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/cse571-17/

Overview

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

Cyber Security Facts

- Cyber crime cost could hit $6 Trillion annually by 2021.
- Over 169 million personal records were exposed in 781 publicized breaches in 1015
- In 2015 38 percent more security incidents detected in 2015 than in 2014
- Majority (91.3%) of malware use DNS to carry out attack
- Browser extensions are used to steal data and account information
- Use of HTTPS is increasing reducing the effectiveness of firewalls

Ref: https://swimlane.com/10-hard-hitting-cyber-security-statistics/
Cisco 2016 Annual Security Report, http://www.cisco.com/c/m/en_us/offers/sc04/2016-annual-security-report/index.html
CSO, "Top 5 cybersecurity facts, figures, and statistics for 2017,"
http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

Cyber Warfare

- Security of computers, companies, smart grid, and nations
- Nation States are penetrating other nations computers
  5th domain of warfare (after land, sea, air, space)
- In 2010, US set up US Cyber Command
- UK, China, Russia, Israel, North Korea have similar centers
- Many cyber wars: North Korea vs. USA, Israel vs. Syria, South Korea vs. North Korea, India vs. Pakistan, …

Old

New

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

DEFCON 2015

DEFCON 2015 (Cont)

- Hacking a Linux rifle
- Hacking smart safes
- Wirelessly steal cars
- Hack a Tesla
- Hack ZigBee
- Hacking IoT baby monitors
- Hacking FitBit Aria
- Cracking crypto currency
- Hack out of home detention
- Insteon's false security
- Hacking RFID, NFC
- DARPA Cyber Grand Challenge **$2M**

Ref: https://www.ethicalhacker.net/features/opinions/first-timers-experience-black-hat-defcon

Cyber Security Opportunities

- Federal government and most foreign governments are quickly staffing up for cyber security
- Unfilled cyber security jobs could reach 1.5 million by 2019

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

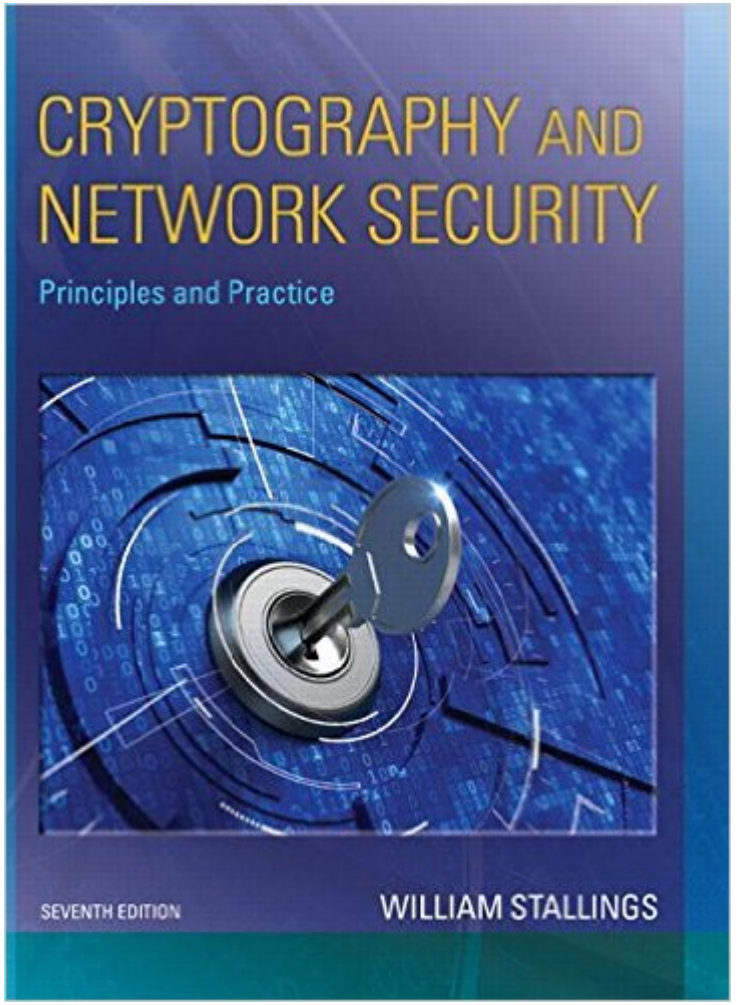
- ISO/OSI reference model
- TCP/IP protocol stack
- Full-Duplex vs. half-duplex
- Cyclic Redundancy Check (CRC)
- CRC Polynomial
- Ethernet
- IEEE 802 MAC Addresses
- Bridging and Routing
- IEEE 802.11 LAN

