Sinteza
Međunarodna naučna konferencija Univerziteta Singidunum

Impact of Internet on Business Activities in Serbia and Worldwide
Uticaj Interneta na poslovanje u Srbiji i svetu

DOI: 10.15308/SINTEZA-2014-203-208

ZAŠTITA IDENTITETA NA INTERNETU KORIŠĆENJEM ANONIMNIH MREŽA

Nada Staletić
Visoka škola elektrotehnike i računarstva strukovnih studija, Beograd

Abstract:
Interesovanje za temu zaštita identiteta na Internetu stalno dobija na značaju, sa progresivnim rastom digitalne komunikacije i primene Interneta kao informacione i komunikacione tehnologije u modernom dobu, sve većom cenzurom koju primenjuju bezbednosne agencije vlada savremenih država, ISP kompanije (kroz zakonsku obavezu o zadržavanju podataka o aktivnostima korisnika), kompanije radi industrijske špijunaže i marketing kompanije radi utvrđivanja ciljnog tržišta. Ovde spadaju i brojne druge organizacije i pojedinci koji motivisani različitim interesima tragaju za informacijama koje u suštini zadiru u privatnost pojedinaca ili kompanija.
U radu se analizira zaštita identiteta na internetu korišćenjem anonimnih mreža. Pod anonimnim mrežama podrazumevaju se pristupi globalnoj mreži korišćenjem VPN (Virtual Private network), web proxy i anonimnih mreža. Fokus analize je na topografiji i sigurnosti u zaštititi identiteta koju pruža Tor anonimna mreža.

Key words:
anonimne mreže,
Tor,
web proxy,
zaštita indentiteta na internetu,
internet cenzura,

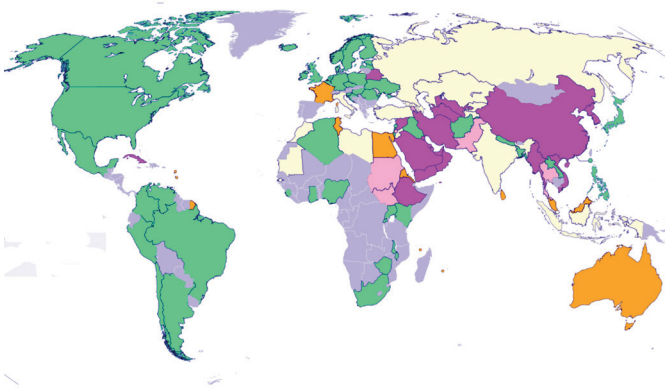
UVOD

Internet je najveće javno dobro koje je krajem dvadesetog veka osmislio čovek. U međuvremenu, Internet kao informaciona i komunikaciona tehnologija poprimio je tako široku primenu da se moderan svet komunikacija bez njega ne može zamisliti. Internet se koristi u poslovanju, obrazovanju, kao globalni medij, kao nepregledna arhiva podataka u digitalnoj formi, kao kanal komunikacije između ljudi iz udaljenih svetskih regiona koji se možda nikad neće sresti, kao kanal promocije i izvor marketing istraživanja, mesto za razonodu i dr. Upravo zbog tako široke primene i obima informacija od različitog značaja koje se prenose putem Interneta, pitanje zaštite identiteta korisnika na Internetu postaje aktuelno i značajno, jer postoji potreba da se uđe u trag našeg digitalnog otiska (računar; IP adresa; elektronska pošta; nalog u banci; nalog na društvenoj mreži; Voip komunikacija; Internet destinacije koje najčešće posećujemo; jednom rečju, koje su naše navike i kakva su ponašanja u odnosu na izazove na Internetu. Uspeh u našem vremenu presudno zavisi od blagovremene i tačne informacije. U poslovnom svetu prevladava načelo: ko prvi stigne do informacije, on je pobednik.

Boravak na Internetu danas, bez odgovarajuće zaštite, u trajanju od jednog minuta ili od jednog dana, isti je rizik za neopreznog pojedinca ili za njegovu organizaciju. Gubitak kontrole nad računarom, gubitak parametara za autentifkaciju u elektronskoj korespodenciji, na društvenim mrežama ili u elektronskom bankarstvu, instant messagining servisima i dr, to je nešto što se neprekidno događa, pri čemu korisnici često sa zakašnjenjem postaju svesni posledica.

Krajem 2013. godine nacionalne bezbednosne službe SAD procenile su da najveći neprijatelj države nisu neprijateljski režimi (poput Irana, Severne Koreje i Sirije), niti militantne islamske grupe, a ni Rusija, kao nuklearna supersila.

Globalni pogled na Internet cenzuru prikazan je na Sl. 1. Legenda: zelena: minimalna cenzura. Siva: nedostupni podaci; ružičasta: veliki deo saobraćaja potpuno je blokiran u više kategorija; svetlo ružičasta: veliki deo saobraćaja blokiran je u različitim kategorijama, a ostalo se cenzuriše; žuta boja: mali deo Internet sadržaja je podložan cenzuri ili je potpuno blokiran.



