Kriptografija i sigurnost Onion protokola

Tončetić, Lea

Master's thesis / Diplomski rad

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Pula / Sveučilište Jurja Dobrile u Puli**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:137:488874

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-28**

Image not found or type unknown

Repository / Repozitorij:

Digital Repository Juraj Dobrila University of Pula

zir.nsk.hr

Image not found or type unknown

Sveučilište Jurja Dobrile u Puli
Fakultet Informatike u Puli

LEA TONČETIĆ

KRIPTOGRAFIJA I SIGURNOST ONION PROTOKOLA

Diplomski rad

Pula, rujan 2019.

Sveučilište Jurja Dobrile u Puli
Fakultet Informatike u Puli

LEA TONČETIĆ

KRIPTOGRAFIJA I SIGURNOST ONION PROTOKOLA

Diplomski rad

JMBAG: 0242023431, redoviti student

Studijski smjer: Informatika

Predmet: Kriptografija

Znanstveno područje: Društvena znanost
Znanstveno polje: Informacijske i komunikacijske znanosti
Znanstvena grana: Informacijski sustavi i informatologija

Mentor: dr.sc.Siniša Miličić

Pula, rujan 2019.



IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani Lea Tončetić, kandidat za magistra informatike ovime izjavljujem da je ovaj Diplomski rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Diplomskog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student
Lea Tončetić

U Puli, 25. rujna, 2019. godine

IZJAVA

o korištenju autorskog djela

Ja, Lea Tončetić dajem odobrenje Sveučilištu Jurja Dobrile u Puli, kao nositelju prava iskorištavanja, da moj diplomski rad pod nazivom Kriptografija i sigurnost Onion protokola koristi na način da gore navedeno autorsko djelo, kao cjeloviti tekst trajno objavi u javnoj internetskoj bazi Sveučilišne knjižnice Sveučilišta Jurja Dobrile u Puli te kopira u javnu internetsku bazu završnih radova Nacionalne i sveučilišne knjižnice (stavljanje na raspolaganje javnosti), sve u skladu s Zakonom o autorskom pravu i drugim srodnim pravima i dobrom akademskom praksom, a radi promicanja otvorenoga, slobodnoga pristupa znanstvenim informacijama.

Za korištenje autorskog djela na gore navedeni način ne potražujem naknadu.

U Puli, 25. rujna 2019. godine

Potpis

Lea Tončetić

SADRŽAJ

1. UVOD 1
2. ONION PROTOKOL 2
2.1. PREDNOSTI I NEDOSTACI ONION PROTOKOLA 5
2.2. ODABIR ČVOROVA I PRIJENOS PODATAKA 6
3. TOR 7
3.1. POVIJEST TOR-A 9
3.2. TEHNIČKA POZADINA TOR-A 10
3.2.1. IMENIK TOR ČVOROVA 10
3.2.2. ZAŠTITNICI ULAZA 11
3.2.3. MOSNI TOR ČVOROVI 12
3.2.4. SAKRIVENI TOR SERVISI 12
3.3. POSTUPAK INSTALACIJE TOR BROWSERA 13
3.4. KORIŠTENJE TOR BROWSERA 15
3.5. SIGURNOST TOR MREŽE 17
3.6. GUARD NODES – ZAŠTITNI ČVOREVI 22
3.7. PRIKAZ UČESTALOSTI KORIŠTENJA TOR MREŽE 23
4. NAPADI NA TOR MREŽU 27
4.1. VRSTE NAPADA 27
4.2. MODELI NAPADAČA NA TOR MREŽU 31
4.5. TIMING ATTACK 33
5. ANONIMNOST, KRIPTOGRAFIJA I PROTOKOLI KORIŠTENI U TOR MREŽI 35
5.1. ANONIMNOST 35
5.2. KRIPTOGRAFIJA 35
5.3. TLS 35
5.4. RSA 36

5.5. DIFFIE – HELLMANOV PROTOKOL 37
6. SIMULACIJA TIMING ATTACK NAPADA 39
6.1. O SIMULUACIJI 40
6.2. TOR i SSFNet 41
6.3. IMPLEMENTACIJA TOR-a i SSFNet-a 42
6.5. TOPOLOGIJA 43
6.6. NAPAD I REZULTAT 44
6.12. ALATI 53
6.13. KORACI U PROVEDBI ISTRAŽIVANJA 54
6.14. MJERENJE UČINKOVITOSTI NAPADA 55
7. ZAKLJUČAK 59
POPIS SLIKA 63

1. UVOD

Tema ovog diplomskog rada je kriptografija te sigurnost korištenja Onion protokola. Pretraživanje Interneta te korištenje društvenih mreža dio su našeg svakodnevnog života. Prilikom korištenja društvenih mreža poput Facebooka, Instagrama, Twittera ne razmišlja se o negativnim aspektima prilikom dijeljenja osobnih podataka, slika, lokacija na kojima se nalazimo. Pregledavanjem društvenih mreža zlonamjerni korisnici mogu iskoristiti naše podatke na nepoželjan način. No, ne predstavljaju samo društvene mreže probleme sa privatnošću. Kada bezazleno „surfamo“ Internetom pretraživajući stvari koje si želimo primjerice kupiti, „web agenti“ prate naše aktivnosti, te se vrlo često dešava da se nakon pretraživanja u donjem kutu ekrana javljaju oglasi sa artiklima koji su traženi. Kako bi se očuvala privatnost, odnosno anonimnost prilikom pretraživanja weba potrebno je koristiti Tor pretraživač. Tor je vrsta pretraživača poput Chroma / Firefoxa, no za razliku od njih omogućava da prilikom pretraživanja mreže nitko ne može pratiti aktivnosti korisnika. Tor radi na Onion principu, što znači da je protokol građen na principu luka te se sastoji od više slojeva.

U prvom dijelu diplomskoga rada biti će kroz uvod objašnjena tema i cilj diplomskog rada.

Drugi dio veže se uz Onion protokol te način na koji funkcionira, te biti će navedene njegove prednosti i nedostaci.

Treći dio diplomskog rada veže se uz TOR. Biti će objašnjeno što je to Tor, kako je tekao razvoj Tor-a kroz povijest. Biti će objašnjena i slikama popraćena implementacija Tor Browsera te korištenje Tor Browsera.

U četvrtom dijelu biti će riječ o napadima na Tor mrežu.

Peti dio diplomskog rada odnosi se na anonimnost te na korištene kriptografske metode i protokole.

Šesti dio veže se uz simulaciju timing attack napada, biti će opisane razne metode simulacije i napada, te koja od njih najviše ugrožava anonimnost Tor mreže.

Sedmi dio diplomskog rada pripada zaključku.

2. ONION PROTOKOL

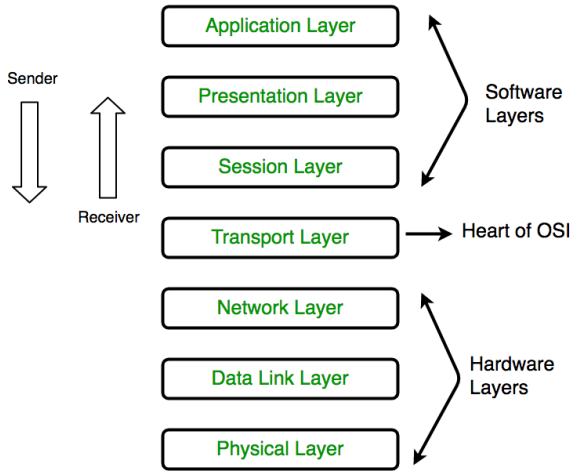
Onion protokol je naziv za tehnologiju anonimne komunikacije koja se odvija putem računalnih mreža. Engleska riječ „onion“ u prijevodu znači luk. Analogija s lukom na najbolji način opisuje podatkovnu strukturu. Zadatak svakog usmjerivača je da nakon primitka poruke „guli“ jedan sloj luka na način da koristi vlastiti privatni enkripcijski ključ te na taj način dolazi do potrebnih podataka kako bi mogao usmjeriti ostatak podatkovne strukture. Ostatak podatkovne strukture sastoji se od poruke te uputa za usmjeravanje. Onion usmjerivač funkcionira na način da početnu poruku kriptira u više slojeva, dok svaki sljedeći usmjerivač dekriptira po jedan sloj. Onion usmjeravanje predstavlja anonimnu komunikaciju unutar računalne mreže koja je razvijena od strane Davida Goldschagla, Michaela Redda i Paula Sysversona. Onion usmjeravanje temelji se na izmiješanim mrežama Davida Chuma, no podrazumijeva brojne izmjene i nadogradnje koje uključuju uvođenje koncepta Onion usmjerivača.[1]

Onion usmjeravanje je tehnika pomoću koje se korištenjem kriptografije i prosljeđivanjem poruka kroz niz posrednika povećava anonimnost korisnika Interneta. S obzirom da je TOR program koji je nastao u sklopu projekta „The Onion routing“ on ima zadatak implementiranja tehnike Onion usmjeravanja, te njegovim korištenjem korisnici mogu anonimno pretraživati Internet, razgovarati ili dijeliti digitalne sadržaje. Ideja Onion usmjeravanja je da se pošalje poruka kroz više čvorova u mreži na način da svaki čvor dešifrira dio poruke. Najprije se kriptira početna poruka na način da izvor kriptira poruku u više slojeva. Dok svaki sljedeći usmjeritelj ima zadatak da dekriptira po jedan sloj. Prilikom komunikacije unutar neke mreže nužno je da poruka koja se prenosi između čvorova ima unaprijed dogovorenu strukturu. OSI model komunikacije sastoji se od 7 slojeva.[2]

1 CarNet Hrvatska akademska i istraživačka mreža, „Tor – mreža za anonimnost“ CCERT-PUBDOC-2007-07-197, Revizija V1.1, 2007., str 7/15. Dostupno na: CERT.hr, (pristupljeno 16.lipnja 2018.).

2 Centar informacijske sigurnosti,“Onion routing“, CIS-DOC-2012-09-061, 2012., str. 5. Dostupno na CIS.hr, (pristupljeno: 18. lipnja 2018.).

Izvor 1.https://www.geeksforgeeks.org/layers-osi-model/



Slika 1. Prikaz OSI modela

Prilikom slanja poruke primjenskim programom na poslani tekst se na svakom od slojeva dodaju zaglavlja. Može se reći da su od sedam slojeva OSI modela najvažniji transportni i mrežni sloj koji se brinu za komunikaciju između dviju krajnjih točaka. Zadaća mrežnog sloja je ispravno usmjeravanje paketa unutar mreže dok je zadaća transportnog sloja pouzdana usluga. Oba sloja na poslanu poruku nadodaju svoja zaglavlja kao što su to činili i slojevi prije njih. S obzirom na to da dva čvora koja žele komunicirati uglavnom nisu smještena na istoj mreži, tada je nužno da paketi pomoću kojih komuniciraju prođu kroz više čvorova do samog odredišnog čvora.

Primjerice, ukoliko bi student želio sa svoga računala otvoriti Internetsku stranicu Sveučilišta Jurja Dobrile u Puli, tada taj zahtjev prolazi kroz niz čvorova dok ne dođe do odredišta. Na isti način će se podaci koji je Sveučilišni poslužitelj poslao vraćati kroz niz čvorova.

TOR mreža štiti korisnike od analize prometa (eng. traffic analaysis).[3] To je oblik nadzora Internet aktivnosti korisnika koji omogućavaju utvrđivanje izvorišta i odredišta komunikacije. Podatkovni paketi na Internetu građeni su od korisničkih podataka i zaglavlja koje se koristi za njihovo usmjeravanje. Korisnički podaci su podaci koji se šalju poput elektroničkih pisama, web stranica, itd. Iako su podaci kriptirani analizom

3 Ibidem., str. 5/15

prometa moguće je puno saznati o korisnikovim aktivnostima te o podacima koje šalje ili prima. Sama analiza je usmjerena na zaglavlje paketa što uključuje izvorište, odredište, veličinu te vrijeme slanja. Problematika privatnosti leži u tome da primatelj može saznati podatke o pošiljatelju ukoliko analizira zaglavlja paketa. Jednostavniji oblik analize prometa predstavlja presretanje paketa na putu od izvorišta ka odredištu te pregledavanjem njihovih zaglavlja. Kako bi se onemogućila analiza prometa, komunikacija se distribuira preko većeg broja posrednika od kojih niti jedan ne poznaje izvorište ni odredište paketa. Svaki pojedini poslužitelj zna od koga je zaprimio određeni paket te kome ih treba proslijediti. Kako bi se sve to postignulo koristi se zasebni enkripcijski ključ u svakom koraku. Samim time, TOR mreža omogućuje isključivo zaštitu prema TCP protokolu. Moguće joj je pristupiti svim aplikacijama koje podržavaju SOCK (eng. SOCKETS) protokol. [4] Onion usmjerivači provode enkripciju podataka koji su korišteni za usmjeravanje u nekoliko enkripcijskih slojeva.

Onion usmjeravanje se koristi kako bi se očuvala privatnost kako pošiljatelja poruke tako i primatelja poruke, no najbitnije je zaštititi sadržaj poruke koji putuje mrežom. Poslana poruka mrežom putuje preko niza posrednih poslužitelja (eng.proxy server). Posredni poslužitelji se koriste kako bi poruku preusmjerili na nepredvidljiv način. Kako bi se onemogućilo prisluškivanje poruke tijekom putovanja mrežom poruku je potrebno kriptirati. Poruke u Onion mreži su višestruko kriptirane, te ukoliko napadač upije pristupiti jednom ili čak više Onion poslužitelja anonimnost komunikacije neće biti ugrožena. U slučaju da napadač uspije pristupiti svim poslužiteljima tada dolazi do ugrožene tajnosti sadržaja poruke, primatelja i pošiljaoca.

Mreže Onion usmjerivača prilikom usmjeravanja koriste posebne podatkovne strukture koje služe za uspostavljanje veze putem kojih se šalju poruke. Podatkovna struktura se formira na način da onaj usmjerivač kojeg postavimo kao početni nasumičnim odabirom bira određeni broj usmjerivača, te svaki od njih prima poruku koja sadrži simetrični ključ koji se koristi za dekriptiranje poruke te upute koja je potrebna prilikom prosljeđivanja poruke idućem usmjerivaču. Dakle, svaka od poruka kriptirana je javnim ključem pojedinog usmjerivača. Podatkovna struktura građena je po slojevima. Slojevi se dekriptiraju od vanjskih prema unutarnjima. Podatkovna

4 Ibidem, str. 6/15

struktura se koristi za uspostavljanje veze za slanje poruka. Početni usmjerivač slučajnim izborom bira određeni broj onion usmjerivača te svakome šalje poruku koja sadrži simetrični ključ za dekripciju podataka te upute za prosljeđivanje poruke idućem usmjerivaču. Svaka od poruka kriptirana je javnim ključem odgovarajućeg usmjerivača. Onion usmjeravanje primatelju poruke omogućuje slanje odgovora bez otkrivanja identiteta dviju strana te korištenje podatkovne strukture za odgovaranje na poruke (eng. replay onion). Onion za odgovaranje sadrži opis puta natrag prema pošiljatelju. Važno je za napomenuti da pošiljatelj stvara onion i onion za odgovaranje koji se dostavlja zajedno sa poslanom porukom.

2.1. PREDNOSTI I NEDOSTACI ONION PROTOKOLA

Onion protokol omogućava individualnim korisnicima ili pak skupini korisnika da anonimno komuniciraju putem Interneta bez bojazni da netko prati njihove aktivnosti i komunikaciju. Nadalje, Onion protokol omogućava pojedincima koji imaju zabranu pristupa web stranicama poput Vladinih stranica, da tim stranicama ipak pristupe. Osobe koje su žrtve nasilja ili pak boluju od pojedinih bolesti mogu komunicirati putem različitih foruma bez da itko sazna njihov identitet. Samim time se kao najveća prednost Onion protokola ističe anonimnost. Time se promiču ljudska prava i demokracija te pravo slobode govora. Što se nedostataka tiče, Onion protokol sa jedne strane korisnicima Interneta omogućava pravo da štite svoju privatnost, no sa druge strane zlonamjernim korisnicima služi za sakrivanje njihovih aktivnosti. Ukoliko zlonamjerni korisnici nelegalno kopiraju te distribuiraju materijale sa filmske i glazbene industrije policija ni Vlada ne mogu im ući u trag.[5]

5 Centar informacijske sigurnosti,“Onion routing“, CIS-DOC-2012-09-061, 2012., str. 10. Dostupno na CIS.hr, (pristupljeno: 18. lipnja 2018.).

2.2. ODABIR ČVOROVA I PRIJENOS PODATAKA

TOR klijent odabire čvoreve kruga vodeći se zastavicama koje im je dodijelio odredišni server za vrijeme glasanja. Sa sigurnosne perspektive sljedeća pravila su najvažnija za odabir čvorova :

1. Niti jedan relay se ne odabire dvaput
2. Iz iste obitelji odabire se samo po jedan relay. Potiče se operatore relaya da se tijekom konfiguracije relaya navede tko pripada istoj obitelji, odnosno svaki od relaya u krugu trebao bi biti kontroliran od strane drugog operatora
3. Odabire se samo jedan relay koji iznosi /16 IP podmreže. Ovo upućuje na to da nisu svi relayevi blizu locirani što znači da dva relaya mogu biti promatrana od strane napadača u isto vrijeme
4. Entry node, ulazni čvor mora imati guard flag

Nakon što Tor klijent odabere tri čvora, krug čvorova se gradi. Veza između dva relaya, odnosno između klijenta i relaya osigurana je TLS – om. Klijent osigura TLS vezu na ulaznom čvoru, te isto to rade svi čvorovi u krug. TLS se koristi za prijenos podataka u Tor protokolu, primjerice za kreiranje krugova i prijenos podatak kroz krug. Višestruki krugovi multipleksirani su unutar TLS veze. TLS se iskorištava na način da vanjski napadač može izmijeniti podatke poslane kroz vezu, ili mogu pak pogledati vezu. Kako se TLS veze koristi za prijenos podataka u Tor protokolu, tako je Tor osmislio ćelije fiksnih veličina koje si dijele na dvije vrste : control cells i relay cells.

