Alternative la rețeaua Tor

Filip Tudor-Mihail
Ichim Cosmin-Ștefan
Nistor Ștefan
Roman Ștefan

14 mai 2024

Rezumat

Această lucrare discută eficacitatea rețelei Tor, un instrument popular pentru îmbunătățirea anonimatului și securității online, care redirecționează traficul printr-o vastă rețea de noduri, maschează identitatea utilizatorilor și protejează împotriva supravegherii traficului. Deși Tor oferă o protecție substanțială, prezintă vulnerabilități, cum ar fi posibilitatea analizei traficului de către nodurile rău intenționate și creșterea latenței. Lucrarea explorează, de asemenea, tehnologii alternative, inclusiv Rețelele Private Virtuale (VPN), Proiectul Internetului Invizibil (I2P) și Rețelele Private Virtuale descentralizate (dVPN), fiecare oferind diferite niveluri de securitate, anonimizare și de experiență pentru utilizator.

1 Introducere

Astăzi, activitatea noastră digitală este urmărită mai mult decât niciodată, cu scopul de a fi profilați și pentru a ni se servi reclame cât mai specifice. Cu toate acestea, nu toate companiile ce practică acest lucru respectă cele mai bune standarde când vine vorba de securizarea și stocarea datelor cu caracter personal, iar acest lucru poate duce la breșe de securitate și posibila pierdere a acestora. Una dintre soluțiile posibile pentru această problemă este rețeaua Tor, abreviere de la "The Onion Router", ce este o unealtă foarte bine cunoscută și des utilizată în creșterea nivelului de securitate și anonimitate online. Principiul de bază de funcționare al acesteia este de a ghida traficul online printr-o rețea de aproximativ 8000 de noduri astfel încât să ascundă pe cât posibil identitatea utilizatorilor, protejându-i astfel de supravegherea traficului de internet și de analizei traficului.

1.1 Cum funcționează rețeaua Tor?

Cum a fost mentionat anterior, reteaua Tor, in procesul de transmisie al datelor, trece traficul printr-o vastă rețea de noduri. Standardul definește comunicarea prin reteaua Tor ca avand trei noduri intermediare in comunicare, unul de intrare, unul intermediar și unul de ieșire.

1.1.1 Nodul de intrare

Nodul de intrare este cel la care utilizatorul se conecteaza și prin care își va începe comunicarea în rețeaua Tor. Așadar, din moment ce acest nod este punctul de intrare al utilizatorului se poate concluziona că acesta va cunoaște adresa IP a utilizatorului, dar nu va cunoaște destinația finală a comunicării.

1.1.2 Nodul intermediar

Nodul intermediar este responsabil pentru redirectarea traficului de la nodul de intrare la de iesire. Astfel, putem spune ca acesta nu va cunoaste nici utilizatorul cat nici destinatia finala ci doar nodurile de intrare si iesire. Acest lucru creste nivelul de siguranta al sistemului.

1.1.3 Nodul de iesire

Nodul de iesire este cel care realizeaza comunicarea cu serviciul destinatie, deci se poate spune ca acesta cunoaste a doua jumatate a procesului de comunicare, dar nu cunoaste identitatea utilizatorului, neputand astfel sa faca corelarea intre un utilizator si cererea finala.

1.1.4 Utilizarea encripției

În acelasi timp, reteaua Tor se foloseste si de criptare pentru a contura și mai bine securitatea și anonimitatea acestui proces, pentru că, fără acesta, unui posibil atacator i-ar putea fi usor să urmărească traficul prin rețeaua Tor prin simpla ascultare a mesajelor în tranzit.
Procesul de criptare funcționează in felul urmator: Tor se foloseste la nivelul clientului de criptare stratificată, unde fiecărui strat îi poate fi asociat o cheie.
La nivelul procesului client, mesajul este criptat stratificat cu cheile celor trei noduri și este trimis către nodul de intrare. Acesta preia mesajul, il decripteaza utilizandu-se de cheia proprie și il trimite mai departe către nodul intermediar. Acesta procedează în același fel și îl trimite către nodul de ieșire, ce va proceda in acelasi mod și va trimite pachetul final catre destinația finală.
Prin acest procedeu in care sunt utilizate trei noduri intermediare in comunicare, unde fiecare este responsabil doar pentru transimiterea mai departe a mesajului fara sa poata corela provenienta acestuia cu serviciul final, reteaua Tor ofera un nivel ridicat de securitate in comparație cu o comunicare obișnuită.

