ВИСОКА ПОСЛОВНА ШКОЛА
СТРУКОВНИХ СТУДИЈА – БЛАЦЕ
Часопис из области економије, менаџмента и информатике *„БизИнфо“*
Година 2013, годиште 4, број 2, стр. 39-48
Адреса: Краља Петра I, бр.70, 18420 Блаце

Стручни рад

УДК: 004.7 ; 004.715

OSTVARIVANJE ANONIMNOSTI NA INTERNETU KORIŠĆENJEM TOR MREŽE

CREATING ANONYMITY ON THE INTERNET USING TOR NETWORK

Vladica Ubavić[1]
Danilo Oklobdžija
Visoka poslovna škola strukovnih studija Blace

Rezime: *Na samom početku pitamo se šta je to zapravo anonimnost. Biti anónima, na Internetu znači da ne želimo ostavljati ikakav trag o svojoj prisusnosti ili ne želimo otkriti svoj identitet. Anonimnost na Internetu daje veću hrabrost u samoj komunikaciji načinu na koji radimo, kometarišemo ili pišemo blogove. Anoniman rad drastično se razlikuje od rada na „mreži“ gde ostavljamo svoje tragove. Ipak pitamo se da li je anonimnost uopšte važna i koji su razlozi da neka osoba uopšte želi biti anonimna. Važno je da ne ostavljamo lične podatke na Internetu ako ne želimo da se neko njima posluži.Na kraju krajeva, svako je sam odgovoran i zadužen za svoju privatnost. Tu kao odgovor nastupa* ***“Onion routing“.***
Ključne reči: *anonimnost, TOR, sigurnost, onion*

Abstract: *At the beginning I wonder what it is actually anonymity. Being anonymous on the Internet means that we do not want to leave any trace of their prisusnosti or do not wish to reveal their identity. The anonymity of the Internet gives more courage in itself communicate the way we work, commenting or writing blogs. Anonymous work is drastically different from the work on the*

[1] ubavic@vpskp.edu.rs

"network" which leaves their mark. Yet we wonder whether the general anonymity is important, and what are the reasons that some people do want to be anonymous. It is important not to leave personal information on the Internet if you do not want to be someone they serve. However, everyone was responsible and in charge of their privacy. This response performance, "Onion routing".
Key words: *anonymity, TOR, security, onion*

1. UVOD

Sama arhitektura odnosno samo funkcionisanje Interneta kao globalne mreže po sebi ne osigurava anonimnost. Zaglavlje svakog IP paketa sadrži podatke pomoću kojih se vrlo lako dolazi do samog izvora. Adresa izvora koja, s obzirom na blok IP adresa kojoj pripada, može odati davaoca usluga (provajdera) Interneta (engl. Internet Service Provider), a samim time i geografsku lokaciju samog korisnika. Naravno po slovu zakona Internet provajderi su dužni da uz sudski nalog, na temelju IP adrese i vremena korišćenja, pruže informacije o stvarnom pretplatničkom identitetu korisnika, što se neretko zloupotrebljava u raznorazne svrhe. Situacija je malo drugačija kod privatnih mreža. Zbog relativno malog broja IPv4 adresa, za upotrebu u privatnim mrežama rezervisane su privatne IP adrese. U slučaju izlaska paketa iz privatne mreže na Internet, koristimo NAT (engl. Network Address Translation) koji privatne (lokalne) IP adrese multipleksira na javne IP adrese. NAT, dakle, donekle čuva anonimnost korisnika sa privatnom adresom jer više korisnika komunicira sa WAN mrežom (Internetom) pomoću jedne javne IP adrese koju dodeljuje provajder. Da bi adekvatno odgovorili izazovu anonimnosti moramo upoznati načine odavanja identiteta, odnosno metode narušavanja anonimnosti.

Po snazi napada napadač može biti aktivan odnosno unutrašnji ili pasivan odnosno spoljašni. *Aktivni ili unutaršnji napadač* može kompromitovati odnosno ugroziti čvorove, ili upravljati delom čvorova sistema i samim tim može menjati poruke odnosno pakete. *Spoljašnji* ili *pasivni napadač* ne može kompromitovati veze, nema kontrolu nad nijednim čvorom, ali može prisluškivati saobraćaj među njima.

Po opsegu napada napadač može biti lokalani ili globalani. *Globalni napadač* je sveprisutan i ima pristup celoj mreži odnosno svim

vezama i čvorovima. *Lokalni napadač* je ograničeno prisutan i ima pristup delu mreže odnosno samo delu veza i čvorova.

