ECE 499/590 – Cyber-Physical Sytems Security

Department of Electrical and Computer Engineering
George Mason University
Spring 2016

Class Meeting Information: Wednesday, 4:30-7:10 pm
Location: Engineering 1107

Instructor: Lloyd Griffiths
Office: Engineering Building, Room 3206
Phone: 703-993-1729
Email Address: griffiths@gmu.edu
Office Hours: Monday 3-5 pm, Other times by appointment

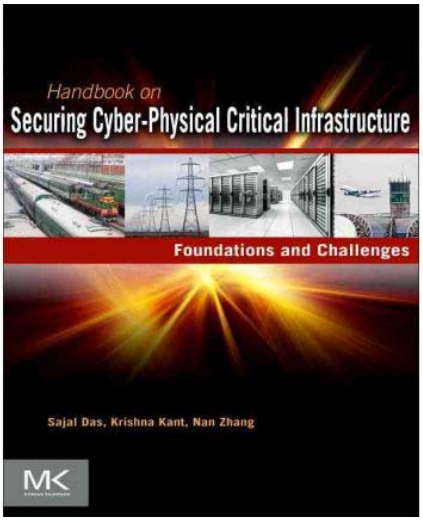
Course Website

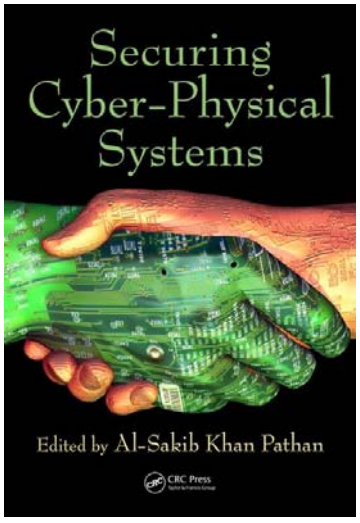
- Go to mymason.gmu.edu and login with your Mason email username and password
- Click on "Courses". Under "Course List", click on: "ECE-590-002 (Spring 2016)"

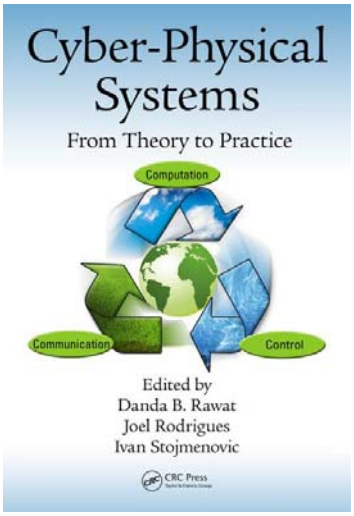
Reading assignments, problem sets, projects, solutions, announcements, and any miscellaneous handouts will be posted on the website.

Recommended Textbooks

1) Sajal K. Das, Krishna Kant and Nan Zhang, *Securing Cyber-Physical Critical Infrastructure*, Elselvier, 2012.
2) Al-Sakib Khan Pathan, *Securing Cyber-Physical Systems*, CRC Press, 2016.
3) Danda B. Rawat, Joel J.P.C. Rodrigues, Ivan Stojmenovic, "*Cyber-Physical Systems: From Theory to Practice*", CCRC Press 2016







Prerequisites

For graduate students enrolling in ECE 590 the prerequisite of the course is prior knowledge in statistics and probability. Undergraduate students may enroll in ECE 499, the prerequisite for the students in this course is STAT 346 and senior standing in the major.

Course Topics

- Foundations of Security
- The Stuxnet Worm and Its impact
- Cloud Computing and Data Security
- Security for Sensor Networks
- Security for Wireless Mobile Networks
- Security for Electrical Power Grids
- Securing Transportation Cyber-Physical Systems
- Automobile Security
- Remotely piloted Drones and Security

Class Attendance

There is no explicit attendance requirement for this course. However, it is expected that you will attend class meetings. It is strongly recommended that you do the assigned reading before coming to class. If you are absent, you are responsible for the material covered during the class and for obtaining notes from another student. Additionally, you are responsible for turning in any assignments due at the beginning of the class period.

Problem Sets

Problem sets will be assigned during the course. Problem sets are due at the beginning of the class period on the due date. No late problem sets will be accepted. Solutions will be posted on the course website.

Problem sets should be written neatly. Pages should be stapled, and problems should appear in order. The instructor reserves the right to return problem sets ungraded if they don't meet these requirements. You are encouraged to work in groups and discuss the assigned problems. However, the work you turn in must be your own. Copying or other forms of cheating will not be tolerated. Copying existing solutions will be treated as a violation of the honor code.

Student Presentations

Students in the class will be divided up into teams of 3-4 members. During the semester, each team will receive assignments involving reading and research of a specific topic. For example: *Security and Privacy in the Smart Grid*. Each team will be required to perform research using existing papers, publications, and web-based information on the assigned topic. Their research will be summarized as a PowerPoint presentation and will be presented orally to the entire class during one class period. All members of the team will be required to participate in the presentation.

Grading

Grading will be determine from the in-class team presentations and from individual assignments that involve preparing a written report on a pre-assigned topic. The latter will be done individually by students throughout the course.

Grade Changes

A request for a grade change for any assignment must be provided to the instructor within two class periods (e.g. two weeks) after the assignment is returned. The request must include the graded assignment in question and a statement describing why a grade change is requested.

Honor Code

All students are expected to abide by the George Mason University Honor Code. Any reasonable suspicion of an honor code violation will be reported.

Grading

Your final score will be based on a weighted combination of your quiz, problem set, project, and exam grades as follows:

- Problem Sets: 20%
- Team Projects: 50%
- Final Project: 30%

Tentative Weekly Schedule

January 20	–	Review of Basic Material Needed for Class
January 27	–	Theoretical Foundations of Security
February 3	–	Mobile Wireless Network Security
February 10	–	Robust Wireless Infrastructure and Mobile Ad Hoc Networks
February 17	–	Security for Sensor Networks
February 24	–	Platform Security
March 2	–	Project Presentations – in Class
March 9	–	Spring Break
March 16	–	Cloud Computing and Data Security
March 23	–	Event Monitoring
March 30	–	SmartGrid
April 6	–	Vehicular Networks
April 13	–	Overview of Class Subject Matter
April 20	–	Final Project In-Class Prresentations
April 27	–	Final Project In-Class Prresentations