Seth Lunders

CS336 Homework Assignment #6

Due: Friday Dec 10th, 2021 5:00pm.

Points: 100 pts

1. (10 pts) Can link and end-to-end encryption both be used on the same communication? What would be the advantage of that? Cite a situation in which both forms of encryption might be desirable.
    a. Yes, they can both be used. If I'm sending sensitive information over a network, I could encrypt the info at the application level, *and* as it is being transferred over the network. Then if the network encryption fails, the data is still protected by the end-to-end encryption.
2. (10 pts) Recall that packet reordering and reassembly occurs at the transport level of the TCP/IP protocol suite. A firewall will operate at a lower layer, either the internet or data layer. How can a stateful inspection firewall determine anything about a traffic stream when the stream may be out of order or damaged?
    a. From what I understand, a stateful inspection firewall doesn't necessarily care what is *in* the packages, but where they are coming from and how many. Our book gives this example: say a certain IP tries to connect to port 1, then port 2, then 3, then 4 and so on, one right after the other. At a certain point, the firewall will determine that the IP address is malicious and can then block access from it.
3. (5 pts) Cite a reason that an organization might want two or more firewalls on a single network.
    a. They may have different levels of security for different users/connection types. The UIdaho CS servers may be a good example of this. Devices *outside* the UI network are prohibited from connecting to the CS servers, but can still access some UI services, like VandalWeb. Only devices *inside* the UI network (or using the VPN) have access to the CS servers.
4. (5 pts) One form of IDS starts operation by generating an alert for every action. Over time, the administrator adjusts the setting of the IDS so that common, benign activities do not generate alarms. What are the advantages and disadvantages of this design for an IDS?
    a. Advantages: The administrator now has time for potentially more important tasks, and there are fewer false positives.
    b. Disadvantages: It is more likely that a malicious action will not get reported, if the attacker can make it seem benign.
5. (5 pts) Should a network administrator put a firewall in front of a honeypot? Why or why not?
    a. A honeypot works on the idea that the attacker doesn't *know* they're being monitored. I would think you would want some sort of believable firewall, even if it does have some flaw they can exploit to get around it.
6. (10 pts) How can a website distinguish between lack of capacity and a denial-of-service attack? For example, websites often experience a tremendous increase in volume of traffic right after an advertisement with the site's URL is shown on television during the broadcast of a popular sporting event. That spike in usage is the result of normal access that happens to occur at the same time. How can a site determine that high traffic is reasonable?

    a. Tracking the source of the traffic could help the site determine if the traffic is legitimate. If there is a lot of traffic coming from relatively few IP addresses, it’s more likely that they are being attacked. Also, I would expect the advertisers would have some idea of the estimated traffic after an ad has run. If they know their infrastructure can handle that much traffic, but it is still being overwhelmed, it’s more likely to be a DoS attack.

7. (5 pts) Explain why spam senders frequently change from one email address and one domain to another. Explain why changing the address does not prevent their victims from responding to their messages.
    a. If the spammers didn’t use various emails, stopping them would be as easy as blocking their one address. By using many emails, it’s much harder to keep track of and block all of them.
    b. Furthermore, emails can be set up to go to the same account, so the spammers could have many different accounts to send from, but still easily manage incoming emails.
8. (10 pts) Why does a web server need to know the address, browser type, and cookies for a requesting client?
    a. The web server needs to know the address so it knows what information the user is requesting (e.g. google.com for search vs images.google.com for image search) I’m a little unsure why the server needs to know the browser type. It could be to ensure they are sending a version of the web page that the browser can properly display (like a mobile version of site on a smartphone). The server needs the cookies for authentication purposes between webpages on the same site, and likely for collecting user data for profit.
9. (5 pts) What is clickjacking attack? Suggest a technique by which a browser could detect and block clickjacking attacks?
    a. A clickjacking attack takes place when elements on a webpage are so positioned that the user *thinks* they are clicking on one link while they are *actually* clicking on an invisible link ‘between’ their cursor and the button they wanted to press.
    b. One possible way a browser could help you avoid clickjacking attacks is to check if links overlap each other, and if they do, ask the user for confirmation before sending them to the page.
10. (10 pts) You have forgotten your password, so you click on “forgot my password” to have a new password sent by email. Sometimes the site tells you what your password was; other times, it sends you a new (usually temporary) password. What are the privacy implications of each approach?
    a. The second option is better. For the site to be able to tell you your password, it has to have a plaintext/encrypted form of your password. If attackers were able to break into the database & the encryption, they could gain access to your exact password.
    b. In the second case, the site is likely only storing a salted hash of your password. This means, even if attackers did gain access to the database, they would only have access to the hashes of the passwords, which aren’t very useful if the hash function used is effective. Even *if* they did find a collision, they would only be able to use that password on that site, assuming other sites use different hashes/salts.
11. (10 pts) Suppose a telephone company maintained records on every telephone call it handled, showing the calling phone number, the called phone number, and the time, date, and duration of the call.

a. What uses might the telephone company make of those records?

i. Keeping track of billing info. Tailoring plans to your usage.

b. What uses might commercial marketers make?

i. Suggest products based on the preferences of the people you communicate with.

c. What uses might a rival telephone company make?

i. Giving you a better deal that fits your usage well.

d. What uses might a government make?

i. Keeping tabs on people, and who is communicating with who.

e. Which of those uses violate individuals' privacy rights?

i. I feel like most of them do, but if commercial marketers have your info it's probably because you (likely unknowingly) agreed to your service provider selling your info in some privacy agreement.

12. (10 pts) Consider the first step of the common attack methodology we describe, which is to gather publicly available information on possible targets.

a. What types of information could be used?

i. From what I've learned in this class, virtually *any* information is potentially useful for an attacker. Even knowing a name of someone who works for a company would help someone in executing a social engineering attack.

b. What does this use suggest to you about the content and detail of such information?

i. Since almost any information can be misused by someone with malicious intent, it is important to train employees well to protect against attacks that would use public information. In addition, it seems wise to keep as much information from becoming public as possible; not to hide your company's activities from the public, but to protect the company from people who would misuse the information.

c. How does this correlate with the organization's business and legal requirements?

i. The level of secrecy required will vary based on the organization. For example, a medical organization will be legally obligated to keep their patients' information confidential. They will need higher security, than, say, a bakery. These requirements aren't always legal requirements. Say a bakery has a secret recipe for amazing bread; they aren't legally obligated to protect it, but it is probably in their business' best interests to protect the recipe anyways.

13. (5 pts) Distinguish between copyright, patent, trade secret, and trademark (in your own words).

a. Copyright: The legal right to some creative work

b. Patent: The legal right to manufacture/produce some useful invention

c. Trade secret: A highly guarded secret that makes your company unique: (KFC's 11 Herbs & Spices)

d. Trademark: Legal ownership of some identifying logo, like the Apple logo.