TELFOR 2024

RNIDS

DNS – The Domain Name System

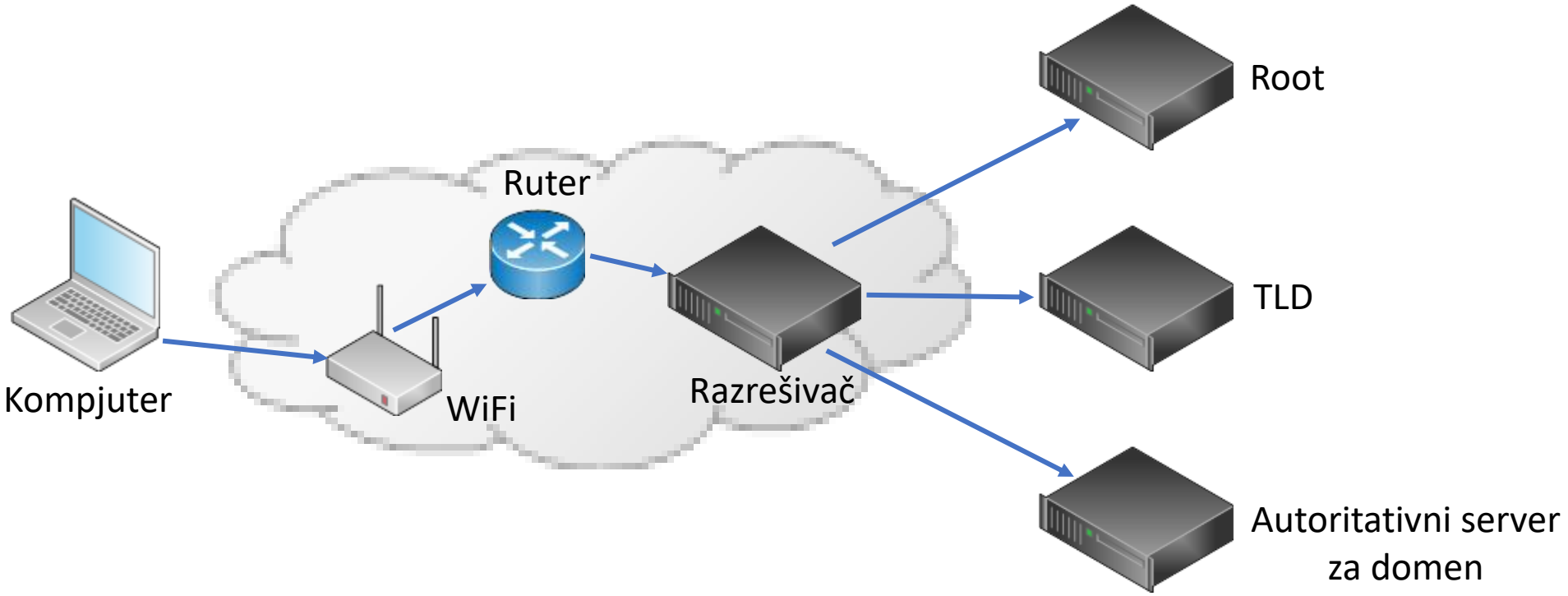
Ustanovljen 1979. godine (*Paul Mockapetris*)

U vreme kada je DNS osmišljen nije bilo realne potrebe za bezbednosnim merama!

DNS je poslednji internet protokol koji koristi isključivo otvoreni tekst.

RNIDS

DNS uključuje mnogo aktera



Zloupotreba DNS-a

- Preusmeravanje korisnika
- Hakovanje
- Krađa podataka (DNS tunel)
- Napad na druge sisteme (amplificirani DDoS)

RNIDS

DNSSEC

DNSSEC je DNS proširenje koje obezbeđuje autentičnost i integritet DNS odgovora.

