UNIVERSITATEA DIN BACĂU
FACULTATEA DE INGINERIE

POPA SORIN EUGEN

SECURITATEA SISTEMELOR INFORMATICE

note de curs şi aplicații
pentru studenții Facultății de Inginerie

2007

Cuvânt înainte,

Cursul "Securitatea sistemelor informatice" se adresează studenților de la specializarea Tehnologia informației anul III.

Cursul este structurat pe două părți, prima de teorie conține 8 capitole referitoare la definiții, clasificări, proceduri, programe şi sisteme de asigurare a securității sistemelor informatice şi a informațiilor şi a doua parte conține 6 lucrări practice de laborator.

Partea teoretică începe cu noțiuni generale privind securitatea informațiilor, cu definirea noțiunilor privind securitatea şi prezentarea standardului de securitate ISO / IEC 17799.

În al doilea capitol se prezintă clasificarea modernă a informațiilor, criteriile de clasificare funcție de domeniul de activitate, principii de clasificare, declasificare şi degradare a informațiilor.

Al treilea capitol tratează aspecte privind accesul personalului în sistemele informatice, cu tipuri de control al accesului, metode de autentificare şi identificare a utilizatorilor.

Capitolul patru, intitulat "Criptografia" tratează aspecte ale metodelor de ascundere a informațiilor astfel încât acestea să fie accesibile doar destinatarului acestora. Se prezintă definițiile de bază a criptografiei, steganografiei, filigranării, principiile de criptare prin cheie publică şi prin cheie privată, noțiuni privind semnătura digitală şi a sistemelor de certificare a cheilor publice.

În al patrulea capitol, intitulat "Modele şi programe de securitate", se prezintă modelele de securitate multinivel şi multilateral, precum şi programe, politici, norme şi standarde de securitate.

Capitolul şase face o introducere în securitatea rețelelor de calculatoare, prezentându-se principalele mecanisme utilizate în securitatea rețelelor de calculatoare: DHCP, firewall, servere proxy, filtrele de pachete, precum şi tehnica rețelelor VPN.

Capitolul al şaptelea prezintă tehnici, servicii şi soluții de securitate pentru Intranet-uri şi portaluri, cu detalierea unor aspecte prinvind tehnicile de criptare şi a funcțiilor folosite pentru transmiterea securizată a cheilor de criptare, autentificarea Kerberis 5, SSL/TTL, NTLM, SSH, S/MIME şi prezentarea firewall-urilor.

Ultimul capitol, al optulea, prezintă Strategii de securitate ale războiului informațional.

A doua parte a volumului conține șase lucrări practice de laborator în care se vor experimenta și verifica noțiunile și tehnicile de securitate predate în cadrul cursului.

Cele șase lucrări de laborator tratează următoarele probleme: criptarea și steganografia, instalarea și configurarea firewall-urilor, instalarea și configurarea serverelor proxy sub Windows și sub Linux, realizarea unei rețele VPN printr-un tunel OpenVPN.

Autorul

1. Noțiuni privind securitatea informațiilor

1.1. Introducere

Societatea îmbrățișează din ce în ce mai mult tehnologia informației. Informația care până nu de mult avea la bază hârtia, îmbracă acum forma electronică. Informația pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o stampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puțin din punct de vedere funcțional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil şi un mijloc de comunicare prin tehnologii precum poşta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri specifice. Măsurile ar trebui să asigure protecția informațiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informației gestionată de sistemele informatice în noul context tehnologic.

Securitatea informației este un concept mai larg care se referă la asigurarea integrității, confidențialității şi disponibilității informației. Dinamica tehnologiei informației induce noi riscuri pentru care organizațiile trebuie să implementeze noi măsuri de control. De exemplu, popularizarea unităților de inscripționat CD-uri sau a memoriilor portabile de capacitate mare, induce riscuri de copiere neautorizată sau furt de date.

Lucrul în rețea şi conectarea la Internet induc şi ele riscuri suplimentare, de acces neautorizat la date sau chiar frauda.

Dezvoltarea tehnologică a fost acompaniată şi de soluții de securitate, producătorii de echipamente şi aplicații incluzând metode tehnice de protecție din ce în ce mai performante. Totuşi, în timp ce în domeniul tehnologiilor informaționale schimbarea este exponențială, componenta umană rămâne neschimbată. Asigurarea securității informațiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană.

Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puțin din cauza unei deficiențe a mecanismelor de securitate.

Este important ca organizațiile să conştientizeze riscurile asociate cu utilizarea tehnologiei şi gestionarea informațiilor şi să abordeze pozitiv acest subiect printr-o conştientizare în rândul angajaților a importanței securității informațiilor, înțelegerea tipologiei amenințărilor, riscurilor şi vulnerabilităților specifice mediilor informatizate şi aplicarea practicilor de control.

Organizația Internaționala pentru Standardizare (ISO) împreuna cu *Comisia Internațională Electrotehnică (IEC)* alcătuiesc un forum specializat pentru standardizare. Organismele naționale care sunt membre ale ISO şi IEC participă la dezvoltarea standardelor internaționale prin intermediul comitetelor tehnice. Statele Unite ale Americii, prin Institutul Național de Standardizare, ocupă poziția de Secretar, 24 de țări au statut de Participanți (Brazilia, Franța, Regatul Unit al Marii Britanii, Coreea, Cehia, Germania, Danemarca, Belgia, Portugalia, Japonia, Olanda, Irlanda, Norvegia, Africa de Sud, Australia, Canada, Finlanda, Suedia, Slovenia, Elveția, Noua Zeelandă şi Italia) şi alte 40 de țări au statut de Observatori.

Prin activitatea susținuta de Ministerul Comunicațiilor şi Tehnologiei Informației (MCTI) de adoptare la nivel național a standardelor europene şi internaționale recunoscute, standardul ISO/IEC 17799 - "Tehnologia Informației – Cod de bună practică pentru managementul securității informației" a fost adoptat şi în România de către Asociația de Standardizare din România (ASRO), din toamna anului 2004. Standardul este recunoscut în rezoluțiile Consiliului Europei, implementarea acestuia la nivelul organizațiilor fiind opțională.

1.2. Definirea noțiunii de securitatea Informațiilor

Ca şi acțiunile prin care o organizație îşi apără angajații şi bunurile, securitatea informațiilor este folosită în primul rând pentru a oferi asigurări că drepturile care derivă din proprietatea intelectuală sunt protejate în mod corespunzător.

Obiectivul principal al unui program pentru protecția informațiilor îl reprezintă asigurarea încrederii partenerilor de afaceri, avantajul competitiv, conformitatea cu cerințele legale şi maximizarea investițiilor.

Indiferent de forma pe care o îmbracă, mijloacele prin care este memorată, transmisă sau distribuită, informația trebuie protejată.

ISO/IEC 17799 tratează securitatea informațiilor prin prisma a trei elemente principale:

- Confidențialitatea – informațiile sunt accesibile doar persoanelor autorizate;
- Integritatea – asigurarea acurateței şi completitudinii metodelor prin care se realizează prelucrarea informațiilor;
- Disponibilitatea – utilizatorii autorizați au acces la informații şi la activele asociate în momente oportune.

Pentru a putea realiza un program de securitate eficient este nevoie de politici, proceduri, practici, standarde, descrieri ale sarcinilor şi responsabilităților de serviciu, precum şi de o arhitectură generală a securității.

Aceste controale trebuie implementate pentru a se atinge obiectivele specifice ale securității şi pe cele generale ale organizației.

Dependența din ce în ce mai mare de sistemele informaționale conduce la creşterea tipologiei vulnerabilităților cărora organizațiile trebuie să le facă față. Mai mult, problema protecție trebuie să aibă în vedere de multe ori interconectarea rețelelor private cu serviciile publice. Dacă la acest aspect mai adăugam şi problema partajării informațiilor se conturează un tablou destul de complicat în care implementarea unor controale eficiente devine o sarcină dificilă pentru specialistul IT&C.

Multe din sistemele existente pe piață au fost proiectate după metodologia structurată dar nu au avut ca principal obiectiv şi asigurarea unui anumit grad de securitate pentru că la momentul respectiv tehnologia nu era atât de dezvoltată şi nici atât de accesibilă neinițiaților. Odată însă cu proliferarea Internetului ca şi mijloc important al comunicării moderne nevoia unor mecanisme de securitate proactivă a devenit o certitudine. În practică remarcăm că multe instituții apelează la soluții tehnice externe care să le rezolve problemele de securitate fără a căuta să-şi identifice nevoile şi cerințele specifice.

Identificarea controalelor interne care să asigure un grad corespunzător de securitate activelor informaționale ale unei instituții presupune o planificare riguroasă şi identificarea exactă a obiectivelor respectivei instituții. Pentru a fi însă eficiente aceste

controale trebuie să aibă în vedere pe toți angajații şi nu doar pe cei din compartimentul IT sau care au legătură directă cu acest domeniu.

Securitatea informațiilor nu este doar o problemă tehnică. Ea este în primul rând o problemă managerială.

Standardul de securitate ISO/IEC 17799 răspunde nevoilor organizațiilor de orice tip, publice sau private, printr-o serie de practici de gestiune a securității informațiilor.

Standardul poate fi folosit în funcție de gradul de expunere a fiecărei organizații în parte, pentru a conştientiza la nivelul conducerii aspectele legate de securitatea informației, sau pentru a crea o cultură organizațională în ceea ce priveşte securitatea informațiilor, sau pentru a obține certificarea sistemului de securitate.

Gradul de expunere a sistemelor informaționale variază cu industria în care activează fiecare organizație. Cu cât acest risc este mai mare, atenția care trebuie acordată securității datelor ar trebui să fie mai mare.

Instituțiile financiare, industria apărării, aerospațială, industria tehnologiei informației, industria electronică sunt sectoarele cu cel mai mare grad de risc în ceea ce priveşte securitatea informațiilor. Tot în această categorie de risc ridicat intră şi instituțiile guvernamentale, motiv pentru care adoptarea unei culturi organizaționale pe baza standardului ISO/IEC 17799 are un rol fundamental.

Stabilirea cerințelor

Este important ca fiecare organizație să poată să-şi identifice propriile cerințe de securitate. Pentru aceasta ea trebuie sa facă apel la trei surse principale:

- analiza riscurilor;
- legislația existentă;
- standardele şi procedurile interne.

Folosind o metodologie corespunzătoare pentru a analiza riscurile organizația îşi poate identifica propriile cerințe legate de securitate. Un astfel de proces presupune în general patru etape principale:

- identificare activelor care trebuie protejate;
- identificarea riscurilor/amenințărilor specifice fiecărui activ;
- ierarhizarea riscurilor;
- identificarea controalelor prin care vor fi eliminate/diminuate riscurile

Nu trebuie însă trecute cu vederea nici aspectele financiare.

Fiind un obiectiv comun, dictat de cerințele de afacere, pentru că până la urmă orice activitate derulată de o organizație are o rațiune economica, în implementarea unei arhitecturi de securitate trebuie puse în balanță costurile şi beneficiile.

Un mecanism de control nu trebuie să coste organizația mai mult decât bunul ce trebuie protejat.

Stabilirea cerințelor de securitate, a măsurilor necesare pentru a asigura nivelul de control dorit, are o componentă deseori subiectivă, fiind dificil de cuantificat în temeni monetari pierderea suferită în cazul unui incident de securitate. Aspectele intangibile precum alterarea imaginii organizației pe piață, credibilitatea în fața clienților sau efectele indirecte ale unui incident de securitate major, sunt cel mai greu de apreciat. Aceasta este rațiunea şi pentru care adoptarea unor standarde şi practici general acceptate, susținute de evaluări periodice independente este de recomandat.

Acest proces nu este unul static, altfel spus trebuie avute în permanenta în vedere schimbările care intervin în viata organizației pentru a fi reflectate corespunzător în planul de securitate. Dacă spre exemplu apare o modificare legislativă cu impact asupra instituției, trebuie avut în vedere din nou modelul folosit pentru evaluarea riscurilor pentru a vedea dacă acesta reflectă riscurile apărute ca urmare a acestei modificări.

În acest sens, ISO/IEC 17799 propune o serie de obiective de securitate şi controale din rândul cărora profesioniştii le pot selecta pe acelea care corespund afacerii în care funcționează. Pe de altă parte acest standard nu trebuie considerat un panaceu al securității informațiilor atât timp cât el oferă doar recomandări celor care răspund de implementarea şi managementul unui sistem de securitate în cadrul unei organizații.

De unde se începe

Controalele interne pot fi considerate principiile care stau la baza implementării unui sistem de management al securității. Chiar dacă sursele unor astfel de măsuri pot fi destul de variate, punctul de plecare într-un astfel de demers îl reprezintă legislația aplicabilă. Este foarte important ca cel care se ocupă de implementarea unui sistem de management al securității să aibă cunoştințe despre actualele cerințe legislative:

- Legea nr. 161 din 19 aprilie 2003 privind unele masuri pentru asigurarea transparentei în exercitarea demnitarilor publice, a funcțiilor publice si în mediul de afaceri, prevenirea si sancționarea corupției.
- Legea nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal si protecția vieții private în sectorul comunicațiilor electronice.
- Legea nr. 677 din 21 noiembrie 2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulație a acestor date.
- Legea nr. 455 din 18 iulie 2001 privind semnătura electronica.
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public.
- Hotărârea nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice si metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronica.
- Ordinul Avocatului Poporului nr. 52 din 18 aprilie 2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal.
- Ordinul Avocatului Poporului nr. 53 din 18 aprilie 2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulație a acestor date.
- Ordinul Avocatului Poporului nr. 54 din 18 aprilie 2002 privind stabilirea unor situații în care nu este necesara notificarea prelucrării unor date cu caracter personal care cad sub incidenta Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal si libera circulație a acestor date.
- Hotărârea nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu.
- Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate.

Pe lângă legislația internă trebuie avute în vedere şi *Convenţiile internaţionale* şi *Reglementările comunitare* semnate de România sau în care România este parte.

Selectarea controalelor trebuie să țină cont de specificul organizației. Nu toate recomandările pot fi aplicate, cum nu toate sunt justificate din punct de vedere al costurilor. Eficacitatea sistemului de securitate depinde de:

- stabilirea unor obiective de securitate care să reflecte cerințele organizației;
- sprijinului conducerii;
- existența abilităților necesare realizării analizei riscurilor, a vulnerabilităților şi a analizei de impact;
- instruirea angajaților;
- monitorizata controalelor implementate.

ISO/IEC 17799 a fost dezvoltat ca punct de plecare în dezvoltarea unui sistem de management al securității specific fiecărei instituții în parte. De aici rezultă caracterul său general, controalele prezentate în standard putând fi luate ca exemple pentru situații specifice fiecărei instituții în parte.

Primele două secțiuni ale standardului prezintă *Scopul* respectiv *Termeni şi Definiții*. Scopul standardului ISO/IEC 17799 stabileşte rolul acestui document ca fiind un ghid pentru domeniul securității informaționale.

Prin prezentarea Termenilor şi Definițiilor din secțiunea a doua, standardul asigură un limbaj comun pentru profesioniştii domeniului. Următoarele secțiuni prezintă obiectivele de control şi măsurile prin care se pot atinge aceste obiective.

1.3. Secțiunile standardului de securitate ISO / IEC 17799.

1.3.1. Politica de securitate

Obiectivul politicii de securitate este să ofere managementului instituției sprijinul necesar asigurării securității informațiilor din cadrul organizației.

Conducerea oricărei instituții trebuie să ofere suportul necesar prin elaborarea unui document intitulat Politica de Securitate, document care trebuie adus la cunoştință tuturor angajaților.

Fără un astfel de document există riscul ca rolurile şi responsabilitățile relative la asigurarea securității informaționale să fie greşit înțelese. Nedezvoltarea unui astfel de document şi neaducerea la cunoştința angajaților a politicii de securitate a companiei induce de cele mai multe ori o stare de superficialitate în tratarea acestor aspecte. Existenta unei viziuni clare a conducerii şi o comunicare efectivă a acesteia către angajați este fundamentală pentru asigurarea eficienței oricăror proceduri şi măsuri de securitate specifice.

1.3.2. Organizarea securității

Organizarea securității are ca obiectiv asigurarea unei administrări unitare în cadrul organizației.

Fiecare utilizator al sistemului informațional este responsabil cu asigurarea securității datelor pe care le manipulează. Existența unei structuri organizatorice unitare

care să inițieze şi să controleze implementarea mecanismelor de securitate în cadrul organizației, presupune un punct central de coordonare – responsabil cu securitatea.

Rolul şi atribuțiile persoanei care ocupă poziția de responsabil cu securitatea informațiilor se referă la coordonarea şi urmărirea respectării procedurilor şi politicilor de securitate.

Organizarea securității nu se limitează doar la personalul intern, trebuie avute în vedere şi riscurile induse de terți sau subcontractori care au acces la sistemul informațional. Acest risc nu este deloc de neglijat, ultimele tendințe ale pieței globale ne arată o reconsiderare a poziției companiilor față de externalizarea funcțiilor IT, tocmai datorită riscului mare indus de subcontractarea acestora.

Obiectivul organizării securității, aşa cum este documentat în standard este şi menținerea securității tuturor facilităților IT şi activelor informaționale accesate de către terțe persoane, fiind recomandată stabilirea unui proces prin care accesul terților să fie controlat.

1.3.3. Clasificarea şi controlul activelor

Măsurile de protecție sunt proiectate în funcție de gradul de senzitivitate, şi de semnificația economică a resurselor vizate. Perimetrele în care sunt amplasate echipamentele de procesare, vor fi protejate cu bariere de acces suplimentare. La fel şi telecomunicațiile cu un nivel ridicat de confidențialitate ar trebui criptate. Pentru a avea totuşi o abordare coerentă asupra măsurilor specifice de protecție, în funcție de gradul de senzitivitate al fiecărei resurse în parte se practică o clasificare a informațiilor.

Clasificarea informațiilor este necesară atât pentru a permite alocarea resurselor necesare protejării acestora, cât şi pentru a determina pierderile potențiale care pot să apară ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Obiectivul clasificării este crearea premizelor necesare asigurării unei protecții corespunzătoare valorii activelor instituției. Toate activele organizației trebuie să aibă asociat un proprietar. Politica de securitate trebuie să identifice angajații cu rol de proprietar, custode, client, utilizator.

1.3.4. Securitatea personalului

Cele mai multe incidente de securitate sunt generate de personal din interiorul organizației, prin acțiuni rău intenționate sau chiar erori sau neglijență în utilizarea resurselor informaționale.

Standardul ISO/IEC 17799 tratează riscurile de natură umană ce pot fi induse din interiorul organizației prin măsuri specifice precum includerea responsabilităților legate de securitatea informațiilor în descrierea şi sarcinile de serviciu ale postului, implementarea unor politici de verificare a angajaților, încheierea unor acorduri de confidențialitate şi prin clauze specifice în contractele de muncă.

Securitatea informațiilor este un aspect ce trebuie avut în vedere încă din etapa de selecție a angajaților. Angajații trebuie monitorizați pe întreaga perioadă de valabilitate a contractului de muncă şi trebuie să aibă cunoştință de prevederile politicilor de securitate. Clauzele de confidențialitate, definirea conflictelor de interese, distribuirea şi divulgarea informațiilor trebuie avute în vedere pentru fiecare post în parte.

Pentru a evita neglijența sau greşelile de operare, utilizatorii ar trebui informați cu privire la amenințările la care sunt supuse informațiile manipulate. Instruirea ar

trebui să ofere cunoştinţele necesare asigurării securităţii acestora în timpul programului normal de lucru.

Utilizatorii trebuie instruiți cu privire la procedurile de securitate ce trebuie urmate şi utilizarea facilităţilor IT în conformitate cu politica organizației.

Ar trebui să existe un program coerent de instruire a angajaților pe diverse niveluri de interes, pe lângă o instruire generală în gestiunea securității fiind necesare şi specializări pentru administratorii sistemului informatic în tehnologii de securitate specifice.

Chiar dacă securitatea unei anumite zone IT, cum ar fi securitatea rețelei revine unei entități externe, este o practică bună ca şi în interiorul organizației să existe competențele şi abilitatea de a evalua cum sunt satisfăcute cerințele de securitate.

Instruirea este necesară şi pentru a crea abilitatea de reacție la apariția unor incidente de securitate.

Raportarea incidentelor de securitate are ca obiectiv minimizarea efectelor negative sau a incorectei funcționări a echipamentelor. Monitorizarea unor astfel de incidente permite determinarea performantei sistemelor de securitate şi îmbunătățirea continuă.

Politicile şi procedurile de securitate trebuie implementate astfel încât să asigure un răspuns consistent la astfel de incidente.

1.3.5. Securitatea fizică

Delimitarea zonelor securizate are ca obiectiv prevenirea accesului neautorizat sau afectarea facilităților oferite de sistemul informațional.

Aceasta secțiune vizează mecanismele prin care se asigură securitatea fizică a imobilului în care organizația îşi desfăşoară activitatea.

Alt aspect important al securității fizice este cel legat de protecția echipamentelor, prin prevenirea pierderii, distrugerii sau compromiterii funcționării echipamentelor care pot afecta funcționarea organizației.

Echipamentele de calcul trebuie să fie protejate fizic împotriva amenințărilor voite sau accidentale. În acest sens trebuie dezvoltate standarde şi proceduri pentru securizarea atât a serverelor, cât şi a stațiilor de lucru ale utilizatorilor.

Măsurile de control al accesului, implementate la nivelul aplicației, bazelor de date sau rețelei pot deveni inutile dacă există şi o protecție fizică corespunzătoare.

1.3.6. Managementul comunicațiilor şi al operării

Operarea calculatoarelor trebuie să asigure funcționarea fără riscuri şi în bune condiții a resurselor organizației. Această funcție vizează atât echipamentele şi aplicațiile software, cât şi celelalte elemente necesare procesării informației şi susținerii funcțiilor de afacere.

Practicile de control recomandate pentru asigurarea operării de o manieră corectă şi sigură, constau în documentarea procedurilor de operare, controlul modificărilor aduse sistemului informatic, atât la nivel hardware cât şi software, formalizarea tratării incidentelor de securitate şi separarea responsabilităților.

Dinamica mediului informațional dată de schimbările tehnologice continue cât şi de apariția de noi cerințe din partea afacerii supune sistemul informatic la noi dezvoltări. Dezvoltarea şi testarea modificărilor aduse sistemului existent pot cauza probleme serioase operării curente. Pentru a controla aceste riscuri sunt recomandate separări

clare ale responsabilităților între dezvoltare, testare şi exploatare susținute şi de o separare a mediilor folosite pentru aceste activități.

Accesul programatorilor pe mediul de producție nu ar trebui permis, iar dacă anumite situații excepționale o cer, atunci ar trebui controlat îndeaproape.

Planificarea capacității sistemului este un alt obiectiv al operării calculatoarelor care are ca obiectiv minimizarea riscurilor întreruperii sistemului ca urmare a atingerii capacității maxime de procesare.

Asigurarea unei capacități corespunzătoare de procesare implică o planificare riguroasă a activităților sprijinite de sistemul informațional.

Trebuie dezvoltate proceduri şi mecanisme de raportare care să identifice utilizarea necorespunzătoare a resurselor precum şi perioadele de utilizare.

Protecția împotriva software-ului malițios este un aspect important întrucât cea mai mare amenințare a activelor informatice este dată de pierderea sau indisponibilitatea datelor ca urmare a infestării cu viruşi informatici. În toate sondajele, viruşii se află printre primele locuri ca sursă a incidentelor de securitate. Milioane de viruşi informatici sunt raportați anual. Protecția împotriva viruşilor nu o asigură doar administratorul sistemului, ci şi utilizatorul.

Asigurarea integrității datelor şi a aplicațiilor software necesită măsuri de protecție prin care să se prevină şi să se detecteze introducerea unor aplicații ilegale în sistemul organizației.

Aplicațiile tip antivirus trebuie instalate pe toate calculatoarele din sistem iar utilizatorii trebuie instruiți cu privire la folosirea acestora.

Alte aspecte ce fac obiectul managementului operării şi comunicațiilor vizează:

- întreținerea sistemului, incluzând realizarea copiilor de siguranță, întreținerea jurnalelor de operare, menținerea înregistrărilor cu erori de operare şi execuție.
- managementul rețelei, necesar asigurării rețelelor de calculatoare.
- manipularea şi securitatea mediilor de stocare, pentru a preveni întreruperea activităților afacerii.
- schimbul de aplicații şi date între organizații, pentru a preveni pierderea, alterarea sau utilizarea improprie a informației.

Întreținerea sistemului are ca obiectiv menținerea disponibilității şi integrității serviciilor IT.

Trebuie dezvoltate proceduri specifice care să descrie acțiunile prin care se realizează întreținerea serviciilor şi echipamentelor IT. Întreținerea sistemului trebuie să fie un proces continuu care să includă obligatoriu instalarea corecțiilor de securitate a aplicațiilor, sistemelor de operare şi sistemelor de gestiune a bazelor de date, realizarea copiilor de siguranță, jurnalizarea activităților realizate în şi de către sistem.

Managementul rețelei are ca obiectiv asigurarea protecției datelor transmise prin rețea şi a infrastructurii fizice a rețelei.

Pentru protecția rețelei sunt disponibile tehnologii specializate ce pot fi folosite în implementarea măsurilor de securitate şi atingerea obiectivelor de control:

- filtru – set de reguli implementate la nivelul unui router sau firewall prin care acesta permite tranzitarea sau nu a traficului către şi dinspre rețeaua unei companii;
- firewall – dispozitiv prin care este controlat traficul dintre rețeaua companiei şi rețelele externe acesteia;

- Sistem pentru Detectarea Intruziunilor (IDS – Intrusion Detection System), dispozitiv (hardware sau software) dedicat inspectării traficului unei rețele cu scopul identificării automate a activităților ilicite;
- criptare comunicații – procesul prin care datele sunt aduse într-o formă neinteligibilă persoanelor neautorizate;
- Rețea Virtuală Privată (VPN – Virtual Private Network) - o rețea care permite comunicarea între două dispozitive prin intermediul unei infrastructuri publice (nesigure)
- zona demilitarizată (DMZ) este o parte a rețelei care permite accesul controlat din rețeaua Internet. Maşinile dependente de accesul direct la rețeaua Internet, cum ar fi serverele de email şi cele de web sunt adesea plasate în astfel de zone, izolate de rețeaua internă a organizației.

Măsurile tehnice singure nu pot asigura nivelul de protecție necesar, fără un management corespunzător. Standardul ISO/IEC 17799 prezintă controalele necesare gestiunii corespunzătoare a securității comunicațiilor.

Prevenirea distrugerii mediilor de stocare al cărei efect s-ar concretiza în întreruperea serviciilor sistemului informatic s-ar putea asigura prin controlarea şi protejarea mediilor de stocare. Trebuie dezvoltate proceduri prin care este controlat accesul la orice mediu de stocare şi la documentația sistemului.

1.3.7. Controlul accesului

Confidențialitatea vizează protejarea informațiilor împotriva oricărui acces neautorizat. Uneori este interpretat în mod greşit ca această cerință este specifică domeniului militar şi serviciilor de informații care trebuie să-şi protejeze planurile de luptă, amplasamentul depozitelor de muniție sau al rachetelor strategice, notele informative. Este însă la fel de importantă pentru o organizație care doreşte să-şi apere proprietatea intelectuală, rețetele de producție, datele despre personalul angajat, etc. Pentru o instituție publică, datorită caracterului informației pe care o gestionează este important să asigure în primul rând integritatea şi disponibilitatea datelor.

Controlul accesului începe cu stabilirea cerințelor de acordare a drepturilor de utilizare a informațiilor.

Accesul la facilitățile şi serviciile oferite de sistemul informațional trebuie controlat în funcție de specificul şi cerințele mediului în care îşi desfăşoară activitatea organizația.

Pentru a răspunde acestor cerințe sunt în general definite o serie de reguli de acces corelate cu atribuțiile fiecărui utilizator al sistemului informatic.

Menținerea acestor reguli în linie cu cerințele organizației implică un proces de gestiune a accesului utilizatorilor sistemului. Obiectivul acestui proces este să prevină utilizarea neautorizată a calculatoarelor.

Trebuie să existe proceduri formale prin care să se controleze alocarea drepturilor de acces la serviciile şi resursele IT.

Utilizatorii autorizați trebuie instruiți cu privire la maniera în care trebuie raportate activitățile sau acțiunile considerate suspecte.

Fiecare componentă a sistemului informațional trebuie să facă obiectul măsurilor de control al accesului, datele trebuie protejate indiferent de forma sau starea care le caracterizează, fie că este vorba de aplicații software, sisteme de operare, baze de date sau rețele de comunicații. Tehnologiile mai vechi de gestiune a bazelor de date precum

Fox Pro, de exemplu, nu pot asigura o protecţie a informaţiilor la nivelul bazei de date, acestea fiind stocate în fişiere necriptate, accesibile oricărui utilizator, indiferent de drepturile de acces care i-au fost atribuite la nivelul aplicaţiei. Sistemele de operare precum DOS sau Windows 95/98 nu au mecanisme de control al accesului, nefiind posibilă restricţionarea drepturilor de utilizare a datelor la acest nivel. Standardul prevede însă măsuri de control pentru fiecare nivel al sistemului informaţional:

- controlul accesului la serviciile reţelei - conexiunile la serviciile reţelei trebuie controlate iar pentru obţinerea accesului la astfel de servicii este recomandată implementarea unei proceduri formale.
- controlul accesului la nivelul sistemului de operare – sistemul de operare trebuie să prevadă măsuri de restricţionare a accesului la date existente pe calculatore.
- controlul accesului la aplicaţii - prevenirea accesului neautorizat la informaţiile gestionate de aplicaţiile software.

Oricât de elaborate ar fi măsurile de control al accesului există totdeauna posibilitatea unei intruziuni, sau utilizarea inadecvată a resurselor existente.

Pentru a detecta potenţialele activităţi neautorizate este necesară monitorizarea accesului şi utilizării sistemului informatic.

Monitorizarea are un caracter continuu şi implică păstrarea şi revizuirea periodică a înregistrărilor cu evenimentele de sistem, şi a activităţii utilizatorilor.

1.3.8. Dezvoltarea şi întreţinerea sistemului

Aproape mereu, atunci când e vorba de dezvoltarea şi implementarea unui sistem informatic, cerinţele de securitate sunt neglijate. Eforturile sunt îndreptate mai mult spre aspectele funcţionale şi mai puţin pe controlul riscurilor de integritate şi confidenţialitate a informaţiilor. Organizaţiile se expun la riscuri majore de operare ce pot rezulta în pierderi financiare semnificative prin neglijarea unor măsuri minimale de control al procesului de dezvoltare şi implementare. Testarea aplicaţiilor nu este formalizată, ceea ce nu garantează calitatea dezvoltărilor, programatorilor li se permite accesul la mediul de producţie pentru corectarea unor erori nedetectate în procesul de testare, inducând riscuri de integritate şi disponibilitate a datelor.

Aspectele de securitate nu trebuie neglijate în partea de dezvoltare şi implementare, deşi acestea s-ar putea să deranjeze şi să nu aducă aparent nici un beneficiu. Fără a ţine cont de recomandările de control ale acestui proces, organizaţia riscă să investească într-o aplicaţie sau echipament care să nu-i ofere nici o garanţie asupra informaţiilor gestionate.

Obiectivele de control prevăzute în această secţiune a standardului sunt menite să asigure că noile sisteme dezvoltate au prevăzute mecanisme de securitate, prin:

- dezvoltarea cerinţelor şi analiza specificaţiilor de securitate;
- validarea datelor de intrare
- controlul procesării interne
- autentificarea mesajelor transmise electronic
- validarea datelor de ieşire
- utilizarea tehnicilor de criptare
- utilizarea mecanismelor de semnare electronică

- protejarea codului aplicațiilor şi a fişierelor sistemului de operare

De asemenea, este necesară şi asigurarea securității mediilor de dezvoltare şi a serviciilor suport. Mediile în care se dezvoltă aplicații sau proiecte noi trebuie strict controlate. Mediul de testare trebuie separat de mediul de producție, datelor de test asigurându-li-se protecția corespunzătoare.

1.3.9. Planificarea continuității afacerii

Un plan de continuitate a afacerii reprezintă o serie de măsuri de reacție în caz de urgență, de operare alternativă şi de restaurare a situației în caz de dezastru pentru a asigura disponibilitatea resurselor critice şi pentru a permite continuarea activității în cazul unor incidente majore. Majoritatea companiilor nu au un astfel de plan de continuitate, de cele mai multe ori aceste aspecte sunt neglijate sau sunt limitate la achiziționarea unor echipamente de rezervă sau tolerante la defecte.

Scopul unui plan de continuitate este de a asista organizațiile în a continua să funcționeze atunci când activitatea normală este întreruptă. Este mult mai bine ca acest lucru să fie planificat în avans, printr-o atitudine proactivă.

Planurile pentru continuitatea afacerii trebuie să asigure disponibilitatea proceselor considerate critice pentru funcționarea organizației în cazul apariției unor dezastre sau întreruperi de funcționare.

Asigurarea continuității afacerii presupune parcurgerea etapelor de documentare, testare şi implementare a planului de continuitate a afacerii.

Implementarea presupune instruirea personalului şi dezvoltarea unor procese speciale de gestiune a situației de criză, precum şi de actualizare periodică.

1.3.10. Conformitatea

Proiectarea, operarea sau gestiunea sistemelor informaționale pot face obiectul unor reglementari, legi sau angajamente contractuale în ceea ce privește securitatea.

Pentru a evita încălcarea dispozițiilor statutare sau legale, standardul prevede o serie de măsuri precum:

- identificarea legislației aplicabile
- utilizarea adecvată a licențelor software sau a materialelor protejate de drepturi de autor
- protejarea înregistrărilor organizației (înregistrări contabile, chei de criptare, jurnale de activitate, medii de stocare, proceduri de lucru)

Pentru a asigura conformitatea cu politicile şi standardele de securitate ale organizației, securitatea sistemului informațional trebuie revizuită periodic pentru a reflecta schimbările tehnologice sau organizatorice.

2. Clasificarea informațiilor

2.1. Noțiuni introductive privind clasificarea modernă a informațiilor

Clasificarea înseamnă etichetări crescătoare ale documentelor sau informațiilor, de la cel mai de jos nivel, unde se situează informațiile deschise su neclasificate, la cele confidențiale, urcând spre informații secrete şi strict secrete.

În clasificarea informațiilor s-a plecat de la ideea că informațiile care prin compromitere pot costa vieți umane sunt marcate drept secret, în timp ce informațiile a căror compromitere costă pierderea multor vieți umane sunt definite strict secrete.

Personalul din domeniu securității sistemelor sunt investiți cu drepturi diverse, de a lucra cu anumite categorii de informații. Pe lini accesului la unele categorii de informații, pentru exercitarea controlului lucrurile sunt destul de clare: un angajat poate citi documentele dintr-o anumită categorie numai dacă el are cel puțin dreptul de accesare a informațiilor din acea categorie sau din una superioară. Regula este că informațiile pot circula doar în sus, de la confidențial la secret şi strict secret, în timp ce în sens invers, de sus în jos, pot circula doar dacă o persoană autorizată ia decizia de declasificare a acestora.

Se utilizează două strategii de bază privind securitatea națională, şi anume:

- tot ceea ce nu este interzis este permis;
- tot ceea ce nu este permis este interzis.

Se apelează la două tactici de implementare a strategiei fundamentale privind protejarea informațiilor deosebite:

- controlul discreționar al accesului;
- controlul legal al accesului.

Prima tactică de control al accesului implementează principiul celui mai mic privilegiu: nici o persoană, în virtutea rangului sau poziției ce o deține, nu are drepturi nelimitate de a vedea informațiile deosebite, iar persoanele care au o astfel de facilitate trebuie să le vadă numai pe cele care intră în sfera lor de activitate.

Controlul discreționar al accesului este aplicat printr-o matrice de control, conform modelului prezentat în figura 2.1. Pentru fiecare persoană aflată pe listă şi pentru fiecare informație, matricea arată ceea ce poate face fiecare subiect cu obiectele din listă: citire, scriere, execuție, aprobare etc.

Subiect	**Obiect 1**	**Obiect 2**	**Obiect 3**
Subiect 1	Execută	Citeşte	Citeşte
Subiect 2	Citeşte	Citeşte/Scrie	Aprobă
Subiect 3	Citeşte/Scrie	Aprobă	Citeşte/Scrie
Subiect 4	Aprobă	Execută	Execută
Subiect 5	Execută	Citeşte	Aprobă

Fig. 2.1: Matricea de control al accesului.

Controlul legal al accesului îşi exercită forța pe baza legilor existente (legea securității naționale), prin care sunt stabilite două tipuri de structuri de control: ierarhizate şi neierarhizate.

Structura ierarhizată încadrează informațiile senzitive în patru categorii: strict secrete, secrete, confidențiale şi neclasificate;

În structura neierarhizată, sunt două categorii: compartimentate şi cu obiecții sau ascunse vederii unor categorii de persoane. Compartimentările pot avea nume scurte, sugestive, care să scoată în relief anumite aspecte. Categoria cu obiecții priveşte ăn special naționalitatea potențialilor cititori şi autori ai obiectelor.

