Introduction
CS 239
Advanced Topics in Network Security
Peter Reiher
April 5, 2004

Outline

- Subject of class
- Class topics and organization
- Reading material
- Class web page
- Grading
- Projects
- Office hours

Subject of Class

- Problems and solutions in network security
- Concentrating on unsolved problems and recent research
- Mostly on wide area infrastructure
- Not really on securing your LAN or individual machine
- Intended for students with serious research interest in network security

Class Organization

- Graduate level seminar class
- Concerning topics of ongoing research in network security
- Based around group discussions
  - Not formal lectures

A Typical Class

- Someone (usually one of you) will spend 15-20 minutes outlining a topic
- Remainder of class will be spent discussing it
- Whoever presented it should lead discussion
- Generally, everyone will lead a discussion at some point

Topics to Be Covered

- IP spoofing
- Routing security
- Secure DNS
- Secure wireless ad hoc networks
- Security for ubiquitous networks
- DDoS defense
- Worm defense

More Topics

- Secure multicast
- Evaluating network defenses
- Handling spam
- Anonymization and privacy
- Security alert systems
- Secure interactions with untrusted systems

Assigning Topics

- I’ll take the first class (on IP spoofing)
- Each of you should volunteer to take one of the others
- To be decided at the end of second class
- First come, first served

Reading Material

- No textbook
- 3-5 papers for each class
  - Some selected by me
  - Some by class leader
- Papers will be made available on class web page
- In some cases, web pages may be used instead of papers

Class Web Page

- http://www.lasr.cs.ucla.edu/classes/239_2.spring04
- Will show class schedule
- And list papers for each class
  - With links to them
- Other useful information also there

Grading

- 20% midterm
- 40% class participation
- 40% project
- No final exam

Midterm Exam

- Essay questions based on material in first half of class
- Probably three questions
- Open notes
  - Including papers

Class Participation

- Covers both class you lead (15%) and participation in other classes (25%)
- Not graded on brilliance
- But on involvement and ability to contribute to discussion
- If you can’t regularly attend this class, you won’t do well in it

Leading a Class Discussion

- Should focus on:
  - Analysis of the problem
  - Critiques of existing solutions
  - Suggested improvements to those
    - Or new solution approaches
- Think of it as being part of a research team looking at this problem
- Goal is to spark a discussion
  - Not to spend two hours reviewing the papers that were assigned

Slides for Presentations

- Not required, but a good idea
- If possible, send them to me ahead of time
  - So I can post them on the web page
- I’ll bring a projector to every class

Class Projects

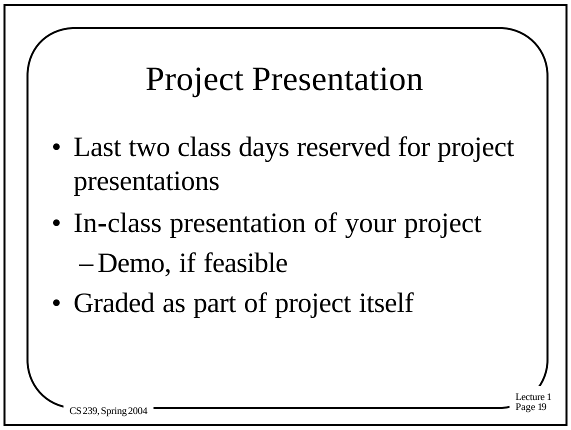
- Half of your grade
- Group projects (2-3 people)
- On some topic involving network security
- Must be a research topic
  - Not just implementing known stuff

Project Proposals

- Project proposals due at end of 3d week of class (April 23)
- 1-page summary of what you want to do
- Can be submitted as hard copy or email
- Not graded, but required

