

DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

STUDIJSKI PROGRAM

SAVREMENE INFORMACIONE TEHNOLOGIJE

ANONIMNOST NA INTERNETU –Tor Rešenje

- MASTER RAD -

Mentor:

prof. dr Mladen Veinović

Kandidat:

Vladimir Stanojević

2012/410453

Beograd, 2013.

Anonimnost na internetu –Tor rešenje

Sažetak

Pri komunikaciji kroz internet kao medijum, izložen je kako identitet pojedinca koji razmenjuje podatke preko interneta, tako i sami sadržaji u toj komunikaciji. Velika većina korisnika interneta toga nije svesna ili im to nije bitno. Međutim sa sve većom ulogom koju u našim životima igra internet, potreba za zaštitom našeg identiteta i privatnosti raste srazmerno. U ovom radu su prikazane tehnike zaštite identiteta(ostvarenje anonimnosti) i privatnosti pri komunikaciji na internet, sa posebnim akcentom na Tor rešenje.

Ključne reči: Internet, komunikacija, tehnike zaštite, privatnost, anonimnost, Tor rešenje.

Internet communication anonymity -Tor

Abstract

While using the Internet as medium for communication, one's identity is exposed as well as the contents of communication. Most of internet users are not aware of this, or just doesn't care about it. But, while the Internet begins to play more and more important role in our lives (both in quality and quantity aspects), the importance of protecting our identity and privacy rises proportionally. In this study we present the techniques to ensure anonymity (protect one's identity) and privacy while communicating over internet, with highlight of Tor solution.

Keywords: Internet, communication, protection techniques, privacy, anonymity, Tor, Onion Routing.

Indeks slika

1. Slojevi OSI Modela.....	11
2. Postupak enkapsulacije/dekapsulacije informacije u OSI modelu.....	11
3. Komparativni prikaz slojeva OSI i TCP/IP modela.....	12
4. Struktura IP header-a.....	13
5. Mesto i funkcija Proxy servera u računarskoj mreži.....	16
6. Primer setovanja MS Internet Explorer-a da koristi proxy server.....	18
7. Primer setovanja Mozilla Firefox-a da koristi proxy server.....	19
8. Anonym.OS Live screenshot 1.....	24
9. Anonym.OS Live screenshot 2.....	25
10. Uprošćeni prikaz korišćenja Tor rešenja.....	31
11. Paket podataka „obložen“ višestrukim šifrovanjem koji se transportuje kroz Tor oblak.....	32
12. Ilustracija kako je paket podataka (Data) višeslojno šifovan kao slojevi crnog luka.....	38
13. Kontrolna aplikacija Tor-a na PC računaru.....	44
14. Početni ekran Tor Browser-a.....	45
15. Slika 15. Detaljni prikaz sa grafičkim prikazom uspostavljene Tor putanje...46	

Indeks tabela i grafikona

1. Dinamika uvođenja „private browseing-a“
2. Statistika korišćenja operativnih sistema, decembar 2012.....
3. Statistika korišćenja Web browser-a, decembar 2012.....
4. Prosečno vreme transporta paketa kroz Tor oblak.....
5. Procenat „neostvarenih veza“ kroz Tor mrežu.....

SADRŽAJ

I METODOLOGIJA	7
I.1. UVODNE NAPOMENE	7
I.2. PREDMET ISTRAŽIVANJA	7
I.3. HIPOTEZA.....	7
I.4. CILJEVI ISTRAŽIVANJA	8
I.5. KORIŠĆENE NAUČNE METODE	8
II UVOD.....	9
II.1 ANONIMNOST	9
II.2 PRIVATNOST	9
II.3 KOLIKO JE REALNO NAŠ IDENTITET I PRIVATNOST IZLOŽENA NA INTERNETU	10
II.4 STRUKTURA INTERNET KOMUNIKACIONIH PROTOKOLA	10
II.5. IP PROTOKOL.....	13
III RASPOLOŽIVE TEHNIKE I REŠENJA ZA POSTIZANJE ANONIMOSTI NA INTERNETU	16
III.1. ANONIMNI PROXY SERVERI.....	16
III.2. Live OS REŠENJA ZA ZAŠTITU PRIVATNOSTI	21
III.3. PRIVATE/INCOGNITO METODE UGRAĐENE U WEB BROWSER-E	26
III.4. OSTALA REŠENJA	28
IV TOR REŠENJE	29
IV.1. ŠTA JE TOR PROJEKT I KAKO JE NASTAO	29
IV.2. KAKO TOR FUNKCIONIŠE.....	31
IV.2.1. OSNOVNI PRINCIPI	31
IV.2.2. TEORETSKA PODLOGA.....	33
IV.2.3. RSA ALGORITAM	33
IV.3. TOR REŠENJE –ANALIZA „SLOJ PO SLOJ“	37

IV.3.1. ENKRIPCIIJA/DEKRIPCIIJA PAKETA KROZ TOR MREŽU	37
IV.3.2. REDIREKCIJA PAKETA KROZ TOR MREŽU I NAČIN POSTIZANJA ANONIMNOSTI	39
IV.3.3. ALGORITAM RUTIRANJA PAKETA KROZ TOR MREŽU	40
IV.4 TOR REŠENJE U PRAKSI.....	42
IV.4.1. STATISTIKA KORIŠĆENJA TOR REŠENJA.....	42
IV.4.2. KAKO KORISTITI TOR REŠENJE ZA SOPSTVENE POTREBE	44
IV.4.3 TOR REŠENJE ZA WEB SERWISE	48
IV.5. DOKUMENTOVANE SLABOSTI TOR REŠENJA.....	49
V ZAKLJUČAK	51
VI LITERATURA	54

I METODOLOGIJA

I.1. UVODNE NAPOMENE

U ovom istraživanju obrađen je koncept anonimnosti/privatnosti na internetu.

Korišćenje interneta je postala svakodnevna aktivnost široke populacije. Rastom kako kvantitativne dimenzije korišćenja internet, proporcionalno se uvećala i kvalitativna dimenzija, u smislu da se broj i vrste naših svakodневnih aktivnosti na internet umnožava svakodnevno. Uz sve dobre strane, korišćenje interneta donosi sa sobom i rizike narušavanja privatnosti i/ili zloupotrebe ličnih ili poslovnih podataka.

U ovom radu su istražene i opisane tehnike za postizanje anonimnosti i zaštitu privatnosti na internet, sa akcentom na Tor rešenju kao trenutno najefikasnijem načinu za postizanje istih.

I.2. PREDMET ISTRAŽIVANJA

Predmet istraživanja su načini za ostvarivanje anonimnosti i zaštite privatnosti na internetu. Obuhvaćeni su pojmovi anonimnosti i zaštite privatnosti na internetu u smislu tačnog definisanja istih, i predložena su razna dostupna rešenja za postizanje što višeg nivoa željene zaštite kako svog identiteta, tako i svojih bitnih ličnih/poslovnih podataka pri komunikaciji na internetu. Zatim je od tih više prikazanih rešenja izdvojeno Tor rešenje kao najefikasnije, detaljno prikazano, i dokumentovane njegove prednosti i slabosti.

I.3. HIPOTEZA

Opšta hipoteza: Komunicirajući tj. razmenjujući podatke na internetu identitet korisnika tj. izvor svakog podatka/aktivnosti na internetu je javno dostupan, te time postoji mogućnost zlonamernih aktivnosti ka konkretnom korisniku kao i zloupotreba privatnih/poslovnih podataka svakog pojedinog korisnika. Svako treba da bude svestan toga i da u potrebnoj meri zaštititi svoj identitet i svoje podatke.

Posebna/radna hipoteza: Postoje mnogobrojne pretnje/rizici po anonimnost/privatnost korisnika interneta, te su vremenom evoluirale razne tehnike i alati koji omogućavaju anonimnost/zaštitu privatnosti korisnika interneta. Tor rešenje je najefikasnije javno dostupno rešenje za postizanje anonimnosti i zaštitu privatnosti korisnika na internetu.

I.4. CILJEVI ISTRAŽIVANJA

Naučni cilj:

Da se istraže i opišu najzastupljenije pretnje po anonimnost/privatnost korisnika na internetu i analitički i komparativno ispituju i opišu najzastupljenija tehnička rešenja za zaštitu istih, te izdvoji najefikasnije od njih. Zatim da se to rešenje detaljno dokumentuje i prikažu njegove prednosti i eventualne slabosti.

Društveni ciljevi su:

1. Da se korisnici interneta pravilno informišu o pretnjama/rizicima komunikacije na internetu po bezbednost njihovog identiteta i/ili njihovih privatnih/poslovnih podataka.
2. Da se korisnici interneta upoznaju sa aktuelnim tehnikama zaštite anonimnosti/privatnosti podataka, sa njihovim mogućnostima i dometima (ograničenjima), i kako da ih pravilno primene.

I.5. KORIŠĆENE NAUČNE METODE

U ovom istraživanju su korišćene:

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

pri identifikovanju rizika/pretnji i vrednovanju tehničkih rešenja koja su dostupna za zaštitu od istih.

Pri prikupljanju i obradi podataka korišćene su metode analize sadržaja kako već dostupnih istraživanja i literature iz šire oblasti istraživanja, tako i eksperimentalno testiranje najzastupljenijih tehničkih rešenja zaštite koja su predmet ovog istraživanja, te vrednovanje i iskazivanje rezultata tih eksperimenata.

II UVOD

POJAM KONCEPTA ANONIMNOSTI/PRIVATNOSTI NA INTERNETU

II.1 ANONIMNOST

Samim povezivanjem na internet, naš identitet je dostupan. Prvo je dostupan našem ISP (Internet Service Provider)-u, koji je **dužan** po važećim zakonskim propisima da čuva evidenciju o svakom vašem konektovanju, o momentu konektovanja i trajanju konekcije. Ti podaci se čuvaju u slučaju da neki državni organ zatraži iste od ISP-a, ako se istražuje neka kriminalna aktivnost nekog korisnika na internetu. Međutim naš „identitet“, je izložen tokom celokupne naše aktivnosti na internetu, jer put koji svaka informacija prelazi od nas do odredišta i nazad ka nama je dostupna bilo kome na internetu ko vlada odgovarajućim znanjima i tehnikom. Samim uvidom u svaki taj „paket podataka“ koji putuje internetom direktno je moguće direktno identifikovati pošiljaoca i primaoca svakog podatka. Međutim, jednako značajno je naglasiti da je moguće ne samo identifikovati pojedinog korisnika kao individuu, nego identifikovanje korisnika pojedinog web servisa ili servera koji je meta praćenja, te to može zloupotrebljavati npr. poslovna konkurencija da sazna identitet korisnika njihovog poslovnog konkurenta. Ili neka treća strana koja će te podatke iskoristiti bilo direktno ili će ih ustupiti/prodati nekom drugom u svrhe ciljanog marketinga ili sl.

II.2 PRIVATNOST

Osim utvrđivanja identiteta korisnika, na internetu je jednako lako pratiti i aktivnosti pojedinog korisnika, odnosno aktivnosti na pojedinom web servisu/serveru. I to ne samo opisno, već tačno koji korisnik koga dana, u kolikom trajanju, čak u većini slučajeva i kompletan transkript komunikacije konkretnog korisnika sa određenim web servisom/serverom. Ovaj rizik možemo posmatrati odvojeno u smislu da se radi o „presretnutoj komunikaciji“, ili o pregledu log-ova internet browser-a na samom računaru korisnika, naročito ako se radi o „deljenom“ ili „javnom“ računaru npr. negde u nekom preduzeću, ili internet caffè-u i sl.

II.3 KOLIKO JE REALNO NAŠ IDENTITET I PRIVATNOST IZLOŽENA NA INTERNETU

Kao što smo videli iz gore navedenog, naš identitet u smislu naše tačne lokacije sa koje pristupamo internetu, i konkretne identifikacije našeg uređaja (desktop računara, laptopa ili mobilnog telefona) koji koristimo na internetu je “objavljen i dostupan” već od momenta kada smo se konektovali na internet.

Dakle naš identitet i lokaciju je moguće utvrditi od momenta konekcije na internet.

Osim našeg identiteta/lokacije, ono što je takođe dostupno “trećoj strani” je i naša aktivnost na internetu, u smislu sa kojim web servisima ostvarujemo konekciju i čak u određenim okolnostima i kompletan sadržaj naše međusobne komunikacije sa tim pojedinim web servisima.

Razlog za ovo je, u velikoj meri, sama struktura komunikacionog protokola kojim naš računar komunicira sa drugim računarom kroz internet.

II.4 STRUKTURA INTERNET KOMUNIKACIONIH PROTOKOLA

Na internetu su u svakom trenutku povezani i međusobno komuniciraju milioni računara. Potpuno je iracionalno i praktično nemoguće ostvariti fizičku direktnu vezu između svakog od tih računara. Kada bi to bilo tehnološki svrsishodno i moguće, onda bi svaki računar komunicirao direktno sa drugim računarom, i u teoriji dva korisnika bi mogla da definišu svoj komunikacioni protokol poznat samo njima i tako ostvare razmenu podataka između svoja dva računara.

Ovakva situacija bi predstavljala izazov i zahtevala određene resurse treće strane da presretne, sluša, analizira, dešifruje i/ili izmeni te sadržaje ili zloupotrebi to na neki drugi način.

Međutim kao što smo rekli, realna topologija veza između dva računara na internetu je drugačija. Internet kao “mreža svih mreža” je to i postao tako što je prevazišao ograničenje za potrebom direktne komunikacione veze između dva računara.

Krajem 1970-ih godina, ISO¹ je definisala “Open Systems Interconnection Model” (OSI)[1], čime su pružili softverskim inženjerima i arhitektama računarskih mreža modularan i fleksibilan okvir za dalji razvoj komunikacionih sistema. Na slici 1. Je prikazana opšta struktura “slojeva” OSI modela.

¹ ISO -International Organization for Standardization, <http://www.iso.org>



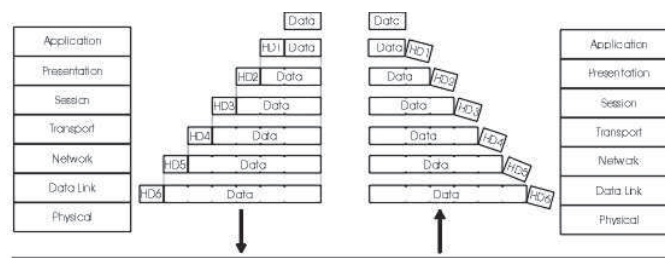
SLIKA 1. Slojevi OSI Modela.

Ove slojeve možemo prosto predstaviti kao jedno pismo. Dakle mi pišemo rukom slova na papiru, pa taj papir spakujemo u kovertu i adresiramo je na primaoca a sa zadnje strane naznačimo naše podatke (adresa pošiljaoca), te poneseemo u poštu. Tamo u pošti na tu kovertu se doda i markica i poštanski pečat sa šifrom pošte iz koje koverta kreće.

Zatim ta koverta putuje kroz jedan ili više distributivnih centara pošte odakle se svakim korakom približava adresi primaoca. Konačno pismo biva isporučeno primaocu, koji najčešće tu kovertu otvori i baci, jer je ona odradila svoje, i pročita pismo koje mu je upućeno.

Dakle izvorna informacija se, kada kreće na svoj put ka odredištu, “spušta” kroz ove slojeve od aplikativnog do fizičkog nivoa, i svaki od tih slojeva enkapsulira (oblaže, umotava) izvornu informaciju iz prethodnog sloja nekim svojim relevantnim podacima (headerom-zaglavljem), što je ekvivalentno našem prethodnom primeru operaciji pakovanja pisma u kovertu, pa adresiranje te koverta, pa markica, pa pečat pošte...

