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

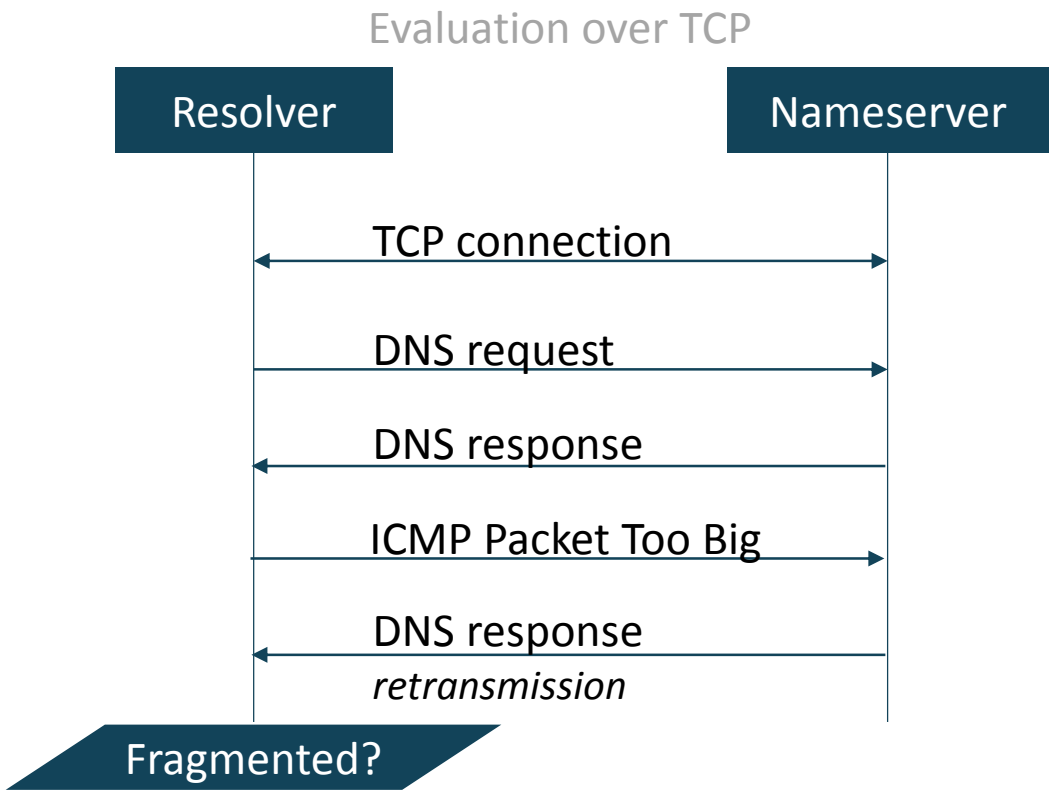
“TCP normally implements PMTUD and can avoid IP fragmentation of TCP segments.”

