HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Tor - mreža za anonimnost

CCERT-PUBDOC-2007-07-197

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument, koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument predstavlja vlasništvo CARNet-a (CARNet CERT-a). Namijenjen je za javnu objavu, njime se može svatko koristiti, na njega se pozivati, ali samo u originalnom obliku, bez ikakvih izmjena, uz obavezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima, povreda je autorskih prava CARNet-a, sukladno Zakonu o autorskim pravima. Počinitelj takve aktivnosti podliježe kaznenoj odgovornosti koja je regulirana Kaznenim zakonom RH.

Sadržaj

1. Uvod

Tor (eng *The Onion Router*) je besplatna implementacija druge generacije tzv. *onion* mrežnog usmjeravanja. Riječ je o sustavu koje omogućuje sigurno i anonimno korištenje Interneta, pretraživanje i objavljivanje web stranica, korištenje sustava trenutnih poruka te usluga koje koriste IRC (eng. *Internet Relay Chat*), SSH (eng. *Secure Shell*) i ostale protokole građene na TCP (eng. *Transmission Control Protocol*) protokolu. Tor pored toga predstavlja platformu koja omogućuje izgradnju novih aplikacija s ugrađenim mogućnostima zaštite privatnosti korisnika i različitim sigurnosnim elementima.

Sigurnost i anonimnost Internet prometa Tor osigurava sprečavanjem analiziranja ostvarenog mrežnog prometa, oblika mrežnog nadzora koji može ugroziti anonimnost i privatnost korisnika te povjerljive poslovne aktivnosti. Komunikacija se preusmjerava unutar distribuirane mreže poslužitelja, tzv. *onion* poslužitelja, čime se korisnika štiti od web stranica koje neovlašteno sakupljaju podatke o posjetiteljima, od napadača koji pokušavaju steći pristup potencijalno osjetljivim podacima pa čak i od samih *onion* poslužitelja.

Pojedinci Tor koriste kako bi web stranicama onemogućili praćenje njihovih aktivnosti te za pregledavanje web stranica ili za povezivanje na sustave trenutnih poruka koje njihovi lokalni davatelj Internet usluga blokiraju. Tor također omogućuje objavljivanje web stranica i drugih usluga bez otkrivanja njihove lokacije. Učestala je upotreba ovog sustava za socijalno osjetljivu komunikaciju, kao što su sobe za razgovor ili web forumi namijenjeni žrtvama nasilja ili oboljelim osobama.

Novinari koriste Tor za sigurnu komunikaciju s prokazivačima i disidentima. Članovi različitih nevladinih organizacija, tijekom boravka u stranim zemljama, pomoću Tor mreže prikrivaju posjećivanje web stranica svojih organizacija. Unutar velikih tvrtki Tor sustav koristi se za sigurno provođenje analize konkurentnosti te kao zamjena za tradicionalne VPN (eng. *Virtual Private Network*) mreže koje otkrivaju točno vrijeme provođenja komunikacije kao i količinu prenesenih podataka.

Raznolikost korisnika Tor mreže dodatno povećava razinu privatnosti jer se Internet aktivnosti pojedinog korisnika kamufliraju aktivnostima svih ostalih korisnika ovog sustava. Zbog toga povećanje broja korisnika i njihova raznolikost ujedno znači i povećanje razine zaštite koju Tor mreža pruža.

2. Principi rada Tor mreže

2.1. Analiza prometa

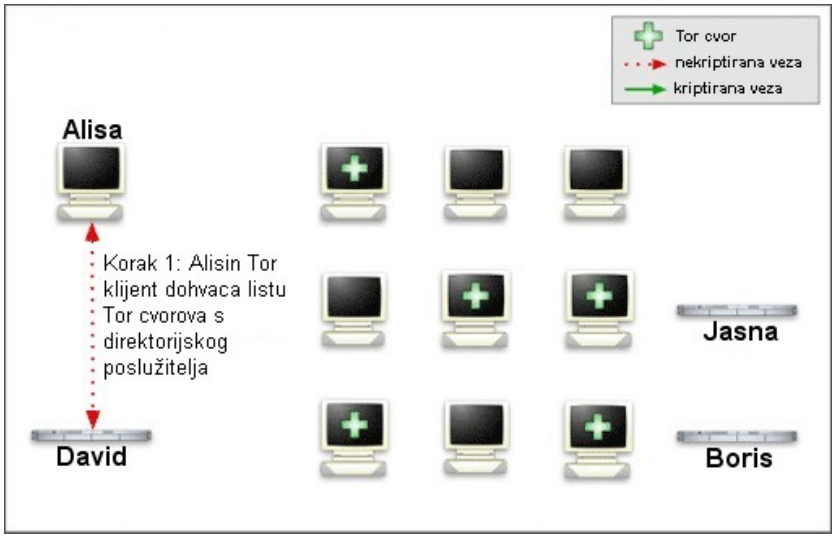
Tor mreža korisnike štiti od tzv. analize prometa (eng. *traffic analysis*), oblika nadzora Internet aktivnosti koji omogućuje utvrđivanje izvorišta i odredišta komunikacije. Takva znanja zlonamjernom korisniku mogu otkriti podatke o navikama i interesima pojedinaca. Komercijalne web stranice mogu, korištenjem podataka prikupljenih analizom prometa, prilagođavati cijene proizvoda i usluga na temelju zemlje ili institucije iz koje korisnik pristupa stranici. Fizička sigurnost korisnika također može biti ugrožena analizom prometa, na primjer u slučaju pristupanja zabranjenim web stranicama iz zemalja u kojima su na vlasti opresivni režimi.