Na odredištu se dešava obrnut proces gde se informacija “penje” iz fizičkog sloja do aplikativnog i pritom se “vadi” tj. izdvaja samo informacija bitna sledećem višem sloju, a onaj deo koji je bio bitan do prethodnog sloja ostaje odbačen (ekvivalentno našem prethodnom primeru kada primalac otvori i baci kovertu, a zadrži samo pismo). Ovaj proces je prikazan na slici 2.²



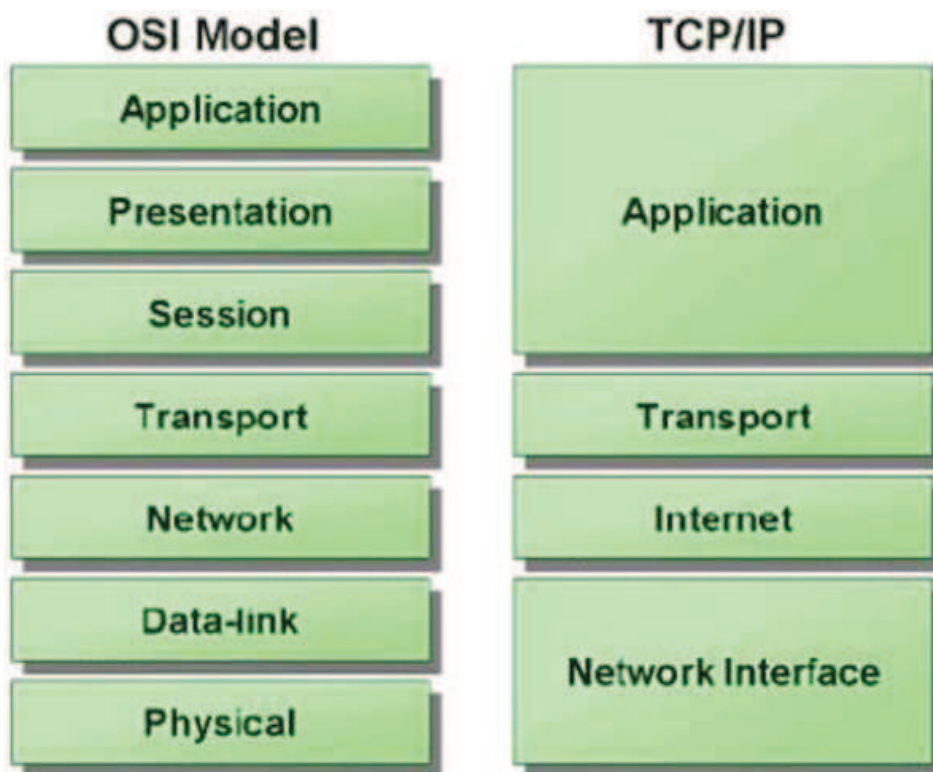
Slika 2. Postupak enkapsulacije/dekapsulacije informacije u OSI modelu.

² <http://www.lrgnetworks.com>

OSI Model je bio samo uzor po kome je nastao kasnije TCP/IP komunikacioni model protokola. Namerno kažemo TCP/IP **model** a ne protokol, jer su danas TCP i IP u stvari nezavisni protokoli, i to na različitim nivoima. Ovo je česta zabluda, te moramo napraviti jasnu razliku.

1970-ih, Vinton Cerf, Jon Postel i mnogi drugi u njihovom timu su razvili inicijalni TCP protokol u okviru projekta koji je finansiralo ministarstvo odbrane Sjedinjenih Američkih Država, preko agencije DARPA. Prva verzija TCP je objavljena kao „Stanford University TCP Project“[2] i ona je sadržala u sebi objedinjene funkcionalnosti koje su kasnije podeljene u dva nezavisna protokola na različitim mrežnim nivoima (slojevima): TCP i IP protokol.

Bilo je više faza u razvoju i implementaciji ova dva protokola, ali pošto to nije suština teme ovoga rada, samo ćemo pomenuti da je IP protokol konačno objavljen kao RFC 791[3] septembra 1981, a revidirani danas aktuelni TCP protokol je objavljen kao RFC 793[4] takođe septembra 1981.



Slika 3. Komparativni prikaz slojeva OSI i TCP/IP modela.

II.5. IP PROTOKOL

Sa aspekta anonimnosti/zaštite privatnosti na internetu nama je bitno razumevanje IP protokola. U gore navedenom TCP/IP modelu, on se nalazi u drugom sloju (internet). On je dizajniran da omogući adresiranje i rutiranje (trasiranje-prosleđivanje) paketa podataka kroz internet. Konkretno kada se paket podataka „spušta“ na ovaj nivo na polazištu on biva „obogaćen“ tj. dopunjen informacijama koje se pakuju u „header“ (zaglavlje) paketa podataka iz protokola višeg nivoa. Tako upotpunjen paket se naziva „IP Paket“. Taj paket biva nepromenjen prosleđivan kroz neograničen broj čvorišta kroz internet sve do odredišta gde se „raspakuje“ i ekstraktuje sam paket podataka iz protokola višeg nivoa i takav prosleđuje protokolu višeg nivoa na odredištu. Na slici br. 4 prikazana je struktura IP header-a.

0										1										2										3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1								
Version				IHL				TOS/DSCP/ECN								Total Length																							
Identification												Flags				Fragment Offset																							
Time To Live								Protocol								Header Checksum																							
Source Address																																							
Destination Address																																							
Options																												Padding											

Slika 4. –struktura IP header-a.

Svo vreme svog „putovanja“ od polazišta do odredišta taj „IP paket“ sadrži u svom header-u podatke o jedinstvenoj identifikaciji pošiljaoca i primaoca. Konkretno to su IP adresa pošiljaoca i primaoca. Naravno to znači da IP adresa mora jedinstveno i unikatno označava pošiljaoca i primaoca.

Prvobitni dizajn IP protokola iz 1981 je predvideo 32bit-ni opseg za IP adrese, što u praksi znači da je bilo moguće dodeliti korisnicima ukupno 2^{32} (nešto manje od 4.3 biliona) IP adresa koje bi ih jednoznačno određivale, i koriste se za pošiljalac/primalac adresiranje IP paketa. Ovo je naravno teoretski opseg, ali u praksi je nešto drugačije.

Neke od tih adresa su rezervisane za specifične namene. Na primer tri opsega adresa su rezervisane za privatne/lokalne mreže[5] . To su:

10.0.0.0<----->10.255.255.255

172.16.0.0<----->172.31.255.255

192.168.0.0<----->192.168.255.255

Takođe postoje i posebni rezervisani opsezi IP adresa dodeljenih u danima početka interneta čiji je najočigledniji primer dodela celog opsega adresa „A klase“ 18.*.*.* (koji dakle obuhvata preko 16 miliona pojedinačnih IP adresa) MIT univerzitetu.

To naravno nije delovalo kao ograničavajući faktor u ranom dobu interneta, ali nagla ekspanzija korišćenja interneta, a posebno eksponencijalno uvećanje prisustva mobilnih uređaja koji takođe koriste internet (smart mobilni telefoni i sl) je uzrokovala „netašicu“ dostupnih IP adresa.

Tako je poslednjih pet IPv4 adresnih opsega IANA³ raspodelila među 5 RIR (Regional Internet Registries) agencija februara 2011.⁴

Naravno, to nije bio „smak sveta“ niti kraj ili dostizanje krajnje tačke širenja interneta, jer je već 1998. godine objavljena specifikacija IPv6 protokola[7]. IPv6 protokol za razliku od prvobitnog IPv4 protokola predviđa 128-bitni opseg za IP adrese. Dakle moguće je adresirati 2^{128} jedinstvenih IP adresa što je oko 340 undecilionu. IP Adrese IPv6 protokola se u „ljudski čitljivom formatu“ zapisuju i prezentuju kao 8 četvorocifrenih heksadecimalnih brojeva.

Npr: 2001:01e8:5922:0000:0000:0001:341d:0001

Ovaj protkol je uneo još neke bitne izmene u odnosu na IPv4 protokol, ali pošto one nisu direktno bitne za predmet ovog istraživanja, ovde ćemo ih samo pomenuti.

Kao prvo, IPv6 header za razliku od IPv4 ne sadrži checksum, nego je detekcija validnosti paketa u potpunosti prepuštena protokolima višeg nivoa. Ovo donosi značajnu prednost u performansama protoka, jer ne mora na svakom čvorištu ruter da izračunava i upoređuje checksum headera svakog paketa.

Takođe, dužina headera kod IPv6 paketa je uvek fiksna, što takođe ubrzava transport paketa kroz rutere.

Značajno unapređenje u odnosu na IPv4 protkool IPv6 donosi u tome što je dizajniran da nativno podržava IPSec.

Dakle osim direktno našeg identiteta i lokacije, „trećoj strani“ je dostupna i informacija o „drugoj strani“ sa kojom mi komuniciramo. Iz svakog paketa podataka koji razmenimo (pošaljemo ili primimo) može se direktno saznati informacija (IP adresa) koja će jasno identifikovati nas i drugu stranu (primaoca ili pošiljaoca) svakog paketa podataka.

Ovim ne samo da može biti narušena naša anonimnost već i naša privatnost jer „neko sa strane“ može da prati naše aktivnosti na internetu, te da saznaje naša interesovanja. Takođe bilo koja „treća strana“ može da saznaje sadržaj podataka koje razmenjujemo kroz internet, da ih čuva, kopira, menja, itd.

Posebno treba naglasiti da se može direktno po samoj vrednosti IP adrese locirati geografski položaj pojedinog korisnika (do nivoa preciznosti Država/(eventualno) grad), što se recimo svakodnevno koristi za „ciljano“ reklamiranje u smislu da se pojedinim korisnicima interneta prezentuju reklame relevantne ponude za njihovo goeografsko prebivalište.

³ IANA-Internet Assigned Numbers Authority

⁴ Lawson, Stephen, „IPv6 Doomsday Won't hit in 2012, Experts say.“, PCWorld, 29. decembar 2011,
http://www.pcworld.com/businesscenter/article/247091/ipv6_doomsday_wont_hit_in_2012_experts_say.html (čitano 19.1.2013)

Baza podataka o tome se zove GeoIP, i postoje brojni internet servisi dostupni za identifikovanje zemlje/grada pojedine IP adrese. Kao primer možemo navesti:

<http://www.geoptool.com/>

http://www.maxmind.com/en/locate_my_ip

Da ne bude zabune, na ovim gornjim linkovima možemo proveriti tu funkcionalnost na svojoj IP adresi, ali takođe ako neko drugi želi da locira nas preko naše IP adrese, ili mi nekoga preko njegove, eto koliko je to lako i dostupno čak i laiku.

Naravno, pošto prosečan korisnik najčešće ostvaruje vezu prema internetu preko svog ISP-a, podatak koji ovde možemo dobiti završava na ISP-u koji je konkretnu IP adresu dodelio konkretnom korisniku u toj sesiji. Ako bi hteli da lociramo baš samog korisnika morali bi da imamo pristup log-ovima tog konkretnog ISP-a. To su međutim podaci koji nisu javno dostupni, ali u situacijama predviđenim zakonom, ISP je dužan da nadležnim organima pruži tu informaciju.

Takođe veliki broj korisnika zadnjih godina, uglavnom za poslovne potrebe kod svog ISP-a zakupljuje fiksnu „javnu“ IP adresu koja na internetu figurira kao samostalni entitet koji najčešće ima pridružen i domen (opisno ime koje odgovara toj IP adresi), npr. domen „singidunum.ac.rs“ je ekvivalent za IP adresu 50.116.73.209, koju na gore navedeni način možemo „locirati“ tj. ustanoviti da je taj domen/IP adresa „hostovan“ kod kompanije Websitewelcome.com, koja se nalazi u ulici Hewitt drive, u gradu Huston, savezna država Texas, SAD.

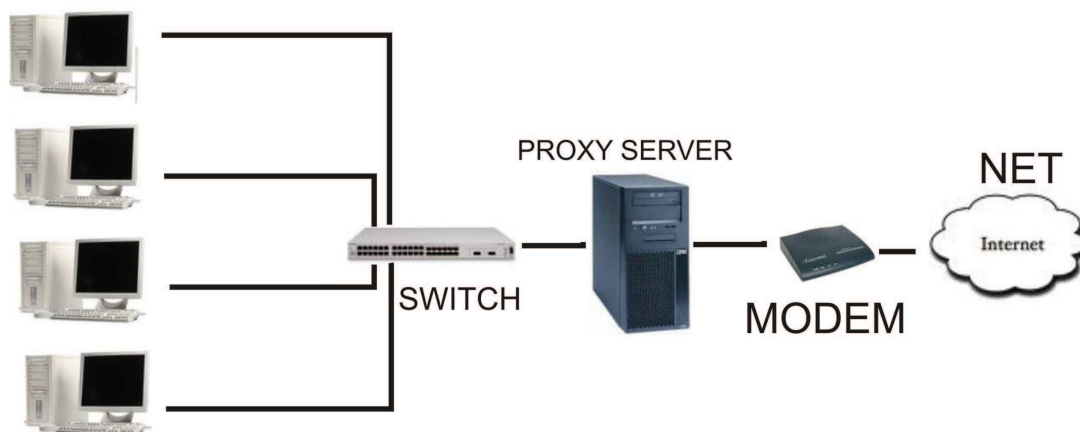
III RASPOLOŽIVE TEHNIKE I REŠENJA ZA POSTIZANJE ANONIMOSTI NA INTERNETU

III.1. ANONIMNI PROXY SERVERI

Pod pojmom proxy servera u ovom radu podrazumevamo funkcionalnu instancu proxy servera koja može biti hardverski implementirana ili softverska aplikacija koja se izvršava na računaru bilo samostalno ili naporedo sa drugim serverskim ili sličnim instancama u okviru računarske mreže.

Proxy server je vrlo kompleksan, i ima široku primenu u računarskim mrežama. Ovde ćemo se ograničiti na razmatranje samo onih aspekata koji se odnose na predmet ovog rada. U tom smislu bitna odlika proxy servera je da on služi kao „posrednik“ između pojedinog konkretnog korisnika (tj. njegovog računara) i „spoljašnjeg sveta“, u konkretnom slučaju interneta. U tom svom „posredovanju“, proxy server može da modifikuje odlazni/dolazni paket podataka na nivou IP protokola, u smislu da IP adresu „pošiljaoca paketa“, koji taj paket podataka šalje kroz internet, zameni svojom IP adresom, te paket koji nastavlja svoj put prema odredištu, posle proxy servera u okviru header-a na nivou IP protokola kao IP adresa pošiljaoca figurira IP adresa proxy servera koji obrađuje tj. prosleđuje taj paket dalje. Šematski prikaz korišćenja proxy servera je dat na slici 5.

CLIENT



Slika 5. Mesto i funkcija Proxy servera u računarskoj mreži.

Međutim kod „regularnih“ proxy servera, pošto im to nije primarna svrha, u okviru IP paketa, proxy „prepakuje“ primljeni IP paket i dodaje mu tzv „X-Forwarded-For element“ u viši nivo header-a. Na nivou IP paketa IP adresa pošiljaoca se menja adresom proxy-ja, i paket se dalje prosleđuje ka prvobitnom odredištu. Međutim kako na odredištu, tako i u bilo kom trenutku/koraku dok paket putuje od polazišta do odredišta isti je izložen da ga treća strana preuzme i njegovom direktnom analizom, osim provere IP adrese

polazišta, direktno se može potražiti X-Forwarded-for polje u paketu i ako isto postoji, iz njega pročitati direktno IP adresu originalnog pošiljaoca.

Npr. ako pogledamo jedan internet paket koji sadrži X-forwarded polje:

X-Forwarded-For: 10.208.4.38, 58.163.175.187

Možemo zaključiti da je lokalna (privatna) IP adresa pošiljaoca paketa **10.208.4.38**, a adresa proxy servera kroz koji je „prošao“/prosleđen taj paket je **58.163.175.187**. Logično, bilo kojoj trećoj strani, ova lokalna IP adresa pošiljaoca ne govori ništa vredno, ali IP adresa proxy servera ako se proverí npr. u GeoIP bazi, dobićemo informaciju da se ta IP adresa koristi (dakle naš korisnik je tamo) u centralnoj Australiji, čak sa prilično tačnom geografskom lokacijom dodeljene IP adrese⁵. Tako neka državna agencija u slučaju potrebe otkrivanja počinioca nekog kriminalnog dela može da locira tačnu privatnu mrežu, u okviru koje se nalazi računar koji je korišćen za izvršenje tog kriminalnog dela, pa onda daljom analizom log-ova u lokalnoj mreži da locira i sam taj računar.

Međutim, ovde nije kraj priče oko X-Forwarded-For polja, jer se isto može proširivati IP adresama svakog narednog proxy servera kroz koji paket prođe na svom putu ka odredištu.

