EE5900-01: Computer & Network Security

(Spring 2005)

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

Lectures:

TR 9:35-10:50am, EERC 216
Office hours: TR 11:00am-12:00pm, or by appointment
Course Homepage: http://www.ee.mtu.edu/ee/faculty/cchigan/EE5723-Security/index.html
Course Mailing List: ee5900-l@mtu.edu

Required Text:

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

Course Objective:

• Learn fundamentals of cryptography and its application to network security.
• Understand network security threats, security services, and countermeasures.
• Acquire background on well known network security protocols such as IPSec, SSL, WEP.
• Understand vulnerability analysis of network security.
• Acquire background on hash functions; authentication; firewalls; intrusion detection techniques.
• Gain hands-on experience with programming and simulation techniques for security protocols.
• Obtain background for original research in network security, especially wireless network and MANET security.
• Understand the tradeoffs and criteria/concerns for security countermeasure development.

Course Outline:

The coursework will include reading assignment, homework, programming project/term paper, and two exams. As a graduate level course, in addition to the basic material covered in the lectures, the course project and term paper are designed to motivate the students' further interests on the state-of-the-art technologies and research topics within the network security community. The required text "Network Security: Private Communication in a PUBLIC World" covers most of the lecture and homework material. The supplemental material (research papers, articles, Standards, and URLs)
related to the course will be provided via the course webpage.

**Evaluation/Grading:**

<table>
<thead>
<tr>
<th></th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Homework</td>
<td>20</td>
</tr>
<tr>
<td>2 Exams</td>
<td>40</td>
</tr>
<tr>
<td>Project/Term paper</td>
<td>30</td>
</tr>
<tr>
<td>Class Participation</td>
<td>10</td>
</tr>
</tbody>
</table>

Notes:

1. Active class participation contributes to 10% of the final grades.
2. Midterm: 20%; Final: 20%. The exams will be closed book/notes.
3. For the project, 3 work phases together contribute to the total of 30%. Phase I, 5%; Phase II, 10%, Phase III, 15%

   A 90% or above
   AB: 85–90%
   B: 80–85%
   BC: 75–80%
   C 70–75%

**More on Project/Term paper:**

Each student is required to complete a mid-size project individually, which includes proposal, implementation, and final demo or paper.

- Can be but not limited to
  - Design of new security algorithms or protocols
  - Analysis/evaluation/comparison of existing algorithms or protocols
  - New attacks/vulnerabilities in algorithms or protocols
  - Must have novel contribution in terms of Research/Simulation/Implementation

- Deliverables
  - Phase I: proposal (as document)
  - Phase II: mid-term report (as powerpoint slides, and document)
  - Phase III: Final demo/report (as a document); Presentation
  - Critique of other’s projects

Tentative Project topics (subject to update) include but are not limited to:

- Intrusion detection in ad-hoc networks, 2G/3G/4G networks
- Novel Threats/attacks/Vulnerabilities in wireline/wireless networks
- Public key infrastructure implementation for wireless networks
- Intrusion tolerant in wireline/wireless networks
• Key distribution and management in MANET
• Investigate and develop suitable metrics for Threat Index, Security Index
• Characterize and define cost-benefit functions and analysis approach for various security services associated with different implementation options at different protocol layers.
• Techniques to address distributed denial of service attacks
• Secure group communication/Multicast security
• Security considerations in sensor networks
• Secure network management systems
• Use of redundancy (multipaths in ad-hoc networks) to enhance security
• Cross-layer network attacks and mitigation
• Secure Routing protocols/Transmission protocols for wireless network
• Implementation of secret key cryptography
• Implementation of public key cryptography
• Developing new attack methods
• Analysis of security protocols (e.g, IPSec, and WEP implemented in different networks)
• Design of new authentication protocols
• Theoretical study and modeling of network security

The project could be a programming based implementation with final demo, or an academic paper with your own proposed mechanism, protocol, and algorithm. You are free to use whatever programming language (C/C++/Java, ns2) to work on your project. The academic term paper requires literature study on the latest development/research issues with your own findings and proposed work. The finalized project topics will be distributed on the week of Feb. 7th. Check out http://www.ee.mtu.edu/ee/faculty/cchigan/EE5723-Security/projects-Spring05.html for the most updated information.

Course Policies & Notices:

  o Attendance of the lectures is strongly recommended. The instructor is not responsible for the material covered in your absence. If you have a legitimate reason for the absence of any lecture session, please let me know BEFORE the lecture session.
  o The course mailing list is ee5900-l@mtu.edu. All registered students should be able to access this mailing list. Course announcements such as schedule changes and changes on any assignments will be posted via this mailing list. It is the students’ responsibility to keep up to the most updated announcements.
  o Homework assignment and its due date will be distributed via the course mailing list and posted on the course webpage. Late assignment will be penalized 20% of the earned points for each class day. Exceptions to this rule will only be made for cases brought to the instructor’s attention PRIOR to the due date.
  o I will answer questions regarding assignments in office, lecture and via email. However, I will cease to respond to an assignment 24 hours prior to the due date.
  o Discussions on the assignments are allowed, however, copying or representing someone else’s work or any forms of cheating may cause a grade of F as the penalty.