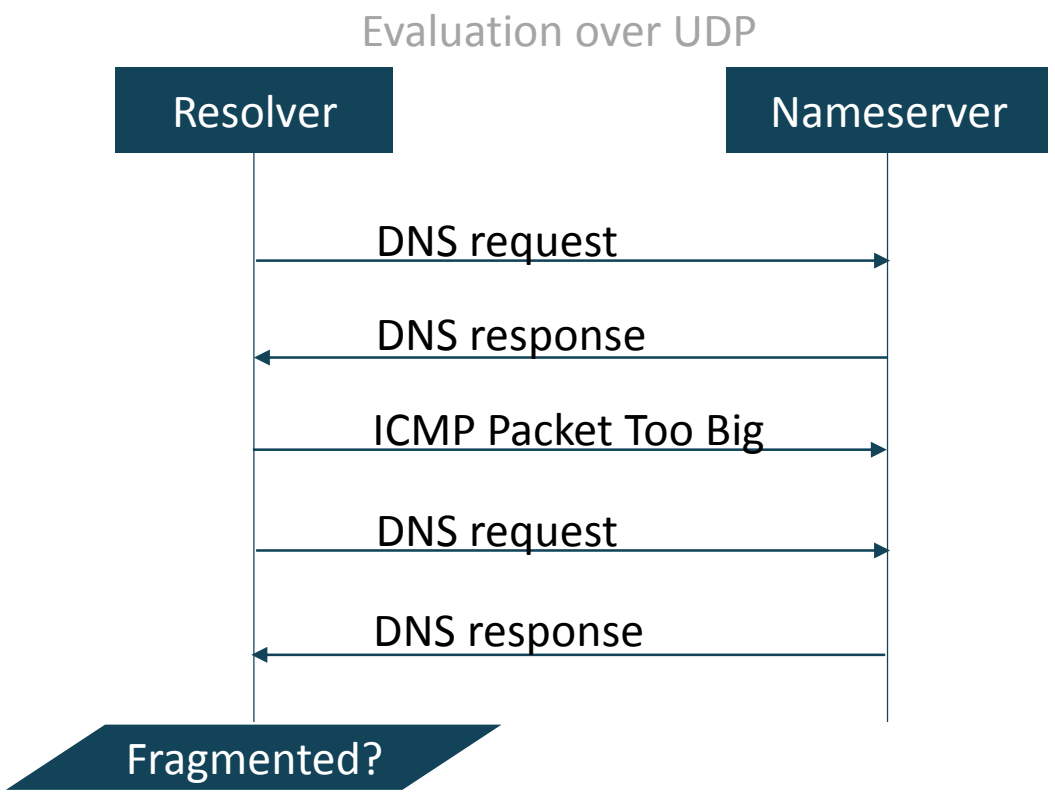
---- DNS Flag Day 2020

Really???

Evaluation in the Internet

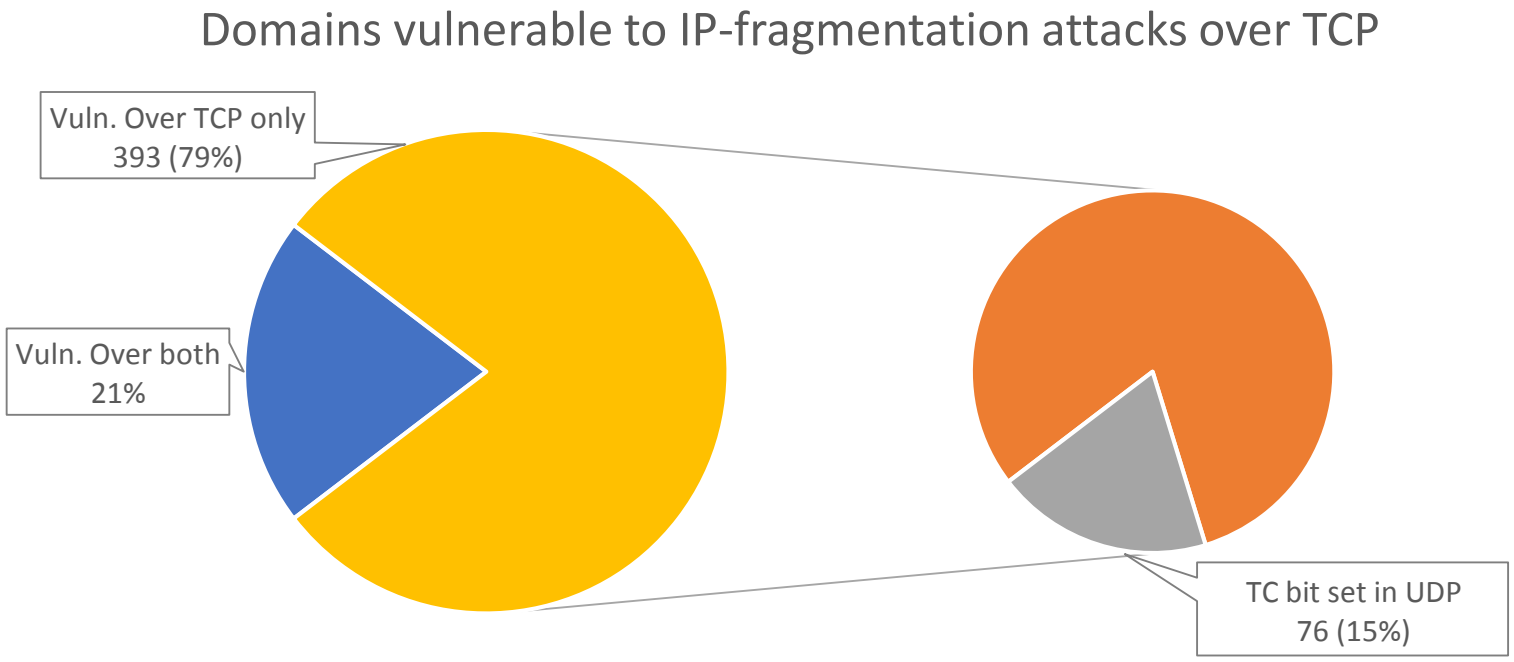
- Trigger fragmentation over TCP on nameservers in the Internet
  - Compare with UDP





