Capitolul 6

Securitatea informatiilor pe Internet

Acest capitol va prezinta cateva aspecte legate de securitatea pe Internet. Vor fi prezentate notiuni de baza, deoarece subiectele sunt foarte vaste si fiecare ar putea fi studiat in detaliu in capitole separate. Vor fi prezentate aspecte legate de :

- firewall-uri: de ce sunt necesare si cum functioneaza
- criptografie: cele doua metode de criptografie secreta si publica, si unde este utilizata criptografia publica in transmiterea sigura a informatiilor
- servere web securizate, necesare in special in comertul electronic, tranzactii bancare online etc.
- semnaturi digitale
- VPN-uri

6.1 Firewall-uri

Termenul "fire wall" (zid de foc) initial avea semnificatia, si inca o are, de zid ignifug ce avea rolul de a preveni extinderea focului dintr-o incapere sau arie a unei cladiri catre restul zonelor. Internetul este un mediu volatil si nesigur din punct de vedere al securitatii calculatoarelor, de aceea "firewall" este un termen foarte bun pentru securitatea retelelor.

Toate firewall-urile, indiferent de tipul lor, au un fapt important in comun: receptioneaza, analizeaza si iau decizii pentru toate pachetele sosite inainte ca acestea sa ajunga in celelalte parti ale retelei interne. Aceasta inseamna ca prelucreaza pachetle si sunt plasate strategic la punctul de intrare al sistemului sau retelei pe care o protejeaza.
Firewall-ul este primul program care receptioneaza si prelucreaza traficul de intrare, si este ultimul care prelucreaza traficul de iesire. Logica este simpla: firewall-ul trebuie situat astfel

incat sa controleze tot traficul de intrare si iesire. Daca un alt program are acest control, nu exista firewall.

O configuratie tipica de firewall este aratata in figura 6.1. DMZ este abrevierea pentru **De-Militarized Zone**, ce este o parte separata a retelei. Nu apartine nici retelei interne si nici nu este conectat direct la Internet. Este locul in care de obicei se afla serverele retelei, ce trebuie sa fie accesibile din Internet cum ar fi serverele web, mail, ftp, DNS, etc. Acestea au adrese IP reale, si firewall-ul permite accesul la servere, in functie de ce servicii ofera acestea.

