DOH, OR DON'T?

CARSTEN STROTMANN, DNSWORKSHOP.DE

CCCAMP 2019

Created: 2019-08-21 Wed 08:37

AGENDA

- DNS-Privacy
- DoH/DoT/DoQ
- The Dilemma
- Summary

ABOUT ME?

Carsten Strotmann

dnsworkshop.de

DNS(SEC)/DANE/DHCP/IPv6 trainer and supporter

RIPE/IETF

PRIVACY IN DNS?

- in recent years, the IETF has expanded the DNS protocol with privacy features
  - DNS-over-TLS (transport encryption between DNS client and DNS resolver)
  - DNS-over-HTTPS (transport encryption between DNS client and DNS resolver)
  - QNAME Minimization (less metadata in DNS)
  - EDNS-Padding (*hiding* of DNS data in encrypted connections)

THE NEED FOR MORE DNS PRIVACY

- a study presented at IETF 105 during the Applied Networking Research Workshop in July 2019 found that
  - 8.5 % of networks (AS) intercept DNS queries (27.9% in China)
  - (today) most queries are answered un-altered
- but the situation might change, intercept server might change DNS answers

ENCRYPTED TRANSPORT FOR DNS

- Terminology
  - Do53 = **DNS-over-Port53** - classic DNS (UDP/TCP port 53)
  - DoT = **DNS-over-TLS** - TLS as the transport for DNS
  - DoH = **DNS-over-HTTPS** - HTTPS as the transport for DNS
  - DoQ = **DNS-over-QUIC** - QUIC as the transport for DNS
  - DoC = **DNS-over-Cloud** - DNS resolution via cloud services (Google, Q9, Cloudflare ...)

PERFORMANCE OF DOT/DOH (1/2)

- with TLS 1.3 performance of DoT/DoH is quite good
- with established connections, performance can be similar to DNS-over-UDP due to
  - Pipelining
  - TCP fast open
  - 0-RTT resume
- on connections with packet loss, DoT/DoH can be faster and more reliable than Do53!
- not all implementations are fully optimized

PERFORMANCE OF DOT/DOH (2/2)

- Mozilla found that in lossy networks DoH can be faster and more reliable than Do53
- The study "Analyzing the Costs (and Benefits) of DNS, DoT, and DoH for the Modern Web" presented at Applied Networking Research Workshop July 2019 confirms that finding

DOT - DNS-OVER-TLS

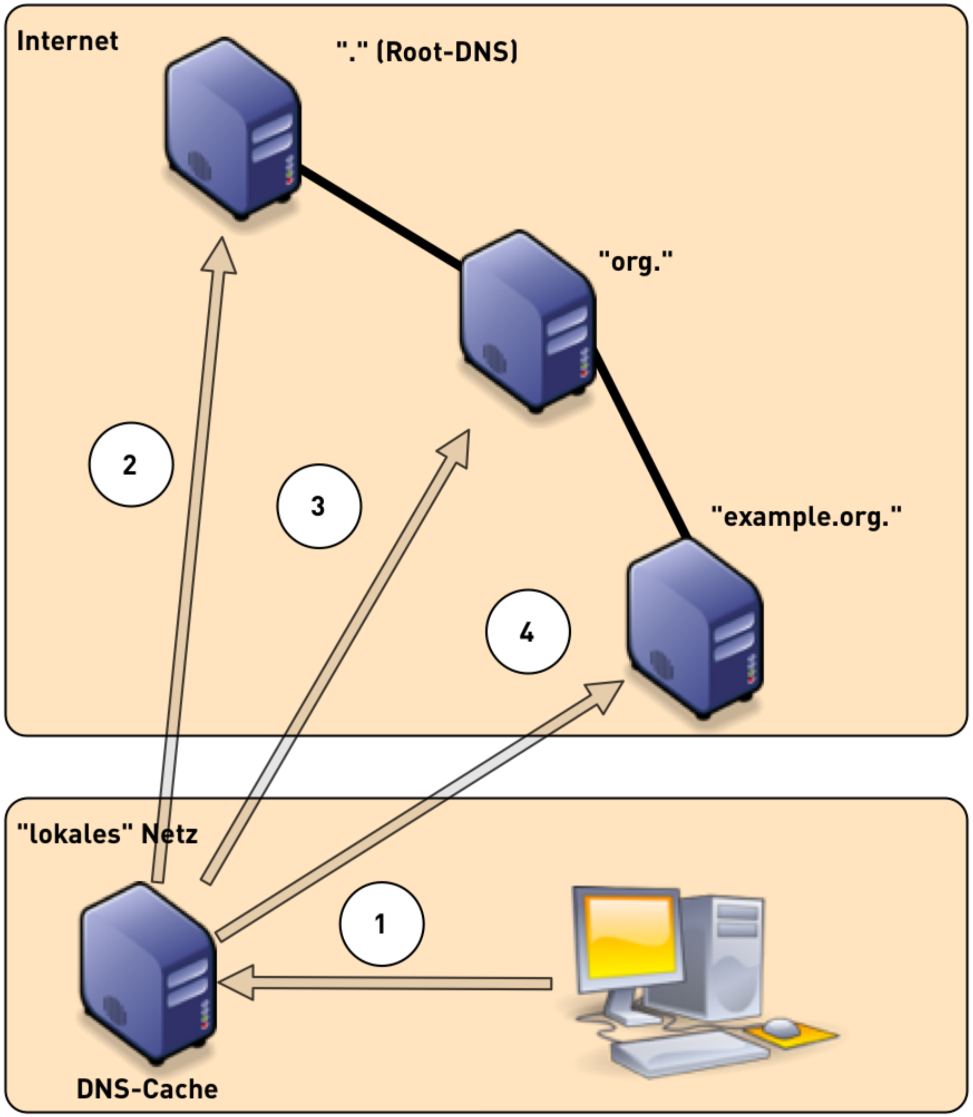
- RFC 7858 "Specification for DNS over Transport Layer Security (TLS)"
- DNS wireformat over TLS over TCP
- Port 853 (TCP)
- Encryption and Authentication (Internet PKI or via DANE)

DNS-OVER-TLS (1/3)

