Better don't be too QUIC(K)

Yuri Gbur



Better don't be too QUIC(K) | Yuri Gbur | IT-SECX 2023 | 2023-10-13 © 2023 SEC Consult | All rights reserved

Yuri Gbur

- MSc in Computer Science at Technische • Universität (TU) Berlin
- Security Consultant at SEC Consult ٠
- Head of Cloud Security •

y.gbur@sec-consult.com

y@yukonsec yukonsec@infosec.exchange



- 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



APACHE GOOGLE CLOUDFLARE moz://a Microsoft



• RFC 8999

• RFC 9000

RFC 9001

• RFC 9002

• RFC 9115

(HTTP/3)





ent			Ser\
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]	



ient				Ser
	Initial[0]	:	CRYPTO[CH]	
				1
	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]	











Challenges with Securing QUIC / HTTP3



Better don't be too QUIC(K) | Yuri Gbur | IT-SECX 2023 | 2023-10-13 © 2023 SEC Consult | All rights reserved

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





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

SEC Consult

١V

(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





PNr Len Packet Number Length



Long Header





Controllable Bytes for Protocol Impersonation





Controllable Bytes for Protocol Impersonation









la Time Source Destination Protocol Length Info	No Time Course Destination Distance Longht lafe
- 13.3.538438 & 8.8.8. 192.168.217.1.0UIC 13.Thitial_SCID=00000000000000	NO. Inne Source Destination Product Lengt Hild 12.2 528428 & 8 & 8 & 102.168.217.1 DNS 12.DNS Stateful energing (DSO) Avc812[Malformed Dacket]
14 3 538771 102 168 217 1 8 8 8 8 0 0 0 0 Version Negotiation DCD=000000000109	13 5.500 40 0 10.0.10 132.100.217.1. Dio 15 Dio 500 600 0000 0000 0000 0000 00000 000000 0000
15 3, 558935, 8.8, 8.8, 8 192,168,217.1, OUTC 15253 \rightarrow 12345 Len=110[Malformed Packet]	153 558935 8 8 8 8 192 168 217 1 DNS 152 Standard query excessors a Qx2990 A tu-berlin de A 10012 A 100150 7 69 A 17
Frame 14: 200 butes on wire (1600 bits) 200 butes contured (1600 bits) on interface energy id 0	is discosting of the second se
Frame 14: 200 bytes on wire (1600 bits), 200 bytes captured (1600 bits) on interface ensas, 10 0	Frame 14: 200 bytes on Wire (1600 bits), 200 bytes captured (1600 bits) on interface ens33, 10 0
Ethernet 1, 510: VMWare_5e:ba:92 (00:00:29:5e:ba:92), D51: VMWare_16:95:10 (00:50:56:16:95:10)	> Ethernet 11, Src: VMWare_5e:6a:92 (00:00:29:5e:6a:92), Dst: VMWare_T6:95:1C (00:50:56:T6:95:1C)
Microfiel 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
OUZO DALAGRAM PROLOCOL, SEC POEL: 12345, DSL POEL: 53	User Datagram Protocol, Src Port: 12345, Dst Port: 53
	- Domain Name System (query)
Quic connection information	Transaction ID: 0xC900
[Packet Length: 156]	> Flags: 0x0000 Standard query
1 Header Form: Long Header (1)	Questions: /
	Answer KKS: 0
Version Version Regoliation (0x00000000)	Authority RRS: 0
Destination Connection ID Length: /	Additional RKS: 1
Destination Connection ID: 000000000000000	• Queries
Source connection ID Length: 116	> tu-berlin.de: type A, class IN
Source connection in: //sdb2b3/26cabeed26455000001000100001000100000100001000010	> <root>: type A, class IN</root>
Supported Version: V2-Gratt-01 (0x70935064)	> <root>: type A, class IN</root>
Supported Version: 1 (0x00000000)	> <root>: Type A, class IN</root>
Supported Version: draft-32 (0x11000020)	> <root>: Type A, class IN</root>
Supported Version: draft 20 (0xff00001)	> <rool: a,="" class="" in<="" td="" type=""></rool:>
Supported Version: draft-30 (0xf1000014)	> <rool>: Lype A, CLASS IN</rool>
Supported Version: draft-29 (0x1000010)	Additional records
Supported Version: Unknown (0x4a0ababa) (GREASE)	> <rools: class="" td="" type="" unknown<="" unused,=""></rools:>
Frame (frame), 200 bytes Packets: 31 · Displayed: 3 (9.7%) Profile: Default	Frame (frame), 200 bytes Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) 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	<pre>> Domain Name System (response)</pre>
> QUIC Connection information	Transaction ID: 0xc900
[Malformed Packet: QUIC]	▶ Elags: 0x8080 Standard guery response. No error
[Event The (Even (N-) formed), N-) formed Deduct (Eventien conversel)]	Tager one contained dury responsed no error
<pre>~ [Expert into (Error/Maitormed): Maitormed Packet (Exception occurred)]</pre>	Questions: 1
[Expert into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)]	Questions: 1 Answer RRs: 5
<pre>[Expert into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0
<pre>[Expert into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 Additional RRs: 0
<pre>~ [Expert Into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 Additional RRs: 0 > Queries
<pre>~ [Expert Into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 Additional RRs: 0 > Queries * Answers
<pre>~ [Expert Into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 Additional RRs: 0 • Queries • Answers • tu-berlin.de: type A, class IN, addr 10.150.7.69
<pre>~ [Expert Into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 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
<pre>* [Expert Into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 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 10.150.7.68
<pre>* [Expert Into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 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 10.150.7.67
<pre>* [Expert Into (Error/Malformed): Malformed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed]</pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 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 10.150.7.67 > tu-berlin.de: type A, class IN, addr 10.150.7.70
<pre> [Expert Into (Error/Maitormed): Maitormed Packet (Exception occurred)] [Malformed Packet (Exception occurred)] [Severity level: Error] [Group: Malformed] </pre>	Questions: 1 Answer RRs: 5 Authority RRs: 0 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: 0.02016270, seconds]