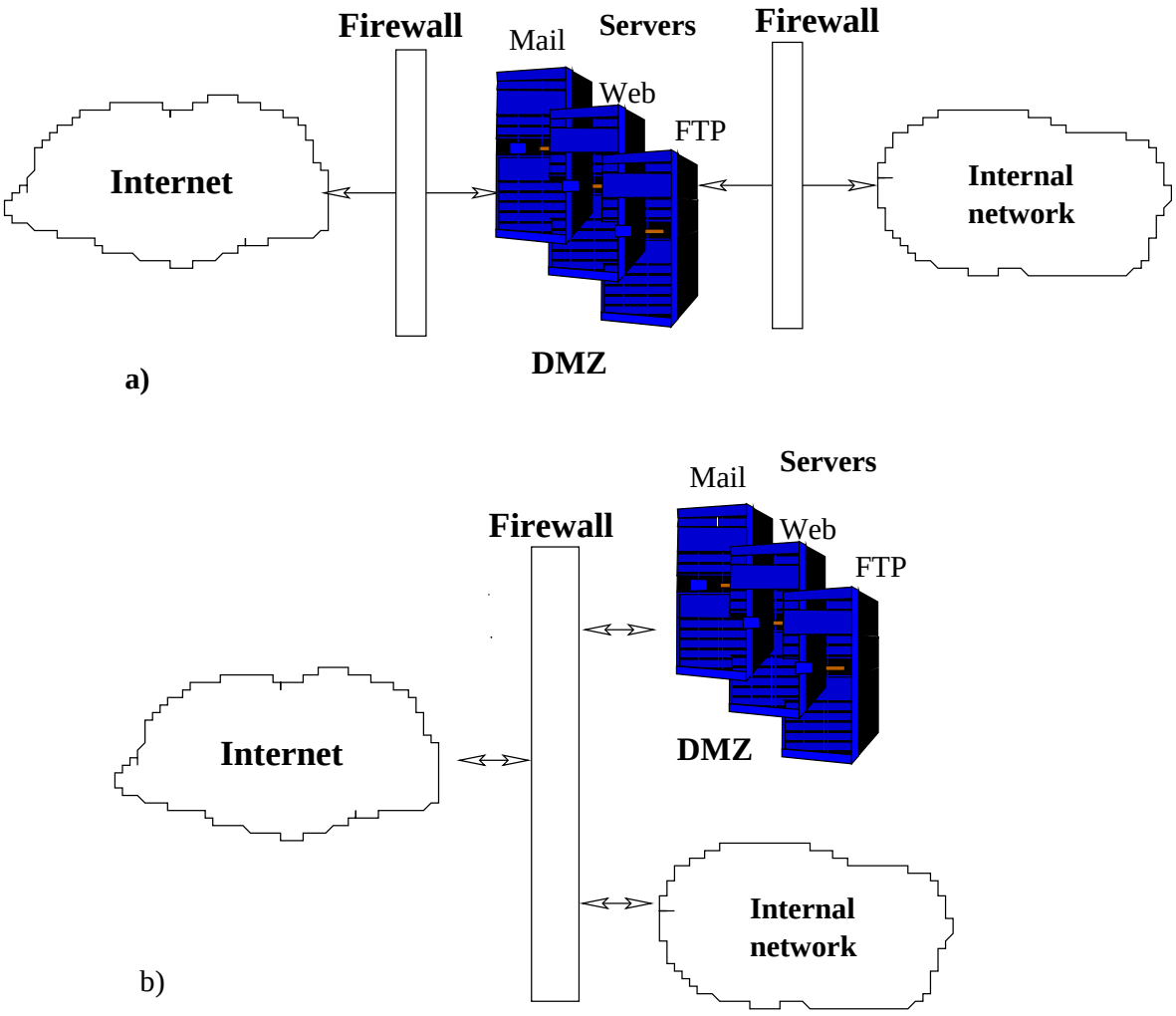

Figura 6.1: Configuratie tipica pentru firewall

In figura 6.1 este indicata o configuratie unde exista un firewall separat (extern) intre zona DMZ si Internet, si un altul pentru reteaua interna privata. Astfel reteaua companiei este protejata de un firewall dublu. In figura 6.1b este un singur firewall ce controleaza traficul catre DMZ si reteaua interna. Acest lucru poate fi facut cu un sistem hardware dedicat (ruter special cu firewall inclus), sau un calculator cu sistem de operare ce ruleaza si un software firewall.

Exista doua tipuri de firewall: la nivel aplicatie (proxy-uri) si la nivel retea (filtrare de pachete).

In cazul unui firewall **proxy**, acesta realizeaza tot schimbul de date cu sistemul de la distanta in "numele" aplicatiilor din reteaua interna. Astfel calculatoarele sunt "vazute" de catre firewall, dar sunt total invizibile pentru sistemele de la distanta. Poate permite sau refuza trafic pe baza unor reguli foarte clare si stricte, de exemplu limitarea accesului la fisiere cu anumita extensie (.mov, .avi) diverse reguli in functie de utilizatorul conectat etc. De asemenea poate fi setat sa porneasca o alarma sau sa notifice un operator cand apar anumite conditii.
Dezavantajul este ca setarea poate fi foarte complexa, necesitand atentie detaliata pentru aplicatiile individuale ce folosesc serverul proxy.

Filtrarea de pachete este tipul cel mai simplu si primul tip de firewall.
Cum s-a explicat in primul capitol tot traficul Internet este transmis in forma de pachete. Un pachet este o cantitate de date de dimensiune limitata pentru a usura prelucrarea lui. Cand sunt transmise cantitati mari de date, acestea sunt impartite in mai multe pachete numerotate care la partea de receptie sunt reasamblate. Tot traficul Internet: fisierele transferate, paginile web, mesajele electronics sunt transmise in pachete.
In principiu un pachet este o serie de numere digitale, ce consta din:

- datele in sine de transmis, confirmarea, cererea de la sistemul sursa
- adresa IP si portul sursa
- adresa IP si portul destinatie
- informatii despre protocolul utilizat (IP, TCP, UDP) prin care este transmis pachetul
- informatie de verificare a erorii

La filtrarea de pachete numai informatia de protocol si adresa este examinata. Continutul si contextul pachetului (relatia fata de alte pachete si aplicatia careia ii este destinata) sunt ignorate. Firewall-ul nu ia in considerare aplicatia de pe host sau din retea careia ii este destinat pachetul si nu "stie" nimic despre sursa (aplicatia) datelor sosite. Filtrarea consta din examinarea pechetelor sosite si/sau trimise, si permiterea sau refuzarea transmiterii acestora pe baza regulilor configurabile, numite **politici de filtrare**.
Regulile filtrelor de pachete pot fi facute pe urmatoarele criterii:

- permite sau refuza pachetul pe baza adresei sursa
- permite sau refuza pachetul pe baza portului destinatie
- permite sau refuza pachetele pe baza protocolului utilizat.

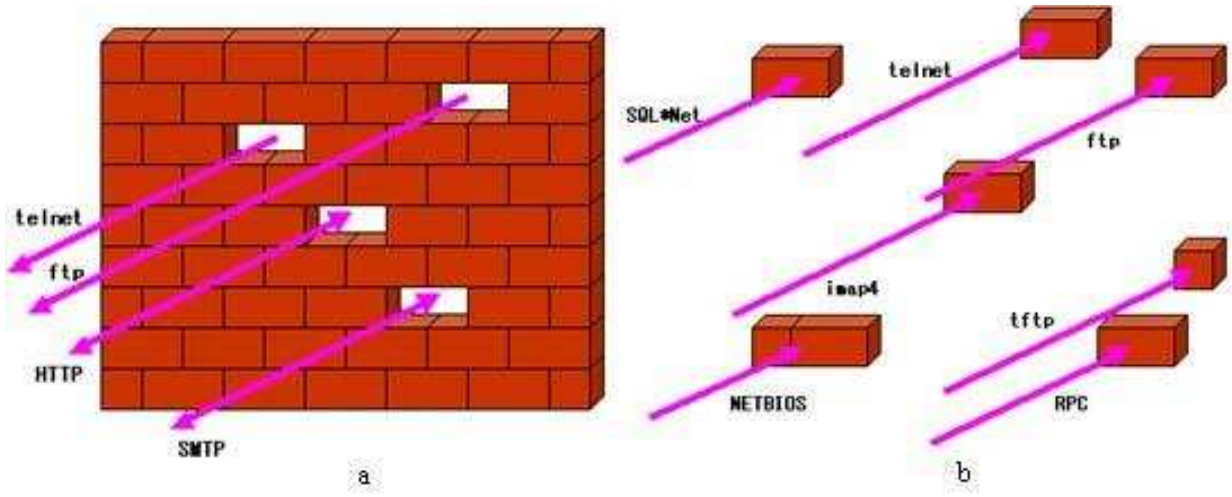

Figura 6.2: Filtrare de pachete pe baza numarului de port

Cum este indicat in figura 6.2, filtrarea este realizata pe baza porturilor sursa si destinatie.

