UConn CSE 5095: Network Security, Fall 2024

HW 4: DoS, submit in Husky by Nov. 24th, 11:59pm

You may work in pairs. Printed solutions receive 10 points bonus. Prof. Amir Herzberg.

Name(s): Luke Pepin

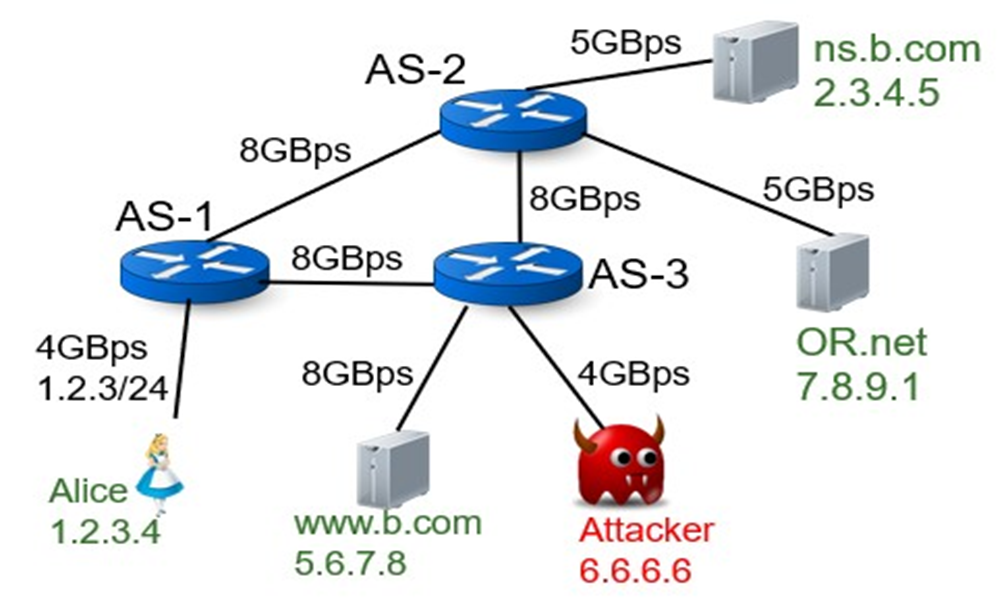
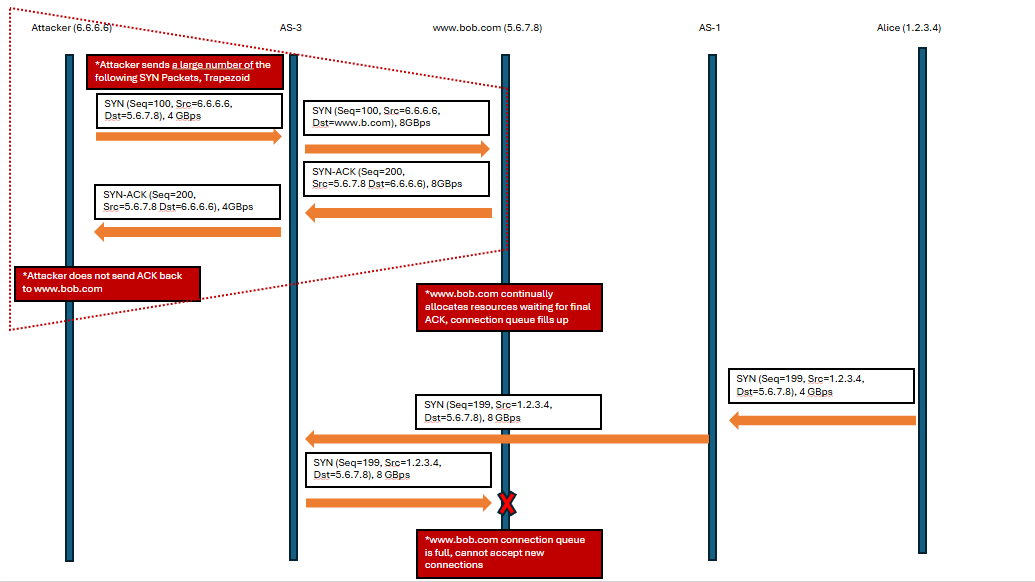


Figure 1: Topology. Assume shortest-path routing. OR.net is an open resolver.

Consider the scenario in Figure 1; assume the specified bandwidth, in GigaByte per second (GBps) is for both directions, independently of traffic in the reverse direction. Assume shortest-path routing and that packets sent to non-existing IP addresses are (silently) dropped. Each link is associated with a 1GB buffer. Assume that the DNS server and resolver both support UDP, with requests of size 100Bytes and responses of size 2KB, and do not impose rate limits on clients. The attacker’s goal is to prevent Alice from communicating with the web-server *www.b.com*; assume that, without attack, Alice sends requests at rate 1KBps and receives responses at rate 1MBps. Assume no network traffic except this traffic between Alice and the server and the traffic due to the attacks. Use the simplified formula given in the lecture for losses and for the TCP bandwidth as function of delays and losses, and MSS of 1KB.

1. Show, with a sequence diagram, an efficient and effective attack whereby the attacker can prevent the server from accepting any new connections (from Alice and other clients).



