

Better don't be too QUIC(K)

Yuri Gbur

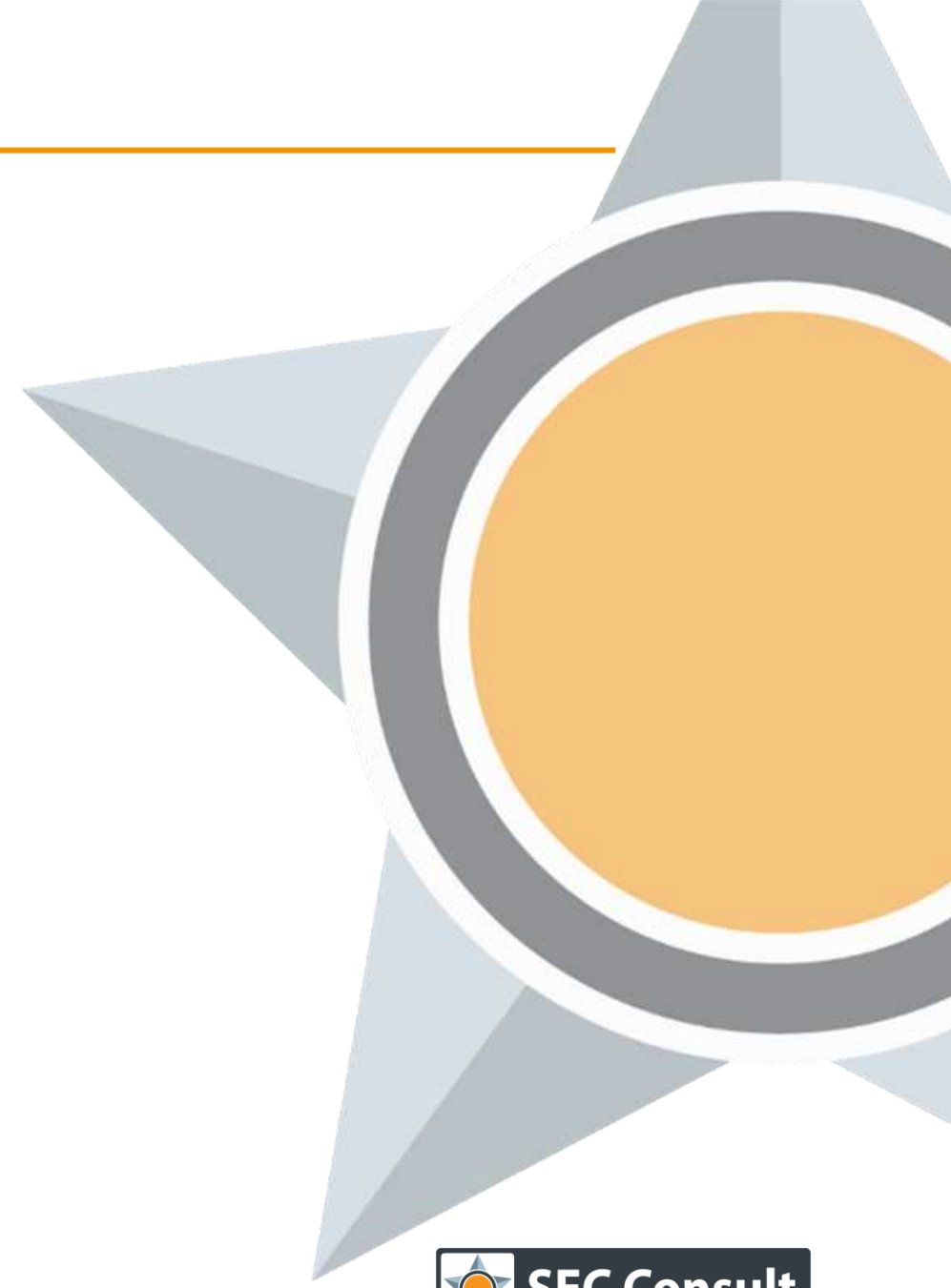
Yuri Gbur

- MSc in Computer Science at Technische Universität (TU) Berlin
- Security Consultant at SEC Consult
- Head of Cloud Security

y.gbur@sec-consult.com

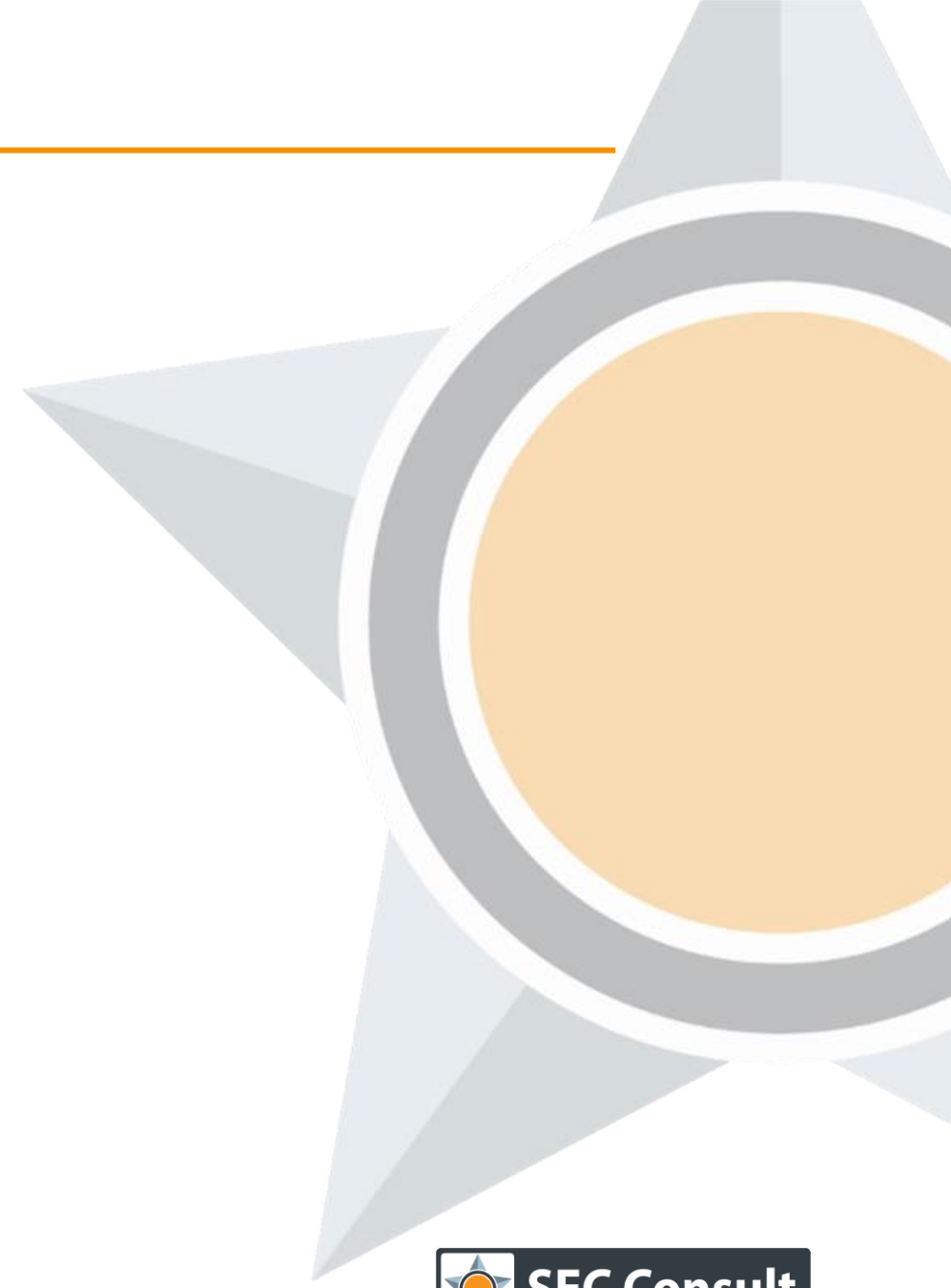
 @yukonsec

 yukonsec@infosec.exchange



Agenda

- QUIC Background
- Challenges with Securing QUIC / HTTP3
 - Differences to TCP/TLS
 - Missing Vendor Support
- Request Forgery in QUIC
 - Protocol Impersonation
 - Traffic Amplification



QUIC(K) Background

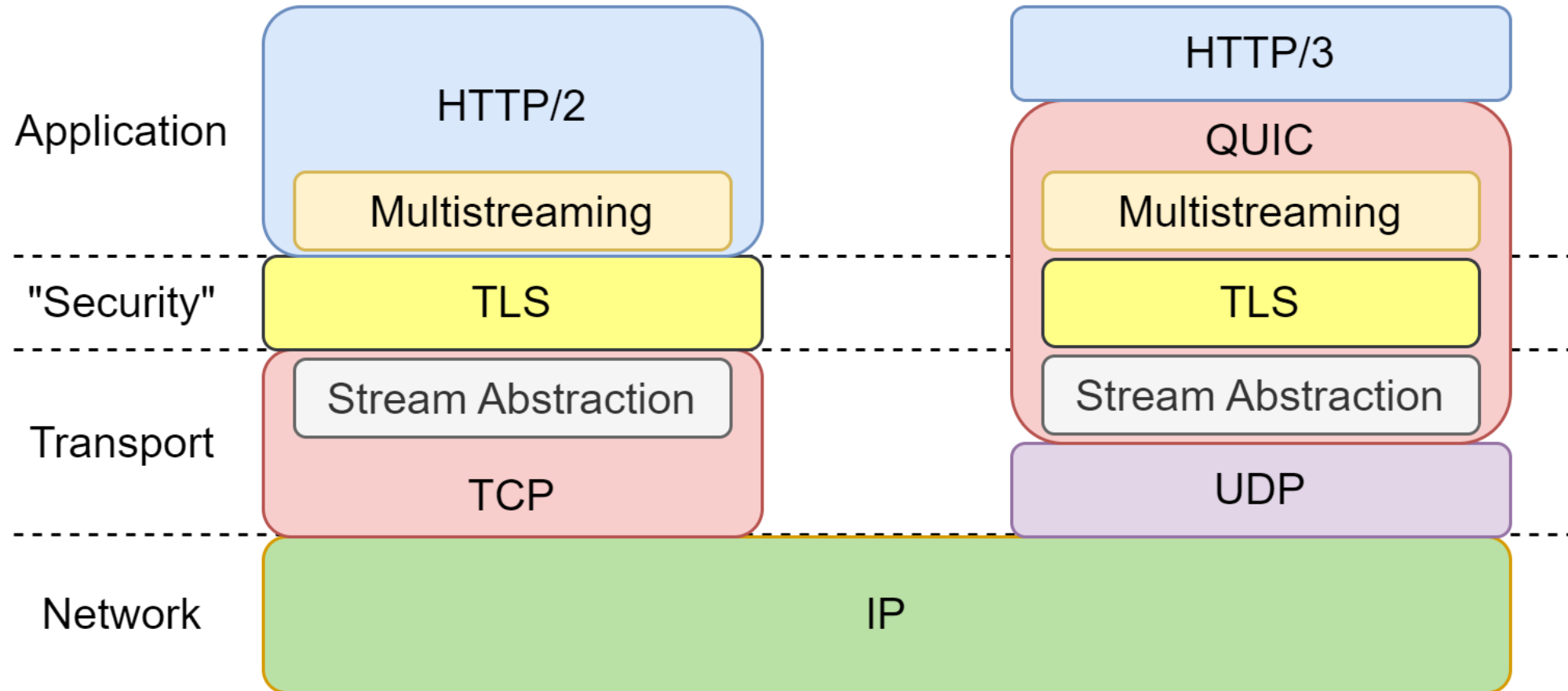
Why QUIC?

- RFC 8999
- RFC 9000
- RFC 9001
- RFC 9002

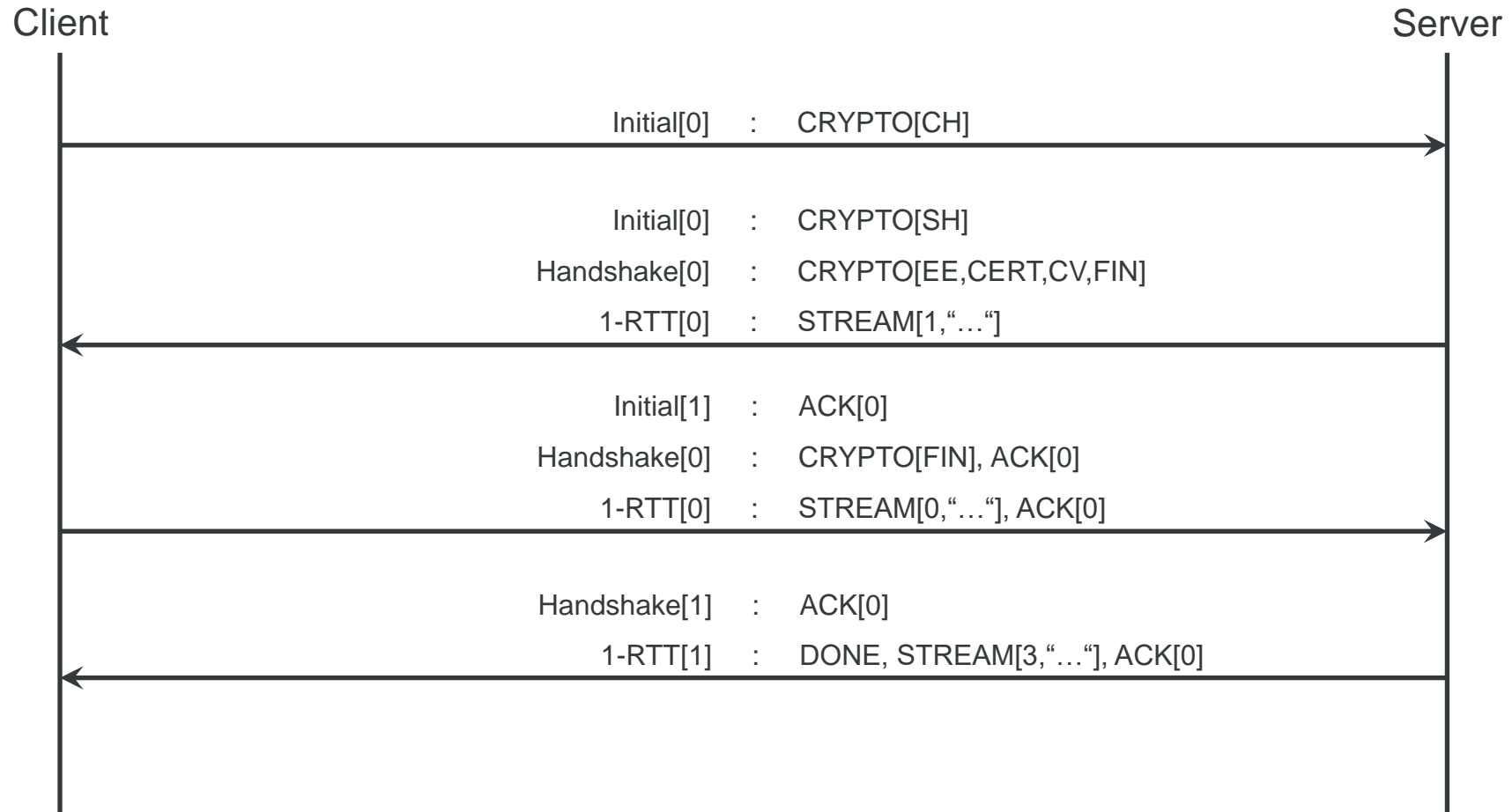
- RFC 9115
(HTTP/3)



