



ATHENE

Nationales Forschungszentrum
für angewandte Cybersicherheit

DNS-over-TCP Considered Vulnerable

Tianxiang Dai, Haya Shulman and Michael Waidner

German National Research Center for Applied Cybersecurity ATHENE
Fraunhofer Institute for Secure Information Technology SIT

Overview

- Motivation
- Evaluation in the Internet
- Potential Exploit
- Countermeasures & Conclusions

Motivation

- DNS-over-UDP is vulnerable to IP fragmentation attacks.
- What about DNS-over-TCP?

“Alternatives to IP Fragmentation: TCP with PMTUD”

---- IETF BCP WIP: IP Fragmentation Considered Fragile

“TCP is considered resistant against IP fragmentation attacks”

---- IETF BCP WIP: Fragmentation Avoidance in DNS

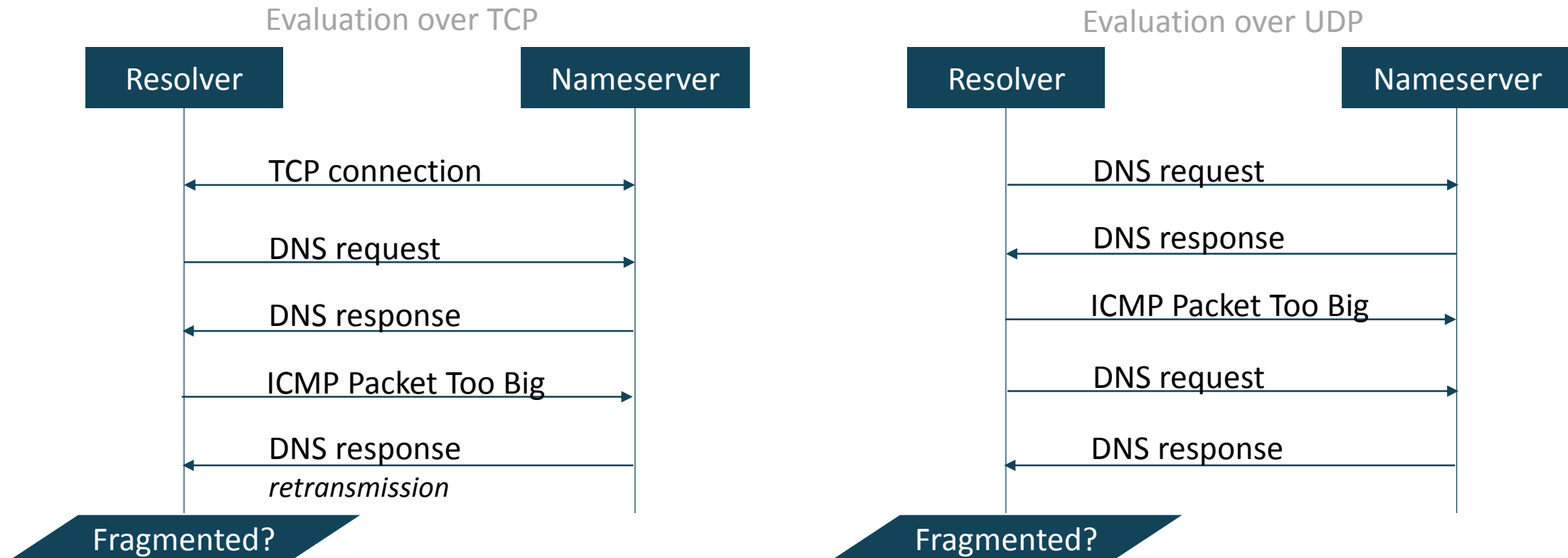
“TCP normally implements PMTUD and can avoid IP fragmentation of TCP segments.”

---- DNS Flag Day 2020

Really???

