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/cse571-11/

Overview

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

Internet Security Issues

- No authentication:
  - DNS attack: All YouTube traffic went to a black hole in Pakistan
- Phishing: Enter personal information on fake websites
- Spam
- Cyber warfare

SPAM

© Original Artist
Reproduction rights obtainable from
www.CartoonStock.com

"Wow! I've got one from some

- ❑ Averages 78% of all emails sent
- ❑ 81% of spam is about pharmaceutical drugs
- ❑ Cost businesses $100 Billion in 2007
- ❑ CAN-SPAM act of 2003
- ❑ Sent through Botnets of infected computers

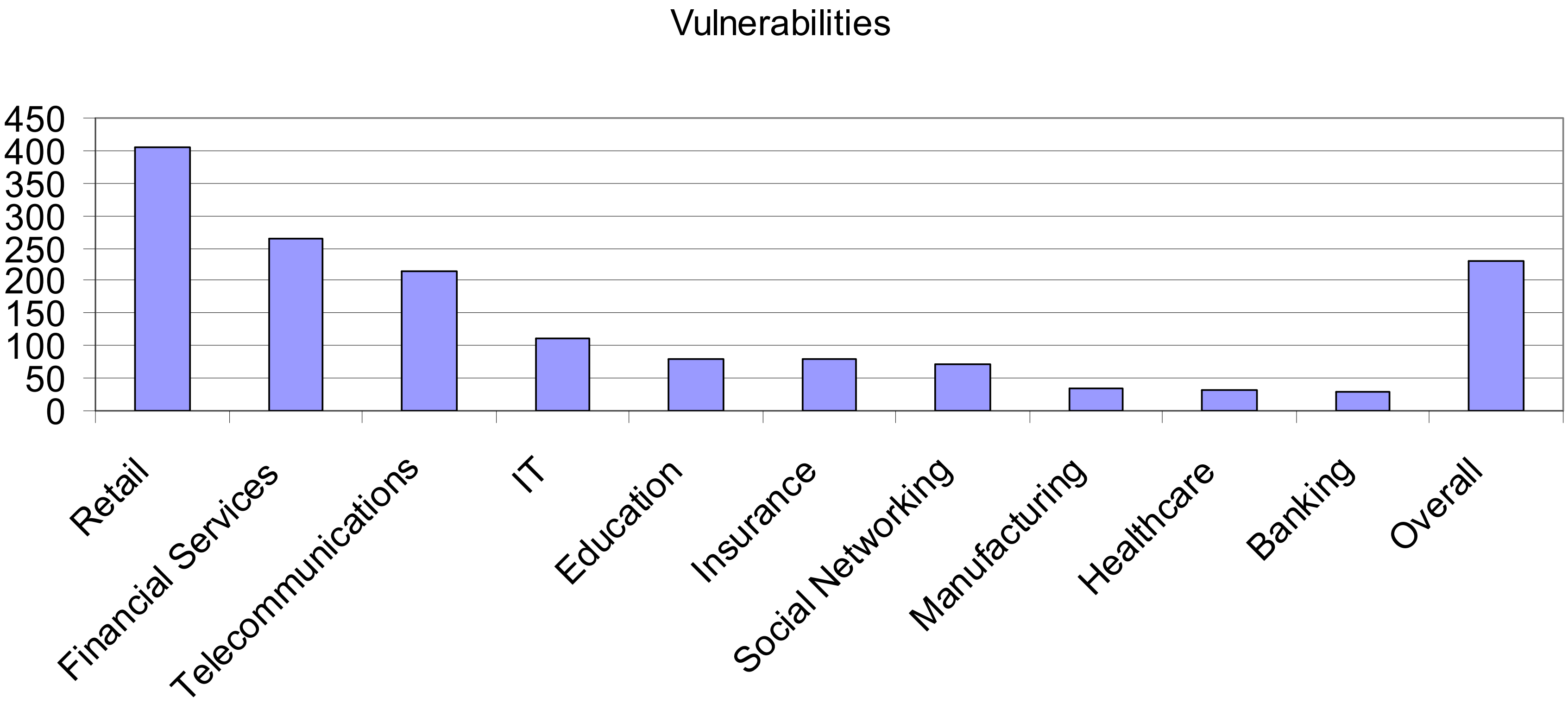
Ref: http://en.wikipedia.org/wiki/Email_spam

Cyber Warfare

- Nation States are penetrating other nations computers
- In 2009, US set up a cyber command
- UK, China, Russia, Israel, North Korea have similar centers
- Targets: Telecommunications, Transportations, Power Grid
- Pentagon spent more than $100 million in first half of 2009 in repairing damages from cyber attacks.

