What's the name? DNS / DNSSec

Jan Pohlmeyer

03. Dezember 2019

Inhalt

Was ist das DNS?

Was ist das DNS?

- **D**omain **N**ame **S**ystem
- Telefonbuch/Telefonauskunft des Internets
- Bisher: Kommunikation über IP-Adressen
  - Rechner können besser mit Zahlen
  - für Menschen schwer zu behalten (spätestens bei IPv6)
- Jetzt: Adressen einen Namen geben
- für Menschen einfacher zu merken
- muss für Rechner aber wieder in Zahlen umgewandelt werden
- z.B. 2a00:1450:4001:808::200e $\Leftrightarrow$ google.com.

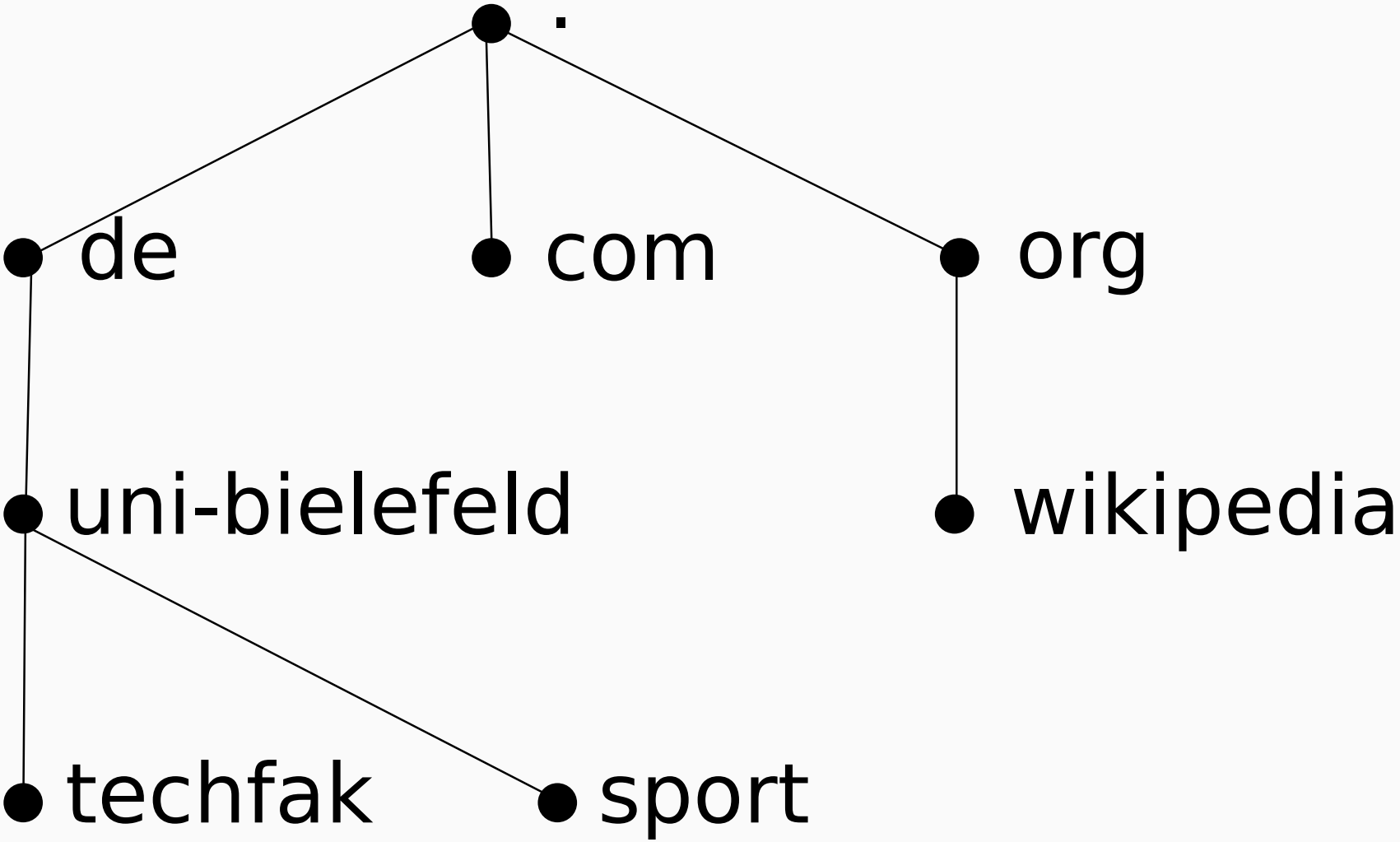
Geschichte

- zentrale HOSTS.TXT in ARPANET (gepflegt per Telefon)
- Anfang 1980er: zentrale Speicherung zu langsam
- 1983: Einführung eines Konzepts zur verteilten Speicherung in RFC 882/883
- 1984: Erste Implementation von BIND (Berkeley Internet Name Domain)
  - noch immer die am meisten verwendete DNS Software
- 1987: Einführung von DNS in RFC 1034/1035
- Erweiterungen/Nachspezifikationen z.B. in RFC2181, RFC5892

Wie funktioniert das DNS?

