14-741/18-631: Test 3
Nov. 24th, 2020

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 (25 pts max):

Total (100 pts max):

Guidelines

- This exam contains 5 problems and is 16 pages long. Check you have all pages.
- **Do not write answers on the back of the pages. They will not be graded**
- 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 proof, 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.

1 DDoS (25 pts)

The Network Time Protocol (NTP) is designed to allow devices connected to the internet to synchronize their clocks. NTP servers in the network receive requests from devices and send responses back to the source IP addresses in the requests. For debugging purposes, the `monlist` command retrieves information from the monitoring facility about traffic associated with the NTP service. The NTP server responds with the last 600 source IP addresses of requests, which have been made to the NTP server. An 80 Byte `monlist` request, on the average generates a response of 16KB. Many servers have `monlist` enabled and publicly accessible and respond to any request.

1.1 The attack (5 pts)

Alice wants to mount a DDoS attack against a web server S, even thought Alice's network has much less capacity than S. How can Alice leverage NTP for the attack? List each attack step clearly.

1.2 Defenses (20 pts)

Alice also has the option to DDos the web server S by controlling bots to visit the website. Images and videos requested from the bots can generate enough network traffic to take S down. Are the following mechanisms effective for mitigating the above mentioned DDos attacks (NTP-based and bot-based). Why or why not?

1. egress filtering (filter at the server end) for NTP-based
2. egress filtering (filter at the server end) for bot-based
3. ingress filtering (filter at the origin of the "attack" traffic) for NTP-based
4. ingress filtering (filter at the origin of the "attack" traffic) for bot-based

2 Web Security (25 pts)

2.1 HTTPS (10pts)

Bob is the admin of a shopping website. HTTPS encrypts communication between the web servers and the browser. Bob thinks that using HTTPS for the website helps prevent Cross-Site-Request-Forgery (CSRF) attacks. Do you agree with Bob? Why or why not?

2.2 XSS and Network attackers (5pts)

Describe a mechanism for preventing malicious scripts from being injected to a website against network attackers.

2.3 XSS and Web attackers (5pts)

Describe a mechanism for preventing malicious scripts from being injected to a website against web attackers.

2.4 SQL injection (5pts)

Which security policy(ies)/property(ies) does the SQL injection attack violate?

3 Anonymous Fund Raiser(15 pts)

Bob is running an anonymous fund raising campaign. That is, the true identity of the donors is not known to Bob or the public. He does not want to use platforms like gofundme, as the system knows the creditcard number and the name of donors. An insider, or an attack on the servers, could leak donor's information. Bob is considering using Bitcoin instead.

3.1 Bitcoin? (5 pts)

Can Bob keep his donors completely anonymous to the public by using Bitcoin? Explain why or why not.

3.2 Who has it? (5 pts)

Bob posts his Bitcoin wallet address on his fund raising website, so donors can send coins to that address. You plan to donate to Bob's campaign, assuming you have the correct url to Bob's fund raising page. You sent your coin to that wallet. After seeing your transaction verified by the network. Are you confident that your coin was collected by Bob's campaign? Why or why not? There is no standard answer for this question. Reasonable assumptions about Bob's website is allowed.

4 2Bitcoin (10 pts)

2Bitcoin is a variant of Bitcoin that uses a completely decentralized verification system, based on hash chains, as follows. All current transactions are broadcast over the entire Bitcoin network, and appended to a current "block." The current block b_n contains the hash of the previous block, the set of pending, unconfirmed transactions, and an integer nonce N:

$$b_n = \{H(b_{n-1}), (T_1, \ldots, T_q), N\} \ ,$$

where $T_1, \ldots T_q$ each contains records of, e.g., Alice sending a coin to Bob, Bob sending five coins to Charlie, Emma sending two coins to Zoe, etc. A fixed "genesis" block b_0 was created when the Bitcoin network was started.