1.2 Tor Hidden Services - servicii ascunse prin intermediul Tor

Un tip de comunicare prin reteaua Tor este cel descris anterior, în care un utilizator isi doreste sa acceseze o resursa din internetul public, dar utilizant reteaua si protocolul Tor. Tor Hidden Services este un alt scenariu de utilizare al retelei Tor, in care un utilizator isi doreste sa acceseze o resursa care nu este publica si care reprezinta la randul ei un nod Tor. În acest mod, rețeaua este utilizată pentru a menține secretă identitatea utilizatorului cât și cea a serviciului accesat.

1.2.1 Cum funcționează Tor Hidden Service?

La creare, un astfel de serviciu isi alege in mod aleatoriu trei puncte de introducere (IP - introduction point) si va realiza cu fiecare dintre acestea câte un circuit Tor, cu cate trei noduri intermediare. Astfel, aceste IP au rolul de a conecta utilizatori cu serviciul, fara a-l cunoaste. Odată realizate aceste conexiuni cu IP-urile, serviciul va crea o intrare intr-un tabel de dispersie distribuit (DHT - distributed hash table) a carei cheie va fi adresa *.onion* a serviciului (care este secretă, dar derivată din cheia publica de criptare a serviciului). În final, valoarea va fi un *hidden service descriptor*, ce va contine la rândul lui adresele IP-urilor și cheia publica de criptare a serviciului.

1.2.2 Cum accesează un utilizator Tor Hidden Service?

Pentru ca un utilizator să poata accesa Tor Hidden Service trebuie să cunoască adresa .onion a acestuia, aceste adrese nefiind publice în rețeaua Tor, ci trebuie aflate prin intermediul alte surse. Daca utilizatorul are aceasta adresa, el poate cere, pe baza tabelului de dispersie distribuit adresele punctelor de introducere ale serviciului si va alege aleatoriu unul dintre ele, prin intermediul caruia va incerca sa acceseze resursa dorită. Pentru a incepe comunicarea cu acest IP, utilizatorul va alege un nod oarecare din reteaua Tor care va servi rolul de punct de *rendezvous* (comunicarea utilizatorului cu acest *rendezvous* point se va face doar prin alte două noduri, întrucat chiar cel din urma va avea rol de nod de iesire între un IP și utilizator). La randul său, punctul de rendezvous își creaza un circuit Tor cu trei noduri pentru a comunica cu IP-ul ales de utilizator.
Pana acum comunicarea se va realiza astfel, utilizatorul trimite un mesaj de autentificare pentru serviciul final in prima faza prin punctul de *rendezvous*; acest punct trimite IP-ului mesajul de autentificare si propria adresă, iar cel din urma nod paseăza aceste informații către serviciu.
In cazul in care cererea de comunicare este acceptata de catre serviciu, serverul va crea un nou ciclu Tor cu care se va conecta la punctul de *rendezvous* (prin intermediul adresei sale atasate la mesajul

utilizatorului). Astfel comunicarea între utilizator si serviciu se realizează prin intemediul punctului de *rendezvous*, fără să se cunoască unul pe celălalt.

1.3 Slăbiciuni ale rețelei Tor și ale Tor Hidden Services

In ciuda avantajelor ce reies din mecanismele lor de functionare descrise mai sus, atat reteaua Tor cat si Tor Hidden Services sufera de mai mulți posibili vectori de atac prin care securitatea și anonimitatea oferită de acestea să fie periclitate. Un astfel de exemplu este cazul în care un utilizator rau intenționat deține numeroase noduri Tor, facand astfel posibilă analiza traficul prin acestea, care poate conduce la deducerea originii și destinației comunicărilor. Totodată, un alt aspect ce poate afecta unele tipuri de servicii este latența crescută ce vine o data cu redirectarea mesajelor prin multiple noduri, ce adeseori sunt aflate la distante geografice mari.
În continuare, in acest document vor fi prezentate alte alternative de anonimizare si securizare a traficului online, ce vor fi comparate atat din punct de vedere teoretic cat si din punct de vedere practic intre ele cât si cu rețeaua Tor.

2 Rețeaua privată virtuală sau VPN

În ultimul timp, VPN-urile au crescut foarte mult in popularitate datorita reclamei agresive realizate pe toate mediile de comunicare de catre companiile ce ofera astfel de produse. Totodata, in contextul actual in care utilizatorii isi doresct mai multa siguranta si libertate in mediul online, aceste valuri de publicitate au dus la un numar foarte ridicat de persoane din toate mediile sociale sa recurga la utilizarea unui VPN.