Evaluation: Results

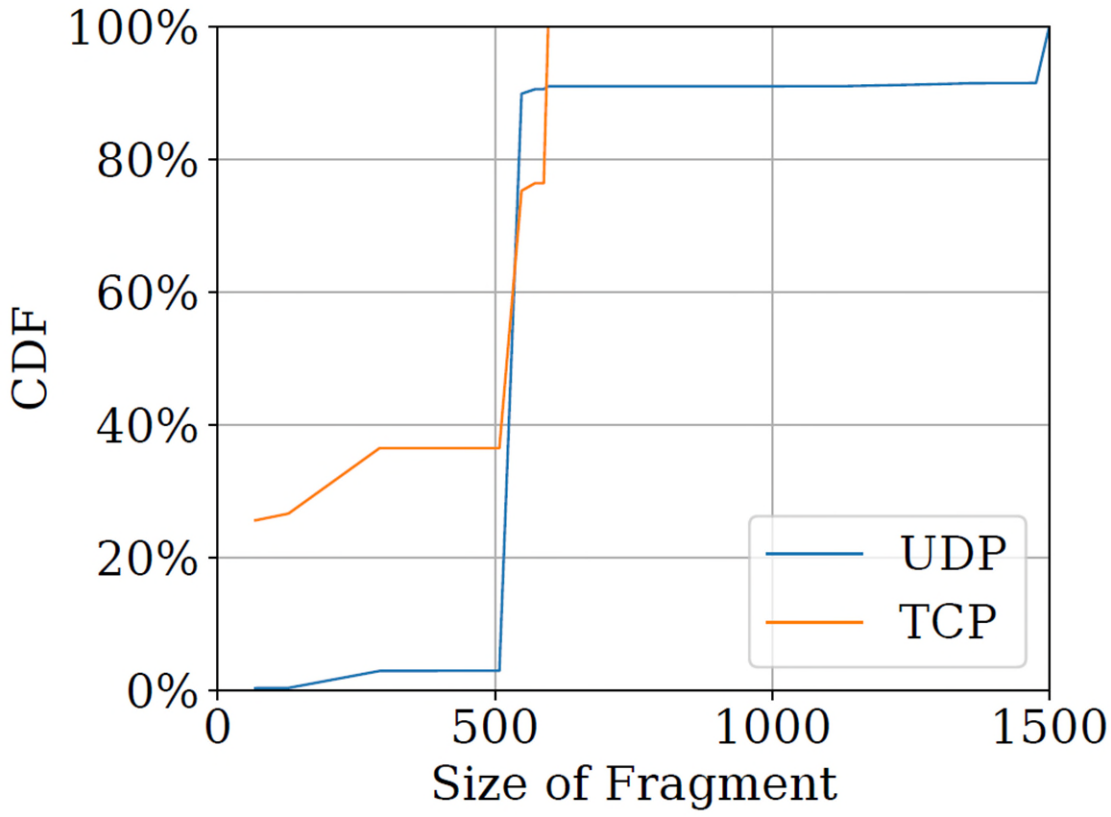
- Dataset: Alexa top 100K domains
- Fragmented:
  - **TCP: 496**
  - UDP: 9,854



