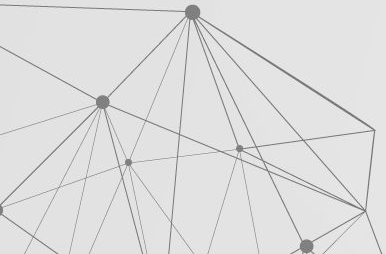
Bezpečnosť DNS

Ľubor Jurena, CCIE #51635
skHosting.eu

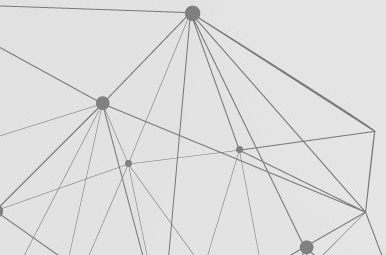
Čo je to DNS?

- Domain Name System
- RFC 1035
- 1987
- Systém na preklad mien na IP adresy alebo aj IP adries na mená
- Decentralizovaný hierarchický systém
- UDP, port 53
    - výnimočne TCP



Problémy v DNS

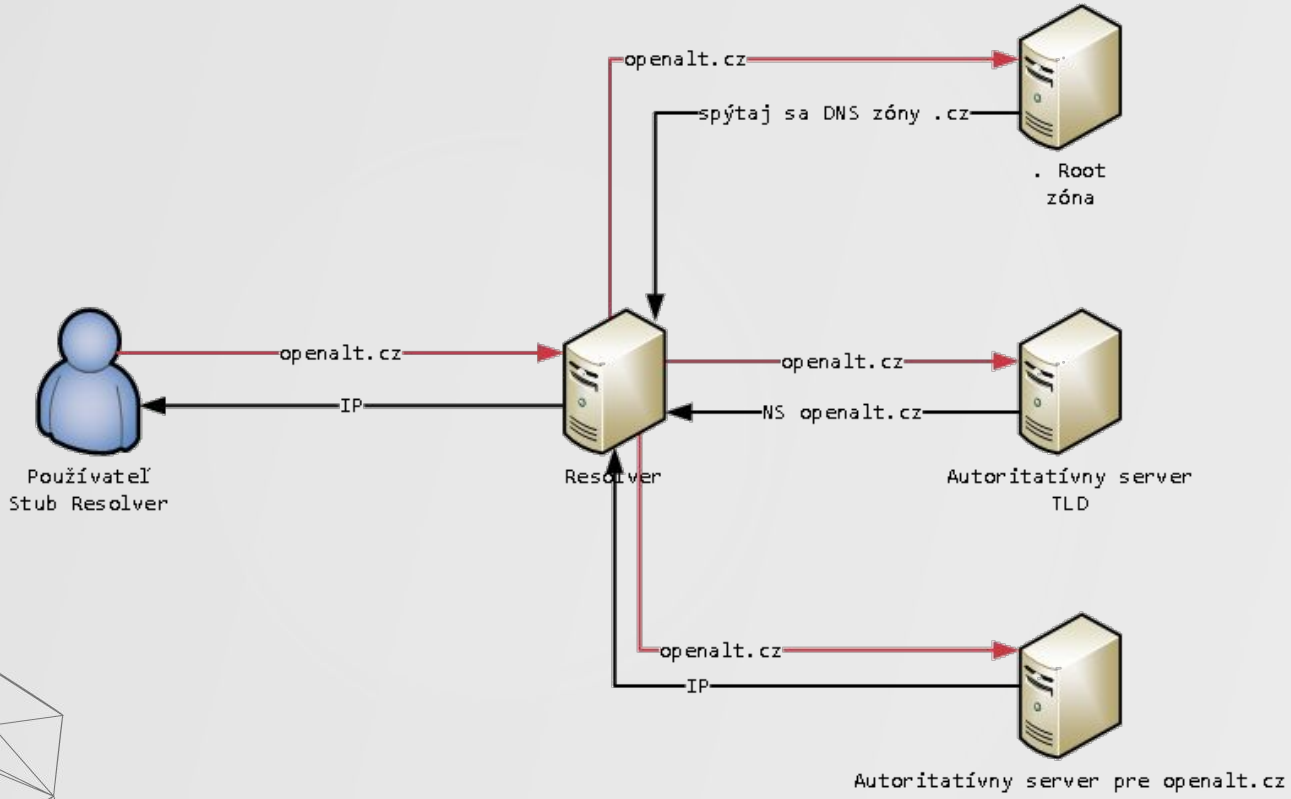
- Nízka úroveň bezpečnosti
  - dáta sa prenášajú v plaintexte
  - ľahká možnosť odpočúvania a zmeny prenášaných dát
- Najjednoduchší spôsob blokovania stránok



