Anton Luka Šijanec
Projektna naloga za Informatiko
Princip in delovanje omrežja Tor

Gimnazija Bežigrad
16. april 2020

Princip in delovanje omrežja Tor

Omrežje za anonimen prenos podatkov po Internetu

Kazalo vsebine

Ključne besede

Omrežja, internet, računalništvo, tehnologije, anonimnost, varen pretok informacij, informacijska varnost, protokol omrežja Tor, Tor, Čebulno posredovanje, zgodovina Tora, uporaba Tora, cenzura Interneta, uporaba Tor omrežja.

Povzetek

Ta dokument predstavlja bistvo omrežja Tor in bralca nauči predvsem o tehničnih značilnostih omrežja in omeni in razloži protokole, ki se uporabijo za varen in anonimen oziroma anonimiziran pretok informacij po medmrežju s pomočjo enega izmed standardnih primerov uporabe čebulnega posredovanja, predstavi njihove pomanjkljivosti in izpostavi njihove prednosti ter lastnosti.

1. Uvod

1.1. Zgodovina in nastanek

Z začetkom 21. stoletja in pojavom vse več novih iznajdb na področju informatike se je vedno bolj postavljalo vprašanje o nadzoru in cenzuri na tedaj vedno bolj razvitem delu Interneta, *World Wide Webu*. Vedno več držav se je zbalo prekomernega dostopa državljanov do širšega sveta, saj bi tako vse lažje prišlo do uporov, državnih udarov in protestov glede državnih uradov in njihovega načina delovanja. Cenzura prenesenih podatkov in informacijskih služb velja predvsem za manj razvite države, ki še vedno delujejo na bolj totalitarističnem principu vladanja, kot na demokratičnem.

Prav zato so leta 2002 ameriški računalniški programerji in podporniki svobodne in odprte programske opreme, na čelu z Rogerjem Dingledinom in Nickom Mathewsonom, na podlagi Čebulnega raznašanja informacij (angl. Onion routing) ameriškega NRL raziskovalnega laboratorija izdelali brezplačno programsko opremo Tor oziroma The Onion Router, katere glavni cilj je prikriti identiteto vseh uporabnikov omrežja in jim zagotoviti čim večjo anonimnost, tako lastnikom spletnih mest in drugih storitev, kot tudi končnim uporabnikom storitev v Tor omrežju in storitev v celem Internetu.

Omrežje in omrežni protokol Tor sta postajala vedno popularnejša in dobivala sta vedno več uporabnikov, kar je temelj in prvi korak k zdravemu omrežju.

1.2. Stanje Tora dandanes

Programska oprema je še dandanes redno posodobljena in na sploh zaupana s strani največjih organizacij, podjetij in milijonov uporabnikov po celem svetu. Slehernemu uporabniku nudi popolno anonimnost in nezmožnost sledenja.

Njihov največji in najuspešnejši projekt je Tor Browser, ki tudi tehnološko manj izobražene uporabnike računalnikov z nekaj kliki poveže v Tor in jim ponudi vse funkcije navadnega brskalnika, le da so popolnoma anonimni in enolično prikazani spletnim stranem in vsakemu drugemu uporabniku Tor mreže.

