Course Overview

Presenter: Yinzhi Cao
Lehigh University
Who am I?

- Yinzhi Cao
- It is kinda like [yihn jee] [chow]
- If you feel that it is really difficult, call me Ian.
- My research focuses on cyber-security, such as web security and mobile security.
- I am a new assistant professor in CSE department.
Course Logistics (1)

Course web site: http://www.yinzhicao.org/courses/f15/cse343443/
Course Email: cse343443@gmail.com
Office Hours: Thursday (3:30pm – 4:30pm)
Half lecture + half seminar
In the lecture, I (Yinzhi Cao) will teach basic cyber security concept.
In the seminar, you (students) will learn how to present, defend, and offend a research paper.
Course Logistics (2)

CSE 343 (Undergraduate Students):

- Homework (40%)
- Paper Summary (10%)
  - You can miss two without penalty
- Class Project (40% = 20% mid-term Presentation + 20% final Presentation)
- Class Participation (10%)
- Paper Presentation (+10%, optional)
Course Logistics (3)

- CSE 443 (Graduate Students)
  - Paper Presentation (20% = 10% + 10%)
  - Paper Summary (15%)
    - You can miss two without penalty
  - Class Project (55%)
    - Mid-term Presentation 10%
    - Final Presentation 20%
    - Weekly report and final deliverable 25%
  - Class Participation (10%)
  - Homework (HW1+HW2, optional, +10%)
Paper Summary

- Summarize the paper sufficiently to demonstrate your understanding.

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

Due 24 hours before the class

- Late penalty: 10% for the first 24hrs, 40% for up to 2 days
- You can miss two without penalty
Paper Presentation

Two teams: defense and offense.

- The defense team: 30mins
  - What are the compelling motivations for the stated work?
  - What are the major contributions over state-of-the-art work in the literature?
  - How does the paper achieve their stated goals?

- The offense team: 25mins
  - What are the limitations in the paper’s motivation?
  - What are the technical limitations of the paper?
  - What are the possible improvements or future work of the paper?

- Discussion between two teams and the rest of the class.
Paper Presentation Cont’d

* Presentation slides are due 48 hours before the class.
  - Please adhere to the rule!
* You are welcome to look at and borrow contents from the authors’ original slides (especially for defense team).
Homework

- HW1 shellcode (10%) due Sept 10th
- HW2 buffer overflow (15% = 7%+5%+3%) due Sept 29th
- HW3 cross-site scripting (9%) Due Oct 29th
- HW4 firewall (6%) Due Nov 17th

All dues are at the beginning of that day’s 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.
Class Projects

A team with

- Graduate students
  - Responsible for weekly report (due at the beginning of Tuesday class)
  - Responsible for weekly meeting (for research project, please schedule a time with the instructor)
  - Responsible for final report and deliverable (due by the end of the semester)
  - Mid-term and Final Presentation

- One or two undergraduate students
  - Participate in the project and finish the assigned task(s) from the graduate students
  - Mid-term and Final Presentation
Class Schedule Overview

http://www.yinzhicao.org/courses/f15/cse343443/schedule.html
Paper Presentation Pitching
Class Project Pitching and Forming Teams

- Team 1:
- Team 2:
- Team 3:
- ...
Class Participation

- Attending the class
- Raising questions during the paper presentation
Why Cyber-security? (1)

The past decade has seen an explosion in concern about information security

- G-20 countries recently urged to treat cyber-attacks as threat to global economy.
- G20 have lost 2.5 million jobs to counterfeiting and piracy, and lost $125 billion annually to cyber-attacks.
Why Cyber-security? (2)

Security specialist markets are expanding!

- “Salary Premiums for Security Certifications Increasing” (Computerworld 2007)
  - Up to 15% more salary
  - Demand is being driven not only by compliance and government regulation, but also by customers who are "demanding more security" from companies
Why Cyber-security? (3)

It is in the everyday news:

- The Office of Personnel Management (OPM) Hack: Sensitive personal information of roughly 21.5 million people from both inside and outside the government.
- Sony Picture Entertainment Hack: 47,000 unique Social Security numbers
- Target Data Breach: 40 million credit cards
- And so on and on...
What is Cyber-security?

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. – Wikipedia

CIA Triad

- Confidentiality
- Integrity
- Availability
Confidentiality

Confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes”.

Attacks: Package Sniffing, Phishing, Password Attacks

Defense: e.g., Access Control
Integrity

- Data integrity means maintaining and assuring the accuracy and completeness of data over its entire life-cycle.
- Attacks: Man-in-the-middle attacks, Session hijacking attacks,
- Defense: e.g., TLS/SSL
For any information system to serve its purpose, the information must be available when it is needed.

**Attacks:** Deny-of-Service Attack (DOS, e.g., SYN flood attacks and ICMP flood attacks), Distributed Deny-of-Service Attack (DDoS)

**Defense:** Increase bandwidth and decrease processing time
In addition to CIA (1)

- **Authenticity**
  - Authenticity is assurance that a message, transaction, or other exchange of information is from the source it claims to be from.
  - E.g., password, single sign-on
- **Accountability**
- **Non-repudiation**
- **Reliability**
In addition to CIA (2)

- Authenticity
- Accountability
  - Accountability is the property that ensures that the actions of an entity can be traced solely to this entity.
  - E.g., use MAC and IP address to track a physical machine
- Non-repudiation
- Reliability
In addition to CIA (3)

- **Authenticity**
- **Accountability**
- **Non-repudiation**
  - Nonrepudiation is the assurance that someone cannot deny something, such as the receipt of a message or the authenticity of a statement or contract.
  - E.g., Digital Signature
- **Reliability**
In addition to CIA (4)

- Authenticity
- Accountability
- Non-repudiation
- Reliability

  Reliability is the property of leading to consistent intended behavior and results.