Universitatea Politehnica București

Facultatea de Electronică, Telecomunicații și Tehnologia Informației

VPN (Virtual Private Network)

**Tudor Ioana** Coordonator științific: **Popa Marius** Conf. Dr. Ing. **Ștefan Stăncescu**

Grupa: 441A

**2016**

Cuprins

1. Prezentare generală a rețelelor virtuale – Popa Marius
2. Securitatea VPN-urilor – Tudor Ioana, Popa Marius
3. Algoritmi de criptare – Tudor Ioana
4. Aplicații VPN– Popa Marius
5. Principiul de funcționare al aplicației LogMeInHamachi – Tudor Ioana
6. Principalele probleme ale aplicației LogMeIn Hamachi – Tudor Ioana
7. Bibliografie
8. Prezentare generală a rețelelor virtuale

O rețea privată virtuală extinde o rețea privată peste o rețea publică. Aceasta folosește aceleași politici de securitate și performanță ca și cele dintr-o rețea publică. Permite unui calculator să acceseze datele din reteaua privată peste alte retele publice ca și cum ar fi conectat la aceasta și beneficiind de securitatea și politicile rețelei publice. Conexiunile VPN sunt o alternativă de cost redus pentru rețelele WAN private. Aceastea sunt ușor de implementat. VPN-urile transmit datele prin “tunelare”. Înainte ca un pachet sa fie transmis, acesta este încapsulat într-un pachet nou și cu un alt header. Acest header asigură informațiile de rutare necesare pentru ca pachetul să traverseze rețelele publice până ajunge la destinație. Acest drum parcurs este cunoscut sub numele de tunel. Când pachetul ajunge la sfârșitul tunelului, este decapsulat și trimis mai departe către destinația finală.

Utilizarea VPN-ului se poate realiza în următoarele moduri:

* Acces VPN - permite ca utilizatorul să se conecteze de la distanță (de acasă, de pe telefonul mobil) la sediul firmei. Această metodă utilizează conexiuni securizate, criptate.
* Intranet VPN - permite conectarea între sedii folosind legături dedicate, fixe
* Extranet VPN - utilizat pentru stabilirea legaturii dintre clienți și sediul firmei folosind linii dedicate
* Substituent pentru WAN (Wide Area Network) – în cazul în care VPN oferă o alternativă mai buna. VPN-ul necesită o cheltuială redusă în comparație cu WAN. De asemenea, oferă o scalabilitate mai mare, dar, totuși, performanțele pot fi mai scăzute din cauza problemelor ce pot aparea prin tunelare.

**Remote Access VPN (Acces de la distanţă)**

Accesul la distanță se poate realiza prin doua tipuri: **conexiune iniţiată de client** şi **conexiune iniţiată de server**.

1. **Conexiune iniţiată de client** . Aceasta se realizează prin intermediul unui soft instalat pe calculatorul clientului, care asigură criptarea datelor ce se transmit către sediul ISP-ului. Datele sunt transmise către sediul firmei tot criptate, deci întregul circuit al informaţiei se realizează în mod criptat. De asemenea, și în acest caz sunt utilizați o mulțime de clienți VPN (de exemplu Cisco Secure VPN). În schema urmatoare este reprezentat acest tip de Access VPN :

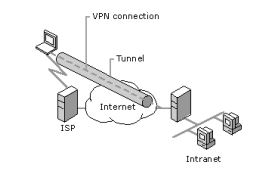


Fig. 1 – Schema conexiunii

1. **Access VPN iniţiat de serverul de acces**

Acest tip de acces nu necesită utilizarea unui client de VPN. În acest caz, spre deosebire de cel precedent, criptarea se realizează doar pe porțiunea dintre server-ul de acces al ISP-ului și serverul firmei, în timp ce securitatea între client și server-ul de acces este asigurată de liniile telefonice (poate reprezenta un dezavantaj).

**Avantajele utilizarii unui VPN:**

1. **Securitate sporită:** atunci când se realizează o conexiune la o rețea prin intermediul unui VPN, datele transmise sunt securizate și criptate. În acest mod informațiile sunt ferite de eventualele atacuri.
2. **Distribuire de fișiere:** Un serviciu VPN poate fi utilizat dacă într-un grup e nevoie să fie distribuite fișiere în mod sigur pentru o perioadă lungă de timp.
3. **Anonimitate online:** Prin intermediul VPN-ului se pot accesa paginile web în completă anonimitate. În comparație cu software-urile de ascundere a adreselor IP, VPN-ul permite accesul atât a aplicațiilor web, cât și a site-urilor, fără a putea fi detectată identitatea.
4. **Schimbarea adresei ip:** dacă se dorește obținerea unei adrese IP dintr-o alta țară, atunci cu VPN se poate rezolva această problemă
5. **Performanțe mai bune:** Lațimea de bandă și eficiența rețelei pot crește, odata ce este implementata o soluție VPN
6. **Scalabilitate:** VPN-urile sunt flexibile în ceea ce privește dezvoltarea unei companii și adaugarea unor utilizatori noi în rețea, fără a fi necesar să se adauge componente noi pentru a face fața creșterii.
7. **Reducerea costurilor:** VPN-urile sunt mult mei ieftine decat retelele private ale companiilor, in special prin costurile de operare (echipamente, administratori).