Control cells se razmjenjuju između dva susjedna čvora te se te su uvijek protumačene od strane čvora koji ih prima. Rellay cells su kriptirane se serijom ključeva. Posrednik čvorova u krugu ne može vidjeti značenje relay cells te tada samo prenosi na susjedan čvor u krugu.

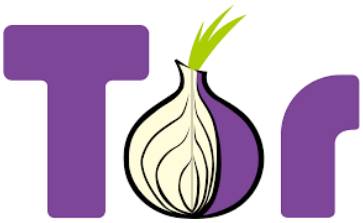
3. TOR

Tor je skraćenica od The Onion Router. Dakle, kao što i samo ime govori Tor je program koji se temelji na principu Onion Routinga. S obzirom na to da su Tor i Onion routing sinonimni, važno je za napomenuti da se Onion routing promatra kao ideja, dok je Tor implementacija programa.

Tor je jedna od najpoznatijih mreža koja se koristi za anonimnu komunikaciju. Što se više korisnika zainteresira za anonimnu komunikaciju, to će korištenje Tor mreže porasti. Tor se koristi za različite aktivnosti koje uključuju pretraživanje web-a, prijenos podataka te razmjenu poruka. Također, neke od vrlo bitnih značajki Tor-a su fleksibilnost, upotrebljivost te jednostavan dizajn. Tor protokol uključuje kriptografski algoritam toka, kriptografiju javnog ključa, hash funkciju te Diffie–Hellmanov protokol.[6]

.

Izvor 2.https://upload.wikimedia.org/wikipedia/commons/1/15/Tor-logo-2011-flat.svg



Slika 2. Tor logo

Kako bi promet kroz Tor mrežu bio jedinstven koristi se TLS protokol te vlastita simetrična i asimetrična kriptografija. TLS (eng. Transport Layer Security) je protokol čija je uloga zaštita podataka u komunikaciji te osiguravanje autentifikacije sugovornika. Koristi se u raznim domenama poput udaljenog pristupa, poruka

6 R. Dingledne, N. Mathewson i P. Syverson, „Tor: The Second-Generation Onion Router“, SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium, Vol. 13, 2004., str. 5-6.

elektroničke pošte itd. te donosi mnogo prednosti vezanih uz autentifikaciju i fleksibilnost.[7]

Prilikom korištenja simetrične kriptografije riječ je o 128-bitnom AES algoritmu, dok je kod asimetrične kriptografije riječ o 1024-bitnom RSA algoritmu.

AES (eng. Advanced Encryption Standard) je kriptografski algoritam koji se koristi za zaštitu digitalnih podataka. NIST (National Institute of Standards and Technology) započeo je razvoj AES standarda 1997. godine kada se pokazala potreba da se zamijeni DES standard (Data Encryption Standard) koji je postao nedovoljna zaštita za pojedine vrste napada.[8]

RSA je prvi algoritam šifre javnog ključa. To je kriptosustav kojeg su izumili trojica znanstvenika Ron Rivest, Adi Shamir i Len Adleman 1977. godine. Kriptopustav je dobio ime po početnom slovu prezimena znanstvenika. Sigurnost RSA kriptosustav zasnovana je na teškoći faktorizacije velikih cijelih brojeva. RSA je asimetričan kriptosustav što znači da je potrebno generirati par ključeva, privatni i javni.[9]

Kako bi cijeli sustav ispravno funkcionirao koristi se i Diffie-Hellmanov protokol te SHA-1 algoritam.[10]

Diffie – Hellmanov protokol objavljen je 1976.godine, a koristi se za razmjenu tajnog ključa. Omogućava razmjenu tajnih ključeva no bez prethodnog dogovora. Protokol je dobio naziv po tvorcima Whitfieldu Diffie i Martinu Hellmanu.

Tor mreža se temelji na višeslojnom umrežavanju. Svaki onion ruter se pokreće poput normalnog korisničkog procesa pritom ne koristeći nikakve posebne funkcije. Dakle, svaki onion ruter sadrži TLS vezu na svaki od preostalih onion rutera. Svaki od korisnika pokreće lokalni softver koji se naziva onion posrednik (eng. proxy) pa sve do središnjih direktorija(eng. fetch directories), zatim uspostavlja krugove kroz mrežu te

7 CarNet Hrvatska akademska i istraživačka mreža, „TLS protokol“ CCERT-PUBDOC-2009-03-257, Revizija 1.04, 2009., str 4-5/29. Dostupno na: CERT.hr, (pristupljeno 20. lipnja 2018.).

8 CarNet Hrvatska akademska i istraživačka mreža, „AES algoritam“, CCERT-PUBDOC-2003-08-37, revizija v1.1, 2003., Dostupno na: CERT.hr, (pristupljeno 15. srpnja 2018.).

9 AMI Familiy, „How does RSA work?“ [website], 2017., https://hackernoon.com/how-does-rsa-work-f44918df914b (pristupljeno: 15. srpnja 2019.).

10 V. Ubavić i D. Oklonđija, „Ostvarivanje anonimnosti na Internetu korištenjem Tor mreže“, Visoka poslovna škola profesionalnih studija – Blace, Časopis za ekonomiju, menadžment i informatiku 2013., Vol.2, 2013., str. 45

rukovodi vezama korisničke aplikacije. Onion posrednici prihvaćaju TCP tokove te ih umnožavaju kroz krugove. Onion ruter koji se nalazi na drugoj strani krugova spaja se na zahtijevano odredište. Svaki od Onion rutera sadrže dugoročni identifikacijski ključ i kratkoročni Onion ključ. Identifikacijski ključ se koristi za potvrđivanje TLS certifikata te za potpisivanje direktorija. Onion ključ se koristi za dekriptiranje zahtjeva od strane korisnika da se kreira krug. Kratkoročni ključevi se izmjenjuju periodično te samostalno kako bi se ograničio utjecaj ključnih kompromisa. TLS protokol također uspostavlja kratkoročni ključ prilikom komunikacije između Onion rutera. Dakle, Tor se temelji na tehnologiji slojevitog usmjeravanja.

3.1. POVIJEST TOR-A

Termini vezani uz Tor i Onion usmjeravanje počeli su se upotrebljavati 1996. godine, te se to doba naziva „nulta generacija.“. Nulta generacija podrazumijeva osnovne principe nastanka Tor-a. Razvijena je od strane Paula Syversona koji je bio zaposlenik Američkog pomorskog laboratorija, te dvojice računalnih znanstvenika Michaela G. Reeda te Davida Goldschlaga. Njihov cilj razvoja Tora bio je u svrhu zaštite internetskih obavještajnih komunikacija SAD-a. Onion usmjeravanje razvijeno je 1997.godine od strane DARPA. DARPA[11] je agencija Ministarstva obrane Sjedinjenih Američkih Država koja za cilj ima razvoj novih tehnologija za uporabu vojske.

„Prva generacija“ kreće od početnog dizajna te sve polako vodi ka nastanku Tor mreže. „Druga generacija“ poznata pod nazivom „Tor“ trajala je od 2002. – 2004. godine. Za njezin razvoj zaslužni su Syverson koji je začetnik ideje Tor-a, te računalni znanstvenici Roger Dingledine i Nick Mathewson. The Onion Routing projekt pokrenuli su 20. rujna 2002. godine. Prvo javno predstavljanje Tor-a zbilo se 13. kolovoza 2004.godine, kada su Syverson, Dingledine i Mathewson predstavili „Tor : The Second Generation Onion Router“. U prosincu 2006. godine su Dingledine, Matheson te još nekoliko tvrtki utemeljili „The Tor Project“.[12] Dakle, Tor protokol je druga generacija

11 Defense Advanced Research Project Agency

12 N. Staletić, P. Staletić, A. Simović, „Sigurnost Tor mreže u zaštiti identiteta na Internetu“ Infoteh-Jahorina, Vol. 13., 2014., str. 914.

Onion usmjerivača koji ima za cilj mrežni promet održati anonimnim korištenjem niske latencije.

3.2. TEHNIČKA POZADINA TOR-A

Osnovni dio Tor mreže čine Tor čvorovi koji mogu predstavljati bilo koje računalo na kojem Tor softver funkcionira kao prenositelj poruka. Za Tor čvorove zaduženi su volonteri diljem svijeta čija je zadaća da ih postavljaju i održavaju. Tor čvorovi imaju različite uloge kao što su primjerice zaštitnici ulaza i mosni čvorovi. Vrlo bitan dio Tor mreže je imenik Tor čvorova.[13]

3.2.1. IMENIK TOR ČVOROVA

Tor mreža ne može funkcionirati bez imenika Tor čvorova. Prilikom spajanja korisnika na Tor mrežu putem Tor aplikacije koja je instalirana na računalu potrebno je istražiti koji su čvorovi dostupni. S obzirom na to da su u Tor softver ugrađene IP adrese te kriptografski ključevi oni omogućavaju sigurno pristupanje Tor čvorovima.

Radnje koje Tor softver obavlja prilikom pretraživanja dostupnih čvorova su sljedeće:

Tor softver ponajprije preuzima popis Tor čvora neovisno o tome koji imenik koristi. Vrlo je bitno da preuzeti popis digitalno potpišu svi imenici Tor čvorova. Zatim korištenjem ugrađenih kriptografskih ključeva provjerava koliko je zaista Tor čvorova na ispravan način potpisalo preuzeti popis. Ukoliko je preuzeti popis na ispravan način potpisalo više od pola imenika Tor čvorova tada se on smatra valjanim te se može koristiti prilikom spajanja na Tor mrežu. Cijeli ovaj postupak koji izvodi Tor softver provodi se kako bi se u slučaju napada na popis čvorova Tor mreže otežalo na način da mora zapravo kompromitirati više od polovice imenika Tor čvorova. Dakle, digitalno potpisani potpis Tor čvorova namijenjen je korisnicima Tor mreže. Volonteri koji se

13 CarNet Hrvatska akademska i istraživačka mreža, „Tor mreža – tehnička pozadina i napredno korištenje“, NCERT-PUBDOC-2018-2-356, 2018., str. 5/20. Dostupno na: CERT.hr, (pristupljeno: 15. studeni 2018.).

brinu o Tor čvorovima su osobe koje su vrlo dugo aktivne u Tor zajednici te u koje Tor zajednica ima vrlo visoku razinu povjerenja. [14]

Na slici 3. su prikazani detalji koje sadrže imenici Tor čvorova.

Izvor 3.https://metrics.torproject.org/rs.html#search/flag:authority



flag:authority

Show 10 entries

Nickname†	Advertised Bandwidth	Uptime	Country	IPv4	IPv6	Flags	Add. Flags	ORPort	DirPort	Type
dizum (1)	3.07 MiB/s	29d 21h		194.109.206.212	-			443	80	Relay
Serge (1)	1.61 MiB/s	6d 3h		66.111.2.131	2610:1c0:0:5::131			9001	9030	Relay
moria1 (1)	500 KiB/s	14d 21h		128.31.0.34	-			9101	9131	Relay
tor26 (1)	75 KiB/s	3d 7h		86.59.21.38	2001:858:2:2:aabb:0:563b:1526			443	80	Relay
bastet (1)	50 KiB/s	31d 2h		204.13.164.118	2620:13:4000:6000::1000:118			443	80	Relay
maatuska (8)	50 KiB/s	15d 4h		171.25.193.9	2001:67c:289c::9			80	443	Relay
dannenberg (1)	40 KiB/s	3d 22h		193.23.244.244	2001:678:558:1000::244			443	80	Relay
Faravahar (1)	40 KiB/s	72d 16h		154.35.175.225	2607:8500:154::3			443	80	Relay
gabelmoo (1)	40 KiB/s	83d 3h		131.188.40.189	2001:638:a000:4140::ffff:189			443	80	Relay
longclaw (1)	38 KiB/s	2h 51m		199.58.81.140	-			443	80	Relay
Total	5.49 MiB/s									

Slika 3. Prikaz popisa imenika Tor čvorova

3.2.2. ZAŠTITNICI ULAZA

Koncept zaštitnika ulaza (eng. entry guards) uveden je kako bi se spriječilo da napadač ima kontrolu nad ulaznim odnosno, prvim Tor čvorom pojedinog korisnika. Iako je Tor mreža većim dijelom sigurna postoji mogućnost da napadač naruši anonimnost korisnika u slučaju da uspije nadzirati oba kraja komunikacije. Dakle, ukoliko napadač ima kontrolu nad ulaznim čvorom kojeg određeni korisnik koristi tada ima i kontrolu nad onom stranicom koju korisnik posjećuje. Ukoliko stranica koju je korisnik posjetio istovremeno ima više korisnika, tada napadač ne zna tko je od njih korisnik kojeg „prati“ niti što radi na web stranici. Da bi napadač doznao posjećuje li praćeni korisnik stranicu te što pretražuje koristi metodu analize prometa što znači da uspoređuje vrijeme i veličinu paketa koju korisnik šalje u Tor mrežu te i paketa koji stižu na posjećenu web stranicu. Metodom analize prometa i pristupom ulaznom i izlaznom čvoru narušava se privatnost korisnika. Kako bi se spriječilo da napadač pristupi ulaznom čvoru koristi se koncept zaštitnika ulaza što znači da će Tor softver prilikom spajanja na Tor mrežu birati kao ulazne čvorove samo one čvorove koji sadrže

14 Ibidem, str. 6/20

zastavicu zaštitnika (eng. guard flag). Zastavicu zaštitnika imenici Tor čvorova dodjeljuju samo određenim čvorovima, odnosno onim čvorovima koji su određeni period dio mreže i koji obrađuju veću količinu prometa.[15]

3.2.3. MOSNI TOR ČVOROVI

Mosni Tor čvorovi (eng. Tor bridges) su koncept koji omogućavaju blokiranje Tor mreže. Do blokiranja Tor mreže može doći iz raznih razloga, primjerice pružatelji mrežnih usluga mogu blokirati pristup Tor mreži. S obzirom na to da se može preuzeti popis Tor čvorova od imenika Tor čvorova sa pripadajućim IP adresama cenzori mogu vrlo jednostavno zabraniti pristup Tor mreži na način da blokiraju veze s IP adresama postojećih Tor čvorova.

Mosni Tor čvorovi pomažu prilikom sprječavanja blokiranja zato što njihove IP adrese ne postoje u javnim imenicima Tor čvorova.[16]

3.2.4. SAKRIVENI TOR SERVISI

Prilikom normalnog korištenja Tor mreže pruža se korisnicima anonimnost prilikom pregledavanja određenih web stranica što znači da im se omogućava anonimnost kako bi se komuniciralo s poslužiteljima. No isto tako je i pružateljima usluga potrebna anonimnost mrežnih poslužitelja. Tor mreža im to omogućava korištenjem Tor sakrivenih servisa. Tor sakriveni servisi imaju vrlo složenu tehničku pozadinu. To su zapravo poslužitelji koji su sakriveni unutar Tor mreže.

Tor ruter ima sposobnost obavljanja osam različitih funkcija[17] :

1. *Directory authority* funkcija je zapravo ruter koji se koristi i kao imenik

15 Ibidem, str. 6
16 Ibidem, str. 7
17 V. Ubavić i D. Oklonđija, „Ostvarivanje anonimnosti na Internetu korištenjem Tor mreže“, Visoka poslovna škola profesionalnih studija – Blace, Časopis za ekonomiju, menadžment i informatiku 2013., Vol.2, 2013., str. 45

2. *Directory cache* funkcija je ruter čiji je zadatak rasterećenje servera imenika
3. *Bridge router* funkcija je ruter koji se koristi za prijenos podataka u Tor mreži. Nalazi se u zasebnim listama koje se preuzimaju ručno te na isti način održavaju.
4. *Exit router* je funkcija rutera koja omogućava spajanje na mrežna odredišta koja se nalaze izvan okvira Tor mreže
5. *Hidden service* je funkcija rutera koja izvršava sakrivene usluge
6. *Hidden service directory* je funkcija rutera koja omogućava i pristup registru sakrivenih usluga
7. *Introduction point* je funkcija rutera koja se koristi kao čvor uvoda sakrivene usluge, ona je posrednik prilikom procesa povezivanja
8. *Rendezvous point* je funkcija rutera preko kojeg se odvija komunikacija između klijenta i sakrivene usluge

3.3. POSTUPAK INSTALACIJE TOR BROWSERA

Tor Browser je program koji se može instalirati na Windows, Linux, Mac OS X te Unix operacijskim sustavima. Kako bi se koristio Tor browser potrebno ga je preuzeti sa Interneta. S obzirom na to da je moguće preuzimanje sa više web stranica, najpoželjnije je da ga se preuzme sa https://www.torproject.org. Prilikom uvida u sadržaj stranice torproject.org odabire se ona verzija koja odgovara korištenom operacijskom sustavu. Nakon što se datoteka preuzme, javlja se prozor u kojem se odabire se željeni jezik korištenja Tor-a.

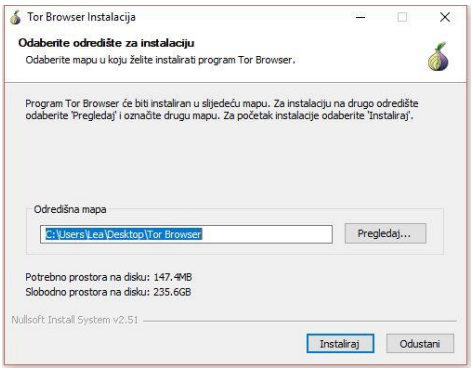
Izvor 4. Izradila autorica



Slika 4.Odabir jezika prilikom instaliranja TOR-a

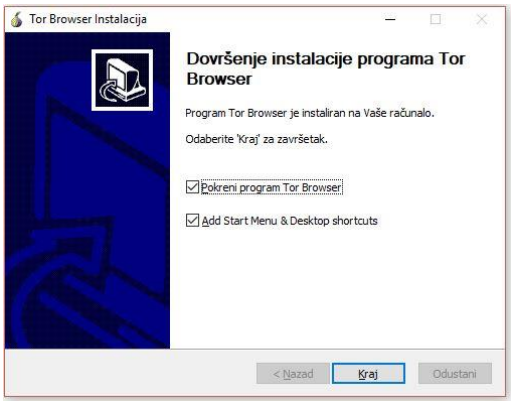
Nakon odabira jezika, odabire se mapa u koju će se prilikom instalacije spremiti Tor program. Kada se odabere mapa, odnosno mjesto pohrane Tor programa potrebno je pokrenuti instalaciju.

