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?

- Packets sent to a specific MAC address should only be received by machines with that MAC address. The MAC address specifies the destination machine on the LAN. The special MAC address FF:FF:FF:FF:FF:FF allows a message to be broadcast to all machines on a LAN, and is used for ARP discovery.

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

- Promiscuous mode forwards all network traffic a device receives to the CPU, regardless of intended destination. This can be used for packet sniffing on a LAN network.
- A non-routing node in promiscuous mode can typically just read/monitor/record network traffic on the LAN, but cannot modify.
- If a routing node is in promiscuous mode, it is possible for it to alter data and relay on the modified data.
- Promiscuous mode is also helpful for non-malicious purposes, such as diagnosing network issues and determining traffic loads.

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, but MAC addresses are needed by the physical layer to specify source and destination on a LAN. ARP resolution takes place on Layer 2 of the TCP/IP model.
- ARP works by broadcasting a query packet to all devices (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.)

- Facebook collects an enormous amount of data on it's users, and utilizes this data to make inferences about it's users. It determines users position among a large variety of categories, including political views, sex, relationship status, social trends, travel, and many more. This information is shared with advertisers and others who pay for the data.
- It has become known that during the recent 2016 U.S. Presidential Election, Russia and Cambridge Analytica were able to use this data to determine the likely outcome of the election, as well as how to manipulate results based on analyzing regional data and knowing who to target.
- Cambridge Analytica CEO Alexander Nix was even caught on camera discussing potential bribery and entrapment, which are illegal, yet alone unethical.

- There are several ethical issues with this:
  - Facebook permitted access to almost all users data, including very sensitive information, which allowed third parties to analyze, target, and draw conclusions on users from this data. This data was possible by apps requesting access to your data, but being permitted access to even friends of friends data.
  - Cambridge Analytica exploited this data source for malicious, potentially illegal purposes. They worked with and shared this data and conclusions with any interested paying party, even Russian groups interested in manipulating the U.S. Presidential Election.
  - Russian Groups: It is an ethical issue to attempt to meddle with and influence an election, especially an election for another country. Russian groups should not have been able to obtain the data they did, and their influence should have been discovered much earlier, by organizations such as the NSA.

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.
- **Amazon:** Amazon can substantially increase their profits using targeted advertisements and recommendations, as well as making it easier for users to make purchases. As such, they collect lots of user data.

    - With the breadth of products Amazon has recently released, including Alexa, Amazon has lots of points to collect data from, including search/browsing history, purchase history, voice, and cookies.
    - Many Amazon users are aware their data is being used to make recommendations/ads, but have no idea what other purposes their data is used for.
- **Equifax:** Credit bureaus generate all their revenue from collecting and selling data about users.
    - They primarily collect financial records, including bank accounts, credit accounts, loans, debts, assets, income, and expenses. However, they also work to collect additional data, which they can profit from.
    - Most users, especially before the recent large Equifax leak, are unfamiliar with data collected by credit bureaus, who has access to it, 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)
    - Robert Boisjoly was a rocket booster engineer at Morton Thiokol and one of the first to notice and raise concerns about defective O-rings. He noticed during an early post-flight inspection that hot gasses had compromised several O-rings, and continuously raised objections leading up to the Challenger launch. He knew the solid rocket boosters were likely to blame for the explosion.
    - Morton Thiokol: Contractor responsible for designing the solid rocket booster and O-rights. Discovered and knew the O-rings could be compromised by deformation of the

rocket booster shell. They even recommended NASA delay the launch, due to the issues as well as very low overnight temperatures the night before the launch.

- NASA: Organization responsible for space exploration and orchestrating shuttle flights, including the Challenger.
- Presidential Commission: Board of scientists, politicians, astronauts, and military officers tasked with determining what happened following the Challenger explosion

- 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)