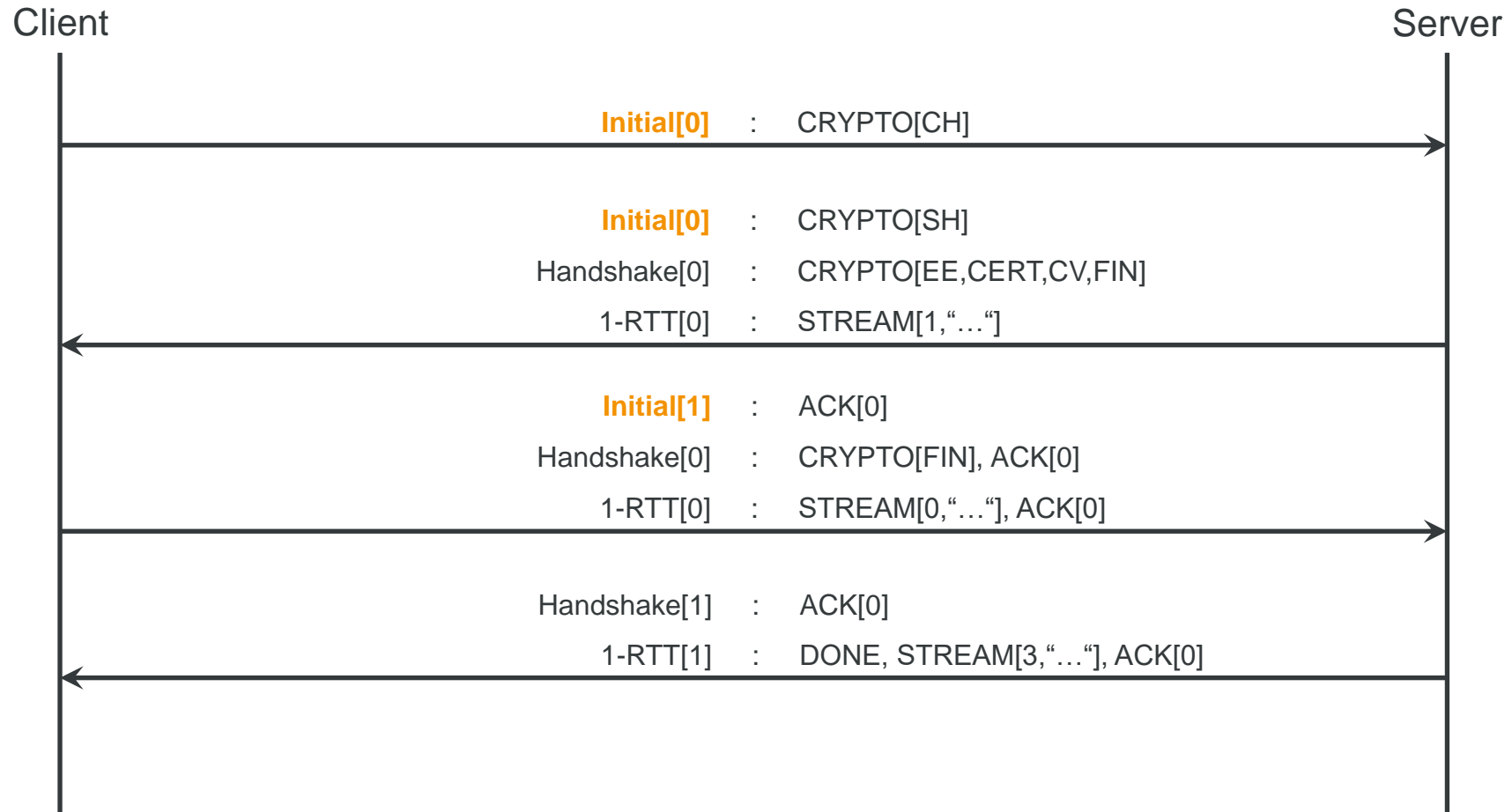
HTTP/2 VS HTTP/3



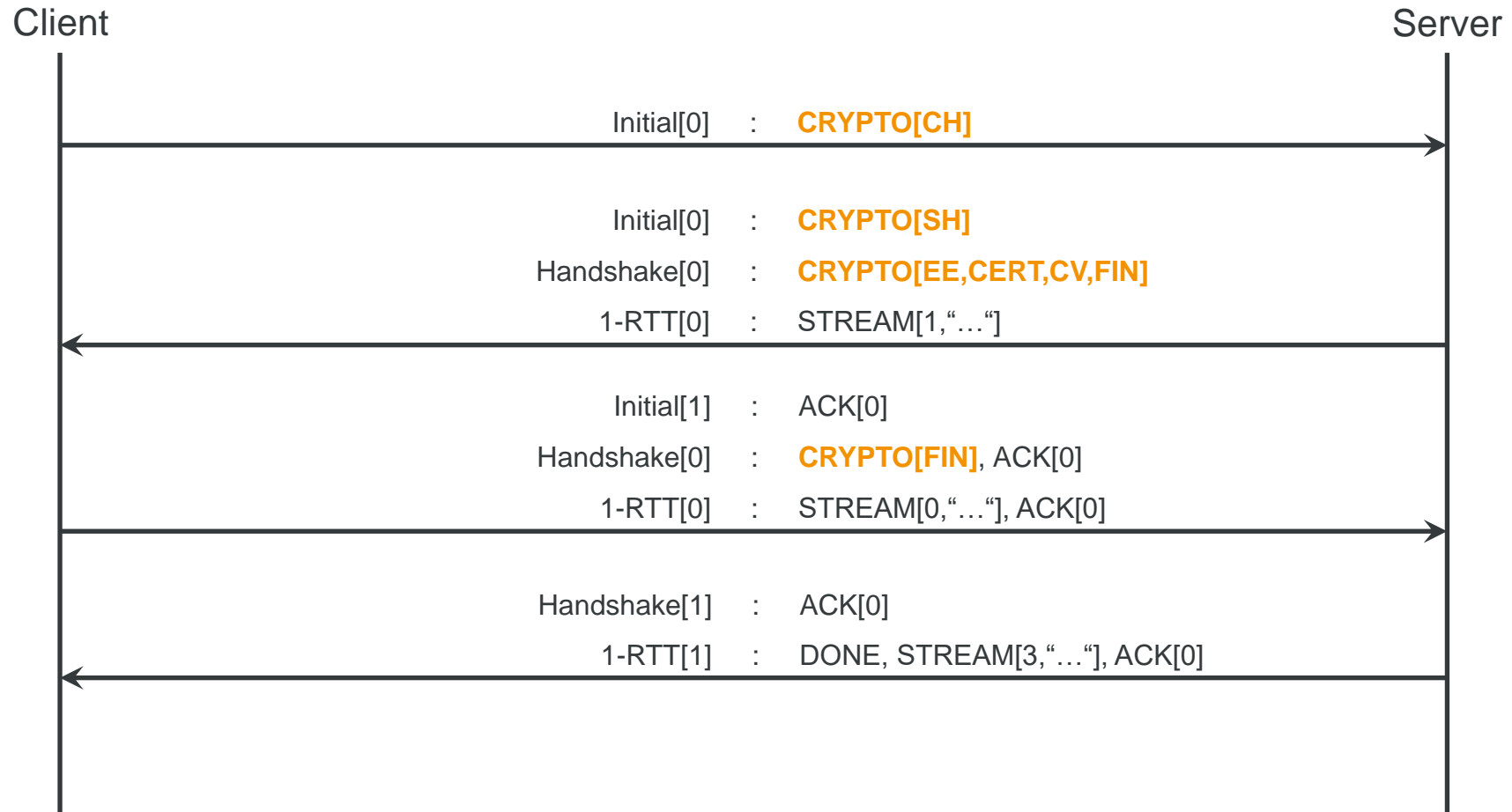
QUIC Handshake



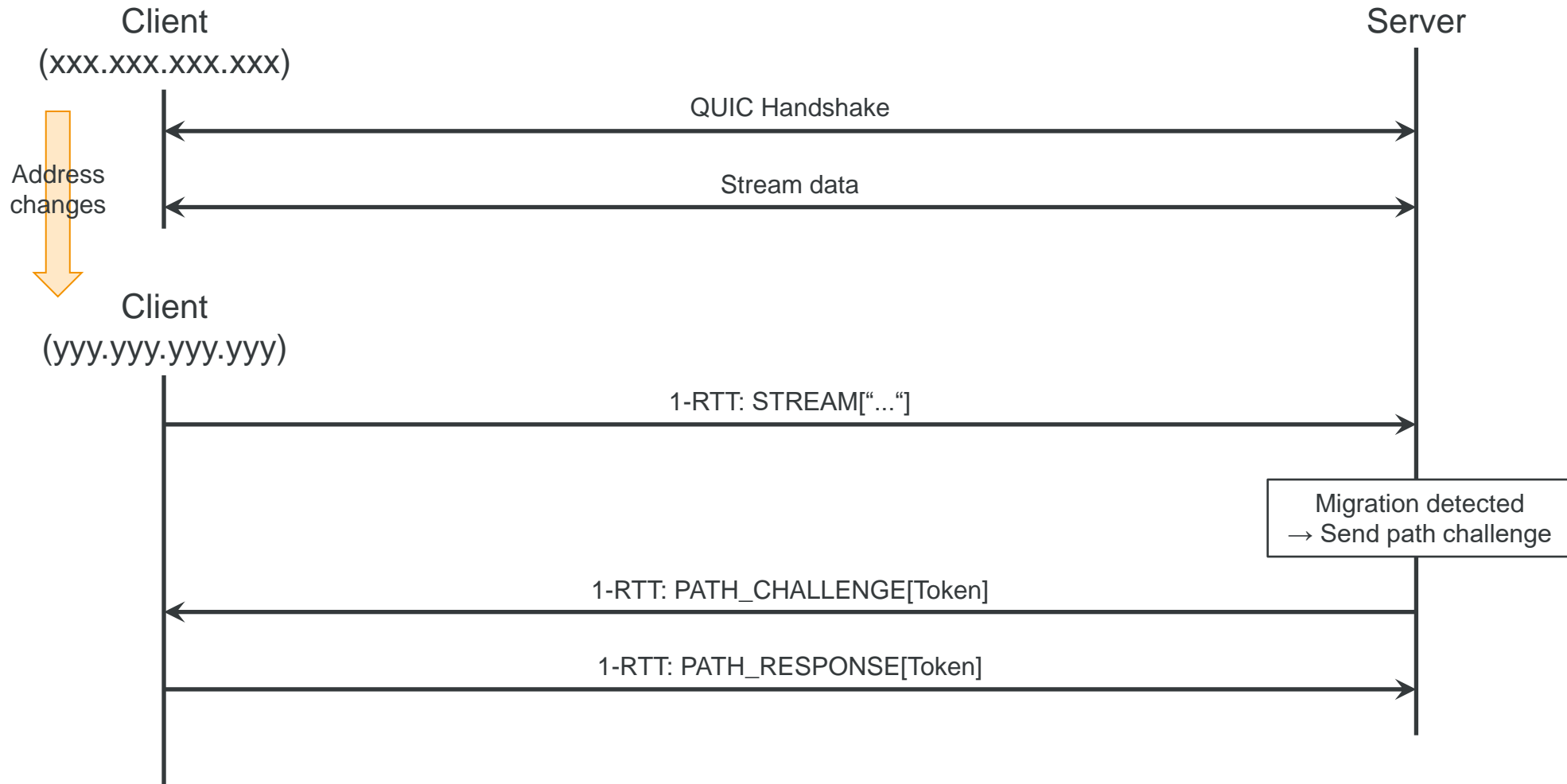
QUIC Handshake



QUIC Handshake



Connection Migration



Challenges with Securing QUIC / HTTP3

Living in the User Land

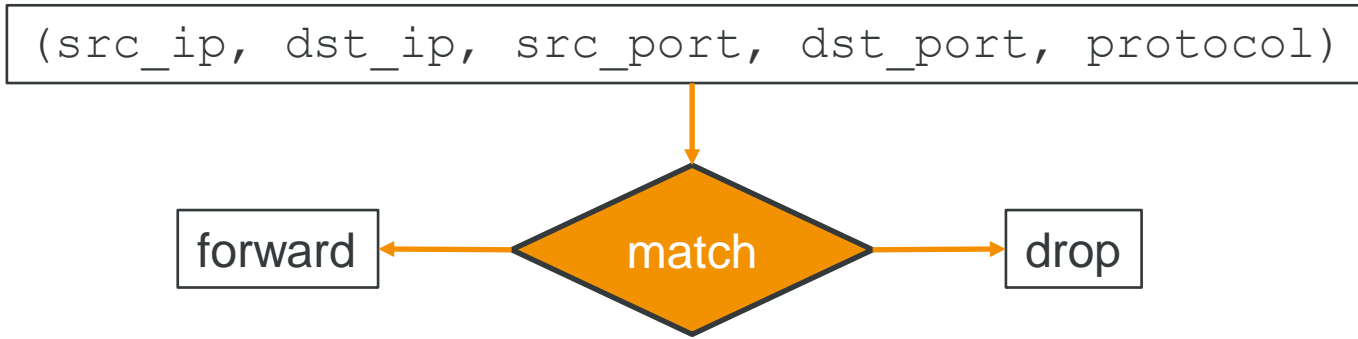
Pro

- Easier / faster updates of the “transport” layer.
- Less complex and error-prone code in the Kernel.

Con

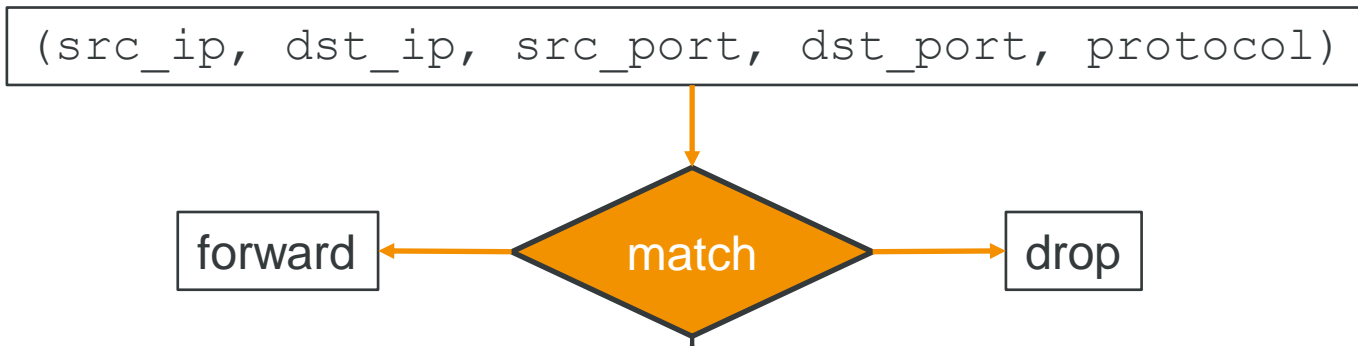
- No common TCP syscalls (e.g. listen, connect).
- Larger attack surface and weaker security boundaries.
- Lots of different / custom implementations of the same network functionality.