Podatkovni paketi na Internetu građeni su od korisničkih podataka i zaglavlja koje se koristi za njihovo usmjeravanje. Korisnički dio paketa predstavlja podatke koji se šalju, a to na primjer mogu biti elektronička pisma, web stranice, multimedijalne datoteke i dr. Čak i ako su ti podaci kriptirani, analizom prometa moguće je puno saznati o korisnikovim aktivnostima i o podacima koje šalje ili prima. To je moguće zbog toga što je analiza usmjerena na zaglavlja paketa, koja otkrivaju njihovo izvorište i odredište, veličinu, vrijeme slanja i brojne druge podatke.

Osnova problema privatnosti korisnika leži u činjenici da primatelj može saznati navedene podatke o pošiljatelju analizom zaglavlja paketa. Isto je moguće i ovlaštenim posrednicima u komunikaciji, kao što su pružatelji Internet usluga, ali ponekad i neovlaštenim napadačima. Jednostavniji oblik analize prometa je presretanje paketa na putu od izvorišta ka odredištu i pregledavanje njihovih zaglavlja. Naprednija analiza može uključivati prisluškivanje nekoliko ogranaka Interneta i korištenje složenih statističkih metoda za praćenje komunikacijskih uzoraka brojnih organizacija i pojedinaca.

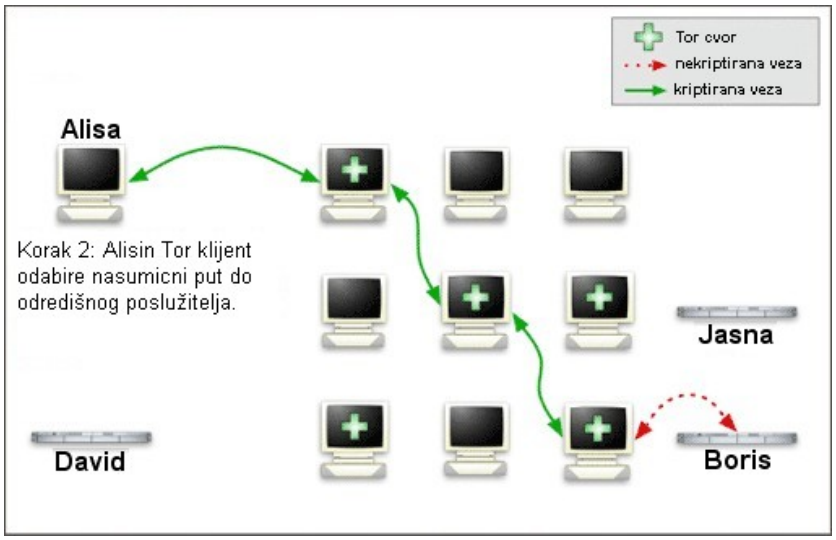
2.2. Distribuirana anonimna mreža

Kako bi se onemogućila analiza prometa, transakcije se unutar Tor mreže distribuiraju preko većeg broja posrednika od kojih ni jedan ne poznaje izvorište, a niti odredište paketa. Umjesto izravnog slanja podataka od pošiljatelja prema primatelju, oni se šalju preko većeg broja nasumično odabranih poslužitelja.



Slika 1: Izgradnja liste Tor čvorova

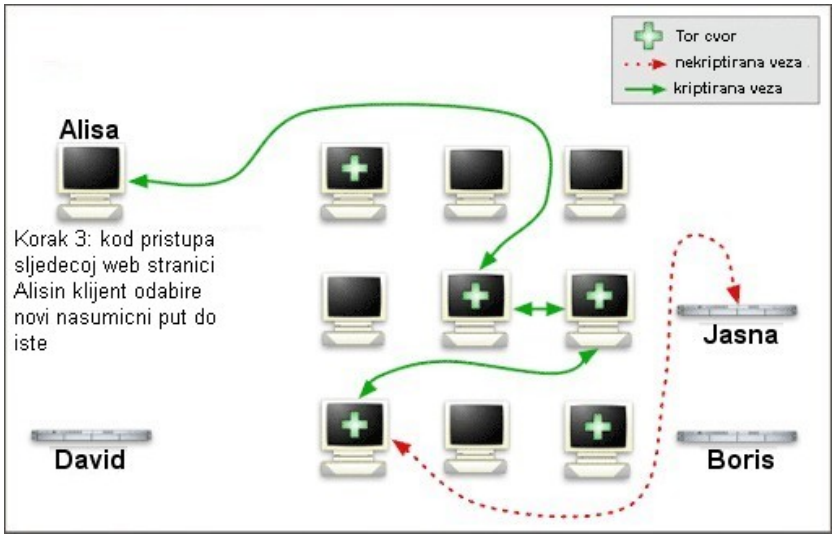
Kako bi se stvorila privatna i zaštićena veza unutar Tor mreže, klijentska aplikacija inkrementalno izgrađuje vezu između izvorišta i odredišta podatkovnih paketa, a koja se sastoji od kriptiranih veza među nasumično odabranim poslužiteljima. Ova veza nastaje u koracima tako da pojedini poslužitelj zna samo od kojeg poslužitelja je dobio pakete i kojem poslužitelju ih treba proslijediti. To se postiže korištenjem zasebnog enkripcijskog ključa u svakom koraku.



