DIPLOMSKI RAD br. 1784:

Analiza i prikupljanje DNS paketa

Dinko Korunić

mentor: prof. dr. sc. Vlado Sruk

Sadržaj

1. Kratki uvod u DNS: hijerarhija, rezolucija, komunikacija, zapisi, itd.
2. DNS sigurnosni problemi, postojeći DNS softver i mane
3. Distribuirani DNS analizator: implementacija, mogućnosti, zaštita komunikacije, standardi, performanse
4. Provedena mjerenja i rezultati
5. Zaključak

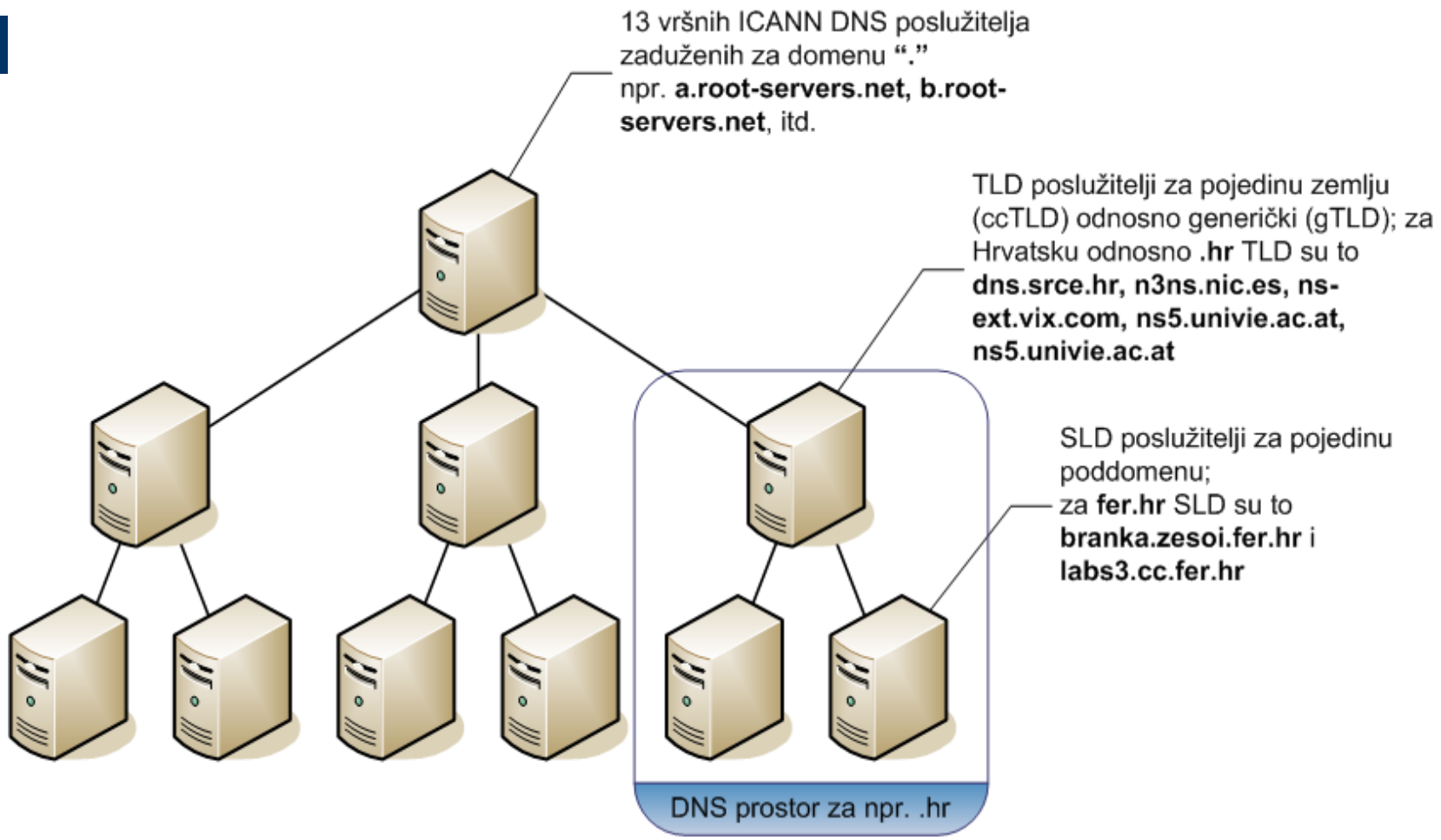
DNS uvod

- DNS - tri osnovne funkcionalnosti:
  - komunikacijska: protokol, paketi, zapisi, itd.
  - sustav poslužitelja i podataka: hijerhijski, imenički i distribuirani sustav
  - administrativna: upravljanje domenama (vršne i poddomene), registracija domena, delegacija, itd.
- jedan od osnovnih protokola na Internetu
- lakše pamtimo slovne labele umjesto adresa
- host, domain, zone, resource record, ...