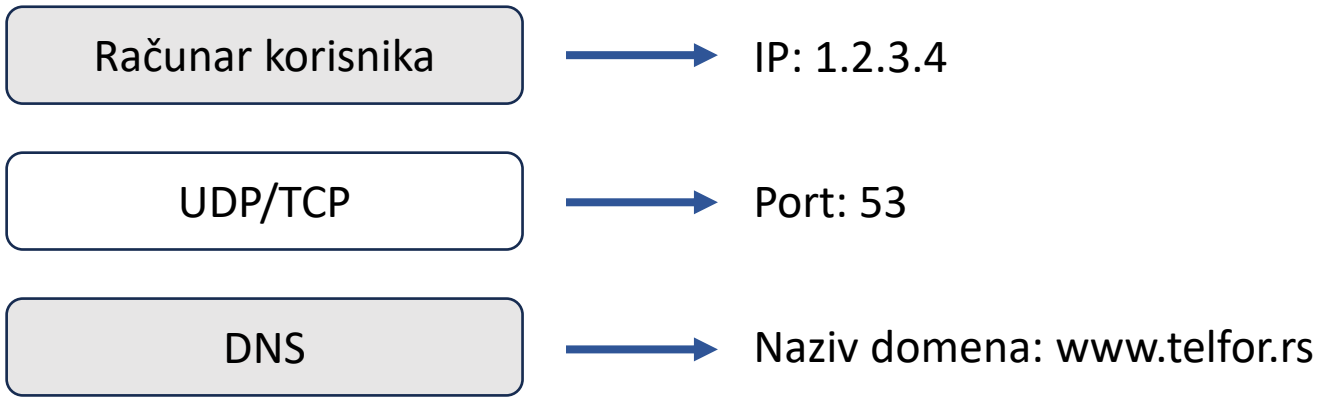
A privatnost? (Datira mnogo ranije od GDPR-a)

DNS i privatnost korisnika

- DNScurve/DNScrypto (2009.) – jednostavan transport šifrovanih DNS poruka.
- Query minimization – slanje upita samo sa delom naziva domena koji odgovara određenom hijerarhijskom nivou (*rs* –> root; *ac.rs* –> RNIDS; *bg.ac.rs* -> AMRES; *etf.bg.ac.rs* ->RCUB; *www.etf.bg.ac.rs* -> ETF)
- DoT (DNS over TLS) i DoH (DNS over HTTPS) – razmena DNS poruka uz pomoć standardnih šifrovanih TCP protokola

