# 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
- Deputy Lead for Cloud Security

#### y.gbur@sec-consult.com

@yukonsec
 @yukonsec@infosec.exchange



# QUIC(K) Background

APACHE GOOGLE CLOUDFLARE moz://a Microsoft 💪 🎸 LITESPEED

• RFC 8999

• RFC 9000

RFC 9001

• RFC 9002

• RFC 9115

(HTTP/3)



ent			Serv
Initial[	0] :	CRYPTO[CH]	
Initial	0] :	CRYPTO[SH]	
Handshake	0] :	CRYPTO[EE,CERT,CV,FIN]	
1-RTT[	0] :	STREAM[1,"…"]	
Initial[	1] :	ACK[0]	
Handshake[	0] :	CRYPTO[FIN], ACK[0]	
1-RTT[	. [0]	STREAM[0,""], ACK[0]	
Handshake[	[1] :	ACK[0]	
1-RTT[	[1] :	DONE, STREAM[3,"…"], ACK[0]	

ent			Serv
Initial[0]	:	CRYPTO[CH]	
Initial[0]	:	CRYPTO[SH]	
Handshake[0]	:	CRYPTO[EE,CERT,CV,FIN]	
1-RTT[0]	:	STREAM[1,""]	
Initial[1]	:	ACK[0]	
Handshake[0]	:	CRYPTO[FIN], ACK[0]	
1-RTT[0]	:	STREAM[0,""], ACK[0]	
Handshake[1]	:	ACK[0]	
1-RTT[1]	:	DONE, STREAM[3,"…"], ACK[0]	

	Initial[0]	:	CRYPTO[CH]	
				<i>F</i>
	Initial[0]	:	CRYPTO[SH]	
	Handshake[0]	:	CRYPTO[EE,CERT,CV,FIN]	
,	1-RTT[0]	:	STREAM[1,""]	
~				
	Initial[1]	:	ACK[0]	
	Handshake[0]	:	CRYPTO[FIN], ACK[0]	
	1-RTT[0]	:	STREAM[0,"…"], ACK[0]	$\longrightarrow$
	Llondoboko[4]			
	Handshake[1]	•	ACK[U]	
·	1-RTT[1]	:	DONE, STREAM[3,""], ACK[0]	



# Challenges with Securing QUIC

#### Pro

• Easier / faster updates of the "transport" layer.

#### 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**



#### **Stateful Tracking**





#### **Routing / Optimization**

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

#### **Application Layer Security**

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

#### **General Tooling Support**

ΤοοΙ	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	×	quicat by pas2k
		<b>Disclaimer</b> : No guarantees for an 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