2.1 Cum funcționează un VPN?

Ideea principala de functionare a unui VPN este de a lua traficul utilizatorului, a-l cripta si a-l trasmite catre resursele dorite prin intermediul unui server intermediar. Astfel, rezultatul obtinut este ca serviciile accesate nu cunosc identitatea utilizatorului ce le-a accesat.

2.1.1 Realizarea conexiunii

Pentru ca un utilizator sa se conecteze un server VPN, dispozitivul acestuia va crea un canal de comunicare cu VPN-ul, care va fi criptat pentru a proteja datele in tranzit.

2.1.2 Transmiterea datelor

Odata ce conexiunea cu serverul VPN este realizata utilizatorul va putea accesa internetul oricum isi doreste si din cadrul oricarui program, traficul sau fiind redirectionat catre serverul VPN. Astfel, pentru observatori externi traficul va parea ca originand de la serverul VPN si nu de la un alt utilizator.

2.1.3 Primirea datelor

Serverul VPN acceseaza internetul in locul utilizatorului, acesta primind raspunsurile de la resursele accesate, raspunsuri care le va trimite, prin canalul criptat, inapoi catre utilizator.

2.2 Care sunt avantajele unui VPN?

- Viteza. Un prim avantaj pe care il au VPN-urile in comparatie cu reteaua Tor este viteza, intrucat rutarea traficului de internet se face doar printr-un singur nod, nu prin trei (cu o posibilitate crescuta si ca distanta geografica intre acestea trei sa fie foarte mare). Tot din punct de vedere al vitezei este si faptul ca prin utilizarea unui VPN utilizatorul isi poate alege un server mai apropiat de el, asfel crescandu-si viteza, prin comparatie cu reteaua Tor unde nu sunt alese de catre utilizator nodurile prin care se face comunicarea.

- Simplitatea. Este mult mai usor pentru un utilizator obisnuit sa isi descarce o aplicatie si sa o porneasca pentru a obtine efectul de a-si anonimiza intreg traficul de internet decat sa utilizeze

reteaua Tor. Pentru a utiliza reteaua Tor este obligat sa utilizeze un browser specific, fara un mod intuitiv de a-si redirectiona toata activitatea pe internet prin reteaua Tor.

- Mascarea si schimbarea geolocatiei. VPN-urile sunt unelte foarte simple pentru a evita restrictii privind geolocatia sa, fenomen des intalnit pe platformele de streaming.

2.3 Care este dezavantajul unui VPN față de rețeaua Tor?

Anonimitatea si securitatea, printe singurele motive pentru care multe persoane aleg sa foloseasca un VPN.
In timp ce un VPN ofera o mai buna anonimitate utilizatorului prin comparatie cu utilizarea sa normala, nu ofera acelasi nivel de anonimitate ca reteaua Tor. In reteaua Tor sunt folosite trei noduri pentru a ascunde identitatea utilizatorului, dintre care doar unul ii cunoaste adresa, VPN-urile se folosesc doar de un singur nod intermediar. Acest lucru este o problema deoarece, in cazul in care compania ce detine VPN-ul pastreaza note legate de traficul de internet care il traverseaza, se poate ajuge usor intr-o situatie in care toti utilizatorii acestuia sunt deanonimizati, impreuna cu intreaga lor istorie.

2.4 Concluzie referitoare la VPN-uri

In concluzie, VPN-urile sunt o unealta in arsenalul de securitate digitala al utilizatorilor, care poate servi foarte bine cu scopul de a evita restrictii bazate pe geolocatia sa si care poate fi si folosit pentru a masca traficul sau de internet, cu mentiunea ca intreg traficul sau trece prin acest VPN si ca depinde de securitatea si principiile de functionare ale companiei ce il detine.

3 Proiectul Internetului Invizibil sau I2P

Asemenea retelei Tor si a VPN-urilor, IP2 serveste ca o alta unealta de securitate si de anonimizare care se afla la dispozitia utilizatorilor. Aceasta este o retea anonima suprapusa, conceputa pentru a permite utilizatorilor sa comunice anonim cu ajutorul propriului set de canale criptate, cunoscute drept "tunele". Un aspect ce trebuie luat in considerare in cazul I2P este faptul ca acest proiect este mai asemanator cu Tor Hidden Services din punct de vedere al resurselor ce pot fi accesate, fata de VPN-uri sau reteaua Tor simpla. Datorita faptului ca I2P este construit ca o retea P2P, prin intermediul acestuia se pot accesa doar alte resurse care se afla tot in cadrul aceleiasi retelei, facand astfel cazurile in care poate fi utilizata aceasta foarte limitate si specifice.