						-
No. Time Source	Destination	Protocol Length Info				xc813[Malformed_Packet]
☐ 13 3.538438 8.8.8.8	192.168.217.1.	.QUIC 13Initial, S	SCID=0000000000109			in.de A <root> A <root> A <root></root></root></root>
14 3.538771 192.168	217.1 8.8.8.8	QUIC 200 Version No	egotiation, DCID=00000	00000109		A tu-berlin.de A 10.150.7.69 A 17
- 15 3.558935 8.8.8.8	192.168.217.1.	. QUIC 152 53 → 1234	5 Len=110[Malformed Pac	ket]		5:f6:95:1c)
▶ Frame 14: 200 bytes o	n wire (1600 bits), 2	00 bytes captured (1	600 bits) on interface	ens33, id 0		
Ethernet II, Src: VMw	are_5e:6a:92 (00:0c:2	9:5e:6a:92), Dst: VM	ware_f6:95:1c (00:50:50	3:f6:95:1c)		
Internet Protocol Ver	sion 4, Src: 192.168.	217.131, Dst: 8.8.8.8	8			
User Datagram Protoco	l, Src Port: 12345, D	st Port: 53				
- QUIC IETF						
QUIC Connection inf	ormation					
[Packet Length: 158]					
1 = Header	Form: Long Header (1)					
.100 1001 = Unused:	0x49					
Version: Version Ne	gotiation (0x00000000)				
Destination Connect	ion ID Length: 7					
Destination Connect	ion ID: 0000000000010	9				played: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default
Source Connection I	D Length: 116					ens33, id 0
Source Connection I	D: 752d6265726c696e02	64650000010001000001	00010000010001000001000)10000010001		29.50.00.92)
Supported Version:	v2-draft-01 (0x709a50	c4)				
Supported Version:	1 (0x0000001)					
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 · D	isplayed: 3 (9.7%)	Profile: Default	
			[11me. 0.0201030/9 Seco	nuoj		



