PROTEJAREA IDENTITĂȚILOR, PROTEJAREA CONFIDENȚIALITĂȚII: O EXAMINARE A TEHNICILOR UTILIZATE DE REȚELELE ANONIME

Ion STRONCEA

Departamentul Ingineria Software și Automatică, Student programul masterat, grupa TI-231M, Facultatea Calculatoare Informatică și Microelectronică, Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Autorul corespondent: Ion STRONCEA, e-mail: ion.stroncea@isa.utm.md

Îndrumătorul/coordonatorul științific **Cristina BODOGA**, asistentă universitară,
Universitatea Tehnică a Moldovei, Chișinău, Republica Moldova

Rezumat. *VPN-urile sunt prima etapă în protejarea identității online a utilizatorilor, servind ca un intermediar între client și serviciul accesat. Atunci când atacatorii încearcă să intercepteze traficul, aceștia nu pot face legătura directă între client și serviciu.*
Există două tipuri principale de tehnici pentru protejarea identității: manipularea pachetelor și rutarea pachetelor. Tehnicile de manipulare a pachetelor includ folosirea pachetelor de mărimi egale și segmentarea lor pentru a confunda atacatorii. Sincronizarea pachetelor, de asemenea, întârzie retransmiterea pachetelor pentru a preveni corelarea timpilor de transmitere.
Tehnicile de rutare a pachetelor se bazează pe metode și arhitecturi precum Onion routing, utilizată în rețele precum Tor, și Garlic routing, utilizată în rețeaua I2P. Aceste tehnici criptează și redirecționează datele prin mai multe noduri, protejând astfel identitatea utilizatorilor și împiedicând atacatorii să identifice conexiunea dintre client și serviciu.

Cuvinte cheie. *VPN, identitate, protejare, pachet, Onion routing, Garlic routing, tunel*

Introducere

În prezent tehnicile și protocoalele utilizate în internet oferă o securitate înaltă a conținutului mesajelor transmise. Exemplu este protocolul HTTPS, TLS etc. Dar pe cât de protejat este conținutul mesajului, pe atât de neprotejate sunt datele referitoare a actorilor care participă în comunicare. Acesta înseamnă că oricine captează pachetul, din cauza structurii la nivelul trei, nivelul de rețea al modelului OSI al internetului, acesta poate spune exact și fără greutăți cine sunt membrii comunicării, sursa și destinația. O dată cunoscând adresa IP a persoanei, un atacator poate afla data ca: adresa acestuia, numele persoanei, date confidențiale. Cunoașterea acestor data pun în pericol persoana. Din această cauză protejarea identității este un aspect important în securitatea pe internet.

În această lucrare vor fi studiate tehnicile pentru protejarea identității , utilizate de către rețelele anonime.

VPN

Prima etapă în protejarea identității este utilizarea VPN-urile. Modalitatea prin care VPN-urile protejează identitatea este faptul că servesc ca un punct intermediar între client și serviciul accesat, astfel că la captarea pachetului de către un răufăcător acesta va putea doar înțelege că pachetul merge de la utilizator la VPN server sau de la VPN server la serviciu, dar nu va putea face legătura directă între client și serviciu, Fig. 1.

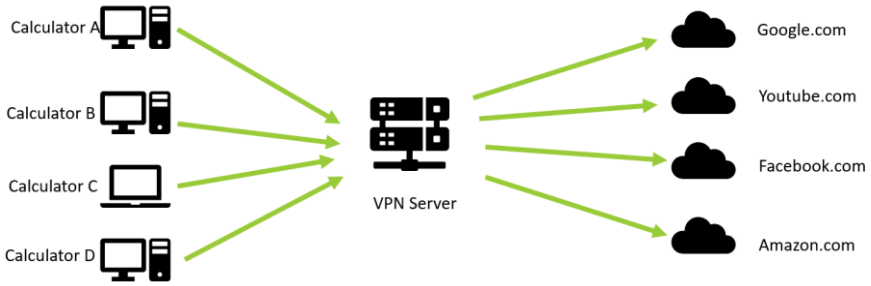

Figura 1. Exemplu de utilizare a VPN-urilor

Tehnici de protejarea anonimității

Restul tehnicilor utilizate vor fi divizate în două grupe: tehnici de manipularea pachetelor și tehnici de rutarea pachetelor.

Tehnicile de manipularea pachetelor reprezintă tehnicile care au ca scop protejarea identității prin manipulări cu mărimile pachetelor și a timpului de retransmitere a acestora.

