

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/cse571-09/>

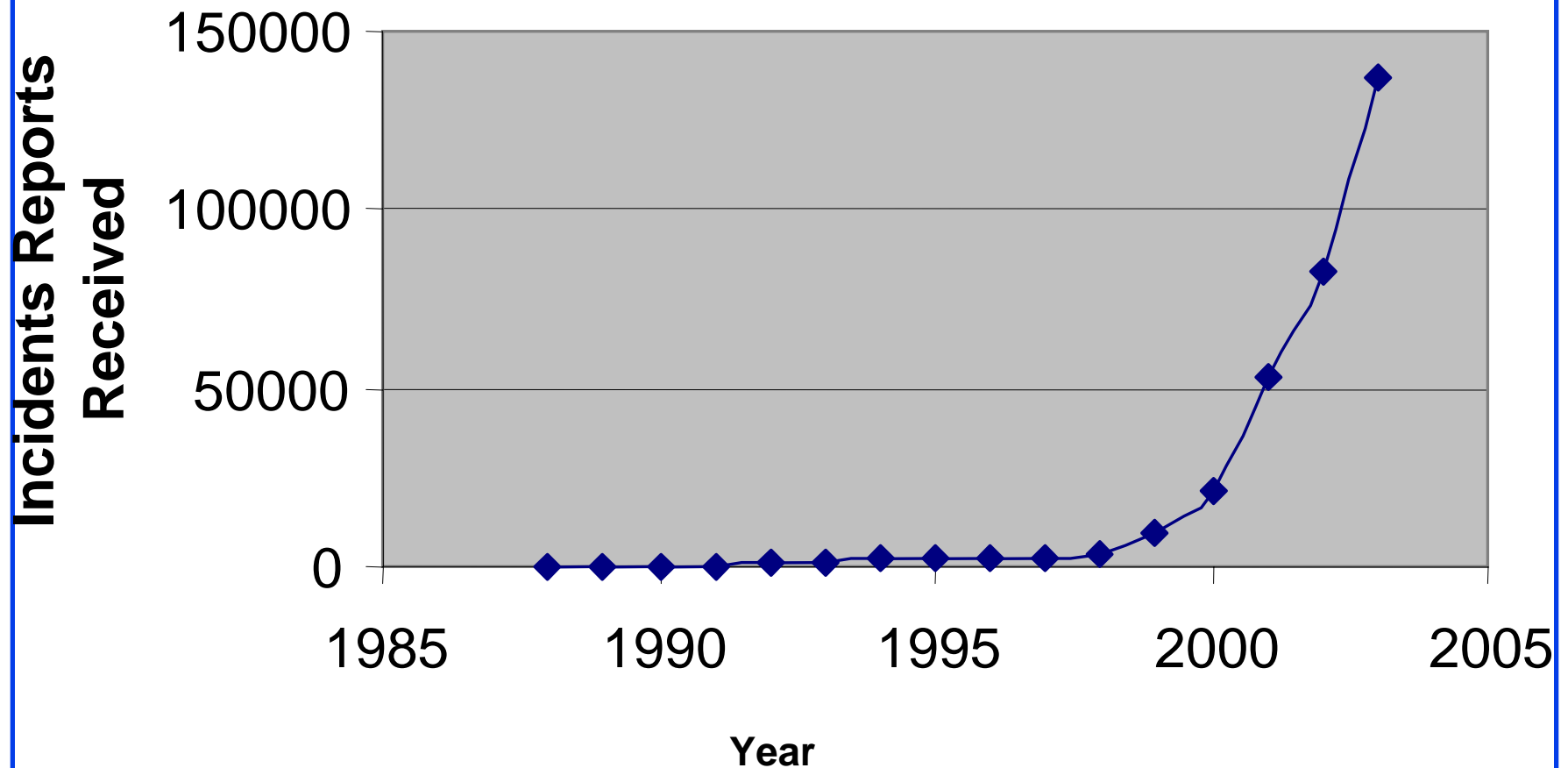


- ❑ Goal of this Course
- ❑ Grading
- ❑ Prerequisites
- ❑ Tentative Schedule
- ❑ Project

