Assignment - PSO 5

Purdue CS426 - Computer Security - Prof. Spafford

Harris Christiansen - February 21, 2018
christih@purdue.edu

Read the following:

- TCP/IP Five Layer Software Model: microchipdeveloper.com/tcpip:tcp-ip-five-layer-model
- Promiscuous Mode: https://en.wikipedia.org/wiki/Promiscuous_mode
- Routing Table: https://en.wikipedia.org/wiki/Routing_table
- Roger Boisjoly: https://en.wikipedia.org/wiki/Roger_Boisjoly
- ACM Code of Ethics: www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

Problem 1

List the layers of the TCP/IP 5 layer model. In your own words and in a few sentences explain what each layer does. (50 pts.)

- 1. Physical Layer: The base layer which is responsible for all communication in/out of the device. Includes the transceiver for sending/receiving bits of data.
- 2. Data Link Layer: Encodes and decodes data into frames (which house the data packets and include source and destination info in the form of MAC address).
- 3. Network Layer: Sends and receives data packets, using IP address to specify source and destination.
- 4. Transport Layer: Responsible for establishing a connection between hosts, and tracking assigned port numbers and the status of active connections. Connections are formed using TCP (which ensures that every messages makes it to the destination, and in the correct order) or UDP (which allows messages to be sent at a very high rate, with no guarantee of delivery or order).
- 5. Application Layer: Applications and programs, which can use the transport layer to send data between devices. Users mostly interact with applications which exist in the application layer.

Problem 2

(40 pts.)

What does the acronym MAC stand for in terms of the data link layer?

- Media Access Control

How many bytes is a MAC address for Ethernet?

- Ethernet (802.3) mac addresses are 6 bytes.

How does a network interface and operating system use a MAC address when receiving packets?

- Answer

Describe promiscuous mode with respect to network interface and MAC addresses.

- Answer

Problem 3

(20 pts)

(Based on a Cisco Interview Question) What information does an operating system get back from the system's IP routing table?

- The IP routing table contains the following information:
  - Network ID
  - Subnet mask (which is used to determine the network ID from the IP address)
  - Forwarding address
  - Receiving and forwarding port number
  - Priority/metric (usually determined from number of hops necessary to reach destination)
- The operating system uses this information to determine how to route a data packet for a particular network to the appropriate destination.

Before a system can send a packet using the information from the Routing table, it must make a query to the ARP cache. Why is this the case?

- ARP (address resolution protocol) is used to resolve an IP address to a MAC address.
- This is necessary as the IP routing table stores clients by IP address, and MAC addresses are needed by the physical layer to specify source and destination. ARP resolution takes place on Layer 2 of the TCP/IP model.
- ARP works by broadcasting a query packet (using the MAC address ff:ff:ff:ff:ff:ff), and receives a response with the destination hosts MAC address.

Problem 4

Fill in the blanks and explain: An ARP request attempts to resolve a/an _____ to a/an _____. (30 pts.)

- An ARP request attempts to resolve an IP address to a MAC address.
- MAC addresses are used to reach another machine when sending data, and are important for the physical and data link layers which uses MAC addresses to specify source and destination.
- If an ARP request cannot resolve an IP address to a MAC address, communication cannot occur.

Problem 5

Describe what happens when an ARP request is spoofed and why an attacker would want to spoof an ARP request. (40 pts.)

- Spoofing an ARP request allows an attacker to intercept an ARP request, and return an incorrect MAC address to the requester. If the attacker can do this quick enough, they can fool other machines into sending messages meant for one target IP to a machine of their choice (such as themselves).
- This can be used to fool clients on a network into associating your MAC address with the IP of another machine, allowing you to intercept data frames intended for the recipient, as well as modify or even halt all traffic.

Problem 6

(40 pts.)

DNS resolves a/an _____ and returns a/an _____. Why does this need to happen?

- DNS resolves a hostname and returns an IP address.
- This is necessary as the network uses IP addresses to specify destination, so hostnames (such as in URLs) must be resoles to an IP address.
- DNS works by maintaining a known local cache (with expiration times) which it can use for quick resolution. If a hostname is not in the local cache, it must be queried on a

nameserver, which will recursively query for the hostname until it finds a resolution, and then return it to the requestor.

How do DNS and DNSSEC differ?