Informațiile strict secrete, care sunt într-o anumită măsură compartimentare, se numesc informații senzitive compartimentate şi presupun o atenție deosebită la întrebuințare. Doar o categorie de informații este superioară acesteia din urmă, şi anume despre informațiile din planul operativ integrat unic sau răspunsul național în caz de război.

2.2. Clasificarea informațiilor

Guvernele pleacă de la o clasificare mai largă a informațiilor, şi anume: informații subiective şi informații obiective (față de împărțirea în clasificate şi neclasificate).

2.2.1. Informațiile subiective

Informațiile subiective au mai fost caracterizate şi ca "secrete adevărate" sau informații operaționale. Aceste informații sunt unice pentru guvern, în sensul că el decide asupra modului în care se vor derula principalele activități ce-i revin. Cât timp guvernul controlează şi protejează informațiile pe baza cărora ia decizii, acele informații nu pot fi dezvăluite independent de către adversar.

Aceste informații au următoarele caracteristici:

- dimensiune redusă – secretul poate fi exprimat doar prin câteva cuvinte; din care cauză poate să fie uşor furat şi distribuit altora;
- perceptibilitate universală – nu este nevoie de pregătire specială pentru a înțelege secretul, oricine poate să-l fure;
- supuse arbitrarului – pentru a intra în posesia lor un adversar le poate fura, secretul nu poate fi descoperit independent;
- conținutul poate fi schimbat – secretul poate fi modificat şi în ultima clipă;
- sunt perisabile după scurt timp – secretele au o viață scurtă, el poate fi ținut doar pentru o perioadă scurtă de timp.

2.2.2. Informații obiective

Informațiile obiective sunt acelea care chiar dacă sunt descoperite, dezvoltate sau controlate de către guvern, pot fi deja cunoscute sau descoperite independent de o altă țară. În această categorie intră informațiile ştiințifice sau secretele ştiințifice. Aceste informații nu pot avea un control absolut, ele țin de natura lucrurilor nu de un secret.

Informațiile obiective au următoarele caracteristici:

- sunt confuze – de regulă, nu se bazează pe o formulă magică, pentru descrierea informațiilor ştiințifice sunt necesare rapoarte lungi, din această cauză ele nu se pot transmite uşor;
- pot fi înțelese numai de oamenii de ştiință;

- nu sunt supuse arbitrarului – şi alţii pot să afle răspunsul la o anumită întrebare ştiinţifică, dacă formulează întrebarea respectivă;
- nu sunt supuse schimbării – au caracter etern; un fenomen natural are o singură valoare;
- pot avea o viaţă lungă ca secret – alţii pot descoperi informaţiile în mod independent, dar o astfel de descoperire necesită mult timp, ceea ce va conduce la păstrarea secretului pentru o lungă perioadă de timp.

Informaţiile tehnice – secrete obiective

O altă categorie de informaţii nu se încadrează perfect în categoriile cunoscute, obiective sau subiective, ele fiind informaţiile tehnice, de genul proiectelor şi execuţiilor tehnice ale unor noi arme (de exemplu), diferite de caracterul ştiinţific al proiectării, şi sunt cunoscute ca informaţii tehnice văzute ca secrete obiective.

Caracteristicile informaţiilor tehnice sunt asemănătoare celor ştiinţifice, dar există unele diferenţe. Faţă de informaţiile ştiinţifice, informaţiile tehnice nu sunt fenomene naturale, ci înseamnă o metodă, un proces, o tehnică sau un echipament angajate în crearea unui produs. Se poate afirma că informaţiile tehnice sunt utilizate pentru exploatarea informaţiilor ştiinţifice.

Secrete comerciale

Secretele comerciale includ informaţiile despre procesele de fabricaţie, reţetele unor produse, precum şi alte informaţii obiective care pot fi descoperite independent de către alţii. Multe secrete comerciale sunt asemănătoare informaţiilor ştiinţifice şi tehnice.

2.2.3. Determinarea necesităţii clasificării informaţiilor

În cazul procesului de clasificare a informaţiilor se parcurg trei etape:

- stabilirea nevoii de clasificare;
- determinarea nivelului clasificării;
- determinarea duratei clasificării.

Etapa de stabilire a nevoii de clasificare se realizează în cinci paşi, astfel:

- definirea cu exactitate a informaţiilor de clasificat (opţional, dar recomandat);
- stabilirea dacă informaţiile se încadrează în unul din domeniile supuse clasificării;
- verificarea dacă informaţiile se află sub control guvernamental;
- determinarea dacă dezvăluirea informaţiilor poate conduce la producerea de daune pentru securitatea naţională;
- specificarea precisă a nevoii de clasificare a informaţiilor.

Determinarea nivelurilor clasificării

La clasificarea unei informaţii, acesteia i se va atribui un nivel de clasificare, care va evidenţia importanţa relativă a informaţiei clasificate.

Un sistem de clasificare eficient se bazează pentru niveluri de clasificare definite cu mare claritate.

În legea 182/2002 privind protecţia informaţiilor clasificate, din România, informaţiile clasificate din clasa secretelor de stat sunt încadrate pe trei niveluri:

- strict secrete de importanță deosebită – sunt informații a căror divulgare neautorizată este de natură să producă daune de o gravitate excepțională securității naționale;
- strict secrete - sunt informațiile a căror divulgare neautorizată este de natură să producă daune grave securității naționale;
- secrete - sunt informațiile a căror divulgare neautorizată este de natură să producă daune securității naționale;

Determinarea duratei clasificării

Guvernele clasifică informațiile şi aplică proceduri de securitate specială documentelor şi materialelor ce le conțin sau sunt purtătoare ale acestor informații pentru a preîntâmpina obținerea lor de către adversari, cu intenția de a le folosi împotriva deținătorului autorizat. În consecință, se foloseşte metoda clasificării informațiilor pentru a asigura păstrarea secretului.

În general, informațiile, oricât ar fi de prețioase, nu pot fi păstrate o perioadă nelimitată de timp fără să fie aflate de adversari.

Chiar dacă informațiile pot fi păstrate ani mulți fără a fi aflate de adversari, nu este, de regulă, recomandat să se păstreze perioade îndelungate. Clasificatorii informațiilor sunt cei ce vor hotărî dacă este cazul să se specifice timpul de păstrare a informației clasificate sau să se indice momentul în care va interveni declasificarea automată. Durata informațiilor clasificate trebuie să fie atât de scurtă cât să nu genereze costuri fără rost cu păstrarea lor. Nici duratele prea scurte nu sunt recomandate, deoarece adversarii ar intra prea devreme în posesia lor şi ar putea acționa pentru şubrezirea întregului sistem de securitate națională. Deci, doar clasificatorul trebuie să aibă grija stabilirii duratei de clasificare.

Durata clasificării informațiilor se determină prin una din următoarele metode:

- ca perioadă de timp măsurată de la data emiterii documentului;
- în funcție de un eveniment viitor ce poate să apară înaintea operațiunii de declasificare;
- dacă data, respectiv evenimentul nu pot fi specificate, atunci documentul conținând informații clasificate va fi marcat, pentru a se identifica instituția aflată la originea lui, ce va avea şi sarcina declasificării.

2.3. Declasifcarea şi degradarea informațiilor clasificate

Atunci când se realizează clasificarea informației se au în vedere anumite cerințe. Când, din diferite cauze, se schimbă circumstanțele, firesc, şi cerințele îndeplinite inițial se modifică, caz în care informațiile clasificate se declasifică sau trec pe un nivel inferior de clasificare.

Declasificarea informațiilor se efectuează de către reprezentanți ai guvernului, cărora le revine misiunea de declasificare. Trebuie făcută diferența între declasificarea informațiilor şi declasificarea documentelor sau materialelor. Ultima categorie poate fi efectuată şi de către contractorii guvernamentali.

Degradarea informațiilor clasificate înseamnă reducerea nivelului clasificării. În acest mod, informațiile stric secrete pot fi degradate la nivelul secret sau confidențial. Informațiile secrete pot fi degradate în informații confidențiale, iar cele confidențiale pot fi declasificate sau, dacă este cazul, ridicate pe un nivel superior.

Degradarea se efectuează de către persoanele care au clasificat inițial informațiile, de către succesorii acestora, şefii lor sau să către alți oficiali

2.4. Principiile protejării informațiilor speciale

Pentru protejarea informațiilor speciale se pot defini zece principii:

1. **principiul delimitării autorizării** – repartizarea informațiilor pe tipuri va consta într-o grupare ierarhică plus suma compartimentărilor în care se regăseşte informația. Autorizarea unei persoane presupune stabilirea sferei de exercitate a funcției şi ea constă din autorizarea pe criteriul ierarhic al persoanei plus suma autorizărilor compartimentărilor persoanelor din subordinea sa.
2. **principiul securității simple** – nici o persoană, dintr-o anumită subordonare, nu trebuie să vadă informația unei categorii care depăşeşte autorizarea sa.
3. **principiul stea** – nici o persoană nu va scrie ceva pe obiectele dintr-o categorie inferioară celei la care persoana are acces.
4. **primul principiu al integrității** – nici un program de calculator nu va accept informații de la un program inferior lui, pe linia privilegiilor;
5. **al doilea principiu al integrității** – nici un program pentru calculator nu va scrie ceva într-un program superior lui, prin prisma privilegiilor;
6. **principiul etichetării –** fiecare purtător de informații va fi etichetat clar cu categoria informațiilor conținute, în format accesibil omului şi în format sesizabil de către echipamentele periferice;
7. **principiul clarificării –** nici o persoană sau procedură nu va schimba categoriile existente ale informațiilor şi nici autorizările existente, conform unor proceduri în vigoare;
8. **principiul inaccesibilității** – nici o informație nu va fi lăsată la dispoziția altor persoane sau procese, cu excepția celor consemnate prin norme interne;
9. **principiul verificabilității** – pentru toate activitățile semnificative pe linia securității se vor crea înregistrări imposibil de şters, cu rolul facilitării verificării sistemului.
10. **principiul încrederii în software** – cât timp nici un calculator nu poate controla perfect respectarea principiilor anterioare, dar, totuşi, efectuează activități utile, încrederea în software va permite apariția unor excepții de la regulă, dacă este cazul.

Există patru moduri de funcționare prin care sistemele de prelucrare automată a datelor pot asigura protecția informațiilor speciale:

- ***modul dedicat*** – toate informațiile prelucrate de sistem fac parte din aceeaşi categorie, iar persoanele sistemului posedă autorizație de acces la categoria respectivă;
- ***modul sistem superior*** – informațiile prelucrate de sistem pot să aparțină unor categorii diferite, dar toate persoanele angajate în această operațiune posedă autorizații care să le ofere accesul la nivelul cel mai ridicat al informațiilor prelucrate;
- ***modul controlat*** – un sistem poate prelucra informații din categorii diverse şi persoanele să aibă autorizații diferite, iar sistemul se va baza pe restricții fizice, prin care să se respecte toate principiile securității informațiilor – operațiune destul de dificilă.

- ***Modul securității stratificate*** – sistemele prelucrează informații aparținând diverselor categorii, iar personalul, de asemenea, dispune de autorizații diferite. Conceptul credibilității componentelor informatice (hardware, software şi firmware – softul aflat în memoria ROM) rezolvă o astfel de problemă a "turnului Babel" al securității sistemului, asigurându-se realizarea tuturor principiilor enunțate anterior.

2.5. Protejarea mediilor de stocare a informațiilor

Toate mediile de stocare care conțin informații obținute în urma prelucrării automate a datelor trebuie să fie catalogate ca documente ale prelucrării automate a datelor. Acestea pot fi CD-uri, DVD-uri, benzi magnetice, diskete, hardiscuri, circuite electronice etc. Regimul lor de lucru trebuie să fie similar documentelor ce ar conține aceleaşi date în condițiile prelucrării tradiționale.

Toate materialele intermediare şi informațiile obținute în timpul prelucrării automate a datelor trebuie să fie considerate ca materiale auxiliare. Acestea includ materiale anulate (benzi şi discuri magnetice, hârtie tipărită, benzi tuşate etc.) şi trebuie să fie supuse clasificărilor în funcție de informațiile ce le conțin.

Ştergerea informațiilor clasificate este o operație de importanță deosebită.

Persoanele care autorizează operațiuni de prelucrare automată a datelor trebuie să verifice existența unei fişe de securitate, care să conțină categoria persoanei executante, categoria informațiilor prelucrate şi instrucțiuni privind statutul informațiilor rezultate. Se vor consemna, de asemenea, date privind durata prelucrării, timpul de utilizare a componentelor bazei de date, generațiile reținute (fiu, tată, bunic) astfel încât să poată fi reconstituită baza de date în caz de avarii, precum şi alte cerințe pe linia păstrării copiilor de siguranță.

2.5.1. Marcarea materialelor cu regim special

Documentele aflate sub regim special trebuie să fie numerotate şi înregistrate pentru a se putea şti ce s-a folosit sau ce s-a văzut din ele.

Toate documentele obținute din prelucrarea automată a datelor (hârtia de imprimantă) trebuie să fie marcate astfel încât să fie vizibilă categoria din care fac parte, prin plasarea marcajului în colțul din dreapta sus, precum şi în partea inferioară a fiecărei pagini, la care se va adăuga şi numărul de exemplare al fiecărui document.

În cazul prelucrării automate a datelor, un ecran cu informații este tratat ca o pagină de document, şi încadrarea într-o categorie sau alta se va face pe o linie distinctă a acestuia.

Marcarea în cod maşină trebuie să se efectueze prin coduri sesizabile de echipamente, astfel încât să rezulte foarte clar din ce categorie fac parte informațiile prelucrate şi la ce operațiuni pot fi supuse. Codul trebuie să fie una dintre primele informații ce vor fi date sistemului, astfel încât să nu fie posibilă accesare altor date înainte de a se şti statutul lor. Codul poate fi ultimul caracter al numelui fişierului, iar caracterul folosit să aibă valorile:

- S – special;
- C – confidențial;
- P – private;
- R – cu restricții;
- N – neclasificate.

Marcarea fizică se referă la toate suporturile supuse prelucrării automate a datelor. Marcajul trebuie să reziste în timp şi să nu fie afectat sau să afecteze prelucrarea automată a datelor. Marcarea se poate realiza chiar pe suport sau pe ambalajul care-l conține. Suporturile reutilizabile trebuie să fie marcate cu etichete adezive sau creioane ce pot fi şterse ulterior.

Marcarea suporturilor de hârtie au marcajul prin culori distincte: orange – control special, roz – confidențial, verde – privat, galben – cu restricții, albe – comune. Dacă numai o parte a pachetului conține informații protejate, tot volumul va căpăta acelaşi statut.

Marcarea cutiilor şi a carcaselor este necesară atunci când suporturile de memorare sunt păstrate în astfel de condiții, care în care se impune etichetarea clară a acestora, precum şi scrierea fişierelor conținute de suporturile din interior.

Marcarea benzilor magnetice se face cu etichete lipite chiar pe bandă, fără să afecteze prelucrarea datelor.

Marcarea pachetelor de discuri se realizează cu carioca în mijlocul acestora.

Marcarea microfilmelor se face pe prima imagine cadru sau pe cutie, cu carioca.

2.5.2. Păstrarea şi distrugerea mediilor de păstrare a informațiilor

Mediile pe care păstrează date supuse prelucrării automate a datelor şi cele auxiliare se păstrează în camere speciale.

Documentele ce conțin informații aflate sub un control special se păstrează în seifuri sau în locuri protejate prin sisteme speciale.

Operațiunea de distrugere trebuie să urmeze proceduri speciale. Cea mai bună cale de distrugere este **arderea**, folosită, de regulă, pentru gunoaie informatice adunate în pungi speciale. La operația de distrugere vor participa două persoane, care vor ține un registru special de consemnare a materialelor ce se distrug. Cenuşa trebuie să fie împrăştiată pentru eliminarea oricărei posibilități de reconstituire a datelor distruse.

Transformarea în pastă este posibilă doar pentru reziduurile din hârtie.

Fărâmițarea se aplică pentru hârtie, indigo, bandă magnetică, microfilme. Înaintea acestei operațiuni, în cazul benzilor magnetice trebuie tăiată întreaga rolă. Procedurile internaționale prevăd ca particulele rezultate în urma acestei operații să nu fie mai mari de 1/32inch (0,0125mm). Procedura de fărâmițare se aplică, de obicei, înaintea arderii.

În cazul mediilor magnetice refolosibile, dacă acestea de refolosesc în aceeaşi unitate, noul utilizator trebuie să aibă cel puțin aceeaşi autorizare pe linia accesului la informații ca şi precedentul. Dacă se utilizează în afara unității emitente, vor fi luate măsuri suplimentare şi nu se va declara utilizarea anterioară.

2.6. Clasificarea informațiilor organizațiilor

La nivelul unei organizații, informațiile se încadrează pe mai multe categorii, în acelaşi mod ca şi informațiile naționale. Aceste categorii sunt:

Informații care necesită un control special – sunt acele informații cunoscute ca fiind ***strict secrete***. La nivelul organizației acestea se numesc ***speciale***, şi sunt marcate cu **S**. În această categorie intră informațiile şi materialele a căror dezvăluire ar duce la pierderea a 10% din profitul brut anual.

Informații confidențiale la nivel de unitate, notate cu **C**, şi care corespund informațiilor secrete la nivel național. Această încadrare se atribuie informațiilor şi materialelor a căror compromitere ar duce pa pierderea unui procent din profitul anual net.

Informațiile private, notate cu **P**, cuprind informațiile şi materialele a căror compromitere poate prejudicia statutul unei persoane din unitate sau al corporației.

Informații de uz intern, notate cu **R**, nu fac parte din categoriile anterioare, dar prezintă restricții în utilizare.

Informații publice, sau informații neclasificate, sun notate cu **N**.

La nivel guvernamental, orice informație neîncadrată într-una din categoriile speciale, sub incidența legii accesului liber la informațiile publice, poate fi publicată de orice organ de presă scrisă, video sau audio, sub motivația că "tot ceea ce nu este interzis este permis".

La nivelul organizațiilor private, lucrurile stau invers, doar informațiile care sunt specificate "pentru public" pot fi făcute publice, mergându-se pe principiul "tot ceea ce nu este permis este interzis".

Un tratament special îl au informațiile solicitate de organismele guvernamentale de la unitățile private.

2.6.1. Criterii de clasificare a informațiilor la nivelul organizațiilor

Valoarea – constituie criteriul principal de clasificare. Dacă o informație este valoroasă pentru o organizație sau pentru concurenții ei, atunci ea trebuie să fie clasificată.

Vârsta – conduce la stabilirea unei valori diferențiale. Cu cât vechimea este mai mare, cu atât informațiile pierd din valoare. De regulă, în domeniul apărării, informațiile clasificate se declasifică după un anumit număr de ani.

Uzura morală – ca şi la mijloacele fixe, atunci când informațiile sunt înlocuite de altele noi, sau când în organizație s-au produs modificări radicale, vechea clasificare devine perimată şi va fi înlocuită cu alta.

Asocierea cu persoanele – are influență în procesul de clasificare în funcție de importanța persoanelor care reglementează regimul datelor personale.

2.6.2. Proceduri de clasificare a informațiilor

În procesul de clasificare, trebuie urmăriți anumiți paşi, după o anumită ordine de prioritate, astfel:

- identificarea administratorului/custodelui;
- specificarea criteriilor după care vor fi clasificate şi etichetate informațiile;
- clasificarea datelor după proprietar, care devine subiect supus auditării efectuate de un superior;
- precizarea şi documentarea oricăror excepții de la politicile de securitate;
- precizarea controalelor aplicate fiecărui nivel de clasificare;
- specificarea procedurilor de declasificare a informațiilor sau pentru transferarea custodiei unei alte entități;
- crearea unui program de conştientizare la nivel de organizație despre controalele pe linia clasificării informațiilor.

2.6.3. Roluri şi responsabilități în procesul de clasificare a informațiilor

Principalele roluri în procesul de clasificare le au proprietarul, utilizatorul sau custodele datelor clasificate.

Proprietarul informațiilor poate fi administratorul sau directorul unei organizații. O astfel de persoană răspunde de averile informaționale încredințate. Spre deosebire de custode, proprietarul are responsabilitatea finală a protecției datelor şi răspunde în fața legii în cazul neachitării de această obligație. Cu toate acestea, tendința actuală este de deplasare în afara unității, de externalizare, prin semnarea actelor de custodie.

Printre responsabilitățile unui proprietar se află:

- întreprinde demersuri pentru stabilirea nivelului de clasificare a informațiilor, care înseamnă, de fapt, cerințele organizației de protejare a acestora;
- efectuează verificări periodice ale clasificărilor existente, în vederea adaptării la cerințele organizației;
- deleagă responsabilitatea protejării datelor către un custode specializat şi autorizat.

Custodele informațiilor este cel care prestează un serviciu externalizat organizației, delegându-i-se responsabilitățile pe linia protejării informațiilor. Acest rol este îndeplinit de specialişti în tehnologii informaționale. Dintre obligațiile acestuia, amintim:

- efectuează copii de siguranță periodice şi teste de rutină a validității datelor;
- efectuează restaurări de dare din copiile de siguranță, când este cazul;
- întreține datele înregistrate, în concordanță cu politicile de clasificare a informațiilor.

De multe ori, custodele are şi obligația alcătuirii schemei de clasificare a informațiilor, preluând aceste prerogative de la proprietarul lor.

Utilizatorul. Un utilizator final este considerat orice persoană, operator, angajat, persoană din afară, care foloseşte informațiile. El este considerat consumator de date care are nevoie, zilnic, să acceseze informații pentru a-şi duce la îndeplinire obligațiile de serviciu ce îi revin.

Obligațiile utilizatorilor sunt:

- de a urma întocmai procedurile de funcționare, definite prin politicile de securitate ale organizației, şi să respecte normele publicate privind utilizarea informațiilor;
- să acorde toată atenția menținerii informațiilor în timpul activității prestate, după cum se stipulează în politicile de utilizare a informațiilor emise de organizația proprietară. Ei trebuie să asigure protejarea împotriva accesului neautorizat la informațiile clasificate;
- să folosească resursele informaționale ale firmei numai în scopul urmărit de aceasta, nu şi în scop personal.

3. Controlul accesului în sistemele informatice

3.1. Tipuri de control al accesului în sistem

Controlul accesului în sistem este implementat pentru reducerea riscului la care sunt supuse sistemele şi pentru reducerea eventualelor pierderi. Controlul poate fi preventiv, detectiv sau corectiv.

Controlul preventiv are ca scop preîntâmpinarea apariției unor incidente în sistem. ***Controlul detectiv*** presupune descoperirea unor apariții ciudate în sistem, iar ***controlul corectiv*** este folosit pentru readucerea la normalitate a sistemului după anumite incidente la care a fost expus.

Pentru a putea fi atinse obiectivele enumerate mai sus, controalele pot fi administrative, logice sau tehnice şi fizice.

Controlul administrativ este exercitat prin politici şi proceduri, instruire cu scop de conştientizare, verificări generale, verificări la locul de muncă, verificarea pe timpul concediilor şi o supraveghere exigentă.

Controlul logic sau tehnic cuprinde restricții la accesarea sistemului şi măsuri prin care se asigură protecția informațiilor. Din această categorie fac parte sistemele de criptare, cardurile de acces, listele de control al accesului şi protocoalele de transmisie.

Controlul fizic este reprezentat de gărzile de pază şi protecție, securitatea clădirilor: sisteme de încuiere a uşilor, securizarea camerelor cu servere, protecția cablurilor, separarea atribuțiilor de serviciu, şi nu în ultimul rând realizarea copiilor de siguranță a fişierelor.

Controalele vizează responsabilizarea persoanelor care accesează informații sensibile. Responsabilizarea este înfăptuită prin mecanisme de control al accesului care necesită, la rândul lor, exercitarea funcțiilor de identificare, autentificare şi auditare. Controalele trebuie să fie în deplină concordanță cu politica de securitate a organizației, iar procedurile de asigurare au scopul de a demonstra că prin mecanismele de control se implementează corect politicile de securitate pentru întregul ciclu de viață aş sistemului informațional.

3.1.1. Modele de control al accesului

Controlul accesului de către un subiect asupra unui obiect presupune stabilirea unor reguli de acces. Aceste reguli pot fi clasificate în trei categorii sau modele: controlul obligatoriu al accesului, controlul discreționar al accesului şi controlul nediscreționar al accesului.

Controlul obligatoriu al accesului – în acest caz, autorizarea accesului unui subiect la un obiect depinde de ***etichetă***, care va specifica nivelul de autorizare al subiectului precum şi clasificarea sau senzitivitatea obiectului. Controlul bazat pe reguli de acces este un tip aparte de control obligatoriu al accesului, pentru că el este posibil doar pe bază de reguli şi nu doar pe baza identității subiecților şi obiectelor. (un subiect trebuie să aibă şi dreptul să acceseze un obiect anume).

Controlul discreționar al accesului – în acest caz subiectul are autoritatea în cadrul unor limite bine stabilite, să specifice obiectele care pot fi accesibile. Se poate

folosi o listă de control al accesului al subiecților la obiect. Acest tip de acces este folosit în situații locale, dinamice, în care se lasă la discreția subiecților specificarea tipurilor de resurse permise utilizatorilor să le acceseze.

Când un utilizator, în condiții bine specificate, are dreptul să modifice controlul accesului pentru anumite obiecte, se spună că avem un "control discreționar al accesului direcționat către utilizator". Un control bazat pe identitate este un alt tip de control discreționar al accesului care se bazează pe identitatea unei persoane.

Controlul nediscreționar al accesului – o autoritate centrală stabilește subiecții care pot să aibă acces la anumite obiecte, în funcție de politica de securitate organizațională. Controlul accesului poate să se bazeze pe rolul individual într-o organizație (control bazat pe sarcini). Acest tip de control nu necesită schimbări atunci când un rol va fi jucat de o altă persoană.

3.1.2. Forme combinate de control

Prin combinarea controlului preventiv şi detectiv cu mijloacele celorlalte tipuri de control – administrativ, tehnic (logic) şi fizic – se obțin următoarele combinații:

- preventiv – administrativ;
- preventiv – tehnic;
- preventiv – fizic:
  - detectiv-administrativ;
  - detectiv-tehnic;
- detectiv – fizic.

În figura 3.1 se prezintă schematic aceste perechi.

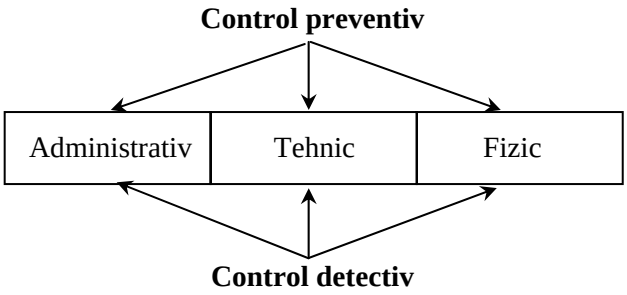


Fig.3.1: Combinarea formelor de control

Controlul preventiv – administrativ

În acest caz accentul se pune pe mecanismele software care contribuie la atingerea obiectivelor controlului accesului. Aceste mecanisme cuprind politicile şi procedurile organizaționale, verificările de fond înainte de angajare, practicile de încetare a contractului de muncă în condiții normale şi anormale, planificarea plecărilor în concediu, etichetarea sau marcarea materialelor speciale, supravegherea mai exigentă, cursuri de instruire în scopul conştientizării importanței securității, conştientizarea modului de comportare precum şi procedurile de semnare a contractului în vederea obținerii accesului la sistemul informațional şi la rețea.

Controlul preventiv – tehnic

Acest tip de control vizează utilizarea tehnologiilor pentru consolidarea politicilor de control al accesului. Controlul tehnic se mai numeşte şi control logic şi poate fi realizat prin sistemele de operare, prin aplicații sau printr-o componentă suplimentară hard/soft. Dintre aceste controale, fac parte: protocoalele, criptarea, cardurile de acces inteligente, biometria, pachetele software pentru realizarea controlului local sau de la distanță, parolele, meniurile , softul de scanare a virușilor etc.

Protocoalele, criptarea şi cardurile inteligente sunt mecanisme tehnice de protejare a informațiilor şi parolelor împotriva eventualelor deconspirări.

Biometria apelează la tehnologii precum amprenta digitală, a retinei, irisului pentru autentificarea solicitanților de accesare a resurselor sistemului.

Pachetele software ce realizează controlul accesului gestionează accesul la resursele ce dețin informații aflate pe plan local sau la distanță.

Controlul preventiv – fizic

Aceste măsuri de control sunt de tip intuitiv. Ele vizează restricționarea accesului fizic în zonele ce conțin informații sensibile ale sistemului. Zonele respective sunt definite printr-un așa zis perimetru de securitate, aflat sub controlul accesului.

În această categorie intră împrejmuirile cu gard, ecusoanele, uşile multiple (după trecerea printr-o uşă, aceasta se blochează automat, iar la următoarea trebuie cunoscut sistemul de deschidere, persoana fiind captivă între două uşi - uşi capcană), sisteme de intrare pe bază de cartelă magnetică, aparatura biometrică pentru identificare, serviciul de pază, sisteme de control al mediului, schița clădirii şi a căilor de acces, locurile special amenajate pentru depozitarea mediilor de stocare a datelor.

Controlul obiectiv – administrativ

În parte, acest tip de control se suprapune peste controlul preventiv-administrativ, pentru că acestea pot fi exercitate cu scopul prevenirii posibilelor încălcări ale politicilor de securitate sau pentru detectarea celor în curs. Din această categorie fac parte procedurile şi politicile de securitate, verificările de fond, planificarea plecărilor în concediu, marcarea sau etichetarea documentelor speciale, instruiri şi cursuri, revizuirea înregistrărilor cu scop de auditare.

Controlul detectiv – fizic

Acest tip de control urmăreşte evidențierea violării politicii de securitate folosind mijloacele tehnice. Aceste măsuri se referă la sistemele de detectare a intruşilor şi la rapoartele privind violările securității, generate automat pe baza informațiilor colectate. Rapoartele pot evidenția abaterile de la funcționarea normală sau să detecteze semnături cunoscute al unor episoade de acces neautorizat. Datorită importanței lor, informațiile folosite în auditare trebuie să fie protejate la cel mai înalt nivel posibil din sistem.

Controlul detectiv – fizic

Acest tip de control necesită intervenția omului pentru evaluarea parametrilor pe care îi oferă senzorii sau camerele video pentru a stabili dacă există un pericol real pentru sistem. În acest caz, controlul se exercită prin camere video, detectoare termice, de fum şi de mişcare.

3.2. Identificarea şi autentificare

În orice sistem de bariere fizice, sistemul de securitate trebuie să discearnă care sunt persoanele autorizate, care sunt vizitatori şi care sunt categoriile neautorizate. Autentificarea poate fi realizată de corpul de pază, de alte persoane care se ocupă de controlarea accesului sau de sisteme automate specializate.

Identificarea şi autentificarea persoanelor se efectuează în patru moduri:

- **ceva aflat în posesia persoanei** – chei, cartele magnetice, cartele speciale, echipamente de identificare personală şi jetoane. Acestea permit un prim pas de accesare a sistemului şi există marele pericol al pierderii lor sau de înstrăinare spre utilizarea de către alte persoane.
- **ceva care individualizează persoana** – această metodă presupune identificarea biometrică, care poate fi dată de: amprenta digitală, a buzelor, semnătura, vocea, forma mâinii, imaginea retinei, venele de pe fața externă a

mâinii, liniile din palmă, imaginea feței etc. Toate aceste tehnici sunt foarte scumpe, în comparație cu cele clasice, şi deseori sunt incomode sau neplăcute la utilizare.

- **ceva ce persoana ştie** – o parolă, doar că aceasta se află la discreția oamenilor şi securitatea sistemului depinde de modul de păstrare a secretului ei sau de uşurința cu care poate fi aflată.
- **locul geografic** – unde este înregistrat calculatorul.

Metodele de control al accesului trebuie să se bazeze pe cel puțin două din cele patru enumerate mai sus, de cele mai multe ori se apelează la combinațiile cartelă-parolă, cheie-parolă, jeton-parolă. În ultimul timp se recomandă să se folosească şi un al treilea elemente – cel biometric.

3.2.1. Principiile de bază ale controlului accesului

Ca principiu general, **simpla posesie a unui element de control al accesului nu trebuie să constituie şi proba accesului privilegiat** la informațiile importante ale firmei, întrucât el poate fi dobândit şi pe căi ilegale dau poate fi contrafăcut.

Un al doilea principiu arată că **atunci când valorile patrimoniale sunt deosebit de importante şi mecanismul de protecție trebuie să fie pe măsură**, iar persoanele cu drept de acces să fie cât mai puține.

Al treilea principiu, de regulă aplicat informațiilor secrete, este acela că **nici unei persoane nu trebuie să i se garanteze accesul permanent, gestiunea sau cunoaşterea informațiilor secrete numai pe motivul poziției ierarhice pe care o deține**.

Fiecare centru de prelucrare automată a datelor cu mai mult de 25 de angajați trebuie să apeleze la sistemul ecusoanelor şi la biometrie, ca măsuri suplimentare față de protecțiile realizate prin alte metode privind accesul în clădire.

Locurile care nu dispun de uşi ce pot fi încuiate trebuie să aibă intrările supravegheate, iar o persoană să răspundă de această operațiune. Cu acelaşi scop, poate fu utilizată şi televiziunea cu circuit închis, cu condiția ca o persoană să nu supravegheze mai mult de trei monitoare.

Controlul accesului prin obiecte

Una din metodele folosite pentru accesul în clădiri sau săli este utilizarea unei cartele de plastic sau a unui jeton, care oferă informații despre purtător, cum ar fi: numele, adresa, codul cardului, contul bancar, informații medicale, drepturi de acces. Toate aceste informații pot fi codificate prin coduri de bară, peliculă magnetică, microprocesor. Unele carduri conțin şi fotografia titularului.

Există şi carduri inteligente care se utilizează pentru criptarea şi decriptarea datelor, semnarea mesajelor şi introducerea de plăți electronice. Aceste carduri controlează accesul în clădire, la locurile de parcare, în săli, la calculator şi la alte date personale ale deținătorului.

Se mai pot folosi şi ecusoane active, care realizează identificarea prin frecvențe radio, sau prun infraroşu, putându-se citi cartele de la câțiva metri.

Majoritatea cartelelor sunt auto-exprinate, cu ajutorul unor tehnologii termice sau a unor vopsele speciale.

Controlul accesului prin biometrie

Principalele elemente ale corpului uman care se folosesc pentru identificarea individului sunt: recunoaşterea feţei, amprenta digitală, recunoaşterea irisului şi recunoaşterea formei mâinii.

În tabelul 3.1 se prezintă o comparaţie a celor patru tehnologii biometrice funcţie de performanţe şi costuri.

Tabelul 3.1

Compararea principalelor tehnologii biometrice

Caracteristici	Recunoaşterea feţei	Amprenta digitală	Recunoaşterea irisului	Forma mâinii
Rata respingerilor eronate	3,3÷70%	0,2÷36%	1,9÷6%	0÷5%
Rata acceptărilor eronate	0,3÷5%	0÷8%	< 1%	0÷2,1%
Timpul pentru o verificare	10 sec	9÷19 sec	12 sec	6÷10 sec
Mărimea probei culese	84÷1300 KB	250÷1000 KB	512 Bytes	9 Bytes
Preţul echipamentelor	Moderat	Mic	Mare	Moderat
Factorii care afectează probele luate	Lumina, orientarea feţei, ochelarii	Murdăria, degetele deshidratate sau accidentele	Vederea slabă, încruntarea, reflexia	Răni, artrită, umflături

Controlul accesului prin parole

Parolele sunt utilizate pentru a permite accesul la un calculator, fie ca utilizator, fie sub forma grupurilor de utilizatori, fie ca personal al sistemului de prelucrare automată a datelor. După identificarea persoanei şi eventual oferirea unei cartele de acces, utilizatorul prezintă sistemului parola proprie, fie prin tastarea la un terminal fie prin introducerea unei cartele care conţine parola. Calculatorul compară parola introdusă cu o listă aprobată şi îi permite sau nu utilizatorului accesul şi îi garantează respectarea drepturilor definite la anumite resurse ale sistemului, drepturi care pot fi:

- execuţie – poate lansa în execuţie un program, dar nu i se permite să umble la configurarea acestuia, prin adăugarea sau modificarea unor linii;
- citire – poate citi un fişier dar nu mai poate realiza nici o altă operaţie;
- scriere – se pot scrie date în acel fişier, dar fără alte drepturi;
- citire-scriere – se poate citi fişierul şi se poate scrie în el;
- adăugare – se pot doar adăuga date la fişier, nu se pot modifica datele introduse şi nici citi;
- ştergere – dă dreptul de a şterge date din fişier.

Oricât de complex ar fi sistemul cu parole, el nu realizează şi o securitate sigură, ea depinzând de modul de păstrare a integrităţii parolei.

Problema principală a parolelor este alegerea nejudicioasă a acestora de către utilizatorii lor, şi anume: numele unor eroi din filme sau basme, al soţiei, a soţului sau a copiilor, numărul de înmatriculare etc., toate vulnerabile în faţa unor spărgători calificaţi. O altă greşeală majoră este notarea parolelor de teama de a nu fi uitate, şi lăsarea acestor notiţe la vedere, astfel încât orice poate vedea parola.