Transport Layer Firewalls



Stateless

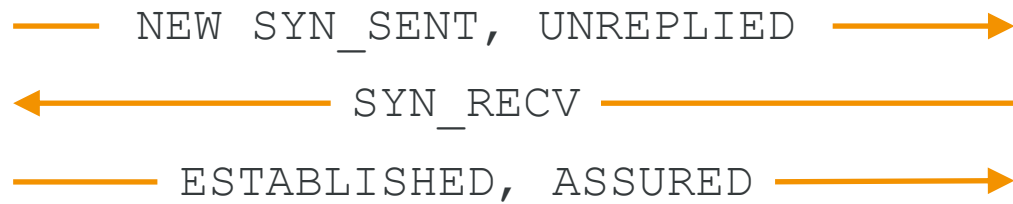
Stateful



(.111, .234, 1234, 443, TCP)	SYN_SENT, UNREPLIED
(.112, .234, 2345, 443, TCP)	SYN_RECV
(.113, .234, 3456, 443, TCP)	ESTABLISHED, ASSURED
(.114, .234, 4567, 443, TCP)	FIN_WAIT

Stateful Tracking

TCP

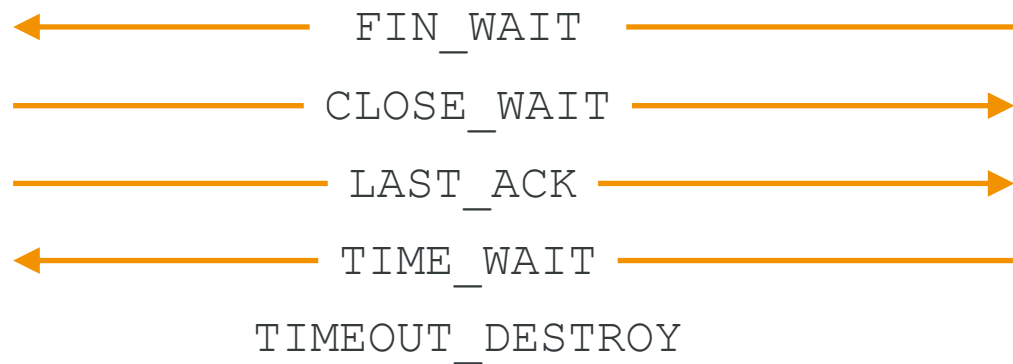


UDP



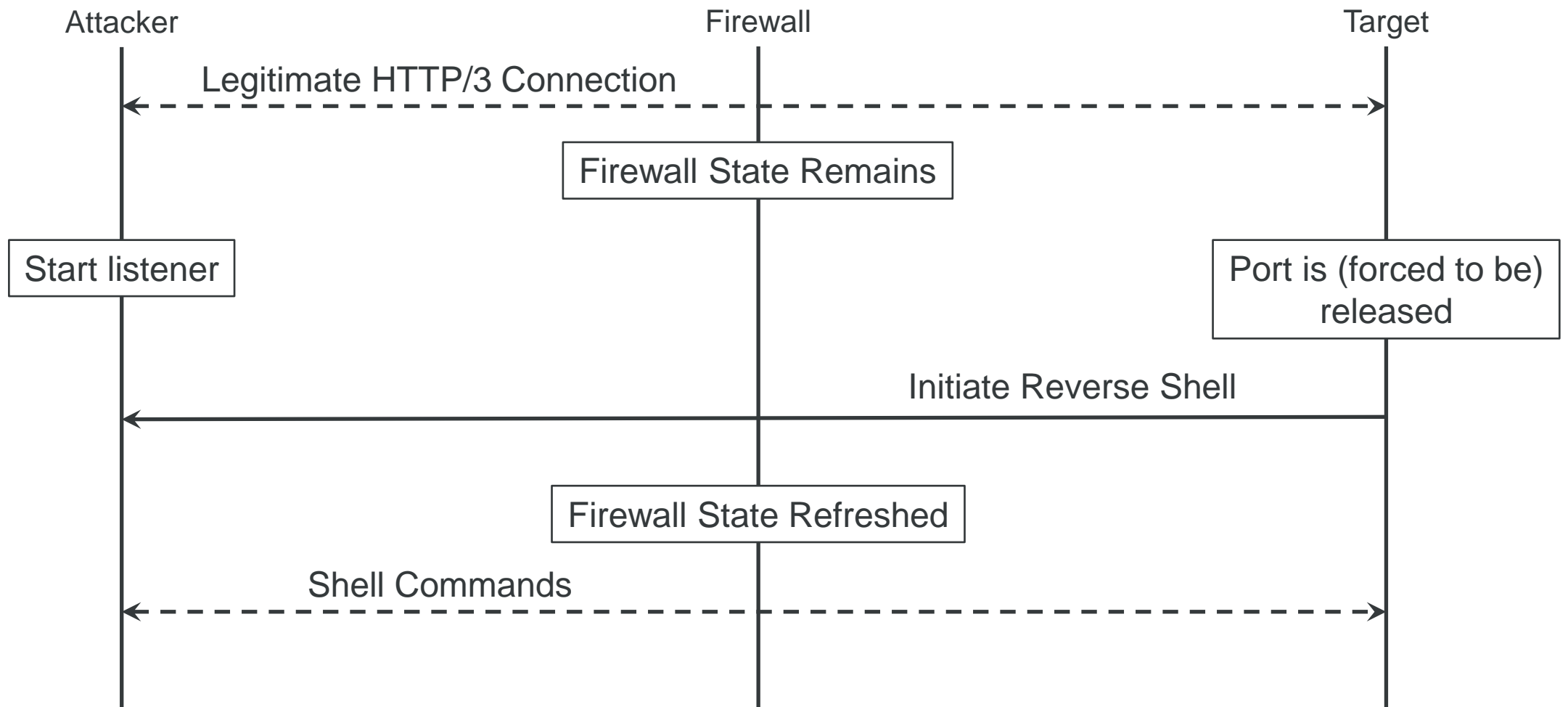
Setup

Teardown



TIMEOUT_DESTROY

UDP Hole Punching



Deep Packet Inspection with QUIC

Routing / Optimization

- Important metadata headers are encrypted → Impact on routing strategies.
- Limited support by load balancers → Bypasses possible.

Application Layer Security

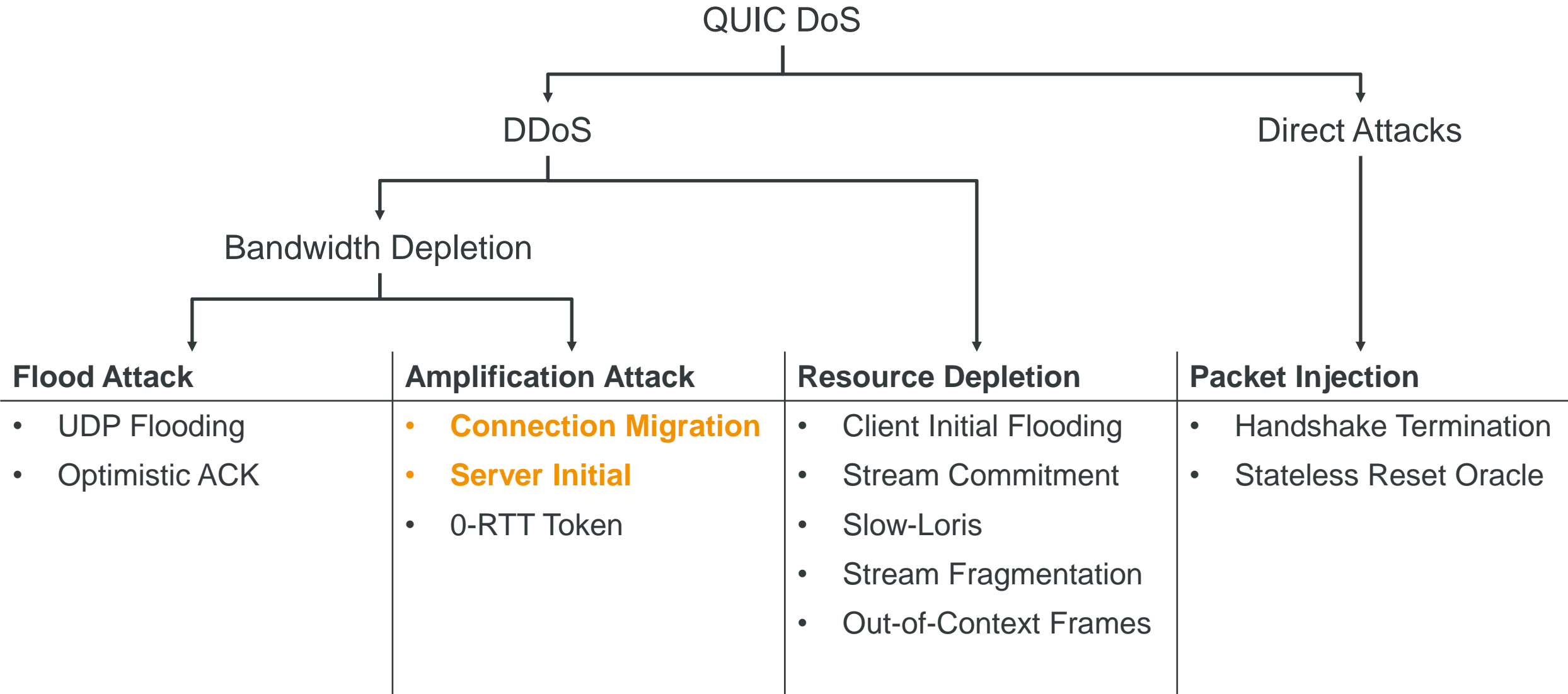
- Very limited support by existing WAFs.
- No support for the integrated multistreaming.

General Tooling Support

Tool	QUIC / HTTP/3	Alternatives
Wireshark	✓	
Chrome / Firefox	✓	
BurpSuite	✗	-
OWASP ZAP	✗	-
Nessus	✗	-
testssl, sslscan, ...	✗	-
Postman	✗	Pororoca
curl (Experimental)	(✓)	
mitmproxy (Experimental, Forks)	(✓)	mitmproxy by meitinger
netcat	✗	quiccat by rossia (limited features)
socat	✗	quiccat by pas2k

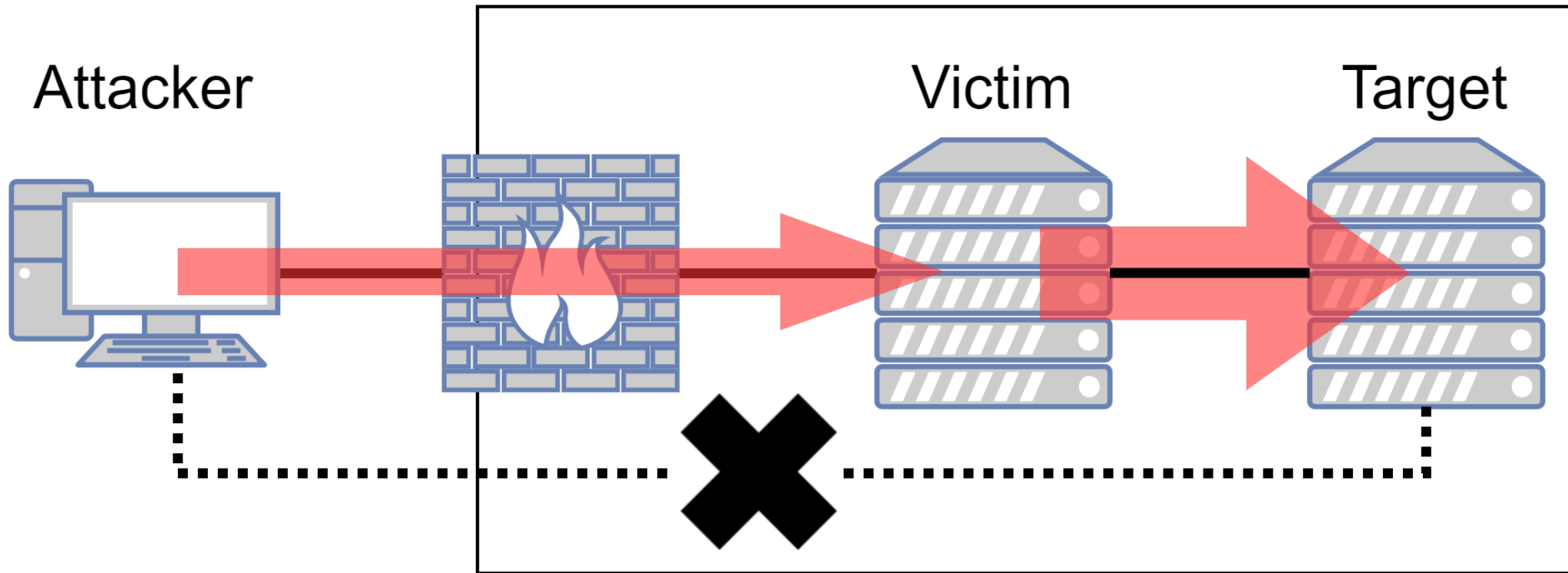
Disclaimer: No guarantees for any of those tools. Use carefully!