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

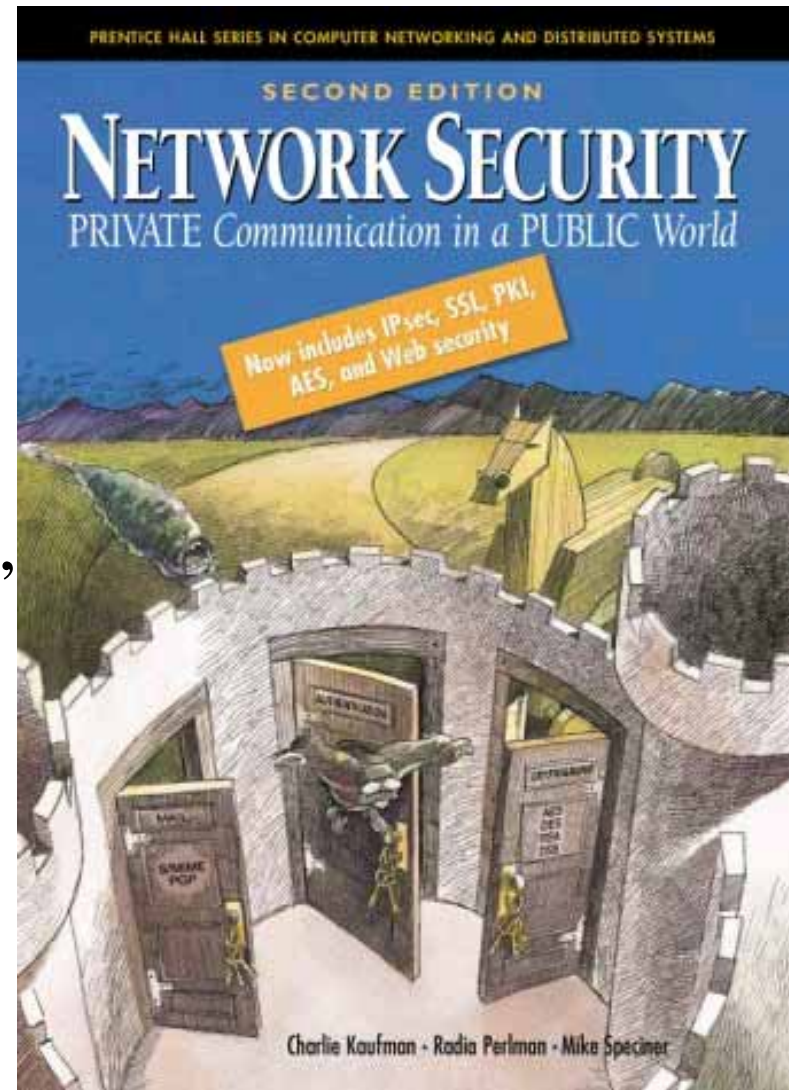
- ❑ ISO/OSI reference model
- ❑ TCP/IP protocol stack
- ❑ Full-Duplex vs half-duplex
- ❑ UTP vs Satellite link vs Wireless
- ❑ Cyclic Redundancy Check (CRC)
- ❑ CRC Polynomial
- ❑ Ethernet
- ❑ IEEE 802 MAC Addresses
- ❑ Bridging and Routing
- ❑ IEEE 802.11 LAN

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.



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.
- ❑ Jan Harrington, "**Network Security : A Practical Approach**," Morgan Kaufmann Pub, Mar-05, 365 pp., ISBN:123116333.
- ❑ William Stallings, "**Cryptography and Network Security**," 4th Edition, Prentice-Hall, 2006, 680 pp., ISBN:0131873164.
- ❑ Gert DeLaet, Gert X. Schauwers, "**Network Security Fundamentals**," Cisco Press, Sep-04, 400 pp., ISBN:1587051672.

Supporting Books (Cont)

- ❑ Alex W. Dent, Chris J. Mitchell, "**User's Guide To Cryptography And Standards (Hardcover)**," Artech House Publishers, October 2004, 402 pp., ISBN:1580535305.
- ❑ Richard Bejtlich, "**The Tao Of Network Security Monitoring: Beyond Intrusion Detection**," Addison-Wesley, Jul-04, 798 pp., ISBN:321246772.
- ❑ Jon Edney and William A. Arbaugh, "**Real 802.11 Security: Wi-Fi Protected Access and 802.11i**," Addison-Wesley, 2004, 451 pp., ISBN:0321136209
- ❑ Saadat Malik, "**Network Security Principles and Practices**," Macmillan Technical Pub, Nov-02, 400 pp., ISBN:1587050250.

Supporting Books (Cont)

- ❑ Krishna Shankar, et al, "**Cisco Wireless LAN Security**," Cisco Press, 2005, 420 pp, ISBN:1587051540
- ❑ 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.