Npr:

X-Forwarded-For: 10.208.4.38, 58.163.1.4, 58.163.175.187, ako paket prolazi kroz dva „spoljnja“ proxy servera na svom putu, ili

X-Forwarded-For: 10.208.4.38, 10.10.300.23, 58.163.175.187, ako paket prolazi kroz jedan proxy server na privatnoj/lokalnoj mreži, pa tek onda kroz neki proxy server npr. ISP-a, ili drugi.

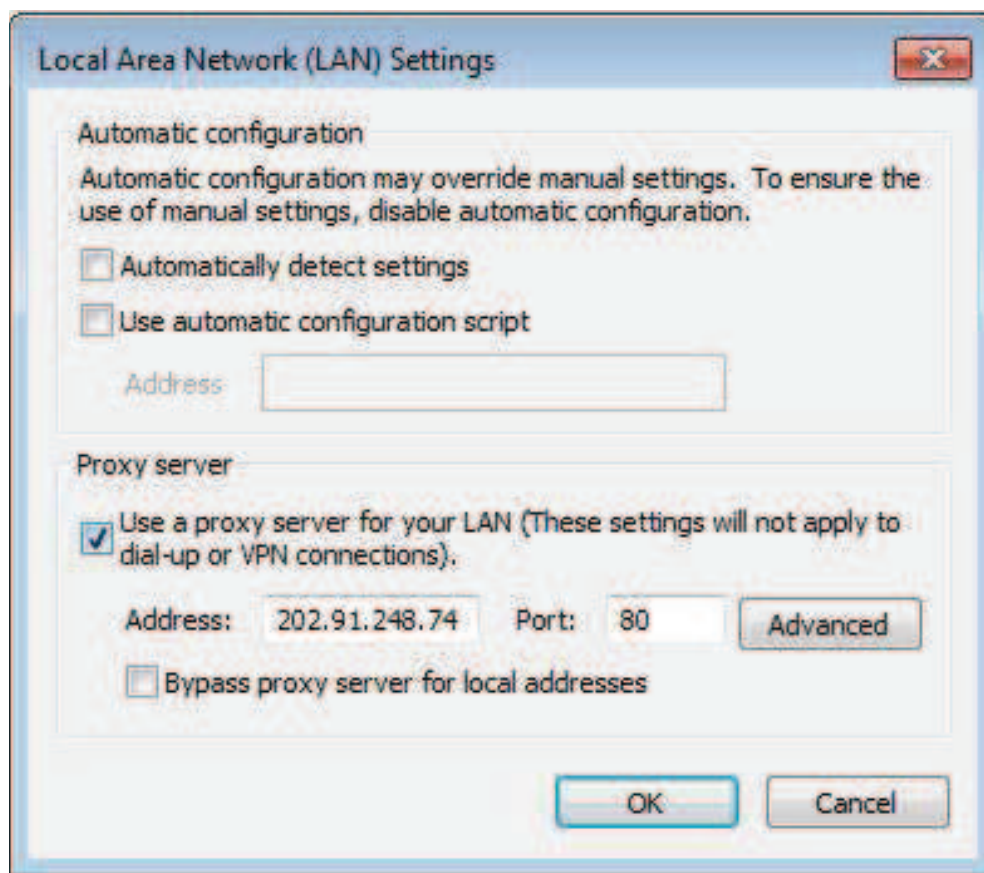
U svakom slučaju svaki takav paket presretnut i analiziran u bilo kojoj etapi u bilo kom od opisanih slučajeva sadrži direktno dostupne podatke o identitetu/lokaciji i pošiljaoca i primaoca svakog tog paketa.

Kao „kontramera“ tj. jedan od načina da se zaštiti identitet izvornog pošiljaoca nekog paketa podataka preko interneta se koriste „Anonimni proxy serveri“ ili „Anonimizirajući proxy serveri“, koji dakle u potpunosti uklanjaju podatke o izvornom pošiljaocu paketa podataka koji zatim prepakuju a kao izvornog pošiljaoca paketa postavljaju svoju IP adresu. Time se postiže da od tog trenutka paket podataka **nastavlja** svoj put do odredišta kao da je krenuo od tog proxy servera, i više ne sadrži podatke na osnovu koga bilo primalac ili bilo koja treća strana mogu identifikovati pošiljaoca direktno analizom header-a paketa podataka.

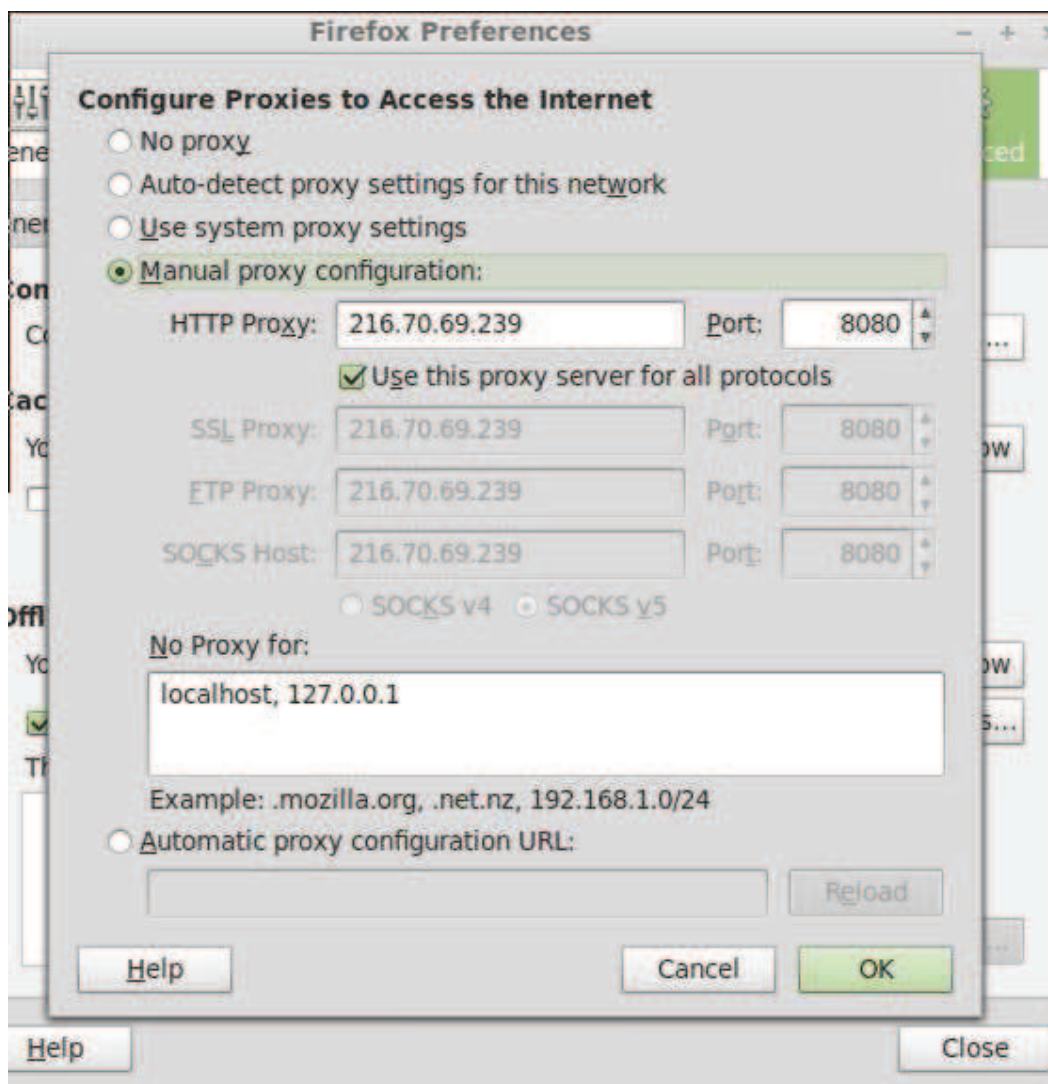
⁵ <http://freegeoip.net>

Postoje brojni „javni anonimni proxy serveri“, koje hostuju entuzijasti širom sveta, i ne samo oni, a liste istih možemo naći na internetu na npr: <http://spys.ru/en> ili <http://anonymousproxy1.org>.

Tako da ako korisnik koji želi da zaštiti svoj identitet od npr. servera/web servisa kome pristupa, to direktno može uraditi tako što će podesiti svoj web browser da koristi željeni anonimni proxy. Tako da ako bi određeni server/web servis želeo da identifikuje/locira korisnika/klijenta po IP adresi istog, dobio bi samo IP adresu proxy servera kroz koji mu se taj klijent obratio. Tako da je taj podatak neupotrebljiv za neku statistiku, ban-ovanje, ciljno reklamiranje ili neku zlonamernu/nelegitimnu akciju prema tom korisniku. Na donjim slikama dat je konkretan primer setovanja najkorišćenijih web browser-a tako da koriste uslugu redirekcije internet saobraćaja kroz anonimni proxy server.



Slika 6. Primer setovanja MS Internet Explorer-a da koristi proxy server



Slika 7. Primer setovanja Mozilla Firefox-a da koristi proxy server

Korišćenje anonimnih proxy servera pruža određeni stepen zaštite identiteta, ali ako se pažljivo razmotri, ovakvo rešenje pruža vrlo nizak stepen zaštite kako identiteta tako i privatnosti, a čak može da bude i izvor ugrožavanja istog.

Očigledna slabost ovog metoda je u tome što paket podataka koji putuje od izvora (pošiljaoca) do anonimnog proxy-ja sadrži podatke o konkretnom pošiljaocu, i može biti presretnut tako što treća strana nadgleda i analizira pakete koji dolaze na anonimni proxy, i time lako identifikuje konkretnog korisnika/pošiljaoca.

Posebna tehnika za zaštitu anonimnosti internet korisnika i njihove privatnosti kao i samog sadržaja podataka koje razmenjuju kroz internet je T.O.R. (The Onion Routing)⁶.

⁶ <https://www.torproject.org/>

Međutim, postoje još dva fenomena često zastupljena na internetu, a vezana za anonimne proxy servere.

Oni se u žargonu nazivaju „honeypot“ (vrč sa medom –prev. aut) i „shugarcane“ (šećerni štapić –prev. aut). To su svojevrsne „zamke“ koje postavljaju npr. vladine agencije u zemljama sa strogom internet cenzurom da bi detektovali i suzbili disidentsku aktivnost, ili u nekim razvijenim zemljama da bi detektovali i suzbili npr. distribuciju dečije pornografije koju počinioči teže da obavljaju preko anonimnih internet proxy servera da bi prikrili svoj identitet. Takođe te zamke mogu biti postavljene i od strane pojedinaca koji time žele da ostvare neku ličnu korist od otkrivanja nečijih privatnih podataka, aktivnosti i sl.

U suštini korisnik koji koristi neki javni anonimni internet proxy server to radi „na slepo poverenje“ da vlasnik tog proxy servera nema „zadnjih namera ili skrivenih motiva“ koji bi ugrozili otkrivanje/zloupotrebu identiteta ili privatnih podataka konkretnog korisnika, a nema nikakav način da to zna.

Čak i ako je na neki način siguran u „legitimnost“ anonimnog proxy servera koji koristi, ne može biti siguran da neka treća strana kojoj je poznato postojanje tog proxy servera, ne „prisluškuje“ sav dolazni saobraćaj prema tom proxy serveru, te time korisnik sebe još više „izlaže kao metu“ na „internet radaru za sumnjive aktivnosti“, bilo prema nekim državnim institucijama što mu je problem ako se na internetu bavi zakonom sankcionisanim aktivnostima, bilo prema zlonamernim pojedncima koji mogu zloupotребiti lične ili poslovne podatke koje korisnik razmenjuje preko interneta.

Postoje i raznolika rešenja koja su namenjena za one korisnike koji bi da instaliraju i koriste sopstveni anonimni proxy.

Karakteristični primeri takvih softverskih rešenja su:

- Privoxy⁷
- Polipo⁸
- Proxomitron⁹

⁷ <http://www.privoxy.org/>, pristupano 21.01.2013.

⁸ <http://www.pps.univ-paris-diderot.fr/~jch/software/polipo>, pristupano 21.01.2013

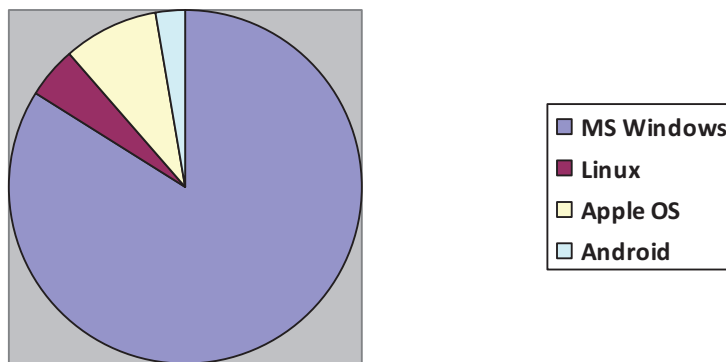
⁹ <http://www.proxomitron.info/>, pristupano 21.01.2013

III.2. Live OS REŠENJA ZA ZAŠTITU PRIVATNOSTI

Osim informacija koje su dostupne kroz sadržaj paketa zbog strukture komunikacionih protkola goreopisanih, postoje i rizici koji potiču sa samog računara/uređaja korisnika.

Ti rizici se ogledaju u ranjivosti samog korišćenog operativnog sistema i aplikativnog softvera koji je instaliran na korisnikovom računaru.

Na grafikonu 1. dat je statistički prikaz strukture operativnih sistema koji se koriste širom sveta za pristup internetu.¹⁰

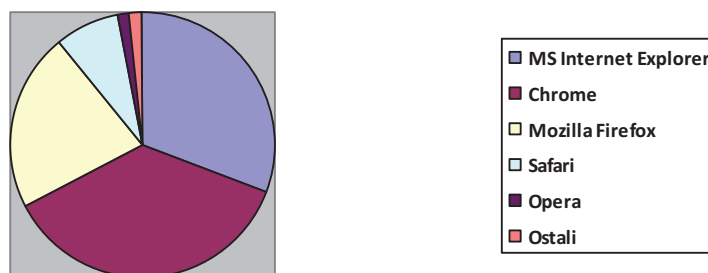


Grafikon 1. –Statistika korišćenja operativnih sistema, decembar 2012.

Na grafikonu 2. dat je statistički prikaz vrsta internet browser-a koje koriste korisnici širom sveta.¹¹

¹⁰ Izvor podataka: http://www.w3schools.com/browsers/browsers_os.asp, pristupano 22.01.2013.

¹¹ Izvor podataka: <http://gs.statcounter.com/#browser-ww-monthly-201112-201212>, pristupano 22.1.2013.



Grafikon 2. –Statistika korišćenja Web browser-a, decembar 2012.

Zaključak koji se nameće je da statistički najveći broj korisnika koristi MS Windows operativni sistem i Internet Explorer web browser. I Windows OS i Internet Explorer su poznati po brojnim bezbednosnim propustima. Ti bezbednosni propusti su raznovrsni ali sa aspekta ovog rada nama su interesantni rizici kojima su izloženi korisnici MS OS-a i/ili Internet Explorer-a koji se povezuju na internet sa računara sa tim OS-om i/ili web browser-om.

Bezbednosni propusti u MS Windows operativnim sistemima su nadaleko poznati, i nemoguće ih je sve pobrojati. Sa svakom novom verzijom Windows-a, Microsoft je objavljivao ogroman broj patch-eva (zakrpa-prev.aut) za korisnike svesne rizika koji su se redovno obaveštavali o istima i instalirali čim se pojave. Takođe, periodično ali ne tako često, Microsoft je objavljivao sumarnu kompilaciju svih patch-eva za konkretnu verziju Windows-a koju nazivaju „service pack“.

Rizici koji „vrebaju“ prosečnog korisnika koji koristi MS Windows i Internet Explorer su toliko brojni da ih ovde nećemo posebno analizirati, već samo napomenuti glavne aspekte istih, te značaj i smisao korišćenja Live OS rešenja.

Glavni rizici po bezbednost podataka prosečnog korisnika leže u razumno velikoj verovatnoći da se na korisnikovom računaru u pozadini izvršava neki maliciozni softver (kao npr. neki KeyLogger ili sličan spyware), koji može da „prepozna“ kada korisnik unosi neku lozinku npr. za logovanje na neki web server/servis ili npr. broj neke kreditne kartice ili slične podatke koji se mogu zloupotrebiti na razne načine.