Moving from one block to the next works as follows. As they receive notification of transactions, in parallel, all mining clients attempt to find a number N so that $h(b_n)$ starts and ends with a number s of zeros a priori agreed upon by the network. The hash function h is SHA-256, which has a 256 bit output. That is, each node attempts to solve the following problem:

Given $s \in \mathbb{N}$, $T_1, \ldots T_q$, and b_{n-1},
find $N \in \mathbb{N}$, such that
$H(\{H(b_{n-1}), (T_1, \ldots, T_q), N\}) = \underbrace{000...0}_{s \text{ bits}} \ \underbrace{XX...XX}_{256-2s \text{ bits}} \ \underbrace{000...0}_{s \text{ bits}},$

with $H =$ SHA-256. The first node to solve the puzzle "wins," and broadcasts the solution to the other nodes. Ignore the fact that nodes receive new transaction records as they are trying to solve this puzzle.

4.1 Speed (5 pts)

How can the system ensure that the network is verifying transactions at an expected speed (e.g., generating/verifying a block roughly at every 20 minutes)? (5pts)

4.2 Double spending? (5 pts)

Bitcoin could suffer from double spending if one entity owns 51% of the whole network's hashing power. Discuss whether 2Bitcoin is susceptible to the same attack. (5pts)

5 A Domain Name Service (25 pts)

Here is the format of your answers for the following questions. to explain why you agree that a protocol is correct, describe how the crypto primitives provide desired properties. To explain why you do not agree, or the protocol is incorrect, describe an attack by Mallory with detailed message exchange steps, using the same (step number. A → B: Message) format as below.

At a high level the DNS protocol functions as follows. Alice wants to know the IP address of Bob. She contacts Trent, the DNS server, and sends a request including a nonce N. Trent replies using the same nonce, and providing the IP address of Bob, and a lifetime L for this response to be considered as valid.

$$\begin{array}{ll} 1. & A \rightarrow T: \quad A, B, N \\ 2. & T \rightarrow A: \quad T, B, IP(B), N, L \end{array}$$

5.1 Nonce (5 pts)

Explain why the nonce N need to be unpredictable. Demonstrate an attack where Mallory can trick Alice into accepting Mallory's IP address as Bob's. You must assume that Mallory cannot eavesdrop on Alice's messages.

5.2 An improvement? (10 pts)

ICANN Engineer Charlie proposes the following new protocol, where N can be implemented as a counter and so that we don't need to worry about Mallory in the same network as Alice or Mallory. In this proposal, everybody shares a secret session key with Trent. K_{AT} is shared between Alice and Trent, K_{BT} is shared between Bob and Trent, and K_{MT} is shared between Mallory and Trent. For each session between Alice and Trent, the counter starts from 1 and increments by 1 after every request that Alice sends. When N reaches 1000, after Alice sends the 999th message, Alice resets her counter to 1, and Alice and Trent discard their session key and exchange a new one securely, (e.g., via RSA or Diffie-Hellman) for the next 999 requests.

Bob will send encrypted N and encrypted IP address of Bob back to Alice. Both using K_{AT}.

$$\begin{array}{ll} 1. & A \rightarrow T: \quad A, B, N \\ 2. & T \rightarrow A: \quad A, B, \{IP(B)\}_{K_{AT}}, \{N\}_{K_{AT}} \end{array}$$

Charlie asserts that even if there is an active network attacker Mallory, which is in the same network as Alice or Trent, Mallory cannot trick Alice into accepting an IP address of someone else (e.g., Mallory's) as Bob's. Do you agree? Explain why or why not.

5.3 Another design (10 pts)

Another ICANN engineer Dave has a competing design. Dave not only changes the second message, but also adds a third message where Alice acknowledges the recipient of Bob's IP address by sending A, B, and the encryption of the pair of the IP address and N incremented by 1 back to Trent. When Trent receives it, he will check to make sure that Alice has gotten the correct address. If everything is correct, Trent will send Alice an encrypted OK message. If Alice does not receive the OK message from Trent, Alice will discard the IP address and ask another server.

1. $A \to T :\quad A, B, N$
2. $T \to A :\quad A, B, \{IP(B), N\}_{K_{AT}}$
3. $A \to T :\quad A, B, \{IP(B), N+1\}_{K_{AT}}$
4. $T \to A :\quad \{OK\}_{K_{AT}}$

Dave also asserts even if there is an active network attacker Mallory, which is in the same network as Alice or Trent, Mallory cannot trick Alice into accepting an IP address of someone else (e.g., Mallory's) as Bob's. Do you agree? Explain why or why not.