QUIC Attacks: Implementation and Analysis

STUDENT

YUCHEN WANG

ADVISOR

SHAN CHEN

Goal

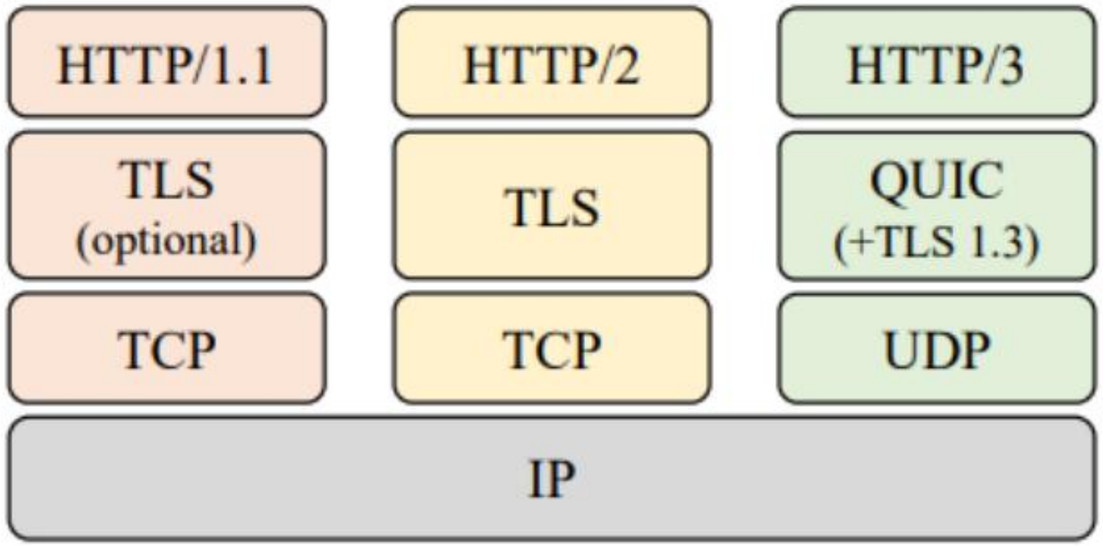
I Implement Version Negotiation Request Forgery (VNRF)

II Implement Connection Migration Request Forgery (CMRF)

