Centar Informacijske Sigurnosti

Onion routing

rujan 2012.

CIS-DOC-2012-09-061

Upozorenje

Podaci, informacije, tvrdnje i stavovi navedeni u ovom dokumentu nastali su dobrom namjerom i dobrom voljom te profesionalnim radom CIS-ovih stručnjaka, a temelje se na njihovom znanju i petnaestak godina iskustva u radu u informacijskoj sigurnosti. Namjera je da budu točni, precizni, aktualni, potpuni i nepristrani.

Ipak, oni su dani samo kao izvor informacija i CIS ne snosi nikakvu izravnu ili posrednu odgovornost za bilo kakve posljedice nastale korištenjem podataka iz ovog dokumenta.

Ukoliko primijetite bilo kakve netočnosti, krive podatke ili pogreške u ovom dokumentu, ili imate potrebu komentirati sadržaj molimo Vas da to javite elektroničkom poštom na adresu info@CIS.hr.

O CIS-u

CIS izrađuje pregledne dokumente (eng. white paper) na teme iz područja informacijske sigurnosti koji će biti korisni zainteresiranoj javnosti, a u svrhu **podizanje njezine svijesti o informacijskoj sigurnosti** i **sposobnosti za čuvanje i zaštitu informacija i informacijskih sustava**. Pored toga, CIS razvija i održava mrežni portal www.CIS.hr kao referalnu točku za informacijsku sigurnost za cjelokupnu javnost; izrađuje obrazovne materijale namijenjene javnosti; organizira događaje za podizanje svijesti o informacijskoj sigurnosti u javnosti i pojedinim skupinama te djeluje u suradnji sa svim medijima.

CIS **okuplja mlade** zainteresirane za informacijsku sigurnost i radi na njihovom pravilnom odgoju i obrazovanju u području informacijske sigurnosti te pripremu za **profesionalno bavljenje informacijskom sigurnošću**.

Centar informacijske sigurnosti [CIS] nastao je 2010. godine na poticaj Laboratorija za sustave i signale[LSS] Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu, a kao posljedica 15togodišnjeg rada na istraživanju, razvoju i primjeni informacijske sigurnosti. LSS je među ostalim potaknuo osnivanje CARNetovog CERTa i sudjelovao u izradi Nacionalnog programa informacijske sigurnosti RH.

Smisao CISa je da bude **referentno mjesto za informacijsku sigurnost** za javnost, informatičare i posebno za mlade te da sustavno podiže njihovu svijest i sposobnosti u području informacijske sigurnosti.

Rad CISa podržava Ministarstvo znanosti, obrazovanja i sporta Republike Hrvatske, a omogućuju sponzori.

Prava korištenja

Sadržaj

1. Uvod

U obilju sličnih usluga koje se nude na Internetu korisnici vrlo često za korištenje odabiru one „pametnije“. To su usluge koje korisnicima nude sadržaje kakve oni žele i kakvi ih najviše zanimaju. Većina ljudi se s time susreće svakodnevno prilikom korištenja tražilice Google ili pregledavanja Youtube videa. Na prvi pogled odlično djeluje činjenica da Youtube zna koji spot želite pogledati pa vam ga ponudi prvoga u odabiru. Isto tako je odlično da Google zna što korisnika zanima pa takve sadržaje ponudi prve u izboru. No postavlja se pitanje koliko takvi servisi znaju o nama.

Činjenica je da velike kompanije prikupljaju podatke o ponašanju korisnika te da iste koriste u svrhu unaprjeđivanja svojih usluga. Koriste li te podatke i u druge svrhe? Prodaju li ih Vladama ili nekim drugim agencijama? Teško je odgovoriti na to pitanje, no zastrašujuća je pomisao da našu aktivnost na Internetu cijelo vrijeme netko nadzire. Naravno, nisu velike kompanije jedini sudionici koji žele prisluškivati korisnike Interneta. Prisluškivanjem se mogu baviti i razne kompanije koje žele saznati tajne podatke neke druge konkurentske tvrtke. Isto tako prisluškivati je moguće i intimne razgovore i aktivnosti nekog pojedinca bilo na privatnoj ili na poslovnoj razini. Zapravo, razloga za prisluškivanje ima mnogo te je jedino bitno da korisnici budu svjesni da će prije ili kasnije netko bilježiti njihovu aktivnost na Internetu.

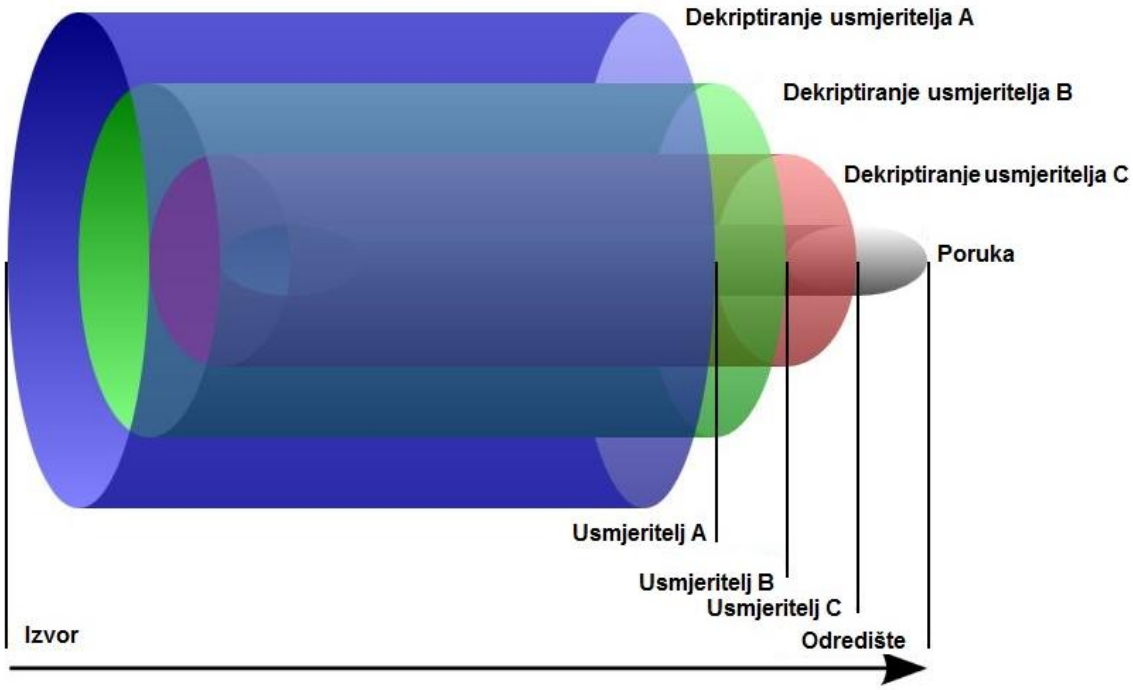
Kada se u cijelu priču uključe zakoni poput SOPA (eng. *Stop Online Piracy Act*) ili PIPA (eng. *Protect IP Act*) , mogućnosti praćenja korisnika koji neovlašteno dijele autorske sadržaje, cenzure koje pojedine države uvode za svoje stanovnike, opstanak Interneta kao posljednjeg slobodnog medija je upitan.

Onion routing je ideja koja se danas dosta dobro nosi s prijetnjama privatnosti korisnika. Pomoću *Onion routinga* moguće je povećati anonimnost korisnika na Internetu, bez drastičnog smanjivanja kvalitete usluge. Korištenjem *Onion routinga* se osim šifriranja sadržaja poruke skrivaju i izvorište odnosno odredište komunikacije, tako da napadač ne može saznati ništa o komunikaciji čak i ako uspije presresti poruku. Nije moguće utvrditi tko je poruku poslao, te je na taj način sakriven identitet korisnika koji koristi Internet uslugu. Zbog načina na koji se poruka kriptira i šalje Onion *routing* je moguće koristiti za različite svrhe Internet komunikacije kao što su pretraživanje stranica, različite komunikacije porukama, razmjena podataka itd.

