EECE 6580: Computer Network Security (Spring 2017)

Instructor: Prof. Tricia Chigan (Tricia_Chigan@uml.edu)

Lectures:

Wednesday 3:30pm-6:20pm, Ball Hall 412
Office hours: Tuesday 4:00pm-5:30pm, or by appointment
Course Homepage: http://faculty.uml.edu/Tricia_Chigan/Courses/16_658/CNS_Page.html

Required Text:

Network Security: Private Communication in a PUBLIC World, 2nd edition, by C. Kaufman, 2002

Reference Texts:

1) Fundamentals of Computer Security Technology, by Edward Amoroso, 1994
2) Network Security Essentials, 4th edition, by William Stallings, 2010
3) The Practice of Network Security, by Allan Liska, 2003
4) Cryptography & Network Security: Principles & Practices, 4th edition, by William Stallings, 2005
5) Security in Computing, by Charles P. Pfleeger, Shari Lawrence Pfleeger, 2006
6) Research Papers on VANET, Smart Grid, Cognitive Radio Network, Internet of Things, Social Network, and Cloud Computing Security, Cyber Security in Connected and Autonomous Vehicles, Security of Cyber Physical Systems, and Big Data Security and Privacy

Prerequisites:

The students should have already taken a computer network course. Experience on some programming languages (C/C++/Java) is needed.

Course Objective:

This course will cover two categories of topics: One part is the fundamental principles of cryptography and its application to network and communication security in general. This part focuses on the introduction of the fundamental tools in cryptography and the protocols that enable its application to network and communication security. The second part covers the advanced topics on VANET, Smart Grid, Cognitive Radio Network, Internet of Things, Social Network, and Cloud Computing security issues. This part focuses on diverse literature review on the unique challenges (due to the lack of infrastructure, resource constraints and large scalability, etc) faced by MANET/VANET/WSN, Smart Grid, Cognitive Radio Network, Social Network, Internet of Things, or Cloud Computing, Connected and Autonomous Vehicles, and Big Data for security provisioning. The following topics (*tentative*) will be covered (*fundamental topics are in Italic*):

- *Cryptography and its application to network security*
- *Key distribution and management*
- *Security handshake pitfalls and authentications*
- *Well known network security protocols such as Kerberos, IPSec, SSL, PGP& PKI, WEP*
- Threat Model in MANET/WSN/VANET
- Secure routing in MANET/WSN/VANET
- Denial-of-service attacks and countermeasures
- Energy-aware security mechanisms
- Distributed certification authority & self-organized key management
- MAC misbehavior & countermeasures in MANET/WSN/VANET
- Countermeasure selfish attacks and trust establishment in MANET/WSN/VANET
- Location privacy in WSN
- RFID Security
- Cyber-security for Critical Infrastructures (e.g., Power Infrastructure)

- Cognitive Radio Network Security
- Cloud Computing Security
- Social Network Security
- EHealth Security
- Smartphone Security
- Security in Internet of Things
- Cyber Security in Connected and Autonomous Vehicles
- Big Data Security and Privacy

Course Outline and Grading System: The coursework will include homework assignments, 1 midterm exam, the advanced topic presentation, and the course project assignment with the option of the research project or the programming project. The required text "Network Security: Private Communication in a PUBLIC World" covers most of the fundamental topics, the homework, and the exam material. The course reading list provides the material for the advanced topics and the research projects option.

Class Attendance	5%
Homework	20 %
Midterm Exam	30 %
Advanced Topic Presentation	20 %
Course Projects & Presentation	25 %

Notes: A: 90% or above; AB: 85~90% ; B: 80~85%; BC: 75~80%; C 70~75%

More On Advanced Topic Presentation: Each team of 2 students will be required to give a 60-minute presentation on one advanced topic on security issues of the emerging areas of MANET/VANET/WSN, Smart Grid, Cognitive Radio Network, Internet of Things, Social Network, or Cloud Computing Security Issues, Cyber Security of Connected and Autonomous Security, and etc. The presentation should follow the style of teaching fellow students on the selected topic. The finalized list of the advanced topics will be provided by the instructor by the end of the 4th week. The students have to choose their topics by the end of the 6th week. The topic bidding procedure will follow the First Come First Serve rule. The presentation slides draft is due 1 week before the scheduled presentation date.

More on Course Project: Students can choose to work either on a research project or the programming project of 2 implementation tasks (10% and 15% respectively). The research project focuses on one or more aspects of the open security issues in areas of MANET/VANET/WSN, Smart Grid, Cognitive Radio Network, Internet of Things, Social Network, and Cloud Computing security issues, etc. The research project topics and programming project assignments will be distributed on the 4th week followed by an in-class discussion. Each research project will include project proposal, design and implementation, and final report (with demo or short in-class presentation). 3 working phases of the research project together contribute to the total of 25% of the final grades.

- Phase I (5%): 1 page project proposal
- Phase II (5%): 2~3 pages mid-term report
- Phase III (15%): 7~10 pages final report; In-class final presentation (and demo)

Often a research project will demand performance evaluation via simulations. The programming project option includes 2 implementation assignments. You are allowed to use any programming language (C/C++/Java, ns2, OPNET, etc) for your project implementation.