Course Introduction

Professor Patrick McDaniel
CSE545 - Advanced Network Security
Spring 2011
Network Security

• No really good definition, so we will accept the following for this course:

  The study of the security of systems, applications, infrastructure, and tools that relate to computer-based communication.

• Implication

  › Networks: physical layer, protocols, and flows
  › Applications: how they are designed and
  › People and Policy: how do we use these system and what kinds of security do we need?
Topic Areas

1. Secure network communication
2. Routing security
3. Multiparty secure communication
4. Privacy Preserving communication
5. Telecommunications security (cellular, VoIP)
6. Cell Phone Security
Why are we here? -- Goals

• Our goal: to provide students with the tools to perform research in:
  ‣ Evaluating network security techniques
  ‣ Designing network security solutions
  ‣ Attacking network infrastructure
  ‣ Developing analysis methods

• This is going to be a time-consuming 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: network security research competence is a necessary, rare, valuable skill
Course Materials

• Website - We are maintaining the course website at:
  
  http://www.cse.psu.edu/~mcdaniel/cse545-s11/

• Course assignments, slides, and other artifacts will be made available on the course websites.
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).
Evaluation Policy

• Grading
  ‣ 45% Course Projects
  ‣ 20% Mid-term (in class - 3/3/10)
  ‣ 25% Final Exam
  ‣ 10% Course participation

• 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 me excuses. Students with legitimate reasons who contact the professor before the deadline may apply for an extension.
Course Projects

• This class will assign 5 C++ programming assignments that require the student to build a working protocol stack (in user-space) on top of a distributed system framework.

• **Note:** The assignments must be carried out without any assistance or discussion between students (no sharing of information with anyone inside the class or outside of it is allowed).

• **Note:** No code can be copied from any source, including old assignments, the Internet, textbooks, etc. Any instance of this conduct will be considered plagiarism.
Exams

- There will be two exams, a mid-term and a final. This is about 1/2 the grade for the class and should be taken very seriously.
  - Exams will cover readings, lectures, discussions, and assignments.
  - The final will be cumulative with an emphasis on the material appearing after the mid-term.
  - Closed note and book.
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.

Any instance of sharing of plagiarism, copying, cheating on tests, or other disallowed behavior will constitute a breach of ethics and will result in dismissal from the class with a failing grade.

Students are responsible for reporting any violation of these rules by other students, and failure to constitutes a ethical violation that carries with it similar penalties.

When in doubt, please contact the course professor 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.
Dear Professor McDaniel,

I have read and understand the ethics statement provided on the course website and accept its terms. I understand that all assignments and tests must be carried out without any assistance or discussion between students (no sharing of information with anyone inside the class or outside of it is allowed). I understand that any instance of sharing, plagiarism, copying, cheating on tests, or other disallowed behavior will constitute a breach of ethics and will result in my dismissal from the class with a failing grade. Students are responsible for reporting any violation of these rules by other students, and failure to constitute a ethical violation that carries with it similar penalties.

- ***INSERT STUDENT NAME***, ***INSERT DATE***
Assignment #1

• (see handout)
Network Security Questions

• How is this different than other types of security?
• Is the distinction between network security and other types of security meaningful any more?
• Is there anything more to study?
Network Security

- Network security covers a spectrum of security from global protections to single port firewalls.

  Smaller
  - Host Security (Personal Firewalls)

  Enterprise Security (VPNs)

  Global Security (BGP)

  Larger

- This course will sample from amongst these.
Network vs. Web

• The network is a service ...
  ‣ A conduit for data to be passed between systems.
  ‣ Layers services (generally) to allow flexibility.
  ‣ Highly scalable.
  ‣ This is a public channel.

• The Web is an application
  ‣ This is an application for viewing/manipulating content.
  ‣ The services are unbounded by services, e.g., Java.
  ‣ This can either be public (as in CNN’s website), or private (as in enterprise internal HR websites).
The E2E Argument

• **Idea**: most systems require end-to-end communication service, but low-level features have costs (performance) incurred by all users ... thus ...

• It is important that the features provided at a low level remain very simple ... yielding ...

  Smart endpoints ... dumb minimal network

• **Consequence**: the network is simple and not very receptive to new (often complicated) security services being added into them. Need to implement security as a service (e.g., bump in the stack--IPsec)
Challenges

• The network is ...
  ‣ administered unevenly and often poorly
  ‣ hard to change
  ‣ very simple
  ‣ unreliable
  ‣ ...
Security Terms

- Guarantees
  - Confidentiality
  - Integrity
  - Non-repudability
  - Availability

- Attacks
  - Passive vs. active
  - Denial of service
  - Traffic analysis

Make sure you have these in your head!
Recent CERT Reports

- Vulnerability Note VU#159528
  - What happened?
  - Why?
  - Fix?

- Vulnerability Note VU#251133
  - What happened?
  - Why?
  - Fix?

- Vulnerability Note VU#261869
  - What happened?
  - Why?
  - Fix?
Next meeting

• Bring laptop: in class laboratory to setup VMs and get a jump on assignment #1