#### **Controllable Bytes for Protocol Impersonation**



#### **Controllable Bytes for Protocol Impersonation**





#### Impersonating DNS Requests with VNRF (cont'd)

No. Time	Source D	Destination Protoco	ol Length Info		No	o. Time	Source	Destination Proto	col Length Info
	8.8.8.8	192.168.217.1 QUIC	13 Initial, SCID=0000	5000000109		- 13 3.538438.	8.8.8.8	192.168.217.1 DNS	13DNS Stateful operations (DSO) 0xc813[Malformed Packet]
14 3.538771	192.168.217.1 8	8.8.8.8 QUIC	200 Version Negotiatio	on, DCID=0000000000109		→ 14 3.538771.	. 192.168.217.	18.8.8.8 DNS	200 Standard query 0xc900 A tu-berlin.de A <root> A <root> A <root></root></root></root>
- 15 3.558935	8.8.8.8	192.168.217.1 QUIC	152 53 → 12345 Len=110	o[Malformed Packet]	a4 	- 15 3.558935.	8.8.8.8	192.168.217.1 DNS	5 152 Standard query response 0xc900 A tu-berlin.de A 10.150.7.69 A 17
Frame 14: 200	) bytes on wire (	(1600 bits), 200 by	tes captured (1600 bits	) on interface ens33, id 0	•	Frame 14: 20	0 bytes on wir	re (1600 bits), 200 b	ytes captured (1600 bits) on interface ens33, id 0
Ethernet II,	Src: VMware_5e:6	6a:92 (00:0c:29:5e:	6a:92), Dst: VMware_f6:	95:1c (00:50:56:f6:95:1c)	Þ	Ethernet II,	Src: VMware_5	5e:6a:92 (00:0c:29:5e	:6a:92),
Internet Prot	cocol Version 4,	Src: 192.168.217.1	31, Dst: 8.8.8.8		•	Internet Pro	tocol Version	4, Src: 192.168.217.	131, Dst: 8.8.8.8
User Datagram	n Protocol, Src F	Port: 12345, Dst Po	rt: 53		+	User Datagra	m Protocol, Sr	rc Port: 12345, Dst P	ort: 53
- QUIC IETF					-	Domain Name	System (query)	)	
> QUIC Connect	tion informatior	n				Transactio	n ID: 0xc900		
[Packet Ler	ngth: 158]					Flags: 0x0	000 Standard c	query	
1 =	Header Form: Lo	ong Header (1)				Questions:	7		
.100 1001 =	Unused: 0x49					Answer RRs	: 0		
Version: Ve	ersion Negotiatio	on (0x0000000)				Authority	RRs: 0		
Destinatior	n Connection ID L	Length: 7				Additional	RRs: 1		
Destinatior	Connection ID:	00000000000109				- Queries			
Source Conr	nection ID Length	h: 116				↓ tu-berli	n.de: type A,	class IN	
Source Conr	nection ID: 752d6	6265726c696e0264650	00001000100000100010000	91000100000100010000010001		<pre>     <root>: </root></pre>	type A, class	IN	
Supported \	/ersion: v2-draft	t-01 (0x709a50c4)				<pre>     <root>: </root></pre>	type A, class	IN	
Supported \	/ersion: 1 (0x000	000001)				<pre>     <root>: </root></pre>	type A, class	IN	
Supported \	/ersion: draft-32	2 (0xff000020)				<pre>     <root>: </root></pre>	type A, class	IN	
Supported \	/ersion: draft-31	1 (0xff00001f)				<pre>     <root>: </root></pre>	type A, class	IN	
Supported \	/ersion: draft-30	0 (0xff00001e)				<pre>     <root>: </root></pre>	type A, class	IN	
Sunnorted \	/ersion: draft-29	9 (0xff00001d)							
Suppor ceu	crozonn arare ze	5 (0/11000014)				<ul> <li>Additional</li> </ul>	records		
Supported \	/ersion: Unknown	(0x4a0ababa) (GREA	SE)			Additional <root>:</root>	records type Unused, c	lass Unknown	
Supported \	/ersion: Unknown	(0x4a0ababa) (GREA	SE)			Additional < Root>: [Response]	records type Unused, c <u>In: 15]</u>	lass Unknown	
Supported \ Supported \ Frame (frame)	/ersion: Unknown	(0x4a0ababa) (GREA	SE)	Packets: 31 · Displayed: 3 (9.7%)	Profile: Default	<ul> <li>Additional</li> <li><root>:</root></li> <li>[Response]</li> <li>Frame (frame)</li> </ul>	records type Unused, c In: 15] ),200 bytes	lass Unknown	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default
<ul> <li>Supported \</li> <li>Supported \</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> </ul>	/ersion: Unknown	(0x4a0ababa) (GREA	SE)	Packets: 31 · Displayed: 3 (9.7%)	Profile: Default	<ul> <li>Additional</li> <li><root>:</root></li> <li>[Response]</li> <li>Frame (frame)</li> <li>Enamo 15: 1</li> </ul>	records type Unused, c In: 15] ),200 bytes	ire (1216 bits) 152	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default
<ul> <li>Supported \</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> </ul>	200 bytes 52 bytes on wire	(0x4a0ababa) (GREA	SE) pytes captured (1216 bit	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 · 6a · 92 (00 · 00 · 20 · 5a · 6a · 92)	Profile: Default 📢	<ul> <li>Additional</li> <li><root>:</root></li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> </ul>	records type Unused, c In: 15] ),200 bytes 52 bytes on wi	lass Unknown ire (1216 bits), 152	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:05:10) Det: VMware 50:63:92 (00:00:20:56:63:92)