U ovom dokumentu detaljnije će se obraditi *Onion routing* te komentirati njegove prednosti i nedostatke. U idućem poglavlju opisana je ideja *Onion routinga* te osnovni principi na kojima se on temelji. Nakon toga je opisan način na koji je moguće koristiti *Onion Routing* prilikom svakodnevnog korištenja Interneta. Poglavlja nakon toga dotiču se alternativnih koncepata te predviđanja budućnosti ove ideje. Isto tako spomenuti će se i nedostaci koje ovako moćna metoda povlači za sobom.[1][8]

2. Što je *Onion routing*?

Kao što je rečeno u uvodu, *Onion routing* je tehnika pomoću koje se postiže veća razina anonimnosti na Internetu. To znači da treća strana ne može pratiti našu aktivnost. Ideja *Onion routinga* je poslati poruku kroz više čvorova u mreži na način da svaki čvor dešifrira dio poruke (slika 1). Zbog sličnosti s lukom (engl. *Onion*) koji se guli na način da mu se skida sloj po sloj ova tehnika je nazvana Onion *routing*.



Slika 1. Način dekriptiranja poruke u Onion routingu
Izvor: Wikipedia

Začeci ove ideje sežu u 1995. godinu dok je patent (US Patent No. 6266704) nastao 1999. godine. Glavni istraživači na projektu bili su Michael G. Reed, Paul F. Syverson i David M. Goldschlag.

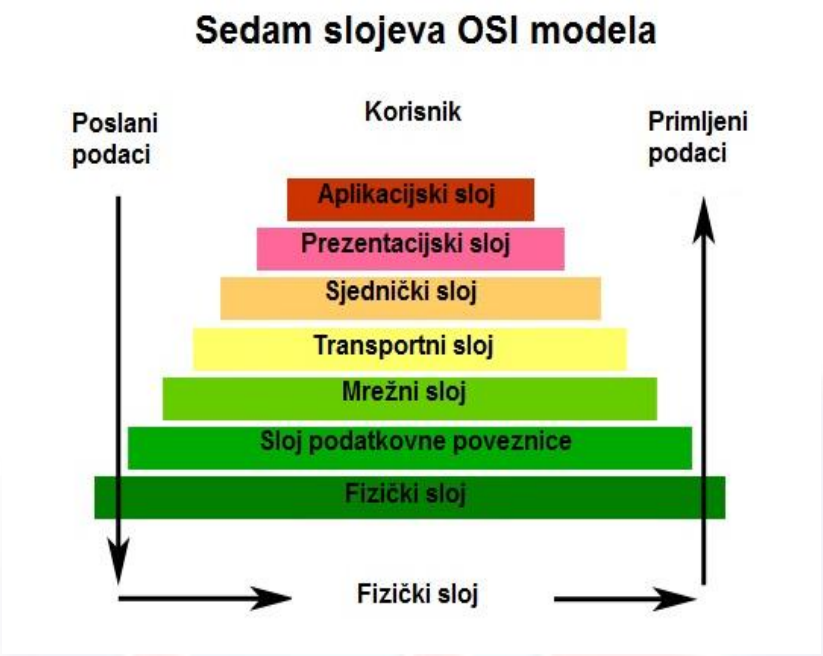
Na temelju te ideje počele su se razvijati različite implementacije od kojih najzapaženiju ulogu ima TOR (eng. *The onion router*) o kojemu će biti riječ u sljedećem poglavlju.[1]

2.1. Ideja Onion routinga

Kao što je već rečeno temeljna ideja na kojoj se zasniva ovaj koncept je kriptirati početnu poruku na način da izvor kriptira poruku u više slojeva, a svaki sljedeći usmjeritelj skine (dekriptira) po jedan takav sloj. Za razumijevanje problematike koja se javlja prilikom provedbe ove ideje u praksu prvo je potrebno proučiti način na koji se obavlja normalna komunikacija u mreži.

2.1.1. Komunikacija u mreži

Prilikom komunikacije unutar neke mreže nužno je da poruka koja se prenosi između čvorova ima unaprijed dogovorenu strukturu. Komunikacijska struktura u mreži podijeljena je na slojeve koje predstavljaju OSI (eng. *Open Systems Interconnection*) model komunikacije[1] (slika 2).



Slika 2. OSI model komunikacije
Izvor: Washington

Kada primjenski program (bilo preglednik, program za instant poruke ili neka treća) želi poslati poruku nekom odredištu na tekst te poruke se dodaju zaglavlja svakog od slojeva. Na kraju se poruka prenosi fizičkim putem (fizički sloj) u obliku jedinica i nula te se na odredištu radi dekompozicija takve poruke obrnutim putem. U ovom dokumentu se neće ići u dublju analizu slojeva te će se zadržati pažnja na transportnom i mrežnom sloju koji su odgovorni za prijenos poruke u mreži.

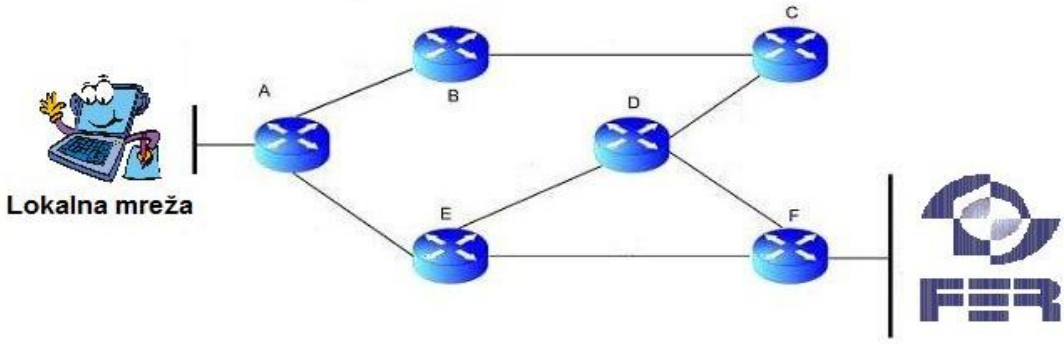
Ta dva sloja brinu se za komunikaciju između dviju krajnjih točaka. Mrežni sloj zadužen je za ispravno usmjeravanje paketa unutar mreže dok je transportni sloj zadužen za pouzdanu uslugu.

Za razumijevanje problematike nije potrebno ići u detalje, jedino je bitno znati da transportni i mrežni sloj na korisne podatke (poruku) nadodaju svoja zaglavlja nakon što ih isto tako nadodaju i slojevi viši od njih. Iz tih podataka moguće je saznati korisne podatke o točkama koje komuniciraju. Između ostalog u zaglavljima mrežnog sloja nalaze se podaci o izvorištu i odredištu paketa iz kojih je moguće saznati autora poruke i kome je namijenjena. Isto tako iz transportnog sloja je moguće pročitati priključnice (engl. *port*) na koje se šalju poruke te se iz toga može saznati ponešto o primjenskim programima koji se koriste. Na primjer ukoliko je odredišni priključak 80 znamo da korisnik putem preglednika pokušava dohvatiti web stranicu s tražene adrese.

Na taj način moguće je otkriti sudionike komunikacije i njihovu namjeru čak i ukoliko ne pročitamo korisne podatke odnosno poruku koja se šalje.

[1] The Open Systems Interconnection (OSI) model (ISO/IEC 7498-1) grupira slične funkcionalnosti komunikacije u logičke slojeve.

Dva čvora koja žele komunicirati najčešće nisu smještena u istoj mreži te je nužno da paketi kojima komuniciraju prođu kroz više čvorova kako bi došli do odredišnog čvora (slika 3).



Slika 3. Usmjeravanje u mreži
Izvor: CIS

Na primjer ukoliko korisnik želi sa svoga računala otvoriti Internet stranicu Fera, zahtjev će proći kroz niz čvorova dok ne dođe do odredišta. Isto tako će se podaci koje će Ferov poslužitelj vraćati vratiti kroz niz čvorova. Važno je napomenuti da putovi kojima paketi prolaze nisu uvijek isti te oni ovise o više čimbenika.