Filtrarea de pachete este foarte eficienta dar nu ofera securitate totala. Poate bloca tot traficul, ceea ce ar insemna securitate absoluta. Dar pentru a avea o retea folositoare, trebuie sa permita accesul unor pachete.
Punctele slabe sunt:

- informatia legata de adresa in cadrul pachetului poate fi falsificata de catre transmitator (atacator)
- data, cererea din pachetul ce a fost acceptat poate in final cauza lucruri nedorite, atacatorul putand exploata un bug cunoscut intr-o aplicatie (de ex, server web), sau sa utilizeze o parola primita pentru a obtine acces pe server.

Avantajul filtrarii de pachete este simplitatea relativa si usurinta implementarii.

6.2 Criptografia

Odata cu dezvoltarea Internetului si aparitia unor aplicatii pe web cum ar fi e-commerce a devenit foarte stringenta problema securitatii datelor transmise prin Internet. Exista multe informatii care se transmit prin acesta retea, ceea ce necesita existenta unei metode de a proteja datele. Cateva exemple de date transmise ce necesita protectie ar fi:

- informatii despre carti de credit
- corespondenta privata sau secreta

- date personale, informatii secrete ale unor companii
- informatii legate de conturi bancare, trimise in timpul unor tranzactii

Cea mai populara metoda de a proteja datele in domeniul calculatoarelor si pe Internet este criptarea datelor, adica procesul de codare a informatiei astfel incat numai cel care detine **cheia** sa poata decripta datele.

Criptografia este folosita de foarte mult timp, de pe vremea cand s-a inceput comunicarea, si oamenii au incercat sa gaseasca metode de a garanta securitatea mesajelor. Armatele romane utilizau cifrul lui Caesar pentru comunicare, ce consta din deplasarea alfabetului cu 3 litere.
In timpul secolului al 19-lea s-au dezvoltat mai multe tehnici de codificare. Kerchoffs a publicat principiile criptografiei moderne. Una din aceste principii afirma ca securitatea unui sistem criptografic nu se bazeaza pe procesul de criptarea, ci pe cheia care este utilizata.

Fiecare sistem de criptare contine 4 parti fundamentale:

- mesajul ce trebuie criptat
- mesajul criptat
- algoritmul de criptare, ce este o functie matematica folosita pentru criptarea unui mesaj
- cheia (sau cheile), ce poate fi un numar, un cuvant sau o fraza ce este utilizat in algoritmul de criptare.

Scopul criptografiei este sa faca imposibila reproducerea textului initial avand textul criptat, fara cheia corepunzatoare.
In criptografie se folosesc 2 metode: cu cheie privata si cu cheie publica.

6.2.1 Criptografia cu cheie privata

In acest caz expeditorul si destinatarul folosesc aceeasi cheie comuna ce trebuie tinuta secreta. Daca o persoana doreste sa transmita date prin aceasta metoda, in prealabil trebuie sa trimita cheia secreta destinatarului, proces numit distributia cheii, pentru ca acesta sa poata interpreta datele primite de la expeditor.
Problema la aceasta metoda este transmiterea cheii, ce presupune existenta unei cai sigure de a transmite datele, care daca exista atunci nu mai are sens transmiterea cheii secrete. In trecut pentru distribuirea cheilor secrete SUA utiliza curieri, persoane ce transportau cheile secrete.
Criptografia cu **cheie privata** este denumita si **criptografie simetrica**, deoarece se foloseste aceeasi cheie de catre ambele parti ce comunica.

La criptografia cu cheie privata problema principala este distribuirea cheilor. De exemplu daca 3 persoane doresc sa aiba o comunicare securizata (6.3) au nevoie de 3 chei secrete.