**Dezavantajele utilizarii unui VPN:**

1. Implementarea acesteia poate fi complexa. Acest lucru înseamna că este necesar un profesionist de nivel înalt care să înțeleagă foarte bine protocoalele de comunicație și configurările rețelelor și eventualele probleme de securitate ce pot apărea.
2. Dacă este necesară dezvoltatea infrastructurii, acest lucru poate produce probleme, în sensul că solutiile noi pot fi incompatibile dacă se utilizeaza un alt furnizor.
3. Complexitatea configurarii poate crește dacă se dorește și posibilitatea conectarii de pe telefoanele mobile, pentru că poate influența securitatea, mai ales dacă conexiunea este una wireless.
4. **SECURITATEA VPN-urilor**

Conceptul de bază al mecanismelor de securitate aplicate VPN-urilor constă în permisiunea accesului doar utilizatorilor autentificați și utilizarea tehnicilor de criptare. Criptarea datelor face imposibilă citirea acestora de către utilizatorii neaturozitați și presupune cunoașterea regulilor folosite la transformarea mesajului original, atât de către emițător cât și de receptor. Toate tehnicile de criptare VPN presupun utilizarea unui algoritm și a unei chei. Algoritmul este o funcție matematică care combină un mesaj cu o cheie, gradul de securitate al acestuia fiind direct proporțional cu lungimea cheii.

Tehnicile de autentificare și de criptare alese formează o asociație de securitate (SA – Security Association). Asociația de securitate reprezintă defapt o relație unidirecționață între sursă și destinație care asigură servicii de securitate traficului căruia îi este atribuită.

Protocolul AH (Authentication Header) este un protocol de încapsulare ce furnizează autentificarea originii datelor, integritatea lor și protecția la redare însă nu oferă confidențialitate. Prin urmare, datele sunt trimise transparent și pot fi ușor interceptate. Protocolul ESP (Encapsulation Security Payload) furnizează confidențialitatea datelor și opțional funcțiunile protocolului AH. VPN permite combinarea acestor două protocoale configurate în modul transport, în cazul conexiunilor gazdă-la-gazdă.

Fiecare SA are drept identificatori un număr aleator denumit identificator de securitate (SPI – Security Parameter Index), o adresă IP de destinație și un protocol de securitate (AH sau ESP). SPI constă într-un și de biți inclus în header-ul AH/ESP ce permite destinației să selecteze asociația de securitate potrivită pentru procesarea pachetului primit. Adresa IP de destinație este adresa nodului care primește pachetul, acest nod putând fi un calculator sau un echipament de comunicație (router,firewall, access point). Identificatorul protocolului de securitate specifică dacă SA lucrează pentru AH sau pentru ESP.

Fiecare nivel al modelului OSI dispune de anumite protocoale de de securizare. De exemplu:

* Nivelul legăturii de date: L2TP (Layer2 Tunelling Protocol) care deși este definit pe acest nivel operează pe nivelul sesiune
* Nivelul rețea: IPSec (IP Security) oferă servicii de autentificare, de control al accesului și de confidențialitate și integritate a datelor
* Nivelul transport: TLS (Transport Layer Security), SSL (Security Socket Layer)
* Nivelul aplicație: SSH (Security Shell), PGP (Pretty Good Privacy)

**Protocoalele de securitate** pentru VPN-uri stabilesc modul în care sunt utilizate serviciile de securitate și cum functionează pe diferite nivele ale modelului OSI. Acestea utilizează criptarea ca metodă de asigurare a confidențialitații datelor. Din momentul în care este instalat VPN-ul, acesta se asigură că pachetele ce sunt transmise prin tunel sunt indescifrabile fără cheile de decriptare corespunzătoare, deci datele nu pot fi modificate pe parcursul transmisiunii în cazul în care se încearcă interceptarea lor. O altă metodă de securitate a VPN-urilor este de a verifica integritatea datelor. Acesta se rezumă de obicei la un mesaj transmis care asigură că datele au ajuns cu succes și nu au fost modificate pe parcursul transmisiunii.

**IPsec**

Pe nivelul de rețea este întâlnit protocolul **IPsec** **(Internet Protocol Security Facility).** Acesta a fost creat de IEFT (Internet Engineering Task Force) pentru a securiza transferul, pe nivelul trei al modelului OSI, prin rețele neprotejate, cum ar fi Internetul. Prin intermediul acestuia se realizează autentificările și criptările pachetelor IP. Arhitectura acestui protocol este compatibilă atât cu stiva IPv4, cât și cu stiva IPv6. IPsec este utilizat pentru a realiza securitatea comunicațiilor între două sau mai multe calculatoare, între subrețele și între calculatoare independete și subrețele. Serviciile oferite de acest protocol sunt:

* integritatea conexiunii (oferă o permanentă protecție împotriva eventualelor dispozitive neautorizate ce încearcă să se conecteze la rețeaua respectivă),
* verificarea sursei (se asigură autenticitatea mesajelor),
* criptări de date (mesajele sunt transmise într-o formă ce nu poate fi interpretată decât de calculatorul destinație
* protecția în cazul atacurilor (un exemplu ar fi pachetele care se transmit fără o ordine anume, la infinit prin retea si pot crea blocaje).

