Swasti Mishra
Stella Sun
COSC 434
19 February 2023

COSC 434 Written Assignment 1

Question 1

How the Internet Is Glued Together: What are the five layers in the Internet protocol stack? What are the principal responsibilities of each of these layers?

The five layers of the internet protocol stack are the physical layer, the data link layer, the network (or internet) layer, the transport layer, and the application layer.

The physical layer is concerned with the actual 1s and 0s of information and how they get from one device to another. Radio waves, WIFI, ethernet cables, wires, and USB are examples of transmissions mediums for the physical layer. The next layer is the data link layer, which handles direct communication between devices that are local. Devices that are on WIFI together or are wired to each other are examples of networks that utilize the data link layer. Further, the data link layer has a few responsibilities; it manages access to the physical layer, detects errors, and is responsible for hardware addressing. Each device on a network has a MAC address, and the data link layer is the layer that puts it on. The third layer is the network layer, which manages routing between networks. It does this by assigning IP addresses to devices and sending traffic between to the networks they are on. The fourth layer is the transport layer, which functions as ports that connect to applications. Basically, it can be thought of as a spot on a computer where something is listening and waiting for a connection. The transport layer provides reliability if necessary- for example, if priority goes to ensuring that all packets are passed over speed, the transport layer is the layer that makes that decision and chooses a protocol. After doing so, it assigns a socket address made up of the transport protocol, the port number, and the IP address. The last layer is the application layer, whose function is more subjective. Lots of things on the internet have their own protocol- for example email, websites, etc. The application layer helps define the message types in a packet, the meaning of information, and the ways to send the message.

Question 2

Threat Models and Risk Assessment: Suppose the course instructor has created a database of all information for this course: homework, exams, handouts, and grades. Create a detailed threat model for this database: what should the security goals be? What are reasonable attacks, and who are the potential attackers? What threats should we explicitly exclude from consideration?

Having a security goal requires identifying who the attackers are. In this example, the hackers are most likely to be students who are interested in gaining undue access to course material or manipulating their grades. The security goals should be to counteract these students' advances- essentially, protect the database from students who want to change their grade or access course material early. Reasonable attacks include accessing or unlocking the database, stealing the professor's passwords, or maybe even just stealing the laptop to prevent bad grades from being filed. We can exclude outlandish situations like students blowing up the instructor's office, and we can probably also exclude other academics from trying to attack the computer, as I would assume that the instructor would freely give course information to other instructors if asked.

Now assume that the database is stored on the instructor's personal laptop, with no network card and no floppy disk drive. Propose at least two security mechanisms that would help counter your threat model (e.g. file or disk encryption, a laptop lock, a safe to store the laptop, a Kevlar laptop sleeve, relocation to Fort Knox...)

I think the professor should at LEAST put a password lock on the laptop and keep a very close eye on it if they ever remove it from their office. In fact, if students come by for office hours, it should probably be kept in a locked desk. The office should also be locked when the professor is not present, and with a different key than the one for the desk.

As for the password lock, it is not very likely that students try to test this security mechanism if the above suggestions are followed. The only situation where I can foresee this happening is one in which the professor has their back turned during office hours (because the professor should not be taking this laptop to class). In this case, it would take a very bold student to try to crack the password. Out of all the students who come to office hours (which is a low number to begin with), I estimate 1 in 100 to try testing this security mechanism. Furthermore, the cost of implementing is lock is very low. Most people have passwords on most of their devices and very quickly develop a muscle memory for them. If the professor uses this solution, it will be the single most important preventative measure they can take to stop students from breaking into the database.

And as for the locked desk, I think that the only situation where this security mechanism is tested is in conjunction with the locked office. It seems unlikely that the professor would not be in the office and would not have locked the office door (just because most office doors lock automatically when shut). For this reason, to test this security mechanism a student would have also had to break into the office. I put the incidence of this happening at 1 in 250. The only reason the incidence is so common is because instructors will occasionally step out without locking their door, and students may wander in. But to wander in and then try breaking into a locked desk? That situation is unlikely to occur and even less likely to succeed. The cost to implement this suggestion is very low. It may be a minor hassle for the professor to lock and unlock their desk and office, but it is practically the same cost as turning off a faucet before leaving the house and locking the front door, which most rational adults quickly become accustomed to doing.[1]

Question 3

Poisoning the DNS Cache: What are the fundamental problems of the DNS protocol that makes it vulnerable to cache poisoning attacks?

The DNS protocol is vulnerable to cache poisoning attacks because senders and receivers are not verified in the cache. This is because DNS was established when the internet was smaller and more trustworthy, but it has since been adopted beyond the developers' initial expectations. Cache poisoning attacks take advantage of that trust by writing false information into the DNS cache. After writing in this incorrect information, queries redirect users to wrong, and often malicious websites. There is no set way for DNS resolvers to fix a poisoned cache. Incorrect data will stay in the cache until the time to live expires, or it is removed manually by a user.

[1] I don't know how strictly self-plagiarism standards are enforced, so I'll tell you all now that this is approximately my answer to this question from last semester. I assume that's acceptable, considering that the question hasn't changed, and I got credit for this answer when I submitted it last.

ÍQuestion 4

DDoS DNS Root Servers: In cyberwars between two countries, the root DNS servers of each side will be primary targets. If country A can bring down all the root servers of country B, A can effectively cut off all communications between B and the outside world. Assume that your job is to manage the root DNS servers for country B, which is a small country that does not have abundant resources to defend against large-scale DDoS attacks from its powerful foe. What can you do?

The first step for country B would be to establish a firewall that protects its DNS servers. Rather than allowing all addresses to be accessed and returned from, the country should prioritize allowing access to necessary services like banks, social media, and informational websites. Honestly, any web service that implements some kind of rate limiter should be acceptable- we just don't want country A spamming country B with useless packets from malicious or useless websites or platforms. After implementing this firewall, country B can then spend time analyzing the types of malicious web traffic country A is sending them, and then open the firewall to more non-malicious types of web traffic (for democracy and free web use etc.) and continue to monitor and limit bad traffic.