Parolele trebuie să fie eliberate doar persoanelor autorizate şi nu trebuie să fie un proces generalizat dându-se tuturor celor care deţin funcţii de conducere în firmă; ele trebuie date doar celor care lucrează cu datele protejate.

Parolele pot fi create şi de utilizatori pentru datele mai puţin importante, dar există unele probleme des întâlnite, şi anume:

- utilizatorii nu-şi schimbă periodic parolele, iar dacă o fac nu aduc modificări importante în structura lor;
- utilizatorii îşi păstrează parolele scrie pe suporturi lăsate în văzul tuturor;
- utilizatorii folosesc nume asocieri nume-cuvinte cunoscute (nume de persoane dragi) ceea ce le face extrem de vulnerabile.

Dintre cuvintele utilizate în mod eronat de utilizatori drept parolă amintim: PASSWORD, PAROLA, SECRET, SMART, CLEVER, DUMMY, CRAZY, sau chiar GHICI.

Deoarece parolele sunt nişte chei de acces la valorile proprii, trebuie protejate cu grijă, şi trebuie respectate câteva reguli de bază la alegerea lor:

- parolele trebuie schimbate cel puțin odată la şase luni, iar pentru datele deosebit de importante şi mai des;
- parolele comune (utilizate de mai mulți) trebuie schimbate imediat ce o persoană părăseşte grupul sau i se retrage dreptul utilizării ei;
- parolele se vor schimba imediat ce apare bănuiala cunoaşterii ei de către persane neautorizate sau dacă din motive de forță majoră secretul lor a trebuit dezvăluit pentru redresarea unei stări anormale temporare;
- parolele trebuie să fie memorate şi nu scrise pe orice, cu excepția următoarelor cazuri:
  - vor fi scrise pentru situații de urgență;
  - fiecare parolă scrisă va fi introdusă într-un plic sigilat şi marcat în exterior cu scurte detalii privind calculatorul la care poate fi folosită şi numele celor autorizați a le folosi;
  - plicul respectiv are tratament asemănător averilor protejate sau al categoriilor de informații accesate prin parolă. După ruperea sigiliului, pe plic vor fi trecute data şi numele celor care au făcut-o;
  - plicurile cu parole se păstrează de către responsabilul cu securitatea sistemului şi seif.
- dacă parolele duplicat se păstrează prin intermediul calculatorului, astfel de fişiere trebuie să fie protejate împotriva accesului neautorizat şi create copii de siguranță. Accesul la acest fişier trebuie să fie înlesnit doar persoanelor autorizate, respectându-se principiul "niciodată singur". Listele cu parole vor fi memorate sub formă criptată;
- parolele nu vor fi afişate niciodată pe echipamentele din configurația sistemului, iar la introducerea lor nu trebuie să se afle persoane străine în preajmă;
- parolele, în cele mai multe cazuri, au cel puțin opt caractere. Ele sunt caractere alfa numerice, folosite în ordine aleatoare, ceea ce ar însemna câteva mii de cuvinte de opt sau mai puține caractere, care pot fi testate cu ajutorul calculatorului, în doar câteva minute, deci sunt suficient de vulnerabile pentru spărgătorii profesionişti;
- pentru blocarea operațiunilor de încercare repetată, de ordinul miilor, calculatoarele trebuie să permită un număr limitat de încercări de introducere a parolelor, de obicei trei. Dacă limita este depăşită de utilizator, intenția este raportată conducătorului sistemului sau responsabilului cu securitatea. În acest timp trebuie să se blocheze terminalul de la care s-au efectuat prea multe încercări nereuşite. În cazul sistemelor speciale se recomandă şi blocarea sălii sau a locului de unde s-a încercat pătrunderea în sistem prin parole eronate repetate, pentru identificarea persoanei respective.

- odată pătruns în sistem, utilizatorului nu trebuie să i se permită să-şi schimbe identitatea cu care a deschis sesiunea şi nici să nu poată pătrunde în partițiile alocate altor utilizatori;
- dacă un termina funcționează o perioadă lungă de timp, procesul de autentificare trebuie să aibă loc la intervale regulate de timp pentru a se asigura că nu foloseşte altcineva sistemul. Dacă terminalul rămâne neutilizat dar deschis, el trebuie să se închidă automat după un anumit interval de timp (10 minute);
- la deschiderea unei noi sesiuni de lucru, utilizatorului trebuie să i se aducă la cunoştință ultimul timp de accesare a sistemului cu parola respectivă, pentru a verifica dacă altcineva a folosit-o între timp.

Pentru preîntâmpinarea unor aspecte vulnerabile din sistemul de protecție prin parole, se recomandă aplecarea la un sistem special sau la o dovadă de recunoaştere a utilizatorului. Acestea pot fi: o cheie de descuiere a consolei, o cartelă magnetică cu microprocesor. Costul foarte ridicat, reduce utilizarea acestui sistem.

Accesului în sistem prin controlul poziției geografice

Autentificarea pe bază de localizare geografică este o metodă de autentificare a entităților din spațiul cibernetic bazată pe localizarea geodezică (latitudine, longitudine şi altitudine a unui loc geografic bine definit). Acest lucru va avea ca efect delimitarea porțiunii din spațiu cibernetic de unde se declanşează un anumit eveniment.

Această autentificare se face pe baza sistemului GPS şi a unui senzor SSL (senzor al semnăturii locale) aflat în posesia utilizatorului.

Caracteristicile principale ale autentificării geodezice sunt:

- asigură o protecție continuă împotriva celor rău intenționați aflați la distanță;
- semnătura locației poate fi folosită ca un mijloc comun de autentificare;
- prin cunoaşterea poziție unui utilizator, se poate identifica uşor un intrus, dar se pot oferi şi probe că o persoană nu a fost în locația respectivă în momentul săvârşirii unei infracțiuni.

O asemenea protecție este recomandată site-urilor fixe.

Ca dezavantaj al autentificării geodezice se menționează:

- refuzul serviciului (accesului la sistem) în cazul bruierii semnalului sau al furtului senzorului;
- uşurința în localizarea unei persoane în caz de război informațional, de aici rezultă că accesul la datele geodezice trebuie să fie restricționat.

4. Criptografia

4.1. Definiții şi noțiuni de bază

Scopul criptografiei este de a proteja informațiile transmise fără să poată fi citite şi înțelese decât de către persoanele cărora le sunt adresate. Teoretic, persoanele neautorizate le pot citi, însă practic, citirea unei comunicații criptate este doar o problemă de timp – egal cu timpul aferent necesar persoanei neautorizate de a decripta mesajul citit.

Algoritmul criptografic este o procedură pas-cu-pas utilizată pentru cifrarea unui text clar şi descifrarea textelor cifrate.

Cheia sau ***variabila*** de criptare este o informație sau o secvență prin care se controlează cifrarea şi descifrarea mesajului.

Cifrarea este o transformare criptografică a unor caractere sau biți.

Criptograma sau ***textul cifrat*** reprezintă un mesaj neinteligibil

Cifrul bloc se obține prin separarea textului inițial în blocuri de câte **n** caractere fiecare (biți) şi aplicarea unui algoritm şi a unei chei identice, **k**, pentru fiecare bloc.

Codurile sunt o transformare care operează la nivelul cuvintelor sau frazelor.

Criptanaliza este actul obținerii textului clar sau a cheii din textul cifrat, care este folosit pentru obținerea informațiilor necesare acestui scop.

Criptarea înseamnă realizarea formei neinteligibile a unui mesaj pentru a nu fi utilizat de persoanele neautorizate să-l acceseze.

Criptarea end-to-end – în acest caz informațiile criptate sunt transmise din punctul de origine la destinația finală.

Cheie simetrică – atât expeditorul cât şi destinatarul folosesc aceeaşi cheie de criptare.

Cheie asimetrică – expeditorul şi destinatarul folosesc chei de criptare diferite.

Criptarea înlănțuită – mesajul circulă prin mai multe noduri între expeditor şi destinatar. Un nod intermediar primeşte mesajul, îl decriptează cu aceeaşi cheie cu care a fost cripta, îl recriptează cu o altă cheie şi îl trimite la următorul nod unde procesul se repetă până când mesajul ajunge la destinatar.

Criptografia este arta şi ştiința ascunderii semnificației unei comunicări împotriva unor interceptări neautorizate. Cuvântul vine din limba greacă, care înseamnă criere ascunsă: *kryptos graphein*.

Criptologia reuneşte criptografia şi criptanaliza.

Decriptarea este procesul prin care un text cifrat este transformat într-un mesaj inteligibil.

Sistemul de criptare este un set de transformări din spațiul mesajului clar la cel al textului cifrat.

Steganografia este o formă de comunicare secretă prin care se încearcă ascunderea mesajului secret într-o imagine digitală.

Textul clar este forma inteligibilă de prezentare a unui mesaj, astfel încât el să fie accesibil oricui.

4.1.1. Tehnici utilizate în criptografie

În prezent există două tipuri principale de tehnici utilizate în criptografie, şi anume:

- criptografia prin cheie simetrice (chei secrete sau chei private) şi,
- criptografia prin chei asimetrice (chei publice).

În cazul cheii simetrice, atât expeditorul cât şi destinatarul mesajului folosesc o cheie comună secretă. În cazul cheii asimetrice, expeditorul şi destinatarul folosesc în comun o cheie publică şi, individual, câte o cheie privată.

4.1.1.1. Substituția

Cea mai simplă metodă de criptare, prin substituție, este cunoscută în zilele noastre sub denumirea de ***cifrul lui Cezar***, după numele împăratului roman care a inventat-o. În acest cifru, caracterele mesajului şi numărul de repetiții ale cheii sunt însumate laolaltă, modulo 26. În adunarea modulo 26, literelor alfabetului latin, de la A la Z, li se dau valori de la 0 la 25 (vezi tabelul 4.1). Pentru cheie trebuie să se ofere doi parametri:

- D – numărul literelor ce se repetă, reprezentând chei;
- K – cu rol de cheie.

Tabelul 4.1

Corespondența litere-numere																									
Litera	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Număr	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pentru a înțelege modul de funcționare, să presupunem că D=3 şi K = BEC, iar mesajul secret este "PAROLA MEA". Atribuind valori numerice mesajului, din tabelul valorii literelor, avem:

P A R O L A M E A
15 0 17 14 11 0 12 4 0
Valorile numerice ale cheii sunt:
B E C = 1 4 2

După aceste corespondențe, cheia criptată 142 se adaugă literelor mesajului, astfel:

Cheia reperată	1	4	2	1	4	2	1	4	2
Mesajul	15	0	17	14	11	0	12	4	0
Echivalentul numeric al textului criptat	16	4	19	15	15	2	13	8	2
Textul criptat	Q	E	T	P	P	C	N	I	C

Convertirea numerelor în literele aferente alfabetului conduce la textul criptat, aşa cum se vede mai sus: "QETPPC NIC"

În cazul cifrului lui Cezar, D = 1 şi cheia este D (3), adică fiecare literă este înlocuită de a treia literă de după ea din alfabet – literele sunt deplasate la dreapta cu trei poziții, (A cu D, B cu E ş.a.m.d.). Criptând mesajul dat în exemplul anterior cu cifrul lui Cezar, obținem:

Cheia reperată	3	3	3	3	3	3	3	3	3
Mesajul	15	0	17	14	11	0	12	4	0
Echivalentul numeric al textului criptat	18	3	20	17	14	3	15	7	3
Textul criptat	S	D	U	R	O	D	P	H	D

Dacă sumele valorilor cheii şi ale numărului aferent literelor sunt mai mari sau egale cu 26, se determină modulo 26 din sumă, adică rezultatul final este obținut prin scăderea din sumă a numărului 26.

Exemplu:

D=3, K=PIC, mesajul este SECRET, rezultatul va fi:

- valorile numerice atribuie mesajului:

S E C R E T

18 4 2 17 4 19

- valorile numerice ale cheii sunt: P I C = 15 8 2

Cheia reperată	15	8	2	15	8	2			
Mesajul	18	4	2	17	4	19			
Echivalentul numeric al textului criptat	33 (8)	12	4	32 (9)	12	21			
Textul criptat	I	M	E	J	M	V			

Valorile 32 şi 33 nu au echivalent în alfabetul latin, caz în care se calculează modulo 26 din 32 şi 33, rezultând valorile 8 şi 9, iar noul echivalent numeric al textului criptate este 8 12 4 9 12 21, iar textul criptat este: IMEJMV.

Cifrurile de mai sus pot fi descrise prin ecuația generală:

$$\mathbf{C = (M + b) \bmod N}$$

unde:

b = un număr întreg fix;

N = numărul literelor din alfabet (26 pentru alfabetul latin);

M = mesajul textului clar în forma numerică;

C = textul criptat scris în forma numerică.

Cifrul lui Cezar, bazându-se pe substituția simplă sau monoalfabetică este uşor de spart, pentru că un caracter este înlocuit de altul şi această schimbare este valabilă în tot textul, iar analiza frecvențelor de apariție a literelor din textele scrise ne va conduce la caracterele adevărate ale textului.

Cifrurile polimorfice sunt realizate prin apelarea la cifruri bazate pe substituția multiplă. De exemplu, dacă se folosesc trei alfabete pentru substituție, definite de cel ce intenționează să cripteze, prima literă din textul clar este înlocuită cu prima literă din primul alfabet, a doua literă a textului clar este înlocuită cu prima literă din al doilea alfabet, a treia literă a textului clar este înlocuită cu prima literă din al doilea alfabet, a patra literă din textul clar este înlocuită de a doua literă din primul alfabet ş.a.m.d.

4.1.2. Permutarea sau transpoziția

Prin această metodă în loc să se înlocuiască un caracter cu un altul, se înlocuieşte ordinea caracterelor. Astfel, se elimină posibilitatea de descifrare a mesajului prin analiza frecvenței de apariție a caracterelor. Totodată, cheia pentru un asemenea cifru nu este standard, în loc de o listă a substituirilor se va folosi o schemă a ordinii. De exemplu, dacă ordinea într-un cuvânt clar este 1,2,3,4,5, într-un text criptat prin transpoziție ordinea poate fi 5,4,1,2,3. de exemplu, cuvântul **PAROLA** poate fi scris **RALOPA**.

Permutările unui astfel de ciclu acționează într-o matrice bloc, ceea ce înseamnă că va fi o matrice de tip "patul lui Procust", în care tot ceea ce nu încape pe o linie se va alinia în cea următoare ș.a.m.d.

De exemplu mesajul CITESTE SI DA MAI DEPARTE, într-o matrice cu cinci coloane devine:

CITES
TESID
AMAID
EPART
E

În această variantă, citindu-se în ordinea liniilor, mesajul criptat va fi:

CITES TESID AMAID EPART E

Dacă se va lucra la coloane, prin folosirea transpoziției controlate prin chei, rezultă altceva. De exemplu, dacă asupra coloanelor se aplică regula 1,2,3,4,5 = 5,3, 1,4,2 – exemplul anterior devine:

E
AMAID
CITES
EPART
TESID

de unde rezultă că textul criptat şi citit pe linie va fi:

E AMAID CITES EPART TESID

Aceleaşi reguli se pot aplica asupra coloanelor sau asupra liniilor şi coloanelor.

Combinarea transpoziției cu substituția poate să conducă la variante aproape imposibil de spart.

4.1.3. Cifrul lui Vernam

Cifrul lui Vernam constă într-o cheie constituită dintr-un şir se caractere aleatoare nerepetitive. Fiecare literă a cheii se adaugă modulo 26 la o literă a mesajului clar. În această variantă, fiecare literă a cheii se foloseşte o singură dată pentru un singur mesaj şi nu va mai putea fi folosită niciodată. Lungimea şirului de caractere a cheii este egală cu lungimea mesajului. Metoda este foarte utilă pentru criptarea mesajelor scurte.

Exemplu: criptarea mesajului: LA MULTI ANI

Mesaj clar	LAMULTIANI	11	0	12	20	11	19	9	0	13	8
Cheie Vernam	VIDAGTSROL	21	8	3	0	6	19	18	17	14	11
Suma aparentă		32	8	15	20	17	38	27	17	27	19
Modulo 26 din sumă		6	8	15	20	17	12	1	17	1	19
Textul criptat		G	I	P	U	R	M	B	R	B	T

Cifrul carte

Acest tip de cifru apelează la diverse surse, de obicei o carte, pentru a cripta un text. Cheia, cunoscută de expeditor şi destinatar, poate fi formată din pagina cărții şi numărul rândului de pe pagina în care se află textul.

Codurile

Codurile sunt folosite pentru a transmite construcții predefinite din anumite domenii. (cum se foloseau la pagere). De regulă, sunt două rânduri de cărți, una conține semnificația în clar a mesajelor în ordinea alfabetică şi codul corespunzător, cealaltă conține ordinea crescătoare a codurilor şi în dreptul lor semnificația în clar.

4.1.4. Ascunderea informațiilor

Ascunderea informațiilor se practică din cele mai vechi timpuri, iar în zilele noastre mesajele secrete pot fi ascunse în fişiere audio MP3, în fişiere video, imagini sau în instrucțiunile executabile ale unui program.

4.1.4.1. Steganografia

Steganografia este arta ascunderii existenței unui mesaj pe un anumit suport. Termenul vine din cuvintele greceşti ***steganos*** care înseamnă acoperit şi ***graphien*** – a scrie.

Prin Steganografia se exprimă interesul pentru confidențialitate, deoarece scopul ei este de a include mesaje într-un anumit mediu astfel încât să rămână insesizabil.

În prezent, o tehnică frecvent utilizată este ascunderea mesajului printre biții imaginilor digitale. Imaginile sunt reprezentate printr-o formă matriceală de pixeli (picture x elements), însemnând puncte din care se realizează imaginea. O imagine "modestă" poate avea 400×300 pixeli. Fiecare pixel este codificat printr-o secvență de biți care stabileşte culoarea. Cea mai simplă formă de codificare este sistemul RBG (red blue, green) prin 24 de biți, adică câte 8 biți pentru fiecare culoare. Cei 8 biți determină realizarea a 256 de variante, prin combinarea lor rezultă aproximativ 17 milioane de nuanțe de culori. Unora dintre biți li se poate da o altă destinație, pentru a codifica mesaje, fără aă fie afectată semnificativ calitatea imaginii.

Ultimul bit, cel mai din dreapta, nu are un rol semnificativ în stabilirea culorii, el schimbă culoarea cu un spectru, echivalent cu modificarea orei cu o secundă (cât reprezintă o secundă dintr-o oră ?).

Biții succesivi ai mesajului vor fi plasați pe poziția biților cel mai puțin semnificativi ai octeților, fără a fi afectată semnificativ imaginea. Făcând un calcul simplu, pentru o imagine de 400×300 pixeli, fiecare cu câte trei octeți, de la care se pot împrumuta 3 biți, rezultă 400×300×3 = 360.000 biți alocați pentru mesajul nostru secret. Un caracter poate fi scris pe 8 biți, deci 360.000 / 8 = 45.000 de caractere poate avea mesajul nostru.

4.1.4.2. Filigranarea

Un filigran este un model distinct încapsulat într-un document, imagine, video sau audio de către cel care se află la originea datelor. Filigranul poate avea câteva scopuri, printre care:

- indicarea proprietarilor datelor;
- ținerea evidenței copiilor datelor;
- verificarea integrității datelor.

Filigranele folosite în bancnote au scopul de a întări încrederea posesorilor că se află în fața banilor originali şi nu a unora contrafăcuți, scopul fiind de securizare împotriva falsificării. Un filigran poate fi invizibil cu ochiul liber sau insesizabil de ureche, dar există mijloace de detectare şi extragere a lui pentru a se verifica autenticitatea datelor sau sursa lor.

Datele filigranate sunt o funcție a unui identificator şi/sau cheie care este unică pentru autor. Aceste valori sunt necesare pentru detectarea sau extragerea filigranului. Dacă mai multe copii ale datelor sursă au fost filigranate separat, fiecare ele va fi prelucrată cu o cheie proprie, deci fiecare copie are amprenta ei. Prin ținerea evidenței fiecărei chei folosite pentru fiecare beneficiar este uşor de urmărit cine a încălcat drepturile de autor.

Filigranele pot fi de două tipuri: fragile sau solide. Filigranele fragile sunt mai uşor de schimbat, dar sunt folosite doar pentru a vedea dacă datele au fost schimbate, în timp ce filigranele solide rezistă tuturor manipulărilor şi manevrelor la care sunt supuse.

Filigranarea este similară cu steganografia şi se bazează pe tehnici de proiectare apropiate.

În spațiul cibernetic, filigranele sunt folosite pentru stabilirea încălcării drepturilor de autor. Digimarc Technologies[1] are un produs pentru protejarea imaginilor puse de proprietar în site-ul propriu. Deținătorii copyright-ului inserează filigranul lor, folosind PhotoShop de la Adobe, sau un alt editor de imagine care înglobează tehnologia Digimarc. Când receptorul foloseşte acelaşi editor pentru vizualizarea imaginilor va fi afişat simbolul de copyright al autorului. Prin selectarea simbolului se realizează legătura cu Digimarc, de unde vor afla cine este deținătorul dreptului de autor. De asemenea, Digimarc are un motor de căutare, MarcSpider, care caută imagini filigranate furate de la autorii lor.

În domeniul pirateriei muzicii, firma Aris Technologies Inc[2] a realizat aplicația MusiCode, care încapsulează informații sursă (titlul, artistul, compania de înregistrare) în fişierul audio. Softul este folosit pe Internet într-un motor de căutare care combate pirații de melodii.

4.1.4.3. Securitatea în domeniul tipăriturilor

În categoria securizării produselor tipărite intră o gamă largă de produse, printre care , cele mai importante sunt: banii, documente oficiale ale guvernelor, componente de avioane sau calculatoare, până la țigări, băuturi alcoolice sau răcoritoare etc.

[1] www.digimarc.com şi www.digimarc-id.com
[2] www.aris-techni.fr/

Majoritatea produselor de securizare nu au pretenția că vor putea stopa pirateria, sau falsificarea, dar scopul acestora este a dovedi încălcarea unor nome comerciale şi juridice.

Se consideră că în cazul bancnotelor false, există trei nivele de verificare prin care falsurile pot sau nu să treacă. Acestea sunt:

- **nivelul primare de verificare** – realizat de persoanele neinstruite sau cu puțină experiență în actele de vânzare-cumpărare;
- **nivelul secundar de verificare** – exercitat de personal competent şi motivat, operatorii de la ghişeele băncilor sau inspectorii calificați ai produselor industriale marcate cu etichete ți/sau timbre fiscale. Aceştia dispun de echipamente speciale (lămpile cu ultraviolete, creioane cu reactivi chimici, scannere sau PC-uri specializate). Aceste echipamente nu pot fi prea numeroase şi nici prea costisitoare, iar falsificatorii le cunosc capacitățile;
- **nivelul trei de verificare** – efectuat în laboratoarele speciale ale producătorilor de elemente de securitate pentru băncile ce realizează emisiuni monetare. Aceste echipamente sunt foarte scumpe şi destul de rare, dar nu pot da rateuri. Ele se folosesc doar în cazuri speciale.

Documentele speciale, hârtiile de valoare folosesc, de regulă, următoarele produse de tipărire:

- **intaglio** sau **gravura cu acizi** – se utilizează pentru fixarea cu mare forță a cernelii pe hârtie. Aceasta tehnică produce o imprimare în relief cu o mare rezoluție – se utilizează la tipărirea banilor şi a paşapoartelor;
- **literă presată** – cerneala este depusă prin rularea caracterelor în relief şi presarea hârtiei pe care se realizează tipărirea, astfel încât să rămână urmele presării. Tehnica se foloseşte pentru imprimarea numerelor ce indică valoarea bancnotelor.
- **procesarea simultană** – este tehnica prin care cerneala se transferă simultan pe ambele fețe ale bancnotei, ceea ce duce o suprapunere perfectă a tipăririi;
- **ştampilele de cauciuc** – se folosesc pentru andosarea documentelor sau pentru ştampilarea fotografiilor pe documente;
- **gofrarea** şi **laminarea** – adică scrierea în relief şi laminarea se folosesc pentru marcarea caracterelor pe carduri şi fixarea fotografiilor, scumpindu-se astfel costurile contrafacerii. Gofrarea se realizează fie fizic sau cu ajutorul laserului pentru fixarea fotografiilor pe documentele de identificare.
- **filigranele** – sunt zone transparente sau marcate cu materiale speciale pentru protejarea hârtiilor de valoare. Se pot utiliza şi fire fluorescente.

Dintre tehnicile cele mai moderne de securizare a documentelor se enumără:

- **cernelurile schimbătoare optic** – îşi pot schimba culoarea (de la verde la galben) funcție de unghiul sub care este privit documentul. Tehnica se mai numeşte "gât de rățoi" sau "guşă de porumbel".
- **cerneala cu proprietăți magnetice** sau **fotoacustice**
- **imprimarea unor semne vizibile doar cu echipamente speciale** – microtipărirea, tipărirea cu cerneluri ultraviolete, infraroşii sau magnetice.

- **firele sau foile metalice** – fire cu irizări simple, ***hologramele*** (realizată optic şi reprezintă obiecte întregi pe un plan îndepărtat) sau ***kinegramele*** (realizate pe calculator, oferă imagini diferite funcție de unghiul de privire).
- **marca digitală a copyright-ului** – este recunoscută de copiatoare şi scanere, care se opresc la întâlnirea ei, împiedicând reproducerile ilegale.
- **unicitatea** – este asigurată prin dispunere aleatoare de fibră magnetică pe hârtie.

În ceea ce priveşte realizarea elementelor de securitate a elementelor tipărite, trebuie să se țină cont şi de următoarele:

- elementele de securitate trebuie să spună ceva, să fie purtătoare ale unui mesaj reprezentativ pentru produs.
- trebuie să-şi găsească locul potrivit, să se încadreze în mod firesc în ansamblul documentului, astfel încât fixarea în mintea utilizatorului să fie naturală.
- efectul lor trebuie să fie evident, distinct şi inteligibil.
- nu trebuie să intre în concurență cu alte produse realizate cât de cât similar, pentru a nu da curs imitărilor sau confuziilor.
- trebuie să fie standardizate.

În cazul bancnotelor, sunt necesare 20 de elemente de securizare care nu sunt mediatizate. Doar câteva dintre ele sunt aduse la cunoştința inspectorilor de specialitate, dar cu timpul acestea sunt aflate şi de falsificatori. După un timp mai îndelungat se află aproape toate cele 20 de elemente de siguranță, moment în care bancnotele sunt retrase şi sunt înlocuite cu un alt model.

4.2. Sisteme de criptare prin chei simetrice (private)

Acest tip e criptografie apelează la o singură cheie atât la expeditor cât şi la destinatar. Expeditorul (emițătorul) criptează textul clar cu ajutorul unei chei secrete, iar destinatarul (receptorul) îl va decripta cu aceeaşi cheie. Reuşita criptării este dată de secretizarea cheii. Ideal ar fi ca o cheie simetrică să se folosească o singură dată.

Un sistem de criptare prin cheie secretă are în structura sa informație publică şi informație privată.

Informația publică cuprinde:

- un algoritm folosit pentru criptarea textului clar în mesaj criptat;
- posibil, un exemplar al textului clar şi textul criptat corespunzător;
- posibil, o variantă criptată a textului clar care a fost aleasă de către un receptor neintenționat.

Informația privată poate fi:

- cheia sau variabila de criptare;
- o anumită transformare criptografică dintr-o mulțime de transformări posibile.

Succesul sistemului se bazează pe dimensiunea cheii. Dacă are mai mult de 128 biți este una destul de sigură, deci sigură în exploatare. Ea se adaugă la rapiditatea cu care se efectuează criptarea şi volumul mare de date asupra cărora poate opera.

Cele trei caracteristici esențiale ale sistemelor bazate pe chei simetrice sunt:

- siguranță;
- rapiditate;
- volum mare de date criptate.

Singura problemă a sistemului constă în folosirea în comun a cheii de criptare de către emițător şi receptor, ceea ce înseamnă că emițătorul trebuie să folosească o paletă largă de chei pentru o mare diversitate a utilizatorilor. Sistemele bazate pe chei publice nu oferă mecanismele necesare autentificării şi nerepudierii.

4.3. Sisteme de criptare prin chei asimetrice (publice)

Spre deosebire de sistemele de criptare bazate pe chei secrete, care presupun o singură cheie cunoscută de emițător şi receptor, sistemele bazate pe chei publice folosesc două chei: una publică şi una privată.

Cheia publică este pusă la dispoziția oricărei persoane care doreşte să trimită un mesaj criptate;

Cheia privată este utilizată pentru decriptarea mesajului, iar nevoia de a face schimb de chei secrete este eliminată.

Funcționarea sistemului:

- cheia publică nu poate decripta un mesaj criptat;
- se recomandă ca o cheie privată să nu derive dintr-o cheie publică;
- un mesaj care a fost criptat printr-o anumită cheie poate fi decriptat cu altă cheie;
- cheia privată nu este făcută publică.

Criptografia prin chei publice este posibilă în aplicațiile care funcționează într-un singur sens. O funcție în sens unic este aceea care este uşor de calculat într-o direcție, dar dificil de calculat în sens invers.

Pentru o asemenea funcție, **y = f(x)**, este simplu de calculat valoarea lui **y** dacă se ştie **x**, dar este foarte greu s-l determinăm pe **x** dacă-l cunoaştem pe **y** (de ex. cartea telefonică, dacă ştim un număr de telefon, este foarte greu să găsim persoana).

Pentru ca funcțiile cu sens unic să fie utile, ele trebuie să aibă o ***trapă***, adică un mecanism secret care să permită realizarea cu uşurință a funcției inverse, astfel încât să se poată obține **x** dacă se ştie **y**.

În contextul criptografiei bazate pe chei publice este foarte dificil să se calculeze cheia privată din cheia publică dacă nu se ştie trapa.

De-a lungul anilor sa-au dezvoltat mai mulți algoritmi pentru cheile publice. Unii dintre ei se folosesc pentru semnătura digitală, pentru criptare sau în ambele scopuri. Din cauza calculelor numeroase solicitate de criptarea prin chei publice, aceasta este de la 1000 la 10.000 ori mai lentă decât criptarea prin chei secrete, au apărut metode hibride, care folosesc criptografia prin chei publice pentru transmiterea sigură a cheilor secrete utilizate în criptografia prin chei simetrice.

Dintre algoritmii importanți ai cheilor publice, amintim Diffie-Hellman, RSA, El Gamal Knapsak şi curba eliptică,.

4.3.1. Semnătura digitală

Inventarea criptografiei prin chei publice a adus două mutații importante. Prima permite transmiterea unui secret către o altă persoană fără să fie nevoie de o a treia persoană de încredere sau de un canal de comunicație off-line pentru a transmite cheia secretă. A doua mutație s-a produs pe planul calculării semnăturii digitale.

Definiție:

O semnătură digitală este un bloc de date (cifre binare) ce se ataşează unui mesaj sau document pentru a întări încrederea unei alte persoane sau entități, legându-le de un anumit emițător.

Legătura este realizată astfel încât semnătura digitală poate fi verificată de receptor sau de o terță persoană şi nu se poate spune dă a fost uitată. Dacă doar o cifră binară nu corespunde, semnătura va fi respinsă în procesul de validare.

Semnătura digitală stabileşte autenticitatea sursei mesajului.

Dacă o persoană nu-şi divulgă cheia personală privată nimeni nu poate să-i imite semnătura. O semnătura privat nu înseamnă şi recunoaşterea dreptului de proprietate asupra textului transmis, ci ea atestă faptul că persoana semnatară a avut acces la el şi l-a semnat.

Atunci când semnarea este cuplată cu crearea documentului, semnătura digitală poate oferi o probă evidentă a originii documentului. În această categorie intră fotografiile făcute cu camere digitale bazate pe chei private, caz în care proba este de necontestat. Procedeul este folosit când se doreşte realizarea protecției împotriva manipulării imaginilor cu calculatorul. În acelaşi mod pot lucra şi camerele video sau alți senzori care-şi pot semna ieşirea pentru a-i certifica originea.

Deşi semnătura digitală este implementată prin sistemul criptografiei cu chei publice, în cazul acesteia componenta privată este folosită pentru semnarea mesajelor în timp ce componenta publică este folosită pentru a verifica semnătura.

Iată care este mecanismul realizării semnăturii digitale: Dacă (A) vrea să semneze un mesaj, va calcula o valoare rezumat a mesajului, care este determinată printre-o funcție publică de dispersie (hashing). În acest moment nu se folosesc chei. În pasul următor (A) va utiliza o cheie privată pentru semnătură $KS_{Apriv.}$ pentru a calcula o transformare criptografică a valorii rezumat a mesajului. Rezultatul, care este semnătura sa pe mesaj, se ataşează mesajului. Din acest moment, mesajul poate fi transmis unei alte persoane, de exemplu (B), sau poate fi stocat într-un fişier.

Când (B) primeşte mesajul, validează semnătura lui (A) cu ajutorul cheii ei publice pentru semnături KS_{Apubl}, ce va fi folosită ca intrare într-o funcție criptografică prin care se va testa dacă valoarea rezumat determinară de (B) este aceeaşi cu valoarea codificată prin semnătura lui (A). Dacă valoarea coincide, (B) va accepta semnătura. De remarcat că nici o cheie a lui (B) nu a fost utilizată în procesul de validare a semnăturii transmise de (A), ci doar cheile lui (A).

Dacă (A) transmite cheia unui mesaj secret către (B), va folosi doar cheile lui (B).

Dacă (A) doreşte să trimită un mesaj, semnat şi criptat, către B, procesul presupune utilizarea cheilor pentru semnături ale lui A (KS_{Apriv} şi KS_{Apub}), a cheilor lui B de criptare (K_{Bpub}) şi o cheie a mesajului, K. În sinteză, procesul este următorul:

- (A) generează o cheie aleatoare a mesajului, K. (A) criptează mesajul M cu cheia K, obținând mesajul criptat MC;
- (A) criptează cheia K folosind cheia publică a lui (B) de criptare K_{Bpub}, rezultând cheia criptată KC;

- (A) realizează o semnătură S folosind cheia sa privată pentru semnătură KS_{Apriv}.;
- (A) trimite către (B) următoarele: KS, MC şi S;
- (B) foloseşte cheia sa privată de criptare, K_{Bpriv}, pentru a decripta KC şi a obține cheia K;
- (B) foloseşte K pentru decriptarea MC şi obține textul clar M;
- (B) foloseşte cheia publică pentru semnătură a lui (A), KS_{Apub}, pentru validarea semnăturii S.

Tot acest proces este utilizat de procesul de criptare a e-mail-urilor, aşa că (A) şi (B) nu vor efectua manual operațiunile de mai sus, ci le va face calculatorul. Pentru a dispune de aceste servicii este necesară contactarea unor firme specializate, de exemplu Verisign (www.verisign.com). Oricum este necesară obținerea unui ID digital[3].

4.3.2. Sisteme de certificare a cheilor publice

Un sistem criptografic bazat pe chei publice poate fi compromis de o persoană (A) care transmite o cheie publică altei persoane (B) către un alt partener (C). În acest caz (C) va folosi cheia publică a lui (B) pentru a cripta mesajul, cu intenția de a ajunge înapoi la (B), numai că (A), folosindu-şi propria cheie privată, va face ca receptorul să fie el, reuşind astfel să decripteze mesajul care era adresat lui (B).

Pentru a evita o astfel de ciudățenie, se recurge la procesul certificării, prin care persoanele sunt legate de cheile lor publice. Documentul oferit de o "Autoritate de Certificare" acționează ca orice alt emis de un notar şi se efectuează după aceleaşi reguli, adică pe baza verificării identității persoanei solicitante, concretizându-se prin atribuirea unei chei publice pentru persoana respectivă. Unitatea de certificare semnează certificatul cu propria cheie privată. Din această cauză, persoana este verificată ca emițător dacă este necesară cheia ei publică pentru deschiderea sesiunii de transmitere a mesajelor criptate şi/sau a semnăturilor electronice. Certificatul conține numele subiectului, cheia lui publică, numele autorității de certificare, perioada de valabilitate a certificatului. Pentru a verifica semnătura autorității de certificare, cheia ei publică trebuie să fie verificată încrucişat cu o altă autoritate de certificare.

Certificatele sunt păstrate într-un Registru, alături de lista certificatelor revocate. În principiu, operațiile pentru obținerea certificatelor digitale şi validarea tranzacțiilor sunt redate în figura 4.1:

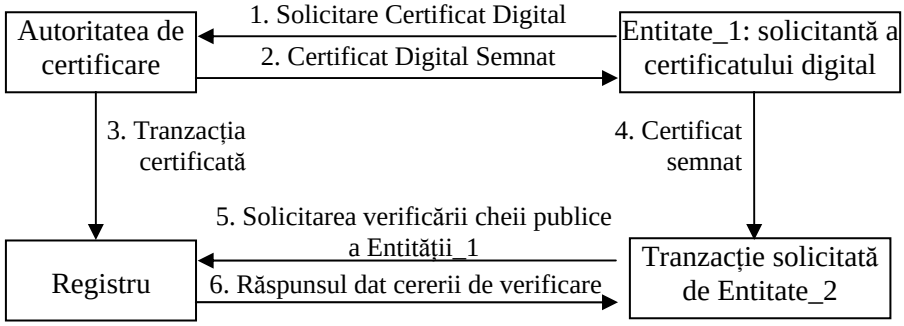


Fig. 4.1: Prezentarea unei tranzacții cu certificate digitale.