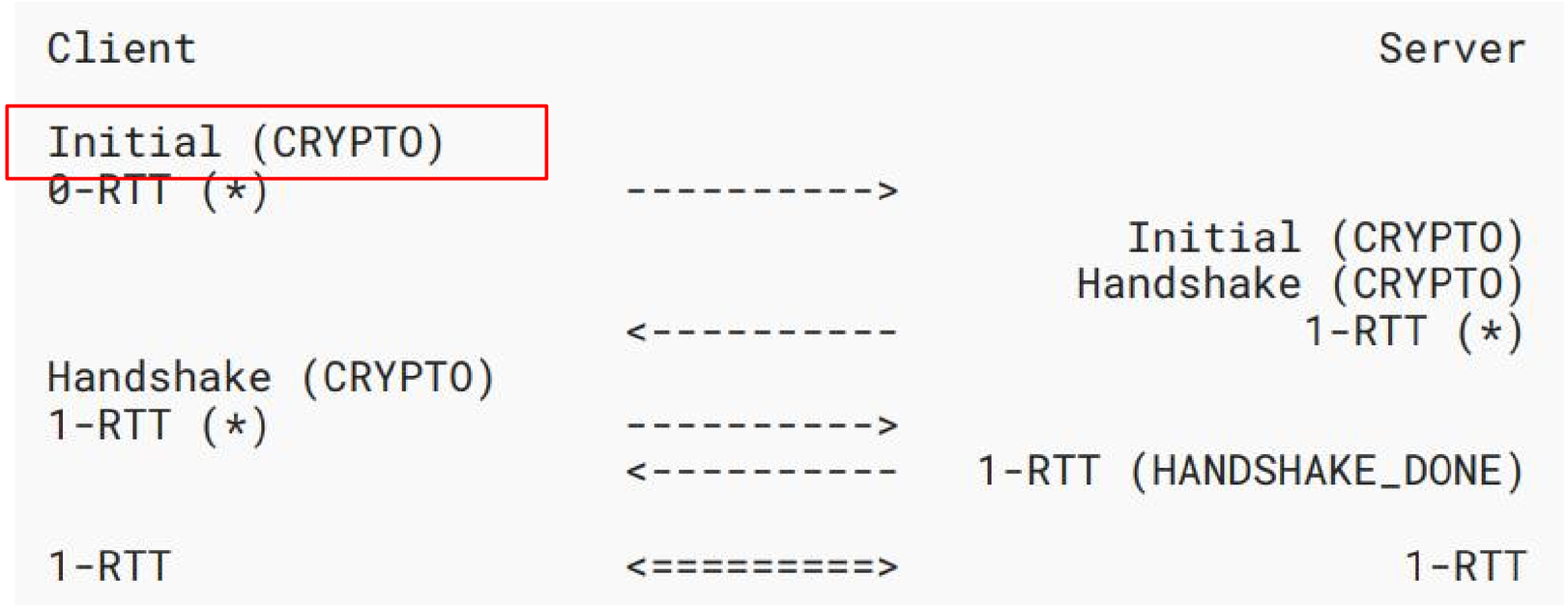
III Mitigation Approaches

Table of Contents

