ECT 582
Secure Electronic Commerce
Winter 2004
Sections 801 & 803
W 5:45 – 9:00 pm, CS & T 228

Professor: Robin Burke
Email: rburke@cti.depaul.edu
Phone: 312-362-5910
Office: CS&T 453
Office hours: Mondays 10 am – 1:00 pm and by appointment
Prerequisites: DS 425 (Distributed Systems Fundamentals) or CS 390 (Fundamentals of Information Assurance)
Course web site: http://josquin.cs.depaul.edu/~rburke/courses/w04/ect582/

Description
This course studies technologies, architectures, and infrastructure for securing electronic transactions over nonproprietary networks. From the difference of paper documents and electronic documents to the implementation and maintenance of mechanisms that secure electronic documents with confidentiality, authentication, integrity, and non-repudiation, the focus is on the technologies of public key certificates, digital signatures and internet security.

Course Objectives
At the completion of this course, students should
1. Understand specific security risks associated with E-commerce,
2. Understand the use of cryptography on the internet,
3. Understand the use of digital certificates and signatures,
4. Understand electronic payment systems,
5. Understand the legal aspects of electronic commerce,
6. Be able to describe the basic components of web security,
7. Understand the use of security measures for servers,
8. Understand the need to protect customer privacy, and
9. Understand the special concerns of e-business security.

Readings
Additional readings may be posted on the course website or distributed in class.

Students are also required to read "The Risks Digest" (http://catless.ncl.ac.uk/Risks) every week and to subscribe to and read the CERT Advisory mailing list (http://www.cert.org/).

We will make use of the “Class Forum” feature of Course On-Line website¹. Students are expected to read and participate in discussions there.

Note
The schedule and other information in the syllabus is subject to change. Consult the course home page for the most up-to-date information.

¹ http://dlweb.cti.depaul.edu/
Resources
We will make use of the course discussion forum feature of Course On-Line. This will be particularly important for students in the distance-learning section. All other course information such as lecture notes, assignments and on-line readings will be found on the course web site. I will try to have slides available 24 hours in advance of class, but I cannot guarantee it.

Assessment
Student progress will be assessed through a combination of regular homework assignments and exams. Class participation is also very important in this course and will be evaluated. These components will be weighted as follows:

- Homework: 35%
- Midterm: 30%
- Final exam: 25%
- Active class participation: 10%. (Participation the on-line discussion forum is counted towards class participation.)

Grading of assignments and exams will performed with the following three-part rubric:

- Knowledge: An assignment/exam/project should demonstrate that the student has the expected technical knowledge.
- Reasoning: Assignments should demonstrate that the student can reason appropriately and solve problems.
- Communication: Written work should communicate effectively.

Grades will be awarded as follows:
A: Excellent work. Demonstrates thorough knowledge of the subject matter, going beyond what is covered in class. Contains well-considered and creative solutions to problems. Well-written answers.
B: Very good work. Demonstrates complete knowledge of the subject matter based on coverage in class and textbook. No major errors of reasoning in problem solutions. Competent written answers.
C: Average work. Some gaps in knowledge of subject matter. Some errors or omissions in problem solving. Written answers may contain grammatical and other errors.
D: Below average work: Substantial gaps in knowledge of subject matter. Problem solving incomplete or incorrect. Poor English in written answers.

Tentative Schedule

1/7: Introduction to the course
Reading: Ford & Baum, Ch. 1 & 2
Assigned: Assignment #1:

1/14: Cryptography
Reading: Ford & Baum, Ch. 4
Due: Assignment #1
Assigned: Assignment #2: Cryptography
1/21: Digital certificates
Reading: Ford & Baum, Ch. 6
Due: Assignment #2
Assigned: Assignment #3: Client-side security paper

1/28: Public key infrastructure
Reading: Ford & Baum, Ch. 7 & 10

2/4: Midterm

2/11: Non-repudiation
Non-repudiation of origin, delivery, and submission. Dispute resolution. Electronic signature law and policy.
Reading: Ford & Baum, Ch. 3, 8, 9
Due: Assignment #3
Assigned: Assignment #4: Secure email

2/18: Electronic payment systems
Reading: TBA
Due: Assignment #4
Assigned: Assignment #5: Protocol design

2/25: Internet security
Reading: Ford & Baum, Ch. 5, CSI/FBI Computer Crime Survey
Due: Assignment #5

3/3: WWW security issues
Reading: TBA
Assigned: Assignment #6: Web application analysis

3/10: Privacy
Privacy and electronic commerce. Tensions between security and privacy.
Reading: TBA
Due: Assignment #6

3/17: Final exam

Policies
Students are expected to attend all classes and participate in in-class exercises. Class will start promptly at 5:45 pm. Students are individually responsible for material they may have missed due to absence or tardiness. Attendance is very important in this course. You are responsible for ensuring that you can attend.
Exams can only be made up with a serious documented excuse (e.g. illness, death in the family). A make-up exam must be arranged as soon as possible and always before the student attends the next class meeting. Arrangements involving other excuses require prior permission from the instructor.

Assignments will be posted online. Do not submit assignments by email. **All assignments should be completed and submitted by class time on the due date.** No late assignments will be accepted.

Assignments must represent a student's individual effort. While students are permitted to discuss assignments at the conceptual level, under no circumstances should students share specific answers (electronically or otherwise).

**Distance Learning Policies**

Distance learning students are also expected to contribute to class discussion. Each distance learning student will be expected to contribute the course discussion forum at least twice per week. Your contribution may consist of a discussion question starting a new discussion thread or a substantive response in an existing discussion thread. These questions and postings can be drawn from the reading, current events or your own experience. See handout for examples of substantive and non-substantive participation.

**School Policies**

**Online Instructor Evaluation**

Course and instructor evaluations are critical for maintaining and improving course quality. To make evaluations as meaningful as possible, we need 100% student participation. Therefore, participation in the School’s web-based academic administration initiative during the eighth and ninth week of this course is a requirement of this course. Failure to participate in this process will result in a grade of incomplete for the course. This incomplete will be automatically removed within seven weeks after the end of the course and replaced by the grade you would have received if you had fulfilled this requirement.

**Email**

Email is the primary means of communication between faculty and students enrolled in this course outside of class time. Students should be sure their email address listed under "demographic information" at http://campusconnect.depaul.edu/ is correct.

**Plagiarism:**

The university and school policy on plagiarism can be summarized as follows: Students in this course, as well as all other courses in which independent research or writing play a vital part in the course requirements, 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 a report, examination paper, computer file, lab report, or other 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.

**Incomplete:**

An incomplete grade is given only for an exceptional reason such as a death in the family, a serious illness, etc. Any such reason must be documented. Any incomplete request must be made at least two weeks before the final, and approved by the Dean of the School of Computer Science, Telecommunications and Information Systems. Any consequences resulting from a poor grade for the course will not be considered as valid reasons for such a request.