2. Uporaba omrežja

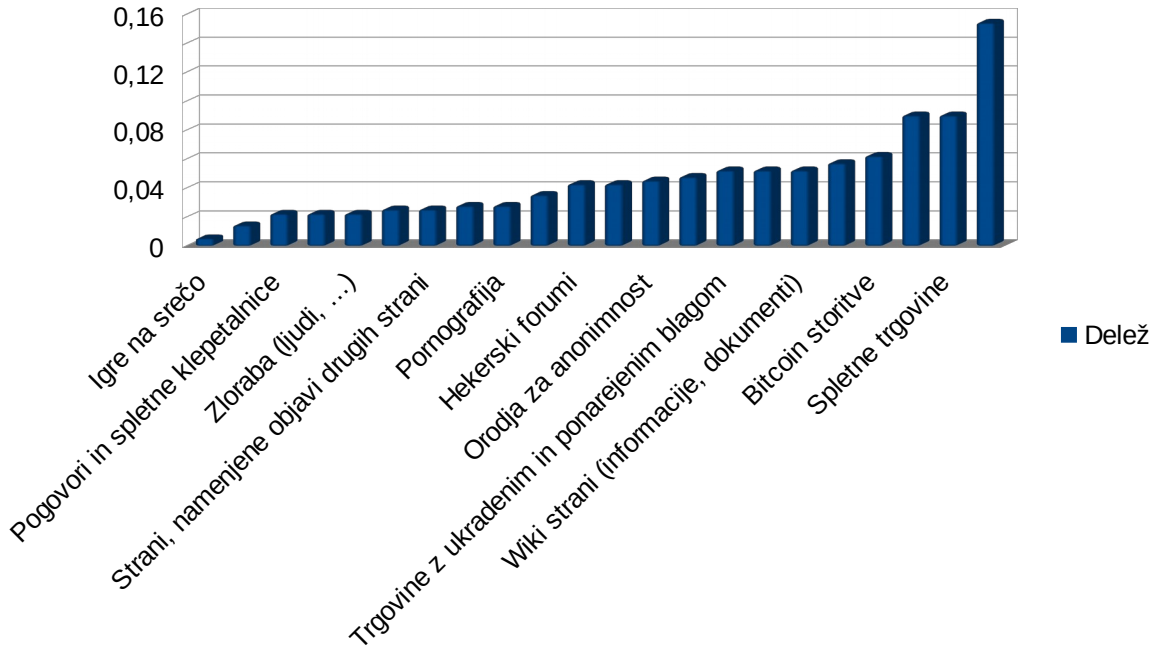
Raziskava Daniela Moora iz leta 2016 nam pokaže, da je Tor omrežje v zadnjih letih še najbolj uporabljeno za ilegalne namene, kar ne preseneča, glede na to da so policijski pregoni težko izvedljivi.

Kljub temu, da je bilo programje sprva namenjeno za posredovanje informacij iz in v cenzurirana območja, so uporabniki naredili oster ovinek in protokole začeli izrabljati za ilegalne in nemoralne namene.

2.1. Preglednica

Kategorija storitve	*Delež*
Igre na srečo	0,5 %
Pištole in drugo orožje	1,4 %
Pogovori in spletne klepetalnice	2,2 %
Nove, še ne indeksirane storitve	2,2 %
Zloraba (ljudi, …)	2,2 %
Splete knjige	2,5 %
Strani, namenjene objavi drugih strani	2,5 %
Osebni blogi in blogi kultur	2,75 %
Pornografija	2,75 %
Gostovanje spletišč	3,5 %
Hekerski forumi	4,25 %
Spletni iskalniki	4,25 %
Orodja za anonimnost	4,5 %
Ostali forumi	4,75 %
Trgovine z ukradenim in ponarejenim blagom	5,2 %
Žvižgači	5,2 %
Wiki strani (informacije, dokumenti)	5,2 %
Ponudniki elektronske pošte	5,7 %
Bitcoin storitve	6,2 %
Prevare, goljufije	9 %
Spletne trgovine	9 %
Droge	15,4 %

2.2. Grafikon



3. Splošna sestava omrežja

Trije ključni elementi oziroma gradniki omrežja Tor so:

- *Directory* strežniki (centralizirani za celotno mrežo)
- Relayi/Nodes oziroma posredniki
- Uporabniki

Uporabnik omrežja je vsak, ki s Tor Brskalnikom obišče neko spletno stran ali uporablja neko spletno storitev preko Tor omrežja, oziroma vsak, ki upravlja spletišče oziroma drugačno skrito storitev na Toru (Hidden Service). To je lahko vsak uporabnik Interneta, ne glede na zaostrene pogoje operaterjev.

Relayi oziroma posredniki so strežniki na Internetu, ki jih upravljajo prostovoljci z namenom širjenja Tor omrežja. Več kot je Tor posredniških strežnikov, hitrejše bodo povezave, omrežje bo bolj zdravo in anonimnost posameznikov bo večja in bolj zagotovljena. Posredniški strežnik lahko gostuje vsak z lastno Internetno povezavo in lastnim naslovom IP, ki prostovoljno želi pripomoči k omrežju in njegovemu razvoju.