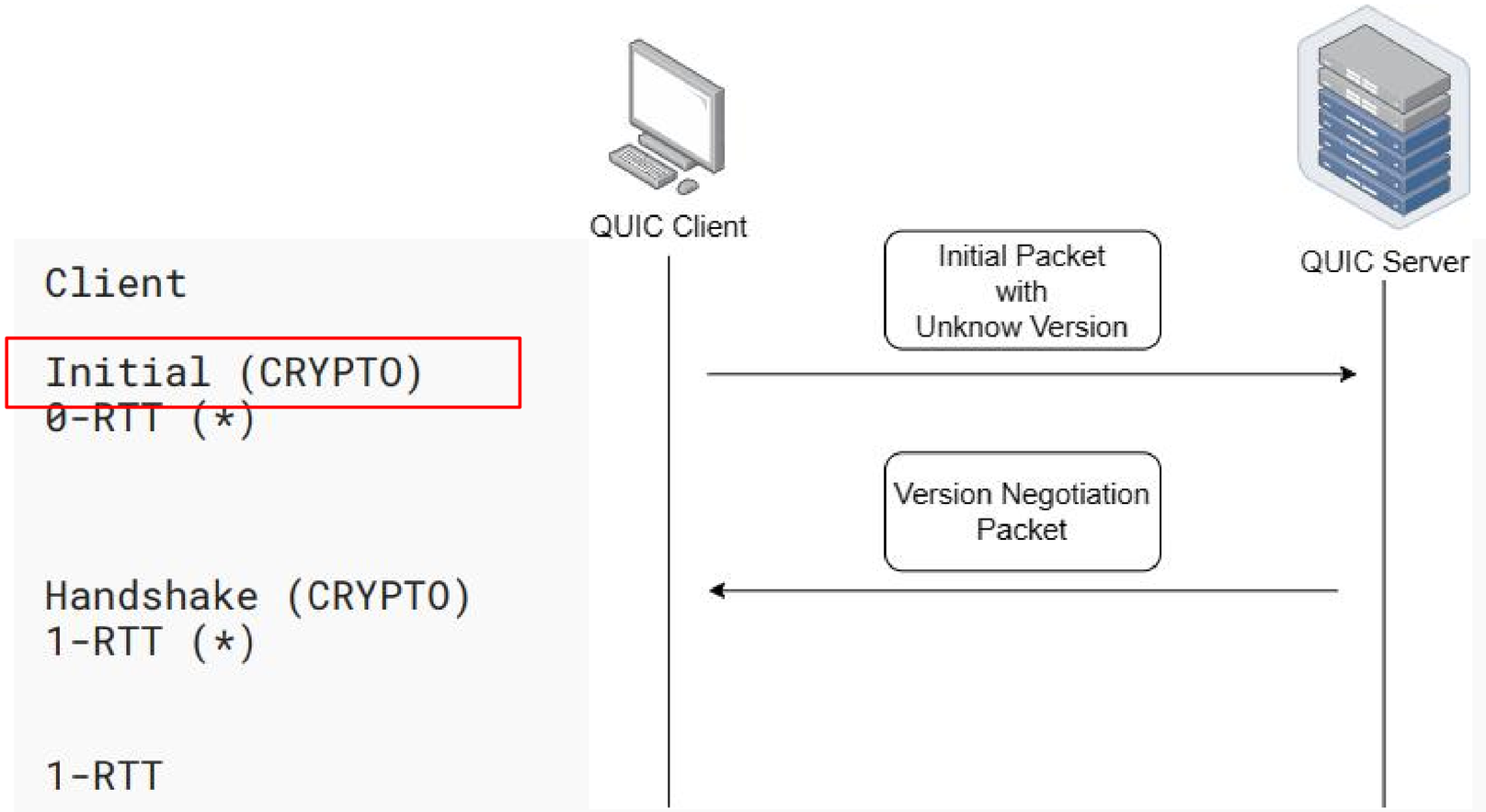
- UDP-based
- Connection Oriented
- TLS Handshake Parameter