Pomoću alata *tracerout* moguće je odrediti put kojim prolaze paketi na svom putu od izvorišta do odredišta. Slika 4 prikazuje put kojim prolazi zahtjev za dohvatom Ferove stranice. Kao što je moguće vidjeti prolazi se kroz niz čvorova na tom putu.

Na svakom od tih čvorova moguće je pratiti pakete koji se usmjeravaju preko njih što znači da osoba koja posjeduje ovlasti nad tim čvorovima može i pratiti promet koji se prosljeđuje preko njih. Najčešće se na tom putu nalaze čvorovi pod nadzorom lokalnih pružatelja usluge poput T-coma, Iskona, Bneta itd. Svi oni mogu nadzirati promet koji prolazi kroz njih. Isto tako, moguća je i situacija da napadači napadnu neki od čvorova kako bi dobili uvid u promet koji prolazi njima. To nije jedini način na koji je moguće špijunirati korisnike Interneta, no najčešće ga koriste pružatelji usluga iz razloga što posjeduju veliki broj čvorova i na taj način lako mogu nadgledati svoje korisnike. S obzirom na to da svaki paket ima svoju izvorišnu i odredišnu adresu nije teško otkriti od kojega korisnika dolazi paket i kome je namijenjen. Isto tako, ukoliko korisni podaci (sadržaj poruke) nisu kriptirani moguće je i njih pročitati.

Očito je da nešto treba promijeniti u samoj komunikaciji kako bi zaštitili privatnost korisnika. Odgovor na to pitanje daje *Onion router*. [9][10]

```
Tracing route to www.fer.hr [161.53.72.119]
over a maximum of 30 hops:

  1     6 ms     1 ms     1 ms  192.168.5.1
  2    36 ms    21 ms    47 ms  bng01-lo1.net.iskon.hr [213.191.132.214]
  3    23 ms     *       21 ms  89.164.86.25
  4    32 ms    26 ms    24 ms  bdr02.net.iskon.hr [89.164.64.217]
  5    25 ms    24 ms    38 ms  bdr01.net.iskon.hr [89.164.64.209]
  6    67 ms    32 ms    37 ms  193.192.15.65
  7    22 ms    22 ms    22 ms  CN-Srce-03-RO.core.carnet.hr [193.198.228.154]
  8    23 ms    33 ms    23 ms  CN-Srce-04-RO.core.carnet.hr [193.198.228.69]
  9    32 ms    22 ms    29 ms  CN-Fer-01-ES.core.carnet.hr [193.198.229.10]
 10    52 ms    27 ms    28 ms  161.53.16.14
 11    23 ms    43 ms    28 ms  skynet.cc.fer.hr [161.53.72.119]

Trace complete.
```

Slika 4. Prikaz rada alata Tracerout
Izvor: CIS

2.1.2. Način rada Onion routera

Ideja u *Onion routeru* je u tome da poruka putuje kroz nepredviđeni niz posrednika (engl. *Onion routers*). Takav pristup temelji se na ideji izmiješanih mreža (engl. *Mix networks*) Davida Chauma[2]. Poruka je kriptirana kriptografijom javnog i privatnog ključa[3] te je na taj način spriječena mogućnost čitanja poruke na posredniku. Jedna od glavnih prednosti ovakve tehnike je da ne morate imati povjerenje u sve posrednike na putu kojem ide poruka. Ukoliko je jedan od posrednika kompromitiran svejedno je moguće ostvariti anonimnu komunikaciju. To je moguće zbog toga što niti jedan posrednik ne dekriptira cjelokupnu poruku, nego se ona dekriptira na svakom od posrednika po malo. Napadač bi mogao pratiti komunikaciju ukoliko bi bio u posjedu svih posrednika na putu poruke, no ukoliko je taj broj ograničen praćenje postaje uvelike otežano. Čak i ukoliko napadač uspije otkriti da je korisnik poslao poruku biti će vrlo teško odrediti kome je ta poruka namijenjena. Poruka (engl. *Onion*) se sastoji od korisnih podataka koji su kriptirani nizom javnih ključeva od svakog pojedinog posrednika na način da ih ti posrednici mogu dekriptirati. Izvorni podaci su vidljivi samo pošiljatelju i primatelju. Ovisno o tehnici koja se koristi nekad je moguće da i posljednji posrednik vidi sadržaj poruke ukoliko on skida posljednji sloj. Ukoliko se radi o tehnici gdje primatelj obavlja posljednje dekriptiranje, tada ni posljednji posrednik ne može pročitati sadržaj poruke.

Da bi se mogla uspostaviti komunikacija putem niza posrednika na opisan način treba zadovoljiti neke uvjete:

1. Korisnik koji želi poslati poruku kontaktira čvor koji sadrži informacije o posrednicima koji mogu prosljeđivati poruke. Ta komunikacija također može biti kriptirana ili decentralizirana. Odabiru se oni čvorovi koji će tvoriti put prema odredištu. Takav niz posrednika zove se lanac. Niti jedan čvor unutar lanca (osim eventualno izlaznog, posljednjeg čvora) ne može odrediti gdje se nalazi unutar lanca, niti koliko čvorova u lancu postoji.
2. Korisnik pomoću javnog ključa kriptira poruku namijenjenu prvom čvoru u lancu za kojeg možemo reći da je ulazni čvor (engl. *Entry node*). Takva poruka sadrži: ID lanca koji je različit od ID-a ostalih stvorenih lanaca, zahtjev za uspostavljanje lanca komunikacije, korisničku polovicu Diffie–Hellman rukovanja (engl. *Diffie–Hellman handshake*)[4].
3. Ulazni čvor odgovara korisniku ne kriptiranom porukom koja sadrži: drugi dio Diffie–Hellman rukovanja i sažetu vrijednost dijeljene tajne.
4. Sada korisnik i ulazni čvor imaju zajedničku tajnu koju mogu koristiti za simetrično kriptiranje podataka koje se odvija puno brže od asimetričnog kriptiranja.
5. Nakon toga korisnik preko ulaznog čvora na sličan način uspostavlja komunikaciju sa sljedećim čvorom u lancu.
6. Čvor odgovara ulaznom čvoru kao što je opisano u točki 3.
7. Ulazni čvor obavještava korisnika da je komunikacija sa sljedećim čvorom uspostavljena, te mu prosljeđuje poruku sa sažetkom tajne i dijelom Diffie-Hellman rukovanja. Korisnik i idući čvor u lancu su uspostavili tajnu za komunikaciju.

Na taj način moguće je proširivati lanac ovisno o potrebi. Detalji ovakvog uspostavljanja komunikacije najčešće su zavisni o konkretnoj implementaciji.

Kada je uspostavljanje lanca završeno korisnik može anonimno slati podatke. Na primjer ukoliko korisnik želi otvoriti neku Internet stranicu njegov preglednik kontaktira čvor (engl. O*nion router*) koji formira poruku na način prikazan na slici 5.

[2] David Chaum je 1981. godine uveo ideju izmiješanih mreža gdje poruka putuje kroz niz posrednika kriptirana pomoću kriptografije javnog i privatnog ključa.

[3] Kriptografija javnog i privatnog ključa temelji se na postojanju dvije vrste ključeva od kojih je jedan svima poznat, dok je drugi poznat samo vlasniku. Poruku kriptiranu javnim ključem, moguće je otključati samo poznavanjem privatnog ključa.

[4] Diffie–Hellman rukovanje je jedan od načina izmjene kriptografskih ključeva sudionika komunikacije.

Slika 5. Izgled poruke kojom se prenosi HTTP zahtjev kroz mrežu
Izvor: CIS

Uzet je primjer s tri čvora u lancu gdje postoji ulazni čvor, srednji čvor i izlazni čvor. Poruka je formirana na način da se unutar vitičastih zagrada nalaze podaci kriptirani tajnom između korisnika i ulaznog čvora, unutar uglatih zagrada nalaze se podaci kriptirani tajnom između korisnika i srednjeg čvora, dok se unutar oblih zagrada nalaze podaci kriptirani tajnom između korisnika i izlaznog čvora.