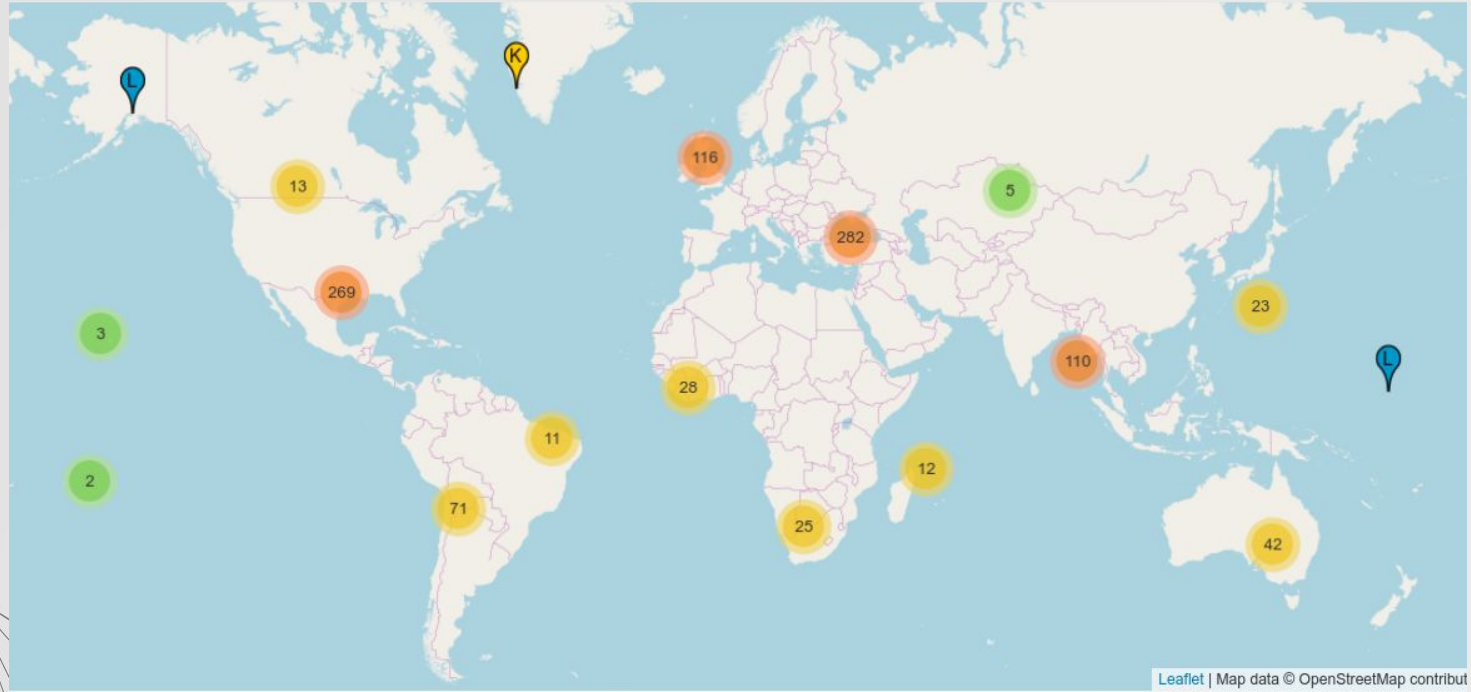
Problémy v DNS

Ako vyzerá DNS komunikácia?

Ako vyzerá DNS komunikácia?