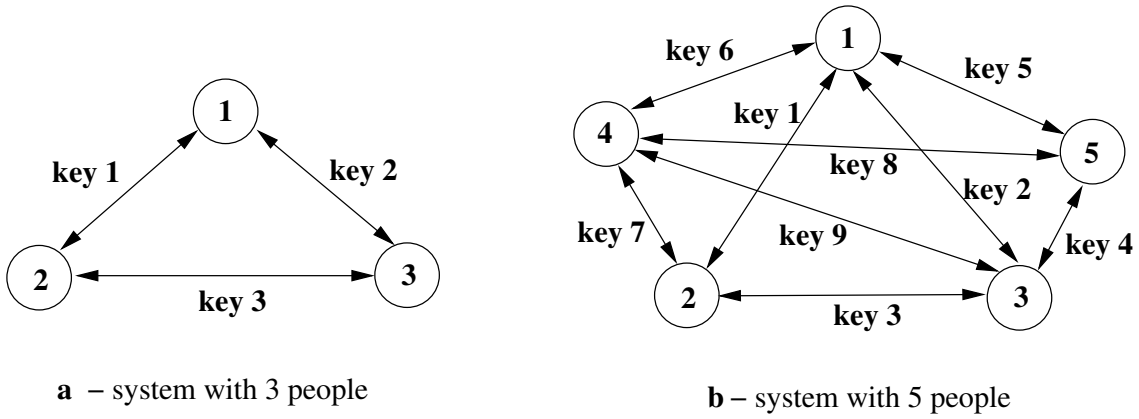

Figura 6.3: Criptografia cu cheie secreta

Persoanele 1 si 2 comunica cu **cheia 1**, 1 si 3 cu **cheia 2**, 2 si 3 cu **cheia 3**. Acesta este un sistem sigur de comunicare intre 3 persoane. Odata cu cresterea numarului persoanelor care comunica in sistem creste si numarul cheilor. In figura 6.3b se observa ca daca sistemului se alatura 2 persoane numarul cheilor creste la 9. Daca n persoane comunica prin acest sistem sunt necesare n*(n-1)/2 chei secrete. La 60.000 de persoane sunt necesare aproape 1,8 miliarde de chei. Problema ramane distribuirea acestor chei.

O solutie este folosirea unui centru de distribuire a cheilor, care creaza cheile si le distribuie la orice pereche de persoane ce doresc sa comunice. La centru se afla cheile secrete a persoanelor ce doresc sa comunice. Inainte de comunicare cel care initiaza comunicarea apeleaza la centru, care ii transmite o **cheie de sesiune** criptata cu cheia secreta a persoanei. Aceeasi cheie de sesiune este transmisa si celeilalti parti criptata cu cheia lui secreta. Astfel ambele parti pot decripta mesajul primit, adica cheia de sesiune, si pe baza acestei chei partile vor comunica. Partea vulnerabila in acest caz este centrul de distributie, care are cheile secrete al tuturor persoanelor. Acest sistem a fost utilizat multi ani de guvernul SUA.

Algoritmii utilizati in criptarea cu cheie secreta:

- **DES**: Data Encryption Standard, a fost adoptat in 1977 ca standard al guvernului american, si ca standard ANSI in 1981. DES utilizeaza o cheie pe 56 de biti. Era un algoritm puternic la vremea respectiva in 1976. Mai multe se pot afla la http://www.eventid.net/docs/desexample.htm
- Intre timp a fost inlocuit cu **3DES** (triple DES), care utilizeaza chei pe 112 biti. Este de 2 ori mai sigur ca DES, utilizand algoritmul DES de 3 ori, cu 2 chei diferite.

- RC2, RC4: Rivestş Code, este denumit dupa coinventatorul algoritmului cu cheie publica RSA
- **IDEA** (International Data Encryption Algorithm)este un algoritm de criptare in bloc, dezvoltat in Zurich, Elvetia in 1990. Utilizeaza cheie pe 128 de biti, si deocamdata s-a dovedit un algoritm puternic.
- **AES**: Advanced Encryption Standard, nou standard de criptare anuntat in octombrie 2000, ce inlocuieste vechiul standard DES, la care lungimea cheii era deja mult prea mica. Se utilizeaza chei de 128, 192 sau 256 de biti.

6.2.2 Criptografia cu cheie publica

In acest sistem printr-un proces matematic se creaza doua chei separate. **Un mesaj criptat cu una din chei poate fi decriptata cu cealalta cheie**. In general prima cheie, cea folosita pentru criptare este cheia publica, si cealalta folosita pentru decriptare este **cheia secreta** (figura 6.4). Cheia publica poate fi cunoscuta de oricine, iar cea secreta o are doar cel care a creat perechea de chei.
Cand expeditorul trimite un mesaj, acesta va cripta mesajul cu cheia publica a destinatarului. Acesta la primirea mesajului va decripta mesajul cu cheia lui secreta.

