ECT 582
Secure Electronic Commerce
Fall 2003
Sections 701 & 702
Th 5:45 – 9:00 pm, CS & T 222

Professor: Robin Burke
Email: rburke@cti.depaul.edu
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)

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. 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
In addition, students are required to read "The Risks Digest" (http://catless.ncl.ac.uk/Risks) every week and to subscribe to 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.
Additional readings will be posted on the web.

Note
The schedule and other information in the syllabus is subject to change. Consult the Course On-Line website and the course home page² for the most up-to-date information.

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. In addition to the resources on the Course On-Line

¹ http://dlweb.cti.depaul.edu/
² http://dlweb.cti.depaul.edu/
site, additional information such as lecture notes and assignments can be found on the course home page.\footnote{2} 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%.

**Tentative Schedule**

**9/11:** Introduction to the course
- Reading: Ford & Baum, Ch. 1 & 2
- Assigned: Assignment #1: Course web page

**9/18:** Cryptography
- Reading: Ford & Baum, Ch. 4
- Due: Assignment #1
- Assigned: Assignment #2: Cryptography

**9/25:** Digital certificates
- Reading: Ford & Baum, Ch. 6
- Due: Assignment #2
- Assigned: Assignment #3: Client-side security paper

**10/2:** Public key infrastructure
- Reading: Ford & Baum, Ch. 7 & 10

**10/9:** Midterm

**10/16:** 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

**10/23:** Electronic payment systems
- Reading: TBA

\footnote{2} http://josquin.cti.depaul.edu/~rburke/courses/f03/ect582/
Due: Assignment #4
Assigned: Assignment #5: Protocol design

10/30: Internet security
Transport Layer Security and SSL.
Reading: Ford & Baum, Ch. 5, CSI/FBI Computer Crime Survey
Due: Assignment #5

11/6: WWW security issues
Web authentication and authorization. Web application vulnerabilities. Denial of service. Executable
content: controls, applets, scripts.
Reading: TBA
Assigned: Assignment #6: Web application analysis

11/13: Privacy
Reading: TBA
Due: Assignment #6

11/20: 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 quiz or test 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 at the Course On-Line site 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 expect to submit two discussion questions by 12 noon on each class day (except for week 1
and the midterm). These questions can be drawn from the reading, current events or your own experience.
Questions should be posted as separate threads on the Course On-Line discussion forum.

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 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.