3.1 Cum funcționează I2P?

Asemanator cu modul de functionare al retelei Tor, si in cazul I2P mesajele sunt trimise prin "tuneluri" alcatuite din minim doua noduri, gateway fiind punctul de plecare si endpoint find cel final, iar intre acestea se pot afla un numar oarecare de routere intermediare. Tot ca si in cazul reletei Tor, pentru a face acest tip de comunicare posibila si sigura este folosita encriptia stratificata, pentru ca nodurile individuale sa nu cunoasca continutul mesajului cat nici identitatile clientului si ale serviciului.
Un prim aspect prin care I2P se diferentiaza de reteaua Tor este separarea functionalitatii acestor tuneluri in tuneluri de intrare si de iesire. Acest lucru este realizat pentru a separa datele de intrare de cele de iesire, complicand procesul de urmarire al mesajelor. In acelasi timp, pentru a fortifica procesul de comunicare, I2P imparte mesajele in mai multe subdivizii, urmand ca fiecare dintre ele sa fie transmise prin cate un tunel diferit, astfel un posibil actor rau intentionat sa nu se poata folosi doar de o bucata a mesajului initial. Acest din urma mecanism este supranumit si ca rutare "garlic", deoarece mesajul este vazut ca un "bulb de usturoi" din prisma faptului ca acesta poate fi impartit in subunitati si "refacut".
Un alt aspect ce merita mentionat este ca aceste tuneluri sunt de scurta durata si create in mod aleator din nodurile retelei, ceea ce face urmarirea mesajelor cu atat mai complicata.

3.2 Comparație cu Tor

Atat I2P cat si Tor sunt proiectate pentru a oferi anonimat utilizatorilor lor, dar modul in care functioneaza difera semnificativ. Tor este optimizat mai ales pentru anonimizarea accesului la internet, redirectionand traficul printr-o retea de noduri intermediare. In contrast, I2P este optimizat pentru comunicatii anonime intre utilizatorii retelei sale. Un alt punct distinctiv este ca I2P foloseste tunele separate pentru traficul de intrare și de iesire, in timp ce Tor foloseste aceeasi cale in ambele directii. Acest lucru face comunicarea prin intermediul I2P sa fie mai rapida decat cea facuta prin reteaua Tor.

3.3 Avantaje și provocări

I2P ofera beneficii unice, cum ar fi o mai mare descentralizare si o specializare pentru comunicatiile anonime end-to-end in interiorul retelei sale. Aceasta poate fi avantajoasa pentru aplicații care necesita comunicare securizata si anonima intre utilizatori, dar poate fi vazuti si ca dezavantajoasa fata de reteaua Tor datorita numarului sau mai mic de utilizatori fata de cea din urma. Un alt aspect este acela ca I2P poate fi mai dificil de configurat si utilizat comparativ cu Tor, ceea ce ar putea limita accesibilitatea sa pentru utilizatorii mai putin tehnici. In plus, in timp ce I2P este puternic in ceea ce privește anonimatul in cadrul propriei rețele, nu furnizeaza aceleasi capacitati de a accesa internetul general in mod anonim, precum Tor.

4 Rețele virtuale private descentralizate sau dVPNs

Retele virtuale private descentralizate vin ca o noua abordare a retelelor virtuale private traditionale, ambele tipuri avand scopul de a prelua traficul de internet al utilizatorului si a-l ruta printr-un server astfel incat sa-i mascheze identitatea, dar in cazul tehnologiei prezentate acum nu exista un astfel de server central, ci o retea descentralizata P2P.

4.1 Cum funcționează rețelele virtuale private descentralizate?

Retelele virtuale private descentralizate folosesc protocoale moderne de criptare si tehnologii de registru distribuit, cum ar fi blockchain, pentru a stabili conexiuni sigure intre utilizatori. In loc sa se bazeze pe o autoritate centrala, participantii la retea, cunoscuti sub numele de noduri, actioneaza atat drept clienti, cat si drept servere, contribuind cu puterea lor de calcul si latimea de banda pentru a facilita serviciul VPN.