- Robert Boisjoly discovers compromised (burned) O-rings during a routine post-flight inspection.
- Robert Boisjoly wrote an internal memo in July 1985 to Morton Thiokol raising concerns about fault design that could lead to catastrophic failure, but was ignored.
- After several more memos, an internal task force (including Boisjoly) was setup to investigate the issue, but still lead to no action.
- Due to action by Boisjoly and colleagues, Morton Thiokol managers finally agreed the launch should be postponed due to the issue. The night before the launch, during the go/no-go telephone conference, Morton Thiokol recommended NASA postpone the launch. NASA does not want to abort without hard evidence, and Thiokol backs down from fighting for a postpone.
- Cold temperatures the night before the launch cause even more concern for damage to parts and a catastrophic failure. These temperatures were far below specifications for many parts, including the O-rings on Morton Thiokol's rocket boosters.
- The Presidential Commission (mentioned above) is formed to determine the cause of the accident. Biosjoly testifies and tells the commission the accident was almost certainly the cause of failed rocket boosters, likely due to failed O-rings.
- The commission, and ultimately the U.S. House release reports determining the O-rings were the cause, and the accident occurred as a result of years of poor technical decision making among management of those involved.

- 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.)

- Previous failed/delayed launches led to news agencies posting bad press about NASA, and put pressure on NASA to launch a flight on schedule.
- NASA engineers took the negative public feedback very personally, and felt pressure to deliver a successful launch.
- Historically high expenses put pressure to complete a working shuttle to prove value.
- To receive additional funding from the government, NASA needed to demonstrate successful shuttle missions as well as continued development progress.
- To receive additional funding from Congress, NASA committed to an unrealistic launch frequency schedule.

- What external pressures were Morton Thiokol employees faced with? (30 pts.)
  - Engineers knew there was an issue, but management was reluctant to listen.
  - Engineers had the burden of proof, with little time, to gather evidence to show the flight should be postponed due to defective parts.
  - NASA was angry with Thiokol for introducing additional launch criteria (temperature), and for delaying launches. They threatened Thiokol to "really think about this decision".
  - Liability concerns are always an issue when a sub-contractor has to admit fault.

- 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.)
  - It's important for all parties involved to be aware of all risks, including time, development, security, and safety risks. The engineers often understand the risks the most, but it's managements job to decide which risks are ok and which are not.
  - In the Challenger example, action should have been taken promptly when Boisjoly discovered the issue, and NASA should have immediately been made aware. Sharing this information early could have revised launch schedules and deadlines around safety.
  - With collaborative communication, it's impossible for everyone to know everything, and even more impossible for management to be deeply familiar with every issue. It's important a chain of command is in place, and all issues are dealt with properly by the earliest person in the chain. If information potentially impacts other portions of the company, that information needs to be shared with those it impacts.

- 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.)
  - Expressing disappointment is a very real pressure that makes it clear you are not happy with a decision. In the corporate world, companies fight for bids, and disappointing a client can cause you to lose future work/money.
  - The pressure caused by expressing disappointment can lead to decisions being made which are not in the best interest of the product or safety, but instead are aimed solely at pleasing the client.
  - In the Challenger example, NASA expressing disappointment caused the management of Morton Thiokol to have a private meeting where they ultimately decided it was in their best interest not to fight for the launch to be postponed.

- 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.)
  - First, a surprisingly few number of engineers seemed to be fighting for the issue. A team of engineers should have early on prepared a report detailing the issue (with tests demonstrating the severity), and this report should have been shared with NASA.
  - After the defect was discovered, there should have been regular meetings with Thiokol and NASA discussing the current state of the problem, determining solutions, and revising launch schedules if necessary.

- 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.)
  - Software engineering at a large company, where you might be pressured by a manager to complete a project by deadline, even if it means releasing with security vulnerabilities, which could even expose sensitive user data.
    - Could be handled by expressing (or even demonstrating) concerns, what data is vulnerable, and what policy is regarding that data.
    - May also be handled by reducing features and delaying them to a future update.

- Designing a hardware product where production costs limit the quality of parts and safety mechanisms. Poor wiring design or lack of safety mechanisms could lead to a fire, or other mechanical malfunctions, which could put the user in danger.
  - Could be handled by reducing features or delaying production, so you can ensure all components are properly designed and cannot have safety issues.
- Working manual labor where not all safety equipment is provided/used, or not all safety procedures are followed. For example:
  - Parachuting from an airplane where the jump instructor is lazy and does not double-check everyone's shoots and harnesses. In this case, establishing and enforcing procedures is an absolute must, and as safety is directly at risk, the issue should be raised to managers/outside enforcers.