14-741/18-631: Final exam
7:30pm-9:30pm EST, Thursday Dec 5th, 2019

Name:

Andrew ID:

Scores

Problem 1 (25 pts max):

Problem 2 (25 pts max):

Problem 3 (15 pts max):

Problem 4 (10 pts max):

Problem 5 (15 pts max):

Problem 6 (10 pts max):

Total (100 pts max):

Guidelines

- This exam contains 6 problems and is 17 pages long. Check you have all pages.
- **Do not write answers on the back of the pages. They will not be graded. If you need more space, please use the extra page in the back.**
- To help us grade as anonymously as possible, please **do not write your name or any other identifying information on any page other than this cover page**.
- Be neat and concise in your explanations. Limit your answers to the space provided. You won't be penalized for using incorrect grammar, but you will get penalized if we can't understand what you are writing.
- Show your work clearly. If your reasoning (in other words, steps) is correct, but your final answer is wrong, you will receive most of the credit. On the other hand, answers without explanation, or argumentation get no credit, *even if they are correct*.
- This exam is open-book. All reference books, class notes, and dictionaries are allowed. **Internet access during the exam is strictly prohibited. Accessing the Internet during the exam constitutes an academic integrity violation and will be punished by failure of the class ("R") and other disciplinary measures at the discretion of the University. Turn off your cell phones and devices!**
- Open-book does not mean open neighbor. Cheating on the exam (including accessing the Internet) automatically results in failure of the class and will be reported to the University administration. We do enforce the INI plagiarism policies strictly.
- It is advantageous to partially answer a question than not attempt it at all.
- Good luck!

1 Short answer (25 pts)

Answer the question (each short answer can be answered in a couple of sentences at most).

1. (5 pts) A developer suggests that prepared SQL queries are too expensive, and that it is more efficient to just disallow use of single quotation marks in input fields. Name one reason this might not be acceptable.

2. (5 pts) Youtube TV, which is a popular live streaming TV service, allows users to stream their programs only if the user is in the US. Why would Tor not be a good strategy for a user in Germany to get around this restriction?

3. (5 pts) Why are strategies in Nash equilibria not always socially optimal?

4. (5pts) Briefly describe players in an online crime ecosystem and their roles (e.g., an illicit drug supply chain).

5. (5 pts) Describe an attack that we discussed in class that is caused by unsanitized input provided by an attacker. Describe the attack scenario. In particular, state the vulnerability, how the attacker exploits the vulnerability, and what the attacker achieves from exploiting the vulnerability

2 Protocol (25 pts)

Charlie wants to implement a protocol that allows two parties to exchange a symmetric key K and then send encrypted messages using the exchanged key. We use the following notations: $\{M\}_K$ is the encryption of message M using the key K. PK_X is the public key of X and SK_X is the private key of X. We will use Alice (A) and Bob (B) to explain how the protocol works.

2.1 First attempt

Charlie came up with the following design. In steps K1 and K2, Alice and Bob exchange a key. From step M1, Alice and Bob start to exchange encrypted messages. In step K1, Alice generates a nonce N, encrypts N using Bob's public key and sends the encrypted nonce to Bob. Bob receives the cyphertext, decrypts it and sends back to Alice, a pair of a symmetric key K and the decrypted nonce N, encrypted using Alice's public key. Alice decrypts the message and checks whether the received nonce is the same as the nonce she has generated earlier for Bob. If so, Alice will accept the key K. After that, Alice and Bob starts to communicate using K to encrypt all messages.

$$\begin{array}{lll} \text{K1.} & A \rightarrow B: & \{N\}_{PK_B} \\ \text{K2.} & B \rightarrow A: & \{K, N\}_{PK_A} \\ \text{M1.} & A \rightarrow B: & \{m_1\}_K \\ \ldots & & \end{array}$$

1. (5 pts) Assuming the nonce is generated using a perfect pseudo random number generator (i.e. truly random and never repeats), does Alice know that the key K is from Bob? Explain why or why not?

2. (5 pts) Charlie decides that the nonce generation algorithm can be implemented as a simple counter (i, $i + 1$ etc.) without compromising the protocol. Do you agree with Charlie? Explain why or why not.