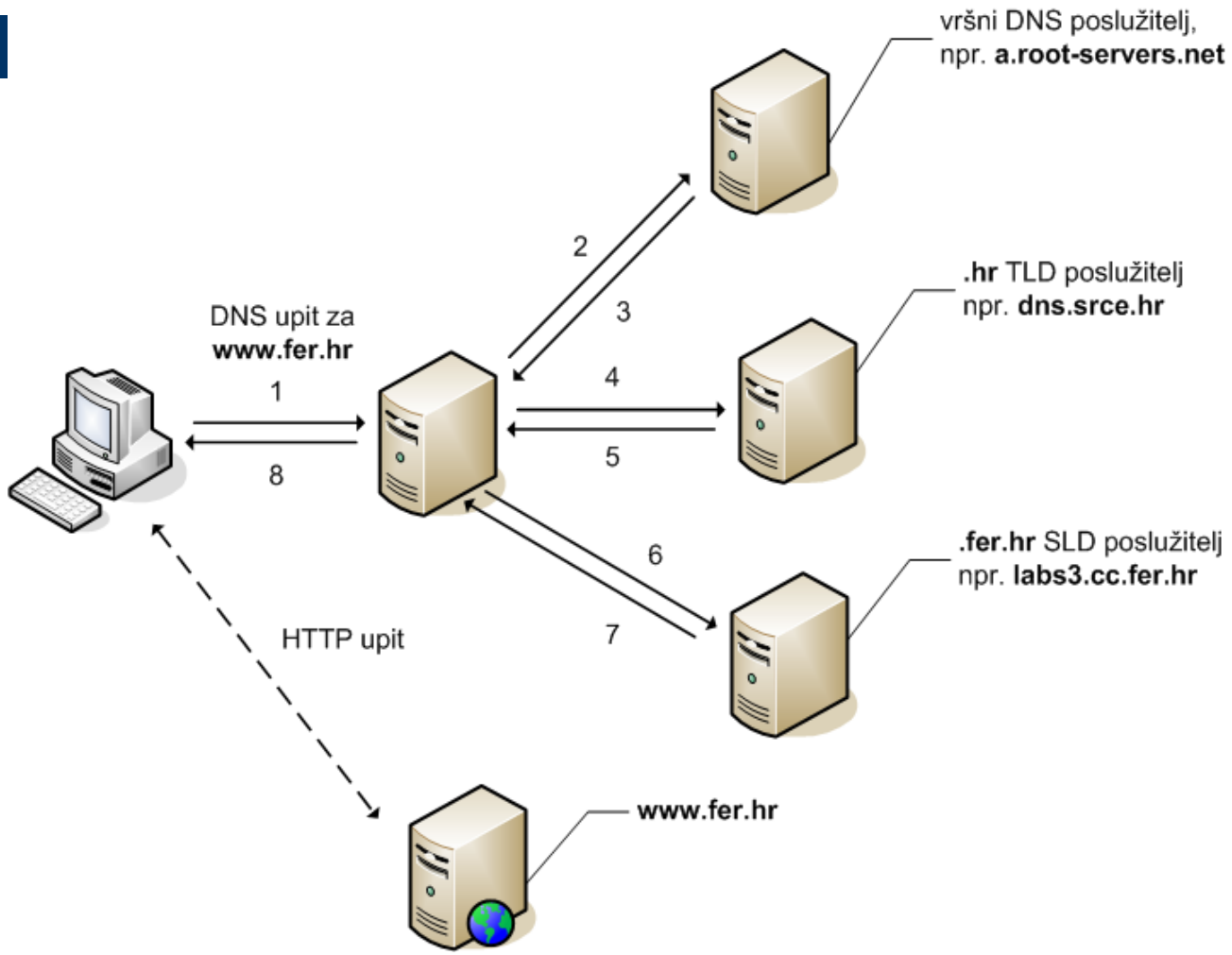
DNS uvod (2)

- "skriven" u pozadini većine aplikativnih protokola (HTTP, SSH, POP3, IMAP4, ...)
- DNS poslužitelji
  - DNS protokol međusobno i prema DNS klijentima
  - rekurzivni, iterativni; primarni, sekundarni, ...
  - svjetski čvorni (root), vršni (ccTLD, gTLD), domenski (SLD, 3LD)
- DNS RR
  - osnovna gradivna jedinica u domeni/zoni
  - A, PTR, CNAME, SOA, MX, SRV, NS, ...

