DNS over http[s]

Janneke Simmering

December 3, 2019

Inhalt

Basics

Basics

- http
- https
- DNS

http

- Protokoll (**H**yper**t**ext **T**ransfer **P**rotocol)
- Application Layer, Layer 7
- TCP/IP based (Port 80)
- Communication between web servers and clients
- e.g. loading Web pages in a browser

https

- Protocol (**H**yper**t**ext **T**ransfer **P**rotocol **S**ecure)
- based on http
- TCP/IP based (Port 443)
- Data that is sent is encrypted (with SSL or TLS)

DNS

- **D**omain **N**ame **S**ystem
- Resolving a domain name to an IP-address
- based on UDP (Port 53)
- clear text
- used since 1985
- "makes internet easy to use"

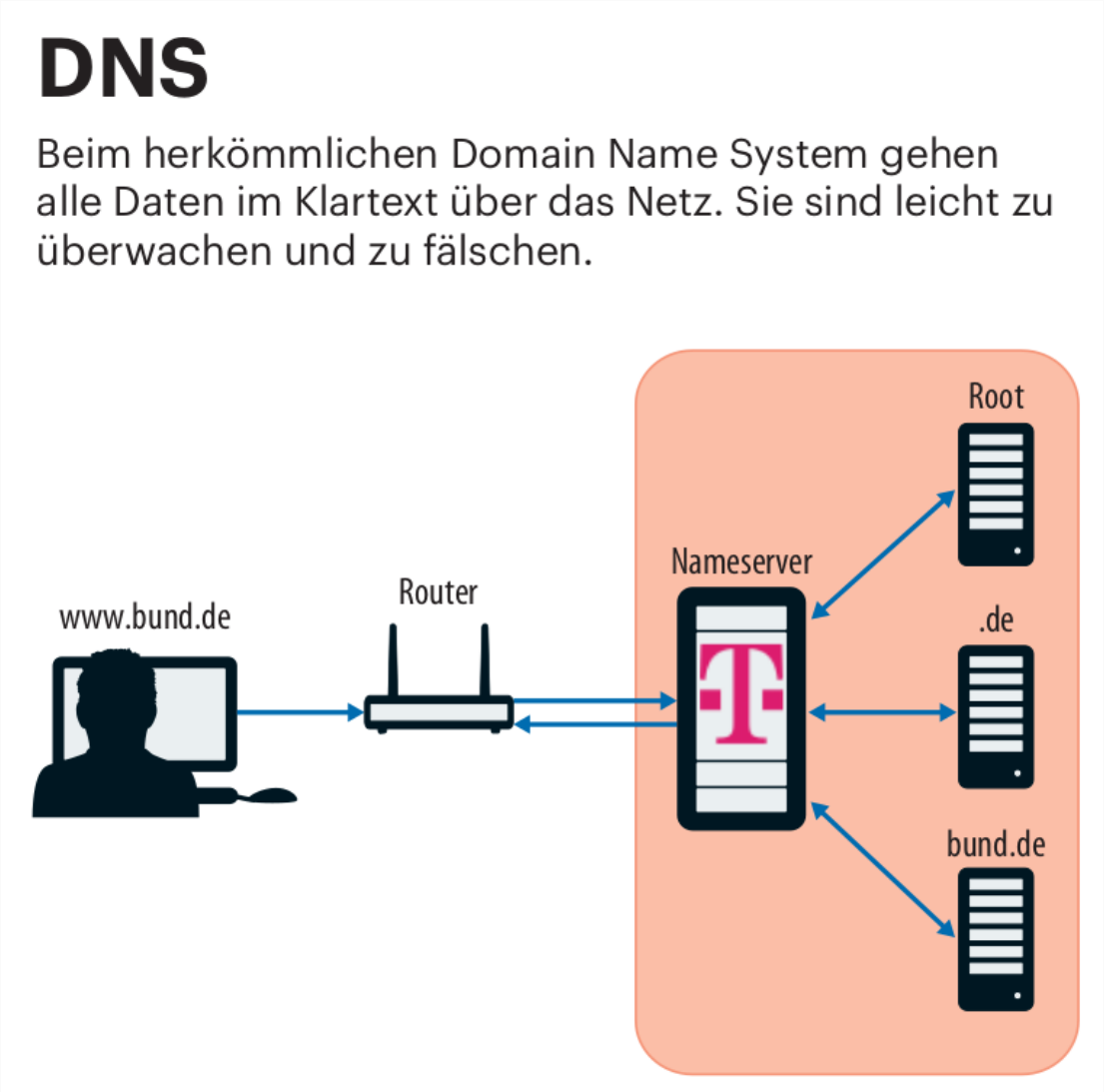

Figure 1: source: c't 2018, Heft 14: DNS mit Privacy

What could be problamatic with DNS?

Why would you want to change something?

Problems with DNS

- uses clear text
- everyone (on the path between you and the servers) can see what domain you are looking for and manipulate the result
  - tracking (full or partial IP is included in request)
  - Spoofing (disguising a communication from an unknown source as being from a known, trusted source)
  - Man-in-the-middle-attacks

DoH - DNS over https

What is DoH?

- **D**NS **o**ver **H**ttps (RFC 8484)
- First launched by CloudFlare
- DNS queries sent over https
- goals:
  - RFC: "preventing on-path devices from interfering with DNS operations"
  - RFC: "allowing web applications to access DNS information via existing browser APIs in a safe way"
  - Wikipedia: "enhance user privacy and security"

What is DoH?