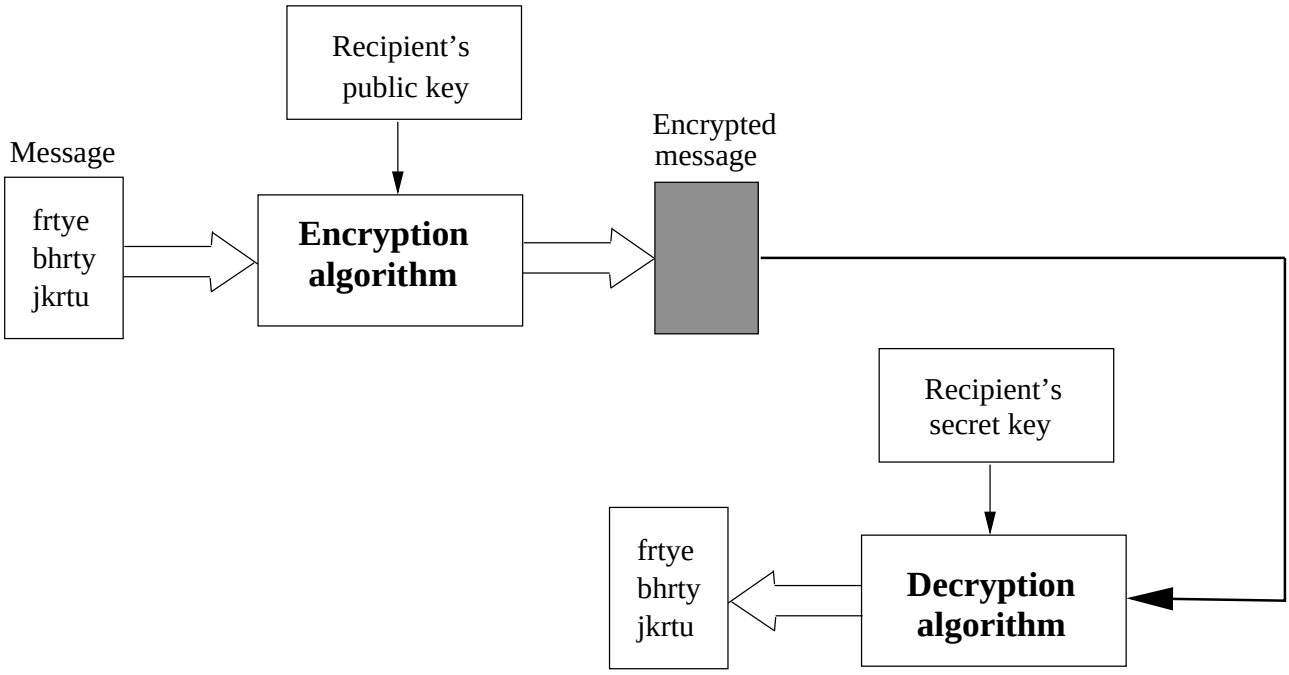

Figura 6.4: Criptarea cu cheie publica

Criptografia cu cheie publica se numeste si **criptografie asimetrica**.
Cel mai utilizat algoritm in acest sistem este RSA denumit dupa cele trei persoane care au

dezvoltat algoritmul, Rivest-Shamir-Adleman.
Avantajul sistemului cu cheie publica este ca cheia poate fi facuta publica, pentru ca acea cheie este utila numai la criptarea mesajelor. Decriptarea poate fi facuta numai cu cheia secreta. Acest lucru permite ca un utilizator sa poata trimite un mesaj criptat unei persoane pe care nu o cunoaste. Va cere cheia lui publica prin e-mail sau de pe pagina web si poate cripta mesajul cu cheia respectiva.

6.2.3 PGP

Pentru protejarea mesajelor transmise prin e-mail unul din cele mai populare programe ce folosesc criptografia asimetrica este **PGP** (Pretty Good Privacy).
Acest program utilizeaza atat criptografia cu cheie publica cat si cea cu cheie privata.

- PGP creeaza pentru fiecare mesaj separat o cheie aleatoare (**cheie de sesiune**)
- utilizeaza algoritmul **IDEA** pentru criptarea mesajului cu cheia de sesiune
- apoi utilizeaza algoritmul RSA pentru a cripta cheia de sesiune cu cheia publica a destinatarului.
- in final se combina mesajul criptat si cheia publica intr-un singur mesaj care este transmis la destinatie.

Criptografia cu cheie publica RSA este utilizata pentru autentificare si criptare in industria calculatoarelor. Principalele caracteristici oferite de PGP:

- **crearea celor doua chei**: secreta si publica. Acestea sunt necesare pentru criptarea si semnarea mesajelor trimise, si decriptarea mesajelor primite de la altii.
  O cheie publica PGP este indicaya in tabelul 6.1.
- **criptarea fisierelor**: fisierul odata criptat poate fi decriptat numai daca se cunoaste parola utilizata la criptare.
- **transmiterea si receptionarea mesajelor** electronice criptate. PGP poate fi utilizat pentru criptarea mesajelor trimise si decriptarea mesajelor primite. La transmiterea unui mesaj se utilizeaza **cheia publica** a destinatarului, si numai acea persoana poate decripta mesajul cu **cheia sa secreta**.
- **administrarea cheilor**: se poate utiliza pentru crearea si administrarea unei baze de date ce contine cheile publice ale persoanelor cu care corespondeaza utilizatorul. Este asemanatoare cu o agenda de adrese, dar care in loc de adrese e-mail contine cheile publice.
- utilizarea **semnaturilor digitale**. PGP poate fi utilizat pentru a semna electronic un document. De asemenea poate fi folosit pentru a verifica semnatura altor persoane.

—BEGIN PGP PUBLIC KEY BLOCK—
Version: PGP Key Server 0.9.5

mQCNAjCmAM4AAAEEAL4x2QLLWfYbb2WJJCG6NJ5J3mxm02Ph6FoWH2h+jn8OC340
RMXYghxEuVxwQskUx87OmLks9aAGPSaTFEgvtllIVbat5Z6ifIxjBinABB/CqQMb
cTn/llFncOTM0AxiGqNyBdqcc37ID3KsT1Jmy/OIdkGtazDu/r5171ip4GslAAUR
tC1KdWRpdGggQS4gU3pla2VseSA8NzY3NjEuMzQwNEBjb21wdXNlcnZlLmNvbT6J
AFUDBRAxu4hQ9yZQAXTvaTEBAXHwAf0RAwAHEpP1CWTWF2Jh8ixFTeaX/J4H+j6Q
SCNjT4WA7FGmzoerLRh5N6e3bBEVCh7q+acemkHRSB6mhINMLTmPtDBKdWRpdGgg
QS4gU3pla2VseSA8SnVkeVN6ZWtlbHlAd29ybGRuZXQuYXR0Lm5ldD6JAJUDBRAz
nJnGvnXvWKngayUBAcK+A/9i8I+qesoA64PHR09speElG3guyj/RwOLOAZUSl9+s
Z50V/mLIPilpdMtuom6Buxghw1h4dgRue92YXeQ5NYiqpRBivAEglronorL5sKay
eDJWbj1ROx1pwqsO8Nk/kdocOHhVqR9cdPzJGZTO2ZtrVSq8PrcmLq7TNXoSL83V
lYkAVQMFEDOcpNL3JlABdO9pMQEBHqcB/ju9P0zDpWIp6EQggO1PfFnnjvshLUhf
ROotcL7YU/zst63AfbnQovrBtdveUfKjsHtYNc/Q4OAY5bw8tOQpYjM=
=40XL
—END PGP PUBLIC KEY BLOCK—

Tabelul 6.1: Cheie publica PGP

- **certificare cheilor**. PGP poate fi utilizat pentru a semna electronic cheile publice ale altor persoane. Utilizat la certificarea si distributia cheilor.
- **utilizarea serverelor de chei PGP**. Se poate adauga cheia publica la o baza de date, si se pot obtine de la server cheile publice ale altor persoane.