2.2 An improvement?

Charlie comes up with a variant of this protocol below.

$$\begin{array}{lll}
\text{K1.} & A \rightarrow B: & \{N\}_{PK_B} \\
\text{K2.} & B \rightarrow A: & \{K\}_{PK_A}, \{N\}_{SK_B} \\
\text{M1.} & A \rightarrow B: & \{m_1\}_K \\
\ldots & &
\end{array}$$

1. (5 pts) After step K2, does Alice know that Bob has seen the nonce N? Explain why or why not.

2. (6 pts) Assuming the nonce is generated using a perfect pseudo random number generator, can an attacker break the protocol? If so, explain the attack scenario in detail, if not, present your reasoning in detail.

3. (4 pts) Under the constraint that the nonce N is implemented as a counter and the first step of the protocol (K1) cannot be changed, fix Charlie's protocol so that Alice and Bob can share a symmetric key and communicate securely. You can safely assume that Alice never have to re-use a counter value. You cannot change step M1; i.e., Alice must use the symmetric key that she has exchanged with Bob in the key exchange steps to encrypt her message. You can change other steps of the key exchange protocol, including changing messages and adding or removing steps.

3 DDoS command and control (15 pts)

Mallory has managed to commandeer 1,000 zombie machines, and has set up the following DDoS framework (described in Figure 1).

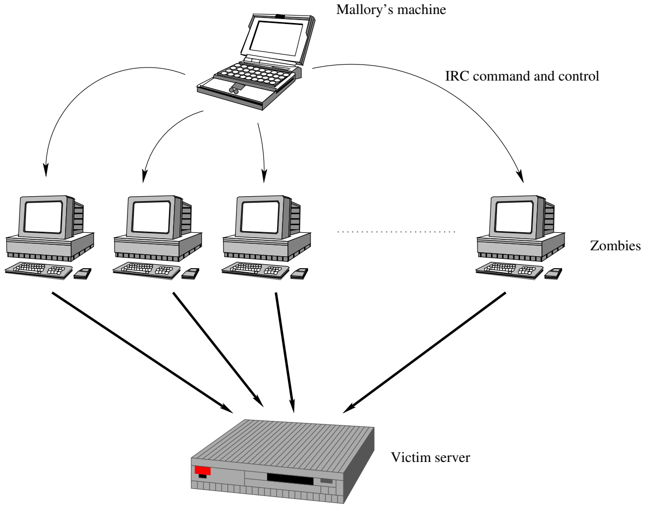

Figure 1: Mallorys DDoS setup.

Mallory's machine directly talks with the zombies, using an Internet Relay Chat (IRC) channel. IRC is an application-layer client-server protocol, that typically runs over TCP, on port 6667 at the IRC server. Unless otherwise specified, messages in IRC are sent in plain text. Using specific IRC messages (not detailed here) sent to the zombies, Mallory can trigger them to attack the victims server, and instruct them when to stop the attack. In the attack phase, the zombies send a bunch of HTTP requests to the victim server. Zombies do not use spoofed IP addresses.

1. (4pts) Initially, Mallory plans on running a regular IRC client at her machine, and IRC servers at all zombies. Does this method guarantee Mallory cannot be traced back? Why or why not? (Justify your answer.)

2. (3 pts) What is the main advantage for Mallory of having the zombies not use spoofed addresses?

3. (3 pts) You are the admin of the victim server, explain an easy strategy to thwart Mallory's attack if she keeps using the same zombies for attacks.

4. (5 pts) The victim server that Mallory has targeted recently has upgraded its infrastructure and can now handle up to 10 times the network traffic that it used to. The 1000 zombies that Mallory controlled now can't generate enough traffic to DDos the victim server any more. Due to various constraints, Mallory can't acquire more zombies. What strategy should Mallory try to generate enough traffic to mount a successful DDos attack to take down the victim server despite the infrastructure upgrade. Please draw the configuration and describe Mallory's new attack in detail.

