SYLLABUS

CSE 343/443 Network Security

Fall 2015
Location: PA 258
Time: 1:10pm—2:25pm (TR)

Instructor: Dr. Yinzhi Cao PA 380
Office Hours: 3:30pm—4:30pm Thursdays (Except for holidays)

I. Course Aims:
To 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 will be based on:
Undergraduate (343): Homework (40%), Paper Summary (10%), Class Participation (10%), Class Project (40%, mid-term presentation 20%, final presentation 20%)
Graduate (443): Paper Summary (15%), Paper Presentation (20%), Class Participation (10%), Class Project (55%, mid-term presentation 10%, final presentation 20%, weekly report and deliverable 25%)

Note:
For undergraduates, if you participate in one paper presentation, you will obtain additional 10%.
For graduates, if you finish homework 1&2, you will obtain additional 10%.

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.

Weekly reports for graduate students are due at the beginning of Tuesday class. 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.

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 30mins, 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 25mins, 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 one graduate student and one or two undergraduate students. The graduate student will be the team leader, and responsible for submitting weekly report. For research-oriented projects, each team (at least the team leader) will have a weekly meeting with the instructor. For other projects, the team is also encouraged to schedule a weekly meeting 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, University Center C212 (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. Tentative Course Schedule

Date	Lectures Topics	Presenter	Assignment
Tue 8/25	Class overview, motivation and overview of computer security	Dr. Yinzhi Cao	
Thu 8/27	Software Vulnerability I	Dr. Yinzhi Cao	
Tue 9/1	Software Vulnerability II	Dr. Yinzhi Cao	HW1 Shellcode out
Thu 9/3	Software Vulnerability Paper Presentation	TBA	
Tue 9/8	Web Security and Privacy I	Dr. Yinzhi Cao	
Thu 9/10	Web Security and Privacy II	Dr. Yinzhi Cao	HW1 Shellcode in
Tue 9/15	Web Paper Presentation I	TBA	HW2 Buffer overflow out
Thu 9/17	Web Paper Presentation II	TBA	
Tue 9/22	Mobile Security and Privacy I	Dr. Yinzhi Cao	
Thu 9/24	Mobile Paper Presentation I	TBA	
Tue 9/29	Mobile Paper Presentation II	TBA	HW2 Buffer overflow in
Thu 10/1	Mobile Paper Presentation III	TBA	
Tue 10/6	Software-defined Network (SDN)	Dr. Yinzhi Cao	
Thu 10/8	SDN Paper Presentation	TBA	
Tue 10/13	Pacing Break		
Thu 10/15	Mid-term Project Presentation	TBA	
Tue 10/20	TLS/SSL	Dr. Yinzhi Cao	HW3 XSS out
Thu 10/22	TLS/SSL Paper Presentation I	TBA	
Tue 10/27	TLS/SSL Paper Presentation II	TBA	
Thu 10/29	Social Network Security and Firewalls	Dr. Yinzhi Cao	HW3 XSS in

Tue 11/3	Social Network Security Paper Presentation	TBA	HW4 Firewall out
Thu 11/5	Machine Learning Security I	Dr. Yinzhi Cao	
Tue 11/10	Machine Learning Security Paper Presentation I	TBA	
Thu 11/12	Machine Learning Security Paper Presentation II	TBA	
Tue 11/17	Machine Learning Security Paper Presentation III	TBA	HW4 Firewall in
Thu 11/19	Privacy	Dr. Yinzhi Cao	
Tue 11/24	Privacy Paper Presentation	TBA	
Thu 11/26	Holiday		
Tue 12/1	Final Project Presentation I		
Thu 12/3	Final Project Presentation II		