klassische DNS Auflösung

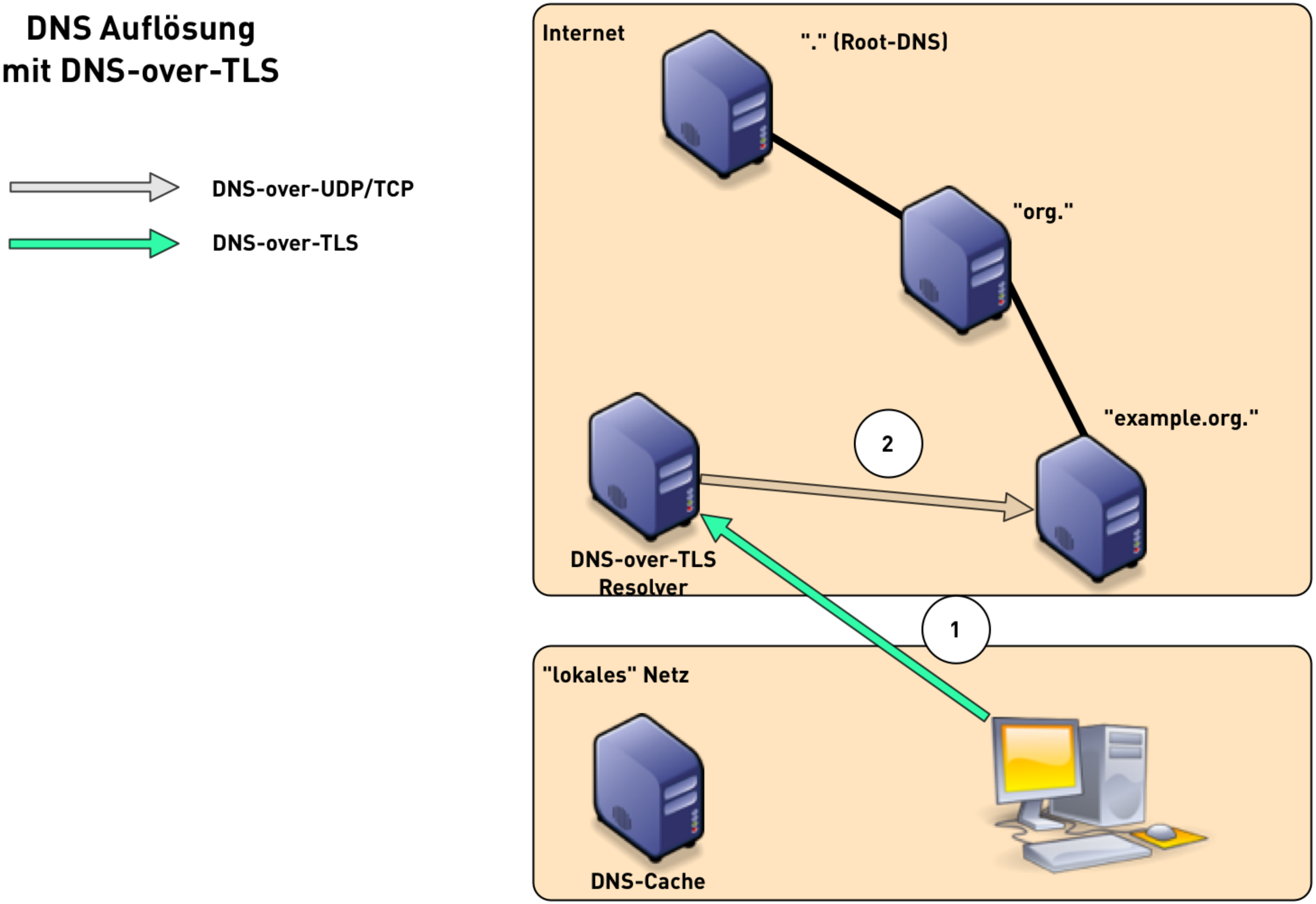
⇨ DNS-over-UDP/TCP

➡ DNS-over-TLS



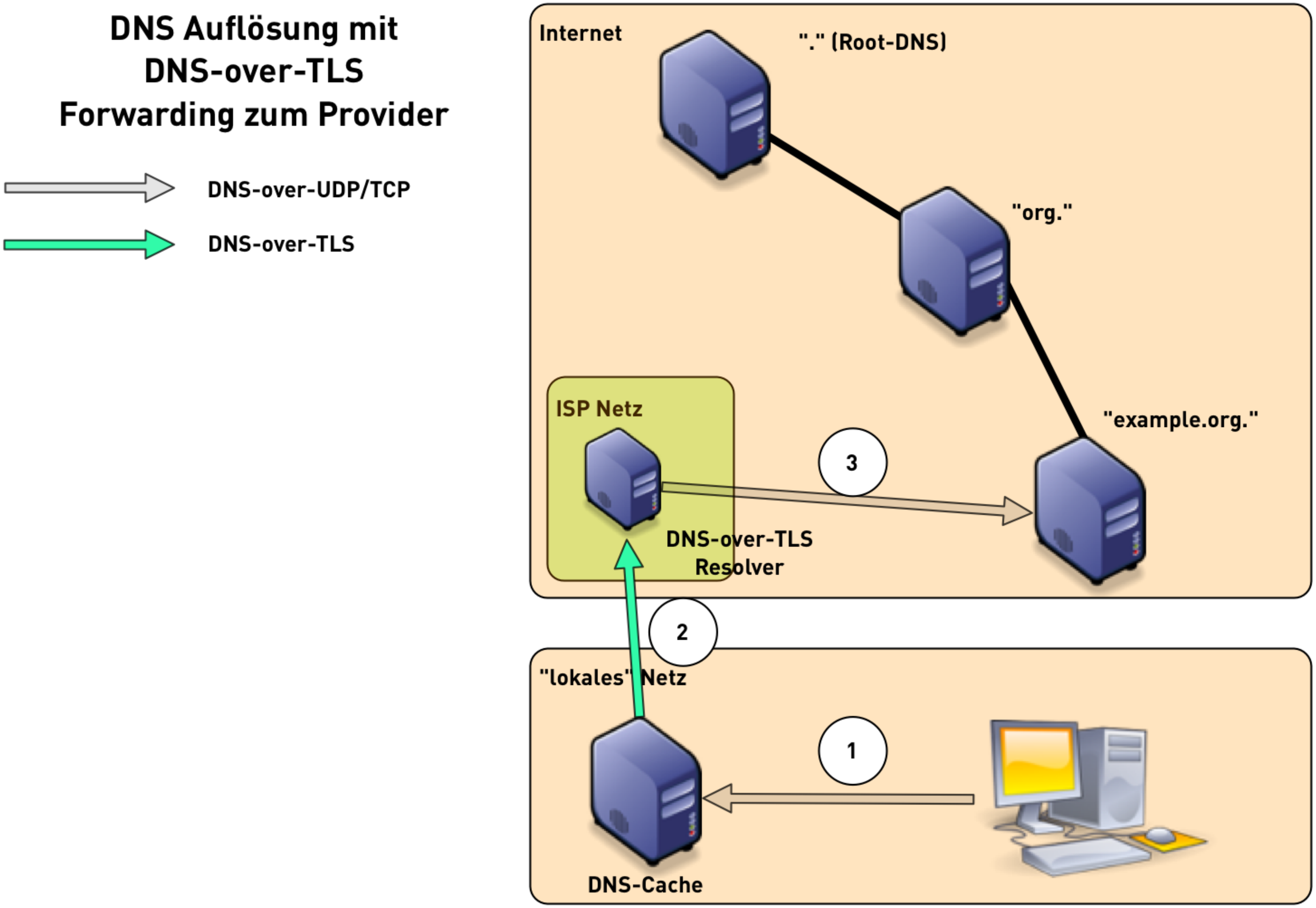
DNS-OVER-TLS (2/3)

DNS Auflösung mit DNS-over-TLS



DNS-OVER-TLS (3/3)

DNS Auflösung mit DNS-over-TLS Forwarding zum Provider



DNS-OVER-TLS MODES

- DNS-over-TLS can be operated in two modes
  - **opportunistic** - try TLS authentication, but still use server in case authentication fails
  - **strict** - only use server if there are no errors in the TLS connection

DNS-OVER-TLS OPERATORS

- Operator
  - Cloudflare/APNIC Resolver (1.1.1.1)
  - Quad9 Resolver (9.9.9.9)
  - SurfNET
  - Digitalcourage (talk to them @camp)
  - Verisign
  - Google (8.8.8.8)
  - viele unabhängige DNS-Resolver

