(Tentative)

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

Lectures:
Tuesday 6:30pm-9:20pm, Ball Hall 328
Office hours: TW 2:00pm-3:30pm, or by appointment
Course Homepage: Coming soon!

Required Text:

Reference Texts:
1) Fundamentals of Computer Security Technology, by Edward Amoroso, 1994

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 MANET (including VANET), WSN, Smart Grid, Cognitive Radio 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, or Cloud Computing 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
- Secure routing in MANET
- Denial-of-service attacks and countermeasures
- Energy-aware security mechanisms
- Distributed certification authority & Self-organized key management
- MAC misbehavior & countermeasures in MANET
- Countermeasure selfish attacks and trust establishment in MANET
- Distribution and revocation of cryptographic keys and light-weight security primitives
- Security bootstrapping & secure neighbor discovery in WSN
- Secure data aggregation in WSN
- Location privacy in WSN
- Cognitive radio network security
- Smart Grid security
- Social network security
- Cloud Computing security issues

Course Outline and Grading System: The coursework will include homework assignment, 1 midterm exam, 1 advanced topic presentation, and 1 course project assignment with the option of research-oriented project or programming-based implementations. 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-oriented course project option.

<table>
<thead>
<tr>
<th>Homework</th>
<th>20%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Midterm Exam</td>
<td>30%</td>
</tr>
<tr>
<td>Advanced Topic Presentation</td>
<td>20%</td>
</tr>
<tr>
<td>Course Project &amp; Presentation</td>
<td>30%</td>
</tr>
</tbody>
</table>

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

More On Advanced Topic Presentation: Each student will be required to give a 50 minutes presentation on one advanced research topic in the area of MANET/VANET, WSN, Smart Grid, Cognitive Radio Network, Social Network, or Cloud Computing security issues. 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 slide draft is due 1 week before the scheduled presentation.

More on Course Project: Students can choose either to work on a research-oriented project (up to 2 students are allowed to form a project team) or to work on programming-based projects individually. The research-oriented project focuses on one or more aspects of the open design issues in the area of MANET/VANET, WSN, Smart Grid, Cognitive Radio Network, and Cloud Computing security issues. The research-oriented project topics and programming-based project(s) assignment will be distributed on the 4th week followed by an in-class discussion. Each research-oriented project will include project proposal, design and implementation, and final report (with demo or short in-class presentation). 3 working phases of the research-oriented project together contribute to the total of 30% of the final grades.

  Phase I (5%): 1 page project proposal
  Phase II (5%): 2~3 pages mid-term report
  Phase III (20%): 6~10 pages final report; In-class final presentation (and demo)

Often a research-oriented project will demand performance evaluation via simulations. The programming-based project option may include up to 2 implementation assignments. You are free to use whatever programming language (C/C++/Java, ns2, OPNET, etc) for your project implementation.