



UNIVERZITET SINGIDUNUM

**-STUDIJSKI PROGRAM-
SAVREMENE INFORMACIONE TEHNOLOGIJE**

Zaštita identiteta i anonimnost na Internetu

- Master rad -

Mentor:
Prof. dr Mladen Veinović

Student:
Grujić Nikola
Br. indeksa: **410440/2013**



Beograd, 2014.

Anonimnost na Internetu

Sažetak: U ovom master radu biće prikazane i objašnjene opasnosti koje se javljaju prilikom korišćenja Internet mreže, a koje mogu ugroziti privatnost i anonimnost. Takođe će biti predstavljeno jedno od rešenja za zaštitu anonimnosti na Internetu. Biće opisan način rada tog rešenja kao i mere opreza koje je potrebno preduzeti, a sve sa ciljem da se svest o tome ko i kako ugrožava korisničku anonimnost, kao i kako se ona može podići na jedan viši nivo.

Ključne reči: anonimnost, napadi, zaštita, maliciozni,...

Anonymity on the Internet

Abstract: : In this thesis, it will be presented and described the dangers that occur when using the Internet network, and which may threaten privacy and anonymity. It will be also presented one of the solutions for protecting the anonymity on the Internet. In addition, It will be described both the operation of the solution and the precautions that should be taken, all with the aim of raising awareness about who endangers our anonymity and how, and how it can be protected up to a higher level.

Keywords: anonymity, attacks, protection, malicious ...

SADRŽAJ

1. METODOLOGIJA.....	- 1 -
1.1 PREDMET ISTRAŽIVANjA	- 1 -
1.2 HIPOTEZA.....	- 1 -
1.3 CILJEVI ISTRAŽIVANjA	- 1 -
1.4 KORIŠĆENE NAUČNE METODE	- 2 -
2. Uvod.....	- 3 -
3. Nivoi privatnosti	- 4 -
3.1 Otkrivanje stvarnog identiteta	- 4 -
3.2 Otkrivanje digitalnog identiteta	- 6 -
4. Rizici Internet opasnosti	- 10 -
4.1 HTTP kolačići	- 10 -
4.2 Fleš kolačići	- 11 -
4.3 Trajni kolačići.....	- 11 -
4.4 Fotografije na Internetu	- 12 -
4.5 Pretraživači	- 13 -
4.6 Ulazni podaci.....	- 14 -
4.7 Privatnost na socijalnim mrežama.....	- 14 -
4.8 Internet provajderi	- 17 -
4.9 Legalne opasnosti	- 18 -
4.10 Drugi potencijalni rizici po privatnost na Internetu.....	- 19 -
5. Tor projekat	- 23 -
5.1 Način rada.....	- 24 -
5.2 Protokoli, šifrovanje i uspostavljanje veze	- 27 -

5.2.1	<i>Tor</i> dizajn.....	- 27 -
5.2.2	Ćelije.....	- 27 -
5.2.3	Putanje i konekcije.....	- 28 -
5.2.4	Konstruisanje putanje	- 29 -
5.2.5	Čvorne poruke	- 30 -
5.3	Aplikacije <i>Tor</i> mreže	- 31 -
5.3.1	<i>Tails</i> (repovi)	- 31 -
5.3.2	<i>Tor Browser Bundle</i>	- 32 -
5.3.3	Orbot.....	- 33 -
5.4	Instalacija i pokretanje <i>Tor</i> pretraživača	- 33 -
5.5	Podешavanje <i>Tor</i> klijenta i <i>Tor</i> pretraživača	- 35 -
5.6	Napadi na mrežu i odbrane	- 40 -
5.6.1	Pasivni napadi.....	- 40 -
5.6.2	Aktivni napadi	- 42 -
5.6.3	Direktori napadi.....	- 44 -
5.6.4	Napadi na tačke sastanka	- 45 -
6.	Zaključak.....	- 47 -

1. METODOLOGIJA

U ovom istraživanju obrađen je koncept zaštite identiteta i anonimnosti na Internetu.

Korisnici današnjih računara ne bi smeli ni da pomisle da pristupe Internet mreži bez posedovanja određene zaštite koja će onemogućiti ili bar otežati napad na računar ili identitet. Današnji napadači se služe različitim tehnikama i alatima u ispunjavanju svog cilja. Potpuna zaštita računara koji je povezan na Internet mrežu ne postoji, i zaštita se najčešće vrši kombinacijom više različitih programa.

U ovom radu su istraženi načini i alati pomoću kojih napadači pokušavaju da ugroze korisničku anonimnost i da otkriju njihov identitet. Prikazan je i opisan jedan od načina koji može pomoći korisniku u zaštiti njegovog identiteta.

1.1 PREDMET ISTRAŽIVANJA

Predmet istraživanja predstavlja izučavanje tehnika i alata sa kojima napadači pokušavaju da ugroze korisničku anonimnost i identitet. Takođe je predstavljen i objašnjen način rada jednog od rešenja za zaštitu anonimnost na Internetu koje se zove *Tor*.

1.2 HIPOTEZA

Opšta hipoteza: Prilikom pristupanja Internet mreži korisnici svesno ili nesvesno otkrivaju svoje podatke čime omogućavaju ostalim korisnicima Interneta da uz pomoć raznih tehnika pokušaju da ugroze njihovu anonimnost. Kako se svakim danom uvećavaju tehnike i vrste napada, tako se uvećavaju alati i metode zaštite korisnika. Pored ogromnog broja različitih programa, izabrano je *Tor* rešenje, koje može pružiti određenu zaštitu anonimnosti korisnika, prilikom korišćenja Internet mreže.

Posebna/radna hipoteza: Bolje razumevanje metoda i alata koje napadači koriste, kao i načina rada alata sa kojima se sprečavaju napadi na anonimnost i privatnost, mogu pomoći da se takvi napadi izbegnu ili bar otežaju.

1.3 CILJEVI ISTRAŽIVANJA

Naučni cilj:

Da se istraže i opišu načini i alati sa kojima napadači ugrožavaju našu anonimnost i identitet, kao i da se prikaže način rada, mane i nedostaci *Tor* mreže.

Društveni cilj:

Da se korisnicima Internet mreže opiše i ponudi jedno od rešenja koje može da im obezbedi veću anonimnost prilikom korišćenja Internet mreže, kao i da se što bolje upoznaju sa tehnikama i alatima sa kojima se napadači služe.

1.4 KORIŠĆENE NAUČNE METODE

U ovom istraživanju su korišćene:

- opšte analitičke metode pri prikupljanju i proučavanju dostupne literature,
- hipotetičko-deduktivne,
- statističke i
- uporedne metode

kako bi se što bolje objasnile i prikazale tehnike i metode napada na korisničku privatnost.

Pri prikupljanju i obradi podataka korišćene su metode analize sadržaja kako već dostupnih istraživanja i literature iz šire oblasti istraživanja, tako i eksperimentalno testiranje određenih metoda sa kojima se može bolje zaštititi korisnička anonimnost.

2. Uvod

Korisnici prilikom korišćenja računara koji je povezan na Internet mrežu, ukoliko žele da zaštite svoj računar, podatke i privatnost, moraju koristiti različita programska rešenja koja ih uglavnom štite samo u određenom domenu za koji su namenjeni. Tako na primer ukoliko je na računaru instaliran program za zaštitu od virusa, ne mora da znači, da je računar zaštićen i od aktivnih napada putem Internet mreže, propusta u radu programa za Internet pretraživanje i td. Protiv određenih metoda kao što su fišing i farming programske metode zaštite tako reći i ne postoje, već je jedini način na koji korisnik može da se zaštiti, predstavlja njegovo poznavanje metoda i načina na koji se ovi napadi izvode. Pored klasičnih napada, korisnici najmanje obraćaju pažnju na napade koji ugrožavaju njihovu anonimnost, jer su posledice takvih napada u većini slučajeva nevidljive ili ih korisnik primeti tek kada je napadač već došao do željenih podataka. Napadi na anonimnost korisnika su se veoma uvećali u zadnjoj deceniji, jer su informacije o tome ko i šta voli, želi, poseduje, postale veoma cenjene na Internet tržištu gde se velike kompanije bore za što veći broj korisnika.

Kroz ovaj master rad biće pokušano da se korisnici Interneta navedu da više povedu računa o načinu na koji koriste ovu mrežu. Biće opisani načini i alati kojima se napadači služe kako bi otkrili identitet, neovlašćeno pristupili podacima i doveli do njihovog gubitka. Takođe će biti predstavljeni generalni aspekti privatnosti na socijalnim mrežama, kojih korisnici najčešće nisu ni svesni. Biće objašnjeni koji sve nivoi privatnosti korisnika Interneta postoje, kao i na koji sve način ona može biti ugrožena. Termini koji će se često pominjati u ovom radu su anonimnost i privatnost.

Anonimnost (bezimenost, nepoznatost), odnosno anoniman (bezimen, bez potpisa, ne potpisan, nepoznat), označava nekoga čiji identitet nije poznat. Privatnost (engleski: *privacy*; španski: *privacidad*; od latinske reči *privatus*), predstavlja pojam kad osoba želi da zadrži određenu stvar, informaciju ili osećanje samo za sebe.

U ovom master radu, takođe će biti predstavljen način rada *Tor* mreže, aplikacija i usluga kao i mogući izvodljivi i neizvodljivi napadi. Koncept rada mreže je jako jednostavan, a aplikacije su napravljene tako da se rad u njima ne razlikuje mnogo od rada u standardnim aplikacijama bilo kog operativnog sistema. *Tor* projekat je zapravo i namenjen korisnicima koji ne poseduju znanja i tehnike iz ove oblasti, a bave se aktivnostima koje zahtevaju određeni nivo anonimnosti na Internetu.

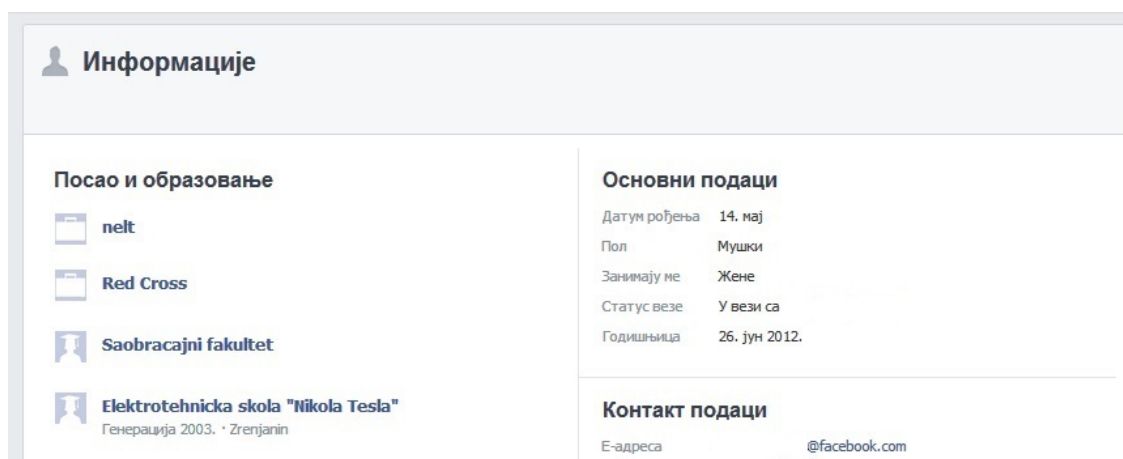
Cilj ovog master rada neće biti da obeshrabri korisnika i udalji ga od korišćenja Internet mreže, već da kroz poznavanje načina i alata putem kojih napadači vrše napade, primeni odgovarajuće metode zaštite. Navedeni sadržaj nije namenjen samo korisnicima koji se bave ovom problematikom, već i najobičnijim korisnicima kojima Internet mreža služi samo kao pomoćni alat prilikom obavljanja drugih poslova i koji nemaju adekvatan nivo znanja iz ove oblasti.

3. Nivoi privatnosti

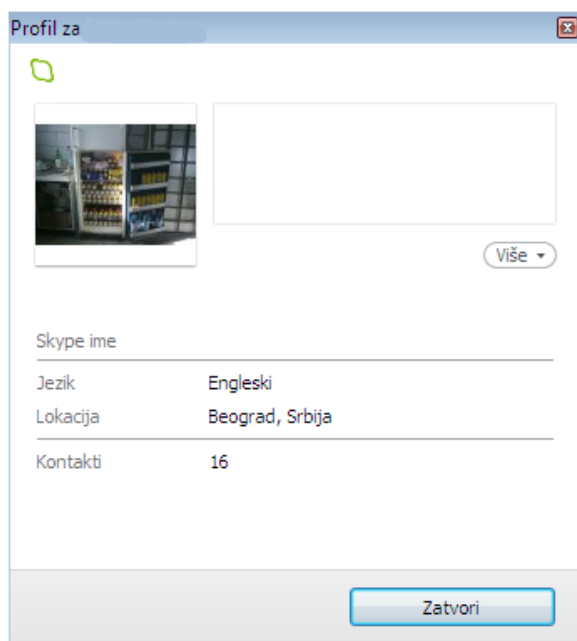
Prilikom pristupanja Internet mreži, korisnik dolazi u opasnost da otkrije jedan od svoja dva identiteta. Prvi identitet je stvaran i čine ga osnovni podaci o korisniku. Druga vrsta identiteta u većini slučajeva ne otkriva korisnikove lične podatke, ali može da bude odgovorna za obelodanjivanje njegovih navika. Ovakva vrsta identiteta se može podvesti pod digitalni identitet koji ujedno predstavlja i najčešću metu napada.

3.1 Otkrivanje stvarnog identiteta

Zaštita anonimnosti na Internetu obuhvata više slojeva zaštite. Najniži sloj zaštite predstavlja svesno otkrivanje podataka o sebi gde korisnik odaje informacije o sebi i čini ih dostupnim svim korisnicima mreže. To se najčešće vrši putem socijalnih mreža kao što su *Facebook*, *Skype* i td. , kao što se može videti na slikama 1 i 2. Pored navedenih podataka korisnici ukoliko žele mogu ostaviti i mnogo više informacija o sebi i tako još više narušiti svoju anonimnost. Ostavljanjem svoje geografske lokacije, omogućujete kompanijama koje se bave marketingom da vas zasipaju reklamnim materijalima firmi baš sa vašeg područja sto može dovesti do odvlačenja pažnje, gubljenja vremena...



Slika 1 Neki od podataka sa Facebook profila koji su javno dostupni



Slika 2 Neki od podataka sa Skype profila koji su javno dostupni

Na slikama su predstavljene samo najosnovnije stvari koje možete prikupiti o nekoj osobi, a sa malo truda moguće je izvući mnogo više informacija.

Takođe ukoliko ste član neke druge socijalne grupe, ostavili podatke na nekom online upitniku ili postavili CV na neki od sajtova koji se bave pronalaženjem posla i slično, vaša anonimnost postaje ugrožena. Vaše ime i svi podaci o vama koje ste tamo negde ostavili mogu biti izlistani korišćenjem Internet pretraživača kao što su *Google*, *Bing*, *Yahoo search*...



Slika 3 Rezultati pretrage po imenu i prezimenu korišćenjem Google pretraživača

Malo napredniji vid zaštite korisnika bi bio fokusiran na delu gde se lične informacije ne ostavljaju svesno na globalnoj mreži, već se one nalaze na samom računaru koji je na nju priključen. Određenim metodama i softverskim alatima, pojedini korisnici i organizacije mogu neovlašćeno upasti u računar i preuzeti ono što oni smatraju da je bitno za njih. Način na koji se to radi jeste ubacivanje nekog malicioznog softvera koji ima za zadatak da otvori takozvana „back door“ ili u prevodu mala vrata, putem kojeg napadač ne samo da može da otkrije identitet korisnika, već i mnogo više od toga.

3.2 Otkrivanje digitalnog identiteta

Digitalni identitet se sastoji od informacija koje su neophodne svakom računaru da bi mogao da se priključi ne samo na Internet, već i na bilo koju računarsku mrežu. Ti podaci čine takozvanu ličnu kartu računara i najvažniji podatak čini Internet IP adresa računara.

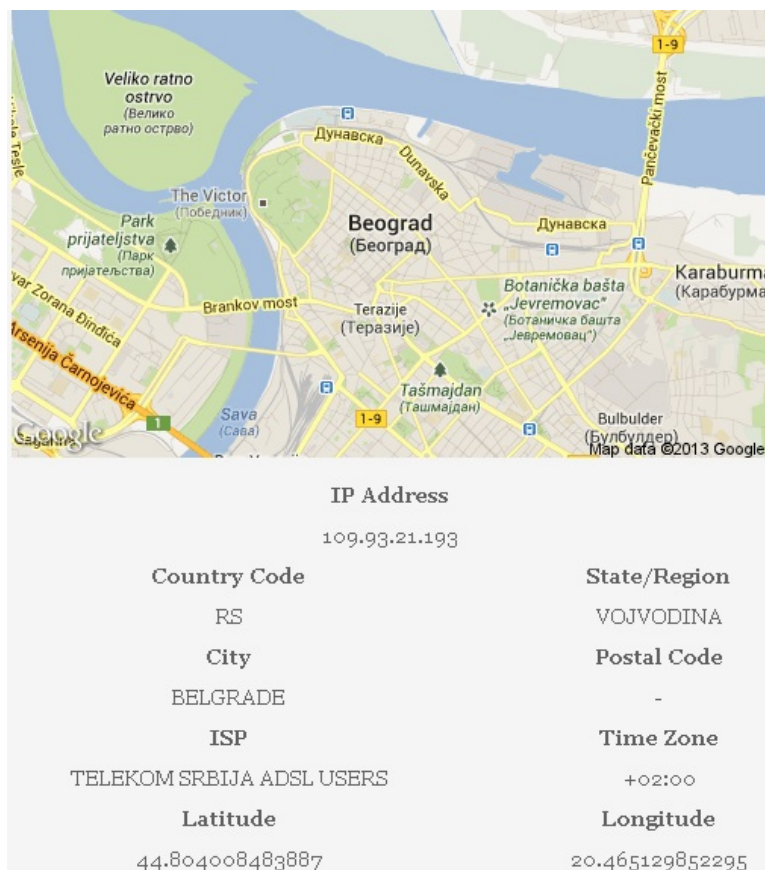
Svaki računar kada pristupa određenoj mreži, mora imati dodeljenu IP adresu na osnovu koje se identifikuje u mreži i koja ga čini jedinstvenom (slika 4). Prilikom slanja zahteva ka drugom članu mreže u zaglavlje IPv4 protokola upisuje se izvorišna adresa koja predstavlja adresu dobijenu od Internet provajdera i odredišna adresa koja je u stvari IP adresa člana sa kojim se uspostavlja komunikacija (74.125.224.72 – jedna od IP adresa za *GOOGLE*).

bit 0-3		4-7		8-15								20-31	
Verzija		Dužina		Tip servisa		Ukupna dužina							
Identifikacija				0		D M		Mesto fragmenta					
				F F									
TTL		Protokol		Čeksuma (Provera bitskih grešaka)									
Izvorišna internet adresa													
Odredišna internet adresa													
Opcije													
Podatak (TCP segment ili UDP datagram)													

Slika 4 Zaglavlje IPv4 protokola [1]

To je jedan od načina kako neko može saznati korisničku IP Internet adresu, a onda putem sajta <http://ip-lookup.net/> možete saznati sve što je javno dostupno za tu adresu.