<ul> <li>Supported \</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> </ul>	200 bytes 52 bytes on wire , Src: VMware_f6	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA	SE) <u> pytes captured (1216 bit</u> 3:95:1c), Dst: VMware_5e - 102 168 217 131	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92)	Profile: Default 🌘	<pre>&gt; Additional &gt; <root>: [Response] ? Frame (frame) &gt; Frame 15: 1 &gt; Ethernet II &gt; Thereat Press </root></pre>	records type Unused, c In: 15] ),200 bytes 52 bytes on wi , Src: VMware_ otocol Version	:lass Unknown ire (1216 bits), 152 _f6:95:1c (00:50:56:f	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1C), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217 131
<ul> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> </ul>	200 bytes 52 bytes on wire , Src: VMware_f6 ptocol Version 4 am Protocol Src	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0abababa) (GREA (0x4a0abababababa) (GREA (0x4a0ababababababababababababababababababa	SE) <b>Dytes captured (1216 bit</b> 5:95:1c), Dst: VMware_5e :: 192.168.217.131 :: 12345	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92)	Profile: Default 🜘	<ul> <li>Additional</li> <li><root>:</root></li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> </ul>	records type Unused, c In: 15] ,200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol S	ire (1216 bits), 152 f6:95:1c (00:50:56:f 1 4, Src: 8.8.8.8, Ds Src Port: 53 Dst Por	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345
Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II Internet Pr User Datagr OUIC FFF	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x50:50:56:f6 , Src: 8.8.8.8, Dst Port: 53, Dst Port	SE) <u>Dytes captured (1216 bit</u> 3:95:1c), Dst: VMware_5e 1: 192.168.217.131 12345	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92)	Profile: Default 🔵	<ul> <li>Additional</li> <li><root>:</root></li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name</li> </ul>	records type Unused, c In: 15] 0,200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo	:lass Unknown ire (1216 bits), 152 _f6:95:1c (00:50:56:f 1 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por Dse)	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345
Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II Internet Pr User Datagr QUIC IETF OUIC Common	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x50:50:50:50:50; (0x50:50:50; (0x50:50; (0x50:50; (0x50:50; (0x50:50; (0x50:50; (0x50	SE) <b>Dytes captured (1216 bit</b> 3:95:1c), Dst: VMware_5e 192.168.217.131 12345	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92)	Profile: Default (	<ul> <li>Additional</li> <li><root>:</root></li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> </ul>	records type Unused, c In: 15] ,200 bytes 52 bytes on wi , Src: VMware, otocol Version am Protocol, S System (respo	Lass Unknown ire (1216 bits), 152 f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse)	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345
<ul> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>QUIC IETF</li> <li>QUIC Conn</li> <li>[Malformed]</li> </ul>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x56) (0x56) (0x5	SE) <u> bytes captured (1216 bit</u> 5:95:1c), Dst: VMware_5e 192.168.217.131 12345	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92)	Profile: Default 📢	<ul> <li>Additional</li> <li><root>:</root></li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x</li> </ul>	records type Unused, c In: 15] ) 200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard	ire (1216 bits), 152 _f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345
Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II Internet Pr User Datagr QUIC IETF QUIC Conn (Malformed (Expert I)	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] ofo (Error/Malfo	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 (00:50:56:f6 (00:50:56:f6 (00:50:56:f6 (00:50:56:f6 (00:50:56:f6 (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:50:56:f6) (00:56:56:56:56) (00:56:56:56:56) (00:56:56) (00:5	SE) pytes captured (1216 bit 5:95:1c), Dst: VMware_5e : 192.168.217.131 :: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92)	Profile: Default	<ul> <li>Additional</li> <li>&lt; Root&gt;:</li> <li>[Response :</li> <li>[Response :</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x Ouestions</li> </ul>	records type Unused, c In: 15] , 200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1	ire (1216 bits), 152 _f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror
<pre>Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II I tethernet Pr User Datagr QUIC IETF QUIC Conn Malformed (Malformed (Malformed)) (Malformed)</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfon med Packet (Excen	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst ; Port: 53, Dst Port con prmed): Malformed Pa pution occurred)]	SE) <b>bytes captured (1216 bit</b> 5:95:1c), Dst: VMware_5e :: 192.168.217.131 :: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92)	Profile: Default	<ul> <li>Additional</li> <li><root>:     <li>[Response :     <li>Frame (frame)     </li> <li>Frame 15: 1     <li>Ethernet II     <li>Internet Pr     <li>User Datagr     <li>Domain Name     Transacti     <li>Flags: 0x     Questions     Answer RR</li> </li></li></li></li></li></li></root></li></ul>	records type Unused, c In: 15] 0,200 bytes 52 bytes on wy , Src: VMware_ otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5	ire (1216 bits), 152 _f6:95:1c (00:50:56:f h 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror
<pre>Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II Internet Pr User Datagr QUIC IETF QUIC Conn [Malformed   [Expert I   [Malform   [Severi I   ]</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfon med Packet (Except ty level: Error]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 5:95:1c (00:50:56:f6 5:95:1c (00:50:56:f6 5:95:1c (00:50:50:f6 5:95:1c (00:50:f6 5:95:1c (00:50:f6 5:95:1c (00:50:f6 5:95:1c (00:f6 5:95:1c (00:f6) 5:95:1c (00:f6 5:95:1c (00:f6) 5:95:1c (00:f6) 5	SE) pytes captured (1216 bit S:95:1c), Dst: VMware_5e :: 192.168.217.131 :: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li><root>:     <li>[Response :     <li>Frame (frame)     </li> <li>Frame 15: 1     <li>Ethernet II     <li>Internet Pr     <li>User Datagr     <li>Domain Name     Transacti     <li>Flags: 0x     Questions     Answer RR     </li> <li>Authority     </li> </li></li></li></li></li></li></root></li></ul>	records type Unused, c In: 15] ) 200 bytes 52 bytes on w , Src: VMware_ otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0	ire (1216 bits), 152 _f6:95:1c (00:50:56:f h 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror
<pre>Supported \ Supported \ Frame 15: 1 Frame 15: 1 Fthernet II Fthernet II Guic Conn Guic Conn Malformed Fthere I Guic Conn Supported Conn Guic Conn Guic</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4, am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malformed Packet (Except ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst : Port: 53, Dst Port .on prmed): Malformed Pa .ption occurred)]	SE) Dytes captured (1216 bit 3:95:1c), Dst: VMware_5e 1: 192.168.217.131 1: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default (	<ul> <li>Additional</li> <li>&lt; (Root&gt;: [Response]</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x Questions Answer RR Authority Additiona</li> </ul>	records type Unused, c In: 15] ,200 bytes 52 bytes on w2 , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0 1 RRs: 0	Lass Unknown Lire (1216 bits), 152 _f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror
<pre>Supported V Supported V Frame (frame) Frame 15: 1 Fthernet II Internet Pr User Datagr QUIC terF QUIC Conn [Malformed [Expert I [Severi [Group:</pre>	200 bytes 200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malformed Packet (Except ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst ; Port: 53, Dst Port .on prmed): Malformed Pa (ption occurred)]	SE) bytes captured (1216 bit 3:95:1c), Dst: VMware_5e 1: 192.168.217.131 1: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default (	<ul> <li>Additional</li> <li>&lt; Root&gt;:</li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x Questions Answer RR Authority</li> <li>Additiona</li> <li>Oueries</li> </ul>	records type Unused, c In: 15] , 200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0 1 RRs: 0	ire (1216 bits), 152 f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror
<pre>Supported \ Supported \ Supported \ Frame 15: 1 Frame 15: 1 Fthernet II Internet Pr User Datagr QUIC IETF QUIC Conn (Malformed    [Expert I    [Malform    [Severi    [Group:</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfon med Packet (Excepty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst ; Port: 53, Dst Port .on prmed): Malformed Pa ption occurred)]	SE) bytes captured (1216 bit 5:95:1c), Dst: VMware_5e 192.168.217.131 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>&lt; (Root&gt;:</li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x Questions Answer RR Authority Additiona</li> <li>Queries</li> <li>Answers</li> </ul>	records type Unused, c In: 15] ),200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0 1 RRs: 0	ire (1216 bits), 152 _f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror
