CMPSC443 - Introduction to Computer and Network Security

Module: Introduction

Professor Patrick McDaniel
Spring 2009
Some bedtime stories …
People are the problem.

- I have seen the enemy and it is us.
  - Walt Kelley (Pogo)
This course

• We are going to explore why these events are not *isolated, infrequent*, or even *unexpected*.

• 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 a systems course covering general topics in computer and network security. We will investigate the tools and problems of contemporary security. Topics will include:

- network security, authentication, security protocol design and analysis, key management, program safety, intrusion detection, DDOS detection and mitigation, architecture/operating systems security, security policy, group systems, biometrics, web security, language-based security, and other emerging topics (as time permits)
You need to understand ...

• IP Networks
• Modern Operating Systems
• Discrete Mathematics
• Basics of systems theory and implementation
  ‣ E.g., File systems, distributed systems, networking, operating systems, ....
Goals

- My goal: *to provide you with the tools to understand and evaluate research in computer security.*
  - Basic technologies
  - Engineering/research trade-offs
  - How to read/write/present security research papers

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

- Pay-off: security competence is a rare, valuable skill
Course Materials

- Website - I am maintaining the course website at
  - http://www.cse.psu.edu/~mcdaniel/cse543-s09/

- Course assignments, slides, and other artifacts will be made available on the course website.

- Course textbook
Course Calendar

• The course calendar as all the relevant readings, assignments and test dates

• The calendar page contains electronic links to online papers assigned for course readings.

• Please check the website frequently for announcements and changes to the schedule. Students are responsible for any change on the schedule (I will try to make announcements in class).
Grading

• The course will be graded on exams, assignments, a final course project, and class participation in the following proportions:

  35%  Course Assignments
  25%  Mid-term Exam
  30%  Final Exam
  10%  Class Participation
Collaboration

• **All assignments are to be completed be each student independently.** Any collaboration not explicitly allowed by Prof. McDaniel is a violation of the class rules and will result in dismissal from the class and an assignment of an 'F' grade. Please review the Academic Integrity Policy below for more information.
Readings

• There are a large amount of readings in this course covering various topics. These assignments are intended to:
  ‣ Support the lectures in the course (provide clarity)
  ‣ Augment the lectures and provide a broader exposure to security topics.

• Students are **required** to do the reading!

• *About 10-20% of questions on the tests will be off the reading on topics that were not covered in class.* You better do the reading or you are going to be in deep trouble when it comes to grades.
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 and or institution.

• When in doubt, please contact the instructor for advice. Do not undertake any action which could be perceived as technology misuse anywhere and/or under any circumstances unless you have received explicit permission from Professor McDaniel.
Academic Integrity Policy

• Students are required to follow the university guidelines on academic conduct at all times. **Students failing to meet these standards will automatically receive a 'F' grade for the course--no second chances or explanations will be accepted.** The instructor carefully monitors for instances of offenses such as plagiarism and illegal collaboration, so it is very important that students use their best possible judgement in meeting this policy. The instructor will not entertain any discussion on the discovery of an offense, and will assign the 'F' grade and refer the student to the appropriate University bodies for possible further action.

• Note that students are **explicitly forbidden to copy anything off the Internet** (e.g., source code, text) for the purposes of completing an assignment or the final project. Also, students are forbidden from discussing or collaborating on any assignment except were explicitly allowed in writing by the instructor.
Assignment #0 (Due 1/15)

• Please review these slides and the website policies and send the instructor an email acknowledging that you have read and agree to these policies.

• Example:

To: mcdaniel@cse.psu.edu
From: xxx111@psu.edu
Subject: CMPSC443 Course Policy (Spring 2009)
I have read and understand the course policies regarding grades, integrity and ethics. I accept these policies and commit to behaving within the letter and spirit. I further understand that any failure to act within these policies with result in the reception of an ‘F’ for the course.

-Student Van Hauten
Assignment #1 (Due 1/27)

• You will be completing assignment #1 which teaches you how to use cryptographic functions. Please review handout in class.
  • You will need to find a UNIX machine to work on.
  • Bo will help you with this if you need it.
  • Bo is going to provide some slides on using make and tar
OK, what is security?

• In class: define online security?
  ‣ Be prepare to discuss:
    • Explain why you think this definition is correct.
    • What are the objective criteria for security?
    • Name a couple of secure applications/systems?
What is security?

• Garfinkel and Spafford (1991)
  ▸ “A computer is secure if you can depend on it and its software to behave as expected.”

• Harrison, Ruzzo, Ullman (1978)
  ▸ “Prevent access by unauthorized users”

• Not really satisfactory – does not truly capture that security speaks to the behavior of others
  ▸ Expected by whom?
  ▸ Under what circumstances?