[3] cadrul legal de utilizare a semnăturii electronice în România se găseşte la www.legi-internet.ro/lgsemel.htm

4.3.3. Infrastructura cheilor publice (PKI)

Infrastructura cheilor publice (PKI – Public Key Infrastructure) își propune să rezolve probleme manageriale din domeniul cheilor publice, integrând semnături şi certificate digitale cu o mare diversitate de alte servicii specifice comerțului electronic, prin care se solicită oferirea integrității, controlului accesului, confidențialității, autentificării şi a nerepudierii tranzacțiilor electronice.

Infrastructura cheilor publice cuprinde certificatele digitale, autoritățile de certificare, autoritățile de înregistrare, politici şi proceduri cu chei publice, revocarea certificatelor, nerepudierea, marcarea timpului, certificarea încrucişată, aplicații de securitate, LDAP (Lightweight Directory Acces Protocol).

Certificatele cheilor publice pot fi eliberate în regim on-line sau off-line. În sistem off-line, o persoană trebuie să se legitimeze cu un act de identitate. În varianta on-line, certificatele se pot oferi ca răspuns al unei cereri formulate prin e-mail sau direct de pe un site specializat.

Compania Verising oferă trei clase de certificate personale, numite ID digital, toate legate de e-mail:

- **clasa 1 de certificate** – verifică adresa de e-mail a utilizatorului, fără să solicite alte elemente de autentificare. După exprimarea interesului pentru un certificat, sistemul trimite o confirmare cu un PIN pe adresa de e-amil a persoanei. Utilizatorul se întoarce la site-ul anterior (al companiei) şi oferă PIN-ul, după care este generat un ID digital şi se memorează în calculatorul utilizatorului.
- **clasa 2 de certificare** – cere utilizatorului să mai introducă şi Social Security Number, adresa şi seria carnetului de şofer;
- **clasa 3 de certificare** – este destinată companiilor ce publică software, oferindu-le un grad mult mai mare de securitate, dar există şi o variantă pentru persoane fizice ocupate cu transferuri bancare şi contracte.

5. Modele şi programe de securitate

5.1. Modele de securitate multinivel

Din punct de vedere al securității, un sistem este divizat în straturi, prin linii orizontale, realizându-se așa-zisa securitate pe nivele multiple (multinivel) prin care se realizează o delimitare netă între diferite categorii de informații din sistem (publice, confidențiale, secrete, strict secrete). Această delimitare asigură certitudinea accesării informațiilor dintr-o anumită clasificare numai de persoanele care au autorizația de acelaşi nivel (sau mai mare) cu clasificarea informațiilor accesate. Schematic, sistemul multinivel poate fi reprezentat ca în figura 5.1.

Politicile de controlare a accesului sunt foarte clare: o persoană poate accesa un document numai dacă autorizarea sa este cel puțin egală cu nivelul de clasificare al informației citite. Ca efect, *informațiile vor circula doar de jos în sus*, de la nivelul CONFIDENȚIAL, la SECRET, STRICT SECRET ş.a., iar de sus în jos nu au voie să circule decât dacă o persoană autorizată le declasifică.

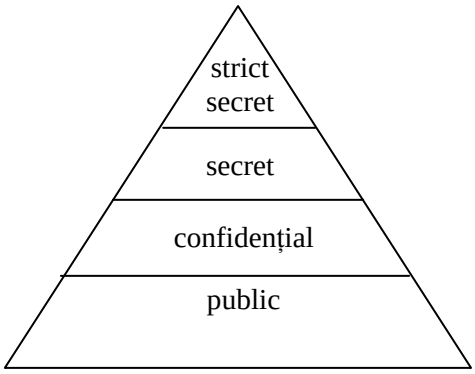


Fig. 5.1: Modelul de securitate multinivel

5.1.1. Modelul Bell-LaPadula

Unul din cele mai cunoscute modele al politicilor de securitate este cel propus de David Bell şi Len LaPadula, în 1973, şi este cunoscut sub numele *Bell-LaPadula* sau *modelul de securitate multinivel*. Sistemele ce le adoptă sunt numite şi „sigure multinivel" sau MLS (*MultiLevel Secure*). Proprietatea de bază a acestor sisteme este aceea că *informațiile pot circula în jos*.

Formal, modelul Bell-LaPadula a introdus trei principii:

- *principiul* (sau proprietatea) *securității simple*, prin care nu-i este permis nici unui proces să citească date aflate pe un nivel superior lui. Este cunoscut şi ca *Nu citi deasupra (No Read Up, NRU)*;
- *principiul* * (se citeşte stea): nici un proces nu poate să scrie date pe un nivel aflat sub el. Este cunoscut şi ca *Nu scrie dedesubt* (*No Write Down, NWD*);
- *principiul securității discreționare* introduce o matrice de acces pentru a specifica controlul accesului discreționar. Este cunoscut şi ca *Trusted Subject* (subiect de încredere). Prin acest principiu, subiectul de încredere violează principiul *, dar nu se abate de la scopul său. Cele trei principii sunt redate în figura 5.2.

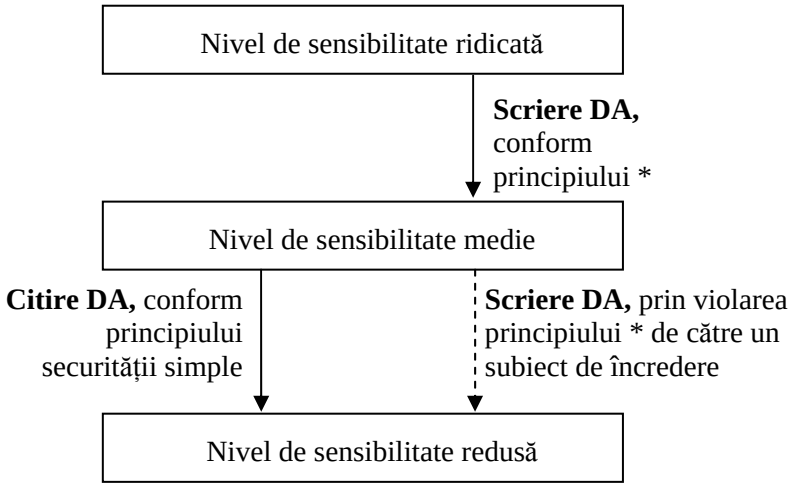


Fig. 5.2: Modelul Bell-LaPadula, cu cele trei principii

5.1.2. Modelul matricei de control al accesului

Printr-o matrice de acces se oferă drepturi de acces pentru *subiecte de încredere* la obiectele sistemului. Drepturile de acces sunt de tipul *citeşte*, *scrie*, *execută* ş.a. Un *subiect de încredere* este o entitate activă care îşi caută drepturile de acces la resurse sau obiecte. Subiectul poate fi o persoană, un program sau un proces. Un *obiect* este o entitate pasivă, cum sunt fişierele sau o resursă de stocare. Sunt cazuri în care un element poate fi, într-un anumit context, subiect şi, în alt context, poate fi obiect. Un exemplu de matrice de acces este redată în figura 5.3.

Coloanele se numesc **Liste de control al accesului**, iar liniile, **Liste de competențe**. Modelul matricei de control al accesului acceptă controlul discreționar al accesului pentru că intrările în matrice sunt la discreția persoanelor care au autorizația de a completa tabelul.

În matricea de control al accesului, competențele unui subiect sunt definite prin tripleta (*obiect, drepturi, număr aleator*).

Obiecte / Subiecte	**Fişier_1**	**Proces_1**	**Fişier_2**	**Fişier_3**
Subiect_1	Citeşte/scrie	Execută	Citeşte	Scrie
Subiect_2	Scrie	Execută	Nimic	Citeşte
Subiect_3	Citeşte/scrie	Execută	Citeşte/scrie	Nimic
Subiect_4	Scrie	Nimic	Scrie	Scrie

Fig. 5.3: Matrice de control al accesului.

5.1.3. Modelul Biba

În multe cărți, este amintit şi modelul Biba, al lui Ken Biba, ocupându-se doar de integritatea sistemelor, nu şi de confidențialitate. El se bazează pe observația că în multe cazuri confidenţialitatea şi integritatea sunt concepte duale: în timp ce prin confidențialitate se impun restricții celor ce pot citi un mesaj, prin integritate sunt controlați cei ce pot să scrie sau să modifice un mesaj.

În unele organizații guvernamentale sau comerciale există aplicații în care integritatea datelor este mult mai importantă decât confidențialitatea, ceea ce a făcut să apară modele formale ale integrității.

Integritatea vizează trei scopuri principale:

- protejarea datelor împotriva modificărilor efectuate de utilizatorii neautorizați;
- protejarea datelor împotriva modificărilor neautorizate efectuate de utilizatori autorizați;
- asigurarea consistenței interne şi externe a datelor.

Modelul a fost realizat în 1977 ca unul al integrității datelor, aşa cum modelul Bell-LaPadula este cunoscut ca modelul confidențialității datelor. Modelul Biba este unul de tip rețea şi foloseşte *relația mai mic sau egal*. O structură a rețelei este definită ca un ansamblu parțial ordonat cu cea mai mică limită superioară, LUB (*Least Upper Bound*), şi cea mai mare limită inferioară, GLB (*Greatest Lower Bound*).

O rețea reprezintă un ansamblu de clase de integritate (CI) şi de relații ordonate între aceste clase. Ea poate fi definită astfel:

(CI <= LUB, GLB).

Aşa cum Bell-LaPadula operează cu niveluri diferite de sensibilitate, modelul Biba clasifică obiectele în diferite niveluri de integritate. Modelul enunță trei axiome ale integrității:

- **axioma integrității simple.** Ea stabileşte că unui subiect aflat pe un anumit nivel de integritate nu-i este permis să observe (citească) un obiect de o integritate mai joasă (*No Read Down*, *Nu citi dedesubt*).
- **axioma integrității *** (se citeşte stea) stabileşte că unui obiect situat pe un anumit nivel de integritate nu-i este permis să modifice (scrie) alt obiect situat pe un nivel mai înalt de integritate (*No Write Up*, *Nu scrie deasupra)*;
- **un subiect de pe un anumit nivel de integritate nu poate solicita un subiect situat pe un nivel de integritate superior.**

Axiomele şi modelul Biba sunt redate în figura 5.4.

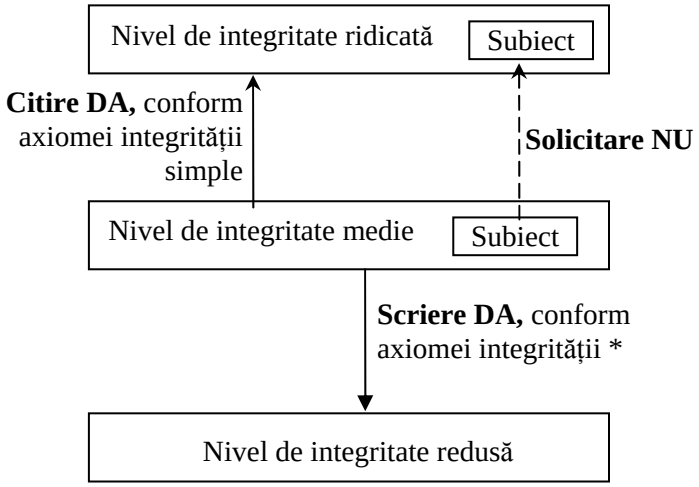


Fig.5.4 : Modelul Biba

În practică au fost implementate mai multe tipuri de sisteme de securitate multinivel, cum sunt SCOMP, Blocker, MLS Unixe, CMWs, NRL Pump, MLS Logistics, Purple Penelope ş.a.

5.2. Modele ale securității multilaterale

Deseori, în realitate, preocupările noastre s-au concentrat nu către prevenirea curgerii **în jos** a informațiilor, ci către stoparea fluxurilor **între** diferite compartimente. În astfel de sisteme, în locul frontierelor orizontale, aşa cum recomandă modelul Bell-LaPadula, s-au creat altele verticale, conform figurii 5.5.

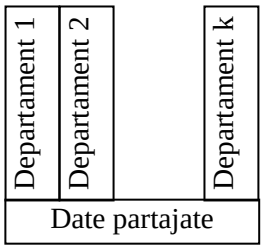


Fig. 5.5: Modelul securității multilaterale

Acest control al fluxurilor informaționale laterale este unul organizațional, aşa cum este cel al organizațiilor secrete, pentru păstrarea în taină a numelor agenților care lucrează în alte țări, fără să fie cunoscuți de alte departamente speciale. La fel se întâmplă şi în companii, unde separarea verticală a compartimentelor, după funcțiile îndeplinite (producție, comercială, personal-salarizare ş.a.), conduce la o situație identică.

Există cel puțin trei modele diferite de implementare a controlului accesului şi de control al fluxurilor informaționale prin **modelul securității multilaterale**. Acestea sunt:

- **compartimentarea**, folosită de comunitatea serviciilor secrete;
- **zidul chinezesc,** folosit la descrierea mecanismelor utilizate pentru prevenirea conflictelor de interese în practicile profesionale;
- **BMA** (*British Medical Association*), dezvoltat pentru descrierea fluxurilor informaționale din domeniul sănătății, conform cu etica medicală.

Compartimentarea şi modelul rețea

Ani mulți acest model a servit ca practică standard, în SUA şi guvernele aliate, pentru restricționarea accesului la informații, prin folosirea cuvintelor-cod şi a clasificărilor. Este arhicunoscut cuvântul-cod *Ultra*, folosit în cel de-al doilea război mondial, de către englezi şi americani, pentru decriptarea mesajelor criptate de germani cu maşina Enigma. Cercul persoanelor cu acces la mesajele decriptate fiind foarte redus, numărul autorizărilor pentru informații de pe cel mai înalt nivel de clasificare era mult mai mare. Prin folosirea cuvintelor-cod se creează o puternică subcompartimentare, chiar a categoriei strict secret şi deasupra ei.

Cuvintele-cod sunt folosite pentru crearea grupurilor de control al accesului printr-o variantă a modelului Bell-LaPadula, numită *modelul rețea*. Clasificările, împreună cu cuvintele-cod, formează o rețea, conform figurii 5.6. Potrivit modelului, o persoană autorizată să aibă acces la informații SECRETE nu poate accesa informații SECRETE CRIPTO, dacă nu are şi autorizație pentru CRIPTO.

Ca un sistem să răspundă acestor cerințe, va trebui ca problemele clasificării informațiilor, ale autorizării persoanelor şi ale etichetelor ce însoțesc informațiile să se transfere în politica de securitate pentru a defini țintele securității, modul de implementare şi evaluare.

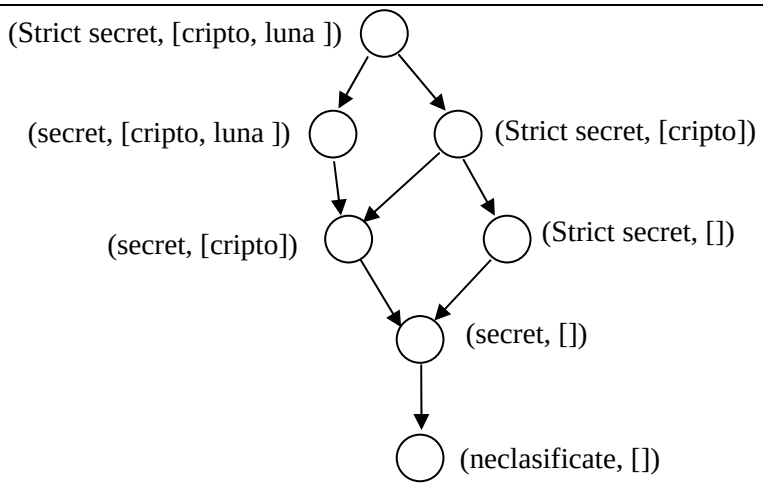


Fig. 5.6: Model rețea cu etichete de securitate.

Modelul zidului chinezesc

Modelul a fost realizat de Brewer şi Nash. Numele provine de la faptul că firmele care prestează servicii financiare, cum sunt băncile de investiții, au normele lor interne pentru a preveni conflictul de interese, norme numite de autori zidul chinezesc. Aria de aplicare este, însă, mai largă. Se poate spune că toate firmele prestatoare de servicii au clienții lor şi pentru a-i păstra se află într-o veritabilă competiție. O regulă tipică este următoarea: „un partener care a lucrat recent pentru o companie dintr-un anumit domeniu de activitate nu poate să aibă acces la documentele companiilor din acel domeniu", cel puțin pentru o perioadă controlată de timp. Prin aceasta, caracteristica modelului zidului chinezesc constă într-un *mix de libertate de opțiune şi de control obligatoriu al accesului*: *oricine este liber să lucreze la orice companie, dar îndată ce a optat pentru una, se supune restricțiilor ce operează în domeniul respectiv de activitate*.

Modelul zidului chinezesc introduce *principiul separării obligațiilor de serviciu*: un utilizator anume poate să prelucreze tranzacțiile A sau B, nu amândouă. Aşadar, putem spune că modelul zidului chinezesc aduce elemente noi pe linia controlării accesului.

Modelul BMA (British Medical Association)

În domeniul medical sunt confruntări serioase privind tocmai sistemele de securitate a datelor pacienților. În efortul multor țări de a introduce carduri inteligente cu datele medicale personale, se înregistrează o puternică opoziție din partea publicului. Acesta invocă vulnerabilitatea individului prin trecerea informațiilor despre anumite boli foarte grave, purtate până acum pe brățara de la mână, pe cartela inteligentă, ceea ce va face ca atunci când se va afla în avion, în țări străine, să fie foarte greu sau chiar imposibil să i se citească informațiile respective. O altă problemă se referă la păstrarea secretului datelor personale sau a unei părți dintre acestea.

Cea mai mare temere vine din cauza proliferării practicilor de **inginerie socială**, putându-se afla cu multă uşurință date personale din baze de date medicale.

Scopul modelului politicii de securitate BMA este acela de consolidare a *principiului consimțământului pacientului* şi de a preveni accesul prea multor persoane la datele personale din bazele de date ce le conțin. Totul s-a rezumat la un nou sistem de codificare. Politica BMA se bazează pe nouă principii, formulate foarte pe scurt astfel:

- controlul accesului,
- deschiderea înregistrărilor, c
- ontrolul modificărilor din liste,
- consimțământul şi notificarea clientului,
- persistența,
- marcarea accesului pentru a servi ca probă în justiție,
- urmărirea fluxului informațiilor,
- controlul agregării informațiilor,
- încrederea în sistemele informatice.

Unii autori susțin că politicile de securitate deseori înseamnă un abuz de mijloace pur manageriale, neglijându-se trei termeni preciși, utilizați pentru descrierea specificațiilor tehnice ale cerințelor sistemelor de securitate, prezentați în continuare.

Modelul politicii de securitate este o declarație succintă a proprietăților sau principiilor securității, ca un sistem sau ca un tip generic de sistem. Punctele sale esențiale pot fi consemnate în scris, pe cel mult o pagină, iar documentul respectiv prevede scopurile protecției unui sistem, agreate de întreaga comunitate sau de linia managerială a clienților. Un astfel de model constituie baza de pornire a analizelor formale matematice.

Ținta securității este o descriere mult mai detaliată a mecanismelor de protecție oferite de o anumită variantă de implementare, precum şi a modului în care ele concură la atingerea obiectivelor de control ale sistemului. Ținta securității formează baza testării şi evaluării produsului implementat.

Profilul protecției, ca şi ținta securității, exprimă o cale independentă de implementare, care să permită evaluări comparative ale produselor sau versiunilor lor.

5.3. Programul de securitate

Programul de securitate al unei companii trebuie să se supună unor elemente constitutive, şi anume: efectuarea structurării programului de securitate, definirea politicilor de securitate, a standardelor, normelor şi a procedurilor.

Fără politici riguroase, programele de securitate vor fi aproape fără suport, ineficiente şi nu se vor alinia strategiei şi obiectivelor organizației. Politicile, standardele, normele şi procedurile constituie fundația programului de securitate al organizației. Politicile eficiente, clar formulate, vor servi proceselor de auditare şi eventualelor litigii. Combinând elementele specificate, o entitate poate implementa controale specifice, procese, programe de conştientizare şi multe altele, tocmai pentru a-i aduce un plus de linişte. Spune românul: paza bună trece primejdia rea.

5.3.1. Politicile de securitate

Atunci când ne referim la securitate informațională, noțiunea de politică de securitate poate avea mai multe înțelesuri, iată câteva dintre ele:

- politica de firewall-uri, utilizate pentru controlarea accesului şi a traseelor pe care circulă informațiile;
- lacătele, cardurile de acces, camerele de luat vederi ce înregistrează totul din perimetrele controlate.

La implementarea politicilor de securitate, trebuie pornit de la vârful piramidei manageriale, unde se află *top managerii*. Aceştia au misiunea de a formula *Declarația politicii organizației*. Aceasta este o formulare generală, o declarație din care să reiasă:

- importanța resurselor informaționale pentru atingerea obiectivelor strategice ale organizației;
- formularea clară a sprijinului acordat tehnologiilor informaționale în unitate;
- angajamentul top managerilor de a autoriza sau coordona activitățile de definire a standardelor, procedurilor şi normelor de securitate de pe nivelurile inferioare.

În afara declarației politicii de securitate la nivelul top managerilor, există şi politici obligatorii, politici recomandate şi politici informative.

Politicile obligatorii sunt politici de securitate pe care organizațiile sunt obligate să le implementeze ca efect al acordurilor, regulamentelor sau al altor prevederi legale. De regulă, aici se încadrează instituțiile financiare, serviciile publice sau orice alt tip de organizație care serveşte interesului public. Aceste politici sunt foarte detaliate şi au elemente specifice, în funcție de domeniul de aplicare.

De regulă, politicile obligatorii au două scopuri de bază:

- asigurarea că o organizație urmează procedurile standard sau politicile de bază din domeniul ei de activitate;
- de a oferi încredere organizațiilor că ele urmează standardele şi politicile de securitate din domeniul de activitate.

Politicile recomandate, prin definiție, nu sunt obligatorii, dar sunt puternic susținute, cu prezentarea consecințelor foarte dure în cazul înregistrării eşecurilor. O organizație este direct interesată ca toți angajații ei să considere aceste politici ca fiind obligatorii. Cele mai multe politici se încadrează în această categorie. Ele sunt foarte clar formulate la toate nivelurile. Cei mai mulți angajați vor fi riguros controlați prin astfel de politici, definindu-le rolurile şi responsabilitățile în organizație.

Politicile informative au scopul de a informa cititorii. Nu poate fi vorba de cerințe specifice, iar interesații de aceste politici pot să se afle în interiorul organizației sau printre partenerii ei.

Elementelor comune tuturor politicilor de securitate, astfel:

- ***domeniul de aplicare***: declararea domeniului de aplicare înseamnă prezentarea intenției vizate de politică şi ea va scoate în relief şi legăturile existente cu întreaga documentație a organizației. Formularea trebuie să fie scurtă şi se plasează la începutul documentului;
- ***declararea politicii top managerilor*** se include la începutul documentului şi are dimensiunea unui singur paragraf, specificând scopul global al politicii;
- ***responsabilitățile*** constituie conținutul unei secțiuni distincte şi cuprind persoanele implicate în asigurarea bunei funcționări a politicii;
- ***consecințele***: printr-o astfel de formulare se prezintă pierderile posibile dacă politica nu va fi respectată;
- ***monitorizarea***: se specifică modul în care se monitorizează respectarea şi actualizarea continuă a politicii;
- ***excepțiile***: se menționează cazurile în care apar excepții şi modalitățile de tratare a lor; de regulă, au o durată limitată de aplicare, de la un caz la altul.

5.3.2. Standardele, normele şi procedurile de securitate

Pe nivelul inferior politicilor se află trei elemente de implementare a politicii: standardele, normele şi procedurile. Ele conţin detaliile politicii, cum ar fi posibilităţile de implementare, ce standarde şi proceduri să fie întrebuinţate. Ele sunt făcute publice la nivel de organizaţie, prin manuale, Intranet, cărţi, cursuri ş.a.

De cele mai multe ori, standardele, normele şi procedurile sunt tratate laolaltă, dar nu este cea mai inspirată idee, fiindcă tratarea separată a lor este justificată de următoarele argumente:

- fiecare dintre ele serveşte unei funcţii diferite şi are propria audienţă; chiar şi distribuţia lor fizică este mai lejeră;
- controalele securităţii pe linia confidenţialităţii sunt diferite pentru fiecare tip de politică;
- actualizarea şi întreţinerea politicii ar deveni mai anevoioase, prin prisma volumului documentaţiei, dacă s-ar trata nediferenţiat.

Standardele

Standardele specifică utilizarea anumitor tehnologii, într-o viziune uniformă. De regulă, standardele sunt obligatorii şi sunt implementate la nivel de unitate, tocmai pentru asigurarea uniformităţii. Elementele principale ale unui standard de securitate informaţională sunt:

- ***scopul şi aria de aplicare,*** prin care se oferă o descriere a intenţiei standardului (realizarea unui tip de server pe o anumită platformă);
- ***roluri şi responsabilităţi*** la nivel de corporaţie pe linia definirii, execuţiei şi promovării standardului;
- ***standardele cadrului de bază,*** prin care sunt prezentate declaraţiile de pe cel mai înalt nivel, aplicabile platformelor şi aplicaţiilor;
- ***standardele tehnologiei*** conţin declaraţiile şi descrierile aferente (configuraţia sistemului sau serviciile nesolicitate de sistem);
- ***standardele administrării*** reglementează administrarea iniţială şi în timpul exploatării platformei şi aplicaţiilor.

Normele

Normele sunt oarecum asemănătoare standardelor, referindu-se la metodologiile sistemelor securizate, numai că ele sunt acţiuni recomandate, nu obligatorii. Sunt mult mai flexibile decât standardele şi iau în considerare naturile diverse ale sistemelor informaţionale. Ele specifică modalităţile de dezvoltare a standardelor sau garantează aderenţa la principiile generale ale securităţii.

Elementele principale ale unei norme de securitate informaţională sunt:

- ***scopul şi aria de aplicare***, descriindu-se intenţia urmărită prin regula respectivă;
- ***roluri şi responsabilităţi*** pe linia definirii, execuţiei şi promovării normei;
- ***declaraţii de orientare*****:** este un proces pas-cu-pas de promovare a tehnologiilor respective;
- ***declaraţii de exploatare***: se definesc obligaţiile zilnice, săptămânale sau lunare pentru o corectă exploatare a tehnologiei respective.

Procedurile

Procedurile prezintă paşii detaliaţi ce trebuie să fie parcurşi pentru execuţia unei activităţi. Se descriu acţiunile concrete pe care trebuie să le efectueze personalul. Prin

ele se oferă cele mai mici detalii pentru implementarea politicilor, standardelor şi normelor. Uneori se foloseşte în locul acestui concept cel de *practici*.

5.3.3. Aspecte practice ale politicii de securitate informațională

Realizarea propriei politici de securitate presupune acoperirea mai multor domenii diferite, iar conform standardului internațional de definire a politicii de securitate, ISO 17799, acestea sunt:

1. Planificarea funcționării neîntrerupte a unității, cu obiectivul contracarării întreruperilor de activitate ale unității şi ale proceselor principale ca efect al unor accidente majore sau dezastre.
2. Controlul accesului în sistem, cu obiectivele:
   a. controlarea accesului la informații;
   b. prevenirea accesului neautorizat în sistemul informațional;
   c. asigurarea protecției serviciilor prestate în rețea;
   d. prevenirea accesului neautorizat la calculatoare;
   e. detectarea activităților neautorizate;
   f. asigurarea securității informațiilor când se folosesc comunicațiile mobile şi tele-activitățile.
3. Dezvoltarea şi întreținerea sistemului, cu obiectivele:
   a. asigurarea securității prin sistemul operațional;
   b. prevenirea pierderilor, modificărilor sau folosirii inadecvate a datelor din aplicațiile sistemului;
   c. protejarea confidențialității, integrității şi autenticității informațiilor;
   d. asigurarea că proiectele informatice şi activitățile colaterale se derulează după proceduri sigure;
   e. menținerea securității softului şi datelor din aplicațiile sistemului.
4. Securitatea fizică şi a mediului, cu obiectivele:
   a. prevenirea accesului neautorizat, a distrugerilor şi interferențelor cu informațiile şi celelalte componente ale sistemului;
   b. prevenirea pierderilor, distrugerilor sau compromiterilor valorilor patrimoniale, precum şi stoparea întreruperilor de activitate;
   c. prevenirea compromiterii sau furtului de informații şi al altor resurse informaționale.
5. *Maleabilitatea*, cu obiectivele:
   a. preîntâmpinarea încălcării cadrului juridic, a celui statutar, regulamentar sau a oricărei obligații contractuale, precum şi a cerințelor pe linia securității;
   b. asigurarea maleabilității sistemului la politicile şi standardele organizaționale pe linia securității;
   c. maximizarea eficienței procesului de auditare a sistemului şi minimizarea interferențelor cu acesta.
6. *Securitatea personalului*, cu obiectivele:
   a. diminuarea riscurilor provocate de factorul uman, fraudă sau folosirea ilegală a componentelor sistemului;
   b. asigurarea că utilizatorii sunt conştienți şi preocupați de preîntâmpinarea sau diminuarea amenințărilor asupra securității informațiilor, susținând politica de securitate a organizației prin tot ceea ce fac zi de zi;
   c. minimizarea pagubelor provocate de incidentele apărute în sistem sau de proasta funcționare a acestuia, precum şi reținerea incidentelor ca lecții

pentru viitor.

7. *Organizarea securității*, cu obiectivele:
   a. asigurarea managementului securității informaționale în cadrul organizației;
   b. asigurarea securității componentelor folosite în prelucrarea informațiilor organizației accesate de către terți;
   c. asigurarea securității informațiilor când responsabilitatea prelucrării acestora revine unei alte organizații, ca serviciu externalizat.
8. *Managementul resurselor informatice şi al exploatării lor*, cu obiectivele:
   a. asigurarea funcționării corecte şi sigure a componentelor sistemului informatic;
   b. minimizarea riscului căderii sistemului;
   c. protejarea integrității softului şi a informațiilor;
   d. asigurarea integrității şi disponibilității informațiilor prelucrate şi comunicate;
   e. asigurarea încrederii în informațiile din rețele şi protejarea infrastructurii corespunzătoare;
   f. prevenirea pierderilor de valori patrimoniale şi a întreruperilor de activitate;
   g. prevenirea pierderilor, modificărilor sau utilizărilor ilegale în schimburile de informații cu alte organizații.
9. *Clasificarea şi controlarea valorilor patrimoniale*, cu obiectivele:
   a. menținerea unei protecții corespunzătoare a valorilor patrimoniale ale organizației;
   b. oferirea încrederii că valorile patrimoniale informaționale au asigurat un nivel de protecție corespunzător .
10. *Politica de securitate*, cu obiectivele:
    a. oferirea de direcții manageriale;
    b. sprijinirea acțiunilor întreprinse pe planul securității informaționale. Fiecare dintre cele zece secțiuni are în structură descrieri detaliate prin care se defineşte standardul ISO 17799.

5.3.4. Exemple de politici de securitate

De remarcat că nu există două organizații care să aibă politici de securitate identice. Din analizarea mai multor politici de securitate se poate realiza o structură generală a acestora, care va fi prezentată în continuare.

Astfel, se începe cu un program de securizare a sistemelor informaționale, situație în care se foloseşte conceptul de **politica programului de securitate informațională**. Ea este acoperişul sub care se vor realiza politici tehnice de securitate, standarde şi norme de aplicare. Într-o unitate sunt necesare politici speciale pentru utilizarea Internetului şi a e-mail-ului, pentru accesarea de la distanță a sistemului, pentru modurile de utilizare a unui sistem informatic, pentru protecția informațiilor ş.a. Aşadar, se poate spune că printr-o politică a programului de securitate informațională se defineşte politica de ansamblu a organizației în acest domeniu, precum şi responsabilitățile din sistem. În aceste condiții, politicile ce se vor emite sunt componente esențiale ale programului şi ele trebuie să răspundă la cinci obiective majore:

- ***prevenire***: abilitatea de prevenire a accesului neautorizat la valorile patrimoniale ale organizației;
- ***asigurare***: asigurarea că politicile, standardele şi normele sunt în concordanță cu

intenţiile organizaţiei pe linia protejării valorilor patrimoniale informaţionale;

- ***detectare***: abilitatea de a detecta intruşii din sistem şi de a lansa arsenalul de contramăsuri corespunzătoare;
- ***investigare***: capacitatea de a folosi tehnici adecvate pentru obținerea informațiilor despre posibilii intruşi din sistem;
- ***continuitate***: posibilitatea de a garanta funcționarea neîntreruptă prin existența unui plan de acțiune în cazul dezastrelor, dezvoltat şi testat în organizație.

În continuare, vom face o descriere succintă a câtorva politici

Politica utilizării adecvate

O astfel de politică trebuie să analizeze şi să definească utilizarea corespunzătoare a resurselor informatice din organizație. Utilizatorii trebuie să o citească şi semneze atunci când îşi exprimă intenția de deschidere a unui cont de utilizator. Responsabilitățile utilizatorului pentru protejarea informațiilor, memorate în conturile lor, trebuie să fie formulate explicit, ca şi nivelurile de utilizare a Internetului şi e-mail-ului. Politica, de asemenea, trebuie să răspundă următoarelor întrebări:

- Trebuie ca utilizatorii să citească şi copieze fişiere care nu sunt ale lor, dar la care au acces?
- Trebuie ca utilizatorii să modifice fişierele la care au drept de scriere, dar nu sunt ale lor?
- Trebuie ca utilizatorii să facă copii ale fişierelor de configurare a sistemului, în scopul folosirii personale sau să le dea altora?
- Trebuie ca utilizatorii să folosească în comun conturile deschise?
- Trebuie ca utilizatorii să aibă dreptul de a face oricâte copii de pe softul care e procurat cu licență de utilizare?

Politica privind conturile utilizatorilor

Politica vizează normele după care se formulează cererile de deschidere a conturilor din sistem şi cum se efectuează întreținerea lor. Este foarte utilă în organizațiile mari, în care utilizatorii au conturi în mai multe sisteme. Este recomandată modalitatea de citire şi semnare a politicii de către utilizator. O astfel de politică trebuie să ofere răspunsuri la întrebări de genul:

- Cine are autoritatea aprobării cererilor de noi conturi-utilizator?
- Cui (angajaților, soțiilor/soților, rudelor, copiilor, vizitatorilor ş.a.) îi este permis să folosească resursele informatice ale organizației?
- Poate un utilizator să aibă mai multe conturi în acelaşi sistem?
- Pot folosi utilizatorii în comun aceleaşi conturi?
- Care sunt drepturile şi obligațiile utilizatorilor?
- Când va fi dezactivat şi arhivat un cont?

Politica accesului de la distanță

Prin ea se definesc modalitățile de conectare de la distanță la rețeaua internă a organizației. Ea este necesară în organizațiile care au utilizatori şi rețele dispersate geografic. Politica trebuie să răspundă următoarelor întrebări:

- Cine poate să aibă dreptul accesării de la distanță?

- Ce metode sunt acceptate de organizație (dial-up, modem)?
- Este permis accesul din afară la rețeaua internă prin modem?
- Se impun anumite condiții, cum ar fi soft antivirus şi de securitate, pentru accesarea de la distanță?
- Pot alți membri ai familiei să acceseze rețeaua?
- Sunt restricții privind tipul datelor ce pot fi accesate de la distanță?

Politica protecției informațiilor

Printr-o astfel de politică se aduc la cunoştința utilizatorilor condițiile prelucrării, stocării şi transmiterii informațiilor sensibile. Scopul principal al acestei politici este asigurarea că informațiile sunt protejate, în mod corespunzător, împotriva modificărilor sau dezvăluirii neautorizate. O astfel de politică trebuie semnată de toți angajații. Ea trebuie să dea răspuns cel puțin la următoarele întrebări:

- Care sunt nivelurile de sensibilitate ale informațiilor?
- Cine poate să aibă acces la informațiile sensibile?
- Cum sunt stocate şi transmise informațiile sensibile?
- Ce niveluri de informații sensibile pot fi listate pe imprimante publice?
- Cum trebuie să fie şterse informațiile sensibile de pe suporturi (tocarea şi arderea hârtiilor, curățirea discurilor ş.a.)?

Politica gestionării firewall-urilor

Politica gestionării firewall-urilor descrie modul în care sunt gestionate hardul şi softul şi cum sunt formulate şi aprobate cererile de schimbare din sistem. O astfel de politică trebuie să dea răspuns la următoarele întrebări:

- Cine are acces la sistemele firewall?
- Cine trebuie să primească solicitările de efectuare a schimbărilor în configurația firewall-urilor?
- Cine trebuie să aprobe efectuarea schimbărilor în configurația firewall-urilor?
- Cine poate să vadă normele şi listele de acces la configurația firewall-ului?
- Cât de des trebuie efectuată revizia firewall-urilor?