Izvor 5. Izradila autorica



Slika 5. Odabir mjesta pohrane Tor Browsera

Izvor 6. Izradila autorica



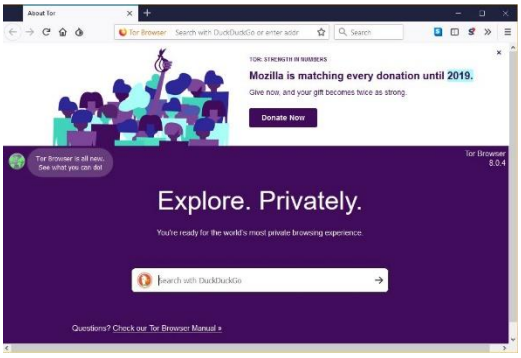
Slika 6. Prozor izgleda završetka instalacije Tor Browsera

Kada se Tor program instalira otvara se prozor u kojem se odabire želi li se da se Tor ikona pojavi na Radnoj površini, te želi li se da se automatski pokrene Tor Browser. Nakon što se odaberu željene opcije klikne se na dugme „Kraj“.

3.4. KORIŠTENJE TOR BROWSERA

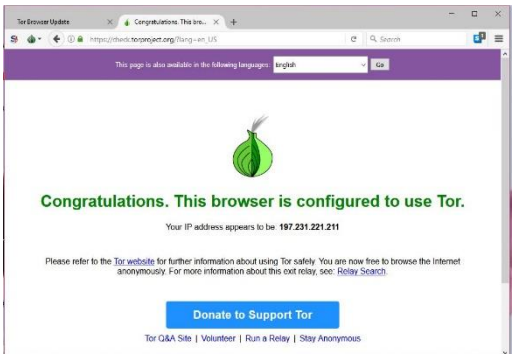
Nakon instalacije TOR preglednika na računalo, pokrećemo ikonicu „Start Tor Browser“ i otvara nam se preglednik kao na slici.

Izvor 7. Izradila autorica



Slika 7. Prikaz početne stranice Tor Browser pretraživača

Izvor 8. Izradila autorica



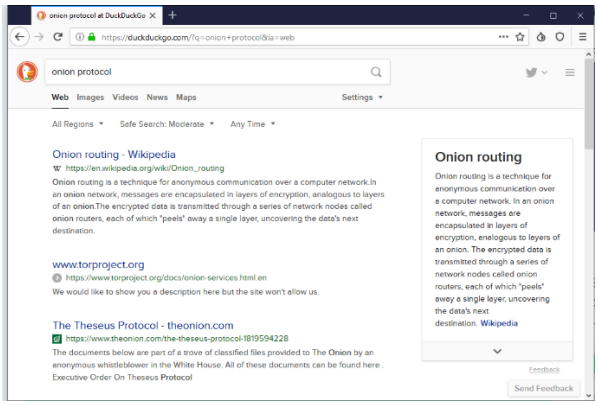
Slika 8. Prikaz ispravno konfigurianog Tor Browsera

Tor Browser se ne razlikuje znatno od ostalih alata za pretraživanje. Na slici se vidi da postoji opcija „Test for Network Settings“ na koju kliknemo kako bismo provjerili je li sve u redu sa Tor mrežom

Nakon što se klikne na „Test network settings“ otvara se zasebna kartica koja izgleda poput ove na slici 8. Kartica nam javlja da je preglednik ispravno konfiguriran za korištenje Tor mreže te nam prikazuje IP adresu.

U okviru Tor mreže postoji mnogo internetskih stranica koje se označavaju *.onion* domenom u obliku <16 alfanumeričkih znakova>.onion. Važno je za napomenuti da to nisu stvarna DNS imena, nego se ona koriste preko zahtjeva na Tor mrežu kako bi se pristupilo tim internetskim stranicama. Dakle, nije poznata IP adresa ni lokacija niti jednoj strani. Slika 9. prikazuje da se Tor Browser pretraživač izgledom ne razlikuje od svakodnevno korištenih pretraživača poput Firexofa, Opere itd.

Izvor 9. Izradila autorica



Slika 9. Pretraživanje koristeći Tor Browser

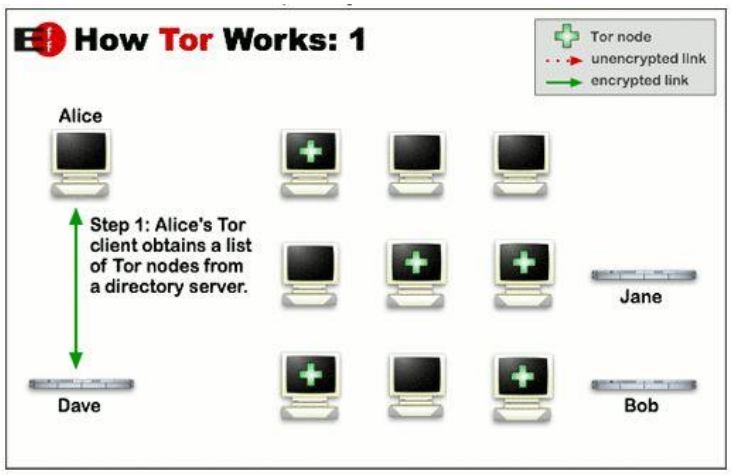
Tor browser može se koristiti i na mobilnom uređaju.

3.5. SIGURNOST TOR MREŽE

Kao što je već napomenuto, Tor mreža funkcionira na način slojevitog usmjeravanja. Kada se govori o prometu Tor mreže klijent bira put kroz mrežu koja je sačinjena od čvorova te na taj način tvori krug. U stvorenom krugu, čvor zna samo tko je poslao paket i kome paket treba proslijediti. Vrlo važna činjenica je da svaki čvor prepoznaje samo čvor od kojeg je zaprimio poruku, te čvor kojemu treba proslijediti poruku. Korisnikova komunikacija se šalje u porukama koje se na samom izvorištu višestruko kriptiraju korištenjem simetričnog ključa koji je dogovoren sa svakim od rutera. Poruke koje su kriptirane se šalju u krug. S obzirom na to da se poruka na izvorištu višestruko kriptira ona se naziva „slojevita poruka“, odnosno kako se poruka šalje od čvora do čvora tako se dekriptira po jedan sloj. Zato se i uspoređuje sa lukom, slojevita poruka predstavlja cijeli luk, kako poruka putuje od čvora do čvora nasumično tako se guli jedan po jedan sloj luka sve dok se ne dođe do zadnjeg unutarnjeg dijela luka koji predstavlja čistu poruku. Dakle, postupka dekriptiranja se ponavlja sve dok poruka ne stigne do zadnjeg čvora u već spomenutom krugu.

Na slici 10. vidimo skup računala koja su spojena na Internet, neka od računala predstavljaju i Tor čvorove preko kojih će se odvijati komunikacija. Da bi u ovom primjeru Alice mogla koristi mrežu potrebno je da na svome svom računalu instalira Tor aplikaciju koja je ujedno i posrednik. Za pristup Tor čvorovima potrebno se je povezati na server imenika u kojem se nalazi spisak svih postojećih Tor rutera.

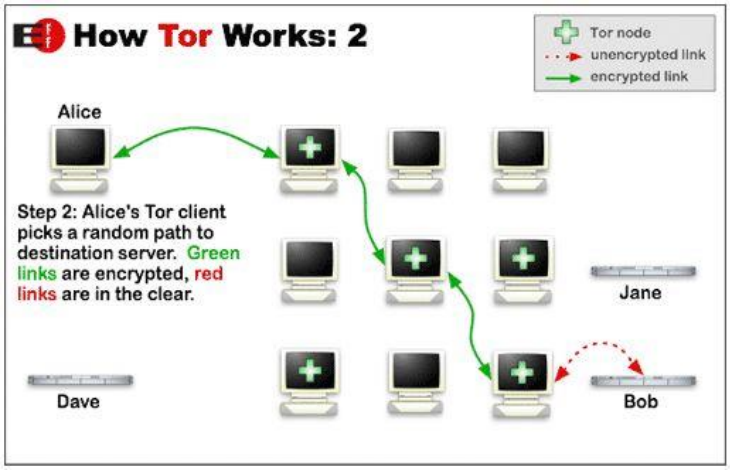
Izvor 10. https://2019.www.torproject.org/images/htw1.png



Slika 10. Prikaz TOR sustava

Alicin Tor posrednik nasumično odabire odredišni server. Na slici 11. vidi se kako se sve do posljednjeg čvora odvija sigurna komunikacija, no rizik se ističe između posljednjeg čvora i odredišne destinacije zato što je to jedini dio mreže koji nije kriptiran. Rizik između posljednjeg čvora i odredišne destinacije može se riješiti korištenjem HTTPS umjesto HTTP protokola.[18]

Izvor 11. https://2019.www.torproject.org/images/htw1.png



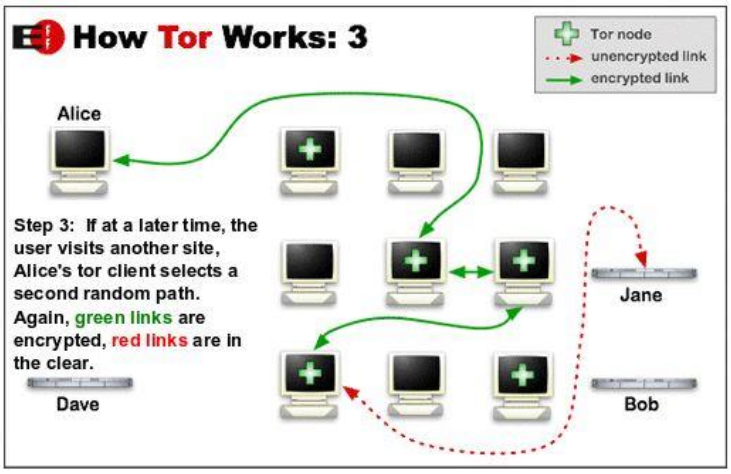
Slika 11. Prikaz dijelova sigurne i nesigurne komunikacije

.

Ukoliko Alice želi pristupiti nekoj drugoj stranici, Tor posrednik koji je instaliran na njezino računalo ponovno odabire nasumične čvorove, te se ponovno odvija siguran prijenos sve do posljednjeg čvora, dok je dio veze između posljednjeg čvora i odredišne destinacije nesiguran.

18 CarNet Hrvatska akademska i istraživačka mreža, „Tor mreža – tehnička pozadina i napredno korištenje“, op-cit., str. 5

Izvor 12. https://2019.www.torproject.org/images/htw1.png



Slika 12. Prikaz odabira nasumičnih čvorova

Kako što je već navedeno, u Onion usmjeravanju poruke su šifrirane nekoliko puta sa različitim ključevima za svaki sloj šifriranja. U TOR mreži klijent uspostavlja krug sa 3 čvora, ulazni čvor, srednji čvor i izlazni čvor, što znači da će originalna poruka primatelju poruke biti šifrirana unutar 3 sloja, jedan sloj za svaki čvor. Originalna poruka biti će poslana primatelju poruke, primjerice u obliku HTTP zahtjeva. Neka klijent, u ovome slučaju Alice šalje luk odnosno poruku šifriranu kroz 3 sloja ulaznom čvoru. Ulazni čvor dekriptira prvi sloj enkripcije i prelazi na srednji čvor. Srednji čvor guli sloj enkripcije i prelazi na idući čvor, koji je ujedno i izlazni čvor. Izlazni čvor guli posljednji sloj enkripcije, čita IP odredišta originalne poruke i vraća odgovor odredišnom serveru, primatelju poruke u ovom slučaju Bobu.

3.5. INFORMACIJSKA SIGURNOST

Tri glavna aspekta informacijske sigurnosti[19]:

- pouzdanost
- integritet
- dostupnost

Pouzdanost se može povezati sa enkripcijom informacija u smislu da samo korisnici u određenom položaju mogu dekriptirati i čitati enkriptirane podatke. Ne skriva tko komunicira sa kime. Pouzdanost može postići zasebnu komunikaciju, no ne i anonimnost. Različiti korisnici komuniciraju preko iste anonimne mreže te pružaju prekriven promet.

Istraživanja o anonimnosti sežu do Chaumns mix mreža. Mix je računalo koje prima poruke, originalne e-mailove, kašnjenja, reorganizira te ih baca u hrpu poruka. Mixes se mogu kombinirati kaskadno, gdje mixes šalju hrpu poruka od jednog mix-a do drugog u namjeri da se na teži način sazna tko je pokretač poruke.

U Chaumns dizajnu poruke su kriptirane po slojevima sa javnim ključem enkripcije te svaki mix miče jedan sloj enkripcije. Osnovni dizajn mješavina kaskada temeljni je za svaki sustav anonimnosti. Anonimni sustavi podijeljeni su na sustave niske i visoke latencije anonimnosti sustava. Visoka latencija sustava sadrži globalnog napadača koji ima sposobnost promatrati cijelu mrežu, sve ulazne poruke, prijelazne i izlazne.

U namjeri da se obrane od ovako jakog napadača uvode veliko nasumično kašnjenje prije nego je poruka poslana te je iz ovog razloga prikladno za aplikacije toleriranja visoke latencije poput e-maila. Takav sustav pruža vrlo visoku sigurnost, no nije pogodno za interaktivne aplikacije zato što korisnici očekuju brze odgovore takvi aplikacija.

[19] Müller K., Defending End-to-End Confirmation Attacks against the Tor Network, Department of Computer Science and MTDMT Technology, 2015, str. 5

Sustavi niske latencije kao što je TOR imaju slabiji model te se ne pokušavaju braniti globalnog napadača te ne dopuštaju velika kašnjenja sa namjerom da podupiru interaktivne aplikacije poput *web browsinga* i brzih poruka. Ovo zapravo može voditi većem stupnju anonimnosti uspoređujući sa sustavima visoke latencije. Danas je TOR najviše široko rasprostranjena implementacija anonimnosti sistema niske latencije.

Anonimni sustav treba korisnika koji omogućava promet ka drugim korisnicima. Veći skup anonimnosti može pružiti bolju anonimnost zato što je teže napadaču povezati mrežne aktivnosti pojedinih korisnika. Svaki korisnik ima različite zahtjeve u pogledu sigurnosti i anonimnosti, no i u načinu korištenja anonimnog sustava.

Vrlo osjetljivi korisnici imaju veće zahtjeve sigurnosti i anonimnosti kao i manje osjetljiviji korisnici. Imaju mogućnost odabira sustava A, koji je iznimno siguran no ima manje sposobnosti i jedino je koristan za rukovanje aplikacijama. Ovaj sustav ima manji set anonimnosti koji se sastoji od vrlo osjetljivih korisnika, te ne može osigurati dovoljno anonimnosti. Dok, primjerice sustav B, ima mnogo manje osjetljivih korisnika koji im pruža jaku anonimnost te otpornost protiv napada iako teorijski ovaj sustav nije siguran kao sustav A.

Zaključak je da je ponekada bolje za anonimnost imati više korisnika i slabiju anonimnost, nego vrlo visoki sustav anonimnosti a manje korisnika. To zapravo pokazuje da su upotrebljivost i izvođenje sustava jednako važni kao i sigurnosne i anonimne postavke. Sam siguran sustav nije dovoljan, iskoristivost je ključan faktor za privlačenje većeg broja korisnika. Vrlo je teško „izgraditi" anonimni sustav koji je u jednu ruku siguran, a i drugu iskoristiv/upotrebljiv.

Korisnici bi se trebali ponašati svi na isti način, onaj korisnik koji se ponaša drugačije od ostalih odvaja se od njih te time ga je time jednostavnije prepoznati. Mijenjanjem postavki korisnici pokušavaju povećati svoju sigurnost, no time zapravo mogu smanjiti anonimnost zato što se uspoređuju postavke jednog sustava sa postavkama preostalih sustava, te naravno one postavke koje su izmijenjene dolaze do izražaja. [20]

[20] Ibidem, str. 6

3.6. GUARD NODES – ZAŠTITNI ČVOREVI

U smislu *end to end* napada, koncept *guard nodes* je vrlo bitan za sigurnost sustava. Cilj napadača je kontrolirati ulazni i izlazni čvor u krugu kako bi mogao korelirati promet. Ukoliko napadač kontrolira C u N čvorova i čvorovi se odabiru nasumično, vjerojatnost odabira ugroženog kruga sa napadačevim praćenjem ulaznog i izlaznog čvora jednaka je $(C/N)^2$.

S vremenom ova vjerojatnost ide do 1, kada klijent gradi nasumične krugove. Napadaču je jedino potrebno sačekati na klijent stvori ugroženi krug. Koncept guard nodes pokušava ublažiti napade. *Directory authorities* dodaju *guard flag* čvorevima koji bi trebali biti korišteni kao *guard nodes*. Svaki Tor klijent odabire malu skupinu ulaznih čvorova, obično tri, te se uvijek koristi jedan od ulaznih čvorova za ulazak u krug. Kada se odabiru ulazni čvorovi, moguća su dva rezultata. Prvi, da je čvor ugrožen od strane napadača te da je ugrožen i cijeli krug. Dok je drugo moguće da čvor nije ugrožen od strane napadača te da napadač nikada neće imati priliku ugroziti krug. To zapravo povećava trošak za napadače jer zato što moraju pokrenuti mnogo čvorova u namjeri da naprave uspješan napad.

No, ova metoda ima i manu. S obzirom na to da klijenti ne mijenjaju svoje čvorove i da novi klijenti odabiru iste ulazne čvorove, trebaju nagomilati sve više i više klijenata te prometa koji trebaju izvršiti. Iz ovog razloga klijenti rotiraju svoje ulazne čvorove svakih 8 do 12 tjedana. To pomaže raspodijeliti promet kroz sve ulazne čvorove. Tor programeri rade na cilju jednog zaštitnog čvora i vremena izmjene od 9 do 10 mjeseci, zato što su istraživanja pokazala da trenutna implementacija ulaznog zaštitnog čvora ima limit.

Cilj je smanjiti napade zato što sa ovim parametrima napadač mora čekati malo duže prije nego li klijent odbere tri kontrolirana čvora.

