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/

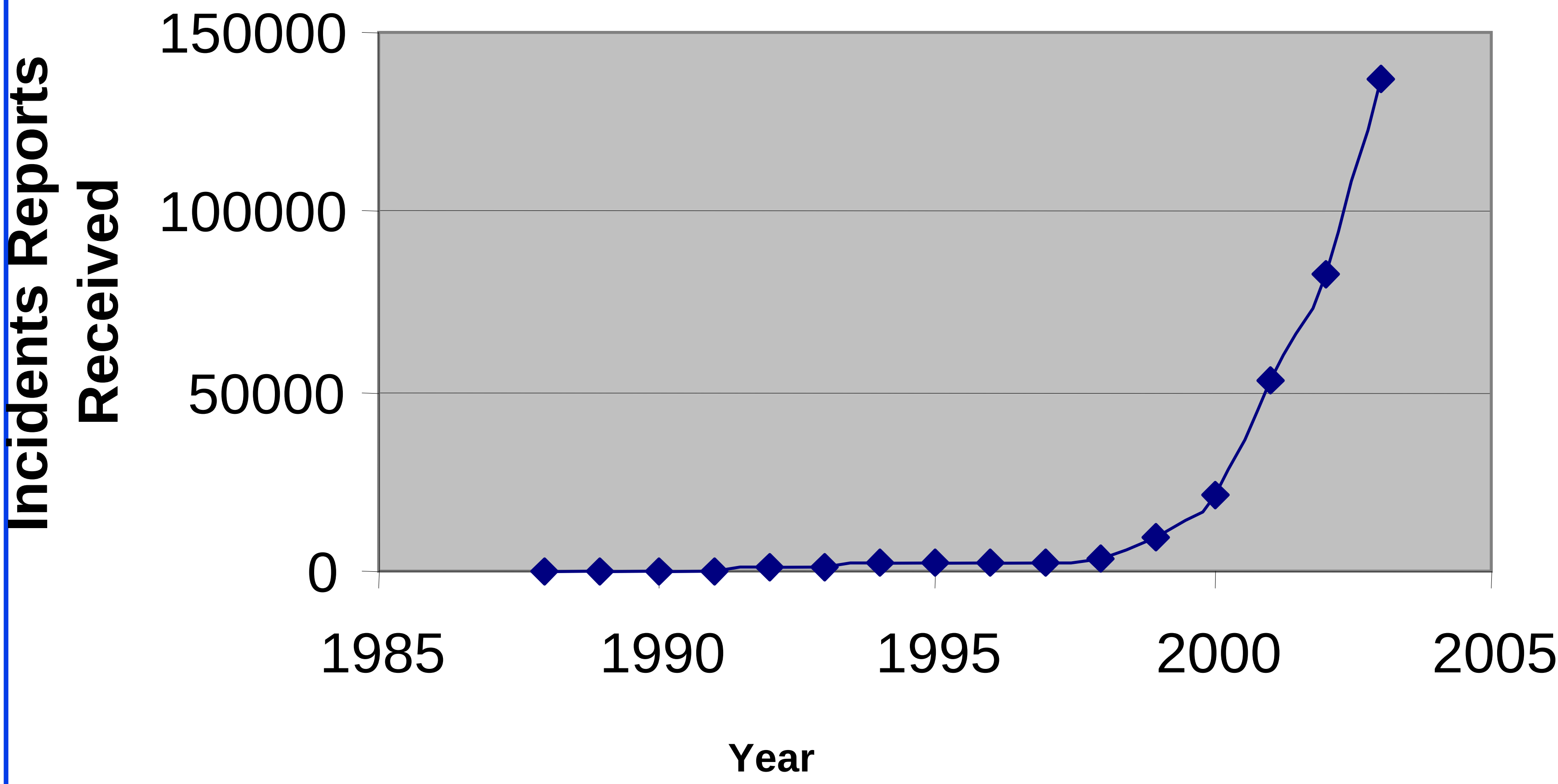
Overview

- 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

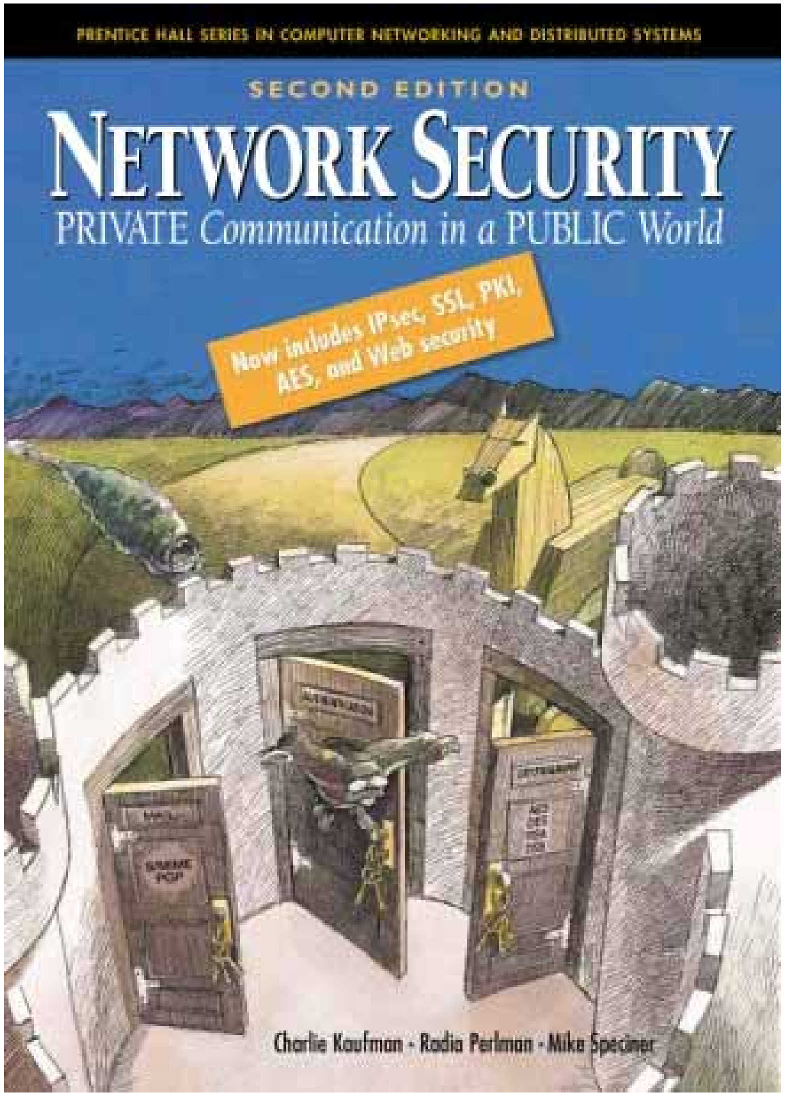
- ISO/OSI reference model
- TCP/IP protocol stack
- Full-Duplex vs half-duplex
- UTP vs Satellite link vs Wireless
- Cyclic Redundancy Check (CRC)
- CRC Polynomial
- Ethernet
- IEEE 802 MAC Addresses
- Bridging and Routing
- IEEE 802.11 LAN