Ili zamislimo drugi scenario, naročito aktuelan za prosečnog korisnika koji nije IT profesionalac koji nosi svoj mobilni uređaj sa sobom, već rečimo klasičan porodični čovek ili tinejdžer, koji na putu -recimo na godišnjem odmoru ili nekom drugom prilikom, ima potrebu da pristupi svom email nalogu, da proveri stanje na svom bankovnom računu ili izvrši neko online plaćanje, ili prosto da pristupi nekoj socijalnoj mreži. Takav korisnik je upućen na neki „javni računar“ kao npr. u nekom Netcaffe-u, ili sl. Na takvim računarima rizik od prisustva malicioznog softvera je eksponencionalno veći. Samim tim i rizik da će privatni podaci korisnika biti dostupni i zloupotrebljeni od treće strane se eksponencionalno uvećava.

Koliko je ovaj tip rizika rasprostranjen govori npr. jedna afera iz 2005. godine, čiji glavni antagonist je bila SONY korporacija.¹² Naime, krajem oktobra 2005. je nekoliko nezavisnih istraživača obznanilo da je SONY na originalne muzičke CD-ove ugradio sistem za zaštitu od kopiranja sadržaja, koji je totalno bezopasan ako se CD reprodukuje na audio uređaju. Stvar je međutim mnogo drugačija kada se CD ubaci u PC računar na kome je Microsoft Windows. Naime, tom prilikom bi se bez znanja i pristanka korisnika računara automatski instalirao maliciozni softver koji je koristio neke ranjivosti Windows operativnog sistema da bi se „krio“ i onemogućavao korisnika da ga isključi/deinstalira, a pritom mu je jedna od funkcija bila da neke (nikada tačno utvrđeno koje sve) podatke o korisniku šalje SONY korporaciji.

Osim ovoga, tu se „provukao“ još jedan opasniji rizik, zvanično potvrđen i proglašen kao „slučajan propust“, a odnosi se na to da je taj softver koji se „samoinstalirao“ bio u suštini rootkit¹³ koji je omogućavao nekom da preko interneta pristupi vašem računaru tj. podacima i takođe da „preuzme kontrolu“ nad vašim računarom i isti zloupotrebi za svoje namere. Ako bi neki iskusniji korisnik na bilo koji način postao svestan da mu na računaru egzistira softver koji ne želi, u konkretnom slučaju nije bilo moguće regularno deaktivirati/ukloniti taj softver, a ako bi neki napredniji korisnik to i uspeo koristeći više trikova, time bi urušio svoj Windows operativni sistem.

Razmišljajući u kontekstu rizika egzistencije malicioznog softvera na računaru, čijeg prisustva korisnik nije ni svestan, ponuđeno rešenje/kontramera je korišćenje nekog Live OS-a.

Karakterističan primer ovakvog rešenja je Anonym.OS. Razvila ga je firma kaos.theory security research¹⁴ i prezentovala 2006. godine.

Anonym.OS je LiveCD distribucija zasnovana na OpenBSD¹⁵ operativnom sistemu, ali „nadograđen“ sa mnogim bezbednosnim poboljšanjima i setovanjima koje bi inače prosečan korisnik malo verovatno znao da obavi. Dakle pri pokretanju tj. boot-ovanju Anonym.OS-a aktivira se operativni sistem koji je sigurno „čist“ od malicioznog softvera koji potencijalno „vreba“ u pozadini, te se taj rizik realno može eliminisati iz razmatranja. Dakle nebitno na kom/čijem računaru pokrenemo taj Live CD, on podiže operativni sistem učitavajući ga u RAM memoriju računara u celosti, bez ikakvog pristupa memoriji Hard diska računara.

¹² <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/02/AR2005110202362.html>, pristupano 22.01.2013.

¹³ <http://en.wikipedia.org/wiki/Rootkit>, pristupano 22.01.2013

¹⁴ <http://kaos.to>, pristupano 22.01.2013

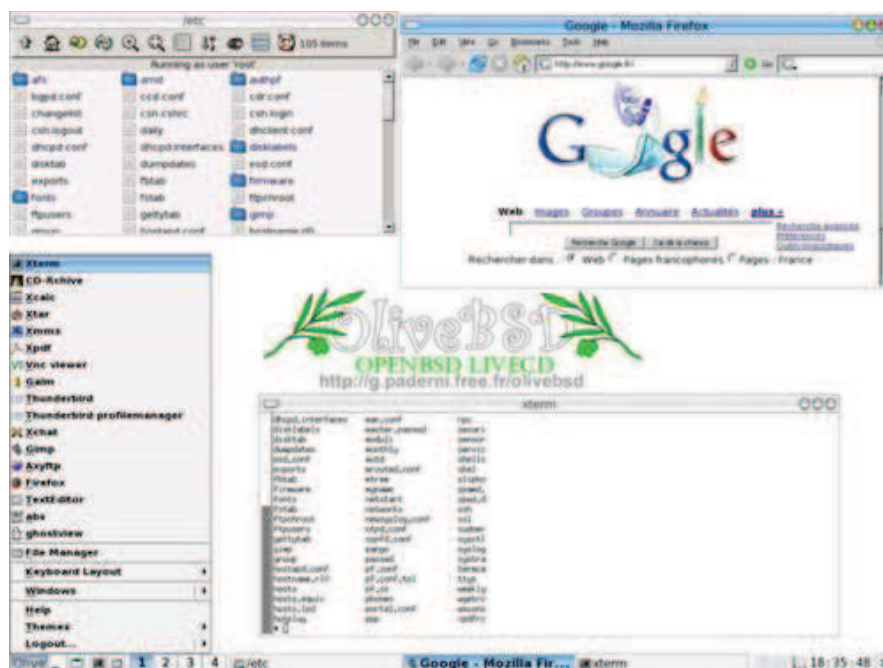
¹⁵ <http://www.openbsd.org/>, pristupano 22.01.2013

Značaj ovakvog (LiveOS) pristupa sa aspekta zaštite privatnosti se odražava na dva bitna načina:

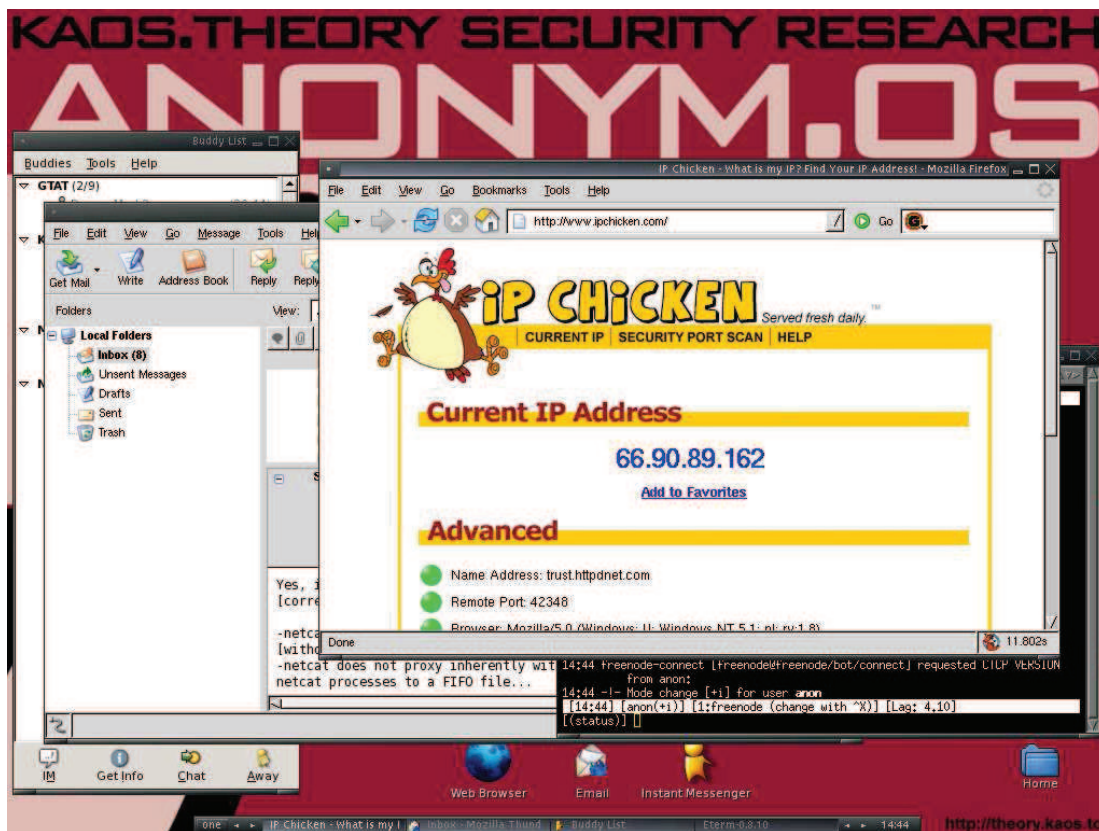
1. Pošto se operativni sistem učitava uvek „svež“, „nekompromitovan“, sa read-only medijuma (CD), nema bojazni od prisustva malicioznog softvera na računaru na kome se pokreće. Ovim se korisnik zaštićen od real-time napada tj. logovanja ili ometanja aktivnosti.
2. Pošto je sav sadržaj operativnog sistema smešten i izvršava se kompletno u RAM memoriji računara, potpuno izolovan od neke trajne memorije računara na kome se izvršava (hard disk), po završetku rada tj. gašenju ili restartu računara **ne ostaju nikakvi tragovi u bilo kom obliku** o bilo kakvim aktivnostima korisnika na tom računaru za vreme trajanja te Live sesije. Ovim je korisnik zaštićen od offline napada tipa naknadne analize korisnikovih aktivnosti i eventualno zaostalih podataka na računaru.

Kritičari ovakvog rešenja ukazuju da takva LiveOS rešenja imaju i jednu nepremostivu manu a to je mogućnost reboot-a računara koji se uslužno koristi kao npr. u netcafé-u i sl. jer tamo te mogućnosti nema, ili nema dostupnog optičkog uređaja.

Dalji razvoj takvih rešenja ide u pravcu stvaranja LiveUSB rešenja umesto LiveCD rešenja, ali pošto je zadnjih godina trend eksponencijalnog porasta broja mobilnih uređaja, dostupnih i tinejdžerima i prosečnim porodičnim ljudima na putu, LiveOS rešenja za zaštitu privatnosti gube na značaju.



Slika 8. Anonym.OS Live screenshot 1



Slika 9. Anonym.OS Live screenshot 2

III.3. PRIVATE/INCOGNITO METODE UGRAĐENE U WEB BROWSER-E

Od 11.9.2000, pa nadalje, naročito u SAD, ali sa efektom „prelivanja“ u ostatku sveta, uvedene su strožije bezbednosne provere i mere zaštite u svim sferama života, pa i u nadzoru elektronskih komunikacija, čemu je na ruku išao i razvoj novih tehnologija i resursa za nadzor elektronskih komunikacija, kao i eksponencijalna ekspanzija svakodneve komunikacije kroz internet, zatim bum „socijalnih mreža“ itd.

Sa druge strane to je rezultiralo „većom izloženošću“ pojedinaca uopšte na internetu znatizeljnim/zlonamernim državnim agencijama/pojedincima. Samim tim, poralo je i interesovanje opšte populacije za zaštitom svoje privatnosti u tim aktivnostima.

Pošto velika većina prosečnih korisnika teži tehnički jednostavnim/nezahtevnim rešenjima, koja ne zahtevaju stručna znanja i veštine, ugradnja mehanizama koji to bar u nekoj meri omogućavaju „jednim klikom“ je prvi put ponuđena u web browser-u Safari na Macintosh računarima 2005. godine. Zatim su i drugi proizvođači web browser-a ponudili tu funkcionalnost u vremenskoj dinamici koja je prikazana u tabeli br. 1.

<i>Datum uvođenja „private“/„incognito“ moda</i>	<i>Web Browser</i>	<i>Tačan naziv te funkcionalnosti</i>
29. april 2005.	SAFARI v2.0	Private Browsing
11. decembar 2008.	Google Chrome v1.0	Incognito
19. mart 2009.	Internet Explorer v8	InPrivate Browsing
30. jun 2009.	Mozilla Firefox v3.5	Private Browsing
3. mart 2010.	Opera 10.50	Private Tab / Private Window

Tabela br. 1 –Dinamika uvođenja „private browsing-a“¹⁶

¹⁶ http://en.wikipedia.org/wiki/Privacy_mode

Na ovaj način korisnik može da se efikasno zaštititi od sledećih oblika ugrožavanja njegove privatnosti:

- „offline“ napadi na njegove lozinke i lične podatke
- Svi cookies i slični sadržaji koji dospeju na računar koji korisnik koristi, su smešteni u zaštićen prostor – „sandbox“, i brišu se po okončanju sesije na internetu.
- Istorija poseta web stranama se uopšte ne beleži i ne ostaje trag o istoj nigde u log-ovima i sl.

Na taj način, računar koji je korisnik koristio ostaje „čist“ od svih tragova korišćenja istog za internet sesiju posle korisnika koji je tu sesiju koristio u private/incognito modu.

Ograničenje ovog pristupa se ogleda u tome što korišćenje ove metode za zaštitu privatnosti ne isključuje mogućnost da na računaru korisnika mimo samog web browser-a postoji neki maliciozni softver koji u pozadini prati i negde beleži kako korisnikove aktivnosti tako i unete lozinke i podatke i sl. Ovaj rizik je naročito izražen tamo gde je korisniku zaštita privatnosti najbitnija tj. na „javnim računarima“.

III.4. OSTALA REŠENJA

Osim gore razvrstanih rešenja, postoje i druga rešenja koja razvijaju raznovrsne kompanije, neka od njih su besplatna, a neka su komercijalna (plaćaju se). U ta rešenja su ugrađene gore navedene tehnike u kombinaciji. Karakteristični primeri tih rešenja su:

- SpotFlux¹⁷
- HotSpot Shield¹⁸
- CyberGhost¹⁹
- COMODO Internet Security²⁰
- ZoneAlarm²¹

¹⁷ <http://www.spotflux.com>

¹⁸ <http://www.hotspotshield.com/en>

¹⁹ <http://cyberghostvpn.com>

²⁰ <http://www.comodo.com/home/internet-security/free-internet-security.php>

²¹ <http://www.zonealarm.com/security/en-us/zonealarm-computer-security-suite.htm>

IV TOR REŠENJE

IV.1. ŠTA JE TOR PROJEKT I KAKO JE NASTAO

Tor projekt je softversko rešenje, namerno ga nazivamo rešenjem jer obuhvata višeslojne i višestruke aplikacije i serverske instance, i implementira se na više fizički udaljenih računara, da bi se postigla željena funkcionalnost.

Tor projekt je rešenje koje se koristi da bi se sa visokim stepenom anonimnosti pristupilo web servisima ili međusobno komuniciralo uz visok stepen zaštite privatnosti razmenjenih podataka koristeći internet kao medijum za tu komunikaciju.

Koristeći Tor ne samo da pojedinci mogu da štite svoj identitet i podatke kao korisnici/klijenti web servisa na internetu, već takođe i provajderi raznih web servisa mogu štititi svoj identitet/lokaciju kao i sadržaje koje pružaju svojim korisnicima koristeći Tor rešenje. Ovaj drugi slučaj je manje zastupljen iz tehnoloških razloga koji ograničavaju performanse web servisa koji bi se štitili na taj način, ali teoretski ostvariv i korišćen od strane pojedinih provajdera web servisa koji imaju takvu potrebu.

Tor projekt je prvobitno nastao kao Onion²² Routing projekat. Onion Routing je nastao pod okriljem ministarstva odbrane S.A.D., konkretno u njihovoj "U.S. Naval Research Lab"²³, a u okviru koje postoji "Center for High Assurance Computer Systems"²⁴.

Autori Onion Routing-a su Michael G. Reed, Paul F. Syverson, and David M. Goldschlag. Onion Routing je patentiran od strane U.S. Navy 1998. Godine²⁵.

Namena tog rešenja je bila da obaveštajcima američke ratne mornarice u inostranstvu omogući da razmenjuju podatke sa svojim obaveštajnim centralama preko interneta, koristeći dakle infrastrukturu javne međunarodne mreže, bez posebne hardverske opreme, a da pritom onemoguće efikasno presretanje, analizu saobraćaja pa čak i detektovanje konkretne aktivnosti koja bi bila predmet nekog konstantnog nadzora. Ovde se misli na "prolazak ispod radara" automatskih sistema za presretanje internet komunikacije kojima raspolaže svaka država, i koja iste koristi za detektovanje, presretanje i samim tim i nadzor one komunikacije koja im je u datom trenutku od značaja.