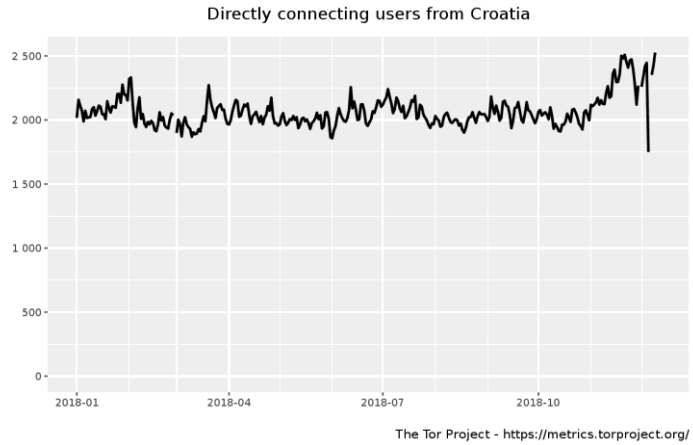
Važno je za napomenuti da dizajn *guard nodes* ne *spriječava end to end* napade, umjesto toga su dizajnirani da smanje napade te da naprave napade neprivlačnima zbog vremena koje je potrebno za pokretanje čvora.[21]

[21] Müller K., Defending End-to-End Confirmation Attacks against the Tor Network, Department of Computer Science and MTDMT Technology, 2015, str. 9, 10

3.7. PRIKAZ UČESTALOSTI KORIŠTENJA TOR MREŽE

Na Tor službenoj stranici nalaze se mnogi podaci o korištenju Tor mreže ovisno o tome spajaju li se klijenti koristeći *relay* ili pak mostove (eng. bridge), ovisno o korištenoj verziji IP adrese i sl.

Izvor 13. https://metrics.torproject.org



Slika 13. Prikaz broja direkno povezanih Tor klijenata u Hrvatskoj

Na slici 13. graf prikazuje procijenjeni broj direktno povezanih klijenata na Tor mrežu u Hrvatskoj no isključuje one klijente koji se povezuju korištenjem mostova. Graf prikazuje podatke za Hrvatsku u razdoblju od 01.01.2018. do 12.12.2018. Početkom godine u Hrvatskoj je bilo oko 2100 povezanih klijenata te je taj broj kroz cijelu godinu padao i rastao u rasponu od stotinjak klijenata. Najmanji broj povezanih klijenata bio je u mjesecu studenom i iznosio je oko 1800 klijenata, dok ih na dan 12.12.2018. ima oko 2500. Kako postoje podaci za Hrvatsku tako su dostupni i podaci za većinu zemalja svijeta.

Na sljedećoj slici 14., nalazi se tablica sa poretkom top 10 zemalja sa trenutno direktno spojenim klijentima. Vidljivo je da prvo mjesto uvjerljivo zauzimaju Ujedinjene države sa 367235 klijenata, zatim slijede Rusija, Njemačka, Ujedinjeni Arapski Emirati, Indonezija, Francuska, Ukrajina, Ujedinjeno kraljevstvo, Indija te naposljetku Nizozemska sa 43419 direktno povezanih klijenata.

Izvor 14.https://metrics.torproject.org

Country	Mean daily users
United States	367235 (18.94 %)
Russia	247473 (12.76 %)
Germany	156731 (8.08 %)
United Arab Emirates	108930 (5.62 %)
Indonesia	107656 (5.55 %)
France	81684 (4.21 %)
Ukraine	77606 (4.00 %)
United Kingdom	62746 (3.24 %)
India	48313 (2.49 %)
Netherlands	43419 (2.24 %)

Slika 14. Prikaz top 10 zemalja po direktno spojenim klijentima

Iduća slika prikazuje top 10 zemalja s obzirom na direktno povezane klijente koji koriste mostove za spajanje. Na prvom mjestu je Rusija sa 10503 klijenata što znači da ima dvostruko više klijenata od drugo plasiranih Sjedinjenih država koji imaju 5987 klijenata koji za spajanje koriste mostove. Zatim slijede Iran, Turska, Indonezija, Indija, Brazil, Kina, Vijetnam i Njemačka koja kao posljednja plasirana u top 10 ima 1767 povezanih klijenata.

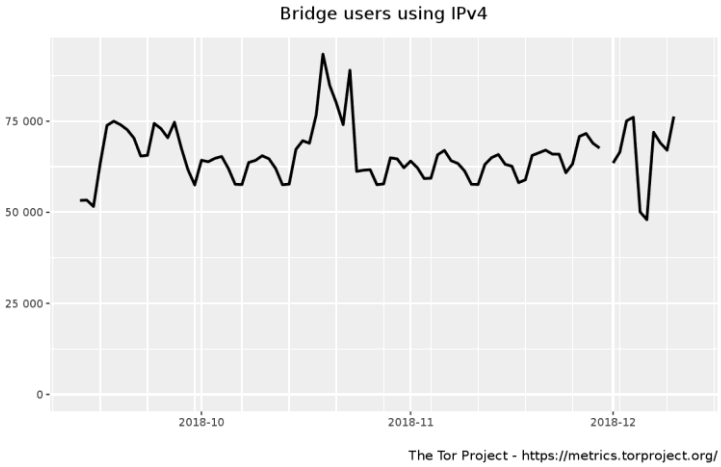
Izvor 15. https://metrics.torproject.org

Country	Mean daily users
Russia	10503 (15.92 %)
United States	5987 (9.08 %)
Iran	4584 (6.95 %)
Turkey	3931 (5.96 %)
Indonesia	3568 (5.41 %)
India	3198 (4.85 %)
Brazil	2281 (3.46 %)
China	2188 (3.32 %)
Vietnam	1958 (2.97 %)
Germany	1767 (2.68 %)

Slika 15 Prikaz top 10 zemalja po korištenju mostova za spajanje

Vrlo važna je usporedba IPv4 i IPv6 protokola, te koji je protokol korišteniji prilikom korištenja Tor mreže.

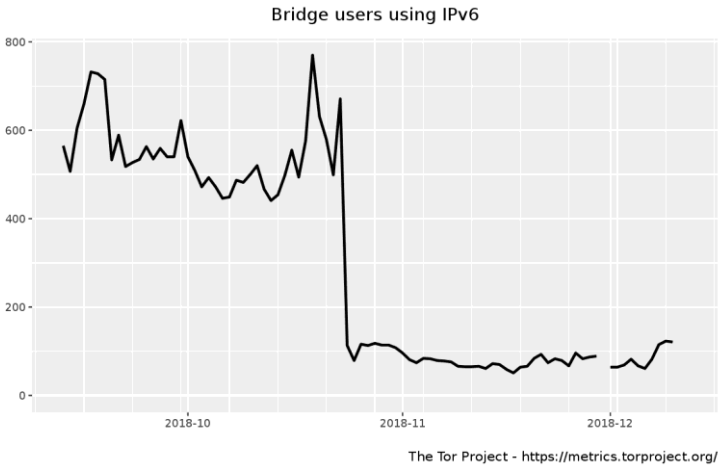
Izvor 16. https://metrics.torproject.org



Slika 16. Prikaz korištenja IPv4 protokola u posljednja 3 mjeseca

Slika 16. prikazuje korištenje IPv4 protokola u posljednja 3 mjeseca, dakle u razdoblju od polovice rujna do polovice prosinca 2018. godine. Vidljivo je da je polovicom rujna IPv4 protokol koristilo oko 52 000 korisnika te je taj broj do kraja rujna rastao do 75 000 uz manji pad i rast, sredinom mjeseca listopada došlo je do porasta od oko 82 tisuće korisnika, te je došlo do naglog smanjenja tijekom mjeseca prosinca gdje se broj korisnika kretao od oko 53 000 do 70 000, nakon toga je uslijedio nagli pad početkom mjeseca prosinca na 50 000 korisnika.

Izvor 17.https://metrics.torproject.org

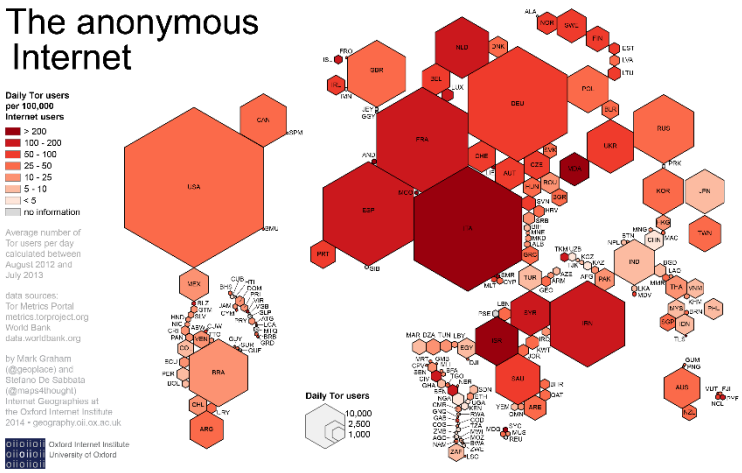


Slika 17. Prikaz učestalosti korištenja IPv6 protokola u razdoblju od 3 mjeseca

Usporedno sa korištenjem IPv4 protokola, na slici 17. je prikazan graf koji prikazuje učestalost korištenja IPv6 protokola u jednakom vremenskom razdoblju. Dok je broj korisnika IPv4 korisnika sezao do maksimalno oko 82 000 korisnika, IPv6 protokol seže do maksimalno 800 korisnika, što je enormna razlika. Od polovice mjeseca rujna pa do kraja studenog IPv6 protokol imao je rasta i padova, broj korisnika kretao se od oko 500 do maksimalno 750 korisnika sve dok nije u jednom trenutku dosegnuo razinu od oko 100 korisnika, te ostao na toj razini uz vrlo blagi rast i pad sve do mjeseca prosinca.

Vrlo zanimljiva je i vizualizacija koju je napravio Oxford Internet institut koja predstavlja odnos Tor korisnika i cijele Internet populacije. Prilikom izrade vizualizacije korišten je prosječan broj Tor korisnika u određenoj zemlji od srpnja 2012. godine do srpnja 2013. godine te su stavljeni u usporedbu sa ukupnim brojem Internet korisnika u određenoj zemlji.

Izvor 18.https://metrics.torproject.org



Slika 18.Prikaz vizualizacije prosječnog broja korisnika po zemljama

S obzirom na to da se Tor koristi diljem svijeta procjenjuje se da ga dnevno koristi oko 750000 internet korisnika. Više od polovice Tor korisnika locirano je upravo na području Europe, te se procjenjuje da prosječno Tor mrežu svakodnevno koristi od 80 do 100000 europskih stanovnika. Italija broji oko 76 000 Tor korisnika dnevno, dok ju ipak predvode Ujedinjene države sa procjenom od 126 000 korisnika dnevno. Stotine Internet korisnika svaki dan koriste Tor iz zemalja kao što su San Marino, Monako, Andora i Linhenštajn koji uključuju malene Internet populacije.

4. NAPADI NA TOR MREŽU

4.1. VRSTE NAPADA

Postoji nekoliko vrsta napada na TOR mrežu. Osnovna podjela uključuje *pasivan napad, aktivan napad, directory napade* te *napade protiv točaka susreta.*[22]

Pasivni napadi uključuju :

1. Promatranje korisničkih uzoraka prometa

Ukoliko napadač promatra korisnikovu vezu prometa neće otkriti odredište veze ili podatke, već obrasce prometa koji su poslani i primljeni. Ako se promatra profiliranje putem korisnika, obrasci povezivanja zahtijevaju daljnju obradu. Poanta je u tome da višestruko aplikacijski tokovi mogu raditi istodobno ili pak u seriji preko jednog kruga.

2. Promatranje korisničkih sadržaja

Sadržaj koji se nalazi na kraju korisnika je šifriran, dok veze sa odgovornima ne moraju biti šifrirane. S obzirom na to da „filtriranje sadržaja“ nije primaran cilj Onion usmjeravanja , TOR ima mogućnost izravnog korištenja privoxy-a te povezanih usluga filtriranja kako bi se očuvala anonimnost aplikacijskih tokova podataka.

3. Mogućnost razlikovanja

Klijentima je omogućeno biranje opcija postavki. Primjerice, klijenti koji su zabrinuti oko zahtjeva povezivosti trebali bi zaokretati krugove mnogo češće od onih klijenata koji su zabrinuti za zahtjev slijeđenja. Pružanje mogućnosti izbora može privući korisnike sa različitim potrebama, no oni korisnici koji su u manjini mogu izgubiti više anonimnosti pojavljivanjem razlike koju mogu dobiti optimiziranjem njihovog ponašanja.

22 R. Dingledne N. i Mathewson, op. cit.

4. Otisak prstiju na web-u

Svi učinkoviti pasivni napadi koji su dosad navedeni su zapravo napadi na potvrdu prometa. Postoje i analize prometa pasivnih napada koje su potencijalno učinkovite.

Kako ne bi tražio izlazne veze za vremenske korelacije, napadač može izgraditi bazu podataka „otisaka prstiju“ koja bi sadržavala veličinu datoteka te obrasce pristupa na ciljanu web stranicu. Na taj način kasnije se može potvrditi korisnikova veza na datu web stranicu jednostavno provjeravajući bazu podataka „otisaka prstiju“.

Aktivni napadi uključuju:

1. Kompromisne ključevi

Napadač koji poznaje TLS razmjenu ključeva može pratiti kontrolu ćelija te kriptirani prijenos ćelija na svakom krugu povezanosti. Napadač koji poznaje Onion protokol i TLS privatni ključ može utjeloviti Onion protokol ukoliko sazna vijek trajanja TLS ključa. Također mora znati i Onion ključ kako bi mogao dekriptirati kreirane ćelije. Periodičan ključ rotacije ograničava prilike za takve napade.

S druge strane, napadač koji poznaje osobni ključ čvora može zamijeniti taj čvor nedefinirano na način da pošalje nove krivotvorene opise direktoriju servera.

2. Pokretanje onion proxy

Očekivano je da će krajnji korisnik uvijek pokrenuti vlastiti lokalni onion proxy. No, u nekim slučajevima moguće je da će se proxy morati pokrenuti daljinski posebice u ustanovama koje žele pratiti aktivnosti onih koji se povezuju s proxy poslužiteljem. Ukoliko se kompromitira onion proxy dolazi do kompromitiranja svih budućih veza.

3. Označavanje napada

Neprijateljski čvor može označiti ćeliju ažuriranjem. Ukoliko je primjerice poslan ne kriptirani upit određenoj web stranici tada iskrivljeno značenje dolazi u prikladno

vrijeme kako bi potvrdilo pridruživanje. Međutim, cjelovite provjere ćelija sprječavaju ovakve napade.

4. Ponavljanje napada

Neki od anonimnih protokola su ranjivi na ponavljanje napada. No, Tor ne spada u tu skupinu. Ponavljanje jedne strane rukovanja rezultirati će drugačijem dogovorenom ključu sesije te time ostatak sesije ne može biti korišten.

5. Distribuiran neprijateljski kod

Napadač može pokušati prevariti korisnike na način da pokrene srušeni Tor softver koji zapravo nije anonimizirao njihove veze. Također može prevariti Onion protokol pokretanjem slabijeg softvera koji je time korisnicima pružio manje anonimnosti. Taj problem se može riješiti, no ne u potpunosti, potpisivanjem svih Tor izdanja sa službenim javnim ključem. Uključujući ulaz u direktorij, imenik koji bilježi verzije koje su trenutno sigurne. Kako bi se spriječilo da napadači prevare korisnike preko oslabljenog Tor softvera potiče se provjeravanje revizije izvora te se vrlo često upozorava korisnike da ne vjeruju u vjerodostojnost svakog softvera ukoliko dolazi bez izvora.

Napadi na imenike:

1. Uništenje poslužitelja imenika

Ukoliko nekoliko poslužitelja imenika nestane, ostali još uvijek odlučuju o valjanosti imenika. Koliko dugo neki od imenika servera ostaju u funkciji oni će i dalje prenositi njihove preglede mreže i stvoriti imenika koncenzusa. Ukoliko se dogodi da je više od pola imenika uništeno, on neće imati dovoljno potpisa za klijente da ga koriste automatski. Tada će za klijente biti potrebna ljudska pomoć o odluci hoće li klijent imati povjerenja u navedeni imenik.

2. Srušen server imenika

Preuzimanje imenika servera napadač može djelomično utjecati na krajnji imenik. Onion protokol je uključen ili isključen većinskim glasovanjem, te time jedan od korumpiranih imenika može donijeti odlučujući glas koji uključuje rubni Onion protokol. Postavlja se pitanje koliko se često takvi rubni slučajevi događaju u praksi.

3. Sabotiranje većine poslužitelja imenika

Napadač koji kontrolira više od pola imenika može se uključiti kao većina ugroženih Onion protokola u krajnjem imeniku ukoliko to želi. Potrebno se je osigurati da su operatori imenika servera neovisni te otporni protiv napada.

4. Uvjeravanje imenika da neispravan Onion protokol radi

U trenutnoj Tor implementaciji, serveri imenika pretpostavljaju da Onion protokol radi ispravno ukoliko je moguća uspostava TLS veze sa njime. Neprijateljski Onion protokol mogao bi narušiti taj test prihvaćanjem TLS veze sa Onion protokolom no ignoriranjem svih ćelija. Imenici servera morali bi aktivno provoditi testiranja Onion protokola adekvatno gradeći krugove i tokove.

Napadi na točke susreta

1. Napraviti mnogo uvodnih zahtjeva

Napadač može pokušati napasti Bobov sustav preopterećivanjem točaka susreta sa upitima. Točke susreta mogu blokirati upite, no potrebna je oznaka odobrenja. Bob može ograničiti veličinu zahtjeva koju prima ili pak zahtijevati određeni izračun za svaki od primljenih zahtjeva.

2. Napad na uvodnu točku

Napadač može poremetiti sakrivene usluge lokacije onemogućavanjem točaka uvođenja. S obzirom na to da je identitet usluge povezan sa javnim ključem usluga se

može jednostavno ponovno reklamirati na drugačijim uvodnim točkama. Oglasi se mogu objavljivati tajno te bi tada samo vrlo važni klijenti znali adrese Bobovih uvodnih točaka. Time se prisiljava napadača da onemogući sve moguće točke uvođenja.

3. Ugroženo mjesto napada

Točka sastanka nije osjetljivija od nekog drugog 0nion protokola u krugu zato što svi podaci prolaze kroz sastanak koji je šifriran sesijskim ključem kojeg dijele Alice i Bob.