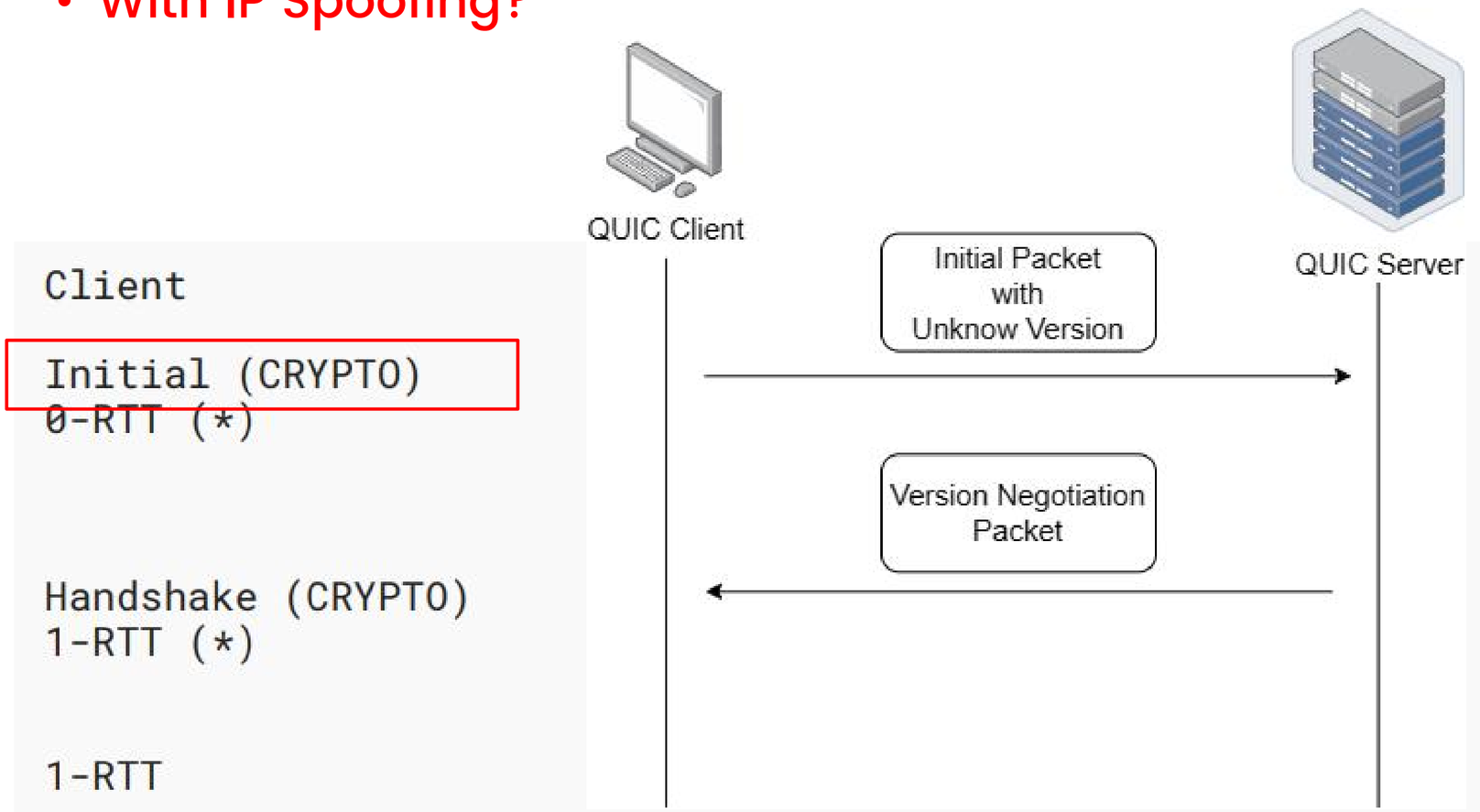
- Version Negotiation
- Triggered by unknown version