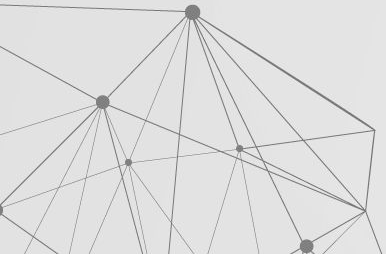
Root servery vo svete



https://root-servers.org/

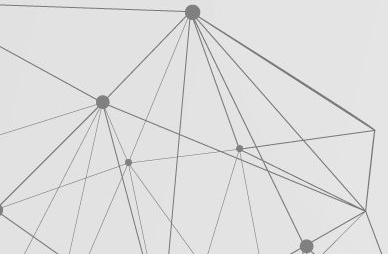
DNSSEC

- 1999
- Zabezpečenie autenticity DNS údajov medzi autoritatívnym a rekurzívnym serverom
- Asymetrická kryptografia
- Pridáva podpis k existujúcim DNS záznamom (A, AAAA, MX, …)
- Správca domény vygeneruje privátny a verejný kľúč
- Vytvára reťaz dôvery



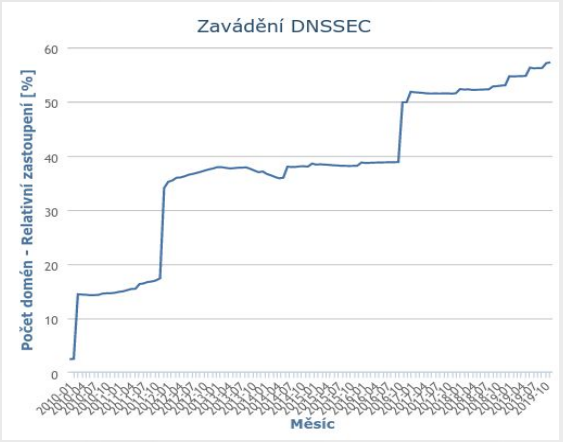
DNSSEC

- Musí byť podpora na strane TLD (napr. .SK, .COM, .CZ, …)
    - TLD musí byť podpísaná v root zóne
- Doména musí byť podpísaná
- Validácia musí byť zapnutá na strane resolvera
    - validovať je možnosť, nie povinnosť
- Nevalídna odpoveď sa ku klientovi nedostane
    - validujúci resolver vráti chybu “SERVFAIL”



DNSSEC

- Podpora DNSSEC
  - .cz od 2008
    - ➢ cca 60% podpísaných domén
    - ➢ automatické podpisovanie
  - . (root) od 2010
  - .sk od 2019
    - ➢ cca 3% podpísaných domén



stats.nic.cz

Dobrý deň,

automatizovane to náš systém naozaj nepodporuje, ak ale potrebujete, vieme Vám to nastaviť aj takto (s nastavením na Vaše NS), no v tomto prípade je to spoplatnené sumou 20€ bez DPH/doménu. V takom prípade nám ale musíte dodať tieto DNSSEC, ktoré nám zašlite cez control panel. (ak nie sú DNS na nás nemáme ich ako vygenerovať)

Pre hodnotenie odpovede a zobrazenie histórie správy kliknite na:
https://www.onlinepodpora.sk[redacted]