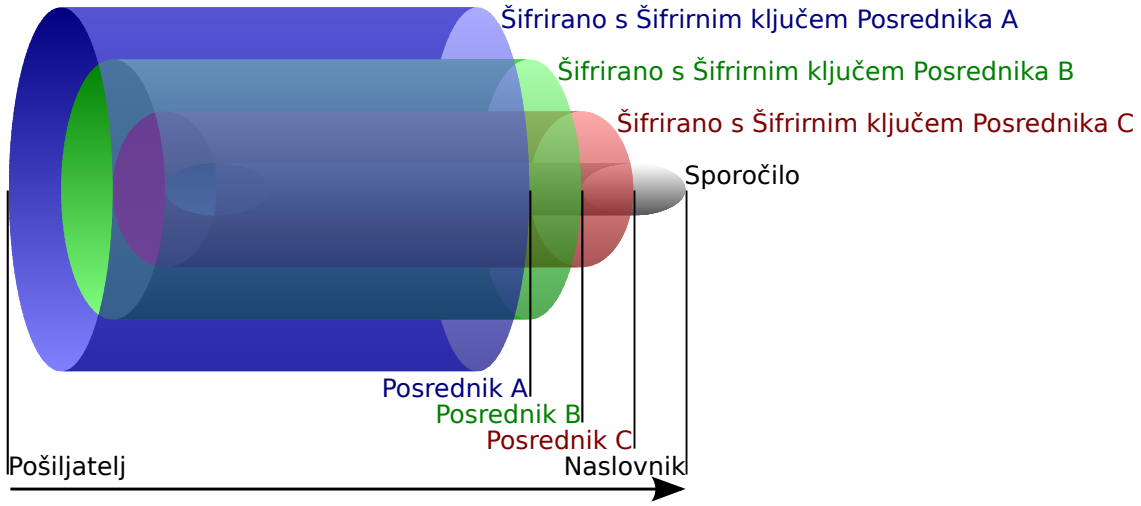
Directory strežniki se uporabijo za gostovanje informacij o relayih. Vsak IP naslov relaya je javno objavljen v directory strežnikih, ki jih upravlja organizacija Tor. Vsake toliko časa bo vsak Tor program na uporabniških napravah zahteval ta seznam posrednikov, da osveži lokalno kopijo.

4. Povezave na principu Čebulnega posredovanja

Čebulno posredovanje oziroma Onion Routing je izjemno pomemben faktor ohranjanja skrivne identitete. Vsaka povezava uporabnika do uporabnika, ne glede na vrsto prenesenih podatkov poteka prek šestih naključno izbranih posredniških strežnikov v omrežju. Da so končni podatki neberljivi slehernemu posredniškemu strežniku, je uporabljeno šifriranje. Le šifriranje pa ni dovolj, saj individualen posredniški strežnik iz njemu nedešifrabilnih podatkov ne bi uspel izluščiti destinacije mrežnega paketa. Zato je uporabljeno Čebulno posredovanje in šifriranje.

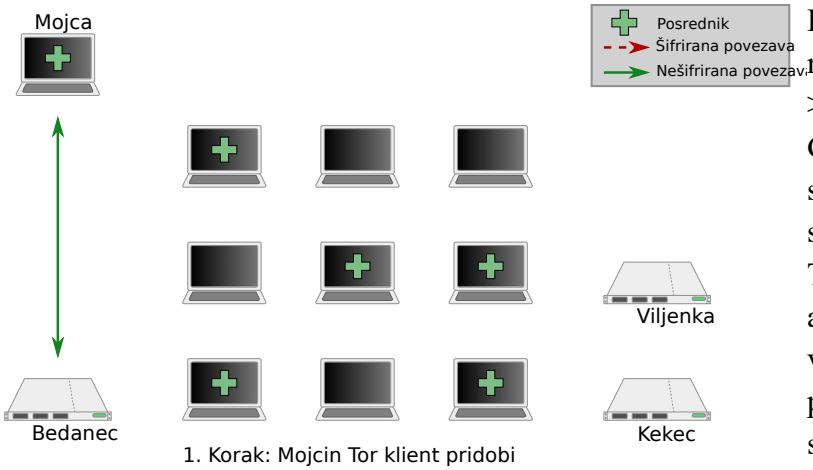
Čebulno posredovanje oziroma šifriranje deluje tako, da ima vsak strežnik na poti informacij vpogled v le njemu namenjenemu sklopu informacij. Ko en uporabnik pošlje paket informacij drugemu, ga predhodno šestkrat zašifrira oziroma »zavije« v šest slojev enkripcije, v takem vrstnem redu, da jih bodo lahko zaporedno dešifrirali le posamezni posredniki, a le toliko, da preberejo destinacijo šifriranega paketa in ga posredujejo naprej, ne pa da preberejo vse informacije. Na šestem in zadnjem posredniku, kjer paket prevzame naslovnik/drug uporabnik, je prisotna le informacija, namenjena njemu, ne pa tudi ostale informacije o poti, ki jo je paket prepotoval.