Aceste tehnici includ:

- Pachete de mărimi egale
- Segmentarea pachetelor
- Retransmiterea sincronă

Problemă pachetelor de mărimi aleatoare

Chiar și utilizând VPN-urile pentru a proteja identitatea, un atacator poate utiliza metode de restabili conexiunea pierdută dintre pachetele de până la intrarea în VPN și cele de la ieșire.

Una din metode este după mărimea pachetelor. Astfel un atacator captând pachetele de până la un VPN și cele la ieșirea din VPN, ordonându-le după mărime pe cele de la intrare și cele de la ieșire poate presupune care din pachetele de până la VPN sunt acele de după VPN, astfel restabilind conexiunea dintre client și serviciul accesat, Fig. 2.

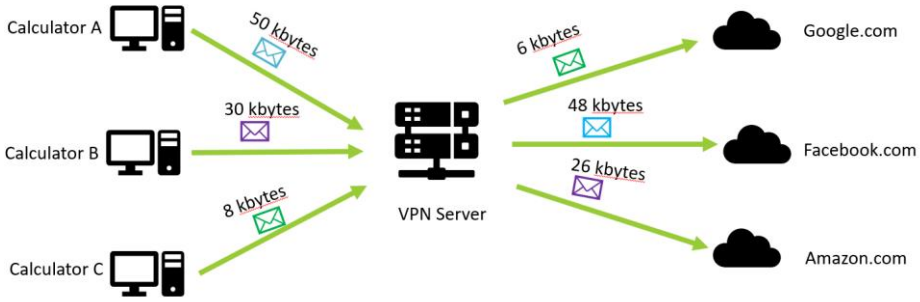

Figura 2. Exemplu de problema pachetelor de mărimi aleatoare

Una din metodele de a combate această problemă este utilizarea pachetelor de mărime exactă. Această metodă presupune că în loc de folosirea pachetelor de mărimilor aleatoare folosirea pachetelor de mărimi prestabilite, egale.

Aceasta poate fi pus ca regulă la nivel de rețea astfel că pachetele de la clienți la VPN server vor trebuie să aibă de la început mărimea necesară, iar pachetele necorespunzătoarea vor fi omise de VPN server.

Altfel această metodă poate fi implementată la nivel doar de VPN server. Astfel clienții transmit pachete de mărimi aleatoare iar serverul le transformă în pachete de mărimi egale mărindu-le pe cele care au fost de mărimi mai mici.

În rezultat un atacator nu va putea recrea conexiunea între client și serviciu accesat bazându-se pe mărimea pachetelor, Fig. 3.

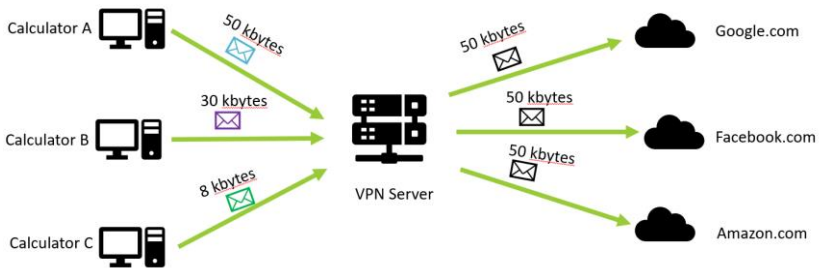

Figura 3. Exemplu utilizare a pachetelor de mărimi egale

Încă o metodă de a combate problema pachetelor de mărimi aleatorii este segmentarea pachetelor. Această metodă presupune că clienții transmit pachetele în mod obișnuit către VPN server, iar acesta le segmentează în pachete mai mici și doar după aceasta le retransmite. În rezultat un atacator obține la ieșire mai mute pachetele de mărimi mai mici decât cele de la intrare, ceea ce îi îngreunează procesul de restabilire a conexiunii, Fig. 4.