Na slici 5 mogu se videti neki od podataka koji se dobijaju proverom određene Internet adrese.



Slika 5: Podaci dobijeni „WHOIS“ pretragom

Prilikom ovakve pretrage, nije moguće saznati podatke o stvarnom identitetu korisnika, ali videćemo da je ovo sasvim dovoljno informacija.

Određeni programi koji rade na bazi Internet adrese mogu putem Interneta slati serveru za proveru licenci podatke o ID broju vašeg hard diska ili MAC adresi mrežne karte koji se šalju u bloku koji je predviđen za slanje podataka i time mogu blokirati pristup sajtu ili korišćenje programa ukoliko nije plaćeno pravo korišćenja za određeni proizvod. Na ovom sajtu se može pogledati način takvog licenciranja softvera <http://www.solver.com/pricing-flexible-use-concurrent-licenses>.

Većina današnjih Internet pretraživača kao što su *Internet Explorer*, *Google Chrome*, *Mozilla Firefox*, *Opera* i drugi, imaju opciju automatskog čuvanja određene vrste sadržaja prilikom poseta sajtovima. Ta opcija se zove *cookies*, odnosno „kolačići“ i u principu bi trebala da pomogne korisnicima prilikom vršenja pretraga, ili ponovnog posećivanja određenog sajta kako bi skratila vreme do prave informacije. Te iste podatke mogu da pročitaju i sajtovi kojima se pristupa, kako bi ponudili baš ono što korisnik želi ili izvukli informacije o tome koje stranice su posećene. Ti podaci se najčešće smeštaju u „temporary Internet files folder“ i pražnjenjem tog foldera se brišu i podaci o pristupu sajtovima. Ukoliko je potrebno da se anonimnost sačuva, onemogućavanje „kolačića“ je svakako jedna od opcija koju bi trebalo uključiti.

Na slici 6 može se videti primer kako kompanija *Facebook* ubacuje reklame na osnovu lokacije korisničkog Internet provajdera.



Slika 6 Reklamiranje putem kompanije Facebook

Ukoliko se poseduje prenosivi računar, tablet ili neki od pametnih telefona koji se ponese na putovanje u inostranstvo, povezivanjem na neku od lokalnih mreža koje imaju pristup Internetu (što je sada praksa za skoro sve hotele i restorane), može se primetiti, da će se na ovom mestu pojavljivati reklame na jeziku države u kojoj se korisnik nalazi. Tada će Internet adresa uređaja biti vezana za provajdera u toj državi i korisnik će onda biti svrstan u to geografsko područje.

Pretpostaviti je da se za svakog korisnika zapamti geografska lokacija Internet provajdera kojeg najviše koristi prilikom pristupanja nekom od svojih naloga na društvenim mrežama. Potom neka se zabeleži svaka njihova geografska pozicija na osnovu izvorišne adrese kada otputuju negde. Količina informacija koja bi mogla da se proda raznim kompanijama bi bila ogromna a korisnik od toga ne bi dobio ništa. Neke od mogućih informacija koje se mogu iskoristiti su:

- Približan broj ljudi koji je otputovao iz zemlje (automatski broj ljudi koji je ostao)
- Približan broj ljudi te zemlje koji je posetio određenu zemlju
- Trajanje boravka van zemlje
- Periodi u toku godine kada ljudi putuju

Ovakve informacije više ne razotkrivaju anonimnost samo pojedinca, već celokupne nacije.

Prema tvrdnji određenih novinskih izvora u Srbiji već odavno postoje programi koji na osnovu vaše IP adrese mogu da prate sve što određeni korisnici posećuju na Internetu i to bez njihovog odobrenja ili odobrnja neke nadležne institucije. Ovakvi programi rade na

principu da „osluškuju“ Internet mrežu filtrirajući pakete koji se šalju samo sa određene Internet adrese i da pored toga šta se posećuje mogu da saznaju i sadržaj polja sa podacima [18].

4. Rizici Internet opasnosti

Prilikom pristupanja Internet mreži, gotovo je nemoguće izbeći sve zamke i napade, koje imaju za cilj da onеспособе pristup, preuzmu kontrolu nad računаром, neovlašćeno preuzmu podatke kao što su lozinke, brojevi kreditnih kartica i lični podaci. Metode kojima se napadači služe su mnogobrojne i većina njih koristi neopreznost korisnika kako bi se ostvario željeni cilj. Opasnost prethodi ne samo od ljudi koji se bave time zarad lične koristi, već i od velikih i uglednih kompanija, a mete ne moraju biti samo obični korisnici već smo sve češće svedoci napada na institucije i organizacije koje za jedan od ciljeva imaju sprečavanje ovakvih aktivnosti.

Napadači se koriste svim mogućim sredstvima kako bi izvršili svoj cilj. Sredstva kojima se služe su različita, a najčešće predstavljaju posebne softverske alatke (Maliciozne programe), propuste u sigurnosti kod operativnih sistema i Internet pretraživača kao i razne prevare putem elektronske pošte.

4.1 HTTP kolačići

Prilikom dizajniranja HTTP protokola, dizajneri nisu ostavili mogućnost da se prati šta se događa između dve uzastopne posete korisnika Internet strani. Naknadno je osmišljen dodatni mehanizam kojim bi se odgovarajuće informacije razmenjivale unutar HTTP zahteva i odgovora. Mehanizam koji je osmišljen omogućava serveru da čuva i ponovo isčitava informacije iz korisničke aplikacije. Web-orjentisane aplikacije tako stiču mogućnost da čuvaju informacije o izabranim stranama, korisničkim navikama, informacijama o registraciji korisnika i ostalim informacijama koje se mogu koristiti nakon završene posete nekoj Internet stranici. Ovakvi kolačići se mogu generisati samo za jednu sesiju, kada se nalaze u operativnoj memoriji, odakle se brišu kada se zatvori čitač ili im istekne tajmer.

Postoje tri načina kako se mogu generisati kolačići za Microsoftov Internet pretraživač:

- Korišćenjem Microsoftove Java skripte
- Korišćenjem WinINet funkcije
- Korišćenjem CGI skripte

```
<SCRIPT language="JavaScript">
<!--
    document.cookie = "SomeValueName =
Some_Value";
-->
</SCRIPT>
```

Primer generisanja kolačića putem Java skripte [3]

Kolačići mogu biti generisani kao „first party“ kolačići koji pamte korisničke podatke prilikom popunjavanja registracionih upitnika . Legitimni sajtovi ih koriste kako bi pravili posebne ponude korisnicima, kao i da bi pratili rezultate njihovog reklamiranja. Druga vrsta kolačića koji se generišu kao „third-party“ kolačići koje koriste reklamne kuće kako bi iskoristile istoriju pregledanja koja se nalazi na računaru i dobijene podatke podelile sa ostalim kompanijama koje se bave reklamiranjem. Ova vrsta se još naziva kolačićima za praćenje.

4.2 Fleš kolačići

Mnogi Internet sajtovi generišu kolačiće koji se nazivaju fleš kolačići, ponekad i super kolačići, a koji su mnogo „uporniji“ od običnih kolačića. Standardne procedure kao što su brisanje običnih kolačića, brisanje istorije pregledanja, brisanje keša ili brisanje privatnih podataka u okviru pretraživača neće uticati na fleš kolačiće. Oni će i dalje ostati sačuvani na računaru i pored korisničkih napora da ih izbriše. Oni se ne mogu izbrisati pomoću standardnih „antispysware“ programa ili programa za uklanjanje reklama , a koji su namenjeni za komercijalnu upotrebu. Jedan od načina zaštite jeste korišćenje „Firefox“ pretraživača koji poseduje dodatak „BetterPrivacy“ koji može pomoći u brisanju fleš kolačića.

Tokom jula i avgusta 2010 godine, pokrenute su tri tužbe protiv velikih kompanija zbog korišćenja fleš kolačića. One su bile optužene da su svesno pratile korisnike na način koji je narušavao njihovu privatnost. Ceo postupak je okončan nagodbom, a šteta koja je prilikom toga isplaćena je iznosila 3,2 miliona dolara [4].

4.3 Trajni kolačići

Trajni kolačići (eng. *Evercookie*) predstavljaju aplikaciju zasnovanu na java skripti koja proizvodi izuzetno uporne kolačiće u okviru Internet pretraživača. Cilj ovakvih kolačića je da se izvrši identifikacija klijenta i nakon što klijent uradi standardnu proceduru brisanja kolačića, fleš kolačića i ostalih stvari.

Ovakav način rada se postiže tako što se podaci o kolačiću čuvaju uz pomoć više različitih tipova mehanizama za čuvanje koji su dostupni u okviru lokalnog pretraživača. Kolačić tada ima mogućnost da se ponovo stvori, ukoliko korisnik ukloni bilo koji od tipova tog kolačića , koristeći pritom svaki mogući mehanizam. Konkretno, prilikom stvaranja novog kolačića koriste se sledeći mehanizmi za čuvanje ukoliko su dostupni:

- Standardni HTTP kolačići
- Fleš kolačići
- *Silverlight Isolated Storage*
- Čuvanje kolačića u obliku auto-generisanih RGB vrednosti
- Čuvanje kolačića u istoriji pretraživača
- Smeštanje kolačića u HTTP Etag-ove
- Čuvanje kolačića u Web kešu
- window.name kešovanje
- Čuvanje u okviru Internet Explorer *userData*

- HTML5 *Session Storage*
- HTML5 *Local Storage*
- HTML5 *Global Storage*
- HTML5 *Database Storage* pomoću SQLite [7]

4.4 Fotografije na Internetu

Danas gotovo da i ne postoji uređaj za komunikaciju koji na sebi ne poseduje kameru. U prodavnici tehničke opreme ne možete naći prenosivi računar, tablet ili telefon novije generacije a da ne poseduje kameru. Kućni računar je gotovo nemoguće zamisliti bez kamere, pomoću koje korisnik može obavljati video pozive koristeći neki od programa za komunikaciju. Porodica bez digitalnog fotoaparata ili kamere je takođe nezamisliva stvar današnjice.

Problem nastaje kada se fotografije koje je korisnik ili neko drugi uslikao u privatnosti, pojave na Internetu. Iako zakoni mnogih zemalja ne dozvoljavaju objavljivanje fotografija osobe koja im nije dala saglasnost za to, postoje razni načini kako naneti štetu nekome a da za to ne odgovarate.

Jedan od najčešćih načina zloupotrebe fotografija predstavljaju socijalne mreže. Korisnici socijalnih mreža mogu okačiti fotografiju na kojoj se nalazi neka druga osoba, pa čak je i označiti sa punim imenom i prezimenom a da ta osoba toga nije ni svesna. Klikom na mesto na kojem je ona označena, a ukoliko korisnik koji obavlja tu radnju poseduje nalog na istoj socijalnoj mreži, može pristupiti osnovnim podacima u vidu „treće“ osobe, iako to možda nije bila želja ni korisnika čiji je to nalog, a ni onoga ko je fotografiju postavio. Najveća socijalna mreža na svetu Fejsbuk, pored opcija koje nudi, samostalno prikuplja podatke o tome ko označava sliku korisnika, svrstava ih u grupe i na osnovu tagova pravi profile o korisnicima. Prilikom pravljenja reklama, ukoliko je neko obožavatelj određene stranice, Fejsbuk može slobodno da koristi njegovu profilnu fotografiju kako bi preporučio određenu stvar prijateljima sa korisničkog profila. Određene aplikacije i apleti koji se instaliraju u okviru pretraživača, a služe za otpremanje slika na nalog, prenose određene podatke Fejsbuk serveru, ali kako oni kažu „obzirom da već otpremate slike na naš sajt“ ne remete korisničku privatnost. Fotografije koje su postavljene na Fejsbuk socijalnoj mreži, ostaju sačuvane na serveru sve dok se nalog ne isključi. Podaci o korisniku mogu ostati u pomoćnoj kopiji na Fejsbuk serveru i do devedeset dana nakon brisanja naloga. Postavljanjem fotografija na Fejsbuk, gubi se pravo na ličnu svojinu nad tom fotografijom i daje se dozvola fejsbuk mreži da može da je koristi bez plaćanja nadoknade.

Prilikom koršćenja uređaja kao što su „pametni“ telefoni, tableti i drugi, kada se otpremaju fotografije, najčešće se otpremaju i metapodatci koji mogu otkriti tačnu geografsku lokaciju korisnika u tom trenutku. Opcija da uređaji ne šalju metapodatke, mora ručno da se ukloni, a najčešće je ona automatski uključena.

“U slučaju sadržaja koji je zaštićen pravom intelektualne svojine, poput fotografija i video zapisa (IP sadržaj), dajete nam sledeću, izričitu dozvolu, u skladu sa vašim postavke privatnosti i aplikacije: dodeljujete nam neekskluzivnu, prenosivu dozvolu koja se može podlicencirati, za koju se ne plaća naknada i koja važi za ceo svet da koristimo bilo koji IP sadržaj koji objavite na usluzi Facebook ili u vezi sa istom (IP dozvola). Ta IP dozvola prestaje da važi kada izbrišete IP sadržaj ili nalog, osim u slučaju da je sadržaj već podeljen sa drugima, koji isti nisu izbrisali.”

-Fejsbuk izjava o pravima i obavezama: Deljenje sadržaja informacija

Tehnologija prepoznavanja lica takođe može biti iskorišćena kako bi se uz pomoć fotografije pristupilo ličnim podacima osobe. Istraživači sa Karnegi Melon Univerziteta objedinili su skeniranje slika, „cloud computing“ i javne profile sa socijalnih mreža kako bi pokušali da identifikuju ljude u stvarnom svetu. Rezultati koje su dobili su veoma uznemirujući, jer su za neke osobe uspeali čak da dobiju njihov broj socijalnog osiguranja. Tim sa Karnegi Melon Univerziteta je iskobinovao tehnologiju „off- the – shelf“ prepoznavanja lica i slike studenata sa Fejsbuk mreže i tako uspeo da identifikuje preko trideset procenata studenata koji su šetali kampusom [5]. Nakon ovoga sve velike kompanije poput Fejsbuka, Googla i ostalih su počele da rade na sličnim idejama. Fejsbuk je na osnovu ove tehnologije omogućio korisnicima da lakše prepoznaju prijatelje na fotografijama što znači da se korisnički podaci za prepoznavanje putem slika već odavno nalaze u bazama za prepoznavanje.

4.5 Pretraživači

Mnogi korisnici se kreću po Internetu koristeći pretraživače (eng. search engines). Pretraživači poseduju i koriste mogućnost da prate svaku našu izvršenu pretragu. Pamte IP adrese, termine korišćene prilikom pretraživanja, vreme kada je to urađeno kao i druge informacije. Tako se može desiti da kroz pretraživanje, korisnik nenamerno otkrije informacije o sebi. Primer toga bi mogao biti kada bi korisnik pokušao da pretraži Internet sa ciljem da utvrdi da li se negde javlja njegov jedinstveni matični broj građana. Kada bi slučajno dodatno pokušao da pretragu izvrši dodajući svoje ime i prezime, to bi značilo da je pretraživač sačuvao osnovne podatke o njemu.

Najveći vlasnici pretraživača se pravdaju činjenicom da moraju da čuvaju lične podatke kako bi pružili bolju uslugu, da smanje bezbednosne pretnje, spreče ljude da upadnu u razne Internet prevare itd.. Međutim, vremenski period u kojem se čuvaju podaci je nekada i više od godinu dana, što može dovesti u sumnju navedene razloge za čuvanje ličnih podataka. Pojedini tvorci pretraživača su smanjili vreme čuvanja korisničkih IP adresa, dok je vreme čuvanja IP adresa kod vodećih pretraživača svedeno na:

- Yahoo – 18 meseci
- Bing – 6 meseci
- Google – 9 meseci [6]

Kompanija AOL sadrži bazu od preko dvadeset miliona članova, gde svaki od njih poseduje lični identifikacioni broj. Podešavanja AOL pretrage omogućavaju AOL-u da

vodi evidenciju o svim sajtovima koje posećuju članovi. Na taj način se ne otkriva stvarni identitet osobe, ali se može saznati jako mnogo samo na osnovu analiziranih pretraga.

4.6 Ulazni podaci

Prilikom korišćenja računara, tačnije operativnih sistema na njima, ili pojedinih programa, najčešće postoje forme za logovanje koje pored osnovnog pristupa računaru, omogućuju i snimanje provedenog vremena na njemu kao i posete Internet sajtovima. Ukoliko računar koristi više korisnika, privatnost korisnika može biti ugrožena. Način na koji se taj rizik može smanjiti jeste onemogućavanje logovanja drugim korisnicima kao i redovnim čišćenjem formi za logovanje. Još jedna od mogućnosti pristupa takvim sistemima mogu biti softverski „keylogeri“. Oni mogu prikupljati podatke o tome šta se unosi na tastaturi, pamtit ih u nekom fajlu na računaru ili slati putem Internet mreže na udaljenu lokaciju.