Slika 2: Prijenos podataka kriptiranim vezama među nasumično odabranim poslužiteljima

Jednom kada je veza uspostavljena njome je moguće prenošenje različitih vrsta podataka korištenjem različitih programskih paketa. Zbog prirode Tor mreže niti zlonamjerni korisnik koji prisluškuje neku od veza među poslužiteljima, a niti kompromitirani poslužitelj ne mogu korištenjem analize prometa povezati izvorište pojedinog paketa s njegovim odredištem. Tor mreža isključivo omogućuje zaštitu komunikacije prema TCP protokolu, a moguće joj je pristupiti svim aplikacijama koje podržavaju SOCKS (eng. *SOCKetS*) protokol.

Kako bi se poboljšale performanse, Tor aplikacije preko ostvarene veze provode svu komunikaciju, ali samo u trajanju od otprilike jedne minute. Nakon toga se postupak ostvarivanja nasumične veze ponavlja, čime se zlonamjernom korisniku onemogućuje povezivanje prošlih aktivnosti s trenutnima.



Slika 3: Odabir nove nasumične putanje

2.3. Skrivene usluge

Tor sustav korisnicima, koji nude različite usluge, omogućuje zaštitu privatnosti, odnosno skrivanje njihova identiteta. Spomenute usluge mogu, na primjer, obuhvaćati objavljivanje web stranica ili održavanje poslužitelja sustava trenutnih poruka. Korištenjem Tor pristupnih točaka ostali korisnici mogu pristupiti takvim skrivenim uslugama (eng. *hidden services*) bez poznavanja identiteta pružatelja usluge. Na ovaj je način moguće postaviti web stranicu na kojoj korisnici, bez straha od

cenzure, mogu objavljivati vlastite sadržaje, a da pri tome nije moguće utvrditi ni tko je postavio takvu stranicu niti tko su korisnici koji na njoj objavljuju sadržaje.

2.4. *Onion* usmjeravanje

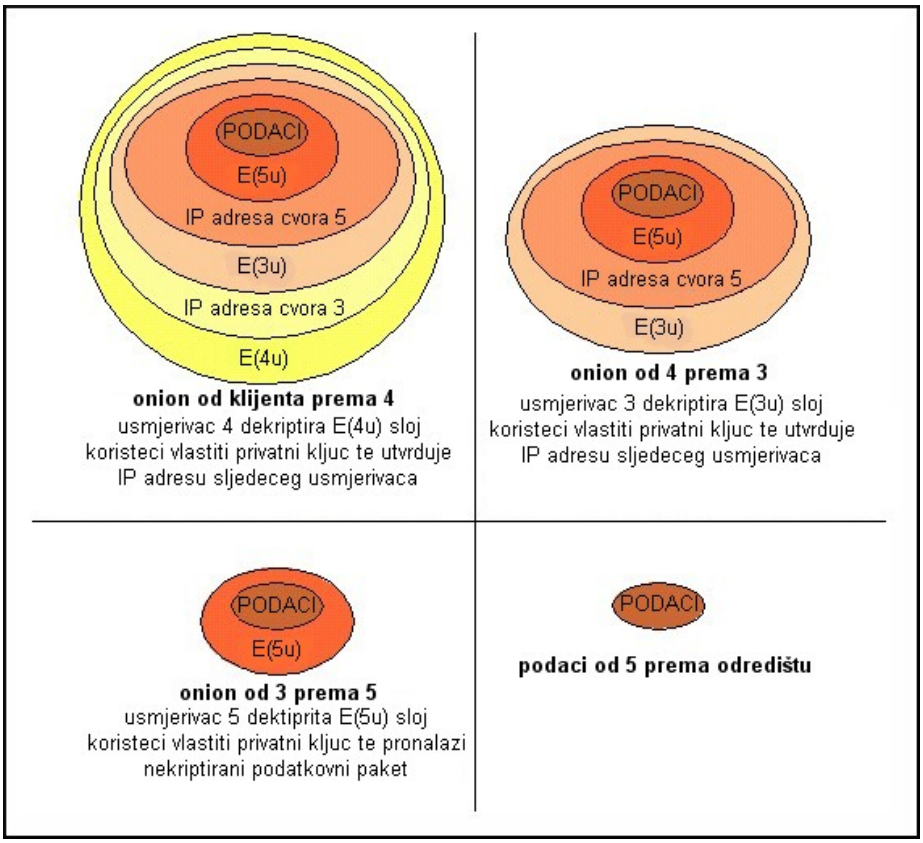
Opisana funkcionalnost Tor mreže temelji se na tzv. *onion* usmjeravanju. Riječ je o tehnici pseudoanonimne (ili anonimne) komunikacije unutar računalne mreže koju su razvili David Goldschlag, Michael Reed i Paul Syverson. *Onion* usmjeravanje temelji se na miješanim mrežama (eng. *mix networks*) Davida Chauma, ali uključuje i brojne izmjene i nadogradnje ove tehnike od kojih je najznačajnija uvođenje koncepta *onion* usmjerivača. Ovi usmjerivači provode enkripciju podataka korištenih za usmjeravanje u nekoliko enkripcijskih slojeva.