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**," 7th Edition, Pearson, 2017, ISBN:1-292-15858-1
- **Required**. Get the latest edition. Do not use older editions. If you use international edition, it should be dated 2017.



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	Ch.
1	Wed	1/18	Security Overview	1
2	Mon	1/23	Block Ciphers and DES	3
3	Wed	1/25	Basic Concepts in Number Theory and Finite Fields	4
4	Mon	1/30	Advanced Encryption Standard (AES)	5
5	Wed	2/1	Block Cipher Operations	6
6	Mon	2/6	Pseudo Random Number Generation and Stream Ciphers	7
7	Wed	2/8	Number Theory	8
8	**Mon**	**2/13**	**Exam 1**	

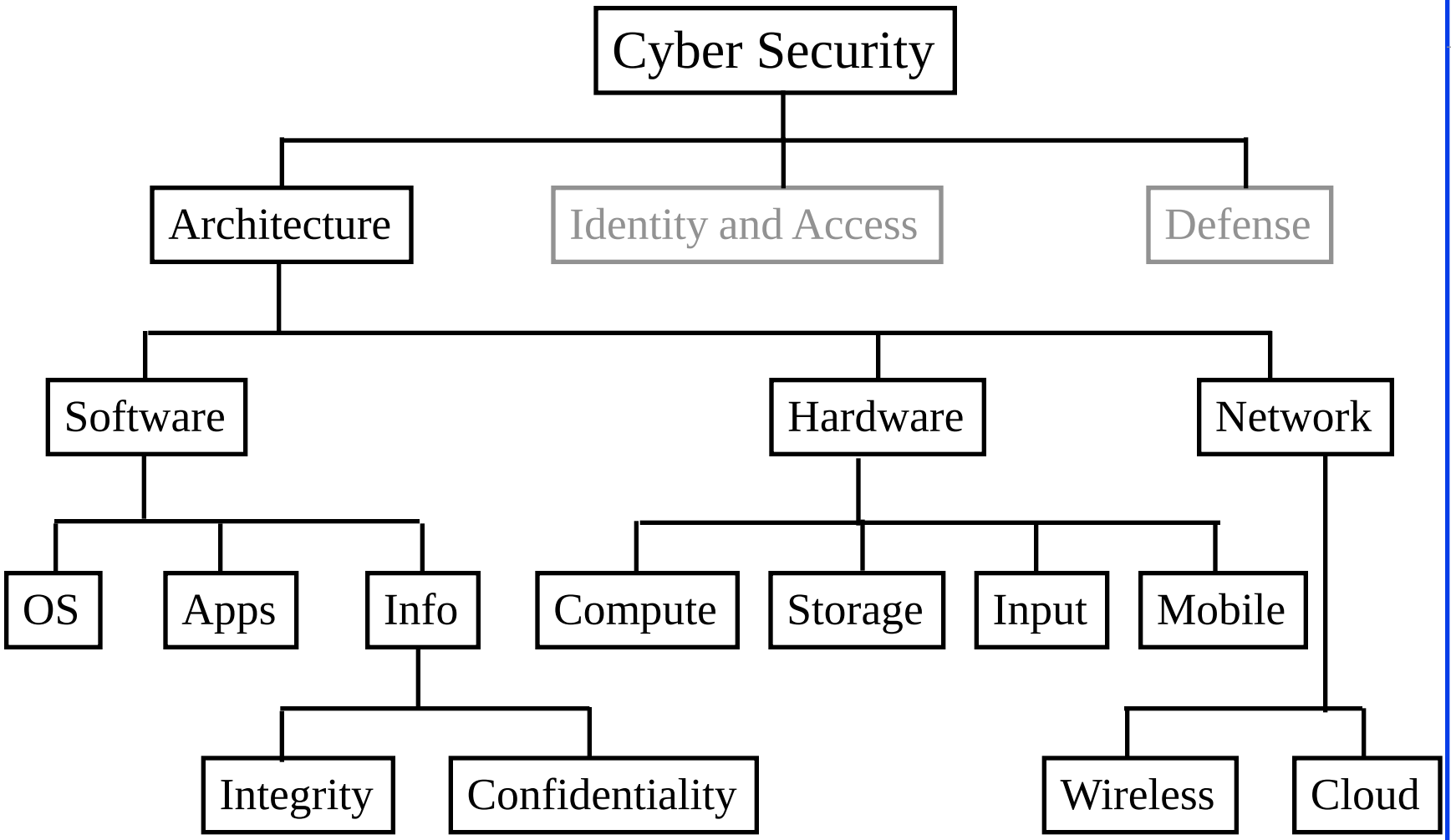
Tentative Schedule (Cont)

