Syllabus
Research Seminar in Cybersecurity, Spring 2014

Instructors
Dr. Matt Bishop, University of California, Davis (UC Davis)
Dr. Brandeis Marshall, Purdue University (PU)
Dr. Tommy Morris, Mississippi State University (MSU)
Dr. Alan T. Sherman, University of Maryland, Baltimore County (UMBC)

Meeting Time
The synchronized distance-education meeting time will be Fridays 1-3pm EST (12-2pm CST, 10am-12 PST).

Course Description
Working in small groups under the mentorship of technical clients from government and industry, each student will formulate, carry out, and present original research on current cybersecurity problems of interest to the nation. Clients will provide a list of unclassified research problems, and students may also suggest their own problems. This course will engage students in important challenging cybersecurity problems. Students will learn how to apply research techniques, think clearly about cybersecurity issues, formulate and analyze potential solutions, and communicate their results.

The course will be run in a synchronized distance fashion from special classrooms coordinating with our partner schools (Mississippi State, Purdue, UC Davis, UMBC) and our technical clients (from NSA and industry). Research groups will collaborate using an appropriate file-sharing technology (e.g., HUBzero). Support for this course is provided in part by the National Science Foundation under grant 1344369.

Credits: 3

Required Work
Working in small teams, each student will carry out an original research project. The main deliverables are a written technical report and an oral presentation describing the team's new and significant findings (similar in form and length to those from technical research conferences such as USENIX Security). Each student is expected to participate actively in class.

Expected Outcomes
By the end of the course, students will be expected to: (1) be familiar with important current cybersecurity challenges, (2) think clearly about cybersecurity issues, (3) formulate and analyze potential solutions, (4) work cooperatively in groups, and (5) communicate results effectively in a technical report and oral presentation.

Grading Policy
Grades will be assigned as measures of performance on required activities. The project will be evaluated on the basis of scientific merit and effective presentation. The project report will count for 45% of the semester grade. Late work will not be accepted. For more details on the grading policy, including the weight of each required activity, and separate expectations for undergraduate and graduate students, see the separate document on assessment policy.

Prerequisites
Each student must have the ability, background, and motivation to carry out original research in cybersecurity. Students are expected to have completed most of the requirements for admission into the MS or PhD program in computer science at UMBC. Students may come from computer science,
computer engineering, or any related technical field (e.g., electrical engineering, information systems, math). Each student is expected to bring significant expertise, interest, and experience in at least one relevant technical area. This course targets primarily MS and PhD students interested in doing research in cybersecurity; qualified undergraduates, MPS (cybersecurity), and special students are also welcome.

Ideally, each student would have completed each of the core courses (or equivalents) in a computer science major (e.g., architecture, operating systems, algorithms, and networks), and at least one course in security. We recognize, however, that many qualified students will not yet have completed all of these courses. Each student must come with sufficient knowledge and skills to be able to contribute to a successful research team in solving some cybersecurity research problem. For school specific detailed information about prerequisites, see the separate document on prerequisites.

Clients
Each team will interact with a technical client a participating company. Confirmed partners include: National Security Agency (NSA) and Assured Information Security (AIS).

Principles
This course rests in part on the following principles. (1) Collaboration—including among industry, government, and different universities—can facilitate learning and the advancement of science and technology. (2) All course activities and deliverables model those of professional cybersecurity researchers. (3) Excellent research bridges both theory and practice. (4) All participants in the course are expected to conduct themselves in their speech, behaviors, and computer interactions with integrity and with respect for others. (5) Facilitate CAE-Rs to find solutions to real-work classified and unclassified cybersecurity problems.

Academic Integrity
Each student is expected to be familiar with, and abide by, the policies of his or her university pertaining to academic integrity and appropriate computer usage. One serious type of misconduct is plagiarism, which in its many forms, involves representing someone else’s work as your own. Buying, selling, acquiring term papers, or facilitating such activities, is also misconduct. Academic misconduct will result in failure of the course and in additional disciplinary action.

``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].

For more information, see:
http://owl.english.purdue.edu/owl/resource/589/01/
http://www.umbc.edu/undergrad_ed/ai/
http://www.honorcode.msstate.edu/pdf/honor-code.pdf

Academic Support
In compliance with and in the spirit of the American's with Disabilities Act (ADA), academic accommodations are made for any student with a documented disability. Any student who believes they may need accommodations in this class are encouraged to contact Student Support Services. For more information, see:
http://www.sss.msstate.edu/
http://www.umbc.edu/sss/
http://www.sss.msstate.edu/
**Recordings**
By enrolling in this course the student acknowledges and grants permission that each class or group session may be recorded (e.g., to facilitate distance education).

**Additional Course Documents**
Various aspects of the course will be described in more detail in additional documents, including: assessment policy, prerequisites, schedule, project, supplemental reading, clients and partner schools, lists of suggested research problems, project presentation feedback, and self assessment.