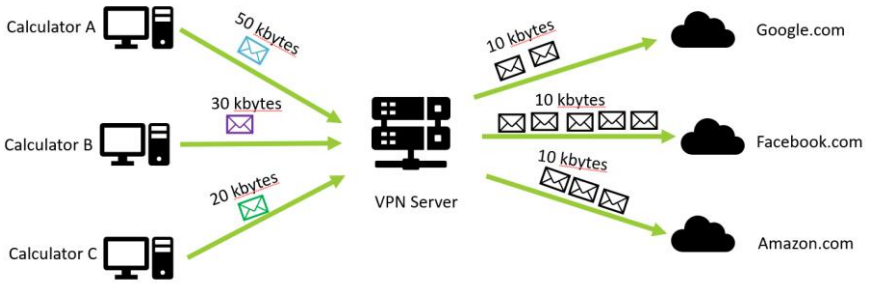

Figura 4. Exemplu de utilizare a segmentării pachetelor

Sincronizarea pachetelor

O altă metodă prin care un atacator poate restabili conexiunea dintre client și serviciu este prin timpul de retransmisiunea a pachetelor de către serverul VPN.

În mod normal un VPN server este orientat să retransmită pachetele cât mai rapid posibil, fapt de care se pot folosi atacatorii. Un atacator poate capta pachetele de la intrare și ieșire pe o perioadă de timp, apoi să le sorteze după timpul când acestea au fost captate și datorită faptului că într-un VPN server primul pachet recepționat va fi și primul retransmis, să restabilească conexiunea dintre client și server, Fig. 5.

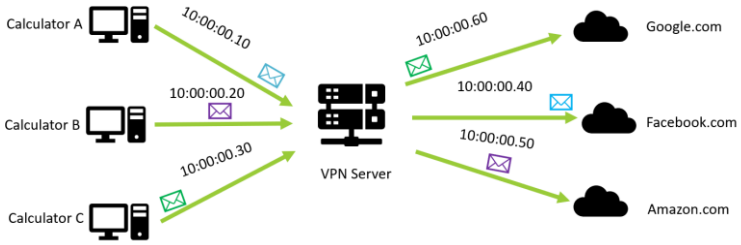

Figura 5. Exemplu problemei a retransmiterii pachetelor în mod asincron

Pentru a proteja față de un astfel de atac este utilizată metoda de sincronizare a pachetelor. Astfel VPN serverul recepționează pachetele, le prelucrează dar nu le transmite mai departe deodată. Acesta așteaptă o perioadă, fie după numărul de pachete, fie după o durată de timp prestabilită, și după le transmite pe toate odată. Astfel un atacator la ieșire obține simultan multe pachete și nu poate restabili conexiunea bazându-se pe timpul pachetelor, Fig. 6.

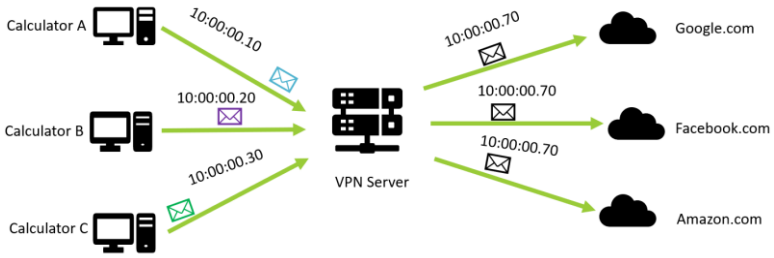

Figura 6. Exemplu a retransmiterii pachetelor în mod sincron

Tehnici de rutarea pachetelor

Tehnicile de rutarea pachetelor sunt tehnicile de protejarea identității care utilizează la bază diferite metode și arhitecturi ce țin de rutarea pachetelor, în loc de manipulări asupra acestora. Se vor analiza tehnicile utilizate de rețelele anonimi existente ca TOR și I2P.

Onion routing

Onion routing (sau rutarea în straturi de tip ceapă) este o tehnică de anonimizare a traficului de date utilizată în rețele precum Tor (The Onion Router). Această metodă este concepută pentru a ascunde identitatea expeditorului și a destinatarului mesajelor, precum și conținutul lor, prin criptarea și redirecționarea datelor printr-o serie de noduri intermediare [1].

Onion routing – Rețea

Utilizarea VPN-urilor ca metodă de protejarea a identității fiind una din cele mai simple și efective a adus la ideea de utilizarea nu a unui server VPN, ci a mai multor, unuia după altuia. Astfel în rețeaua Onion avem o rețea creată doar din noduri care lucrează în esență fiecare ca un VPN server.

Astfel un tunel dintre client și serviciul accesat constă din minim trei noduri. Nodul de intrare reprezintă nodul prin care pachetele clientului intră în rețeaua Onion. Nodurile intermediare sunt nodurile prin care pachetele circulă în interiorul rețelei. Este necesar de minim un nod intermediar. Nodul de ieșire este nodul în care pachetele ies din rețeaua Onion și pleacă la serviciu. În rețeaua Onion același tunel este utilizat atât pentru cerere atât și pentru răspuns [1], Fig. 7.