4.2. MODELI NAPADAČA NA TOR MREŽU

Pomoću zaglavlja IP paketa i podataka koje ono sadrži može se na jednostavan način doći do samog izvora. Analiziranjem adrese izvora može se saznati tko je davalac usluga te koja je geografska lokacija samog korisnika.

Napadači na Tor mrežu dijele se prema [23]:

1. Snazi napadača – snaga napadača dijeli napadače na pasivne i aktivne
2. Opsegu napada – opseg napada dijeli napadače na lokalne i globalne
3. Prilagodljivosti – prilagodljivost dijeli napadače na statičke i dinamičke.

Da bi napadač bio aktivan mora biti sposoban ugroziti čvorove sistema. Ukoliko ugrozi čvorove sistema, tada mu se pruža mogućnost upravljanja dijelom čvorova sistema. Za razliku od aktivnog napadača, pasivni napadač ne može ostvariti kontrolu nad niti jednim čvorom. Jedina mogućnost koja se pruža pasivnom napadaču je prisluškivanje prometa koji se odvija između čvorova.

Lokalni napadač osigurava pristup samo jednom dijelu veze, dok globalni napadač ima osiguran pristup cijeloj mreži, dakle vlada nad svim vezama i čvorovima.

Dinamički napadač funkcionira na način da prikupi sve moguće podatke sa ugroženih veza i čvorova. Na taj način otkriva tko je poslao ili pak primio paket. Da bi prikupio sve podatke koristi dvije vrste znanja, znanje za koje nije potrebno iskustvo te

23 Kelly, D.: A taxonomy for and analysis of anonymous communication networks, dissertation, Air force institute of technology, Wright-Patterson Air Force Base, Ohio, March 2009.

znanje koje izričito ovisi o iskustvu. Za razliku od njega, statički napadač se koristi znanjem koje ne ovisi o iskustvu.[24]

4.3. END TO END CONFIRMATION ATTACKS – napad s kraja na kraj

End to end napadi proučavaju se u kontekstu visoke i niske latencije anonimnih sustava. Biti će opisani kroz dva pasivna napada na sustave niske latencije. Glavna ideja je praćenje ulaznih i izlaznih veza čvorova u mreži. Prvi napad odnosi se na praćenje, brojenje broja poruka na ulazu i izlazu iz svakog čvora. Veze sa sličnim brojem poruka odgovaraju jedna drugoj.

Drugi napad prati početak veze, kada je na ulaznoj vezi uočeno mnogo prometa, te kada je ubrzo nakon toga uočeno više prometa na izlaznoj vezi tada se zna da obje veze pripadaju jednakom prometnom toku. Ista se tehnika može koristiti od strane globalnog napadača za praćenje prometa od jednog čvora do drugog kroz cijelu mrežu.

4.4. STATISCAL DISCLOUSURE ATTACK

Glavna ideja ovog napada je da korisnici komuniciraju sa fiksnim brojem primatelja, te da je pozadinski promet ostalih korisnika ravnomjerno raspoređen na sve primatelje. Napadač želi potvrditi primatelja određenog korisnika unutar jednog sustava. Kako bi se ovo ostvarilo potrebno je promatrati svaku poruku koje pristiže i odlazi. U svakoj rundi poruke se šalju u mix, koji ih pretvara u sadržaje fiksne veličine. Napadač pamti svakog primatelja poruke u svakoj rundi kao kandidata korisnikovog pošiljatelja. Promatranjem velikog broja krugova otkrivaju se najvjerojatniji kandidati zato što će oni dobiti značajno više poruka u usporedbi sa ravnomjernim pozadinskim prometom.

24 V. Ubavić i D. Oklonđija, op. cit., str. 41

Statistic disclosure napad proučava mix koji prosljeđuje poruke u serijama. Iako, analize miješaju prosljeđivanje svake poruke zasebno, no poruka se može odgoditi sa nasumično odabranim vremenom. Opisani napad određuje se testom statističke hipoteze uspoređujući ako jedan uzorak odgovara drugom uzorku na odlaznoj vezi. Veze se najvećom sličnošću su veze koje pripadaju uzorku unosa. Ista tehnika može se koristi za povezivanje prometa na rubovima mreže zbog čega je napad prikladan kao krajnji napad potvrde.

Klasa *end to end* napada potvrde protiv mreže anonimnosti s niskom latencijom su vremenski napadi koji koriste vrijeme kako bi korelirali promatrane poruke. Primjerice, promatran promet podijeljen je u susjedne intervale te je svaki interval zauzvrat u prozorima fiksne veličine. Za svaki prozor računa se broj prenesenih paketa. Različiti intervali mogli bi se statistički povezati kako bi pronašli podudaranja između promatranog prometa. Jedan od načina obrane je konstantno prikrivanje prometa kojeg korisnik šalje kako se obrasci prometa ne bi razlikovali. Ideja je zapravo poslati prekriveni promet koji se nalazi između korisnika i odredišta. Ovakav potez može zbuniti napadače zato što promet koji ulazi i izlazi iz mreže izlaže različite obrasce. Jedan od pristupa je i adaptivno podmetanje. Korištenjem prilagodljivog podmetanja čvorovi unutar mreže ubacuju neke vjerojatne poruke između korisnika kako bi zbunili napadača uništavanjem obrasca prometa. Prednost prilagodljivog podmetanja je u tome što prirodno odgađaju poruke od korisnika.

4.5. TIMING ATTACK

Izraz timing attack se u kriptografiji koristi za napad koji se odvija na strani kanala u kojemu napadač pokušava kompromititirati kriptosustav na način da analizira vrijeme koje je potrebno da se izvrši kriptografski algoritam. Prilikom mjerenja vremena koje je potrebno da se odgovori na određene upite postoji mogućnost curenja informacija iz određenog sustava. Poprilično je upitno koliko takve informacije mogu pomoći napadaču, no to ovisi o mnogim čimbenicima poput kakav je dizajn kripto sustava, koji algoritmi se koriste, koji CPU pokreće sustav, kakve su protumjere

mjerača vremena, kolika je točnost vremenskih mjerenja i slično. Prilikom projektiranja se timing attack vrlo često zanemaruje, a zapravo je vrlo ovisan o samoj implementaciji. Ukoliko se izbjegne korištenje timing attack-a ono podrazumijeva implementaciju konstantnih funkcija te vrlo pažljivo testiranje konačnog izvršnog koda.[25]

Timing attack u velikoj mjeri ugrožava anonimnost Tor mreže. Ukoliko netko pruzme kontrolu nad ulaznim i izlaznim čvorištem dolazi to timing attack napada. Vrlo jednostavnom statistikom mogu se upariti paketi te je tada samo nekoliko minuta dovoljno da se otkrije identitet pošiljatelja. [26]

25 Novosel, Ćosić, Sigurnost informacijskih sustava, „Problemi i rješavanje curenja podataka – Timing atttack“, 2018.
[website]: https://github.com/dinovos/SIS_RPi3_Tor/wiki/5.-Problemi-i-rješavanje-curenja-podataka Datum pristupanja : 13. ožujka 2019.
26 Ibidem

5. ANONIMNOST, KRIPTOGRAFIJA I PROTOKOLI KORIŠTENI U TOR MREŽI

5.1. ANONIMNOST

Riječ anoniman znači kojemu se ne zna ime, bezimen, nepoznat.[27]
Prilikom korištenja, odnosno pretraživanja Interneta u današnjem svijetu gotovo da i ne postoji pojam anonimnosti. Korištenjem raznih društvenih mreža i pretraživanje internetskih stranica koji su popraćeni raznim „kolačićima“ naši su životi i aktivnosti izloženi javnosti. Korištenjem uobičajenih Internetskih pretraživača omogućavamo drugoj strani da prati naše aktivnosti, te nas na taj način obasipaju nepotrebnim reklamama. Jedini način da se u većoj mjeri zaštite osobni podaci te aktivnosti pretraživanja je korištenje Tor browsera.

5.2. KRIPTOGRAFIJA

Kriptografija je znanstvena disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. [28] Kriptografski algoritam je matematička funkcija koja se koristi za šifriranje i dešifriranje. Postoji jedna funkcija koja se odnosi na šifriranje, a druga za dešifriranje. Šifriranje (eng. encryption) je pretvaranje izvornog teksta (plaintext) u šifrirani tekst (chipertext) pomoću određene šifre (algoritma – AES , 3DES). Dešifriranje (eng. decryption) se odnosi na omogućavanje čitanja šifriranih podataka korisnicima koji posjeduju ključ. [29] Prilikom korištenja TOR mreže vrlo su bitni pojmovi šifriranja i dešifriranja.

5.3. TLS

TLS (eng. Transport Layer Security) je sigurnosni protokol koji se temelji na SSL 3.0 (eng. Secure Sockets Layer) te koristi digitalni certifikat kako bi autentificirao

27 Hrvatski jezični portal. Dostupno na: hjp-znanje.hr, (pristupljeno : 10. lipnja 2019.).
28 A. Dujella, „Klasična kriptografija, Osnovni pojmovi“, [website] https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html, (pristupljeno : 10. lipnja 2019.).
29 Centar informacijske sigurnosti, „ Kriptiranje podataka“ [website], 2011., https://www.cis.hr/sigurnosni-alati/kriptiranje-podataka.html , (pristupljeno : 12. lipnja 2019.).

korisnika jednako dobro kao i autentifikaciju mreže. Dakle, pruža aplikacijama sigurnu komunikaciju putem mreže. TLS je protokol čiji je zadatak spriječiti prisluškivanje, izmjenu te lažiranje poruka. Korištenjem kriptografije pruža autentifikaciju krajnjih točaka te povjerljivost komunikacije putem Internet mreže.

Vrlo bitna značajka je da je TLS prisvojio mnogo sigurniji kod za provjeru autentičnosti poruke, HMAC. HMAC (eng. Hash – based Message Authentication Code) je kod koji se koristi za provjeru autentičnosti poruke. Njegova specifičnost je da koristi kriptografski ključ zajedno s hash funkcijom.[30]TLS klijent koristi javni ključ servera kako bi napravio enkripciju nasumičnog broja i poslao ga natrag serveru. Nasumični broj u kombinaciji sa već korištenim nasumičnim brojevima koristi se za generiranje tajne sesije ključeva.

5.4. RSA

Ronald Rives, Adi Shamir i Leonard Adleman su 1977. godine iskoristili ideju koju su iznijeli Diffie i Hellman te su time izumili prvi i najšire korišteni kriptosustav, RSA kriptosustav. Glavna odlika RSA kriptosustava je upravo u tome da je fatkorizacija velikih prirodnih brojeva na produkt dva prosta broja izuzetno teška.

Definiranje RSA kriptosustava[31]:

1. Neka je n = pg , gdje su p i q prosti brojevi . Neka je P = C = Z_n = { 0, 1, 2, ….., n – 1}

   K = { (n, p, q, d, e) : n = pq, p,g prostim d ≡ 1 (mod ϕ (n))} , gdje je ϕ (n) Eulerova funkcija, koja prirodnom broju n pridružuje broj prirodnih brojeva manjih od n, koji su relativno prosti s n.
2. Za K = (n, p, q, d, e) ∈ K definira se

   $E_K(x) = x^e \bmod n$ $d_K(y) = y^d \bmod n$

30 M. Rouse, „Hash – based Message Authentication Code(HMAC)“, 2010. , website : https://searchsecurity.techtarget.com/definition/Hash-based-Message-Authentication-Code-HMAC

31B. Ibrahimpašić, „RSA Kriptopsustav“, Osječki matematički list 5, 2005., str. 104.

Gdje su x, y ∈ Z_n.

Vrijednosti n i e su javne, dok su vrijednosti p, q i d tajne

I u prošlosti je korištenje RSA algoritma predstavljao dominantan mehanizam razmjene ključeva u većini TLS implementacija. Klijent generira simetričan ključ, zatim ga šifrira javnim ključem i šalje ga poslužitelju koji ga koristi kao simetričan ključ za uspostavljenu vezu. Poslužitelj koristi svoj vlastiti privatni ključ za dešifriranje poslanog simetričnog ključa te je time razmjena ključeva dovršena. Od toga trenutka klijent i poslužitelj koriste pregovarački simetrični ključ za šifriranje svoje veze. RSA algoritam ima i kritičnu slabost, a to je da se isti par javnih i privatnih ključeva koristi za provjeru autentičnosti poslužitelja te za šifriranje simetričnog ključa sesije, veze poslane poslužitelju. Rezultat toga je da ukoliko napadač dobije pristup privatnom ključu i prisluškuje ga na razmjeni tada zapravo može dešifrirati cijelu sesiju. Također, postoji mogućnost da ukoliko napadač trenutno nema pristup privatnom ključu on još uvijek može snimiti šifriranu sesiju te kasnije dovršiti dešifriranje nakon što doznaju privatni ključ.[32]

5.5. DIFFIE – HELLMANOV PROTOKOL

Ideju kriptosustava sa javnim ključem iznijeli su Whitfield Diffie i Martin Hellman te su ga nazvali *kriptosustav javnog ključa.*

Diffie – Hellmanov postupak razmjene ključa je kriptografski protokol koji omogućuje osobama koje se ne poznaju da razmijene simetrični tajni ključ preko nezaštićenog komunikacijskog kanala. [33] 1976. godine su Diffie i Hellman objavili njihov postupak uspostave simetričnog kriptosustava između dva partnera, ujedno bili

32 I. Grigorik, „High Preformance Browser Networking, Transport Layer Security (TLS)“, Networking 101, Chapter 4, [website], 2013., https://hpbn.co/transport-layer-security-tls/#rsa-diffie-hellman-and-forward-secrecy, (pristupljeno: 15. srpnja 2019.).

33 CarNet Hrvatska akademska i istraživačka mreža, „Diffie – Hellmanov protkol“, NCERT-PUBDOC-2009-12-284, 2009., str. 11

su prvi koji objavili postupak za razmjenu tajnog ključa koji je potreban za kriptiranje poruka korištenjem simetričnog kriptosustava.

Diffie - Hellmanov postupak se odvija na sljedeći način [34]:

1. Neka se dvije osobe na neki način unaprijed dogovore o dva velika broja koja će se dodijeliti vrijednostima *n* i *g*. Broj g je relativno prost s obzirom na n, treba uzeti u obzir da im je najveći zajednički djelitelj broj 1.

nzd (g,n) = 1

Najbolje bi bilo kada bi se za n odabrao veliki prosti broj p. Brojevi p i g ne moraju biti tajni.

2. Prvi korisnik, neka to bude Alice, odabere veliki nasumični prirodni privatno broj x. Drugi korisnik, neka je to Bob, odabere također nasumično veliki prirodni broj y.
3. Alice želi uspostaviti komunikaciju sa Bob-om, šalje rezultat izjednačavanja operacije modulo

$$X = g^{x} \pmod{p}$$

4. Bob šalje Alice svoj rezultat izračunavanja operacije modulo te u jednadžbi koristi svoj privatni broj y:

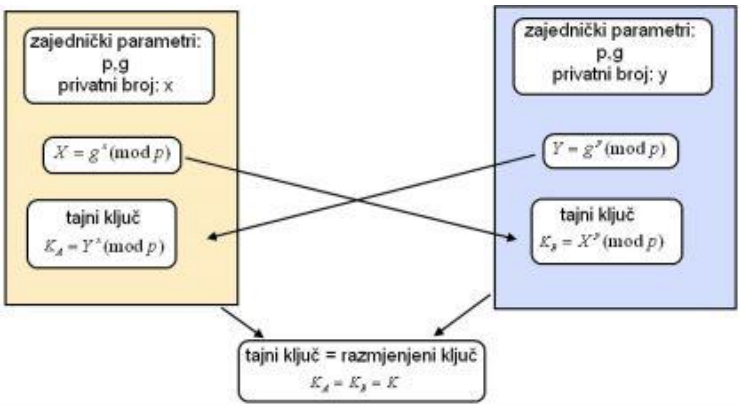
$$Y = g^{y} \pmod{p}$$

5. Alice izračunava : $K = Y^{x} \pmod{p} = (g^{y})^{x} \pmod{p} = g^{xy} \pmod{p}$. Time je Alice izračunala ključ koji se može koristiti za kriptiranje poruka.
6. Bob izračunava sljedeće : $K = X^{y} \pmod{p} = (g^{x})^{y} \pmod{p} = g^{xy} \pmod{p}$. Bob je također izračunao ključ kriptiranja koji je jednak ključu koji je Alice izračunala

S obzirom na to da su ključevi koje su Alice i Bob izračunali jednaki, oni su time zapravo razmijenili simetričan ključ kriptiranja.

34 Loc.cit.

Izvor 19. https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2009-12-284.pdf



Slika 19. Prikaz Diffie - Hellamanove razmjene ključeva

Diffie – Hellmanova razmjena ključeva omogućava klijentu i naravno poslužitelju da se dogovore o njihovoj zajedničkoj tajni bez izričitog komuniciranja. Komunikacija se odvija na način da se privatni ključ poslužitelja koristi za potpisivanje i provjeru rukovanja, no uspostavljeni simetrični ključ koristi samo klijent te ga na taj način ne može presresti pasivno napadač čak i ako ima pristup privatnom ključu. Diffie – Hellmanova razmjena ključeva može se koristiti za smanjenje rizika kompromisa prošlih komunikacijskih sesija. To se može napraviti na način da se generira novi „prolazni“ simetrični ključ kao dio svake razmjene ključeva te tada odbaciti prethodne ključeve. S obzirom na to da „prolazni“ ključevi nikada ne komuniciraju te jedino aktivno pregovaraju za svaku od novih sesija tada napadač u najgorem slučaju može kompromitrati klijenta ili poslužitelja te pristupiti ključevima sesije trenutnih i budućih sesija. Poznavanje privatnog ili trenutnog ključa ne pomaže napadaču da dešifrira neku od prethodno snimljenih sesija.[35]

6. SIMULACIJA TIMING ATTACK NAPADA

35I. Grigorik, op.cit.

Simulacija pripada alternativnoj metodi. Umjesto da se izvode pravi eksperimenti u TOR mreži, eksperiment su simulirani. Ovaj pristup je vrlo pouzdan zato što se ponavljaju isti parametri pa bi simulacije trebale dati iste rezultate. Pojedinačni parametri mogu se manipulirati te se njihov učinak proučavao radi otkrivanja uzročno posljedičnih veza. Simulacije su odličan izbor jer su jeftine i mogu se izvršiti automatski. Iako pružajući kontrolirano okruženje za eksperimente, simulacije imaju jednak nedostatak kao privatne istraživačke mreže u tome što njihovi rezultati možda neće biti prenosivi na pravu Tor mrežu. No, simulacije se mogu uspješno koristiti za istraživanje TOR-a.

