nedeljainformatike v9.0

Tor mreža

Stefan Ćurčić

Matematička gimnazija

15. 05. 2024.

Agenda

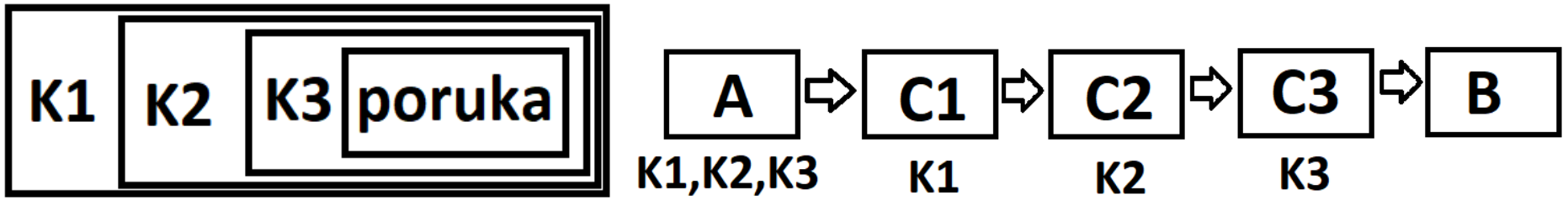
1. Onion rutiranje

2. Onion servisi

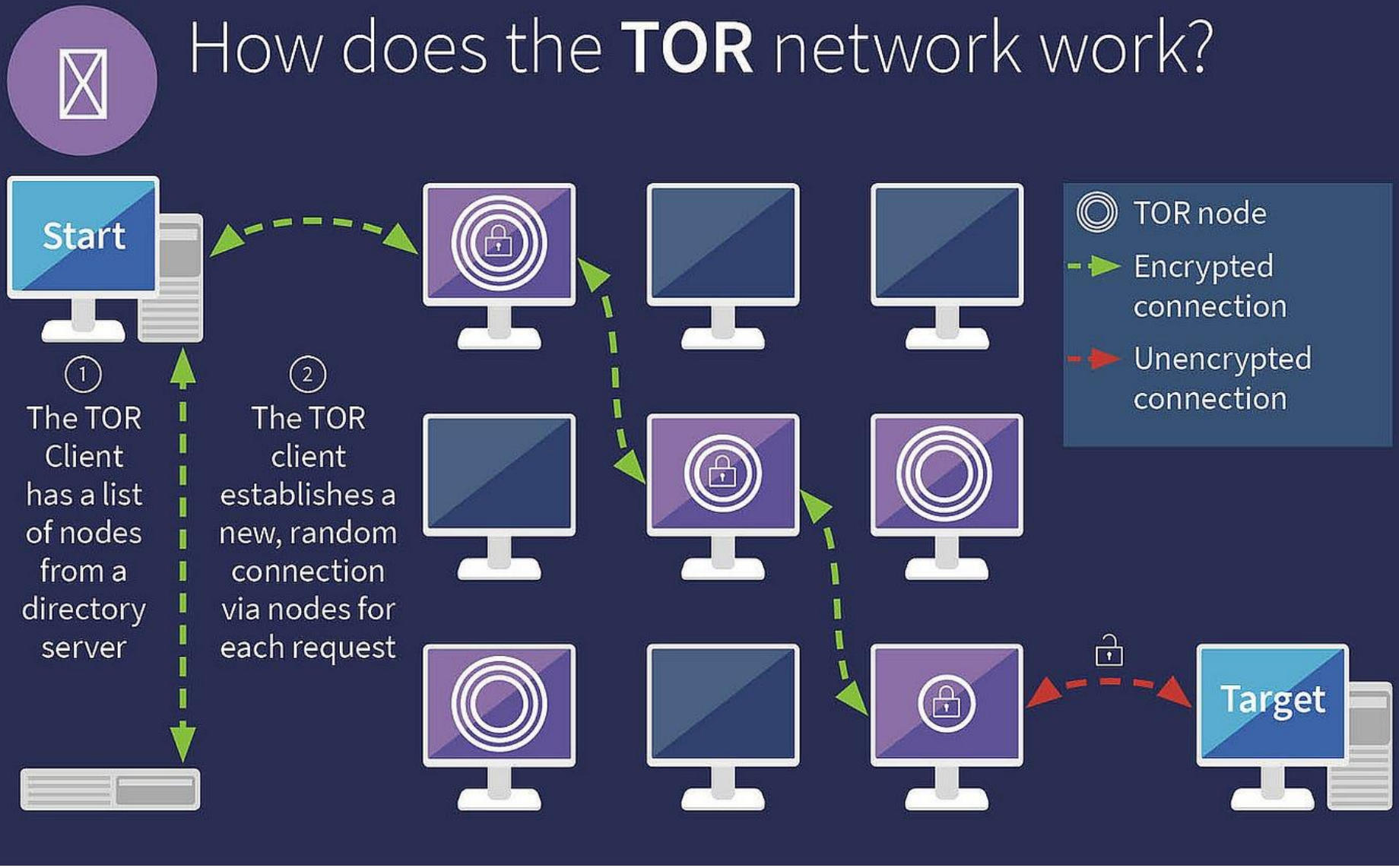
3. Directory authority I blokiranje

Onion rutiranje

- Šta je onion rutiranje (onion routing)?
  - Način anonimne komunikacije više kompjutera preko interneta
  - Poslati podaci ne idu direktno od kompjutera to kompjutera, nego putuju dodatno preko još (obično 3) kompjutera, koji dešifruju podatke koji su im poslati
- Kako se izvršava?
  - Kompjuter A želi da pošalje podatak kompjuteru B
  - A napravi onion rutu kompjutera C1, C2, C3
  - A ima ključeve K1, K2, K3, koje on deli sa C1, C2, C3 koji služe sa enkriptovanje podataka
  - A prvo šifruje podatak ključem K3, pa onda K2, pa onda K1
