**
Week 9	**Cloud Computing Security (continued)** **Mobile Security** **Application Security**
Week 10	**E-payment Systems** **Ecommerce & Electronic Signature Laws** **Security Architecture Frameworks** **Security Architecture Design Considerations**
Week 11	**Final Exam (No lecture)**