4 Anonymous Communication (10 points)

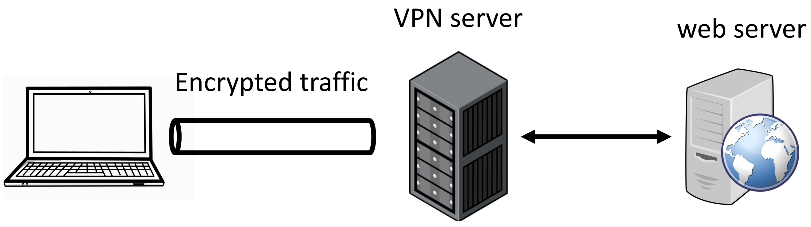

Figure 2: VPN

Millions of users use Virtual Private Network (VPN) technology (Figure 2) to bolster their online privacy, secure public Wi-Fi connections, and visit blocked websites. At a high-level, VPN works as follows. The user registers an account with a VPN service. When the user starts a VPN application, the application connects to the VPN server and exchanges a symmetric key with the VPN server using TLS. Subsequent communications between the client and the VPN server will be encrypted using the shared key, which is also referred to as being tunneled between the client and the VPN server. When the client's machine sents requests to a server (e.g., www.cnn.com), the requests will be sent to the VPN server, and the VPN server will send the requests to www.cnn.com as if the requests are from an IP address within the VPN server's network (not related to the client's real IP address). When the VPN server receives responses for the web server, it will send the responses back to the client.

1. (4 pts) Explain why VPN technology help users to communicate to web servers anonymously. Please pay special attention to the details in describing the anonymity properties.

2. (6 pts) Is Tor better than VPN for anonymous communications? For each aspect in consideration, discuss in detail why or why not. We expect the answer to compare a minimum of two aspects. Please do not consider traffic analysis or side channel attacks such as timing.

5 Bitcoin (15 points)

1. (5 pts) Bitcoin addresses are public keys. Explain why symmetric keys cannot be used here.

2. (5 pts). Alice is worried about her devices containing private keys getting stolen, so she plan to store her bitcoins in such a way that they can be redeemed via knowledge of a 12 character password. Alice stores them with the following ScriptPubKey. The long string on the second line is the hash of Alice's password. Alice can later redeem the bitcoins by providing a ScriptSig: `<XYZ>`, where XYZ is Alice's password. Explain why this is less secure than using a private key.

```
OP_SHA1
<0xeb3e2927c2340d01cbcb0e621291cbc0f22e578ff69b>
OP_EQUAL
```

3. (5 pts) Bob came up with a business plan to offer an anonymous bitcoin service. Bob plans to act as a Mix. Bob's customers would send bitcoins and recipient's wallet address to Bob. Bob will take a small fee, which is 10% of the transaction and send the remaining coins to the recipient's wallet. Say Alice needs to pay Charlie 10 bitcoins, Alice will pay Bob 10 bitcoins in one transaction. Bob will pay himself 1 bitcoins and pay Charlie 9 bitcoins in one transaction. Does Bob's proposed system provide anonymity to his customers? Explain why or why not?

6 The tale of another retail store (10 pts)

HD is a retail store that has both physical stores and online stores. Similar to T, which we talked about in class, HD also has a network to which both HD's point-of-sale (POS) systems and other corporate servers are connected to. HD also gives contractors access to its network. HD's CEO hired very bright security experts when its information security department was formed a few years ago. Experts in this department have proposed segregated networks, so that the POS systems are on a dedicated and separate network from the rest of the corporate network. However, the CEO shot down the idea because of the cost. The employees in the security department have been growing increasingly frustrated as most of their suggestions to improve HD's security were met with rejections from the CEO due to high cost. In company meetings, the CEO had openly criticized the security team as being paranoid and costing the company too much money.

Most recently, the security team asked HD's CEO for funds to update the companys POS systems so that they run new operating systems and to upgrade the anti-virus protections to the newest version. The CEO argued that HD's current practices are compliant to the payment card industry (PCI) standard. Further, the CEO said it is too costly and the old systems are patched routinely anyway, even though the systems themselves have been several generations behind. The CEO also argued that the probability of an attack is low and the impact of an attack is low. HD suffered a similar attack as T and lost tens of millions of credit card numbers of its customers.

1. (5 pts) Explain why compliant to PCI standard doesn't mean strong security guarantees. Suggest a better approach to evaluate the security guarantees.

2. (5pts) What are potential management issues with the CEO not taking valuable suggestions from security team? Imagine you are in the CEO's shoes: what would be a better process to follow?

Extra Page