Sl. 1. *Globalni pogled na cenzuru Interneta u 2013. godini* [1]

Iz napred navedenih razloga, savremene države ubrzano menjaju zakonodavstvo i proširuju nadležnosti bezbednosnih agencija, stavljajući, faktički, pod kontrolu (cenzuru) sadržaje koji se ostvaruju putem elektronske komunikacije. Posle dva teroristička napada u Madridu (2006), Evropska Unija donela je 2006. godine Direktivu 2006/24EC o obaveznom zadržavanju podataka učesnika u elektronskoj komunikaciji (od strane ISP i operatera mobilne i fiksne telefonije. Zemljama članicama ostavljeno je da same odrede vreme zadržavanja informacija o aktivnostima korisnika (u periodu od 6 – 24 meseci) [2]. Srbija je 2010. godine donela Zakon o elektronskim komunikacijama, koji obavezuje kompanije registrovane za pružanje usluga Interneta, mobilne i fiksne telefonije da zadržavaju podatke korisnika (meta podaci), koji obuhvataju IP adresu korisnika, adresu i sadržaj e-pošte u odlaznom i dolaznom saobraćaju i druge aktivnosti na osnovu kojih se može napraviti analiza saobraćaja korisnika (čak i kad su sadržaji šifrovani), iz koje se sa velikom preciznošću može sačiniti analiza web lokacija koje često posećuje, odnosno na osnovu koje može da se uradi *lični profil* pojedinca na Internetu.

Osim vladinih bezbednosnih agencija, razne privatne organizacije zainteresovane su za otkrivanje identiteta korisnika na Internetu. Razlozi su različiti: neovlašćeno dolaženje do tehnoloških inovacija, zatim sakupljanje informacija o poslovanju i strateškim planovima konkurentskih kompanija, kao i o njihovim problemima. Ovoj grupi organizacija pripadaju, između ostalog, marketinške agencije, koje putem Interneta i drugih formi dvosmerne elektronske komunikacije sprovode istraživanje radi definisanja ciljnog tržišta (*tržišta potrošača*) kompanija sa kojima posluju, ostvarujući ciljeve narušavanjem digitalnog otiska pojedinca ili organizacije na Internetu (ubacivanjem virusa trojanca, *spyware,* u računare ciljanih korisnika; preuzimanjem dns keša iz tuđih računara, radi analize najčešće posećivanih web lokacija i dr).

Stalne inovacije u oblasti Internet tehnologija imaju svoje dobre i loše strane. Migracija sa IPv4 na IPv6 protokol omogućila je proširenje adresnog resursa na globalnoj mreži dvanaest puta. Međutim, IPv6 protokol omogućio je daleko kvalitetniji nadzor aktivnosti pojedinca na Internetu, pošto je on sakriven iza statične IP adrese, koja se daleko lakše cenzuriše i nadzire od dinamičke adrese.

Cloud Computing tehnologija, koja podrazumeva migraciju aplikacija i drugih digitalnih sadržaja iz naših računara na Internet, skopčana je sa transferom osetljivih podataka putem VPN mreže, ali i tu postoji rizik od presretanja i hakovanja podataka i potencijalno velike štete koju pojedinac ili organizacija može da ima. Tokom 2013. godine publikovani su radovi koji pokazuju da se infiltriranjem virusa može steći kontrola nad VPN mrežom. Očekuje se da će tokom 2014. godine oko 70% kompanija svoje elektronsko poslovanje postaviti na Cloud.

Naposletku, zbog visoke cene informacija danas, Internet servis provajderi, koji su u obavezi da zadržavaju podatke o aktivnostima korisnika na Internetu, mogu da se pojave kao neovlašćeni prodavci informacija o našim digitalnim identitetima. Teško je ustanoviti kontrolu upotrebe zadržanih informacija, a filtriranje zadržanih informacija prema zadatom ključu je moguće. Osim toga, takvu aktivnost koja duboko zadire u privatnost pojedinca, teško je dokazati.

Da bi zaštitili digitalni otisak na Internetu, korisnici preduzimaju različite mere, kao što su: brisanje dns keša u računarima povezanim na Internet; pristup Internet servisima preko virtuelnih privatnih mreža (VPN); pristup web lokacijama putem web proksi servisa i pristup Internetu preko anonimnih mreža.

Virtuelne privatne mreže su softverski definisane mreže koje se oslanjaju na Internet infrastrukturu. Na postojeći Internet protokol (npr. TCP) nadgrađuje se protokol VPN kao novi transportni sloj. Privatne mreže služe za zaštitu podataka i zaštitu privatnosti korisnika na Internetu. Sastoje se iz računara klijenata sa stalnim ili povremenim pristupom i računara servera, postavljenih na određenim čvorištima. Podržavaju SSL i TLS enkripciju. SSL enkripcija štiti podatke tokom njihovog tranzita od klijenta ka serveru. Ova enkripcija predstavlja zaštitni tunel za podatke tokom komunikacije između klijenta i servera. VPN mrežama kompanije se povezuju u jedinstvenu računarsku mrežu, odnosno organizacione jedinice koje se nalaze van njenog sedišta (IT centra). Za povezivanje na VPN mrežu potreban je odgovarajući klijentski softver i odobrenje za pristup mreži, koje se dobija sa parametrima za autentifikaciju.