  - Taj podatak C1 dešifruje sa K1 pa salje C2, C2 dešifruje i salje C3 i on dešifruje i šalje B



Onion rutiranje



Onion rutiranje

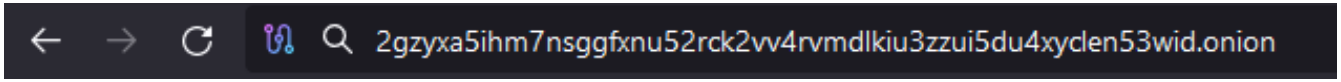
- Šta smo postigli?
  - Pošto je onion rutiranje **ANONIMNI** način da se komunicira preko interneta, cilj je da niko ko prisluškuje ne može znati da kompjuter A komunicira sa kompjuterom B
  - Ako neko prisluškuje kompjuter A, on vidi da on šalje podatak C1
  - Ako neko prisluškuje C1, idalje ne može saznati gde je on poslao tu poruku
  - Ni jedan od kompjutera ne zna kompletnu putanju podataka (sem A), nijedan ne može da zaključi da B šalje podatak ka A.

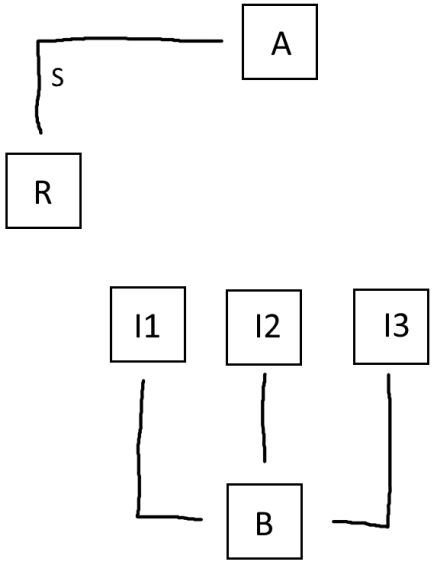
Agenda

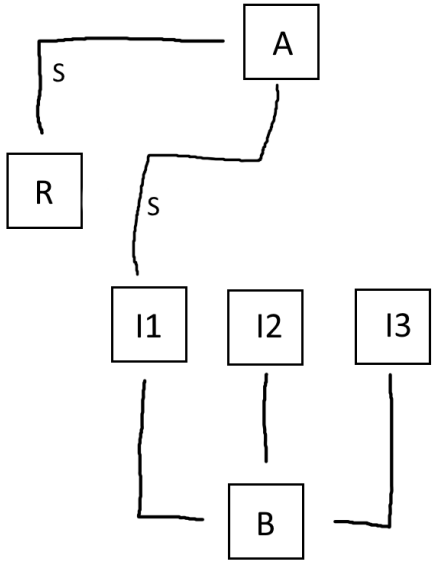
1. Onion rutiranje
2. Onion servisi
3. Directory authority I blokiranje