Ulazni podaci se najčešće koriste u sistemima automatskog upravljanja gde je tačnost i brzina prikupljanja podataka jako bitna. Primer takvih informacionih sistema za logovanje su sistemi koji mogu sakupljati različite fizičke veličine: vreme, intenzitet svetlosti, jačinu struje, pritisak itd.

4.7 Privatnost na socijalnim mrežama

Pojava socijalnih mreža na Internetu je dovela do toga, da Internet postane prava baza podataka stanovnika iz celog sveta. Informacijama koje poseduju pojedine socijalne mreže, ne bi mogle da se pohvale ni najbolje državne bezbednosne agencije. Socijalne mreže ne samo da imaju mogućnost da od svojih korisnika dobrovoljno dobiju osnovne lične podatke već i brojeve mobilnih telefona, bračni status, prijatelje, rodbinske veze itd.. Za prikupljanje ovakvih podataka bilo bi potrebno da se uloži ogromno vreme i resursi, a socijalne mreže prikupe ove podatke za jako kratko vreme tako što im korisnici sami to obelodane.

Jedna od prvih socijalnih mreža koja i danas postoji se zove „Spokeo“. Mreža funkcioniše kao pretraživač stanovnika. U njoj su objedinjeni svi podaci dostupni putem Interneta kao što su: bele strane, javni zapisi o ljudima, socijalne mreže i drugi. Mreža sama pretražuje Internet i skuplja podatke o korisnicima. „Spokeo“ ne garantuje tačnost informacija, ali podaci koje je on uspeo da skupi su neverovatni. Pored standardnih informacija kao što su ime, prezime, pol i uzrast, ova mreža nudi i adresu, broj telefona, rodbinske veze, bračni status i sve ono što je moglo da se „izvuče“ sa Internet mreže.

The screenshot displays the Spokeo website interface for a user named John Doe. The top navigation bar includes fields for Name, Email, Phone, Username, and Address, with a search bar and links for Sign up and Login. The main content area is divided into several sections:

- Profile Summary:** Shows John Doe's profile picture, a 'Get Full Results' button, and a '100% Satisfaction Guarantee' badge. It lists key details: Gender (Male), Current Address (1111 N 1st St, Alhambra, CA 91801), and Marital Status (See Available Results).
- Location History:** A map view showing John Doe's current location in Alhambra, CA 91801, with details about the property (4 beds, 3 baths, 1,825 sq ft, 6,381 sq ft lot).
- Family Background:** A family tree diagram showing John Doe as the son of Father (John Doe) and Mother (Patricia Doe).
- Photo and Social Profiles:** A section titled 'Unlock Photos & Videos for John Doe' with a 'Search and Get Full Results' button.

The bottom of the page features a footer with copyright information (© 2008-2014 Spokeo, Inc.) and various links including Mobile, About, News, Blog, Privacy, Terms, Directory, Affiliates, Community, and Contact.

Slika 7 Nasumično izabrana osoba i dobijeni podaci o njoj.

Broj korisnika na socijalnim mrežama je odavno premašio polovinu stanovništva planete. Prema informacijama „Statistic Brains“, preko 58% svetskog stanovništva koristi neku od socijalnih mreža. „Facebook“ je ubedljivo najveća socijalna mreža sa 56% od ukupnog broja ljudi koji koriste socijalne mreže. Socijalne mreže su tako zadobile pristup ogromnoj količini ličnih informacija. Prilikom formiranja korisničkog naloga, korisnici to čine uz prava i obaveze izabrane socijalne mreže. Tako napravljeni profili stvaraju deo njihovog „online“ identiteta.

Problem je počeo da se javlja kada je primećeno povećano korišćenje "third-party" servera u odnosu na "first-party" server socijalne mreže, a koristi se za prikazivanje sadržaja i reklama koje pripadaju primarnom serveru. Neki od „third-party“ servera predstavljaju agregatore korisničkih pregledačkih navika kroz različite „first-party“ servere, često koristeći se kolačićima za praćenje. Razlog za još jednu sumnju je u tome što je najvećih deset „third-party“ servera putem velikog broja Internet sajtova uvećalo svoj sadržaj za 30% u roku od dve godine [19], a nikada nije ispitano da li neki od tih servera možda sadrži i informacije koje mogu otkriti korisnički identitet. To bi značilo da "third-party" serveri ne sakupljaju samo pregledačke navike bilo koje osobe, već tačno određenog korisnika.

Verovatnoća, da se takav sadržaj može naći na „third-party“ serverima je ipak velika, jer se ispostavilo da postoji „curenje“ informacija između „first-party“ i „third-party“ servera. Ovo „curenje“ se javlja prilikom kombinovanja informacije iz HTTP zaglavlja i kolačića koji se šalje „third-party“ serveru za agregaciju. Drugi način predstavljaju kolačići za praćenje koji mogu imati skrivene funkcije, poznate samo strani koja ga je dizajnirala. Treći način na koji „third-party“ serveri mogu doći do informacija su zahtevi za linkom („Request-URI“).

```
GET /clk;203330889;26770264;z;u=ds&sv1=170988623...  
Host: ad.doubleclick.net  
Referer: http://www.facebook.com/profile.php?  
id=123456789&ref=name  
Cookie: id=2015bdfb9ec|t=1234359834|et=730|cs=7aepmsks
```

```
GET ...&g=http%3A//digg.com/users/jdoe&...  
Host: z.digg.com  
Referer: http://digg.com/users/jdoe  
Cookie: s_sq=...http%25253A//digg.com/users/jdoe...
```

```
GET /__utm.gif?..utmhn=twitter.com&utmp=/profile/jdoe  
Host: www.google-analytics.com  
Referer: http://twitter.com/jdoe
```

- Načini „curenja“ informacija putem: HTTP zaglavlja, „Request-URL“, kolačića

Prava i obaveze, kao i uslovi korišćenja na socijalnim mrežama omogućavaju korisnicima da svoj sadržaj učine nevidljivim za korisnike kojima to oni nisu odobrili. Najveći broj korisnika nije upoznato ili ih ne zanimaju ovakva podešavanja pa između 55 i 90% korisnika socijalnih mreža ima podrazumevana podešavanja svojih naloga, dok 80-97% njih poseduje podrazumevana podešavanja za dozvolu pristupa listi prijatelja.

Tabela 1 Mogućnost dostupnosti informacijama za 12 socijalnih mreža [8].

Lične Informacije	Nivo pristupa			
	Uvek dostupno	Dostupno kao podrazumevano	Nedostupno kao podrazumevano	Uvek nedostupno
Lična fotografija	9	2	1	0
Lokacija	5	7	0	0
Pol	4	6	0	2
Ime i prezime	5	6	1	0
Prijatelji	1	10	1	0
Aktivnosti	2	8	0	2
Fotografije	0	9	0	3
Datum rođenja/godine starosti	2	5	4	1
Pohađane škole	0	8	1	3
Poslodavac	0	6	1	5
Rodendan	0	4	7	1
Poštanski broj	0	0	10	2
Adresa elektronske pošte	0	0	12	0
Broj telefona	0	0	6	6
Adresa stanovanja	0	0	4	8

4.8 Internet provajderi

Internet provajderi (ISP), omogućavaju svojim korisnicima pristup Internet mreži. Oni su zaduženi za dodeljivanje jedinstvene IP adrese sa kojom se pristupa Internet mreži. Pošto sav saobraćaj ka Internet mreži mora da prođe preko Internet provajdera, oni su jedini koji sa sigurnošću mogu pratiti vaš saobraćaj. Međutim, u većini slučajeva operateri

su sprečeni zakonskim regulativama, etičkim i poslovnim normama da monitorišu Internet saobraćaj.

Korisnici najčešće dobijaju dinamičke IP adrese koje se periodično ili resetovanjem adaptera menjaju. Problem se javlja iz razloga što i pored činjenice da se IP adrese periodično menjaju Internet provajderi ih čuvaju još neko određeno vreme. Vreme čuvanja IP adresa varira od provajdera do provajdera, a mnogi od njih čak ni ne obelodanjuju politiku čuvanja. Ovakav podatak onemogućava korisnike da pronađu Internet provajdera koji može da garantuje za njihovu privatnost.

Prilikom pristupanja bilo kom Internet sajtu korisnici otkrivaju svoju IP adresu. Na taj način omogućuju stranici koju su posetili da sazna geografsku lokaciju njihovog Internet provajdera. Dizajneri Internet sajtova tako mogu da im plasiraju reklame i sadržaj namenjen samo za njihovo geografsko područje. Ukoliko se Internetu pristupa putem „pametnih“ ili drugih mobilnih uređaja, mobilni operateri ih preusmeravaju na Internet mrežu prema njihovom planu rutiranja i ujedno prave statistiku njihovog korišćenja Interneta. Prilikom povezivanja na Internet putem javnih bežičnih mreža, nivo anonimnosti se ne može odrediti. Pored standardne bezbednosne pretnje koje su osnovna mana bežičnih mreža, sigurnost i anonimnost povezanih korisnika zavisi od administratora odnosno provajdera bežične mreže.

4.9 Legalne opasnosti

Pod legalnim opasnostima, porazumevaju se sve zakonski dozvoljene metode pomoću kojih bezbednosne službe mogu pribaviti podatke sa korisničkog hard diska i Internet saobraćaja.

Velika Britanija je prva država koja je omogućila pristup korisničkim računarima samo uz nalog ovlašćenog lica, koji uz sumnju da korisnik čini ozbiljan prestup, može narediti „daljinsko pretraživanje“. Podaci koji se pri tom pronađu, mogu biti korišćeni kao dokazni materijal kasnije u postupku. Evropska Unija je prateći primer Velike Britanije takođe odobrila policiji iz EU da može da koristi usluge daljinskog pretraživanja koje sprovodi britanska policija.

Pored ovako drastičnih zakona, koji apsolutno poništavaju svaku anonimnost i privatnost ostale države su u većoj ili manjoj meri uvele nadzor nad Internet provajderima, odnosno Internet saobraćajem. Među poslednjim državama koje su uvele ili pojačale nadzor Interneta, čime se omogućava zabrana pristupa određenim Internet stranicama, nadzor nad Internet saobraćajem i druge radnje kojima se mogu ugroziti anonimnost i privatnost su Turska [10] i Francuska [11], dok se za američku Nacionalnu službu bezbednosti veruje da može da nadzire 75% Interneta u SAD [9].

Razlozi za donošenje ovakvih zakona i propisa su uglavnom isti. Najčešće se to čini u cilju sprečavanja raznih kriminalnih aktivnosti kao što su Internet prevare, trgovina ljudima, trgovina drogom, dečija pornografija, terorizam kao i za jačanje nacionalne bezbednosti. Svaka država koja je donela ovakve zakone tvrdi da su oni u skladu sa ljudskim pravima, ali nijedna od njih nema definisano telo koje bi nadziralo da li se zakoni nad nadzorom Internet saobraćaja sprovode bez nepotrebnog zadiranja u privatnost, a

samim tim i anonimnost ljudi. Iz tog razloga postoji opravdana sumnja da u državama u kojima postoje ovakvi zakoni postoji nedovoljna anonimnost korisnika Internet mreže.

4.10 Drugi potencijalni rizici po privatnost na Internetu

Jedan od možda najopasnijih rizika po privatnost korisnika predstavljaju programska rešenja ili aktivni napadi ljudi koji su obučeni za takve radnje. Najčešća programska rešenja koja se koriste kako bi se ugrozila anonimnost korisnika su malveri, spajveri i veb bube. Kada je u pitanju uloga čoveka, onda se načini na koji oni pristupaju vašem računaru nazivaju fišing i farming [12].

Malver (engl. *Malwer*) predstavlja maliciozni program. To je vrsta neželjenog programa koji se instalira na vaš računar bez prethodnog odobrenja. Virusi, crvi i trojanski konji predstavljaju primere malicioznih programa koji se često stavljaju u istu grupu i nazivaju jednim imenom.

- **Virusi** predstavljaju male programe koji su predviđeni da se šire od računara do računara ugrožavajući pritom njegovo normalno funkcionisanje. Oni mogu oštetiti ili izbrisati podatke sa računara, upotrebiti korisnički klijent elektronske pošte kako bi se raširio na ostale računare, ili čak izbrisati kompletan sadržaj hard diska. Virusi su odgovorni za štete koje se mere u milijardama dolara. Jedan od najpoznatijih virusa koji je gotovo ugušio servere elektronske pošte, se zvao „Melisa“ virus. Kreirao ga je 1999. godine Dejvid L. Smit (*David L. Smith*) i bio je baziran na Mikrosoftovom Word makrou. Cilj virusa je bio da se putem elektronske pošte sam replicira i šalje kontaktima koje je korisnik posedovao u računaru.[2]
- **Crvi** (engl. *Worms*) su kompjuterski programi koji imaju mogućnost da se kopiraju sa računara na računar. Prilikom izvršavanja tih radnji oni koriste procesorsko vreme i mrežni protok, a takođe mogu sa sobom nositi i sadržaj koji može prouzrokovati značajnu štetu. Crv često pronalazi „rupe u bezbednosti“ u delu korisničkog programa ili operativnog sistema. Najpoznatiji i najrasprostranjeniji crv se pojavio 2007. godine pod nazivom „Storm“. On je uspeo da zarazi između milion i pedeset miliona računara. Tokom određenog perioda bio je odgovoran za 20% ukupne „spam“ elektronske pošte [13].
- **Trojanski konj** (engl. Trojan horse) predstavlja kompjuterski malver koji nema mogućnost repliciranja samog sebe. Program se najčešće infiltrira u sistem tako što se korisniku ponudi određena aplikacija koja ima zadatak da bude sto primamljivija. Pored osnovnog zadatka koji podrazumeva brisanje podataka i moguće nanošenje štete operativnom sistemu, trojanski konj se može koristiti još i za generisanje „malih vrata“, kako bi se omogućio skriveni pristup računaru. Detektovanje ovakvih malicioznih programa je jako teško, a njihova aktivnost može znatno ugroziti rad računara. Trojanski konj, za razliku od ostalih malicioznih programa, ne pokušava da se replicira i širi po mreži ili infiltrira u druge fajlove. Korišćenjem trojanskih proksi server programa, moguće je pretvoriti inficirani

računar u termin „zombi“ računar, kada napadač ima potpunu kontrolu nad korisničkim računarom i koristi ga za obavljanje raznih nedozvoljenih radnji prikrivajući tako svoj identitet.

Spajveri (engl. *Spyware*) predstavljaju generalni termin za opisivanje programa koji ispoljavaju određeni vid ponašanja bez prethodne dozvole korisnika. Svrha postojanja ovakvih programa je sledeća:

- Reklamiranje
- Sakupljanje ličnih informacija
- Izmene u podešavanjima računara

Najčešći primeri ovakvih programa se mogu naći u vidu programa za reklamiranje (adveri, engl. *Adware*) ili specijalnih programa koji prate lične ili ciljane informacije. Uklanjanje ovakvih programa je jako teško. Izmene u podešavanjima koje se mogu napraviti na računaru mogu dovesti do toga da se izgubi mnogo vremena u pokušajima da se ukloni sadržaj koji se prikazuje, uspori rad računara ili obori operativni sistem [14]. Prisutnost ovakvih programa se najčešće može primetiti po promenjenoj početnoj stranici u okviru Internet pretraživača ili po dodacima u okviru pretraživača za koje nije dato odobrenje. Sve ovo može prouzrokovati jako veliki gubitak vremena u pokušaju da se vrate sva podešavanja u početno stanje.

Veb bube (engl. *Web bugs*) predstavljaju grafičku zamku u okviru Internet stranice ili poruke elektronske pošte. Svrha ovakvih programa je da se sazna IP adresa osobe koja posećuje Internet stranicu ili poruku iz elektronske pošte na kojoj se takav program nalazi. Veličina ovakvih grafika je obično 1x1 piksel i to je razlog zašto ostaje neprimetna. Informacije koje se mogu poslati serveru prilikom pregledanja veb bube su sledeće:

- IP adresa računara koji se „upecao“ na veb bubu
- URL adresa stranice na kojoj se nalazi veb buba
- URL adresa na kojoj se nalazi slika veb bube
- Vreme kada je veb buba pogledana
- Vrsta Internet pretraživača koji je pristupio veb bubi
- Prethodna vrednost kolačića

Veb buba predstavlja deo koda u okviru HTML koda i neprimetna je osim ako se ne pogleda izvorni kod. Prilikom pretraživanja koda, potrebno je tražiti „IMG tagove“ čije dimenzije su najčešće podešene na 1x1 piksel, a izvorna adresa fotografije se učitava sa neke druge Internet adrese. Primer dela izvornog koda na kojem se nalazi jedna veb buba se može videti ispod [15].

```
<iframe id="destination_publishing_iframe_fedex_0"
src="https://fedex.demdex.net/dest4.html?d_nsid=0#https%3A%2F%2Fwww.
fedex.com%2Ffedextrack%2F%3Faction%3Dtrack%26cntry_code%3Dus"
style="display: none; width: 0px; height: 0px;"></iframe>
```

Čitanje elektronske pošte takođe može ugroziti vašu anonimnost, iz razloga što se često u okviru poruka koje se prime može naći veb buba koja dostavljanjem određenih informacija bez korisničke saglasnosti, narušava njegovu digitalnu anonimnost. Veb buba u poruci elektronske pošte, najčešće može imati za cilj da otkrije da li je i u koje vreme pročitana tačno određena poruka, prosledi korisničku IP adresu iako je on želeo da ostane anoniman i ukoliko je korisnik radnik u nekoj kompaniji, ona može skupiti podatke o tome koliko je puta neka poruka bila pročitana i prosleđena dalje. Izgled primera koda koji predstavlja veb bubu u okviru poruke elektronske pošte možete videti ispod [15].