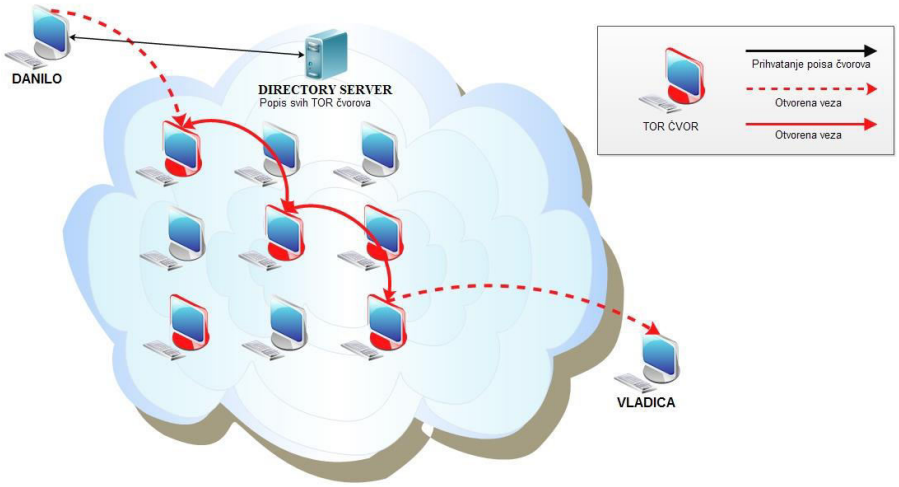
Po prilagodljivosti napadač može biti statički ili dinamički. *Dinamčki napadač* prikuplja sve raspoložive podatke sa kompromitovanih veza i čvorova kako bi otkrio ko je poslao ili primio paket, tj. koristi apriorno znanje (znanje koje je nezavisno od iskustva) i aposteriorono tj. odnosno znanje (znanje koje je stečeno iskustvom). *Statički napadač* koristi samo apriorno znanje.

Slojevito rutiranje (engl. onion routing) je mehanizam koji omogućava anonimnu komunikaciju korišćenjem prekrivajuće (engl. overlay) mreže niske latencije.

2. PRINCIP RADA TOR MREŽE

Za razliku od drugih sistema anonimnosti koji zahtevaju primenu posebnih aplikacija ili dodataka, slojevito rutiranje mogu primeniti sve aplikacije koje koriste SOCKS (engl. Socket Secure) protokol. Slojevito rutiranje opslužuju čvorovi zvani slojeviti ruteri (engl. onion routers), ili kraće "OR", preko kojih putuju poruke raznim, za posmatrača nepoznatim, putevima. Klijent bira put kroz mrežu sačinjen od čvorova (engl. nodes) i stvara "krug" (engl. circuit), u kome svaki čvor zna samo ko mu je poslao paket i kome paket treba proslediti. To znači da ni jedan čvor u krugu ne poznaje čitav put odnosno odakle je poslata poruka ni kome je namenjena. Komunikacija klijenta putuje porukama koje se na izvorištu višestruko kriptuju simetričnim ključem, dogovorenim sa svakim ruterom. Kriptovane poruke se šalju u krug. Višestruko slojevita struktura podataka koja enkapsulira saobraćaj namenjen pojedinom čvoru se zove *slojevita poruka* (engl. onion). U svakom čvoru kruga se dekriptuje jedan "sloj", slično ljušćenju slojeva luka, i "oljuštena" poruka se šalje sledećem čvoru na putu. Postupak se ponavlja u sledećem čvoru sve dok poruka ne stigne do zadnjeg čvora u krugu. Tamo se "ljušti" zadnji sloj kriptovanja i dobija čist podatak koji napušta krug do svog odredišta. Slika 1 prikazuje skup računara spojenih na Internetu, od kojih su neki Tor ruteri. Vlada bira tri rutera, gradi krug kojim uspostavlja anonimni kontakt sa Danilom. Sva komunikacija do zadnjeg rutera u krugu je kriptovana, a iz mreže Tor izlazi kao čist podatak.

Slika 1. Primena TOR rutera



Kako bi mogao koristiti mrežu, Danilo mora na svom računaru instalirati Tor aplikaciju (posrednik) (*engl. onion proxy*). Tor je aplikacija koja se izvršava kao korisnički proces bez posebnih prava. Pre nego što može da počne da koristi mrežu Vlada mora da zna kako da dođe do Tor čvora, stoga se povezuje na server imenika (*engl. directory server*) koji poseduje spisak svih TOR rutera (*engl. onion router*). Popis čvorova mreže naziva se koncenzus stanja mreže (*engl. network status consensus*).