Nakon što prihvati i dekriptira poruku ulazni čvor vidi poruku na način prikazan na slici 6.

Slika 6. Izgled poruke nakon dekriptiranja prvog sloja
Izvor: CIS

S obzirom na to da je komunikacija uspostavljena ranije svaki čvor zna kome treba proslijediti poruku, te korisnik ne treba brinuti o tome.

Srednji čvor vidi poruku na način prikazan na slici 7.

Slika 7. Izgled poruke nakon dekriptiranja drugog sloja
Izvor: CIS

Te poruku u takvom obliku prosljeđuje izlaznom čvoru koji dekriptira posljednji sloj te može pročitati protokol HTTP (engl. *Hypertext Transfer Protoco,* HTTPl) zahtjev.

Izlazni čvor nastavlja standardnu komunikaciju ovisno o HTTP zahtjevu. Na taj način je završeno slanje zahtijeva za dohvatom web stranice, no isto tako očekuje se i odgovor od poslužitelja te stranice. Poslužitelj odgovara izlaznom čvoru na standardan način putem HTTP odgovor koji sadrži HTML kod stranice. Izlazni čvor kriptira poruku zajedničkom tajnom između njega i korisnika te šalje poruku u suprotnom smjeru od one kojim je došla. Postupak se nastavlja sve dok poruka ne dođe nazad do korisnika. Korisnik mora tri puta dekriptirati poruku s tri različita ključa čvorova u lancu kako bi došao do sadržaja poruke.

Takvo višestruko kriptiranje poruke ne povećava razinu sigurnosti samog kriptografskog algoritma već osigurava sigurnu distribuciju poruke kroz mrežu. Kada bi na primjer poruku kriptirao samo izlazni čvor, a ostali je čvorovi samo prosljeđivali napadač bi trebao samo otkriti tajnu između korisnika i izlaznog čvora. Višestrukim kriptiranjem s različitim ključevima onemogućava se dekriptiranje bez poznavanja svih ključeva. Ukoliko napadač dođe u posjed ključa izlaznog čvora te presretne poruku prije nego što je neki drugi čvor dodatno kriptira moguće je pročitati sadržaj poruke no nije moguće odrediti kome je poruka namijenjena.

Ideja *Onion routinga* odnosi se na komunikaciju između korisnika (začetnika komunikacije) i izlaznog čvora. Iako se nisu mijenjali osnovni principi komunikacije opisani u poglavlju 2.1.1., pomoću tehnika kriptiranja i tehnike izmiješanih mreža Davida Chauma moguće je postići veću razinu anonimnost od one kakve ju imaju korisnici prilikom standardne komunikacije.[1][2]

2.1.3. Nedostaci i ranjivosti *Onion routrea*

Vremenska analiza je jedan od nedostataka pomoću koje je moguće praćenjem čvorova otkriti koji paket pripada kojem korisniku. Ukoliko se prati čvor koji nije jako opterećen prometom moguće je vremenskom analizom povezati ulaznu poruku s izlaznom prema nekom drugom čvoru. Na taj način je moguće pratiti komunikaciju. Rješenje tog problema moguće je pomoću spremnika koji čeka da se nakupi određeni broj poruka koje se nakon toga šalju nekim pseudoslučajnim algoritmom.

Napad na prekretnici (engl. *Intersection attacks*) događa se u situacijama kad se čvorovi periodički kvare ili napuštaju mrežu. Lanac koji je ostao u funkciji nije mogao biti usmjeravan preko čvora koji je napustio mrežu ili onoga koji se nedavno priključio mreži, a to povećava šanse za uspješnu analizu prometa.

Promet je moguće pratiti i pomoću promjena sjednica koje se događaju periodički. Ukoliko ista sjednica doživi više promjena lanaca kompromitirani čvor koji je promatra pokušat će se češće spajati na tu sjednicu te na taj način pokušati obavljati analizu prometa.

Prisluškivanjem izlaznog čvora moguće je saznati sadržaj poruke. Ukoliko se u poruci nalaze tajni podaci poput lozinki ili neki drugi važni podaci, moguće ih je pročitati ukoliko napadač dođe do ovlasti u izlaznom čvoru. Ovaj problem se rješava kriptiranjem s kraja na kraj (engl. *End to end*) u kojem se sadržaj poruke dodatno kriptira tako da ga ni izlazni čvor ne može pročitati. Jedan od načina na koji se to može napraviti je pomoću protokola SSL (eng. *Secure Sockets Layer*)[5].

Jedan od glavnih nedostataka ove tehnologije je usporavanje komunikacije zbog potrebe za uspostavom dodatnih veza te odašiljanje poruke preko dodatnih čvorova. Također za uspostavu ovakve komunikacije potrebno je imat posrednike odnosno čvorove koji znaju na koji način se odvija komunikacija putem *Onion routera* što zahtijeva dodatnu infrastrukturu. Čak i ako se koriste volonterski posrednici nužno je na njima ugraditi ispravnu programsku podršku.

Za posrednike možemo reći da su vitalni organi *Onion routinga* jer bez njih ne bi bilo moguće izvoditi prosljeđivanje poruka. Zbog toga je potrebno onesposobiti što veći broj posrednika ukoliko se želi onemogućiti komunikaciju putem ove tehnike. S obzirom na to da je broj posrednika relativno velik, te da zahtjevi za performansama nisu pretjerani, može se naći dovoljno velik broj volontera koji žele biti posrednici tako da je teško očekivati onemogućavanje svih posrednika u mreži.[1]

[5] Secure Sockets Layer je protokol pomoću kojeg se ostvaruje kriptiranje sadržaja u Internet komunikaciji.

3. *Onion routing* u stvarnoj primjeni

Onion rounting, opisan u prethodnom poglavlju, je ideja i kao takav ne postoji u stvarnoj primjeni. Svaku ideju je moguće iskoristiti te je prilagoditi stvarnom svijetu te od nje napraviti funkcionalan proizvod. Iako je *Onion routing* moguće koristiti i u okviru lokalnih mreža najveći potencijal postići će naravno u Internet svijetu. Zbog činjenice da je Internet opasno mjesto gdje je prisluškivanje gotovo svakodnevnica razvili su se programi koji u svojoj ideji imaju *Onion routing*, te služe za sakrivanje informacija koje korisnici koriste na Internetu.

Treba imati na umu da postoje različiti načini na koje je moguće prisluškivati korisnike. Već su navedene mogućnosti praćenja korisnika korištenjem kolačića ili superkolačića, a tu je još i otisak web preglednika kao metoda pomoću koje je moguće prepoznati korisnika neovisno o izvorišnoj adresi. Zbog toga programi za zaštitu privatnosti korisnika proširuju svoje mogućnosti na način da izoliraju sve vrste napada na koji je moguće napasti korisnike. Zbog toga se različite ideje i implementacije mijenjaju kroz vrijeme. Ideja *Onion routinga* uvelike je promijenjena danas u odnosu na početnu ideju koja je nastala 1995. godine. Osim toga, u programima koji koriste *Onion routing* uvedeni su i dodatni mehanizmi koji štite korisnike. Tako danas postoje različiti dodaci preglednicima koji blokiraju kolačiće i superkolačiće, mehanizmi koji paze na komunikaciju instant porukama itd.[2]

3.1. Sakrivene usluge

Još jedna korisna stvar osim anonimiziranja korisnika koju omogućuje *Onion routing* je sakrivanje usluga. Usluge na Internetu su najčešće meta napada u kojima ih se pokušava onesposobiti. Takvi napadi mogu biti na logičkoj ili na fizičkoj razini. Radi povećanja razine sigurnosti moguće je sakriti uslugu (fizički i logički). Fizičko sakrivanje usluge je intuitivno i izvodi se na način da uslugu spremimo na poslužitelj te sakrijemo informacije koje otkrivaju da se ta usluga odvija na tom poslužitelju. Uslugu na logičkoj razini možemo sakriti pomoću *Onion routinga*. To je moguće izvesti na način da korisnici ne pristupaju usluzi putem neke IP adrese kao što je to uobičajeno već se koriste posrednici *Onion routinga* za pristup toj usluzi. Na taj način je i računalo na kojem se nalazi usluga logički sakriveno od korisnika koji je koriste. [2]