#	Day	Date	Topic	Ch.
9	Wed	2/15	Public Key Cryptography	9
10	Mon	2/20	Other Public Key Cryptosystems	10
11	Wed	2/22	Cryptographic Hash Functions	11
12	Mon	2/27	Message Authentication Codes	12
13	Wed	3/1	Digital Signatures	13
14	Mon	3/6	Key Management and Distribution	14
15	Wed	3/8	User Authentication Protocols, AAA, Single-Sign On	15
	Mon	*3/13*	*Spring Break*	
	Wed	*3/15*	*Spring Break*	
16	**Mon**	**3/20**	**Exam 2**	

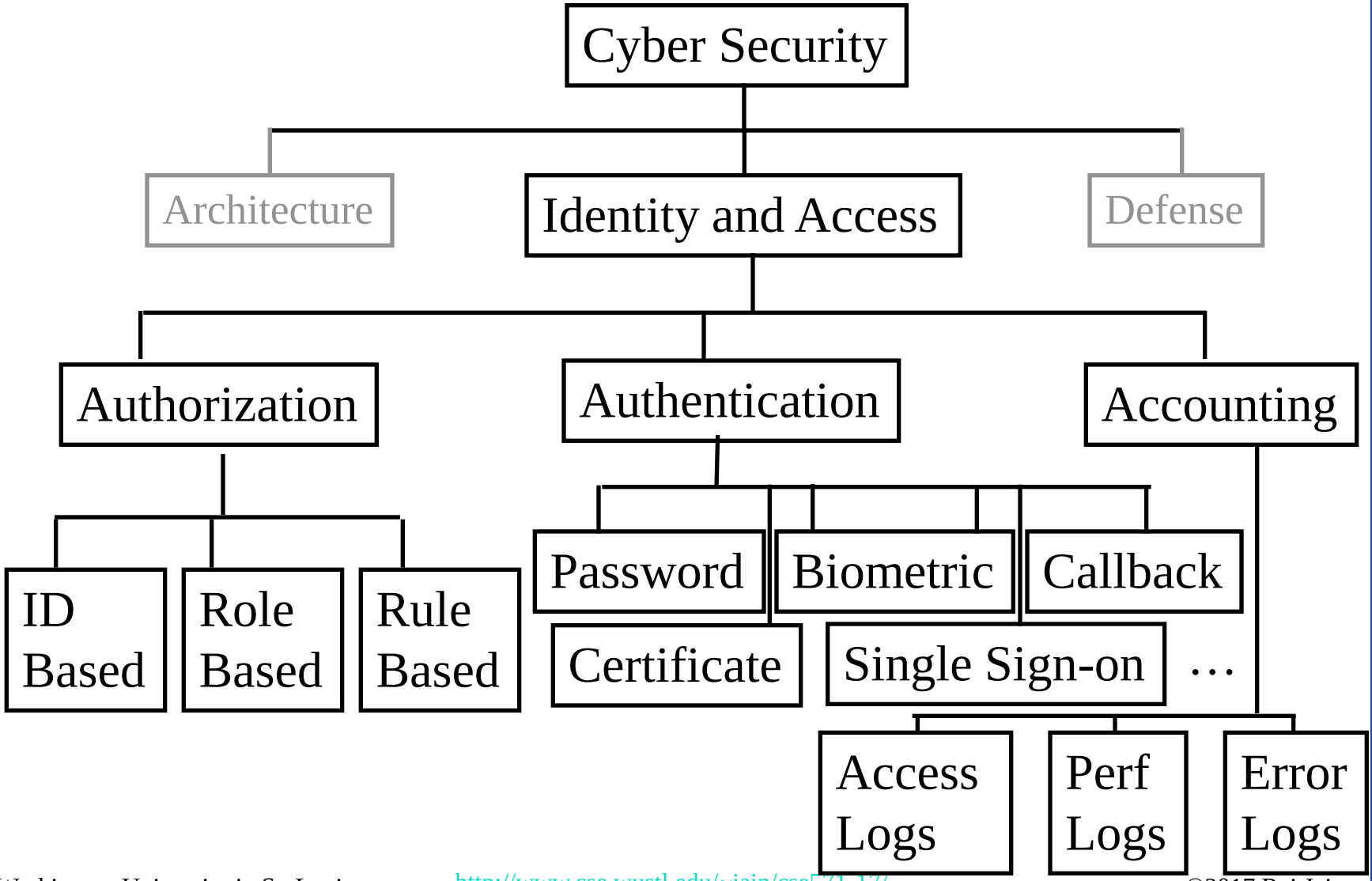
Tentative Schedule (Cont)