No. Time Source	Destination	Protocol Length Info			xc813[Malformed Packet]
<mark>13 3.538438… 8.8.8</mark>	.8 192.168.21	7.1… QUIC 13… Initia	1, SCID=0000000000109		in.de A <root> A <root> A <root> A <root> A</root></root></root></root>
14 3.538771 192.:	.68.217.1 8.8.8.8	QUIC 200 Versio	n Negotiation, DCID=0000000000010	9	ens33, id 0
L 15 3.558935 8.8.	.8 192.168.21	7.1… OUIC 152 53 → 1	2345 Len=110[Malformed Packet]		5:f6:95:1c)
→ Frame 14: 200 byte	s on wire (1600 bits)	, 200 bytes captured	(1600 bits) on interface ens33,	id 0	
Ethernet II, Src:	VMware_5e:6a:92 (00:0	c:29:5e:6a:92), Dst:	VMware_f6:95:1c (00:50:56:f6:95:	1c)	
Internet Protocol	Version 4, Src: 192.:	68.217.131, Dst: 8.8	.8.8		
User Datagram Prot	ocol, Src Port: 1234	5, Dst Port: 53			
▼ QUIC IETF					
QUIC Connection	information				
[Packet Length:	158]				
1 = Head	er Form: Long Header	(1)			
.100 1001 = Unus	ed: 0x49				
Version: Versior	Negotiation (0x00000	0000)			
Destination Conr	ection ID Length: 7				
Destination Conr	ection ID: 000000000	00109			played: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default
Source Connectio	n ID Length: 116				ens33, id 0
Source Connectio	n ID: 752d6265726c690	e0264650000010001000	001000100000100010000010001000001	0001	29:50:6a:92)
Supported Versio	n: v2-draft-01 (0x709	a50c4)			
Supported Versio	n: 1 (0x00000001)				
Supported Versio	n: draft-32 (0xff0000)20)			
Supported Versio	n: draft-31 (0xff0000	01f)			
Supported Versio	n: draft-30 (0xff0000)1e)			
Supported Versio	n: draft-29 (0xff0000	01d)			
Supported Versio	n: Unknown (0x4a0abal	a) (GREASE)			
	-				
🔵 🏹 Frame (frame), 200 bvt	25		Packets: 31 · Displayed: 3 (9.7%) Profile: Default	
			[Time: 0.020163079 seconds]		



No. Time	Source	Destination	Protocol	Lengtr Info		xc813[Malformed Packet]
<u> </u>	. 8.8.8.8	192.168.217.1	QUIC	13… Initial, SCID=000000000000000		in.de A <root> A <root> A <root> A</root></root></root>
14 3.538771	. 192.168.217.1	8.8.8.8	QUIC	200 Version Negotiation, DCID=00000000000109		A tu-berlin.de A 10.150.7.69 A 172
– 15 3.558935.	. 8.8.8.8	192.168.217.1	QUIC	152 53 → 12345 Len=110[Malformed Packet]		3:f6:95:1c)
▶ Frame 14: 20	0 bvtes on wir	e (1600 bits), 2	00 bvt	ces captured (1600 bits) on interface ens33, id 0		
Ethernet II.	Src: VMware 5	e:6a:92 (00:0c:2	9:5e:6	a:92), Dst: VMware f6:95:1c (00:50:56:f6:95:1c)		
Internet Pro	tocol Version	4. Src: 192.168.	217.13	31. Dst: 8.8.8.8		
User Datagra	m Protocol. Sr	c Port: 12345. D	st Por	-t: 53		
- OUIC IETF						
OUIC Conne	ction informat	ion				
[Packet Le	ngth: 158]					
1	= Header Form:	Long Header (1)	٦			
.100 1001	= Unused: 0x49					
Version: V	ersion Negotia	tion (0x00000000)			
Destinatio	n Connection I	D Length: 7	_			
Destinatio	n Connection I	D: 000000000000000	9			played: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default
Source Con	nection ID Len	gth: 116				ens33, id 0
Source Con	nection ID: 75	2d6265726c696e02	646500	00010001000010001000010001000010001000010000		29:50:60:92)
Supported	Version: v2-dr	aft-01 (0x709a50	c4)			
Supported	Version: 1 (0x	00000001)				
Supported	Version: draft	-32 (0xff000020)				
Supported	Version: draft	-31 (0xff00001f)				
Supported	Version: draft	-30 (0xff00001e)				
Supported	Version: draft	-29 (0xff00001d)				
Supported	Version: Unkno	wn (0x4a0ababa)	(GREAS	SE)		
🥚 🎽 Frame (frame)), 200 bytes			Packets: 31 · Displayed: 3 (9.7%)	Profile: Default	
	-			[Time: 0.020163079 seconds]		