²² Onion- glavica crnog luka, prev aut.

²³ Istraživačka laboratorija ratne mornarice Sjedinjenih Američkih Država

²⁴ Centar za računarske sisteme visoke pouzdanosti

²⁵ US Patent No. 6266704

Npr. bezbednosnim strukturama neke države je interesantna sva internet komunikacija kao i identitet onoga ko pristupa sajtu www.cia.gov, ili www.defense.gov.

Ako se sistem za automatsku detekciju i nadzor sve komunikacije koju bilo ko u konkretnoj državi ostvaruje na te sajtove aktivira, potpuno je trivijalno otkriti identitet onoga ko razmenjuje podatke “sa stranom od bezbednosnog značaja”, pa time predstavlja potencijalnu bezbednosnu pretnju itd. To se postiže prostim upitom u registar aktivnih IP adresa kod konkretnog web provajdera ako se radi o dinamički dodeljenoj IP adresi nekog privatnog korisnika, ili direktnom identifikacijom korisnika javne statičke IP adrese. Po identifikovanju “počinioca”, isti se može staviti pod intenzivniji nadzor ne samo u smislu njegove celokupne internet aktivnosti. Dakle ovo rešenje je namenjeno prvobitno izbegavanju “internet radara” bezbednosnih službi. Međutim, tu se ne završava priča o funkcionalnostima Tor rešenja. Pomenuli smo da ono štiti u visokoj meri i privatnost podataka koji se razmenjuju. Tako da osim što “internet radari” prate ostvarene konekcije u smislu povezivanja korisnika sa web serverima “od posebnog bezbednosnog interesa”, isti se mogu konfigurisati i za nadzor samog sadržaja podataka koji se razmenjuju bez obzira na odredište. Tor rešenje omogućava da se uspostavi šifrovana komunikacija između korisnikovog računara i interneta i time se izbegne “internet radar” koji bi nadzirao komunikaciju za određene sadržaje.

20. septembra 2002. godine, Roger Dingledine sa MIT-a je objavio inicijalnu verziju Onion Routing rešenja u javnosti[27], i pozvao javno sve zainteresovane entuzijaste da se priključe i omasovljavanjem korišćenja Tor rešenja doprinesu njegovoj što većoj upotrebnoj vrednosti.

Međutim, tada to još nije imalo primenu u široj javnosti. Tek 13. avgusta 2004. godine, na 13. USENIX²⁶ simpozijumu, Roger Dingledine, Nick Mathewson i Paul Syverson prezentuju „drugu generaciju onion routing-a“[28].

U periodu 2004-2005, Tor razvija i finansira Electronic Frontier Foundation²⁷, a od 2005 pa nadalje Tor projekt je postao istraživačko-edukativna neprofitna organizacija pod istim imenom²⁸.

²⁶ USENIX - The Advanced Computing Systems Association, <http://www.usenix.org>

²⁷ Electronic Frontier Foundation - http://en.wikipedia.org/wiki/Electronic_Frontier_Foundation

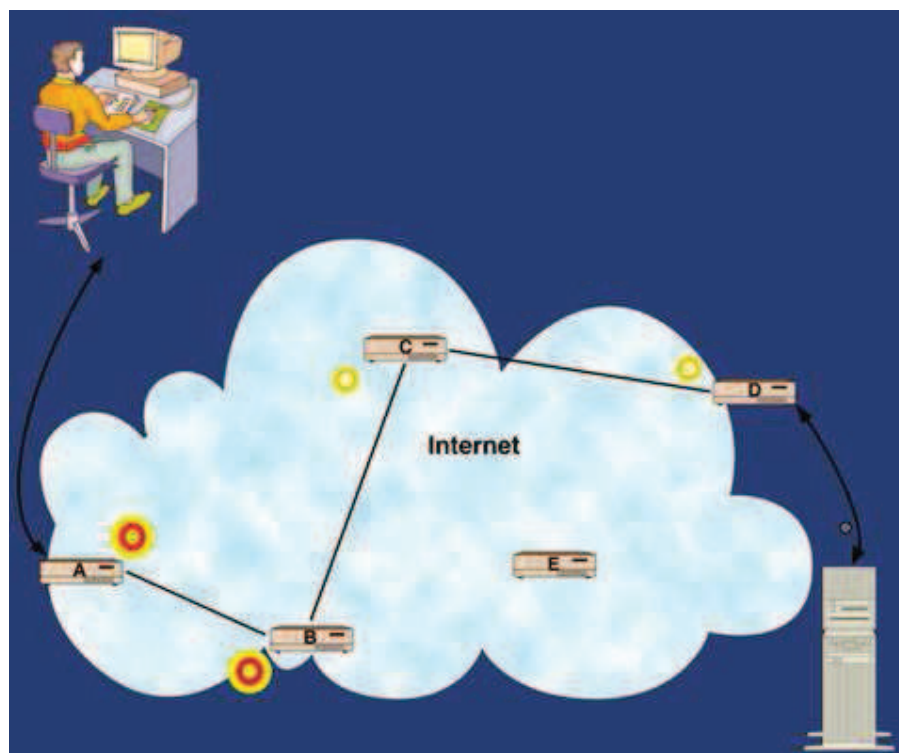
²⁸ Tor Projekt organizacija - <https://www.torproject.org/>

IV.2. KAKO TOR FUNKCIONIŠE

IV.2.1. OSNOVNI PRINCIPI

Tor rešenje nudi izuzetno visok nivo zaštite pojedinog korisnika interneta (u daljem razmatranju koristićemo pojam klijent) kao i privatnosti sadržaja koji klijent razmenjuje sa nekim web servisom/serverom preko interneta. Bilo koji napad tipa analize mrežnog saobraćaja se sreće sa dva praktično nerešiva problema. Prvi je što napadač ne može da utvrdi ni tačno polazište ni tačno odredište pojedinog paketa, a drugi je da je paket višeslojno (višestruko) šifrovan te je praktično nemoguće (ili bar ne blagovremeno) dešifrovati paket i doći do njegove sadržine.

To se postiže tako što se konekcija između klijenta i nekog servera kroz internet ne ostvaruje “direktno”, u smislu da IP paket koji pođe od klijenta putuje kroz regularne internet rutere do servera (i eventualni odgovor od servera nazad do klijenta) sve vreme noseći u svom header-u podatke o pošiljaocu i primaocu. Nego se pribegava tehnici preusmeravanja svakog paketa kroz “Tor mrežu” kako je to uprošćeno prikazano na slici 1.



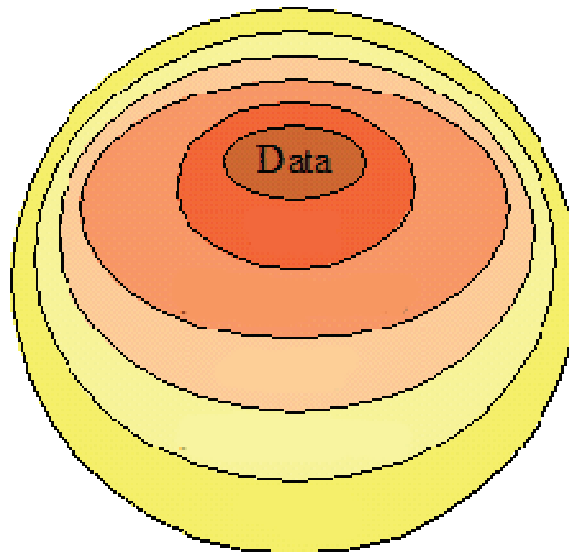
Slika 10. –Uprošćeni prikaz korišćenja Tor rešenja

Dakle, veza se ostvaruje od klijenta do “A” čvora Tor mreže, koji u ovom primeru igra ulogu “ulaznog čvora”. Tu se paket “prepakuje” i šalje po unapred određenoj slučajnoj putanji kroz čvorove “B”, “C” i “D” do odredišta. Bitno je uočiti da u ovom

primeru paket nije putovao kroz čvor "E". Dakle, od "N" dostupnih čvorova, paket će putovati samo kroz neke od njih, kroz "M" čvorova, gde je uvek $M \leq N$. Takođe, eventualni odgovor od servera prema klijentu neće ići istim putem nazad, već sasvim drugom slučajno generisanom trasom, kroz K broj čvorova gde je $K \leq N$, i $K \neq M$. U toj trasi će možda učestvovati neki od čvorova kojim je paket došao do servera, ili neće, što je potpuno prepušteno slučajnosti, kao i redosled kojim će paket proći kroz tih K čvorova.

Takođe, ako realno pretpostavimo da neki napadač može da presretne (što je u praksi sasvim realna mogućnost) mrežni saobraćaj tj. paket podataka koji putuje između dva susedna čvora Tor mreže, njegovom analizom on može samo da ustanovi sa kog poslednjeg čvora je paket krenuo i na koji sledeći čvor se uputio. Ne može nikako iz IP header-a presretnutnog paketa saznati adresu pa time ni identitet i/ili lokaciju pošiljaoca ni adresu konačnog odredišta.

Dodatnu Zaštitu pruža i to što se paket šalje od pošiljaoca već šifrovan do „ulaznog TOR čvora“, i tamo se dodatno šifruje višestruko (M-tostruko, gde je M=broj tranzitnih TOR čvorova kroz koje je projektovano da će paket proći do odredišta) i tako „višeslojno obložen“ u šifri kao sloj u glavici crnog luka, paket kreće na put ka odredištu kroz „Tor oblak“, kao što je ilustrovano na slici 2.



Slika 11. Paket podataka „obložen“ višestrukim šifrovanjem koji se transportuje kroz Tor oblak.

Ovako „ušušani“ podaci su u veoma visokoj meri zaštićeni od dekriptacije, tako da i ako budu presretnuti, u realnom vremenu je prosto nemoguće probiti sve nivoe enkripcije koji „obmotavaju“ sam paket podataka. A u nekom konačnom dugom vremenu koje bi neko i utrošio da dekriptuje paket podataka, to što bi dobio je samo mali delić ukupne razmene podataka tog konkretnog korisnika sa nekim web serverom, tako da je statistički najverovatnije da je tako izdvojeni mali segment podataka praktično neupotrebljiv.

Zbog algoritma kojim Tor rešenje preusmerava pakete različitih klijenata različitim putanjama, sa velikom verovatnoćom će se dogoditi da dva enkriptovana paketa podataka koji uzastopno krenu sa ili stižu ka čvorištu na kome napadač presreće saobraćaj zasigurno nisu potekli sa istog polazišta, i nemaju ni isto krajnje odredište, što čini efikasno presretanje željenog toka podataka virtuelno nemogućim.

IV.2.2. TEORETSKA PODLOGA

Teoretsku osnovu za Tor mrežu kao rešenje za postizanje visokog stepena (u praksi potpun stepen) autonomije je rad Davida Chauma[29] sa Berkli univerziteta, SAD.

On je u svom radu prezentovao rešenje za „anonimnu“ i „privatnu“ razmenu elektronske pošte, uz korišćenje sistema „javnih i privatnih ključeva“. Međutim, originalna premisa u njegovom radu je bila isticanje da u kriptografskom sistemu „javnih i privatnih ključeva“ obe strane u komunikaciji „veruju“ u neku „centralnu certifikacionu treću stranu“.

Idealno bi bilo, kaže on ako bi svaka strana u komunikaciji bila „validno certifikaciono telo“, ne formalno, nego u praksi, tako da svi veruju sebi, i nikome više, čime se isključuje postojanje bilo koje treće strane u komunikaciji kojoj se „veruje“ a koja može praktično da ugrozi anonimnost strana koje komuniciraju i/ili privatnost sadržaja koje razmenjuju.

IV.2.3. RSA ALGORITAM

Jedan od najčešće korišćenih kriptografskih algoritama je RSA algoritam koji je nazvan po početnim slovima prezimena trojice njegovih autora (Rivest, Shamir i Adleman). Princip po kome je razvijen algoritam se može prezentovati kao efikasno rešenje za sledeći problem:

Osoba X na računaru A treba da pošalje poverljiv podatak na server B, svoje kompanije Y.

Ovaj proces se odvija u sledećim fazama:

1. Klijent uspostavlja komunikaciju sa serverom i traži od njega (serverov), „javni ključ“.
2. Server šalje klijentu svoj javni ključ.
3. Klijent kriptuje (šifruje) podatak koristeći dobijeni javni ključ

4. Klijent tako šifrovan podatak šalje serveru.
5. Server dekriptuje (dešifruje) primljeni podatak koristeći svoj tajni ključ.

Ovde ćemo objasniti kako konkretno funkcioniše RSA algoritam do najsitnijih detalja, uz napomenu da ćemo za očigledan primer koristiti besmisleno „slab“ tj. kratak ključ zbog lake (čitljive) demonstracije.

Dakle, idemo po funkcionalnim fazama. Počnimo od toga kako se generiše javni i tajni ključ. U praksi to ne radi server koji vrši komunikaciju, već se specijalizovani tim bavi periodičnim generisanjem (obnavljanjem, osvežavanjem šifre) tih ključeva, a server ih samo koristi.

Prvo je potrebno odabrati **2 prosta broja**. U našem primeru uzećemo brojeve 3 i 11, i uvesti ih kao promenjive **p** i **q**.

-Zatim računamo:

broj $n = p * q = 3 * 11 = 33$, pa $z = (p-1) * (q-1) = (3-1) * (11-1) = 2 * 10 = 20$.

-Zatim se bira **prost** broj **k** koji je manji od **z**, ali pritom **z** NE SME BITI DELJIV sa **k**. U našem primeru uzećemo 7 jer 5 ne zadovoljava kriterijum da **z** (20) nije deljiv sa **k**. Dakle **k=7**.

-Brojevi **n** i **k** su ovom primeru „javni ključ“ servera B. U teoriji RSA algoritma **n** figurira kao „modulus“, a **k** kao „javni eksponent“, „enkripcioni eksponent“ ili samo „eksponent“.[30]

Još nam je potreban i „tajni ključ“. Tajni ključ je broj koji je u matematičkoj korelaciji sa javnim ključem, očigledno, ali se on računa tako da obezbeđuje dovoljan stepen zaštite srazmerno podacima koji se štite (kasnije više o tome) da ga je dovoljno teško (tj. sa prevelikom vremenskom zadržskom u kojoj tajnost prenesene informacije više nema vitalnu vrednost) izračunati.

Dakle tajni ključ se računa (generiše) na sledeći način:

U našem primeru to će biti broj **j** koji se dobija iz sledećih relacija:

$$k * j = x \text{ i za koje važi da je } x \bmod z = 1$$

U našem primeru to bi bilo: $7 * j = x \bmod 20 = 1$, što kao rezultat daje da je $x = 21 \Rightarrow j = 21/7$; **j=3**.

Taj broj **j** je „tajni“ (privatni) ključ servera B. U teoriji RSA algoritma on figurira kao „tajni eksponent“, ili „dekripcioni eksponent“.

Tajni ključ servera B nikada neće biti ni na koji način objavljen ili slat bilo kome spolja. Zato se i zove tajni. Tajnost privatnog tj. tajnog ključa i počiva na toj premisi.

Sledeći korak se događa na računaru A klijenta X, gde se poverljivi podatak za koji ćemo u našem primeru uzeti samo jedan bajt konkretno vrednost **14**(u daljem tekstu ćemo ga označiti velikim slovom **P**), šifruje koristeći dobijeni javni ključ od servera. To se radi prateći sledeći algoritam:

$E = P^k \bmod n$, gde je **E** naš poverljivi podatak, sada u šifrovanom obliku.

Ako ubacimo konkretne vrednosti iz našeg primera u gornju jednačinu dobijamo:

$$E = 14^7 \bmod 33$$

Što je ako upotrebimo digitron: **$E = 105413504 \bmod 33 \Rightarrow E = 20$** .

Dakle, klijent A sa svoga računara X na server Y šalje šifrovanu poruku koja u našem primeru sadrži samo jedan bajt vrednosti 20.