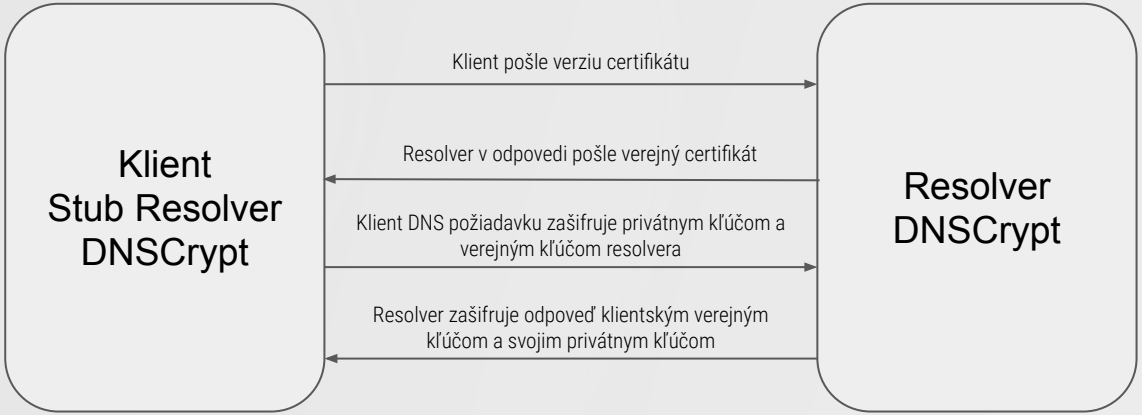
S pozdravom
[redacted]
Helpdesk

+421 2 581 010 64
info@nic.sk

NIC hosting, s.r.o.
NIC.sk

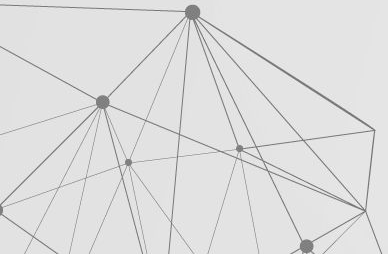
DNSCrypt

- 2013
- OpenDNS
- Podpora TCP aj UDP
- Protokol pre bezpečnú komunikáciu medzi stub resolverom a rekurzívnym resolverom
- Zabraňuje sledovaniu komunikácie
- Nie je štandardom



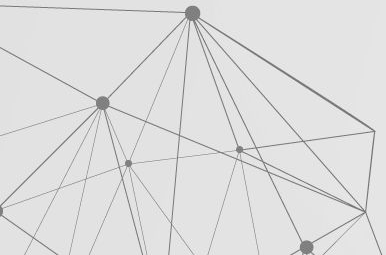
DNS over TLS

- RFC 7858
- rok 2016
- TCP, port 853
- Pri použití s TLS 1.3 zanedbateľná strata výkonu
- DNS zabalené do TCP a TLS
- Šifrovaný prenos dát medzi stub resolverom a rekurzívnym resolverom



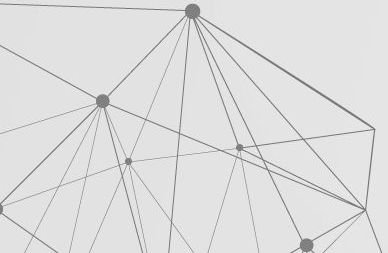
DNS over TLS

- Chýba implementácia v OS
  - Unbound, Knot Resolver, ...
- Public DNS: Cloudflare, Google, Quad9, nic.cz odvr
- Deep Packet Inspection



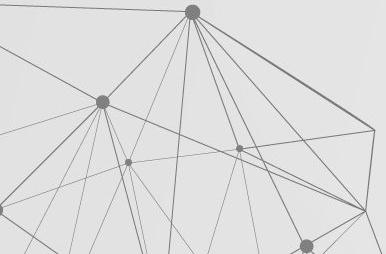
DNS over HTTPS

- HTTP/2 so server push
- MIME type application/dns-message
- Obtiažne detekovať a blokovať
- Implementácie vo Firefoxe, Chrome, experimentálne vo Opere, Knot Resolver
- Klienti pre operačné systémy
- Ľahko implementovateľný do aplikácií
- Potencionálne možnosti úniku metadát
    - OCSP, SNI



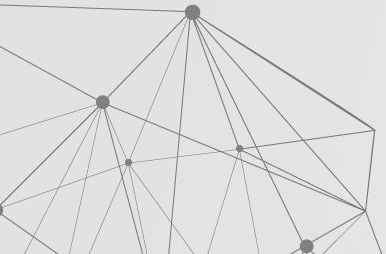
DNS over DTLS

- UDP, port 853
- DNS zabelené do UDP a TLS
- Experimentálne
- Problémy s fragmentáciou
- Žiadne známe implementácie



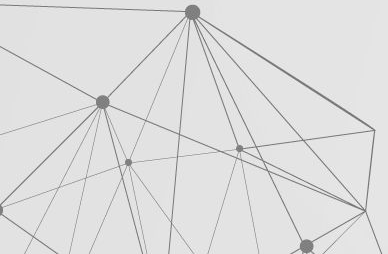
DNS over *

- DNS over QUIC
  - UDP s funkciami TCP
- DNS over IPSec
- DNS over TOR
  - veľká časť exit nodov používa Google Public DNS a/alebo Cloudflare DNS