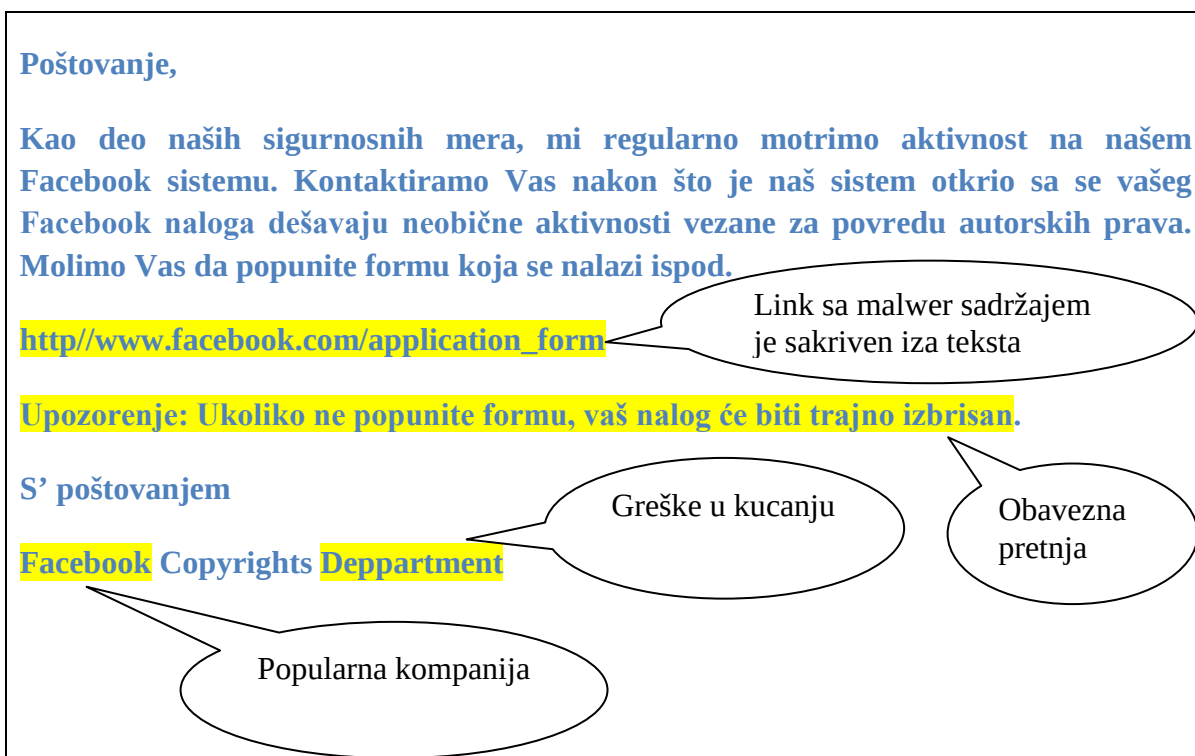
```

<IMG SRC="http://email.bn.com/cgi-bin/flosensing?x=ABYoAEhouX">
```

Glavni problem sa veb bubama predstavlja to što se ne može zaštititi od njih. Pošto su deo izvornog koda neke Internet stranice, ne mogu se ukloniti niti blokirati. Ne postoje propisi koji ograničavaju dizajnere da postave obaveštenje o tome da se na toj Internet stranici nalazi nešto što ugrožava nečiju anonimnost, tako da korisniku preostaje samo da koristi rešenja koja onemogućavaju učitavanje grafičkih delova stranice. Ovakav način prikupljanja informacija koriste najviše agencije koje se bave reklamiranjem, ali i mnoge velike kompanije.

Fišing (engl. Phishing) je način na koji određene osobe pokušavaju da dodju do korisničkih privatnih informacija, kako bi pomoću njih mogli da ostvare finansijsku korist. Lozinke, brojevi kreditnih kartica, LIB, brojevi socijalnog osiguranja predstavljaju informacije koje se sakupljaju uz pomoć fišinga. Ovakava vrsta ugrožavanja privatnosti predstavlja krivično delo i kažnjiva je zakonom.

Postupci na koji se „sajber“ kriminalci dovijaju kako bi pribavili privatne podatke su različiti. Jedan od načina predstavlja ubacivanje malicioznih softvera na računar. Najčešće to rade uz pomoć lažnih elektronskih poruka, lažnih sajtova, telefonskih poziva itd. Kako bi se korisnik zaštitio od fišinga, mora dobro voditi računa kada otvara poruke elektronske pošte, naročito ako su poslate kao zvanična upozorenja ili obaveštenja od poznatih kompanija. Prilikom pretraživanja Interneta, potrebno je ukucavati tačne nazive Internet stranica, jer se često iza Internet stranica koje se razlikuju samo u jednom slovu od željene stranice, nalaze osobe koje se bave fišingom. Prilikom posećivanja linkova na sajtovima koji nisu zadobili korisničko poverenje, potrebno je paziti da putanja linka ne sarži na kraju adrese „.exe“, jer se u tom slučaju sigurno radi o malicioznom softveru. Prilikom prijema poruka elektronske pošte, treba voditi računa da ukoliko poruka dolazi sa nekog zvaničnog sajta sadrži autentičan način predstavljanja (adresa, naziv, logo). Promena samo jednog slova u nazivu neke firme može ostati neprimetna. Tako korisnik može pomisliti da se radi o autentičnoj poruci i postati žrtva fišinga. Primer fišing poruke sa detaljima na koje se mora obratiti pažnja možete videti ispod.



Slika 8 Primer najčešće primene fišing metode putem elektronske pošte [17]

Farming (engl. Pharming) predstavlja još jednu vrstu „sajber“ napada pomoću koje napadač stiče mogućnost da redirektuje saobraćaj na lažnu Internet stranicu. Kompromitovanjem korisničkog DNS servera koristeći se propustima u softveru ili menjanjem host datoteka na računaru žrtve, svaki korisnički klik ili unos se šalje direktno napadaču. DNS serveri nad kojima su izvršene promene se često nazivaju „zatrovanim“. Farming je kao princip razotkrivanja anonimnosti jako sličan fišingu i najčešće predstavlja prvi korak u njegovom sprovođenju.

5. *Tor* projekat

Tor predstavlja jedno od rešenja za zaštitu anonimnosti na Internetu i predstavlja treću generaciju *onion routing* („crni luk“ rutiranje) [20] projekta američke mornaričke istraživačke laboratorije. Originalno je napravljen sa ciljem primarne upotrebe u zaštiti vladinih komunikacija. Prva verzija ovog softvera izašla je sredinom 1996. godine. Pošto su uvideli da potrebe zaštite anonimnosti na Internetu nisu vezane samo za bezbednosne strukture i vladu, već bi mogle da nađu primenu i u civilnom svetu, sredinom 2002. godine izbacili su prvu verziju *Tor*-a, koja ujedno pretstavlja treću verziju *onion routing* projekta. Danas ga koriste obični ljudi, vojska, novinari, policija, aktivisti i mnogi drugi. Glavni zadatak *Tor*-a je da zaštiti korisnike od onih koji žele da analiziraju njihov saobraćaj na mreži, „mrvice“ koje ostavljaju prilikom korišćenja Interneta i ostalih spoljnih napada od strane drugih korisnika.

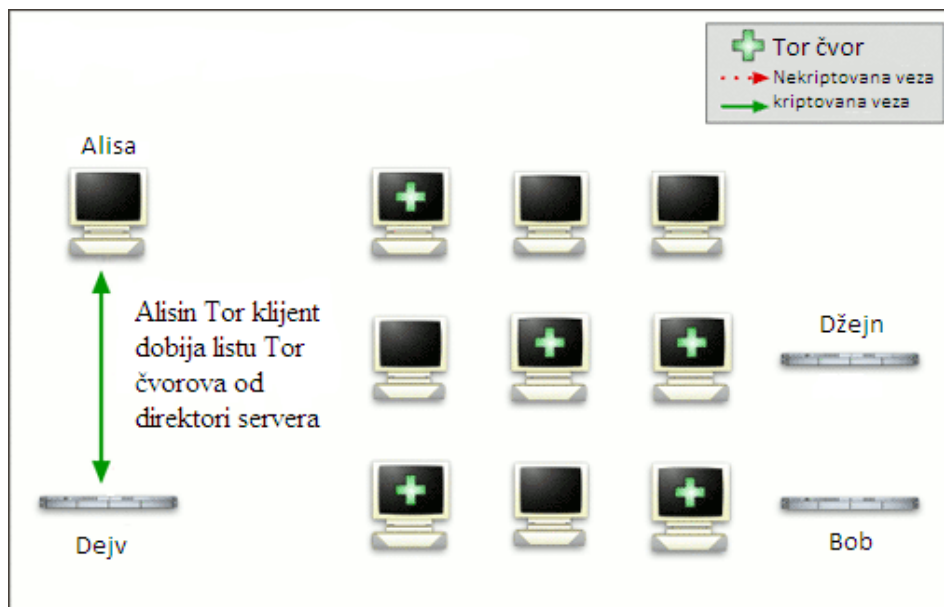
Sredinom 2004. godine *Tor* mreža se sastojala od 32 čvora, 24 u SAD i 8 u Evropi, međutim taj broj se do danas dosta uvećao. Brzina protoka se kretala od 768Kb/768Kb, a neki su imali čak i 10Mb konekcije [21]. Broj korisnika varira, tako da je veoma teško reći ukupan broj, ali je sigurno da ih ima nekoliko stotina. Većina njih su administratori par velikih kompanija koji šalju svoj mrežni sadržaj preko Interneta putem *Tor* mreže, kako bi onemogućili ostale odseke firme da prate njihov saobraćaj. Korisnici *Tor* mreže su prijavili da koriste mrežu za pretraživanje Interneta, FTP, IRC, AIM, Kazaa, SSH i za prijem anonimnih poruka putem „tački za sastanak“. Jedan korisnik je čak uspeo da postavi „Wiki“ kao skrivenu uslugu, gde su ostali mogli da objavljuju adrese njihovih skrivenih usluga.

Svaki čvor trenutno prosleđuje oko 800.000 (oko pola GB) čvornih ćelija nedeljno. U proseku oko 80% od svakog prostora za podatke je popunjen u povratku ka klijentu, a sa oko 40% popunjenosti odlazi od klijenta [21]. Ovakav odnos je zasnovan na tome što korisnici u većini slučajeva skidaju podatke sa Interneta, dok je količina podataka koje se šalje znatno manja.

Najveći deo članova *Tor* mreže zapravo čine volonteri koji postavljanjem svojih *Tor* klijenata za pristupne tačke, šire mrežu i doprinose njenoj popularizaciji. Korisnici mreže su takođe ti koji postavljaju takozvane skrivene usluge putem kojih nude različite servise ostalim korisnicima. Takođe način na koji se korisnici ophode prema mreži i koraci koje oni mogu preduzeti u sprečavanju određenih napada na *Tor* mrežu su jako važni i bitni kako bi se mreža sačuvala.

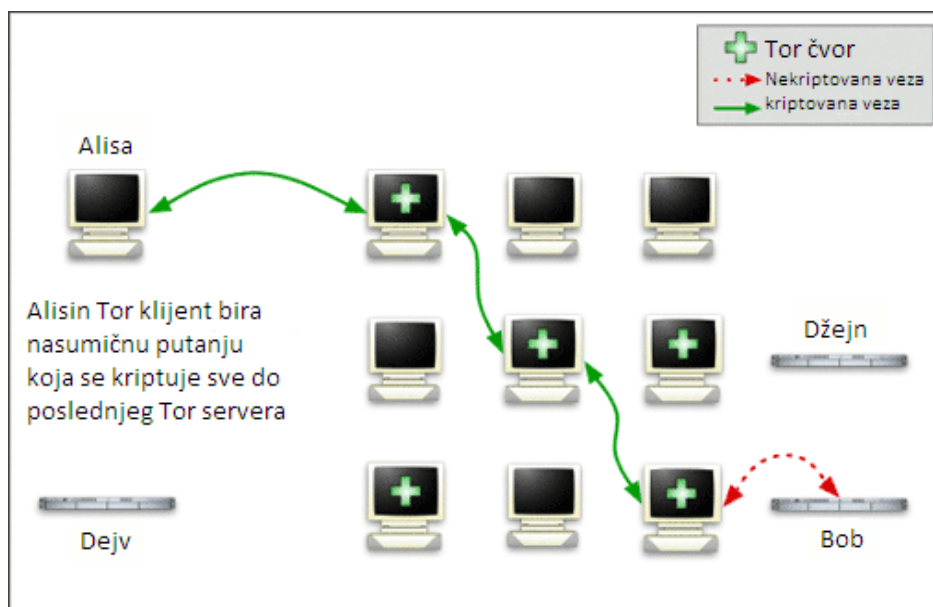
5.1 Način rada

Celokupan projekat je zamišljen da radi na sledeći način. Prvo Alisin *Tor* klijent dobija listu *Tor* čvorova od direktori servera slika 9.



Slika 9 Dobijanje liste *Tor* servera

Nakon toga Alisin *Tor* klijent bira nasumičnu putanju do odredišnog servera. Putanje između *Tor* servera i Alise su šifrovane, a putanja od poslednjeg servera do odredišne adrese, u ovom slučaju Boba, je otvorena.

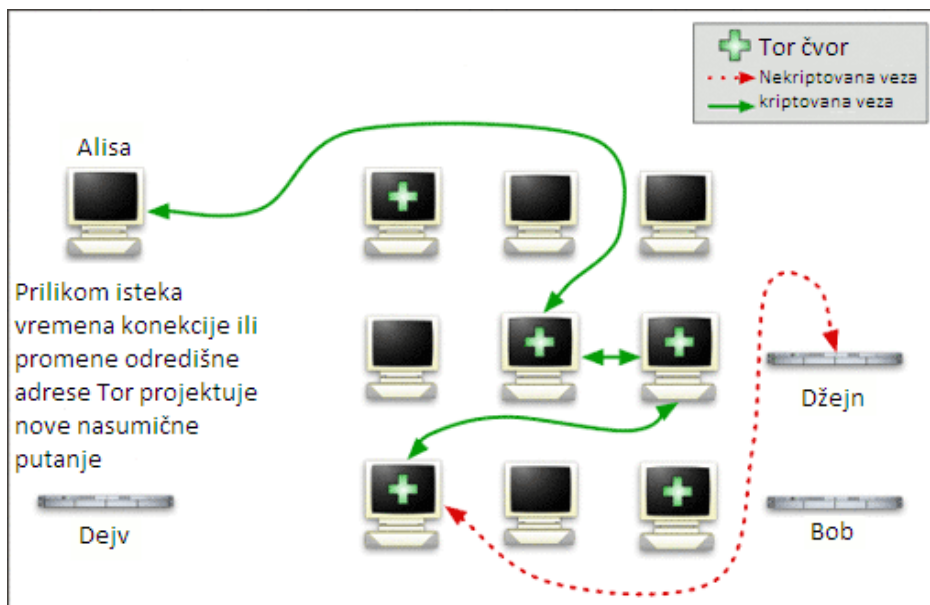


Slika 10 Uspostavljanje veze putem *Tor* servera

Kada se veza uspostavi, različiti tipovi podataka mogu da se razmenjuju i nekoliko različitih vrsta programskih aplikacija mogu da se isporuče preko *Tor* mreže. Pošto nijedan čvor ne vidi više od jednog „skoka“ u putanji, analiziranjem saobraćaja putem „mrvice“ ili

kompromitovanjem čvora nije moguće odrediti izvorišnu i odredišnu adresu. *Tor* jedino radi sa TCP strimovima i može ga koristiti bilo koja aplikacija koja ima podršku za SOCKS.

Kako bi bio efikasniji *Tor* program koristi istu putanju za ostvarivanje konekcije samo ako ona traje neprekidnih 10 minuta. U suprotnom, šalje se zahtev za uspostavljanjem nove putanje, kako bi se ranije započeta akcija mogla nastaviti po novim putanjama. Isto se dešava ukoliko je potreban prelazak na neku drugu odredišnu adresu.



