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/cse571-14/

Overview

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

Cyber Security Facts

- Federal government has suffered 680% increase in cyber security breaches in the past six years
- Governments, not hackers, are most likely to launch cyber attacks
- More than 600,000 accounts are compromised every day on Facebook alone
- National Nuclear Security Administration records 10 million attempted hacks a day
- US Navy receives 110,000 attacks per hour
- Every second 18 adults suffer cybercrime (1.5 million/day)
- Global spam rate in 2013 is 68%. Of these 61% are sex/dating messages, 28% are pharmaceutical.

Ref: https://www.allclearid.com/blog/9-cyber-security-facts, http://www.itu.int/en/ITU-D/Partners/Pages/Call4Partners/CYBLDCStats.aspx, http://www.floridatechonline.com/resources/cybersecurity-information-assurance/interesting-facts-on-cybersecurity/#.U_E0PmOQvCY

Cyber Security Opportunities

- Federal government and most foreign governments are quickly staffing up for cyber security
- Job growth for security analysts during 2012-22 is 37% per year (53% by some sources)

Ref: http://motherboard.vice.com/blog/the-cybersecurity-industry-is-hiring-but-young-people-arent-interested, http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

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

A Sample of What Will You Learn?

- Cryptography:
  - Different encryption techniques – DES, AES
  - Different hashing techniques SHA
- Network Security issues and Protocols: SSL (HTTPS)
- How to exchange security keys over public network
- How you can sign a message confirming that you sent it? You can't deny it in a court of law.
- What are certificates?
  How you confirm that you are talking to Amazon?
  Why can't you use Amazon's certificate?
- How to store passwords so that system administrators can't read them?

Prerequisites

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

Prerequisites

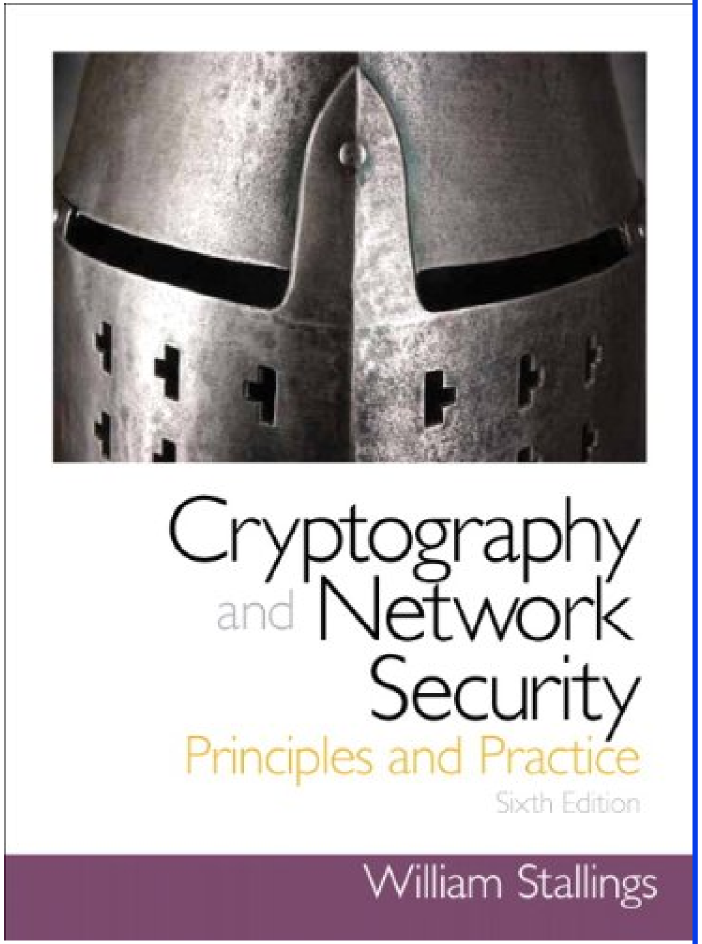
- ISO/OSI reference model
- TCP/IP protocol stack
- Full-Duplex vs. half-duplex
- Cyclic Redundancy Check (CRC)
- CRC Polynomial
- Ethernet
- IEEE 802 MAC Addresses
- Bridging and Routing
- IEEE 802.11 LAN