Semnatura digitala este o semnatura electronica (asemanatoare cheii publice) ce poate fi folosita pentru a autentifica identitatea persoanei care a transmis mesajul si faptul ca continutul mesajului original nu a fost alterat. Semnaturile digitale sunt usor de transportat, nu pot fi imitate de alte persoane. Semnatura digitala poate fi folosita cu orice tip de mesaj, indiferent daca este criptata sau nu, pentru a dovedi destinatarului identitatea expeditorului si faptul ca mesajul este intact.
La semnarea unui mesaj se parcurg urmatoarele etape:

- programul utilizat, de exemplu PGP, creaza mesajul **hash** al mesajului original. Acesta se obtine folosind **algoritmul hash** asupra mesajului original. Un simplu exemplu ar fi obtinerea valorii hash al unui numar inmultindu-l cu un numar aleator. Practic numarul original nu poate fi gasit fara a sti acea valoare aleatoare. Daca se folosesc numere foarte mari pe 40 sau 128 de biti, practic este imposibil de a deriva valoarea initiala din valoarea hash.
  Algoritmul hash este transformarea unui sir de caractere intr-un numar de lungime fix, ce reprezinta sirul original. Este folosit pentru a indexa si extrage valori dintr-o baza de

daet, pentru ca o valoare se gaseste mult mai rapid utilizand valoarea scurta hash decat valoarea originala. Si bineinteles este folosit si in criptografie. Una din functiile hash mult utilizate este **MD5** *sau* **SHA**.

- aceasta valoare se cripteaza cu cheia secreta, astfel asigurand autenticitatea, deoarece numai expeditorul detine cheia secreta.

- valoarea hash criptata devine semnatura digitala a mesajului.

La primirea mesajului destinatarul efectueaza operatiile:

- creaza mesajul hash al mesajului primit

- cu cheia publica a expeditorului se decripteaza semnatura, care de fapt este valoarea hash a mesajului original

- daca cele doua mesaje hash coincid inseamna ca mesajul nu a fost alterat dupa ce expeditorul a semnat mesajul.

Criptarea si semnatura digitala pot fi folosite simultan sau separat. Un mesaj poate fi:

- criptat fara sa fie semnat

- semnat dar necriptat

- intai criptat si apoi semnat

- intai semnat si apoi criptat.

Prin protejarea informatiei se asigura urmatoarele:

- intimitatea datelor: pentru a proteja datele personale si a preveni accesarea mesajele personale de o a treia persoana

- integritatea datelor: pentru a fi siguri ca ceea ce s-a primit este intr-adevar ce s-a transmis de la sursa

- pentru ca persoana care a trimis mesajul sa nu poata nega ca a trimis acel mesaj

- autenticitatea datelor: ofera siguranta ca mesajul este intr-adevar de la persoana a carui nume apare ca expeditor.

6.3 Server de web Securizat - SSL

Protocolul ce implementeaza criptarea cu cheie publica este numit **SSL** (Secure Socket Layer), dezvoltat de Netscape. Acest protocol este utilizat de catre navigatoare si servere de web pentru a transmite date pe cale sigura, deci a fost creat pentru a fi utilizat de catre protocolul HTTP. De-a lungul anilor a inceput sa fie folosit si pentru alte protocoale pentru securizarea transmiterii informatiei, ca POP3, SMTP, IMAP.

Prin server de web securizat (secure server) se intelege un server ce utilizeaza SSL pentru comunicare, si nu unul care este protejat impotriva atacurilor. Pentru a avea acces la o pagina web securizata, se utilizeaza **portul 443**, folosit pentru comunicarea prin metoda de criptare bazata pe SSL. Conectarea la un server de web securizat se face prin mentionarea in URL a protocolului **https** in loc de **http**:

https://vega.unitbv.ro

adica accesul la pagina de web securizata este indicat prin protocol, si nu numele serverului.

Un server de web securizat ofera:

- **transfer sigur al informatiei**: datele transmise intre server si navigator nu pot fi decriptate in cazul interceptarii lor.
- **autentificare server**: daca serverul web a primit un **certificat** de la o bf autoritate de certificare (CA), clientii care se conecteaza la el pot fi protejati impotriva redirectionarii catre un alt server, care pretinde a fi serverul la care se doreste conectarea, prin verificarea continutului certificatului.

6.3.1 Functionarea unui server web securizat

Pentru a rula un server de web securizat aceasta trebuie sa suporte **protocolul SSL**, si sa **detina un certificat digital** (optional) de la una din autoritatile de certificare. Certificatul poate fi creat si de catre administratorul serverului de web, caz in care in momentul cand un utilizator acceseaza pagina ii apare un mesaj ce-l avertizeza ca certificatul nu a fost eliberat de o autoritate de certificare cunoscuta. Acest mesaj este indicat in figura 6.5.