Cilj *onion* usmjeravanja je očuvati privatnost pošiljatelja i primatelja poruke, kao i zaštititi sadržaj same poruke tijekom putovanja mrežom. To se postiže korištenjem Chaumovih miješanih kaskada: poruka mrežom putuje preko niza posrednih poslužitelja (eng. *proxy server*), koji se ovdje nazivaju *onion* poslužiteljima i koji spomenutu poruku preusmjeravaju na nepredvidljiv način. Poruke se prije prijenosa među poslužiteljima kriptira, kako bi se onemogućilo neovlašteno pregledavanje njihova sadržaja, tzv. prisluškivanje (eng. *eavesdropping*).

Osnovna prednost *onion* usmjeravanja, i općenito miješanih kaskada, leži u činjenici da za anonimnu komunikaciju nije nužan ispravan rad svih poslužitelja preko kojih je ostvarena veza. Ako napadač uspije steći pristup jednom, ili čak nekoliko, *onion* poslužitelja, anonimnost korisnika koji preko njih ostvaruju komunikaciju nije ugrožena. To je moguće zbog toga što su poruke u OR (eng. *Onion Routing*) mreži višestruko kriptirane. Jedini način da se rekonstruira put poruke OR mrežom je stjecanje kontrole nad svim poslužiteljima.

2.4.1. Podatkovne strukture za usmjeravanje

OR mreže za usmjeravanje koriste posebne podatkovne strukture (eng. *routing onions*) pomoću kojih se uspostavlja veza za slanje poruke. Kako bi se formirala takva struktura, početni usmjerivač nasumično odabire određeni broj *onion* usmjerivača i svakome šalje poruku koja sadrži simetrični ključ za dekripciju poruka i upute za prosljeđivanje poruke sljedećem usmjerivaču. Svaka od ovih poruka, kao i izvorna poruka, kriptirana je javnim ključem odgovarajućeg usmjerivača. Rezultirajuća podatkovna struktura građena je slojevito te je potrebno dekriptirati vanjske slojeve kako bi se došlo do unutrašnjih.



Slika 4: Podatkovna struktura za usmjeravanja, *onion*

Analogija s lukom (eng. *onion* - luk) najbolje opisuje korištenu podatkovnu strukturu. Svaki usmjerivač nakon primitka poruke „guli" jedan sloj takvog „luka" korištenjem vlastitog privatnog enkripcijskog ključa i tako dolazi do potrebnih mu podataka za usmjeravanje ostatka podatkovne strukture. Proslijeđeni ostatak sastoji se od poruke i uputa za usmjeravanje namijenjenih svim sljedećim usmjerivačima. Posljednji usmjerivač na vezi uklanja posljednji enkripcijski sloj i odredištu dostavlja izvornu poruku, kao na slici Slika 4. Zbog ovakve organizacije usmjeravanja, potpuni sadržaj podatkovne strukture moguće je otkriti samo ako ona ispravnim redoslijedom prođe kroz sve čvorove utvrđene veze.

2.4.2. Odgovaranje na poruku

Onion usmjeravanje primaocu poruke omogućuje slanje odgovora, bez otkrivanja identiteta dviju strana, korištenjem podatkovne strukture za odgovaranje na poruke (eng. *reply onion*). Riječ je o strukturi sličnoj opisanoj podatkovnoj strukturi za usmjeravanje, a osnovna razlika je u tome što *onion* za odgovaranje sadrži opis puta natrag prema pošiljatelju. Kako bi se pokrenula dvosmjerna komunikacija pošiljatelj stvara *onion* i *onion* za odgovaranje. Primaocu se zajedno s poslanom porukom dostavlja *onion* za odgovaranje, kojega je potom moguće iskoristiti za slanje poruke pošiljaocu. Identitet pošiljaoca strukture za odgovaranje maksimalno je zaštićen višeslojnom enkripcijom pa je ugrožavanje njegove anonimnosti moguće samo u slučajevima probijanja enkripcije s javnim ključem ili uspješnim napadom na sve usmjerivače koji se nalaze na povratnoj vezi.

3. Korištenje Tor mreže

Tor sustav moguće je koristit na Windows, Mac OS X, Linux, BSD i Unix operacijskim sustavima. Kako su kod prva dva navedena operacijska sustava postupci instalacije i podešavanja implementirani u poznatim i intuitivnim grafičkim okruženjima, u nastavku su dane upute koje vrijede za Linux, BSD i Unix operacijske sustave. Pored toga ukratko je opisan Pivoxy posredni poslužitelj često korišten s Tor sustavom.