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**," 6th Edition, Prentice Hall, 2013,
ISBN:0-13-335469-5
- **Required**. Get the latest edition. Do not use older editions. If you use international edition, it should be dated 2013. It should have last page number 731. ISBN: 978-0-13-339469-5, or 0-13-339469-5



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

#	Day	Date	Topic	Chapter
1	Monday	8/25/2014	Course Introduction	
2	Wednesday	8/27/2014	Security Overview	1
			Classical Encryption Techniques	2
	Monday	9/1/2014	Holiday - Labor Day	
3	Wednesday	9/3/2014	Block Ciphers and DES	3
4	Monday	9/8/2014	Basic Concepts in Number Theory and Finite Fields	4
5	Wednesday	9/10/2014	Advanced Encryption Standard (AES)	5
6	Monday	9/15/2014	Block Cipher Operations	6
			Pseudo Random Number Generation and Stream Ciphers	7
7	Wednesday	9/17/2014	Number Theory	8
8	Monday	9/22/2014	Public Key Cryptography	9
9	Wednesday	9/24/2014	Other Public Key Cryptosystems	10
10	Monday	9/29/2014	**Exam 1**	

Tentative Schedule (Cont)

#	Day	Date	Topic	Chapter
11	Wednesday	10/1/2014	Cryptographic Hash Functions	11
12	Monday	10/6/2014	Project Guidelines	
13	Wednesday	10/8/2014	Message Authentication Codes	12
14	Monday	10/13/2014	Digital Signatures	13
15	Wednesday	10/15/2014	Key Management and Distribution	14
16	Monday	10/20/2014	User Authentication Protocols	15
17	Wednesday	10/22/2014	Authentication,Authorization,Accounting (AAA)	16
18	Monday	10/27/2014	Transport Level Security	17
19	Wednesday	10/29/2014	Wireless Network Security (Part 1)	18
20	Monday	11/3/2014	**Exam 2**	18

Tentative Schedule (Cont)

#	Day	Date	Topic	Chapter
21	Wednesday	11/5/2014	Wireless Network Security (Part 2)	
22	Monday	11/10/2014	Project Guidelines (Part 2)	
23	Wednesday	11/12/2014	Wireless Network Security (Part 3)	18
24	Monday	11/17/2014	Electronic Mail Security	19
25	Wednesday	11/19/2014	IP Security	20
26	Monday	11/24/2014	Intrusion Detection	
	Wednesday	11/26/2014	*Thanksgiving Break*	
27	Monday	12/1/2014	TBD	
28	Wednesday	12/3/2014	**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 recent network security topic
  - Select from a list of current topics provided in the class
  - 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.

Project Examples 2011

- Android Trojan Horse
- OpenPacketPro: A libcap extension framework for sniffing outgoing traffic
- A Survey of Recent Advances in Video Security
- A Survey of Cloud Security Issues and Offerings
- Comprehensive Survey of Cyber-Terrorism
- A Survey of Digital Rights Management Technologies
- Survey of Biometrics Security Systems
- A Quick Glance of Digital Watermarking
- A Survey of Privacy and Security Issues in Social Networks
- Cyber Warfare: The Newest Battlefield
- A Survey of Cybercrime
- Virtualization Security in Data Centers and Clouds
- Mobile Device Security
- Tools and Protocols for Anonymity on the Internet
- Survey of Industrial Control Systems Security

Project Examples 2009

- Unseen: An Overview of Steganography and Presentation of Associated Java Application C-Hide
- E-ZeePass: A web-based username and password hash
- A Practical Guide to Honeypots
- A survey of WiMAX security threats
- Social Network Security: A Brief Overview of Risks and Solutions
- A Survey of Kerberos V and Public-Key Kerberos Security
- Security in Private Networks of Appliance Sensors and Actuators
- Access Control Service Oriented Architecture Security
- Understanding Worms, Their Behavior and Containing Them
- A Survey of WiMAX and Mobile Broadband Security
- A Survey on the Security of Virtual Machines
- Cloud Computing Challenges and Related Security Issues