Korisnicima Interneta stoje na raspolaganju besplatne i komercijalne virtuelne privatne mreže, radi obavljanja poslova sa visokim stepenom zaštite podataka na Internetu. Banke i druge organizacije oslanjaju se na SSL protokol i enkripciju u poslovima transfera novca, kao i drugih poverljivih podataka preko Interneta. Povezivanje i tok sesije na Cloud Computing servisu zasnovan je VPN mreži i SSL enkripciji u transferu podataka u oba smera.

Web proxy servis je jedan od načina zaštite identiteta na Internetu koji se široko primenjuje. Pomoću web proksija moguće je sakriti IP adresu pojedinca, međutim ostali podaci koji se šalju preko otvorenog http protokola, kao što su zaglavlja i sadržaji elektronske pošte i adrese posećenih web lokacija, ostaju otvorene za presretanje. Sigurnost zaštite identiteta korišćenjem proksi servisa povećava se kada je tok konekcije od korisnika do ciljanog servera pod SSL ili TLS protokolom.

Web proksi servis zasniva se na preusmerenju Internet saobraćaja korisnika preko računara u javnoj kompjuterskoj mreži koji ima statičnu IP adresu. Web proksi server je poslužilac koji propušta internet saobraćaj korisnika preko svoje IP adrese i preko odgovarajućeg porta računara poslužioca (npr: 3128). Web proxy server je deo uobičajene lokalne računarske mreže kompanije koja je povezana na Internet, s tim što se putem ovog servera vrši filtriranje izlaznog saobraćaja. Ograničenja se mogu postaviti u odnosu na portove (obično je dozvoljen port 8080 za pristup web servisu i servisu elektronske pošte na rezervisanom portu 21 korisnicima u lokalnoj računarskoj mreži. Web proksi server može se koristiti i za pristup određenim web lokacijama koje su politikom kompanije zabranjene. Tako, na primer, brojne kompanije zabranjuju pristup društvenim mrežama zaposlenima.

Korisnicima je na Internetu na raspolaganju veliki broj besplatnih web proksi servisa. Korišćenjem web proxy servisa može se sakriti digitalni otisak na webu. IP adresa korisnika čiji je Internet saobraćaj preusmeren preko odgovarajućeg proksi servera transformiše se i vidljiva je na odredišnom web serveru kao adresa web proksi servisa. Pristup Internetu preko web proxy servisa ima više nedostataka. Ako je proxy server postavljen na Internet čvorištu sa skromnim propusnim opsegom (Bandwidth), korisnici će to osetiti po sporom učitavanju sadržaja, odnosno po sporom Internetu. Isto se događa u vremenu većeg opterećenja proksi servisa, a to je onaj deo dana kada servis koristi najviše korisnika (obično se radi o ranim večernjim satima), zbog povećanog internet saobraćaja koji proksi server treba da propusti kroz odgovarajući port. Slaba strana je i to što korisnici ne znaju s kojim ciljem je formiran slobodan web proxy i da li se informacije o korisnicima (čije su IP adrese vidljive na tom serveru) zadržavaju i kasnije neovlašćeno koriste. Ovde je reč o poverenju korisnika u administratore i vlasnike web proxy servisa. Web proxy je jedno od rešenja u situaciji kad je nivou država zabranila vidljivost određenog sajta. Način da se zaobiđe cenzura i da se koristi uspešno određena web destinacija jeste preusmerenje web saobraćaja na web proksi server koji se nalazi u zemlji u kojoj je ta lokacija dozvoljena. Na taj način korisnici vrše neku vrstu *bajpasa* i bez problema pristupaju zabranjenom sajtu. Turska je dvadesetog marta 2014. godine zabranila pristup *Twitter* društvenoj mreži preko svih ISP u zemlji. Međutim, već 21. marta aktivnost Twitter korisnika iz te zemlje dostigao je apsolutni maksimum. Ovo pokazuje da pojedini oblici cenzure u sve više povezanom svetu ne mogu da donesu velike efekte.