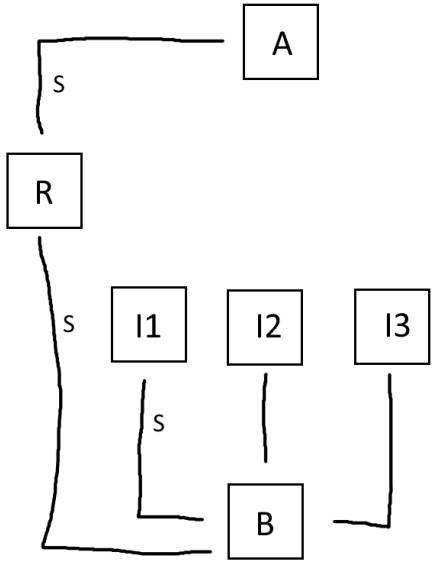
Onion servisi

- U prethodnom slučaju A zna koja je adresa od B, ali šta ako B želi da ostane anoniman?
- B pravi tzv. onion servis
- Bira 3 kompjutera na toru, formira rutu do njih (2 tor kompjutera između)
- A pravi rutu, i sa poslednjim kompjutera u toj ruti komunicira sa jednim od 3 kompjutera koji reprezentuje B, i onda se poveže na B



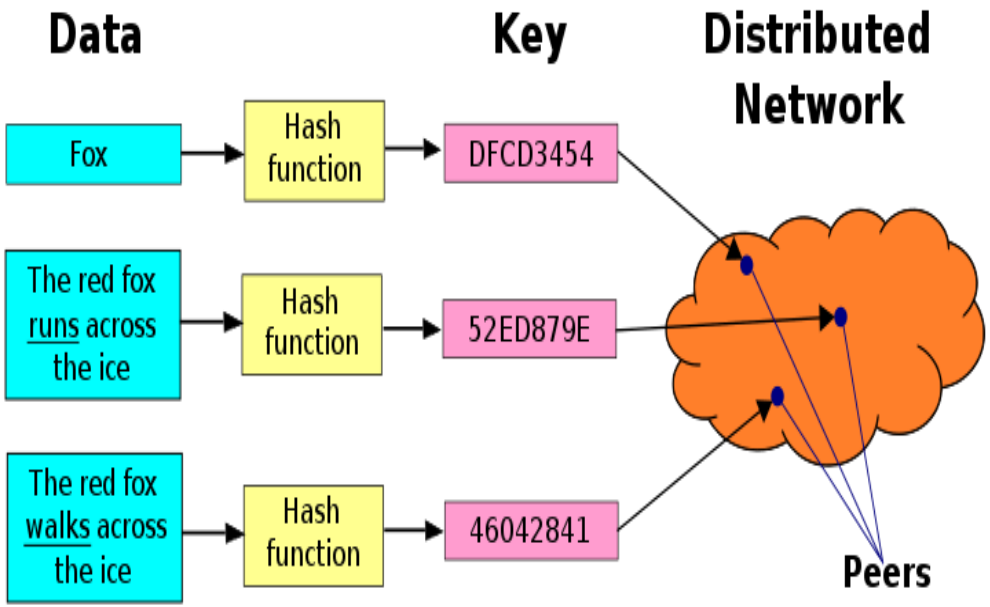


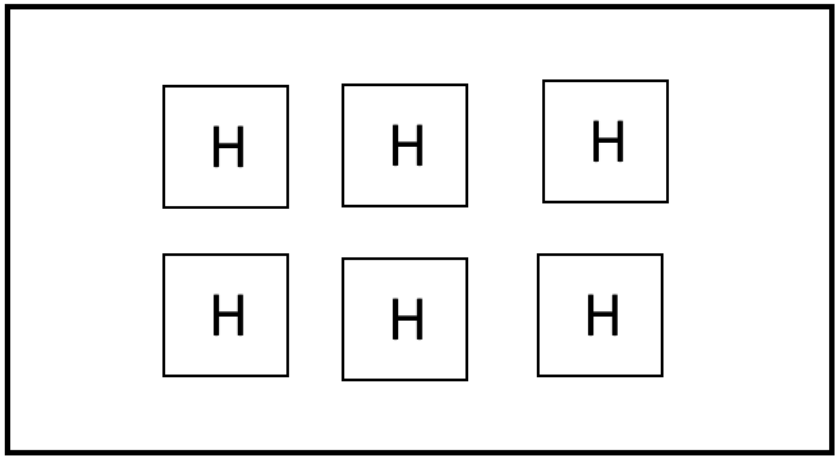




Onion servisi

- **Distributed Hash Table**





(K, V): K <= H1 <= H2 <= H3

(K, V) ⇨ H1

(K, V) ⇨ H2

(K, V) ⇨ H3

Agenda

1. Onion rutiranje
2. Onion servisi
3. Directory authority I blokiranje

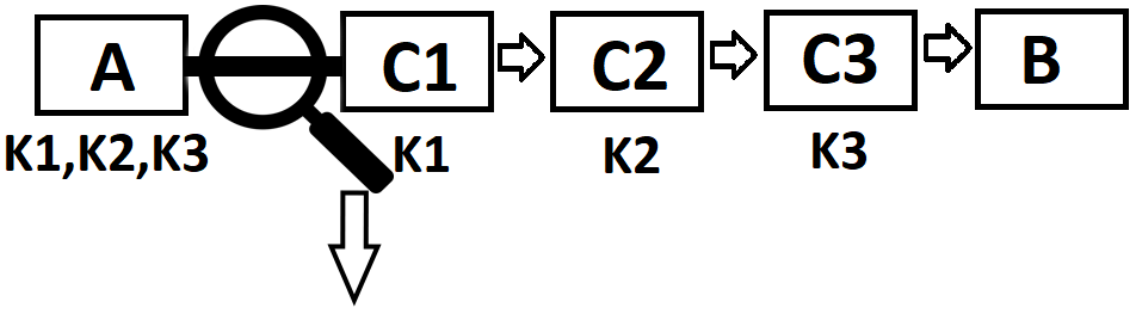
Directory authority I blokiranje

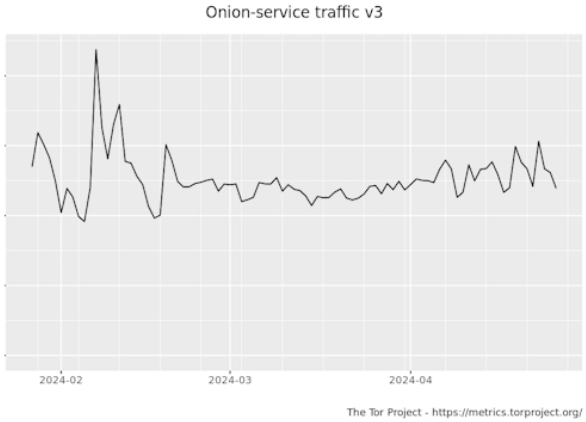
- Pridruživanje na tor mrežu se vrši preko Directory Authorities (DA)
  - DA daju informacije o tor nodovima na koje se naš računar povezuje
  - Trenutno, ima ih 9
  - U njih ide velika količina poverenja, mogući teoretski napadi

Nickname†	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
dannenberg (1)	100 KiB/s	3d 14h		193.23.244.244	2001:678:558:1000::244			443	80	Relay