Politica accesului special

Prin ea se definesc condițiile formulării cererilor de obținere a dreptului de utilizare a unor conturi speciale din sistem (root, Administrator ş.a.). Ea trebuie să ofere răspunsurile la următoarele întrebări:

- Cine trebuie să primească cererile pentru acces special?
- Cine trebuie să aprobe cererile pentru acces special?
- Care sunt regulile parolelor pentru conturile cu acces special?
- Cât de des se schimbă parolele?
- Care sunt motivele sau situațiile ce vor conduce la revocarea privilegiului de a avea acces special?

Politica de conectare la o rețea locală

Prin ea se definesc condițiile adăugării de noi echipamente la rețea şi trebuie să răspundă la întrebările:

- Cine poate instala o resursă nouă în rețea?
- Cine trebuie să aprobe instalarea de noi echipamente?

- Cui trebuie să i se aducă la cunoştinţă faptul că au fost adăugate noi echipamente în reţea?
- Sunt unele restricţii pe linia securităţii în legătură cu echipamentele adăugate în reţea?

Politica partenerului de afaceri

O astfel de politică stabileşte ce măsuri de securitate trebuie să respecte fiecare companie parteneră. Ea este o politică cu atât mai necesară acum când organizaţiile oferă reţeaua lor internă partenerilor, clienţilor, furnizorilor. Deşi o astfel de politică este diferită de la o organizaţie la alta, ea, totuşi, trebuie să ofere răspunsuri la următoarele întrebări:

- I se cere fiecărei organizaţii să aibă scrisă o politică de securitate?
- Trebuie ca fiecare organizaţie să aibă un firewall sau alte echipamente de securitate a perimetrului?
- Cum se vor realiza comunicaţiile (linie închiriată, VPN prin Internet ş.a.)?
- Cum se vor formula cererile pentru accesarea resurselor partenerului?

Politica managementului parolelor

Deseori este inima politicilor de securitate dintr-o organizaţie. De regulă, ea reglementează problemele expirării parolelor, ale lungimii lor şi altor verificări necesare. Iată câteva recomandări de surprins printr-o astfel de politică:

- lungimea minimă a unei parole trebuie să fie de cel puţin opt caractere;
- parola nu trebuie să fie un cuvânt din dicţionar;
- ea trebuie să fie o combinaţie de litere şi simboluri speciale;
- parola trebuie să expire după o anumită perioadă de timp predeterminată;
- parolele administratorilor de reţele trebuie să expire mult mai repede şi trebuie să fie mai lungi;
- parolele din organizaţie trebuie să difere de cele folosite în alte sisteme;
- trebuie să fie păstrată o listă cu vechile parole pentru a preveni reutilizarea (ultimele şase parole nu trebuie să se repete);
- parolele utilizatorilor noi trebuie să fie unice şi greu de ghicit.

Politica folosirii Internetului

Politica utilizării Internetului, referită deseori prin acronimul I-AUP (*Internet Acceptable Use Policy*), este documentul prin care se detaliază modurile în care utilizatorii unei reţele a organizaţiei trebuie să folosească serviciul public Internet. Politica va descrie softul folosit pentru filtrare şi blocare, cu scopul protejării organizaţiei, dar şi activităţile specifice permise, precum şi cine sunt beneficiarii acestor drepturi de acces şi cui i se interzic. Ea este bine să se refere şi la metodele de autentificare înaintea accesării Internetului în afara organizaţiei/ţării pentru a preveni personalul că foloseşte reţeaua organizaţiei în scopuri ilegale.

Protocoalele specifice acoperite printr-o politică de utilizare a Internetului sunt următoarele:

- **Poşta electronică.** Aceasta vizează toate formele de e-mail utilizate de o organizaţie, definindu-se ceea ce se acceptă a se folosi, declarându-se softul utilizat pentru filtrare şi scanare. Ea trebuie să sublinieze cerinţele specifice referitoare la datele ce nu pot fi transmise prin e-mail şi procedurile de urmat în cazul în care un utilizator primeşte mesaje cu date de acest gen. Prin această politică trebuie prevăzute şi măsurile luate în cazul nerespectării condiţiilor de utilizare a e-mail-ului;

- **Web**. Politica va prevedea condiţiile specifice de realizare a traficului Web. Cât timp WWW (World Wide Web) foloseşte HTTP-ul (HyperText Transport Protocol) pentru transferarea informaţiilor, prin politica de faţă vor fi definite clar tipurile de site-uri Web care sunt strict interzise, de genul celor porno, jocurilor de noroc ş.a.;
- **FTP.** Permiţând utilizatorilor accesul la FTP (File Transfer Protocol), se deschide calea descărcării cu uşurinţă în sistemul organizaţiei a viruşilor, dar şi transmiterea pe serverele din afara orgnizaţiei a unor informaţii confidenţiale. Pentru specialiştii organizaţiei trebuie să se asigure un nivel de acces FTP pentru efectuarea unor descărcări de fişiere în vederea actualizării softului existent, dar politica de faţă trebuie să stabilească autorizările de utilizare FTP;
- **Chat/IRC**. IRC-ul (Internet Relay Chat) este mai puţin folosit în mediul organizaţional faţă de alte programe de chat (dialoguri Internet), cum sunt Yahoo, ICQ şi AOL Instant Messenger (AIM). Astfel de programe sunt foarte riscante pentru organizaţie deoarece informaţiile sunt transmise unor servere externe fără o protecţie corespunzătoare. Politica de faţă trebuie să stabilească în ce măsură produsele de tip *chat* servesc intereselor organizaţiei.

În general, prin politica Internet se face referire la următoarele aspecte:

- acceptarea folosirii şi condiţiile de accept pentru:
  - descărcările de fişiere;
  - newsgroup-uri;
  - comunicarea datelor sensibile;
  - tipurile de fişiere ataşate;
  - dimensiunea mesajelor;
  - softul f ără licenţă;
  - pachete de aplicaţii soft neaprobate;
  - exportul informaţiilor sensibile;
  - protecţia fişierelor;
  - protecţia împotriva viruşilor;
- managementul schimbărilor din sistem;
- practicile de stocare a datelor;
- siguranţă şi disponibilitate;
- protecţia informaţiilor prin clasificarea lor;
- controlul accesului;
- e-mail-ul şi datele ce pot fi reţinute/stocate în unitate;
- monitorizarea;
- excepţiile şi amendamentele politicii Internet.

6 Securitatea rețelelor de calculatoare

6.1 Mecanisme utilizate în securizarea rețelelor

Dynamic Host Configuration Protocol – DHCP - este o modalitate rapidă şi simplă de a asigna adrese IP unui număr mare de clienți.

Există nevoia de a defini un interval de IP-uri valide şi de a le asigna automat clienților din rețea; de asemenea, a apărut nevoia de a defini o durata de viata unui IP.

6.1.1 Functionarea DHCP

DHCP **implementează un model client-server şi un agent cu rol de releu** (relay agent). Acest agent gestionează interacțiunea dintre clienți şi server. Deoarece **clientul** este principalul partener de comunicație în această situație, el **inițiază toate sesiunile cu serverul**, lucru care are loc în faza de bootare. DHCP are următoarele facilități:

- suportă alocarea dinamică;
- suportă alocarea statică;
- repartizează adrese;
- suporta repartizarea persistenta
- reintegrează repartițiile expirate.

În esență, DHCP este însărcinat cu manipularea a două seturi de date: repartițiile (IP-urile alocate) şi fondul de adrese (IP-uri disponibile). Repartițiile sunt alocate clienților conform unei proceduri, care este destul de simplă.

Cum primesc clienții numere IP

Iată modul de funcționare a DHCP din acest punct de vedere:

1. Clientul cere un IP printr-o difuzare de tip *DhcpDiscover*. Dacă clientul are o repartiție persistentă, poate cere inițial acea repartiție.

2. Serverul alege un IP din fondul de adrese şi întoarce un pachet *DhcpOffer* cu un IP disponibil ataşat.

3. În cazul în care clientul doreşte mai multe oferte IP, o va alege pe prima sau pe cea cu repartiția dorită.

4. Clientul difuzează un pachet *DhcpRequest* cu un identificator pentru un server şi trece în aşteptare

5. Fiecare server care analizează pachetul şi nu îşi detectează identificatorul va ignora pachetul. După ce serverul cu identificatorul corespunzător primeşte pachetul, el va trimite un *DhcpAck* (sau *DhcpNak* - daca IP-ul cerut este deja alocat, ceea ce înseamnă că repartiția a expirat).

6. După ce clientul primeşte pachetul DhcpAck, el începe să folosească IP-ul alocat. În cazul în care primeşte DhcpNak, va rula de la început secvența de cerere a unui IP. Dacă IP-ul reprezintă o problema din punct de vedere al clientului, acesta trimite un pachet *DhcpDecline* către server şi reia secvența de cerere a unui IP.

Funcționarea într-o rețea LAN:

În etapa de lansare a sistemului de operare se emite o cerere de alocare IP însoțită de adresa MAC a emițătorului către toată rețeaua va primi un răspuns de la primul server DHCP împreuna cu o adresa IP, masca, gateway-ul şi serverele DNS.

Dacă DHCP alocă unui utilizator nou o adresă IP nerutabilă cu care nu poate face mai nimic. Trebuie luat legătura cu administratorul de sistem şi memorată adresa sa într-un tabel NAT.

NAT – Networking Addressing Table – tabel de adresare în rețea – este o soluție care permite ca în zona rețelei locale să se utilizeze exclusiv adrese private. Routerul converteşte toate cererile modificând headerul care însoțeşte pachetul de date astfel încât acestea să apară originate de către router şi nu de sistemul din spatele lui.

Avantaje :

- există o singura adresa IP publică şi se pot deservi oricâte adrese IP private;
- oferă protecție pentru flood - ignora informațiile care nu adresează o adresă din tabela de NAT-are;
- toți cei din rețeaua locală nu există pentru rețeaua Internet
- un sistem local nu poate oferi un serviciu în afara zonei locale, cum ar fi un setarea unui server

Se poate defini un DMZ – zona demilitarizată – astfel încâz toate sistemele să primească informații din rețeaua WAN indiferent de conținutul tabelei de NAT-are.

În cazul în care într-un LAN există 2 sau mai multe sisteme cu aceleaşi adrese IP routerul le ignoră cererile ceea înseamnă ca nu va funcționa nici unul dintre sisteme.

6.1.2 Noțiuni privind securizarea rețelei

Firewall-urile şi serverele proxy, ca şi criptarea şi autentificarea, sunt proiectate pentru asigurarea securității datelor. Motivația este simplă: dacă se dispune de o conexiune la Internet, teoretic, oricine, oriunde s-ar afla în lume, poate accesa rețeaua (în anumite condiții, evident). Dacă nu există nici un mecanism de securitate, orice persoană care are acces la Internet, de oriunde din lume, poate folosi TCP/IP pentru a trece prin gateway-ul rețelei locale, către orice maşina din rețea.

Ideea este de a proteja două lucruri: datele stocate în rețea şi echipamentele hardware, conectate la rețea. Intruşii sau hackerii pot intra în rețea şi pot modifica orice, pot accesa orice fel de date sau chiar pot cauza deteriorări fizice ale sistemelor.

Există multe moduri în care intruşii pot accesa o rețea:

- exploatând breşe de securitate din sistemele de operare şi aplicații;
- pin "inginerie socială", care constă în convingerea cuiva, sub diferite pretexte, să comunice nume şi parole asociate.

Rolul unui firewall este să prevină pătrunderile neautorizate.

O alta problemă de securitate: ***blocarea serviciului*** (denial of service). Are loc când hackerii nu vă permit folosirea normală a propriilor sisteme. Blocare serviciului are multe forme. Un exemplu tipic este inundarea unui serviciu (gen email), adică acelui serviciului îi sunt trimise atât de multe date încât devine supraîncărcat şi se blochează sau rulează în buclă infinită.

Există mai multe modalități de protejare a rețelei.

O metodă ar fi anonimatul: dacă nimeni nu ştie nimic despre reţeaua dv, atunci datele sunt în siguranţă. Însă este o falsă securitate, pentru că exista o mulţime de moduri prin care se poate afla ce se află pe Internet.

Cea mai răspândită formă de securitate se numeşte ***securitatea la nivel de gazdă*** (host security) şi se referă la securizarea separată a fiecărei maşini din reţea. Vă bazaţi pe acest tip de securitate când setaţi permisiunile de acces în Windows sau permisiunile UNIX pentru fişiere şi directoare. Este suficient însă o singură breşă pentru ca întreaga reţea să fie deschisă hackerilor. De asemenea, pentru că securitatea la nivel de gazdă nu este aplicată egal tuturor maşinilor, pot fi exploatate serviciile unei maşini slab protejate pentru a accesa o maşină cu securitate puternica.

6.1.3 Firewalls

Un ***firewall*** este un computer, un router sau orice alt dispozitiv de comunicaţie care controlează fluxul de date între reţele. În general, un firewall este prima linie împotriva atacurilor din afara reţelei.

Poate fi implementat:

- **hardware** - este un router special cu filtre adiţionale şi capacităţi de management;
- **software** - rulează pe un sistem de operare oarecare şi transformă un PC într-un firewall.

Conceptual, dispozitivele firewall pot acţiona la :

- nivelul "Retea" - sunt de obicei foarte rapide. Ele controlează traficul pe baza adreselor sursă şi destinaţie, precum şi a numerelor de port;
- nivelul "Aplicaţie" - nu permit traficul direct între reţele. De obicei ele sunt computere care rulează **servere proxy**. Acestea pot implementa proceduri de securitate specifice. De exemplu, se poate configura aşa încât să permită funcţionarea numai a protocolul de email.

Din cadrul aplicaţiilor firewall ce oferă o protecţie bună la atacurile tipice din reţea putem aminti de Zone Alarm, Agnitum Outpost şi Firewall-urile integrate din Windows XP şi unele variante din Linux.

De exemplu în Windows XP se deschide icoana ce reprezintă conexiunea curentă spre Internet şi se activează firewall-ul, aşa cum se poate observa în figura 6.1.

Din opţiunea Settings se pot configura serviciile ce pot fi accesate de utilizatorii de pe Internet.

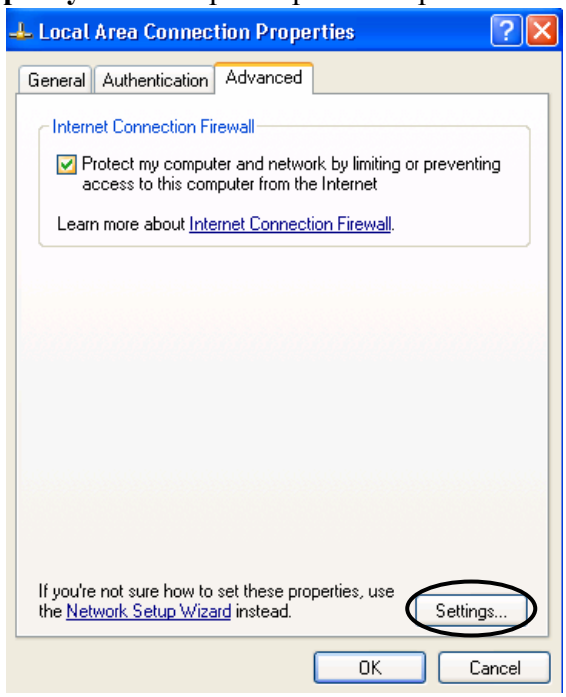


Fig. 6.1: Activarea firewall-ului din WindowsXP

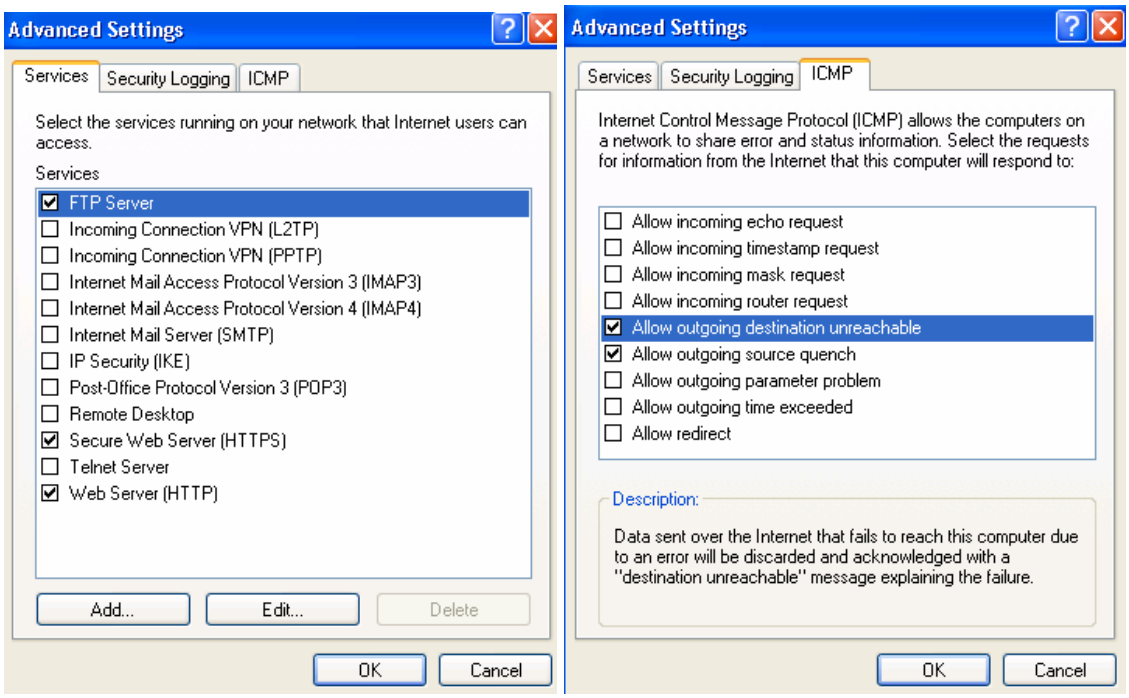


Fig. 6.2: Serviciile ce pot fi accesate prin Firewall şi suportul pentru mesaje ICMP

Rolul firewall-urilor

Tipul de securitate important este securitatea la nivel de rețea. Presupune securizarea tuturor punctelor de acces la rețea. Componenta cheia este acest firewall – o maşină care se comportă ca o interfață între rețea şi Internet, având doar preocuparea securității. Un firewall are mai multe roluri:

- permite accesul la rețea numai din anumite locații;
- interzice utilizatorilor neautorizați să obțină acces la rețea;
- forțează traficul dinspre rețea spre Internet să treacă prin anumite puncte securizate;
- previne atacurile de tipul blocarea serviciului;
- impune restricții asupra acțiunilor pe care un utilizator de pe Internet le poate face în rețea.

Conceptul de firewall presupune canalizarea întregului trafic către şi dinspre rețea prin unul sau mai multe puncte care sunt configurate pentru a controla accesul şi serviciile.

Utilizarea firewall-urilor

Multe persoane consideră un firewall ca fiind o singură maşină, ceea ce uneori este adevărat. Există maşini dedicate doar acestei funcții. Totuşi, termenul firewall se referă mai mult la funcțiile îndeplinite decât la un dispozitiv fizic. Un firewall poate consta din mai multe maşini care conlucrează, sau pot fi folosite mai multe programe cu funcție de firewall. Firewall-urile pot să îndeplinească şi alte funcții decât simpla monitorizare a accesului la rețea.

Firewall-urile nu sunt invincibile. Ele sunt vulnerabile din cauza defectelor de proiectare, sau a implementării (care necesită timp şi bani pentru instalare şi configurare).

Un firewall oferă un singur punct de implementare a securității din rețea, deci eventualele schimbări se fac pe o singură maşină şi nu pe toate celelalte din rețea (de ex, se poate interzice accesul FTP anonim). Firewall-urile pot aplica politici de securitate la nivelul întregii rețele, interzicând de exemplu accesul la anumite servicii de pe Internet pentru toți utilizatorii din rețea.

Totuşi, orice firewall are limitări. Ele sunt utile doar pentru conexiunea rețea-Internet. Ele nu opresc persoanele din rețea să facă orice vor altor maşini din rețea.

Ele nu pot proteja împotriva pătrunderilor neautorizate dacă aveți alte conexiuni, ca un calculator care este conectat printr-un modem la Internet prin intermediul unui ISP (conexiune care nu trece printr-un firewall). Un firewall nu poate preveni multe probleme distribuite prin Internet, cum sunt viruşii şi caii troieni.

Există două moduri principale de implementare:

- construirea unui firewall propriu din servicii de rețea elementare.
- cumpărarea unui produs comercial.

La instalarea unui firewall, manual sau comercial, se pot controla mai multe fațete, depinde de administrator dacă doreşte sau nu activarea lor. Unele din aceste fațete ar fi:

- serverele proxy
- filtrele de pachete.

6.1.4 Proxy-uri

Soluție care permite accesarea informației de după un router logic. Reprezintă un sistem de intermediere a traficului, adică primeşte cererile, identifică răspunsurile, le memorează şi le trimite solicitantului.

Posedă o adresa IP publică şi una privată – deci **este un sistem cu două placi de rețea**. **Avantajul este CACHE-ul folosit de proxy**. Fiecare pagină are o dată şi o oră de expirare.

De asemenea se poate folosi un proxy transparent în sensul că cererea din router este redirectată către un proxy.

Serverele proxy

Un astfel de server este plasat între rețea şi Internet şi acceptă cereri pentru un serviciu, le analizează şi le trimite mai departe, în funcție de permisiuni. Serviciul de proxy oferă o conexiune cu rol de înlocuitor pentru acel serviciu, motiv pentru care se comportă ca un intermediar (proxy). Serverul proxy se plasează la mijloc, ascunde anumite informații, dar permite desfăşurarea serviciului prin el.

Ideea este că, fără proxy, adresa IP a maşinii gazdă este trimisă în pachete, prin Internet. Hackerii pot determina dimensiunea rețelei, de exemplu. Un server proxy schimbă adresa IP cu adresa lui şi foloseşte o tabelă internă pentru a redirecta traficul care soseşte şi care pleacă spre destinațiile corecte. Pentru exterior va fi vizibilă o singură adresă IP (a serverului proxy).

Serverele proxy sunt întotdeauna implementate prin software şi nu trebuie să facă parte dintr-un pachet de firewall, deşi sunt de obicei incluse.

Windows XP suportă împărțirea conexiunii la Internet (Internet Sharing) folosind opțiunea Network Setup Wizard din Start/Settings/Network Connections. Însă soluția aceasta nu funcționează întotdeauna.

O soluție mult mai bună pentru un server proxy este aplicația software FreeProxy (www.handcraftedsoftware.org)

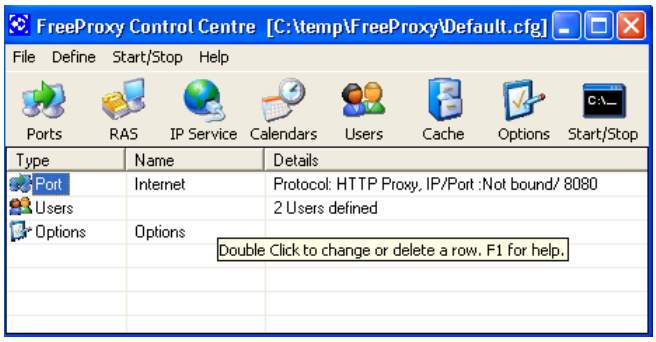


Fig. 6.3: Interfața aplicației FreeProxy

Se configurează programul prin crearea unui serviciu IP în care se alege placa de rețea ce face legătura la Internet. Sistemul pe care funcționează această aplicație are două plăci de rețea şi se comportă ca un gateway.

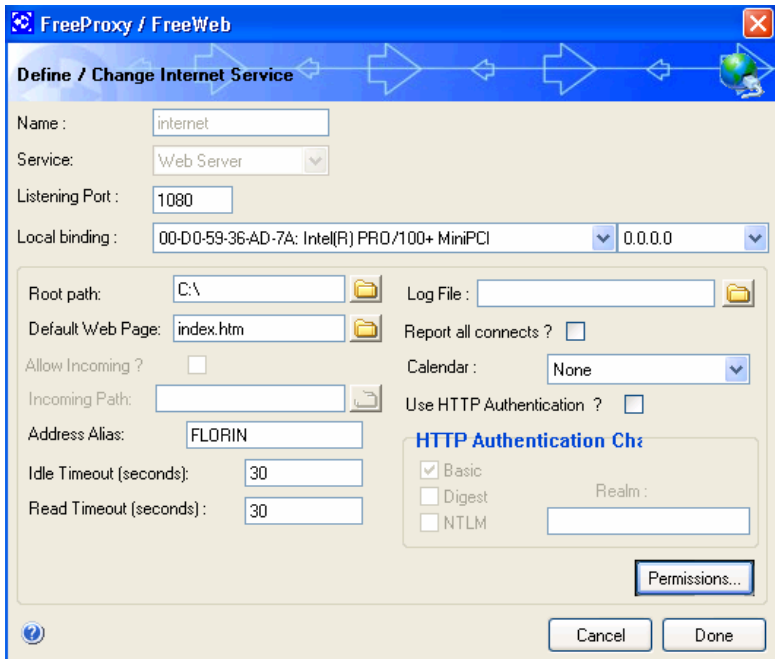


Fig. 6.4: Setarea unui gateway

Opțiunea Permissions oferă selecția unui serviciu Proxy şi a drepturilor ce pot fi oferite diverşilor utilizatori. Pornirea serverului Proxy se execută prin selectarea opțiunii Start/Stop.

Odată executată, aplicația Proxy rămâne rezidentă în memorie şi porneşte automat la deschiderea calculatorului şi inițializarea sistemului de operare.

Pe celelalte calculatoare, care au acces prin acest proxy server trebuie realizate câteva setări. Astfel din Control Panel avem Internet Options, Connections şi apoi Lan Settings unde trebuie bifată opțiunea de folosire a unui server Proxy şi introdusă adresa IP împreuna cu portul de acces al acestuia.

6.1.5 Filtrele de pachete

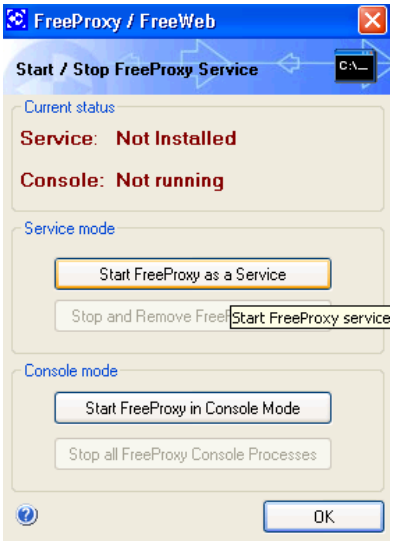


Fig. 6.5: Pornirea serverului Proxy

Un astfel de sistem permite pachetelor să treacă din rețea către Internet şi invers, dar selectiv. Pachetele sunt identificate după tipul aplicației care le-a construit (unele informații se afla în antet). Antetul unui pachet TCP/IP conține adresele IP sursă şi destinație, porturile sursă şi destinație şi aşa mai departe. Dacă se decide blocarea oricărui trafic FTP, de exemplu, software-ul de filtrare a pachetelor va detecta toate pachetele care au numărul de port 20 sau 21 şi le va interzice trecerea.

Unii cred că se poate ocoli un sistem de filtrare schimbând numărul portului, lucru posibil într-o oarecare măsura. Totuşi, deoarece software-ul de filtrare este rezident în rețeaua dv, el poate determina către ce interfață se îndreaptă pachetul şi de unde provine. În consecință, chiar dacă numerele de port TCP sunt diferite, software-ul de filtrare poate uneori să blocheze corect traficul.

Se poate folosi software-ul de filtrare a pachetelor în mai multe moduri. Cel mai obişnuit, se blochează un serviciu, gen FTP sau Telnet. Se pot desemna de asemenea maşini care trebuiesc împiedicate sau lăsate să acceseze rețeaua – de exemplu, dacă se constată ca o anumită rețea a fost sursa unor probleme, se poate comanda software-ul aşa încât să respingă orice pachet de la acea rețea. În unele cazuri se pot bloca toate serviciile, sau se poate permite numai anumitor servicii, gen e-mail, se treacă prin filtru.

6.2 Rețele VPN

O soluție alternativă o constituie o rețea VPN (Virtual Private Network).

Rețelele VPN sunt bazate pe o infrastructură accesibilă în mod public, cum ar fi Internetul sau rețeaua de telefonie.

Ele prezintă diferite forme de criptare şi au de obicei procedee solide de autentificare a utilizatorului.

În esență, VPN este o formă de WAN; diferența este utilizarea de rețele publice mai degrabă decât linii private (închiriate). O rețea VPN are aceleaşi servicii Intranet ca şi WAN, dar suportă şi servicii de acces la distanță (liniile închiriate, din cazul WAN, nu se extind de obicei la case particulare şi nu se aplică în cazul călătoriilor).

Un utilizator VPN se poate conecta printr-un ISP (Internet Service Provider) în modul obişnuit, eliminând costurile legate de accesul la distante mari. **Utilizatorul poate iniția o cerere "tunnel" către serverul destinație.** Serverul autentifică utilizatorul şi creează celalalt capăt al "tunelului".

Softul VPN criptează datele, le formatează în pachete IP (pentru compatibilitate Internet) şi le trimite prin "tunel", unde sunt decriptate la celalalt capăt.

Exista câteva "tunneling protocol":

- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)
- IP security (IPsec)

6.2.1 Point-to-Point Tunneling Protocol (PPTP)

Este rezultatul cooperării dintre mai multe firme (3Com, US Robotics, Microsoft etc). Utilizatorii pot să se conecteze telefonic (dial-in) la furnizorul de servicii Internet (ISP) local şi apoi să se conecteze securizat printr-un tunel virtual la rețeaua corporației lor.

PPTP este un protocol orientat pe modelul client/server, proiectat special pentru asigurarea de tuneluri virtuale prin rețele IP utilizând PPP şi nivelul 2. **PPTP suportă mai multe conexiuni PPP printr-un singur tunel PPTP**. Aceste tuneluri virtuale sunt denumite în general *rețele virtuale private* (VPN – Virtual Private Networks).

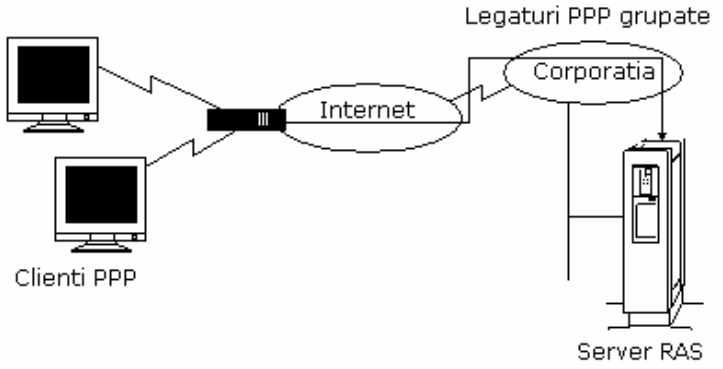


Fig. 6.6: Structura PPTP

Cea mai uzuală implementare este de **a oferi serviciul prin un *punct de prezență* (Point of Presence – POP) dial-up**.

După ce conexiunea fizică a fost stabilită şi utilizatorul autentificat, PPTP se bazează pe PPP pentru crearea diagramelor. Apoi PPTP încapsulează pachetele PPP pentru transmisia prin tunelul IP.

Canalul de control separat

PPTP foloseşte două canale pentru a suporta conexiunea:

- un canal de date
- un canal de control - rulează peste legătura TCP, portul 1723. Acest canal conține informații referitoare la starea legăturii şi mesaje de management. Mesajele de management sunt responsabile cu stabilirea, gestionarea şi închiderea tunelului PPTP.

Suportul pentru mai multe protocoale

O facilitate interesanta a PPTP este suportul pentru protocoale gen NetBEUI, IPX sau AppleTalk. Deoarece PPTP este un protocol de nivelul 2, el include şi un antet de mediu de transmisie care îi permite să opereze prin Ethernet sau conexiuni PPP.

Autentificarea şi securitatea datelor

Criptarea şi autentificarea datelor nu fac parte din PPTP. Acesta se bazează pe funcțiile protocolul PPP.

Tipuri de tuneluri PPTP

Calculatorul utilizatorului va determina capătul tunelului:

- fie un server de acces de la distanță (*Remote Access Server* – RAS) al ISP-ului ,

- fie chiar calculatorul respectiv.

Există tuneluri voluntare şi tuneluri obligatorii.

Într-un tunel voluntar, utilizatorul inițiază conexiunea PPTP către un calculator din corporație. În acest caz, ISP nu trebuie decât să asigure servicii IP elementare. Dacă ISP asigură un server RAS, clientul are nevoie doar de PPP. În orice caz, utilizatorul nu are control asupra tunelului.

În cazul tunelurilor obligatorii, avantajul este că folosirea Internetului poate fi controlată de corporații; de asemenea, au capacitatea de a grupa traficul, mai mulți clienți PPP putând fi grupați într-o singură conexiune PPTP către Intranetul companiei.

6.2.2 Layer 2 Tunneling Protocol (L2TP)

Este asemănător cu PPTP, combinând PPTP cu protocolul *Layer 2 Forwarding* (L2F) de la firma Cisco. Avantajul este că poate fi compatibil cu alte medii de transfer, precum ATM, şi cu alte rețele pe baza de pachete, gen X.25.

L2F

La fel ca şi PPTP, L2F a folosit PPP ca suport pentru asigurarea conexiunii inițiale şi a serviciilor precum autentificarea. Spre deosebire de PPTP, L2F a folosit *Terminal Access Controller Access-Control System* (TACACS) – protocol brevetat de Cisco, care oferă autentificare, autorizare şi administrare.

L2F foloseşte şi el definiții de conexiuni tunel. Suportă şi un nivel suplimentar de autentificare. L2F oferă autentificare la nivel de gateway sau firewall.

Suportul pentru IPsec

IPsec diferă de celelalte servicii pentru că este o specificație deschisă care suportă nu numai autentificarea, dar şi securitatea.

Ca şi PPTP, L2TP apelează la PPP pentru stabilirea conexiunii. **L2TP se aşteaptă ca PPP să stabilească conexiunea fizică, să facă autentificarea inițială, să creeze datagramele şi, după terminarea sesiunii, să închidă conexiunea**. Dar L2TP va comunica cu celalalt nod pentru a determina dacă nodul care face apelul este autorizat şi dacă punctul final doreşte să suporte conexiune L2TP. Dacă nu, sesiunea este închisă.

Ca şi PPTP, L2TP defineşte două tipuri de mesaje:

- de date
- de control - folosite pentru a stabili şi menține tunelul virtual şi pentru a controla transmisia şi recepția datelor.

Spre deosebire de PPTP, care necesită două canale, L2TP combină canalele de date şi de control într-un singur flux. Într-o rețea IP, acest lucru se prezintă sub forma împachetării datelor şi a mesajelor într-o datagrama UDP.

Datele utile constau în esență din pachetul PPP, minus elementele de încadrare specifice mediului de transmisie. Deoarece L2TP este de nivel 2, el trebuie să includă un antet pentru mediul de transmisie cu scopul de a-i indica nivelului superior modul în care trebuie transmis pachetul. Aceasta transmisie poate avea loc pe Ethernet, rețele *frame relay*, X.25, ATM, sau prin legătură PPP inițială.

Pentru reducerea congestionării rețelei, **L2TP suportă controlul fluxului**. Acesta este implementat într-un *concentrator de acces L2TP* (L2TP Access Concentrator – LAC), care funcționează ca server de acces la rețea, şi un *server L2TP de acces la rețea* (L2TP Network Access Server – LNS), care are rolul de a asigura

accesul la rețeaua corporației. Mesajele de control conțin informații privind ratele de transmisie şi parametrii zonelor tampon. Comunicându-şi reciproc aceste informații, serverele LAC şi LNS pot controla fluxul de date.

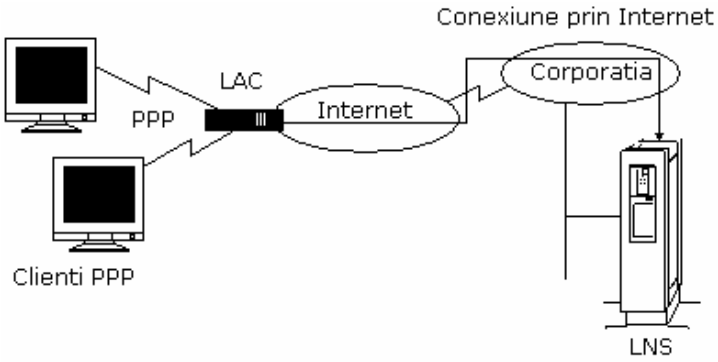


Fig. 7: Structura L2TP

O altă metodă pentru reducerea încărcării rețelei este compresia anteturilor pachetelor.