Slika 11 Ponovno uspostavljanje nasumične putanje.

```

\Download\Tor Browser\App\tor.exe
Oct 16 20:47:11.733 [notice] Tor v0.2.3.25 (git-17c24b3118224d65) running on Windows 7.
Oct 16 20:47:11.737 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Oct 16 20:47:11.820 [notice] Configuration file "C:\Users\grni07\AppData\Roaming\tor\torrc" not present, using reasonable defaults.
Oct 16 20:47:11.997 [notice] Initialized libevent version 2.0.21-stable using method win32. Good.
Oct 16 20:47:11.997 [notice] Opening Socks listener on 127.0.0.1:9050
Oct 16 20:47:12.000 [notice] No AES engine found; using AES_* functions.
Oct 16 20:47:12.000 [notice] This OpenSSL has a good implementation of counter mode; using it.
Oct 16 20:47:13.000 [notice] OpenSSL OpenSSL 1.0.0k 5 Feb 2013 looks like version 0.9.8m or later; I will try SSL_OP to enable renegotiation
Oct 16 20:47:14.000 [notice] Reloaded microdescriptor cache. Found 4657 descriptors.
Oct 16 20:47:14.000 [notice] We now have enough directory information to build circuits.
Oct 16 20:47:14.000 [notice] Bootstrapped 80%: Connecting to the Tor network.
Oct 16 20:47:15.000 [notice] Heartbeat: Tor's uptime is 0:00 hours, with 1 circuit open. I've sent 0 kB and received 0 kB.
Oct 16 20:47:15.000 [notice] Bootstrapped 85%: Finishing handshake with first hop.
Oct 16 20:47:15.000 [notice] Bootstrapped 90%: Establishing a Tor circuit.
Oct 16 20:47:17.000 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
Oct 16 20:47:17.000 [notice] Bootstrapped 100%: Done.

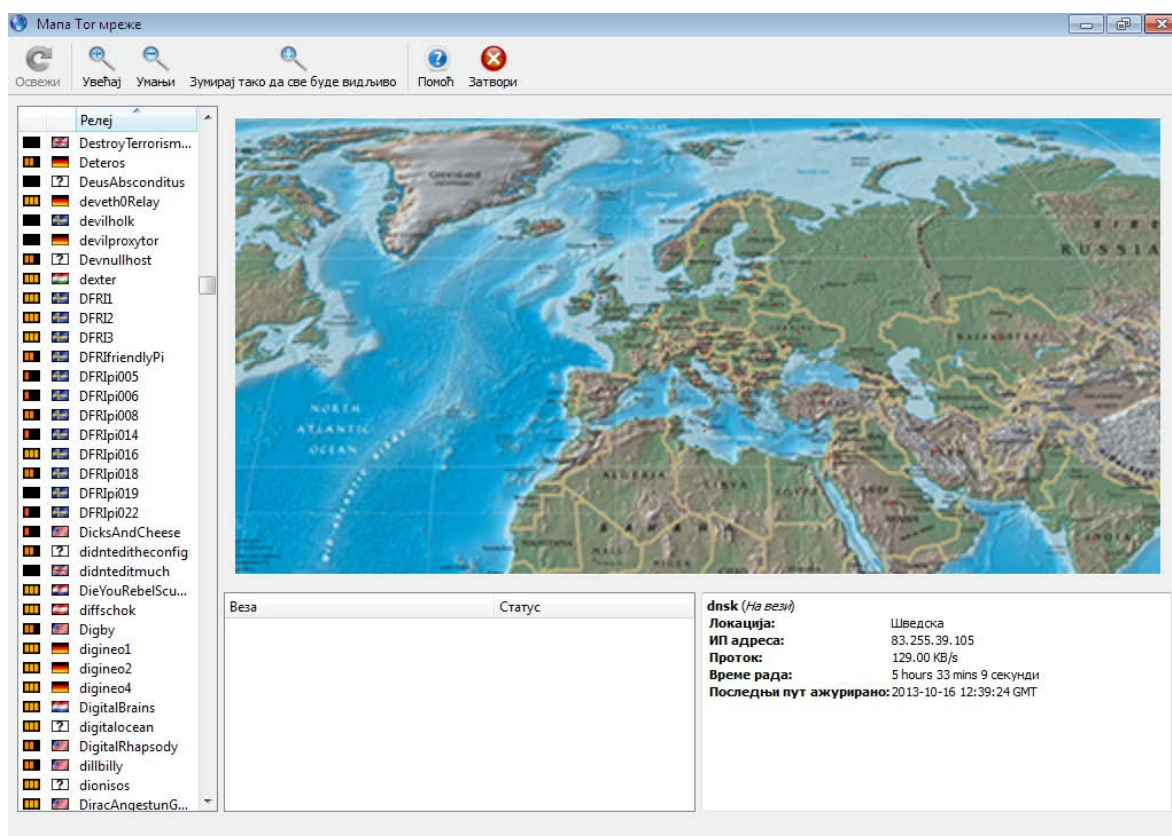
```

Slika 12 Pokretanje *Tor* klijenta i način uspostavljanja veze

Na slici 12 može se videti kako izgleda stvarno povezivanje na *Tor* mrežu koje je gore objašnjeno.

Tor takođe omogućava korisnicima da sakriju svoju lokaciju dok nude razne vrste usluga, kao što su mrežno izdavaštvo ili postavljanje servera za slanje instant poruka.

Korišćenjem *Tor* „tački za sastanke“ ostali *Tor* korisnici mogu da se povežu na ove skrivene usluge, a pritom da ne znaju međusobni mrežni identitet. Ovaj „oblak“ usluga sa skrivenom funkcionalnošću, omogućava *Tor* korisnicima da postave Internet sajt gde ljudi ne moraju da brinu o cenzuri. Niko ne bi bio u mogućnosti da odredi ko nudi usluge sajta i niko ko nudi te usluge ne bi mogao da sazna ko ga je posećivao. Na slici 13 mogu se videti neki od članova koji su bili priključeni na *Tor* mrežu kao i geografske lokacije *Tor* tačaka.



Slika 13 *Tor* mreža sa nekim od njenih korisnika i osnovnim pristupnim tačkama

Tor ne može da reši sve probleme anonimnosti. Njegov način rada je zasnovan na zaštiti transportnih podataka. Ako je potrebno da sajtovi koji se posećuju ne vide informacije koje identifikuju korisnika, moraju se koristiti posebni protokol programi za podršku kao što je na primer *Tor Browser Bundle*.

Projekat takođe sadrži još aplikacija koje pomažu korisniku da ostane anoniman nezavisno od geografske lokacije i Internet provajdera, a njihov način rada će biti predstavljen u narednim odeljcima.

5.2 Protokoli, šifrovanje i uspostavljanje veze

5.2.1 Tor dizajn

Prilikom ostvarivanja konekcija korisnik-čvor ili čvor-čvor svi *onion* ruteri (OR) rade na standardnom korisničkom nivou bez specijalnih privilegija. Svaki OR se povezuje sa susednim putem TLS konekcije. Svaki korisnik sa svog računara pokreće program koji se zove *onion proxy* (OP) kako bi se zakačio na direktori servere. Time uspostavlja putanju kroz mrežu i povezivanje sa korisničkim aplikacijama. Ovi OP prihvataju TCP strimove i multipleksiraju ih duž putanje. OR sa druge strane putanje pravi konekcije ka željenim destinacijama i preusmerava podatke kroz mrežu.

Svaki OR poseduje dugoročan ključ identiteta i kratkoročan *onion* ključ. Ključ identiteta se koristi da bi se potpisali TLS sertifikati, OR-ski deskriptor (suma njegovih ključeva, adresa, propusnog opsega, izlaznih pravila i td.) i potpisivanje direktorija (od strane direktori servera). *Onion* ključ se koristi da se dešifruje zahtev od korisnika prilikom uspostavljanja putanje i prilikom dogovaranja kratkotrajnih ključeva. TLS protokol takođe uspostavlja kratkotrajni link ključ kada komunicira između OR-a. Kratkotrajni ključevi se rotiraju periodično i nezavisno, kako bi bio onemogućen napad na ključ a samim tim i njegova kompromitacija.

5.2.2 Čelije

Onion ruteri komuniciraju sa korisničkim OP i međusobno putem TLS konekcije sa kratkotrajnim ključevima. Korišćenjem TLS protokola podatak ostaje sakriven putem PFS¹ konekcije, sprečavajući tako napadača da naruši integritet podatka ili da se predstavi kao korisnikov OR.

Saobraćaj koji se odvija duž ove konekcije, prosleđuje se u ćelijama od kojih svaka sadrži 512 bajtova. Čelija se sastoji od zaglavlja i mesta za podatke. Zaglavlje sadrži identifikator putanje (circID) koji specificira koja putanja se odnosi na koju ćeliju (razlog za to je što više putanja može biti multipleksirano kroz jednu TLS konekciju), kao i komandu koja opisuje šta da se radi sa prostorom za podatke. Svaka putanja ima različit identifikator putanje na svakom prelazu između OP-OR ili OR-OR. U zavisnosti od komande koju sadrže ćelije se dele na:

- Kontrolne ćelije (control cells)- tumači ih uvek čvor koji ih prima
- Čvorne ćelije (relay cells)- služe za prenos podataka sa kraja na kraj

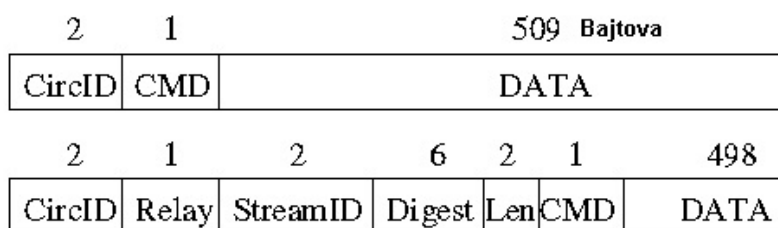
¹ Perfect forward secrecy- Metod za kriptovanje podataka

Kontrolne ćelijske komande su:

- punjenje (*padding*)- trenutno označavaju „održavanje u životu“, ali mogu služiti za postavljanje linka
- napravi ili napravljeno (*create or creted*)- koristi se za postavljanje nove putanje
- uništi (*destroy*)- koristi se za raskidanje putanje

Čvorne ćelije sadrže dodatno zaglavlje (čvorno zaglavlje) ispred dela za prenos podataka koje sadrži identifikator protoka (streamID), kontrolnu sumu sa kraja na kraj radi provere integriteta, dužinu čvornog prostora za podatke i komandu čvora. Celokupan sadržaj zaglavlja čvora i prostora za podatke ćelije čvora se šifrjuje ili dešifrjuje zajedno kako se ćelija čvora kreće po putanji, koristeći pritom 128-bitni AES šifrat. Komande čvora koje se koriste za kontrolu protoka su:

- čvorni podaci (*relay data*)- označava protok podataka
- startovanje čvora (*relay begin*)- komanda za propuštanje protoka
- zaustavljanje čvora (*relay end*)- uredno zaustavljanje protoka
- raskidanje čvora (*relay teardown*)- prekidanje neispravnog protoka
- čvor je povezan (*relay connected*)- obaveštava OP da je čvor startovan uspešno
- proširenje čvora i čvor je proširen (*relay extend, relay extended*)- proširivanje putanje za jedan „skok“ i potvrda da je to urađeno
- čvor se izostavlja i čvor je izostavljen (*relay truncate, relay truncated*)- prekidanje samo dela putanje i potvrda da je to urađeno
- čvor „pošalji mi“ (*relay sendme*)- koristi se za kontrolu zagušenja
- čvor „ispusti“ (*relay drop*) koristi se kako bi se implementirale „lutke“ dalekog dometa



Slika 14 Izgled zaglavlja ćelije i čvora

5.2.3 Putanje i konekcije

Onion Routing originalno pravi putanje za svaki TCP protok. Iz razloga što pravljenje putanje može potrajati nekoliko desetina sekunde (zbog šifrovanja sa javnim

ključem i mrežnog kašnjenja), ovaj dizajn pravi veliki utrošak vremena aplikacijama kao što su web pretraživači koji otvaraju mnogo TCP protoka.

Tor projekat, omogućava deljenje putanje sa mnogo TCP tokova. Da bi se izbegla kašnjenja, korisnik preventivno konstruiše putanju. Kako bi se limitirao problem zagušenosti linka, korisnikov OP pravi nove putanje ako prethodne nisu bile u upotrebi, i postavlja kao neaktivne sve stare putanje po kojima nema započetog saobraćaja. OP-iji razmatraju prelazak na novu putanju jednom u minuti, iako i najzahtevniji korisnici potroše neznatno vreme u kreiranju putanja. Ovo se radi iz razloga što ipak postoji ograničen broj zahteva koji mogu biti povezani jedan sa drugim kroz zadati izlazni čvor. Takođe pošto se putanje prave u pozadini, OP-iji mogu da se oporave ukoliko dođe do prekida u stvaranju putanje bez da korisnik to primeti.

5.2.4 Konstruisanje putanje

Korisnički OP konstruiše putanje postepeno, dogovarajući simetrični ključ sa svakim OR-om koji se nalazi na putanji, praveći jedan po jedan skok. Prilikom započinjanja pravljenja nove putanje, Alisin OP šalje komandu *create cell* do prvog čvora u izabranoj putanji (taj čvor ćemo da nazovemo Bob). Alisa bira novi *cicrID* C_{Ab} koji trenutno nije iskorišćen za ostvarivanje konekcije između nje i Boba. Napravljena ćelija u svom delu za podatke sadrži prvu polovinu Difi-Helman metode razmene ključeva (g^x) i šifrue ga sa Bobovim *onion* ključem. Bob odgovara kreirajući ćeliju koja sadrži g^y i hašovanu vrednost dogovorenog ključa $K = g^{xy}$.

Jednom kada je putanja uspostavljena, Alisa i Bob mogu da šalju jedno drugome čvorne ćelije šifrovane dogovorenim ključem. Kako bi se putanja proširila Alisa šalje komandu *relay extend cell* Bobu, precizirajući adresu sledećeg OR-a koga ćemo nazvati Kerol. U isto vreme Bob prosleđuje šifrovano g^{x_2} od Alise. Bob kopira polovinu dogovora i pakuje ga u ćeliju sa komandom *create cell* i prosleđuje je do Kerol čime proširuje putanju. Bob bira novi *cicrID* C_{BC} za ostvarivanje konekcije sa Kerol. Kada Kerol odgovori sa komandom *created*, Bob pakuje prostor za podatke u proširenu čvornu ćeliju i prosleđuje je nazad do Alise. Sada je putanja proširena do Kerol, a Alisa i Kerol dele zajednički ključ $K_2 = g^{x_2 y_2}$. Kako bi se putanja proširila za još jedan čvor, Alisa ponavlja radnje od malopre, govoreći uvek poslednjem čvoru u putanji da se proširi za još jedan skok dalje.

Korišćenjem ovog protokola za uspostavljanje putanje postiže se jednostrana autentifikacija korisnika i ključa. Alisa zna da se dogovara sa OR-om, a OR-u nije bitno ko otvara putanju. Alisa ne koristi nikakav javni ključ i tako ostaje anonimna iz razloga što se Alisa i OR dogovaraju oko ključa za koji Alisa saznaje samo da ga je OR „naučio“. Takođe se postiže unapređena tajnost i „svežina“ ključeva. Ozbiljnije gledajući, protokol izgleda ovako:

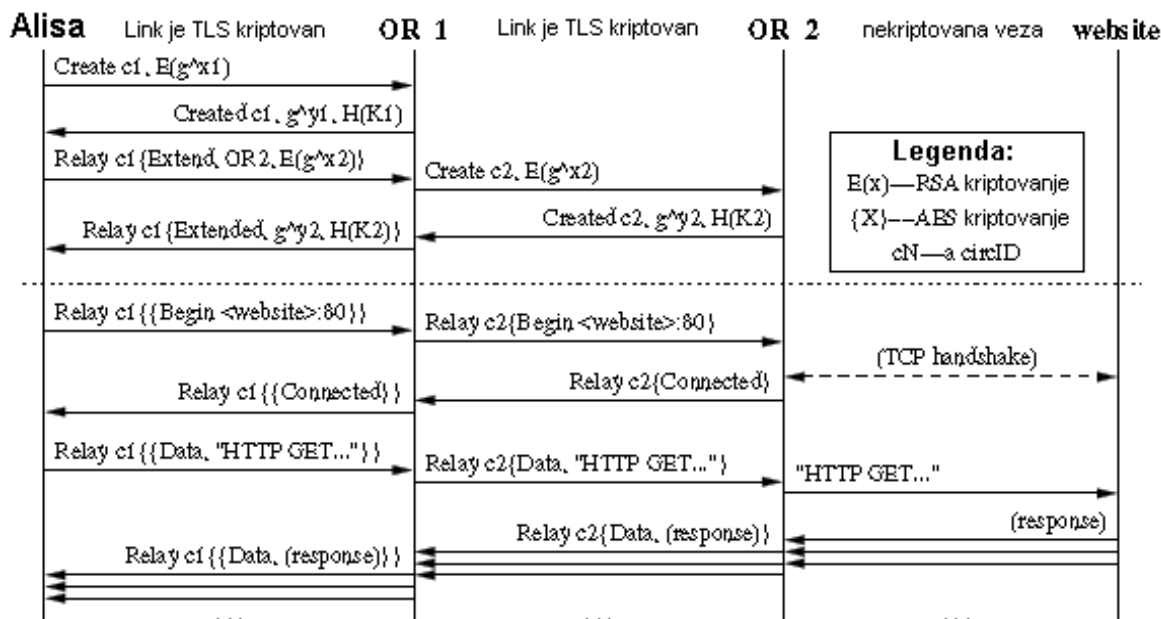
$$\text{Alisa} \rightarrow \text{Bob} : E_{PK_{\text{Bob}}}(g^x)$$

$$\text{Bob} \rightarrow \text{Alisa} : g^y, H(K \mid \text{“rukovanje“})$$

Gde je:

- $E_{PK_{Bob}}(\cdot)$ šifrovano sa Bobovim javnim ključem
- H je sigurna haš funkcija

U drugom koraku, Bob dokazuje da je on taj koji prima g^x , i onaj koji bira y . U prvom koraku koristi se šifrovanje sa javnim ključem iz razloga što je jedna ćelija previše mala da bi sadržala i javni ključ i potpis. Nezvanične analize sa NRL protokol analizatorom pokazuju da je protokol bezbedan (uključujući i PFS (*Perfect Forward Secrecy*)) upoređujući ga sa tradicionalnim *Dolev-Yao* modelom.



Slika 15 Protokol uspostavljanja veze

5.2.5 Čvorne poruke

Kada je konekcija uspostavljena Alisa može da šalje čvorne ćelije. Kada OR primi ćeliju on traga za odgovarajućom putanjom i dešifruje čvorno zaglavlje i prostor za podatke sesijski ključem za tu putanju. Ako je ćelija upućena od Alise, OR proverava da li dešifrovana ćelija ima validan broj bitova. Ako je važeća, on prihvata čvornu ćeliju i prosleđuje je na način koji ću opisati ispod. U suprotnom, OR traga za circID i OR-om kao sledeći korak putanje. On zamenjuje circID odgovarajućim i šalje dešifrovanu čvornu ćeliju do sledećeg OR-a. Kada krajnji čvor u putanji primi neprepoznatljivu čvornu ćeliju, javlja se greška i putanja se prekida.

OP-iji tretiraju dolazeće čvorne ćelije veoma slično. Oni neprestano dešifruju čvorna zaglavlja i prostor sa porukom ključem sesije koji deli svaki čvor u putanji. Ako je bitska provera važeća, OR mora da odredi poreklo ćelije koju je upravo dešifrovao. Kako bi konstruisala poruku koju šalje ka OR-u, Alisa dodeljuje bitsku vrednost i onda neprestano šifruje prostor za podatke (tačnije čvorno zaglavlje i prostor za podatke) sa

istim simetričnim ključem za svaki „skok“ do određenog OR-a. Pošto je bitski broj šifrovan na različitu vrednost za svaki skok, samo ciljani OR će moći da dobije smislen rezultat. Ovakav način, koji podseća na cev koja curi na sve strane omogućava da Alisin saobraćaj može da se preusmerava na više različitih izlaza u okviru iste putanje. Alisa onda može da bira izlazne tačke, na osnovu njihovih izlaznih pravila ili da onemogući OR-e da saznaju da su dva protoka u stvari upućena od iste osobe.

