Lecture 1 - Overview

CSE497b - Spring 2007
Introduction to Computer and Network Security
Professor Jaeger

www.cse.psu.edu/~tjaeger/cse497b-s07/
From small vulnerabilities come ...
People are part of the problem ...
And the rest ...

• Hardware
  – E.g., Ford Pinto
  – E.g., ext2

• Physical Access
  – E.g., ATMs

• Users
  – E.g., Phishing
  – E.g., Social engineering
  – E.g., Misplaced trust
Where is all of this going?

• We are at a unique point in history.
  – We have little security.
  – We have little usable theory on what is secure.
  – We have little knowledge of how to get it.
  – Workable tools are rudimentary, but sometimes effective.

• However, we have a huge amount of risk riding on computer and network security.
  – Financial
  – Medical
  – Personal ...

• Every computing system we use is insecure ...
This course …

• We are going to explore the tools that the address these frequent and expected vulnerabilities.

  – Why are we doing so poorly in computing systems at protecting our users and data from inadvertent or intentional harm?

The answer: stay tuned!
This course is an applied *applied systems* course covering introductory topics in computer and network security. We will investigate the tools and problems of contemporary security:

This course provides an *introduction to the theory and application of security in computer and network environments*. Students will develop the skills necessary to formulate and address the security needs of enterprise and personal environments. The course will begin by describing the goals and mechanisms of security as motivated by recent incidents in the area. Topics will cover cryptography, authentication, secure programming, security in operating systems, network security, secure storage, access control, denial-of-service, and file systems, and conclude with emerging trends in secure systems design.
You need a basic understanding of …

• IP Networks
• Operating Systems
• Discrete Mathematics
• Basics of systems theory and implementation
  – E.g., File systems, distributed systems, networking, operating systems, ....
• Programming in C/Linux
Why are we here? -- Goals

• Our goal: **to provide you with the tools to apply current and future approaches to computer security.**
  – Formulating a security strategy
  – Basic technologies
  – Engineering trade-offs

• **This is going to be a hard course.** The key to success is sustained effort. Failure to keep up with readings and assignments will likely result in poor grades, and little understanding of the course material.

• **Pay-off:** security competence is a necessary, rare, valuable skill
Course Challenges

• Security is relative
  – Good understanding of other computer technologies are necessary

• Security is terminology
  – Each application of security has different terms for concepts

• Security is defensive
  – Consider the function available to the attacker not the user
Course Materials

• Website - We are maintaining the course website at http://www.cse.psu.edu/~tjaeger/cse497b-s07
  – Course assignments, slides, and other artifacts will be made available on the course website.

• Course textbooks
Course Calendar

- The course calendar as all the relevant readings, assignments and test dates
- Please check the website frequently for announcements and changes to the schedule. **Students are responsible for any change on the schedule** (we will try to make announcements in class).
Grades

- Grading policy
  - 20% Mid-term exam (3/8, 6:30-7:45, 113 IST)
  - 35% Course Projects (6-7)
  - 15% Quizzes and Class Participation
  - 30% Final exam (end of semester)

- Lateness policy - Assignments are assessed a 10% per-day late penalty, up to a maximum of 4 days. Unless the problem is apocalyptic, don't give us excuses. Students with legitimate reasons who contact the professor before the deadline may apply for an extension.
Ethics Statement

This course considers topics involving personal and public privacy and security. As part of this investigation we will cover technologies whose abuse may infringe on the rights of others. As an instructor, I rely on the ethical use of these technologies. Unethical use may include circumvention of existing security or privacy measurements for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Exceptions to these guidelines may occur in the process of reporting vulnerabilities through public and authoritative channels. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class.

When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse under any circumstances unless you have received explicit permission from Professor Jaeger.
And the rest of this course …

• Outline
  1. Overview
  2. Basics
  3. Cryptography
  4. Network Security
  5. Application Security
  6. Systems Security
  7. Policy
  8. Misc Topics