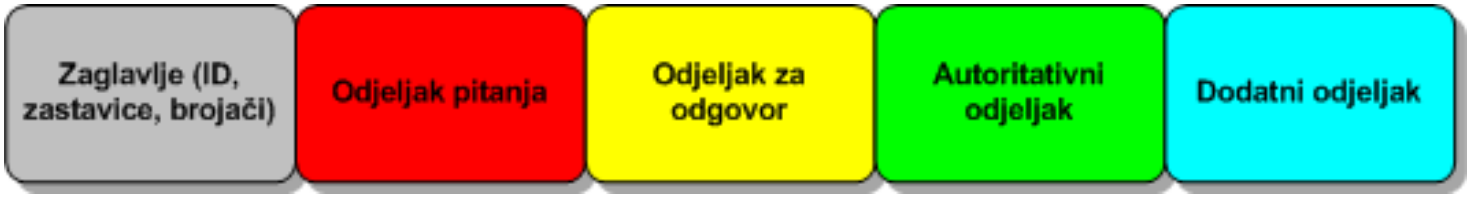
Hijerarhija poslužitelja



Razrješenje DNS upita - rezolucija



DNS komunikacijski paket



- strogo definiran izgled
- odgovor uvijek sadrži kopiju upita
- veličina:
  - do 512 bajtova za UDP, ako je veći onda retransmisija kroz TCP, izuzev za EDNS0
  - kompresija DNS oznaka, 13 RR maksimalno

Sigurnosni problemi

- kritičan servis sa brojnim problemima:
  - izvana: trovanje DNS-a (utiče na sve klijente!), napadi koristeći otvorene rekurzivne poslužitelje (npr. FER-ovi DNS poslužitelji) za DDoS svrhe
  - iznutra: trovanje (malware ili napadači), neispravne DNS konfiguracije (RFC1918 upiti, A-za-A upiti, upiti za krivim TLD-ovima, dinamički DNS, paketi neispravnog oblika, ...)
  - neispravni klijenti (Windows, stari Un*xi)
  - neispravni/ranjivi poslužitelji (Bind4, Bind8, ...)
  - problemi u mreži se koncentriraju na DNS-ovima

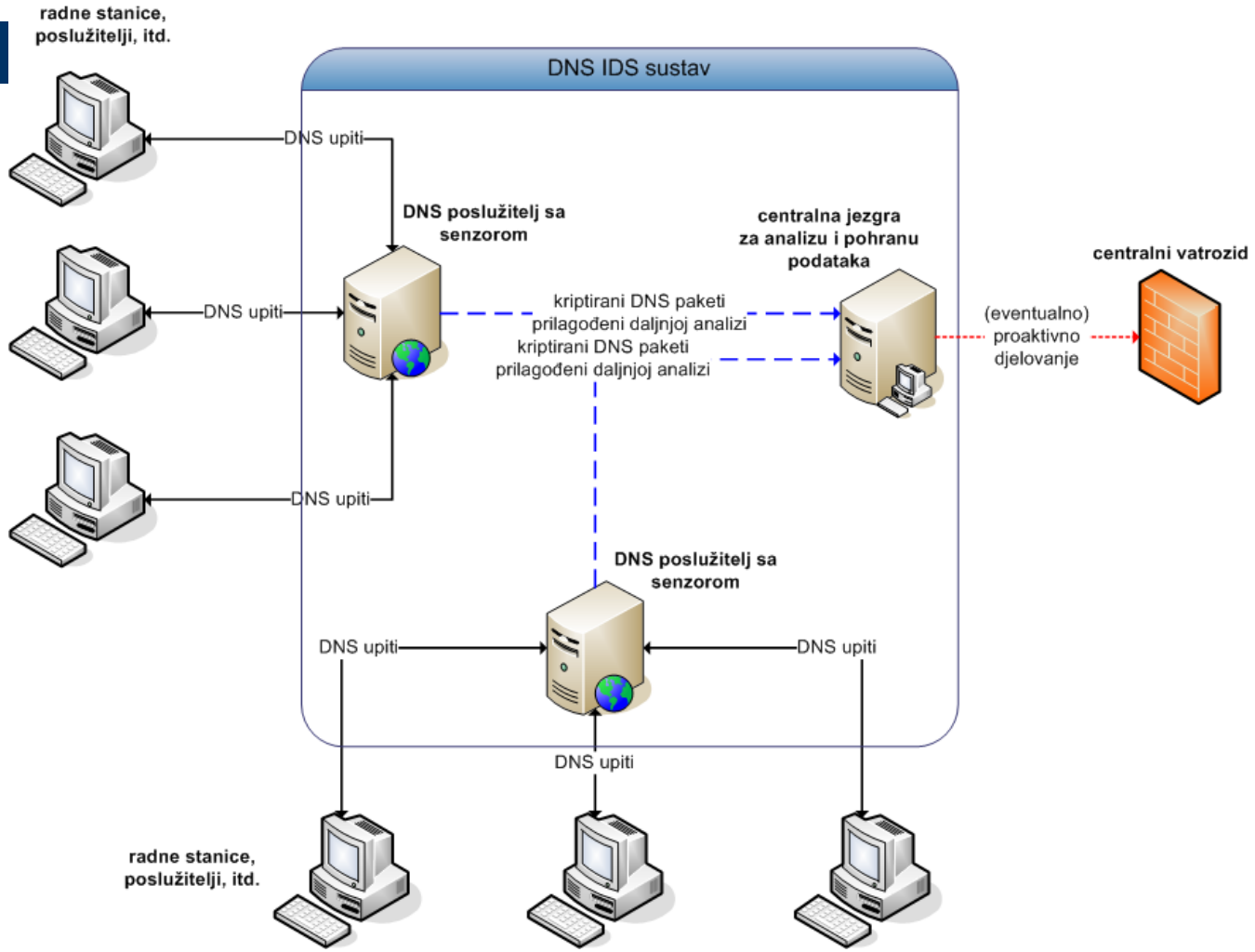
Sigurnosni problemi (2)