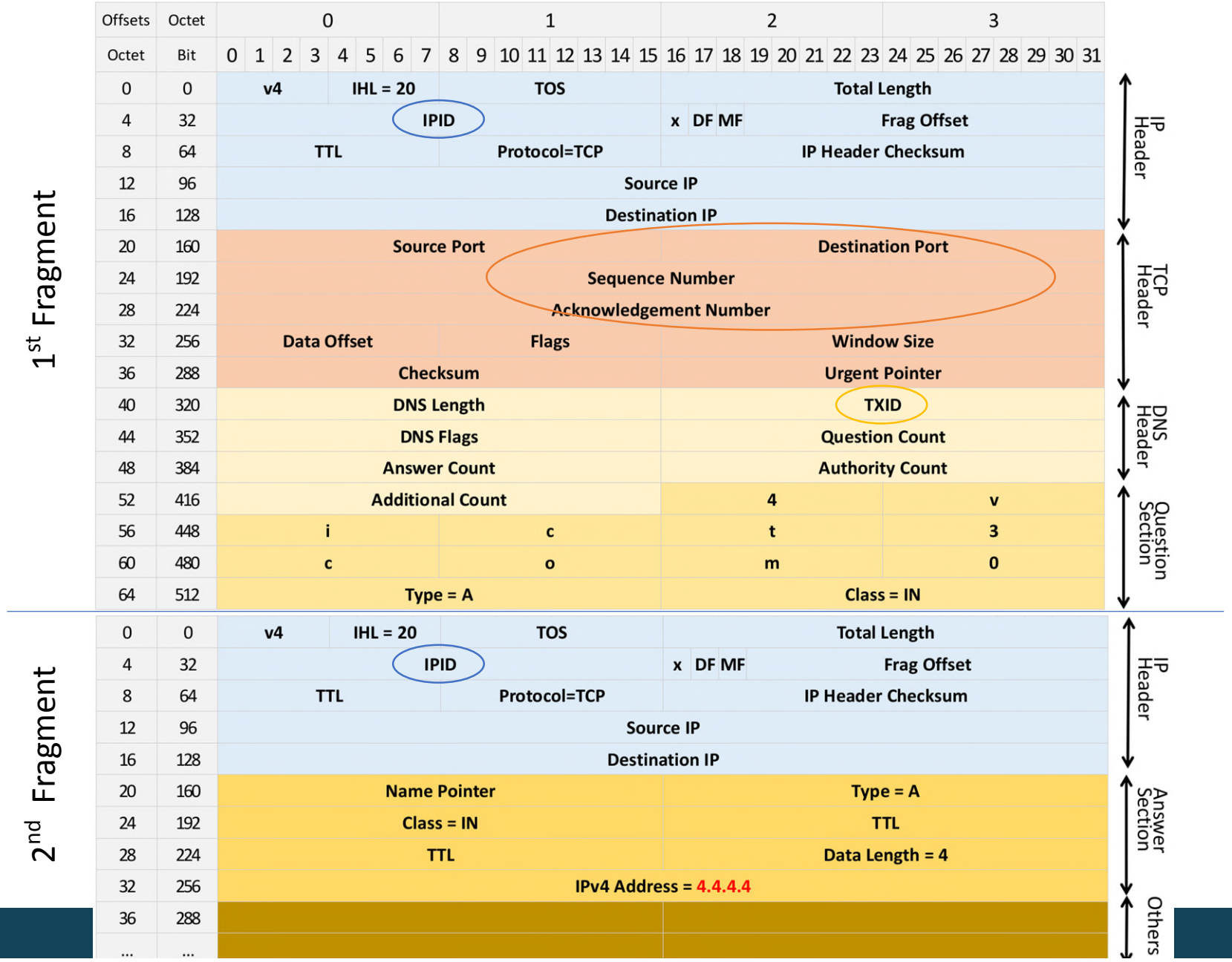
Evaluation: Results

- TCP tends to get ***smaller*** fragments than UDP
- Fragment Size:
  - **TCP: 40% <= 292 Bytes**
  - UDP: 90% >= 548 Bytes

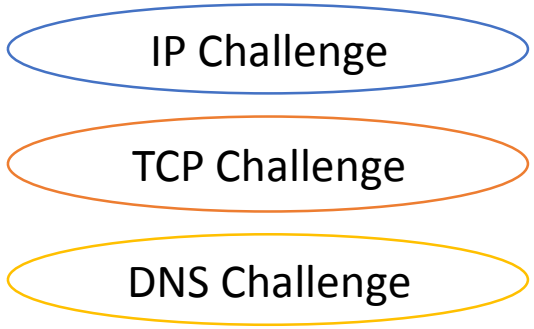
Smaller fragments
→ More payloads injectable
→ Stronger exploits



Potential Exploit



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



- **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