Nakon što je dohvatio koncenzus stanja mreže, Vlada nasumce odabira jedan čvor iz konsenzusa i otvara Tor vezu prema njemu. Potom prvom ruteru naređuje da otvori Tor vezu prema sledećem ruteru. Na isti način drugi ruter otvara Tor vezu prema zadnjem ruteru. Takođe, svaki TOR ruter ugovara poseban ključ veze sa svakim čvorom na putu i time osigurava da nijedan čvor, izuzev onog kojem je poruka namenjena ne može prisluškivati saobraćaj. Sve TCP veze između čvorova zaštićene su TLS (engl. Transport Layer Security) protokolom.

Tor, kao što smo rekli, podržava isključivo povezivanje preko TCP-a. Mogu ga upotrebiti sve aplikacije koje koriste SOCS protokol, dakle mora postojati lokalno instalirani web proxy. Ako korisnička aplikacija ne koristi SOCS, nego sama vrši DNS razrešavanje adresa time odaje IP adresu računara domaćina i samim tim kompromituje identitet. Ovo se naziva (*DNS curenje).*

Ako korisnička aplikacija uvek koristi web proxy u radu, tada Tor anonimizuje TCP tunele klijentskih aplikacija, ali ne deluje iznad sloja sesije OSI modela. Efektivno, ako tunelizovani saobraćaj kroz virtuelni kanal sadrži IP adresu i ona stigne na odredište, znači da je samo izvorište kompromitovano. Naravno doći do IP adrese klijenta uz pomoć raznih dodataka plaginova koje korisnik sam instalira u svoj pretraživač je veoma lako: JavaScript, Java appleti, Flash i Adobe dodaci za pretraživač samo su neki od mogućih sigurnosnih propusta. Kolačići (*engl. cookie*) su takođe ozbiljan sigurnosni rizik.

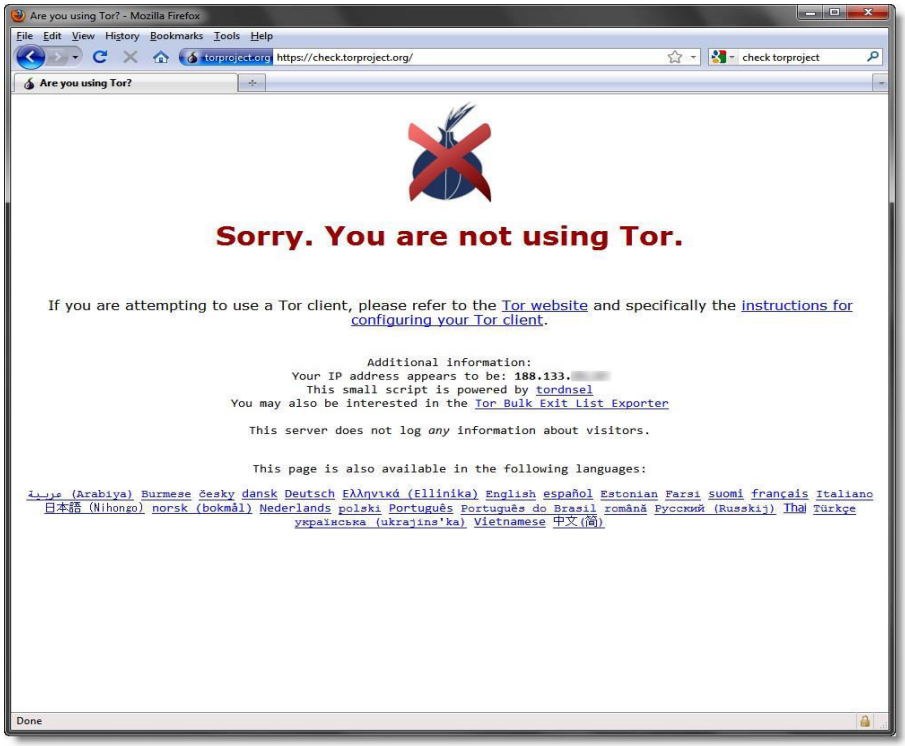
Ovaj problem može se rešiti na nekoliko načina. Osim standardnog web pretraživača, preporučuje se instalacija još jednog pretraživača za anonimni saobraćaj. "Službeni" pretraživač je *Firefox* s Torbutton dodatkom kojim je moguće isključiti sve poznate opcije koje mogu odati IP adresu. Takođe, postoji još niz drugih pretraživača prilagođenih anonimnom saobraćaju Tor mrežom. Postoji i varijanta gde se pretraživač može kopirati na USB memoriju, i samim tim koristiti bez instalacije te se svi generisani (privremeni) podaci zapisuju na USB memoriju. Nadalje postoje i *LiveCD* distribucije Linux operativnih sistema (*Amnesia*, *Incognito, Tork, JanusVM*) u kojima su svi servisi pročišćeni na takav način da ne odaju osetljive informacije. Odabir same metode zavisi o visini željene anonimnosti.

