Bangladesh University of Engineering and Technology

CSE 406

Commputer Security Sessional

Design Report

# TCP Reset Attack on Video Streaming

*Author:*
Kishore Kumar Dash

*Student ID:*
1505028

January 25, 2021

# Contents



# List of Figures

# 1 Introduction

TCP RST packets are used to urgently end connection.The objective of a TCP reset attack is to break an existing TCP connection between two victim hosts. The attacker can forge these packets using IP and MAC spoofing and can pretend to be one of the communicators. In the case of reset attack on video streaming, a TCP RST packet is sent to victim's machine and the TCP connection is broken with the video hosting server.

# 2 Definition

Normally, TCP follows FIN protocol that uses FIN bit of the 6 code bits of TCP header to close an existing connection. On the other hand, to immediately break the connection, a single RST packet is sent to either side of the connection that uses the RST bit of those 6 code bits. When this RST packet is used to break the TCP connection with a video streaming Server, it is called TCP reset attack on Video Streaming.

# 3 TCP FIN Protocol timing diagram

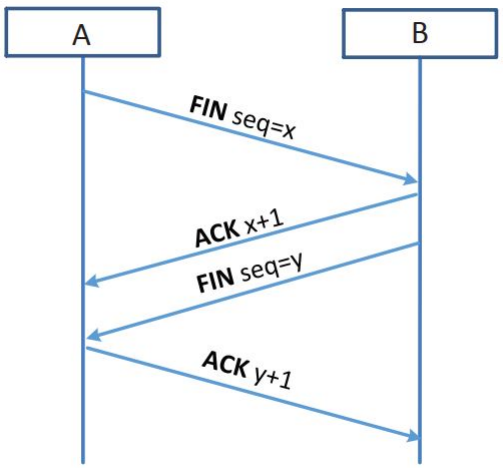


Figure 1: TCP FIN Protocol timing diagram

An end A sends out a FIN packet after finishing sending all data to the other end B. FIN bit is one of the six code bits in the TCP header. After receiving the packet, B replies with an ACK packet. After this, the A-to-B direction of the connection is closed, but the other direction (B-to-A) is still open. To close that direction, B sends a FIN packet to A, and A will reply with an ACK packet.At this point, the entire TCP connection is closed.

# 4 TCP RST Protocol timing diagram

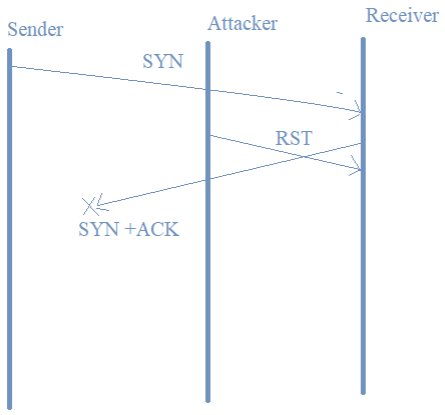


Figure 2: TCP RST Protocol timing diagram

One end simply sends a single TCP RST packet to the other end, immediately breaking the connection. RST is also one of the six code bits in the TCP header. This approach is mainly used in emergency situations.

# 5 Topology diagram

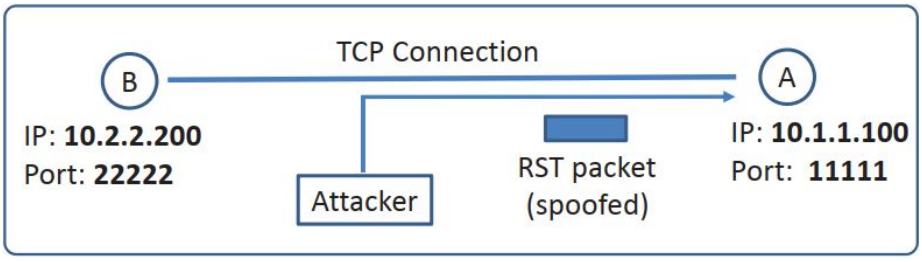


Figure 3: TCP Reset Attack Topology Diagram

The attacker intervenes in the connection and attacks by RST packet.

