SE-610 Software Systems Security

Fall 2006

Location: HH B1

Time: W 4:30PM – 7:15PM

Instructor:

Jiacun Wang

Email: jwang@monmouth.edu

Office: HH B-12

Office Phone: (732)571-4449

Office Hours: T 3:00 – 4:00, W 1:00 – 2:00, TH 11:00 – 12:00. Other time by appointment.

Course Objectives

The course covers theory and practice of computer security, focusing in particular on the security aspects of the web and Internet. It reviews cryptographic tools used to provide security, such as shared key encryption; public key encryption, key exchange, and digital signature. It then deals with the practice of network security: practical applications that have been implemented and are in use to provide network security. Some common system security issues, such as viruses, intrusion, firewalls, will also be covered.

Textbook

William Stallings, *Cryptography and Network Security: Principles and Practice*, Prentice Hall, 3rd Edition, 2003.

Purchase of this book is required.

Course Work

Homework assignments: There will be 4 homework assignments.

Research projects: Students are expected to make research on a specific area and give a 20 – 30 minute presentation.

Development projects: Development projects are actually big programming projects. I expect security-demanding network programming applications here. For example, electronic voting, writing a plug-in for Netscape messenger or MS Outlook for improved security, online banking, etc. Research-driven projects are also welcome. Depending on the scope, development projects may be done in groups.

Final exam: Open-book.

Grading

Homework	40%
Final exam	20%
Research Project	20%
Development Project	20%

Class Participation

Class participation is strongly recommended. If you miss a class, it is your responsibility to find out what is covered and what announcements are made in the class.

Withdrawal

Last date to withdraw with automatic assignment of a "W" grade, Tuesday November 8, 2005.

Academic Honesty

Everything you turn in for grading must be your own work. Academic dishonesty subverts the University's mission and undermines the student's intellectual growth. Therefore, we will not tolerate violations of the code of academic honesty. Penalties for such violations include suspension or dismissal and are elaborated upon in the Student Handbook.

Special Accommodations:

Students with disabilities who need special accommodations for this class are encouraged to meet with the instructor or the appropriate disability service provider on campus as soon as possible. In order to receive accommodations, students must be registered with the appropriate disability service provider as set forth in the student handbook and must follow the University procedure for self-disclosure, which is stated in the University *Guide to Services and Accommodations for Students with Disabilities*. Students will not be afforded special accommodations for academic work done prior to completion of the documentation process with the appropriate disability service office.

Tentative Course Contents

1. Security overview
2. Symmetric Ciphers
   - Classic Encryption Techniques
   - Data Encryption Standard
   - Advanced Encryption Standard
   - Contemporary Symmetric Ciphers
   - Confidentiality using Symmetric Encryption
3. Public-Key Encryption and Hash Function
   - Public-Key Cryptography
   - Key Management
   - Message Authentication and Hash Functions
   - Digital Signatures
4. Network Security Practice
   - Authentication Applications
   - Electronic Mail Security
   - IP Security
   - Web Security
5. System Security
   - Intruders
   - Malicious Software
   - Firewalls