3.1. Pivoxy

Pivoxy je posredni poslužitelj s naprednim mogućnostima filtriranja prometa koje omogućuju zaštitu privatnosti korisnika, izmjenu sadržaja web stranica, rukovanje *cookies* podatkovnim strukturama, kontrolu pristupa sadržajima te selektivno uklanjanje neželjenih sadržaja (reklame, tzv. *banners* i *pop-ups*). Riječ je paketu koji je moguće u velikoj mjeri prilagoditi pojedinim primjenama, kako na osobnim računalima tako i na računalnim mrežama s većim brojem korisnika.
Ovaj se poslužitelj temelji na Internet Junkbuster posrednom web poslužitelju i distribuira se pod *GNU General Public License* licencom. Na raspolaganju su inačice Pivoxy paketa namijenjene Linux, Windows, Mac OS X, AmigaOS, BeOS i većini inačica Unix operacijskih sustava. Gotovo svaki web preglednik u radu može koristiti funkcionalnosti ovog poslužitelja, uz minimalne prilagodbe.

3.2. Tor klijent

3.2.1. Instalacija Tor klijenta

Prvi korak u postavljanju Tor klijenta je dohvaćanje i instalacija programskog paketa. Ako se instalacija provodi prevođenjem izvornog programskog koda, prethodni je potrebno instalirati:

- *libevent* programsko sučelje (eng. *Application Programming Interface - API*), koje omogućuje pokretanje tzv. *callback* funkcija u slučaju ispunjenja postavljenih uvjeta,
- *openssl* besplatnu implementaciju SSL (eng. *Secure Socket Layer*) i TLS (eng. *Transport Security Layer*) protokola te
- *zlib* programsku biblioteku za sažimanje podataka.

Nakon instalacije navedenih paketa, npr. u direktoriju */src/or*, potrebno je izvesti slijedeće naredbe:

```
$ tar xzf tor-0.1.2.15.tar.gz
$ cd tor-0.1.2.15
$ ./configure && make
```

Tada je Tor paket moguće pokrenuti naredbom:

```
$ src/or/tor
```

Druga mogućnost je, s povlaštenim korisničkim ovlastima, izvesti naredbu:

```
$ make install
```

koja instalira aplikaciju u */usr/local* direktorij pa ju je jednostavno moguće pokrenuti naredbom:

```
$ tor
```

Tor programski paket nakon instalacije izvorno je podešen kao klijent. Postavke klijentske aplikacije nalaze se u konfiguracijskoj datoteci čija podešenja zadovoljavaju potrebe većine prosječnih korisnika.

3.2.2. Podešavanje Pivoxy poslužitelja

Nakon instalacije Tor programskoga paketa potrebno je instalirati Pivoxy poslužitelj i podesiti ga tako da u radu koristi Tor mrežu. To je moguće učiniti dodavanjem linije:

```
forward-socks4a / 127.0.0.1:9050 .
```

na početak konfiguracijske datoteke poslužitelja, a koja se nalazi u */etc/pivoxy* ili */usr/local/etc* direktoriju.

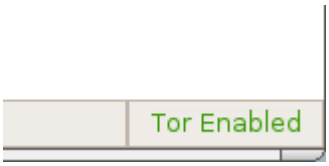
Prema izvornim podešenjima, Pivoxy paket sav promet bilježi u dnevničkim datotekama. Dnevnički zapisi onemogućuju se komentiranjem triju linija unutar konfiguracijske datoteke, unošenjem znaka # na njihovu početku. Linije koje je potrebno komentirati su:

```
logfile logfile
jarfil jarfile
debug 1 # show each GET/POST/CONNECT request
```

Pivoxy poslužitelja potrebno je iznova pokrenuti kako bi učinjene izmjene postale važeće.

3.2.3. Podešavanje aplikacija za korištenje na Tor mreži

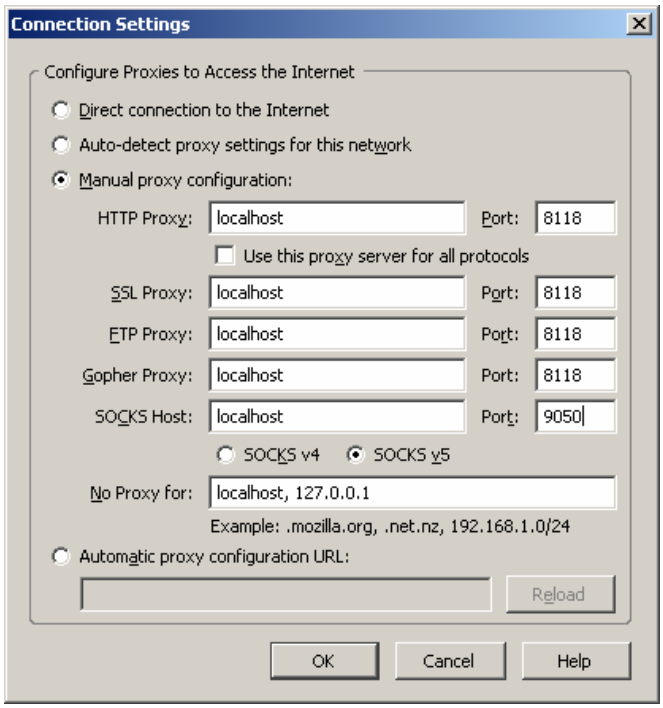
Nakon instalacije Tor i Pivoxy programskih paketa potrebno je podesiti pojedine aplikacije tako da Internet uslugama pristupaju preko njih. To se prije svega odnosi na podešavanje web preglednika. Ako se radi o Firefox pregledniku podešavanje se svodi na instalaciju Torbutton dodatka i ponovno pokretanje preglednika nakon kojega je u donjem desnom uglu Firefox prozora vidljiva opcija, kao na slici Slika 5. Pomoću ove opcije jednim je klikom moguće omogućiti, odnosno onemogućiti, korištenje Tor mreže od strane Firefox preglednika.