Cand un utilizator se conecteaza la reteaua VPN descentralizata, traficul sau este criptat si apoi directionat prin mai multe noduri din retea, creand un strat suplimentar de confidentialitate. Acest proces ajuta la prevenirea interceptarii, cenzurii si supravegherii, deoarece devine semnificativ mai dificil de identificat originea si destinatia datelor.

4.2 Care sunt avantajele unui dVPN față de rețeaua Tor?

- Arhitectura descentralizata. Spre deosebire de Tor, care se bazeaza pe un numar fix de noduri operate de voluntari, dVPN-urile folosesc un model peer-to-peer care poate include potential mii de noduri. Aceasta descentralizare poate oferi o mai mare rezistenta impotriva atacurilor sau eșecurilor retelei, deoarece nu exista o dependinta unica de care sa depinda intreg sistemul.

- Performanta. dVPN-urile pot oferi viteze mai rapide comparativ cu Tor, deoarece traficul nu trebuie neaparat sa treaca prin atat de multe salturi si poate lua rute mai directe intre noduri. Acest lucru este benefic in special pentru activitati care necesita o latime de banda mare, cum ar fi streaming-ul sau descarcarea de fisiere mari.

- Premierea utilizatorilor. Multe dVPN-uri ofera stimulente economice pentru utilizatori pentru a impartasi resursele, ceea ce poate incuraja o participare mai mare si astfel poate creste potential capacitatea si fiabilitatea retelei.

4.3 Care sunt dezavantajele unui dVPN comparativ cu rețeaua Tor?

- Probleme de incredere si securitate. In cazul dVPN-urilor, utilizatorii trebuie uneori sa se bazeze pe increderea in nodurile retelei, care s-ar putea sa nu fie verificate la fel de riguros ca nodurile din reteaua Tor. Aceasta poate ridica probleme de securitate daca nodurile rau intentionate participa la retea. Pentru a putea rezolva aceste probleme dVPN-urile necesita mecanisme de incredere si securitate mai complexe, cum ar fi sistemele de reputatie, ceea ce poate introduce noi vulnerabilități sau dependente.

- Valabilitate si fiabilitate. Din moment ce dVPN-urile depinde foarte puternic de nodurile participante in retea, functionabilitatea acesteia este puternic influentata de numarul de noduri disponibile, distributia lor geografica dar cat si de stabilitatea conexiunii acestor noduri (in unele zone/cazuri reteaua poate fi instabila intr-un areal zonal mare, lucru care duce la un produs nefiabil).

5 Rezultatele unui simplu test practic

Pentru a test latenta, viteza de download, de upload cat si latentele corespondente am accesat speedtest.net utilizand urmatoarele metode de anonimizare: reteaua Tor, un VPN (cel inclus in browser-ul Opera) cat si un dVPN. Pentru I2P trebuie gandit un alt test, intrucat prin I2P pot fi accesate doar noduri din retea si pentru a accesa un site ca speedtest.net ar fi nevoie de un outproxy in reteaua I2P, dar din pacate, din motive de siguranta, acestea sunt inchise le fel de repede pe cat apar. Acest lucru face foarte grea adaugarea in aceasta comparatie si a I2P.

Tehnologie	Ping (ms)	Viteză download (Mbps)	Viteză upload (Mbps)	Latență download (ms)	Latență upload (ms)
Control	4	950	950	11	51
VPN	49	550	170	75	75
TOR	647	1.44	4.35	3392	4650
dVPN	100	350	110	200	120

6 Concluzii

Analiza comparativa a Tor, VPN-urilor, I2P si dVPN-urilor evidentiaza punctele forte si limitarile diverse in securizarea si anonimizarea traficului online. Tor ramane neegalat pentru anonimizarea accesului la internetul mai larg, in ciuda problemelor sale de latenta si a riscului prezentat, adica de posibilul control asupra mai multor noduri. VPN-urile ofera viteze mai rapide si usurinta in utilizare, fiind potrivite pentru ocolirea restrictiilor geografice de continut, dar depind in mare masura de increderea in furnizorii de VPN. I2P se specializeaza in comunicatii securizate si anonime specifice retelei, dar nu ofera accesibilitate la internetul mai larg. VPN-urile descentralizate (dVPN) introduc o abordare peer-to-peer, crescand potential viteza si rezistenta la cenzura, dar depind de robustetea retelei si mecanismele de incredere intre noduri. Aceste constatari subliniaza necesitatea de a alege tehnologia adecvata in functie de cerintele specifice de securitate, viteza si accesibilitate, deoarece nicio solutie singulara nu se potriveste tuturor contextelor.