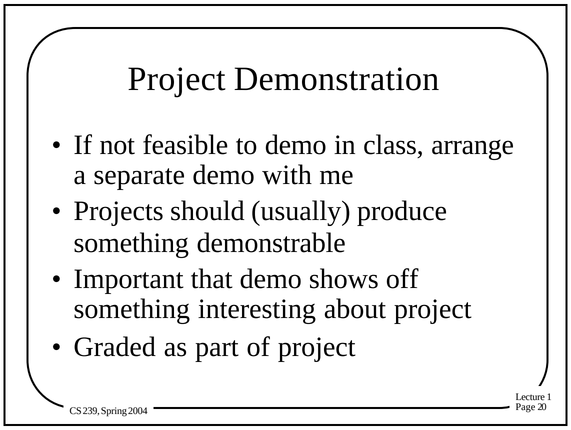
Project Status Reports

- Due at end of 7th week of classes (May 21)
- 1-3 page summaries of the progress you’ve made to that date
  - Hint: there should be some
- Hard copy or email OK
- Not graded, but required



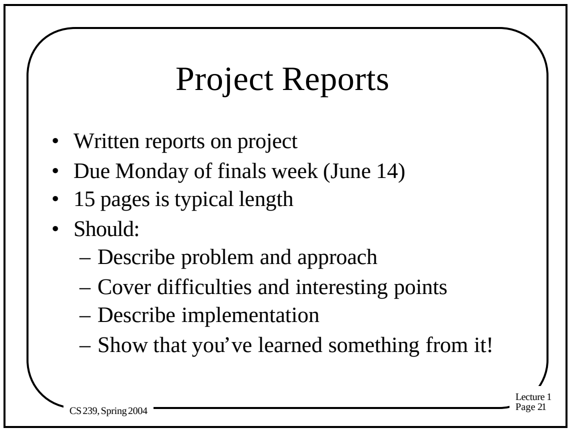
Project Presentation

- Last two class days reserved for project presentations
- In-class presentation of your project
  - Demo, if feasible
- Graded as part of project itself



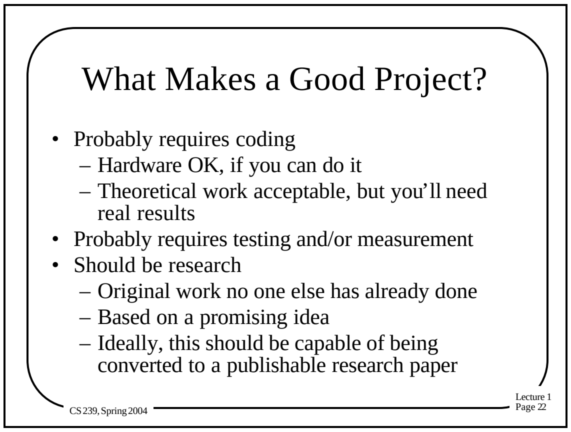
Project Demonstration

- If not feasible to demo in class, arrange a separate demo with me
- Projects should (usually) produce something demonstrable
- Important that demo shows off something interesting about project
- Graded as part of project



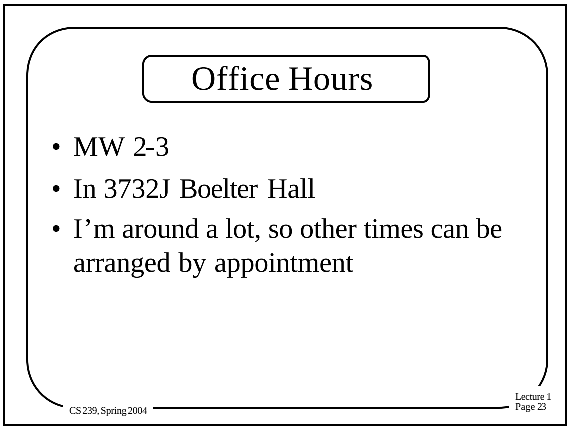
Project Reports

- Written reports on project
- Due Monday of finals week (June 14)
- 15 pages is typical length
- Should:
  - Describe problem and approach
  - Cover difficulties and interesting points
  - Describe implementation
  - Show that you’ve learned something from it!