Server B, kompanije Y, prima šifrovanu poruku 20 i dešifruje je koristeći svoj „tajni“ (privatni) ključ **j=3** (iz našeg primera) na sledeći način:

Dekripcioni algoritam tj. formula je sledeća:

$$P_{(\text{izvorna poruka})} = E^j \bmod n$$

Što ako ubacimo vrednosti iz našeg primera daje sledeći rezultat:

$P = 20^3 \bmod 33 \Rightarrow P = 8000 \bmod 33 = 14$. Dakle dobili smo tačan dešifrovani tajni podatak.

Ovde je bitno razmotriti koliko je ovaj metod pouzdano bezbedan za prenos poverljivih informacija, u smislu da je nekom napadaču sa strane moguće da presretne i da sazna javne ključeve servera, kao i samu šifrovanu poruku. Međutim, algoritam je tako dizajniran da čini izuzetno vremenski zahtevnim pokušaj dešifrovanja presretnute šifrovane poruke bez poznavanja „tajnog“ (privatnog) ključa. U praksi se ne napada sam šifrat, nego javni ključ, budući da je taj „tajni ključ“ u matematičkoj korelaciji sa javnim ključem. Kako? Pa ako pogledamo naš primer od početka, Prvi deo javnog ključa **n** je direktan matematički rezultat proizvoda dva prosta broja **p** i **q**. A drugi deo javnog ključa **k** se računa iz **z**, koji je takođe matematički derivat brojeva **p** i **q**. A tajni ključ **j** je derivat brojeva **k** i **z**, koji su, kako smo malopre naglasili, derivati brojeva **p** i **q**. Dakle sledi da je **j** takođe izveden iz **p** i **q**.

Dakle ako napadač hoće da dođe do tajnog ključa, on će pokušati da poznatu mu vrednost n razloži na odgovarajuće p i q , i iz njih generiše j . Ovo je u našem primeru izuzetno lako jer za $n=33$, postoji samo jedna moguća kombinacija 2 prosta broja čiji proizvod daje tu vrednost a to su 3 i 11 što i jesu naši polazni p i q . Daljom direktnom primenom javno poznatog RSA algoritma, napadač će izgenerisati z, k pa j .

Međutim, u realnoj praksi n i k nisu tako mali brojevi kao ovi koje smo koristili u primeru da bi matematika bila što lakša i što preglednija. RSA Laboratories je čak sve do 2007. godine objavljivala redovno pojedine primerke delova generisanih javnih ključeva (broj n) iz našeg primera koji nisu nikada korišćeni u realnom životu, već isključivo za svrhe testiranja, gde je važila i bila isplaćivana novčana nagrada onome ko prvi izvuče ispravne p i q iz datoga n . Npr. Jedan od tih primera je jedan 193-cifarni broj:

$n=3107418240490043721350750035888567930037346022842727545720161948823206$
 $4405180815045563468296717232867824379162728380334154710731085019195485290$
 $07337724822783525742386454014691736602477652346609^{29}$

Taj n je jedan tim istraživača ispravno „razbio“ na njegove p i q koji su:

$p=1634733645809253848443133883865090859841783670033092312181110852389333$
 $100104508151212118167511579$

$q=1900871281664822113126851573935413975471896789968515493666638539088027$
 $103802104498957191261465571$

Istraživački tim koji je uspešno razbio ovaj kod je objavio da su „potrošili“ 30 godina procesorskog vremena jednog 2.2GHz-Opteron procesora. A ovo je primer „srećnog pogotka“, jer je istom tom timu prethodno razbijajući jedan 663-bitni ključ, trebalo 3 meseca neprekidnog rada klastera od 80 2.2GHz-Opteron procesora što je ekvivalent od otprilike 55 godina rada jednog takvog procesora.

²⁹ <http://www.rsa.com/rsalabs/node.asp?id=2093#RSA640>

IV.3. TOR REŠENJE –ANALIZA „SLOJ PO SLOJ“

Kao što smo videli Tor rešenje je bazirano na dve osnovne funkcionalnosti:

- Višestruka (možda je tačnije reći višeslojna) enkripcija paketa podataka
- Nelinearna putanja paketa kroz „Tor mrežu“ koja je plus striktni simpleks u ravnopravnoj dupleks komunikaciji.

IV.3.1. ENKRIPCIIJA/DEKRIPCIIJA PAKETA KROZ TOR MREŽU

Kada neko sa tačke A (klijent) hoće koristeći Tor rešenje da uspostavi komunikaciju i razmeni neke podatke sa serverom ili nekim drugim klijentom na tački B, ta komunikacija niti počinje niti se odvija sve do kraja iste direktno. Dakle po iniciranju konekcije gde klijent sa tačke A „ulaznom Tor čvoru“ saopštava kroz sigurnu konekciju (znači enkriptovano na gore opisani način) i krajnjeodredište i sadržaj paketa podataka.

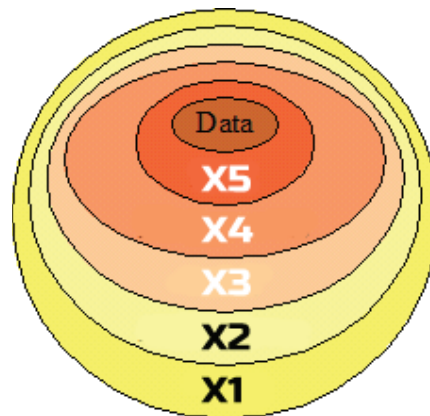
Zatim se po posebnom algoritmu koji je ugrađen u Tor rešenje bira slučajan niz Tor čvorova kroz koje će paket biti poslat do krajnjeg odredišta. Pritom ulazni čvor uspostavlja konekciju sa svakim od tih čvorova i dobija njihove javne ključeve te inicijalni paket podataka prepakuje, analogno kao kada bismo želeli da anonimno pošaljemo klasično poštansko pismo sa tačke A u tačku B, preko „mreže jataka“, ali tako da ni jataci ne znaju za polaznu tačku ni odredišnu tog pisma kao ni sadržaj pisma. To ćemo postići tako što ćemo originalno pismo kovertirati i adresirati na krajnjeg primaoca. Ali nećemo pisati adresu izvornog pošiljaoca na tu kovertu. Zatim ćemo za adresu pošiljaoca navesti našeg jataka X_n , i kovertirati tu celu kovertu u novu kovertu gde ćemo za primaoca navesti adresu našeg jataka X_n , a kao pošiljaoca adresu našeg jataka X_{n-1} . I taj proces ćemo ponavljati sve dok ne budemo imali kovertu u kojoj su kovertirane sve naše koverti jedna u drugoj, a na toj poslednjoj koverti u kojoj su sve ostale kao adresu primaoca navešćemo adresu našeg jataka X_1 , a adresa pošiljaloca će biti naša adresa.

E sad, ako se bojimo da u pošti postoji zavera da neko presreće naša pisma ili prati kome mi pišemo, ako pogleda kovertu u polaznoj pošti videće samo adresu jataka X_1 .

Analogno tome, priča se dalje linerano razvija kada koverta stigne na adresu jataka X_1 , pa on otvori kovertu i sada novu kovertu koja je bila unutra gde je navedena njegova adresa kao adresu pošiljaoca pošalje jataku X_2 , koji ponavlja postupak sve do jataka X_n koji će poslati poslednju kovertu na krajnje odredište.

Time smo sprečili da iko u pošti može da dovede u vezu direktno pošiljaoca i primaoca, a za ovaj segment razmatranja je bitno uvesti analogiju da je sadržaj svakog pisma i adrese na koverti koja je namenjena svakom jataku X_i u nizu šifrovana sa javnim ključem K_i i koju može da dešifruje samo jatak X_i sa svojim privatnim ključem. Tako da

ako bi neko „u pošti“ (naša analogija za Internet tj. javnu mrežu) otvorio kovertu bez odgovarajućeg ključa ne bi mogao da pročita ni sadržaj pisma ni adrese pošiljaoca/primaoca iz unutrašnjih koverti. Ovo je ilustrovano na slici 3.



Slika 12. Ilustracija kako je paket podataka (Data) višeslojno šifovan kao slojevi crnog luka.

Bitno je pritom naglasiti i sledeće: Na svakom tranzitnom Tor čvoru paket se dešifruje (samo jedan sloj) i prosleđuje do sledećeg čvora sa slojem šifre manje. Ovo dodatno otežava nekom napadaču da analizira paket. I na samom kraju kada paket napusti izlazni Tor čvor, on biva totalno „oljušten“ od dodatnih slojeva, i u izvornom obliku prosleđen konačnom odredištu. ALI, bitno je naglasiti da je možda originalno inicirana korespodencija između originalnog pošiljaoca i krajnjeg primaoca takođe šifrovana, tako da paket ni u jednom trenutku ne putuje kroz javnu mrežu (internet) u otvorenom obliku.

Takođe samim tim, i fizička struktura (veličina, checksum, itd) samog paketa koji je došao na neki čvor i „istog tog paketa“ koji nije više isti po toj fizičkoj strukturi se značajno razlikuju i nemoguće je pratiti paket efikasno od jednog do drugog Tor čvora praćenjem kretanja „istog“ paketa po spoljašnjim karakteristikama.

IV.3.2. REDIREKCIJA PAKETA KROZ TOR MREŽU I NAČIN POSTIZANJA ANONIMNOSTI

Kao što smo u prethodnom primeru naveli, Tor rešenje predviđa slanje paketa podataka kroz više „čvorova“ u cilju „zametanja traga“, tj. onemogućivanja efektivnog praćenja toka putovanja paketa koje bi za krajnji cilj imalo tačno identifikovanje pošiljaoca i primaoca tog paketa podataka.

Ovo važi dvojako. Istovremeno sakriva identitet kako pošiljaoca nekog paketa podataka tako i primaoca. To naravno ostavlja širok prostor za razne zloupotrebe tipa hakerske napade na pojedine servere, gde napadnuti server ne može da identifikuje izvor napada, već kao napadača vidi poslednji „izlazni“ Tor čvor sa koga je neki paket koji je napadač uputio stigao do servera. Ako bi server pokušao da se zaštiti od napada tako što bi ignorisao ili odbijao pakete podataka ili odbijao konekcije sa tim entitetom sa interneta kao drugom stranom (izlaznim Tor čvorom preko koga je problematični paket stigao), efektivno ne bi postigao ništa jer će već sledeći paket stići nekom drugom nasumičnom rutom kroz Tor mrežu sa nekog sasvim drugog Tor čvora koji će ovoga puta biti izlazni, i tako u nedogled u praksi.

A napadač koji bi želeo da prati i nadzire nečiji internet saobraćaj bilo nekog klijenta tj. pojedinca koji je iz raznoraznih razloga interesantan tom napadaču, ili nekog servera koji se nadzire iz istih razloga, bio bi onemogućen da to učini efektivno, jer nikada na svome „internet radaru“ ne bi uspeo da detektuje paket podataka koji u svom IP header-u sadrži ciljanu adresu pošiljaoca i/ili ciljanog primaoca paketa.

Takođe su i „Tor čvorovi“ u Tor mreži anonimni, u smislu da pošiljalac paketa podataka ne može da utiče na izbor čvorova koji će biti aktivirani „u lancu“ transmisije njegovog paketa ka odredištu, pa samim tim i ne zna i ne može znati kojim putem će njegov paket podataka putovati do njemu (pošiljaocu) poznatog odredišta.

Ovde je bitno naglasiti još jednu bitnu osobinu kako je adresiranje paketa „spakovano“ u višestrukoj ljušturi enkripcije. Naime, kada Tor-ovan paket prolazi kroz tranzitni čvor X_i on po prijemu paketa „ljušti“ najviši (spoljni) sloj enkripcije tako što primenom svoga tajnog ključa dešifruje paket u toj meri da iz „oljuštenog sloja“ dobije IP adresu sledećeg X_{i+1} -tog Tor čvora kome treba da prosledi paket. Ovo je potpuno analogno našem gore opisanom primeru sa „kovertom u kovrti“.

Naravno iz samog IP headera primljenog paketa on može znati IP adresu prethodnog Tor čvora, ali ne dalje, tj. nema načina da sazna odakle je taj paket stigao do prethodnog čvora, ni koliko čvorova je prošao pre njega, kao ni kroz koliko čvorova posle njega još treba da prođe paket podataka do odredišta kao ni adresu odredišta.

Analogno onoj priči sa jatacima i pismima, i-ti jatak samo može da zna identitet i-1-tog jataka, i i+1-tog jataka, tj. onoga od koga je primio pismo, i sledećeg kome on prosleđuje pismo. Ali pošto on baca kovertu u kojoj je dobio pismo onaj i+1-ti jatak više

nema nikakvo saznanje o i-1-tom jataku, i tako niz ceo lanac do konačnog jataka tj. primaoca pisma.

IV.3.3. ALGORITAM RUTIRANJA PAKETA KROZ TOR MREŽU

Algoritam koji definiše putanju za svaki paket podataka koji putuje kroz Tor mrežu u bilo kom smeru ima nekoliko bitnih karakteristika da bi efikasno onemogućio praćenje paketa od polazišta ka odredištu i/ili nazad. To su:

1. Algoritam je **nedeterministički**, što znači da će dati totalno drugačiji slučajni niz Tor čvorova za transit paketa kao rezultat višestrukog planiranja rute paketa sa istovetnog polazišta ka istovetnom odredištu.
2. Broj tranzitnih čvorova za transport pojedinog paketa kroz Tor mrežu **variraće svaki put**, a taj broj će uvek biti između minimalnog i maksimalnog broja čvorova zadatih kao fiksni parametri u algoritmu.

Pri inicijalizaciji konekcije kao i svakog Tor čvora, kao i u regularnim intervalima svi Tor čvorovi razmenjuju informacije kako o sebi susednim čvorovima, tako i o graničnim čvorovima Tor mreže, da bi bili u toku sa aktuelnim stanjem i u funkciji, i prilagođavali se tekućim izmenama na mreži.

Za generisanje rute projektanti Onion Routinga inicijalno su eksperimentisali sa sledećim algoritmima:[31]

-Algoritam čvora posrednika:

U ovom algoritmu, bi se prvo po nekom slučajnom generatoru birao neki čvor za „centralnog posrednika“, gde je bitan uslov da on nije ni polazište ni odredište paketa. Zatim bi se formirala najkraća ruta od polazišta paketa do tog čvora, i zatim najkraća ruta od tog čvora do odredišta. Onda bi se proveravala ispunjenost uslova da je ukupan broj „koraka“ tj. ukupan broj čvorova od polazišta do odredišta ovako odabran veći od minimalnog propisanog broja koraka, i manji od maksimalnog propisanog broja koraka. Ako je i ovaj zadnji uslov ispunjen, ruta je formirana. U suprotnom, taj slučajno odabrani čvor se dodaje u tabelu „neodgovarajućih tranzitnih čvorova“, i algoritam počinje ponovo da se izvršava birajući novi čvor kao predlog za „centralnog posrednika“. I opet se ispituju gore navedeni uslovi ako je prvenstveno zadovoljen uslov da novoizabrani predloženi centralni posrednik već nije evidentiran u tabeli neodgovarajućih.

-Algoritam slučajne šetnje:

Ovde umesto bitanja jednog centralnog tranzitnog čvora i generisanja puta od njega ka polazištu i odredištu, ovaj algoritam daje dosta raznolikije rezultate. Princip je da se ovde prvo definiše neka slučajna dužina dela putanje. Zatim se „baca novčić“ da se odredi da li se računa deo putanje zadate putanje od polazišta ili od odredišta. Kada se ovo odredi, onda se bira slučajni čvor koji će biti sledeći čvor posrednik. Ali pošto on najverovatnije nije susedan sa polaznim/odredišnim čvorom, proverava se da li je broj „koraka“ da se stigne do njega manji ili jednak zadatoj dužini dela putanje. Sve dok je manji od tog broja ovaj deo algoritma se ponavlja i dodaju se dodatni segmenti tom delu putanje dok se ne dostigne zadata dužina ili sve dok bi dodavanje nove deonice prekoračilo zadatu dimenziju. Tada se formirana deonica „usvaja“, novčić se baca ponovo i postupak se ponavlja dok se ne formira cela putanja od polazišta do odredišta. Ovaj drugi algoritam daje 13 puta raznovrsnije putanje u odnosu na prvi algoritam, kažu autori.