Nedavno je izašao i *Silvertunnel* pretraživač pisan u Java programskom jeziku. Enkapsulira posrednika bez funkcije rutera pa samim tim ne zahteva instalaciju Tor aplikacije na računar domaćina. Postoji međutim jedan nedostatak: potrebno je instalirati JRE na računar domaćina. Ukoliko je JRE instaliran, Silvertunnel se pokreće klikom pomoću JNLP tehnologije.

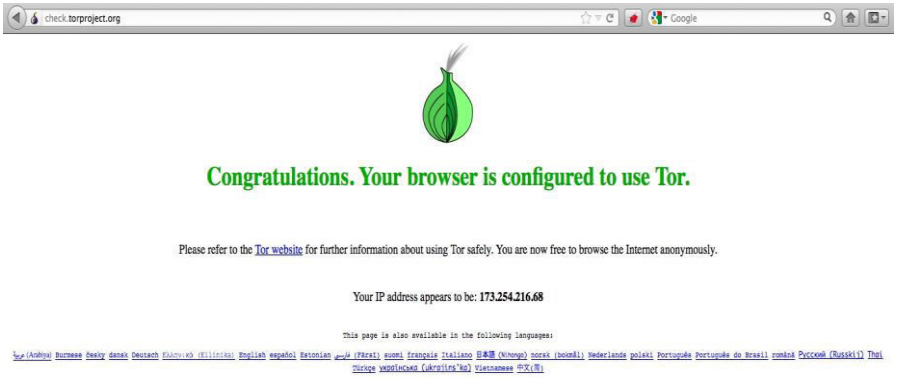
Po pokretanju, odmah se povezuje na Tor mrežu. Kroz statistuku lakoće instalacije i same jednostavnosti korišćenja bez sumnje je nejupotrebljeniji klijent za Tor mrežu.
Tor poseduje jednostavan način provere da li smo na anonimnoj odnosno TOR mreži ili ne. Dovoljno je posetiti sledeći link https://check.torproject.org/

Na sledećim slikama je prikazan pretraživač koji koristi Tor mrežu i pretraživač koji ne koristi Tor mrežu.

Slika 2. Pretraživač ne koristi anonimnu (TOR) mrežu



Sl.3 Pretraživač koristi anonimnu (TOR) mrežu



Što se tiče Tor protokola u njemu postoje dve vrste čvorova:

- *onion proxy* – Klijent
- *onion router* – Tor ruter

Svaki TOR ruter može obavljati jednu ili više od sledećih funkcija:

- *directory authority* – je ruter koji je ujedno ruter i imenik, odnosno opslužuje koncenzus stanja mreže
- *directory cache* – ruter koji ujedno rasterećuje server imenika preuzimajući u potpunosti distribuciju opisa rutera
- *bridge router* – ruter koji služi isključivo prenosu Tor saobraćaja pa se ne nalazi u koncenzsusu stanja mreže, već u posebnim listama koje se održavaju i preuzimaju ručno. Postoje kako bi se Tor mreži moglo pristupiti ukoliko korisnikov ISP blokira Tor saobraćaj.
- *exit router* – ruter koji omogućuje spajanje na mrežna odredišta izvan Tor mreže

- *hidden service* – ruter koji je ujedno i izvršitelj skrivene usluge

- *hidden service directory* – ruter koji je ujedno i davaoc registra skrivenih usluga

- *introduction point* - ruter koji ujedno služi kao čvor uvoda skrivene usluge, odnosno posrednik u procesu povezivanja

- *rendezvous point* – ruter preko koga komuniciraju skrivena usluga i sam klijent

Kako bi posrednik mogao konstruisati i planirati put za virtualni kanal mora znati kakva je izlazna politika poslednjeg čvora na putu, pa samim tim mora takođe znati i verziju protokola svakog rutera na putu. Ovi podaci navedeni su u imeniku rutera. Ruteri prijavljuju značajniju promenu stanja svim davaocima imenika mreže za koje znaju slanjem opisa potpisanog svojim tajnim ključem.
Davaoci imenika stanja mreže smatraju se komponentama od velikog poverenja i stvaraju konsenzus stanja mreže glasanjem.
Integritet i autentičnost toka saobraćaja kroz Tor mrežu osigurana je, osim činjenicom da koristi TLS protokol i upotrebom vlastite simetrične i asimetrične kriptografije, Diffie-Hellmanovg protokola.