Prema članku „Large scale simulation of Tor"[36], navodi se kako nije moguće implementirati globalne pasivne napade na mreže niske latencije. Opisuje se implementacija diskretne simulacije TOR-a prilikom korištenja SSFnet simulatora. Na TOR mreži koja se u ovom slučaju sastoji od oko 6000 čvorova provodi se nekoliko globalnih napada.

Navodi se kako napadi dokazuju veliku pouzdanost sa 80 % korelacije toka za uvijete slabijeg prometa, no prilikom korištenja napučenih veza uspješnost iznosi tek 18 %.

6.1. O SIMULUACIJI

Iako TCP / IP imaju jako veliku ulogu u Internetu, oni nisu osmišljeni na način da pruže anonimnost. Kako bi se riješio problem anonimnosti potiče se stvaranje *overlay* mreže. Zadatak *overlay* mreže je da pruža određenu kontrolu usmjeravanja poruka.

Određena kontrola omogućava skrivanje pošiljateljeve i primateljeve adrese, te na taj način pruža određenu razinu anonimnosti. Potreban je točan testni primjer za implementaciju novih značajki mjerenja anonimnosti u svrhu testiranja napada protiv *overlay* mreža.

[36] Gavin O' Gorman and Stephen Blott, Large Scale Simulation of Tor: Modelling a Global Passive Adversary, Dublin City University, 2007, str. 48

Kada se uspostavljaju testne mreže u laboratoriju to zapravo pruža ograničavajuće opcije. Problem je u tome što takva testna mreža ne može mjeriti sadašnje i buduće veličine implementacije.

Stvaranje sveobuhvatnog analitičkog modela vrlo je teško s obzirom na razinu složenosti overlay mreža. Jedna od opcija koja se pruža je korištenje tajne simulacije temeljene na događajima.

Slijedi opisana simulacija temeljena na događajima anonimne, TOR mreže, koristeći SSFNet simulator. Simulacija modelira Tor usmjeravanje HTTP podataka uključujući krugove koje stvara, tok kodiranja, proxy, rutere te izlazne rutere.

Implementirano je nekoliko preliminarnih pasivnih globalnih napada koristeći oko :

- 4500 HTTP klijenata
- 100 HTTP servera
- 950 TOR rutera

6.2. TOR i SSFNet

Vezano uz sustav TOR, sadašnja Tor mreža sadrži oko 900 čvorova usmjerivača koji sadrže stotine tisuće tokova koji prolaze kroz mrežu. TOR mrežu čine:

- *proxy*
- *onion router*
- *exit router*

Korisnici pokreću TOR proxy na njihovom lokalnom računalu koje pruža SOCKS sučelje za TCP aplikacije/programe. TOR proxy započinje proces uspostavljanja krugova kroz mrežu onion routera, sve do odgovarajućeg izlaznog usmjerivača pa sve do ciljanog TCP poslužitelja. Na uspostavljenim krugovima, nadolazeći TCP tok se usmjerava preko kruga.

SSFNet (Scalable Simulation Framework) je dizajniran za modeliranje simulacija velikih razmjera. Tajna simulacija temeljena na događajima koristi se za stvaranje apstraktne reprezentacije važnih dijelova sustava. Simulacija temeljena na

događajima omogućava izradu modela sustava i istraživanje kako sustav može funkcionirati u različitim uvjetima. Okvir opisuje sučelje za simulacije same jezgre.

Generička jezgra može biti nadograđena za implementaciju raznovrsnih simulatora, od kojih jedan čini mrežni simulator.[37]

6.3. IMPLEMENTACIJA TOR-a i SSFNet-a

Osim nekih specifičnih simulacijskih tehnika za mjerenje linearnog vremena izvršenja događaja, sam kod simulacije je vrlo sličan stvarnoj aplikaciji. Tri različita mrežna elementa su stvorena povrh onih koji su već osigurale knjižice simulacije.

Mrežni elementi su :

- proxy
- router
- exit router

6.4. PROTOKOL

U originalnom TOR dokumentu opisan je protokol uspostavljenih krugova koji je točno simuliran. Enkripcija nije simulirana jer nije bilo potrebe za time.

Promet koji je umjeren kroz modeliranu Tor mrežu je osiguran od strane HTTP generatora prometa.

SSF.OS.WWW je distribuiran korištenjem SSFNet protokola. Podaci koji su zaprimljeni od strane HTTP klijenta razdijeljeni su u ćelije od 512 byta. Označeni su ispravnim ID-om puta te su poslani na ruter koji je povezan sa njime. Kroz svaki se

[37] Ibidem, str. 49

ruter prenose podaci sve dok ih ne primi e*xit router* odnosno izlazni usmjerivač. On ponovno primi izvorne podatke i šalje ih ciljanom poslužitelju.

Nekoliko prometnih tokova može biti multipleksirano preko veze krugova. Primjerice, ukoliko *proxy* zaprimi novu nadolazeću klijentsku vezu i ako se odabere kao pri ruteru čvor na kojem će veza biti dostupna, tada je *socket* ponovno iskorišten. Novi ID toka dodijeljen je toku, time je slijeđena procedura toka te je ispravno usmjeren.[38]

6.5. TOPOLOGIJA

Korištena mrežna topologija preuzeta je sa SSFnet stranice. Topologija se sastoji od 24 međusobno povezana autosustava (AS), gdje se svaki AS sastoji od broja podmreža.[39]

Na svaku od podmreža dodani su :

- *1 proxy*
- *2 onion routera*
- *exit router*

Njihov je zadatak distribuirati čvorove kroz mrežu.

Rezulat koji uključuje:

- *325 proxy*
- *650 router nodes*
- *325 exit nodes*,

u cijeloj mreži, aproksimirajući broj onion routera u trenutnoj razvijenoj TOR mreži. Broj klijenata za LAN postavljen je na 5, rezultirajući sa sveukupno 5760 klijenata.

[38] Ibidem, str. 49
[39] Ibidem, str. 50

6.6. NAPAD I REZULTAT

Implementirani su brojni napadi. Rezultat napada omogućava ispravnu demonstraciju TOR simulacije. Napadi su ostvareni povećanjem broja klijenta za model *povećanja prometa multipleksiranih*[40] *veza.* Što je veći promet, biti će i veće kašnjenje po mreži.[41]

Vrijeme simulacije iznosi 1120 sekundi, toliko dugo se izvodi.

Početnih 1000 sekundi dozvoljeno je za umjeravanje BGP[42] i OSPF[43].

Nakon 1000 sekundi, HTTP klijent započinje povezivanje na TOR mrežu te na ciljani poslužitelj.

Nakon 60 sekundi, u vremenu od 1060 sekundi, tcpdump izlaz se bilježi još 60 sekundi do vremena od 1120 sekundi u čijem trenutku simulacija prestaje.

Početnih 60 sekundi potrebno je za dopuštenje Tor rutera da dođe u ravnotežu.

6.7. CONNECT START TRACKING ATTACK

Napad funkcionira praćenjem vremena inicijalizacije veze prilikom dohvaćanja mreže. Ukoliko tok primijeti ulaze i nakon toga izlaze iz mreže u određenom vremenskom okviru, tada je moguće povezati dva događaja. Napadi zahtijevaju odvojene mreže za uspješno povezani tok.

Na zauzetoj strani *multiplexed* mreža, započinje i završava veza praćenjem servera kao efektivnih filtera za reduciranje broja potencijalnih tokova.

U implementaciji napada, uzima se vrijeme prvog HTTP odgovora paketa, dodaje se varijabla kašnjenja *d*, te na nju radimo i usporedbu vremena sa svim

[40] Multiplexed – popularna mrežna tehnologija koja spaja višestruke signale u jedan signal

[41] Ibidem, str. 50

[42] BGP (eng. Border gateway protocol) – usmjerivački protokol koji služi za komunikaciju između autoimunih sustava. Omogućava da Internet radi usmjeravanjem podataka na Internetu)

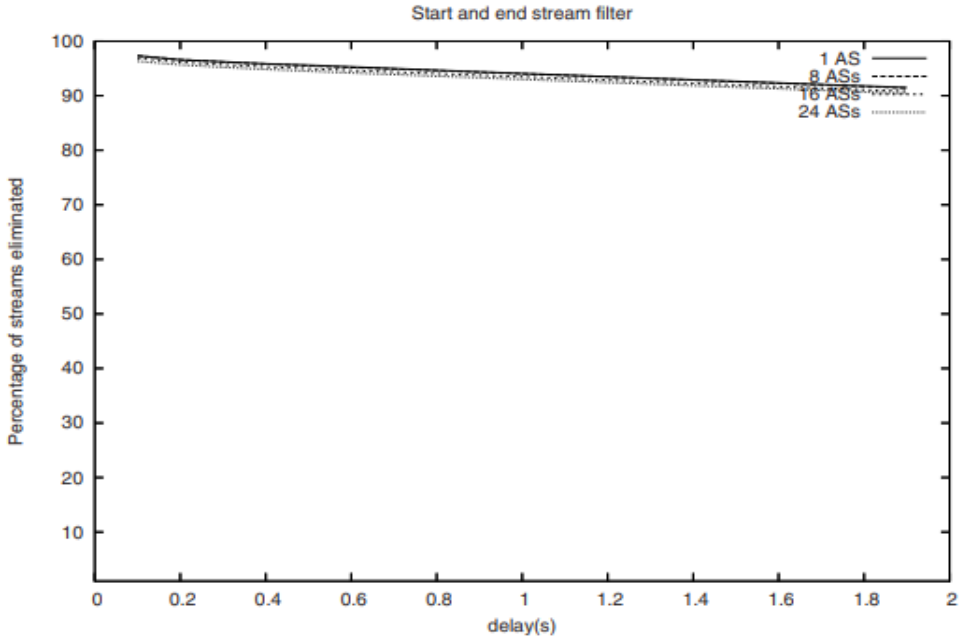
[43] OSPF(eng. Open shortest path first) otvoreni usmjerivački protokol čije su specifikacije javne, koristi Dijakstrin SPF algoritam za pronalaženje najkraćeg puta

zabilježenim TOR protocima. S obzirom na to da je promet *multiplexed,* nije moguće otkriti točno kada je promet tokova započeo i završio.[44]

Sa dodatno uzrokovanim kašnjenjem za više prometa, postoji potreba za varijablom vrijednosti kašnjenja.

Izvođenjem napada korištenjem vrijednosti od *d* rangiraju se od .1 do 2 sekunde, povećanjem koraka od .1s i povećanjem broja klijenata.

Izvor 20.advances-in-computer-science-asian-2007-computer-and-network-se-2007.pdf



Slika 20. Praćenje postotka toka

Kao što se vidi na slici početni i završni filter za praćenje eliminira visoki postotak protoka:

- do 98 % na mreži rjeđeg prometa mreže
- 96 % najgušćeg prometa mreže

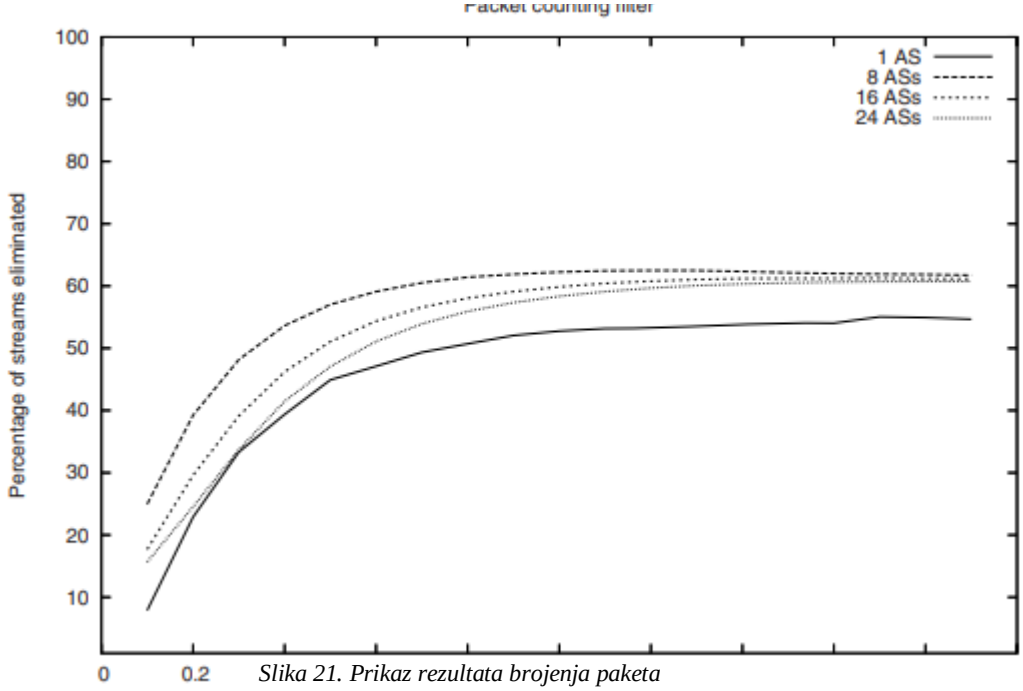
[44] Ibidem, str. 50

6.8. PACKED COUNTING ATTACK

Napad brojenja paketa sastoji se od računanja broja paketa čvorova koji ulaze i onih koji izlaze iz njega za određeni vremenski interval. Uspoređujući broj paketa za određeni tok, ulazni čvor, sa brojem paketa koji napuštaju čvor. Može biti moguće odrediti koji čvor povezuje pakete koji se šalju.

Osnovna ideja napada je ponovno korištenje te radna obrana od pasivnih vremenskih napada te pretvaranje u obranu protiv *timing attack* napada. Paketi se šalju preko nekoliko staza kroz mrežu anonimnosti prema korištenoj obrani, dakle šalju se na svaki čvor u određeno vrijeme. Ukoliko napadač ne kontrolira većinu mreže tada se aktivni napadi mogu braniti jer paketi nad kojima se ne manipulira uvijek stižu na odredište na vrijeme. Poanta je da ukoliko se može pronaći efikasna obrana od pasivnih napada vremena tada se ta ista obrana može koristiti za borbu protiv aktivnih vremenskih napada.[45]

Izvor 21. advances-in-computer-science-asian-2007-computer-and-net



Slika 21. Prikaz rezultata brojenja paketa

[45] Ibidem, str.51

Jednaka metoda, varirujućih *d* vrijednosti korištena je kao u prethodnom primjeru. No, korišteni tokovi su analizirani, odnosno to su oni tokovi koji su prije bili filtrirani na početku i kraju napada. Slika 21. prikazuje da 2% do 4% tokova je napušteno od početka i kraja vremena napada te se dodatno smanjuju za otprilike 5% do 15% sa brojenjem paketa napada.[46]

6.9. STREAM CORRELATION ATTACK - fixed the window

Tehnika je postavljanje veličine prozora *w* te brojenje broja primljenih paketa, započeto u vrijeme *t*, kroz veličinu prozora.

Proces je ponovljen za trajanje toka. Slijed brojenja paketa može biti uspoređen sa slijedom drugih tokova u mreži. Križanje funkcija koeficijenta korelacije koristi se uspoređivanjem nizova. [47]

Koristi se formula:

$$r(d) = \frac{\sum_i ((x_i - \mu)(x'_{i+d} - \mu'))}{\sqrt{\sum_i (x_i - \mu)^2} \sqrt{\sum_i (x'_{i+d} - \mu')^2}}$$

- 2 toka uspoređena su sa *x* i *x'* sa *d* koji predstavlja vrijeme kašnjenja.
- x_i je i-ti paket toka *x* i *xi'* je i-ti paket računan od toka *x'*
- *μ* je prosjek broja paketa računanih u toku, *μ'* je prosjek broja paketa u toku *x'*

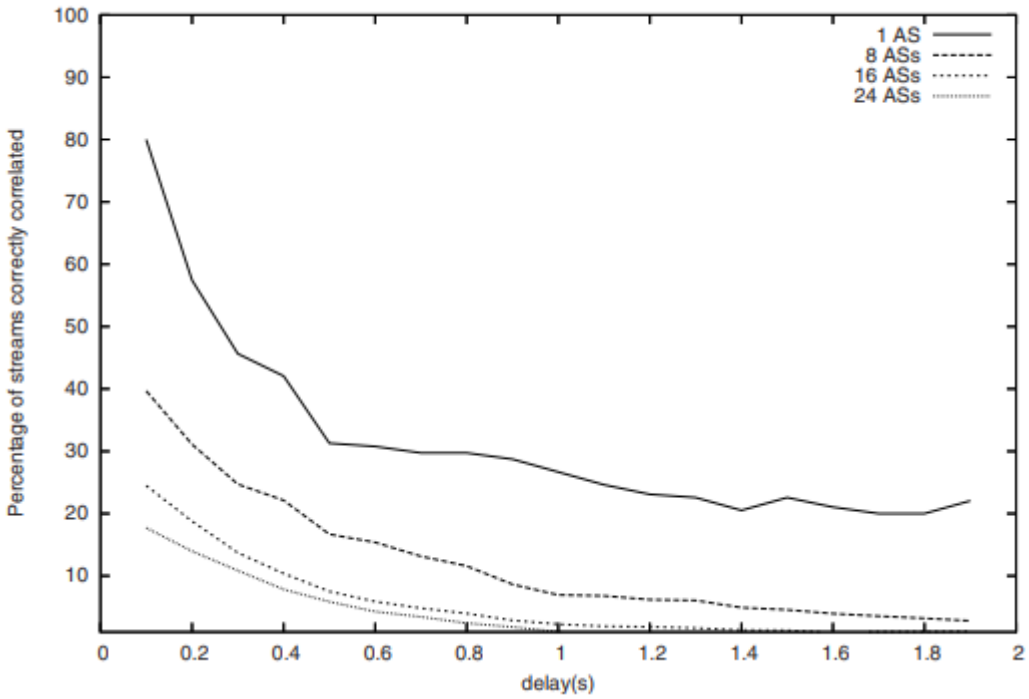
Što rezultat više teži ka 1, veća je sličnost tokova.