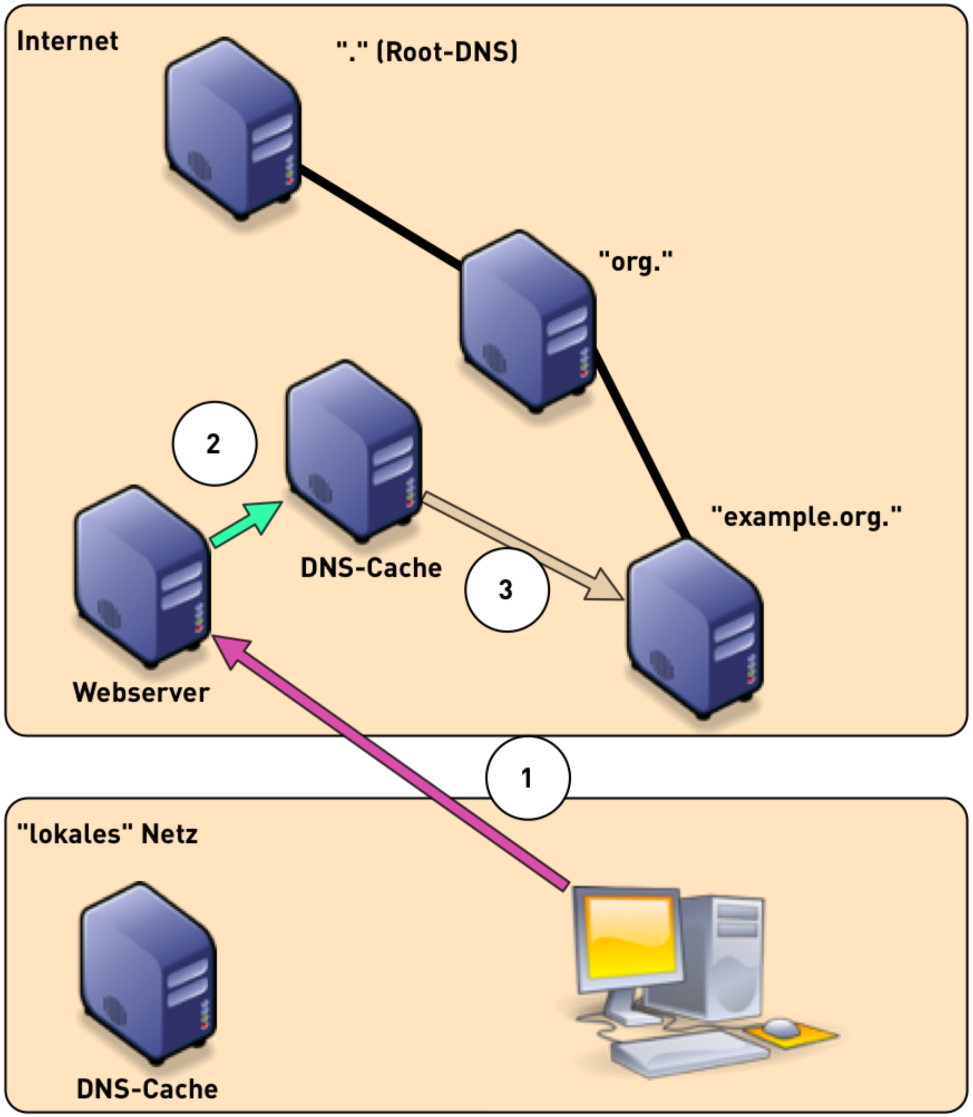
DOH - DNS OVER HTTP(S)

- RFC 8484 *DNS Queries over HTTPS (DoH)* (P. Hoffman, ICANN and P. McManus, Mozilla) https://tools.ietf.org/html/rfc8484
- DNS HTTP-Format over HTTPS over TCP, Port 443 (HTTP/2)
- URL: https://server/dns-query{?dns}"
- Encryption, Authentication and Cloaking

DOH - DNS-OVER-HTTPS

DNS Auflösung mit DNS-over-HTTPS

- ⇨ DNS-over-UDP/TCP
- 🟩 DNS-over-TLS
- 🟪 DNS-over-HTTPS



DOH TIMELINE

- IETF 100 - November 2017 - *DNS over HTTP(S)* (DoH) workinggroup started: https://datatracker.ietf.org/wg/doh/about/
- IETF 101 - March 2018 - work on *DNS Queries over HTTPS* finished, start of *working group last call* (WGLC) in April 2018
- October 2018 - RFC 8484 published

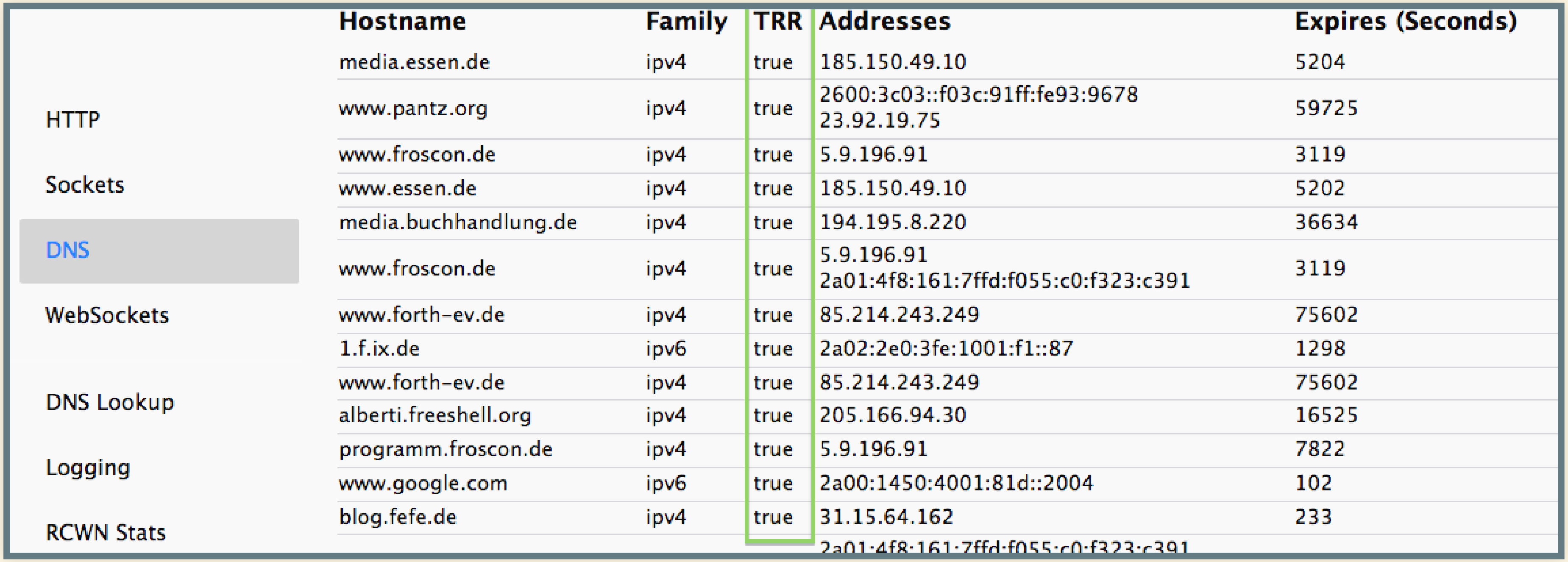
DNS-OVER-HTTPS AND IDS/NETWORK-FILTER

Quote from RFC 8484:

> *Operational Considerations […] Filtering or inspection systems that rely on unsecured transport of DNS will not function in a DNS over HTTPS environment due to the confidentiality and integrity protection provided by TLS.*

DOH IN FIREFOX (1/3)

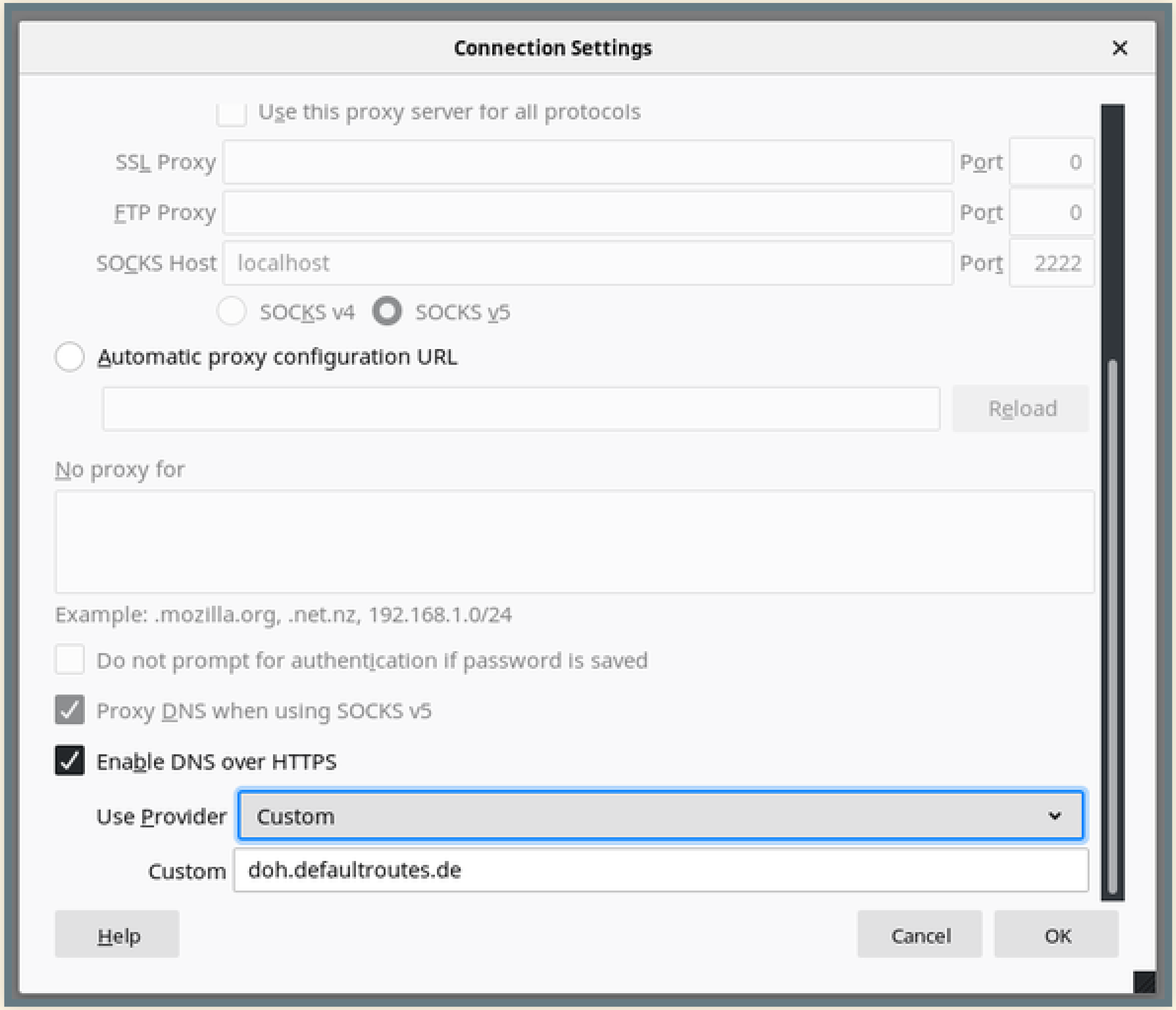
- Firefox 61+ (manual switch)
- Firefox TRR Konfigurations Optionen



Hostname	Family	TRR	Addresses	Expires (Seconds)
media.essen.de	ipv4	true	185.150.49.10	5204
www.pantz.org	ipv4	true	2600:3c03::f03c:91ff:fe93:9678 23.92.19.75	59725
www.froscon.de	ipv4	true	5.9.196.91	3119
www.essen.de	ipv4	true	185.150.49.10	5202
media.buchhandlung.de	ipv4	true	194.195.8.220	36634
www.froscon.de	ipv4	true	5.9.196.91 2a01:4f8:161:7ffd:f055:c0:f323:c391	3119
www.forth-ev.de	ipv4	true	85.214.243.249	75602
1.f.ix.de	ipv6	true	2a02:2e0:3fe:1001:f1::87	1298
www.forth-ev.de	ipv4	true	85.214.243.249	75602
alberti.freeshell.org	ipv4	true	205.166.94.30	16525
programm.froscon.de	ipv4	true	5.9.196.91	7822
www.google.com	ipv6	true	2a00:1450:4001:81d::2004	102
blog.fefe.de	ipv4	true	31.15.64.162	233
			2a01:4f8:161:7ffd:f055:c0:f323:c391	

DOH IN FIREFOX (2/3)

- Firefox Quantum (Screenshot FF 68)



Connection Settings

□ Use this proxy server for all protocols

SSL Proxy Port 0

FTP Proxy Port 0

SOCKS Host localhost Port 2222

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

□ Do not prompt for authentication if password is saved

☑ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

Use Provider Custom

Custom doh.defaultroutes.de

DOH IN FIREFOX (3/3)

- Mozilla plans to enable DoH in Firefox by default in the future. No date announced.
- User can select among a list of **certified** DoH operators per "region"
- operators of DoH services can apply for privacy certification
- *Mozilla Policy Requirements for DNS over HTTPs Partners*: https://wiki.mozilla.org/Security/DOH-resolver-policy

DOH IN GOOGLE CHROME

- currently, DoH can be enabled in Chrome via commandline switches https://judge.sh/how-to-enable-dns-over-https-on-chrome-right-now/
- a GUI configuration is coming with Chrome Version 78
- Google has no plans to enable DoH by default

DOH OPERATORS (SELECTION)

- Cloudflare https://cloudflare-dns.com/dns-query
- Cloudflare/Mozilla https://mozilla.cloudflare-dns.com/dns-query
- Clean Browsing https://doh.cleanbrowsing.org/doh/family-filter/
- PowerDNS https://doh.powerdns.org
- BlahDNS (de) https://doh.de.blahdns.com/dns-query
- SecureDNS https://doh.securedns.eu/dns-query