IPsec permite sistemelor să negocieze protocoalele de securitate, algoritmii și cheile secrete ce urmează a fi folosite. Se folosește, la randul său, de alte două protocoale de securitate:

* AH (Authentication header) – este un protocol ce verifică autentificatea sursei și integritatea pachelor transmise, dar nu conține niciun modul de criptare. Headerul acestui protocol conține date, secvențe numerice și alte informații pentru a se putea verifica expeditorul, asigură integritatea datelor și prevenirea atacurilor.
* ESP (Encapsulated Security Payload) – spre deosebire de AH, acesta utilizează algoritmi de criptare a datelor, cum ar fi 3DES, pentru a asigura confidențialitatea acestora. Tutusi, de-a lungul timpului, s-a demonstrat că acest algoritm nu este printre cei mai eficienți.

Ipsec suportă doua tipuri de chei folosite pentru securitate:

1. Automate – Protocolul de bază utilizat de IPsec pentru a negocia protocoalele, algoritmii și cheile este IKE (Internet Key Exchange). Pe tunelul dintre cele două entitați (expeditor si destinatar), se negociază o asociere de securitate (SA). Utilizatorii se autentifică, semnând astfel datele utilizandu-și cheia, iar când acestea ajung la destinație, acea semnatură este verificată. Versiunea a doua pentru acest protocol, IKEv2, pe langă toate functionalitațile oferite de prima varianta, suportă și NAT (Network Address Translation) și asigură o flexibilitate mărită.
2. Manuale – SA (asocierile de securitate) și cheile secrete sunt configurate manual în ambele capete ale conexiunii, inainte să se înceapă comunicarea și transmisia datelor. Acestea sunt cunoscute doar de expeditor și de destinatar, pentru a se evita decriptarea lor în cazul unor atacuri în timpul transmisiunii.

IPSec reprezintă o suită de protocoale care asigură confidențialitatea și integritatea pachetelor IP transmise printr-un tunel VPN folosind funcții matematice și algoritmi de criptare pentru autentificare. Securizarea transmisiei se realizează la ambele capete ale căii de comunicație implementându-se IPSec pe cele două echipamente pereche. IPSec oferă următoarele servicii de securitate:

* Integritatea conexiunii – asigură faptul că în timpul comunicării dintre două dispozitive nu interv entități neautorizate care să modifice datele sau să transmită mesaje false
* Autentificarea sursei de date – permite identificarea sursei și asigură autenticitatea mesajelor
* Criptarea datelor – asigură confidențialitatea mesajelor transmise și imposibilitatea preluării neautorizate a acestora
* Protecția împotriva atacurilor la rețea – detectează pachete repetitive sau clonele unui pachet care se transmit la infinit în rețea producând blocaje

Entitățile IPSec utilizează identificatorul SPI al asociației de securitate și adresa IP de destinație a pachetului ce urmează a fi supus procesului de criptare sau autentificare pentru a știi oricând ce transformare trebuie aplicată unui pachet astfel încât acesta să poată fi decriptat la receptor și corect interpretat.

IPSec poate fi împărțit în două categorii, în funcție de tipul entității pe care este implementat:

* Site-to-Site – cele două entități se comportă ca un gateway, criptând și decriptând traficul destinat subrețelor aflate în administrarea lor
* Remote-Access – entitățile reprezintă gateway-uri ce au în administrare o subrețea și un calculator care dorește să acceseze acea rețea.

Pentru a se autentifica și pentru a negocia parametrii asocierii de securitate, entitățile utilizează un protocol propriu IPSec deumit IKE (Internet Key Exchange) ce are mai multe moduri de a realiza autentificarea:

* PSK (Pre-Shared Key) – fiecare entitate are preconfigurată o cheie secretă sau o parolă. În momentul în care se realizează negocierea IKE, entitatea trimite această cheie pe rețea pentru a fi verificată de entitatea destinație. Cele două entități trebuie sa aibe definită aceeași parolă.
* PKI (Public Key Infrastructure) – fiecare entitate are un certificat digital pe care îl trimite către destinație pentru a fi verificat și verifică la rândul ei certificatul digital al destinației.
* EAP (Extensible Authentication Protocol)

Deși IPSec permite o gamă largă de configurații, unele dintre acestea prezintă vulnerabilități ce pot fi exploatatede atacatori. Una dintre aceste configurații presupune utilizarea protocolului ESP în modul de funcționare tunel cu opțiunea confidentiality only sau opțiunea integrity protection oferită de AH. Folosind această vulnerabilitate atacatorii care pot intercepta pachetele IPSec și ICMP dintre două entități pot lansa atacuri de tip Destination Address Rewriting, IP Options Modification și Protocol Field Modification, devenind astfel posibilă extragerea datelor. Prin urmare, este recomandat să se utilizeze atât opțiunea confidentiality only cât și opțiunea integrity protection.