Jednaka korelacijska funkcija koristi se za *end to end* potvrdu prometa. No, potrebne su manje izmjene napada. Potrebno je da TOR protokol podijeli HTTP podatak u 512 *bytne* ćelije. Broj paketa poslanih sa HTTP servera nije isti kao broj

[46] Ibidem, str.51
[47] Ibidem, str.51

paketa koji je zaprimljen od TOR proxy-a. Za određeni interval napada, vrijeme window od 1s je fiksno. Fiksno vrijeme intervala je vrlo efikasno.

Izvor 22. advances-in-computer-science-asian-2007-computer-and-net



Slika 22. Prikaz konstantnog vremena prvog napada

Slika br. 22 prikazuje da je 80 % toka točno identificiranog na niskoj mreži prometa. Većina korelacija odvojenih tokova je vrlo jednostavno korelirana.

Na gušćoj mreži napad pokušava biti manje efektivan, no sa dodanim šumom multiplexed prometa.

Kako se vrijeme kašnjenja povećava, točnost napada ubrzano pada. Korištenjem gušće mreže, najtočniji napadi su svejedno na prvom kašnjenju. Time prikazuje da mrežna zakrčenost ne dokazuje prvotna predviđanja. Najvjerojatniji je rezultat visoke

propusnosti klijenata i server. Realna vrijednost propusnosti i povećan promet mogu demonstrirati efekt zakrčenosti mreže. [48]

[48] Ibidem, str. 52

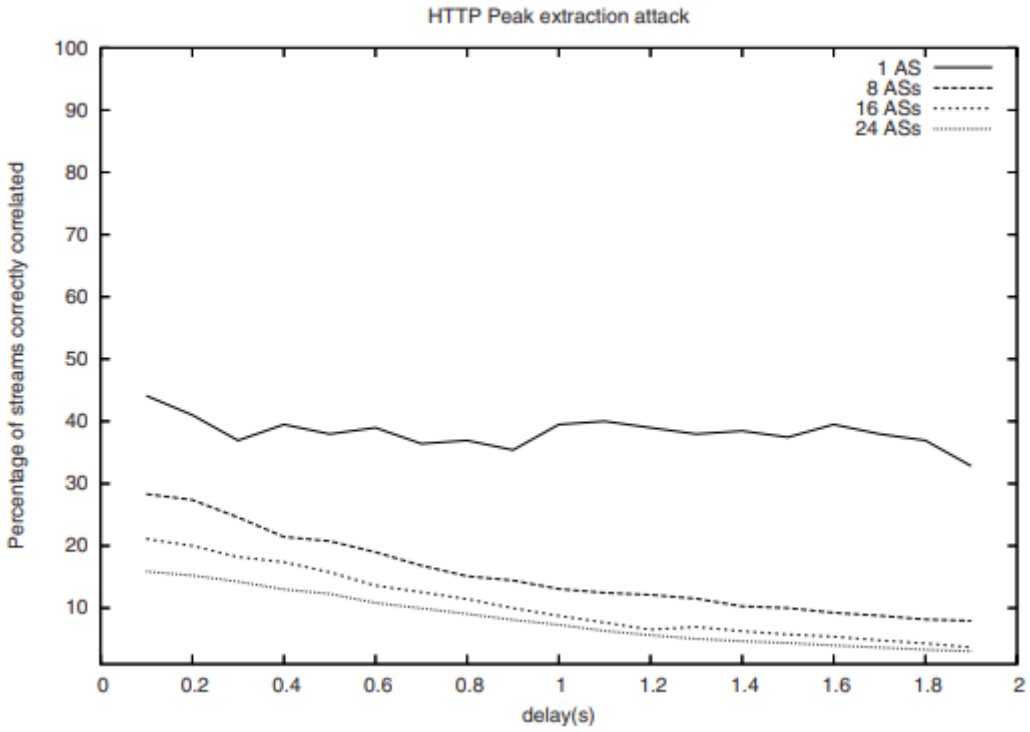
6.10. PEAK EXTRACTION

Alternativa za korištenje fiksnog vremenskog intervala je prekinuti svaki tok u fiksiranom dijeljenju. Računajući broj paketa u promatranom dijeljenju te korelirajući ih sa prethodno navedenom funkcijom. Vrijednosti dijeljenja mogu biti određene ispitivanjem HTTP toka. HTTP promet je ujedno i najgušći.

Određena web stranica će sadržavati broj objekata, svaki od objekata je preuzet zasebno te može poslužiti kao najizraženiji/prasak promet, ili pak kao vrh kroz vezu.

Dobiveni su omjeri za svaki završetak vrha. Omjeri mogu biti primijenjeni u TOR toku. Dopuštajući da za vrijeme kašnjenja d, odgovarajući paket brojenja trebao bi biti jednak.[49]

Izvor 23.advances-in-computer-science-asian-2007-computer-and-net



Slika 23. Peak exctraction napad

[49] Ibidem, str. 52

Rezultati peak extraction napada prikazani su na slici 23. Napad nije toliko utjecajan kao fiksni prozor prvog napada, no malo je robusniji kada se koriste netočne informacije kašnjenja. Postotak stream uspješno identificiran opada nižom brzinom od napada fiksnog intervala. Stopa uspjeha nadmašuje napad fiksnog intervala za veće vrijednosti kašnjenja. [50]

Početni analitički rad pomoću prometnih matrica pružio je mjerne podatke za mjerenje napora koji je potreban da bi se spriječili napadi korelacijske struje. Ovaj rad sadrži i entropiju za mjerenje anonimnosti. Uzimaju se stvarna mjerenja u prometu iz mreže kampusa no napadi nisu opisani.

Levine i sur. opisuju globalne pasivne protivničke napade za korelacijske streamove. Korištena tehnika opisana je u odjeljku sa rezultatima. Levine i sur., napadi ne vode računa o multipleksiranju prometnih tokova. Bissias i sur. kasnije su koristili koeficijent unakrsne korelacije da bi se povezali šifrirani HTTP protoci.

Shmatinkov i Wang nad Levinov rad predlažu testiranje nove obrane. Nova obrane uključuje prilagodljivo podmetanje i primjenu padding-a kako bi se osigurali da se tokovi ne razlikuju jedan od drugog.

U napadima su filtrirani rezultati provjeravajući vrijeme početka i završetka. Zhu i sur., koriste međusobnu analizu informacija i frekvencija za korelaciju TCP tokova prometa. U tekućem eksperimentnom radu primijenjena je analiza informacija i frekvencija na HTTP tokove generirane simulacijom. Točnost metode vrlo je niska te se kao priroda HTTP prometa ne posuđuje frekvencijskoj analizi.

Bauer i sur., proveli su najambicijoznije napade do danas korištenjem oko 60 Tor čvorova distribuiranih u testnoj mreži. Naša simulacija za razliku koristi 6000 čvorova. [51]

Početni rad na TCP *streamovima* analize, korištenje valova te četverostruke preobrazbe djeluje obećavajuće.

Namjera je razviti napade u suradnji sa više realistične topologije. Dodatni rad na provjeri točnosti simulacije u pravi Torov klijent sastoji se od *broja paketa i vremenske analize* u malim razmjerima mreža. Uz to, mjeriti će se i prosječno kašnjenje za tokove koji prolaze kroz mreže te uvođenje kašnjenja u Tor čvorove. Može se izmjeriti utjecaj kakav ima na mreži u pogledu kvalitete usluge te učinkovitosti

[50] Ibidem, str. 52
[51] Ibidem, str. 53

korelacije streama. Opći cilj je odrediti optimalan kompromis između kašnjenja i anonimnosti anonimne mreže.

Razvijena je početna TOR simulacija. Započeta je prevođenjem ranije razmotrenih napada i dobivenih rezultata. Simulaciju je potrebno proširiti kako bi se replicirao promet Gorman i S. Blott tehnike kontrole koje Tor koristi. Ovisno o tome moći će se pouzdano izmjeriti kvaliteta usluge preko mreže. Ovakva kombinacija s predstavljenim napadima kvantificirati će kompromis između kašnjenja i anonimnosti za datu mrežnu konfiguraciju. Mogućnosti testiranja i implementacije novih značajki Tor-ove simulacije pokazali su se neprocjenjivi za programere i buduće istraživače TOR-a.[52]

Napadi brojenja paketa, praćenja početka veze i opisani napad vremena unutar prilagođenog TOR simulatora su napadi od strane globalnog napadača koji mogu biti vrlo učinkoviti ako se promet prenosi zajedničkom vezom, no kada se poveća količina prometa na vezi tada pak postaje manje učinkovit. Vremenski napad end to end tj., napad s kraja na kraj protiv TOR mreže je također vrlo učinkovit. Analizom prometa TOR mreže, praćenjem ulaznog i izlaznog čvora može se potvrditi da određena veza prolazi kroz oba čvora. Ovaj napad otkriva korisnike i prije nego što se prenesu podaci. Napad je potvrđen eksperimentom u laboratorijskom okruženju kako bi se izbjegli mogući negativni učinci na stvarnoj TOR mreži. [53]

Skrivene usluge su tehnike pružanja anonimnosti, prekrivanjem IP adrese. Napad koristi proširenu verziju napada brojenja paketa uključivanjem informacija o vremenu kako bi se otkrila stvarna IP adresa skrivene usluge. Napad skrivenih usluga se demonstrira na TOR mreži uživo napadajući vlastite kontrolirane skrivene usluge. Pasivni napadi *end to end* se mogu vrlo uspješno upotrijebiti protiv TOR mreže. [54]

Kako bi se potvrdio napad *end to end* koreliranjem mrežne statistike prometa. Kada se korisnik poveže na poslužitelja pod kontrolom napadača tada poslužitelj šalje odgovor korisniku. Prijenos odgovora sadrži prepoznatljiv prometni obrazac. Ukoliko

[52] Ibidem, str. 53
[53] Ibidem, str. 53, 54
[54] Müller K., Defending End-to-End Confirmation Attacks against the Tor Network, Department of Computer Science and MTDMT Technology, 2015

se koristi standardni softver za upravljanjem prometom nad usmjerivačima između korisnika i ulaznog čvora, te izlaznog čvora i statistike o prometu tada se prikupljaju i povezuju kako bi se uvjerilo da je korisnik pristupio zlonamjernom poslužitelju. Predlaže se obrana od konkretnog napada. Obrana se oslanja na lažne pakete s malom vrijednošću „time to live“ , TTL, koje se navodi u IP zaglavlju poslanom iz ulaznog čvora prema korisniku. Kako je vrijednost TTL vrlo mala, paketi padaju na posredničkim usmjerivačima vrlo brzo te na taj način nikada ne dopru do korisnika. [55]

6.11. METODE

Moguće je korištenje 3 različite metode : simulacije, laboratorijski eksperimenti na testnoj TOR mreži te eksperimenti na trenutnoj TOR mreži.[56] S obzirom da je velika količina podataka dostupna na The Tor Project svatko tko je zainteresiran može koristiti željene podatke te provoditi istraživanja. Problemi se javljaju ukoliko eksperiment ne može biti valjan ili ponovljiv, zato što korisnikova aktivnost nikad nije ista te se može promijeniti kroz vrijeme. Korisnici TOR čvorova konstantno se pridružuju i odlaze iz mreže.

Defending End-to-End Confirmation Attacks against the Tor Network. Korisnici se nikada ne bi trebali identificirati tijekom eksperimenta iako se ljudi oslanjaju na TOR zbog anonimne komunikacije. Eksperimenti mrežnog rada trebali bi biti pažljivo osmišljeni kako ne bi naškodili korisnicima sustava.

Laboratorijski eksperimenti na testnoj TOR mreži. Ukoliko su eksperimenti s Live TOR mrežom nemogući, idealno rješenje su privatne laboratorijske mreže. Istraživači su postavili svoju privatnu TOR mrežu te su na njoj proveli svoje eksperimente. Eksperimenti ne ometaju mrežu uživo te se izvode u kontroliranom okruženju. Privatne mreže mnogo su manje od stvarne Tor mreže te je vrlo teško stimulirati stvarnu korisničku aktivnost i promet. [57]

[55] Ibidem, str. 13
[56] Ibidem, str. 15
[57] Ibidem, str. 15

6.12. ALATI

U korištenju TOR sustava razvijena su dva alata, ExperimentTor i Shadow.[58] ExsperimetTor omogućava okretanje realističkih TOR eksperimenata pružanjem emulirane virtualne mreže s realnim mrežnim svojstvima kao što su latencija, propusnost te brzina pada paketa. Eksperimentni TOR oponaša cijelu TOR mrežu s istim karakteristikama kao prava TOR mreža. Prave aplikacije poput samog Tor-a ili web preglednika izvode se kontrolirano i povezuju se s virtualnom mrežom. To pruža istraživačima da stvore realistične eksperimente, što zapravo omogućava proučavanje učinaka na cijelu mrežu modificirane TOR mreže. Primjerice, moglo bi se primijeniti novu obrnu od napada uvjerenjem end to end napada i proučavati učinke poput performansi ili pak opterećenja na cijeloj mreži kada svi klijenti koriste obranu. ExperimentTOR upotrebljava po jedan čvor koji oponaša virtualnu mrežu i nekoliko rubnih čvorova koje se povezuju na virtualnu mrežu i pokreću aplikacije.

Shadow koristi simulaciju kako bi osigurao efikasne, točne i kontrolirane eksperimente. Shadow je jedinstven program koji tijekom simulacije izvršava stvarne i nemodificrane aplikacije poput TOR-a. Aplikacije su integrirane u Shadow putem dodatka. Shadow simulira virtualnu mrežu s latencijom i propusnošću, realističnu Tor mrežu sa kriptografijom i CPU operacijama. Shadow i ExperimentTor mogu se koristiti u iste svrhe, no Shadow ima veliku prednost, omogućava rad na jednom računalu i ne zahtjeva postavljanje različitih čvorova poput ExperimentTor-a.[59]

Sve tri opisane metode su prikladne za istraživačka pitanja. Kako bi se proučila učinkovitost napada uvjerenje end to end protiv trenutne veličine Tor mreže. Eksperimenti u mreži na živo su potrebni jer samo oni mogu dati točne odgovore u pogledu stvarne mreže. Napadi end to end mogu se proučiti jednostavnim postavljanjem dva TOR čvora, ulaznog i izlaznog čvora te usmjeravanje vlastitog klijentskog prometa preko oba čvora. Obrane koje zahtijevaju suradnju mnogi TOR čvorova potrebno je proučavati mrežom ili simulacijom jer se obrana ne može rasporediti na cijelu mrežu u živo.[60]

[58] Ibidem, str. 16
[59] Ibidem, str. 16
[60] Ibidem, str. 17

6.13. KORACI U PROVEDBI ISTRAŽIVANJA

Koraci u provedbi istraživanja kombinacijom eksperimenata na živoj Tor mreži te putem simulacija.[61]

1. Instalacija ulaznog i izlaznog čvora u live Tor mrežu te provedba end to end napada koreliranjem prometa kontroliranog klijenta koji prolazi kroz oba čvora. Istraživanje koliko može biti učinkovit napad protiv stvarne Tor mreže
2. Implementacija obrane od napada uvjerenja i ponavljanja koraka jedan s ciljem proučavanja učinkovitosti obrane u usporedbi s uspjehom napadača bez obrane. Procjenjuje se učinkovitost obrane za jednog klijenta koji koristi obranu izolirano,
3. Proučavanje učinkovitosti obrane u slučaju da svi klijenti zajedno koriste istu obranu provođenjem simulacije sa Sadow
4. Mjerenje kaznene performanse koju je obrana izrekla za cijelu Tor mrežu izvođenjem simulacije s Shadow i svim klijentima koji koriste obranu

[61] Ibidem, str.17

6.14. MJERENJE UČINKOVITOSTI NAPADA

Učinkovitost napada konačnog potvrđivanja mjeri se lažno pozitivnim i lažnim negativnim stopama. Lažno pozitivan događaj dogodio se kada napad odluči da dva prometna obrasca odgovaraju jedan drugome, dok zapravo ne odgovaraju. Lažno negativan je suprotan događaj kada napad ne može odgovarati dvojim odgovarajućim obrascima. Jednaka stopa pogreške (ERR) daje stopu po kojoj su i stope lažno pozitivne i lažno negativne. Napadač ima namjeru smanjiti ERR, dok bi učinkovita obrana trebala maksimalno povećati ERR za napadača. Za procjenu troškova povezanih sa obranom potrebno je izmjeriti performanse mreže i opterećenje mreže. Performanse procjenjuju klijenti. Preuzimaju jednake dokumente preko TOR mreže i mjere vrijeme potrebno za preuzimanje s omogućenom i neomogućenom obranom. Alat Torperf preuzima datoteke putem TOR-a i mjeri potrebno vrijeme. Svaki Tor čvor objavljuje statistiku o tome koliko je podataka prenio.[62]

Da bi se odgovorilo na pitanje, provedeni end to end napad i njegova učinkovitost opisani su kao vremenski napad. Ovaj napad izabran je u TOR-u kako izvesti eksperiment.

End to end cofirmation je napad koji nikada nije bio izveden putem mreže. Napad je ostvaren putem simulacija. Napadač kontrolira ili promatra dva čvora unutar mreže anonimnosti. Korisnik stvara stazu kroz mrežu s tim da je jedan od dva čvora prvi skočni put, a drugi čvor je posljednji skok. Napadač može utvrditi da promet u prvom skoku potječe od korisnika i da promet na zadnjem skoku ostavlja mrežu do krajnjeg odredišta. Ako napadač može pravilno uskladiti promet dva čvora, korisnik može povezati korisnika sa odredištem. Pretpostavlja se da napadač može razlikovati prometne informacije od različit korisnika na oba čvora. Korisnik A odabire put P_A kroz mrežu sa $H^A_1..H^A_N$ na putu, gdje napadač kontrolira H_1 kao prvi čvor i H_n kao posljednji čvor. Za ovaj napad je nebitan broj čvoreva, važni su samo prvi i posljednji čvor. Usporedno sa time, korisnik B stvara put P_B kroz mrežu. Napadač bilježi promet u oba čvora. Kada se opažaju obrasci prometa u H^A_1 i H^B_n, cilj je utvrditi je li A = B.[63]

[62] Ibidem, str. 18
[63] Ibidem, str. 23

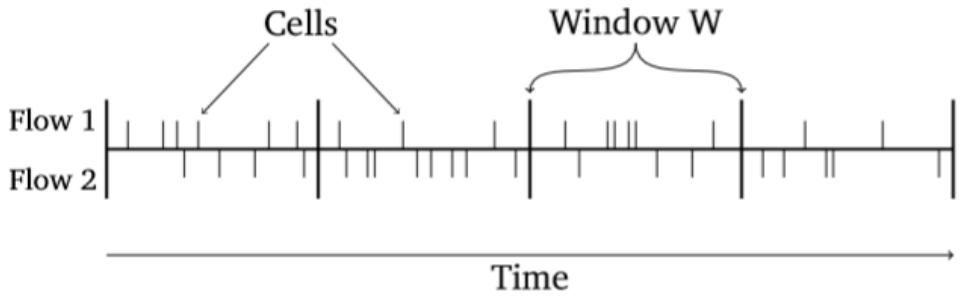
Napadač mora uskladiti sav promet na H_n s prometon korisnika A na H_1. Zbog toga preostali korisnici proizvode promet za korisnika A, ako napadač ne može pravilno povezati A promet.

