95-753

Telecommunication Security

Introductory Material

Richard J. Orgass
H. John Heinz III School of Public Policy and Management
Carnegie Mellon University

Agenda

- Instructor and TA Contact Information
- Cheating Policy
- Communication
- Course Objectives
- Textbooks
- Syllabus
- Grading
- Homework Plan
- Reading Assignments
- Present and Near Future Telecommunications Industry
- IPv6

Instructor Contact Information

- Richard J. (Dick) Orgass
- Office
  - 2806A Hamburg Hall
- E-mail: orgass+@cs.cmu.edu
- Telephone: (412) 268-8408
- Office Hours
  - Discuss in Class
- Other times: call to find out if I'm available
- www.cs.cmu.edu/~orgass

TA Contact Information

- Chris Gribble
  - INI Graduate Student
- Office: INI Grad Student Cluster
- E-mail: cgribble@andrew.cmu.edu
- Office Hours: Discuss in Class

Cheating

- CMU Student Handbook Describes Campus Cheating Policy including penalties
- Instructors must specify cheating policy for each course.
- In this Course:

You cheat if you represent someone else's work as your own.

- Each document, presentation, code fragment, etc. should show the name(s) of the author(s) and acknowledge contributions from others.
- Let's not have to mention the subject again.

Communication

- Web Site
  - www.cs.cmu.edu/~orgass/95-753
  - contains
    - lecture materials
    - homework solutions
    - some homework assignments (see below)
- BBoard / News group
  - academic.ism.95-753 (andrew)
  - cyrus.academic.ism.95-753 (cs)
  - Intended Uses
    - Publish Homework Problems
    - Ask and answer questions
    - Discuss issues
    - Students encouraged to ask and answer questions
  - TA and Instructor will monitor actively

Communication -- 2

- E-mail to instructor or TA
  - private question and answer
  - may be answered in news group but will ask first
  - if we don't want to answer your question, we'll send e-mail telling you why we don't want to answer

Course Objectives

- Create an awareness of
  - risks associated with using the internet
  - lack of adequate security in many places
  - elementary steps to improve security
- Management Level Understanding of
  - Routine technical steps to increase security
  - Understand Security and Technologies at
    - Enterprise/Establishment Level
    - Small Business Level
- Create a firm understanding that

A perfectly secure system that can be used does not exist

Textbooks

- Jonathan Littman. *The Watchman*. Little Brown, April 1997. ISBN 0316528579.
- Clifford Stoll. *The Cuckoo's Egg*. New York, Pocket Books, 1990. ISBN 0671726889.
- Scott Mann, Ellen L. Mitchell. Linux System Security. Prentice-Hall, 2000. ISBN 0-13-015807-0.
- Bruce Schneier. *Secrets and Lies*. John Wiley & Sons, 2000. ISBN 0-471-25311-1.

Syllabus

- Week 1
  - Telecommunications Industry Today.
    - David Clark paper plus Orgass's comments
  - IPv6, David Johnson, Computer Science, Rice University
- Week 2
  - Kevin Poulsen's Exploits (Part 1)
  - Network Structures for Security
- Week 3
  - Kevin Poulsen's Exploits (Part 2)
  - Vulnerability Survey, Security Policies
- Week 4
  - A classic Internet breakin (Part 1)
    - Cliff Stoll's tracking of a Berkeley break-in
  - Topics in Linux/Unix System Security

Syllabus -- II

- Week 5
  - A Classic Internet Breakin (Part 2)
  - Users, Permissions and File Systems
- Week 6
  - System security for a co-location facility
  - Ed DeHart, CEO of aspStation
- Week 7
  - Security Landscape
    - Digital Threats
    - Adversaries
    - Security Needs
  - System Security for an ISP (tentative)
    - Speaker to be determined

Syllabus -- 3 --

- Week 8
  - Security Technologies 1
    - Cryptography
    - Cryptography in Context
    - Computer Security
    - Identfication and Authentication
    - Networked Computer Security
  - CERT Data Collection Work (tentative)
    - Brian King, MTS in CERT
- Week 9
  - Security Technologies 2
    - Network Security
    - Network Defenses
    - Sofware Reliability
    - Secure Hardware
    - Certificates and Credentials