Evaluation in the Internet

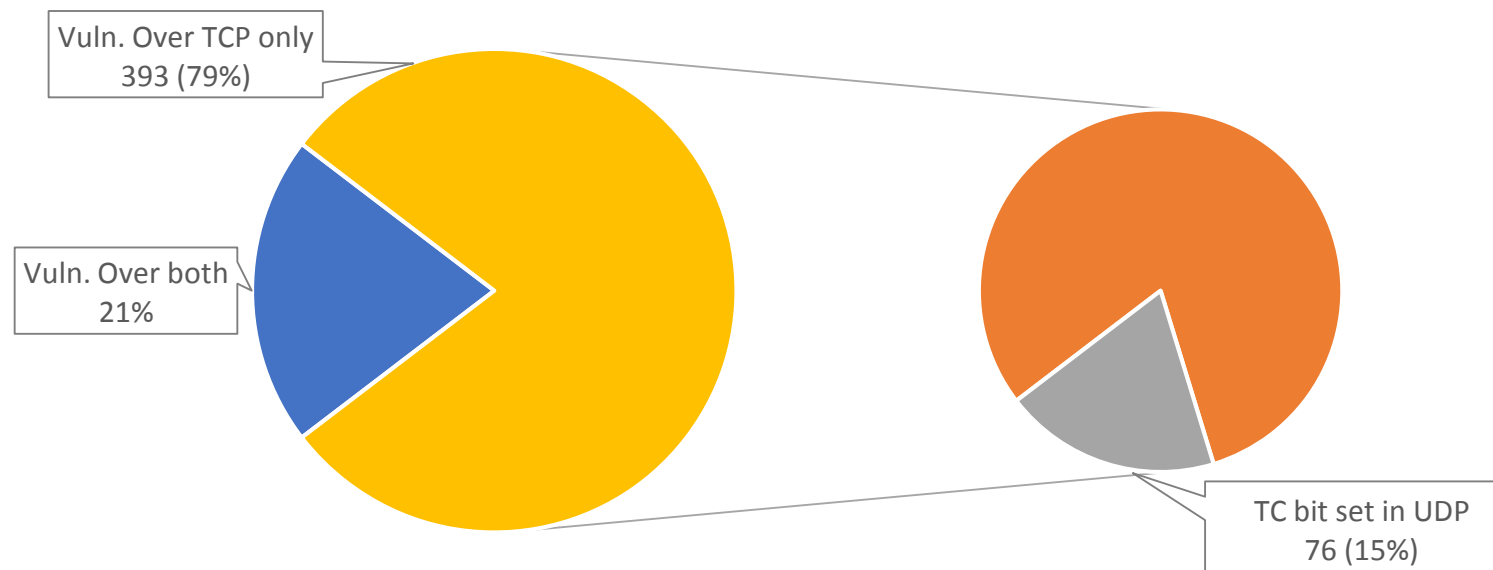
- Trigger fragmentation over TCP on nameservers in the Internet
 - Compare with UDP