<pre>Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II Internet Pr User Datagr QUIC IETF QUIC Conn [Malformed "[Expert I [Severi [Group:</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfor med Packet (Except ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst ; Port: 53, Dst Port con prmed): Malformed Pa (ption occurred)]	SE) pytes captured (1216 bit 5:95:1c), Dst: VMware_5e :: 192.168.217.131 :: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>&lt; Root&gt;:</li> <li>[Response :</li> <li>[Response :</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x Questions Answer RR Authority Additiona</li> <li>Queries</li> <li>Answers</li> <li>Answers</li> <li>tu-berl</li> </ul>	records type Unused, c In: 15] ),200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0 l RRs: 0 in.de: type A,	:lass Unknown ire (1216 bits), 152 _f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e . class IN, addr 10.1	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror 50.7.69
Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II Internet Pr User Datagr QUIC IETF QUIC Conn [Malformed [Expert I [Malforn [Severi [Group:	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malformed Packet: (Except ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 5:95:1c (00:50:56:f6 5:95:1c (00:50:56:f6 5:95:1c (00:50:50:f6 5:95:1c (00:50:f6 5:95:1c (00:50:f6 5:95:1c (00:f6 5:95:1c (00:	SE) pytes captured (1216 bit S:95:1c), Dst: VMware_5e :: 192.168.217.131 :: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>«Root&gt;:     <li>[Response :     <li>Frame (frame)     </li> <li>Frame 15: 1     <li>Ethernet II     <li>Internet Pr     <li>User Datagr     <li>Domain Name     Transacti     <li>Flags: 0x     <li>Questions     </li> <li>Answer RR     Authority     Additiona     </li> <li>Queries     </li> <li>Answers     </li> <li>tu-berl     </li> <li>tu-berl     </li> </li></li></li></li></li></li></li></li></ul>	records type Unused, c In: 15] ,200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 S: 5 RRs: 0 1 RRs: 0 in.de: type A, in.de: type A,	Lass Unknown ire (1216 bits), 152 _f6:95:1c (00:50:56:f h 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e . class IN, addr 10.1 . class IN, addr 172.	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror 50.7.69 31.25.70
<pre>Supported \ Supported \ Frame 15: 1 Frame 15: 1 Fthernet II Fthernet II Guic Conn Guic Conn Malformed Ftheref I Malform Severi Group:</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4, am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malformed Packet: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst : Port: 53, Dst Port .on prmed): Malformed Pa .ption occurred)]	SE) Dytes captured (1216 bit 3:95:1c), Dst: VMware_5e 1: 192.168.217.131 1: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>&lt; (Root&gt;: 1/(Response)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Internet II</li> <li>Internet II</li> <li>Internet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x</li> <li>Questions</li> <li>Answer RR</li> <li>Authority</li> <li>Additiona</li> <li>Queries</li> <li>Answers</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> </ul>	records type Unused, c In: 15] ,200 bytes 52 bytes on w3 , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0 1 RRs: 0 in.de: type A, in.de: type A, in.de: type A,	Lass Unknown ire (1216 bits), 152 f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e . class IN, addr 10.1 . class IN, addr 10.1	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror 50.7.69 31.25.70 50.7.68
<pre>Supported \ Supported \ Supported \ Frame 15: 1 Frame 15: 1 Fthernet II Internet Pr User Datagr QUIC IETF QUIC Conn. Malformed (Malformed (Expert I [Malfor] [Severi] [Group:</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4, am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfon med Packet (Exception) ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst : Port: 53, Dst Port .on prmed): Malformed Pa :ption occurred)]	SE) <del>Dytes captured (1216 bit</del> 3:95:1c), Dst: VMware_5e 1: 192.168.217.131 1: 12345 Acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>&lt; (Root&gt;:</li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Fthernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x</li> <li>Questions</li> <li>Answer RR</li> <li>Authority</li> <li>Additiona</li> <li>Queries</li> <li>Answers</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> </ul>	records type Unused, c In: 15] , 200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0 1 RRs: 0 in.de: type A, in.de: type A, in.de: type A, in.de: type A,	<pre>ire (1216 bits), 152     f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse)     query response, No e     class IN, addr 10.1     class IN, addr 172.     class IN, addr 10.1     class IN, addr 10.1</pre>	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror 50.7.69 31.25.70 50.7.68 50.7.67