(D)DoS – Same Same but Different



Request Forgery

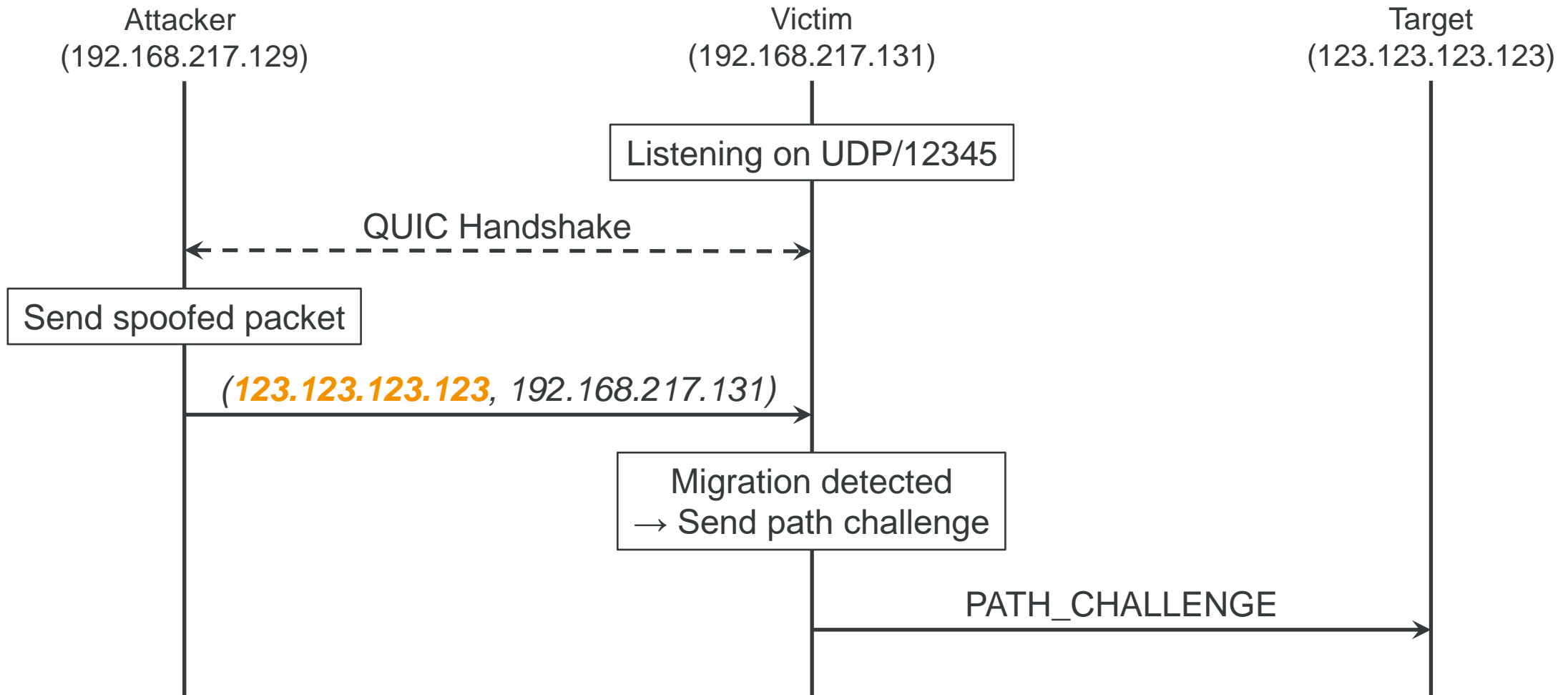
Client-side Request Forgery



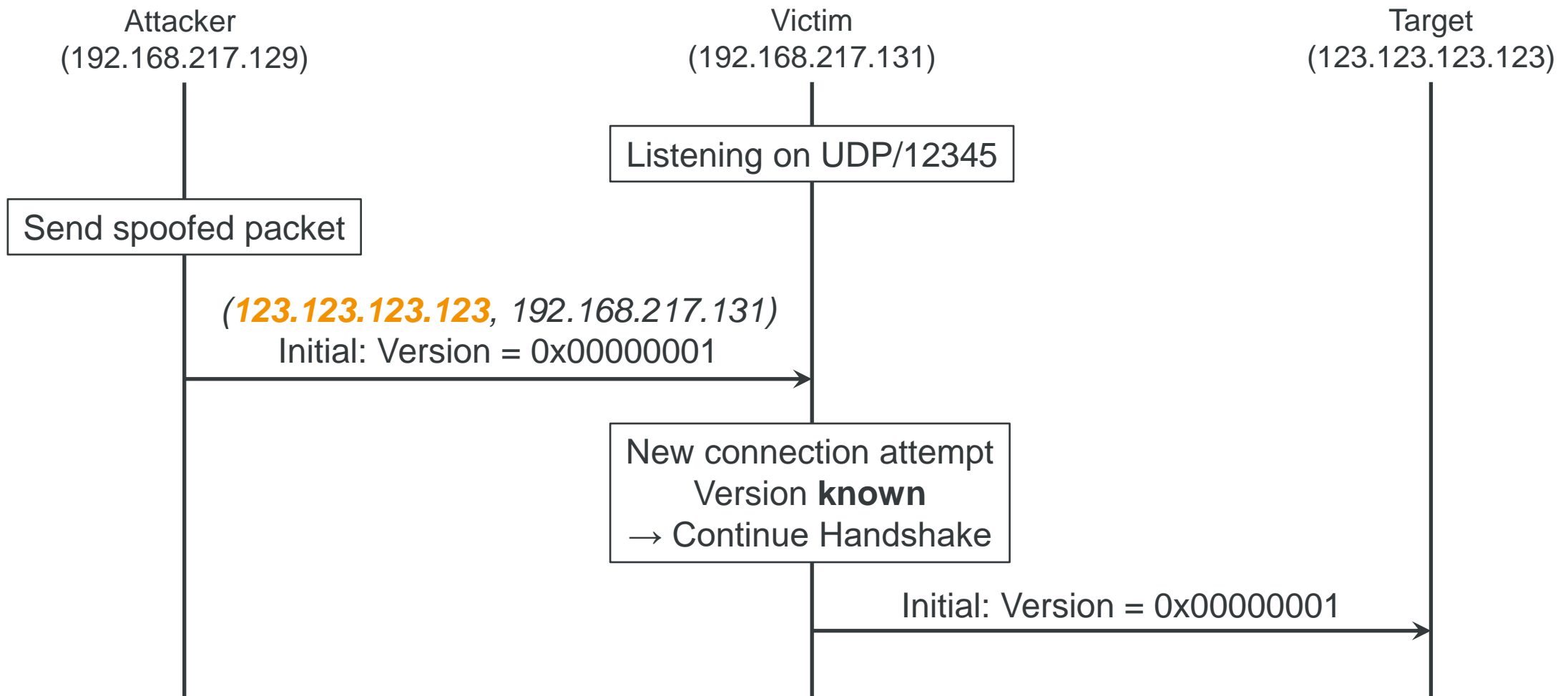
— Bypassing Network Restrictions

➔ Utilizing Victim Resources

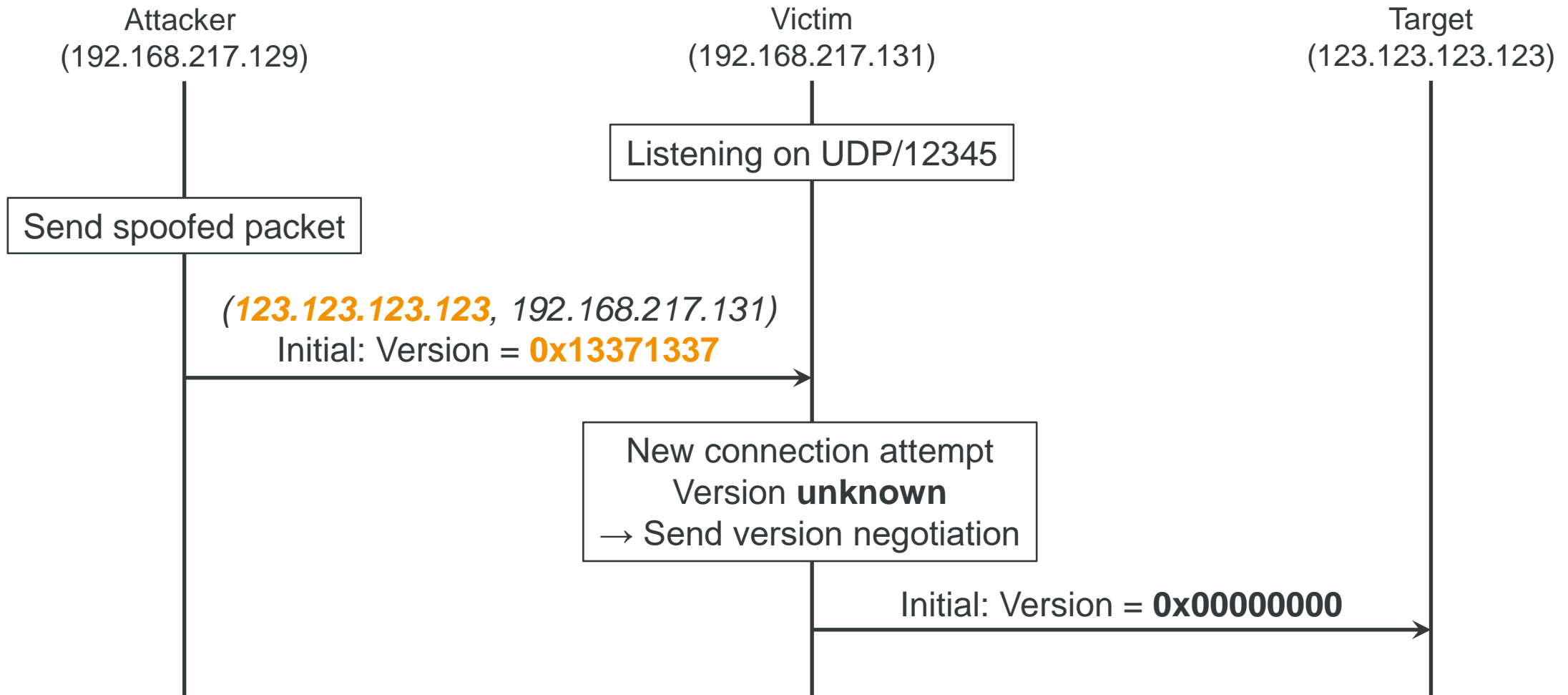
Connection Migration Request Forgery (CMRF)



Server Initial Request Forgery (SIRF)

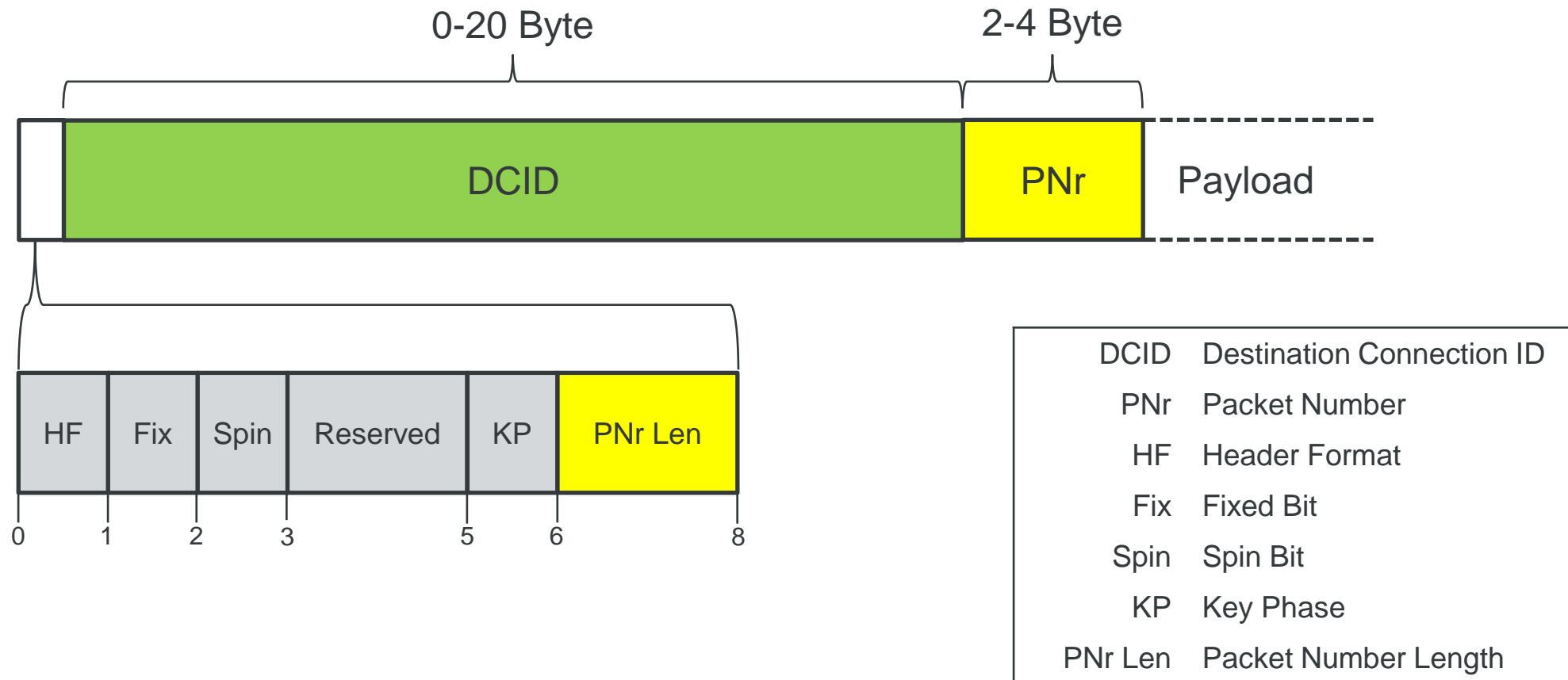


Version Negotiation Request Forgery (VNRf)



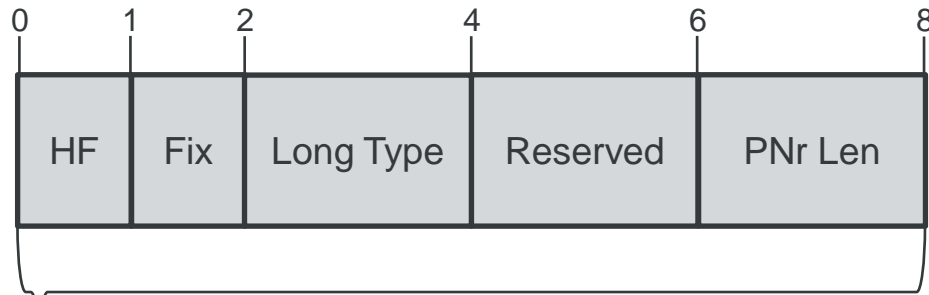
Protocol Impersonation

Short Header

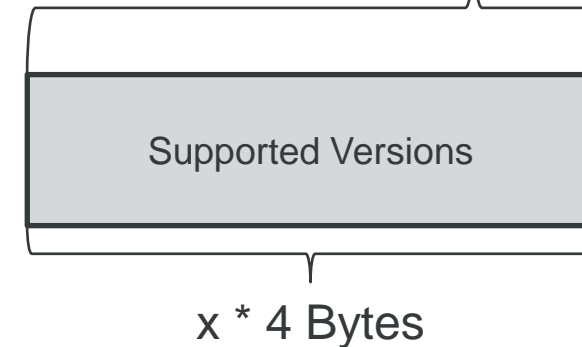
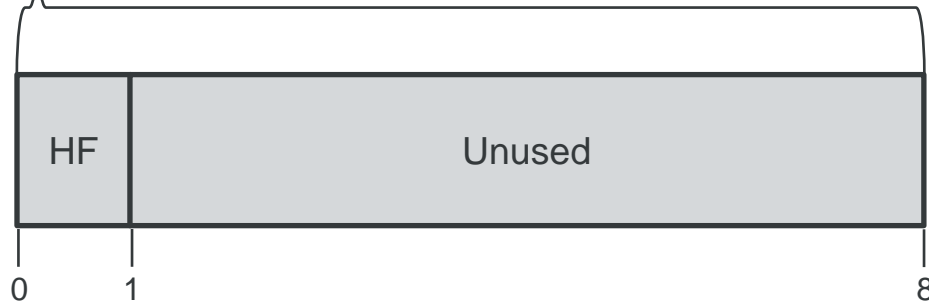
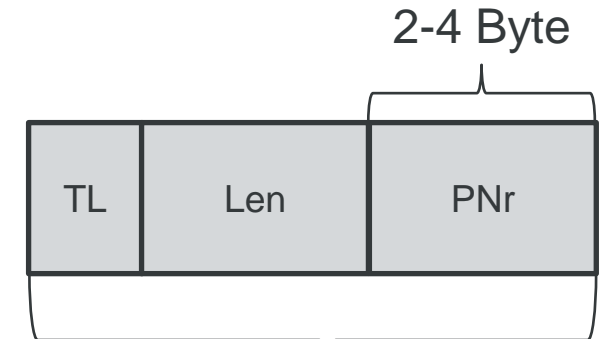


