CSE 571S: Network Security

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

These slides are available on-line at:
http://www.cse.wustl.edu/~jain/cse571-07/
Overview

- Goal of this Course
- Grading
- Prerequisites
- Tentative Schedule
- Project
Goal of This Course

- Comprehensive course on network security
- Includes both theory and practice
- Theory: Cryptography, Hashes, key exchange, Email Security, Web Security
- Practice: Hacking and Anti-Hacker techniques
- Graduate course: (Advanced Topics)
  ⇒ Lot of independent reading and writing
  ⇒ Project/Survey paper
CERT Statistics

- Computer emergency response team (CERT)
- Security is a #1 concern about Internet.
- Significant industry and government investment in security
Prerequisites

- CSE 473S (Introduction to Computer Networking) or equivalent
Prerequisites

- ISO/OSI reference model
- TCP/IP protocol stack
- Full-Duplex vs half-duplex
- UTP vs Satellite link vs Wireless
- Cyclic Redundancy Check (CRC)
- CRC Polynomial
- Ethernet
- IEEE 802 MAC Addresses
- Bridging and Routing
- IEEE 802.11 LAN
Prerequisites (Cont)

- IP Address
- Subnets
- Private vs Public Addresses
- Address Resolution Protocol (ARP)
- Internet Control Message Protocol (ICMP)
- IPV6 addresses
- Routing - Dijkstra's algorithm
- Transport Control Protocol (TCP)
- User Datagram Protocol (UDP)
- TCP connection setup
- TCP Checksum
- Hypertext Transfer Protocol (HTTP)
Text Book

Supporting Books

On 2hr reserve at WUSTL Olin Library

Supporting Books (Cont)

## Tentative Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>8/29</td>
<td>Course Overview</td>
</tr>
<tr>
<td>9/3</td>
<td>Labor Day Holiday</td>
</tr>
<tr>
<td>9/5</td>
<td>Types of attacks, TCP IP Attacks</td>
</tr>
<tr>
<td>9/10</td>
<td>Operating Systems Security</td>
</tr>
<tr>
<td>9/12</td>
<td>Monitoring and Attack Tools</td>
</tr>
<tr>
<td>9/17</td>
<td>Secret Key Cryptography (Chapter 3)</td>
</tr>
<tr>
<td>9/19</td>
<td>Modes of Operation (Chapter 4)</td>
</tr>
<tr>
<td>9/24</td>
<td>Hashes and Message Digest (Chapter 5)</td>
</tr>
<tr>
<td>9/26</td>
<td>Public Key Cryptography (Chapter 6)</td>
</tr>
<tr>
<td>10/1</td>
<td>Authentication: Passwords, Biometrics (Chapter 10)</td>
</tr>
<tr>
<td><strong>10/3</strong></td>
<td>Exam 1</td>
</tr>
</tbody>
</table>

Washington University in St. Louis  
CSE571S  
©2007 Raj Jain
# Tentative Schedule (Cont)

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/8</td>
<td>Kerberos (Chapter 14)</td>
</tr>
<tr>
<td>10/10</td>
<td>Public Key Infrastructure (Chapter 15)</td>
</tr>
<tr>
<td>10/15</td>
<td>IPSec (Chapter 17)</td>
</tr>
<tr>
<td>10/17</td>
<td>Internet Key Exchange (IKE) (Chapter 18)</td>
</tr>
<tr>
<td>10/22</td>
<td>Web Security: SSL/TLS (Chapter 19)</td>
</tr>
<tr>
<td>10/24</td>
<td>Email Security: PGP (Chapter 22)</td>
</tr>
<tr>
<td>10/29</td>
<td>Firewalls (Chapter 23)</td>
</tr>
<tr>
<td>10/31</td>
<td>LAN Access Control: 802.1x</td>
</tr>
<tr>
<td>11/5</td>
<td><strong>Exam 2</strong></td>
</tr>
</tbody>
</table>
# Tentative Schedule

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/7</td>
<td>Network Access Controls: AAA</td>
</tr>
<tr>
<td>11/12</td>
<td>VPNs</td>
</tr>
<tr>
<td>11/14</td>
<td>Wireless Security</td>
</tr>
<tr>
<td>11/19</td>
<td>Routing Protocol Security</td>
</tr>
<tr>
<td>11/21</td>
<td>Thanksgiving Holiday</td>
</tr>
<tr>
<td>11/26</td>
<td>Thanksgiving Holiday</td>
</tr>
<tr>
<td>11/28</td>
<td>Intrusion Detection</td>
</tr>
<tr>
<td>12/3</td>
<td>TBD</td>
</tr>
<tr>
<td>12/5</td>
<td>TBD</td>
</tr>
<tr>
<td>12/10</td>
<td>TBD</td>
</tr>
<tr>
<td><strong>12/12</strong></td>
<td><strong>Final Exam</strong></td>
</tr>
<tr>
<td>12/17</td>
<td>Grade Review</td>
</tr>
</tbody>
</table>
Grading