<pre>Supported V Supported V Frame (frame) Frame 15: 1 Ethernet II Internet Pr User Datagr QUIC IETF OUIC Conn (Malformed (Expert I [Severi] [Group:</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfon ned Packet (Excepty) ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst : Port: 53, Dst Port .on prmed): Malformed Pa :ption occurred)]	SE) bytes captured (1216 bit 5:95:1c), Dst: VMware_5e 192.168.217.131 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>&lt; (Root&gt;:</li> <li>[Response]</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x Questions Answer RR Authority Additiona</li> <li>Queries</li> <li>Answers</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> </ul>	records type Unused, c In: 15] ) 200 bytes 52 bytes on wi , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 s: 5 RRs: 0 1 RRs: 0 in.de: type A, in.de: type A, in.de: type A, in.de: type A, in.de: type A,	<pre>:lass Unknown ire (1216 bits), 152 _f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e query response, No e . class IN, addr 10.1 . class IN, addr 172. . class IN, addr 10.1 . class IN, addr 10.1 . class IN, addr 10.1</pre>	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror 50.7.69 31.25.70 50.7.68 50.7.67 50.7.70
<pre>Supported \ Supported \ Frame (frame) Frame 15: 1 Ethernet II I Ethernet II I User Datagr QUIC IETF QUIC Conn [Malformed] [Expert I [Malforn] [Severi] [Group:</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4 am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfoo ned Packet (Except ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 , Src: 8.8.8.8, Dst : Port: 53, Dst Port con prmed): Malformed Pa (ption occurred)]	SE) pytes captured (1216 bit S:95:1c), Dst: VMware_5e :: 192.168.217.131 :: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>&lt; (Root&gt;: )</li> <li>(Response : )</li> <li>(Response : )</li> <li>Frame (frame)</li> <li>Frame 15: 1</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name Transacti</li> <li>Flags: 0x Questions</li> <li>Answer RR Authority</li> <li>Additiona</li> <li>Queries</li> <li>Answers</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>tu-berl</li> <li>Request</li> </ul>	records type Unused, c In: 15] , 200 bytes 52 bytes on wight , Src: VMware_ otocol Version am Protocol, S System (respondent on ID: 0xc900 8080 Standard : 1 S: 5 RRs: 0 1 RRs: 0 in.de: type A, in.de: type A	<pre>:lass Unknown ire (1216 bits), 152 _f6:95:1c (00:50:56:f n 4, Src: 8.8.8.8, Ds Src Port: 53, Dst Por onse) query response, No e query response, No e . class IN, addr 10.1 . class IN, addr 10.1 . class IN, addr 10.1</pre>	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror 50.7.69 31.25.70 50.7.68 50.7.67 50.7.70
<pre>Supported \ Supported \ Supported \ Frame 15: 1 Frame 15: 1 Ethernet II Internet Pr User Datagr QUIC IETF QUIC Conn [Malformed [Expert I [Malformed [Severi [Group:</pre>	200 bytes 52 bytes on wire , Src: VMware_f6 otocol Version 4, am Protocol, Src ection informatic Packet: QUIC] nfo (Error/Malfon med Packet (Except ty level: Error] Malformed]	(0x4a0ababa) (GREA (0x4a0ababa) (GREA (0x4a0ababa) (GREA (00:50:56:f6 5:95:1c (00:50:56:f6 5:95:1c (00:50:56:f6 5:95:1c (00:50:50:f6 5:95:1c (00:50:f6 5:95:1c (00:50:f6 5:95:1c (00:50:f6 5:95:1c (00:f6 5:95:1c (	SE) pytes captured (1216 bit S:95:1c), Dst: VMware_5e :: 192.168.217.131 :: 12345 acket (Exception occurre	Packets: 31 · Displayed: 3 (9.7%) s) on interface ens33, id 0 :6a:92 (00:0c:29:5e:6a:92) d)]	Profile: Default	<ul> <li>Additional</li> <li>&lt; <pre>&lt; Root&gt;:</pre> <li>[Response] <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Frame (frame)</li> <li>Ethernet II</li> <li>Internet Pr</li> <li>User Datagr</li> <li>Domain Name</li> <li>Transacti</li> <li>Flags: 0x</li> <li>Questions</li> <li>Answer RR</li> <li>Authority</li> <li>Additiona</li> <li>Queries</li> <li>Answers</li> <li>tu-berl</li> </li></li></ul>	records type Unused, c In: 15] , 200 bytes 52 bytes on w2 , Src: VMware otocol Version am Protocol, S System (respo on ID: 0xc900 8080 Standard : 1 S: 5 RRs: 0 1 RRs: 0 in.de: type A, in.de: type A,	Liass Unknown Lire (1216 bits), 152 	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default bytes captured (1216 bits) on interface ens33, id 0 6:95:1c), Dst: VMware_5e:6a:92 (00:0c:29:5e:6a:92) t: 192.168.217.131 t: 12345 rror 50.7.69 31.25.70 50.7.68 50.7.67 50.7.70