Končni rezultat je torej tak, da lahko vsak posrednik izve le toliko informacij, da lahko paket posreduje, torej je seznanjen le z izvorom paketa in z naslednjim posrednikom, nikakor pa ne z obema uporabnikoma v procesu pogovora.

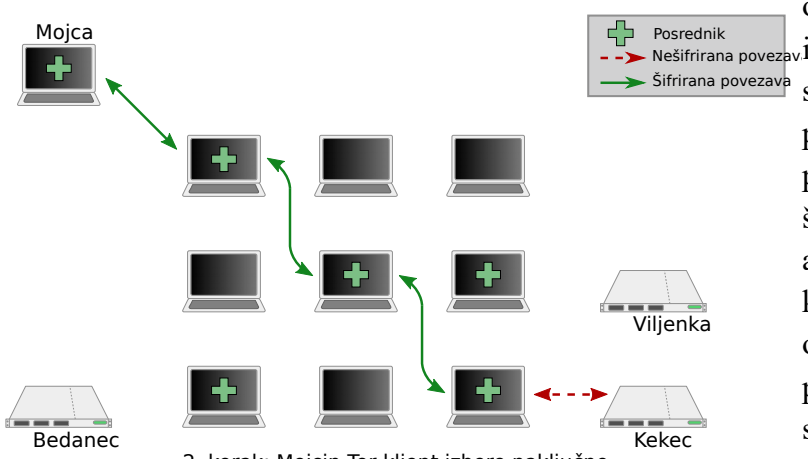


5. Izdelovanje povezav med uporabniki

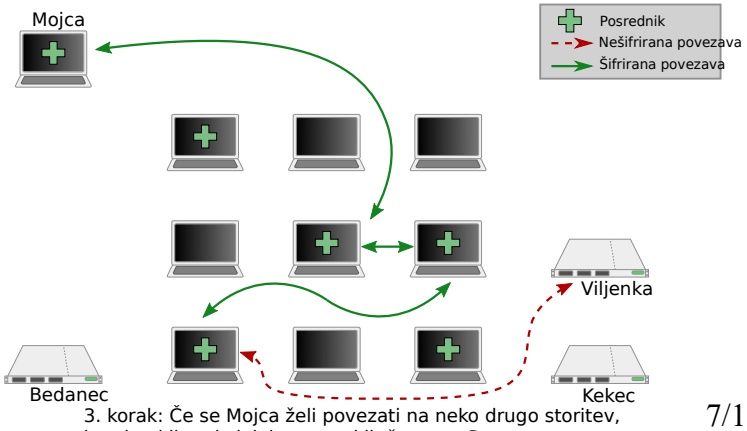
Če gre za spletišče, klepetalnico ali katero koli mrežno storitev, danes vse temeljijo na posredovanju informacij v delčkih prek Internetnih paketov oziroma transportnih pretokov, še najpogosteje z uporabo transportnega kontrolnega protokola oziroma angleško TCPja. Prav ti TCP paketi se po Toru pošiljajo tako, kot je omenjeno zgoraj, prek več različnih naključno izbranih posredniških strežnikov, kar otežuje njihovo sledenje. Kako pa se taka pot oziroma Tor *circuit* vzpostavi? Vse je po korakih opisano spodaj.