IV.4 TOR REŠENJE U PRAKSI

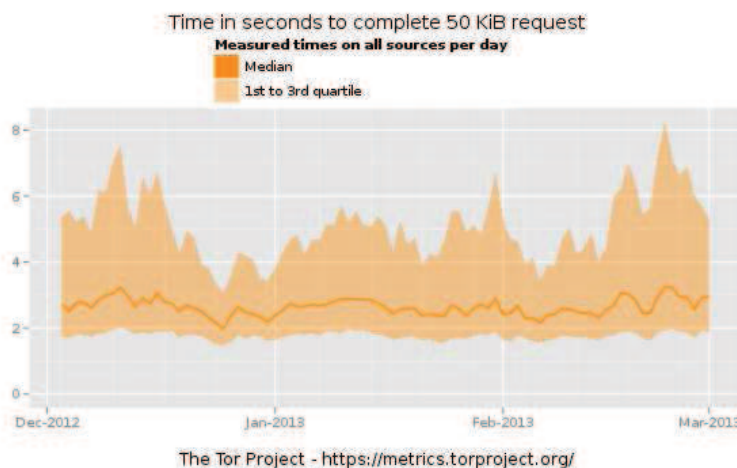
IV.4.1. STATISTIKA KORIŠĆENJA TOR REŠENJA

Od kada je Onion Routing zaživeo u javnosti, ne samo da je moguće doći do kvantitativnih podataka o korišćenju istog, nego čak i do dosta detaljnih kvalitativnih podataka o Tor čvorovima. Ovi podaci nikako ne ugrožavaju anonimnost/privatnost korisnika Tor rešenja, već naprotiv doprinose povećanju bezbednosti na Tor mreži.

Ovo funkcioniše na taj način što su svi Tor čvorovi, izuzetno brojni, sistematski opisani i podaci o njima su zvanično dostupni. Tu postoje razni web servisi³⁰ koji se bave analiziranjem Tor čvorova u realnom vremenu i objavljuju podatke o njima, tako obaveštavajući korisnike Tor-a o legitimnim Tor čvorovima, i eventualno o „podmetnutim presretačima“, koji bi imali vrlo ograničenu mogućnost da išta otkriju jer kao što smo prethodno objasnili jedan jatak u nizu samo zna adrese susednih jataka, ali ne i sadržinu samog podatka koji prenosi kao ni izvornog pošiljaoca odnosno konačno odredište.

Takođe što se tiče kvantitativne statistike, ovde ćemo samo prikazati neke od aktuelnih razmera korišćenja Tor rešenja.

Na grafikonu 3. prikazano je vreme trajanja transfera paketa podataka veličine 50Kb kroz Tor mrežu³¹. Podaci se dnevno ažuriraju.



Grafikon 3. – Prosečno vreme transporta paketa kroz Tor oblak

³⁰ <http://torstatus.blutmagie.de/>

³¹ <https://metrics.torproject.org/performance.html>

Na ovom grafiku možemo uočiti dve izuzetno interesantne stvari.

Prvo, Tor mreža zahvaljujući sve većem obimu učesnika u korišćenju iste ima sasvim pristojne performanse u odnosu na stepen zaštite koji nudi.

Drugo, Ako pogledamo vremensku osu, izuzetno je interesantno uočiti da je „zagušenje“ tj. opterećenje, tj. intenzitet korišćenja Tor mreže simptomatično opada u vreme praznika npr. božića koji je lako uočiti na ovom grafikonu.

To nas navodi na zaključak da se Tor pretežno koristi za poslovnu upotrebu, jer u vreme praznika nivo intenziteta opada drastično... Očigledno se u razvijenom svetu industrijskoj špijunaži i kontrašpijunaži, kao i poslovnim tajnama pridaje mnogo veći značaj nego na našim prostorima.

Takođe, ako globalno posmatramo ceo svet, ima država u kojima je pristup internetu ili određenim internet sadržajima striktno cenzurisan. U tim državama je najveći broj individualnih korisnika Tor rešenja koji na taj način pokušavaju da izbegnu tu cenzuru i/ili detektovanje od strane državnih organa da pristupaju sankcionisanim sadržajima ili šalju informacije koje se strogo cenzurišu iz političko/bezbednosnih razloga. Te bezbednosne službe pokušavaju očigledno da spreče korišćenje Tor rešenja, a Tor zajednica stalno uvodi nove kontra-kontramere da omogući onima koji to žele da koriste Tor i pored toga[32]. Te države u vreme pisanja ovog rada su(rangirane po nivou intenzivnosti cenzurisanja korišćenja Tor rešenja):

1. Sirija
2. Iran
3. Moldavija
4. Kina
5. Tanzania
6. Vijetnam
7. Gibraltar
8. Južna Koreja
9. Malawi
10. Tadžikistan

Ovde možemo da uočimo da spisak ne oslikava „Top 10 nedemokratskih država –diktatura“, već i neke države za koje važe da pripadaju „demokratskom svetu“, kao npr. Gibraltar (Britanska kolonija na jugu Španije), ili Južna Koreja?!?

IV.4.2. KAKO KORISTITI TOR REŠENJE ZA SOPSTVENE POTREBE

Svako ko bi želeo da koristi Tor rešenje da bi zaštitio svoju anonimnost i/ili privatnost svojih podataka, može sa zvaničnog sajta Tor projekta³² da preuzme softverski paket koji će sve automatski setovati i omogućiti laiku da bude zaštićen punom snagom Tor rešenja. Običnom ad-hoc korisniku je potreban Tor-Browser bundle paket. On je ukupne veličine manje od 30Mb i veoma brzo se skida sa interneta. Zatim se pokreće „Start Tor Browser.exe“ aplikacija. Na slici 13. prikazan je osnovni kontrolni ekran „Vidalia Control Panel“ koji se prvi otvara i po uspostavljanju veze sa Tor mrežom, pokreće Web browser koji je na Mozilla Firefox platformi, ali specijalno prilagođen da u maksimalnoj meri koristi Tor rešenje za zaštitu korisnika.



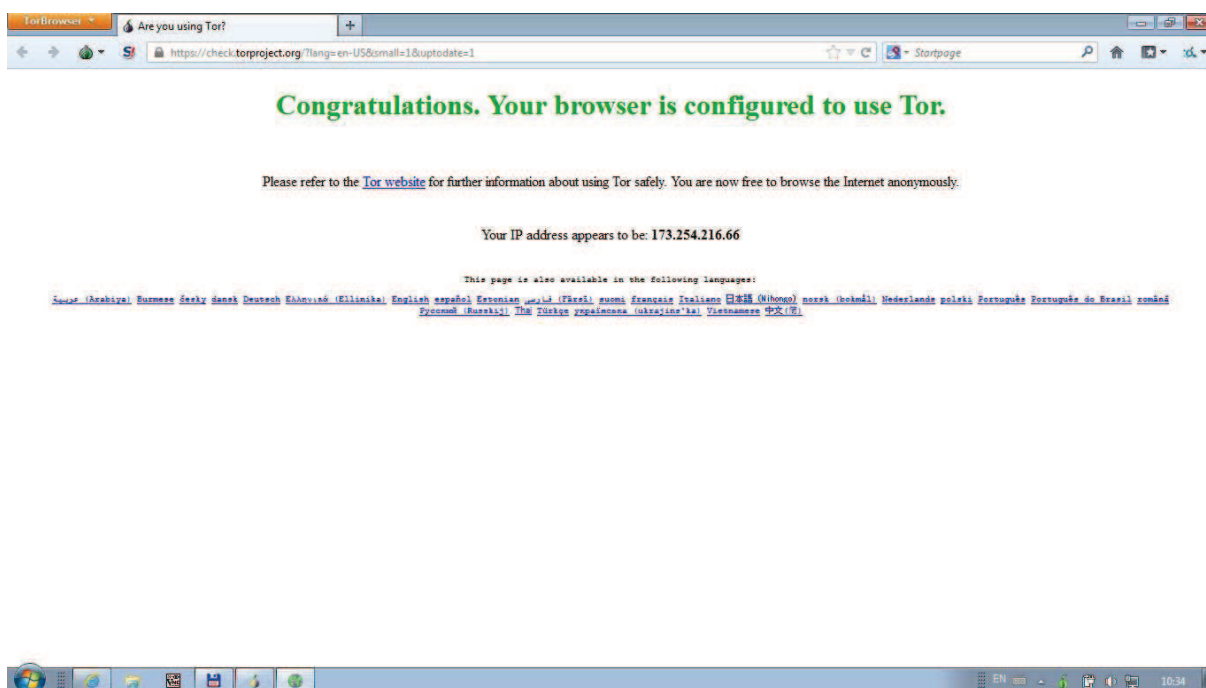
Slika 13. Kontrolna aplikacija Tor-a na PC računaru.

Ovde je posebno interesantna opcija „Setup relaying“, gde korisnik može da bira da koristi Tor rešenje strogo kao klijent, ili da istovremeno postane i Tor čvor za ostale korisnike Tor mreže, a posebno kao opcija je da bude „izlazni čvor“, gde će se onda IP adresa tog korisnika pojavljivati kao polazište odredišnoj strani, što može prouzrokovati brojne probleme kako praktične, tako i zakonske ako neko zloupotrebi Tor mrežu i baš

³² Zvanični sajt Tor projekta: <https://www.torproject.org/download/download.html.en>

preko korisnikovog čvora objavi ili poseti neki sadržaj vezan za npr. dečiju pornografiju i sl. Za one korisnike koji bi želeli da se aktivno uključe u Tor projekat i da omoguće korisnicima Tor rešenja da preko njihovog računara/IP adrese napuštaju Tor mrežu, trebalo bi da se dodatno informišu o dobroj praksi da bi se što efikasnije zaštitili od takvih zloupotreba³³.

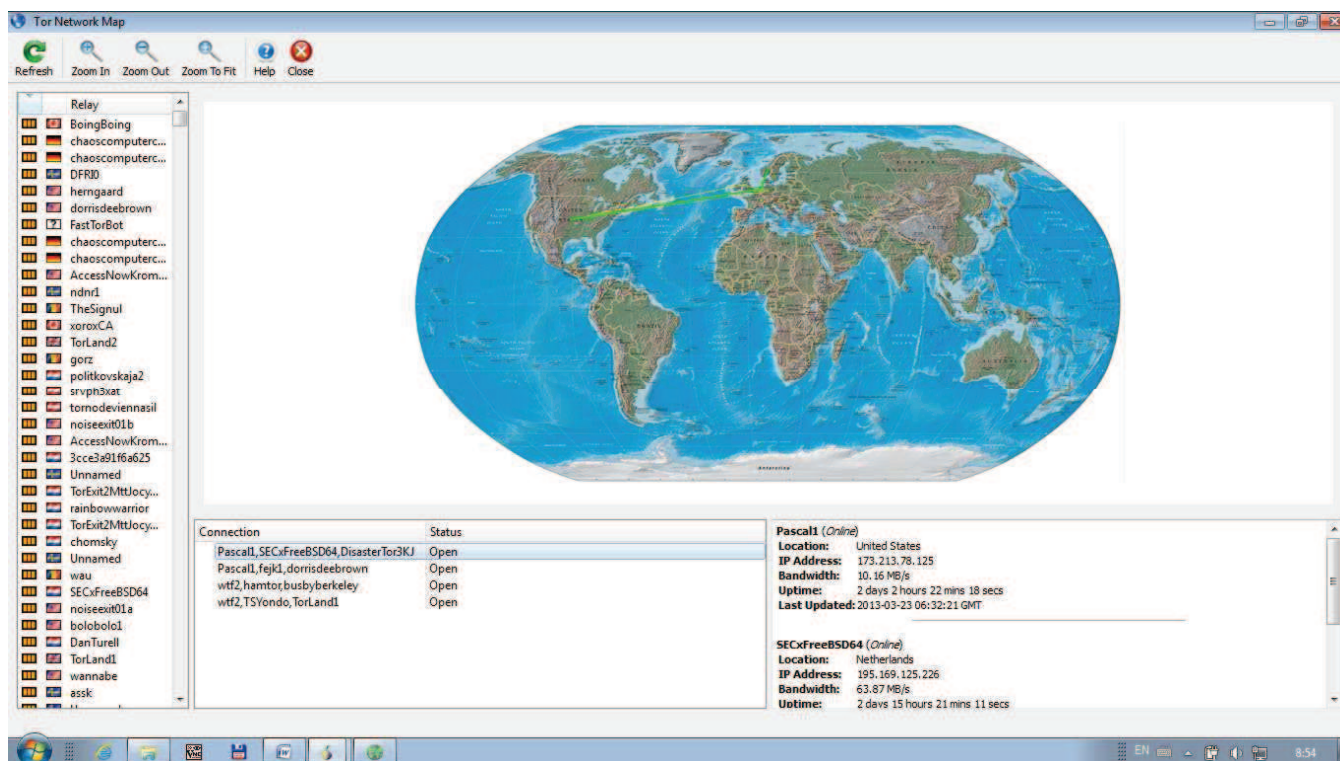
Prosečan korisnik računara, bez naprednog tehničkog znanja je dovoljno da download-uje i pokrene Tor, i sve ostalo sam Tor odradi za njega. Dakle, setuje Tor putanju za njega, i po uspešnom uspostavljanju veze sa Tor mrežom automatski se pokreće „Tor browser“ koji je napravljen na osnovi Firefox-a, a takav mu je i korisnički interfejs. Na slici 14. Je prikazan početni ekran Tor browser-a koji vas odmah obaveštava o vašem „virtuelnom identitetu“ tj. IP adresi sa koje „izlazite na internet“, umesto sa svoje.



Slika 14. Početni ekran Tor Browser-a

Dakle svako ko monitoruje vašu aktivnost može da je prati unazad do te IP adrese koja je u stvari IP adresa izlaznog Tor čvora, tj. računar koji se fizički nalazi negde sasvim drugde, najverovatnije u drugoj državi ili čak kontinentu. Mapu vaše konkretne „putanje“ kroz Tor mrežu možete da vidite aktivirajući „View the Network“ ikonicu u Vidalia control panel-u, i dobićete ekran kao što je prikazan na slici 15.

³³ Tor Izlazni čvor-praktični aspekti: <https://blog.torproject.org/running-exit-node>



Slika 15. Detaljni prikaz sa grafičkim prikazom uspostavljene Tor putanje

Za one koji bi samo da budu korisnici Tor rešenja, bitno je poštovati sledeća pravila:

1. Korisite isključivo Tor Browser.

On je već pre-konfigurisan za vašu maksimalnu bezbednost.

2. Ne uključujte niti instalirajte browser plugin-ove.

Flash, RealPlayer, Quicktime, Adobe PDF I slični plugin-ovi mogu predstavljati veoma verovatan rizik po vašu anonimnost pre svega, jer interaktivni sadržaji podrazumevano ostvaruju vezu sa serverima tih sadržaja direktno mimo Tor mreže. A time je vaš identitet izložen.

3. Koristite https verzije web sajtova kad god je to moguće.

Tor rešenje šifrjuje sav sadržaj dok on putuje kroz Tor mrežu. Međutim da li će sadržaj biti šifrovan i kada napusti Tor mrežu u poslednjem koraku prema odredištu, zavisi od samog odredišta. Dakle, preferirano koristite https sajtove za razmenu poverljivih podataka.

4. NIKADA ne otvarajte dokumente koje ste skinuli sa interneta dok ste online.

Ovo se posebno odnosi na .DOC ili .PDF dokumente jer u njima mogu biti sadržane reference na neke internet sadržaje, a koji će direktno mimo Tor mreže pristupiti tim sadržajima, čime će biti dostupna vaša prava IP adresa bilo kojoj zainteresovanoj trećoj strani. Dakle, kada treba da otvorite takva dokumenta, obavezno to uradite ili kada se

offline, ili u nekoj virtuelnoj mašini pokrenutoj na vašem računaru bez mrežne konekcije, ili recimo koristeći neko Live OS rešenje kao što je Tails³⁴.

5. Koristite Tor relejne mostove za ostvarivanje konekcije na Tor mrežu kad god je to moguće.

Iako Tor savršeno štiti vašu anonimnost prema spoljnom svetu i privatnost vaših podataka, činjenica da koristite Tor može biti dostupna vašem ISP-u, a samim tim i nadležnim službama u vašoj državi, tj. u državi u kojoj se konektujete na Tor mrežu. Ako vam ovo predstavlja rizik ili problem, to možete izbeći tako što ćete se prvo konektovati na neki anonimizirajući proxy, pa preko njega na Tor npr, ili korišćenjem „Tor relejnih mostova“ koji su Tor čvorovi koji nisu na zvaničnoj listi u Tor katalogu, koji je javno dostupan, pa bi neko mogao da nadzire vaše konektovanje na iste.