Za konekciju na web proksi servis nije potreban dodatni softver i hardver. Dovoljan je računar povezan na Internet i pregledač weba (*browser*). Na Internetu treba pronaći slobodan (besplatan) web proksi [3]. Pri odabiru, zemlja u kojoj se server fizički nalazi je vrlo značajna, kako zbog oblika i dubine cenzure koja se primenjuje prema korisnicima Interneta, tako i zbog širine propusnog opsega. Važna su dva podatka za preusmerenje Internet saobraćaja na izabrani proksi server: IP adresa i port preko kojega se vrši preusmerenje. U pregledaču weba (npr. *Google Chrome*), pokrenuti podešavanja. Izabrati vezu: Napredna podešavanja. U sekciji: Mreža, izabrati: Promeni podešavanja proksija… U dijaloškom okviru Internet – Svojstva na inicijalnoj kartici Veze izabrati sekciju: Postavljanje LAN-a, čekirati: Koristiti proksi server za LAN. Upisati IP adresu u polje levo. U polje, desno, upisati port proksi servera. Za kraj, izabrati dugme: U redu.

NASTANAK I RAZVOJ TOR MREŽE

Tor je softverski definisana mreža virtuelnih tunela, dizajnirana da sačuva identitet, lokaciju osobe i aktivnost na Internetu. Mreža omogućava programerima da kreiraju nove komunikacione alate sa ugrađenim funkcijama za privatnost (slobodni kod). Tor pruža osnove za niz aplikacija koje omogućavaju organizacijama i pojedincima da dele informacije preko Interneta, bez ugrožavanja njihove privatnosti. Bazira se na slobodnom softveru i podrški, koji projektu daju vlade, organizacije i pojedinci, udruženi u naporu za slobodan pristup Internet servisima, bez cenzure i analize saobraćaja korisnika [4].

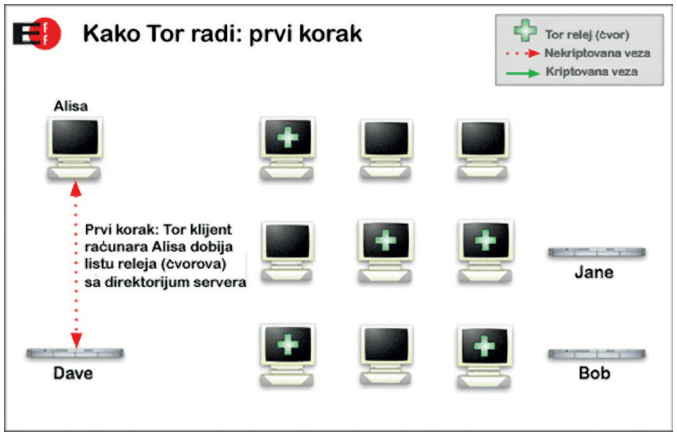
Naziv Tor nastao je kao akronim od *The Onion Router*. Rodžer Dingledine, Nik Mathevson, i Paul Siverson su dizajneri anonimne mreže (2002). Od 2006. godine Tor projekt ima široku bazu finansijske podrške: Američko ministarstvo spoljnih poslova (60%), Nacionalna fondacija za nauku, Google, Švedska vlada i hiljade drugih sponzora, uključujući i hiljade organizacija i pojedinaca širom sveta. Na službenoj web lokaciji Tor projekta, omogućena je donacija putem elektronske uplate u dolarima (najmanji iznos je 5 dolara) i bitkoinima, kao i donacija u vidu aktivnog pristupa Tor projektu doniranjem računara stalno povezanog na Internet kao releja, odnosno servera, sa najmanjim ustupljenim propusnim opsegom od 50 kb/sec. Godišnji budžet neprofitne organizacije Tor iznosi 2 miliona američkih dolara [5].

Interesovanje za pristup Tor anonimnoj mreži u svetu naglo raste posle saznanja da se Internet komunikacije i servisi cenzurišu na globalnom i nacionalnom nivou (2013) i da će u budućnosti zadržavanje meta podataka i drugi oblici cenzure biti deo svakodnevice. Tor je zbog svog izuzetnog dizajna i sigurnosti ubrzo dobio reputaciju najbezbednije besplatne anonimne mreže na Internetu.

Na službenoj web lokaciji projekta – www.torproject.org korisnici mogu besplatno preuzeti informacije o istoriji mreže, izvorima finansiranja, preuzimanju i optimizaciji softvera na klijentskoj i relej (serverskoj) strani. Korisnicima su na raspolaganju softverski proizvodi treće generacije: Tor Browser Bundle (verzija: 3.5.2), koji sadrži unapređenu verziju Firefox pregledača weba, dizajniranog za pristup Tor anonimnoj mreži (za operativne sisteme: Windows (XP, Vista, 7 i 8), 32-bit i 64-bit, OSX (Leopard i Lion), Android i Unix. Tor Browser Bundle je inicijalno konfigurisan da zaštiti privatnost i anonimnost korisnika na Internetu. Korisnicima je na raspolaganju imidž (.iso) datoteka pod nazivom Tails, za izradu butabilnog diska (kompakt disk ili na fleš memorijsku jedinicu), sa operativnim sistemom Linux i Tor aplikacijama. Konačno, Tor Cloud aplikacija (most) za besplatne i komercijalne korisnike registrovane na Amazon Cloud.