Utilizatorul poate alege sa intre sau nu pe pagina respectiva.
Inainte de a transmite pagina web, intre server si client au loc urmatoarele tranzactii:

- navigatorul cere inceperea unei sesiuni sigure cu serverul
- serverul intoarce certificatul site-ului si **cheia sa publica**

Figura 6.5: Mesaj in cazul unui certificat creat local, nu de o autoritate de certificare

- navigatorul verifica validitatea certificatului. Daca certificatul nu este eliberat de catre o autoritate de certificare, atunci apare mesajul din figura 6.5.
- navigatorul creaza o **cheie de sesiune** (valabila numai pe durata acestei conexiuni intre server si navigator) care este criptata cu cheia publica a serverului, care apoi este trimisa la server.
- serverul decripteaza informatia, adica cheia de sesiune, folosind cheia lui privata
- dupa aceasta ambele parti (navigatorul si serverul) utilizeaza aceeasi cheie de sesiune, si toate datele transmise vor fi criptate si decriptate cu aceasta cheie.

Un aspect important este **lungimea cheii** cu care se cripteaza informatiile. In cazul in care se cere un nivel foarte mare de securitate si navigatorul nu este capabil de criptare la 128 de biti, serverul poate trimite un mesaj utilizatorului ca sa instaleze un browser capabil de criptare la 128 de biti.
Navigatoarele mai vechi folosesc chei pe 40 sau 56 de biti, iar cele noi cripteaza cu chei de 128 de biti. Expertii in criptografie considera criptarea pe 128 de biti imposibil de spart, pentru ca ar dura milioane de ani chiar si cu cele mai performante calculatoare. In schimb cheile de 40 sau 56 de biti nu sunt atat de puternice, si se pot incerca toate combinatiile.

In ziua de azi exista si solutii oferite de firme (**www.thawte.com**), prin care un server de web poate "ridica" nivelul de cripotare la 128 de bit cand transfera informatii spre navigatoare ce ofera un nivel de criptare mai scazut. Dupa ce ambele parti utilizeaza aceeasi cheie secreta pentru criptarea si decriptarea informatiei, pot avea **un anumit nivel de siguranta** ca mesajul nu va fi interceptat si decodificat, acest lucru depinzand si de nivelul de criptare utilizat.

Pentru vizitatorul site-ului apare un mic icon in bara de jos (vezi figura 6.6) ce arata un lacat inchis, indicand ca transferul se face securizat (prin SSL).

Figura 6.6: Bara de stare a navigatorului indica transfer securizat

6.3.2 Despre certificate

Acesta este o "carte de credit" electronica ce dovedeste autenticitatea unui server web cand face tranzactii cu un client. Contine numele, un numar serial si o **copie a cheii publice** a celui care detine certificatul si **semnatura digitala** a autoritatii care a eliberat certificatul. Acesta garanteaza vizitatorului ca serverul web a fost verificat de catre o autoritate neutra, numita **autoritate de certificare**, cum este Verisign sau Thawte. Rolul acestor autoritati este de a garanta vizitatorului ca a accesat un site detinut si operat de catre cel care a cumparat certificatul. Autoritatea ofera certificatul numai companiei care detine domeniul respectiv. Obtinerea certificatului consta din urmatorii pasi:

- generarea unei cereri de certificare (**CSR** - Certificate Signing Request). Acesta consta in crearea unui sir de cifre si numere ce contin informatii ca: numele organizatiei, adresa IP, numele serverului, tara, etc. De asemenea cel care creaza cererea trebuie sa stie la care autoritate de certificare va apela.

- autoritatea de certificare va face investigatii, pentru a se asigura ca cel care cere certificarea este intr-adevar organizatia care pretinde a fi.

- certificatul primit va fi instalat pe server.

Un astfel de certificatul primit arata ca mai jos:

—BEGIN CERTIFICATE—
MIICcDCCAd0CEAUiHXBciZ0WRiWOiOArE+AwDQYJKoZIhvcNAQEEBQAwXzELMAkG
A1UEBhMCVVMxIDAeBgNVBAoTF1JTQSBEYXRhIFNlY3VyaXR5LCBJbmMuMS4wLAYD
VQQLEyVTZWN1cmUgU2VydmVyIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTk5
MTEyMjAwMDAwMFoXDTAwqTEyMTIzNTk1OVowgdoxCzAJBgNVBAYTAlVTMREwDwYD
VQQIEwhOZXcgWW9yazETMBEqA1UEBxQKUm9ua29ua29tYTEkMCIGA1UEChQbQW1i
YW89aXNzdXJhbmNlIENvcnBvcmF0aW9uMScwJQYDVQQLFB5DYWRyZSBGaW5hbmNp
YWwgU2VydmljZXMsIEluY4xMzAxBgNVBAsUKlRlcm1zIG9mIHVzZSBhdCB3d3cu
dmVyaXNpZ24uY29A78CQQgboYyk5OTEfMB0GA1UEAxQWc2VjdXJlLmFtYmFjLWNh
ZHJlLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQClKPd7umQ9lJjaXiYKhRB1
xQZf27qMorxTmIlMmM4sHNA78CQQgbJeAbRqVHhb+t81eROsfegJ9WF8lalJEXIL
AgMBAAEwDQYJKoZIhvcNAQEEBQADfgAyIG9lkpvXlQr9lLSnOptgBYRTqJgboRrs
ik+suY5y15BVfnAV38akogNnub6izGMqddJTKoZ56nKGXNRkY6glqya3rPaGiD5G
MMR9v6LSFd3XnA2YvCKm/WvbDrt9x2dzz/bTAqmUxKr/qo0fblb8ChTqgWUqEo27
gjDVbQ==
—END CERTIFICATE—