No. Time Source	Destination	Protocol Length Info				xc813[Ma]	formed Packet]
☐ 13 3.538438 8.8.8	8 192.168.217.1	L… QUIC 13… Initial	, SCID=0000000000	109		in.de A <	Root> A <root> A <root> A</root></root>
14 3.538771 192.10	8.217.1 8.8.8.8	QUIC 200 Versior	Negotiation, DCID	=00000000000109		A tu-berl ens33. i	in.de A 10.150.7.69 A 172
L 15 3.558935 8.8.8	8 192.168.217.1	L… QUIC 152 53 → 12	2345 Len=110[Malfor	med Packet]		5:f6:95:1	.c)
→ Frame 14: 200 bytes	on wire (1600 bits),	200 bytes captured	(1600 bits) on int	erface ens33, id 0			
Ethernet II, Src: V	Mware_5e:6a:92 (00:0c:	29:5e:6a:92), Dst:	VMware_f6:95:1c (0	0:50:56:f6:95:1c)			
Internet Protocol V	ersion 4, Src: 192.168	.217.131, Dst: 8.8.	8.8				
User Datagram Proto	col, Src Port: 12345,	Dst Port: 53					
- QUIC IETF							
▶ QUIC Connection i	nformation						
[Packet Length: 1	58]						
1 = Heade	r Form: Long Header (1	.)					
.100 1001 = Unuse	d: 0x49						
Version: Version	Negotiation (0x0000000	0)					
Destination Conne	ction ID Length: 7						
Destination Conne	ction ID: 000000000001	.09				played: 3 (9.79	%) · Dropped: 0 (0.0%) Profile: Default
Source Connectior	ID Length: 116					ens33,	id 0
Source Connectior	ID: 752d6265726c696e0	2646500000100010000	010001000001000100	000100010000010001		29.50.00.1	52)
Supported Version	: v2-draft-01 (0x709a5	0C4)					
Supported Versior	: 1 (0x0000001)						
Supported Versior	: draft-32 (0xff000020))					
Supported Versior	: draft-31 (0xff00001f	·)					
Supported Versior	: draft-30 (0xff00001e)					
Supported Versior	: draft-29 (0xff00001d)					
Supported Versior	: Unknown (0x4a0ababa)	(GREASE)					
🔵 🌌 Frame (frame), 200 bytes			Pack	cets: 31 · Displayed: 3 (9.7%)	Prof	file: Default	
			[Time: 0.020	163079 seconds]			