Slika 5: Opcija za o(ne)mogućavanje korištenja Tor mreže kod Firefox preglednika

Kod ostalih web preglednika potrebno je vlastoručno podesiti podešenja posrednih poslužitelja (eng. *proxs settings*), a isto je moguće i kod Firefox preglednika pa tako za korištenje Tor mreže nije nužna instalacija spomenutog dodatka. Postavkama posrednih poslužitelja pristupa se:

- kod Mozilla i Firefox preglednika na Windows operacijskim sustavima:
  - *Tools → Options → Advanced → Network → Connection*
- kod Firefox preglednika na Mac OS X operacijskom sustavu:
  - *Firefox → Preferences → General → Connection Settings*
- kod Firefox preglednika na Linux operacijskim sustavima:
  - *Edit → Preferences → Advanced → Proxies*
- kod Internet Explorer preglednika:
  - *Interner Option → Connections → Lan Settings → Check Proxy Server→ Advanced*



Slika 6: Postavke web poslužitelja za korištenje Tor mreže

Na slici Slika 6 prikazane su ispravno podešene postavke posrednih poslužitelja kod Firefox preglednika na Windows XP operacijskom sustavu. Prva četiri protokola (HTTP, SSL, FTP i Gopher) postavkama *localhost* i *8118* usmjeravaju se prema Pivoxy poslužitelju i nužno ih je ovako podesiti iako Pivoxy ne podržava FTP i Gopher protokole. Socks posredni poslužitelj podešava se na *localhost* i *9050* čime se svi protokoli, osim navedena četiri, usmjeravaju izravno prema Tor klijentu.
Korištenje Pivoxy poslužitelja nužno je zbog toga što web preglednici zlonamjernom napadaču omogućuju pristup DNS (eng. *Domain Name Service*) zahtjevima u slučaju izravnog korištenja SOCKS posrednog poslužitelja. Pored toga, Pivoxy uklanja određena potencijalno opasna zaglavlja web zahtjeva te onemogućuje pojedine agresivne reklamne web stranice.
Ostale aplikacije se za korištenje Tor mreže podešavaju njihovim usmjeravanjem prema Pivoxy poslužitelju (*localhost*, *8118*). Za izravno korištenje SOCKS poslužitelja, na primjer za IM klijente, potrebno ih je usmjeriti izravno prema Tor klijentu (*localhost*, *9050*). U slučaju korištenja aplikacija koje ne podržavaju HTTP i SOCKS protokole, potrebno je podesiti *tsocks* programsku biblioteku. Radi se o sučelju takvih aplikacija prema SOCKS protokolu koje omogućuje njihovo korištenje na Tor mreži bez dodatnih podešavanja samih aplikacija.

3.3. Tor poslužitelj

Tor mreža temelji se na dobrovoljnom ustupanju komunikacijskih resursa od strane korisnika. Što više korisnika održava Tor poslužitelje, to će mreža u cjelini biti brža, a i veći broj raštrkanih poslužitelja mrežu čini robusnijom. Za postavljanje poslužitelja potrebna je propusnost od barem 20kB/s u oba smjera. Korištenjem Tor programskog paketa kao klijenta i istovremeno kao poslužitelja korisnik osigurava dodatnu razinu anonimnosti zbog toga što napadač ne može razlikovati korisnikovu komunikaciju od one drugih korisnika proslijeđene prema poslužitelju.
Neke od mogućnosti Tor poslužitelja su:

- Tor poslužitelj omogućuje ograničavanje prometa, i to ograničavanje brzine pristupa kao i ograničavanje ukupnog prometa u određenom vremenskom razdoblju.
- Svaki Tor poslužitelj posjeduje tzv. *exit policy* skup pravila kojim je određeno kojim uslugama je moguće pristupiti preko njega. Na primjer, moguće je zabraniti izlazak iz Tor mreže i omogućiti samo prosljeđivanje paketa prema drugim Tor poslužiteljima.
- Tor mreža posjeduje sustav uočavanja nedostupnosti poslužitelja tako da njihovo isključivanje s mreže ima minimalan učinak na performanse mreže.

- Mreža podržava poslužitelje s dinamičkim IP adresama, ali pod uvjetom da je poslužitelju poznata njegova adresa.
- Tor poslužitelj koji se nalazi iza NAT (eng. *Network Address Translation*) poslužitelja ne poznaje svoju javnu IP adresu pa je potrebno podesiti prosljeđivanje portova.
- Poslužitelj samostalno procjenjuje i obznanjuje raspoloživu propusnost pa poslužitelji s brzim vezama poslužuje veći broj korisnika.

U postupku podešavanja Tor poslužitelja potrebno je:

1. Provjeriti ispravnost sustavskog vremena i, ako je moguće, podesiti sinkronizaciju sata.
2. Provjeriti ispravnost razlučivanja imena (eng. *Internet name resolution*).
3. Unutar *torrc* konfiguracijske datoteke definirati *Nickname*, *ORPort* i *DataDirectory* polja.
4. U slučaju korištenja vatrozida potrebno ga je podesiti tako da propušta dolazne pakete na podešene portove (*ORPort* i *DirPort*, ako je omogućen) te omogućiti sve veze prema van, kako bi se poslužitelj mogao povezati s drugim Tor poslužiteljima.