6.4 VPN(Virtual Private Network)

O retea virtuala privata este o conexiune sigura peste o retea nesigura cum este Internet-ul. Prin **virtual** se intelege existenta unei retele unice, indiferent de topologie, adica un grup de calculatoare distribuite geografic ce comunica si pot fi administrate ca o singura retea.
Prin **privat** se intelege o retea virtuala cu control al accesului. De asemenea privat mai inseamna si securitatea, adica o retea virtuala ce ofera confidentialitate integritatea mesajelor si autentificare intre utilizatorii si calculatoarele ce participa in comunicare.

Exista foarte multe topologii VPN, dar majoritatea se pot incadra in una din urmatoarele doua configuratii:

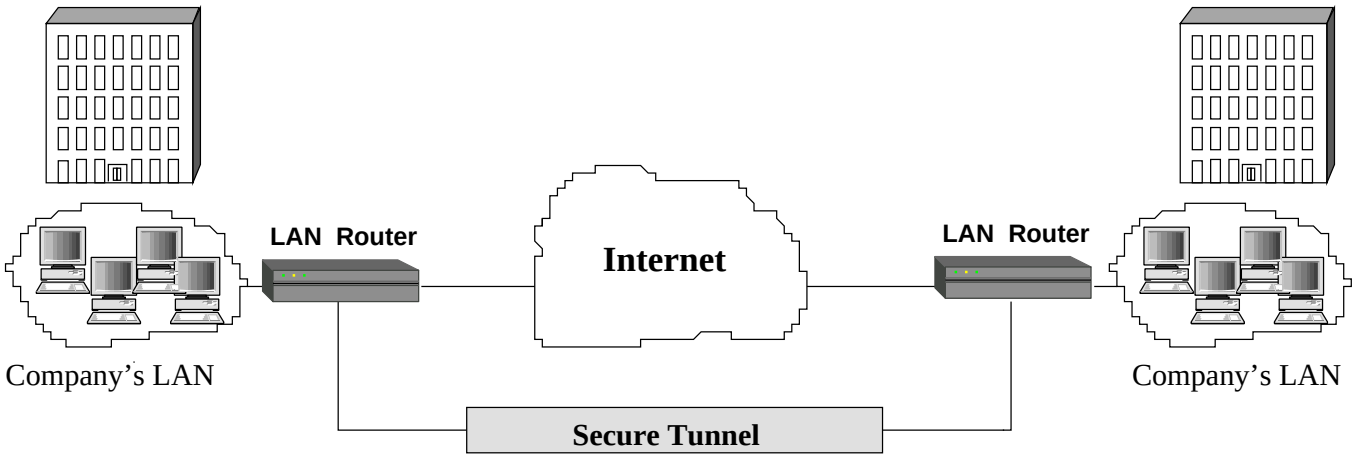

Figura 6.7: VPN intre site-uri

- grupuri de lucru private pot fi asigurate printr-o conexiune sigura intre 2 site-uri (figura 6.7), chiar daca LAN-urile ce contine acele grupuri de lucru sunt distribuie din punct de vedere geografic.

- acces de la distanta securizat pentru utilizatorii (figura 6.8)

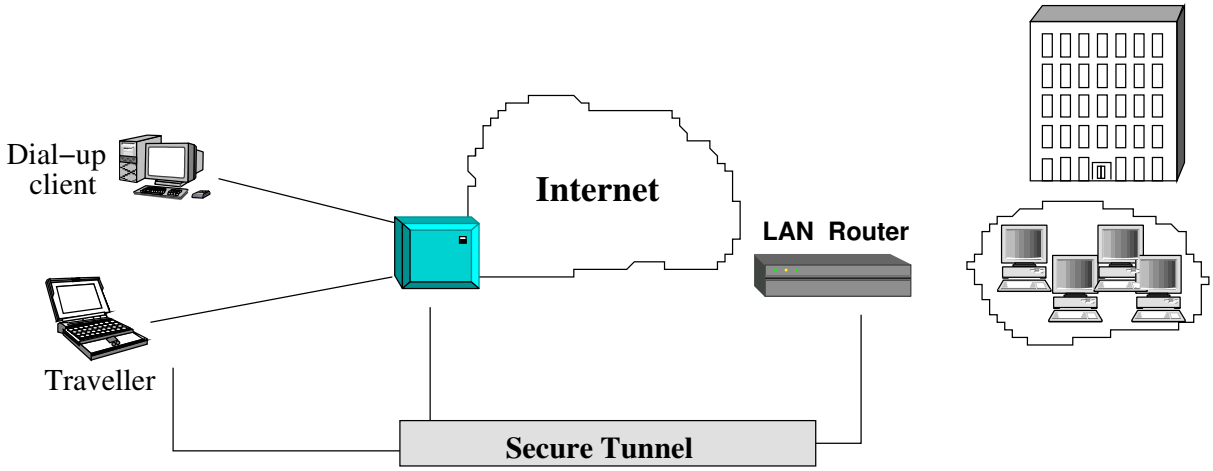

Figura 6.8: VPN for remote access