- DNS is necessary, but inherently vulnerable. Attackers can create bogus nameserver entries, which if used by a client, can cause DNS to resolve a hostname to an incorrect (potentially malicious) IP address. This can be used to send clients to bogus, phishing webservers, even though they have the correct url.
- DNSSEC secures this vulnerability, using public-key cryptography to sign DNS entries, and can be used to verify the DNS resolution you receive is the correct address.

Why would you want to use DNSSEC?

- Using DNSSEC is important if you think attackers might want to (or can gain something from) hijacking traffic to your hostname and sending it to their own servers.
- As such, DNSSEC is very important for financial websites/services, governments, corporations, healthcare, and more.

Problem 7

Explain why this statement is true or false. When using WiFi you do not have to worry about someone eavesdropping because you do not share wires with other machines (20 pts.)

- False. You are still just as susceptible to many forms of eavesdropping.
- For one, the router or the connection upstream of the router could be malicious, and could be recording all network traffic.
- In addition, using ARP spoofing, another client on your same network could be intercepting and even modifying your network traffic.

Problem 8

Explain why laws and regulations should be a "lower bound" on ethical practices. (20 pts.)

- Laws and regulations are the absolute requirements which must be upheld, especially when considering security.
- Any corporation or entity can do much more than the absolute requirements when it comes to security, including ensuring that data and systems are secure and cannot be tampered with or experience unauthorized access.

- Many ethical practices are not required by law, but should still be followed, if you want to be morally good and secure.

Problem 9

Read the articles below and feel free to explore other sources as needed.

- NY Times: https://www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html
- CNN: https://www.cnn.com/2018/03/20/politics/alexander-nix-cambridge-analytica/index.html

Briefly describe the situation with Facebook, Russian Election meddling through Facebook, and Cambridge Analytica. Identify at least 3 ethical issues raised here and explain/justify what the ethical action is in the situation. State whether the company or individual took the ethical action you identified and if not, explain why not. (60 pts.)

- Answer

Problem 10

(60 pts.)

Name 3 companies that generate revenue by using information collected from their users. Explain your answer and explain if you think users are fully aware of how they are a part of the business model.

- **Google:** One of Google's primary purposes is data collection on it's users. Google collects and uses data for everything, including search, gmail, maps, drive, android, voice, chrome, and more.
  - This data is used for a variety of purposes, including analytics, advertising, data sourcing, bug tracking, and also profit (by selling the data to other businesses).
  - For instance, maps data is used to maintain accurate maps, calculate realtime traffic information, and even track where you go and what you do (for recent destinations and advertising).
  - Google is known to be a top data collector, but users do not realize what all data is collected and what it is used for.
-

Identify 2 ethical obligations a software developer should have when working inside such a company when it comes to the data of the end users.

- Software developers should make sure that a specific security and data access plan is in place for the protection of user data, as well as make sure that it is properly enforced across all systems.
- Software developers should write tests and perform security audits on code to ensure that no bugs or vulnerabilities exist which could expose user data (in any sort) to an unauthorized user.

Problem 11

As a primer to the lectures on ethics, laws, and regulations watch the documentary on the Challenger Disaster (1.5 hrs)

- https://www.youtube.com/watch?v=P9LSerNokJk

- The key companies and governmental agencies involved- The key people involved (20 pts)
  - Answer

- The series of events from the first concern of an issue well before the launch, the critical meeting before the launch disaster, and the investigation after the incident (30 pts)
  - Answer

- What external pressure was NASA under from the general public and how did it impact their decision making? What external pressure was NASA under when it came to asking funding from the government and how did it impact what they communicated when attempting to secure funding? (40 pts.)
  - Answer

- What external pressures were Morton Thiokol employees faced with? (30 pts.)
  - Answer

- Use this incident as an example. Describe how communication style plays into effectively convincing supervisors of risks. Will a collaborative communication style always work? Explain. (30 pts.)
  - Answer

- Use this incident as an example. Describe how indirectly expressing disappointment as a supervisor or client as NASA did impacts decision making of subordinates/contractors. (30 pts.)
  - Answer

- What if anything would you think you would have done differently if you were one of the technical experts in this situation? Explain your answer in at least a paragraph. (30 pts.)
  - Answer

- The Challenger Disaster is often used as a case study in several disciplines. Identify 3 possible scenarios that you may encounter as you start out in industry or graduate school where you may be pressured by external factors to ignore technically sound or ethical practices. Describe the situation, sources of external pressure, and how you could see yourself handling the situation. (60 pts.)
  - Answer