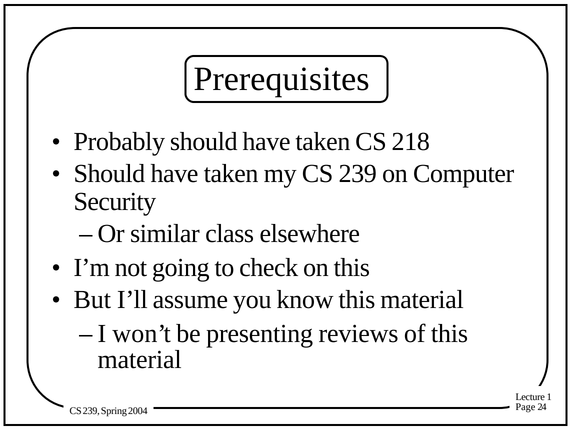
What Makes a Good Project?

- Probably requires coding
  - Hardware OK, if you can do it
  - Theoretical work acceptable, but you’ll need real results
- Probably requires testing and/or measurement
- Should be research
  - Original work no one else has already done
  - Based on a promising idea
  - Ideally, this should be capable of being converted to a publishable research paper



Office Hours

- MW 2-3
- In 3732J Boelter Hall
- I’m around a lot, so other times can be arranged by appointment



Prerequisites

- Probably should have taken CS 218
- Should have taken my CS 239 on Computer Security
  - Or similar class elsewhere
- I’m not going to check on this
- But I’ll assume you know this material
  - I won’t be presenting reviews of this material

Kinds of Security Things You Should Know About

- IPsec
- Security protocols
- Key exchange, certificates, certification hierarchies
- Basics of security threats and mechanisms
- Use of cryptography for authentication, privacy, and other purposes
- Basics of firewalls and virus protection systems
- Basics of viruses and worms

Kinds of Networking Things You Should Know About

- TCP/IP
- Routing protocols
- How DNS works
- Multicast protocols
- Basic ad hoc networking
- Basics of wireless networks
- Basic design and architecture of the Internet

A Short Introduction

- What is this class really about?
- Protecting computer networks and the machines attached to them
- Focusing on the network threats
  - Bad things that can happen due to networking
  - Attacks on network components

What's In

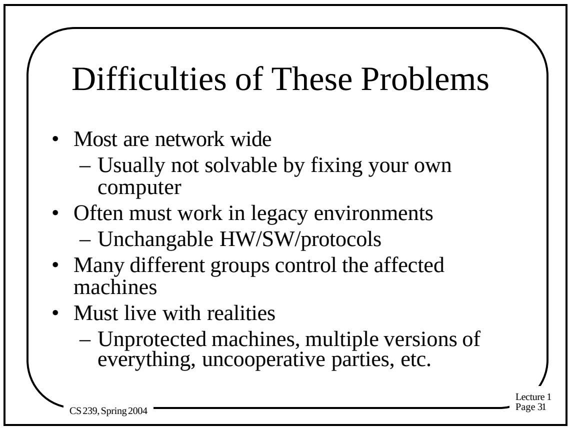
- Security of routing protocols, DNS, multicast protocols, resource reservation protocols
- Network-wide attacks (DDoS, Worms)
- Security of specialized networks (sensor networks, ad hoc networks)
- Related topics (measurement issues, privacy, legal issues)

What's Out

- Cryptography (except as a tool)
- Securing LANs (firewalls, intrusion detection systems, etc.)
- Securing individual computers (virus scanning, hardening against buffer overflow attacks, etc.)
- Security policy issues
- Auditing, logging, formal methods, VPNs

Scope of the Problem

- Viruses and worms are becoming a major threat
- Everyone hates spam
- DDoS attacks are beginning to be used by real criminals
- Some attacks on network infrastructure have occurred
- 78% of FBI survey respondents report attacks from across Internet



Difficulties of These Problems

- Most are network wide
  - Usually not solvable by fixing your own computer
- Often must work in legacy environments
  - Unchangable HW/SW/protocols
- Many different groups control the affected machines
- Must live with realities
  - Unprotected machines, multiple versions of everything, uncooperative parties, etc.