3.3.2. Provjera ispravnosti Tor poslužitelja

Poslužitelj, neposredno nakon uključivanja na Tor mrežu, pokušava utvrditi jesu li podešeni portovi dostupni s mreže. Ovaj postupak može potrajati do dvadeset minuta. U slučaju uspješne provjere u dnevničkom zapisu pojavljuje se unos:

```
Self-testing indicates your ORPort is rechable from the outside.
Excellent.
```

Ako se navedena poruka ne pojavi, podešeni portovi nisu dostupni s mreže i potrebno je provjeriti postavke vatrozida i Tor poslužitelja.
Nakon uspješne provjere dostupnosti portova, poslužitelj na bazu podataka, koja sadrži podatke o Tor mreži (eng. *directory*), postavlja tzv. *server descriptor* podatkovnu strukturu. Time se Tor klijentima na znanje daju sve informacije potrebne za pristup poslužitelju.

3.3.3. Prijavljivanje poslužitelja

Tor poslužitelje moguće je prijaviti slanjem elektroničkog pisma na adresu *tor-ops@freehaven.net*. Vlasnike prijavljenih poslužitelja redovno se obaviješta o nadogradnjama sustava i eventualnim poteškoćama u radu Tor mreže. Naslov elektroničkog pisma potrebno je oblikovati kao: „*[New Server] <nadimak poslužitelja>*“, a u samom pismu potrebno je navesti:

- nadimak poslužitelja,
- otisak identifikacijske oznake poslužitelja koji je moguće iščitati iz dnevničkih zapisa, a oblikovan je kao:

```
moria1 FFCB 46DB DA84 674C 70D7 CB58 6434 C437 0441
```

- podatke za kontakt te
- vrstu veze poslužitelja za pristup Internetu.

3.4. Tor skrivene usluge

Tor klijenti i poslužitelji mogu održavati različite usluge, npr. web ili SSH poslužitelje, bez otkrivanja svoje IP adrese korisnicima usluga. Jer se za skrivene usluge ne koriste javne adrese, moguće ih je postaviti iza vatrozida. U nastavku je opisan postupak stvaranja skrivenog web poslužitelja.

3.4.1. Lokalno postavljanje web poslužitelja

Prije podešavanja skrivene usluge potrebno je postaviti web poslužitelj. Korisnicima Linux, Unix i OS X operacijskih sustava preporuča se instalacija i pokretanje *thttpd* web poslužitelja, na primjer na portu 5222, sljedećim nizom naredbi:

```
$ ./configure && make
$ mkdir hidserv
$ cd hidserv
$ ../thttpd -p 5222 -h localhost
```

Windows korisnici mogu, na primjer, postaviti Savant ili Apache web poslužitelj pri čemu je potrebno odabranog poslužitelja podesiti tako da se povezuje na *localhost*, kako ne bi bio javno dostupan, i utvrditi na kojim portovima očekuje promet.
Nakon postavljanja poslužitelja, njegova ispravnost provjerava se unošenjem adrese http://localhost:5222 u web pregledniku. Ako je odabran neki drugi port, u navedenoj adresi zamijeniti 5222 brojevnom oznakom odabranog porta.

3.4.2. Podešavanje skrivene usluge

Postavljeni web poslužitelj potrebno je učiniti dostupnim usmjeravanjem skrivene usluge prema njemu. U *torrc* konfiguracijskoj datoteci potrebno je pronaći unos:

```
################ This section is just for location-hidden services ###
```

iza kojega slijede grupirani unosi. Svaka grupa unosa odgovara jednoj skrivenoj usluzi, a izvorno sve linije započinju znakom *#*, što znači da su skrivene usluge onemogućene. Grupe unosa sastoje se od jedne *HiddenServiceDir* linije te jedne ili više *HiddenServicePort* linija:

- *HiddenServiceDir* unos označuje direktorij u kojega Tor paket pohranjuje podatke vezane uz pripadnu skrivenu uslugu. U ovaj direktorij nije potrebno dodavati datoteke.
- *HiddenServicePort* unos omogućuje stvaranje virtualnih portova te podešavanje IP adrese i porta za usmjeravanje veza prema spomenutom virtualnom portu.

U *torrc* datoteku potrebno je dodati:

```
HiddenServiceDir   C:\Documents   and   Settings\username\Application
Data\hidden_service\
HiddenServicePort 80 127.0.0.1:5222
```

te nakon toga ugasiti Tor aplikaciju i ponovno ju pokrenuti. Prilikom pokretanja automatski se stvara podešeni *HiddenServiceDir* direktorij te dvije datoteke u njemu:

- *private_key* datoteka sadrži par enkripcijskih ključeva (javni i privatni) skrivene usluge,
- *hostname* sadrži sažetak javnog ključa koji je oblikovan kao: *6sxoyfb3h2nvok2d.onion* i koji predstavlja javno ime skrivene usluge.