1. Korak: Mojcin Tor klient pridobi seznam Tor posrednikov od directory strežnika Bedanca.



2. korak: Mojcin Tor klient izbere naključno pot do destinacijskega strežninka. **Zelene povezave** so šifrirane, **rdeče** niso več (so praviloma znotraj enega strež



3. korak: Če se Mojca želi povezati na neko drugo storitev, bo njen klient izdelal novo naključno pot. Spet, **z elene povezave** so šifrirane, **rdeče** so znotraj enega strežnika, zategadeljci

Povezave se vzpostavljajo po običajnem načelu klient->gostitelj (angleško client->host), tako kot pri večini storitev Interneta. Gostitelj je v primeru Tor omrežja neka storitev na nekem strežniku, ki ne želi izdati svoje lokacije oziroma svojega naslova IP. Take storitve imenujemo skrite storitve ali angleško Hidden Services. Ko v Tor želimo vpeljati novo skrito storitev, po vpisu v program Tor le-ta avtomatsko pošlje vsem strežnikom, ki so del Tor omrežja, tako imenovani Hidden Service Descriptor ali opis skrite storitve. Ta vsebuje osnovne informacije za povezavo na našo skrito storitev in se po uporabniških in posredniških napravah razpošilja s protokolom DHT. Vsak zapis v tej tabeli je šifriran s 16 ali 56 znakovnim alfanumeričnim ključem, ki služi kot javni ključ za šifriranje in podpisovanje sporočil od in k skriti storitvi. S tem šifriranjem podatkov zagotovimo tudi to, da skrite storitve brez imetja tega sicer javnega ključa nihče ne bo našel. Ta alfanumerični ključ služi tudi kot domena storitve, ki se na strani klienta uporablja kot <ključ>.onion in unikatno identificira skrito storitev.

Vsaka skrita storitev ob svojem nastanku najprej vzpostavi tri polovične poti (circuite). Polovične so zato, ker še nimajo nobene destinacije, ampak samo čakajo, da se kdo na njih priklopi. Na enem koncu take poti je strežnik s skrito storitvijo, na drugem

pa trije naključno izbrani posredniki. Ko skrita storitev objavi svoj opis, vanj vključi IP naslove teh treh posrednikov.

Pa denimo, da se kot klient želimo povezati na skrito spletno stran z brskalnikom Tor Browser. Vanj bomo vnesli domeno <alfanumerični ključ skrite storitve>.onion in se povezali v Tor. Naš Tor program bo v decentralizirani mreži DHT vnosov našel tistega za našo željeno skrito storitev ter iz njega po dešifraciji z uporabo alfanumeričnega ključa iz domene izluščil tri IP naslove. Takrat naš Tor program (klient) izdela dve polovični poti, ki sestojita iz po treh naključno izbranih posrednikov. Zadnjemu posredniku prve poti pove naključno generirano zaporedje bajtov, ki ga imenujemo avtentikacijski piškotek ali angleško authentication-cookie. Z drugo potjo se nato poveže na enega izmed treh IP naslovov iz opisa skrite storitve.

Sedaj je Tor klient povezan s Tor storitvijo po enosmerni povezavi, ki deluje samo od klienta proti storitvi in storitvi pošlje sporočilo z avtentikacijskim piškotkom in IP naslovom zadnjega posredniškega strežnika na klientovi prvi prej-vzpostavljeni polovični poti. Ta posredniški strežnik imenujemo rendezvous point (izgovorimo [randevu pojnt]) oziroma slovensko točka zmenka. Skrita storitev tedaj vzpostavi novo povezavo prek treh novih naključnih posrednikov do točke zmenka in ji pove avtentikacijski piškotek, ki ga je dobila od Tor klienta.

Ker vsak paket, poslan med skrito storitvijo in klientom, vsebuje piškotek, ki je zapisan v sloju šifrirne čebule, ki ga lahko prebere točka zmenka, bo slednja točno vedela, kam mora naprej posredovati paket. Potrebno je vedeti, da skrita storitev ve samo za štiri posrednike, najbližje sebi, klient pa le tri posrednike, najbližje sebi, nikakor pa ne celotne poti, zato je piškotek edini identifikator, ki točki zmenka pove, kam naj naprej pošlje paket. Na eni točki zmenka je namreč hkrati lahko vzpostavljeno več povezav hkrati, vsaka pa je identificirana z identifikacijskim piškotkom.

Tako je vzpostavljena dvosmerna TCP povezava med storitvijo in klientom prek skupne točke zmenka. Za zaščito vpletenih povezave lahko obstajajo maksimalno okoli deset minut, po preteku tega intervala je povezavo treba ponovno vzpostaviti. To je lahko problem za aplikacijske protokole, ki se zanašajo na neprestano vzpostavljeni povezavi in niso bili izdelani z mislijo na Tor. Taki protokoli so na primer IRC in FTP ali različni zaprti protokoli računalniških igric.