Topografija mreže: Mrežu čine dve vrste računara: klijenti, koji imaju stalni ili povremeni pristup mreži i računari releji, serveri ili čvorišta u anonimnoj mreži. Pored direktorijum servera, koji sadrži javne IP adrese aktivnih releja na Mreži, postoje tri vrste releja (servera). Ulazni releji (serveri), releji (serveri) koji služe kao mostovi i izlazni releji (serveri). Status releja stalno se menja i određen je luk rutiranjem (*onion routing*), koje se inicira na klijentskoj strani. Računari u mreži povezani su TCP mrežnim protokolom, na kojem je implementiran transportni sloj, Tor protokol, što zajedno uspostavlja stabilnu anonimnu mrežu.

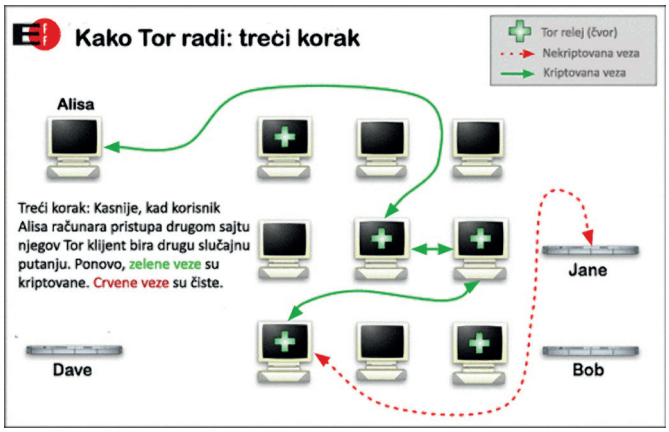
Kad klijent računara Alisa pokrene Tor aplikaciju, dobija izmenjenu (netačnu; lažnu) IP adresu, prema kojoj je vidljiv na Internetu. Unošenjem ciljne web adrese u Tor pregledač weba, inicijalno se šalje zahtev za pribavljanje liste aktivnih Tor releja (servera) direktorijumu servera (host pod nazivom Dave, Sl. 2).



Sl 2. Računar Alisa dobavlja listu releja sa direktorijuma servera

Direktorijum servera u svakom trenutku ima podatke o aktivnim relejima na Tor mreži (IP adrese).

U drugom koraku računar klijenta (Alisa) metodom slučajnog izbora određuje putanju kojom će se kretati podaci, koji prolaze kroz tri Tor releja. Na svakom releju vrši se dekripcija i enkripcija podataka o klijentu i sadržaj koji se transportuje. Enkripcijom i dekripcijom podataka upravlja Tor aplikacija klijenta. Drugi korak prikazan je na Sl. 3.

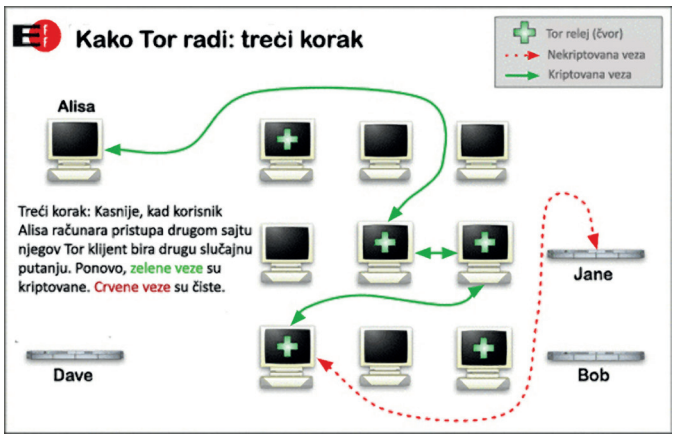


Sl. 3. Računar Alisa pravi kolo od tri slučajna releja i šalje sadržaj (zahtev) na server Bob, koji se nalazi na javnoj mreži

U trećem koraku, na izlaznom releju vrši se dekodiranje sadržaja zahteva klijenta i upućuje direktorijum serveru domena na globalnoj mreži, za povezivanje sa web sajtom. Veb server isporučuje odgovor na zahtev izdavanjem http specifikacije, koji ponovo prolazi isti enkriptovani put preko istog kola releja Tor mreže, do računara klijenta Sl. 4.

Posle nekog vremena, klijent računara Alisa napušta početnu web destinaciju i url-uje drugu web adresu. Rutiranje se sada obavlja preko drugih aktivnih releja, tako što se određuje nova slučajna putanja preko tri Tor releja prema ciljanom web serveru. Tok konekcije prikazan je na Sl. 4.

Tor klijent aplikacija postepeno gradi kolo šifrovanih veza preko releja na mreži. Svaki relej (u izabranom kolu koji pravi tunel) znâ samo koji je relej dao podatke i kome releju treba isporučiti podatke. Nijedan pojedinačni relej nikada ne zna kompletan put koji paket podataka prolazi. Klijent ugovara poseban set ključeva za šifrovanje za svaki prolaz duž kola releja kako bi se osiguralo da svaki prolazni relej ne može da prati ove veze (luk rutiranje).



