CSC 290A – Network Security

Hofstra University – Fall 2003

Instructor: Vinnie Costa

Phone: (212) 438-3269

E-Mail: vcosta@optonline.net (preferred)
vincent_costa@standardandpoors.com

Class Meets: Tuesday, 8:15-10:05, Adams, Rm: 200

Office hours: Before/after class or by appointment

September 2, 2003

1. Course Overview and Description

Survey of current issues, techniques, software, hardware and architectures related to network security. Examination of the protocols used for Internet services, their vulnerabilities and how they can be secured. Analysis of firewall design, cryptographic techniques, intrusion detection, port scanning, viruses, trojan horses and denial of services attacks. Basic principles of secure networking and application design will be studied and discussed.

2. Required Text

William Stallings, *Network Security Essentials: Applications and Standards – 2/e*, Prentice-Hall, 2003, 432 pp., ISBN 0-13-035128-8

2.1 Reference

William Stallings, *Business Data Communications,* 4/e, Prentice-Hall, 2001, 659 pp., ISBN 0-13-088263-1

Cheswick, W. and Bellovin, S., *Firewalls and Network Security: Repelling the Wiley Hacker*, Addison Wesley, 1994, 306 pp., ISBN 0-201-63357-4

William Stallings, *Cryptography and Network Security: Principles and Practice*, 2/e, Prentice Hall, 1999, 569 pp., ISBN 0-13-869017-0

Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2/e, Wiley, 1995, xxx pp., ISBN 0471117099

3. Grading

There will be several **assignments** during the class, three of these will count towards your grade (you'll get advanced notice). There will also be a **mid-term** and an **end-term** exam. These will be take home exams assigned a week before the due date.

Class participation and involvement counts. This should be an interactive experience. Please feel free to share information and ideas. Be willing to assist others.

The will be a final project or paper due toward the end of the semester. The purpose of this is to encourage extensive research in the network security field.

There will be no makeup tests (mid-term and end-term exams) or extended deadlines. Submitting the test on an alternative date is at the discretion of the instructor, but prior arrangements should be made (unless, in case of emergencies, in which case, proper documents should be provided).

3.1 Point Allocation:

Assignments 1-3: 5% each
Final Project: 30%
Mid-Term: 25%
End-Term: 25%
Participation: 5%

4. Attendance

Attendance will be taken at each class but it is not mandatory. However, if you do not attend class regularly, you will have a high probability of failing. Participation is important to fully appreciate the subject. If you cannot make a class for some reason (travel, business commitments, etc.) try to let me know.

5. Course Outline

Table 1 is a rough outline of the course. This schedule may change depending on the pace of the class and threads of discussion. Assignment dates are not shown here. These will be provided at a later date.

WEEK		Tuesday
1	9/2	Introduction
2	9/9	Cryptography
3	9/16	Cryptography
4	9/23	Authentication Applications
5	9/30	E-Mail Security
6	10/14	IP Security, Networking, Tools
7	10/21	IP Security, Networking, Tools - **Mid-Term Exam Due**
8	10/28	Firewalls
9	11/4	Web Security
10	11/11	Electronic Commerce
11	11/18	Intruder, Viruses and Denial of Service
12	11/25	Network Management Security - **Final Project/Paper Due**
13	12/2	Intrusion Detection / Special Topics
14	12/9	Special Topics/ Review
15	12/16	**End-Term Exam Due**

Table 1: Course Outline

6. Programming Assignments

There may be some programming assignments but these will involve examining and modifiying public domain code. The programs will be graded 80% on correctness and 20% on style (general structure, comments, etc.) Make sure your programs compile and run on the Sun machines in the school lab.

7. Slides, Links and News

I will try to have the slides for each class available on a web site at:

http://www.cs.hofstra.edu/~cscvjc/Fall03

These will be available in HTML and PowerPoint formats. There will also be helpful and interesting links along with news items.

8. Class Rules

- Unless specifically stated otherwise, *assignments are to be completed individually*. You are encouraged to discuss the understanding of a particular issue or class material with fellow students, but code and solutions have to be your own effort.
- *Academic honesty* is to be taken very seriously. If you submit work that references another person's efforts, then you must properly attribute it to that person, otherwise it is plagiarism and you will receive zero credits.
- This is not a course in how to crack systems, it is practically impossible for us to avoid discussing concrete security weaknesses in existing systems. *Any attempt* to use such information to gain *unauthorized access* to any system will be dealt with harshly.