- DNS poslužitelji:
  - Bind, MaraDNS, Microsoft DNS, djbdns, PowerDNS, NSD, Posadis, Dnsmasq, Unbound, Simple DNS Plus, CNS, ANS
- problem:
  - slabo ili nikakvo bilježenje incidenata i anomalija
  - slabe mogućnosti bilježenja dolaznog prometa, najčešće nema nikakve mogućnosti bilježenja odlaznog prometa
- ideja: distribuirani DNS IDS/IPS!

DNS analizatori

- postojeći alati:
  - Snort IDS, dnstop, dnspktflow, Wireshark, dnscap
  - bilježenje DNS prometa, grafički prikaz, eventualni prikaz top DNS upita
  - **nisu specijalizirani**, nedostaje:
    - detekcija anomalija/incidenata/napada
    - bilježenje podataka u prezentiranom zapisu iz svih razina (Ethernet, IP, DNS, DNS upit, DNS odgovor)
    - distribuiranost + samostojeći rad
    - dobro skaliranje s opterećenjem, odgovarajuće performanse, itd.

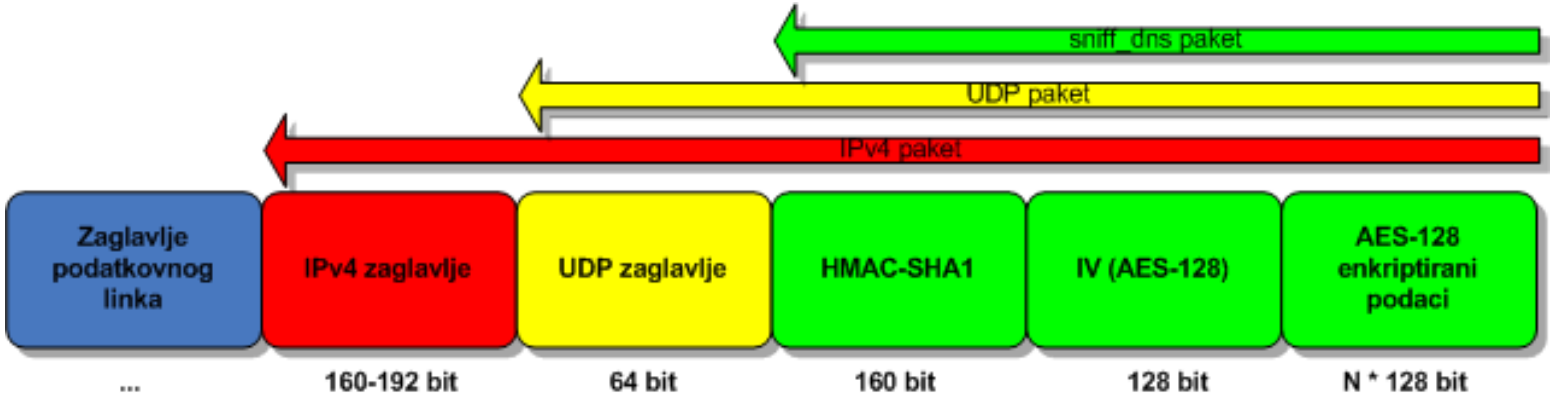
Arhitektura distribuiranog IDS-a



Implementacija DNS IDS-a

- Python - multiplatformsko, prenosivo rješenje
- senzor + centralna jezgra + DNS IDS rutine
- višedretveni rad, redovi poruka, callbackovi
- BPF/PCAP sučelje (raw socket...)
- sukladnost važećim DNS standardima - PROTOS DNS Test Suite: 35 tisuća testova
- minimalan utjecaj na performanse:
  - ispod 5% gubitka vršnih performansi (25000 QPS vs. 26000 QPS), stvarni poslužitelj ~10000 QPS