Ref: http://en.wikipedia.org/wiki/Cyber_war

Web Security Statistics 2010



- ❑ Based upon a survey of 3000 websites
- ❑ Most websites are exposed to average one vulnerability per day
- ❑ Source: WhiteHat Website Security Statistics Report – Winter 2011, 11th Edition, https://www.whitehatsec.com/resource/stats.html
- ❑

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
- Textbook covers only the theory part
- Graduate course: (Advanced Topics)
  ⇒ Lot of independent reading and writing
  ⇒ Project/Survey paper

Prerequisites

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

Prerequisites

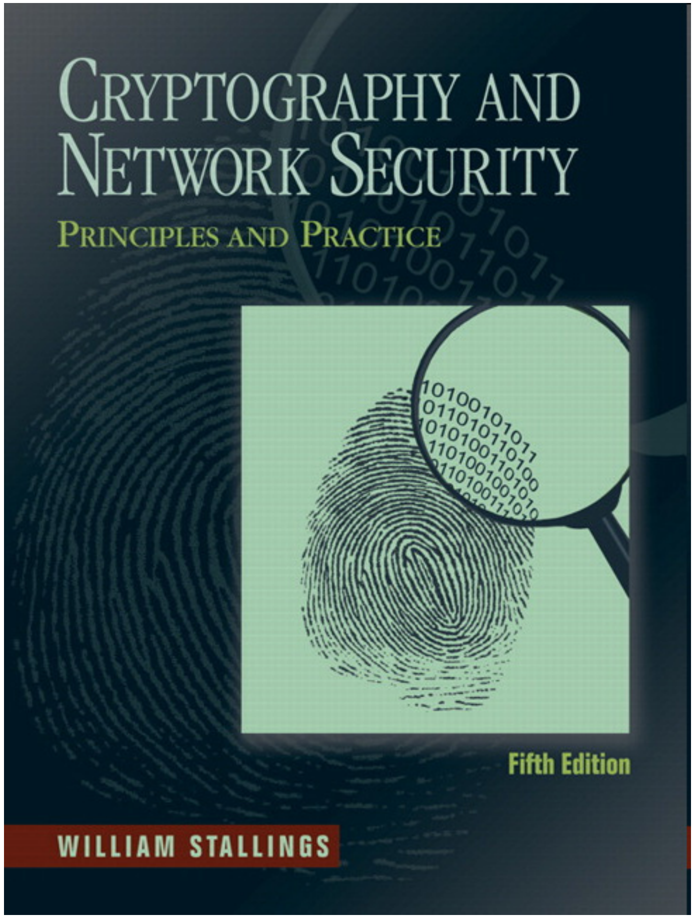
- ISO/OSI reference model
- TCP/IP protocol stack
- Full-Duplex vs half-duplex
- UTP vs Satellite link vs Wireless
- Cyclic Redundancy Check (CRC)
- CRC Polynomial
- Ethernet
- IEEE 802 MAC Addresses
- Bridging and Routing
- IEEE 802.11 LAN

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

- William Stallings, "**Cryptography and Network Security: Principles and Practice**," 5th Edition, Prentice Hall, 2011, ISBN:0-13-609704-9
- **Required**. Get the latest edition. Do not use older editions. If you use international edition, it should be dated 2011. It should have last page number 719. ISBN: 978-0-13-609704-9, or 0-13-609704-9
- **Errata**: http://www.box.net/shared/7978zk32dk



Textbook (Cont)

- It is recommended that you read the relevant chapter of the book chapter before coming to the class ⇒ Class time will be used for discussing and clarifying key concepts
- Only key concepts will be covered in the class.
  You are expected to read the rest from the book.
- Please ask questions in the next class about any concepts that are not clear to you
- Material covered in the class will include some concepts from other textbooks. Please pay attention to the class lecture.

Tentative Schedule

#	Date	Topic	Chapter
1	8/31	Course Intro	
2	9/5	Holiday - Labor Day	
3	9/7	Security Overview	1, 2
4	9/12	Block Ciphers and DES	3
5	9/14	AES and Block Cipher Operations	5, 6
6	9/19	Stream Ciphers	7
7	9/21	Public Key Cryptography	9
8	9/26	Other Public Key Cryptosystems	10
9	9/28	Cryptographic Hash Functions	11
10	10/3	Exam 1	

Tentative Schedule (Cont)

