Network Security

Problem 1: Coronavirus Cybersecurity

As a result of the current coronavirus pandemic, many malicious parties have taken advantage of global panic to spread misinformation or scam others. In certain extreme cases, entities like hospitals, health care organizations, or employees of large corporations who have since transitioned to working from home have been targeted by hackers. This Wall Street Journal article elaborates more on these issues: [https://www.wsj.com/articles/cybercriminals-sweep-in-to-take-advantage-of-coronavirus-11585056466](https://www.wsj.com/articles/cybercriminals-sweep-in-to-take-advantage-of-coronavirus-11585056466)

Additionally, as an attempt to curtail the spread of the virus, many governments have started to track their citizens' phones to create heat maps of human movement, understand contagion trends, identify people who may have had interactions with infected individuals, and help enforce quarantines. Other initiatives, such as the volunteer-based CovidWatch, use voluntary information gathered and released through a mobile app to send out alerts to its users about potentially being in contact with the virus. Please read the following:

- The CovidWatch whitepaper: [https://www.covid-watch.org/article](https://www.covid-watch.org/article)

The following questions are open-ended and will be graded for thought and justification. Please reference and/or quote specific arguments from the readings in your answers.

**Question a)** In your opinion, should there be stricter penalties for those staging cyberattacks against essential entities like hospitals in times of crisis (such as during a pandemic)? If so, how should these penalties be enforced?

**Question b)** Imagine a scenario in which you discover a significant vulnerability in a hospital's application(s) or website(s) that reveals sensitive information about patients who tested positive for COVID-19. Using what you know about responsible, full, and private disclosure from Homework 3, which do you think would be the least ethical form of disclosure to use?

**Question c)** Choose two countries from the Business Insider article. Summarize the ways they are tracking citizens, and compare and contrast them. Should either of these methods of tracking be considered a violation of privacy rights? Justify your answer.

**Question d)** How does CovidWatch differ from the two tracking methods you discussed in part (c)? What are some potential benefits and drawbacks to releasing the open-source code this app is built upon?

---

1. The Wall Street Journal article may be paywall-gated, but the Brown Library provides free Wall Street Journal accounts via which you can access the article without having to pay for a subscription—you can find instructions on how to set up this account here: [https://library.brown.edu/eresources/wsjournal.php](https://library.brown.edu/eresources/wsjournal.php)
Problem 2: Network Switches

Consider the network represented in Figure 1, a subnet whose addresses all take the form 192.168.1.*. Each router and host is labeled with its IP address and MAC address.

![Figure 1: The network diagram for the “Network Switches” problem.](image)

**Question a)** Host B wants to intercept Host A’s traffic with Host C. What can B do to cause A to send their traffic to B instead of C? Be specific—don’t just say “B could spoof so-and-so’s IP address.” (*Hint:* In carrying out this attack, B needs to be careful not to accidentally break other hosts’ connections. How can B make sure that their attack only targets A?)

**Question b)** Host B is now intercepting Host A’s traffic, but this means that Host C isn’t getting the traffic. As a result, A may soon notice that something is going wrong and give up, which will limit the amount of information that B can intercept. How can B make sure that the communication still works as A intended, while also guaranteeing that B has access to the traffic? Again, be specific. (*Note:* C should not receive traffic that was not intended for it.)

**Question c)** Host B is now intercepting Host A’s traffic, and Host C is also getting the traffic and responding properly, so A is none the wiser. However, B would also like to intercept the responses, as they may contain important information. How can B accomplish this? Again, be specific.

**Question d)** How would these techniques differ if Host B wanted to intercept Host A’s communication with 128.148.32.12, a host that is not within the subnet? (*Hint:* Since 128.148.32.12 is not on B’s subnet, it will not suffice to spoof 128.148.32.12’s MAC address.)

Problem 3: Handshakes for Data Transfer

Suppose that a client with port $P_C$ connects to a server with port $P_S$, and then performs the following TCP handshake and initial data transfer:
(1) Client sends \texttt{SYN} with sequence number \texttt{SEQ} = A (where A is random).
(2) Server sends \texttt{SYN-ACK} with \texttt{SEQ} = B (where B is random) and \texttt{ACK} = A + 1.
(3) Client sends \texttt{ACK} with \texttt{SEQ} = A + 1 and \texttt{ACK} = B + 1.
(4) Client sends \texttt{DATA} of length \(L_1\) with \texttt{SEQ} = A + 1 and \texttt{ACK} = B + 1.
(5) Server sends \texttt{DATA} of length \(L_2\) with \texttt{SEQ} = B + 1 and \texttt{ACK} = A + 1 + \(L_1\).
(6) Client sends \texttt{DATA} of length \(L_3\) with \texttt{SEQ} = A + 1 + \(L_1\) and \texttt{ACK} = B + 1 + \(L_2\).

