Survey of the (Open Source) DNS Privacy Landscape

MEN&MICE

RIPE78 Reykjavik

Carsten Strotmann

About Men & Mice

Men & Mice provides API-driven DNS, DHCP and IPAM software solutions to global enterprise, education and government organizations for effective management, visibility, control, automation and security of complex, hybrid IP infrastructure. Network Managers at some of the world's largest organizations rely on Men & Mice to increase network portability and adapt to changing network needs.

MEN&MICE

DNS privacy software

- new DNS privacy protocols sparked a large number of new software projects
  - and much debate in the IETF and the larger DNS community

DNS privacy software

- this talk will visit the software side of these new protocols
  - 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

DNS Privacy Protocols - a short refresher

- DNS queries and responses are used to spy on users
- DNS traffic is being altered "on the transport"
- DNS queries are blocked to implement censorship

DNS Privacy Protocols - a short refresher

- two new protocols have been developed in the IETF
  - DNS-over-TLS (RFC 7858)
  - DNS-over-HTTPS (RFC 8484)

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

`https://tools.ietf.org/html/rfc7858`

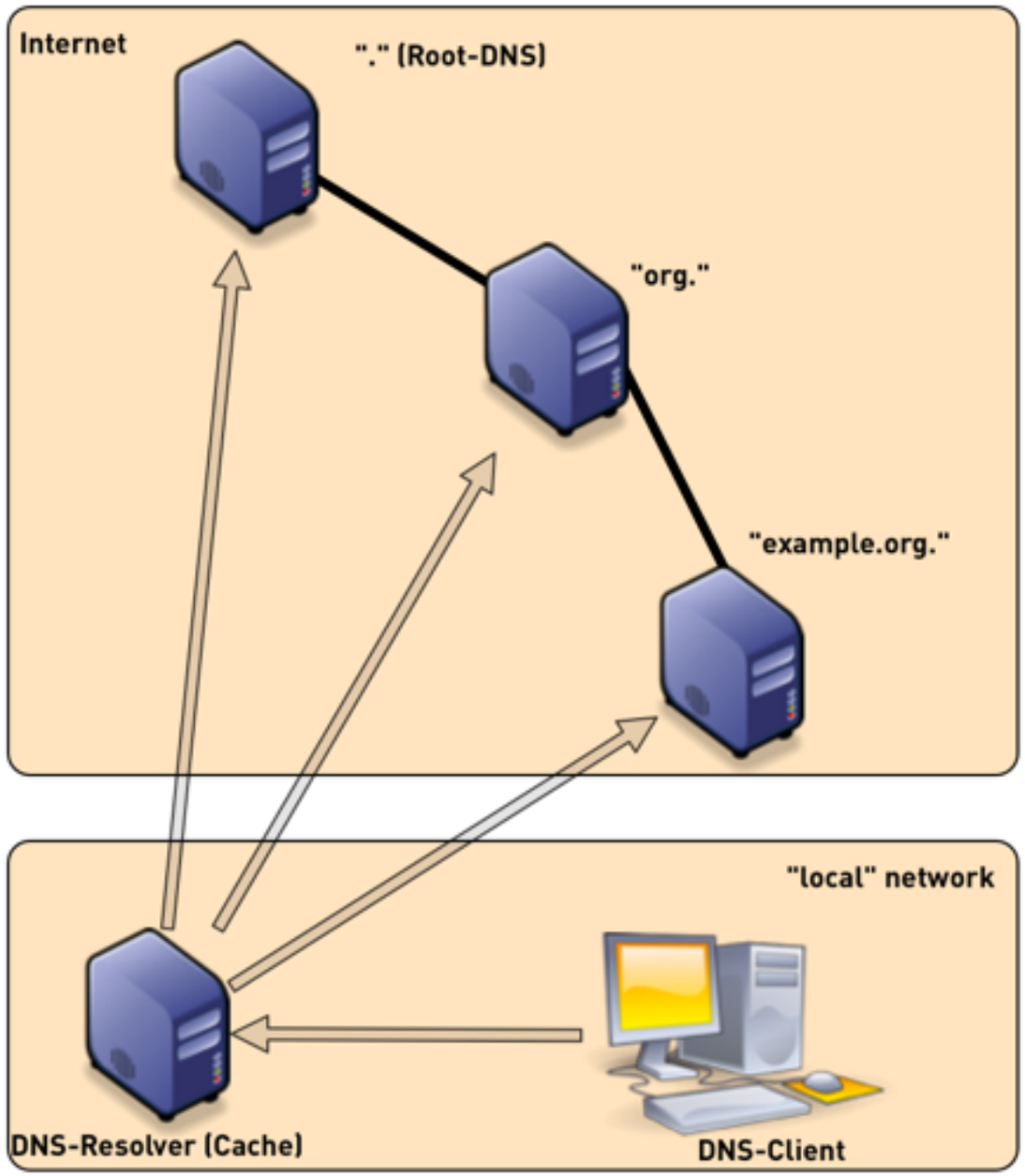
DoH - DNS over HTTP(S)