Aufbau des DNS

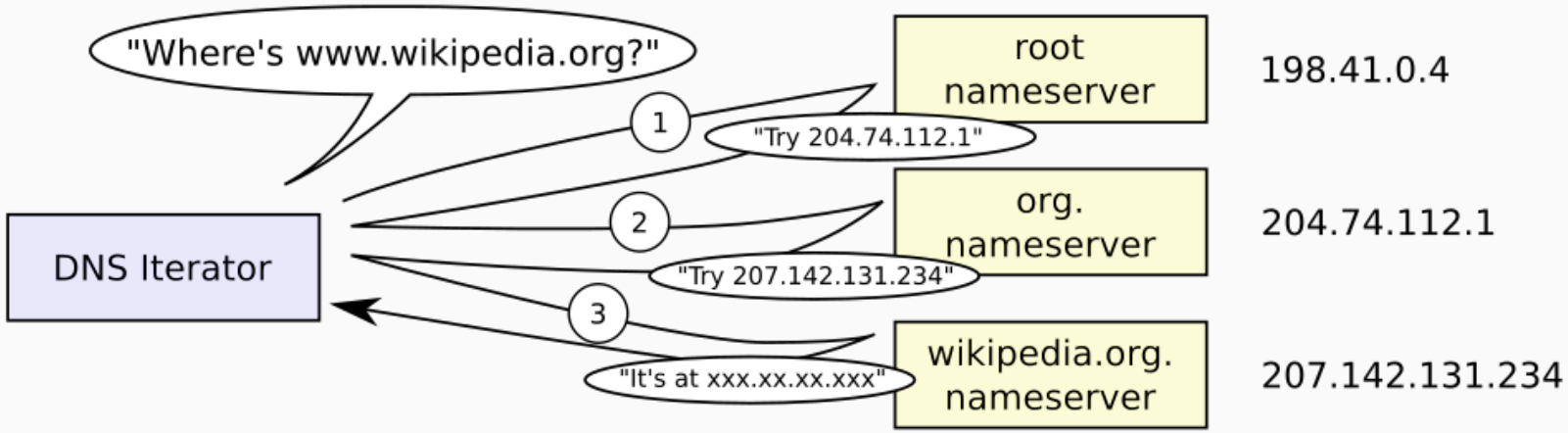
- Verteiltes hierarchisches System
- Aufteilung in Zonen



Aufbau eines Namen

- von rechts nach links zu lesen, zonen durch punkt getrennt
- Beispiel: google.com.
- von rechts:
  - root zone (.)
  - danach TLD (top-level-domain) (com, de, org, ...)
  - danach subdomains (google, ...)
  - ...
- insgesamt bis zu 127 ebenen
- jede subdomain kann bis zu 63 zeichen lang sein
- insgesamt nicht mehr als 253 zeichen in der kompletten adresse