#	Day	Date	Topic	Ch.
17	Wed	3/22	Network Access Control and Cloud Security	16
18	Mon	3/27	Transport Level Security	17
19	Wed	3/29	Wireless Network Security	18
20	Mon	4/3	Electronic Mail Security	19
21	Wed	4/5	IP Security	20
22	Mon	4/10	Malicious Software	21
23	Wed	4/12	Intrusion Detection, Firewalls, VPN	22
24	Mon	4/17	Forensics	
25	Wed	4/19	Cryptocurrencies and Blockchains	
26	Mon	4/24	Security Standards and Laws	
27	**Wed**	**4/26**	**Final Exam**	

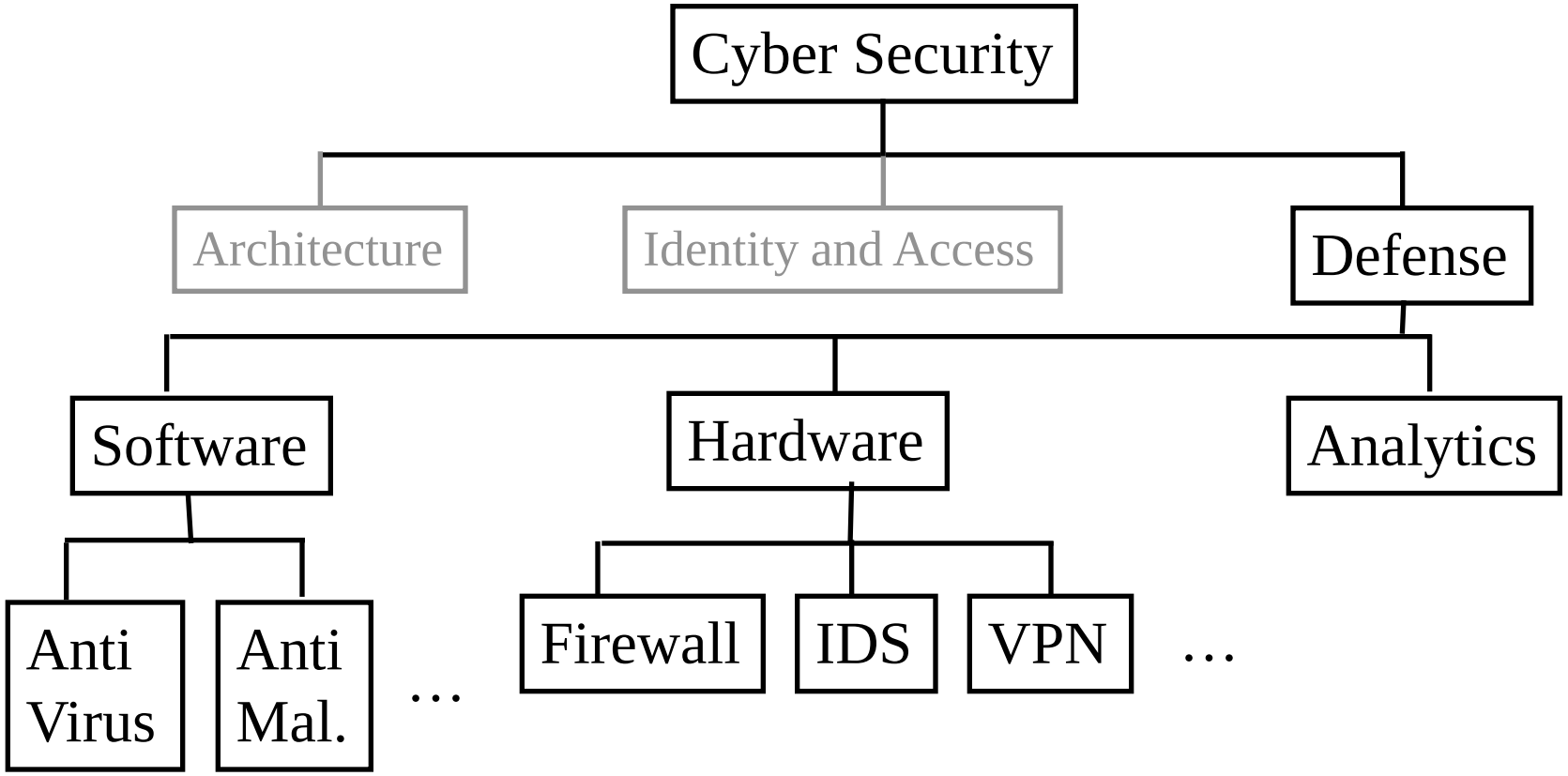
Cyber Security: Complete Picture



Complete Picture (Cont)



Complete Picture (Cont)



- Software, hardware distinction is arbitrary.
- Analytics can be applied to any counter-measure
- Also need to know security/privacy laws and standards

Exams

- There are two mid-terms and one final exam.
- All exams are 1 hour long. One note sheet of 8.5”x11” (both sides) is allowed along with a simple calculator (TI-30).
- 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 seniors are graded the same way.
- Your grade depends upon the performance of the rest of the class.

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
  $\Rightarrow$ Plan your travel accordingly.
- Best of the two mid-terms is used.

Grading

- Mid-Term Exams (Best of 2) 30%
- Final Exam 30%
- Class participation 5%
- Homeworks 20%
- Labs 15%

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.
- The first page of all homeworks/labs submitted should be blank with only your name on the top-right corner

Homework Grading

- Grading basis: Method + Correct answer
- Show how you got your answer
  - Show intermediate calculations.
  - Show equations or formulas used.
  - If you use a spreadsheet, a statistical package, or write a program, print it out and turn it in with the homework.
  - For Excel, set the print area and scale the page accordingly to fit to a page. (See Page Setup)

Quizzes

- There may 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.

