

# Introduction to Cyber Security Lab

CS498sh

Susan Hinrichs

Spring 2008

# Administrivia

- Meet Tuesdays/Thursdays 11:00-12:15  
1131 Siebel
- Security lab in 222 SC
- Office hours in lab, time TBA
  - [shinrich@cs.uiuc.edu](mailto:shinrich@cs.uiuc.edu)
  - Office 4224 SC
- Newsgroup `cs.class.cs498sh`
- Web site  
<http://www.cs.uiuc.edu/class/cs498sh>

# Class Structure

- Complements introductory security courses like Information Assurance
  - Teach computer and network security mechanisms used in the field
  - Teach design techniques
  - A sampling of security technologies
- Class meetings
  - Lectures on background material
  - In class exercises in lab
  - Guest lectures

# Class Non-Goal

- Class will **not** make you expert in any particular security technology
- If that is your goal, better to take a specific technology training course or self study

# Topics

- Secure Programming
  - Least-privilege programming and impersonation
  - Worm anatomy
  - Malware frameworks
- OS security
  - Windows ACLs and security policies
  - Vista security additions
  - SE Linux domain type enforcement policies
  - Mandatory access controls in SE Linux and perhaps other OS's
  - User identity
- Database Security

# More Topics

- Network Security
  - Firewall configuration
  - IPSec
  - IPv6
  - Access control servers
  - Network intrusion detection and monitoring
  - Honey pots
  - Wireless security
  - Network scanning
- Defensive system design
  - Security architectures
  - Penetration testing

# Reading Materials

- Introductory Security Text for reference
  - Like Pfleeger and Pfleeger from Information Assurance, or Bishop's text, or Stalling's text
- Supplemented with many papers and manuals

# Course Evaluation

- ~5 Lab exercises – 50%
- ~2 Papers – 25%
- Final design project – 25%
- Folks taking for graduate credit
  - Research/deploy an additional technology
    - Pick your technology soon
    - e.g. PAM, App Armour, BitLocker

# Questions for the class

- Have you taken an introductory security class?
- Are you familiar with Windows and/or Linux?
- Are you comfortable with C, C++, and/or Java?
- Are you familiar with IP networking?
- What do you hope to get out of this class?