6. Slabosti in nepopolnosti Tora

Večinoma sem našteval same dobre lastnosti protokola Tor, sedaj pa bom izpostavil še nekaj slabih.

- Povezave se prekinejo po desetih minutah.
  - Secure SHell aplikacijski protokol potrebuje neprestano TCP povezavo, drugače se moramo ponovno prijaviti.
  - Igranje nekaterih iger prek Tora povzroči konstantno odklapljanje, saj potrebujejo neprestano TCP povezavo (npr. Minecraft)
- Vzpostavljanje povezave je zamudno
  - Aplikacijski protokoli, ki potrebujejo več povezav, so lahko zelo neefektivni.
    - Simultan prenos večih datotek po protokolu FTP za vsako datoteko vzpostavi novo povezavo. V primeru prenosa veliko malih datotek lahko napačna konfiguracija FTP klienta pripelje do izgube časa. Sicer obstaja boljša alternativa, SFTP, ki lahko po eni povezavi prenaša več datotek hkrati.
    - HTTP/1.0 standardni aplikacijski protokol po prenosu datoteke prekine povezavo. Strežniki s spletnimi stranmi z veliko slikami in HTTP/1.0 so prek Tora težko uporabni. Sicer obstaja boljša alternativa, HTTP/1.1, ki jo podpira skoraj vsak strežniški in klient program za HTTP.
- Latenca prenosa je velika
  - Tudi pri vzpostavljeni povezavi gre vsak paket skozi šest posrednikov, torej bi igranje igric hitro postala težava.

7. Razkrivanje identitet uporabnikov Tor omrežja

Kljub varnosti in praktični ne-sledljivosti uporabnikov obstajajo še vedno možnosti za odkrivanje IP naslovov in posledično identitet uporabnikov, ki se skrivajo za Tor klienti. Še največkrat to odkrivanje ni posledica napake v Tor protokolu, ki skoraj vedno doseže največjo anonimnost. Usodne napake ponavadi uporabniki z napačno konfiguracijo zagrešijo sami. Največja varnostna luknja so storitve in aplikacije, ki tečejo za Tor požarnim zidom. To so bodisi dodatki brskalnikov bodisi aplikacije, ki niso bile namenjene za namestitev v pretirano anonimna okolja.

7.1. Spletne strani in aplikacije, ki jih le-te poganjajo

Programska oprema, ki teče v ozadju spletnih strani in je namenjena menedžmentu vsebine (angleško CMS-Content Management System) je ponavadi prva vstopna točka za napadalce v sistem. Če je različica slednje programske opreme zastarela, bo napadalec z nekaj iskalnimi poizvedbami našel javno objavljeno varnostno luknjo. Tako napadalec pride v sistem in z zahtevo na njegovo kontrolirano spletno mesto iz strežnika žrtve ugotovi njegov Internetni naslov.

Seveda je to le en od načinov za pridobitev identitete oziroma lokacije strežnika v Internetu. Velikokrat spletne aplikacije, še posebej forumi in blogi dovolijo opcijo nalaganja slik iz drugih spletišč. To lahko napadalec izrabi, saj spletne aplikacije ne pridobivajo teh slik prek Tor omrežja, temveč prek navaMed najpogostejšimi in verjetno tudi najhitrejše popravljenimi in odkritimi napadi je napad z napačnim ali prirejenim Host headerjem. Vsakič ko na spletišče naredimo zahtevo, med parametre zahteve ali natančnejše headerje vpišemo tudi domeno, katere spletno stran zahtevamo. To se je uveljavilo predvsem zato, da lahko strežniki gostujejo več spletnih strani iz istega IP naslova.

Napačno nastavljeni strežniki (predvsem Apache 2) prikažejo privzeto spletno stran v primeru, da Host header ni prisoten. Če ista Apache inštalacija gostuje tako spletno stran na Internetu, kot tudi spletno stran na Toru, lahko ob napačni konfiguraciji strežnika prek Tor spletišča dobimo Internetno spletišče tako, da Host header spremenimo bodisi na prazno vrednost bodisi na domeno, za katero pričakujemo, da je gostovana na istem strežniku.