Steps (4), (5), and (6) repeat until both sides are done sending data, at which point the connection is cleanly terminated using a \texttt{FIN / ACK} handshake.

**Question a)** Assume that the next transmission in this connection will be \texttt{DATA} of length \(L_4\) from the server to the client. Fill in the table below with the headers of this TCP packet:

<table>
<thead>
<tr>
<th>SEQ</th>
<th>ACK</th>
<th>Source Port</th>
<th>Destination Port</th>
</tr>
</thead>
</table>

**Question b)** Consider each of the following attackers who each have knowledge of the client and server’s IP address. For each attacker, answer: can the attacker hijack the communication between the client and the server? If so, outline an attack; if not, explain why.

(i) Andy, a network attacker who can observe traffic between the client and the server and can inject packets into the network, but cannot modify existing network traffic.
(ii) William, a network attacker who cannot observe or modify traffic between the client and the server, but can inject packets into the network.

**Problem 4: Query IDs**

Recall that when one queries records from a DNS server, their query is associated with a \textit{query ID}.

**Question a)** Explain why having DNS query IDs is more secure than \textit{no} query IDs (maximum 25 words).

**Question b)** Explain why having \textit{randomized} DNS query IDs is more secure than having \textit{sequential} query IDs (maximum 25 words).

**Question c)** You might think that, for a space consisting of \(2^n\) IDs, you couldn’t do better than having a \(\left(\frac{1}{2}\right)^n\) probability of guessing a query ID correctly. Explain how the Kaminsky attack manages to do better than this.

**Problem 5: DNSSEC**

At the end of the \textit{Networks III: DNS} lecture, we briefly discussed DNSSEC, a form of DNS that adds a layer of trust on top of DNS by providing authentication via \textit{digital signature chains}. At a high-level, DNSSEC provides message integrity by providing digital signatures on all DNS records between nameservers—specifically, it signs the \textit{message body} (containing the contents of the actual DNS records it is sending back to the querying server), but it does not sign the headers of the DNS record (such as the query ID, etc.). A nameserver receiving a DNS response can use the answering nameserver’s public key to verify that the response was actually sent by that name server (and not another server).

**Question a)** What attack does DNSSEC prevent against that exists in the regular DNS protocol?

**Question b)** If we ask DNS for the IP address of a domain that does not exist, the DNS protocol simply returns an empty message body marked with the \texttt{NXDOMAIN} header, which signifies a \textit{negative result} (that the domain did not have any associated records). However, the empty message body presents a problem for DNSSEC, since then DNSSEC has nothing to sign!

---

2You can see this for yourself by using the \texttt{host(1)} command on an invalid domain, which will print out the message “Host <domain> not found: 3(NXDOMAIN)”.

3
One fix for the “nothing to sign” issue is to instead return a signature on the \texttt{NXDOMAIN} header. Then, the receiving nameserver could then use the responding server’s public key to verify that "\texttt{NXDOMAIN}" was actually sent by the nameserver. However, this is a bad idea in terms of security. Why? (Hint: In \textsc{DNSSEC}, signatures are usually valid for one month after signing.)

**Question c)** \textsc{DNSSEC} resolves the “empty message body” issue described in part (b) by adding the NSEC RR record type, which is used to represent negative results. The way the protocol works is as follows: on the case of a negative result, the nameserver returns a signed pair of domains that are alphabetically before and after the requested name. For example, suppose the following domains exist on records in the nameserver for \texttt{brown.edu}, in alphabetical order:

\{
\ldots, covid.brown.edu, cs.brown.edu, dam.brown.edu, \ldots\}

Suppose one makes a \textsc{DNSSEC} query for \texttt{crowd.brown.edu} (which is alphabetically between \texttt{covid.brown.edu} and \texttt{cs.brown.edu}). In response, the name server would return an NSEC RR record that, in informal terms, states “the name in alphabetical order that comes after \texttt{covid.brown.edu} is \texttt{cs.brown.edu},” with each domain name in the record associated with a signature made using \texttt{brown.edu}’s key.

Does this fully fix the issue identified in part (b)? Explain.

**Question d)** The protocol described in part (c) seemed unnecessarily complicated to Zachary, who proposed the following modification to \textsc{DNSSEC}: simply return a signature of the requested domain on a negative result. This has several benefits: it avoids the need to maintain a sorted list of domain records; it also can substantially reduce the packet size of a negative result, which would increase performance.

As to be expected with these kinds of hypotheticals—this is a bad idea. Why?