Sl 4. Računar Alisa gradi konekciju preko izlaznog releja otvorenim protokolom sa web serverom računara Jane

Računa se da Tor anonimna mreža danas broji šest hiljada releja, koji stoje na raspolaganju klijentima. Sa tako velikim brojem releja, smanjuje se rizik od uspostavljanja potpune ili delimične kontrole nad mrežom. Najbezbedniji način pristupa web servisu podrazumeva da su ciljane web lokacije pod https protokolom.

U Tor pregledaču weba iz bezbednosnih razloga inicijalno je isključeno preuzimanje i obrada datoteka u javi, .avi, .mov, .flv formatima i, uopšte, multimedija koja se preuzima preko youtube-a ili obrađuje preko media player-a.Takođe, preko Tor mreže ne može se pristupiti torentima (P2P sharing), radi preuzimanja digitalnog sadržaja koji uglavnom podleže zaštiti autorskih prava [6]. Transfer datoteka Bitorrent protokolom je transparentan i može se pratiti. Osim toga, u toku transfera, menjaju se portovi kroz koji prolazi sadržaj, što Tor protokoli, isto kao i protokoli VPN mreža, ne podržavaju.

Pored web servisa, preko Tor anonimne mreže pristupa se SSH protokolima za prenos datoteka, putem posebne aplikacije koja se nalazi u paketu klijentskog softvera, kao i aplikacija za slanje kratkih tekstualnih poruka (Instant Messaging), sa korisnicima koji su povezani na Tor u realnom vremenu ili sa pojedincima koji su putem odgovarajućih klijenata povezani na globalnu mrežu. Elektronska pošta ažurira se, takođe, preko Tor mreže.

Skrivene usluge Tor mreže (Hidden Services) omogućavaju pojedincima da postavljaju web sajtove, e-prodavnice, blogove i druge sadržaje, koji nisu vidljivi sa globalne kompjuterske mreže i koje ne može da identifikuje i indeksira Google. Ovaj deo Tora službeno se naziva „dubinski web“. Neki autori zbog prirode sadržaja koji je tamo postavljen, koriste naziv „dark web“.

Krstarenje webom preko Tora skopčano je sa sporim učitavanjem sadržaja. Kašnjenje je uslovljeno kodiranjem i dekodiranjem sadržaja na svakom od releja u kolu u odlaznom i dolaznom saobraćaju. Dodatni problem čini širina propusnog opsega (Bandwidth), koja je limitirana na gornjoj granici od 239 kb/sec.

Korisnici mreže: Tor mrežu čine pojedinci koji su iz različitih razloga motivisani da stalno ili povremeno obav-

ljaju aktivnosti na Internetu, pristupajući preko Tora. Kao anonimna mreža, Tor nudi brojne pogodnosti, zbog čega pojedinci koriste mrežu. Pristup Internetu, posebno web servisu, putem Tor mreže oslobađa nas brojnih uobičajenih rizika i briga. Obzirom da je naša IP adresa, kao digitalni otisak, sakrivena ili netačno prikazana na globalnoj mreži, softver koji se povlači sa web sajtova, kao što su različite vrste virusa trojanaca, ne može da ostvari cilj. Takođe, brojni *kolačići* koje web strane ostavljaju u računare korisnika jesu neupotrebljivi, jer ne mogu do njega da stignu. Pojedinac je lišen rizika svih tih svakodnevnih pošasti koje dolaze kao nenajavljeni i vrlo neprijatni gosti u računar preko Interneta.

Pojedinci koriste Tor da bi sačuvali sebe i svoje porodice od praćenja od strane raznih veb sajtova, ili da se povežu sa izvorima informacija, servisima za razmenu brzih poruka i slično, kada su takve servise blokirali pojedini davaoci Internet usluga (bajpas cenzura). U poslednje vreme države preuzimaju sve veću kontrolu nad Internetom. Zabranjeni web sajtovi koji su vidljivi na globalnoj mreži, vidljivi su i na Toru. Pojedinci takođe koriste Tor za komunikaciju o društveno-osetljivim pitanjima: sobe za ćaskanje i veb forumi za zlostavljane ili bolesne osobe, na primer. Novinari koriste Tor za bezbedniju komunikaciju sa uzbunjivačima i disidentima. Nevladine organizacije koriste Tor da bi omogućile svojim radnicima da kontaktiraju svoje matične sajtove dok su u inostranstvu, bez obaveštavanja svih oko sebe da sarađuju sa tom organizacijom. Mreža je u javnosti postala poznata u vreme socijalnih promena u nekim severnoafričkim zemljama, koja su poznata pod nazivom "Afričko proleće". Kasnije se pokazalo da su organizatori građanskih protesta bili povezani i međusobno su komunicirali vrlo uspešno skrivajući digitalni identitet, korišćenjem Tora.