- Simetrična kriptografija - 128-bitni AES algoritam

- Asimetrična kriptografija – 1024-bitni RSA algoritam

- Protokol Diffie-Hellman

- SHA-1 algoritam

Čvorovi koriste ključeve za enkripciju veze:

- Asimetrični ključ veze rutera – služi za (de) kriptovanje TLS kanala. Trajanje: reda veličine jednog dana (PK^{TLS}, SK^{TLS})

- Simetrični ključ za enkripciju saobraćaja AES algoritmom na virtualnom kanalu dogovoren protokolom Diffie-

Hellman (K^{OP-OR})

Ključevi koji se koriste autentifikaciju veze:

- Lukov ključ rutera – služi za (de) kriptovanje zahteva za otvaranjem virtualnih kanala.
  Trajanje: reda veličine jednog dana (PK^{ON} , SK^{ON})

Kako bi se osigurao integritet konsenzusa mreže, koriste se sledeći asimetrični ključevi:

- Ključ identiteta davaoca imenika – služi za potpisivanje sertifikata koji garantuje verodostojnost ključa za potpisivanje konsenzusa stanja mreže. Trajanje: od tri do dvanaest meseci. (PK^{DA} , SK^{DA})

- Ključ za potpisivanje glasova i koncenzusa stanja mreže– Trajanje: nije navedeno, najverovatnije do mesec dana. (PK^{sgnDA} , SK^{sgnDA})

- Ključ identiteta rutera – služi za potpisivanje TLS sertifikata i directory servera.
  Trajanje: do mesec dana. (PK^{ID} , SK^{ID})

3. ZAKLJUČAK

Pojam anonimne komunikacije vrlo je mlad i vezuje se za sam početak 1981. godine. Prva anonimna mreža s visokim kašnjenjem krenula je sa radom devedesetih, dok je prva anonimna mreža s niskim kašnjenjem implementirana početkom 21. veka. Pošto je to veoma novo područje, postoji još dosta pitanja vezanih za anonimizaciju komunikacije preko računarskih mreža.

U nekim delovima sveta gde ne postoji slobodno komuniciranje Internetom, sloboda govora, a pogotovo tamo gde gotovo ne postoji sloboda mišljenja, raste i ogromna potreba za anonimnošću. Na mreži je prikupljanje informacija o pojedincima, njihovom učešću u diskusionim grupama, blogovima ili postovima sve češće i obilnije. To je razlog da i osobe u razvijenim demokratskim državama žele sačuvati svoje delove života svojim, odnosno tajnim. Anonimnost i tajnost su stvarne potrebe modernog društva.

Trenutno ne postoji opšteprihvaćeni i sveobuhvatni Internet standard

koji nam može omogućiti odnosno osigurati anonimnost, već postoje pojedine aplikacije odnosno razne implementacije koje se još uvek razvijaju. Jedan od tih Sistema anonimnosti je i Tor.

Međutim sama anonimnost vrlo lako oslobađa od odgovornosti što neretko mnogi iskorišćavaju, samim tim dovodeći u pitanje postojanje anonimnih sistema. Jedan od glavnih načina kojim se pokušavaju smanjiti zloupotrebe u takvim mrežama su reputacijski sistemi. Međutim, postoji veliki problem jer su reputacije vezane za identitet pa je poseban izazov implementirati reputaciju i istu sakriti u jednom anonimnom sistemu.

REFERENCE

1. Atul Singh, Tsuen-Wan "Johnny" Ngan, Peter Druschel, Dan Wallach, "Eclipse Attacks on Overlay Networks: Threats and Defenses". *IEEE Infocom* , 2006.

2. Tor official web site documentation. URL: https://www.torproject.org/docs/documentation.html.en

3. Tor Tor (anonymity network) From Wikipedia, the free encyclopedia.URL: https://www.torproject.org/docs/documentation.html.en

4. Tor Status URL:

http://torstatus.blutmagie.de/

5. Attacking Tor: how the NSA targets users' online anonymity

URL: http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

6. Tor Network Status - Network Detail
URL: http://torstatus.blutmagie.de/network_detail.php

7. Electronic Frontier Foundation – What is TOR
URL: https://www.eff.org/torchallenge/what-is-tor

Rad je primljen 11.12.2013.
Prihvaćen za objavljivanje 16.12.2013.