Kada OR kasnije odgovori Alisi sa porukom *relay cell*, on šifrjuje ćelijsko zaglavlje i prostor za podatke sa jednim ključem koji deli sa Alisom i šalje ga nazad Alisi duž putanje. Sledeći OR-i naknadno šifruju poruku kako je prosleđuju nazad do Alise.

Da bi raskinula putanju, Alisa šalje kontrolnu komandu *destroy cell*. Svaki OR u putanji prima komandu, zatvara sve konekcije na putanji i prosleđuje novu *destroy cell* poruku dalje. Baš kao što se putanja pravi postepeno, ona isto tako može biti uništena. Alisa može poslati komandu *relay truncate cell* jednom OR-u na putanji. Taj OR onda šalje *destroy cell* komandu dalje i obaveštava Alisu sa komandom *relay truncated cell*. Alisa onda može da proširi putanju na različite čvorove, bez potrebe da obaveštava posredne čvorove o tome. Slično tako, ako čvor na putanji otkáže, susedni čvor šalje *relay truncated cell* komandu nazad do Alise.

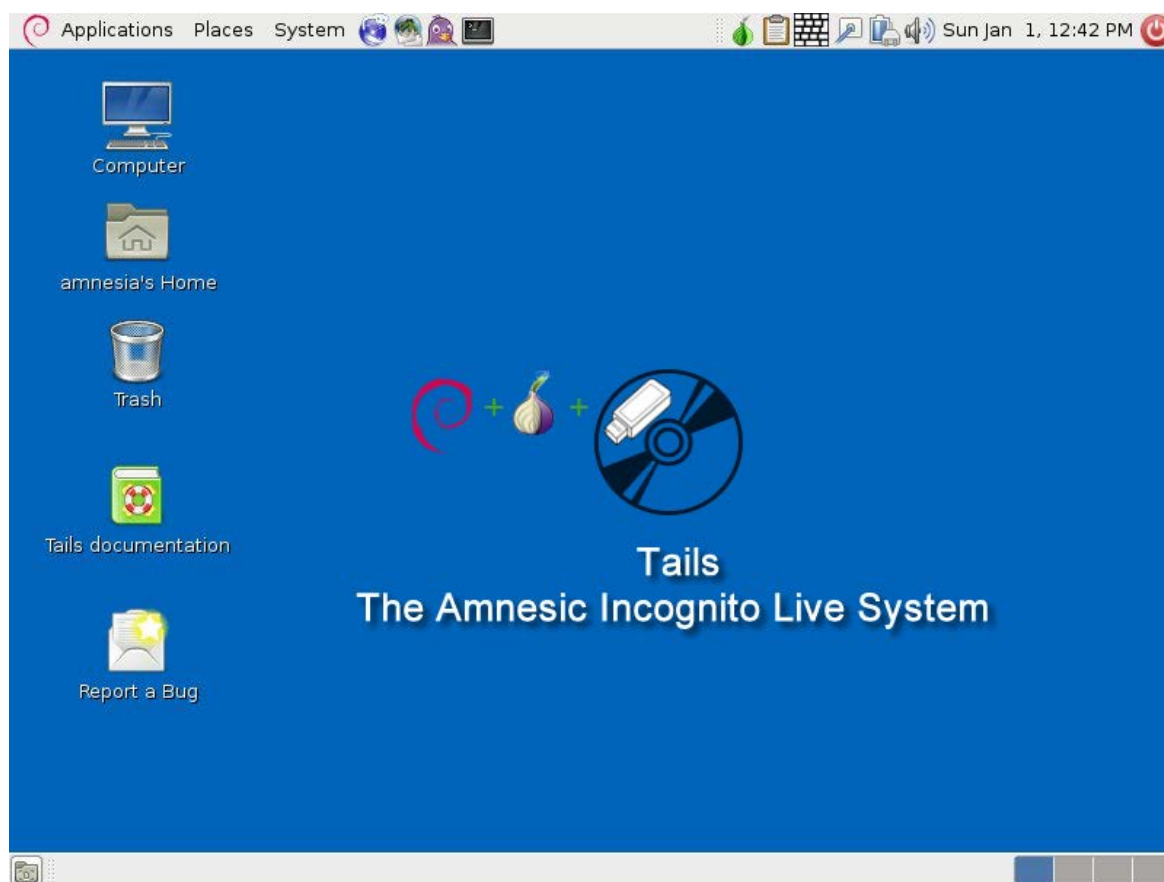
5.3 Aplikacije Tor mreže

5.3.1 Tails (repovi)

Tails predstavlja živi sistem koji je napravljen sa ciljem da se sačuva korisnička privatnost i anonimnost. Pruža pomoć u korišćenju Interneta, anonimno zaobilazeći cenzuru na svakom računaru, pritom ne ostavljajući nikakve tragove, osim ako se to eksplicitno ne zatraži.

Ova aplikacija predstavlja kompletan operativni sistem, napravljen da se koristi putem DVD diska ili USB memorije nezavisno od operativnog sistema koji se nalazi na samom računaru. Pošto je softver besplatan, osnovu sistema čini DEBIAN GNU/Linux platforma. Uz nju se dobija nekoliko aplikacija koje su prekonfigurisane da budu bezbedne. To su: Internet pretraživač, klijent za instant poruke, klijent elektronske pošte, paket za kancelarijsko poslovanje, editor slike i zvuka i td.

Tails je konfigurisan sa posebnom brigom o tome da ne koristi hard disk računara na kojem je podignut, čak i ako postoji slobodan prostor za razmenu na njemu. Jedini prostor za čuvanje podataka koji se koristi je RAM memorija, koja se automatski briše kada se računar isključi. Sa ovakvim načinom rada, *Tails* sistem neće ostaviti nikakav trag, niti se može videti da je računar korišćen. Na slici 16 može se videti izgled aplikacije.



Slika 16 Tails aplikacija podignuta sa USB memorijskog diska

5.3.2 Tor Browser Bundle

Ova aplikacija predstavlja samostalni Internet pretraživač koji putem Tor mreže štiti korisničku konekciju, sakrivajući podatke od onoga ko ga posmatra i pokušava da otkrije koje sajtove posećuje, a sajtove koje posećuje sprečava u otkrivanju njegove geografske lokacije i tako mu omogućava pristup mestima koja su blokirana za njegovo geografsko područje.

Dizajneri ove aplikacije su omogućili da bude kompatibilna sa operativnim sistemima kao što su Windows, Mac OS X i Linux operativni sistem, a da pritom ne mora da se instalira nikakav dodatni program. Moguće ga je čak postaviti da se pokreće sa USB prenosivog diska, gde je prekonfigurisan kako bi zaštitio identitet korisnika, a takođe je i samo- održiv.

Pretraživač je delom zasnovan na *Mozilla Firefox ESR* platformi i poseduje mogućnosti dorade izgleda.

Glavna stvar kod ovog pretraživača je u tome što su onemogućene sve stavke koje mogu da zaobiđu *Tor* mrežu i izađu nezaštićeno na Internet kao što su *Java* i *Flash player* dodaci.

5.3.3 Orbot

Orbot predstavlja besplatnu *Tor* aplikaciju za mobilne telefone sa Android operativnim sistemom. On omogućava ostalim aplikacijama da sigurnije koriste Internet. Orbot koristi *Tor* kako bi šifrovao korisnički Internet saobraćaj i onda ga „sakrio“ iza niza računara po celom svetu. Licenca za korišćenje je besplatna i program pomaže da se izbori sa „oslušivanjem“ mrežnog saobraćaja. Orbot je osvojio nagradu u organizaciji *Electronic Frontier Foundation* u 2012. godini.

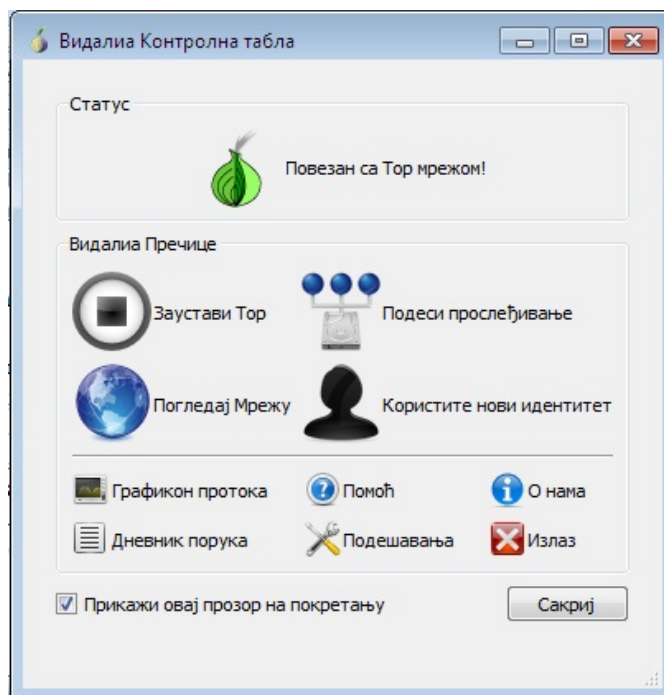


Slika 17 Izgled Orbot platforme za android mobilne telefone

5.4 Instalacija i pokretanje *Tor* pretraživača

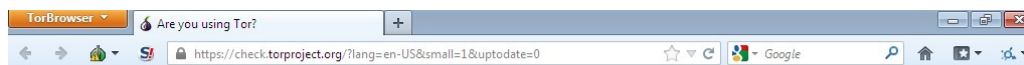
U ovom delu će biti prikazana instalacija *Tor* pretraživača samo na Windows 7 platformi, a uputstva za instalaciju na ostalim operativnim sistemima se mogu pogledati na sledećem linku <https://www.torproject.org/projects/torbrowser.html.en>.

Instalacija je u principu jako jednostavna, dovoljno je samo skinuti datoteku sa *Tor* servera, raspakovati je na određenoj lokaciji i zatim pokrenuti fajl „*Start Tor Browser.exe*“. Pokretanjem te aplikacije u stvari se pokreće „*Vidalia kontrolna tabla*“ koju ujedno pokreće i *Tor* klijent sa kojim se povezujemo na *Tor* mrežu.



Slika 18 Vidalia kontrolna tabla

Nakon pokretanja kontrolne table i uspostavljanja konekcije sa *Tor* mrežom, otvara se prozor *Tor* pretraživača sa početnim informacijama, gde se već na prvi pogled može videti da je IP adresa računara promenjena i da se digitalno gledano, nalazi na sasvim drugom geografskom području.



Congratulations. Your browser is configured to use Tor.

There is a security update available for the Tor Browser Bundle.

[Click here to go to the download page](#)

Please refer to the [Tor website](#) for further information about using Tor safely. You are now free to browse the Internet anonymously.

Your IP address appears to be **46.249.58.148** ← FIKTIVNA IP ADRESA

This page is also available in the following languages:

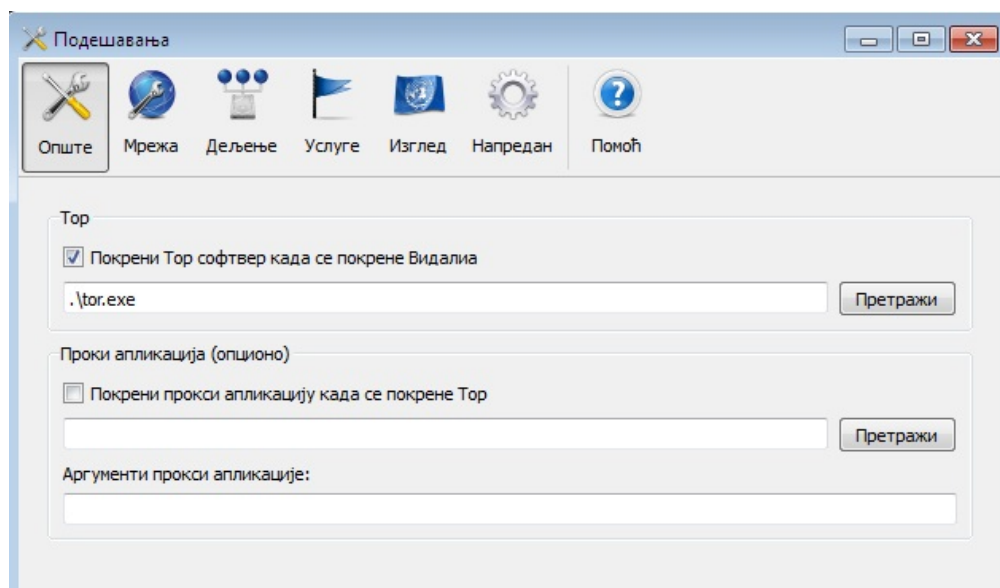
[العربية](#) (Arabijski) [Бурмес](#) [Česky](#) [danek](#) [Deutsch](#) [Ελληνικά](#) (Ellinika) [English](#) [español](#) [Estonian](#) [فارسی](#) (Fārsi) [suomi](#) [français](#) [Italiano](#) [日本語](#) (Nihongo) [norsk](#) (bokmål) [Nederlands](#) [polski](#) [Português](#) [Português do Brasil](#) [română](#) [Русский](#) (Russkij) [ไทย](#) [Türkçe](#) [українська](#) (ukrajins'ka) [Vietnamese](#) [中文](#) (Zhōng)

Slika 19 Tor Browser početna stranica

Raspakovanu datoteku je moguće presnimati na prenosivi USB disk, i potom je pokrenuti na bilo kom drugom računaru, čak iako se ne poseduju administratorske privilegije na njemu. Jedino što mora biti omogućeno je pristup USB portu na računaru.

5.5 Podešavanje Tor klijenta i Tor pretraživača

Konfiguracija *Tor* klijenta se započinje pritiskom na dugme „podešavanja“ u Vidalia kontrolnoj tabli. Nakon toga se otvara prozor koji je prikazan na slici 20, koji sadrži više kartica podešavanja u zavisnosti od usluge koja je potrebna.



Slika 20 Prozor sa karticama za konfigurisanje *Tor* klijenta

Podešavanja klijenta su veoma jednostavna ukoliko se poznaje značenje i način rada opcije koja se podešava, pa će u narednom delu upravo to biti i objašnjeno.

- Proksi pristup Internetu

Ukoliko je korisnički računar deo neke lokalne mreže (poslovna, akademska), najverovatnije će njegov pristup Internetu biti ili limitiran ili će mu biti potrebni neki autentifikacioni parametri da bi se spojio sa *Tor* mrežom.

- Zaštitni zid (Firewall)

Još jedna od zaštita koja može da blokira pristup *Tor* mreži. Potrebno je da se poznaju portovi po kojima aplikacija može da komunicira sa *Tor* mrežom.

- Blokiranje pristupa *Tor* mreži od strane provajdera

Ovaj podatak može ozbiljno ugroziti pristup *Tor* mreži, jer takva blokada ne samo da joj onemogućava pristup, već najčešće iza toga stoje politički, ideološki, ili bezbednosni razlozi države u kojoj se nalazi korisnički provajder pa možda i sam korisnik. Problem je moguće prevazići, ali korisnik može snositi određene posledice zbog toga.

Da bi se problem rešio potrebno je da se nadje „prijatelj“ koji takođe koristi *Tor* mrežu a nalazi se u državi gde mu nije zabranjen pristup od strane Internet provajdera. „Prijatelj“ mora da napravi „most“ preko kojeg će omogućiti korisniku da se povezivanjem preko njegovog *Tor* klijenta pristupi *Tor* mreži. „Prijatelji“ se mogu naći i na sajtu <https://bridges.torproject.org/>, a može se napraviti i lični dogovor sa osobom koja je spremna da pruži takvu vrstu usluge.

- *Reley traffic inside Tor network (non exit relay)*

Ova opcija predstavlja definisanje takozvanog „mosta“ putem kojeg korisnik postaje „prijatelj“ nekome kome je putem Internet provajdera blokiran pristup *Tor* mreži. Ova opcija dozvoljava članovima *Tor* mreže da ga koriste samo kao čvornu tačku ka ostalim tačkama *Tor* mreže.

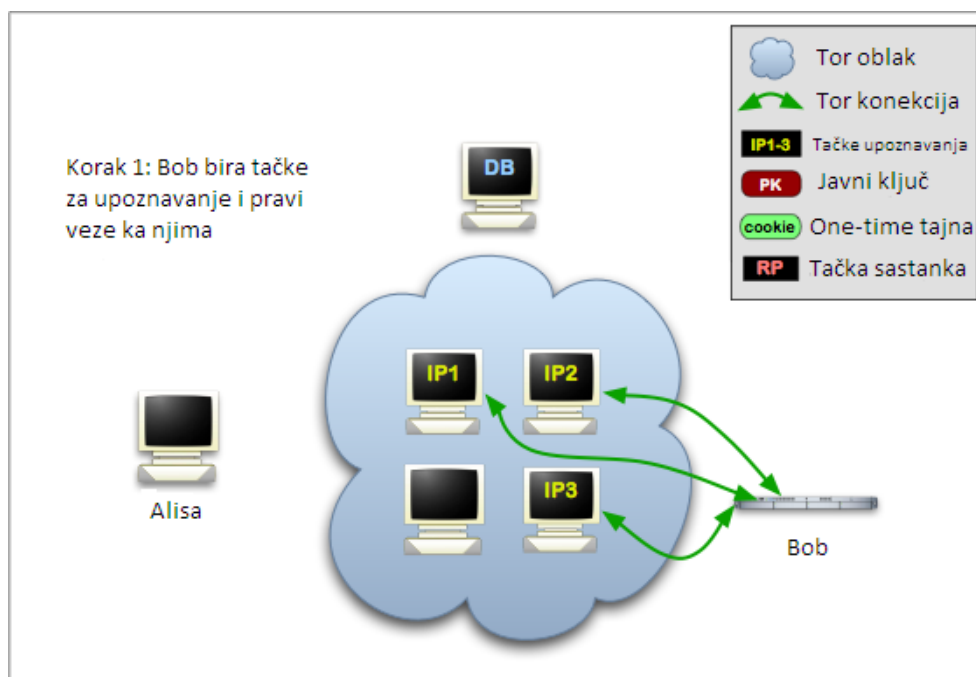
- *Reley traffic inside Tor network (exit relay)*

Kao što smo do sada uvideli, *Tor* mreža se sastoji od ulaznih čvorova (korisnička aplikacija), čvorova (zvaničnih i nezvaničnih) i izlaznih čvorova koji omogućavaju ponovni izlaz na Internet mrežu. Ova opcija pretvara korisničkog *Tor* klijenta u izlazni čvor koji omogućava korisnicima da pristupe Internet stranicama preko njega. Takođe se kroz različita pravila dopuštaju ili zabranjuju određene usluge korisnicima.