Serge (3)	100 KiB/s	3d 4h		66.111.2.131	2610:1c0:0:5::131			9001	9030	Relay
dizum (1)	88 KiB/s	5d 3h		45.66.35.11	-			443	80	Relay
tor26 (1)	75 KiB/s	2d 9h		217.196.147.77	2a02:16a8:662:2203::1			443	80	Relay
bastet (1)	50 KiB/s	29d 2h		204.13.164.118	2620:13:4000:6000::1000:118			443	80	Relay
maatuska (3)	50 KiB/s	64d 22m		171.25.193.9	2001:67c:289c::9			80	443	Relay
moria1 (1)	40 KiB/s	5d 17h		128.31.0.39	-			9201	9231	Relay
gabelmoo (1)	40 KiB/s	32d 2h		131.188.40.189	2001:638:a000:4140::ffff:189			443	80	Relay
longclaw (1)	38 KiB/s	5d 27m		199.58.81.140	-			443	80	Relay
Total	**581 KiB/s**									

Directory authority I blokiranje

- Da li neko zna da li koristimo tor?





Tor?

Directory authority I blokiranje

- Pod nekim okolnostima, u nekim državama, nije dozvoljeno pristupati toru, specifično nije dozvoljeno napraviti vezu sa jednim od DA
  - IP adrese tor nodova su javne
  - Bridges (mostovi) rešavaju taj problem
  - Idalje problem nadziranja, nekad se zahtevaju pluggable transports
    - obfs4
    - meek-azure
    - Snowflake
    - WebTunnel

Hvala na pažnji!

Pitanja?