Long Header

Initial Packet

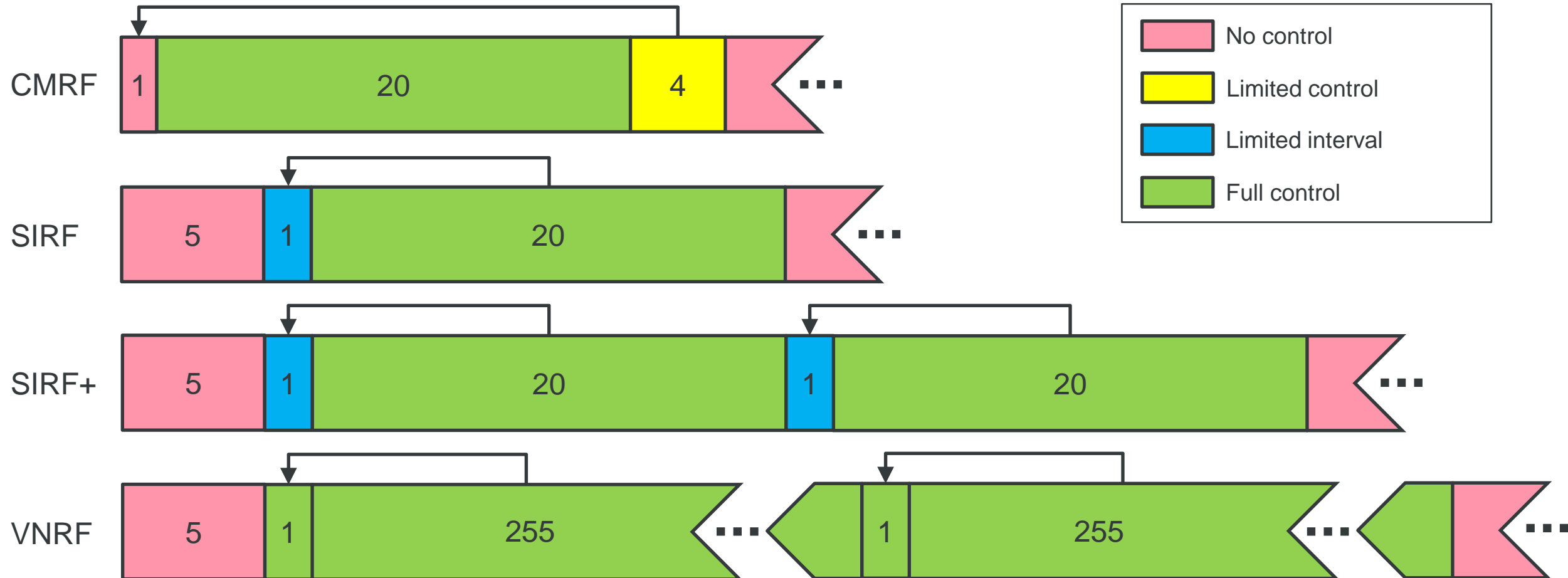


TL	Token Length
Len	Payload Length
DL	DCID Length
SL	SCID Length

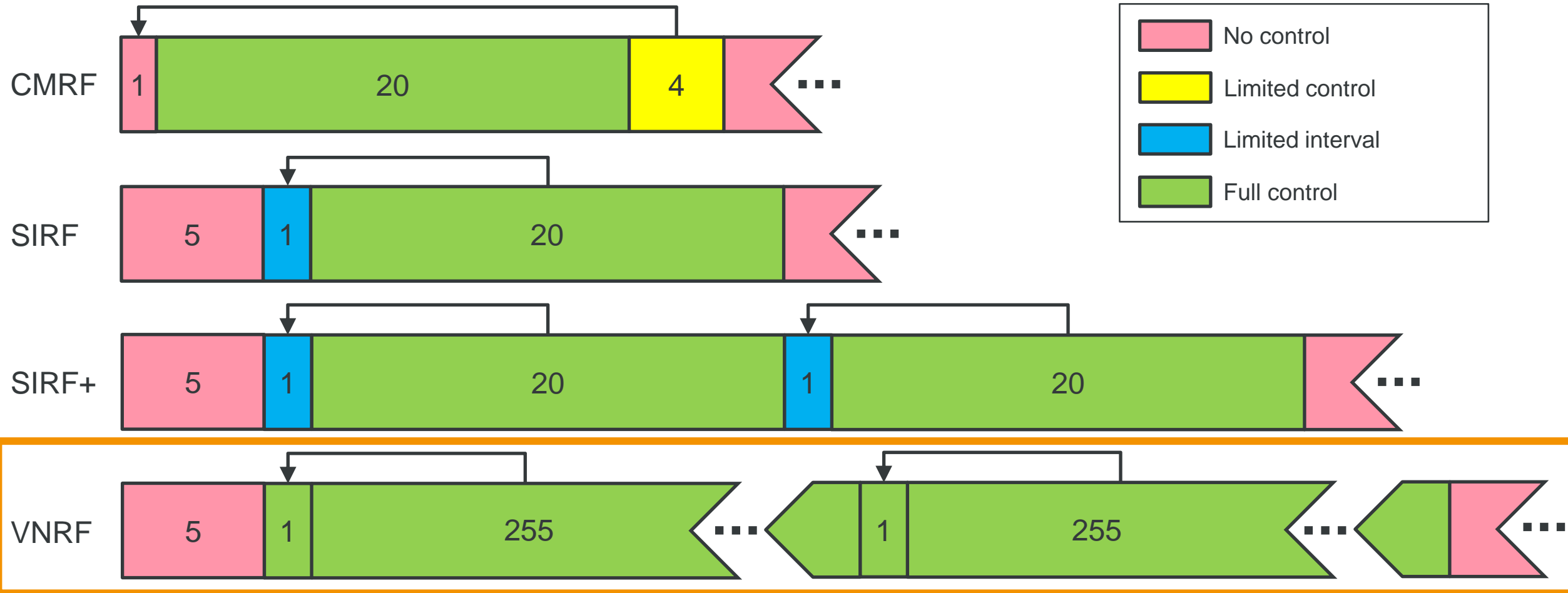


Version Negotiation Packet

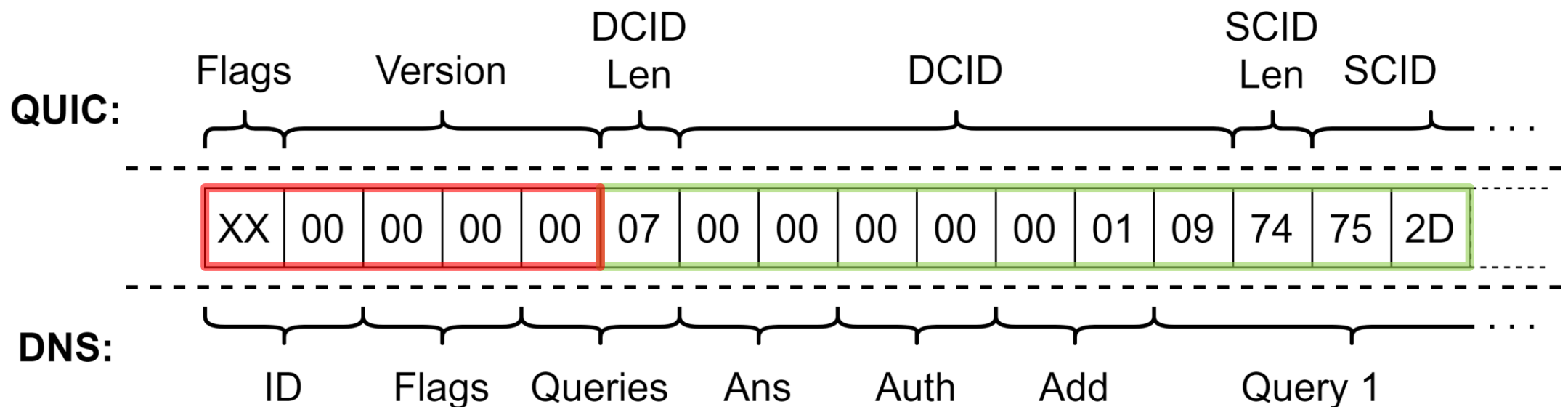
Controllable Bytes for Protocol Impersonation



Controllable Bytes for Protocol Impersonation



Impersonating DNS Requests with VNRF



Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info	No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	QUIC	13...	Initial, SCID=00000000000109	13	3.538438...	8.8.8.8	192.168.217.1...	DNS	13...	DNS Stateful operations (DSO) 0xc813[Malformed Packet]
14	3.538771...	192.168.217.1...	8.8.8.8	QUIC	200	Version Negotiation, DCID=00000000000109	14	3.538771...	192.168.217.1...	8.8.8.8	DNS	200	Standard query 0xc900 A tu-berlin.de A <Root> A <Root> A <Root> A
15	3.558935...	8.8.8.8	192.168.217.1...	QUIC	152	53 → 12345 Len=110[Malformed Packet]	15	3.558935...	8.8.8.8	192.168.217.1...	DNS	152	Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 172
Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0							Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0						
Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)							Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)						
Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8							Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8						
User Datagram Protocol, Src Port: 12345, Dst Port: 53							User Datagram Protocol, Src Port: 12345, Dst Port: 53						
QUIC IETF							Domain Name System (query)						
QUIC Connection information							Transaction ID: 0xc900						
[Packet Length: 158]							Flags: 0x0000 Standard query						
1... .. = Header Form: Long Header (1)							Questions: 7						
.100 1001 = Unused: 0x49							Answer RRs: 0						
Version: Version Negotiation (0x00000000)							Authority RRs: 0						
Destination Connection ID Length: 7							Additional RRs: 1						
Destination Connection ID: 00000000000109							Queries						
Source Connection ID Length: 116							tu-berlin.de: type A, class IN						
Source Connection ID: 752d6265726c696e02646500001000100000100010000010001000001000100000100010000010001...							<Root>: type A, class IN						
Supported Version: v2-draft-01 (0x709a50c4)							<Root>: type A, class IN						
Supported Version: 1 (0x00000001)							<Root>: type A, class IN						
Supported Version: draft-32 (0xff000020)							<Root>: type A, class IN						
Supported Version: draft-31 (0xff00001f)							<Root>: type A, class IN						
Supported Version: draft-30 (0xff00001e)							<Root>: type A, class IN						
Supported Version: draft-29 (0xff00001d)							<Root>: type A, class IN						
Supported Version: Unknown (0x4a0ababa) (GREASE)							Additional records						
							<Root>: type Unused, class Unknown						
							[Response In: 15]						
Frame (frame), 200 bytes							Frame (frame), 200 bytes						
Packets: 31 · Displayed: 3 (9.7%)							Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%)						
Profile: Default							Profile: Default						
Frame 15: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface ens33, id 0							Frame 15: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface ens33, id 0						
Ethernet II, Src: VMware_f6:95:1c (00:50:56:f6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92)							Ethernet II, Src: VMware_f6:95:1c (00:50:56:f6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92)						
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.217.131							Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.217.131						
User Datagram Protocol, Src Port: 53, Dst Port: 12345							User Datagram Protocol, Src Port: 53, Dst Port: 12345						
QUIC IETF							Domain Name System (response)						
QUIC Connection information							Transaction ID: 0xc900						
[Malformed Packet: QUIC]							Flags: 0x8080 Standard query response, No error						
[Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]							Questions: 1						
[Malformed Packet (Exception occurred)]							Answer RRs: 5						
[Severity level: Error]							Authority RRs: 0						
[Group: Malformed]							Additional RRs: 0						
							Queries						
							Answers						
							tu-berlin.de: type A, class IN, addr 10.150.7.69						
							tu-berlin.de: type A, class IN, addr 172.31.25.70						
							tu-berlin.de: type A, class IN, addr 10.150.7.68						
							tu-berlin.de: type A, class IN, addr 10.150.7.67						
							tu-berlin.de: type A, class IN, addr 10.150.7.70						
							[Request In: 14]						
							[Time: 0.020163079 seconds]						

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	QUIC	13...	Initial, SCID=000000000000109
14	3.538771...	192.168.217.1...	8.8.8.8	QUIC	200	Version Negotiation, DCID=000000000000109
15	3.558935...	8.8.8.8	192.168.217.1...	QUIC	152	53 → 12345 Len=110[Malformed Packet]

▶ Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0

- ▶ Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
- ▶ Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
- ▶ User Datagram Protocol, Src Port: 12345, Dst Port: 53
- ▶ QUIC IETF
 - ▶ QUIC Connection information
 - [Packet Length: 158]
 - 1... = Header Form: Long Header (1)
 - .100 1001 = Unused: 0x49
 - Version: Version Negotiation (0x00000000)
 - Destination Connection ID Length: 7
 - Destination Connection ID: 000000000000109
 - Source Connection ID Length: 116
 - Source Connection ID: 752d6265726c696e026465000001000100000100010000010001000001000100000100010000010001...
 - 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 (0x4a0ababa) (GREASE)

Frame (frame), 200 bytes Packets: 31 · Displayed: 3 (9.7%) Profile: Default
[Time: 0.020163079 seconds]

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	QUIC	13...	Initial, SCID=000000000000109
14	3.538771...	192.168.217.1...	8.8.8.8	QUIC	200	Version Negotiation, DCID=000000000000109
15	3.558935...	8.8.8.8	192.168.217.1...	QUIC	152	53 → 12345 Len=110 [Malformed Packet]

▶ Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0

- ▶ Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
- ▶ Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
- ▶ User Datagram Protocol, Src Port: 12345, Dst Port: 53

▼ QUIC IETF

- ▶ QUIC Connection information
 - [Packet Length: 158]
 - 1... = Header Form: Long Header (1)
 - .100 1001 = Unused: 0x49
 - Version: Version Negotiation (0x00000000)
 - Destination Connection ID Length: 7
 - Destination Connection ID: 000000000000109
 - Source Connection ID Length: 116
 - Source Connection ID: 752d6265726c696e026465000001000100000100010000010001000001000100000100010000010001...
 - 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 (0x4a0ababa) (GREASE)

Frame (frame), 200 bytes

Packets: 31 · Displayed: 3 (9.7%) Profile: Default

[Time: 0.020163079 seconds]

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	QUIC	13...	Initial, SCID=000000000000109
14	3.538771...	192.168.217.1...	8.8.8.8	QUIC	200	Version Negotiation, DCID=000000000000109
15	3.558935...	8.8.8.8	192.168.217.1...	QUIC	152	53 → 12345 Len=110[Malformed Packet]

▶ Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0

- ▶ Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
- ▶ Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
- ▶ User Datagram Protocol, Src Port: 12345, Dst Port: 53
- ▶ QUIC IETF
 - ▶ QUIC Connection information
[Packet Length: 158]
1... = Header Form: Long Header (1)
.100 1001 = Unused: 0x49
Version: Version Negotiation (0x00000000)
Destination Connection ID Length: 7
Destination Connection ID: 000000000000109
Source Connection ID Length: 116
Source Connection ID: 752d6265726c696e026465000001000100000100010000010001000001000100000100010000010001...
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 (0x4a0ababa) (GREASE)

Frame (frame), 200 bytes Packets: 31 · Displayed: 3 (9.7%) Profile: Default
[Time: 0.020163079 seconds]

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	QUIC	13...	Initial, SCID=000000000000109
14	3.538771...	192.168.217.1...	8.8.8.8	QUIC	200	Version Negotiation, DCID=000000000000109
15	3.558935...	8.8.8.8	192.168.217.1...	QUIC	152	53 → 12345 Len=110[Malformed Packet]

▶ Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0

- ▶ Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
- ▶ Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
- ▶ User Datagram Protocol, Src Port: 12345, Dst Port: 53

▼ QUIC IETF

- ▶ QUIC Connection information
 - [Packet Length: 158]
 - 1... = Header Form: Long Header (1)
 - .100 1001 = Unused: 0x49
 - Version: Version Negotiation (0x00000000)
 - Destination Connection ID Length: 7**
 - Destination Connection ID: 000000000000109**
 - Source Connection ID Length: 116**
 - Source Connection ID: 752d6265726c696e026465000001000100000100010000010001000001000100000100010000010001...**
 - 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 (0x4a0ababa) (GREASE)

Frame (frame), 200 bytes Packets: 31 · Displayed: 3 (9.7%) Profile: Default
[Time: 0.020163079 seconds]

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	DNS	13...	DNS Stateful operations (DS0) 0xc813[Malformed Packet]
14	3.538771...	192.168.217.1...	8.8.8.8	DNS	200	Standard query 0xc900 A tu-berlin.de A <Root> A <Root> A <Root> A
15	3.558935...	8.8.8.8	192.168.217.1...	DNS	152	Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 172.

Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0

- Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
- Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 12345, Dst Port: 53
- Domain Name System (query)**
 - Transaction ID: 0xc900
 - Flags: 0x0000 Standard query
 - Questions: 7
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries**
 - tu-berlin.de: 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
 - <Root>: type A, class IN
 - Additional records**
 - <Root>: type Unused, class Unknown

[\[Response In: 15\]](#)

Frame (frame), 200 bytes

Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default

[Time: 0.020163079 seconds]

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	DNS	13...	DNS Stateful operations (DSO) 0xc813[Malformed Packet]
14	3.538771...	192.168.217.1...	8.8.8.8	DNS	200	Standard query 0xc900 A tu-berlin.de A <Root> A <Root> A <Root> A
15	3.558935...	8.8.8.8	192.168.217.1...	DNS	152	Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 172

Domain Name System (query)

- Transaction ID: 0xc900
- Flags: 0x0000 Standard query
- Questions: 7
- Answer RRs: 0
- Authority RRs: 0
- Additional RRs: 1

Queries

- tu-berlin.de: 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
- <Root>: type A, class IN

Additional records

- <Root>: type Unused, class Unknown

[\[Response In: 15\]](#)

Malformed Packet: QUIC

[Expert Info (Error/Malformed) [Malformed Packet (Exception) [Severity level: Error] [Group: Malformed]

Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default

[Time: 0.020163079 seconds]

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	DNS	13...	DNS Stateful operations (DSO) 0xc813[Malformed Packet]
14	3.538771...	192.168.217.1...	8.8.8.8	DNS	200	Standard query 0xc900 A tu-berlin.de A <Root> A <Root> A <Root> A
15	3.558935...	8.8.8.8	192.168.217.1...	DNS	152	Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 172.

Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0

- Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
- Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 12345, Dst Port: 53
- Domain Name System (query)**
 - Transaction ID: 0xc900
 - Flags: 0x0000 Standard query
 - Questions: 7
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 1
- Queries
 - tu-berlin.de: 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
 - <Root>: type A, class IN
- Additional records**
 - <Root>: type Unused, class Unknown

[\[Response In: 15\]](#)

Frame 15: 152 bytes on wire (1216 bits), 152 bytes captured (1216 bits) on interface ens33, id 1

- Ethernet II, Src: VMware_f6:95:1c (00:50:56:f6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92)
- Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.217.131
- User Datagram Protocol, Src Port: 53, Dst Port: 12345
- QUIC IETF
 - QUIC Connection information [Packet Length: 158]
 - 1... .. = Header Form: Long
 - .100 1001 = Unused: 0x49
 - Version: Version Negotiation
 - Destination Connection ID Length: 0
 - Destination Connection ID: 00000000
 - Source Connection ID Length: 0
 - Source Connection ID: 752d6268
 - Supported Version: v2-draft-00
 - Supported Version: 1 (0x000000)
 - Supported Version: draft-32 (0x000000)
 - Supported Version: draft-31 (0x000000)
 - Supported Version: draft-30 (0x000000)
 - Supported Version: draft-29 (0x000000)
 - Supported Version: Unknown (0x000000)
- [Malformed Packet: QUIC]**
 - [Expert Info (Error/Malformed)]: [Malformed Packet (Exception)] [Severity level: Error] [Group: Malformed]

Impersonating DNS Requests with VNRF (cont'd)

No.	Time	Source	Destination	Protocol	Length	Info
13	3.538438...	8.8.8.8	192.168.217.1...	DNS	13...	DNS Stateful operations (DSO) 0xc813[Malformed Packet]
14	3.538771...	192.168.217.1...	8.8.8.8	DNS	200	Standard query 0xc900 A tu-berlin.de A <Root> A <Root> A <Root> A
15	3.558935...	8.8.8.8	192.168.217.1...	DNS	152	Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 172.

Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0

- Ethernet II, Src: VMware_5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware_f6:95:1c (00:50:56:f6:95:1c)
- Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8
- User Datagram Protocol, Src Port: 12345, Dst Port: 53
- Domain Name System (query)
 - Transaction ID: 0xc900
 - Flags: 0x0000 Standard query
 - Questions: 7
 - Answer RRs: 0
 - Authority RRs: 0
 - Additional RRs: 1
 - Queries
 - tu-berlin.de: 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
 - <Root>: type A, class IN
 - Additional records
 - <Root>: type Unused, class Unknown

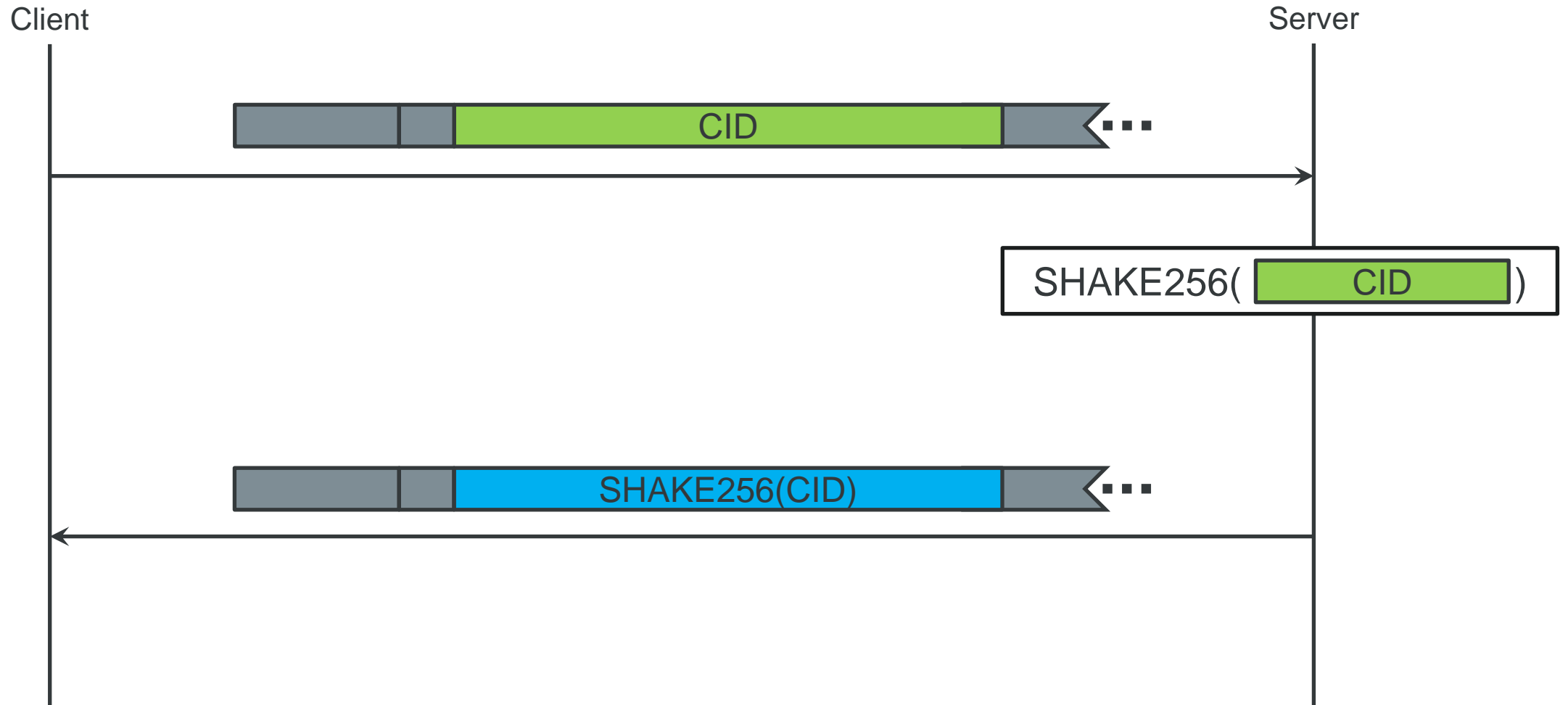
[Response In: 15]

Frame (frame), 200 bytes

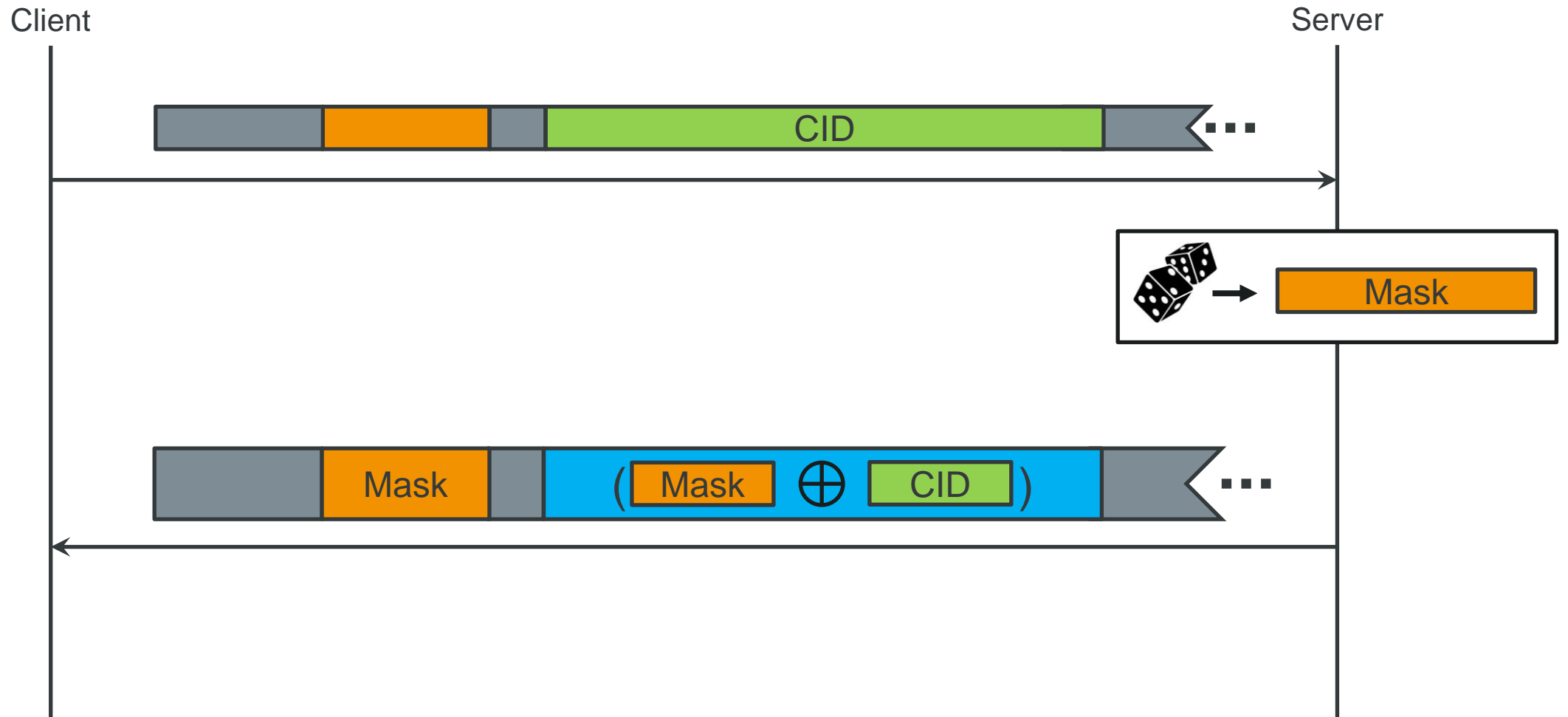
Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default

[Time: 0.020163079 seconds]

Mitigation - Hashing



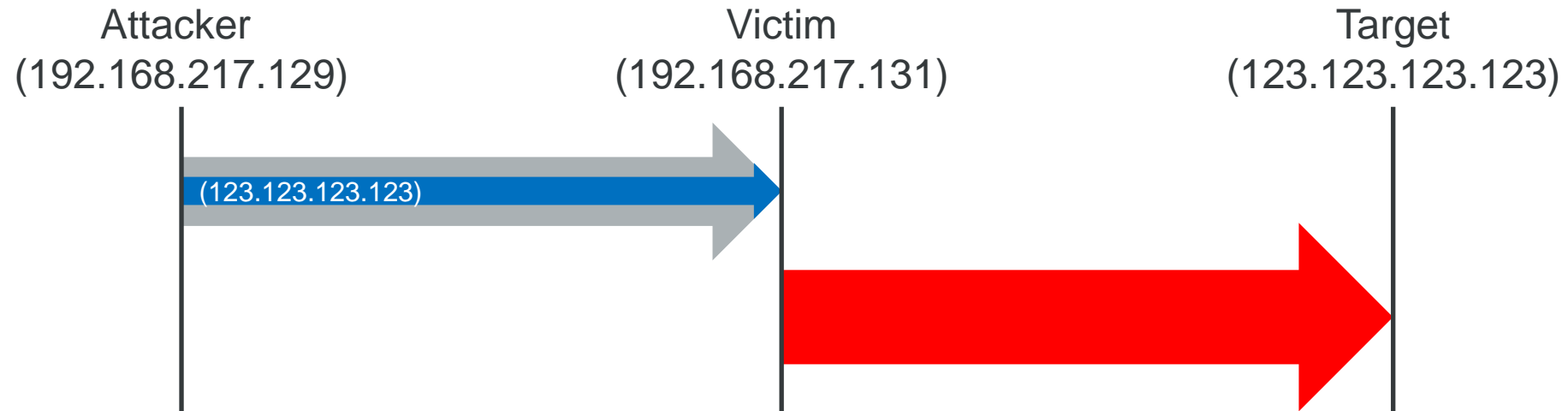
Mitigation - Masking



Traffic Amplification

Path amplification VS Bandwidth Amplification

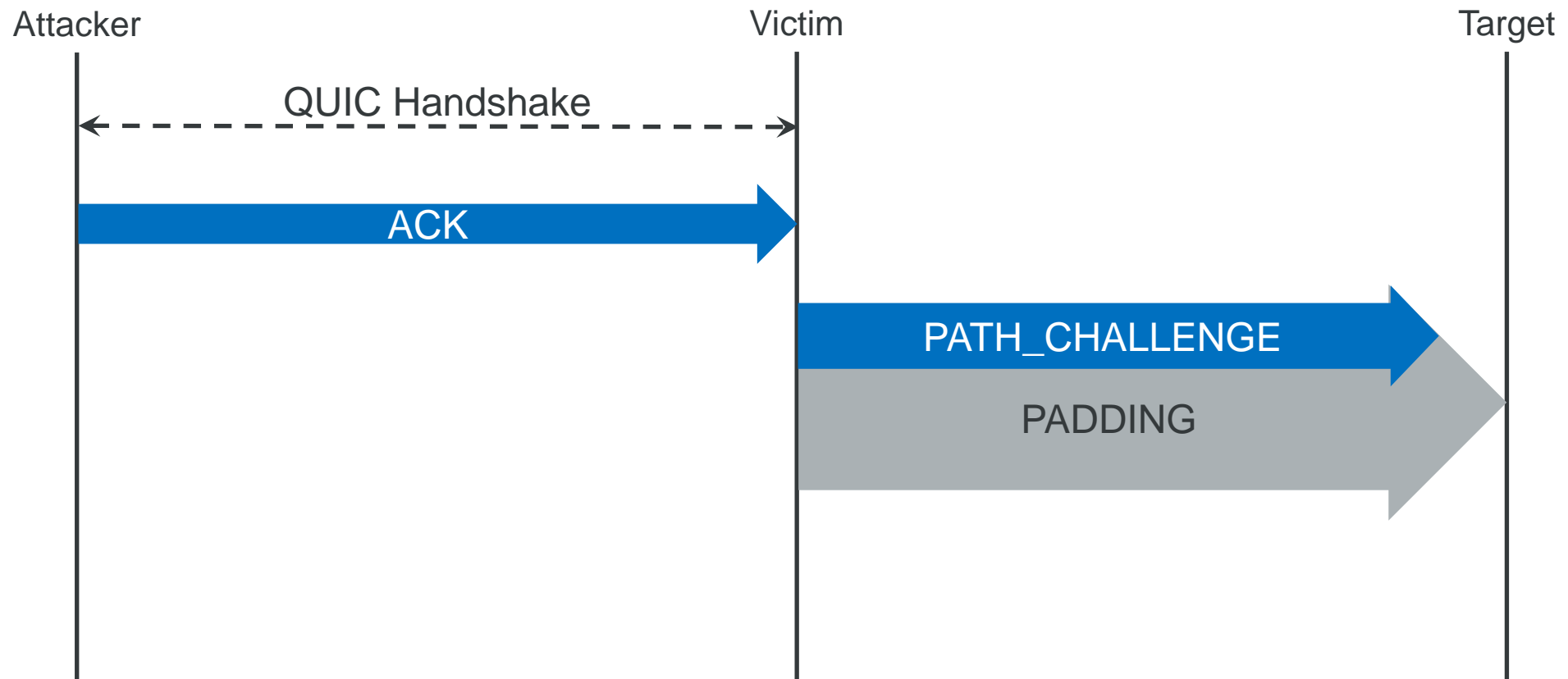
$$PAF = \frac{\# \text{ Bytes from victim to target}}{\# \text{ Bytes from attacker to victim with spoofed address}}$$



$$BAF = \frac{\# \text{ Bytes from victim to target}}{\# \text{ Bytes from attacker to victim}}$$