- **D**NS **o**ver **H**ttps (RFC 8484)
- First launched by CloudFlare
- DNS queries sent over https
- effects:
  - DNS traffic can not be distinguished from normal web traffic
  - no dedicated port that can easily be blocked (all web traffic on port 443 - can not be blocked)
  - enables DNS on Application Level

What is DoH?

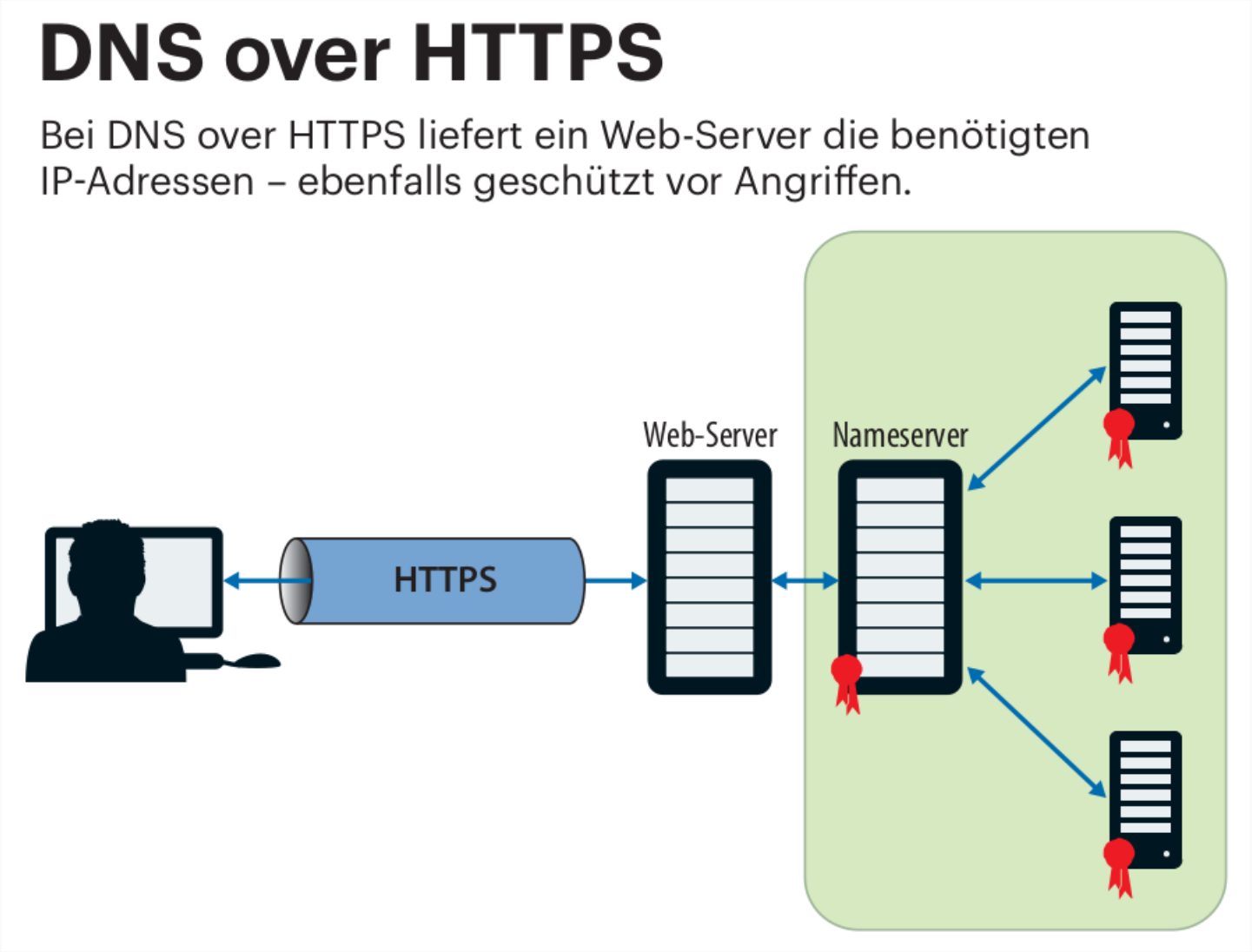

Figure 2: source: c't 2018, Heft 14: DNS mit Privacy

Problems and criticism

- Only encrypts between user and DNS Resolver not necessarily the whole way
- How to incorporate DNS Resolver which are local in a network?
- Administrators have to find new ways to secure and monitor their network
- "Mozilla or cloudfare get all the data"
  - if the big browser are automatically configured to use DoH automatically the services they use are favored and all DNS data goes to those few companies
  - during testing firefox used cloudflare
  - you can manually edit the DoH-Server, but so far there aren't many of these services and they are not necessarily compatible with the browser

Thank you for your attention!

Are there any questions?

Discussion

Do you think DoH is more secure than DNS or DNSSec?

Does it protect the users privacy?

Would you use DoH? What would be requirements for you to use DoH?

Sources

Sources

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

https://www.youtube.com/watch?v=rfyMYM4wsJc

c't 2018, Heft 14: DNS mit Privacy

c't 2019, Heft 7: Domain Name System

c't 21/2019 S.58: Browser verschlüsseln DNS-Anfragen

https://hacks.mozilla.org/2018/05/a-cartoon-intro-to-dns-over-https/

https://en.wikipedia.org/wiki/DNS_over_HTTPS

https://www.youtube.com/watch?v=po3zYOe00O4

https://www.youtube.com/watch?v=Rck3BALhI5c

https://www.youtube.com/watch?v=72snZctFFtA

https://en.wikipedia.org/wiki/Domain_Name_System

https://www.youtube.com/watch?v=pjin3nv8jAo