- Skriveni servisi

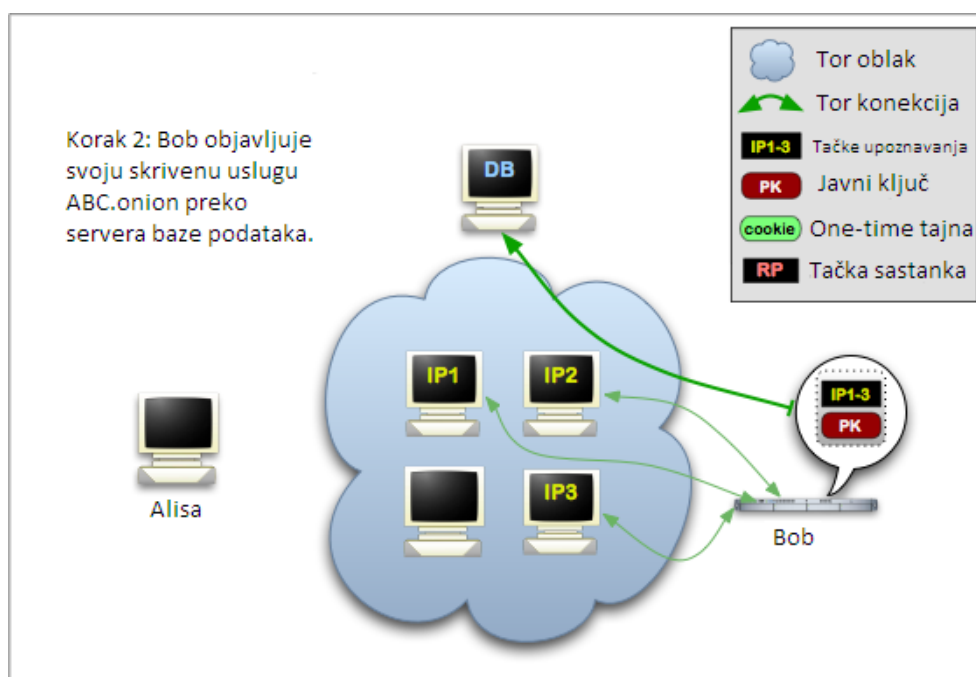
Ova opcija predstavlja mogućnost korišćenja određenih servisa putem *Tor* mreže, pod uslovom da su korisnici *Tor* mreže upoznati da takvi servisi postoje. Mogućnosti su razne, a jedne od najčešćih su Internet oglašavanje i postavljanje servera za brze poruke.

Skriveni servisi moraju na neki način da reklamiraju svoje postojanje na *Tor* mreži pre nego što klijenti budu u mogućnosti da ih kontaktiraju. Usluga zato nasumično bira čvorne tačke, pravi veze sa njima i prosleđuje im zahtev da se ponašaju kao tačke za upoznavanje, ostavljajući im svoj javni ključ. To se radi iz razloga što je jako teško povezati nekoga sa tačkom za upoznavanje a da pritom imate sakrivenu IP adresu servera. Otkrivajući im identitet skrivene usluge putem javnog ključa oni ne moraju znati sakrivenu IP adresu servera.



Slika 21 Postavljanje tačaka za upoznavanje

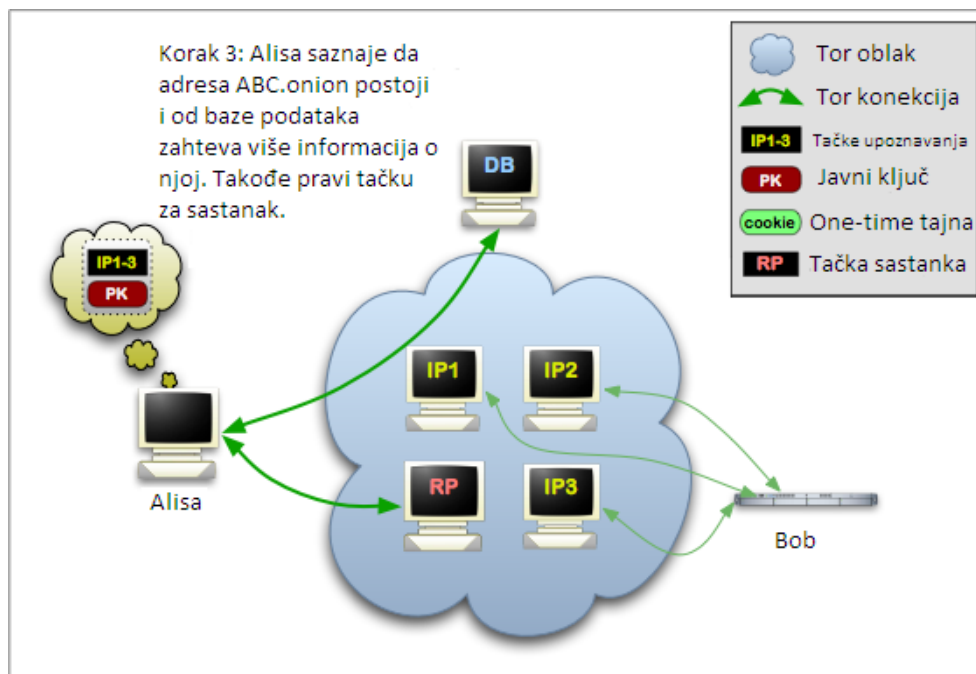
Skriveni servis se zatim objedinjuje u deskriptor istih, koji sadrži javni ključ i sve tačke upoznavanja. Sve ovo se potpisuje sa skrivenim ključem i taj deskriptor se otprema u distribuiranu heš tabelu. Klijenti koji šalju zahtev ka ABC.onion (gde je ABC ime od 16 karaktera koje potiče od javnog ključa) biće upućeni na deskriptor. Nakon ovog koraka skrivena usluga je postavljena.



Slika 22 Objavljivanje skrivene usluge

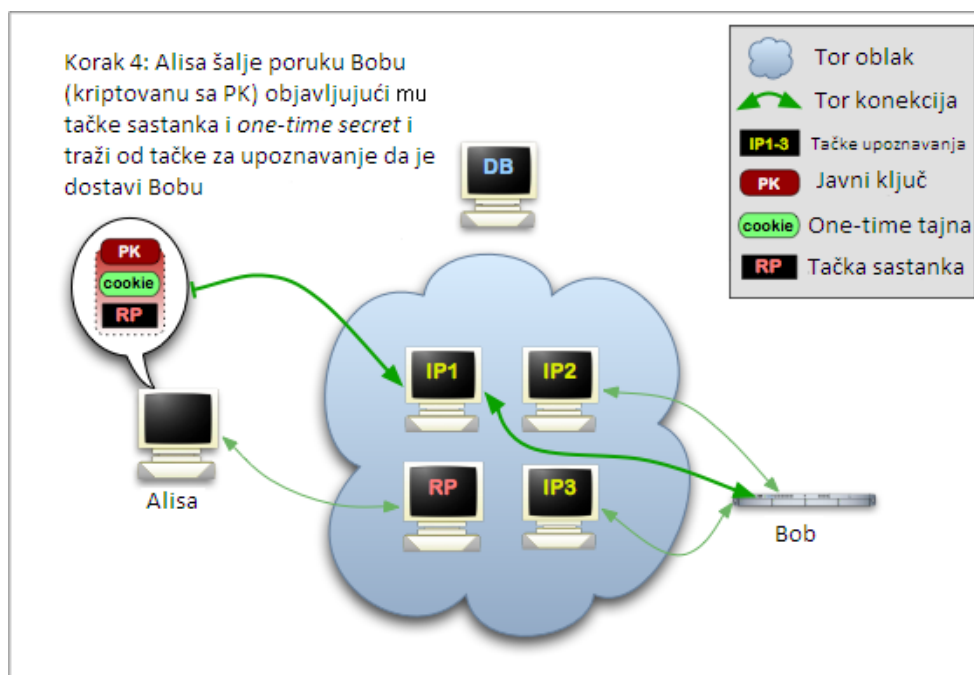
Klijent koji želi da koristi skrivenu uslugu mora prvo da sazna njenu *onion* adresu. Nakon toga klijent može da zahteva uspostavu veze, skidajući deskriptor iz distribuirane

heš tabele. Ako postoji deskriptor za ABC.onion (može se desiti da je servis nedostupan, odavno napušten ili greška u kucanju adrese) klijent saznaje koje su tačke upoznavanja i koji su pravi javni ključevi. U isto vreme, klijent takođe kreira vezu ka nasumično izabranom čvoru i zahteva od njega da se ponaša kao tačka za sastanak prosledjujući *one-time secret* (vremenski sesijski žeton).



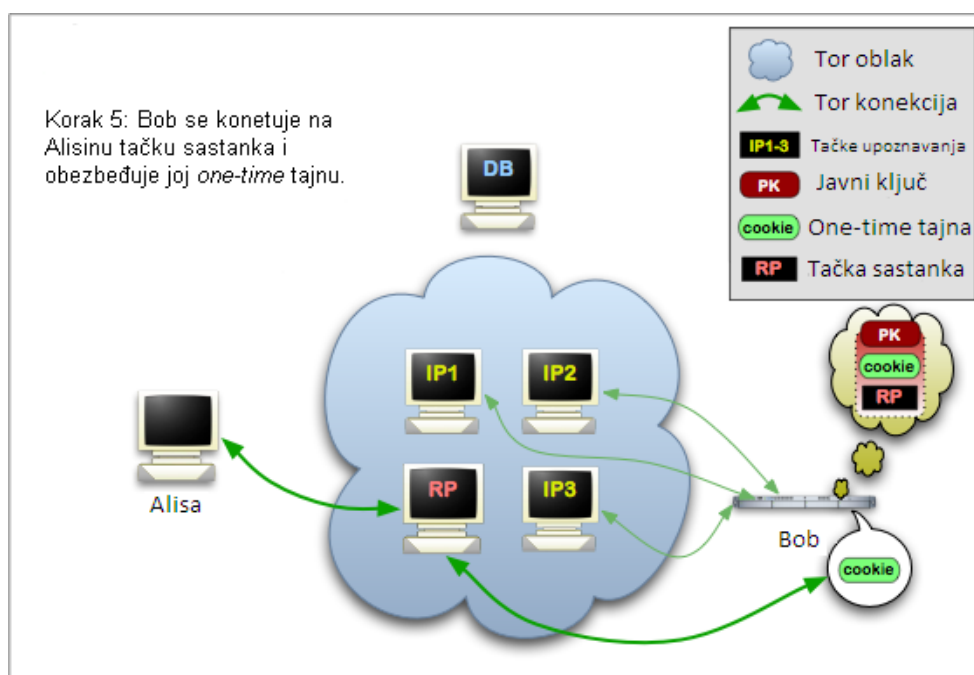
Slika 23 Kreiranje tačke sastanka i prijem parametara za ABC.onion

Kada su završeni prethodni koraci klijent kreira poruku predstavljanja (šifrovanu javnim ključem skrivenog servisa) koja uključuje adresu tačke sastanka i *one-time secret* žeton. Poruka se šalje ka jednoj od tačaka za upoznavanje, sa zahtevom da se prosledi ka skrivenoj usluzi. Pošto se celokupna komunikacija obavlja putem *Tor* mreže, niko ne može da poveže poruku sa IP adresom pošiljaoca, tako da klijent koji je šalje ostaje anonimn.



Slika 24 Alisa šalje poruku Bobu

U sledećem koraku skrivena usluga dešifruje poruku koju je dobila od klijenta i pronalazi adresu tačke sastanka i *one-time* tajne. Usluga kreira putanju do tačke sastanka i šalje joj *one-time* tajnu upakovanu u poruku. Od ovog trenutka jako je važno da skrivena usluga bude vezana isključivo za isti set „ulaznih čuvara“ kada kreira novu putanju. U suprotnom, napadač bi mogao da pokrene sopstveni čvor i prisili skrivenu uslugu da napravi proizvoljan broj čvorova u nadi da će podmetnuti čvor biti izabran kao ulazni čvor i tako saznati IP adresu skrivene usluge koristeći vremensku analizu.

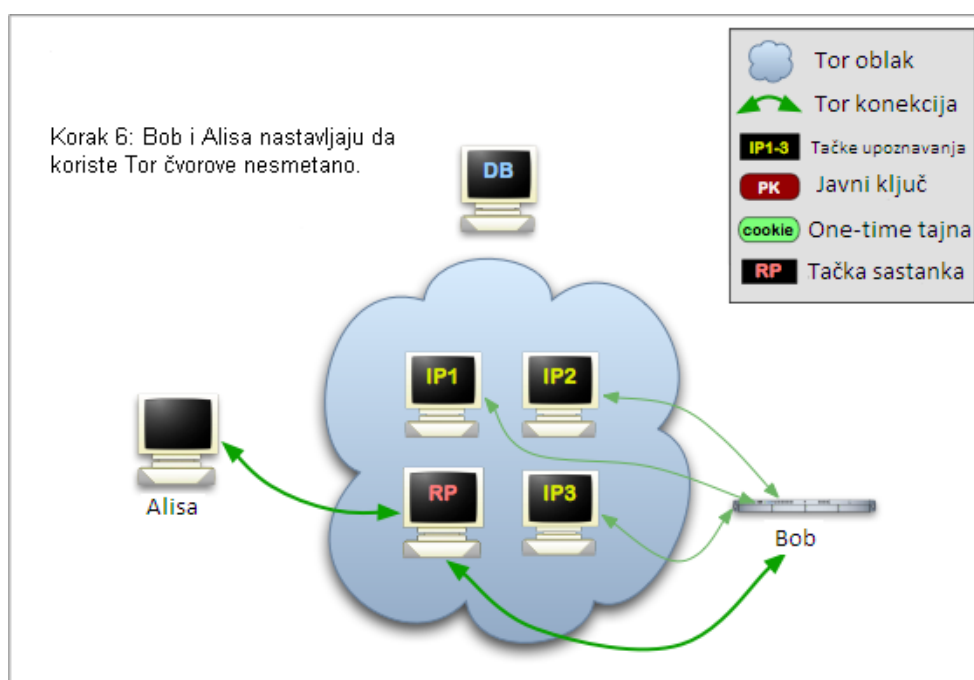


Slika 25 Povezivanje sa tačkom sastanka

U poslednjem koraku tačka sastanka obaveštava klijenta o uspešnom ostvarivanju veze. Nakon toga oba klijenta i skrivena usluga mogu koristiti putanje do tačke sastanka kako bi komunicirali međusobno. Tačka sastanka prosto preusmerava (potpuno šifrovano) poruku od klijenta do skrivene usluge i obrnuto.

Jedan od razloga zašto se ne koristi tačka upoznavanja kako bi se preko nje obavljala komunikacije je iz razloga što ni jedan čvor ne sme biti odgovoran za pružanje skrivene usluge. Po ovom principu rada tačka sastanka nikada ne može da sazna identitet skrivene usluge.

Uopšteno, celokupna veza između klijenta i skrivene usluge sastoji se iz šest čvorova, tri su izabrana od strane klijenta (gde treći čini tačku sastanka) a tri sa strane skrivene usluge.



Slika 26 Uspešno uspostavljanje skrivene usluge

5.6 Napadi na mrežu i odbrane

5.6.1 Pasivni napadi

- Nadgledanje korisničkih obrazaca ponašanja

Nadgledanje korisnikove mreže neće otkriti destinaciju kojoj korisnik pristupa, ali može otkriti njegove obrasce ponašanja (misli se na korisnikov saobraćaj) u odlazu i dolazu. Profilisanje na osnovu korisničkih konekcija zahteva naknadnu obradu iz razloga

što se višestruke aplikacijske veze mogu odvijati istovremeno ili u serijama po istoj uspostavljenoj putanji.

- Nadgledanje korisničkog sadržaja

Obzirom da je celokupan sadržaj u okviru *Tor* mreže šifrovan, sadržaj između izlaznog čvora i destinacije nije. Iako filtriranje nije primarni cilj *Tor* mreže, *Tor* može direktno, koristeći *Privoxy* i slične filter usluge uklanjati protoke podataka određenih aplikacija.

- Opciona raznolikost

Pošto je korisnicima dopušteno da sami biraju konfiguracione portove, to može privući korisnike sa drugim potrebama, a klijenti koji su u manjini mogu izgubiti više na anonimnosti nego što bi dobili, u pokušaju da optimiziraju njihovo ponašanje na mreži.

- Vremenska povezanost „sa kraja na kraj“

Tor minimalno sakriva ovu korelaciju. Napadač koji vrši nadzor saobraćaja i utvrđuje pravila ponašanja može dovesti pošiljaoca i primaoca u vezu i to sa velikom verovatnoćom. Jedna od zaštita koja bi mogla da pomogne je podizanje „zaštitnog zida“, mada ni u tom slučaju zaštita ne bi bila potpuna.

- Korelacija „sa kraja na kraj“

Prosto brojanje paketa takođe može biti efektivno u potvrđivanju krajnjih tačaka konekcije. Ovaj problem donekle rešava topologija izbušene cevi iz razloga što različiti broj paketa može da uđe na jedan kraj a izađe na drugi.