Toate aceste măsuri fac ca un atacator poate spune doar că clientul a trimis pachete în rețeaua Onion și că careva pachete au venit la serviciu din rețeaua Onion, dar fac extraordinar de greu găsirea drumului în interiorul rețelei, din această cauză atacatorul nu poate restabili conexiunea dintre client și serviciu și astfel rămâne protejată identitatea utilizatorului [1], Fig. 8.

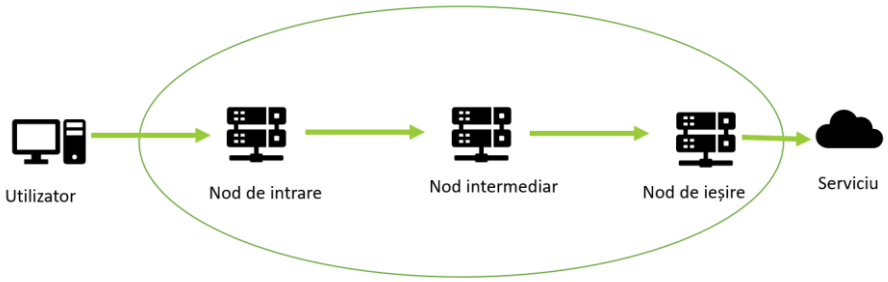

Figura 7. Schiță a tunelului în rețeaua Onion

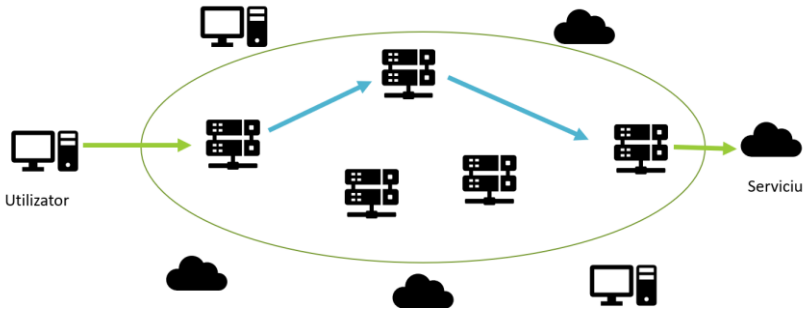

Figura 8. Schiță a rețelei Onion și drumului imposibil de recunoscut din exterior

Onion routing – criptarea pe straturi

Principala metodă care protejează identitatea în rețeaua Onion, chiar și dacă unele noduri sunt conpromise, este criptarea pe straturi, criptarea ceapă. Ea constă că pachetul inițial este criptat de mai multe ori cu cheile publice a nodurilor prin care se preconizează să treacă pachetul, de la sfârșit spre început. Când pachetul ajunge la nod, acesta îl decriptează, și cunoaște doar unde trebuie să retransmită pachetul și de unde a venit însă nu tot drumul. Acest fapt protejează identitatea chiar și prin coruperea cărorva din noduri. Din cauza că niciun nod nu știe tot drumul, atacatorii nu pot restabili conexiunea dintre client și server.

Garlic routing

"Garlic routing" este o metodă de anonimizare a traficului de date și de îmbunătățire a securității în rețea, specifică rețelei de anonimizare I2P (Invisible Internet Project).

Garlic routing – tunele separate

În rutarea Garlic, creatorii au creat că fiecare client are nevoie de minim două tunele pentru comunicare, unul de intrare, altul de ieșire (Fig. 9) [2]. Astfel pentru ca două calculatoare să comunice, este nevoie de patru tuneluri, câte două pentru fiecare calculator. Două de intrare și două de ieșire [3].

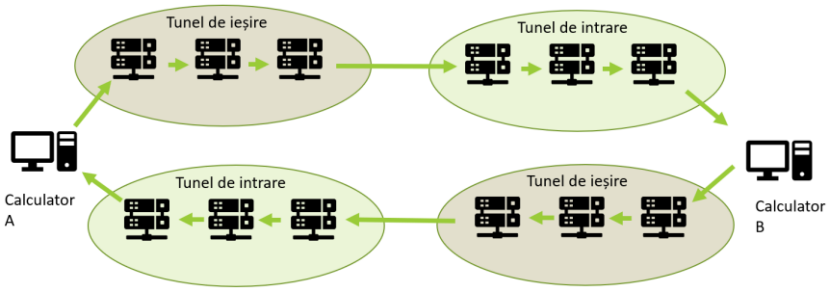

Figura 9. Exemplu de comunicare între două calculatoare în garlic routing

Garlic routing – gruparea pachetelor

Principala metodă a rutării Garlic este gruparea pachetelor pentru transmitea în interiorul unui tunel.