DOT VS DOH

- differences between DoT and DoH
    - DoT can be easily blocked, because it is running on an dedicated port (853)
    - DoH is made to look like normal HTTPS traffic, selective blocking of DoH is difficult
    - DoH seems to be easier to implement, because of existing HTTPS library functions in programming languages
    - DoH enables developers to do DNS name resolution on an application level, which some people think is bad

THE DOH DILEMMA

- to reach the Internet users that are in need of privacy, DoH needs to be enabled by default
    - DoH Server selection can be seen as similar to the CA selections browsers do
- a fixed selection "per region" will (still) lead to centralization of all DNS queries with a few DNS operators
    - but that might still be the case even without DoH, some countries in Asia send > 90% of DNS queries to DoC (Google)

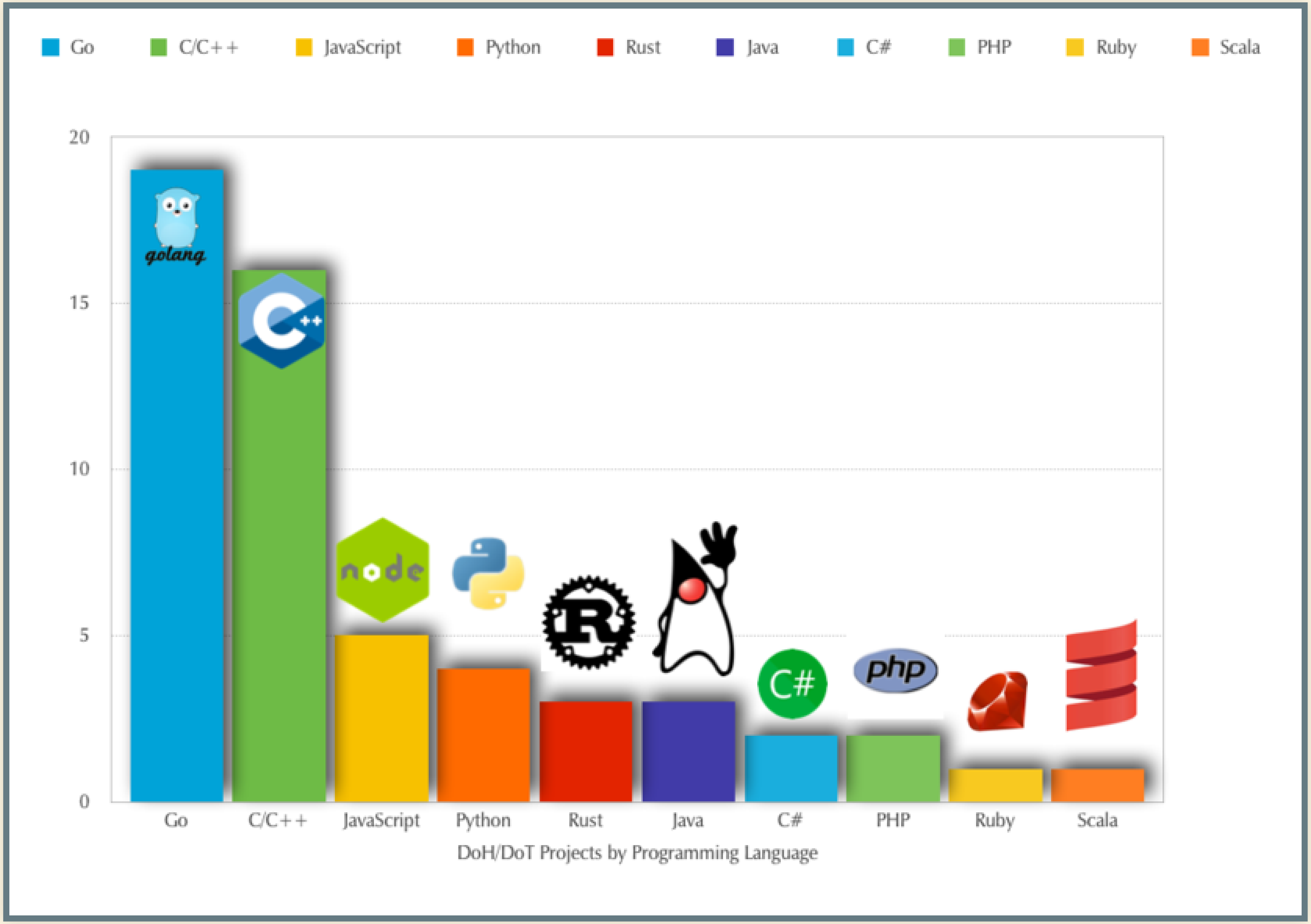
DOH AND DOT SOFTWARE - ONLY BROWSER?

- new DNS privacy protocols sparked a large number of new software projects
- this part of the presentation will look at
  - comparison of the start of new software projects in comparison to the new standards
  - number of projects for DNS-over-HTTPS vs. DNS-over-TLS
  - programming languages used to implement the new protocols

THE SURVEY

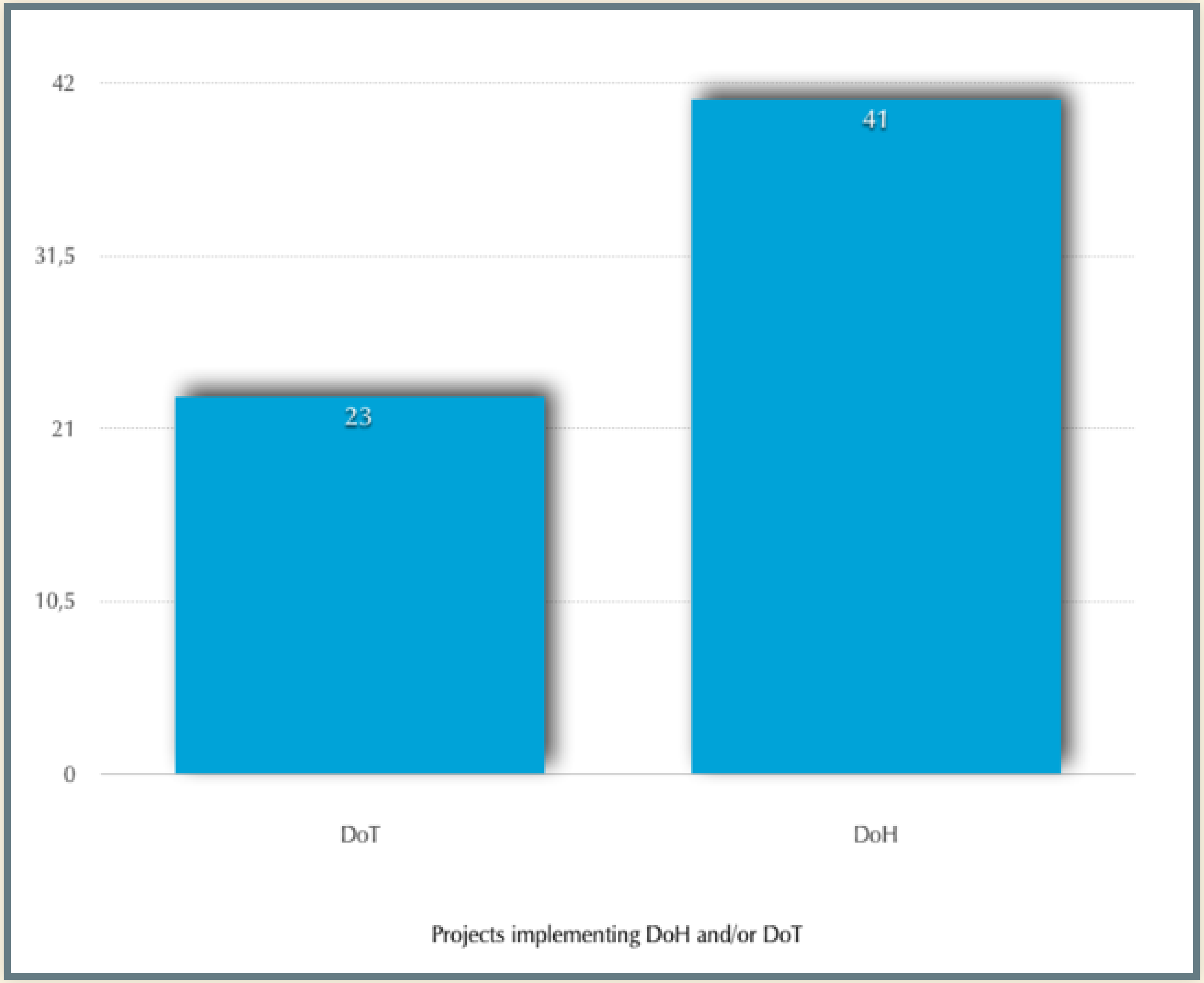
- looked at 55 DoT/DoH open source software projects on Github and Gitlab
- done in May 2019 and June 2019
- only software products, no composition projects (Docker Container etc)
- full list: https://doh.defaultroutes.de/implementations.html
- see presentation at RIPE 78 and recent blog post in the APNIC blog (linked from the page above)