Academic Integrity

- Academic integrity is expected in homeworks
- All solutions submitted are expected to be yours and not copied from others or from solution manuals or from Internet
- All integrity violations will be reported to the department and action taken

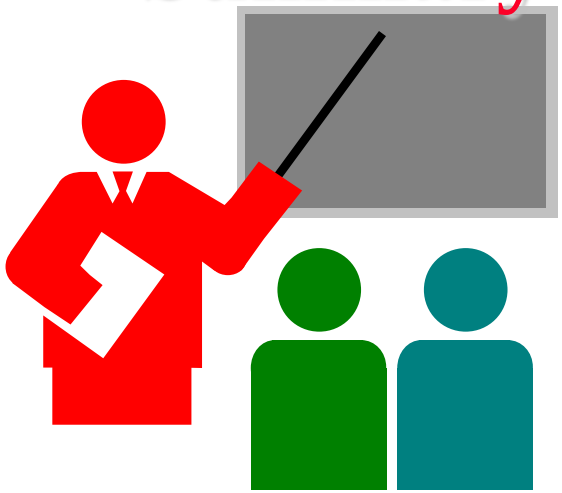
Office Hours

- Monday: 11:00AM to 12:00 noon
  Wednesday: 11:00AM to 12:00noon
  (By appointment only)
- Office: Jolly 208
- Teaching Assistants:
  - Tara Salman, tara.salman@wustl.edu
  - Jolly 323 Thursday/Sunday 1PM-2PM

Class Discussions

- We will use Piazza for class discussion.
- Find our class page at: https://piazza.com/wustl/fall2017/cse571/home
- You can sign up at: https://piazza.com/wustl/fall2017/cse571

Summary



- Goal: To prepare you for a cyber security job
- 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

On MAC/Linux

- 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

Lab Homework 1 (Cont)

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

o o Subnet mask of 255.255.255.254 will allow 254 nodes on the LAN.

o o Time to live (TTL) of 8 means that the packet can travel at most 8 hops.

o o IP Address 128.256.210.12 is an invalid IP address

o o DHCP server is used for dynamic IP address assignment

o o DNS helps translate an name to MAC address

o o Port 80 is used for FTP.

o o IPv6 addresses are 32 bits long.

o o New connection setup message in TCP contains a syn flag.

o o 192.168.0.1 is a public address.

Marks = Correct Answers _____ - Incorrect Answers _____ = _____

Acronyms

- AES Advanced Encryption Standard
- ARP Address Resolution Protocol (ARP)
- CRC Cyclic Redundancy Check (CRC)
- CSO Chief Security Officer
- DARPA Defense Advanced Research Project Agency
- DEFCON D-E-F Conference
- DES Data Encryption Standard
- DHCP Dynamic Host Control Protocol
- DNS Domain Name System
- DOS Denial of Service
- FTP File Transfer Protocol
- HTTP Hypertext Transfer Protocol
- HTTPS Secur Hyper-Text Transfer Protocol
- ICMP Internet Control Message Protocol (ICMP)
- ID Identifier
- IDS Intrusion Detection

Acronyms (Cont)

- IEEE Institution of Electric and Electronics Engineers
- IoT Internet of Things
- IP Internet Protocol
- IPv6 Internet Protocol Version 6
- ISO International Standards Organization
- LAN Local Area Network
- MAC Media Access Control
- NFC Near Field Communication
- OS Operating System
- OSI Open System Interconnection
- RFID Radio Frequency Identifier
- SHA Secure Hash Algorithm
- TCP Transmission Control Protocol
- TI Texas Instruments
- TTL Time to Live
- UDP User Datagram Protocol
- VPN Virtual Private Network

Scan This to Download These Slides

Raj Jain
http://rajjain.com

Related Modules

CSE571S: Network Security (Spring 2017),
http://www.cse.wustl.edu/~jain/cse571-17/index.html

CSE473S: Introduction to Computer Networks (Fall 2016),
http://www.cse.wustl.edu/~jain/cse473-16/index.html

Wireless and Mobile Networking (Spring 2016),
http://www.cse.wustl.edu/~jain/cse574-16/index.html

CSE571S: Network Security (Fall 2014),
http://www.cse.wustl.edu/~jain/cse571-14/index.html

Audio/Video Recordings and Podcasts of
Professor Raj Jain's Lectures,
https://www.youtube.com/channel/UCN4-5wzNP9-ruOzQMs-8NUw