CSE597B: Special Topics in Network and Systems Security

Course Introduction

Dr. Sencun Zhu

The Instructor

- Dr. Sencun Zhu, Asst. Prof. CSE&IST
- Email: szhu@cse.psu.edu
- Web: http://www.cse.psu.edu/~szhu
- Office: 338F, IST Building
- Tel: 814-865-0995
- Office hours: Thursday 10:00-12:00am
- Course meeting times: TR 1:00-2:15pm
- Meeting place: TBA

Course Objective

- Understand the basic issues, concepts, principles, and mechanisms in security
  - Introduction to modern cryptography
- Know the state of the art of some of the hottest research areas
  - Read papers in advanced topics
- Prepare students for research in network and systems security
  - Project with the goal of publishing in peer reviewed (and hopefully major) conferences
Overview of Modern Cryptography

- Security Objectives
- Symmetric key encryption
- Public key cryptography
- Authentication and identification
- Hash functions
- Pseudo-random numbers
- Classes of attacks and security models
- And more…

Advanced Topics

- Group key management for secure multicast
- Broadcast authentication
- Wireless mobile ad hoc network security
- Sensor network security
- P2P and overlay network security
- Intrusion Detection
- Anti- Spam
- Anti-DDoS
- Worm, Untrusted Code
- Grid computing security
- AI-based security
- Privacy-preserving data mining and Privacy Issues in RFID

May not be able to do all the above, subject to our progress

Major Conferences

- Security
  - The best
    - ACM Computer and Communications Security (CCS), IEEE
      Symposium on Security & Privacy
  - The good
    - ISOC NDSS, USENIX Security Symposium
- Cryptography
  - Crypto, Eurocrypt
- Networking
  - The best
    - ACM Sigcomm, ACM Mobicom
  - The good
    - ACM: SenSys, MobiHoc
    - IEEE: Infocom, ICNP, ICCDS
Prerequisite

- Enforced
  - Networking
  - Operating system
- Necessary for great success
  - Programming skills
  - Scientific writing
  - Motivation
  - Hardworking

Textbooks and Papers

- No textbooks
- Reference books
  - Handbook of Applied Cryptography by Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone (http://www.cacr.math.uwaterloo.ca/hac/)
  - Practical Cryptography by Niels Ferguson, Bruce Schneier
- Papers and Slides
  - Links in the course syllabus

Course Resources

- Course website
  - http://www.cse.psu.edu/~szhu/teach/cse597b
  - For course materials, e.g., papers, homework, project assignment.
  - Check frequently for updates
- Angel
  - For discussions, Q&As, surveys
Course Format

- I will lecture the first six (or so) classes
- For each of the paper reading classes
  - One to two papers to read
  - You must read, write, and turn in a review
    - Review form will be given
    - What you like about the paper
    - What you do not like about the paper
    - How can the paper be improved (optional)
    - Review will be graded
  - Two discussion leaders

Course Format(2)

- Discussion Leaders
  - Collaborate, may play different roles
  - Read all the assigned papers and give reviews
    - Should send (by email) reviews to the instructor two days before the class
    - Should list at least three questions you consider worth of discussion
  - Summarize the class discussion and make it available in class website

Project

- Group
  - 2~3 students
  - Working alone must be justified
  - Roles can be negotiated inside the group
- Topics
  - Should be relevant to the class
  - Each group can come up with one
  - The instructor can also give topics
    - Available soon
Documents for Project

- Proposal
  - At least 3 pages
  - Including the problem, the importance, preliminary literature study, proposed approach, the evaluation method, time plans
- Milestone
  - At least 6 pages
  - Detail the proposal write-up
- Final Paper
  - At least 10 pages
  - Should be a complete research paper

Presentation

- Proposal
  - 5 minutes
  - Including motivation, idea
- Final
  - 12 minutes
  - Including motivation, clear idea, important results, contributions compared to related work

Grading

- Project
  - 45%
- Homework
  - 5%
- Paper review
  - 20%
- Discussion leader effort
  - 10%
- Participation
  - 5%
- Class presentation
  - 15%