Project Examples 2007

- Cafe Cracks: Attacks on Unsecured Wireless Networks
- Net Vigilant: Network Monitor
- Secure Data Exchange System: Minimizing Security Attacks Risks while Preserving Bandwidth
- PHP Vulnerabilities in Web Servers
- Type 2 Cross-site Scripting: An Attack Demonstration
- Hacking Organizations, Conferences, Publications, and Effects on Society
- Web Single Sign-On Systems
- Wireless Hacking Tools
- Survey of Current Network Intrusion Detection Techniques
- A Survey of the Prominent Quantum Key Distribution Protocols
- Secure Ballots Using Quantum Cryptography
- A Survey of Peer-to-Peer Network Security Issues
- Generic Security Services Application Programming Interface

Project Schedule

Mon 10/6/14	Topic Selection/Proposal
Mon 10/13/11	References Due
Mon 10/20/11	Outline Due
Mon 11/10/11	Final Report/Demo Due
Mon 11/17/11	Reviews/comments Returned
Mon 11/24/11	Revised Report Due

Office Hours

- Monday: 12 Noon to 1 PM
  Wednesday: 12 Noon to 1 PM
- Office: Bryan 523
- **Teaching Assistant**: Yijian Li, yijianlikaka@gmail.com
  Office Hours: Thursday 1-2PM, Sunday 1-2PM
- CSE 571 Security Lab: Bryan 516
  (Only remotely accessible)

Exams

- Exams consist of numerical, fill-in-the-blank and multiple-choice (true-false) questions.
- There is negative grading on incorrect multiple-choice questions. Grade: +1 for correct. -1/(n-1) for incorrect.
  ⇒ For True-False: +1 for Correct, -1 for Incorrect
  This ensures that random marking will produce an average of 0.
- Everyone including the graduating students are graded the same way.
- Highest score achieved becomes 100% for that exam.
  ⇒ Measures relative performance of the student
  Effect of all other factors, such as time allotted, hardness of questions are eliminated.

Exams (Cont)

- All exams are closed book.
  One 8.5”X11” cheat sheet with your notes on both sides is allowed.
- No smart phones allowed.
  Only simple TI-30 or equivalent calculator allowed for calculations.
- Exam dates are fixed and there are no substitute exams
  ⇒ Plan your travel accordingly.
- Best of the two mid-terms is used.

Homework Submission

- All homeworks are due on the following Monday at the beginning of the class unless specified otherwise.
- Any late submissions, if allowed, will *always* have a penalty.
- All homeworks should be submitted in hardcopy
- All homeworks are identified by the class handout number.
- All homeworks should be on a separate sheet.
  Your name should be on every page.
- 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.

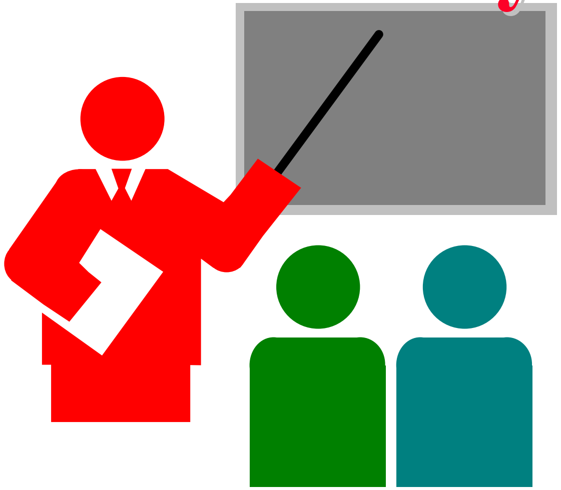
Quizzes

- There will be a short 5-minute quiz at the beginning of each class to check if you have read the topics covered in the last class.

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

Lab Homework 1: Gathering Info

- Execute the following commands on windows DOS box and try all variations:
  - ipconfig /help
  - ping /help
  - arp /help
  - netsh
    - >Help
  - nslookup
    - >help
  - tracert -?
  - netstat /help
  - route /help

<u>On MAC/Linux</u>

- man ifconfig
- man ping
- man arp
- man nslookup
- man tracert
- man netstat
- man route

- 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. Use netsh to 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?

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: ___________