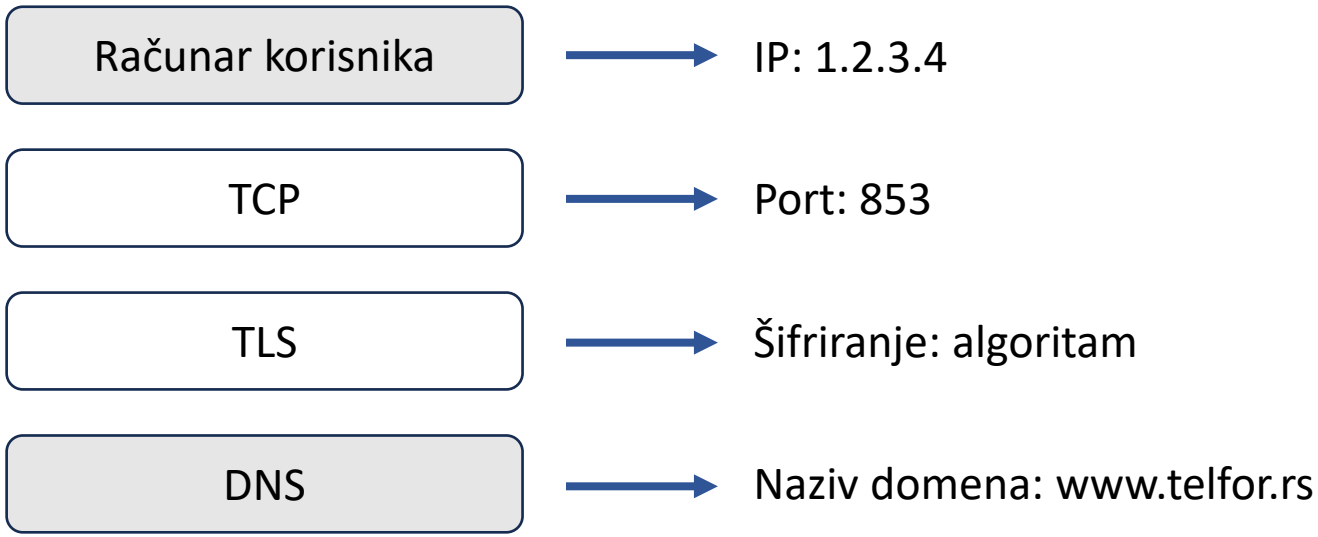
RNIDS

DNS


Računar korisnika
IP: 1.2.3.4
UDP/TCP
Port: 53
DNS
Naziv domena: www.telfor.rs

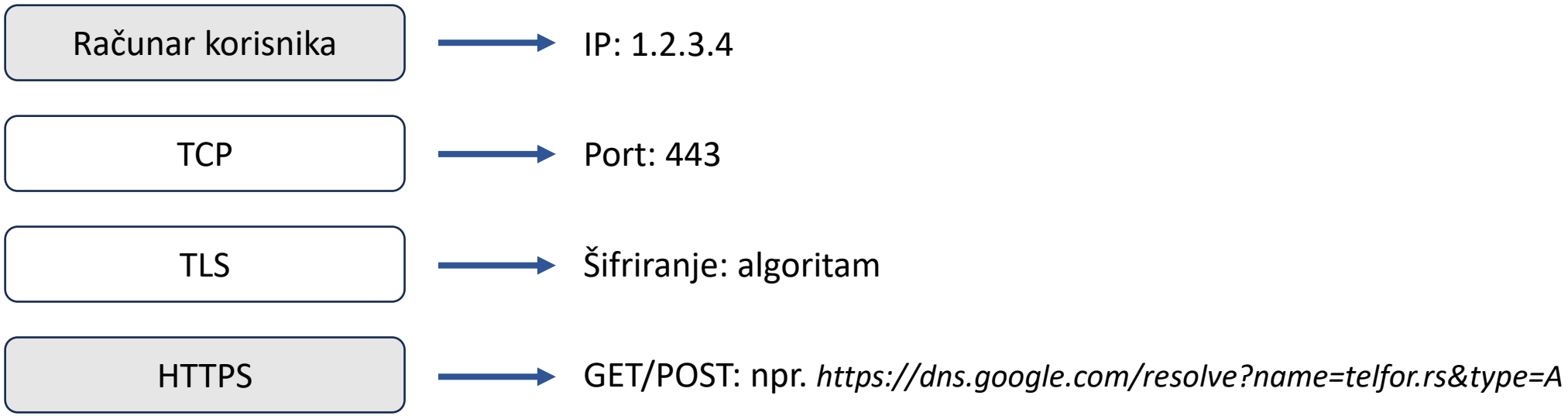
RNIDS

DNS over TLS (DoT)

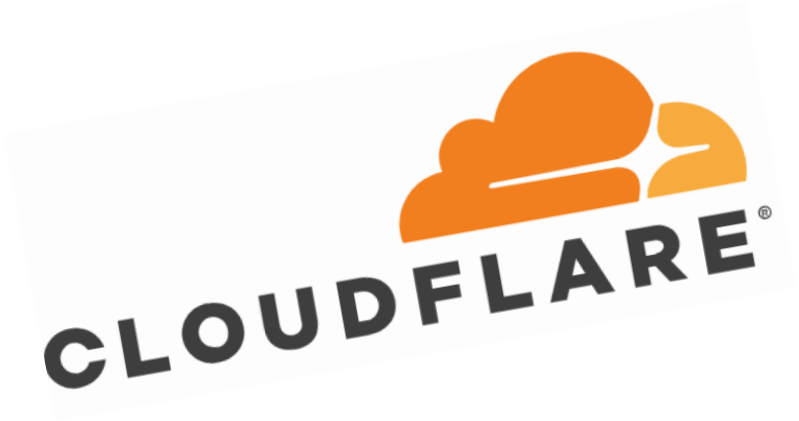


RNIDS

DNS over HTTPS (DoH)



DoT i DoH privatnost



RNIDS

Hvala na pažnji!