# 6 TCP Reset Attack Strategy

To break up a TCP connection between A and B, the attacker spoofs a TCP RST packet from A to B or from B to A. However, to make the attack successful,the following things need to be considered:

- Several fields of the IP and TCP headers such as source IP address, source port, destination IP address, and destination port need to be filled out correctly.
- These four fields in the spoofed packet need to be the same as those used by the connection.
- The sequence number in the spoofed packet needs to be correct, or the receiver will discard the packet.

# 7 Attacking Strategy for Video Streaming

Theoretically the strategy extends the behaviour of the TCP reset attack, but there is a unique challenge for resetting video-streaming connections.The challenge is the sequence number.In video-streaming connections, there is no way to stop the packets between the client and the server, so the sequence number increases very fast. So, we have to automate our attack,instead of using the manual sniff-and-type approach. This strategy is called *sniff-and-spoof* approach.

## 7.1 Sniff-and-Spoof Attacking Strategy

In this strategy, a program will be run that:

- Sniffs the video-streaming packets
- Gets the sequence numbers and the other essential parameters
- Automatically sends out spoofed TCP RST packets

# 8 TCP and IP Header Modifications

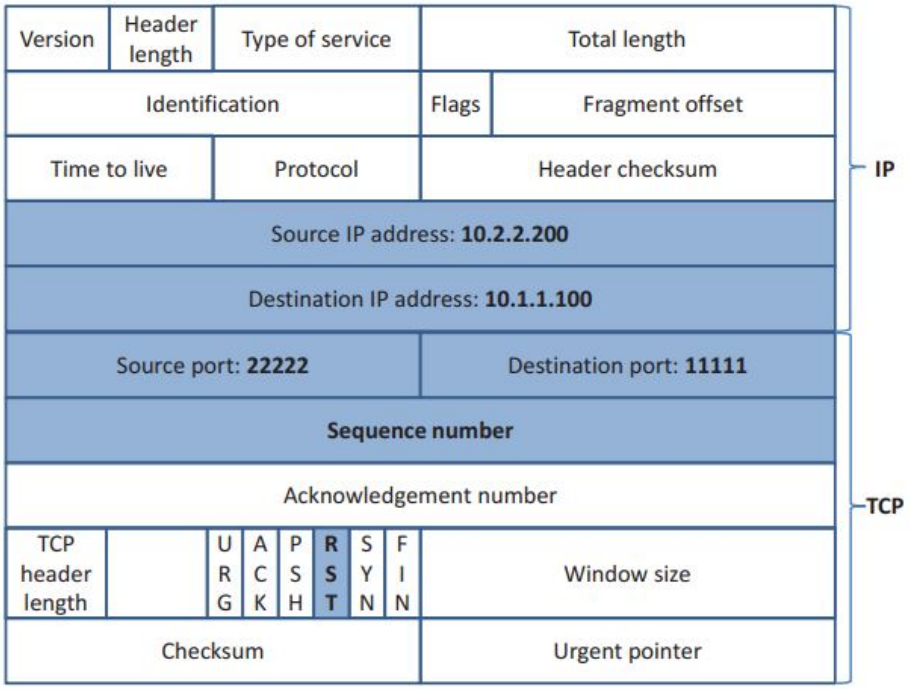


Figure 4: Modified Attack Packet

Relevant fields with the information needed to Spoof:

- Source IP address
- Destination IP address
- Destination Port Address
- Source Port Address
- Sequence Number
- RST bit of the 6 code bits field

If the video is streamed on a non-well-known port, the attacker needs to guess both the port numbers as well as the sequence number in this case.

# 9 Tools to be used

- Virtual Machine

- Seed Labs Ubuntu
- Websites providing online video streaming
- C/Python as programming language
- Scapy package

## 10 Justification

The design should work correctly because :

- RST bit is used to break the TCP connection immediately
- Several fields of the IP and TCP headers are filled out correctly
- Guessing the correct sequence number
- Using automatics sniff-and-spoof approach to send packets
- The attacker is on the same network as either the client or the server