ENSE 698C: Cybersecurity for Smart Grid

Course Description

With the rapid growth of smart power grid and the increasing concerns on the grid's security and user's privacy, there is an urgent need of workforce with knowledge on both power systems and security. The traditional courses on power systems cover very limited scope of smart power grids and almost nothing on the security aspect, while a semester-long security course normally struggles to include all the standard security materials and will have little room for power grid security.

This special topic course is created to fill this gap. The course will be jointly taught by faculty in the University of Maryland and researchers from NIST. It will be suitable for graduate students in the system engineering masters program and the electrical and computer engineering department, as well as senior undergraduates.

The course will cover the fundamentals of smart power grid and the necessary background in computer security; a comprehensive study on the potential threats, vulnerabilities, and risks of smart grid; and recent research advances and industrial practices on smart grid cybersecurity. The class will be designed to accommodate a mixture of lectures, paper presentations, in-class discussion, and guest lectures from invited industry/government/academic speakers.

Lecture information

Lecture: MW 5:00 – 6:15 pm EGR 2154

Class URL: http://elms.umd.edu

Class Text: No required textbook.

1. (recommended) Eric Knapp and Raj Samani. Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure. Elsevier Inc. 2013.
2. (recommended) Gilbert N. Sorebo, Michael C. Echols, and Michael Assante. Smart Grid Security: An End-to-End View of Security in the New Electrical Grid. CRC Press, 2012.
3. (recommended) Ross Anderson. Security Engineering: A Guide to Building Dependable Distributed Systems. Second Edition. Wiley Publishing Inc. 2008.
4. Reading materials provided by the instructors.

Instructors:

Primary instructor:

Dr. Gang Qu	ECE/ISR, UMD	gangqu@umd.edu

Office: 1417 A.V. Williams Building
Office hours: MW 10:30 – 11:45 am or by appointment

Guest lecturers:

Dr. DhananjayAnand	NIST	dhananjay.anand@nist.gov
Mr. Jonathan Margulies	Qmulos	margulies@gmail.com
Ms. Victoria Pillitteri	NIST	victoria.yan@nist.gov
Dr. Paul Timmel	NIST	paul.timmel@nist.gov

Prerequisites

ENEE 244 and ENEE 350; or graduate student standing; or permission of the instructor. Background on power systems, computer networks, and/or security is recommended, but not required.

The course will be available for undergraduate students who meet the following requirements:

- Must have earned at least 60 credits and have a cumulative GPA of a 3.0
- Must have successfully completed ENEE244 and ENEE350 with at least a "B-"

Grading Policy

The class will meet twice a week with two 75-minute lectures. No recitation will be held. Course grades will be given based on the followings:

4-6 homework assignments	20%
one midterm exam	40%
one in-class presentation	15%
one final project report/presentation	25%

Course Topics

1. Cybersecurity from system engineering perspectives: information assurance: confidentiality, integrity, authentication, availability, risk management, threats and vulnerabilities, balancing cost, functionality, and security.
2. Smart grid and risk management: background on smart grid: traditional power grid, smart grid architecture, smart grid security threats and reported vulnerabilities.
3. Introduction to computer networks: network architecture, basic routing and switching, networking technologies.
4. Common security tools: firewalls, access control list, virtual private network, intrusion detection system, security information and event management, and anti-virus.
5. Industrial control systems security and tools: real-time, reliability and compatibility, unidirectional gateways, ICS-aware security products.
6. Fundamentals of applied cryptography: symmetric and asymmetric crypto, one-way functions, common applications and implementations.
7. Smart grid cybersecurity:
   a. advanced metering infrastructure security
   b. demand response security issues in smart grid
   c. home area network, gateway, and neighborhood area network security
   d. supervisory control and data acquisition system security
   e. plug in electric vehicles security
8. Smart grid system performance evaluation:
   a. smart grid risks versus benefits
   b. smart grid standards, laws, and industry guidance
   c. smart grid operations, cost of maintenance and support
   d. identifying and recovering grid from cyber-disaster
   e. consumer's role in smart grid