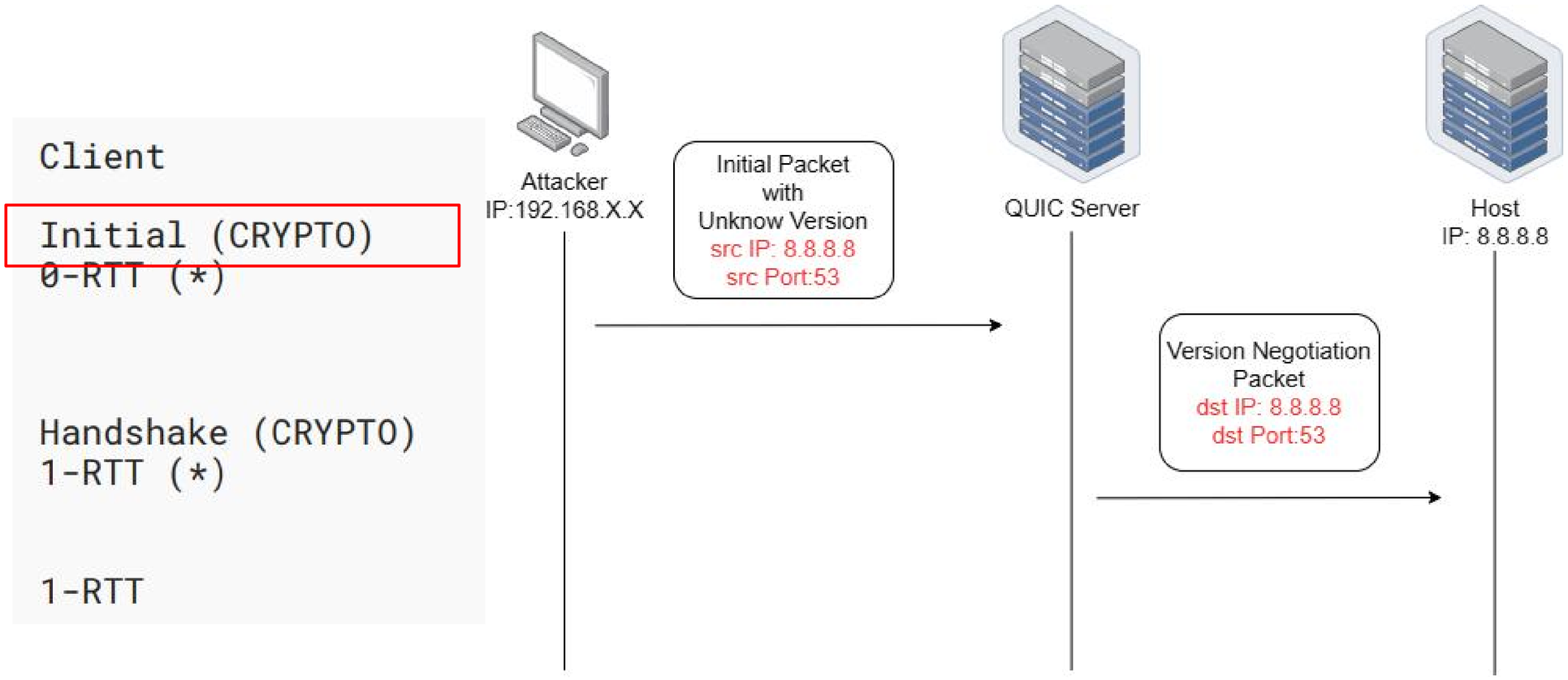
- Version Negotiation
- Triggered by unknown version