**SSL**

Pe nivelul de transport este intâlnit protocolul **SSL VPN (Secure Socket Layer)** care asigură o comunicație securizată între doua aplicații, permițand ca informațiile private, cum ar fi numarul cardului de credit, pin-ul, parole etc. să nu poată fi înțelese. Aceasta permite utilizatorilor să se conecteze la dispozitivele VPN folosind browser-ele web. Pentru a evita ca în eventualitatea în care pe parcursul transmisiunii datele să fie interceptate de către alte instanțe, acest protocol criptează datele pentru a se asigura că nu le și întelege. Astfel, în momentul comunicării, utilizatorul logat știe sigur că datele sale ajung la destinația potrivită și că nu este interceptat și/sau modificat pe parcurs. Pentru criptarea datelor se utilizează două chei de autentificare(una publică și una privată). Complexitatea protocolului rămâne invizibilă pentru utilizatori. Însă, semnul folosit pentru a înstiința utilizatorul că este utilizat protocolul SSL pentru comunicația în curs este un lacat auriu afișat în colțul din dreapta jos al browser-ului utilizat. În cazul versiunilor mai noi, înștiințarea utilizatorului în momentul în care folosesc o conexiune securizată este un chenar verde însoțit de un lacăt, afișat în stanga adresei către care s-a navigat.

Acest protocol utilizează un sistem de criptare bazat pe două chei: una publică și una privată ce este cunoscută numai de destinatarul pachetului. SSL presupune parcurgerea a două etape: Handshake și Transfer. În etapa Handshake entitățile stabilesc un set de algoritmi ce vor fi utilizați pentru realizarea criptării, stabilesc cheile și se autentifică. În a doua etapă, datele sunt împărțite în blocuri de dimensiuni mai mici ce sunt criptate și transmise prin rețea.

Etapa de Handshake presupune parcurgerea următorilor pași:

1. Entitatea1 trimite versiunea SSL utilizată, lista algoritmilor de criptare suportați și un număr generat aleator.
2. Entitatea2 alege algoritmul ce va fi utilizat, trimite un mesaj de confirmare și trimite ulterior certificatul său însoțit de un număr generat aleator.
3. Entitatea1 verifică certificatul primit și dacă este de încredere extrage cheia publică. Apoi criptează o parolă cu ajutorul cheii publice primtie și o trimite entității2.
4. Pe baza parolei și numerelor generate aleator cele două entități stabilesc un set de chei ce vor fi utilizate în criptarea mesajelor.

Pașii efectuati de browser și server-ul destinație pentru a se stabili dacă conexiunea este una validă sunt:

1. Browser-ul se conectează la server securizat cu SSL și îi cere să se identifice.
2. Serverul trimite o copie a certificatului SSL, inclusiv cheia publică utilizată.
3. Browser-ul verifică autenticitatea certificatului. Dacă acesta nu este expirată sau revocată, browser-ul trimite înapoi serverului o cheie de sesiune criptată utilizând cheia publică pe care a primit-o.
4. Serverul decriptează informația primită și trimite înapoi un mesaj de confirmare că se poate începe sesiunea de comunicație.
5. În acest moment, cele doua capete ale comunicației iși transmit date criptate utilizând SSL.

**TLS**

Protocolul TLSeste succesorul protocolului SSL. Acesta, la rândul său, funcționează pe baza a două etape: una dintre ele asigură o conexiune securizată pe baza unei metode de criptare cum ar fi DES (Data Encryption Standard), iar cealaltă (TLS Handshake Protocol) permite clientului și server-ului să se autentifice și să stabilească de comun acord un algoritm de criptare și cheile utilizate. Toate acestea se desfașoară înainte ca comunicația propriu-zisă să înceapă.

Între protocoalele întalnite pe nivelul de aplicație se enumeră SSH (Secure Shell), PGP (Pretty Good Privacy) și S/MINE (Secure Multipurpose Internet Mail Extension).

**SSH**

**SSH (Secure Shell)** este un protocol de rețea din nivelul 7 al stivei OSI care permite autentificarea de la distanță pe o stație în mod securizat. Acesta asigură un canal prin care să se realizeze comunicația între două stații. SSH a fost proiectat ca o alternativă pentru Telnet și pentru alte protocoale nesecurizate, cum ar fi rlogin, rsh etc. Acestea trimit informații, cum ar fi parolele, în “plaintext”, făcându-le astfel predispuse la interceptări și divulgari pe parcursul comunicației. Criptarea utilizată de SSH este menită să aducă un plus de confidențialitate și de siguranță peste rețele nesecurizate, cum ar fi Internetul. Există mai multe metode de a utiliza SSH-ul: una dintre ele este generarea automată de perechi de chei publice-private utilizate pentru conexiune. O altă metodă folosește generarea manuală de chei pentru autentificare, permițand astfel utilizatorilor să se logheze fără a fi nevoie să introducă o parolă. În acest caz, cheia publică se află pe toate calculatoarele care trebuie să permită accesul deținatorului cheii private.

Acest protocol asigură confidențialitatea și integritatea datelor utilizând criptarea cu chei asimetrice. Fiecare entitate deține o pereche de chei: una publică și una privată. Cheia publică este trimisă entității cu care se stabilește legătura VPN iar cea privată rămâne pe stația locală. Stabilirea unei conexiuni SSH presupune parcurgerea următoarelor etape:

1. Cele două entități folosesc protocolul Diffie-Helman pentru a stabili o cheie de sesiune.
2. Entitatea2 criptează o parolă secretă cu ajutorul cheii de sesiunii și trimite rezultatul entității1 alături de cheia sa publică. Dacă entitatea1 nu are cheia publică a entității2 o folosește pe cea trimisă pentru a decripta semnătura autentificând astfel entitatea2. Faptul că entitatea1 utilizează cheia publică a entității2 înainte ca aceasta să fi fost autentificată reprezintă o vulnerabilitate.
3. Entitatea2 autentifică entitatea1 prin aceeași metodă.