- Mid-Terms (Best 1 of 2) 30%
- Final Exam 30%
- Class participation 5%
- Homeworks 15%
- Project 20%
Projects

- A survey paper on a network security topic
  - Wireless Network Security
  - Key Exchange Protocols
  - Comprehensive Survey:
    Technical Papers, Industry Standards, Products
- A real attack and protection exercise on the security of a system (web server, Mail server, …) – Groups of 2 students (Hacker and Administrator)
- Average 6 Hrs/week/person on project + 9 Hrs/week/person on class
- Recent Developments: Last 5 to 10 years ⇒ Not in books
- Better ones may be submitted to magazines or journals
Projects (Cont)

- Develop a hack tool to break the security of a system.
- Develop a tool to protect from the hack tool.
- **Goal:** Provide an insight (or information) not obvious before the project.
- **Real Problems:** Thesis work, or job
- **Homeworks:** Apply techniques learnt to your system.
Project Schedule

Mon 10/8/07 Topic Selection/Proposal
Mon 10/15/07 References Due
Mon 10/29/07 Outline Due
Mon 11/12/07 First Draft/Demo Due
Mon 11/19/07 Reviews/comments Returned
Mon 12/3/07 Final Report Due
Office Hours

- Monday: 11 AM to 12 noon
- Wednesday: 11 AM to 12 noon

- Office: Bryan 405D

- Teaching Assistant: Chakchai So-in, Bryan 516
  1 hour/week – Group meeting

- CSE 571 Security Lab: Bryan 516
Frequently Asked Questions

- Yes, I do use “curve”. Your grade depends upon the performance of the rest of the class.
- All homeworks are due on the following Monday unless specified otherwise.
- Any late submissions, if allowed, will *always* have a penalty.
- All exams are open-book and extremely time limited.
- Exams consist of numerical as well as multiple-choice (true-false) questions.
- There is a negative grading on incorrect multiple-choice questions. Grade: +1 for correct. -1/(n-1) for incorrect.
- Everyone including the graduating students are graded the same way.
Goal: To prepare you for a job as a secure systems administrator

There will be a lot of self-reading and writing

Get ready to work hard
Student Questionnaire

- Name: _________________________________________
- Email: _________________________________________
- Phone: _________________________________________
- Degree: ______________ Expected Date: _________________
- Technical Interest Area(s): _____________________________
- Prior networking related courses/activities:________________
- Prior security related courses: ____________________________
- If you have a laptop or desktop, it’s operating system: _______
  Do you have a WiFi interface? _____
- I agree to abide by the rules and will not use the techniques on
  any computer other than mine or CSE 571 security lab.
- Signature: _______________________ Date: _____________
Lab Homework 1: Gathering Info

Learn about IPconfig, ping, arp, nslookup, whois, tracert, netstat, route, hosts file

1. Find the IP addresses of www.google.com
2. Modify the hosts file to map www.google.com to 128.252.166.33 and do a google search. Remove the modification to the host file and repeat.
3. Find the domain name of 128.272.165.7 (reverse the address and add .in-addr.arpa)
4. Find the owner of wustl.edu domain
5. Find route from your computer to www.google.com
6. Find the MAC address of your computer
7. Print your ARP cache table. Find a server on your local network. Change its ARP entry in your computer to point to your computer’s MAC address. Print new ARP cache table. Now use the service and see what happens.
8. Print your routing table and explain each line (up to line #20 if too many)
9. What is the number of packets sent with “destination unreachable”
10. Find the location of 128.252.166.33 (use ipaddresslocation.org)
Quiz 0: Prerequisites

True or False?

T  F

- Subnet mask of 255.255.255.254 will allow 254 nodes on the LAN.
- Time to live (TTL) of 8 means that the packet can travel at most 8 hops.
- IP Address 128.256.210.12 is an invalid IP address.
- CRC Polynomial x32+x15+1 will produce a 32 bit CRC.
- DHCP server is required for dynamic IP address assignment.
- DNS helps translate an name to MAC address.
- Port 80 is used for FTP.
- IPv6 addresses are 32 bits long.
- New connection setup message in TCP contains a syn flag.
- 192.168.0.1 is a public address.

Marks = Correct Answers _____ - Incorrect Answers _____ = ______