Primer: Ob obisku Tor spletne strani namesto <tordomene>.onion v Host header ne napišemo nič. Apache strežnik bo v takem primeru poslal spletno stran, ki je nastavljena prva v konfiguracijski datoteki.

Zaščita pred take vrste deanonimizacijo: Dediciranje strežnika samo za Tor ali uporaba nginx strežniške opreme.dnega Interneta.

Zaščita pred take vrste deanonimizacijo: Pisanje programske opreme, namenjene prav za uporabo na Toru ali Torificiranje celotnega strežnika.

7.2. Strežniška programska oprema HTTP strežnikov

Med najpogostejšimi in verjetno tudi najhitrejše popravljenimi in odkritimi napadi je napad z napačnim ali prirejenim Host headerjem. Vsakič ko na spletišče naredimo zahtevo, med parametre zahteve ali natančnejše headerje vpišemo tudi domeno, katere spletno stran zahtevamo. To se je uveljavilo predvsem zato, da lahko strežniki gostujejo več spletnih strani iz istega IP naslova.

Napačno nastavljeni strežniki (predvsem Apache 2) prikažejo privzeto spletno stran v primeru, da Host header ni prisoten. Če ista Apache inštalacija gostuje tako spletno stran na Internetu, kot tudi spletno stran na Toru, lahko ob napačni konfiguraciji strežnika prek Tor spletišča dobimo Internetno spletišče tako, da Host header spremenimo bodisi na prazno vrednost bodisi na domeno, za katero pričakujemo, da je gostovana na istem strežniku.

Primer: Ob obisku Tor spletne strani namesto <tordomene>.onion v Host header ne napišemo nič. Apache strežnik bo v takem primeru poslal spletno stran, ki je nastavljena prva v konfiguracijski datoteki.

Zaščita pred take vrste deanonimizacijo: Dediciranje strežnika samo za Tor ali uporaba nginx strežniške opreme.

7.3. WebRTC

V zadnjih letih je bilo povpraševanje po videokomunikaciji vedno večje, zato so brskalniki hiteli k uveljavljanju novih tehnologij za čim hitrejši prenos videa in zvoka. Ena izmed takih tehnologij je WebRTC, ki med drugim omogoča peer-to-peer direktno povezavo med kličočimi za večjo pasovno širino in manjšo latenco. Verjetno je bil po pomoti integriran v Tor Browser, zato so ga spletne storitve, predvsem obveščevalne agencije s pridom izkoriščale nekaj dni za identifikacijo obiskovalcev strani z ilegalo vsebino. Sicer je bil takrat Tor brskalnik zasnovan in priporočen za uporabo še brez vklopljenega javascripta, ki omogoča WebRTC protokol, vendar je večina uporabnikov te smernice ignorirala. Tako je bil nevede vklopljen tudi WebRTC, ki po sami zasnovi kot odgovor na zahtevo javascript klica strežniku pošlje IP naslov računalnika. Tako je, ob vklopljenem WebRTCju, lastnik spletne strani dobil IP naslove svojih klientov. Na srečo je večina ljudi zadnje čase za virtualno NAT mrežo, torej je spletna stran dobila le privatni in nepomemben IP naslov, nekateri, priklopljeni direktno v Internet, pa so bili odkriti med brskanjem po vsebini na skriti spletni strani, za katero so stale obveščevalne agencije, še najpogosteje nemški BND in ameriška FBI in CIA.

8. Zaključek

Kljub svojim pomanjkljivostim je Tor izjemno dobro izdelan protokol in prava izbira za anonimizacijo podatkov, na katero se lahko zanesemo. Zaradi svojega odprtokodnega in prostega načina delovanja bo ostal v uporabi še veliko desetletij in v prihodnosti verjetno postal vzor novim Internernetnim protokolom in specifikacijam, saj je trenutno centralizirano stanje medmrežja nedopustno.

9. Viri

Tor (anonymity network). [internet]. 2020. [citirano 6. 2. 2020]. Dostopno na naslovu: https://w.wiki/GkF.

HANtwister@en.Wikipedia. Onion diagram.svg. [internet]. 2008. [citirano 6. 2. 2020]. Dostopno na naslovu: https://w.wiki/Gk$. Licenca: GNU 1.2, CC-BY-SA-3.0.