Na Tor mreži istovremeno su aktivni dobri i loši momci. Loši momci koriste anonimnu mrežu da bi se bavili aktivnostima koje su u sukobu sa moralom i zakonom, kao što su različite prevare, prodaja droge i oružja, distribucija pornografskog sadržaja i druge aktivnosti koje spadaju u cyber criminal.

Pojedine provajderske kuće, prilikom prijave pojedinaca na Tor mrežu, prepoznaju anonimnost korisnika i automatski prekidaju pristup Internetu. Najveći broj ISP u svetu dozvoljava anonimni pristup putem Tor mreže. Većina ISP u Srbiji dozvoljava pristup globalnoj mreži preko Tora. Sa gledišta legaliteta, Tor mreža je dozvoljena u većini država savremenog sveta. U Sjedinjenim Američkim Državama, gde je sedište Tor projekta, ne postoje propisi koji ograničavaju upotrebu Tora [7].

Tor mreža je pouzdana i besplatna za korisnike koji globalnoj mreži pristupaju sa najpopularnijih operativnih sistema. Posle objavljivanja informacije da su sve elektronske komunikacije u svetu pod nadzorom američke agencije za bezbednost (u avgustu 2013. godine), broj korisnika naglo je porastao. Tor mreža krajem 2013. godine broji šest miliona korisnika.

U Tabeli 1 [8] prikazan je dnevni prosek korišćenja Tor mreže prema nacionalnom ključu. Kina se ne nalazi na listi, jer je u toj zemlji preko ISP zabranjeno korišćenje Tor mreže.

Tabela 1. Deset zemalja čiji korisnici najviše koriste Tor (dnevni prosek)

Država	*udeo korisnika (%)*
Sjedinjene Američke Države	10,69
Iran	9,12
Holandija	6,84
Indija	4,79
Italija	3,13
Rusija	3.03
Francuska	2,71
Kanada	2,53
Nemačka	2,11

SIGURNOST TOR MREŽE

U svetu IT tehnologija, predvođenih Internetom, u kojem inovacije sustižu jedna drugu, pitanje potpune sigurnosti pojedinaca na Internetu je diskutabilno. Ako SAD, koje ulažu ogromna sredstva u zaštitu i sigurnost svojih elektronskih komunikacija na globalnoj mreži, stoje na stanovištu da su hakerski napadi najveći bezbednosni izazov današnjice, može se zaključiti da se o apsolutnoj pouzdanosti u pogledu zaštite anonimnosti na Internetu ne može govoriti.

Tor mreža može biti manje ili više pouzdana, u zavisnosti od ljudskog faktora – pojedinaca koji predstavljaju klijenti i volonteri, vlasnici releja. Klijenti će osigurati pouzdanost pristupa putem Tor klijentske aplikacije ako mreži pristupe sa butabilnog diska ili fleša, izbegavajući da izlože memorijske jedinice svog računara, na kojima su smeštene datoteke i aplikacije koje bi mogle da posluže za analizu profila korisnika. Stalno obnavljanje verzije Tor aplikacije sa službene web lokacije značajno doprinosi povećanju pouzdanosti. Čitanje dokumentacije preuzete sa globalne mreže u vreme sesije predstavlja bezbednosni rizik. Na serverskoj strani, ranjivi su računari koji imaju status izlaznog releja, posebno kad se izlazi na globalnu mrežu prekidanjem SSL protokola.

Francuski istraživači iz ESIEA, francuske inženjering škole [9] došli su na ideju, analizirajući topografiju Tor mreže, da je moguće uspostaviti kontrolu nad mrežom ubacivanjem virusa u računare releje. Najpre se pribavljaju IP adrese svih releja, putem odgovarajuće skripte koju su razvili. Odgovarajućom metodom u ranjive releje ubacuje se virus. Pošto uspostave administratorske privilegije nad zaraženim relejima, primenjuju dvostruki napad: lokalizovana zagušenja, koji podrazumeva slanje velikog broja zahteva prema neinficiranim relejima, a zatim se okreće paket sa virusom, implementiran u zaraženim relejima, koji se priloži nezaraženim serverima u petlji kola da ih popuni.

Početkom oktobra 2013. godine engleski časopis The Gardian [9] preneo je je na svom web sajtu informaciju da je američka Agencija za nacionalnu bezbednost objavila da je dizajnirala skriptu pod kodnim nazivom *Egotistical-*

Giraffe pomoću koje se dekodira enkripcija podataka na Tor mreži. Iz informacije se može zaključiti da je ranjivost pokazala Firefox aplikacija, adaptirana u Tor aplikaciju.

ZAKLJUČAK

Sve veća primena digitalne komunikacije i Interneta (kao okosnice) ima za posledicu stavljanje u prvi plan fenomena zaštite privatnosti pojedinca. Fokus na zaštitu digitalnog identiteta postavljen je u javnosti pošto se došlo do saznanja da je privatnost pojedinca na Internetu ozbiljno ugrožena i da će u bliskoj budućnosti problem poprimiti još šire razmere. Zaštita identiteta na Internetu je kompleksan problem, koji podjednako tangira pojedince, različite organizacije i države. Problem ima svoju filozofsku dimenziju (kao narušavanje slobode), pravnu, sociološku i psihološku dimenziju.