3.2. The onion router

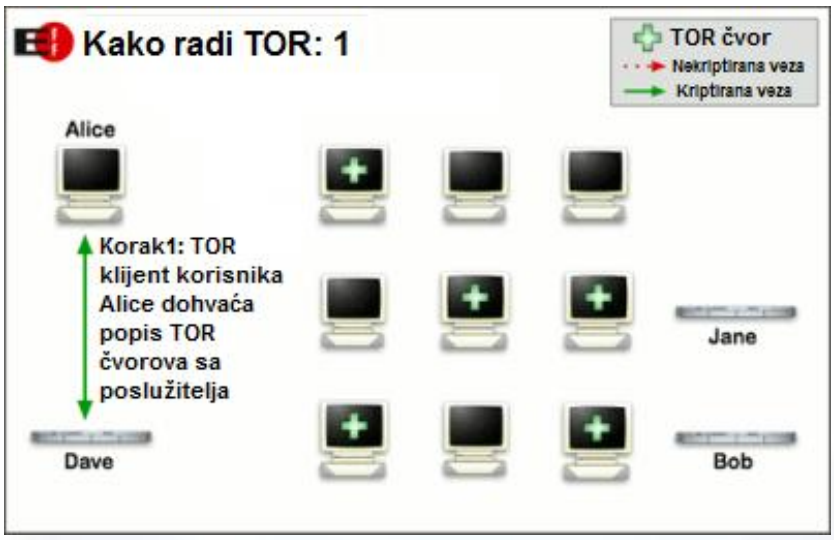
The onion router (TOR) je najpoznatiji i najkorišteniji program koji se temelji na ideji *Onion routinga*. Iako se često koriste kao sinonimi treba razlikovati TOR kao implementaciju, a *Onion routing* kao ideju.

Projekt iz kojeg se razvio TOR započet je 2002. godine i u početku je bio namijenjen za osiguravanje komunikacija u američkoj vojsci i vladi. Sam razvoj *Onion routinga* temelji se na razvoju TOR-a. *Onion routing* možemo podijeliti na generacije po kojima se razvijao. Nulta generacija smatra se početna ideja koja je nastala 1995./1996. godine. Za prvu generaciju uzimaju se sve promjene nastale prije nastanka prvog TOR-a. Drugu generaciju *Onion routinga* predstavlja TOR u razdoblju između 2002. i 2005. godine. Za treću generaciju uzima se TOR od tada pa do danas. Iz toga se vidi da je TOR zapravo temeljni nositelj ideje *Onion routing* te da on danas predstavlja tu ideju oblikovanu u konkretni primjenski program.

TOR je u današnje vrijeme namijenjen svim korisnicima Interneta te je dostupan na svim popularnijim operacijskim sustavima (Windows, Linux, Mac OS). Broj posrednika koji danas rade u sklopu TOR-ove mreže broji se u tisućama, dok je broj korisnika porastao na nekoliko desetaka pa i stotina tisuća.

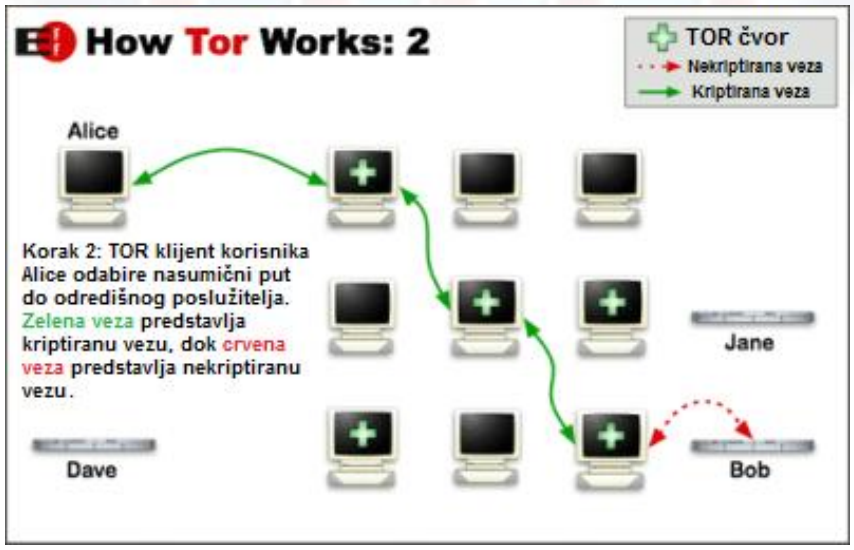
3.2.1. Način rada The onion routera

Ukoliko osoba nazvana Alice želi komunicirati sa osobom Bob uz pomoć TOR-a mora prvo dohvatiti listu poznatih TOR čvorova (slika 5).



Slika 8. Način rada TOR-a
Izvor: Torproject

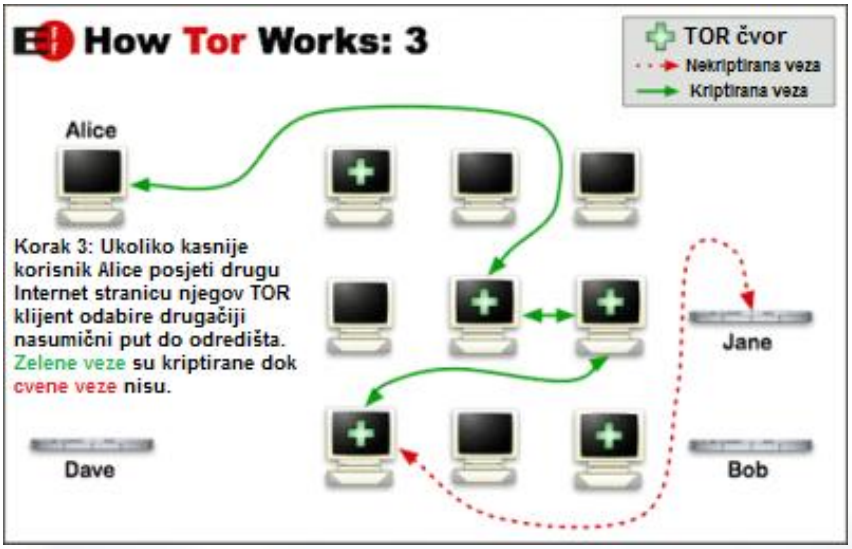
Nakon što se dohvate potencijalni posrednici potrebno je formirati lanac između izvorišta i odredišta. Komunikacija između izvorišta i čvorova međusobno je kriptirana kao što je prikazano na Slici 6. Nakon što je komunikacija uspostavljena moguće je anonimno komunicirati između odredišta i izvorišta.



Slika 9. Način rada TOR-a
Izvor: Torproject

Nakon desetak minuta ili nakon što korisnik odredi drugačije odredište stvara se novi lanac sačinjen od drugih čvorova. Na taj način otežava se napadačima analiza prometa i prepoznavanje korisnika (slika 7).

Kao što se vidi iz priloženih slika i opisa, način rada TOR-a ne razlikuje se od početnog koncepta *Onion routera* navedenog u prethodnom poglavlju. Naravno, u implementaciji TOR-a bilo je potrebno implementirani i mnogo drugih detalja koje rješavaju probleme koji se javljaju kao što je mogućnost ispadanja čvorova, problematika centralizacije čvora sa podacima o posrednicima, protokoli komunikacije posrednika itd. [3]



Slika 10. Način rada TOR-a
Izvor: Torproject

3.2.2. Mogućnosti *The onion routera*

Kao što je već navedeno projekt TOR bavi se s puno širom problematikom od samog razvoja koncepta *Onion routinga*. S obzirom na to razvio se čitav niz programa podrške anonimnosti klijenata. Osim osnovnog TOR programa koji služi kao programska podrška za korištenje *Onion routiga*, postoje još i programi kao što su: Tor Browser, Vidalia, Tor Cloud, Orbot, Arm, Atlas, Obfsproxy, Tails, Tor Button itd.