IDS komunikacijski paket



- efikasno: UDP, male poruke, serijalizacija
- kriptirano između senzora i jezgre: autentikacija, enkripcija, zaštitne sume
- minimalno opterećenje - višedretvenost, efikasne rutine

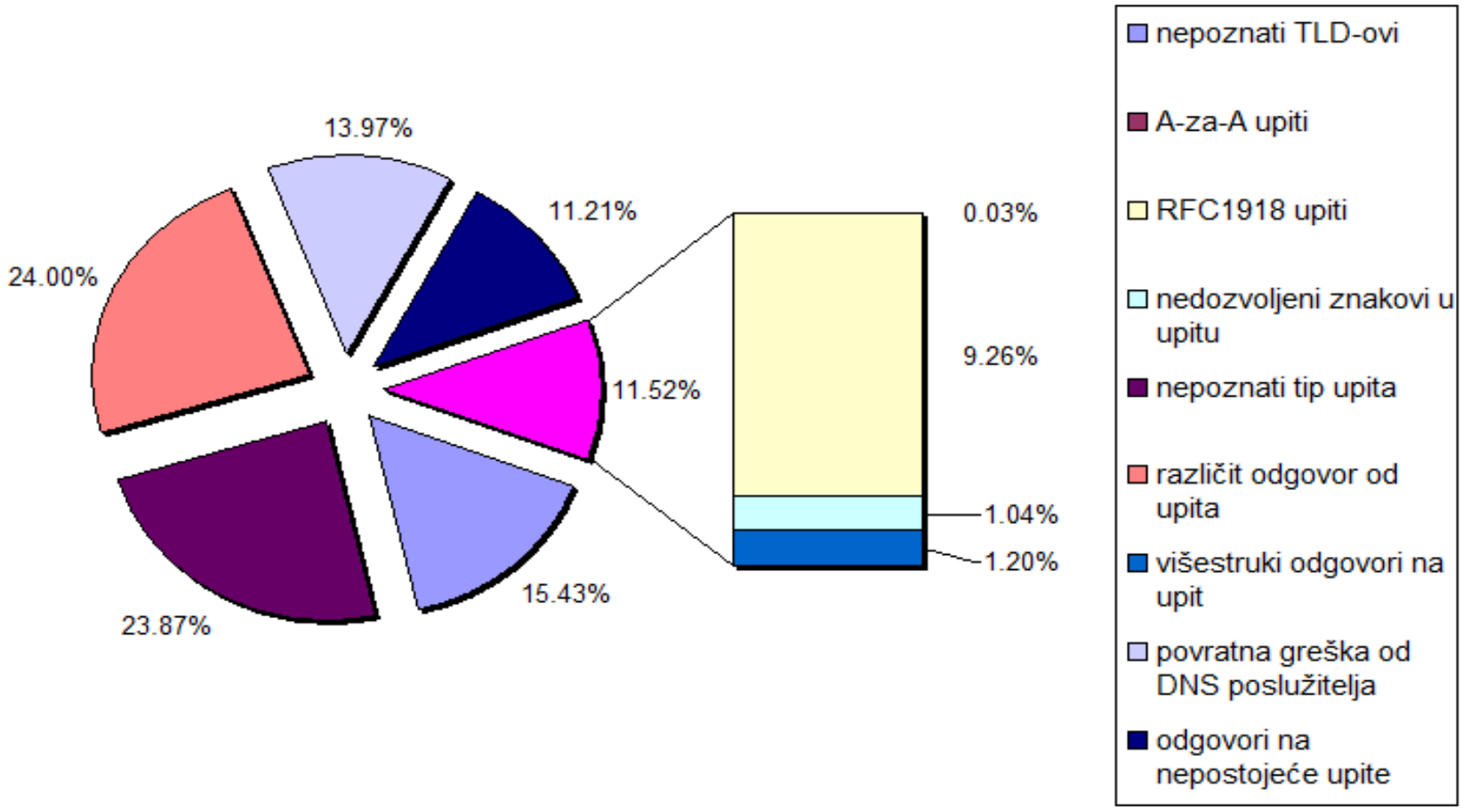
Mogućnosti sustava

- bilježi dolazni i odlazni DNS promet sa svakog senzora (razine: Ethernet, IP, DNS)
- analizira pakete, korelira upite i odgovore
- prepoznaje incidente (12 poznatih tipova) i bilježi
- distribuirani (senzori, jezgra) i samostojeći rad
- nikakav utjecaj na normalan rad (pasivno prisluškivanje)