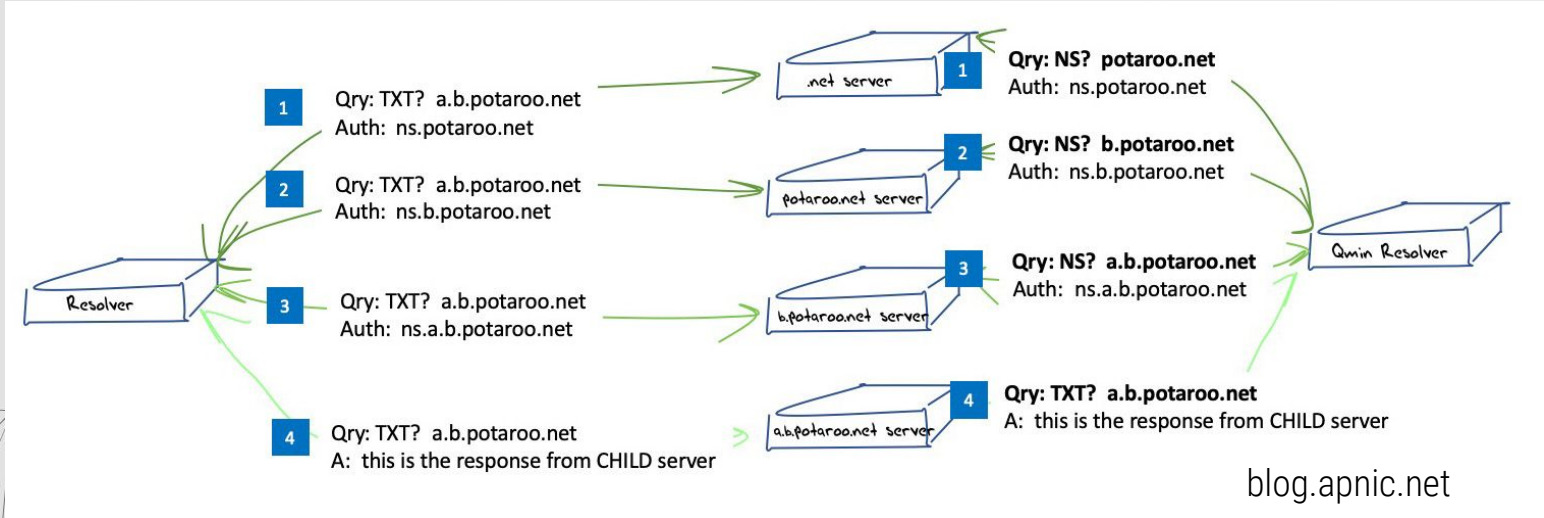
Podpora v Android a iOS

- Od Android 9
  - DNS over TLS
- iOS
  - žiadna podpora
- Cloudflare 1.1.1.1 aplikácia
  - DoH
  - DoT



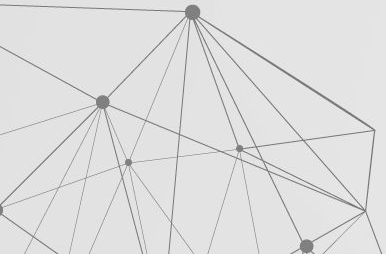
Qname Minimisation

- Podpora v BIND, Knot, Unbound, ...



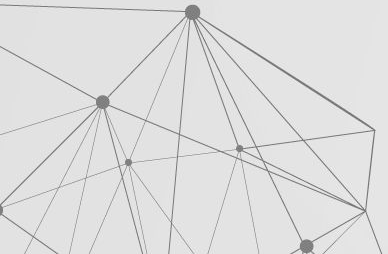
EDNS0 Padding

- Povoľuje pridanie premenlivého počtu bajtov do požiadavky/odpovedi
  - na strane klienta aj servera
- Podpora len v Knot Resolveri a getdns
- Dáva zmysel len pri šifrovanom prenose
- DoH podporuje random padding



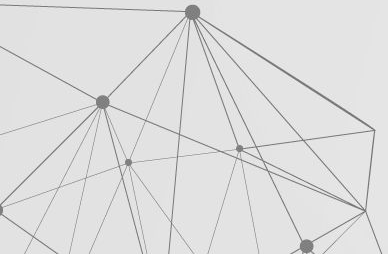
Problémy verejných rekurzívnych resolverov

- Výpadky
  - 2016, 2019 - Google
  - 2018 - Cloudflare
- Podpora EDNS Subnet
- DNS over HTTPS implementované v prehliadači
- Dôverujeme im?



Rozhodnutie

- DNSSEC
- Rekurzívny resolver / Forwarder
  - Verejný?
  - Vlastný?
  - Vlastný na každom zariadení?



Ďakujem za pozornosť