Konkretan napad djeluje na sljedeći način:

Vrijeme promatranja, odnosno vrijeme u kojem napadač bilježi promet podijeljeno je u susjedne vremenske prozore W., sugerira se da je W = 1 najbolji rezultat, Za svaki prozor napadač broji broj primljenih paketa za svaki promet. xK i x 0 K označavaju broj paketa tijekom kth prozora na prvom i posljednjem čvoru. Za svaku moguću kombinaciju ulaza i izlaza iz prometa, napadač izračunava križnu korelaciju dvije vrijednosti, gdje su μ i μ0 sredstva broja paketa uspoređeni dviju polazni crtica, dok je e u intervalu [-1 ; 1]. Ako je r veći od praga t, napadač odlučuje da oba toka nose isti promet.

Pretpostavka dva prometna mehanizma, obrana krajnjih zaključaka napada protiv TOR mreže A i B. Ako je r > t , no A ≠ B, tada je to lažno pozitivno. Ako je r<t ali je A = B, tada je to lažno negativno. Kada napadač odabere t, takvu da su stope lažne i negativne pogreške jednake. Tada to daje jednaku stopu pogreške napada.[64]

Izvor 24.5be6c8cec71afd8b9514fefe5c4aca906502.pdf



Slika 24. Usporedba dva toka

Provedba napada sastoji se od dva dijela. Prvi dio modificira dva TOR čvora kako bi zabilježili prometne uzorke. Drugi dio je razvoj alata za analizu zabilježeni prometnih obrazaca, izračunavanje međusobne korelacije između obrazaca, odlučivanje o prometu podudarnosti i izračunavanje lažno pozitivnih i lažno negativnih

[64] Ibidem, str. 24

stopa. Ovakav pristup ima prednost zato što je većina logike napada implementirana u alat za analizu. Napad se može prilagoditi bez potrebe za ponovnim snimanjem podataka. Kada se jednom prikupe podaci o prometu, stvarna korelacija prometa se odvija u analizi. Ostali se zapisi ne obrađuju, te time stvaraju tako velike zapise koji sežu do nekoliko stotina megabajta. No to u principu ne stvara problem jer se stvarna analiza prometa računa korištenjem alata za analizu, a najviše vremena se troši na korelaciju prometa što iznosi n x m usporedbi za n ulaznih tokova sa m izlaznih tokova.[65]

Kako bi se zabilježili prometni uzorci, kontrolirani Tor čvorovi modificirani su na način da presijecaju svaku primljenu ćeliju u smjeru prema naprijed. Ćelije koje putuju od klijenta do odredišta i bilježe vrijeme primitka ćelije, ID kruga kojem ćelija pripada, IP adresa pošiljatelja stranice i IP adresa do koje je stranica proslijeđena. Za svaku ćeliju se navedene vrijednosti zapisuju u dnevnik. Prilikom konfiguracije TOR-a na oba kontrolirana čvora potrebno je odrediti kada treba započeti te kada treba zaustaviti snimanje podataka. Stranice se pohranjuju samo nakon što je u potpunosti uspostavljen krug između primatelja i pošiljatelja. To je potrebno kako bi se pouzdano razlikovale stranice koje putu naprijed i nazad. Također to znači da se stranice koje su potrebne za postavljanje kruga ne bilježe. Upravo zato ove ćelije nemaju veliki utjecaj na računanje unakrsne korelacije koja broji broj ćelija, zato što je taj broj zanemarivo malen u odnosu na broj ćelija koji je poslan na stvarni promet korisnika. ID kruga se priprema kako bi se mogao razlikovati promet od različitih korisnika. Izlazni čvor može primjerice primiti promet iz istog srednjeg čvora koji bi mogao pripadati različitim korisnicima. U slučaju ulaznog čvora IP adresa koja šalje pripada korisniku, dok u slučaju izlaznog čvora IP adresa pripada prethodnom srednjem TOR čvoru. U jednom od slučaja moguće je spremiti više IP adresa unaprijed zato što višestruke izlazne veze šalju preko istog kruga korisnički TOR klijent, višestruke veze se ne razlikuju jer dolaze od istog korisnika. U slučaju prometnog podudaranja, svi izlazi su ispravno dodijeljeni istom korisniku. Oba čvora spremaju svaku ćeliju sa primljenim krugovima u smjeru prema naprijed. U prometnom podudaranju, pošiljateljeva IP adresa se na ulaznom čvoru daje korisniku, dok se IP adresama ispred daje izlaznom čvoru odredišta.[66]

[65] Ibidem, str. 24
[66] Ibidem, str. 24

S obzirom na to da se napad izvodi uživo na TOR mreži sa stvarnim korisnicima koji koriste TOR za očuvanje svoje privatnosti i anonimnosti na mreži. Nijedna IP adresa nije izravno pohranjena u zapisnicima prometa. IP adrese se prikrivaju spremanjem kodiranog HMAC-a od IP adrese. Ključ koji se koristi za proračun HMAC-a je fiksiran, tako da jednake IP adrese proizvode isti HMAC. Za analizu snimljenih obrazca prometa nepotrebno je znati stvarne IP adrese sve dok je jednaka IP adresa predstavljena istim HMAC- om, te se time tijekom analize uspoređuju samo HMAC vrijednosti.

Alat za analizu implementiran je u Pytonu. Kao ulaz uzima dva imena naziva prometni zapisa, čita ih te analizira datoteke. Svaki jedinstveni ID kruga predstavlja jedinstveni promet s IP adresom pošiljatelja te prethodne IP adrese. Ako se IP adresa nalazi u prometnom dnevniku te ako je označena da dolazi od kontroliranog klijenta tada također dobiva označen glas. Tijekom svake sekunde snimanja broje se stanice. Nakon što se raščlane oba polja, alat izračunava n x m korelacije svih ulaznih tokova sa svakim izlaznim tokom. [67]

Za svaku korelaciju alat određuje, je li :

Istinito - pozitivna, ako je r >= t tada se označavaju i ulazni i izlazni tokovi
Negativno – pozitivna, ako je r>= t tada jedan, ili oba toka nisu označena
Istinito – negativna, ako je r < t onda jedan ili oba toka nisu označena
Lažno – negativna, ako r< t tada su oba ulaza i izlaza označena

[67] Ibidem, str. 25

7. ZAKLJUČAK

S obzirom na to da je Onion usmjeravanje tehnika pomoću koje se korištenjem kriptografije i prosljeđivanjem poruka kroz niz posrednika povećava anonimnost korisnika Interneta, postoje razno razni napadi koji bi željeli narušiti anonimnost korisnika. Tor mreža štiti korisnike od analize prometa, oblika nadzora Internet aktivnosti korisnika koji omogućavaju utvrđivanje izvorišta i odredišta poruka. Nakon svih navedenih i pojašnjenih napada dolazi se do zaključka da svaki od njih može biti vrlo učinkovit no problem je u tome što nije poznato rade li protiv trenutne, postojane TOR mreže. Napadi brojenja paketa, praćenja početka veza te napad unutar vremena prilagođenog TOR simulatora su zapravo napadi od strane globalnog napadača koji mogu biti vrlo učinkoviti. Sustav ima problema u situaciji kada je mreža prenapučena, te tada postaje manje učinkovit. Napad end to end, se posebno ističe zato što analizom prometa TOR mreže, praćenjem ulaznog i izlaznog čvora može potvrditi da određena veza prolazi kroz oba čvora. Ovaj napad otkriva korisnike prije nego što se prenesu podaci, i vrlo bitno je za napomenuti da je napad potvrđen eksperimentom u laboratorijskom okruženju kako bi se izbjegli negativni učinci na stvarnoj TOR mreži. Pasivni napad end to end se može vrlo uspješno upotrijebiti protiv Tor mreže.

Također, analiza je vrlo bitna zato što korištenje skupih obrana može odbiti korisnike ili pak umanjiti anonimnost preostali korisnika. Nadalje, Tor ne može riješiti sve probleme povezane sa anonimnošću te se prvenstveno fokusira na zaštitu prilikom prijenosa podataka. Anonimni sustav treba korisnika koji omogućava promet ka drugim korisnicima. Veći skup anonimnosti može pružiti bolju anonimnost zato što je napadaču teže povezati mrežne aktivnosti pojedinih korisnika. Za bolju anonimnost je nekada bolje imati više korisnika.

Prilikom proučavanje simulacije uočeno je da je korištena analiza informacija i frekvencija za korelaciju TCP tokova prometa. No točnost metode je vrlo niska zato što se kao priroda HTTP prometa ne posuđuje frekvencijskoj analizi. Rad na TCP streamovima analize, korištenje valove te četverostruke preobrazbe imaju smisla te djeluju obećavajuće. Glavna namjera je razviti napade u suradnji sa više realistične topologije. Kako bi se provjerila točnost simulacije u Toru, provjera se brojanjem paketa te vremenskom analizom u malim razmjerima mreža. Također, mjeri se i prosječno uvođenje kašnjenja u Tor čvorove. Opći cilj je odrediti optimalan kompromis između

kašnjenja i anonimnosti anonimne mreže. Programeri i budući TOR – istraživači imati će nebrojene mogućnosti testiranja i implementacije novih značajki TOR simulacije.

LITERATURA

ČLANCI U ČASOPISU

1. Dingledne R., Mathewson N. i Syverson P., „Tor: The Second-Generation Onion Router“, SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium, Vol. 13, 2004., str. 1-17
2. Ibrahimpašić B., „RSA Kriptopsustav“, Osječki matematički list 5, 2005., str. 101-112
3. Staletić N., Staletić P., Simović A., „Sigurnost Tor mreže u zaštiti identiteta na Internetu“ Infoteh-Jahorina, Vol. 13., 2014., str. 913-917.
4. V. Ubavić i D. Oklonđija, „Ostvarivanje anonimnosti na Internetu korištenjem Tor mreže“, Visoka poslovna škola profesionalnih studija – Blace, Časopis za ekonomiju, menadžment i informatiku 2013., Vol.2, 2013., str. 39-48

ČLANCI U ČASOPISU: ELEKTRONIČKA BAZA

1. CarNet Hrvatska akademska i istraživačka mreža, „Diffie – Hellmanov protkol“, NCERT-PUBDOC-2009-12-284, 2009., str. 1-23. Dostupno na: CERT.hr, (pristupljeno: 20. lipnja 2019.).
2. CarNet Hrvatska akademska i istraživačka mreža, „TLS protokol“ CCERT-PUBDOC-2009-03-257, Revizija 1.04, 2009., str 1-29. Dostupno na: CERT.hr, (pristupljeno 20. lipnja 2018.).
3. CarNet Hrvatska akademska i istraživačka mreža, „Tor – mreža za anonimnost“ CCERT-PUBDOC-2007-07-197, Revizija V1.1, 2007., str. 1-15. Dostupno na: CERT.hr, (pristupljeno 16. lipnja 2019.).
4. CarNet Hrvatska akademska i istraživačka mreža, „Tor mreža – tehnička pozadina i napredno korištenje“, NCERT-PUBDOC-2018-2-356, 2018., str. 1-20. Dostupno na: CERT.hr, (pristupljeno: 15. kolovoza 2019.).
5. Centar informacijske sigurnosti,“Onion routing“, CIS-DOC-2012-09-061, 2012., str. 1-23. Dostupno na CIS.hr, (pristupljeno: 18. lipnja 2019.).
6. Hrvatski jezični portal. Dostupno na: hjp-znanje.hr, (pristupljeno: 10.lipnja 2019.)

ONLINE ČLANCI

1. AMI Familiy, „How does RSA work?“, 2017., https://hackernoon.com/how-does-rsa-work-f44918df914b (pristupljeno: 15. srpnja 2019.).
2. Centar informacijske sigurnosti, „ Kriptiranje podataka“, 2011., https://www.cis.hr/sigurnosni-alati/kriptiranje-podataka.html, (pristupljeno: 10. lipnja 2019.).
3. Dujella A., „Klasična kriptografija, Osnovni pojmovi“, https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html, (pristupljeno: 10. lipnja 2019.).

4. Gavin O' Gorman and Stephen Blott, Large Scale Simulation of Tor: Modelling a Global Passive Adversary, Dublin City University, 2007., str. 48-54
5. Grigorik I., „High Preformance Browser Networking, Transport Layer Security (TLS)", Networking 101, Chapter 4, 2013., https://hpbn.co/transport-layer-security-tls/#rsa-diffie-hellman-and-forward-secrecy, (pristupljeno: 15. srpnja 2019.).
6. Muller K., „Defending End-to-End Confirmation Attacks against the Tor Network", Background, Methods, End - to – End Confirmation Attack, Master of Science in Information Security, 2015., https://pdfs.semanticscholar.org/1aac/5be6c8cec71afd8b9514fefe5c4aca906502.pdf, (pristupljeno, 17. kolovoza 2019.)

POPIS SLIKA

Slika 1. Prikaz OSI modela 3
Slika 2. Tor logo 7
Slika 3. Prikaz popisa imenika Tor čvorova 11
Slika 4.Odabir jezika prilikom instaliranja TOR-a 14
Slika 5. Odabir mjesta pohrane Tor Browsera 14
Slika 6. Prozor izgleda završetka instalacije Tor Browsera 14
Slika 7. Prikaz početne stranice Tor Browser pretraživača 15
Slika 8. Prikaz ispravno konfigurianog Tor Browsera 15
Slika 9. Pretraživanje koristeći Tor Browser 16
Slika 10. Prikaz TOR sustava 17
Slika 11. Prikaz dijelova sigurne i nesigurne komunikacije 18
Slika 12. Prikaz odabira nasumičnih čvorova 19
Slika 13. Prikaz broja direkno povezanih Tor klijenata u Hrvatskoj 23
Slika 14. Prikaz top 10 zemalja po direktno spojenim klijentima 24
Slika 15 Prikaz top 10 zemalja po korištenju mostova za spajanje 24
Slika 16. Prikaz korištenja IPv4 protokola u posljednja 3 mjeseca 25
Slika 17. Prikaz učestalosti korištenja IPv6 protokola u razdoblju od 3 mjeseca 25
Slika 18.Prikaz vizualizacije prosječnog broja korisnika po zemljama 26
Slika 19. Prikaz Diffie - Hellamanove razmjene ključeva 39
Slika 20. Praćenje postotka toka 45
Slika 21. Prikaz rezultata brojenja paketa 46
Slika 22. Prikaz konstantnog vremena prvog napada 48
Slika 23. Peak exctraction napad 49
Slika 24. Usporedba dva toka 56

SAŽETAK

S obzirom na to da se u današnje vrijeme svakodnevno koristi Internet, po nekoliko sati dnevno, potrebno se je zapitati je li pretraživanje Interneta zaista toliko bezazleno ili pak netko pokušava narušiti našu privatnost. Korištenjem Tor pretraživača korisnicima se omogućava anonimna komunikacija. Onion protokol štiti anonimnost pošiljatelja i primatelja poruke. Postoji nekoliko vrsta napada i napadača koji pokušavaju narušiti anonimnost komunikacije, neki od njih su *end to end attack,* napadi brojenja paketa, praćenja početka veze te napad unutar vremena prilagođenog TOR simulatora. Brojenjem paketa i vremenskom analizom provjerava se točnost simulacije u Toru. Moguće je korištenje tri različite metode : simulacije, laboratorijski eksperimenti na testnoj TOR mreži te eksperimenti na trenutnoj TOR mreži.
Sve tri opisane metode su prikladne za istraživačka pitanja. Kako bi se proučila učinkovitost napada uvjerenje end to end protiv trenutne veličine Tor mreže. Eksperimenti u mreži na živo su potrebni jer samo oni mogu dati točne odgovore u pogledu stvarne mreže. Napadi end to end mogu se proučiti jednostavnim postavljanjem dva TOR čvora, ulaznog i izlaznog čvora te usmjeravanje vlastitog klijentskog prometa preko oba čvora. Implementirani su brojni napadi. Rezultat napada omogućava ispravnu demonstraciju TOR simulacije. Što je veći promet, biti će i veće kašnjenje po mreži.

Ključne riječi : Onion protokol, TOR, timing attack, end to end attack, anonimity

SUMMARY

Considering that the Internet is being used on a daily basis nowadays, for several hours a day, it is to ask if the internet search is really that harmless or if someone is trying to violate our privacy. It's really important to think about privacy problems. Using Tor search engines allow users to communicate anonymously. Onion protocol protects the anonymity of the sender and receiver of messages. There are several types of attackers and attackers who have tried to compromise the anonymity of communications, some of them have gone into the ultimate attack, attacked packet numbers, tracked the start of a connection, and attacked within the time adapted to the TOR simulator. Packet counts and time analyzes have verified the accuracy of Tor simulations. Three different methods can be used: simulations, laboratory experiments on the test TOR network, and experiments on the current TOR network. All three methods described are appropriate for research questions. To study the effectiveness of an end-to-end assurance attack against the current size of the Tor network. Live network experiments are needed because only they can give correct answers regarding the real network. End-to-end attacks can be explored by simply deploying two TOR nodes, an inbound and an outbound node, and routing your own client traffic across both nodes. Numerous attacks have been implemented. The result of the attack allows a proper demonstration of the TOR simulation. The higher the traffic, the greater the delay in the network.

Key words: Onion protokol, TOR, timing attack, end to end attack, anonimity