Un tunel constă din 3 tipuri de noduri, poartă, participant și punct final [3].

Poarta captează pachetele un timp anumit, le unește într-un pachet mare, le criptează împreună exact ca și în rutarea Onion și le transmite prin tunel.

Participantul are drept scop simpla retransmitere a pachetelor mai departe prin tunel. Ele pot mai multe la număr în interiorul tunelului, dar minim unul.

Punctul final decriptează pachetul mare, le decuplează și după retransmite fiecare pachet separat.

Denumirea de Garlic – usturoi, provine însăși de la gruparea pachetelor – cățeilor – clove într-un usturoi mare – bulb, Fig. 10.

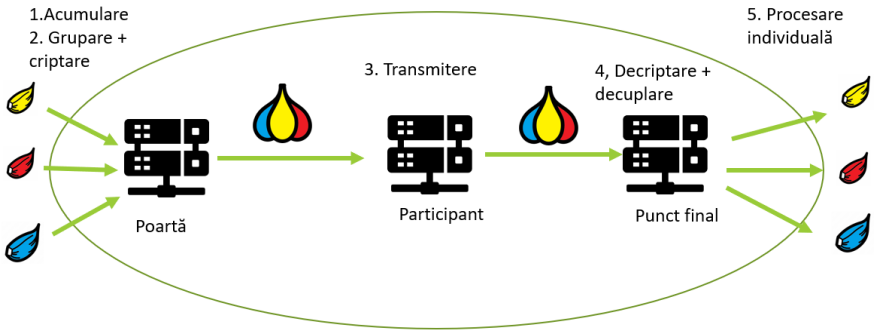

Figura 10. Procesul de transmitere a datelor în tunelul I2P

Concluzii

Tehnicile și protocoalele actuale utilizate pe internet oferă un nivel înalt de securitate pentru conținutul mesajelor transmise, însă, în ceea ce privește datele referitoare la identitatea actorilor implicați în comunicare, acestea pot fi expuse riscurilor. Este esențial să se pună un accent pe protejarea identității în comunicarea online pentru a preveni potențialele atacuri cibernetice care ar putea pune în pericol datele confidențiale ale utilizatorilor.

Utilizarea VPN-urilor este o etapă inițială eficientă pentru protejarea identității, deoarece servește ca un punct intermediar între client și serviciul accesat, ascunzând astfel legătura directă între aceștia. Totuși, pentru a combate riscurile asociate cu pachetele de mărimi aleatorii și timpii de retransmisie, trebuie implementate tehnici de manipulare și rutare a pachetelor.

Metode precum pachetele de mărimi egale, segmentarea pachetelor și sincronizarea pachetelor ajută la contracararea reconstrucției conexiunilor între client și serviciu. În ceea ce privește tehnicile de rutare a pachetelor, soluțiile de rețele anonime precum TOR și I2P, care utilizează tehnici precum Onion Routing și Garlic Routing, oferă mecanisme avansate pentru anonimizarea și protejarea identității utilizatorilor.

Astfel, pentru a obține o protecție adecvată a identității în mediul online, este crucial să se combine tehnici multiple de manipulare și rutare a pachetelor, însoțite de utilizarea rețelelor anonime. Aceasta oferă utilizatorilor un nivel mai mare de siguranță și confidențialitate în timpul comunicării pe internet, asigurându-se că datele lor sunt mai bine protejate împotriva atacatorilor și a altor amenințări cibernetice.

Referințe

[1] „Onion Routing” [Online] Available: https://www.geeksforgeeks.org/onion-routing/
[2] „Tunnel Operation (Message Processing)" Terminology” [Online] Available: https://geti2p.net/en/docs/tunnels/implementation
[3] [„Garlic Routing and "Garlic" Terminology” [Online] Available: https://geti2p.net/en/docs/how/garlic-routing
[4] „"Garlic" Methods in I2P” [Online] Available: https://geti2p.net/en/docs/how/garlic-routing