- RFC 8484 "DNS Queries over HTTPS (DoH)"
  - DNS HTTP-Format over HTTPS over TCP, Port 443 (HTTP/2)
  - Port 443 (TCP)
  - Encryption and authentication

`https://tools.ietf.org/html/rfc8484`

Classic DNS resolution (UDP/TCP)

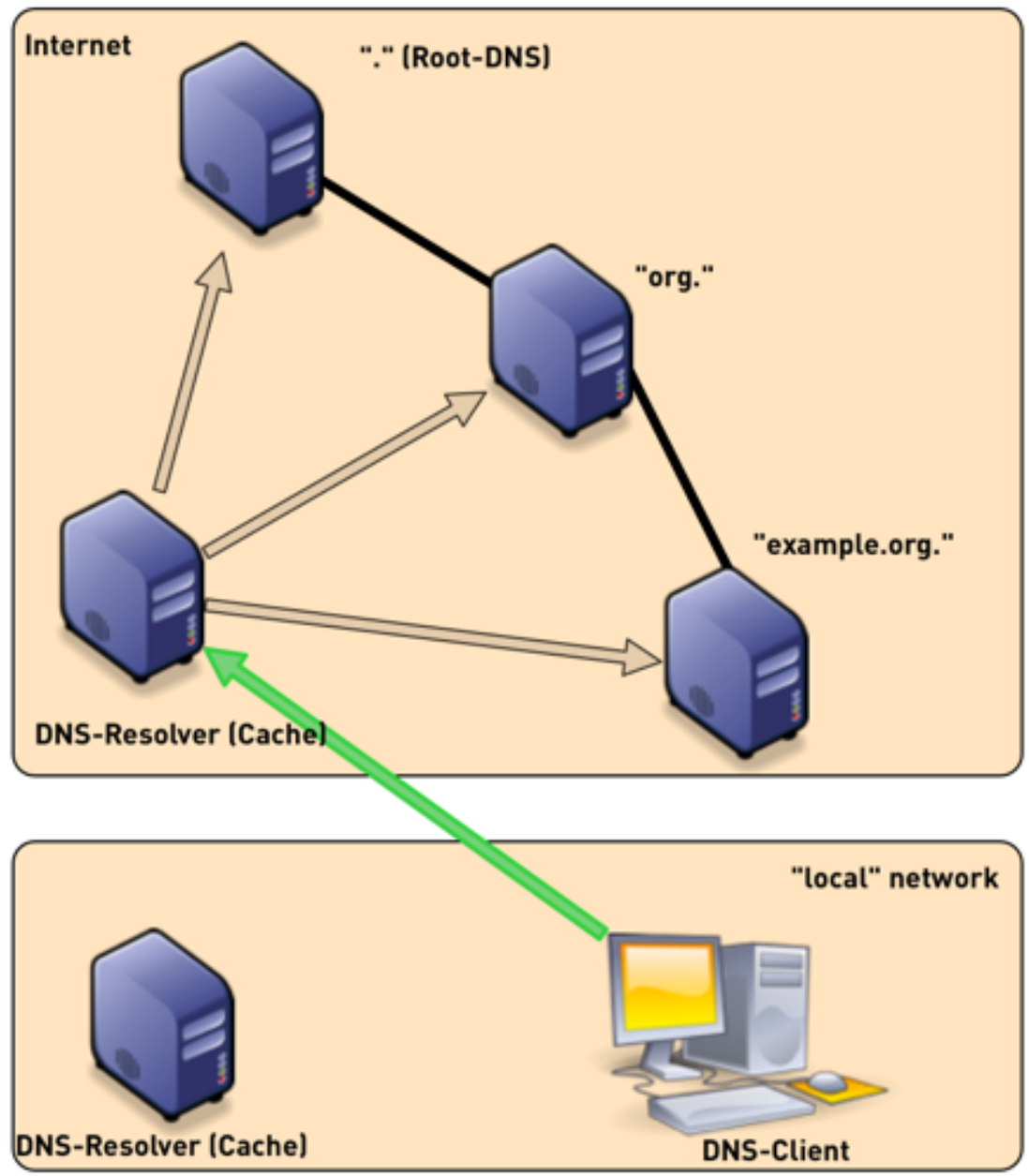
all communication unencrypted and open



classic DNS via UDP/TCP

DoH/DoT DNS resolution (TLS)

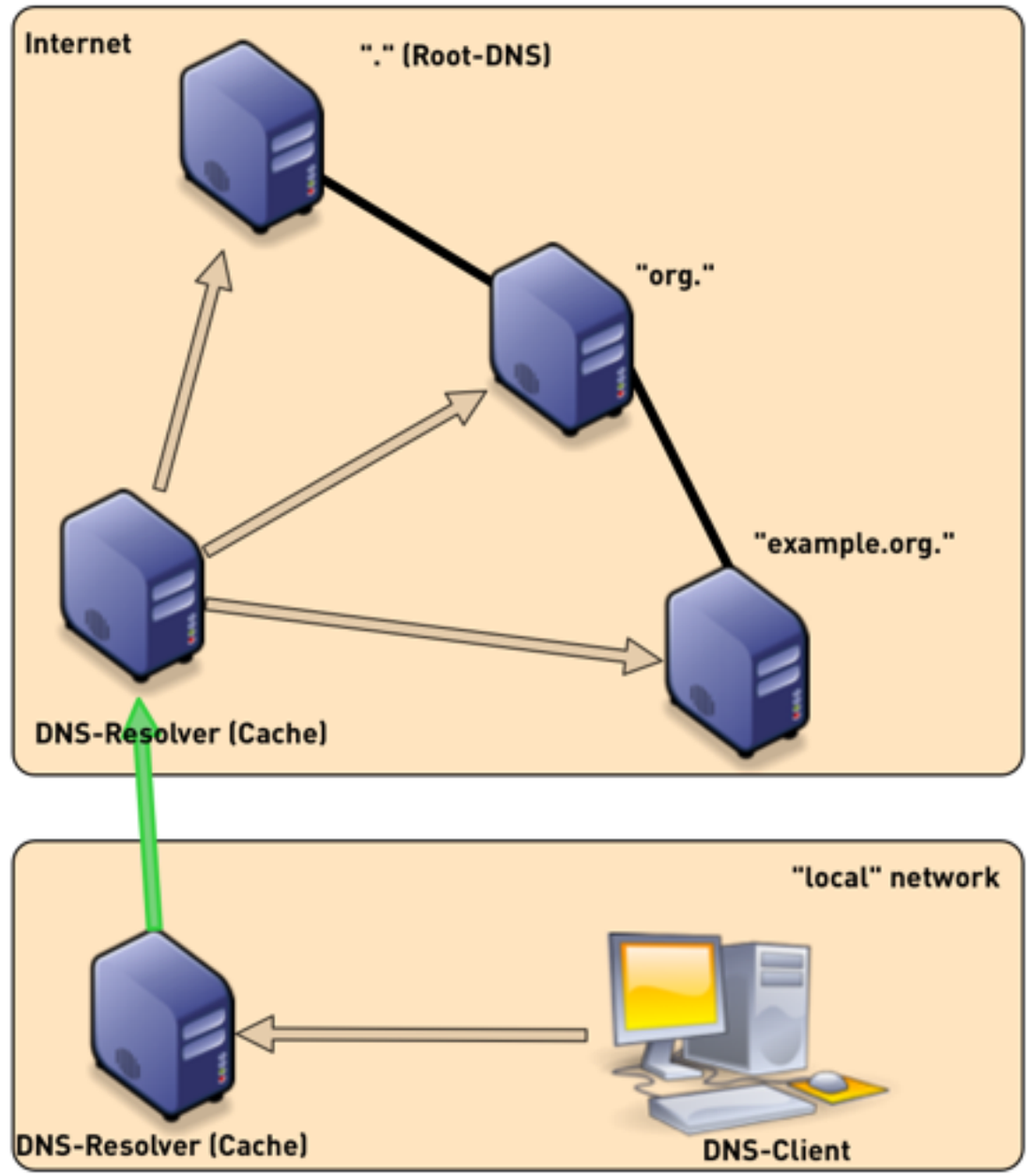
communication between client and DNS-resolver encrypted and authenticated