Syllabus -- 4 --

- Week 9 (continued)
  - CERT Analytical Work (tentative)
    - Tom Longstaff, Manager of Analysis Activity, CERT
- Week 10
  - Security Technologies 3
    - Security "Tricks"
    - ***The Human Factor***
  - Government System Security (tentative)
    - Jeffrey Hunker, Dean of the Heinz School
- Week 11
  - Security Strategies 1
    - Vulnerabilities and the Landscape
    - Threat Modeling and Risk Assessment
    - Security Policies and Countermeasures
    - Attack Trees

Syllabus -- 5 --

- Week 11 (continued)
  - System Security Measures 1
    - Pluggable Authentication Modules
    - One Time Passwords
- Week 12
  - Security Strategies 2
    - Product Testing and Verification
    - Future of Products
    - Security Processes
    - Strategy Conclusion
  - System Security Measures 2
    - System Accounting
    - System Logging
    - Superuser Do

Syllabus -- 6 --

- Week 13
  - System Security Summary
  - System Security Measures 3
    - TCP Wrappers and portmap
    - The Secure Shell (SSH)
    - Log File Management
- Week 14
  - Secure Distributed File Systems
    - Andrew File System (AFS)
    - CODA, casually connected distributed file system
  - System Security Measures 3
    - Crack
    - Auditing with tiger
    - Tripwire
    - Packet Filtering with IP chains (lightly)

Syllabus -- 7 --

- Week 15
  - System Security Measures 4
    - Cryptographic File Systems
    - Implementing and Managing Security
  - Review and Final Questions

Grading

- Two papers
  - CIO to Corporate Management (33%)
    - Vulnerability Analysis
    - Security Policies
    - Required Technical and Human Solutions
  - CIO's Security Plan (33 %)
    - Enterprise is UNIX systems
    - Technical Measures to Apply
    - Human Component of Solution
      - Policies
      - Enforcement
- Two Team Projects (34 %)
  - Secure a Linux System
  - Attempt penetration of another team's secured system
- No formal final exam
- Usual +/- letter grades

Homework Plans

- Weekly Assignment
  - Reading
    - non-technical
    - technical
  - Discussion Questions
    - three discussion questions for each of
      - non-technical reading
      - technical reading
- Two papers
  - Security Business Case
    - Draft due Week 6
    - Returned with comments Week 7
    - Final Version Week 8
  - Security Plan
    - Draft due Week 13
    - Returned with comments Week 14
    - Final Version Week 15

Homework Plans -- 2

- Team Projects
  - Student Selected Groups of 3
    - Team A secures Linux System
    - Team B attempts to penetrate secured system
    - Team A attempts to penetrate system of Team C
    - Team B secures a system for penetration attempt by team D
  - Each Team secures a system and attempts to penetrate a system
  - Project Results due Week 13
    - Start well ahead of due date
    - More information in class
- Install Linux on your notebook
  - Complete by week 7
  - Instructions

    `http://www.mism.cmu.edu/currentStudents/ComputingManuals/LinuxDualBoot Installation.pdf`

Homework Assignments

- For each reading assignment, bring three questions to class and turn them in on paper.
- Week 2
- Read to p. 155 of *The Watchman*
- Week 3
  - Read remainder of *The Watchman*
  - Read Chapters 1-2 of *Linux System Security*
- Week 4
  - Read Chapters 1-32 of *The Cuckoo's Egg*
  - Read Chapter 3 of *Linux System Security*
- Week 5
  - Read Chapters 33-56 of *The Cuckoo's Egg*
  - Read Chapter 4 of *Linux System Security*
- Week 7
  - Read Chapters 1-5 of *Secrets and Lies*

Homework Assignments -- II

- Week 8
  - Read Chapters 6-10 of *Secrets and Lies*
- Week 9
  - Read Chapters 11-16 of *Secrets and Lies*
- Week 10
  - Read Chapter 17 of *Secrets and Lies*
- Week 11
  - Read Chapters 18-21 of *Secrets and Lies*
  - Read Chapters 5-6 of *Linux System Security*
- Week 12
  - Read Chapters 22-25 of *Secrets and Lies*
  - Read Chapters 7-9 of *Linux System Security*

Homework Assignments -- 3 --

- Week 13
  - Read Chapters 10, 11,17 of *Linux System Security*
- Week 14
  - Read Chapters 12-14, 16 of *Linux System Security*
- Week 15
  - Read Chapters 15 and 18 of *Linux System Security*