- „Otisak“ Internet sajta

Svi prethodni napadi su bili zasnovani na potvrđivanju saobraćaja što ih izostavlja izvan ciljeva dizajna *Tor* mreže. Postoji i pasivan napad koji je poprilično efektan, a radi na principu skupljanja „otisaka“ sajtova koji sadrže veličinu fajla i načine na koji se pristupa. Svi ti podaci se snimaju u bazu koja se koristi za proveru korisnikove veze, koja se može iskoristiti propuštanjem sadržaja kroz bazu podataka. *Tor* delimično rešava ovaj problem, jer su različiti pravci multipleksirani kroz istu putanju, a i otisak je smanjen na veličinu ćelije. Dodatna odbrana bi mogla da uključi veću veličinu ćelije i pravljenje šema za grupisanje sajtova u veće setove.

5.6.2 Aktivni napadi

- Kompromitovani ključevi

Napadač koji sazna TLS sesijski ključ može da pristupi kontrolnoj ćeliji i šifrovanoj čvornoj ćeliji za bilo koju putanju te konekcije. Poznavanje ključa mu omogućava da odmotava sloj po sloj šifrata. Napadač koji sazna OR-ov i TLS privatni ključ može da se predstavlja kao OR sve dok vreme trajanja TLS ključa ne istekne. Da bi mogao da funkcioniše kao lažni OR, takođe mora da sazna i *onion* ključ kako bi dešifrovao ćelije, ali i pored toga ne može da „preotme“ uspostavljene veze a da ne iskompromituje postojeće sesijske ključeve. Periodična rotacija ključa ograničava šansu za ovakve napade. Sa druge strane napadač koji sazna čvorni ključ identiteta, može da zameni taj čvor trajno, slanjem lažnih deskriptera direktori serveru.

- Višestruki kompromis

Napadač koji luta u potrazi za metom može da ugrozi OR-e rušenjem konekcije pre nego što se ona uspostavi do kraja, tako što kompromituje čvorove. Da bi to postigao mora da završi svoj napad sve dok se ne završi vreme trajanja konekcije. OR-i se brane na taj način što odbacuju sve važne informacije pre završetka napada. Zahvaljujući PFS ključu sesije, napadač ne može da prisili čvorove da dešifruju snimljeni sadržaj kada je putanja već zatvorena. Dodatno je moguće napraviti zaglavlje koje može naterati OR-e da rade tako nešto i taj fenomen se zove „sudska arbitraža“. Kompanija *Java Anon Proxy* je bila suočena sa takvim zahtevom, jer ih je nemački sud naterao da naprave „mala vrata“ kako bi se omogućio ovakav pristup.

- „Pokreni“ korisnika

Ako napadač koristi mrežni server, veoma lako može doći do vremenskih obrazaca korisnika koji se kači na njega i tako postaviti proizvoljne obrasce kao njegove odgovore. Napad „sa kraja na kraj“ je još lakši. Ako napadač može da navede korisnika da se poveže na njegov mrežni server, dolazi u posed jednog kraja njihove konekcije. Takođe postoji i opasnost od aplikacijskih protokola pridruženih programa koji se mogu navesti da otkriju informacije o korisniku. *Tor* trenutno zavisi od *Privoxy* i sličnih protokola koji rešavaju ovaj drugi problem.

- „Pokreni“ OP

Očekuje se da krajnji korisnici većinom pokreću njihov lokalni OP. Međutim u nekim podešavanjima može biti neophodno da se njihov proksi pokrene daljinski. To je tipično za institucije koje žele da vrše nadzor onih koji se povezuju na proksi. Kompromitacijom OP-a, kompromituju se sve buduće veze kroz njega.

- DoS² nenadgledanih čvorova

Posmatrač koji može samo da prati deo *Tor* mreže, može da poveća obim saobraćaja koji prati, napadajući nenadgledane čvorove. Radnje koje primenjuje nad njima su: isključivanje čvora, smanjivanje njihove pouzdanosti i ubeđivanje korisnika da ti čvorovi nisu bezbedni. Najbolja odbrana od ovakvih napada je robusnost.

- Pokretanje neprijateljskog OR

Kao pokušaj da postane lokalni posmatrač, izolovan neprijateljski OR može da kreira putanju kroz sebe ili da izmeni sobračajne obrasce kako bi uticao na saobraćaj drugih čvorova. Pored toga, neprijateljski čvor mora biti susedni za obe krajnje tačke kako bi mogao da ugrozi anonimnost putanje. Ako napadač može da pokrene višestruke OR-ove i ubedi direktori servere da su ti OR-i pouzdani i nezavisni, vremenom će neki korisnici izabrati te OR-e i postaviti ih kao početne, susedne ili krajnje u putanji. Ako napadač kontroliše $m > 1$ od ukupno N čvorova, on može da ostvari uzajamnu vezu sa najviše $\left(\frac{m}{N}\right)^2$ od ukupnog saobraćaja [21]. Ovo pokazuje da napadač ipak može da privuče jako veliki broj konekcija koristeći OR-e sa popustljivim izlaznim pravilima, ili degradiranjem pouzdanosti ostalih rutera.

- Napad označavanjem

Neprijateljski čvor bi mogao „obeležiti“ čeliju menjajući je. Na primer, ako podatke predstavlja nešifrovan zahtev ka Internet sajtu, iskvareni saobraćaj koji dolazi spolja u odgovarajuće vreme bi mogao da potvrdi vezu između. Ipak, proveru integriteta poruke sprečava ovakav napad.

- Zamenjeni sadržaj kod neautentičnog protokola

Kada se preusmerava neautentičan protokol kao što je HTTP, neprijateljski izlazni čvor može da odglumi ciljanu adresu. Korisnici bi ipak trebalo da biraju protokole koji podržavaju autentifikaciju „sa kraja na kraj“.

- Ponovljeni napadi

Neki protokoli anonimnosti su ranjivi na ponovljene napade. *Tor* nije iz razloga što će odgovor na jedan deo uspostavljanja veze rezultovati drugim dogovorenim sesijskim ključem, tako da se ostatak snimljene sesije ne može upotrebiti.

² DoS – Denial of Service

- Napad na reputaciju

Napadač može da iskoristi *Tor* mrežu za nedozvoljene aktivnosti i tako ugrozi njenu reputaciju i natera operatere da je isključe. Izlazne polise donekle smanjuju mogućnosti ovakvog napada, ali mreža ipak zahteva pojedince koji mogu izdržati malo političkog pritiska.

- Distribuiranje neprijateljskog koda

Napadač može da prevari korisnike da pokrenu prepravljen *Tor* program koji u principu ne narušava anonimnost konekcije, već je u mogućnosti da prevari OR-e da pokrenu oslabljeni softver koji „potura“ korisnicima smanjujući im anonimnost. Ovaj problem je primećen ali ne i rešen. Jedini način zaštite je da ne veruju ni jednom softveru, pa čak ako dolazi i sa zvaničnog sajta, osim ako nije priložen i izvorni kod sa njim.

5.6.3 Direktori napadi

- Uništavanje direktori servera

Ako par direktori servera nestane, ostali će još uvek odlučivati koji direktori je validan. Čak i da ostane jako malo direktori servera, oni će još uvek emitovati njihovo sagledavanje mreže i generisati koncenusus direktorije. Ako dođe do gubitka više od polovine, ljudska intervencija će biti potrebna zato što neće biti dovoljno automatskih potpisa koji klijenti mogu da koriste i klijenti bi sami morali da odlučuju da li da veruju direktoriju ili ne.

- Preuzimanje direktori servera

Preuzimanjem direktori servera, napadač može samo delimično uticati na konačni direktori. Pošto se OR-i isključuju i uključuju glasom većine, preuzeti direktori može samo da prelomi u tom glasanju. Još uvek ostaje da se vidi koliko često se to dešava u praksi. Jedan od zabeleženih slučajeva se desio u septembru prošle godine, kada je američki FBI priznao da je preuzeo kontrolu nad *Tor* serverima, ali samo kako bi uhvatio osobu koja se bavila distribuiranjem dečije pornografije putem *Tor* mreže [22]. Ovakav postupak predstavlja takozvane legalne opasnosti o kojima je već bilo reči.

- Preuzimanje većine direktori servera

Napadač koji kontroliše više od polovine direktori servera može da uvrsti u konačni direktori onoliko OR-a koliko želi. Za ovaj problem kreatori *Tor* mreže se moraju pobrinuti da su direktori server operateri nezavisni i otporni na napade.

- Podsticanje direktori server neslaganja

Protokol za direktori dogovaranja pretpostavlja da su direktori server operateri saglasni sa setom direktori servera. Napadač koji uspe da ubedi neke direktori server operatere da ne veruju jedan drugom, može da ih podeli u međusobno neprijateljske grupe. *Tor* još uvek nije zabeležio ovakav napad.

- Prevariti direktori servere da nabroje neprijateljske OR-e.

Pretpostavlja se da je moguće isfiltrirati OR-e koji predstavljaju najveću pretnju.

- Ubediti direktori servere da je OR koji se nalazi u kvaru zapravo ispravan

U trenutnoj verziji *Tor*-a, direktori serveri pretpostavljaju da OR radi ispravno ako može da uspostavi TLS konekciju. Neprijateljski OR može lako da ga prevari tako što će uspostaviti konekciju, ali će ignorisati ćelije. Direktori serveri moraju stalno testirati OR-e, praveći putanje i saobraćaj kroz njih.

5.6.4 Napadi na tačke sastanka

- Napraviti mnogo zahteva za upoznavanje

Napadač bi mogao da pokuša da sruši Bobovu uslugu zatrpavajući je zahtevima za tačkom upoznavanja. Način zaštite bi bio da Bob ograniči količinu zahteva koju može da primi, odnosno da zahteva određeni proračun za svaki zahtev koji primi.

- Napad na tačku upoznavanja

Napadač može da pokuša da poništi lokaciju skrivene usluge onemogućavanjem tačke upoznavanja. Međutim pošto je identitet usluge prikačen uz njen javni ključ ona prosto može da se ponovo izreklamira i promeni tačku upoznavanja. Ovo prisiljava napadača da mora da onemogućí sve moguće tačke za upoznavanje.

- Kompromitovanje tačke upoznavanja

Napadač koji kontroliše Bobovu tačku upoznavanja može da preplavi Boba sa zahtevima za upoznavanje, ili da spreči važeće zahteve da dođu do njega. Bob može da primeti prekomerni broj zahteva i zatvori putanju, ali da bi primetio da važeći zahtevi ne dolaze do njega mora periodično da šalje test poruku za sastanak koja mora da mu se vrati.

- Kompromitovanje tačke sastanka

Tačka sastanka nije ništa manje osetljivija od bilo kog OR-a na putanji. Pošto svi podaci prolaze kroz tačku sastanka, oni su šifrovani sa sesijskim ključem koji dele Alisa i Bob.

6. Zaključak

Kroz ovaj rad je moglo da se vidi koliko je anonimnost na Internetu stvarno ugrožena. Napadači na korisničke identite ne moraju biti dobro opremljene organizacije koje raspolažu ogromnim ljudstvom i resursima, već to mogu biti pojedinci koji uz poznavanje načina rada računarskih mreža i određenih softverskih alata vrlo lako mogu saznati željene informacije. Pokazano je da je anonimnost na Internetu nevažna čak i za one kompanije koje to isto garantuju svojim korisnicima, a sve zbog finansijske koristi koju dobijaju izdavanjem svog reklamnog prostora.

Termin potpune anonimnosti prilikom korišćenja Internet mreže se mora shvatiti samo kao pojam koji je skoro nemoguće ostvariti u praksi. Zaključak koji pojedini korisnici mogu izvesti jeste da je zaštita nemoguća i odustati od bilo kakvih sigurnosnih mera i tako još više ugroziti svoju anonimnost. To naravno ne bi bio pravilan zaključak jer iako je totalna zaštita anonimnosti na Internetu nemoguća, primena bilo koje metode za zaštitu anonimnosti, preduzimanjem određenih sigurnosnih mera ipak onemogućava ili barem otežava delovanje napadača.

Proučavanjem načina rada *Tor* mreže došlo se do zaključka, da iako nije savršeno, *Tor* rešenje ipak predstavlja viši nivo zaštite privatnosti. Korišćenje ponuđenih aplikacija će sasvim sigurno učiniti korisnika nedostupnim za klasične napade na našu anonimnost ili će barem otežati neke ozbiljnije ciljane napade. Zaključeno je da ovaj projekat sadrži još uvek i dosta nedostataka, od kojih će neki verorovatno biti rešeni u skorije vreme, ali isto tako je sigurno, da je čak i *Tor* mreža neotporna na određene napade. Nedostaci, kao što su uplitanje zakonskih regulativa, koje nameću ubacivanje rešenja za namerno ugrožavanje anonimnosti, predstavljaju jedinu stvarnu opasnost koju dizajneri *Tor* mreže ne mogu da prevaziđu.

Zanimljive aplikacije kao što su *Tails* i *Orbot* predstavljaju jedan novi koncept za obične korisnike. Korišćenjem *Tails* aplikacije sasvim lako se može od običnog korisnika napraviti osoba koja koristeći tuđe računare lako i neprimećeno pristupa Internet mreži neostavljajući nikakve tragove. *Orbot* aplikacija će sasvim pomoći u bezbednijem krstarenju po Internet mreži korišćenjem mobilnih uređaja sa android operativnom platformom, a takođe će onemogućiti sve veći broj instaliranih aplikacija da samostalno šalju razne informacije o korisniku.

Iako se tvrdi da je projekat zasnovan na volonterskoj bazi, sredstva, aplikacije i pre svega koncept mreže daje naznake da iza toga može da stoji neka organizacija koja takav projekat održava u životu. Ukoliko se u budućnosti ova tvrdnja ispostavi tačnom, celokupan koncept zaštite anonimnosti korišćenjem *Tor* mreže bi se mogao dovesti u pitanje. Razlog za to bi bila sumnja u onoga ko je zadužen za održavanje takvog sistema.

Rezime celokupnog rada bi bio da je korišćenje bilo kakvog sistema koji može barem i u određenoj meri zaštititi korisničku anonimnost bolje, nego biti potpuno nezaštićeni. Primena aplikacija, koje nudi *Tor* projekat, može savim dobro kamuflirati korisnički računar u trenutnoj Internet „prašumi“ i tako ga zaštititi barem od najmasovnijih napada na računare koji se trenutno sprovode.

Literatura

- [1] Veinović, M, Jevremović, A., **Računarske Mreže**, prvo izdanje, Univerzitet Singidunum, Beograd, 2011.
- [2] McClure, S., Scabray, J., Kurtz, G. **Hakerske Tajne**, prevod petog izdanja, Mikro knjiga, Beograd, 2006.
- [3] Bezbedno korišćenje Interneta, Pravo na privatnost, dostupno na: <https://www.privacyrights.org/online-privacy-using-internet-safely#cookies> , [pregledano 25.02.2014]
- [4] Fleš kolačići, Zdnet, dostupno na: <http://www.zdnet.com/blog/btl/ad-network-at-center-of-third-flash-cookie-lawsuit/38346> [pregledano 25.02.2014]
- [5] Prepoznavanje lica, eWeek, dostupno na: <http://www.eweek.com/c/a/Security/Facial-Recognition-Tools-Facebook-Photos-Threaten-End-to-Anonymity-Study-565285/> [pregledano 25.02.2014]
- [6] Pretraživači, Pravo na privatnost, dostupno na: <https://www.privacyrights.org/online-privacy-using-internet-safely#engine>, [pregledano 26.02.2014]
- [7] Trajni kolačići, Samy, dostupno na: <http://samy.pl/evercookie/> , [pregledano 26.02.2014]
- [8] Upotreba socijalnih mreža, Statistic Brain, dostupno na: <http://www.statisticbrain.com/social-networking-statistics/> , [pregledano 03.03.2014]
- [9] Nadzor Interneta od strane NSA, B92, dostupno na: http://www.b92.net/info/vesti/index.php?yyyy=2013&mm=08&dd=21&nav_id=744792 , [pregledano 03.03.2014]
- [10] Nadzor Interneta od države Francuske, Poslovni, dostupno na: <http://www.poslovni.hr/tehnologija/francuska-jaca-nadzor-interneta-259123> , [pregledano 04.03.2014]
- [11] Nadzor Interneta od države Turske, Aljazeera, dostupno na: <http://balkans.aljazeera.net/vijesti/parlament-turske-izglasao-nadzor-interneta> , [pregledano 04.03.2014]
- [12] Maliciozni softver, Microsoft, dostupno na: <http://www.microsoft.com/security/pc-security/virus-what-is.aspx> , [pregledano 04.03.2014]
- [13] Worms, How stuff works, dostupno na: <http://computer.howstuffworks.com/virus5.htm> , [pregledano 04.03.2014]
- [14] Spajver, Mikrosoft, dostupno na: <http://www.microsoft.com/security/pc-security/spyware-what-is.aspx> , [pregledano 05.03.2014]
- [15] Veb bube, EFF, dostupno na: https://w2.eff.org/Privacy/Marketing/web_bug.html, [pregledano 05.03.2014]
- [16] Usluge praćenja, Fedex, dostupno na: https://www.fedex.com/fedextrack/?action=track&cntry_code=us ,

[pregledano 06.03.2014]

- [17] Fišing, Mikrosoft, dostupno na: <http://www.microsoft.com/security/online-privacy/phishing-symptoms.aspx>, [pregledano 08.03.2014]
- [18] Spijunski programi u Srbiji, Svet, dostupno na <http://www.svet.rs/hronika/otkrivamo-gradane-srbije-spijunira-firma-iz-surdulice> , [pregledano 18.03.2014]
- [19] Krishnamurthy B., Willis E. C., *On the Leakage of Personally Identifiable Information Via Online Social Networks*, SIGCOMM 2009 worshoop, 21-17. Avgust 2009. godine, Barselona, dostupno na: <http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf>, [pregledano 28.02.2014]
- [20] O Tor-u, Tor projekat, dostupno na <https://www.torproject.org/about/overview.html.en>, [pregledano 04.04.2014]
- [21] Dingledine R., Mathewson N., Syverson P., „Tor Second-Generation Onion Router“, dostupno na, <https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf>, [pregledano 27.03.2014]
- [22] Preuzimanje Tor server, Darkreading, dostupno na: <http://www.darkreading.com/risk-management/fbi-admits-to-tor-server-takeover/d/d-id/1111553>, [pregledano 15.04.2014]