DNS via DoH/DoT (current state)

DoH/DoT DNS resolution (TLS) via forwarding/DNS proxy

communication between client and DNS-resolver encrypted and authenticated



DNS via DoH/DoT (current state)

DoT vs DoH

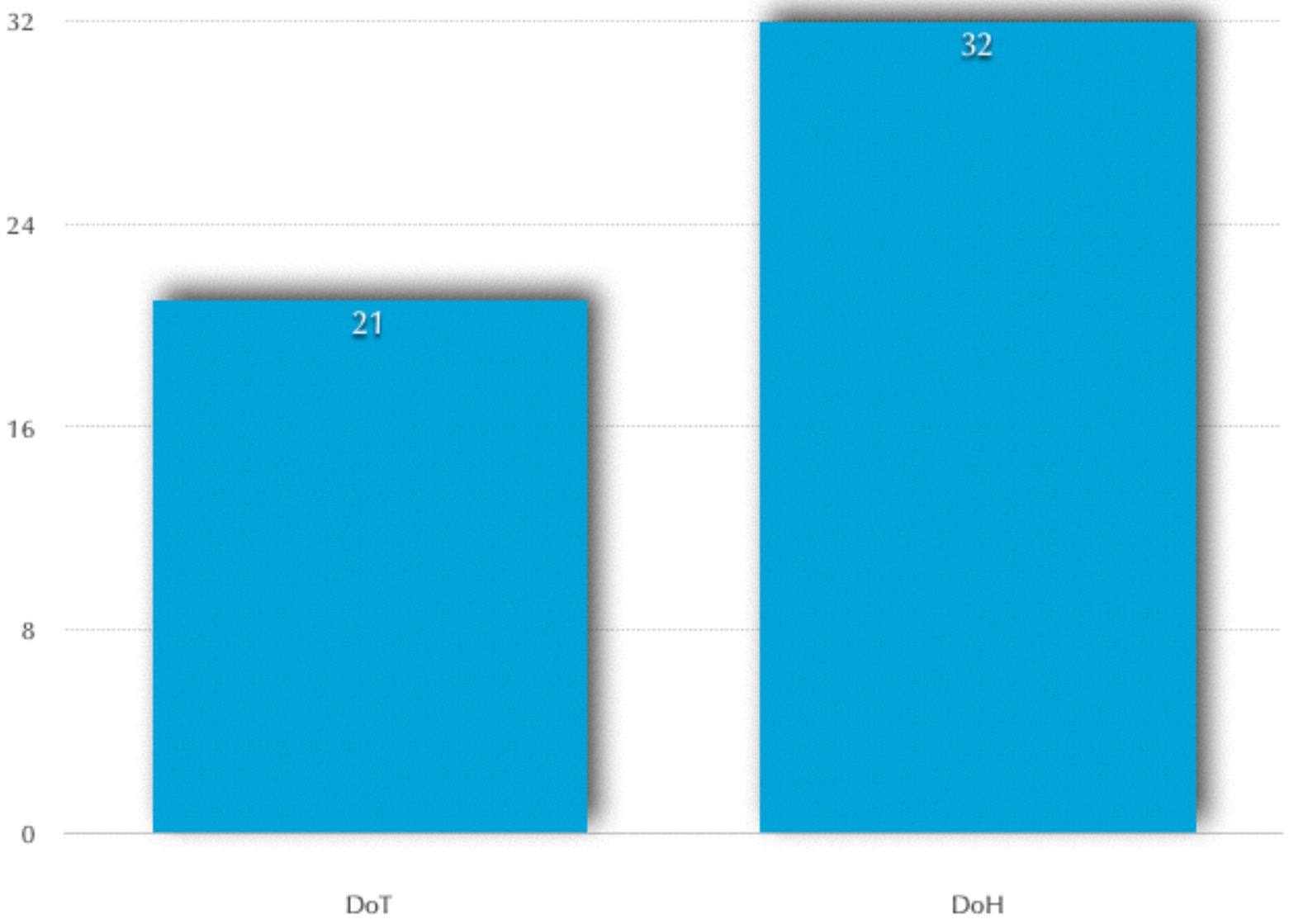
- differences between DoT and DoH
  - DoT is running on an dedicated port (853), can be easily blocked
  - DoH is made to look like normal HTTPS traffic, selective blocking of DoH is difficult
  - existing HTTPS library functions in programming languages give DoH an implementation advantage
  - DoH enables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