L2TP suportă tot două clase de conexiuni, într-o manieră asemănătoare cu PPTP: tuneluri voluntare şi obligatorii.

6.2.3 IPsec

Deoarece protocolul TCP/IP nu oferă nici un fel de protecție, au apărut mai multe metode de a umple acest gol. De aceea, s-a lucrat la un set de protocoale numite IPsec. Documentele pentru aceste standarde au fost gândite pentru standardul IPv6 (publicate în 1995), dar au fost modificate pentru adaptarea lor la IPv4. Arhitectura IPSec este compusă dintr-un set de protocoale pentru autentificarea pachetelor (AH), criptarea şi/sau autentificarea pachetelor (ESP) şi mecanisme pentru stabilirea parametrilor conexiunilor (SA-Security Associations) folosind IKE.

IPSec foloseşte un algoritm pentru schimbarea cheilor între părți, numit *Internet Key Exchange* (IKE), care permite calculatoarelor să negocieze o cheie de sesiune în mod securizat, folosind protocoalele ISAKMP pentru crearea de *Security Associations* şi OAKLEY bazat pe algoritmul *Diffie-Hellman* pentru schimbarea cheilor între cele două părți. IKE se poate folosi în conjuncție cu Kerberos, certificate X.509v3 sau chei *preshared*.

Authentication Header (AH) este ataşat fiecărei datagrame şi conține semnătura sub formă de hash HMAC cu MD5 sau HMAC cu SHA-1.

Encapsulated Security Payload (ESP) criptează conținutul pachetelor în două moduri: transport (protejează doar conținutul pachetului, nu şi header-ul) sau tunel (întreg pachetul este criptat). ESP foloseşte de asemenea hash-uri HMAC cu MD5 sau HMAC cu SHA-1 pentru autentificare şi DES-CBC pentru criptare.

Regulile de bază pentru securizarea traficului cu IPSec

- Crearea unei hărți a traficului în rețea ce include traficul care trebuie permis sau blocat, punctele sursă destinație şi informațiile despre protocoalele folosite.
- Se creează filtre care corespund traficului de rețea identificat anterior

7. Tehnici, servicii şi soluții de securitate pentru Intranet-uri şi portaluri

7.1. Introducere

Cele mai multe aplicații de securitate pot fi privite în termeni de servicii generale pe care le pot oferi. Aplicațiile de securitate sunt instalate pentru a oferi un nivel de bază al securității sau funcții care îmbunătățesc securitatea operațională dintr-o organizație.

Între serviciile de securitate sunt cuprinse şi următoarele:

- ***auditarea*** - un mecanism (de obicei un sistem de jurnalizare) care înregistrează evenimentele care pot să includă accesul utilizatorilor şi al fişierelor;
- ***autentificarea*** - un mecanism prin care se identifică în mod pozitiv un utilizator prin cererea unor date de identificare (parolă, smart card, amprente, date biometrice, etc.);
- ***autorizarea*** - resursele pe care un utilizator le poate accesa după ce a fost autentificat;
- ***disponibilitatea*** - disponibilitatea unei resurse. Un atac împotriva disponibilității unui sistem este cunoscut sub numele de Denial of Service (DoS);
- ***confidențialitatea*** - protecția informațiilor private sau sensibile;
- ***integritate*** - protecția datelor împotriva modificărilor neautorizate. Acest lucru este important mai ales în instituțiile financiare;
- ***nerepudiere*** - un mecanism de prevenire a fraudelor prin care se dovedeşte că un utilizator a executat o anumită acțiune; Toate aceste aplicații obțin nivelul dorit de protecție prin utilizarea criptografiei.

7.2. Criptografia

Criptografia este arta şi ştiința de a ține secrete datele, prin utilizarea criptării folosind un algoritm specific. Un algoritm (numit şi ***cifru)*** este un proces matematic sau o serie de funcții prin care se amestecă datele. Cei mai mulți algoritmi utilizează ***chei***, astfel încât algoritmii pot să nu fie unici pentru o tranzacție, iar detaliile algoritmilor utilizați să nu fie secrete.

Termenul ***cheie*** se referă la informația necesară pentru a cripta sau decripta datele. Securitatea unei chei este deseori discutată în termeni de lungime sau biți ai acesteia, dar o cheie de mărime mare nu garantează securitatea de ansamblu a sistemului.

Există două tipuri generale de criptografie, definite în funcție de tipul de cheie utilizat: criptografia cu *cheie secretă* şi criptografia cu *cheie publică.* Cele mai multe aplicații utilizează principiile unuia sau a ambelor tipuri de criptografie.

7.2.1. Criptografia cu cheie secretă

Criptarea cu cheie secretă, cunoscută sub numele de ***criptare simetrică***, utilizează o singură cheie pentru a cripta sau decripta datele. Securitatea algoritmului cu cheie secretă este deseori legată de cât de bine este păstrată sau distribuită cheia secretă.

Algoritmii de chei secrete sunt împărțiți în *algoritmi de bloc (block cipher),* care procesează datele în blocuri măsurate la un moment dat, sau *algoritmi de şiruri (stream cipher),* care procesează la un moment dat un singur byte. Algoritmii de bloc excelează în criptarea datelor de lungime fixă, în timp ce algoritmii de stream-uri sunt utilizați îndeosebi la criptarea stream-urilor aleatoare de date, precum traficul de rețea între două routere.

Între avantajele criptării cu cheie simetrică se numără rapiditatea procesului de criptare şi simplitatea utilizării acestuia. Dezavantajele sunt legate de distribuirea în siguranță a cheii secrete şi de managementului cheilor.

Printre exemplele cele mai întâlnite de algoritmi cu cheie simetrică cu criptare în bloc se numără *Data Encryption Standard* (DES), *International Data Encryption Algorithm* (IDEA), CAST-128 (numit după inventatorii acestuia - Carlisle, Adams, Stafford, Tavares) şi *Blowfish.* Printre algoritmii de criptare a stream-urilor se numără *Ron 's Cipher 4* (RC4) şi *Software-Optimized Encryption Algorithm* (SEAL).

7.2.2. Criptografia cu cheie publică

Criptografia cu cheie publică sau ***criptografia asimetrică*** utilizează o pereche de chei. Una dintre aceste chei, cheia publică, este distribuită şi publicată, în timp ce cealaltă cheie trebuie ținută secretă. Dată fiind numai cheia publică, este imposibil să se determine cheia secretă. Chiar şi cu cel mai modern hardware, algoritmii de generare a cheilor publice utilizează intensiv procesorul.

Datorită acestei probleme legate de rapiditatea algoritmului, aceştia nu sunt utilizați pentru a cripta datele brute. În schimb, datele sunt criptate cu un algoritm simetric. Multe din tehnologiile prezentate utilizează o combinație de algoritmi cu cheie publică şi secretă în care criptografia cu cheia publică este utilizată pentru a securiza cheia simetrică care este utilizată la criptarea datelor brute. O cheie simetrică care a fost securizată utilizând un algoritm cu cheie publică se numeşte ***plic digital***.

Cheile private corespunzătoare cheilor publice trebuie întotdeauna securizate. Unul dintre mecanismele utilizate pentru stocarea cheii private este *smart card-ul* - un dispozitiv electronic asemănător unei cărți de credit. Un *smart card* criptografic are abilitatea de a genera şi stoca chei în el însuşi, asigurându-se astfel faptul că cheia privată nu este expusă către maşina locală. Smart card-urile pot fi vulnerabile la atacuri, dar oferă o mult mai mare securitate față de stocarea cheilor private pe o maşină locală.

Printre algoritmii cu cheie publică se numără *RSA, ElGamal* şi *Diffie-Hellman Hey Exchange.*

7.2.3. Managementul cheilor şi distribuția acestora

Una din problemele fundamentale atât în sisteme de criptografie cu cheie publică cât şi în cele cu cheie secretă este modalitatea de distribuire şi menținere a cheilor utilizate pentru criptare şi decriptare, în mod securizat.

Algoritmii cu cheie secretă depind de obținerea în mod securizat a cheii de către toate părțile implicate. De exemplu, e-mail-ul nu este considerat un mecanism securizat de distribuire a cheilor, deoarece terțe părți îl pot intercepta în tranzit.

O altă problemă a criptografiei cu cheie secretă este faptul că nu este un sistem la fel de scalabil ca şi criptarea cu cheie publică. De exemplu, în cazul în care se doreşte trimiterea unui mesaj criptat cu o cheie secretă către mai mulţi destinatari, toţi trebuie să primească câte o cheie prin care să se poată decripta mesajul. Astfel, expeditorul trebuie să se asigure de faptul că toţi destinatarii recepţionează cheia, că aceasta nu este interceptată sau compromisă în timpul tranzitului şi că este păstrată în mod securizat în momentul atingerii destinaţiei finale. Pentru fiecare mesaj nou trimis, procesul trebuie să se repete, cu excepţia faptului când se doreşte reutilizarea cheii iniţiale. Reutilizarea cheii originale sporeşte şansele ca aceasta să fie compromisă, iar în cazul în care se doreşte ca fiecare destinatar să aibă o cheie secretă, sistemul de distribuţie nu mai este gestionabil.

Prin utilizarea criptografiei cu cheie publică are loc un singur schimb de chei publice pentru fiecare destinatar, iar acest lucru poate fi uşurat prin plasarea acestora într-un director precum *Lightweight Directory Access Protocol* (LDAP). Totuşi, cheia publică trebuie schimbată printr-un mecanism de încredere şi securizat, având grijă ca acea cheie să aparţină într-adevăr unei anume persoane şi nu unui terţ care impersonează persoana reală.

7.2.4. Funcţiile Hash

O funcţie ***hash*** oferă un mijloc de a crea un conţinut cu lungime fixă prin utilizarea unor date de intrare cu lungime variabilă. Acest lucru mai este cunoscut şi sub numele de ***luarea unei amprente*** a datelor, iar datele de ieşire sunt cunoscute sub numele de ***message digest*** sau ***hash***. În cazul în care datele se modifică după ce a fost calculată funcţia ***hash***, această valoare nu se va mai potrivi la o a doua calculare. Prin utilizarea unui algoritm ***hash*** criptografic, chiar şi o mică modificare precum ştergerea sau adăugarea unei virgule dintr-o propoziţie va crea mari diferenţe între valorile ***hash***. De asemenea, la polul opus, având la dispoziţie un mesaj ***hash*** criptat cu un algoritm criptografic puternic, nu este posibilă determinarea mesajului iniţial.

Valorile *hash* rezolvă problema integrităţii mesajelor, deoarece prin aceste valori se poate verifica dacă datele au fost sau nu modificate.

Între algoritmii de tip *hash* se numără *Secure Hash Algorithm 1* (SHA-1) şi *Message Digest 5* (MD 5).

Securitatea generală atât a cheilor publice cât şi a celor private poate fi discutată şi în termeni de ***lungime***. O cheie de mărime mare nu garantează securitatea de ansamblu a sistemului sau gestiunea securizată a cheilor. De asemenea, aceasta nu rezolvă alte probleme, precum generarea de numere aleatoare (slaba utilizare a generării de numere aleatoare a compromis implementarea SSL originală în browser-ul Netscape). Lungimea unei chei în sine indică numai faptul că algoritmul de criptare utilizat este unul puternic.

Trebuie notat faptul că lungimea cheilor publice şi secrete diferă din punct de vedere al mărimii şi securităţii. De exemplu, o cheie RSA de 512 biţi oferă o securitate mai mică decât o cheie de 128 biţi de tip Blowfish. Tabelul 7.1 rezumă anumite relaţii agreate între cheile publice (RSA) şi cele secrete, din punct de vedere al lungimii.

Tabelul 7.1

Relații agreate între lungimea cheii publice şi cea a cheii private

Lungime cheie secretă (cifru bloc)	Cheie RSA
56 biți	512 biți
80 biți	1024 biți
112 biți	2048 biți
128 biți	3072 biți
256 biți	15360 biți

7.2.5. Utilizarea semnăturilor digitale. Riscuri de securitate

Prin semnarea de către Preşedintele SUA a *The Electronic Signatures in Global and National Commerce Act* în 30 iunie 2000, semnăturile digitale au devenit un subiect din ce în ce mai important. Termenul de *semnătură electronică* are interpretări mai largi, pornind de la semnături criptografice digitale până la o imagine scanată a unei semnături de mână. În ambele cazuri, se defineşte calea pentru utilizarea legală a semnăturilor digitale în comunicațiile electronice.

Semnăturile digitale pot ajuta la identificarea şi autentificarea persoanelor, organizațiilor şi a calculatoarelor prin Internet, putând fi utilizate şi pentru a verifica integritatea datelor după terminarea tranzitului.

Semnăturile digitale sunt asemănătoare semnăturilor de mână, care sunt utilizate zilnic pentru a identifica un individ într-o manieră legală. De exemplu, în momentul în care o persoană se decide asupra termenilor unui contract, includerea unei semnături de mână indică faptul că acea persoană este de acord cu termenii acelui contract. În continuare, persoana respectivă nu ar mai trebui să nege faptul că a semnat acel document sau că termenii acelui contract nu corespund dorințelor lui, decât în caz de falsificare. În mod asemănător, semnăturile digitale pot identifica persoana care a semnat o tranzacție sau un mesaj, dar spre deosebire de semnăturile de mână, o semnătură digitală poate ajuta în verificarea faptului că un document sau o tranzacție nu a fost modificată față de starea originală din momentul semnării.

Deosebirea principală față de semnătura de mână este aceea că, în cazul în care sistemul a fost implementat corespunzător, semnătura digitală nu se poate falsifica. În condiții ideale, acest lucru poate însemna faptul că un mesaj semnat digital trebuie să aparțină persoanei a cărei semnătură apare în mesaj. Incapacitatea de a nega faptul că un mesaj sau o tranzacție a fost executată (semnată, în acest caz) se numeşte ***nerepudiere***.

Semnătura digitală oferă trei servicii de securitate de bază: autentificare, integritate şi nerepudiere.

Semnăturile digitale obțin un grad ridicat de securitate prin utilizarea a două tehnici de criptografie: criptarea cu cheie publică şi hashing. Crearea unei semnături digitale presupune hashing-ul datelor, apoi criptarea mesajului rezultat cu o cheie privată. Orice persoană care deține cheia publică corespondentă va fi capabil să verifice faptul că mesajul hash corespunde mesajului original.

Scopul semnăturilor digitale este acela de a identifica în mod pozitiv expeditorul unui mesaj şi de a asigura faptul că datele nu au fost modificate. Dar, există şi probleme

care pot apărea în timpul instalării şi utilizării acestei tehnologii în mod securizat. De exemplu, utilizarea unui algoritm de hash slab oferă o securitate scăzută în combinație cu un algoritm de criptare puternic. Din nefericire, simpla vizualizare a unui mesaj hash nu este suficientă pentru a detecta utilizarea unui algoritm slab.

Înțelegerea riscurilor asociate cu utilizarea semnăturilor digitale presupune înțelegerea limitărilor acestei tehnologii. Astfel, o semnătură digitală, când nu este legată de numele utilizatorului printr-un certificat digital, nu are nici o semnificație. Distribuirea securizată a semnăturii digitale este singura garanție a securității ei. În cazul în care este nevoie de o distribuire la scară a cheilor publice pentru verificarea semnăturilor digitale, trebuie creată o bază de date la care persoanele interesate să aibă acces de citire, în timp ce scrierea trebuie restricționată cu cele mai puternice tehnologii.

Poate cel mai mare risc al semnăturilor digitale este acordarea unei prea mari încrederi acestei tehnologii. Semnăturile de mână pot fi falsificate sau fotocopiate într-un nou document, dar acest lucru nu ar trebui să fie valabil într-un sistem de semnături digitale implementat în mod corespunzător. O semnătură de mână poate să ofere o certitudine până la ruperea modelului de încredere. Problema cu semnăturile digitale este aceea că nu se ştie încă unde şi când nu se mai poate vorbi de încrederea acordată sistemului.

7.2.6. Certificate digitale. Riscuri de securitate

O semnătură digitală în sine nu oferă o legătură puternică cu o persoană sau o entitate. Cum se poate şti că o cheie publică utilizată pentru a crea o semnătură digitală aparține într-adevăr unui individ anume şi că acea cheie este încă validă? Pentru acest lucru este necesar un mecanism care să ofere o legătură între cheie publică şi un individ real, funcție îndeplinită de ***certificatele digitale***.

Certificatele digitale pot oferi un nivel ridicat de încredere asupra faptului că persoana al cărei nume apare pe acel certificat are ca şi corespondent o anumită cheie publică. Această încredere este realizată prin utilizarea unei terțe părți, cunoscută sub numele de ***Autoritate de Certificare*** (Certificate Authority - CA). O autoritate de certificare semnează un certificat în calitate de garant pentru identitatea unei persoane al cărei nume apare pe certificatul respectiv. Formatul curent acceptat pentru certificate digitale este X.509v3.

Standardul X.509v3 definit în RFC 2459 descrie un format agreat de certificate digitale. Acest standard defineşte elementele unui certificat:

- *Certificate Version* - indică versiunea formatului unui certificat;
- *Serial Number* - un număr unic asignat de către autoritatea de certificare, utilizat pentru urmărirea certificatelor;
- *Signature* - identifică algoritmul de criptare şi funcțiile de tip *message digest* suportate de CA;
- *Issuer name* - numele emitentului (al CA);
- *Period of Validity* - datele între care certificatul este valid. Această perioadă nu exclude ca certificatul să fie revocat;
- *Subject* - numele proprietarului certificatului;
- *Subject's Public Key Info* - cheia publică şi algoritmul asociat cu câmpul Subject;

- *Issuer Unique ID* - un câmp opţional utilizat pentru a identifica emitentul certificatului sau autoritatea de certificare. Utilizarea acestui câmp nu este recomandată în RFC 2459;
- *Extensions* - câmp opţional utilizat pentru extensii proprietare. Acest câmp nu este definit dar cuprinde articole precum: alte denumiri ale subiectului, informaţii pentru utilizarea cheilor şi punctele de distribuţie a listelor de revocare a certificatelor (Certificare Revocation List - CRL);
- *Encrypted* - acest câmp conţine semnătura în sine, identificatorul algoritmului, hash-ul securizat al celorlalte câmpuri din certificat şi o semnătură digitală a hash-ului.

Formatul certificatului digital este relativ uşor de înţeles, dar schimbul de certificate între persoane poate ridica anumite dificultăţi. Asigurarea faptului că un certificat aparţine unui utilizator anume este dificil de realizat. De exemplu, într-o organizaţie pot exista mai multe persoane cu numele *Ioan Popescu*, dar numai unul dintre ei este utilizatorul vizat al certificatului.

Certificatele necesită mijloace de gestionare a creării acestora, distribuirea lor, stocarea centralizată, revocarea, backup-ul cheilor şi actualizarea acestora. Acest sistem de management este cunoscut sub numele de *infrastructura de chei publice* (*Public Key Infrastructure* - PKI).

O infrastructură de chei publice este o arhitectură de securitate creată pentru a facilita instalarea tehnologiei de chei publice. Între componentele unui PKI se pot număra un depozit de certificate (de obicei un serviciu director compatibil LDAP), certificatele digitale, listele de revocare a certificatelor (CRL), software-ul pentru aceste aplicaţii, precum şi aspectul uman al acestor proceduri.

O PKI cuprinde câteva servicii de bază de securitate între care se numără autentificarea utilizatorilor, confidenţialitatea şi integritatea, ajutând de asemenea la implementarea nerepudierii.

O autoritate de certificare este o componentă a infrastructurii generale de chei publice şi este o componentă critică pentru o implementare la scară a acestei infrastructuri. Funcţia principală a unei autorităţi de certificare este aceea de a certifica faptul că perechea cheie publică / cheie privată aparţine într-adevăr unui individ anume.

Obţinerea certificatelor digitale se poate face în mai multe moduri, în funcţie de scopul acestora. De exemplu, se poate utiliza *Microsoft Certificate Services* din Windows 2000/2003 pentru a instala certificate auto-emise.

O altă opţiune este obţinerea unor certificate de la un distribuitor de certificate. Unul dintre cei mai mari distribuitori este VeriSign. Acesta oferă certificate pentru S/MIME, SSL (client şi server), *Server Gated Cryptography* (SGC) pentru instituţii financiare, certificate de tip Authenticode pentru publicarea de software, etc.

Certificatele digitale pot reprezenta un mecanism puternic de autentificare, în special în momentul în care sunt stocate pe smart card-uri. Dar, pentru ca certificatele digitale să reprezinte o securitate adecvată, trebuie rezolvate mai întâi problemele de *încredere*. De exemplu, o autoritate de certificare trebuie să posede mecanisme de securitate puternice pentru a identifica în mod pozitiv toţi participanţii care doresc asemenea certificate. Întrebarea "cât de bine identifică o autoritate de certificare un viitor posesor?" determină securitatea de ansamblu a infrastructurii de chei publice.

Dacă scopul unui certificat este de a lega un individ de o semnătură digitală, cum se poate cunoaşte că certificatul aparţine într-adevăr persoanei reale şi nu unui

impostor? Poate că certificatul aparţine unui utilizator neintenţionat cu acelaşi nume ca şi al utilizatorului real. Multe certificate se bazează pe numele care apar în câmpul *Subject* pentru a identifica posesorul.

În cazul în care funcţia unei autorităţi de certificare este aceea de a certifica identitatea unui individ şi de a oferi servicii de nerepudiere, acest lucru ridică şi probleme de răspundere sau obligaţie.

O altă problemă cu certificatele digitale este reprezentată de faptul că listele de revocare a certificatelor (CRL) sunt verificate foarte rar, inclusiv de către browser-ele Web. Un certificat poate fi revocat din mai multe motive, între care se numără compromiterea cheii, compromiterea autorităţii de certificare sau o schimbare a autorităţii de certificare. Problemele legate de distribuirea listelor de revocare a certificatelor nu au fost încă rezolvate pe deplin.

7.2.7. Autentificarea Kerberos V5

Kerberos V5, protocolul principal de securitate pentru autentificare într-un domeniu, verifică atât identitatea utilizatorului cât şi a serviciilor de reţea. Această dublă verificare este cunoscută şi sub numele de ***autentificare reciprocă***. Acest protocol, dezvoltat iniţial la MIT, este capabil să ofere servicii puternice de autentificare într-un mediu de calcul distribuit. Totodată, prin includerea lui ca protocol de autentificare implicit într-un domeniu Windows 2000/2003, a fost accelerat procesul de dezvoltare a aplicaţiilor bazate pe acesta.

Modelul Kerberos se *bazează* pe faptul că aplicaţia client şi aplicaţia server nu trebuie neapărat să-şi acorde reciproc încredere, ci ambele trebuie să acorde încredere unui centru de distribuţie a cheilor (Key Distribution Center - KDC). Kerberos oferă un sistem de mesaje criptate numite tichete, care asigură în mod securizat încrederea reciprocă dintre două maşini din reţea. Utilizând Kerberos, parolele nu mai sunt transmise în reţea, nici chiar în format criptat. În cazul în care un tichet Kerberos este interceptat, acesta rămâne protejat deoarece este criptat.

Odată ce o maşină client obţine un tichet către un anume server, tichetul este păstrat pe maşina locală până la expirare, făcând astfel Kerberos un sistem de autentificare foarte eficient. În funcţie de implementare, un tichet Kerberos expiră de obicei după opt ore. În mod implicit Kerberos utilizează criptarea cu cheie simetrică. O implementare Kerberos standard are de obicei următoarele componente:

- ***Principal*** - un calculator, utilizator sau entitate care va fi autentificată;
- ***Realm*** (domeniu în Windows 2000/2003) - o grupare logică de obiecte de tip *principal* care va fi protejată de Kerberos. Toate conturile utilizatorilor şi resursele protejate rezidă în interiorul unui realm Kerberos;
- ***Key Distribution Center*** (KDC) - partea din implementarea Kerberos care autentifică obiectele de tip *principal.* KDC distribuie chei secrete şi mediază comunicaţia securizată între un calculator client şi resursele din reţea. Cheile secrete sunt stocate în *Key Distribution Center;*
- ***Ticket Granting Service*** (TGS) - oferă tichete de tip sesiune pentru accesarea altor resurse dintr-un realm Kerberos. De obicei TGS rulează în *Key Distribution Center;*
- ***Ticket Granting Ticket*** (TGT, sau tichet utilizator în Windows 2000/2003) - un jeton de securitate care verifică faptul că o entitate a fost autentificată.

TGT asigură faptul că utilizatorii nu mai trebuie să reintroducă parola după un login iniţial, până la expirarea tichetului.

- ***Session Ticket*** (ST, sau tichet de serviciu în Windows 2000/2003) - un jeton de securitate care permite unui obiect de tip principal să acceseze resurse protejate. Pentru accesarea oricărei aplicaţii care utilizează Kerberos este necesar un tichet de sesiune valid.

7.2.7.1. Cum funcţionează Kerberos V5

Mecanismul de securitate din Kerberos V5 emite tichete pentru accesarea serviciilor de reţea. Aceste tichete conţin date criptate, inclusiv o parolă criptată care confirmă identitatea utilizatorului faţă de serviciul accesat.

Un serviciu important în Kerberos V5 este *Key Distribution Center* (KDC) care rulează pe fiecare controler de domeniu parte a Active Directory, în care se stochează toate parolele clienţilor precum şi alte informaţii.

Procesul de autentificare Kerberos V5 urmează paşii:

- utilizatorul unui sistem client, utilizând o parolă sau un smart card, se autentifică faţă de KDC;
- KDC emite clientului un tichet de tip *Ticket Granting Ticket.* Sistemul client utilizează acest jeton TGT pentru a accesa *Ticket Granting Service* (TGS), care este parte a mecanismului de autentificare dintr-un controler de domeniu;
- TGS emite un tichet de serviciu către client;
- clientul prezintă acest tichet serviciului de reţea accesat. Tichetul de serviciu dovedeşte atât identitatea utilizatorului către serviciu, cât şi a serviciului faţă de client.

În Windows 2000/2003 serviciile Kerberos V5 sunt instalate pe fiecare controler de domeniu, iar clientul Kerberos este instalat pe fiecare staţie de lucru şi server.

Fiecare controler de domeniu se comportă ca şi un *Key Distribution Center*. Un client utilizează *Domain Name Service* (DNS) pentru a localiza cel mai apropiat controler de domeniu, care va funcţiona ca şi KDC preferat pentru utilizator în timpul sesiunii de logon. În cazul în care KDC nu mai este disponibil, sistemul localizează un KDC alternativ, pentru autentificare.

7.2.7.2. Riscuri de securitate în Kerberos

Principala slăbiciune a Kerberos este aceea că rămâne vulnerabil la atacurile date prin "ghicirea" parolei. Dacă utilizatorul alege o parolă "slabă", este posibil ca tichetul să fie colectat şi decriptat, impersonându-se astfel utilizatorul. Parolele statice sunt cel mai mare punct de slăbiciune în orice sistem de securitate, deoarece utilizatorii nu aleg de obicei parole greu de găsit. Prin mariajul tehnologiei de criptare cu cheie publică cu Kerberos se face un pas important în înlăturarea acestei slăbiciuni.

De asemenea, Kerberos presupune faptul că gazdele nu au fost compromise. În esenţă, Kerberos este un model al gazdelor cu relaţii de încredere (sigure) într-o reţea nesigură. În cazul în care viaţa tichetului este setată prea lungă, protocolul devine nesigur prin expunerea unui tichet de serviciu pentru o perioadă de timp prea mare. Iar dacă viaţa tichetului este prea scurtă, aceasta poate avea un impact negativ asupra performanţelor şi utilizării.

Utilizarea DES în Kerberos poate fi de asemenea o problemă, deoarece DES nu mai este considerat un algoritm sigur. Dar Kerberos permite şi utilizarea altor algoritmi de criptare, mai puternici, precum Triple-DES.

Alte riscuri de securitate mai pot fi considerate şi relaţiile tranzitive de încredere şi abilitatea de a înainta tichetele.

7.2.8. Autentificarea SSL/TLS

Secures Sockets Layer (SSL), tehnologia care permite utilizarea certificatelor digitale, este un protocol din nivel transport care oferă o securitate deosebită de tip *end-to-end,* prin securizarea sesiunii din punctul de origine până în punctul destinaţie.

SSL se referă în general la securitatea comunicării între două părţi. Acest lucru poate însemna comunicarea dintre un browser Web şi un server Web, o aplicaţie e-mail şi un server e-mail sau chiar canalele de comunicaţie dintre două servere. SSL poate de asemenea să autentifice un server şi, în mod opţional, un client. SSL a devenit astfel, metoda de facto pentru securizarea comerţului electronic prin Internet.

SSL este un protocol orientat pe conexiuni care necesită ca atât aplicaţia client cât şi serverul să cunoască acest protocol. În cazul în care este necesar SSL la nivelul unui server, aplicaţiile care nu pot să utilizeze acest protocol nu vor putea comunica cu acesta.

SSL oferă servicii de securitate printre care se numără:

- confidenţialitatea (privacy),
- autentificarea şi
- integritatea mesajului.

SSL oferă integritatea mesajului prin utilizarea unei verificări de securitate cunoscută sub numele de *codul de autentificare al mesajului (message authentication code* - MAC). MAC asigură faptul că sesiunile criptate nu sunt modificate în timpul tranzitului.

SSL oferă autentificarea serverului prin utilizarea tehnologiei de criptare cu cheie publică şi, în mod opţional, poate autentifica anumiţi clienţi prin necesitatea existenţei de certificate digitale la nivel de client. În practică, certificatele pentru clienţi nu sunt disponibile pe scară largă deoarece nu sunt uşor portabile între maşini, pot fi uşor pierdute sau distruse, fiind în trecut şi dificil de instalat în aplicaţiile reale. De asemenea, multe site-uri Web au găsit satisfăcătoare din punct de vedere al securităţii pentru cele mai multe cazuri, combinaţia de SSL utilizată împreună cu un nume de utilizator şi o parolă.

Internet Engineering Task Force (IETF) este organizaţia responsabilă pentru dezvoltarea standardului SSL. Noul standard este cunoscut sub numele de *Transport Layer Security* (TLS), dezvoltat iniţial de *Netscape Communications Corporation.* TLS 1.0 definit în RFC 2246, oferă îmbunătăţiri minore faţă de SSL 3.0. În realitate TLS este SSL 3.1

Noile îmbunătăţiri cuprind: raportarea unui număr de versiune, diferenţe în tipurile de protocoale, tipuri de mesaje de autentificare, generarea cheilor şi verificarea certificatelor. În plus, TLS elimină suportul pentru algoritmul Fortezza, o familie de produse de securitate care cuprinde soluţiile de securitate *Personal Computer Memory Card International Association* (PCMCIA). Deoarece TLS este un standard deschis, este de aşteptat ca întreaga comunitate Internet să coopereze pentru îmbunătăţirea performanţei şi securităţii acestuia.

7.2.8.1. Legătura SSL-HTTP

Sesiunile Web standard utilizează *HyperText Transfer Protocol* (HTTP) pentru a stabili canale de comunicație prin rețelele TCP/IP. SSL a fost creat ca şi un protocol de securitate separat, care îmbunătățeşte standardul HTTP.

Din punct de vedere logic, SSL se inserează între protocolul aplicație HTTP şi nivelul de conversație TCP, din punctul de vedere al TCP SSL fiind doar un alt nivel protocol de nivel aplicație. Deoarece SSL se comportă ca o îmbunătățire, adăugarea SSL la protocoalele existente este simplă, nemainecesitând rescrierea protocoalelor de bază.

Din cauza acestui design flexibil, SSL este capabil să cripteze aproape întregul trafic bazat pe TCP. Mai mult, SSL a fost utilizat pentru a oferi securitate la nivel de sesiune pentru e-mail (SMTPS, POP3S, IMAPS), news (NNTPS), LDAP (LDAPS), IRC (IRCS), Telnet (Telnets), FTP (FTPS). Dar SSL nu poate să îmbunătățească transmisiunile prin UDP.

În general traficul Web bazat pe SSL este configurat să utilizeze portul 443 în locul portului standard 80. Browser-ele Web vor crea o sesiune SSL prin utilizarea HTTPS în locul HTTP.

7.2.8.2. Cum funcționează SSL

Pentru funcționarea unei sesiuni bazată pe SSL, trebuie luate în calcul o serie de elemente. Astfel, serverul Web necesită un certificat digital împreună cu o cheie privată corespunzătoare.

Cel mai mare distribuitor de certificate pentru server este VeriSign. Obținerea şi instalarea unui certificat SSL de la VeriSign presupune un proces în mai mulți paşi: generarea unei cereri, trimiterea unui *Certificate Signing Request* (CSR), completarea unui formular prin care se autentifică un utilizator sau o afacere, instalarea identificatorului de server şi activarea SSL pentru serverul Web. Autentificarea prin VeriSign presupune şi verificarea datelor trimise de organizația care necesită un certificat.

Înainte de stabilirea unei sesiuni SSL, clientul trebuie să cunoască de asemenea acest protocol. În momentul existenței elementelor necesare, clientul şi serverul pot stabili o conexiune securizată.

Procesul prin care se stabileşte o conexiune între un client şi un server (de exemplu cumpărare online), se desfăşoară în mai mulți paşi. SSL utilizează o combinație de criptări cu chei publice şi secrete. Datele brute ale unei sesiuni SSL sunt întotdeauna criptate cu cheia secretă, fiind mult mai puțin consumatoare de resurse din punct de vedere al procesării decât criptarea cu cheie publică. Protocolul SSL/TLS suportă mai mulți algoritmi de criptare cu cheie secretă, printre care DES, Triple-DES, IDEA, RC2 şi RC4. Algoritmii cunoscuți pentru schimbarea cheilor cuprind Diffie-Hellman şi RSA.

O sesiune SSL cuprinde următorii paşi:

- **ClientHello** - în acest pas, clientul trimite un mesaj către server (ClientHello) cerând opțiuni de conectare SSL, între care numărul de versiune al SSL, setările cifrului, date generate în mod aleator care stau la baza calculelor criptografice şi metoda de compresie utilizată;
- **ServerHello** - după primirea mesajului ClientHello, serverul ia la cunoştință recepția prin trimiterea unui mesaj ServerHello care conține numărul de

versiune al protocolului, setările cifrului, date generate aleator, metoda de compresie şi identificatorul de sesiune;

- **ServerKeyExchange** - imediat după trimiterea ServerHello, serverul trimite un mesaj de tip ServerKeyExchange către client care conține certificatul cu cheia publică. În cazul în care sunt necesare şi certificate din partea clienților, este generată o cerere în acest sens;
- **ServerHelloDone** - după ServerKeyExchange, serverul trimite un mesaj final prin care se indică finalizarea negocierii inițiale;
- **ClientKeyExchange** - după recepționarea mesajului de tip ServerHelloDone, clientul răspunde cu mesajul ClientKeyExchange care constă în cheia simetrică a sesiunii, criptată cu cheia publică a serverului, primită în pasul 3;
- **ChangeCipherSpec** - în acest pas clientul trimite către server un mesaj de tip ChangeCipherSpec în care specifică ce setări de securitate ar trebui invocate /utilizate;
- **Finished** - clientul trimite mesajul Finished, prin care se permite determinarea finalizării cu succes a negocierii şi dacă opțiunile de securitate au fost sau nu compromise în orice stagiu anterior;
- **ChageCipherSpec** - serverul trimite către client un mesaj de tip ChangeCipherSpec, prin care se activează opțiunile de securitate invocate;
- **Finished** - serverul trimite un mesaj de tip Finished, permițând clientului să verifice opțiunile de securitate activate. După trimiterea acestui mesaj, negocierea este finalizată, iar conexiunea este stabilită. În continuare, toate comunicațiile sunt criptate, până la terminarea sau finalizarea sesiunii.

7.2.8.3. Performanța SSL

Dacă SSL oferă o asemenea securitate, de ce nu se criptează întregul trafic? Deşi este o idee bună, în procesul de criptare şi stabilire a unei conexiuni SSL este implicat şi foarte mult trafic adițional, din cauza naturii protocolului HTTP care creează o nouă sesiune pentru fiecare obiect cerut dintr-o pagină Web.

De exemplu, într-o simplă tranzacție în care browser-ul cere o singură pagină de text cu patru imagini, generează cinci cereri GET (una pentru pagină şi patru pentru imagini). Prin utilizarea SSL, pentru fiecare din aceste sesiuni trebuie negociate chei separate de criptare. Pentru a înrăutăți şi mai mult lucrurile, utilizatorii frustrați de timpul de răspuns reîncarcă pagina în browser-ul Web (refresh), generând şi mai multe conexiuni SSL.

Pentru îmbunătățirea performanțelor SSL se pot aplica următoarele:

- utilizarea de acceleratoare de criptare hardware, proces care nu necesită rescrierea paginilor Web sau achiziționarea de servere adiționale;
- utilizarea de pagini SSL simple, cu cât mai puține imagini; utilizarea SSL numai pentru anumite pagini Web selectate, precum acelea prin care se trimit informații privitoare la cărțile de credit; cache-ingul conexiunilor SSL permite de asemenea îmbunătățirea performanțelor, deoarece stabilirea unei noi conexiuni necesită de cinci ori mai mult timp decât reconectarea la o sesiune păstrată în cache. Cu toate acestea, activarea sesiunilor SSL în cache este dificil de implementat - dacă timpul de expirare este stabilit prea mare, serverul poate consuma prea multă memorie prin păstrarea conexiunilor neutilizate. De asemenea, cache-ul

conexiunilor nu ar putea fi dezirabil din punct de vedere al securității paginilor dintr-un site. De exemplu, o aplicație bancară online ar trebuie să favorizeze securitatea şi să nu activeze cache-ingul conexiunilor.