No. T	Source Dest 3, 538438 8, 8, 8, 8 193	No. Time	Source	Destination	Protoco	l Length Info						
14 3	3.538771 192.168.217.1 8.8	- 13 3.538438	8 8.8.8.8	192.168.217.1	DNS	13 DNS	Stateful	operations	(DSO) 0	xc813[Malfo	rmed Packet]
⊢ 15 3 Eram	3.558935… 8.8.8.8 19: ne 14: 200 bytes on wire (16	+ 14 3.538771	192.168.217.	1 8.8.8.8	DNS	200 Star	ndard quer	y 0xc900 A	tu-berl	in.de A <ro< td=""><td>ot> A <root></root></td><td>> A <root> A</root></td></ro<>	ot> A <root></root>	> A <root> A</root>
▶ Ethe	rnet II, Src: VMware_5e:6a:	4 15 3.558935	5 8.8.8.8	192.168.217.1	DNS	152 Star	ndard quer	y response	0xc900	A tu-berlin	.de A 10.150	0.7.69 A 172
> User	Datagram Protocol, Src Por	→ Frame 14: 20	00 bytes on wi	re (1600 bits).	200 hvt	tes cantur	ed (1600	hits) on i	nterface	ens33, id (9	
v QUIC	IETF IC Connection information	Fthernet II	Src: VMware F	5e:6a:92 (00:0c:	29.56.6	Sa:92) De	t: VMware	f6:95:1c	(00:50:5	6:f6:95:1c)	,	
[Pi	acket Length: 158]	Thternet Pro	, ore: Version	4 Src: 192 168	217 13	21 Det · 8	8888	_10.00.10	(00.00.0	0.10.00.10)		
.10	00 1001 = Unused: 0x49	Lisor Datagra	am Protocol Si	4, STC: 132.100	st Dor	-+· 52	.0.0.0					
Ve	rsion: Version Negotiation stination Connection ID Ler	- Domain Namo	Systom (quory)	C POIL: 12343,	J3L F01	1. 55						
De	stination Connection ID: 00)								
So	urce Connection ID Length: urce Connection ID: 752d620		DN ID: 0xC900									
Su	pported Version: v2-draft-0	er → Flags: Oxe	0000 Standard (query								
Su	pported Version: draft-32 (Questions	: 7									
Su	pported Version: draft-31 (pported Version: draft-30 (Answer RRs	s: 0									
Su	pported Version: draft-29 (Authority	RRs: 0									
Su	pported version: Unknown (e	" Additional	l RRs: 1									
🔴 🖉 F	Frame (frame), 200 bytes	👻 Queries										
→ Fra	ame 15: 152 bytes on wire (↓ tu-berli	in.de: type A,	class IN								
) Int	cernet Protocol Version 4,	s → <root>:</root>	type A, class	IN								
→ Use → QUI	er Datagram Protocol, Src P IC IETF	° → <root>:</root>	type A, class	IN								
→ Q	QUIC Connection information	→ <root>:</root>	type A, class	IN								
· [Expert Info (Error/Malform	• → <root>:</root>	type A, class	IN								
	[Malformed Packet (Except: [Severity level: Error]	i → <root>:</root>	type A, class	IN								
	[Group: Malformed]	→ <root>:</root>	type A, class	IN								
		 Additional 	l records									
		<pre> Root>: </pre>	type Unused, d	class Unknown								
		[Response	In: 15]									
		Crame /frame	a) 200 bytes					Da	ekoter 21 - Di	splayed 2 (0 70/)	Drannadi 0 (0 0%)	Brofilos Dofault
		Frame (frame	e), 200 bytes			Time 0	020163079 second	51 Fd	ckets: 51 · Di	spiayed: 5 (9.7%) • 1	Dropped: 0 (0.0%)	Frome: Default