the survey

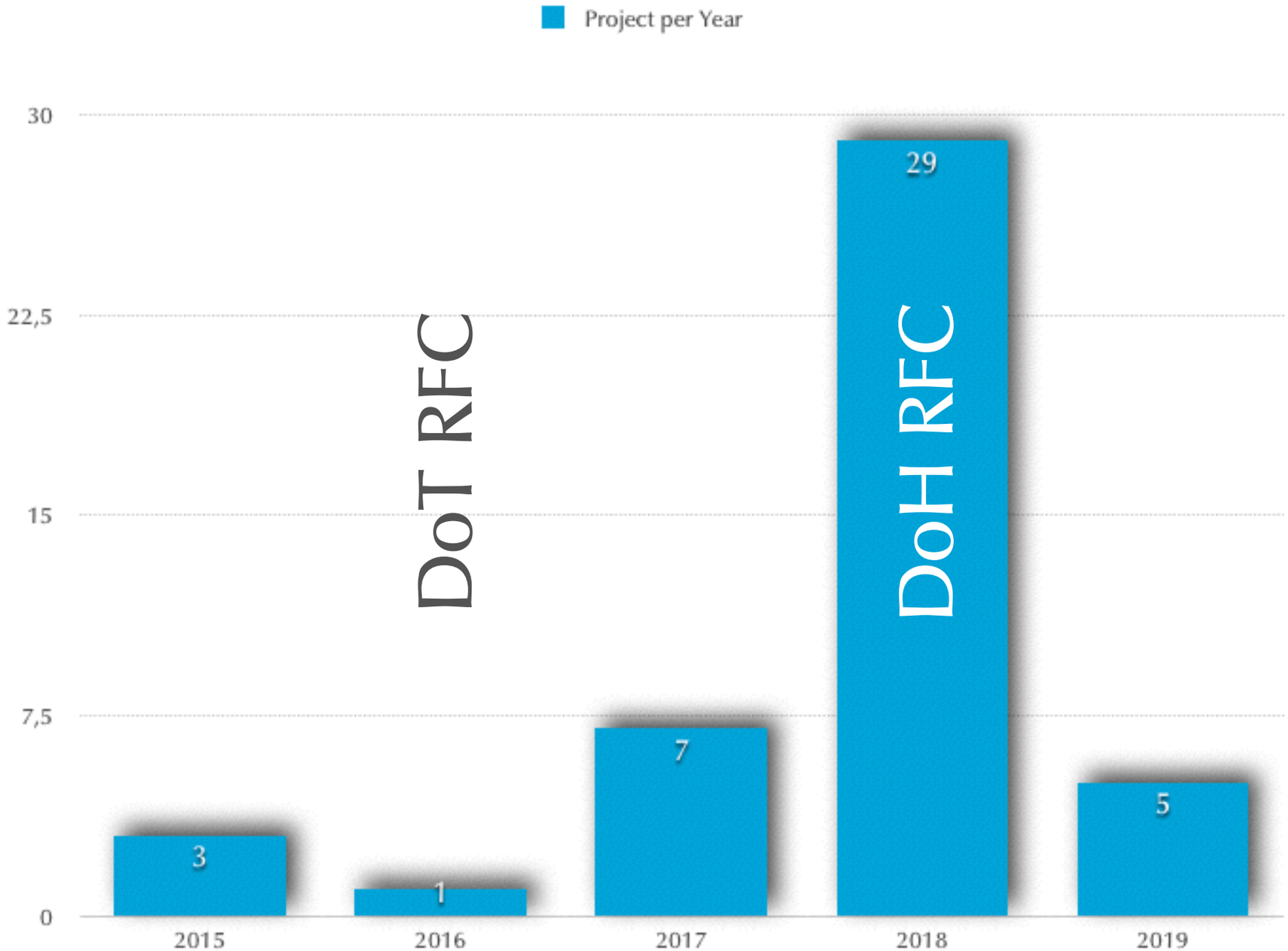
- informal survey, looking at 46 DoT/DoH open source software projects on Github and Gitlab
  - in May 2019
  - only software projects, no composition projects (Docker Container etc)
- full list:

`https://doh.defaultroutes.de/implementations.html`

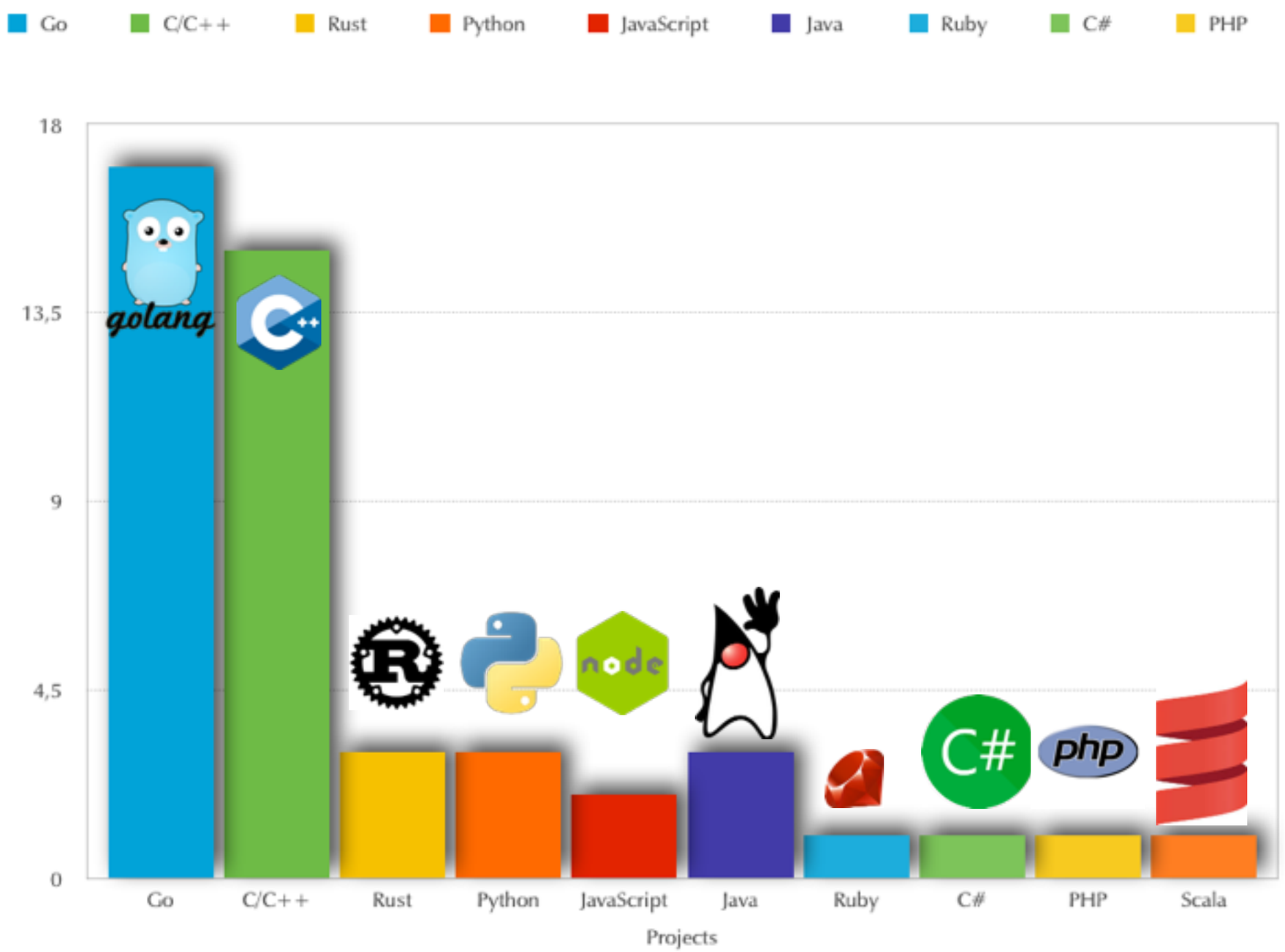
DoH and DoT



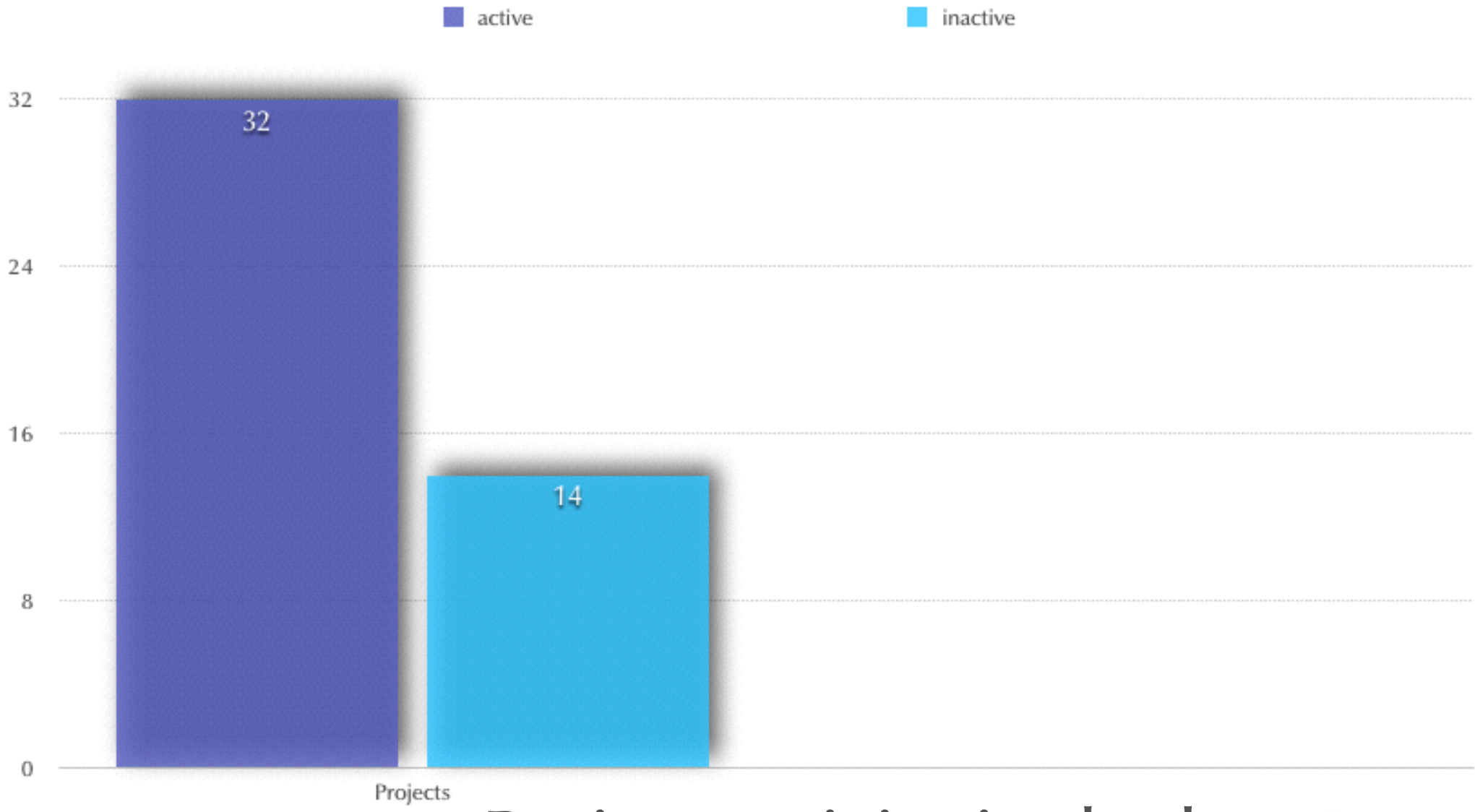
Years of DoH/DoT implementation



Implementation languages



Project liveliness



Project activity in the last 6 month?

Applications

- Firefox
- Chrome
- curl
- Tenta-Browser (Android)
- Bromite Browser (Android)

System Resolver

- systemd-resolved (Systemd-based Linux)
- unwind (OpenBSD) : next talk!
- resolver module for Linux glib (nsswitch.conf)

Client Proxy

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

some client proxies have additional functions, like ad-blocking or load-balancing across multiple upstream server

Server Proxy

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

server proxies add DoT or DoH
to traditional DNS server
(BIND 9, Microsoft DNS, NSD ...)

Dot/DoH Server

- unbound
- Knot
- sdns

DNS server with DoT or DoH
"build in"

Whats missing

- DANE - check of TLS x509 certificates via DNS
- Witness checks for client proxies
  - query multiple upstream DNS resolver and compare the data, protect against rogue server operators
- code security audits

Conclusion

- there is a rich software ecosystem for DoH and DoT
- users can find applications and client proxy systems
- operators can find server proxies or DoH/DoT server

ISPs: start offering DoH/DoT now,
else your customers DNS traffic will
move to the cloud!

Questions!

(please don’t discuss the political issues around DoT and DoH here)

THANK YOU

MEN&MICE

menandmice.com