Tijekom pokretanja Tor aplikacija također stvara i tzv. *hidden service descriptor* podatkovnu strukturu te pronalazi pristupne točke Tor mreži. Spomenuta struktura sadrži listu pristupnih točaka i cjeloviti javni ključ skrivene usluge. Tor aplikacija anonimno postavlja *hidden service descriptor* strukturu na direktorijske poslužitelje odakle ju korisnici, također anonimno, preuzimaju kada pristupaju usluzi.

4. Nedostaci Tor mreže

4.1. Otkrivanje DNS zahtjeva

Kao i kod mnogih drugih sustava za očuvanje anonimnosti Internet korisnika, DNS zahtjevi se upućuju bez korištenja Tor posrednog poslužitelja. Korištenje Pivoxy poslužitelja ili *torify* naredbe Tor programskog paketa omogućuje ispravljanje ovog nedostatka. Također, aplikacije koje koriste SOCKS5 poslužitelja, a koji omogućuje zahtjeve temeljene na imenu, mogu usmjeravati DNS zahtjeve preko Tor mreže pri čemu se pretraživanje zapisa (eng. *lookup*) provodi na izlaznom čvoru pa DNS zahtjevi ostvaruju jednaku razinu anonimnosti kao i sav ostali promet na Tor mreži.

4.2. Analiza prometa

Steven J. Murdoch i George Danezis s *University of Cambridge* sveučilišta objavili su na konferenciji *2005 IEEE Symposium on Security and Privacy, Oakland, California, USA, May 8 – 11, 2005* članak pod naslovom *„Low-Cost Traffic Analysis of Tor"*o ranjivosti Tor mreže na analizu prometa. Njihova tehnika analize omogućuje napadaču, s djelomičnim pristupom mreži, otkrivanje čvorova preko kojih je ostvarena anonimna veza čime Tor mreža značajno gubi na anonimnosti korisnika.

4.3. Zloupotreba

Zbog mogućnosti anonimiziranja proizvoljnog TCP prometa, Tor mreža privlači značajan broj zlonamjernih korisnika. Kako bi se ograničile mogućnosti zlouporabe, Tor sustav omogućuje kreiranje tzv. *exit policy* skupa pravila za pojedine poslužitelje. Ova pravila određuju kojoj vrsti prometa preko danog poslužitelja nije dozvoljen izlazak iz Tor mreže.
Mogući oblici zlouporabe Tor mreže su:

- Prijenos velikih količina podataka preko Tor mreže što se smatra nepristojnim zbog činjenice da poslužitelje održavaju volonteri koji besplatno ustupaju vlastite resurse.
- Anonimnost Tor mreže omogućuje slanje neželjenih elektroničkih pisama, tzv. *spam* pošte, pa je prema izvornim podešenjima Tor poslužitelja onemogućen izlaza paketa iz mreže prema portu 25, kojega koristi SMTP (eng. *Simple Mail Transfer Protocol*) protokol.

5. Zaključak

Tor mreža omogućuje zaštitu anonimnosti korisnika prilikom korištenja i pružanja različitih Internet usluga. Skrivanje identiteta korisnika provodi se onemogućavanjem utvrđivanja izvorišta i odredišta pojedinih podatkovnih paketa pomoću posebnih podatkovnih struktura za usmjeravanje, tzv. *onion* paketa, i mreže usmjerivača, tzv. *onion* usmjerivača.

Onion paketi građeni su od višestrukih enkripcijskih slojeva od kojih svaki sadrži podatke za usmjeravanje potrebne jednom poslužitelju. Kako paket putuje prema odredištu, svaki od nasumično odabranih usmjerivača vlastitim ključem dekriptira jedan sloj poruke. Usmjerivač tako otkriva kojem poslužitelju treba proslijediti ostatak paketa. Ovaj postupak se ponavlja na svakom usmjerivaču, sve do odredišta paketa kojemu se dostavlja izvorna poruka. Niti jednom usmjerivaču nije poznata cijela putanja paketa, već samo usmjerivač od kojega ga je dobio te usmjerivač kojemu je proslijedio paket. Ova karakteristika Tor mrežu čini otpornom na napade na pojedine poslužitelje.

Tor aplikaciju je, osim kao klijenta za anonimno korištenje Interneta, moguće podesiti i kao poslužitelja. Na ovaj način, dobrovoljnim ustupanjem resursa, korisnik može pridonijeti veličini i raznolikosti, a time i sigurnosti, Tor mreže. Pored toga korisnik tako podiže vlastitu razinu anonimnosti jer se njegove aktivnosti miješaju s aktivnostima drugih korisnika koje se provode posredstvom njegova poslužitelja.

Tor mreža omogućuje i anonimno pružanje tzv. *hidden services* usluga. Korisnici mogu, na primjer, objavljivati web stranice ili održavati sustave trenutnih poruka bez otkrivanja vlastitog identiteta i bez ugrožavanja identiteta korisnika skrivenih usluga.

6. Reference

[1] Tor (anonimity network), http://en.wikipedia.org/wiki/Tor_%28anonymity_network%29, srpanj 2007.
[2] Onion routing, http://en.wikipedia.org/wiki/Onion_routing, srpanj 2007.
[3] Tor: Overview, http://tor.eff.org/overview.html.en, srpanj 2007.
[4] Tor: anonimity online, http://tor.eff.org/, srpanj 2007.
[5] Privoxy, http://en.wikipedia.org/wiki/Privoxy, srpanj 2007.