Understanding how modern application use TCP

Magesh Khanna Vadivelu

Shivaraman Janakiraman

IMPLEMENTATION DETAILS:

FLOW IDENTIFICATION:

We use appropriate flag set to identify the start and end of a connection.

CLIENT TO SERVER:

Client to server connection initiation is identified by checking if SYN flag is sent and also if the source port number is greater than 1023.

Connection termination can be identified by FIN + ACK flag set.

I) SEQUENCE NUMBER:

The sequence number is determined at the beginning of each flow by observing the sequence number in the header. Once the connection is initiated by the client, the sequence number is printed out.

II) UNIQUE PACKET SIZES

Every time the callback function is called, a map function is used to keep track of the count of unique packet sizes

III) NUMBER OF FLAGS

Count for different combinations of flags is determined by examining the header. We use separate variable for each flag count. Variable names are follows

i) Just SYN: c2ssyn

ii) SYN + ACK: c2s_syn_ack

iii) Just ACK: c2sack

iv) Just FIN: c2sfin

v) FIN + ACK: c2s_fin_ack

vi) Just PUSH: c2s_psh

vii) PUSH + other flags

viii) Just URG: c2surg

ix) URG + other flags

x) RST

Along with the counts, different types of flags along with the URG are determined.

IV) NUMBER OF TIMES SEQUENCE NUMBER WRAPPED AROUND

Sequence numbers are used to determine the freshness of messages. At startup, the initial sequence numbers to use in message generation are initialized with random values. The packet format used in TCP header the sequence numbers to a 32- bit value. This leads to the occurrence of wrap-around of sequence numbers. In order to check the wraparound, we compare the sequence number of current packet with the previous packet and if the sequence number difference is less than zero then we conclude it to be wrapped around.

V) ADVERTISED WINDOW

We check the advertised window field in the TCP HEADER and keep a track of the unique values of the size of advertised window using the mapper function. Based on the size of advertized window we decide if the window is closed or not. If the advertized window is zero then the window is said to be closed.

SERVER TO CLIENT:

Server to client start of a flow can be identified by SYN+ACK

Termination of a flow is identified by a FIN+ACK

Furthermore Server is identified by source port greater than 1023.

All other details as in client implementation.

Server to client variables can be identified by prefix “stoc” or “s2c”

REFERENCES:

1)http://www.networksorcery.com/enp/protocol/tcp.htm#Options

2) Packet Capture With libpcap and other Low Level Network