#### Impersonating DNS Requests with VNRF (cont'd)

No. Tim	Source	Destination	Protocol	Length Info				xc813[Malformed_Packet]
-133.	38438 8.8.8.8	192.168.217.1.	QUIC	13Initial, SCID=0	000000000000109	)		in.de A <root> A <root> A <root> A</root></root></root>
14 3.	38771 192.168.217	.1 8.8.8.8	QUIC	200 Version Negotia	ation, DCID=00	000000000109		A tu-berlin.de A 10.150.7.69 A 172 ens33. id 0
- 15 3.	58935 8.8.8.8	192.168.217.1.	QUIC	152 53 → 12345 Len=	=110[Malformed	Packet]		5:f6:95:1c)
→ Frame	14: 200 bytes on wi	ire (1600 bits), 2	00 byt	es captured (1600 b:	its) on inter	<sup>-</sup> ace ens33, id 0		
Etherr	et II, Src: VMware_	_5e:6a:92 (00:0c:2	9:5e:6	a:92), Dst: VMware_1	f6:95:1c (00:	50:56:f6:95:1c)		
▶ Interr	et Protocol Versior	n 4, Src: 192.168.	217.13	1, Dst: 8.8.8.8				
⊢ User [	atagram Protocol, S	Src Port: 12345, D	st Por	t: 53				
- QUIC I	ETF							
> QUIC	Connection informa	ation						
[Pac	ket Length: 158]							
1	= Header Form	n: Long Header (1)						
.100	1001 = Unused: 0x4	19						
Vers	ion: Version Negoti	Lation (0x00000000	)					
Dest	ination Connection	ID Length: 7						
Dest	ination Connection	ID: 0000000000010	9					played: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default
Sour	ce Connection ID Le	ength: 116						ens33, id 0 29:5e:6a:92)
Sour	ce Connection ID: 7	752d6265726c696e02	646500	00010001000001000100	00001000100000	)100010000010001		
Supp	orted Version: v2-o	lraft-01 (0x709a50	c4)					
Supp	orted Version: 1 (0	)x00000001)						
Supp	orted Version: draf	⁼t-32 (0xff000020)						
Supp	orted Version: draf	⁼t-31 (0xff00001f)						
Supp	orted Version: draf	⁼t-30 (0xff00001e)						
Supp	orted Version: draf	t-29 (0xff00001d)						
Supp	orted Version: Unkr	10wn (0x4a0ababa)	(GREAS	E)				
🔵 🎽 Fra	ne (frame), 200 bytes				Packets:	31 · Displayed: 3 (9.7%)	Profile: Default	
					[Time: 0.0201630	79 seconds]		