După ce a fost stabilită conexiunea, pachetele sunt transmise în modul următor:

1. Se construiește o sumă de control pe baza numărului de ordine al pachetului și a cheii de sesiune.
2. Se formează pachetul din lungimea datelor, datele propriu-zise, suma de control și o completare cu biți aleatori până la un multiplu al lungimii blocului acceptat de algoritmul de criptare.
3. Pachetul se criptează cu cheia de sesiune.

3.Algoritmi de criptare

După cum se observă în capitolul precedent criptarea poate fi fie simetrică fie asimetrică.

**Criptarea simetrică**:

* Necesită o cheie secretă shared pentru a efectua criptare și decriptarea, adică fiecare entitate trebuie să cunoască această cheie
* Fiecare entitate criptează datele înainte de a le trimite în rețea
* Presupune cunoașterea de către administratorul de rețea a entițăților ce urmează să comunice astfel încât să fie configurată aceeași cheie pe amandouă
* Exemple: DES (Data Encryption Standard), 3DES (Triple DES), AES ( Advanced Encryption Standard)

**Criptare asimetrică:**

* Folosește chei diferite pentru criptare și decriptare
* O entitate trimite o cheie publică către orice altă entitate care dorește să comunice
* Transmițătorul folosește o cheie privată combinată cu cheia public a receptorului pentru a cripta mesajul
* Pentru a decripta mesajul receptorul trebuie să folosească cheia sa privată în combinație cu cheia public a transmițătorului
* Exemple: RSA (Rivest, Shamir and Adleman)

În general pentru verificarea integrității datelor se folosesc algoritmi de hashing. Hash-ul reprezintă un număr generat dintr-un șir de text. Pentru a verifica integritatea unui pachet, transmițătorul generează un astfel de hash pe care îl trimite împreună cu mesajul. Receptorul decriptează mesajul și hash-ul și produce un hash propriu din mesajul recepționat pe care îl compară cu cel generat de transmițător. Dacă cele două hash-uri sunt identice atunci se consider că integritatea mesajului nu a fost afectată.

VPN-urile utilizează un cod de autentificare al mesajelor denumit HMAC (Hashed Message Authentication Code) ce are doi parametric: mesajul ce se dorește a fi transmis și o cheie secretă cunoscută doar de entitățile între care se realizează comunicarea. Exemple de astfel de algoritmi: MD5 ( Message Digest 5) , SHA -1 (Secure Hash Algorithm 1).

Protocolul Diffie-Hellman

Descrie o metodă de distribuție a cheilor publice și poartă numele celor doi specialiști care l-au inventat în 1976: Whitfield Diffie și Martin Hellman. Protocolul presupune în prima etapă că fiecare entitate își generază independent o cheie privată. Apoi, fiecare calculează o cheie publică ca o funcție matematică a cheilor private generate anterior. Următorul pas este cel de interschimbare a cheilor publice, iar în final fiecare entitate calculează o funcție a cheii private proprii și a cheii publice a celeilalte entități. Pentru a calcula cheile publice și cheia mesajului este folosită exponențierea în aritmetică modulară.

Atunci când se realizează o configurație pe un echipament există posibilitatea alegerii unui grup Diffie-Hellman care determină cât de puternice sunt cheile folosite. Cu cât numărul de biți al cheii este mai mare cu atât cheia este mai sigură însă necesită mai mult timp pentru a fi generată. Grupurile Diffie-Hellman sunt:

Diffie-Hellman grup 1  -  coeficient pe 768 biți

Diffie-Hellman grup 2  - coeficient pe 1024 biți

Diffie-Hellman grup 5  - coeficient pe 1536 biți

Diffie-Hellman grup 14 - coeficient pe 2048 biți

Diffie-Hellman grup 19 – curbă eliptică pe 256 biți

Diffie-Hellman grup 20 – curbă eliptică pe 384 biți

Diffie-Hellman grup 21 - curbă eliptică pe 521 biți

Diffie-Hellman grup 24 – MODP 2048 – exponențiere modulară cu coeficient pe 2048 de biți și subgrup de numere prime pe 256 de biți

AES

Cunoscut si sub numele de Rjindael, AES este un algoritm de criptare simetrică, pe blocuri, folosit pe scară largă în aplicații. Lungimea blocului și a cheii pot fi independente și pot avea valorile de 128 biți, 192 biți sau 256 biți. Algoritmul standardizează toate cele trei valori posibile pentru lungimea cheii însă restricționează lungimea blocului la 128 biți. Operațiile algoritmului sunt definite sub forma unor operații pe matrici unde atât cheia cât și blocul sunt reprezentate sub formă de matrice.

