[Paper Review]Resurrection With Side Channel

Shenghan Zheng

July 13th 2022

1 Introduction

1.1 Goal

Guess destination port and TxID to do cahce poisoning

1.2 background

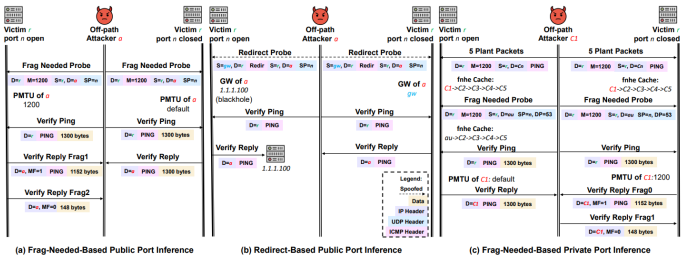
1. By RFC, any UDP ephemeral port will not check source IP because UDP is stateless
2. ICMP error message will contain 4 tuple ((source IP, source port, destination IP, destination port)) to allow source figuring out which packet went wrong
3. 3 types ICMP message: Fragment needed, Redirect, Host/Port unreachable

1.3 attacker

1. Can trigger one or more queries from the target resolver
2. IP spoofing

1.4 steps

1. find victim resolver, victim domain, and its name server
2. slow down name server to extend attack window
3. trigger query on resolver
4. guess ephemeral port
5. brute force TxID with spoofed name server IP
6. If failed, start from 3.



Keys: D=Destination IP, S=Source IP, M=PMTU, SP=Source Port, DP=Destination Port, MF=More Fragment, Cn(C1-C5)=Colliding IPs, au=Authoritative Name Server

Figure 3: Port Number Inference

1.5 Fragment needed based attack

1. public
attacker send a ICMP fragment needed message with his own IP. The embeded UDP header contains guessed ephemeral port.
In the fragment needed message, the attacker is telling the resolver that "previous message"(Linux accepts inner ICMP message as long as the inner source address and port are correct) is too large and showing the MTU set by attacker. The resolver will change this path MTU(PMTU) to the MTU provided by attacker. The attacker will send a PING to resolver with bytes larger than MTU. If the guessed port is correct, the reply will be fragmented. If it's wrong, the resolver will send back a reply with same bytes as the PING. 2. private
In this setting, the resolver will check 4-tuple to locate socket in the connection. Thus, the destination IP should be the IP of name server.The next hop exception cache is also invisible to attacker(can't see whether MTU changes) because it will go to name server directly.
There are 2048 buckets in a linux hash table and each bucket is a linked list with 5 slots. The keyed hash function is public and has a secret. The secret won't be renewed unless reboot.One strategy here is to find 5 different IPs that has the same hash value as the authoritative name server IP. The other is to guess the secret(32-bit). In the second case, we just need to find 5 IPs that have collision with any IP for the hash function in victim resolver. And try different secrets in our own environment by feeding in the 6 IPs. The secret that makes them hash into the same bucket is a possible value of the secret used in resolver. With the secret, it's easy to find 5 IPs with the same hash value as the authoritative name server(one of the IPs should under attacker control). Attacker first set destination port as its own IP and the rest 4 IPs and send the plant packet with low MTU. Then attacker will send fragment needed message with authoritative name server IP as destination port. Since all slots are consumed, the attacker's IP will be replaced by authoritative name server IP. Then, the attacker send the verify PING with default MTU. If the reply sends back packet with same default MTU, the attacker succeeds.

1.6 Redirect based attack

The attacker send a ICMP redirect message to the resolver. If the source port matches the ephemeral port, the resolver will update its routing table and route future packet to attacker through the gateway in redirect message. The gateway is configured to only accept packets. Then, the attacker will send verify PING to resolver. The attacker will not receive any response if the guessed port number is right. Otherwise, attacker will receive a verify reply from resolver.

2 Terms

2.1 4 tuples

(source IP, source port, destination IP, destination port)

2.2 checksum

One error detection technique.
The ICMP packet will carry port info to let sender know which packet went wrong. Step1.
Sender:
If m bits checksum is used, data unit is divided into segment of m bits

2.3 ICMP

Fragment needed and DF set
When the pacaket exceeds the MTU of the destination and don't fragment is enabled, the destination will send back this ICMP response(IPv4). In IPv6 setting, it doesn't have DF bit, thus, it will just return packet too big. Then the IPv6 sender will automatically try to reduce the size for the packet to be sent recursively(maybe too many times will increase the latency????)

2.4 MTU

The maximum transmission unit (MTU) is the largest size frame or packet – in bytes or octets (eight-bit bytes) – that can be transmitted across a data link. It is most used in reference to packet size on an Ethernet network using the Internet Protocol (IP).
If the packet is too large and the next receiving device cannot accept it, the packet is divided into multiple packets and sent. This is called fragmentation.
DF(don't fragment) Bit(Only available in IPv4)
A bit in an IPv4 header that prevents a packet from being fragmented

2.5 IPID

An IP header field, called an IPID, identifies a packet in a communication session by identifying it as an IP address. IPID is primarily intended to recover from IP fragmentation.
It's used to assist network-layer fragmentation and reassembly, the IP identification field (IP-ID) has been used and abused for a range of tasks, from counting hosts behind NAT, to detect router aliases and, lately, to assist detection of censorship in the Internet at large. It can be used as side channels

In 2013, RFC6864 [26] updated the specifications by affirming that the IPv4 ID uniqueness applies to only non-atomic datagrams: in other words, if the don't fragment (DF) bit is set, reassembly is not necessary and hence devices may set the IP-ID to zero

2.6 keyed hashing

An algorithm that creates a message authentication code based on both a message and a secret key shared by two endpoints. Also known as a hash message authentication code algorithm.

2.7 PING

A ping (Packet Internet or Inter-Network Groper) is a basic Internet program that allows a user to test and verify if a particular destination IP address exists and can accept requests in computer network administration.
Ping works by sending an Internet Control Message Protocol (ICMP) Echo Request to a specified interface on the network and waiting for a reply. When a ping command is issued, a ping signal is sent to a specified address. When the target host receives the echo request, it responds by sending an echo reply packet.

2.8 PMTU

Path MTU Discovery. A technique to determine MTU between 2 IP hosts.
1. IPv4
Set DF bit for outgoing packet. Any devices whose MTU is smaller than the packet will drop it and send back a ICMP fragmentation needed message CONTAINING ITS MTU to let the source port reduce its MTU accordingly.
2. IPv6
Path MTU is the same as MTU of link layer by default. Any devices along the path with MTU smaller than the packet will drop it and send back ICMP v6 packet too big message containing its MTU to let the source port reduce its path MTU.

2.9 MSS

The maximum segment size (MSS) is the largest amount of data, specified in bytes, that a computer or communications device can handle in a single, unfragmented piece. For optimum communications, the number of bytes in the data segment and the header must add up to less than the number of bytes in the maximum transmission unit (MTU).

2.10 routing table

A data table stored in a router or a network host that lists the routes to particular network destinations
Content
1. network destination and netmask
2. metric(the route will go to lowest path with lowest metric)
3. next hop(gateway)