SYLLABUS

CSE 350/450 Cyber Defense&Offense

Fall 2016
Location: Christmas-Saucon Hall 203
Time: 1:10pm—2:25pm (TR)

Instructor: Dr. Yinzhi Cao PA 380
Office Hours: 2:30pm—3:30pm Thursdays (Except for holidays)

I. Course Aims:
Students will have an overall knowledge of network security threats & vulnerabilities, learn some techniques & tools for detecting, responding to, and recovering from security incidents. For graduate students, they also learn how to critique others' papers in this area and present own ideas/views via written technical reports.

II. Description:
In this class, you will learn most popular vulnerabilities, such as buffer/heap overflow and cross-site scripting, as well as how to attack and penetrate software with such vulnerabilities. You will also learn to use publicly available tools for detecting, responding, and recovering from security incidents. This class will also cover the techniques used in the real world for detecting and responding to network intrusions. Newly proposed research techniques will also be discussed.

III. Grading Procedures: Grades (105% =100% + 5% (bonus)) will be based on:
Undergraduate (CSE 350): Homework (35%), Paper Summary (10%), Paper Presentation (10%), Class Participation (10%), Class Project (40%, mid-term presentation 10%, final presentation 15%, report and deliverable 15%).
Graduate (CSE 450): Homework (10%), Paper Summary (10%), Paper Presentation (20%), Class Participation (10%), Class Project (55%, mid-term presentation 10%, final presentation 20%, report and deliverable 25%) .

Important: Homeworks and deliverables are collected at the beginning of class on the due date. If your assignment arrives after this time, it is marked late. Late penalties are 10% for the first 24hrs, 20% for up to 2 days late, 30% for up to 3 days late, 40% for up to 4 days late. No assignment is accepted when it is more than 4 days late.

Paper summaries are due 24 hours before the class. Late penalties are 10% for the first 24hrs, 40% for up to 2 days late. No summary is accepted when it is more than 2 days late.

Presentation slides (for paper and projects) are due 48 hours before the class. Please adhere to the rule. Late penalties are 50% for the first 24hrs.

IV. Paper Summary Format:

A paper summary should summarize the paper sufficiently to demonstrate your understanding, should point out the paper's contributions, strengths as well as weaknesses. Think in terms of what makes good research? What qualities make a good paper? What are the potential future impacts of the work? Note that there is no right or wrong answer to these questions. A summary's quality will mainly depend on its thoughtfulness. Restating the abstract/conclusion of the paper will not earn a top grade. In particular, it should cover all of the following aspects:

1. What is the main result of the paper? (One or two sentence summary)
2. What strengths do you see in this paper?
3. What are some key limitations, unproven assumptions, or methodological problems with the work?
4. How could the work be improved?
5. What is its relevance today, or what future work does it suggest?

V. Paper Presentation:

Each presentation will be divided into two teams: defense and offense. The defense team will present for 35mins, including but not limited to the following facts of the paper:

(1) What are the compelling motivations for the stated work?
(2) What are the major contributions over state-of-the-art work in the literature?
(3) How does the paper achieve their stated goals?

The defense team is welcome to look at and borrow useful contents from the original authors' slide when making their own. The defense team should be well prepared for possible critiques from the offense team.

The offense team will present for 20mins, including but not limited to:

(1) What are the limitations in the paper's motivation, e.g., narrow scope?
(2) What are the technical limitations of the paper? For example, will the technique cause false positives or negatives? If it is a defense paper, can an attacker evade the defense; if it is an attack paper, can the attack be deployed in real-world environment?
(3) What are the possible improvements or future work of the paper? If you were the authors of the paper, what would you do instead?

Then, both teams will be following up arguments, and then other students will question either team for clarification or add to discussions. The instructor may ask students to comment based on their paper summaries.

VI. Class Projects:

A class project team will be consisted of 2-3 students. For research-oriented projects, each team will have a meeting with the instructor every other week. For other projects, the team is also encouraged to schedule meeting(s) with the instructor.

Undergraduate students are allowed to form a team themselves, but are encouraged to team up with graduate students. In the case that a team is of only undergraduate students, they should vote a team leader who will be responsible for submitting weekly report.

The format and time for mid-term and final presentation will be announced later once teams are formed.

The topics for class projects will be announced in the class.

VII. Academic Integrity:
Academic integrity is crucial for the pursuit of knowledge. Please refer to Lehigh's policy of academic integrity (http://www.lehigh.edu/~inprv/faculty/academicintegrity.html) for reference.

VIII. Accommodations for students with disabilities:
If you have a disability for which you are or may be requesting accommodations, please contact both your instructor and the Office of Academic Support Services, Williams Hall, Suite 301 (610-758-4152) as early as possible in the semester. You must have documentation from the Academic Support Services office before accommodations can be granted.

IX. The Principles of Our Equitable Community:
Lehigh University endorses The Principles of Our Equitable Community [http://www.lehigh.edu/~inprv/initiatives/PrinciplesEquity_Sheet_v2_032212.pdf]. We expect each member of this class to acknowledge and practice these Principles. Respect for each other and for differing viewpoints is a vital component of the learning environment inside and outside the classroom.