DNS Anfrage I

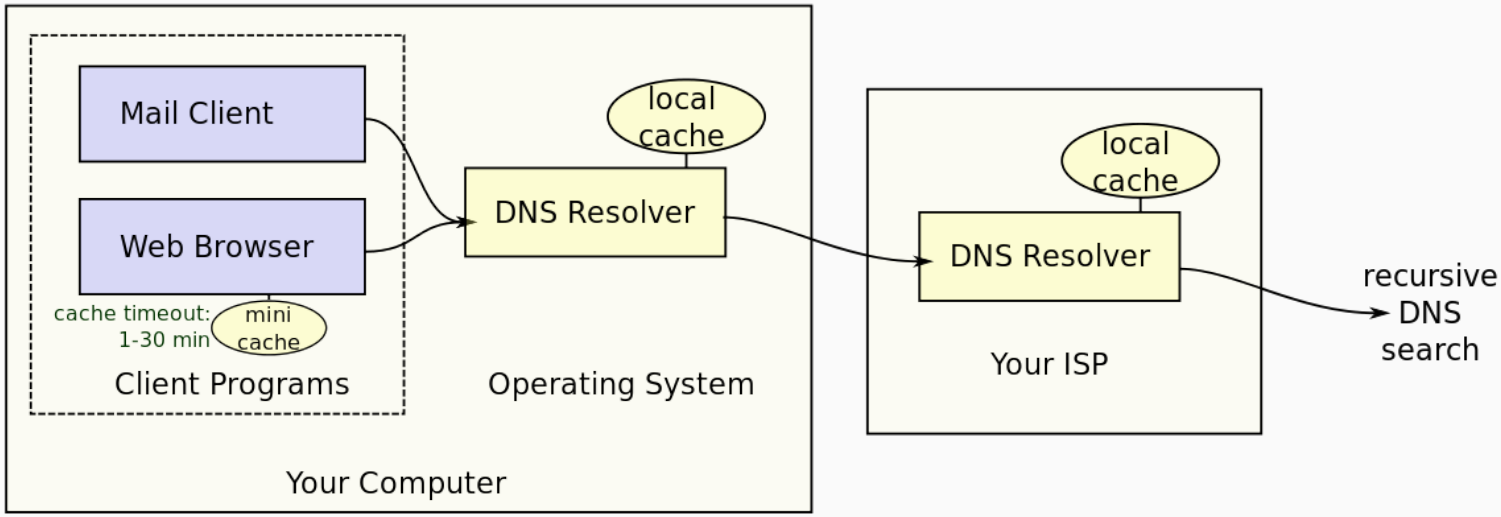


[1] https://upload.wikimedia.org/wikipedia/commons/a/a5/Example_of_an_iterative_DNS_resolver.svg

DNS Anfrage II

- Anfragen üblicherweise auf Port 53/UDP oder 53/TCP
- Wenn alle Anfragen an die root-Server gehen würde wäre das eine ganze Menge
  - zusätzlich zu authorativen DNS-Servern gibt es DNS-Cache-Server
  - DNS-Cache-Server fragen authorative DNS-Server an, speichern DNS-Antworten für eine bestimmte Zeit
  - Nutzer stellt eine Anfrage an den DNS-Cache Server
  - DNS-Cache-Server schaut ob er die Adresse bereits gespeichert hat
  - sonst fragt dann die einzelnen authorativen Nameserver und antwortet, wenn er die entgültige Antwort bekommt
  - $\Rightarrow$ entlastet root-Server
  - DNS Antworten beinhalten eine time to live (TTL), wie lange der DNS Eintrag valide ist bevor er neu angefragt werden muss

DNS Anfrage III



[1] https://upload.wikimedia.org/wikipedia/commons/0/09/DNS_in_the_real_world.svg

Aufbau einer DNS Anfrage

- Am Ende des Header: 16-bit Integer mit Anzahl der Ressourcen
- Für jede Ressource:

Feld	Beschreibung
NAME	Name der angefragten Ressource
TYPE	Typ des Resource Eintrags
CLASS	Code der Klasse des Eintrags

Aufbau eines DNS Eintrags

Feld	Beschreibung	Beispiel
NAME	Name der angefragten Ressource	www.google.com.
TYPE	Typ des Resource Eintrags	z.B. A, AAAA, MX, ...
CLASS	Code der Klasse des Eintrags	IN (für Internet)
TTL	Sekunden die der Eintrag valide bleibt	max. 68 Jahre
RDLENGTH	Länge von RDATA	
RDATA	Inhalt zB. IP-Adresse	172.217.22.110