#	Date	Topic	Chapter
11	10/5	Message Authentication Codes	12
12	10/10	Digital Signatures	13
13	10/12	Key Management	14
14	10/17	User Authentication	15
15	10/19	Transport Level Security	16
16	10/24	Wireless Network Security	17
17	10/26	Electronic Mail Security	18
18	10/31	IP Security	19
19	11/2	Intrusion Detection	20
20	11/7	Exam 2	

Tentative Schedule (Cont)

#	Date	Topic	Chapter
21	11/9	Firewalls	22
22	11/14	Virtual Private Networks (VPN)	
23	11/16	Authentication, Authorization, Accounting (AAA)	
24	11/21	Domain Name System (DNS) Security	
25	11/23	Holiday - Thanks Giving	
26	11/28	Media Access Control (MAC) Security	
27	11/30	TBD	
28	12/5	Student Project Presentations	
29	12/7	Final Exam	

Grading

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

Projects

- A real attack and protection exercise on the security of a system (web server, Mail server, …) – Groups of 2 students (Hacker and Administrator)
  - Develop a hack tool to break the security of a system, or
  - Develop a tool to protect from the hack tool.
- A survey paper on a network security topic
  - Wireless Network Security
  - Key Exchange Protocols
  - Comprehensive Survey:
    Technical Papers, Industry Standards, Products
- 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)

- **Goal:** Provide an insight (or information) not obvious before the project.
- **Real Problems:** Thesis work, or job
- **Homeworks:** Apply techniques learnt to your system.

Sample Survey Paper Topics

- Cyber crime
- Cyber terrorism
- Cyber warfare
- Security of Industrial Controllers
- Mobile device security issues
- Privacy and Security Issues in Social Networks
- Multimedia security
- Digital Rights Management (DRM)
- Multicast Security
- Handover Keying
- Federated Access
- Extensible Messaging and Presence Protocol (XMPP)
- Simple Authentication and Security Layer (SASL)

Sample Survey Paper Topics (Cont)

- Secure DNS
- DNS-based Authentication of Named Entities
- Generic Security Services (GSS) API
- Security Assertion Markup Language (SAML).
- Port-based Access Control 802.1X
- MAC Security 802.1AE
- Secure Device Identity
- Biometric Security Systems

Project Schedule

Mon 10/10/11 Topic Selection/Proposal

Mon 10/17/11 References Due

Mon 10/24/11 Outline Due

Mon 11/14/11 Final Report/Demo Due

Mon 11/21/11 Reviews/comments Returned

Mon 11/28/11 Revised Report Due

Office Hours

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

- Office: Bryan 523

- **Teaching Assistant**: Mart Haitjema, Bryan 422
  Email: mah5@cec.wustl.edu
  Office Hours: Friday/Sunday 3:00-4:00PM

- CSE 571 Security Lab: Bryan 516
  (Only remotely accessible)

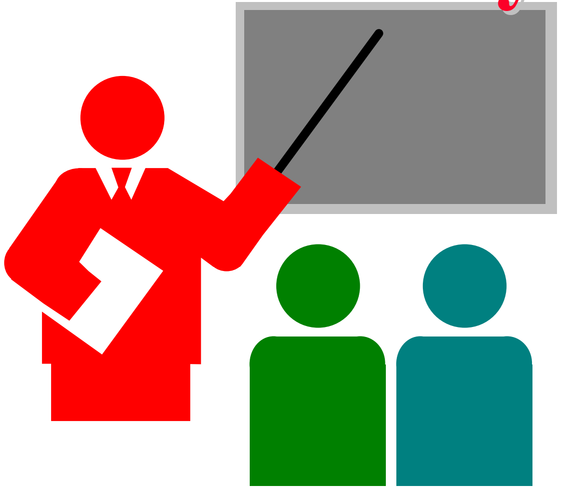
Homework Submission

- 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

- 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

mCLK System for Instant Quizzes

To set up your phone to use mClk (one time setup)

1. I have set-up the keyword "net“ on the mClk system
2. Using your cell phone, send a text message to short code 29671
3. Content of message must be: start net [first initial lastname]
   (example: start net jsmith)
4. A confirmation text message will be sent to your phone.

To use mClk (for each class)

1. On the first mClk question, send a text message to short code 29671 with the message "join" and the session ID that is posted on the screen (example: join 1248).
2. A confirmation text message will be sent to your phone
3. To answer each question, text the question number and your answer to 29671 (example: 1 C). Be sure to separate the question number and your answer with a SPACE.
4. Your response is added to those of the other attendees and results are projected on the screen.

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 phone number of the administrative contact for 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 the top 3 lines of active routes
9. What is the number of packets sent with "destination unreachable"
10. Browse to ipaddresslocation.org and find public information about your computer. Can you guess your city from this information?

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 _____ = ______

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: ____________