Tor Browser je preglednik pomoću kojega je moguće anonimno otvarati Internet stranice. Vidalia je grafičko sučelje za kontrolu posrednika, Orbot je TOR namijenjen Android uređajima.

Tor Button je posebno hvaljen dodatak za preglednik Firefox, a radi modifikacije u samom pregledniku kako bi omogućio sigurnije korištenje preglednika.

Isto tako, TOR projekt uz pomoć *Onion routinga* omogućuje svojim korisnicima stvaranje skrivenih *web* usluga. Na taj način korisnici TOR-a mogu stvoriti svoje *web* stranice ili različite usluge bez da drugi znaju njihovu lokaciju. Na taj način štiti se anonimnost autora stranice i osobe koja objavljuje sadržaj na toj stranici.

Podrška namijenjena programima dostupna je na službenoj stranici TOR projekta:

https://www.torproject.org

3.2.3. Nedostaci *The onion routera*

Mreže čvorova na kojima se zasniva TOR temeljene su na volonterskim čvorovima koji kroz sebe propuštaju dio prometa. Što je više takvih čvorova uključeno u mrežu to je mreža brža i sigurnija. Zbog toga je nužno cijelo vrijeme u mreži imati dovoljan broj čvorova kako bi mreža ispravno radila. Sudionici TOR projekta u stalnoj su potrazi za novim čvorovima kako ne bi došlo do zagušenja usluge zbog velikog porasta broja korisnika.

I sami tvorci TOR-a ističu kako on nije dovoljan za rješavanje svih problema anonimnosti. Najslabija karika u cijeloj priči su ljudi kao korisnici Interneta. Zbog toga se ističe kako ljudi

moraju promijeniti svoje navike i odreći se nekih mogućnosti koje im nude preglednici u zamjenu za tajnost koju TOR može ponuditi.

Sudionici Tor projekta trude se biti u korak s najmodernijim opasnostima koje vrebaju korisnike na Internetu te razvijaju programe koji s tehničke strane pokušavaju stati na kraj modernim tehnikama praćenja korisnika. Tako na primjer Tor Button onemogućava aktivni sadržaj preglednika kao što su kolačići te pokušava prikriti detalje o pregledniku i korisničkom računalu kako bi korisnika tog preglednika uklopio u niz sličnih preglednika na Internetu.

No, sve to pada u vodu ukoliko korisnik svojom nepažnjom ostavlja privatne podatke na stranicama ili na svoju ruku prilagođava svoj preglednik.

Osim toga korisničko računalo također je slaba točka za potencijalne napade. Ukoliko napadač može pratiti promet koji izlazi ili ulazi u korisničko računalo veća je šansa da će uspjeti otkriti detalje poruke pa makar ona bila i kriptirana.[3]

4. Prednosti i nedostaci *Onion routinga*

U prethodnim poglavljima govorilo se o prednostima i nedostacima *Onion routinga* u tehničkom smislu. U ovom poglavlju govoriti će se o posljedicama koje ova tehnika donosi u Internet svijet.

4.1. Prednosti

Prednosti ove tehnike su velike i opravdavaju njeno postojanje i ulaganje u nju. Ona u suštini omogućuje individualnima i skupinama da nesmetano i tajno komuniciraju bez straha da netko zadire u njihovu privatnost.

Također omogućuje korisnicima da komuniciraju putem instant poruka te da posjećuju stranice bez da itko zna njihove aktivnosti. Isto tako pruža korisnicima kojima je zabranjen pristup određenim Internet stranicama (bilo od Vlade ili pružatelja usluga) da takvim stranicama ipak pristupe. Omogućuje se pružanje sadržaja i usluga na Internetu bez opasnosti od otkrivanja lokacije tih sadržaja ili autora. Pristup različitim forumima je omogućen na anoniman način tako da nitko ne može saznati tko se krije iza nekog nadimka.

Novinari mogu anonimno pristupati svojim stranicama čak i iz stranih država. Isto tako različite grupe s posebnim zadacima mogu komunicirati na anoniman i zatvoren način. Također je omogućena i nesmetana i tajna razmjena podataka i različitih sadržaja.

Zapravo, glavna prednost ove metode je anonimnost u svakom pogledu. Na taj način se promiču ljudska prava i demokracija kao i pravo slobode govora koja ja zajamčena ustavom. Mnoge međunarodne kompanije koje se bave ljudskim pravima poput Electronic Frontier Foundation (EFF) ističu TOR (a samim time i *Onion routing* kao koncept) kao jedan od načina borbe za ljudska prava u virtualnom svijetu.[3]

4.2. Nedostaci

Iako TOR omogućuje svim korisnicima Interneta odakle god potjecali da koriste svoje pravo na anonimnost, s druge strane služi i kao odlična metoda zlonamjernim korisnicima da sakriju svoje aktivnosti. Iako je u načelu sama metoda plemenitog karaktera stavlja moćno oružje u ruke ljudi koji ju žele iskoristiti u nelegalne svrhe.

Glazbena i filmska industrija gube milijune zbog nelegalnog kopiranja i distribucije autorskog sadržaja. Pomoću TOR-a odnosno koncepta *Onion routing* takve je sadržaje moguće dijeliti bez opasnosti od otkrivanja od strane Vlade ili policije. Zbog toga je ovaj koncept direktan odgovor zakonima poput SOPA-e jer daje korisnicima u ruke moćnu tehnologiju za daljnje provođenje aktivnosti koje taj zakon brani.

No iza anonimnog korištenja Interneta i skrivenih usluga krije se nešto mnogo opasnije od preuzimanja pjesama ili filmova s Interneta.

4.2.1. Tamna strana Interneta

Tamna strana Interneta ili Tamni Internet (engl. *Dark Internet*) naziv je za ilegalne web stranice i usluge kojima je nemoguće pristupiti na uobičajeni način pomoću preglednika. Adrese takvih stranica ne završavaju klasičnim nastavcima poput .com ili .hr već najčešće završavaju nastavkom .onion. Zbog nestandardiziranih adresa koje ne postoje u registrima domena nije im moguće pristupiti na klasičan način. Za pristupanje takvim stranicama potrebno je imati ispravno instaliran i podešen TOR sustav na računalu.

Adrese stranica takvog tipa izgledaju ovako:

http://kpvz7ki2v5agwt35.onion/wiki/

Navedena adresa je adresa na takozvanu skriveni wiki (engl. *Hidden Wiki*) na kojem je moguće pronaći različite informacije o skrivenim uslugama i stranicama koje se nude u Tamnom Internetu.

Problem u cijeloj priči je što je na takvom mjestu sve anonimno te zbog toga vlada totalna anarhija i bezakonje. Mogućnosti TOR-a kao što su skriveni servisi se iskorištavaju da se na takvim stranicama prodaje droga, oružje ili se distribuiraju različiti seksualni sadržaji. Na žalost, u današnje vrijeme se ove mogućnosti TOR-a vrlo malo koriste za promicanje slobode govora i ljudskih prava, već su nasuprot tome leglo kriminala.

Skriveni servisi u današnje vrijeme nisu ništa drugo nego mjesto gdje se dogovaraju teroristički napadi, preprodaje droga ili organizira šverc oružjem. Kriminal je dosegao tu mjeru da su nastale stranice poput popularne „Silk road“ stranice koja je zapravo svojevrsna inačica Internet trgovine poput Ebaya za drogu i oružje.

S obzirom na to da je put novca lako pratiti nastao je digitalni novac zvan Bitcoin i on je jedno od osnovnih sredstva plaćanja na Tamnom Internetu. Na taj način ljudi mogu trgovati na mjestima poput ovih bez da netko može pratiti tok njihovog novca. Do ovoga trenutka je u opticaj pušteno preko osam milijuna Bitcoinova, dok je u kolovozu ove godine vrijednost jednoga Bitciona bila oko deset američkih dolara. Vjeruje se da je današnja ukupna vrijednost Bitcoinova prešla devedeset milijuna američkih dolara.