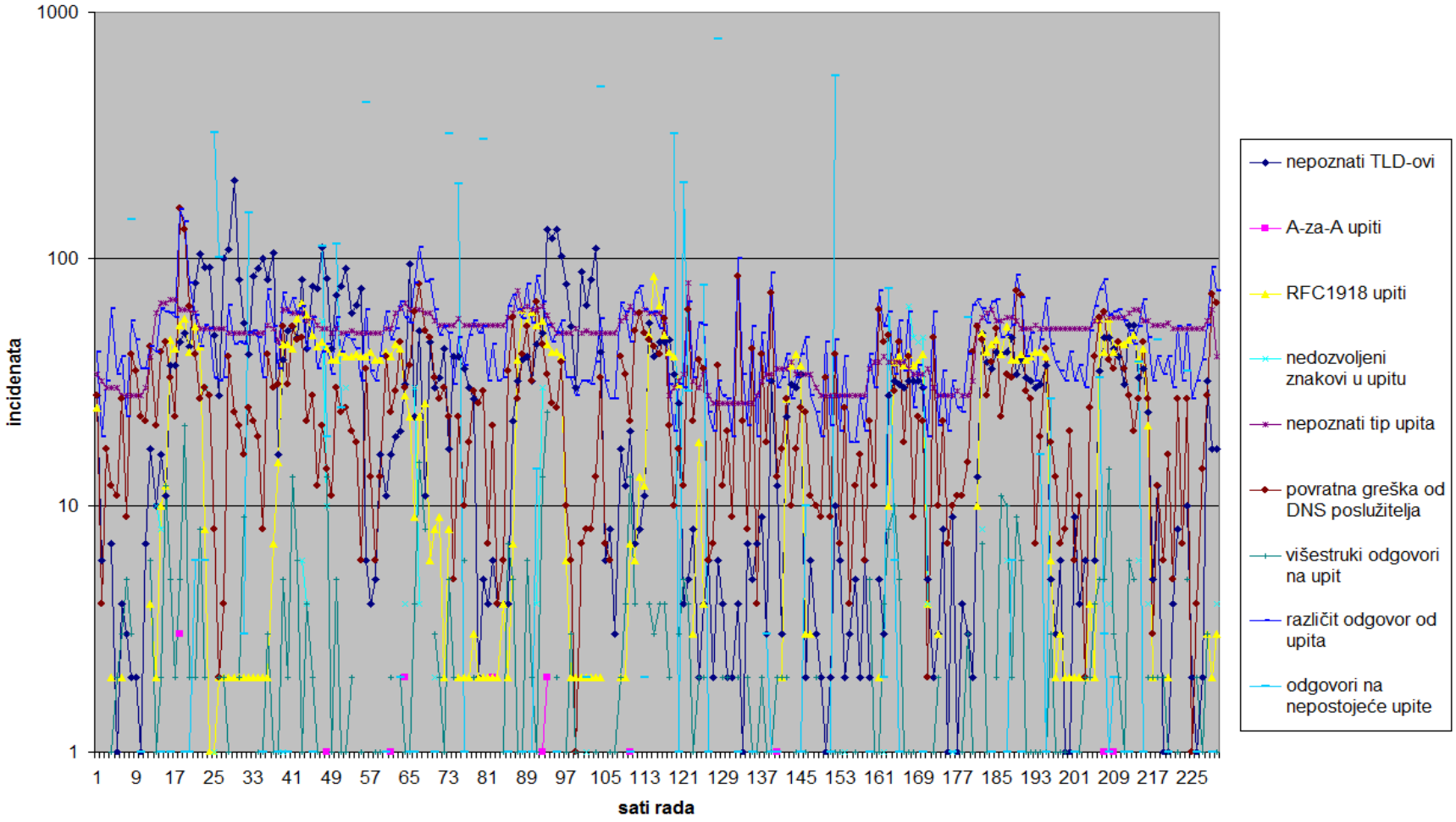
Rezultati - ZEMRIS

- mjerenje na ZEMRIS, FER
  - 60ak računala, manja radna grupa
  - 229 radnih sati
  - 13 milijuna dolaznih i odlaznih DNS paketa
  - 35 tisuća različitih incidenata: prosječno 200 po satu, 0.35% ukupnog prometa
  - 5 tisuća pogrešaka u komunikaciji (neispravni paketi)
  - incidenti pretežno iz lokalne mreže - niz različitih grešaka u DNS konfiguraciji

