EE5723/EE4870: Computer & Network Security (Spring 2008)

(Tentative)

Instructor: Dr. Tricia Chigan (cchigan@mtu.edu)

Lectures:
MWF 9:05-9:55am, EERC 218
Office hours: MW 10:00am-11:00am, or by appointment
Course Homepage: http://www.ee.mtu.edu/ee/faculty/cchigan/EE5723-Security/index.html
Course Mailing List: ee5723-l@mtu.edu & ee4870-l@mtu.edu

Required Text:

Reference Texts:
3) Research Papers on MANET & WSN Security

Course Objective:
This course will cover two categories of the topics: One 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 and WSN security. This part focuses on diverse literature review on the unique challenges (due to the lack of infrastructure and severe resource constraints) faced by MANET and WSN networks for security provisioning. The following topics (tentative) will be covered:
- 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
**Course Outline and Grading System:** The coursework will include homework assignment, 1 midterm exam, 1 advanced topic presentation, and 1 research project. The required text "Network Security: Private Communication in a PUBLIC World” covers most of the fundamental topics and the homework material. The course reading list provides the material for the advanced topics and the course project.

<table>
<thead>
<tr>
<th>Term</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework</td>
<td>20 %</td>
</tr>
<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 60-minute presentation on one advanced research topic in the area of MANET and WSN security. 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 3rd 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:** Up to 2 students are allowed to form a project team working on a research project. Each project focuses on one or more aspects of the open design issues in the area of MANET and WSN security. Project topics 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 and) presentation. 3 working phases of the 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%): 8~10 pages final report; In-class final presentation (and demo)

Often a research project will demand performance evaluation via simulation. You are free to use whatever programming language (C/C++/Java, ns2, OPNET, etc) for your project implementation.