Zbog velike razine kriminala koja se razvila uz pomoć TOR-a postavlja se pitanje je li tehnologija opravdala svoje postojanje ili je zbog nje nastalo više negativnih posljedica. Ideja *Onion routinga* je vrlo moćna te se u skladu s tim mora i koristiti na pravilan način. Takvo oružje u rukama krivih osoba rezultira pojavom stvari kao što je Tamni Internet.[5][6][7]

5. Koncepti slični *Onion routingu*

Osim *Onion routinga* razvili su se još neki koncepti koji kombiniranjem kriptiranja i korištenjem posrednika povećavaju anonimnost na Internetu. Svi ti koncepti su većoj ili manjoj mjeri slični *Onion routingu* ili su se čak razvili iz te ideje.

5.1. Garlic routing

Garlic routing je modifikacija ideje *Onion routinga*. *Garlic* na engleskom znači češnjak što automatski asocira na način spremanja poruke. Jedna poruka koja putuje takvom mrežom sastoji se od više korisničkih poruka baš kao što se češnjak sastoji od više režnjeva. Za razliku od *Onion routinga* gdje jedna poruka predstavlja jednu korisničku poruku kod *Garlic routinga* još je više otežana analiza prometa.

Korisnički programi poput I2P i Perfect Dark su neke od implementacija *Garlic routinga*. U suštini su vrlo slične TOR-u te je jedina bitna razlika u načinu slanja poruke.[11]

5.2. Anonymous P2P

Anonymous P2P je mreža za dijeljenje sadržaja (engl. *Peer-to-peer*) računala u kojima čvorovi mogu komunicirati na anoniman ili pseudoanoniman način. Korisnici u takvoj mreži sudjeluju na način da omogućavaju korištenje dijela njihovog prometa i sadržaja. Tajnost se postiže na način da čvorovi ne znaju fizičku lokaciju ostalih čvorova u mreži. Anoniman način komunikacije podrazumijeva da čvorovi ne znaju nikakve detalje o ostalim čvorovima dok kod pseudoanonimnog način mogu povezati neki nadimak ili ključ sa određenim računalom.[12]

5.3. Java Anon Proxy

Java Anon Proxy poznata još i kao JAP ili JonDonym je sustav posrednika koji omogućavaju korisnicima pretraživanje Interneta na pseaudoanoniman način. To se postiže na način da se korisnička poruka šalje kroz sustav posrednika gdje se poruka izmiješana s ostalim korisničkim porukama pošalje kroz niz čvorova prije stizanja na odredište. Za razliku od TOR-a gdje korisnik ne može odabrati kojim čvorovima prolazi njegova poruka kod JAP-a mu se nudi niz sustava posrednika tako da korisnik može odlučiti kome će vjerovati, a kome ne. Problem nastaje u tome što su detalji o posrednicima poznati te oni mogu postati meta fizičkog (onemogućiti uslugu) ili pravnog (zabrana rada od strane Vlade ili nekog lobija) napada. [13]

6. *Onion routing* u budućnosti

Budućnost *Onion routinga* uvelike je vezana uz projekt TOR. Trenutno stanje u pravu, politici i tehnologiji je takvo da se nastoji što više iskoristiti prilika za nadzor građana. Zbog toga se stvara plodno tlo za ovakve i slične tehnologije od kojih se očekuje dodatan razvoj u budućnosti. Zbog činjenice da će u mnogim zemljama zakoni pritisnuti građane uz zid očekuju se dodatne donacije bilo u samom novcu ili u raspoloživim resursima (posrednicima) koje će pristizati na račun projekata kao što je TOR. Kao što je već rečeno, posrednici u mreži su vitalni organi ove tehnologije te će zbog povećanja broja korisnika nastati potreba za većim brojem posrednika. Zbog toga su i mogući pokušaji napada na te posrednike kako bi se destabilizirala takva mreža, no zbog njenih osobina to je vrlo teško izvesti. Već u današnje vrijeme posrednici su razmješteni po cijelom svijetu tako da jedan napad bilo fizički, logički ili pravni, teško da može uništiti cijelu mrežu. Zbog toga se čini da će TOR tehnologija i u budućnosti voditi glavnu riječ u zaštiti prava korisnika, te da će ju biti vrlo teško ograničiti. Osim toga očekuje se razvoj manjih privatnih mreža koje će se zasnivati na *Onion routingu* ili nekom sličnom konceptu koji će se možda razviti iz njega. Zbog porasta opasnosti od prisluškivanja očekuje se da će i razne organizacije i tvrtke posezati za ovakvim rješenjem radi sakrivanja svojih internih podataka. S obzirom na rast popularnosti mobilnih telefona očekuje se razvijanje ove tehnologije i u tom smjeru. Već danas postoji TOR sustav za platformu Android naziva Orbot, no u budućnosti se očekuje širenje i na druge platforme i uređaje s ograničenim resursima. Ne zna se točno kakve tehnologije će se razviti u budućnosti i na koji način će se to odražavati na korisnike no projekti poput TOR-a moraju biti spremni odgovoriti na sve ukoliko se žele osigurati od propasti. Glavnu opasnost za otkrivanje korisnika koji koristi *Onion routing* je napredna analiza prometa koju napadač može provesti, te se očekuje da će u budućnosti TOR koristiti neke dodatne mehanizme da bi još više otežao povezivanje korisnika s prometom koji je moguće analizirati na posrednicima.

Glavni adut protiv tehnologija ovakve vrste može biti Tamni Internet koji je ovih dana uzeo maha i teško da je moguće spriječiti njegov razvoj. Naprotiv, u skorije vrijeme se očekuje porast kriminalnih usluga koje će se nuditi na Tamnom Internetu, te je neophodno u budućnosti pokušati suzbiti takav rast kriminala. Očekuje se puštanje dodatnog novca Bitcoina u opticaj sve do 21 milijuna kroz idućih deset godina što će dodatno potaknuti taj način trgovine na Internetu.[3][4]

7. Zaključak

Onion routing se u praksi pokazao kao vrlo moćno oružje koje vrlo dobro ispunjava zadaću zbog koje je napravljeno. Kombiniranjem tehnika kriptiranja i promjenom puta poruke moguće je postići visoku razinu anonimnosti bez dubljeg zadiranja i promjene protokola koji se standardno koriste za komunikaciju na Internetu. Kombiniranjem tehnike *Onion routinga* s drugim tehnikama koje sakrivaju identitet korisnika (poput onemogućavanja kolačića) moguće je zaštiti korisnika od napasti današnjeg svijeta koje zadiru u njegovu intimu i pokušavaju ga nadzirati. Zbog toga se TOR prikazuje kao veliki promicatelj slobode govora i temeljnih ljudskih prava jer omogućuje ljudima gdje god bili da koriste Internet na jednak način. Zakoni poput SOPA-e, zabrane određenih Internet stranica u pojedinim državama i zabrana dijeljenja sadržaja ne predstavljaju prepreku za korisnike TOR-a koji na jednostavan način mogu zaobići sve zabrane. Ovakve tehnike ulijevaju nadu da će Internet i u budućnosti biti slobodan medij gdje će svatko moći izraziti svoje mišljenje. S druge strane postoji veliki nedostatak u kriminalu koji se, na žalost, razvija na račun ove tehnike. Kao što to inače biva, ne koriste svi ljudi ono što im se pruži u plemenite svrhe. Kriminalne usluge i stranice koje se razvijaju uz pomoć TOR-a potrebno je ograničiti i ukloniti. No rješenje nije u zabrani tehnike *Onion routinga* ili u zabrani korištenja TOR-a, nego vlada i policija diljem svijeta trebaju naći drugačiji način da stanu na kraj trgovcima droge i oružja koji se kriju iza anonimnosti koju im pruža *Onion routing*.

