Homework 3

CS341 Introduction to Computer Networks, KAIST
(2024 Fall)

Due: 11:59 PM (KST), December 7, 2024

INSTRUCTIONS TO STUDENTS:

- Any collaboration or assistance of any kind is strictly prohibited; all work must be your own.
- Your submission *will surely* be compared with the submissions for your peers for plagiarism detection. Any academic dishonesty will be directly reported to the university.
- Word limit: Your answers should be within the word limit when it is specified in each question. We will *not* read beyond the word limit when grading.
- **NOTE on LLMs:** You are strongly discouraged from using LLMs to generate your answers. Not only your answers may be similar to others (thus, plagiarism), but also the generated answers will likely be surprisingly incorrect or too superficial to get a good grade.

1. Doh! It's Blocked! (40 points)

DNS (Domain Name System) is a critical component of the Internet infrastructure that translates domain names into IP addresses. DNS queries are typically sent in plaintext, which can be intercepted and modified by malicious actors. To address this concern, DNS-over-HTTPS (DoH) was introduced to encrypt DNS queries and responses. As more users around the world adopt DoH, some authoritarian governments wish to block DoH traffic because it bypasses their DNS-based censorship mechanisms. When DoH is blocked, typical browsers immediately fall back to using traditional, plaintext DNS queries. This automatic fallback behavior is a potential problem of DoH as it can be exploited by authoritarian governments to block DoH traffic and conduct censorship based on plaintext DNS queries.

You are asked to help an authoritarian government to block DoH traffic of the citizens in the country. To achieve this goal, you need to provide technical schemes that the government can use to block DoH traffic. Consider that the government can control several major ISPs in the country and thus can monitor and block the traffic that goes through these ISPs. In your answer, you should consider the practical difficulties of each scheme, particularly in terms of the cost of monitoring and blocking traffic and the expected effectiveness of the scheme in blocking DoH traffic.

Provide all (up to four) possible technical schemes of your choice (10 points each). Your answer to each scheme should not exceed 100 words.

(Note: We did not cover the details of DoH in class, so you may need to do some research to answer this question.)

2. Mapping IP Addresses to Onion Addresses (30 points)

Tor is a popular anonymity network that allows users to hide their IP addresses while accessing the Internet services of their choice. Tor onion services additionally allow service providers (e.g., a website operator) to hide their servers' IP addresses while providing services to Tor users. That is, Tor onion services allow both clients and servers to remain anonymous while communicating with each other. Clients use onion addresses (e.g., `facebookcorewwwi.onion`) to access onion services and the Tor network routes the traffic to the correct server without revealing the server's IP address to the client.

Suppose you are a network administrator of a large ISP in a country where Tor is widely used. Working with the law enforcement agency, you are asked to find the IP addresses of as many Tor onion services from a list of onion addresses given to you as possible. The law enforcement agency is interested in identifying the IP addresses of the servers hosting these onion services to investigate illegal activities. Explain whether and how you can achieve this goal. Present the best approach you can think of and discuss its expected cost (in terms of required resources, time, or privileges) and effectiveness.

In your answer, you should consider the practical difficulties of identifying and/or monitoring Tor traffic at the ISP level. You may be able to monitor the traffic that goes through your network, but you cannot decrypt the traffic or modify the Tor protocol and its implementations. Also you are not colluding with other networks or intelligence agencies. You may be able to run some unmodified Tor clients but you cannot run Tor relays or exit nodes. We will grade your answer based on the feasibility, cost, and effectiveness of your approach. Your answers should not exceed 300 words.

(Note: We did not cover Tor onion services in class, so you may need to do some research to answer this question.)

3. SDN for Large-volume DoS Attacks (30 points)

Software-Defined Networking (SDN) is a networking paradigm that separates the control plane from the data plane in network devices. Consider the OpenFlow protocol, which is a popular protocol used in SDN to communicate between the controller and the switches. When a large-volume Denial-of-Service (DoS) attack occurs, a network is overwhelmed with a large volume of traffic, causing the network to become congested and thus disrupting the normal operation of the network.

You are a network administrator of a large network that uses OpenFlow-based SDN, where all the switches in the network are OpenFlow-enabled and controlled by a centralized controller. Explain the main challenges of using SDN to mitigate large-volume DoS attacks (in less than 100 words). Then, propose one or more mechanisms or system components that can be added to your switches and/or controller to mitigate large-volume DoS attacks effectively (in less than 200 words).

Submission

- Please visit Gradescope, where you can answers to the corresponding questions directly through the web interface.