#### Impersonating DNS Requests with VNRF (cont'd)

No. Time Source Dest	No. Time Source Destination Protocol Length Info
13         3.538438         8.8.8.8         192           14         3.538771         192.168.217.1         8.8	- 13 3.538438 8.8.8.8 192.168.217.1 DNS 13 DNS Stateful operations (DSO) 0xc813[Malformed Packet]
L 15 3.558935 8.8.8.8 192	→ 14 3.538771… 192.168.217.1… 8.8.8.8 DNS 200 Standard guery 0xc900 A tu-berlin.de A <root> A <root> A <root> A</root></root></root>
<pre>&gt; Ethernet II, Src: VMware_5e:6a:</pre>	- 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
<ul> <li>Internet Protocol Version 4, Sr</li> <li>User Datagram Protocol, Src Por</li> </ul>	Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, id 0
<ul> <li>QUIC IETF</li> <li>QUIC Connection information</li> </ul>	<pre>Ethernet II, Src: VMware 5e:6a:92 (00:0c:29:5e:6a:92), Dst: VMware f6:95:1c (00:50:56:f6:95:1c)</pre>
[Packet Length: 158] 1 = Header Form: Long	<pre>&gt; Internet Protocol Version 4, Src: 192.168.217.131, Dst: 8.8.8.8</pre>
.100 1001 = Unused: 0x49	<pre>&gt; User Datagram Protocol, Src Port: 12345, Dst Port: 53</pre>
Destination Connection ID Len	- Domain Name System (query)
Source Connection ID Length:	Transaction ID: 0xc900
Source Connection ID: 752d626 Supported Version: v2-draft-0	▶ Flags: 0x0000 Standard query
Supported Version: 1 (0x00000 Supported Version: draft 22 (	Questions: 7
Supported Version: draft-32 (	Answer RRs: 0
Supported Version: draft-30 ( Supported Version: draft-29 (	Authority RRs: 0
Supported Version: Unknown (0	Additional RRs: 1
🔴 🍸 Frame (frame), 200 bytes	- Queries
Frame 15: 152 bytes on wire (1     Ethernot II Src: VMwaro f6:00	tu-berlin.de: type A, class IN
<ul> <li>Internet Protocol Version 4, 5</li> </ul>	<pre>&gt; <root>: type A, class IN</root></pre>
<ul> <li>User Datagram Protocol, Src Po</li> <li>QUIC IETF</li> </ul>	▶ <root>: type A, class IN</root>
QUIC Connection information     Malformed Packet: OUIC1	▶ <root>: type A, class IN</root>
<ul> <li>[Expert Info (Error/Malforme</li> </ul>	▶ <root>: type A, class IN</root>
[Maiformed Packet (Excepting) [Severity level: Error]	▶ <root>: type A, class IN</root>
[Group: Malformed]	▶ <root>: type A, class IN</root>
	Additional records
	Root>: type Unused, class Unknown
	[Response In: 15]
	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default
	[Time: 0.020163079 seconds]

#### **Mitigation**

#### **CID** Reflection

• A server always choses a fresh SCID, also for version negotiation

#### Hashing

- A "seed" for a CID still chosen by the client
- The server uses a hash of the seed as DCID
- An attacker would need to calculate the inverse to create a meaningful payload

#### Masking

- QUIC headers get an additional field containing a masking value
- The masking value is randomly generated by the server
- The entire remaining header is XORed
- Client maintains control over DCID but payloads will appear "random"

# **Traffic Amplification**

#### Path amplification VS Bandwidth Amplification



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

#### Minimum path requirements

- "QUIC must not be used if the network path cannot support 1200 bytes datagrams"
- Ensured through padding of initial packets and path challenges
- Small packets on new paths are an issue
- Server should send two separate path validations

#### **Unbalanced handshake sizes**

- Server initial packets are larger than client intial packets
- Server initial packets should never be larger than 3\*1200 bytes

#### Reliability

- No "typical" reliability in path challenges, server can send multiple challenges
  - Initial bursts
  - Re-send with timeout
- Multiple challenges definitely surpass amplification limits
- Normal packets are re-sent if the acknowledgment is not received
- Server should not re-send server initial packets
  - Retries for the initial messages have to be handled by the client.



#### **Amplification**



### 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.
- 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!