Introduction
CS 236
On-Line MS Program
Networks and Systems Security
Peter Reiher

Purpose of Class

- To prepare students for research and advanced work in security topics
- To familiarize students working in other networking areas with important security issues

Description of Class

- Topics to be covered
- Prerequisites
- Grading
- Reading materials
- Projects
- Office hours
- Web page

Topics to Be Covered

- Cryptography and authentication
  - Use, not design and analysis
- Design of secure protocols
- Network security – threats and countermeasures
- Secure operating systems design
- Practical application of security principles
- Malware, common attacks, and important defenses
- Secure programming
- Privacy

Prerequisites

- CS 118
  - Introductory networking
- CS 111
  - Introductory operating systems
- Both classes were offered in earlier quarters of on-line program

Grading

- Midterm – 25%
- Homework assignments – 50%
- Final – 25%

Class Format

- Class will be taught on-line
- Lectures will be posted in two or three segments
  - Students expected to view all of each lecture
- Generally, a short segment will be available on applying knowledge from previous class

Teaching Assistant

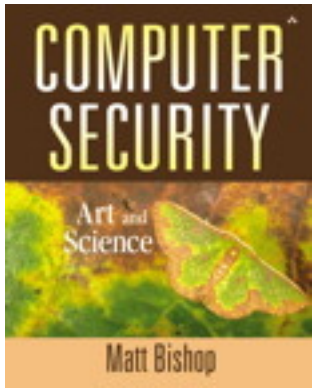
- The TA for this year is Michael Sweatt
  - sweattm92@gmail.com
- The matching slide in the posted version will provide name and contact info
- TA will handle all homework issues
- Office hours: TBA
- On-line recitation sections also TBA

Reading Materials

- Textbook
- Non-required supplemental texts
- Papers and web pages

Textbook

- *Computer Security: Art and Science*
  - By Matt Bishop
  - First edition
- Bishop has a shorter version
  - That's not the one we're using
- Available from on-line booksellers
- First reading assignment: Chapter 1



Supplemental Text 1

- *Applied Cryptography*
  - By Bruce Schneier
- Only covers what its title implies
  - And, as Schneier himself argues, there's a lot more to security
- But an excellent book on its subject
- Not required
  - No reading assignments from this book

Supplemental Text 2

- *Secrets and Lies*
  - Also by Bruce Schneier
- Not a textbook at all
- A philosophy of computer security
- Great for appreciating the field and problems
- Not great for depth of technical details
- Not required
  - No readings will be assigned from this book
  - But if you plan to work in this field, read it

Papers and Web Pages

- Usually one paper per week and a couple of web pages
- Usually made available electronically
  - Through class web page
- Material in papers might or might not be lectured on
  - But it can appear on tests, regardless
- Chosen for interesting and new ideas

Homeworks

- There will be five homework assignments
- Performed individually
- Requires programming and/or data analysis
- To be done on the Deter testbed
  - Accounts will be set up for all
  - And information provided on accessing and using the testbed

Homework Topics

1. Access control and permissions
   - Week 3
2. Exploits
   - Week 4
3. Analysis of attacks and forensics
   - Week 6
4. Man-in-the-middle attacks
   - Week 7
5. Botnets
   - Week 8

More on Homeworks

- Each homework has an associated web page
  - With full instructions and pointers to necessary tools
- Due by midnight on Thursday of indicated week
- Class TA will provide advise and assistance on homeworks

How Will They Work?

- A testing environment will be set up for you on the Deter testbed
- You will need to access that environment and perform certain actions
  - Typically requiring programming, system configuration, analysis
- Generally either finding and fixing security problems
- Or setting up secure configurations

The Deter Testbed

- A set of machines devoted to security research and education
- Located at ISI and SRI
- Accessible remotely
- Special accounts set up for this class
- TA will provide assistance in setting up accounts and learning to use the testbed

Tests

- Midterm – Time to be announced
  - But probably around 5th week
- Final – Time to be announced
  - After 10th week
- Both tests will be open book
  - Essay questions concentrating on applying knowledge
- Either remotely proctored or in person at UCLA

Office Hours

- Most interactions likely to occur through email
  - reiher@cs.ucla.edu
- But physical office hours TTh 2-3
  - Held in 3532F Boelter Hall
- Other times available by prior arrangement

Class Web Page

- http://www.lasr.cs.ucla.edu/classes/236_online.spring16
- PDF or Powerpoint versions of lecture slides
  - Taped lectures posted on regular on-line program web site
- Readings will be posted at above web site
  - With links to papers
- Also links to other interesting info