³⁴ Tails Live OS zvanični websajt: <https://tails.boum.org/>

IV.4.3 TOR REŠENJE ZA WEB SERVICE

Osim za zaštitu anonimnosti pojedinačnih korisnika, Tor nudi rešenje i za web servere/web servise koji bi da budu anonimni, i da zaštiti njihovu privatnost. Ta opcija se naziva „Hidden services“ – skriveni servisi. Počev od 2004. godine to je standardno podržano u Tor mrežama.

Konkretno tu se kroz Tor mrežu krije lokacija (IP adresa) nekog internet servera (internet servisa) što onemogućava kako praćenje aktivnosti istog, tako i identifikovanje korisnika istog. U principu se radi takođe o Tor čvoru ili Tor releju na kome je pokrenut poseban serverski softver koji opslužuje svoje korisnike.

Tim serverima je moguće pristupiti **isključivo** kroz Tor mrežu, jer se njihove lokacije sadrže u pseudo TLD³⁵[33] koji čine svojevrsni „darknet“.

Tor rešenje će ovde dvojako zaštititi i server i pojedinog klijenta jer paket tj.konekcija ne napušta nikada Tor mrežu. Ovo takođe znači da se ti serveri uopšte ne moraju nalaziti na javnim IP adresama, već mogu biti hostovani bilo gde i iza firewall-a ili NAT-ovani npr.

Ove hidden-services najčešće koriste međunarodne organizacije za zaštitu ljudskih prava, ili servisi kao što je odnedavno jako popularni WikiLeaks³⁶ i sl.

³⁵ TLD – Top Level Domain, prim. aut.

³⁶ Zvanični sajt Wikileaks blog-a:<http://wikileaks.org/>

IV.5. DOKUMENTOVANE SLABOSTI TOR REŠENJA

Od kada se Tor rešenje koristi u praksi, bili su brojni sistematski i pojedinačni pokušaji da se pronađu i iskoriste eventualne slabosti u Tor rešenju. Kao prva sistematska slabost je mogućnost nekog napadača da statistički prati pojavu nekog paketa na pojedinom Tor čvoru i odredišnom serveru koji je „pod prismotrom“, te da time identifikuje uzročnu vezu između servera i tor čvora, i tako dalje da prati dinamiku dolaska nekog paketa na taj Tor čvor i slanja paketa sa tog Tor čvora ka posmatranom serveru. Kontramera za ovaj napad bi bila da Tor čvorovi randomalno generišu pakete podataka bez ikakve veze sa pravim podacima i da ih šalju kroz Tor mrežu, u cilju onemogućivanja ovakvog praćenja.

Međutim budući da je Tor mreža izuzetno razgranata, i da kroz jedan čvor istovremeno putuje više „linija“ podataka, ovakav napad je nemoguće efikasno izvesti.

Druga karakteristična uočena slabost je da ako neko zlonameran postavi svoj Tor čvor i deklariše ga kao „izlazni čvor“, on može da pristupi originalnom paketu podataka (ali samo pod uslovom da se radi o „golim“, nezaštićenim podacima, tj. ako nije SSL konekcija npr. u kojoj je i izvorni paket šifrovan). Primer za ovo dao je Švedski istraživač Dan Egerstad, koji je koristeći ovaj metod došao do lozinki za preko 100 email naloga stranih ambasada³⁷.

U ovome su neki istraživači otišli još dalje, razvijajući ideju o „crvljivoj jabuci u korpi“, koju su objavili marta 2011., istraživači iz Francuskog INRIA³⁸ instituta su dokumentovali napad kojim su uspeli da identifikuju BitTorrent³⁹ korisnike određivanjem njihove IP adrese.

Ali ono što je bitno reći je da ova ideja nije nova, i mada je najpoznatija, možda najelegantnija metoda je ona koju su prezentovali istraživači firme za kompjutersku bezbednost i konsalting FORTCONSULT⁴⁰ koji su 2006. godine objavili kako su koristeći metod „crvljive jabuke“ uspevali da identifikuju Tor korisnike po njihovoj IP adresi[34].

Svi ovi napadi, međutim, imaju vrlo mali i ograničen značaj. Kao prvo oni ne koriste slabosti samog Tor rešenja, već slabost na aplikativnom nivou specifične aplikacije (nekog torrent klijenta, ili Flash multimedia). Takođe nemoguće je presretati i nadzirati

³⁷ Bangeman, Eric (2007-08-30). ["Security researcher stumbles across embassy e-mail log-ins"](#)

³⁸ INRIA- Institut National de Recherche en Informatique et en Automatique- <http://www.inria.fr/en/>

³⁹ BitTorrent – Najrasprostranjeniji P2P protocol za razmenu velikih fajlova, http://en.wikipedia.org/wiki/BitTorrent_%28protocol%29

⁴⁰ Zvanični sajt Švedske kompanije FortConsult: <http://www.fortconsult.net/en>

“ciljanog” korisnika na ovaj način, već potencijalno samo one korisnike tj. one sesije razmene podataka koje po slučajnom algoritmu budu redirektovane baš kroz tu konkretnu “crvljivu jabuku”, a time je nemoguće upravljati.

V ZAKLJUČAK

Identitet i privatnost podataka prosečnog korisnika na internetu je kako smo videli veoma izložena tj. ugrožena, i ti podaci su dostupni skoro svakom laiku koji je za iste zainteresovan.

Ako zanemarimo legitimne oblike nadzora internet aktivnosti npr. dece od strane njihovih roditelja ili zaposlenih u kompanijama od strane nadležnih rukovodilaca, postoji ogroman prostor za raznovrsne (zlo)upotrebe.

Ovaj pojam (zlo)upotrebe baš namerno tako navodimo, jer je nekada i u interesu korisnika da neko zna njegov identitet/lokaciju i sl. Npr. na mnogim internet sajtovima postoje multi-jezički sadržaji, i jako je zgodno ako sama web prezentacija na osnovu IP adrese posetioca može da automatski prezentuje sadržaj na domicilnom jeziku posetioca.

Takođe, zloupotrebe mogu biti totalno bezazlene, ali ne i od zanemarljivog značaja kao npr. identifikovanje geografske lokacije pojedinog korisnika za svrhe ciljanog marketinga u smislu da mu se plasiraju reklame koje su relevantne za njegovu geografsku lokaciju.

Osim identifikacije/lociranja konkretnog korisnika, značajne podatke o samom korisniku može da pruži i uvid u njegove „aktivnosti“ na internetu, npr. statistika koliko često posećuje određene sajtove i koliko se zadrži na njima. Time neka treća strana može da stekne uvid u njegova interesovanja i aktivnosti, te se ista mogu takođe (zlo)upotrebiti opet počev od ciljnog marketinga (gde se npr. nekome ko stalno posećuje sajtove posvećene ribolovu, plasiraju reklame proizvođača ribolovačke opreme). Međutim neko te iste podatke može da prati i koristi u svrhe industrijske špijunaže, od strane poslovne konkurencije.

Naravno na svetu ima bezbroj zlonamernih pojedinaca koji mogu te podatke zloupotrebiti na razne načine, počev od neke neslane šale, lažnog predstavljanja ili neke aktivnosti u nečije ime, pa sve do otkrivanja i zloupotrebe osetljivih podataka kao što su npr. nečiji bankovni podaci o platnim karticama i slično.

I ne tako zanemarljiva je ona skupina ljudi koji se upuštaju u nedozvoljene aktivnosti bilo u smislu klasičnog kriminala, ili disidentske aktivnosti, pa im je jako bitno da njihov identitet, aktivnosti i sadržaji ostanu skriveni od strane državnih organa koji bi ih sankcionisali.

Dakle svim korisnicima interneta je njihova anonimnost i privatnost realno ugrožena, i svi oni imaju potrebu da se zaštite u većoj ili manjoj meri.

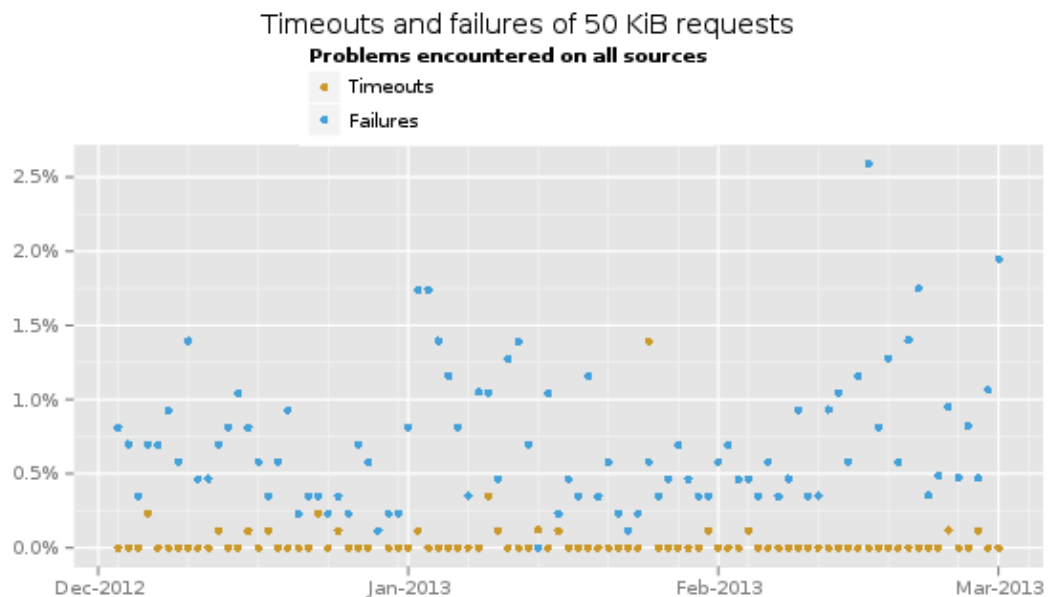
Pošto je izvor i priroda tih rizika raznovrsna, tako svaki korisnik svestan istih može korsititi jedno ili više od dostupnih rešenja kao kontrameru/zaštitu od tih rizika.

Ako npr. korisnik teži da se zaštiti od presretanja i identifikovanja od treće strane online, opredeliće se za tehniku korišćenja anonimnog proxy-ja, ili konkretno Tor rešenja kao najefikasnije varijante.

Tor rešenje omogućava prihvatljivo visok nivo zaštite identiteta i poverljivih sadržaja koje bi neko razmenjivao putem interneta. Prosečan pojedinac ili kompanija koja recimo posluje internacionalno, i koja ima potrebu za razmenom osetljivih podataka putem interneta mogu sa velikom pouzdanošću osigurati tajnovitost kako svoje lokacije/identiteta pojedinaca tako i samih podataka koristeći Tor rešenje.

U prilog ovome govori da trenutno više od 500000 pojedinih korisnika koristi Tor rešenje za prenos vojih podataka/ostvarivanje veze u svakom trenutku širom sveta. Pritom je trenutni prosečni bandwidth preko 350Mbit/sec.

Pritom je pouzdanost prenosa paketa kroz Tor mrežu izuzetno visoka, naročito uzevši u obzir da je čine “nestalni elementi” tj. najčešće PC računari pojedinaca koji u bilo kom trenutku mogu da se diskonektuju sa mreže. Trenutna pouzdanost u smislu prolaza paketa kroz Tor mrežu je veća od 98%, što je izuzetno veliki stepen pouzdanosti, naročito ako se uzme u obzir pomenuta arhitektura mreže. Ovo je ilustrovano na grafikonu 4.



The Tor Project - <https://metrics.torproject.org/>

Grafikon 4. Procenat “neostvarenih veza” kroz Tor mrežu

Ako korisnik teži da se zaštiti od „offline“ napada, tj. da neko analizira tragove „zaostale“ iza korisnika, što je rizik naročito izražen ako se koristi neki „javni“ ili „deljeni“ računar, opredeliće se za private browsing ili neki Live OS ako ima mogućnost za korišćenje istog.

Naravno, i korišćenje ovih tehnika u kombinaciji je jednako moguće, da se korisnik u što većoj meri zaštiti od navedenih rizika.

Svaki korisnik interneta mora biti svestan ovih rizika i preduzeti kontramere da se zaštiti od istih, u onoj meri i obimu koliko mu je bitna anonimnost u internet aktivnostima i u zavisnosti od nivoa poverljivosti podataka koje razmenjuje putem interneta.

VI LITERATURA

- [1] Hubbert Zimmerman, „OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection“ IEEE Transactions on Communications, Vol. COM-28, No 4., April 1980.
- [2] Cerf, Vinton G., „Final Report of the Stanford University TCP project“, Internet experiment note #151, 1. April 1980, <http://www.rfc-editor.org/ien/ien151.txt>
- [3] J. Postel, „RFC 791- Internet Protocol“, information Sciences Insitute, University of Southern California, 1981, <http://www.rfc-editor.org/rfc/rfc791.txt>
- [4] J. Postel, „RFC 793- Transmission Control Protocol“, information Sciences Insitute, University of Southern California, 1981, <http://www.rfc-editor.org/rfc/rfc793.txt>
- [5] Y. Rekhter, B. Moskowitz, D. Karrenber, G. J. De Groot, E. Lear:“RFC 1918: Address Allocation for Private Internets“, IETF 1996, <http://www.rfc-editor.org/rfc/rfc1918.txt>
- [6] Lawson, Stephen, „IPv6 Doomsday Won’t hit in 2012, Experts say.“, PCWorld, 29. decembar 2011, http://www.pcworld.com/businesscenter/article/247091/ipv6_doomsday_wont_hit_in_2012_experts_say.html
- [7] Deering S., Hinden R., „Internet Protocol, Version 6 (IPv6) Specification“, IETF, decembar 1998, <http://www.rfc-editor.org/rfc/rfc2460.txt>
- [8] <http://freegeoip.net>
- [9] <https://www.torproject.org/>
- [10] <http://www.privoxy.org/>
- [11] <http://www.pps.univ-paris-diderot.fr/~jch/software/polipo>
- [12] <http://www.proxomitron.info/>
- [13] http://www.w3schools.com/browsers/browsers_os.asp
- [14] <http://gs.statcounter.com/#browser-ww-monthly-201112-201212>
- [15] <http://www.washingtonpost.com/wp-dyn/content/article/2005/11/02/AR2005110202362.html>
- [16] <http://en.wikipedia.org/wiki/Rootkit>
- [17] <http://kaos.to>

- [18] <http://www.openbsd.org/>
- [19] http://en.wikipedia.org/wiki/Privacy_mode
- [20] <http://www.spotflux.com>
- [21] <http://www.hotspotshield.com/en>
- [22] <http://cyberghostvpn.com>
- [23] <http://www.comodo.com/home/internet-security/free-internet-security.php>
- [24] <http://www.zonealarm.com/security/en-us/zonealarm-computer-security-suite.htm>
- [25] B. Sosinsky, „Networking Bible“, Wiley Publishing, 2009.
- [26] S. Davidoff, J. Ham, „Network Forensics“, Prentice hall 2012.
- [27] Roger Dingledine: „pre-alpha: run an onion proxy now.“, Seoul, 2002.
<http://archives.seul.org/or/dev/Sep-2002/msg00019.html> , pristupano 18.2.2013.
- [28] 13th USENIX Security Symposium, Roger Dingledine, Nick Mathewson, Paul Syverson: „Tor: The Second-Generation Onion Router“, 2004.
<http://static.usenix.org/events/sec04/tech/dingledine.html> , pristupano 20.2.2013.
- [29] D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", 1981., http://www.cs.utexas.edu/~shmat/courses/cs395t_fall04/chaum81.pdf, pristupano 21.2.2013.
- [30] Burton Kalinski, „Some Examples of the PKCS Standards“, RSA Laboratories, 1999.,
<ftp://ftp.rsasecurity.com/pub/pkcs/ascii/examples.asc>, pristupano 25.2.2013.
- [31] George Danezis, „An anomaly-based censorship-detection system for Tor“, Tor Tech Report, September 9, 2011, <http://research.torproject.org/techreports/detector-2011-09-09.pdf>
- [32] FORTCONSULT „Practical Onion Hacking“, 2006.,
http://packetstorm.interhost.co.il/0610-advisories/Practical_Onion_Hacking.pdf
- [33] Frey Donnaly, Adams Richard L. "Pseudo Top-Level Domains" O'Reilly & Associates. 1994. str. 10–11