Syllabus:
CMSC-444/644 Information Assurance
UMBC, Spring 2008

Meeting Time and Place
Mondays, Wednesdays, Fridays 10:00–10:50am, ITE-233.

Instructor
Dr. Alan T. Sherman, Associate Professor of Computer Science, and Director, UMBC Center for Information Security and Assurance (CISA)
www.csee.umbc.edu/~sherman
Office Hours: Wednesdays, 9-10am (while classes are in session), and by appointment, ITE-224 (or ITE-228 Cyber Defense Lab)
email: dralansherman@starpower.net (include “444” or “644” in subject header)
tele: 410-455-2666

Teaching Assistant
None

Course Description
Selected recent research topics in information assurance, such as social engineering, buffer overflow, malicious code, spyware, denial of service, information warfare, computer forensics, recovery and response, enterprise security, clandestine channels and emissions security, security analysis, security models and formal techniques, best practices, and national policy for information assurance. Taking a broad, practical view of security—including people, policies and procedures, and technology—this course will help students devise and implement security solutions that meaningfully raise the level of confidence in computer systems. Required work includes carrying out an original research project. This course will minimize discussion of intrusion detection, firewalls, operating systems security, and mathematical cryptology, which are emphasized in other CMSC security courses.

Prerequisites
CMSC-421 (operating systems) and CMSC-481 (networks); or permission of instructor.

What is Information Assurance?
Information Assurance (IA) encompasses the scientific, technical, and management disciplines required to ensure computer and network security. Information assurance deals with operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation, including operations for the restoration of information systems by incorporating protection, detection, and reaction capabilities. Importantly, information assurance includes and emphasizes availability, detection, and reaction, and not just confidentiality and authentication. Information assurance includes system and network administration and operations, systems security engineering, information assurance systems and product acquisition, cryptography, threat and vulnerability assessment, risk management, web security, operation of emergency response teams, information assurance training, education, and management, computer forensics, and defensive information operations.

Objectives
This course has three main objectives: (1) To introduce students to a broad range of research topics in information assurance, including topics that involve the triad of people, policies and procedures, and technology. (2) To enable students to understand the need for information assurance, identify security vulnerabilities, and devise security solutions that meaningfully raise the level of confidence in computer systems. (3) To help students learn how to read and present research papers, and to carry out new and significant research projects of their own.
**Required Work**

Each student will present recent research papers, carry out and present an original research project of their own (or in a small group), and participate actively in class. In addition, there may be some written assignments, including questions to be answered about presented papers. All requirements will follow the standard expectations of professional researchers in computer science, including the grant proposal process, writing technical reports, making conference presentations, and reviewing research manuscripts. All papers to be presented and project proposals must be approved by the instructor; typically each will be from a high-quality refereed archival research journal or conference. Each project must be focused attempt at making a new and significant contribution to the field; survey papers are not acceptable.

Each student will make three groups of presentations. The first will be on a fundamental topic including an introduction/survey paper and a seminal research paper of very high quality and long-term significance. The second will be a recent reference paper of high quality that serves as a closely-related launching point for your project. The third will be your project presentation. It is suggested, but not required, that your first set of papers be related to the broad area of your project.

Students registered for 444 and 644 will perform the same work, however, with different expectations in the magnitude, difficulty, and originality of assignments—especially the research project. Students in 444 will present at least one paper, whereas students in 644 might be asked to present at least two papers. Also, 644 students will be expected to present more challenging papers. For the project, each student must attempt to solve some original research problem related to one of their paper presentations, with the scope of the project appropriate for 444 or 644.

**Grading Policy**

Grades will be assigned as measures of performance on required activities. Semester grades will be weighted as follows: original research project (60%), paper presentations (30%), class participation (10%). Each required activity will receive a numerical grade, to be interpreted as follows: 90–100 (A), 80–89 (B), 70–79 (C), 60–69 (D), 0–59 (F). There is no final examination. Incomplete grades will be issued only for serious medical reasons, or other such dire emergencies.

**Text**


**References**

Required readings will be recent research articles, such as from the following conferences and journals.

Selected research conferences:
- USENIX Security Symposium
- ACM Conference on Computer and Communications Security (CCS)
- IEEE Information Assurance Workshop at West Point
- IEEE International Information Assurance Workshop
- IEEE Symposium on Security and Privacy (Oakland Conference)

Selected journals:
- ACM Transactions on Information and System Security (TISSEC)
- IEEE Transactions of Dependable and Secure Computing (TDSC)
- IEEE Security and Privacy

**UMBC Center for Information Security and Assurance (CISA)**

The *UMBC Center for Information Security and Assurance (CISA)* has a three-fold mission to promote research, education, and best practices in Information Assurance (www.cisa.umbc.edu). Supported by DoD and CISCO, CISA hosts distinguished lectures and maintains a *Cyber Defense Lab (CDL)* available for student research. Students are encouraged to take advantage of the UMBC CDL.

**Academic Integrity**

```
By enrolling in this course, each student assumes the responsibilities of an active participant in UMBC's scholarly community in which everyone's academic work and behavior are held to the highest standards of
```
honesty. Cheating, fabrication, plagiarism, and helping others to commit these acts are all forms of academic dishonesty, and they are wrong. Academic misconduct could result in disciplinary action that may include, but is not limited to, suspension or dismissal. To read the full Student Academic Conduct Policy, consult the UMBC Student Handbook, the Faculty Handbook, or the UMBC Policies section of the UMBC Directory (or for graduate courses, the Graduate School website)” [from www.umbc.edu/provost/integrity].

One serious type of misconduct is plagiarism, which in its many forms, involves representing someone else’s work as your own. For example, copying homework solutions found on the Internet is misconduct. Buying, selling, acquiring term papers, or facilitating such activities, is also misconduct.

In this course, students are allowed and encouraged to work together while solving problems. However, each student must write up his solution entirely independently, without looking at anyone else’s written solution and without showing anyone his or her written solution.

Students are expected to be familiar with UMBC’s computer usage polices. Students who have enrolled in security courses, including this one, have an especially high responsibility for abiding by these policies. Any such student who violates these policies will be offered no leniency.

Additional Course Information
See separate handouts on course schedule, homework, and research project.