Acest algoritm a fost dezvoltat ca o îmbunătățire a algoritmilor DES și 3DES din următoarele puncte de vedere:

* Securitate – rezistență mărită la atacurile criptanalitice
* Costuri – eficiență computațională mai mare
* Flexibilitate, simplitate și ușurință de implementare

SHA-1

SHA-1 este un algoritm de hashing dezolvat de NIST (National Institute of Standards and Technology) similar cu MD5, ce produce un hash pe 160 de biți. Acesta implică parcurgerea a 80 de pași ceea ce îl face mai lent decât MD5, însă este mai sigur.

4.Aplicații VPN

1. **OpenVPN (Windows/Mac/Linux, Free)**

OpenVPN este o aplicație software care implementează tehnicile VPN pentru crearea conexiunilor punct la punct securizate în configurații de control la distantă. Utilizeaza un protocol de securitate care foloseste SSL/TSL, care este capabil să treaca prin NAT-uri ( Network Address Translators) și firewall-uri.

Metodele de autentificare suportate de acest software sunt: pe baza cheilor prestabilite, pe baza certificatelor și pe baza numelui de utilizator și a parolei. Cea mai simplă metodă este cea care utilizează cheile. OpenVPN suportă IPv6 ca protocol al rețelei virtuale și are abilitatea de a funcționa peste servere proxy, NAT-uri (Network address translation) și firewall-uri.

În ceea ce privește securitatea, OpenVPN realizează criptare pe 256 de biti, bazat pe un protocol SSL/TLS.

Platformele pe care este disponibil acest software sunt: Linux, Windows, Mac OS X. Este de asemenea disponibil și pe sistemele de operare ale telefoanelor mobile, inclusiv Windows Phone, iOS si Android.



Fig. 2 – Client OpenVPN

Unul dintre avantajele OpenVPN îl reprezintă faptul că este un software open-source, ceea ce înseamnă că se pot crea utilizatori pentru orice fel de platformă și dispozitiv, fără nicio restricție. De asemenea, codul este disponibil gratis pentru modificare în funcție de preferințe. De asemenea, OpenVPN conține și o funcționalitate care permite utilizatorilor să iși creeze propriile module de autentificare. Aceasta înseamnă că se poate alege orice număr de întrebări se dorește a fi adresate la logare, iar pe baza raspunsurilor setate anterior, server-ul să accepte sau să respingă cererea de autentificare.

Unul dintre dezavantajele acestui software este complexitatea crescută, care face ca setarea și configurarea corectă a acestuia să fie mai dificila. O altă problemă ce poate apărea este latența crescută datorată numărului mare de servicii pe care le are în funcțiune acest software în timpul rulării. Altă cauză ar mai putea fi procesele de criptare și decriptare.

1. **LogMeIn Hamachi (Windows/Mac/Linux, Free)**

LogMeIn Hamachi este una dintre cele mai utilizate aplicatii VPN. Acest software VPN stabileste legături directe între două calculatoare ce se pot afla în spatele unor firewall-uri care utilizează NAT-uri fără a necesita reconfigurari. Criptarea datelor comunicate se realizează pe 256 de biți, ca și în cazul OpenVPN.

Platformele pe care este disponibil sunt: Windows, Linux si OS X. De asemenea, se poate instala și pe platformele mobile, cum ar fi iOS și Android.



Fig. 3 – Client LogMeIn Hamachi

În ceea ce privește adresarea, fiecarui client îi este asociat o adresa IP atunci când se logheaza în sistem pentru prima oară. Pentru evitarea conflictelor cu rețelele private existente de partea clientului, adresele private uzuale nu sunt utilizate.

1. ExpressVPN

ExpressVPN este cel mai utilizat software VPN în momentul de fața. Aplicația se instalează ușor, fie că este vorba de calculator, telefon sau tableta. Software-ul deține protecție SSL cu criptare pe 256 de biti, iar în ceea ce privește traficul, lațimea de bandă și viteza sunt nelimitate.



Fig. 4 – client ExpressVPN

5. Principiul de funcționare al aplicației

LogMeIn Hamachi

Această aplicație a fost concepută în așa fel încât sa nu necesite niciun fel de configurare, fiind capabilă să stabilească legături directe între calculatoare protejate de firewall-uri ce utilizează NAT fără a fi nevoie de reconfigurare. Cu alte cuvinte, stabilește o conexiune peste Internet care imită conexiunea dintre două calculatoare situate în aceeași rețea locală. În prezent aplicația este valabilă sub forma unei versiuni de producție pentru Microsoft Windows și OS X precum, a unei versiuni beta pentru Linux și sub forma unui client bazat pe VPN compatibil cu IOS și Android.

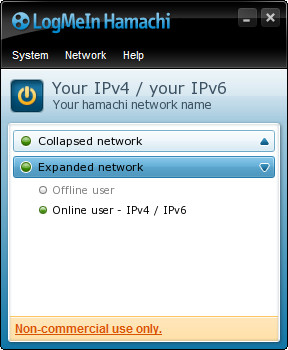
Hamachi este un sistem VPN format dintr-un cluster de servere administrate de un furnizor și utilizate de clientul software care este instalat pe calculatoarele utilizatorilor. Software-ul client adaugă o interfață de rețea virtuală pe un calculator, fiind folosit pentru a intercepta traficul care pleacă precum și traficul VPN care sosește. Traficul outbound trimis de sistemul de operare către interfața de ieșire este preluat de software-ul client care îl criptează și il autentifică, trimițându-l apoi către peer-ul VPN destinație peste o conexiune UDP inițializată special. În prezent Hamachi tratează tunelarea traficului IP, inclusiv al celui de tip broadcast sau multicast. Versiunea pentru Windows poate recunoaște și tunela și traficul IPX.