7.2.8.4. Riscuri de securitate în SSL

SSL nu oferă nici o protecție în afara sesiunilor, iar serverele Web care permit utilizarea SSL nu pot să ofere protecție pentru date care sunt stocate în format text în server.

SSL nu oferă protecție împotriva atacurilor bazate pe Web precum exploatarea diverselor puncte slabe prin scripturi CGI. De asemenea, SSL nu oferă nici un mecanism pentru controlarea drepturilor de securitate (ceea ce îi este permis unei persoane să facă după autentificarea pe un server).

În cele din urmă, SSL nu protejează împotriva atacurilor de tip ***Denial of Service*** şi rămâne vulnerabil la analiza traficului. Pentru a oferi un nivel de securitate adecvat, serverele care lucrează cu SSL ar trebui să suporte criptarea pe 128 biți şi o cheie publică pe 1024 biți.

Certificatele la nivel de server auto-semnate pot oferi securitate, dar nu şi autentificare. Un certificat auto-semnat nu este considerat sigur de către maşina client fără a executa anumiți paşi adiționali.

7.2.9. Autentificarea NTLM

Într-un mediu de rețea, NTLM este utilizat ca şi protocol de autentificare pentru tranzacțiile dintre două calculatoare în care unul dintre ele rulează Windows NT 4.0 sau mai mic iar celălalt Windows 2000 sau mai mare.

În exemplele următoare se utilizează NTLM ca mecanism de autentificare:

- un client Windows 2000 sau Windows XP Professional care se autentifică într-un controler de domeniu Windows NT 4.0;
- o stație de lucru client Windows NT 4.0 Workstation care se autentifică într-un domeniu Windows 2000 sau Windows 2003;
- o stație de lucru Windows NT 4.0 Workstation care se autentifică într-un domeniu Windows NT 4.0;
- utilizatorii dintr-un domeniu Windows NT 4.0 care se autentifică într-un domeniu Windows 2000 sau Windows 2003.

Pe lângă acestea, NTLM este protocolul de autentificare pentru calculatoarele care nu participă într-un domeniu, precum stațiile de lucru sau serverele independente.

7.2.10. Comparație Kerberos - NTLM

Pe măsură ce a crescut popularitatea Windows NT 4.0, a crescut şi interesul de securizare a sistemului, iar prin adăugarea autentificării Kerberos în Windows 2000, Microsoft a crescut în mod semnificativ facilitățile sistemului de operare. În versiunile Windows 2000/2003 NT LAN Manager (NTLM) este oferit numai pentru compatibilitate înapoi, cu Windows NT, şi ar trebui dezactivat îndată ce clienții din rețea se pot autentifica utilizând Kerberos.

Kerberos are anumite beneficii față de NTLM. Astfel, Kerberos se *bazează* pe standarde în vigoare, deci permite Windows 2000/2003 să interacționeze cu alte rețele care utilizează Kerberos V5 ca mecanism de autentificare. NTLM nu poate oferi această

funcționalitate deoarece este un protocol proprietate a sistemelor de operare de la Microsoft.

Conexiunile la serverele de aplicații şi fişiere sunt mai rapide în momentul utilizării autentificării bazate de Kerberos, deoarece serverul Kerberos trebuie să verifice numai datele oferite de client pentru a determina dacă îi permite accesul. Aceleaşi date oferite de client pot fi utilizate în întreaga rețea, pe întreaga durată a sesiunii de logon. În momentul utilizării NTLM, aplicațiile şi serverele trebuie mai întâi să contacteze un controler de domeniu pentru a determina dacă clientului îi este permis accesul.

Autentificarea Kerberos este oferită atât pentru client cât şi pentru server, în timp ce NTLM oferă numai autentificare pentru client. Astfel, clienții NTLM nu ştiu cu siguranță dacă serverul cu care comunică nu este unul fals.

Kerberos oferă şi posibilitatea relațiilor de încredere, fiind baza pentru relațiile tranzitive dintre domenii din Windows 2000/2003. O relație tranzitivă de încredere este o relație în două sensuri deoarece este creată o cheie inter-domenii, partajată de ambele domenii.

Există şi considerații asupra faptului că implementarea Kerberos a Microsoft nu este una standard, mai ales din cauza modificărilor şi extensiilor care au fost aduse protocolului. Aceste modificări privesc mai ales utilizarea Kerberos cu tehnologia de criptare cu cheie publică, făcând astfel posibilă autentificarea prin smart card, care este mult mai sigur decât o parolă statică.

7.2.11. SSH

UNIX este un sistem de operare sofisticat şi matur care a fost dezvoltat de Bell Labs la începutul anilor 1970. Pe măsura trecerii anilor, Unix a avut partea sa de probleme de securitate, multe dintre ele fiind rezolvate. În general, Unix este considerat a fi un sistem de operare sigur şi stabil când este configurat în mod corect. Cu toate acestea, există o serie de protocoale care continuă să defăimeze securitatea sistemelor Unix, printre acestea numărându-se Telnet, FTP precum şi faimoasele comenzi de la Berkley de tip „r*" (rcp, rsh, rlogin). Programe şi protocoale nesigure continuă să ofere acces uşor la sistem atât pentru administratori cât şi pentru utilizatori răuvoitori. Aceste protocoale rămân vulnerabile în mare parte datorită faptului că datele de autentificare sunt trimise prin rețea sub formă de text clar, acesta semnificând că oricine poate să obțină numele de utilizator şi parola, exploatând apoi un serviciu prin impersonarea utilizatorului legitim.

Dezvoltat de Tatu Ylönen în 1995, ***Secure Shell*** (SSH) oferă servicii de securitate la nivel de sesiune precum şi confidențialitatea datelor în rețele nesigure, oferind o înlocuire sigură a comenzilor rsh, rlogin, rcp, telnet, rexec şi ftp. Securitatea SSH este dependentă de criptarea sesiunii de lucru de tip *end-to-end* între un client şi un server. SSH are de asemenea posibilitatea să autentifice în mod sigur maşinile înainte de a trimite informațiile de login.

SSH este utilizat în general pentru a accesa un calculator de la distanță şi pentru a executa comenzi. SSH oferă de asemenea securizarea transferului de fişiere între maşini prin executarea copierii securizate (SCP) şi a transferului de fişiere securizat (SFTP). SSH poate ajuta de asemenea în securizarea traficului X11 prin trimiterea acestuia printr-un tunel criptat. În acest fel SSH a fost utilizat pentru a defini o formă primitivă de rețea privată virtuală între gazde.

Componentele SSH cuprind serverul (SSHD), clientul (SSH), copierea (SCP) securizată a fişierelor şi *ssh-keygen* - o aplicaţie utilizată pentru a crea chei publice şi private utilizate pentru autentificarea maşinilor.

SSH oferă facilităţi de bază pentru translatarea porturilor, prin aceasta permiţându-se utilizatorilor să creeze tuneluri pentru protocoalele existente prin conexiunile SSH existente. De exemplu, transferul de date prin POP (care în mod normal trimite numele de utilizator şi parola sub formă de text clar), pot fi securizate prin SSH. Există şi limitări ale translatării porturilor, deoarece nici intervalele de porturi, nici porturile dinamice nu pot fi specificate.

Deşi translatarea porturilor ajută în securizarea protocoalelor, precum POP, există şi riscuri prin activarea acestei opţiuni - de exemplu, prin activarea unei conexiuni SSH de ieşire se poate permite unui utilizator să traverseze un firewall prin transformarea protocoalelor (tuneluri) de intrare care nu sunt permise de firewall prin sesiuni criptate SSH.

Utilizarea opţiunilor de autentificare a SSH protejează utilizatorii şi maşinile împotriva atacurilor de tip *IP Spoofing*, rutarea sursei IP, spoofing DNS, etc.

SSH constă în trei niveluri: nivelul protocolul de transport, nivelul de autentificare precum şi nivelul conexiune. Protocolul transport este responsabil pentru gestionarea negocierii cheilor de criptare, cererilor de regenerare a cheilor, mesajelor de cereri de servicii precum şi a mesajelor de deconectare a serviciilor. Protocolul de autentificare este responsabil pentru negocierea tipurilor de autentificare, verificarea canalelor securizate înaintea trimiterii informaţiilor de autentificare precum şi pentru cererile de modificare a parolelor. Protocolul de conectare controlează deschiderea şi închiderea canalelor precum şi a translatării porturilor.

Există două versiuni de SSH - v1 şi v2, iar clienţi SSH există pentru mai multe platforme - Unix, Windows, Machintosh, OS/2. Există şi versiuni de componente de server pentru Windows NT/2000.

7.2.11.1. Autentificarea prin SSH

SSH oferă câteva mecanisme pentru autentificarea utilizatorilor în funcţie de versiunea SSH utilizată. Cea mai slabă formă de autentificare este realizată prin intermediului fişierelor .rhosts, această metodă nefiind recomandată a fi selectată deoarece este foarte puţin sigură.

Altă metodă de autentificare este oferită de criptarea prin RSA. Utilizând această metodă, utilizatorul creează o pereche publică/privată de chei prin utilizarea programului *ssh-keygen*, cheia publică fiind stocată în directorul părinte al utilizatorului. În momentul în care clientul se autentifică în faţa serverului, trimite numele de utilizator şi cheia publică spre gazda de la distanţă. Serverul returnează cheia de sesiune criptată cu cheia publică a utilizatorului. Această cheie de sesiune va fi decriptată cu cheia privată a utilizatorului.

Metoda principală de autentificare în SSH este prin intermediul fişierelor .rhosts combinată cu autentificarea RSA. Această metodă autentifică clientul şi serverul şi le protejează împotriva atacurilor curente de tip *IP Spoofing*, *DNS Spoofing*, etc. Există şi posibilitatea instalării de TCPWrapper în locul utilizării fişierelor .rhosts, existând astfel un control mai mare asupra utilizatorilor care încearcă să se conecteze la un serviciu.

În cele din urmă, unui utilizator îi poate fi cerută o combinaţie de nume de utilizator / parolă printr-un canal criptat. De asemenea, în diverse implementări există suport pentru Kerberos, S/KEY şi SecurID.

Stabilirea unei conexiuni SSH este inițiată de comenzile *slogin* sau *ssh*, fapt care duce la verificare autentificării cu cheia publică atât pentru server cât şi pentru client apoi fiind stabilit un canal de comunicație sigur.

7.2.11.2. SSH1

Versiunea originală a SSH, versiunea 1, este distribuită în mod gratuit pentru utilizare necomercială, împreună cu codul sursă. SSH1 are şi variante majore (1.2, 1.3 şi 1.5). Deşi s-au descoperit câteva probleme de securitate, SSH este considerat în continuare sigur, dată fiind atenția acordată metodei de autentificare şi cifrului utilizat. De exemplu, SSH1 este vulnerabil la atacurile prin inserarea datelor, deoarece acesta utilizează CRC pentru verificarea integrității datelor. Dar utilizarea algoritmului de criptare *Triple-DES* rezolvă această problemă.

SSH 1 suportă o mai mare varietate de metode de autentificare față de versiunea 2, între care se numără AFS (bazat pe *Andrew File System* dezvoltat la Carnegie-Mellon) şi Kerberos.

7.2.11.3. SSH 2

SSH 2 este o rescriere completă a SSH1 prin care se adaugă noi facilități, inclusiv suport pentru protocoalele FTP şi TLS. Din cauza diferențelor de implementare a protocoalelor, cele două versiuni nu sunt compatibile în întregime. SSH2 oferă îmbunătățiri în ceea ce priveşte securitatea şi portabilitatea. SSH2 necesită mai puțin cod care să ruleze cu privilegii de *root*, fiind mai puțin expus exploatărilor de tip *buffer overflow;* astfel este mai puțin probabil ca un atacator să rămână pe server cu drepturi de *root.*

SSH2 nu oferă aceleaşi implementări de rețea ca şi SSH 1, deoarece criptează părți diferite ale pachetelor. SSH2 nu suportă metoda de autentificare prin fişierele .rhosts. De asemenea, în SSH2 algoritmul RSA este înlocuit de *Digital Signature Algorithm* (DSA) şi de *Diffie-Hellman*, dar, deoarece patentele RSA au expirat, este de aşteptat suportul în continuare pentru algoritmul RSA în versiunile următoare. SSH2 suportă *Triple-DES, Blowfish, CAST-128* şi *Arcfour.*

Din cauza diferențelor între SSH 1 şi SSH 2 şi din cauza restricțiilor de licențiere, ambele versiuni vor continua să fie utilizate pentru o perioadă de timp.

7.2.11.4. Algoritmii de criptare utilizați

În momentul stabilirii unei sesiuni SSH, atât clientul cât şi serverul SSH negociază un algoritm de criptare. Identitatea serverului este verificată înainte de trimiterea numelui de utilizator şi a parolei, fiind un proces care protejează împotriva aplicațiilor de tip *cal troian* care ar accepta conexiuni şi ar putea să „fure" informații de autentificare.

Pentru ca un client să se poată conecta la un server utilizând autentificarea prin cheie publică, această cheie trebuie distribuită în mod securizat. În funcție de versiune, SSH suportă mai mulți algoritmi de criptare, după cum se poate observa în Tabelul 7.2.

Tabelul 7.2.

Comparaţie între SSH1 şi SSH2	
SSH1	SSH 2
Triple - DES	Triple - DES - algoritm implicit
128bitRC4	128bitRC4
Blowfish	Blowfish
IDEA - algoritm implicit	Twofish
DES	Arcfour
RSA	CAST 128
-	DSA
-	Transferul cheilor prin Diffie Hellman

7.2.11.5. Ce poate proteja SSH. Riscuri de securitate ale SSH

În cazul existenţei conexiunilor de sosire către un server, SSH oferă un mecanism sigur şi eficient prin care se poate face accesul. Deoarece SSH este uşor de instalat, acesta ar trebui să fie singurul mecanism prin care să se ofere funcţionalitate de tip FTP, Telnet sau rlogin într-un mediu securizat, pentru utilizatorul final, SSH fiind aproape transparent.

SSH este o alternativă la programele care execută autentificarea în funcţie de adresa IP, iar în momentul utilizării autentificării cu cheie publică protejează împotriva programelor care utilizează parole reutilizabile. Prin criptarea sesiunii între client şi server se face protecţia împotriva interceptiei parolelor trimise sub formă de text clar.

SSH suferă şi de câteva limitări, între care imposibilitatea de a specifica un interval de porturi sau aceea de a translata porturi dinamice. În plus, versiunea de Windows nu implementează copierea securizată a fişierelor.

7.2.12. PGP. Riscuri de securitate

Trimiterea mesajelor de e-mail prin Internet este foarte asemănătoare cu trimiterea cărţilor poştale - în mod similar, un mesaj de e-mail poate fi citit de oricine care accesează transmisia. Acest lucru se poate întâmpla fără a fi cunoscut de expeditor sau de către destinatar. În plus, un mesaj poate fi interceptat, modificat şi retrimis.

Pretty Good Privacy (PGP) este un program de securitate care pune la dispoziţia utilizatorilor securitate avansată pentru mesaje de e-mail şi fişiere, prin utilizarea semnăturilor digitale şi a criptării. Implementat în mod corespunzător, PGP oferă servicii de confidenţialitate, integritate şi autentificare.

Programul original PGP a fost creat de Philip Zimmermann. Intenţia PGP a fost aceea de a oferi un mecanism pentru comunicare securizată între mai multe persoane cunoscute. Acest program utilizează atât tehnologia de criptare cu cheie publică cât şi pe cea de criptare cu cheie privată. PGP foloseşte algoritmul de 128 biţi IDEA pentru criptarea simetrică a mesajelor. Versiunea 5 şi mai mari suportă algoritmii CAST şi Triple-DES, iar versiunea 7 implementează o versiune a *Twofish.* Cheia secretă este generată pentru fiecare mesaj sau fişier criptat. Prin faptul că nu reutilizează cheia secretă, reduce şansele de reuşită ale cript-analizei (studierea recuperării unui text dintr-un format criptat fără accesul la cheie).

PGP suportă algoritmii de criptare cu cheie publică RSA, DSA şi Diffie-Hellman. Algoritmii de *hash* suportați sunt MD5, RACE *Integrity Primitives Evaluation-Message Digest* (RIPEMD) şi SHA-1.

Aplicația *PGP Desktop Security* cuprinde o serie de facilități de securitate mult mai avansate decât ar fi necesare unui sistem de e-mail, printre care sunt cuprinse un sistem personal de detecție a intruşilor, un firewall personal, comunicare bazată pe VPN sau IP Security (IPSec), criptarea discului cu PGP şi suport pentru certificate digitale X.509v3.

În momentul de față, PGP trece prin procesul de standardizare al IETF sub forma OpenPGP, definit prin RFC 2440.

Expedierea mesajelor PGP nu este complicată - în primul rând, mesajul este criptat cu o cheie aleatoare simetrică a sesiunii. Cheia sesiunii este criptată apoi cu cheia publică a destinatarului. În cazul în care mesajul este semnat, acesta este semnat cu cheia privată a expeditorului. Cheia criptată a sesiunii este apoi trimisă destinatarului împreună cu mesajul criptat. În momentul recepționării mesajului criptat cu PGP se desfăşoară procesul invers. PGP utilizează cheia privată a destinatarului pentru a decripta cheia sesiunii. În cele din urmă cheia sesiunii este utilizată pentru a decripta mesajul, iar clientul de e-mail afişează textul clar al mesajului.

Una din problemele privitoare la cheia publică de criptare este aceea de *încredere* în acea cheie publică. Pentru ca o criptare cu cheie publică să ofere securitatea adecvată, utilizatorii trebuie să fie siguri de faptul că cheia publică cu care se face criptarea aparține într-adevăr destinatarului intenționat. PGP încearcă să rezolve această problemă prin utilizarea unui model în care persoanele se încred reciproc. Această încredere (trust) este exprimată prin semnarea cheii PGP aparținând altei persoane. În realitate, orice utilizator PGP devine *Certificate of Authority* prin semnarea altor chei pentru alți utilizatori. În modelul de încredere PGP nu există nici o diferență între semnarea unei chei în calitate de CA sau de utilizator, lucru care diferă semnificativ în scenariul infrastructurii cu cheie publică, în care numai o autoritate de certificare poate să-şi exprime încrederea într-o cheie publică. Pe măsură ce alți utilizatori semnează cu cheia unui utilizator anume şi acel utilizator semnează alte chei, se creează o plajă de încredere.

Această încredere este bazată atât pe încrederea acordată unei chei publice ca fiind sau nu autentică cât şi pe încrederea acordată altor persoane care au semnat cheia. Acest lucru poate ridica probleme, deoarece cheile ar trebui să prezinte încredere numai în cazul în care există o persoană cunoscută şi de încredere care a semnat deja cheia. În alte cazuri, singura posibilitate de a şti că o cheie este autentică este obținerea acesteia printr-un mecanism foarte sigur, precum o întâlnire față în față. Acest model de încredere este potrivit pentru mesajele informale trimise prin Internet, dar nu se potrivește într-un scenariu de afaceri în care se cere nerespingerea şi contabilizarea utilizatorilor.

Revocarea cheilor PGP care nu mai prezintă încredere poate fi de asemenea o problemă. Singura modalitate de prevenire a utilizării unei chei PGP compromise este trimiterea unui certificat de revocare a cheii către toate persoanele care ar putea utiliza acea cheie. Acest certificat de revocare ar putea fi plasat pe un *keyserver* pentru a avertiza utilizatorii în privința cheii. Deoarece cheile pot fi stocate şi într-un inel de chei (key ring) pe maşina locală, nu există nici o garanție că toate persoanele vor primi avertismentul şi nu vor mai utiliza acea cheie compromisă.

Versiunea 7 a *PGP Desktop Security* introduce şi suport pentru certificatele digitale X.509v3, permițând astfel PGP să participe în infrastructura de chei publice şi să se depărteze (eventual) de modelul de securitate al PGP (plaja de încredere).

Deşi criptografia utilizată de PGP este puternică, există o mulțime de atacuri ce se pot aplica împotriva acestuia. Un tip de atac este cel reprezentat de atacurile prin dicționare asupra frazei de trecere din PGP, prin încercarea fiecărui cuvânt din dicționar şi a combinațiilor.

Securitatea centrală a PGP este dată de puterea frazei de trecere şi de protecția cheii private. Pentru ca fraza de trecere să prezinte securitatea adecvată, ar trebui să aibă o lungime suficientă, nu ar trebui să utilizeze cuvinte comune din dicționare şi ar trebui schimbată frecvent.

În ceea ce privește cheia privată, cât timp aceasta este stocată pe un calculator (şi nu pe un smart card, de exemplu), protecția acesteia este de asemenea importantă.

Pe lângă acestea, modelul de încredere reciprocă în cheile PGP este predispus la erori, iar pentru ca acesta să lucreze în mod corect trebuie ca expeditorul să *creadă* că cheia publică este autentică, aparține utilizatorului real şi nu a fost modificată.

7.2.13. S/MIME

Ca şi PGP, **Secure / Multipurpose Internet Mail Extensions** (S/MIME) încearcă să rezolve problema trimiterii de mesaje între părți care nu s-au întâlnit niciodată prin intermediul criptării. De asemenea, rezolvă problema integrității mesajului, verificării mesajului şi a nerepudierii prin utilizarea semnăturilor digitale.

S/MIME nu oferă criptarea la nivel de sesiune precum SSL, ci securizează mesajele individuale. Acest protocol este de preferat în utilizarea e-mail, în care destinatarul nu este disponibil în momentul în care mesajul a fost trimis.

Utilizând S/MIME, un mesaj poate fi criptat, semnat digital sau se pot alege ambele variante. Deşi S/MIME nu este limitat la securizarea mesajelor de e-mail, aceasta a fost principala sa utilizare până în momentul de față. S/MIME a fost aplicat de asemenea în *Electronic Data Interchange* (EDI), tranzacții online şi mesagerie securizată în aplicații.

Modelul S/MIME este bazat pe tehnologia creată în 1995 de către *RSA Data Security* împreună cu un grup de dezvoltatori de software, între care Netscape, VeriSign şi alții. S/MIME este bazat pe Standardul de criptografie cu cheie publică nr. 7 (PKCS#7 - un set de standarde utilizat pentru implementarea sistemelor de criptare cu cheie publică) pentru trimiterea mesajelor şi pe X.509v3 pentru certificate digitale.

S/MIME oferă îmbunătățiri de securitate față de standardul MIME. Ambele sunt definite prin RFC-uri:

- RFC 1847: Securizarea Multiparte pentru MIME;
- RFC 2045: MIME partea întâi: formatul corpurilor de mesaje din MIME;
- RFC 2046: MIME partea a doua: tipurile media;
- RFC 2047: MIME partea a treia: extensiile antetelor de mesaje pentru text Non-ASCII;
- RFC 2048: MIME partea a patra: procedurile de înregistrare;
- RFC 2049: MIME partea a cincia: criterii de conformare şi exemple;
- RFC 2183: comunicarea informațiilor de prezentare în mesajele Internet;
- RFC 2630: sintaxa mesajelor criptate;
- RFC 2632: gestiunea certificatelor S/MIME V3 ;

- RFC 2633: specificațiile S/MIME V3;
- RFC 2634: servicii îmbunătățite de securitate pentru S/MIME.

S/MIME extinde MIME prin oferirea de servicii de securitate între care se numără autentificarea şi integritatea prin utilizarea semnăturilor digitale şi confidențialitatea prin utilizarea criptării.

MIME este standardul pentru trimiterea fişierelor prin e-mail în Internet prin care se permite trimiterea de mesaje având diferite seturi de caractere şi codarea şi decodarea obiectelor de tip multimedia şi de tip binar pentru a putea fi trimise prin e-mail. Tipurile predefinite MIME cuprind documente Word, fişiere PostScript sau fişiere audio WAV. Codarea MIME este făcută utilizând diferite metode în momentul trimiterii mesajului, la recepție aceste părți fiind decodate în formatul original. Pentru aceasta se adaugă fiecărui fişier câte un antet în care sunt descrise datele conținute precum şi metoda de codare utilizată.

Deoarece MIME este o specificație matură şi bogată utilizată pentru trimiterea de conținut diferit prin Internet, îmbunătățirea acestuia are sens prin adăugarea de facilități de securitate în locul creării unui nou standard, complet diferit.

7.2.13.1. Funcționarea S/MIME

Pentru a putea trimite mesaje securizate de tip S/MIME, atât expeditorul cât şi destinatarul trebuie să utilizeze clienți care cunosc acest standard, precum Outlook, Outlook Express sau Netscape Communicator. În plus, fiecare utilizator trebuie să obțină un certificat digital împreună cu cheie privată corespunzătoare.

S/MIME este un sistem de criptare hibrid care utilizează atât algoritmul de criptare cu cheie publică cât şi pe cel de criptare cu cheie privată. Criptografia cu cheie publică este prea lentă pentru criptarea datelor brute, dar, în acelaşi timp, este dificil de distribuit cheia privată în mod securizat fără criptografia cu cheie publică. În standardul S/MIME criptografia cu cheie publică este utilizată pentru schimbarea cheilor simetrice şi pentru semnături digitale (necesită certificatele X.509). De asemenea, specificațiile S/MIME recomandă utilizarea a trei algoritmi de criptare: DES, Triple-DES şi RC2. Securitatea unui mesaj criptat cu S/MIME depinde în principal de mărimea cheii utilizate de algoritmul de criptare. Un aspect interesant al S/MIME este acela că destinatarul unui mesaj, şi nu expeditorul acestuia, determină metoda de criptare utilizată, bazându-se pe informațiile oferite de certificatele digitale.

Trimiterea mesajelor S/MIME presupune o serie de paşi. In primul rând, mesajul este criptat cu o cheie de sesiune generată în mod aleator. Apoi, cheia sesiunii este criptată utilizând cheia publică a destinatarului. Această cheie a fost fie schimbată în prealabil, fie a fost regăsită într-un serviciu director de tip LDAP. Pasul următor este constituit de împachetarea mesajului criptat, a cheii de sesiune a identificatorilor de algoritm precum şi a altor date într-un obiect binar de formatat în concordanță cu tipul PKCS#7. Acest obiect astfel creat este codat într-un obiect MIME utilizând tipul de conținut *application/pkcs7-mime*, după care mesajul este expediat. La recepționare, plicul digital este desfăcut, iar cheia privată a destinatarului decriptează cheia de sesiune, care este utilizată pentru a decripta mesajul.

Datorită suportului dat de dezvoltatori, S/MIME se pare că va fi standardul de securitate al e-mail. S/MIME joacă de asemenea, un rol cheie în strategia Microsoft Windows 2000/Exchange 2000.

S/MIME şi PGP oferă ambele metode eficiente de securitate pentru criptarea mesajelor de e-mail. Spre deosebire de PGP, care s-a bazat până la versiunea 7.0 pe modelul de securitate al plajei de încredere, S/MIME are ca avantaj principal utilizarea infrastructurii cu chei publice (PKI) şi a certificatelor digitale. De asemenea, S/MIME este integrat în mai mulți clienți de e-mail, în timp ce PGP necesită descărcarea şi instalarea unui plug-in.

7.2.13.2. Riscuri de securitate ale S/MIME

Pentru a funcționa eficient, S/MIME trebuie să utilizeze chei de lungime mare şi algoritmi de criptare puternici, precum Triple-DES. În multe cazuri în care se expediază mesaje de e-mail prin aplicații care suportă S/MIME, singurul format de criptare disponibil este RC4 (40 biți), care nu oferă o lungime suficientă pentru securitatea minimă.

De asemenea, S/MIME are aceleaşi probleme ca şi PGP - pentru o comunicație securizată, trebuie să existe un nivel de siguranță asupra cheii cu care se face criptarea. La fel ca şi la PGP, cheia secretă trebuie să fie securizată din punct de vedere fizic.

7.2.14. Utilizarea firewall-urilor în intraneturi

Zidurile de protecție joacă un rol semnificativ în managementul securității unui intranet. Un zid de protecție este un dispozitiv sau o aplicație care controlează cursul comunicației între rețeaua internă şi o rețea externă precum Internetul. Un zid de protecție (Figura 7.1) serveşte câtorva scopuri:

- acționează ca filtru de intrare pentru traficul Internet către serverele organizației, prevenind ajungerea pachetelor neautorizate în serverele de web şi de aplicații;
- oferă conexiuni prin proxy către Internet, menținând autentificarea utilizatorilor interni;
- jurnalizează traficul, oferind un suport pentru audit, raportare, ca şi pentru planificare.

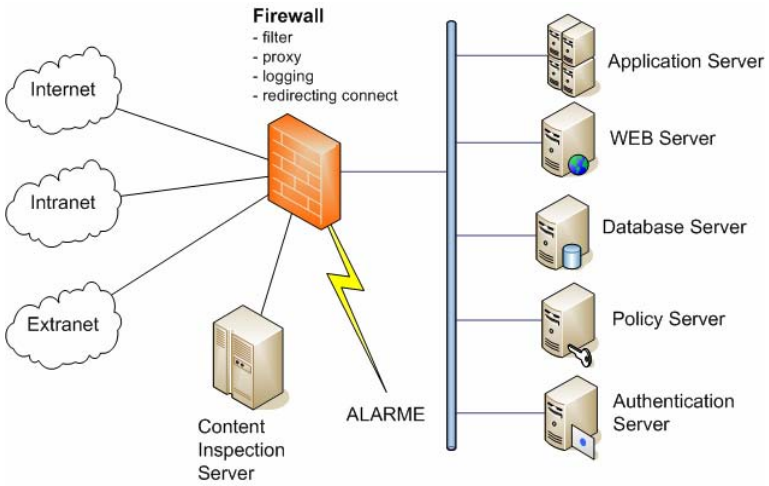


Fig. 7.1: Amplasarea Firewall-ului

Firewall-urile nu funcționează fără riscuri. Acestea sunt în general dificil de penetrat, dar dacă au fost depăşite, rețeaua internă este deschisă pentru intrus. În plus, un firewall nu poate rezolva compromisurile din rețeaua internă. Aproximativ 70% din breşele de securitate au loc în interiorul companiei, adică sunt create de persoane *de*

dincolo de zidul de protecție. Un exemplu poate fi utilizarea unui modem şi a unei conexiuni dial-up.

În practică au fost observate următoarele riscuri cu privire la firewall-uri:

- ***porturile*** - regulile de filtrare sunt bazate pe porturi sursă şi destinație. O maşină care utilizează TCP/IP are 65535 porturi virtuale, din care unele sunt utilizate de către anumite servicii;
- ***rutarea*** - această opțiune IP permite utilizatorilor să definească modalitatea de rutare a pachetelor.
- ***SOCK*** - reprezintă o bibliotecă de aplicații proxy utilizate pentru a permite ca anumite servicii să fie utilizate şi pentru a ține intruşii în afară;
- ***scanare RPC directă*** - portmapper este un serviciu care permite utilizatorilor să identifice porturile pe care rezidă apelurile de proceduri la distanță;
- ***scanare ascunsă*** - un intrus nu încearcă să stabilească o conexiune ci utilizează pachete la nivel de interfață. Aceste pachete ne dau răspunsuri diferite, în funcție de calitatea portului (deschis sau nu).
- ***protocoale fără conexiune*** - firewall-urile au dificultăți în detectarea pachetelor utilizate în servicii care nu necesită stabilirea unei conexiuni, precum UDP;

Pentru Intraneturi este necesară existența unui sistem de detectare a intruziunilor cu scopul protejării perimetrului rețelei de atacuri. Sistemele de detectare a intruşilor pot fi instalate ca şi sonde sau ca agenți. Sondele sunt mult mai eficiente în ceea ce priveşte detectarea intruziunilor deoarece minimizează impactul asupra sistemelor existente prin ascultarea pasivă şi raportarea către consola centrală, fără întrerupere.

Serviciile de detectare a intruşilor execută la nivel de dispozitiv de rețea următoarele funcții:

- inspectează şirul de date care trec prin rețea, identifică semnăturile activităților neautorizate şi activează procedurile de apărare;
- generează alarme în cazul detectării evenimentelor, notificând personalul necesar de securitate;
- activează un răspuns automat în cazul anumitor probleme.

Pe lângă detectarea intruşilor mai poate fi luat în considerare şi un agregator proxy de tip TCP care va îmbunătății securitatea prin firewall prin limitarea porturilor expuse.

Tunneling-ul şi criptarea sunt utilizate pentru a crea rețele punct-la-punct, în general fiind utilizate protocoale precum *Layer 2 Tunneling Protocol* (L2TP), *Point-to-Point Tunneling Protocol* (PPTP), IPSec, precum şi standarde de criptare cum sunt DES, MD5, Triple DES, etc.

Codurile mobile de program precum Java şi ActiveX creează o amenințare în creştere. Aplicațiile care inspectează conținutul trebuie să:

- ofere control asupra codului mobil Java, ActiveX sau altul;
- prevină atacurile prin cod mobil;
- activeze navigarea în siguranță, utilizând în acelaşi timp facilitățile Java şi ActiveX.

În concluzie, managementul securității are o necesitate din ce în ce mai ridicată, atât în rețele de tip intranet cât şi în alte tipuri de rețele de colaborare, datorită mulțimii punctelor de acces în rețea. În acelaşi timp sunt necesare noi unelte şi tehnici, cât şi o combinare a acestora pentru a oferi siguranța maximă posibilă.

8. Strategii de achiziție pentru apărare

8.1. Introducere

Informațiile despre comerțul electronic ***Business-to-Business*** (B-B) îşi croiesc drum în ziare, reviste economice sau în ştirile de la televiziuni. Majoritatea acestor informații sunt centrate pe achiziții electronice (*e-procurement*) sau partea de cumpărare a comerțului electronic pentru că analiştii au confirmat faptul că firmele ce au implementat sisteme de achiziții electronice au înregistrat economii.

Indiferent din ce domeniu este o firmă, achizițiile sunt o importantă funcție economică, acest lucru este valabil şi pentru unitățile din domeniul apărării. Deoarece achizițiile intervin la începutul lanțului valoric, impactul deciziilor de aprovizionare se amplifică pe măsură ce un produs curge spre destinația finală: utilizatorul. Achizițiile implică două tipuri de cheltuieli. O categorie se referă la costul materialelor cumpărate. A doua se referă la costul procesului de achiziție. Acesta cuprinde costurile tranzacției, adică cele cu personalul implicat în proces, cheltuieli indirecte aferente căutării, comparării, negocierii de surse de achiziție. Soluțiile de achiziție electronice pot avea un efect substanțial asupra ambelor categorii.

Comerțul electronic reprezintă schimbul de informații de afaceri, fără ajutorul hârtiei, utilizând schimbul electronic de date (*Electronic Data Interchange*), poşta electronică (*e-mail*), buletinele electronice, transferul electronic de fonduri (*Electronic Funds Transfer*), precum şi alte tehnologii similare. Schimbul electronic de date reprezintă schimbul, între calculatoare, a informațiilor privind tranzacțiile din afaceri, folosind un format standard public.

Introducerea conceptului de *e-business* permite organizațiilor militare să considere comerțul electronic nu numai în viziunea tradițională de achiziție şi plată prin utilizarea tranzacțiilor standard. Conceptul permite luarea în considerare a relațiilor dintre un consumator şi un furnizor şi oferă avantajele date de îmbunătățirea semnificativă a procesului, disponibilă prin implementarea conceptelor şi tehnologiilor de afaceri electronice şi comerț electronic. Acest lucru duce la extinderea aplicațiilor funcționale de la furnizare, achiziție şi contabilitate, la cele legate de alte domenii cum ar fi sănătatea, personalul, sistemul de achiziții şi ştiința şi tehnologia.

Politica organizațiilor militare în ceea ce priveşte introducerea în activitatea curentă a conceptelor *e-business* şi *e-commerce* trebuie să aibă în vedere:

- utilizarea conceptelor şi tehnologiilor de *e-business* şi *e-commerce* în îmbunătățirea proceselor de afaceri şi în eforturile de reinginerie; acest lucru permite introducerea procedeelor de pe piața comercială în diseminarea informațiilor în formă electronică persoanelor în drept, la momentul potrivit, în scopul reducerii duratei procesului; în acest sens, organizațiile militare vor desfăşura următoarele activități:
    - implementarea inițiativelor *e-business* şi *e-commerce* care încorporează „cele mai bune practici în afaceri" în vederea obținerii eficienței şi pentru promovarea eficacității operaționale pentru reducerea semnificativă a timpilor de răspuns;
    - facilitarea utilizării în comun a datelor şi integrarea proceselor de afaceri între organizațiile militare şi partenerii de afaceri;

  - implementarea de soluții deschise flexibile şi interoperabile care să nu interzică sau să îngreuneze utilizarea pe scară largă de soluții tehnologice noi sau competitive;
- utilizarea pe scară largă de standarde *e-business* şi *e-commerce* industriale şi a produselor comerciale – COTS (*commercial-off-the-shelf*);
- implementarea soluțiilor de securitate *e-business* şi *e-commerce* care vor permite securitatea datelor pe baza cerințelor statutare şi ale utilizatorilor, fără degradarea proceselor curente pe care le înlocuiesc;
- stabilirea şi utilizarea de oportunități de afaceri electronice care angajează principii, concepte şi tehnologii de *e-business* şi *e-commerce* în conducerea şi administrarea proceselor militare şi de afaceri;
- aplicarea proceselor de *e-business* şi *e-commerce* în vederea interoperabilității cu partenerii de afaceri pentru integrarea cu sectorul privat;
- protejarea proprietății intelectuale; garantarea integrității datelor şi dreptul la confidențialitatea lor;
- cooperarea cu alte ministere şi agenții pentru dezvoltarea şi implementarea unei arhitecturi operaționale *e-business* şi *e-commerce* în sprijinul programelor guvernului din domeniu;
- asigurarea conformității cu politica de achiziție a M.Ap.N. şi a instrucțiunilor de achiziție.