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

- Charlie Kaufman, Radia Perlman, and Mike Speciner, "**Network Security: Private Communication in a Public World**," 2nd Edition, Prentice Hall, 2002, ISBN: 0130460192.


PRENTICE HALL SERIES IN COMPUTER NETWORKING AND DISTRIBUTED SYSTEMS
SECOND EDITION
NETWORK SECURITY
PRIVATE Communication in a PUBLIC World
Now includes IPsec, SSL, PKI, AES, and Web security
Charlie Kaufman · Radia Perlman · Mike Speciner

Supporting Books

On 2hr reserve at WUSTL Olin Library

- Ankit Fadia, "**Network Security : A Hacker's Perspective**," Course Technology Ptr, May-06, 415 pp., ISBN:1598631632.
- Vincent J. Nestler, et al, "**Computer Security Lab Manual**," McGraw-Hill, 2006, 755 pp., ISBN:0072255080.
- Gert DeLaet, Gert X. Schauwers, "**Network Security Fundamentals**," Cisco Press, Sep-04, 400 pp., ISBN:1587051672.
- Richard Bejtlich, "**The Tao Of Network Security Monitoring: Beyond Intrusion Detection**," Addison-Wesley, Jul-04, 798 pp., ISBN:321246772.
- Eric Rescorla, "**SSL and TLS: Designing and Building Secure Systems**," Addison-Wesley, Oct-00, 499 pp., ISBN:201615983.

Supporting Books (Cont)

- Jon C. Snader, "**VPNs Illustrated: Tunnels, VPNs, and IPsec**," Addison-Wesley Professional, Oct-05, 480 pp., ISBN:032124544X.
- Matt Bishop, "**Introduction to Computer Security**," Addison-Wesley Professional, Oct-04, 784 pp., ISBN:0321247442.
- Saadat Malik, "**Network Security Principles and Practices**," Macmillan Technical Pub, Nov-02, 400 pp., ISBN:1587050250.
- Jan Harrington, "**Network Security: A Practical Approach**," Morgan Kaufmann Pub, Mar-05, 365 pp., ISBN:123116333.
- Wenbo Mao, "**Modern Cryptography: Theory and Practice**," Prentice Hall Ptr, Jul-03, 648 pp., ISBN:0130669431.

Tentative Schedule

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

Tentative Schedule (Cont)

Date	Topic
10/8	Kerberos (Chapter 14)
10/10	Public Key Infrastructure (Chapter 15)
10/15	IPSec (Chapter 17)
10/17	Internet Key Exchange (IKE) (Chapter 18)
10/22	Web Security: SSL/TLS (Chapter 19)
10/24	Email Security: PGP (Chapter 22)
10/29	Firewalls (Chapter 23)
10/31	LAN Access Control: 802.1x
11/5	**Exam 2**

Tentative Schedule

Date	**Topic**
11/7	Network Access Controls:AAA
11/12	VPNs
11/14	Wireless Security
11/19	Routing Protocol Security
11/21	Thanksgiving Holiday
11/26	Thanksgiving Holiday
11/28	Intrusion Detection
12/3	TBD
12/5	TBD
12/10	TBD
12/12	**Final Exam**
12/17	Grade Review

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

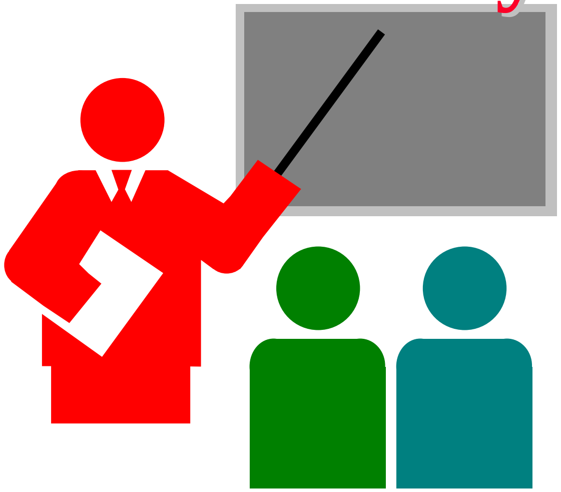
Office Hours

- 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.

Summary



- 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 _____ = ______