Fig 5. Interfață LogMeIn Hamachi

Fiecare client inițiază și menține o conexiune de control către cluster-ul de servere. Când conexiunea este stabilită, clientul trebuie să parcurgă o secvență de autentificare, urmată de un proces de descoperire și de sincronizarea stării. Etapa de logare autentifică clientul pentru server și vice versa. Etapa de descoperire este folosită pentru a determina topologia conexiunii la Internet a clientului, mai exact pentru a detecta prezența configurațiilor NAT și a dispozitivelor firewall prezente pe ruta sa către Internet. Etapa de sincronizare are rolul de a armoniza viziunea clientului asupra rețelelor sale private cu ceilalti membri ale acestor rețele.

Când un membru al rețelei devine online sau offline, server-ul le comunică celorlalte peer-uri fie să inițieze fie să dezactiveze tunelele către membrul respectiv. Atunci când se stabilesc tunele între peer-uri Hamachi utilizează o tehnică “NAT traversal” asistată de server ce este similară cu “UDP hole punching”. Acest proces nu funcționează cu anumite combinații de dispositive NAT, fiind necesar ca utilizatorul să activeze redirecționarea porturilor (“port forwarding”).

În cazul în care se pierde brusc conexiunea cu server-ul , clientul păstrează toate tunelele și verifică starea fiecăruia în parte. În cazul in care server-ul pierde brusc conexiunea cu clientul, acesta informează celelalte peer-uri de acest lucru și așteaptă ca fiecare să verifice starea tunelelor. Acest lucru permite ca tunelele Hamachi să reziste problemelor de rețea ce apar pe ruta dintre client și server precum și perioadelor scurte de timp în care server-ele nu sunt disponibile.

Hamachi este utilizat în general pentru crearea rețelelor locale în jocuri sau pentru administrarea de la distanță a dispozitivelor.

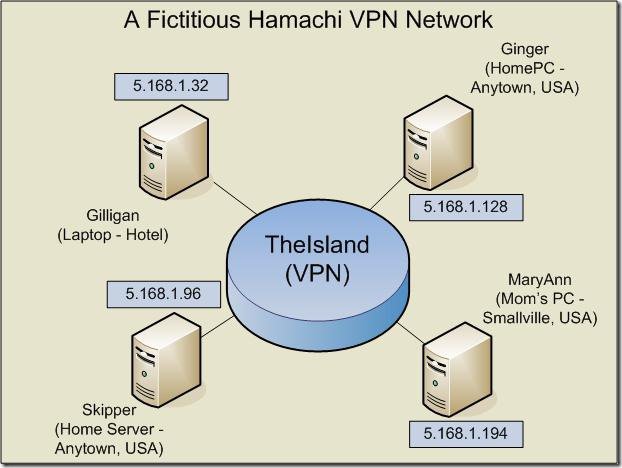


Fig 6. Arhitectură VPN

Modul de adresare

Fiecărui client Hamachi îi este atribuită o adresă IP atunci când se autentifică pe sistem pentru prima oară. Pentru a evita conflictele cu rețelele locale deja existente în partea clientului, blocurile uzuale de adrese IP private 10.0.0.0/8, 172.16.0.0/12 și 192.168.0.0/16 nu sunt folosite. Înainte de 19 Noiembrie 2012 era folosită gama 5.0.0.0/8. Acest bloc era inițial nealocat, însă pe la sfârșitul anului 2010 a fost atribuit lui RIPE NCC, spațiul fiind acum utilizat de furnizorii de servicii de hosting. Prin urmare, Hamachi utilizează acum blocul 25.0.0.0/8.

Adresa IP atribuită clientului Hamachi este asociată așadar cu cheia crypto a acestuia. Atâta timp cât clientul deține cheia, el se poate autentifica pe orice sistem și poate utiliza respectiva adresă IP. Hamachi creează un singur domeniu de broadcast între toți clienții săi. Acest lucru face posibilă utilizarea protocoalelor LAN care se bazează pe mesajele de broadcast pentru servicii de descoperire și anunțare, în rețelele Hamachi.

Arhitectură

Securitatea aplicației este end-to-end. Două noduri Hamachi schimbă informații între ele după autentificare mutuală și potrivirea cheii de sesiune. În timp ce traficul nod către nod (specific VPN), de regulă, evită server-ele LogMeIn și este trimis direct de la un punct la altul, traficul care trebuie transmis prin server este securizat și criptat la sursă și la destinație.

Autentificare

Autentificarea este procesul de verificarea a identității a user-ului și a server-ului. Acest pas are loc la începutul unei conexiuni și are rolul de a se asigura că informațiile sunt schimbate între participanții corecți.