Problem zaštite identiteta je višeslojan; vezan je za informatičku kulturu; navike pojedinca; materijalni status. Izazov počinje od operativnog sistema (licencirani ili piratska verzija), preko softvera koji koristimo u različite svrhe i internet lokacija koje posećujemo.

Virtuelne privatne mreže, web proxy servisi i Tor mreža svakako smanjuju stepen rizika izloženosti pojedinca od gubitka digitanog identiteta. Tor projekat postoji dvanaest godina. Treća generacija aplikacije nudi najbolju zaštitu. Prednost Tor mreža u poređenju sa drugim softverski definisanim anonimnim mrežama ogleda se u luk rutiranju saobraćaja, koji menja čvorišta metodom slučajnog izbora, prilikom svakog url-ovanja nove lokacije na Internetu. Dodatnu sigurnost predstavlja kodiranje i dekodiranje sadržaja na svakom čvorištu. Najbolji rezultati postižu se kad je kompletan saobraćaj pod SSL i TLS protokolom, uključujući i pristup odredišnom serveru na javnoj mreži. Na službenoj web lokaciji Tor korporacije jednom mesečno publikuje se nova verzija softvera, što je vrlo značajno, jer se time pokrivaju uočeni bezbednosni propusti i povećava nivo zaštite.

Povećanje broja releja, koji čine okosnicu privatne mreže, predstavlja dodatnu sigurnost za korisnike. Releji su u najvećem broju u vlasništvu volontera, koji mogu isti računar koristiti i za druge namene i tu leži senka na izuzetno dizajniranoj privatnoj mreži. Rizik od napada virusom kojim se uspostavlja kontrola nad računarom je vrlo velika.

U kategoriji besplatnih anonimnih mreža Tor po sigurnosti nema konkurenciju. Nivo zaštite identiteta nije i ne može biti potpun. Organizacije koje rade za marketing kompanije i hakeri verovatno čine većinu napadača; sakupljača podataka. Tor je za njih veliki izazov i brana. Kad su u pitanju međunarodne agencije za zaštitu intelektualne svojine u oblasti multimedije (filmska industrija), diskografske kuće, i bezbednosne agencije vlada savremenih država, Tor ima ograničeni domet.

Ne postoji aplikacija niti privatna mreža na Internetu koja može da obezbedi stoprocentnu zaštitu digitalnog identiteta pojedinca.

LITERATURA

[1] Internet censorship by country, na web adresi: http://mapsontheweb.zoom-maps.com/post/58162171430/internet-censorship-by-country, 10. mart 2014.

[2] Official Journal of the European Union, L 105/54, 13.4.2006 "Directive 2006/24/EC of the Europian Parlament", http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF, 2. februar 2014.

[3] Proxy.org, "Free web proxies", https://proxy.org/cgi_proxies.shtml, 21. februar 2014.

[4] "Tor Manuals", https://www.torproject.org/docs/manual.html.en, 21. februar 2014.

[5] Wukipedia (Engllish online edition), "Tor (anonymity network)", http://en.wikipedia.org/wiki/Tor_network, 25. februar 2014.

[6] P. Staletić, N. Staletić, "Piraterija digitalnog sadržaja na Internetu", XII međunarodni naućno-stručni simpozijum, Jahorina, 2013.

[7] Keith D. Watson, The Tor Network, "A Global Inquiry into the Legal Status of Anonymity Networks", 11 Wash. U. Glob. Stud. L. Rev. 715, 2012.

[8] Tor, Inception",https://www.torproject.org/about/torusers.html.en, 3. februar 2014.

[9] The hacker News, "Tor anonymizing network compromised by French researchers", http://thehackernews.com/2011/10/tor-anonymizing-network-compromised-by.html, 3. februar 2014.

[10] „Peeling back the layers of Tor with EgotisticalGiraffe", http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document, 25. februar 2014.

Abstract:

Interest in the topic of identity protection on the Internet is constantly gaining in importance, with progressive growth of digital communication and application of the Internet as an information and communication technology in the modern age, the increasing censorship applied by the security agencies, governments of modern states, ISP companies (the legal obligation to retain data user activity), the company operates industrial espionage and marketing companies to determine the target market. There are a number of other organizations and individuals who are motivated diverse interests looking for information that essentially interfere with the privacy of individuals or companies.

This paper analyzes the identity protection on the Internet using anonymous networks. By anonymous networks means access to a global network using VPN (Virtual Private Network), web proxy and an anonymous network. The focus of analysis is on the topography and security to protect the identity provided by the Tor anonymous network.

Key words:

anonymous network,
Thor,
web proxy,
identity protection on the Internet,
internet censorship.