No Time Source Desti					
- 13 3.538438 8.8.8.8 192	No. Time Source	e Destination	Protocol Lengtr Info		-
14 3.538771 192.168.217.1 8.8	13 3.538438 8.8.	.8.8 192.168.217.1	… DNS 13… DNS Stateful ope	erations (DSO) 0xc813[Malformed Packet	:]
Erame 14: 200 bytes on wire (16)	+ 14 3.538771… 192.	.168.217.1 8.8.8.8	DNS 200 Standard query 0	0xc900 A tu-berlin.de A <root> A <root< td=""><td>:> A <root> A</root></td></root<></root>	:> A <root> A</root>
<pre>> Ethernet II, Src: VMware_5e:6a: > Internet Protocol Version 4. Src</pre>	└─ 15 3.558935… 8.8.	.8.8 192.168.217.1	DNS 152 Standard query r	response 0xc900 A tu-berlin.de A 10.15	50.7.69 A 172
 User Datagram Protocol, Src Port OUIC IETF 	▶ Frame 14: 200 byt	es on wire (1600 bits), 🛛	200 bytes captured (1600 bit	s) on interface ens33, id 0	
QUIC Connection information [Packet Length: 158]	Ethernet II, Src:	VMware_5e:6a:92 (00:0c:	29:5e:6a:92), Dst: VMware_f6	3:95:1c (00:50:56:f6:95:1c)	
1 = Header Form: Long	Internet Protocol	. Version 4, Src: 192.168	217.131, Dst: 8.8.8.8		
.100 1001 = Unused: 0x49 Version: Version Negotiation	User Datagram Pro	tocol, Src Port: 12345,	Ost Port: 53		
Destination Connection ID Lene	- Domain Name System	m (query)			
Source Connection ID Length: :	Transaction ID:	0xc900			
Source Connection ID: 752d626 Supported Version: v2-draft-01	▹ Flags: 0x0000 S	tandard query			
Supported Version: 1 (0x000000	Ouestions: 7				
Supported Version: draft-32 ((Supported Version: draft-31 ()	Answer PRs' 0				
Supported Version: draft-30 (Authority PRo:	0			
Supported Version: draft-29 (Supported Version: Unknown (0)	AULIIOTILY RRS.				
	Additional RRs:	1			
Frame (frame), 200 bytes	- Queries				
 Frame 15: 152 bytes on wire (1 Ethernet II, Src: VMware_f6:95 	→ tu-berlin.de:	type A, class IN			
Internet Protocol Version 4, S	Foot>: type i	A, class IN			
• USER Datagram Protocol, Src Po • QUIC IETF	Root>: type	A, class IN			
QUIC Connection information	Root>: type /	A, class IN			
<pre>- [Expert Info (Error/Malforme</pre>	→ <root>: type</root>	A, class IN			
[Malformed Packet (Excepti [Severity level: Error]	→ <root>: type /</root>	A, class IN			
[Group: Malformed]	<pre> <root>: type</root></pre>	A. class IN			
	Additional reco	ords			
		Unused class Unknown			
	[Kesponse III: 1	<u> </u>			
	🥚 🗹 🛛 Frame (frame), 200 by	/tes	[Time: 0.020162070 seconds]	Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default



No. Time Source Dest	No. Time Source De	estination Protoco'	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	92.168.217.1 DNS	13 DNS Stateful operations	s (DSO) 0xc813[Malformed Pa	cket]
- 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>	Root> A <root> A</root>
<pre>> Ethernet II, Src: VMware_5e:6a: > Internet Distance</pre>	↓ 15 3.558935 8.8.8.8 1	92.168.217.1 DNS	152 Standard query response	e 0xc900 A tu-berlin.de A 1	0.150.7.69 A 172
 User Datagram Protocol, Src Por 	> Frame 14: 200 bytes on wire (1	1600 bits), 200 byt	es captured (1600 bits) on :	interface ens33, id 0	
 QUIC IEIF QUIC Connection information 	Ethernet II, Src: VMware_5e:6a	a:92 (00:0c:29:5e:6	a:92), Dst: VMware_f6:95:1c	(00:50:56:f6:95:1c)	
[Packet Length: 158] 1 = Header Form: Long	Internet Protocol Version 4, 5	Src: 192.168.217.13	81, Dst: 8.8.8.8		
.100 1001 = Unused: 0x49 Version: Version Negotiation	User Datagram Protocol, Src Po	ort: 12345, Dst Por	t: 53		
Destination Connection ID Len	🝷 Domain Name System (query)				
Source Connection ID Length:	Transaction ID: 0xc900				
Source Connection ID: 752d626 Supported Version: v2-draft-6	Flags: 0x0000 Standard query	y .			
Supported Version: 1 (0x00000 Supported Version: draft-32 (Questions: 7				
Supported Version: draft-31 (Answer RRs: 0				
Supported Version: draft-30 (Supported Version: draft-29 (Authority RRs: 0				
Supported Version: Unknown (G	Additional RRs: 1				
🔴 🍸 Frame (frame), 200 bytes	▼ Queries				
Frame 15: 152 bytes on wire (Ethernet II Src: VMware f6:00	→ tu-berlin.de: type A, class	ss IN			
 Internet Protocol Version 4, 5 	→ <root>: type A, class IN</root>				
 User Datagram Protocol, Src Po QUIC IETF 	→ <root>: type A, class IN</root>				
QUIC Connection information	→ <root>: type A, class IN</root>				
 [Expert Info (Error/Malforme 	→ <root>: type A, class IN</root>				
[Severity level: Error]	→ <root>: type A, class IN</root>				
[Group: Malformed]	→ <root>: type A, class IN</root>				
	 Additional records 				
	<root>: type Unused, class</root>	s Unknown			
	[Response In: 15]				
	🔴 🗹 Frame (frame), 200 bytes		P	ackets: 31 · Displayed: 3 (9.7%) · Dropped: 0	(0.0%) Profile: Default
			[Time: 0.020163079_seconds]		