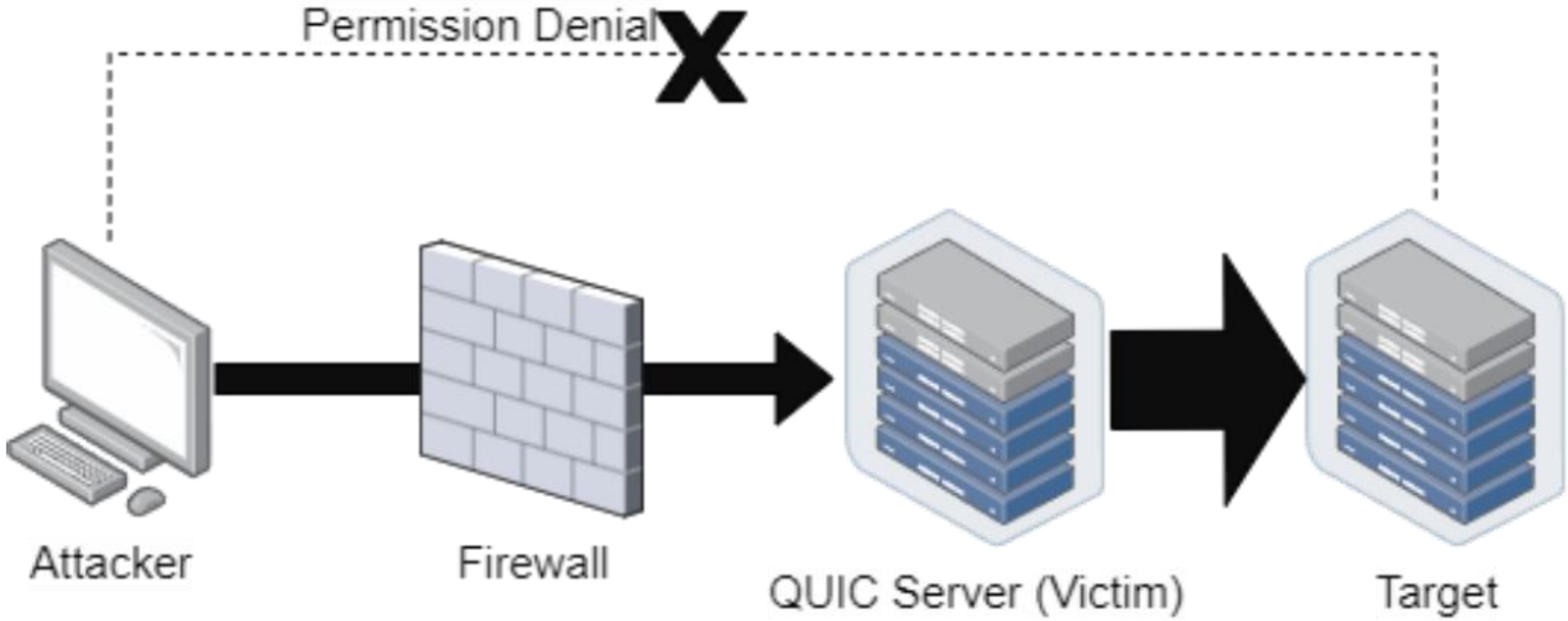
- Version Negotiation
- Triggered by unknown version
- With IP Spoofing?



- Version Negotiation
- Triggered by unknown version
- With IP Spoofing?



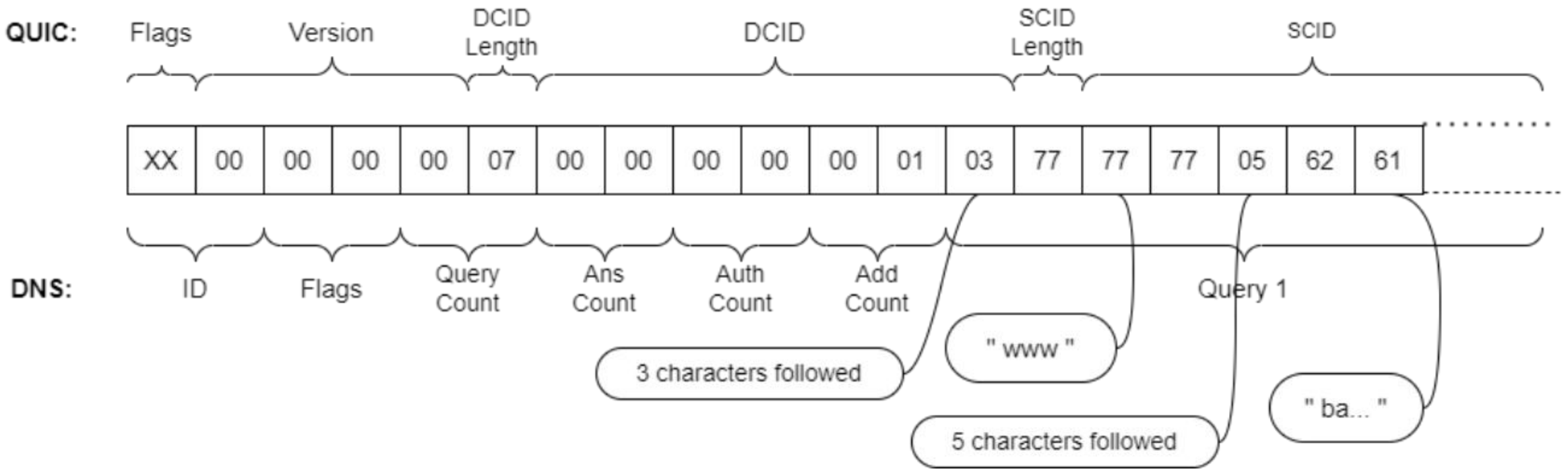
- Request Forgery
- Server send “unintended” request to other host
- Attacker gain high privilege and bandwith