Schwächen von DNS

Schwächen von DNS

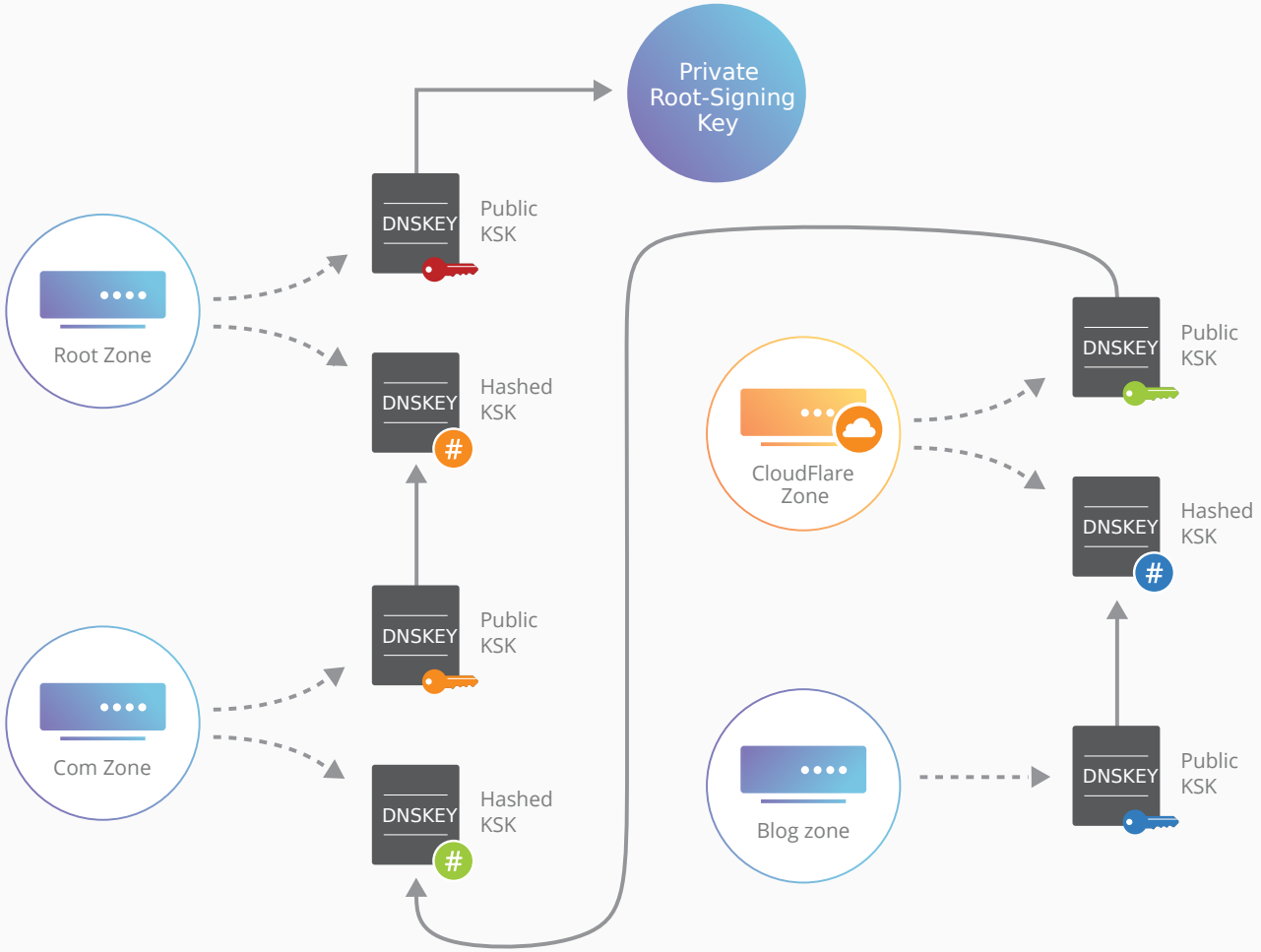
- Pakete sind unverschlüsselt und unsigniert
- Pakete abfangen
- Abhören
- Spoofing (Cache poisoning)
- falsche Antworten senden
- Verstärker für DoS-Attacken

DNSSec

DNSSec

- DNS Security Extensions
- Antworten digital signiert (NICHT verschlüsselt)
  - Zone signing key signiert DNS Antworten für eine Zone
  - Key signing key signiert den Zone signing key für eine Zone
- basiert auf public key cryptography

Chain of Trust



[1] https://www.cloudflare.com/img/products/ssl/diagram-the-chain-of-trust.svg

DNSSec

- Resolver kann prüfen ob die Antwort tatsächlich vom richtigen Server kommt
- löst bei weitem nicht alle Probleme
  - unverschlüsselt, DoS-Attacken, ...

Habt ihr noch Fragen?

Quellen

- *rfc1034*. URL: https://tools.ietf.org/html/rfc1034.
- *Wikipedia DNS*. URL: https://en.wikipedia.org/wiki/Domain_Name_System.
- *Cloudflare DNS*. URL: https://www.cloudflare.com/learning/dns/what-is-dns/.
- *Wikipedia FQDN*. URL: https://en.wikipedia.org/wiki/Fully_qualified_domain_name.
- *rfc3833*. URL: https://www.rfc-archive.org/getrfc.php?rfc=3833.
- *rfc4033*. URL: https://tools.ietf.org/html/rfc4033.
- *Wikipedia DNSSec*. URL: https://en.wikipedia.org/wiki/Domain_Name_System_Security_Extensions.
- *Cloudflare DNSSec*. URL: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/.