No. Time Source Dest	No Timo Sourco Dostinatio	n Protocol Longth Info	
□ 13 3.538438 8.8.8.8 192 □ 14 3.538771 192,168,217,1 8.8	- 13 3 538/38 8 8 8 8 8 102 16	8 217 1 DNS 13 DNS Stateful o	perations (DSO) 0xc813[Malformed Packet]
- 15 3.558935 8.8.8.8 192		8 DNS 200 Standard query	$(0 \times 0 \times 0 \times 0)$ (DSO) (XCOIS[MailOlmed Facker]
Frame 14: 200 bytes on wire (16) Ethernet II, Src: VMware 5e:6a:		8 217 1 DNS 152 Standard query	(response 0 x 000 A tu berlin de A 10 150 7 60 A 172
 Internet Protocol Version 4, Sr 	15 3.556935 0.0.0.0 192.10	6.217.1 DNS 152 Standard query	response 0xc900 A tu-beriin.de A 10.150.7.09 A 172.
▹ User Datagram Protocol, Src Por QUIC IETF	▶ Frame 14: 200 bytes on wire (1600	bits), 200 bytes captured (1600 b	its) on interface ens33, id 0
 QUIC Connection information [Packet Length: 158] 	<pre>> Ethernet II, Src: VMware_5e:6a:92</pre>	(00:0c:29:5e:6a:92),	_f6:95:1c (00:50:56:f6:95:1c)
1 = Header Form: Long	Internet Protocol Version 4, Src:	192.168.217.131, Dst: 8.8.8.8	
.100 1001 = Unused: 0x49 Version: Version Negotiation	User Datagram Protocol, Src Port:	12345, Dst Port: 53	
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	Questions: 7		
Supported Version: draft-32 (Supported Version: draft-31 (Answer RRs: 0		
Supported Version: draft-30 (Supported Version: draft-29 (Authority RRs: 0		
Supported Version: Unknown (6	Additional RRs: 1		
🔴 🍸 Frame (frame), 200 bytes	• Oueries		
Frame 15: 152 bytes on wire (2)	→ tu-berlin.de: type A, class IN		
Ethernet II, Src: VMware_f6:95 Internet Protocol Version 4.	<pre>> <root>: type A, class IN</root></pre>		
• User Datagram Protocol, Src Po	\sim Root>' type A class IN		
<pre>> QUIC Connection information</pre>	\sim Root>: type A, class IN		
[Malformed Packet: QUIC] [Expert Info (Error/Malformed)	<pre>> Class IN > Class IN</pre>		
[Malformed Packet (Excepti	<pre>> ROOL>. type A, class IN > <poot>: type A, class IN</poot></pre>		
[Severity level: Error] [Group: Malformed]	<pre>> <rool>: type A, class IN</rool></pre>		
	→ <root>: TYPE A, CLASS IN</root>		
	 Additional records 		
	Root>: type Unused, class Unk	IOWN	
	[Response In: 15]		
	🔴 🍸 Frame (frame), 200 bytes		Packets: 31 · Displayed: 3 (9.7%) · Dropped: 0 (0.0%) Profile: Default











Traffic Amplification



Path amplification VS Bandwidth Amplification





Amplification Pitfalls – Minimum Path Requirements





Amplification Pitfalls – Minimum Path Requirements

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







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



Amplification Pitfalls – Reliability for Connection Migration





Amplification Pitfalls – Reliability for Connection Migration





Amplification Pitfalls – Reliability During Handshake





Amplification Pitfalls – Reliability During Handshake

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







Evaluation







Amplification Results





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!