Evaluation: Results

- Dataset: Alexa top 100K domains
- Fragmented:
 - **TCP: 496**
 - UDP: 9,854

Domains vulnerable to IP-fragmentation attacks over TCP



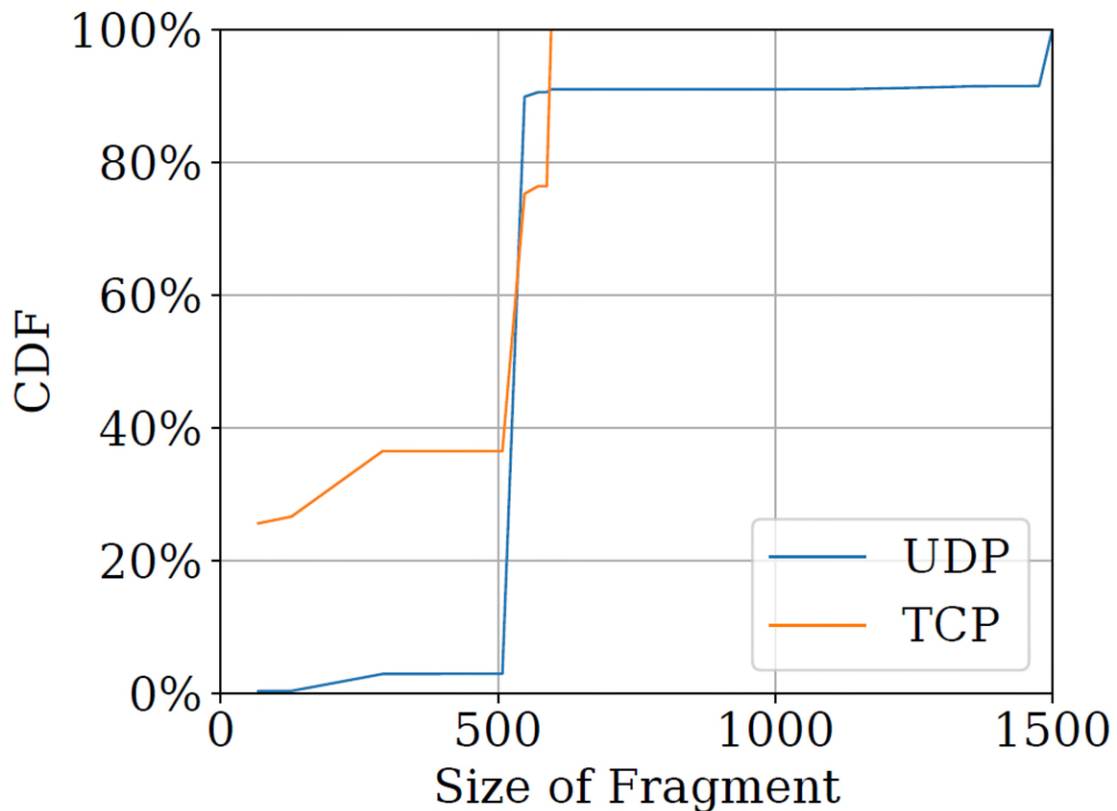
Evaluation: Results

- TCP tends to get ***smaller*** fragments than UDP
- Fragment Size:
 - **TCP: 40% \leq 292 Bytes**
 - **UDP: 90% \geq 548 Bytes**

Smaller fragments

→ More payloads injectable

→ Stronger exploits



Potential Exploit

1st Fragment

Offsets	Octet	0				1				2				3																			
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	v4		IHL = 20				TOS				Total Length																					
4	32	IPID				x DF MF				Frag Offset																							
8	64	TTL				Protocol=TCP				IP Header Checksum																							
12	96	Source IP																															
16	128	Destination IP																															
20	160	Source Port								Destination Port																							
24	192	Sequence Number																															
28	224	Acknowledgement Number																															
32	256	Data Offset				Flags				Window Size																							
36	288	Checksum								Urgent Pointer																							
40	320	DNS Length								TXID																							
44	352	DNS Flags								Question Count																							
48	384	Answer Count								Authority Count																							
52	416	Additional Count								4				v																			
56	448	i				c				t				3																			
60	480	c				o				m				0																			
64	512	Type = A								Class = IN																							

2nd Fragment

0	0	v4		IHL = 20				TOS				Total Length							
4	32	IPID				x DF MF				Frag Offset									
8	64	TTL				Protocol=TCP				IP Header Checksum									
12	96	Source IP																	
16	128	Destination IP																	
20	160	Name Pointer								Type = A									
24	192	Class = IN								TTL									
28	224	TTL								Data Length = 4									
32	256	IPv4 Address = 4.4.4.4																	
36	288																		
...	...																		

- To inject **malicious payload** into **DNS** via **IP** fragmentation over **TCP**

IP Challenge

TCP Challenge

DNS Challenge

- 2,247** domains still use **globally sequential** IPID counter for TCP!

Countermeasures & Conclusions

- Countermeasures
 - IP -- to filter (small) fragments or to randomise IPIDs
 - TCP -- to disable PMTUD and filter ICMP PTB
 - DNS -- to enable DNSSEC and configure properly
- Conclusions
 - DNS-over-TCP is still vulnerable to IP-fragmentation attacks.
 - Current recommendation of using TCP to avoid fragmentation is arguable.

Thank you!

Tianxiang Dai, Fraunhofer SIT
tianxiang.dai@sit.fraunhofer.de

תודה רבה!

çok
teşekkürler

谢谢

Merci
beaucoup!

Thank you
very much!

Dank je
wel!

Vielen
Dank!

Muchas gracias

ありがとうございました

Dziękuję!

zor spas

Grazie mille!

اشكرك