1. What is the (minimal) attacker bandwidth required by the attack (to prevent any new connections)? Assume that the server uses a drop-tail queue allowing up to 100,000 pending connections with pending timeout of 10 seconds and does not use SYN-cookies or other defenses.

The minimal attacker bandwidth required by the attack follows the following formula:

Bandwidth = (SYN packet size \* Queue Size)/ pending timeout.

Using given and expected values:

Bandwidth = (60 bytes \* 100,000)/10s = 6,000,000 bytes/10s = 600 KBps is the minimal attack bandwidth required

1. Explain why the attack of the previous item would fail if the server uses Syn-Cookies. From here on, assume Syn-Cookies.

Syn-Cookies would prevent the previous attack on the server. SYN Cookies do not immediately allocate resources for the connection. Instead, they use cryptographic techniques in the SYN-ACK packet to delay resource allocation until the client responds with an ACK packet. The attack is designed to exploit the fact that the server allocates resources and begins to fill up the connection queue upon receiving an ACK. However, with SYN Cookies, the server only allocates resources after verifying the final ACK, thus preventing the connection queue from filling up with half-open connections.

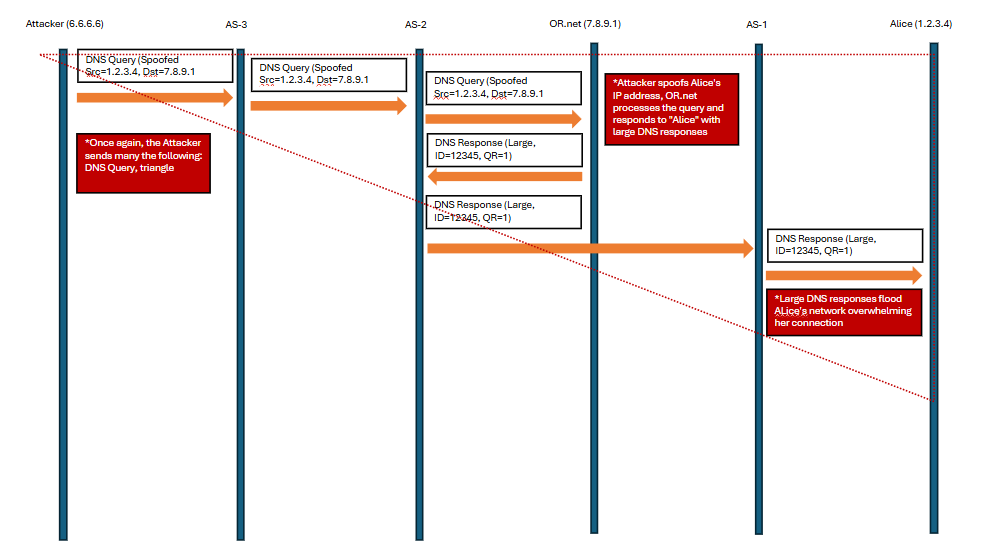
1. Consider an attacker which uses all of the bandwidth to send packets to Alice (direct flood). Approximate the impact in terms of loss rates, bandwidth and latency, for the requests (from Alice to server) and for the responses (from server to Alice).

Loss rates: For both requests and responses, since the attacker's connection to AS-3 (4 GBps) and AS-3's connection to AS-1 (8 GBps) are at or above the connection from Alice to AS-1 (4 GBps), the flood will completely saturate the traffic in the connection between Alice and AS-1. This will result in very high packet loss rates, nearing 100%, with only a few packets possibly slipping through in both directions.

Bandwidth: For both requests and responses, Alice’s bandwidth for sending requests and receiving legitimate responses will be nearly zero due to the high volume of attacker packets in the connection. This will effectively close off Alice's communication.

Latency: For both requests and responses, the latency will increase significantly due to congestion and packet loss. Packets will need to be retransmitted multiple times, causing substantial delays. High packet loss and retransmissions will exacerbate these delays.

1. Present a sequence diagram for a more effective attack, where the attacker does not send any packets directly to Alice’s network (1.2.3/24). Approximate the impact in terms of loss rates, bandwidth and latency, for the requests (from Alice to server) and for the responses (from server to Alice).



Loss rates: For both requests and responses, the attacker's DNS amplification attack will flood Alice's network with large DNS responses. Since the attacker's connection to OR.net (open resolver) and the subsequent connections through AS-2 and AS-1 are capable of handling high traffic volumes, the flood will completely saturate the traffic in the connection between Alice and AS-1 (4 GBps). This will result in very high packet loss rates, nearing 100%, with only a few packets possibly slipping through in both directions.

Bandwidth: For both requests and responses, Alice’s bandwidth for sending requests and receiving legitimate responses will be nearly zero due to the high volume of DNS response packets flooding her network. This will effectively close off Alice's communication.

Latency: For both requests and responses, the latency will increase significantly due to congestion and packet loss. Packets will need to be retransmitted multiple times, causing substantial delays. High packet loss and retransmissions will exacerbate these delays.

1. Explain how the attacker can further improve the attack, i.e., achieve even higher loss rates.

By using multiple open resolvers and other protocols, the attacker can combine multiple vectors to generate a much larger volume of traffic. Additionally, targeting multiple entry points in Alice’s network can further increase the loss rate and improve the effectiveness of the attack. Employing a botnet to distribute the attack can also make it more difficult to mitigate and trace back to the source.