LANGUAGES


Go
C/C++
JavaScript
Python
Rust
Java
C#
PHP
Ruby
Scala
20
15
10
5
0
golang
node
php
C#
Go
C/C++
JavaScript
Python
Rust
Java
C#
PHP
Ruby
Scala
DoH/DoT Projects by Programming Language

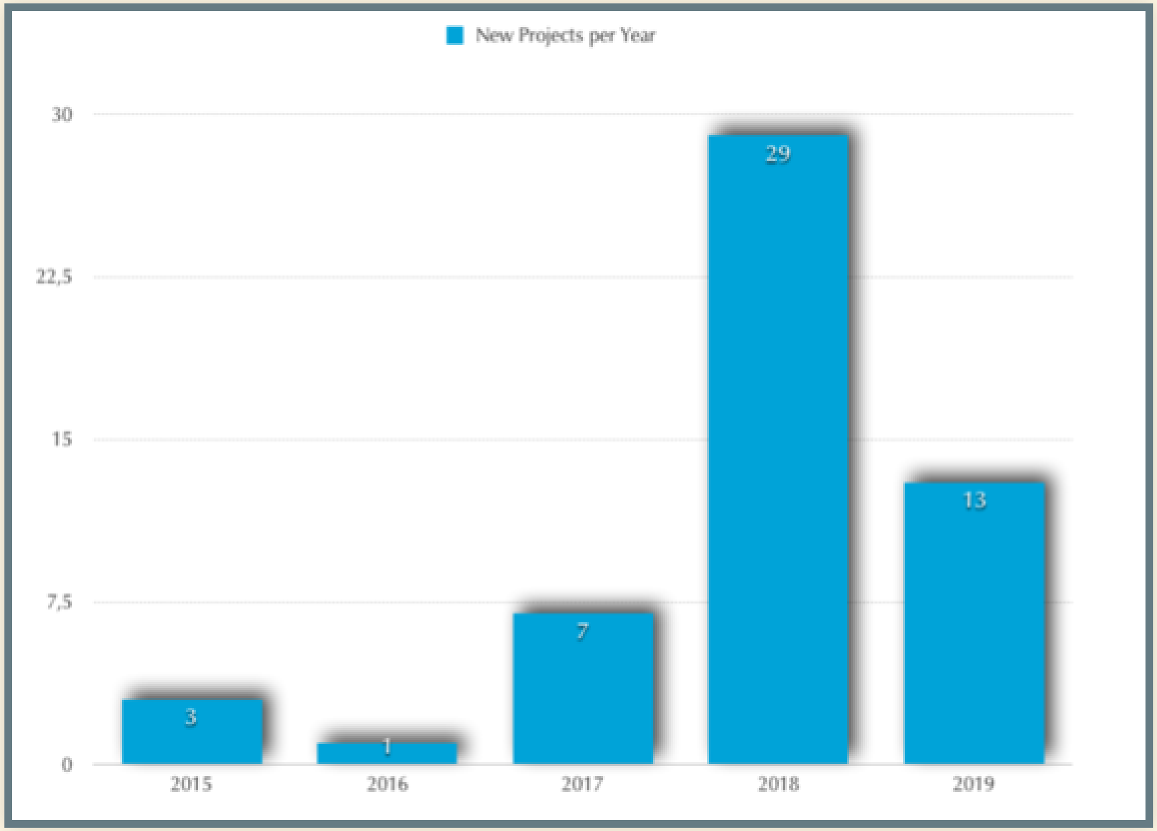
DOT VS DOH

Which protocols are implemented. Some projects implement both:


42
31,5
21
10,5
0
23
41
DoT
DoH
Projects implementing DoH and/or DoT

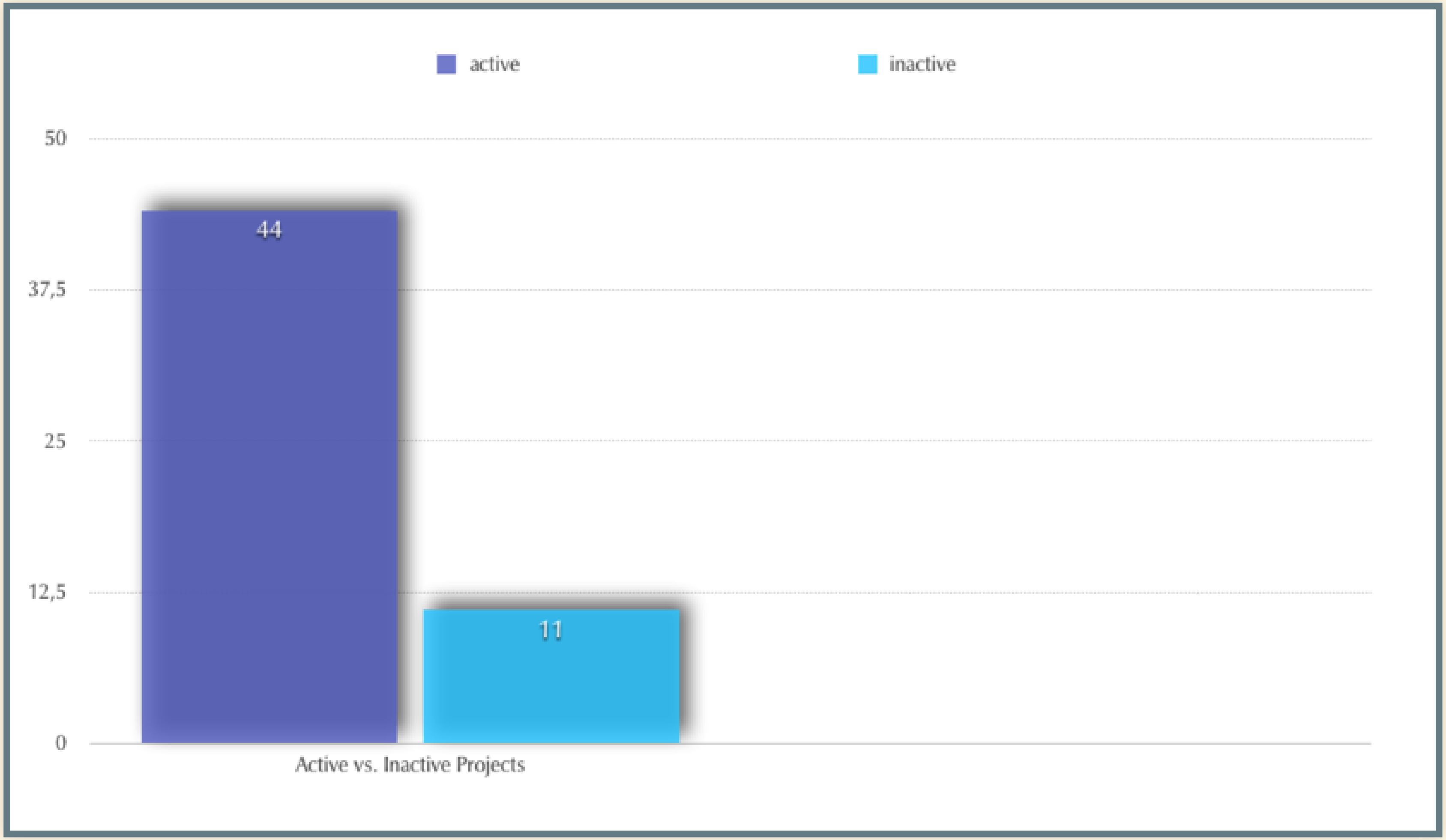
PROJECT START

Year of the first commit, frist release or when DoH/DoT functions were implemented



FRESHNESS

Activity in the project in the last 6 month?



APPLICATIONS

- Firefox
- Chrome
- curl
- Tenta-Browser
- Bromite

SYSTEM RESOLVER

- systemd-resolved
- unwind
- resolver module for Linux glibc

CLIENT-PROXIES

- sdns
- dnscrypt-proxy2
- veild
- stubby
- unbound
- cloudflared
- Dohnut
- dns-over-https

SERVER-PROXIES

- rust-doh
- dnsdist
- dns-over-https

SERVER

- unbound
- Knot
- sdns

WHATS MISSING IN DOH/DOT SOFTWARE

- certificate authentication via DANE
- Wittness function - query multiple provider and compare response data
- security audits of DoH/DoT software

DNS OVER QUIC - THE FUTURE OF DNS?

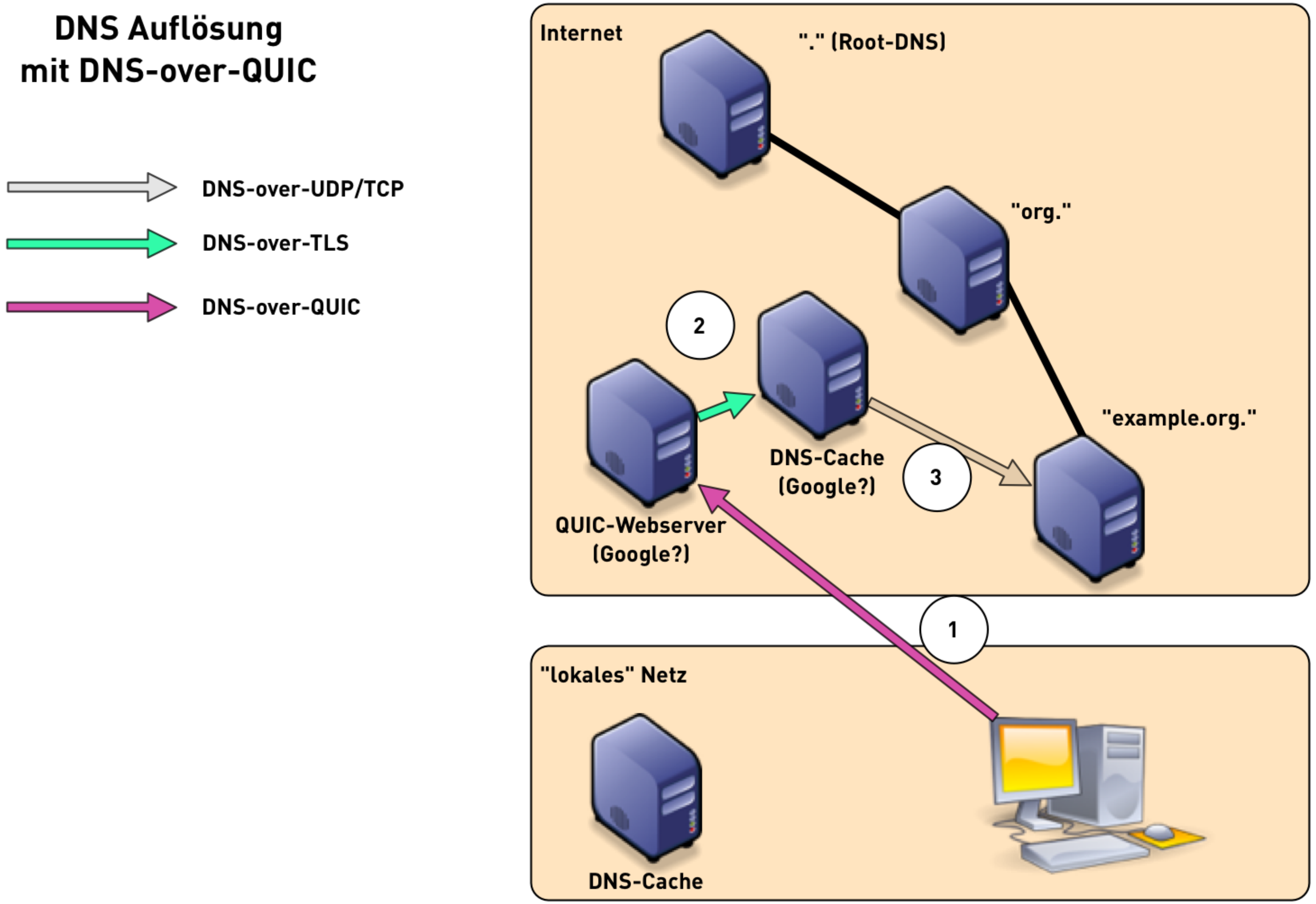
- DNS over QUIC over UDP
- *Specification of DNS over Dedicated QUIC Connections* https://tools.ietf.org/html/draft-huitema-quic-dnsoquic