* Autentificarea asigură faptul că identitățile tuturor din rețelele Hamachi, pornind de la server-ele LogMeIn Hamachi și până la nodurile Hamachi sunt verificate.
* Server-ele LogMeIn autentifică nodurile Hamachi utilizând o pereche de chei RSA. Pentru logare, nodul transmite server-ului identificatorul său și cheia privată. Server-ul verifică semnătura și autentifică clientul.
* Nodurile Hamachi autentifică server-ele LogMeIn folosind o pereche de key rsa. Când nodul se conectează la server, anunță ce cheie așteaptă să aibe server-ul. Dacă acesta are cheia cerută, începe secvența de logare.

Criptare

Criptarea este o metodă care amestecă și reface diverse informații astfel încât ele să poată fi transmise în mode securizat de la o locație la alta. Când două entități schimbă informații una cu cealaltă, un protocol de interschimbare de chei are loc în conjunctură cu pasul obligatoriu de autentificare menționat mai sus. Protocolul de schimbare de chei este Diffie-Hellman cu grupul MODP pe 2048 de biți, după cum este definit în RFC 3526.

* O dată ce o sesiune de chei a fost stabilită, este folosit cifrul AES-256-CBC pentru criptarea și decriptarea datelor.
* Pachetele sunt autentificate cu HMAC-SHA-1-96 (RFC 2404)
* Pachetele sunt numerotate pentru a preveni atacurile de reproducere.

Administrare

Fiecare nod LogMeIn Hamachi are opțiuni de administrare ce au rolul de a ajuta la păstrarea securității rețelelor Hamachi. Următoarele facilități sunt valabile pentru rețelele clienților:

* Protecție cu parolă: doar utilizatorii care cunosc parola rețelei pot să facă parte din ea.
* Restricții de rețea: nu permite anumitor utilizatori să facă parte din ea
* Confirmarea apartenenței: nodurile noi trebuie să trimită o cerere de apartanență care trebuie confirmată manual de proprietarul rețelei.
* Interzicerea membrilor: Un nod poate fi dat afară dintr-o rețea sau îi poate fi interzis accesul la respectiva rețea.

6. Principalele probleme ale aplicației

LogMeIn Hamachi

Problemele majore ale acestei aplicații, ca în cazul tuturor aplicațiilor bazate pe VPN, sunt legate de securitate. Prin urmare:

* Există riscul divulgării informațiilor importante care pot fi stocate sau scrise în log-uri de către server-ul de mediere. Acest risc este minimal acolo unde informațiile nu sunt redirecționate.
* Există riscuri datorate seriviciilor vulnerabile de pe dispozitivele situate la distanță, care în mod normal nu ar putea fi accesate întrucât se află în spatele unui firewall.
* Hamachi utilizează algoritmi puternici, de standard industrial pentru a securiza și a autentifica informațiile, însă acest lucru nu garantează 100% securitatea lor.
* Protocolul client-server existent conține erori, unele care au fost confirmate de furnizor și care urmează a fi corectate, altele care nu au fost confirmate.
* Pentru ca produsul să funcționeze, este necesară existența unui server de mediere, administrat de furnizor.
* Acest server de mediere stochează numele user-ului, parola de administrare, adresa IP din blocul 25.0.0.0/8 alocată pentru și token-ul de autentificare asociat. Prin urmare, poate scrie în log-uri adresele IP ale utilizatorilor VPN precum și alte detalii diverse legate de sesiune.

7.Bibliografie

1. https://secure.logmein.com/products/hamachi
2. www.wikipedia.org
3. http://www.techrepublic.com/blog/it-security/hamachi-is-good-news-for-sohos-but-not-so-good-for-the-enterprise/
4. http://lifehacker.com/5487500/five-best-vpn-tools
5. http://web.info.uvt.ro/~cristiana.dragoescu/ANUl%20II/Curs14\_RC.pdf
6. https://ro.wikipedia.org/wiki/Re%C8%9Bea\_privat%C4%83\_virtual%C4%83
7. http://www.windowsecurity.com/articles-tutorials/firewalls\_and\_VPN/VPN-Options.html
8. <https://vpn-services.bestreviews.net/advantages-and-disadvantages-of-openvpn/>
9. <http://www.slashroot.in/secure-shell-how-does-ssh-work>
10. <http://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS>
11. <http://webhost.uoradea.ro/cpopescu/si/Cursul9.pdf>
12. http://jontech.ro/2015/01/protocoale-de-securitate-ssl-tls-si-ssh-2/
13. http://www.agora.ro/stire/ipsec-esp-este-vulnerabil
14. https://itsecure.wordpress.com/2007/09/21/schimbul-de-chei-diffie-hellman/
15. <https://ro.wikipedia.org/wiki/Re%C8%9Bea_privat%C4%83_virtual%C4%83>

Anexă

Fig. 1 - http://web.info.uvt.ro/~cristiana.dragoescu/ANUl%20II/Curs14\_RC.pdf

Fig. 2,3,4 - http://lifehacker.com/5487500/five-best-vpn-tools

Fig. 5 - https://en.wikipedia.org/wiki/LogMeIn\_Hamachi#/media/File:Hamachi\_(software)\_interface\_screenshot.jpg

Fig 6 - http://wmpoweruser.com/wp-content/uploads/2010/02/hamachi\_thumb.jpg