Tentative Schedule

Date	Topic	Chapters
1/12	Course Overview	
1/14	Security Concepts	
1/19	Holiday	
1/21	TCP/IP Security Attacks	
1/26	Operating Systems Security Attacks	
1/28	Secret Key Cryptography	Chapter 3
2/2	Modes of Operation	Chapter 4
2/4	Hashes and Message Digest	Chapter 5
2/9	Number Theory and Public Key Cryptography	Chapter 7, 6
2/11	Public Key Cryptography (Cont)	Chapter 7, 6
2/16	Exam 1	

Tentative Schedule (Cont)

Date	Topic	Chapters
2/18	Authentication	Chapter 10
2/23	Kerberos V4	Chapter 13
2/25	Kerberos V5	Chapter 14
3/2	Public Key Infrastructure	Chapter 15
3/4	IPsec	Chapter 16, 17
3/9	<i>Spring Vacation Week</i>	
3/11	<i>Spring Vacation Week</i>	
3/16	Internet Key Exchange (IKE)	Chapter 18
3/18	Web Security: SSL/TLS	Chapter 19
3/23	Exam 2	

Tentative Schedule (Cont)

Date	Topic	Chapters
3/25	Email Security	Chapters 20, 21, 22
3/30	Virtual Private Networks (VPNs)	
4/1	Authentication, Authorization, and Accounting (AAA)	
4/6	AAA Part II	
4/8	Wireless LAN Security I	
4/13	Wireless LAN Security II	
4/15	DNS Security	
4/20	Intrusion Detection	
4/22	TBD	
4/27	TBD	
4/29	Final Exam	
5/4	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 \Rightarrow 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 02/09/09	Topic Selection/Proposal
Mon 02/23/09	References Due
Mon 03/02/09	Outline Due
Mon 03/30/09	Final Report/Demo Due
Mon 04/06/09	Reviews/comments Returned
Mon 04/13/09	Revised Report Due

Office Hours

- Monday: 11 AM to 12 noon
Wednesday: 11 AM to 12 noon
- Office: Bryan 523
- Teaching Assistant: Chakchai So-in, Jolley 528
cse571s@gmail.com
Office Hours: Friday 3:00-4:00PM
- CSE 571 Security Lab: Bryan 516

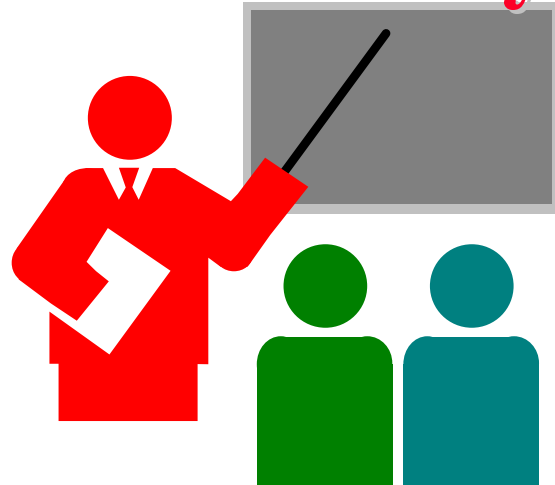
Homework Submission

- ❑ All homeworks are due on the following Monday unless specified otherwise.
- ❑ Any late submissions, if allowed, will ***always*** have a penalty.
- ❑ Please write CSE571 in the subject field of all emails related to this course.
- ❑ Use word “Homework” in the subject field on emails related homework. Also indicate the homework number.
- ❑ All homeworks are identified by the class handout number.
- ❑ All homeworks should be on a separate sheet. Your name should be on every page.

Frequently Asked Questions

- ❑ Yes, I do use “curve”. Your grade depends upon the performance of the rest of the class.
- ❑ All exams are closed-book. One 8.5”x11” sheet allowed.
- ❑ 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

- ❑ Execute the following commands on windows DOS box and try all variations:
 - Ipconfig /help
 - Ping /help
 - Arp /help
 - Nslookup
 - ❑ >help
 - Tracert -?
 - Netstat /help
 - Route /help
- ❑ Browse to whois.net
- ❑ Read about “Hosts File” on wikipedia.org

Lab Homework 1 (Cont)

Submit answers for the following:

1. Find the IP addresses of www.google.com and www.yahoo.com
2. Modify the hosts file to map www.google.com to yahoo's IP address and try to do a google search. Remove the modification to the host file and repeat.
3. Find the domain name of 128.252.160.200 (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 128.252.166.147 (use ipaddresslocation.org)

Security Lab Computer Sharing Rules

- ❑ One client and one server are to be shared among all the students of the class.
- ❑ Time slotted system with each slot of 1 hour starting at 00:00AM.
- ❑ You can use one slot or part of one slot and must disconnect at the end of the slot time.
- ❑ You can come back after 15 minutes, if no one has connected, you can use the remainder of the next slot.
- ❑ You can repeat this 15 minute break + 45 minute work cycle as long as needed.
- ❑ Remember to log off every time before disconnecting. If you forget to log off, connect again and log off.

Sharing Rules (Cont)

- ❑ If you try connecting during first 5 minutes of the hour and find that someone else is logged in, try in the first 5 minutes of the next hour and if the same person is still logged in, you can disconnect him/her and log in. (He/she probably forgot to log out).
- ❑ During 9PM to 12PM, the machines *may be* unreachable due to maintenance/update.
- ❑ Do your exercise early, do not wait till the last day.

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 $x^{32}+x^{15}+1$ 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 _____ = _____