Version Negotiation Request Forgery (VNRF)

```
Version Negotiation Packet {
  Header Form (1) = 1,
  Unused (7),
  Version (32) = 0,
  Destination Connection ID Length (8),
  Destination Connection ID (0..2040),
  Source Connection ID Length (8),
  Source Connection ID (0..2040),
  Supported Version (32) ...,
}
```

Version Negotiation Request Forgery (VNRF)



Experiment

udp.port == 12345

No.	Time	Source	Destination	Protocol	Length	Info
113	11.273585	8.8.8.8	192.168.137.245	QUIC	1322	Initial, SCID=00000000000103
114	11.274494	192.168.137.245	8.8.8.8	QUIC	203	Version Negotiation, DCID=00000000000103

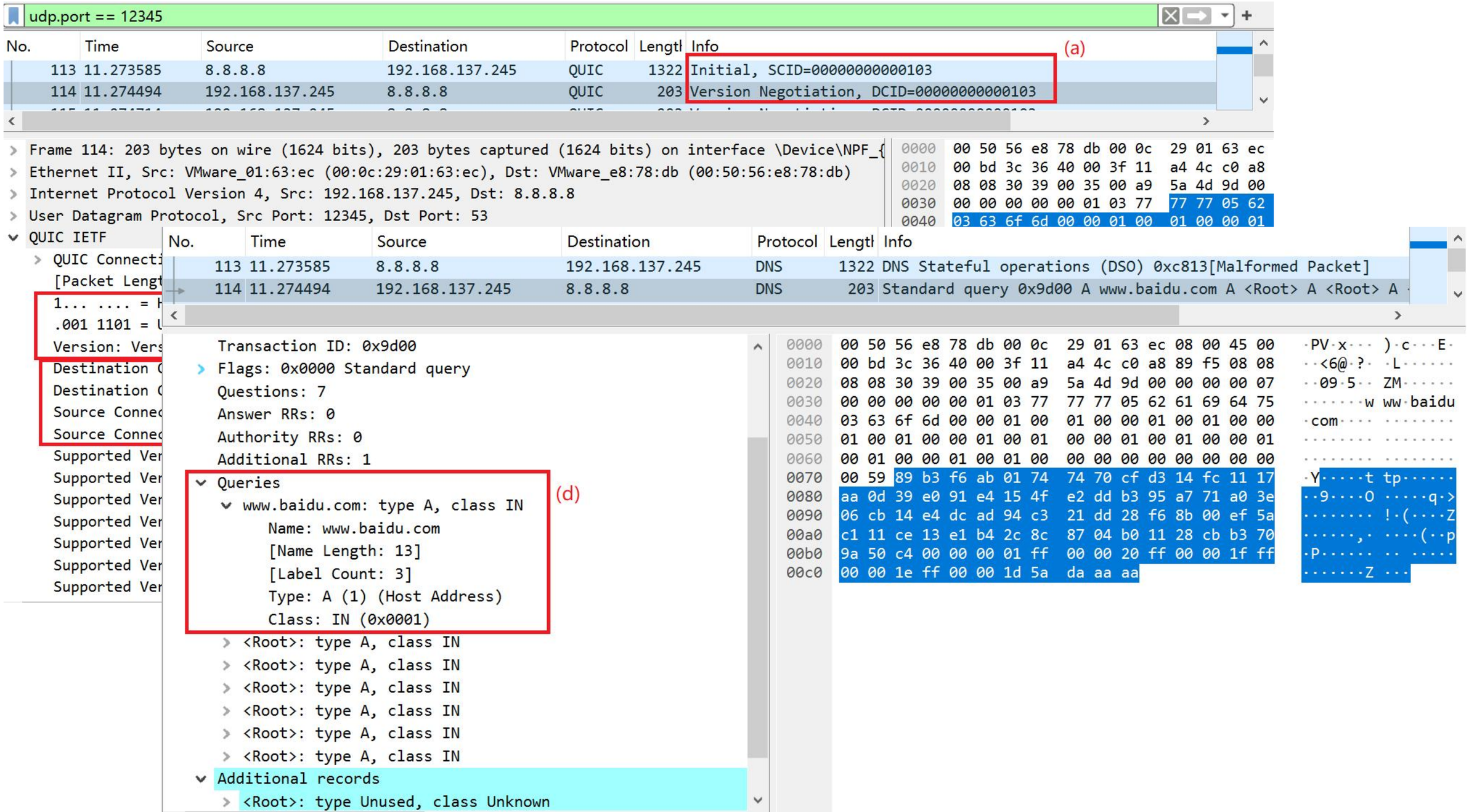
(a)

```
Frame 114: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface \Device\NPF_{
Ethernet II, Src: VMware_01:63:ec (00:0c:29:01:63:ec), Dst: VMware_e8:78:db (00:50:56:e8:78:db)
Internet Protocol Version 4, Src: 192.168.137.245, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 12345, Dst Port: 53
QUIC IETF
  QUIC Connection information
  [Packet Length: 161]
  1... .... = Header Form: Long Header (1)
  .001 1101 = Unused: 0x1d
  Version: Version Negotiation (0x00000000)
  Destination Connection ID Length: 7
  Destination Connection ID: 00000000000103
  Source Connection ID Length: 119
  Source Connection ID [truncated]: 777705626169647503636f6d0000010001000001000100000100010000010
  Supported Version: v2-draft-01 (0x709a50c4)
  Supported Version: 1 (0x00000001)
  Supported Version: draft-32 (0xff000020)
  Supported Version: draft-31 (0xff00001f)
  Supported Version: draft-30 (0xff00001e)
  Supported Version: draft-29 (0xff00001d)
  Supported Version: Unknown (0x5adaaaaa) (GREASE)
```

