EE 599/699-002 CYBERSECURITY

Spring 2015

[Home] [Syllabus]

News

This course has an external class website at http://www.vis.uky.edu/~cheung/courses/ee599/index.html where the lecture notes will be posted. The Blackboard (Bb) site http://elearning.uky.edu will have the other course material.

Instructor: Dr. Sen-ching Cheung (cheung at engr.uky.edu)
Office: DMB 217 (218-0299)
Office hours: Make an appointment

Teaching Assistant: Zhaohong Wang (zhaohong dot wang at uky dot edu)

Lecture

TTh 9:30am-10:45pm (FPAT 265)

Course Description

This course is about cyber-security, which focuses on protecting infrastructure, networks, programs and data from unintended or unauthorized access, change or destruction. As information systems, databases, and Internet-based distributed systems and communication become pervasive, cyber-attacks and digital spying eclipse terrorism to become the top threat to national security. Cyber-security education has emerged as a national goal in the United States and other countries, with implications to both national defense and homeland security.

The goals of this course is to provide an up-to-date survey of developments in cyber-security through study of the theoretical foundation and hands-on practical implementation. Topics covered will include basic security technology, cryptography, security management, risk assessment, operations and physical security, software and network security, as well as ethical and legal issues. A key emphasis of this course is on hands-on experiments which will include encryption/decryption, authentication and authorization protocols, network protection approaches including firewalls and intrusion detection systems, as well as operating systems and application vulnerabilities, exploits, and countermeasures.

Expected outcomes of student learning

- Understand and discuss the concept of cyber-security management
Perform risk assessment of a cyber-system
- Analyze different methods of attacking and defending cyber-systems
- Understand basic cryptographic primitives
- Understand and discuss the concepts of network security and secured protocols
- Explain the legal and ethical issues of cyber-security

Grading

<table>
<thead>
<tr>
<th>Your grade will be based on:</th>
<th>Weights</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Lab exercises</td>
<td>40%</td>
</tr>
<tr>
<td>Midterm, Final</td>
<td>30%</td>
</tr>
<tr>
<td>Final Competition</td>
<td>30%</td>
</tr>
</tbody>
</table>

1. Homework and Laboratory Exercises
   - They will be assigned roughly weekly.
   - While we will discuss homework in class, each student must do his or her homework.
   - Late homework will not be accepted without prior notice.
2. Midterm and Final
   - Online exams in the style of CISSP (Certified Information Systems Security Professional) certification.
   - Closed book and you can take it at home
3. Final Competition
   - It is a team project of two-three students.
   - All teams will participate in a Capture-the-Flag (CTF) that involves hacking and defending a realistic system.
4. Grade Assignment
   - The letter grade assignment is based on the following scale: from 100 to 90 pts => A, from 89 to 80 pts. => B, from 79 to 70 pts => C, from 60 to 69 pts. => D, from 59 to 0 pts. => E.
5. Plagiarism
   - I have a zero-tolerance policy for all forms of plagiarism, from copying a homework answer from your friend or solutions from previous terms to cheating in the exams. Not only you will lose all the points for that assignment, the incident will also be reported to the Department Chair who will determine the appropriate disciplinary action.

Required Text

<table>
<thead>
<tr>
<th>Required Text</th>
<th>Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Singer and Friedman. <em>Cybersecurity and Cyberwar: What Everyone Needs to Know</em>ctice, Oxford, 2013 (optional but highly recommended – Kindle version costs less than two Grande Mocha from Starbucks!)</td>
<td>Selected papers provided by the instructor</td>
</tr>
</tbody>
</table>

Programming Assignments

There is a fair amount of simulation assignments throughout the semester. Basic familiarity of the Unix system is required. We will apply the knowledge from the class in realistic security scenarios, attacking or defending
real servers on the DeterLab testbed for security experimentation. The DeterLab testbed is a general-purpose experimental infrastructure that supports research and development on next-generation cyber security technologies. The testbed allows repeatable medium-scale Internet emulation experiments for a broad range of network security projects, including experiments with malicious code. We will get you accounts on the DeterLab network. For this purpose, your names and email addresses (first.last@uky.edu) will be forwarded to the DeterLab administrator. Furthermore, we will also use an ensemble software of cryptosystems and cryptanalysis tools called Cryptool in learning different types of encryption, hashing, and digital signatures. DeterLab testbed can be accessed via any ssh connection and Cryptool runs on Win32 platform.

---

**Prerequisites:**

This course is suitable as an elective for electrical engineering, computer engineering or computer science seniors and graduate students. Good working knowledge of the following courses or equivalent is required:

1. EE 380 Computer Organization
2. EE 586/CS 571 Computer Networking (desirable)
3. CS 470 Operating System (desirable)