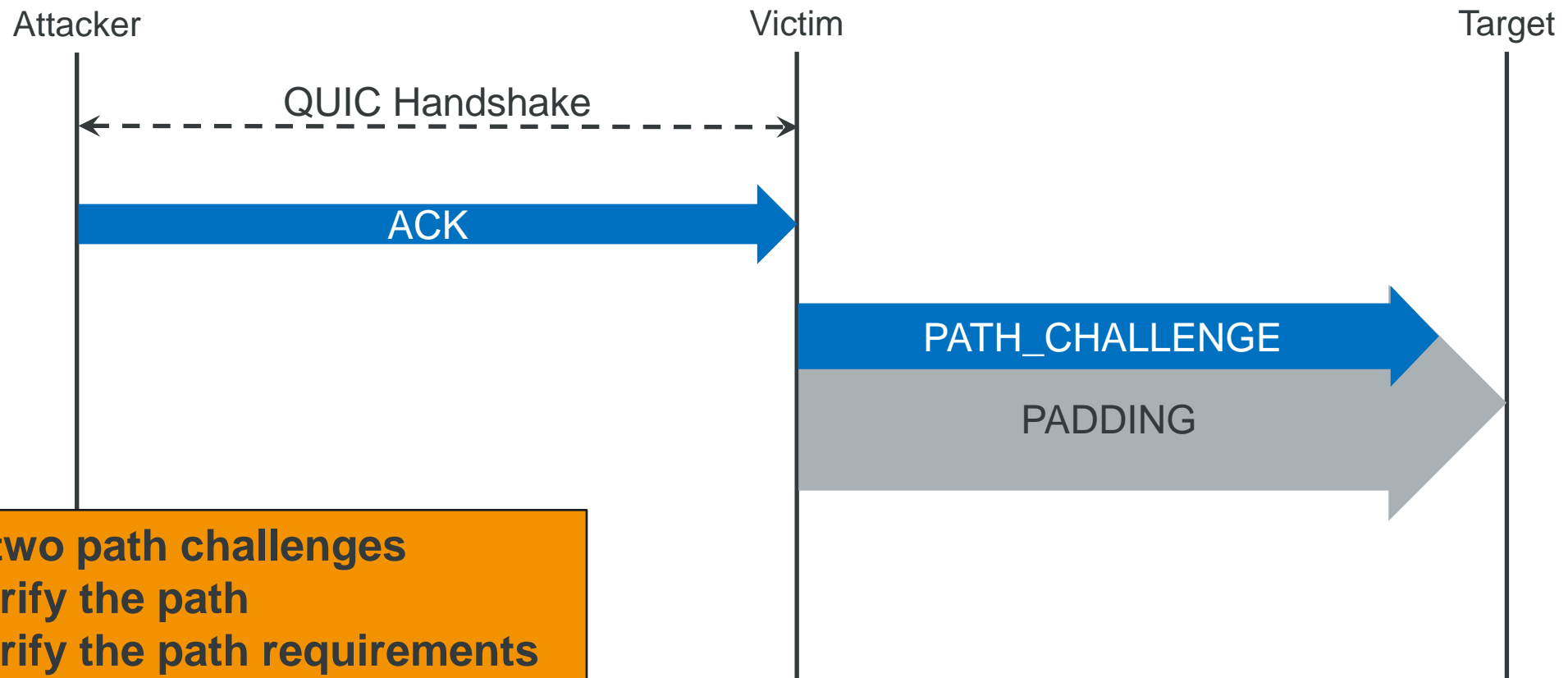
Amplification Pitfalls – Minimum Path Requirements

“[...] not send more than three times the amount of data received on any unvalidated path.”



Amplification Pitfalls – Minimum Path Requirements

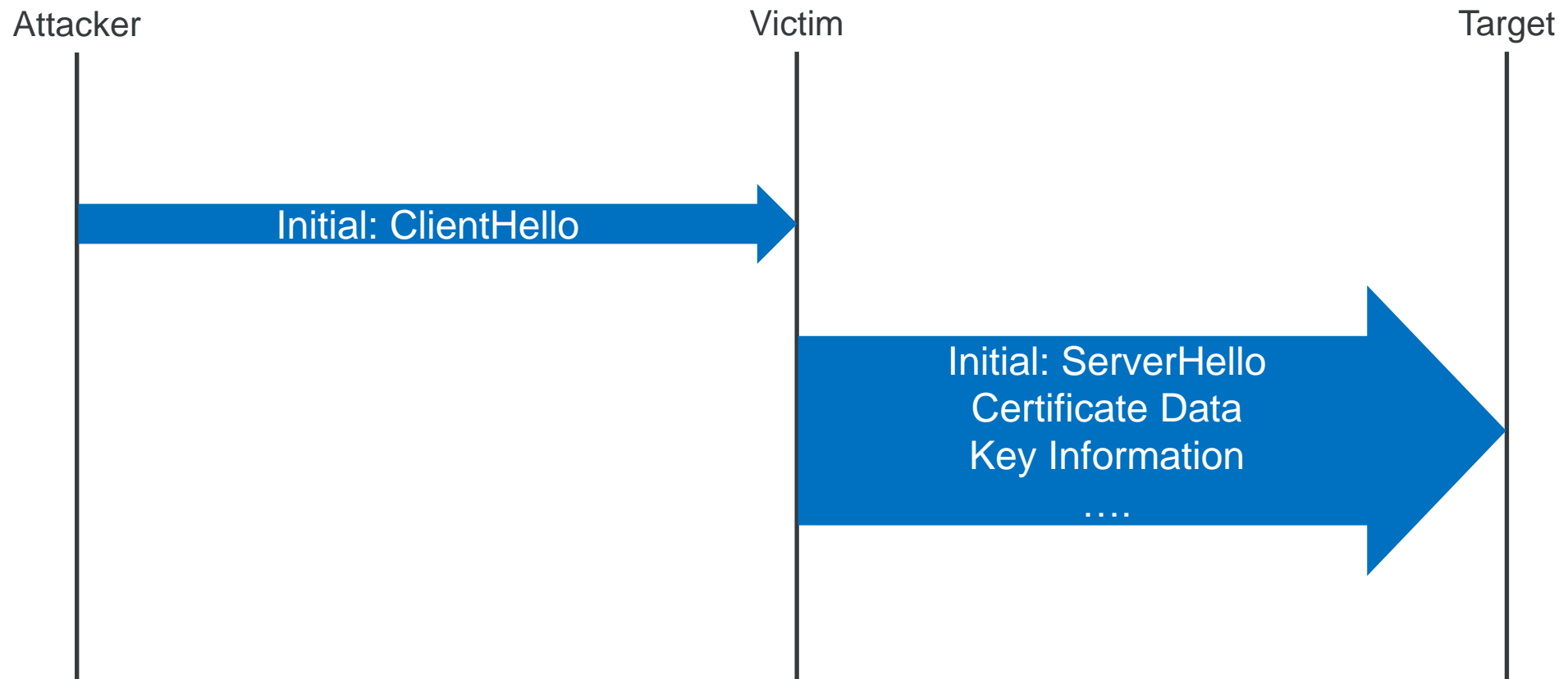
“[...] not send more than three times the amount of data received on any unvalidated path.”



- Send two path challenges**
1. Verify the path
 2. Verify the path requirements

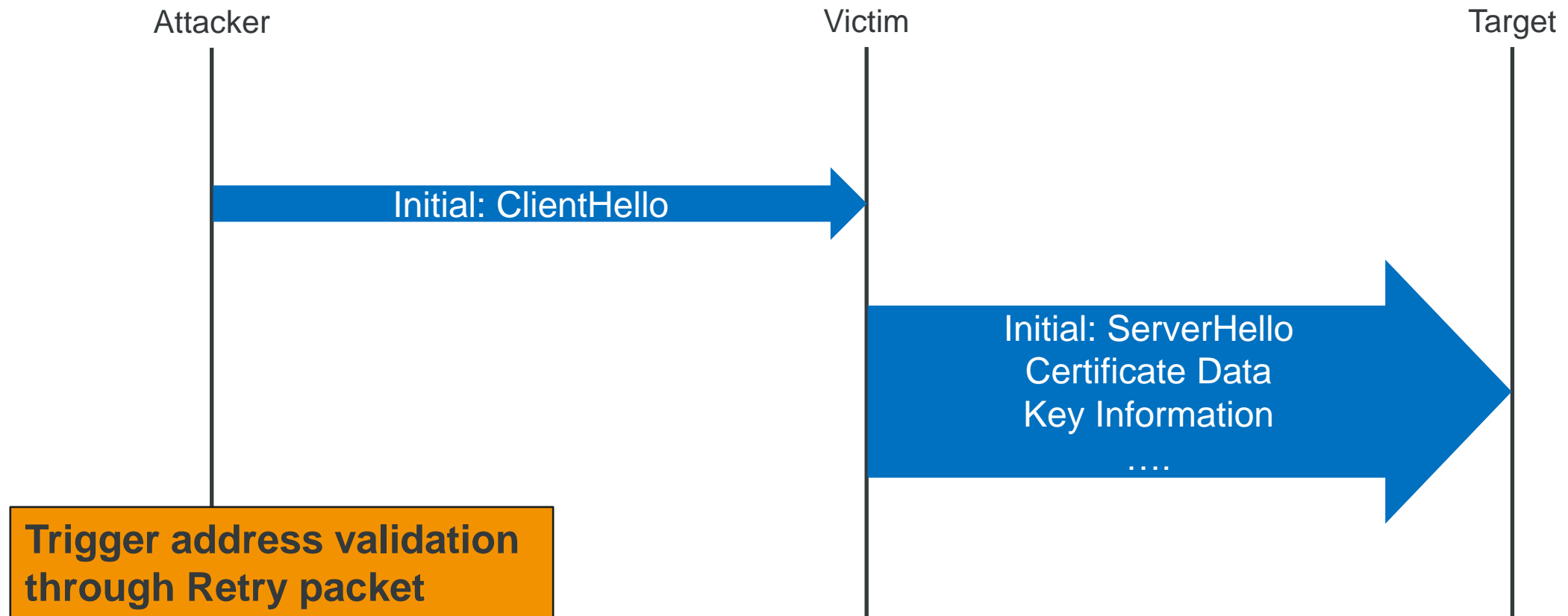
Amplification Pitfalls – Unbalanced Handshake Sizes

“[...] not send more than three times the amount of data received on any unvalidated path.”



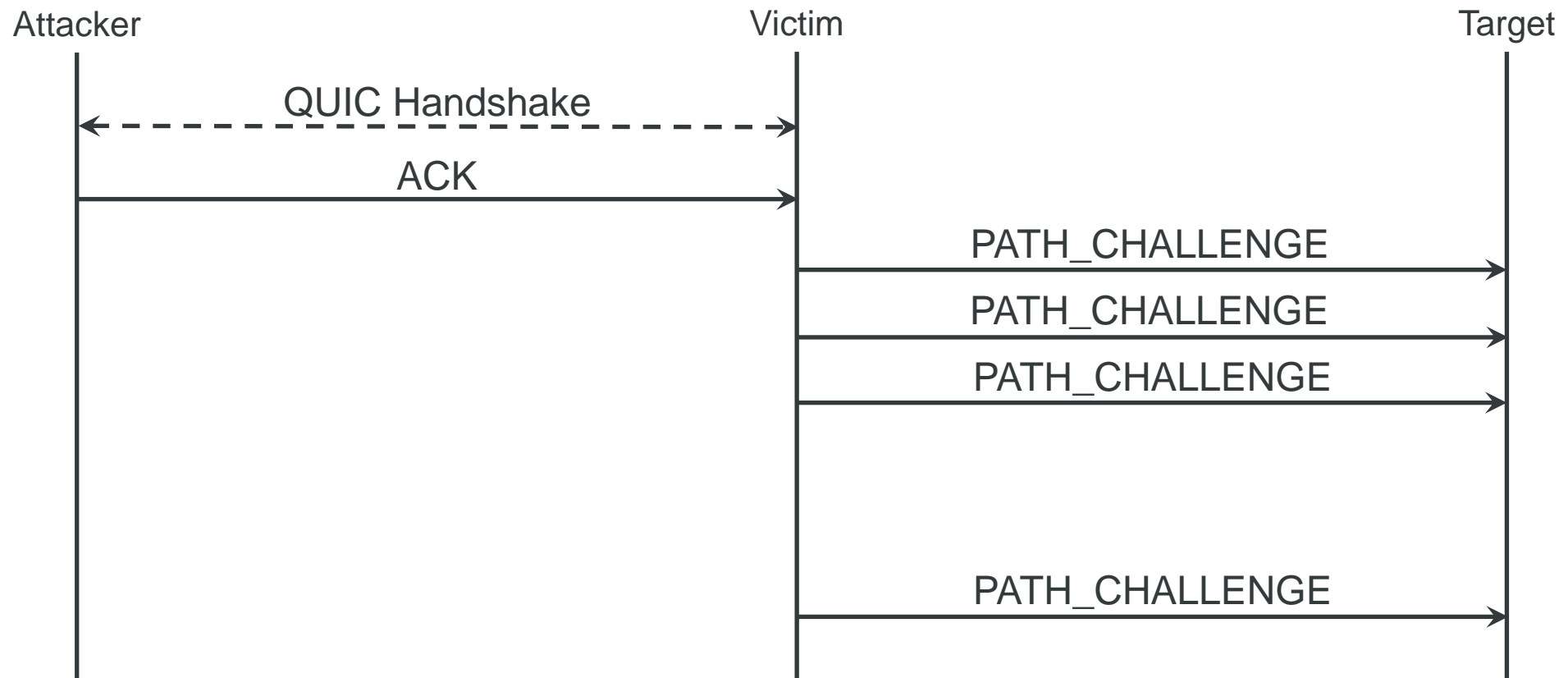
Amplification Pitfalls – Unbalanced Handshake Sizes

“[...] not send more than three times the amount of data received on any unvalidated path.”



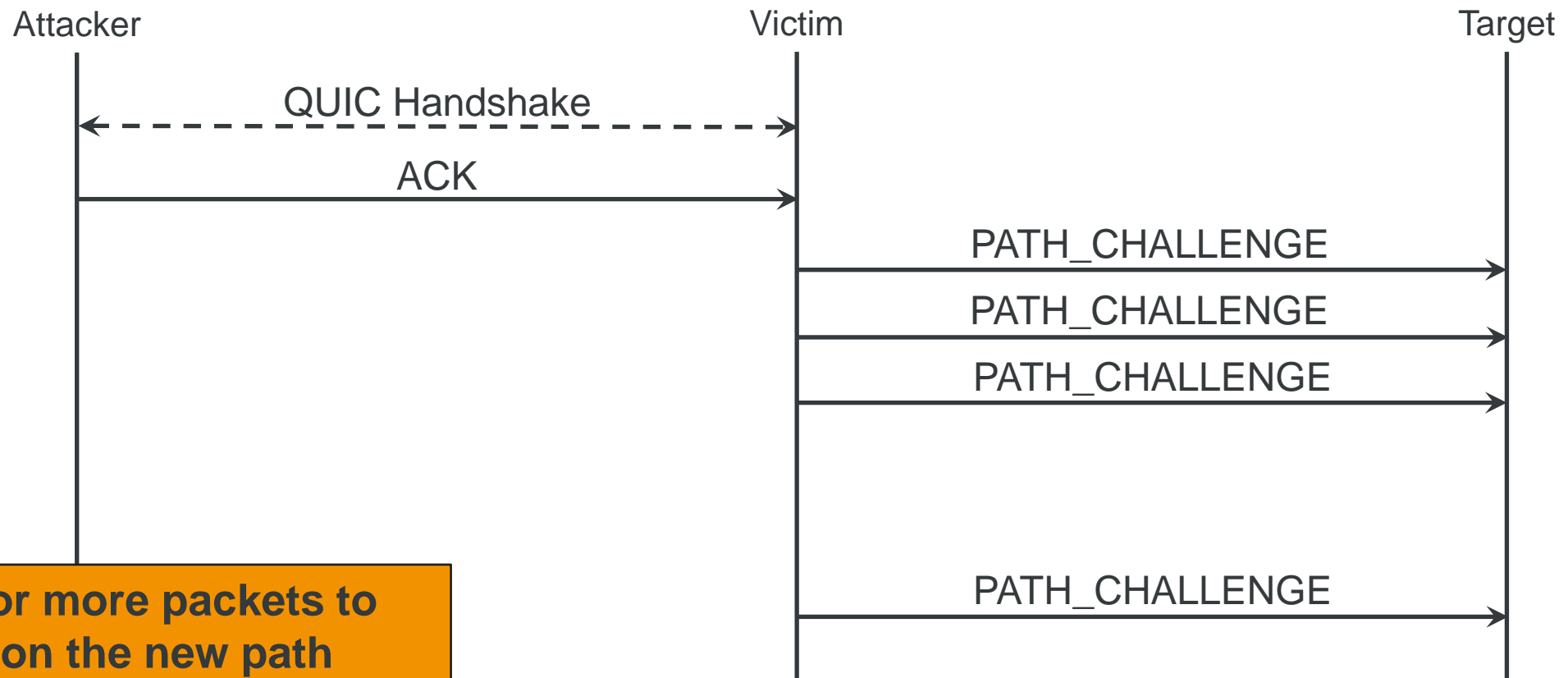
Amplification Pitfalls – Reliability for Connection Migration

“[...] not send more than three times the amount of data received on any unvalidated path.”