8. Leksikon pojmova

DES - DES algoritam šifriranja

Vrlo popularan kriptografski standard, danas zamijenjen standardom AES. - Vrlo popularan kriptografski standard, danas zamijenjen standardom AES. Tajni ključ za šifriranje podataka sastoji se od 56 bita, što znači da postoji ukupno 2^56 (više od 72,000,000,000,000,000) mogućih kombinacija. Za šifriranje poruke se koristi jedan od ključeva iz velikog broja kandidata. Algoritam je simetričan, što znači da obadvije strane moraju imati tajni ključ kako bi mogli komunicirati.

Reference: http://nvl.nist.gov/pub/nistpubs/sp958-lide/250-253.pdf

Ostale poveznice:

http://en.wikipedia.org/wiki/Data_Encryption_Standard

Kolačić

Datoteka koja sadrži podatke o posjeti web stranici. Na taj način vlasnici web stranice rade statistiku posjeta. Cookie također pamti neke postavke koje ste namjestili i podatke koje ste upisali na posjećenoj stranici (npr. lozinku). cookie datoteka.

Reference: http://www.httpwatch.com/httpgallery/cookies/

Ostale poveznice:

http://webdesign.about.com/cs/cookies/a/aa082498a.htm
http://www.nczonline.net/blog/2009/05/05/http-cookies-explained/

DOS napad

Napad uskraćivanjem usluge - Napad na sigurnost na način da se određeni resurs opterećuje onemogućujući mu normalan rad.

Reference: http://searchsoftwarequality.techtarget.com/definition/denial-of-service

Ostale poveznice:

http://www.webopedia.com/TERM/D/DoS_attack.html
http://en.wikipedia.org/wiki/Denial-of-service_attack

MITM napad - Napad ubacivanjem posrednika

Napad na sigurnost pri kojem se zlonamjerni napadač umiješa u komunikaciju na način da se postavi između sugovornika te čita i izmjenjuje poruke.

Reference: https://www.owasp.org/index.php/Man-in-the-middle_attack

Ostale poveznice:

http://www.bsacybersafety.com/threat/man-in-the-middle.cfm
http://www.ethicalhacker.net/content/view/182/1/

Kriptologija - Znanost o kriptiranju i dekriptiranju

Znanost koja obuhvaća pojmove kritpografije i kriptoanalize. Kriptografija je umješnost izmišljanja šifri, dok je kriptoanaliza umješnost njihova probijanja.

Reference: http://searchsecurity.techtarget.com/definition/cryptology

Ostale poveznice:

http://www.math.okstate.edu/~wrightd/crypt/crypt-intro/node2.html
http://www.wisegeek.com/what-is-cryptology.htm

Usmjeritelj

Uređaj koji usmjerava pakete između računalnih mreža. Usmjeritelji su uređaji koji imaju barem dva sučelja na različitim mrežama, a usmjeravaju pakete do njihovog odredišta. Na svom putu, paketi prolaze kroz nekoliko usmjeritelja, a svaki zasebno određuje put kojim će ga dalje slati.

Reference: http://www.webopedia.com/TERM/R/router.html

Ostale poveznice:

http://searchnetworking.techtarget.com/definition/router

IP - IP protokol - Internet Protocol

IP je jedan od glavnih protokola u Internetu, a koristi se za usmjeravanja paketa kroz Internet. U tu namjenu, dodjeljuje IP adrese izvora paketa i njegovog odredišta na temelju kojih će se paketi usmjeravati kroz nekoliko računalnih mreža.

Reference: http://compnetworking.about.com/od/networkprotocolsip/g/ip_protocol.htm

Ostale poveznice:

http://en.wikipedia.org/wiki/Internet_Protocol

http://www.ietf.org/rfc/rfc791.txt

HTTP - HTTP protokol - HyperText Transfer Protocol

Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju. - Osnovna i najčešća metoda prijenosa informacija na Webu. Predstavlja protokol na aplikacijskom sloju OSI modela, a osnovna namjena je prijenos HTML dokumenata (tj. web stranica). HTTP je request/response protokol za komunikaciju između poslužitelja i klijenta. HTTP klijent, kao što je web preglednik najčešće inicira prijenos podataka nakon što uspostavi TCP vezu s udaljenim web poslužiteljem na određenom priključku. Poslužitelj konstantno osluškuje zahtjeve na određenom mrežnom komunikacijskom priključku (tipično priključak 80), čekajući da klijent inicira komunikaciju.

Reference:

http://hr.wikipedia.org/wiki/HTTP

http://www.w3.org/Protocols/

Ostale poveznice:

http://www.ietf.org/rfc/rfc2616.txt

http://compnetworking.about.com/od/networkprotocols/g/bldef_http.htm

OSI model - Open Systems Interconnection model

OSI model se koristi za standardizaciju mrežnih protokola. Definira sedam logičkih razina ili slojeva: aplikacijski, prezentacijski, sjednički, transportni, mrežni, sloj podatkovne poveznice i fizički sloj. Kontrola se prenosi iz jednog sloja u drugi, počevši od aplikacijskog sloja.

Reference: http://www.webopedia.com/quick_ref/OSI_Layers.asp

Ostale poveznice:

http://www.roseindia.net/technology/networking/osi.shtml

Kriptografija

Kriptografija je područje kriptologije koje se bavi stvaranjem kriptografskih algoritama za zaštitu podataka. Točnije, podrazumijeva stvaranje i analizu protokola i algoritama koji osiguravaju siguran prijenos i pohranu informacija, bilo u računalnoj mreži ili mediju za pohranu podataka.

Reference: http://searchsoftwarequality.techtarget.com/definition/cryptography

Ostale poveznice:

http://web.math.pmf.unizg.hr/~duje/kript/kriptografija.html

http://klub.posluh.hr/list/010/kriptografija.htm

http://fly.srk.fer.hr/~peloquin/

Cyber kriminalac

Cyber kriminalac je osoba koja koristi računala i Internet za počinjenje kaznenih dijela.

Reference: http://www.webopedia.com/TERM/C/cyber_crime.html

Ostale poveznice:

http://www.cybercitizenship.org/crime/crime.html

Patent

Patent je isključivo pravo koje se priznaje za izum kojim se daje novo rješenje nekog tehničkog problema. Priznaje se za izume koji se odnose na određeni proizvod, postupak ili primjenu. Patentom se njegovom vlasniku osigurava isključivo pravo na izradu, korištenje, stavljanje u promet ili prodaju izuma zaštićenog patentom.

Reference: http://www.dziv.hr/hr/intelektualno-vlasnistvo/patenti/

9. Reference

[1] Wikipedia: Onion routing, http://en.wikipedia.org/wiki/Onion_routing, rujan 2012.

[2] Onion routing, http://www.onion-router.net/, rujan 2012.

[3] Torpoject, https://www.torproject.org/, rujan 2012.

[4] Better onion anonymity possible, http://www.theregister.co.uk/2012/08/20/making_onion_networks_more_secure/, rujan 2012.

[5] What is Dark Internet, http://www.rogerdavies.com/2011/06/dark-internet/, rujan 2012.

[6] Shopping on The Dark Web, http://www.sabotagetimes.com/life/shopping-on-the-dark-web-pure-drugs-and-plastic-explosives/, rujan 2012.

[7] Wikipedia: Bitcoin, http://en.wikipedia.org/wiki/Bitcoin, rujan 2012.

[8] Wikipedia: Stop Online Piracy Act, http://en.wikipedia.org/wiki/Stop_Online_Piracy_Act, rujan 2012.

[9] Wikipedia: OSI model http://en.wikipedia.org/wiki/OSI_model, rujan 2012.

[10] Wikipedia: Internet communication, http://en.wikipedia.org/wiki/Internet, rujan 2012.

[11] Wikipedia: Garlic routing, http://en.wikipedia.org/wiki/Garlic_routing, rujan 2012.

[12] Wikipedia: Anonymous P2P, http://en.wikipedia.org/wiki/Anonymous_P2P, rujan 2012.

[13] Wikipedia: Java Anon Proxy, http://en.wikipedia.org/wiki/Java_Anon_Proxy, rujan 2012.