

Detailed Course Description

1 Course Information

ECS 289M, Introduction to Research in Computer and Information Security

This course engages students in national cybersecurity and information systems security problems. Students will learn how to apply research techniques, think clearly about these issues, formulate and analyze potential solutions, and communicate their results. 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 and information assurance problems of interest to the nation. Support for this course is provided in part by the National Science Foundation under grant #1344369. As part of the award, this course will be run in a synchronized distance fashion, coordinating some activities with our partner schools (Purdue University, Carnegie-Mellon University, Dakota State University, Iowa State University, Mississippi State University, Northeastern University, University of Texas–Dallas, Stevens University, and University of Maryland–Baltimore County) and our technical clients.

1.1 Prerequisites

Each student must have the ability, background, and motivation to carry out original research in cybersecurity and information assurance. Students may come from computer science, computer engineering, or any related technical field (e.g., electrical engineering, information systems, math). Students are expected to have a good background in computer science and some knowledge of computer security. Each student is expected to bring significant expertise, interest, and experience in at least one relevant technical area.

2 Course Work

Working in teams, each student must complete a research project on a focused topic in cybersecurity. The project must aim to accomplish new, significant results (survey papers are not acceptable). Each student must communicate his or her findings in an oral presentation to the class and in a written report in the format of a computer science technical report (about 10–20 pages). Every aspect of the project (including proposals, reviews, reports, and presentations) is intended to match the process that professional computer science researchers follow in carrying out original research.

Project topics may come from lists of problems supplied by government or industrial partners. All proposals must be approved by the instructor.

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). The teams and technical mentors may agree on other deliverables as well. Each student is expected to participate actively in class.

2.1 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.

2.2 Principles

This course rests in part on the following principles.

1. Collaboration — 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. Students at Centers of Academic Excellence – Research (of which UC Davis is one) can find solutions to real-world cybersecurity problems.

2.3 Assignments and Grading

Along with each assignment, we will make the rubric used to grade that assignment available. Typically, it will be on the assignment itself.

The assignments are weighted as follows:

First Quarter (Winter 2015) Assignments and Weighting			
Assignment	Weight	Assignment	Weight
Project bids	10%	Progress report	20%
Project proposal	20%	Progress report presentation	10%
Literature review	20%	Instructor's assessment	20%

Second Quarter (Spring 2015) Assignments and Weighting			
Assignment	Weight	Assignment	Weight
Penultimate report	20%	Final report	40%
Penultimate presentation	10%	Final presentation	10%
		Weekly progress reports	20%

The project will be evaluated on the basis of scientific merit, effective presentation, and appropriateness to the assignment, weighted as follows:

- Scientific merit, 65%;
- Effective presentation, 20%; and
- Quality of any software, hardware, or other engineering artifacts, 15%; if none, scientific merit will be 80%.

Notice that the weekly progress reports are to be submitted to PURR *and* to SmartSite this quarter. They will be graded.

Please submit your work through SmartSite. We will grade it and return the grades, with our comments, on SmartSite.

2.4 Deadlines and Penalties for Late Work

Late work affects others. Peer review is an important aspect of the course, and peer review requires coordinating schedules, including among different universities. Some projects may depend on other projects. To complete the project by the end of the term, it is important to complete each milestone on time. Professional researchers often have deadlines to meet.

If you are one day late, there will be no penalty other than the opprobrium of the instructor and your fellow students. If you are more than one day late, the instructor reserves the right to deduct points — the exact penalty has not yet been determined (but will probably be something like 20% from the full score per day late).

Should you encounter an unanticipated or uncontrollable event that may prevent you from meeting a deadline, please let me know immediately, and request an extension.

3 Expectations for All Work

One of the course outcomes is to communicate effectively with professional audiences of various types. This requires that one take personal pride in their work, and be held accountable for professional quality work. To this end, we expect your submitted work to meet the following requirements.

- Unless otherwise specified, all work should be formatted as if it were being presented to non-technical business managers. Organization, conciseness, formatting, and style count — make an impression!
- Unless otherwise specified, papers must be formatted with one-inch margins and text in at least 10 point font. You are welcome to use an ACM, IEEE, or USENIX format, or any other format that results in output that is easy to read.
- Organization, presentation style, grammar, and spelling will affect your score on the homework. We will deduct points for poorly organized or unprofessional work. This includes spelling and grammar errors, poor word choice, and poor sentence structure.
- if you have writing difficulties or deficiencies, or English is a foreign language for you, please consider using the services provided for free through the Student Academic Success Center — Writing and ESL Support (<http://success.ucdavis.edu/academic/writing.html>).