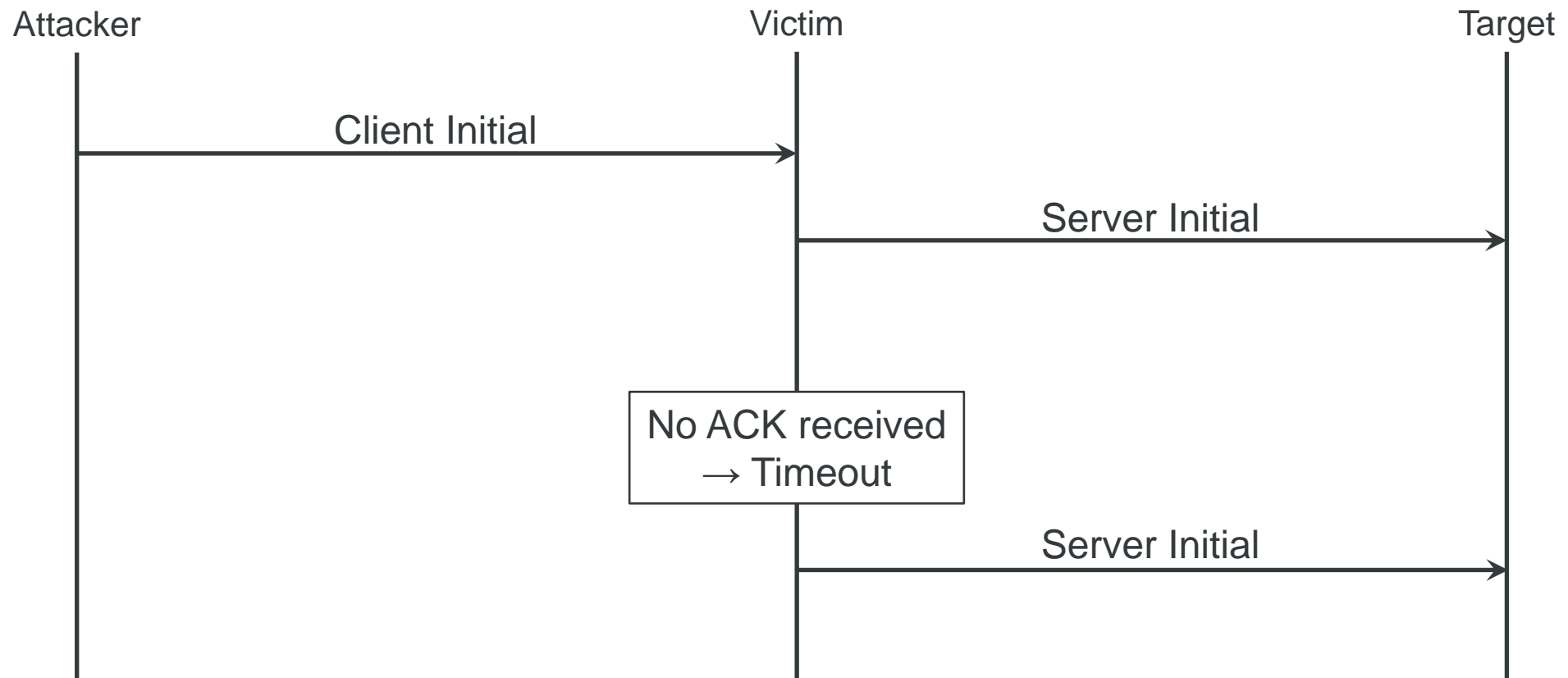
Amplification Pitfalls – Reliability for Connection Migration

“[...] not send more than three times the amount of data received on any unvalidated path.”



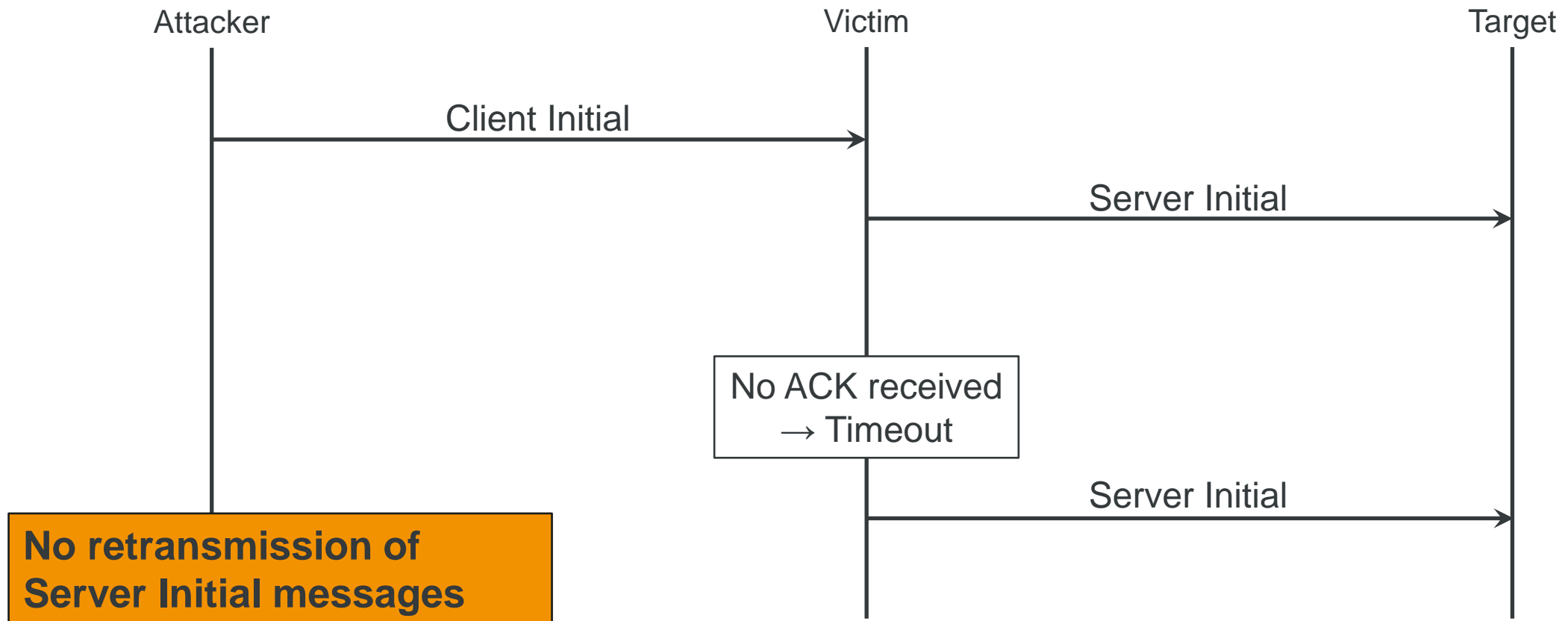
Amplification Pitfalls – Reliability During Handshake

“[...] not send more than three times the amount of data received on any unvalidated path.”



Amplification Pitfalls – Reliability During Handshake

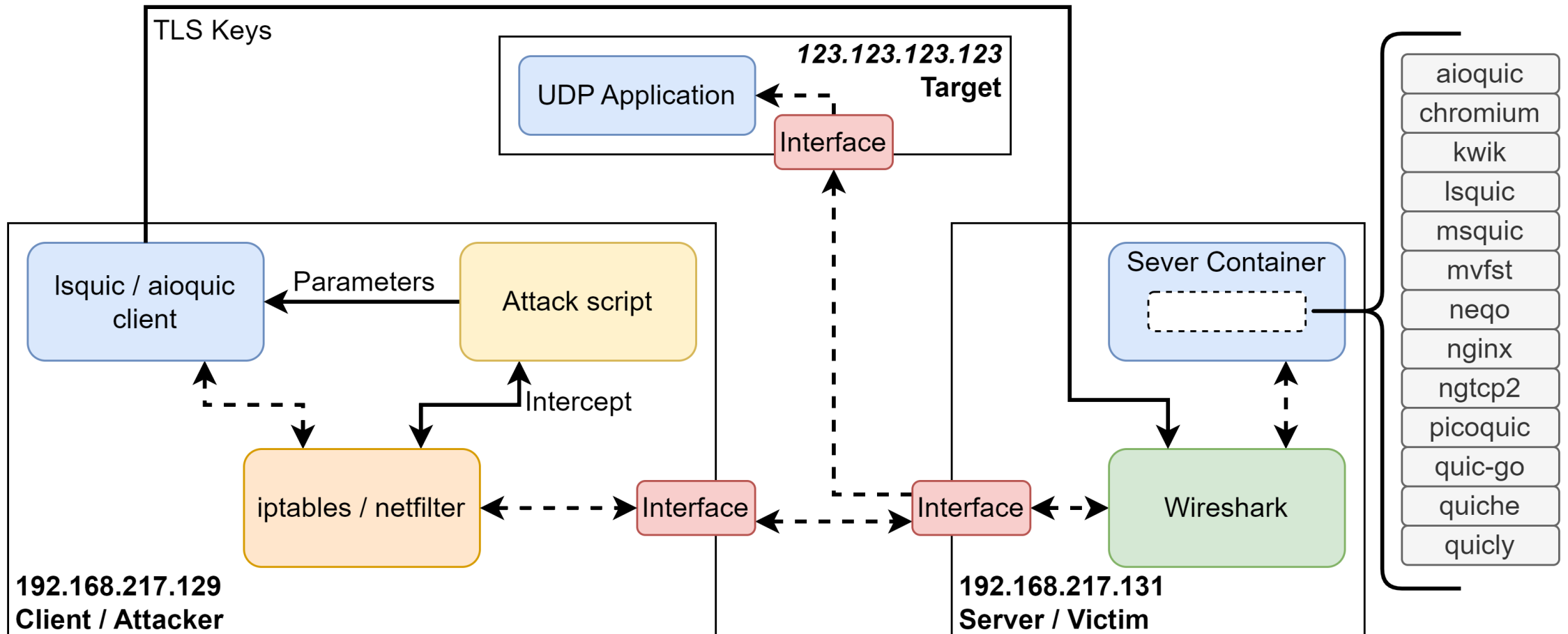
“[...] not send more than three times the amount of data received on any unvalidated path.”



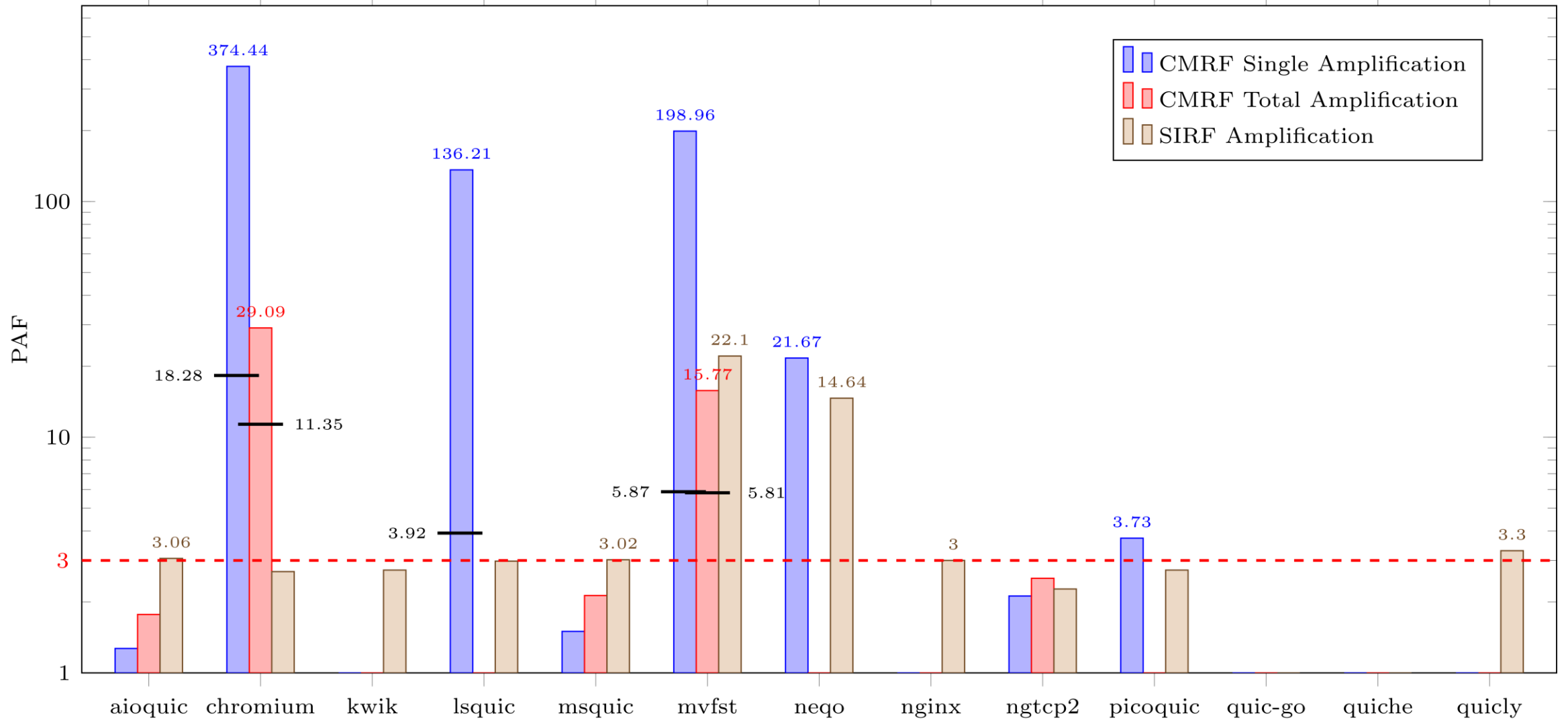
RTFM

Evaluation

Evaluation Setup



Amplification Results



Conclusion

Conclusion

- ***Greater attack surface and room for errors.***
- ***“Old” vulnerabilities become more relevant again.***
- ***Poor tooling support.***
 - Offensive and Defensive.
- ***We see a significant discrepancy between specification and implementations.***
 - PAFs up to 374.44 for CMRF and 22.1 for SIRF
- ***Novel attack vectors like protocol impersonation.***
 - Currently no built-in protection mechanism.

Thanks!



Blogpost with additional technical details:

<https://r.sec-consult.com/quic>



NDSS Paper about request forgery in QUIC:

<https://www.ndss-symposium.org/ndss-paper/quicforge-client-side-request-forgery-in-quic/>



Paper about firewall issues in QUIC:

<https://arxiv.org/abs/2107.05939>

Thanks for listening!