Raspodjela incidenata - ZEMRIS



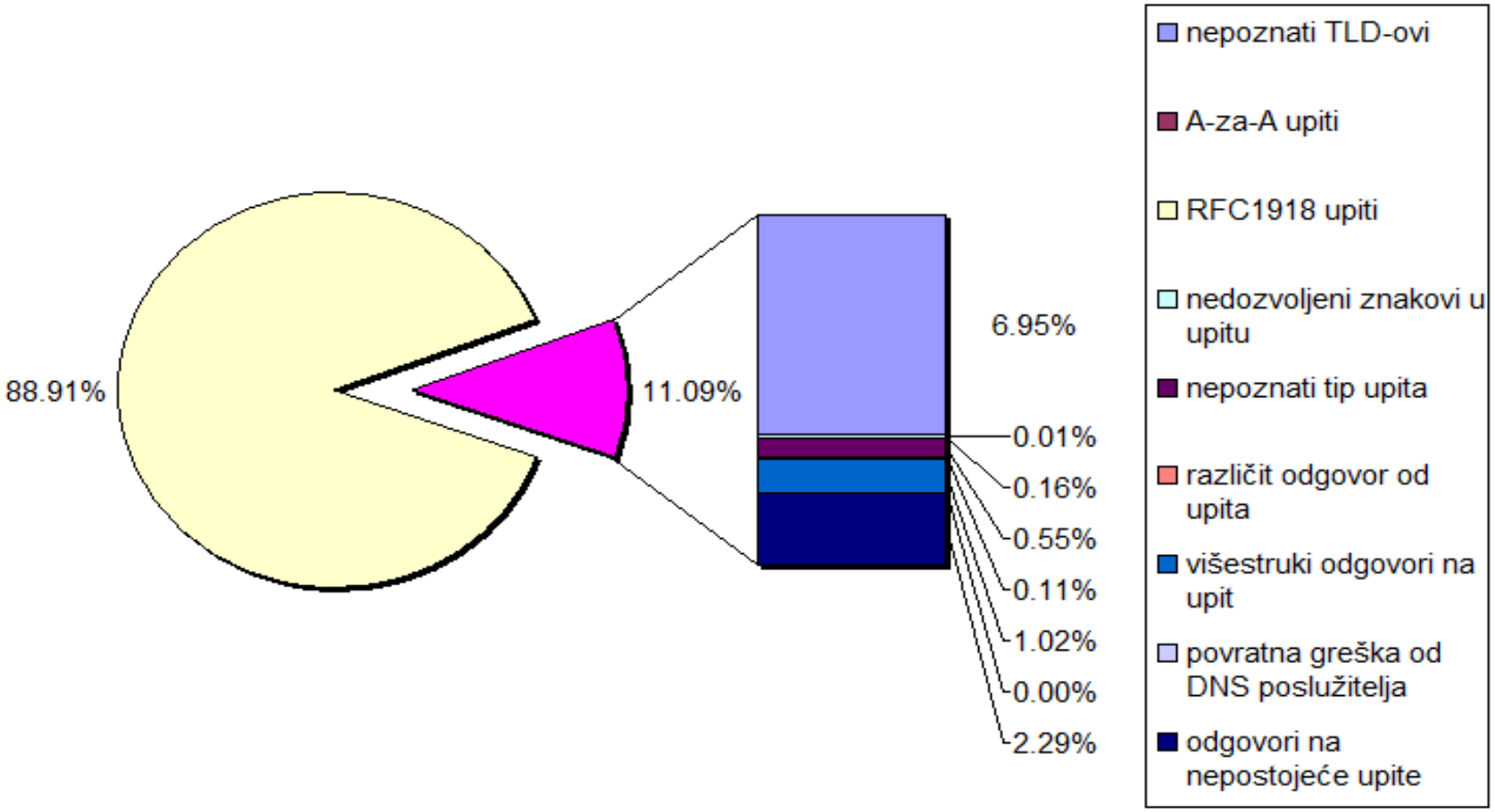
Vremenski prikaz - ZEMRIS



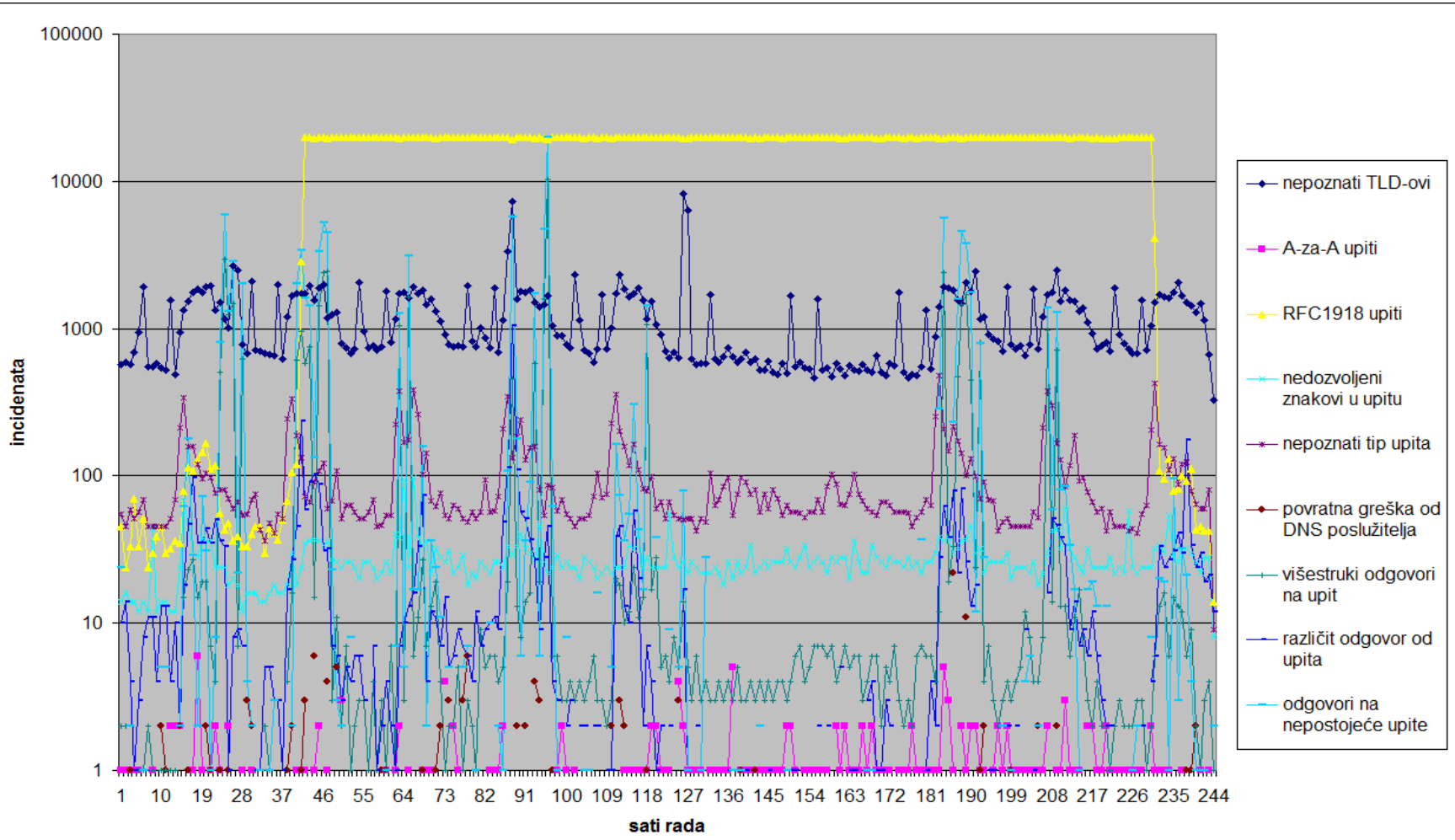
Rezultati - FSB

- mjerenje na centralnom FSB poslužitelju
  - 2000+ računala, različiti OS-ovi i okruženja
  - 243 radnih sati
  - 39 milijuna dolaznih i odlaznih DNS paketa
  - **4 milijuna** različitih incidenata: prosječno **170 tisuća** po satu, 11% ukupnog prometa
  - 7 tisuća pogrešaka u komunikaciji (neispravni paketi)
  - incidenti svih tipova i oblika ...

Raspodjela incidenata - FSB



Vremenski prikaz - FSB



Zaključak

- IDS DNS sustav:
  - moguć i primjeren - bogati rezultati (4+GB zapisa)
  - implementacija zadovoljavajuća: efikasna, stabilna, skromna u potrošnji resursa, prenosiva
- DNS poslužitelji:
  - centralno mjesto gdje je moguće uhvatiti niz incidenata/anomalija
  - moguće otkriti udaljene i lokalne napadače
  - lakše otkrivanje pogrešaka u mrežnoj konfiguraciji (privatne mreže, DNS konfiguracija, viši protokoli)