WHAT IS QUIC

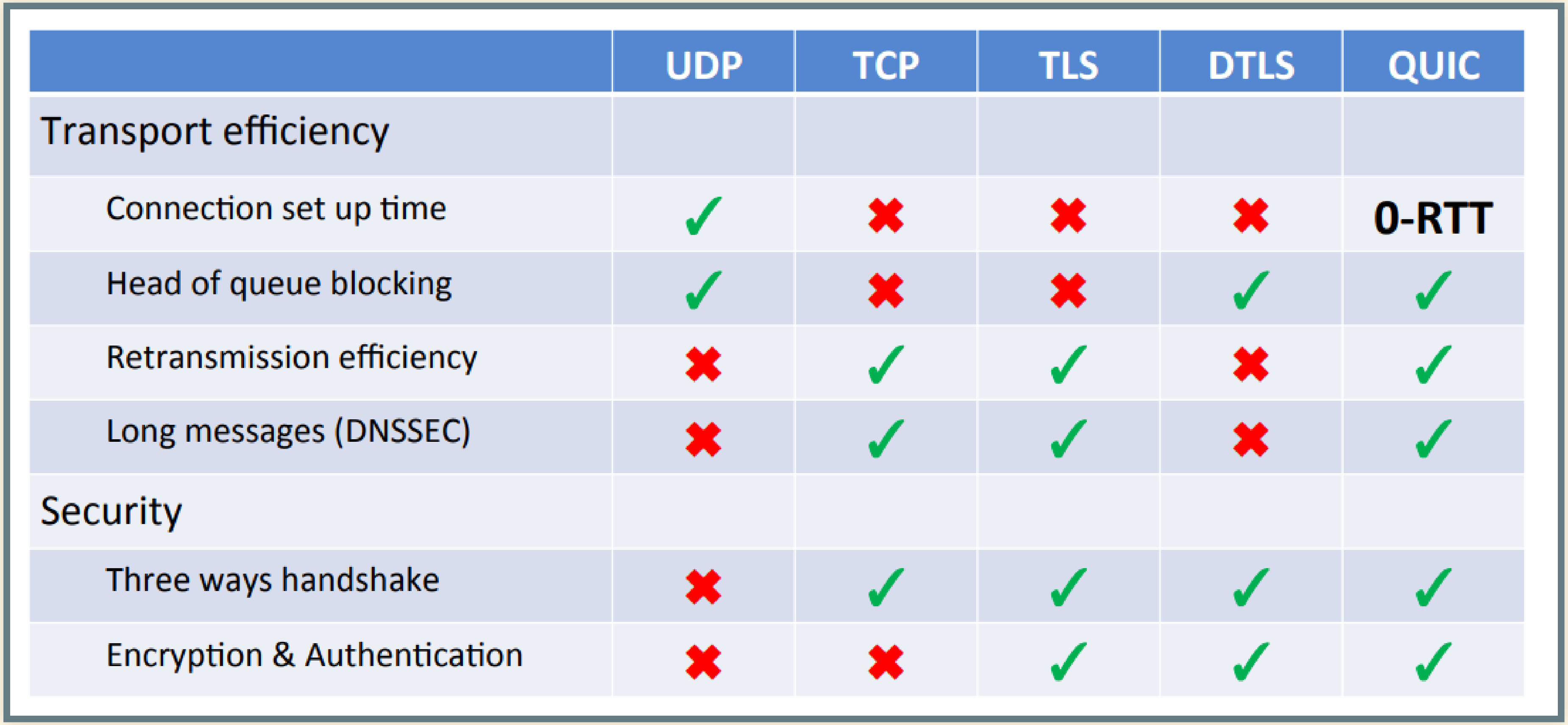
- modern TCP replacement from Google, being currently standardized in the IETF
    - based on UDP, implements TCP features
    - implemented as part of the application, not the OS
    - includes TLS 1.3
    - 0-RTT
- DoQ similar to Do53 (DNS-over-UDP)
- QUIC IETF WG documents https://tools.ietf.org/wg/quic/

DNS OVER QUIC

DNS Auflösung mit DNS-over-QUIC



DNS OVER QUIC COMPARISION



	UDP	TCP	TLS	DTLS	QUIC
Transport efficiency					
Connection set up time	✓	✖	✖	✖	0-RTT
Head of queue blocking	✓	✖	✖	✓	✓
Retransmission efficiency	✖	✓	✓	✖	✓
Long messages (DNSSEC)	✖	✓	✓	✖	✓
Security					
Three ways handshake	✖	✓	✓	✓	✓
Encryption & Authentication	✖	✖	✓	✓	✓

Figure 12: Source:
https://datatracker.ietf.org/meeting/99/materials/slides-

99-dprive-dns-over-quic

SUMMARY (1/2)

- the DNS protocol is evolving fast these days
  - too fast? (see “The DNS Camel”, or, the rise in DNS complexity and RFC 8324 *DNS Privacy, ...: Time for Another Look?*)
- in the future, DNS communication between client and resolver will be encrypted (DNS-over-TLS, DNS-over-HTTPS, DNS-over-QUIC)
- DNS-over-HTTPS/QUIC has potential for centralization or de-centralization

SUMMARY (2/2)

- what can be done?
  - operate DoH or DoT server (responsibly)
  - hack on DoH/DoT software (security audit, "witness" function)
  - bring DoH/DoT into open source operating systems
  - use DoH/DoT and provide feedback to the projects
  - engage with the IETF
  - deploy DNSSEC

THANK YOU

Discussion (@Digitalcourage)

Contact: `cstrotm@dnsworkshop.de`

LINKS

- Passive DNS Replication https://www.first.org/conference/2005/papers/florian paper-1.pdf
- RFC 7858 "Specification for DNS over Transport Layer https://tools.ietf.org/html/rfc7858
- DNS-over-TLS in Android 9
  - https://www.heise.de/security/meldung/Android-P- DNS-Anfragen-4027745.html
  - https://security.googleblog.com/2018/04/dns-over- android-p.html
  - https://android-review.googlesource.com/q/topic:dn

    (status:open+OR+status:merged)

- DNS-over-TLS implementations https://doh.defaultroutes.de/implementations.html
- DNS-over-TLS operator (selection)
    - Cloudflare/APNIC https://developers.cloudflare.com over-tls/
    - Quad9 Resolver https://www.quad9.net/
    - SurfNET https://dnsprivacy.org/wiki/display/DP/DNS+Privac
    - Verisign https://dnsprivacy.org/wiki/display/DP/DNS+Privac
- DNS over HTTPS
    - DNS-over-HTTPS RFC 8484 https://tools.ietf.org/ht
    - Google DNS-over-HTTPS Dienst

    - https://developers.google.com/speed/public-dns/do
      https
    - OpenResolve https://www.openresolve.com/
    - DinGO https://github.com/pforemski/dingo
    - CoreDNS https://coredns.io/2016/11/26/dns-over-
- DNS-over-QUIC
    - IETF Draft https://tools.ietf.org/html/draft-huitema-
    - QUIC Documents https://tools.ietf.org/wg/quic/
- Is the DNS evolving to fast?
    - “The DNS Camel”, or, the rise in DNS complexity https://blog.powerdns.com/2018/03/22/the-dns-ca rise-in-dns-complexit/
    - RFC 8324 - DNS Privacy, … Time for Another Look? https://tools.ietf.org/html/rfc8324

- July 2019 ANRW Workshop (Videos and Proceedings) https://irtf.org/anrw/2019/program.html
- Who Is Answering My Queries:Understanding and Cha Interception of the DNS Resolution Path http://delivery.acm.org/10.1145/3350000/3341122/p
- Analyzing the Costs (and Benefits) of DNS, DoT, and D Modern Web https://irtf.org/anrw/2019/program.htm