(b)

(c)

```
0000  00 50 56 e8 78 db 00 0c  29 01 63 ec
0010  00 bd 3c 36 40 00 3f 11  a4 4c c0 a8
0020  08 08 30 39 00 35 00 a9  5a 4d 9d 00
0030  00 00 00 00 00 01 03 77  77 77 05 62
0040  03 63 6f 6d 00 00 01 00  01 00 00 01
0050  01 00 01 00 00 01 00 01  00 00 01 00
0060  00 01 00 00 01 00 01 00  00 00 00 00
0070  00 59 89 b3 f6 ab 01 74  74 70 cf d3
0080  aa 0d 39 e0 91 e4 15 4f  e2 dd b3 95
0090  06 cb 14 e4 dc ad 94 c3  21 dd 28 f6
00a0  c1 11 ce 13 e1 b4 2c 8c  87 04 b0 11
00b0  9a 50 c4 00 00 00 01 ff  00 00 20 ff
00c0  00 00 1e ff 00 00 1d 5a  da aa aa
```


udp.port == 12345
No. Time Source Destination Protocol Lengtl Info
113 11.273585 8.8.8.8 192.168.137.245 QUIC 1322 Initial, SCID=00000000000103
114 11.274494 192.168.137.245 8.8.8.8 QUIC 203 Version Negotiation, DCID=00000000000103
(a)
Frame 114: 203 bytes on wire (1624 bits), 203 bytes captured (1624 bits) on interface \Device\NPF_{
Ethernet II, Src: VMware_01:63:ec (00:0c:29:01:63:ec), Dst: VMware_e8:78:db (00:50:56:e8:78:db)
Internet Protocol Version 4, Src: 192.168.137.245, Dst: 8.8.8.8
User Datagram Protocol, Src Port: 12345, Dst Port: 53
0000 00 50 56 e8 78 db 00 0c 29 01 63 ec
0010 00 bd 3c 36 40 00 3f 11 a4 4c c0 a8
0020 08 08 30 39 00 35 00 a9 5a 4d 9d 00
0030 00 00 00 00 00 01 03 77 77 77 05 62
0040 03 63 6f 6d 00 00 01 00 01 00 00 01
QUIC IETF
QUIC Connecti
[Packet Lengt
1... .... = H
.001 1101 = U
Version: Vers
Destination C
Destination C
Source Connec
Source Connec
Supported Ver
Supported Ver
Supported Ver
Supported Ver
Supported Ver
Supported Ver
Supported Ver
Supported Ver
No. Time Source Destination Protocol Lengtl Info
113 11.273585 8.8.8.8 192.168.137.245 DNS 1322 DNS Stateful operations (DSO) 0xc813[Malformed Packet]
114 11.274494 192.168.137.245 8.8.8.8 DNS 203 Standard query 0x9d00 A www.baidu.com A <Root> A <Root> A
Transaction ID: 0x9d00
Flags: 0x0000 Standard query
Questions: 7
Answer RRs: 0
Authority RRs: 0
Additional RRs: 1
Queries
www.baidu.com: type A, class IN
Name: www.baidu.com
[Name Length: 13]
[Label Count: 3]
Type: A (1) (Host Address)
Class: IN (0x0001)
(d)
<Root>: type A, class IN
<Root>: type A, class IN
<Root>: type A, class IN
<Root>: type A, class IN
<Root>: type A, class IN
<Root>: type A, class IN
Additional records
<Root>: type Unused, class Unknown
0000 00 50 56 e8 78 db 00 0c 29 01 63 ec 08 00 45 00 ·PV·x···)·c···E·
0010 00 bd 3c 36 40 00 3f 11 a4 4c c0 a8 89 f5 08 08 ··<6@·?· ·L·····
0020 08 08 30 39 00 35 00 a9 5a 4d 9d 00 00 00 00 07 ··09·5·· ZM·····
0030 00 00 00 00 00 01 03 77 77 77 05 62 61 69 64 75 ·····w ww·baidu
0040 03 63 6f 6d 00 00 01 00 01 00 00 01 00 01 00 00 ·com···· ····
0050 01 00 01 00 00 01 00 01 00 00 01 00 01 00 00 01 ····· ····
0060 00 01 00 00 01 00 01 00 00 00 00 00 00 00 00 00 ····· ····
0070 00 59 89 b3 f6 ab 01 74 74 70 cf d3 14 fc 11 17 ·Y····· tp·····
0080 aa 0d 39 e0 91 e4 15 4f e2 dd b3 95 a7 71 a0 3e ··9····O ·····q·>
0090 06 cb 14 e4 dc ad 94 c3 21 dd 28 f6 8b 00 ef 5a ····· !·(····Z
00a0 c1 11 ce 13 e1 b4 2c 8c 87 04 b0 11 28 cb b3 70 ····· ,· ····(··p
00b0 9a 50 c4 00 00 00 01 ff 00 00 20 ff 00 00 1f ff ·P····· ·· ·····
00c0 00 00 1e ff 00 00 1d 5a da aa aa ·····Z ···

No.	Time	Source	Destination	Protocol	Length	Info
114	11.274494	192.168.137.245	8.8.8.8	DNS	203	Standard query 0x9d00 A www.baidu.com A <Root> A <Root> A
115	11.274714	192.168.137.245	8.8.8.8	DNS	203	Standard query 0xd600 A www.baidu.com A <Root> A <Root> A
116	11.289280	8.8.8.8	192.168.137.245	DNS	132	Standard query response 0x9d00 A www.baidu.com CNAME www.a

```
> Frame 116: 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits) on interface \Device\NPF_{1C38514A-1C82-4068-96BE-533F44BA8B0B},
> Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: VMware_01:63:ec (00:0c:29:01:63:ec)
> Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.137.245
> User Datagram Protocol, Src Port: 53, Dst Port: 12345
v Domain Name System (response)
    Transaction ID: 0x9d00
  > Flags: 0x8080 Standard query response, No error
    Questions: 1
    Answer RRs: 3
    Authority RRs: 0
    Additional RRs: 0
  > Queries
  v Answers
    > www.baidu.com: type CNAME, class IN, cname www.a.shifen.com
    > www.a.shifen.com: type A, class IN, addr 183.2.172.42
    > www.a.shifen.com: type A, class IN, addr 183.2.172.185
    [Request In: 114]
    [Time: 0.014786000 seconds]
```

(e)

I Implement Connection Migration Request Forgery (CMRF)

II Mitigation Approaches

Thank you for listening