8.2. Strategii de securitate ale războiului informațional

Securitatea este recunoscută ca fiind un concept multidimensional aşa încât, toate domeniile de activitate (politică, diplomație, economie, apărare, cultură, ştiință etc.) îşi iau măsuri care să asigure promovarea intereselor specifice fiecăreia. Aceste sectoare de activitate nu există independent unul de celalalt, legăturile dintre ele fiind vitale pentru funcționarea optimă.

În acest context, politica de securitate națională este obligată să țină cont de această realitate. Fiind vorba de un sistem al cărui echilibru şi funcționare optimă este de dorit, politica în acest domeniu va trebui să fundamenteze, în plan teoretic şi să întreprindă în plan practic, acele măsuri necesare pentru promovarea intereselor naționale fundamentale şi apărarea lor împotriva oricăror agresiuni, pericole, amenințări, riscuri.

Faptul că informația şi tehnologia schimbă natura conflictelor nu este un lucru nou, dar accentuarea, în prezent, a rolului informației, ca instrument de putere, determină modificări extrem de importante nu numai în activitatea unui serviciu de informații, ci şi la nivelul politicii de apărare, în activitatea organizațiilor militare şi în dezvoltarea infrastructurii informaționale militare.

Războiul şi operațiile informaționale sunt realități deja consacrate în spațiul euro-atlantic, şi nu numai. Capacitățile în acest domeniu constituie, pentru țări cum este şi România, soluții de contrabalansare a asimetriilor de putere.

Acțiunile de natură informațională (în practică, operații informaționale) au şi vor avea loc pe tot parcursul ciclului pace-criză-conflict-pace. Este, aşadar, esențial ca România să dispună de capacități *permanente* de avertizare, evaluare, analiză şi ripostă, precum şi să întrețină o stare continuă de ajustare structurală şi doctrinară, care să-i permită realizarea intereselor naționale în acest mediu informațional.

În societatea informațională, informația ca armă, țintă şi materie primă strategică stă la baza tuturor deciziilor. Adaptarea la acest nou mediu (în care fluxul de informații, în timp real, este în continuă creştere) presupune înțelegerea unor riscuri în zona managementului informațional. O exemplificare a acestui lucru este faptul că operațiile informaționale, aşa cum sunt ele conceptualizate în doctrinele euro-atlantice, au ca țintă de bază ciclul decizional.

Evoluția rapidă a tehnologiei informației a mărit discrepanța dintre capacitatea de producere şi cea de utilizare a informației. Sporirea cantității informațiilor nu atrage după sine şi creşterea calității lor, iar deținerea unor informații de calitate nu este sinonimă cu capacitatea de valorificare a lor.

Din perspectivă civilă, conceptul de război informațional atrage după sine o multiplicare a raporturilor de forță, în timp ce în plan militar există o aparentă limitare a acestora (restrângerea puterii militare, datorită reducerii caracterului violent al confruntărilor). Între cele două perspective există şi puncte comune. În primul rând, un aliat poate fi în acelaşi timp şi adversar (de unde natura dublă cooperare – concurență). În al doilea rând, războiul informațional stabileşte un nou raport între realitățile de ordin strategic, tehnic (prezența tot mai mare a informaticii şi a rețelelor informaționale) şi simbolice.

În sens larg, războiul informațional presupune integrarea a şapte forme diferite de domenii şi discipline:

- *războiul de comandă şi control* (forma exclusiv militară a războiului informațional) – are menirea să anihileze comanda şi sistemele de comandă şi control ale unui adversar prin integrarea operațiilor psihologice, a securității operațiilor, a inducerii în eroare, a războiului electronic şi a distrugerii fizice;
- *războiul bazat pe informații (intelligence)* – constă în proiectarea, protecția şi anihilarea sistemelor care conțin suficiente cunoştințe pentru a domina un spațiu de conflict;
- *războiul electronic* – utilizează tehnologie electronică şi tehnici criptografice pentru dominația spațiului electromagnetic;
- *războiul psihologic* – utilizează informația pentru a modifica atitudinile şi opțiunile amicilor, neutrilor şi adversarilor;
- *războiul hacker-ilor* – constă în atacuri pasive şi active, cu software „malign”, asupra sistemelor informatice;
- *războiul în sfera informațiilor economice* – urmăreşte blocarea sau canalizarea informațiilor, în scopul obținerii supremației economice;
- *războiul în spațiul realității virtuale* – creează, în prezent, imagini ale "realităților"potrivit intereselor actorilor implicați.

În contextul războiului informațional, *securitatea informațională* (INFOSEC-*Information Security*) reprezintă protecția şi apărarea informațiilor şi sistemelor informaționale împotriva accesului neautorizat, a modificării conținutului informațiilor aflate în faza de stocare, prelucrare sau transport şi pentru asigurarea accesului utilizatorilor autorizați către aceste informații. INFOSEC cuprinde acele măsuri destinate pentru descoperirea, informarea şi contracararea acestor tipuri de acțiuni.

Componentele INFOSEC sunt:

- securitatea echipamentelor de calcul (COMPUSEC - *Computer Security*);

- securitatea comunicațiilor (COMSEC - *Communications Security* şi TRANSEC – *Transmission Security*).

COMPUSEC cuprinde acele măsuri şi elemente de control care asigură confidențialitatea, integritatea şi disponibilitatea informațiilor prelucrate şi stocate cu ajutorul calculatoarelor. Aceste măsuri includ proceduri şi instrumente hardware şi software necesare pentru protejarea sistemelor informatice şi a informațiilor stocate în cadrul acestora.

COMSEC cuprinde acele măsuri destinate împiedicării accesului neautorizat la informațiile care pot fi preluate din sistemele de comunicații, precum şi asigurarea autenticității corespondenților pe aceste linii. Foloseşte scramblarea sau tehnicile criptografice pentru a face informația neinteligibilă pentru personalul neautorizat care interceptează comunicația.

Criptografierea este procesul de criptare (translatare) a informației într-un mesaj aparent aleator la emițător, şi apoi de descifrare a mesajului aleator prin decriptare la receptor. Tehnologiile electronice actuale permit desfăşurarea automată a procesului de criptare/decriptare. Procesul implică folosirea unui algoritm matematic şi a unei chei, pentru translatarea informației din clar în stare criptată.

În sistemele de comunicații vocale, care nu necesită securitate ridicată, informația poate fi protejată împotriva interceptării şi prelucrării prin scramblarizare. În acest caz, scramblarea, ca tehnică COMSEC analogică, implică separarea semnalului vocal într-un număr de sub-benzi şi translatarea fiecăreia într-un alt domeniu al spectrului de audiofrecvență, urmată de combinarea sub-benzilor într-un semnal audio compus, care modulează emițătorul.

În criptarea digitală, datele sunt reduse la un flux de date binar. Mecanismul criptografic creează un flux de numere binare ne-repetitiv, extrem de lung, pe baza unei chei de criptare a traficului (TEK - *Traffic Encryption Key*). Fluxul de date este adăugat celui criptografic, creând datele criptate sau textul cifrat. Un flux binar creat în acest mod este inerent impredictibil, furnizând de aceea o metodă foarte sigură de protejare a informației. Toate semnalele analogice sunt mai predictibile şi de aceea mai puțin sigure.

Eficacitatea criptării datelor, care este gradul de dificultate în determinarea conținutului mesajului, este funcție de complexitatea algoritmului matematic şi de chei.

Cheia este o variabilă care modifică resincronizarea algoritmului, protejarea acesteia fiind vitală. Chiar în situația în care se realizează accesul la informația criptată (şi se cunoaşte algoritmul), de către persoane neautorizate, este imposibilă decriptarea informației dacă nu se cunoaşte şi cheia. Acesta este unul din considerentele pentru care e necesară dezvoltarea unor proceduri riguroase de management al cheilor, în scopul protejării, distribuirii, stocării şi folosirii cheilor.

Un tip de sistem de management al cheilor, folosit în sectorul comercial public, este criptografia cu chei publice. Conform acestui standard, fiecare utilizator generează două chei. Una este cheia publică "Y" iar cealaltă este cheia privată "X". Utilizând acest sistem se poate transmite de oriunde un mesaj criptat cu cheia Y, care însă poate fi decriptat numai de către operatorul care deține cheia X. Astfel, într-o rețea care foloseşte acest sistem de chei publice, sunt posibile comunicații secretizate pe două nivele, acesta fiind denumit *sistem de chei asimetric*. Alternativa sa este *sistemul de chei simetric*, în care cu aceeaşi cheie se criptează şi decriptează datele. Deoarece atât cel

care emite mesajul cât şi toți cei care îl primesc trebuie să aibă aceleaşi chei, acest sistem oferă cel mai înalt nivel de securitate.

O soluție recent dezvoltată, aplicabilă rețelelor radio foloseşte reprogramarea prin legătură radio (OTAR - *Over The Air Rekeying*).Această tehnică aproape elimină necesitatea încărcării manuale a cheilor şi realizează un management sigur al cheilor.

OTAR este un sistem de distribuire a cheilor şi include o cheie de criptare a cheii (KEK - *Key Encryption Key*), folosită pentru criptarea cheii de criptare a traficului şi oricăror altor chei operaționale COMSEC sau TRANSEC. Acest proces mai este denumit şi "împachetare" pentru a fi diferențiat de criptarea traficului. Singura cheie care trebuie încărcată inițial atât în unitățile emițătoare cât şi în cele receptoare este cheia KEK.

După "împachetare", distribuirea, procesul care urmează, poate folosi orice mijloace fizice sau electronice. Într-un sistem OTAR, cheile "împachetate"sunt introduse într-un mesaj şi trimise prin legătură radio stației dorite, folosind protocoale de transmisie fără erori (deoarece orice eroare ar face cheile de nefolosit). Legătura folosită pentru transmisie este în general secretizată cu ajutorul cheii de criptare a traficului (TEK) utilizată. Astfel, conținutul cheii este dublu protejat la transmisia prin legătură radio, eliminându-se practic orice posibilitate de compromitere. Pentru un grad de securitate mai ridicat, se obişnuieşte să se digitizeze prin intermediul unui vocoder, semnalul digital rezultant fiind apoi tratat ca orice flux de date.

TRANSEC foloseşte un număr de tehnici pentru a preveni detecția sau bruierea semnalului pe traseul de transmisie. Aceste tehnici includ fie "ascunderea" canalului, fie transformarea acestuia într-o țintă în continuă mişcare.

Pe termen mediu şi lung, o strategie coerentă de acțiune pentru operaționalizarea securității informaționale va trebui să vizeze dezvoltarea conceptuală şi metodologică a domeniului, cu accent pe:

- delimitarea granițelor conceptuale (caracteristici, forme, aspecte etc.) şi definirea cadrului epistemologic de abordare;
- studierea dinamicii modelelor formale ale războiului informațional şi adaptarea acestora la contextul geopolitic, la interesele şi resursele României;
- identificarea factorilor de risc în raport cu slăbiciunile actuale ale Sistemului Național de Securitate;
- fundamentarea teoretică a unui ansamblu de structuri care să permită abordarea instituționalizată a domeniului războiului informațional;
- formularea unei strategii integratoare, la nivel național, care să ofere coordonatele pe termen lung ale dezvoltării domeniului securității informaționale.

Aplicații practice

1 Criptarea ca metodă de securitate a informațiilor

1.1 Obiective:

- înțelegerea şi familiarizarea cu tehnica de criptare prin cheie secretă;
- realizarea criptării şi decriptării mesajelor folosind metoda cifrului lui Cezar;
- realizarea criptării şi decriptării mesajelor folosind metoda cifrului lui Vernam;

În prezent există două tipuri principale de tehnici utilizate în criptografie, şi anume:

- criptografia prin cheie simetrice (chei secrete sau chei private) şi,
- criptografia prin chei asimetrice (chei publice).

În cazul cheii simetrice, atât expeditorul cât şi destinatarul mesajului folosesc o cheie comună secretă. În cazul cheii asimetrice, expeditorul şi destinatarul folosesc în comun o cheie publică şi, individual, câte o cheie privată.

1.2 Cifrul lui Cezar

Cea mai simplă metodă de criptare, prin substituție, este cunoscută în zilele noastre sub denumirea de ***cifrul lui Cezar***, după numele împăratului roman care a inventat-o. În acest cifru, caracterele mesajului şi numărul de repetiții ale cheii sunt însumate laolaltă, modulo 26. În adunarea modulo 26, literelor alfabetului latin, de la A la Z, li se dau valori de la 0 la 25 (vezi tabelul 4.1). Pentru cheie trebuie să se ofere doi parametri:

- D – numărul literelor ce se repetă, reprezentând chei;
- K – cu rol de cheie.

Tabelul 4.1

Corespondența litere-numere																									
Litera	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Număr	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Pentru a înțelege modul de funcționare, să presupunem că D=3 şi K = BEC, iar mesajul secret este "PAROLA MEA". Atribuind valori numerice mesajului, din tabelul valorii literelor, avem:

P A R O L A M E A
15 0 17 14 11 0 12 4 0
Valorile numerice ale cheii sunt:
B E C = 1 4 2

După aceste corespondențe, cheia criptată 142 se adaugă literelor mesajului, astfel:

Cheia reperată	1	4	2	1	4	2	1	4	2
Mesajul	15	0	17	14	11	0	12	4	0
Echivalentul numeric al textului criptat	16	4	19	15	15	2	13	8	2
Textul criptat	Q	E	T	P	P	C	N	I	C

Convertirea numerelor în literele aferente alfabetului conduce la textul criptat, aşa cum se vede mai sus: "QETPPC NIC"

În cazul cifrului lui Cezar, D = 1 şi cheia este D (3), adică fiecare literă este înlocuită de a treia literă de după ea din alfabet – literele sunt deplasate la dreapta cu trei poziții, (A cu D, B cu E ș.a.m.d.). Criptând mesajul dat în exemplul anterior cu cifrul lui Cezar, obținem:

Cheia reperată	3	3	3	3	3	3	3	3	3
Mesajul	15	0	17	14	11	0	12	4	0
Echivalentul numeric al textului criptat	18	3	20	17	14	3	15	7	3
Textul criptat	S	D	U	R	O	D	P	H	D

Dacă sumele valorilor cheii şi ale numărului aferent literelor sunt mai mari sau egale cu 26, se determină modulo 26 din sumă, adică rezultatul final este obținut prin scăderea din sumă a numărului 26.

Exemplu:

D=3, K=PIC, mesajul este SECRET, rezultatul va fi:

- valorile numerice atribuie mesajului:

S E C R E T

18 4 2 17 4 19

- valorile numerice ale cheii sunt: P I C = 15 8 2

Cheia reperată	15	8	2	15	8	2			
Mesajul	18	4	2	17	4	19			
Echivalentul numeric al textului criptat	33 (8)	12	4	32 (9)	12	21			
Textul criptat	I	M	E	J	M	V			

Valorile 32 şi 33 nu au echivalent în alfabetul latin, caz în care se calculează modulo 26 din 32 şi 33, rezultând valorile 8 şi 9, iar noul echivalent numeric al textului criptate este 8 12 4 9 12 21, iar textul criptat este: IMEJMV.

Cifrurile de mai sus pot fi descrise prin ecuația generală:

$$\mathbf{C = (M + b) \bmod N}$$

unde:

b = un număr întreg fix;

N = numărul literelor din alfabet (26 pentru alfabetul latin);

M = mesajul textului clar în forma numerică;

C = textul criptat scris în forma numerică.

Cifrul lui Cezar, bazându-se pe substituția simplă sau monoalfabetică este ușor de spart, pentru că un caracter este înlocuit de altul şi această schimbare este valabilă în tot textul, iar analiza frecvențelor de apariție a literelor din textele scrise ne va conduce la caracterele adevărate ale textului.

Cifrurile polimorfice sunt realizate prin apelarea la cifruri bazate pe substituția multiplă. De exemplu, dacă se folosesc trei alfabete pentru substituție, definite de cel ce intenționează să cripteze, prima literă din textul clar este înlocuită cu prima literă din primul alfabet, a doua literă a textului clar este înlocuită cu prima literă din al doilea

alfabet, a treia literă a textului clar este înlocuită cu prima literă din al doilea alfabet, a patra literă din textul clar este înlocuită de a doua literă din primul alfabet ş.a.m.d.

1.3 Cifrul lui Vernam

Cifrul lui Vernam constă într-o cheie constituită dintr-un şir se caractere aleatoare nerepetitive. Fiecare literă a cheii se adaugă modulo 26 la o literă a mesajului clar. În această variantă, fiecare literă a cheii se foloseşte o singură dată pentru un singur mesaj şi nu va mai putea fi folosită niciodată. Lungimea şirului de caractere a cheii este egală cu lungimea mesajului. Metoda este foarte utilă pentru criptarea mesajelor scurte.

Exemplu: criptarea mesajului: LA MULTI ANI

Mesaj clar	LAMULTIANI	11	0	12	20	11	19	9	0	13	8
Cheie Vernam	VIDAGTSROL	21	8	3	0	6	19	18	17	14	11
Suma aparentă		32	8	15	20	17	38	27	17	27	19
Modulo 26 din sumă		6	8	15	20	17	12	1	17	1	19
Textul criptat		G	I	P	U	R	M	B	R	B	T

1.4 Metodă proprie de criptare

Mircea şi Vasilică vor să-şi trimită mesaje pe care alţii să nu le înţeleagă. Au citit ei despre spioni şi modalităţi de a scrie mesaje şi, în final, au imaginat un mod de criptare a unui mesaj care foloseşte “cuvânt cheie”.

Alegându-şi un cuvânt cheie format numai din litere distincte, ei numără literele acestuia şi împart mesajul în grupe de lungime egală cu numărul de litere ale cuvântului cheie, şi le aşează una sub alta. Desigur, se poate întâmpla ca ultima grupă să fie incompletă, aşa că o completează cu spaţii. Apoi numerotează literele cuvântului cheie în ordinea apariţiei lor în alfabetul englez. În final, rescriu mesajul astfel: coloana de sub litera numerotată cu 1, urmată de coloana de sub litera numerotată cu 2, etc. înlocuind totodată şi spaţiile cu caracterul ‘*’ (asterisc).

Exemplu:

cuvântul cheie **criptam**
mesaj de criptat Incercam sa lucram cu coduri si criptari.
cuvântul cheie **criptam** are 7 litere
numerotare **2635714**
deoarece, avem, în ordine **a**b**c**defgh**i**jkl**m**no**p**q**r**s**t**uvwxzy
1 2 3 4 5 6 7
împărţire în grupe: Incerca | m sa lu | cram cu | coduri | si cri | ptari.
codificare **2635714**
Incerca
m*sa*lu
cram*cu
*coduri
*si*cri
ptari.*

mesaj criptat clcrr.Imc**pcsaoiaauuii*eamd*rn*rcstr**uci
col1 col2 col3 col4 col5 col6 col7

Cerință

Fiind date un cuvânt cheie şi un mesaj criptat, decodificați mesajul trimis de Mircea pentru Vasilică.

Date de intrare

Fişierul de intrare **criptare.in** conține pe prima linie mesajul criptat iar pe linia a doua cuvântul cheie.

Date de ieşire

Fişierul de intrare **criptare.out** conține pe prima linie mesajul decriptat.

Restricții

- lungimea mesajului este de minim 20 şi maxim 1000 caractere
- cuvântul cheie are minim 5 şi maxim 20 de caractere
- cuvântul cheie conține numai litere mici ale alfabetului

1.5 Desfăşurarea lucrării

Studenții vor forma două sau patru echipe, care vor cripta un text dat de îndrumătorul lucrării, după care vor schimba mesajele criptate între ele, şi vor încerca să le decripteze, cunoscând cheile de criptare.

De remarcat, că în mesajele în clar nu se ia în considerare spațiul dintre cuvinte.

2 Steganografia ca metodă de securitate a informațiilor

2.1 Obiective:

- înțelegerea şi familiarizarea cu tehnica de ascundere a informațiilor prin steganografie;
- familiarizarea şi utilizarea unei aplicații de ascundere a informațiilor în imagini steganography;

2.2 Introducere

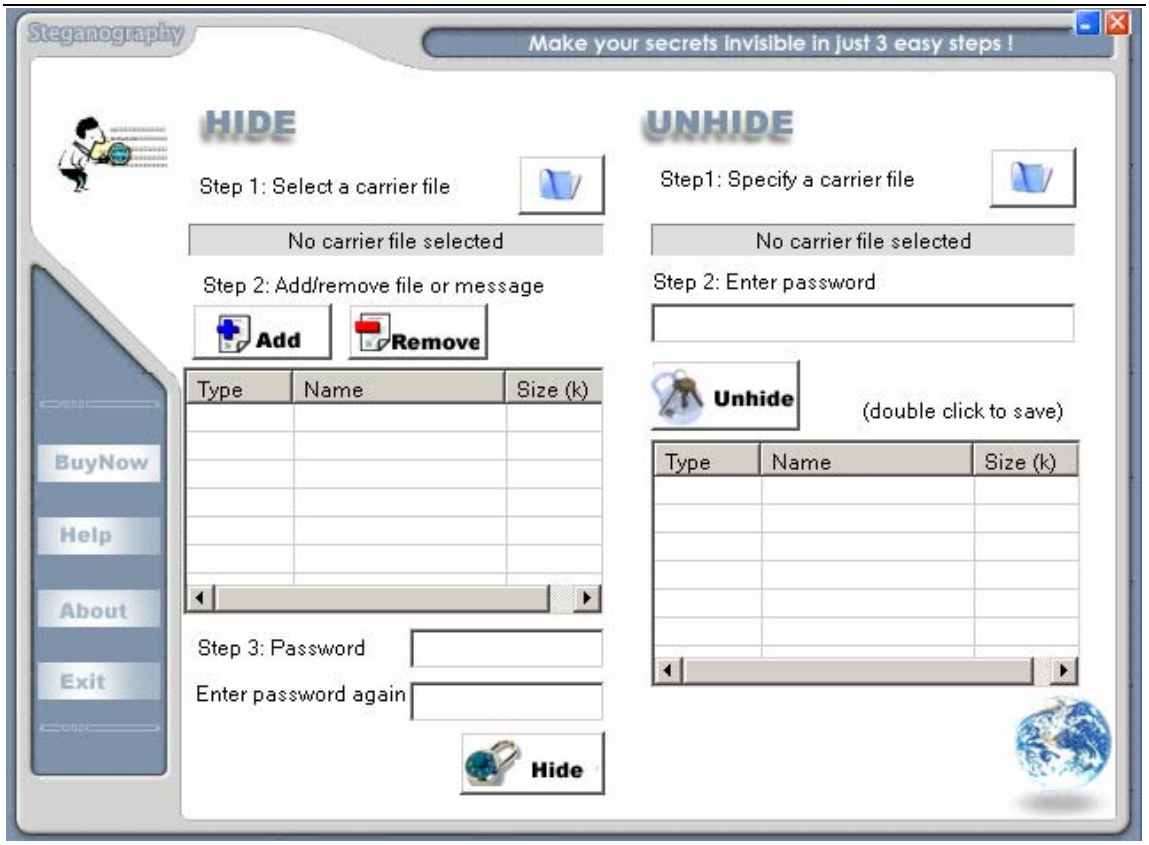
Cuvântul steganografie (steganography) vine din limba greacă unde steganos înseamnă ascuns şi graph scris (scriere ascunsă). Prin urmare putem spune că steganografia este știința sau arta de a scrie mesaje ascunse astfel încât existenta lor să fie cunoscută numai de destinatar şi expeditor. Acest concept îşi are originea în vremuri istorice. De exemplu grecii sau romanii foloseau steganografia pentru a transmite mesaje ascunse, şi anume râdeau părul celui care trebuia să transmită mesajul, scriau mesajul pe pielea capului şi aşteptau ca părul să-i crească la loc. Mesajul putea fi transmis prin intermediul trimisului, nimeni decât cei care ştiau unde se află putându-l citi.

Steganografia este folosită pentru a ascunde mesaje (fişiere) în alte fişiere mai mari şi anume în imagini de tip jpg, bmp, png, în fişiere audio (mp3 sau wav) sau chiar video (avi) fără a exista posibilitatea ca o terță persoană să ştie sau să afle de existența lor. Totuşi una dintre cele mai cunoscute tehnici de steganografie este "cerneala simpatică" (înscrisul devine vizibil după un procedeu - lampa UV, încălzire, etc.). Steganografia nu trebuie confundată cu criptografia. Acesta din urma face ca un mesaj să devină indescifrabil, dar existenta lui este vizibilă, pe când steganografia ascunde existența mesajului şi nu mesajul şi face ca steganografia să fie completarea perfectă pentru codificare.

Aplicația poate fi descărcată de la http://www.securekit.com/.

După instalare, studenții vor efectua ascunderea unui fişier text în spatele unei imagini, care poate fi jpg, bmp, tif, pgn etc.

Lansarea în execuție a aplicației se poate face astfel:
Start → Programs → Steganography → Steganography
Moment în care se va deschide fereastra de mai jos:



2.3 Ascunderea unui fişier

Pasul 1: Selectarea fişierului cărăuş

În acest prim pas se va alege fişierul (imaginea) în care se va ascunde mesajul (sau fişierul) secret.

Click pe butonul  , şi se va alege imaginea care va ascunde mesajul.

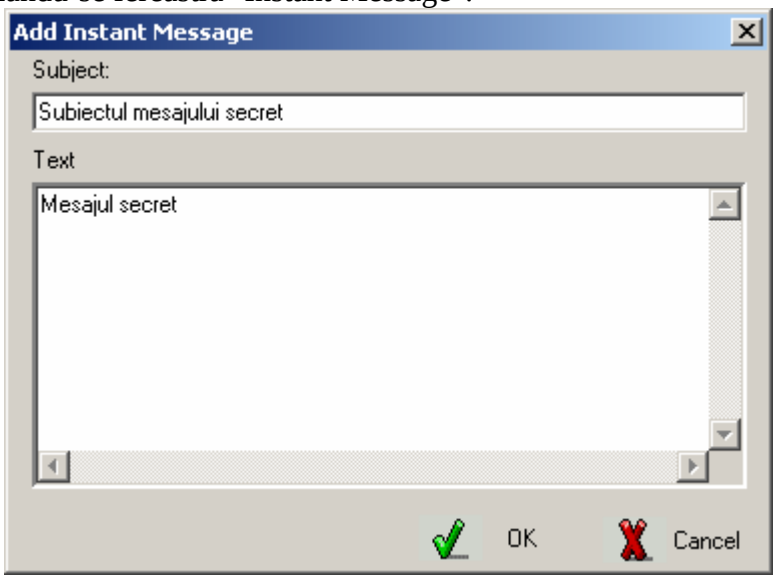
Pasul 2: Adăugarea/înlăturarea mesajului sau a fişierului

În acest pas se selectează un fişier existent în calculator sau se creează un mesaj nou care va fi ascuns. Pot fi ascunse mai multe fişiere sau mesaje în acelaşi timp.

Click pe butonul  , după care se deschide fereastra de adăugat mesaje sau fişiere:

1. Pentru a ascunde un fişier deja existent se apasă "File" şi apoi "Next" , selectându-se de pe hard disc fişierul dorit.

2. Pentru a ascunde un mesaj, se apasă "New Messge" şi apoi "Next", deschizându-se fereastra "Instant Message":



Paşii de mai sus se repetă dacă dorim să ascundem mai multe fişere.

Pentru a îndepărta un fişier sau un mesaj ce trebuia ascuns, se selectează din tabel şi apoi se apasă butonul Remove, 

Pasul 3: Specificarea parolei

La final, se dă click pe butonul 

pentru a porni procesul de ascundere. Când procesul de ascundere este complet, salvați fişierul rezultat.

2.4 Descoperirea unui fişier ascuns

Pasul 1: Alegerea fişierului purtător

Se dă click pe butonul  din dreapta şi se selectează fişierul cărăuş;

Pasul 2: Introducerea parolei de acces

Dacă la ascunderea fişierului original s-a introdus o parolă, acum ea trebuie cunoscută şi introdusă.

Se apasă butonul 

pentru a începe procesul de descoperire a fişierului ascuns. După ce procesul este terminat, în tabelul de dedesubt va apare fişierul ascuns în formă clară. Pentru al deschide se dă dublu clic pe el.

3 Firewall-uri

3.1 Obiective:

- înțelegerea funcționării şi a rolului unui firewall în securitatea sistemelor informatice;
- pornirea şi configurarea firewall-ului sistemului de operare Windows XP;

3.2 Generalități/Definiții Firewall

Un paravan de protecție poate ține la distanță traficul Internet cu intenții rele, de exemplu hackerii, viermii şi anumite tipuri de viruşi, înainte ca aceştia să pună probleme sistemului. În plus, un paravan de protecție poate evita participarea computerului la un atac împotriva altora, fără cunoştința dvs. Utilizarea unui paravan de protecție este importantă în special dacă sunteți conectat în permanență la Internet.

Un **firewall** este o aplicație sau un echipament hardware care monitorizează şi filtrează permanent transmisiile de date realizate între PC sau rețeaua locală şi Internet, în scopul implementării unei "politici" de filtrare. Această politică poate însemna:

- protejarea resurselor rețelei de restul utilizatorilor din alte rețele similare – Internetul -> sunt identificați posibilii "musafiri" nepoftiți, atacurile lor asupra PC-ului sau rețelei locale putând fi oprite.
- Controlul resurselor pe care le vor accesa utilizatorii locali.

3.2.1 Funcționarea firewall-urilor

De fapt, un firewall, lucrează îndeaproape cu un program de routare, examinează fiecare pachet de date din rețea (fie cea locală sau cea exterioară) ce va trece prin serverul gateway pentru a determina dacă va fi trimis mai departe spre destinație. Un firewall include de asemenea sau lucrează împreună cu un server proxy care face cereri de pachete în numele stațiilor de lucru ale utilizatorilor. În cele mai întâlnite cazuri aceste programe de protecție sunt instalate pe calculatoare ce îndeplinesc numai această funcție şi sunt instalate în fața routerelor.

Soluțiile firewall se împart în două mari categorii: prima este reprezentată de soluțiile profesionale hardware sau software dedicate protecției întregului trafic dintre rețeaua unei întreprinderi (instituții -> ex.: Universitatea "Alexandru Ioan Cuza", Iaşi) şi Internet; iar cea de a doua categorie este reprezentată de firewall-urile personale dedicate monitorizării traficului pe calculatorul personal.

Utilizând o aplicație din ce-a de a doua categorie veți putea preîntâmpina atacurile colegilor lipsiți de fair-play care încearcă să acceseze prin mijloace mai mult sau mai puțin ortodoxe resurse de pe PC-ul dumneavoastră. În situația în care dispuneți pe calculatorul de acasă de o conexiune la Internet, un firewall personal vă va oferi un plus de siguranță transmisiilor de date. Cum astăzi majoritatea utilizatorilor tind să schimbe clasica conexiune dial-up cu modalități de conectare mai eficiente (cablu, ISDN, xDSL sau telefon mobil), pericolul unor atacuri reuşite asupra sistemului dumneavoastră creşte. Astfel, mărirea lărgimii de bandă a conexiunii la Internet facilitează posibilitatea de "strecurare" a intruşilor nedoriți.

Astfel, un firewall este folosit pentru două scopuri:

- pentru a păstra în afara rețelei utilizatorii rău intenționati (viruşi, viermi cybernetici, hackeri, crackeri) ;
- pentru a păstra utilizatorii locali (angajații, clienții) în rețea .

3.2.2 Politica Firewall-ului

Înainte de a construi un firewall trebuie hotărâtă politica sa, pentru a şti care va fi funcția sa şi în ce fel se va implementa această funcție.

Politica firewall-ului se poate alege urmând câțiva paşi simpli:

- alege ce servicii va deservi firewall-ul
- desemnează grupuri de utilizatori care vor fi protejați
- defineşte ce fel de protecție are nevoie fiecare grup de utilizatori
- pentru serviciul fiecărui grup descrie cum acesta va fi protejat
- scrie o declarație prin care oricare alte forme de access sunt o ilegalitate

Politica va deveni tot mai complicată cu timpul, dar deocamdată este bine să fie simplă şi la obiect.

3.2.3 Clasificări

Firewall-urile pot fi clasificate după:

- Layerul (stratul) din stiva de rețea la care operează
- Modul de implementare

În funcție de layerul din stiva TCP/IP (sau OSI) la care operează, firewall-urile pot fi:

- Layer 2 (MAC) şi 3 (datagram): packet filtering.
- Layer 4 (transport): tot packet filtering, dar se poate diferența între protocoalele de transport şi există opțiunea de "stateful firewall", în care sistemul ştie în orice moment care sunt principalele caracteristici ale următorului pachet aşteptat, evitând astfel o întreagă clasă de atacuri
- Layer 5 (application): application level firewall (există mai multe denumiri). În general se comportă ca un server proxy pentru diferite protocoale, analizând şi luând decizii pe baza cunoştințelor despre aplicații şi a conținutului conexiunilor. De exemplu, un server SMTP cu antivirus poate fi considerat application firewall pentru email.

Deşi nu este o distincție prea corectă, firewallurile se pot împărți în două mari categorii, în funcție de modul de implementare:

- dedicate, în care dispozitivul care rulează software-ul de filtrare este dedicat acestei operațiuni şi este practic "inserat" în rețea (de obicei chiar după router). Are avantajul unei securități sporite.
- combinate cu alte facilități de networking. De exemplu, routerul poate servi şi pe post de firewall, iar în cazul rețelelor mici acelaşi calculator poate juca în acelați timp rolul de firewall, router, file/print server, etc.

3.2.4 Ce "poate" şi ce "nu poate" să facă un firewall?

Un firewall poate să:

- monitorizeze căile de pătrundere în rețeaua privată, permițând în felul acesta o mai bună monitorizare a traficului şi deci o mai uşoară detectare a încercărilor de infiltrare;
- blocheze la un moment dat traficul în şi dinspre Internet;
- selecteze accesul în spațiul privat pe baza informațiilor conținute în pachete.
- permită sau interzică accesul la rețeaua publică, de pe anumite stații specificate;
- şi nu în cele din urmă, poate izola spațiul privat de cel public şi realiza interfața între cele două.

De asemeni, o aplicație firewall nu poate:

- interzice importul/exportul de informații dăunătoare vehiculate ca urmare a acțiunii răutăcioase a unor utilizatori aparținând spațiului privat (ex: căsuța poştală şi atașamentele);
- interzice scurgerea de informații de pe alte căi care ocolesc firewall-ul (acces prin dial-up ce nu trece prin router);
- apăra rețeaua privată de utilizatorii ce folosesc sisteme fizice mobile de introducere a datelor în rețea (USB Stick, dischetă, CD, etc.)
- preveni manifestarea erorilor de proiectare ale aplicațiilor ce realizează diverse servicii, precum şi punctele slabe ce decurg din exploatarea acestor greşeli

3.3 Informații despre firewall sun Windows XP

3.3.1 Cum încep să utilizez un firewall?

Un firewall este încorporat în Microsoft Windows® XP. Este posibil să începeți chiar astăzi, utilizând caracteristica "Paravan de protecție Windows XP pentru conexiunea Internet". În majoritatea situațiilor, pașii din pagina despre protejarea PC-ului vă ajută să activați firewall-ul pentru conexiunea Internet în Windows XP şi trebuie utilizat dacă aveți un singur computer cu care vă conectați la Internet. Câteva opțiuni suplimentare pentru firewall mai sunt disponibile, acestea fiind soluții software şi hardware. Acestea ar trebui luate în considerare dacă aveți o versiune mai veche de Windows, dacă aveți probleme de compatibilitate cu firewall-ul din Windows XP sau dacă intenționați să utilizați un firewall cu caracteristici diferite.

Versiunile de Windows anterioare Windows XP nu se livrau cu un firewall pentru conexiunea Internet. Dacă aveți un computer cu o versiune mai veche de Windows şi acesta este conectat direct la Internet, ar trebui să cumpărați şi să utilizați un firewall.

3.3.2 Cum aflu ce versiune de Windows utilizez?

1.Faceți clic pe Start, apoi pe Run.
2.În caseta de dialog Executare, tastați winver. Faceți clic pe OK. O casetă de dialog vă va spune ce versiune de Windows executați.

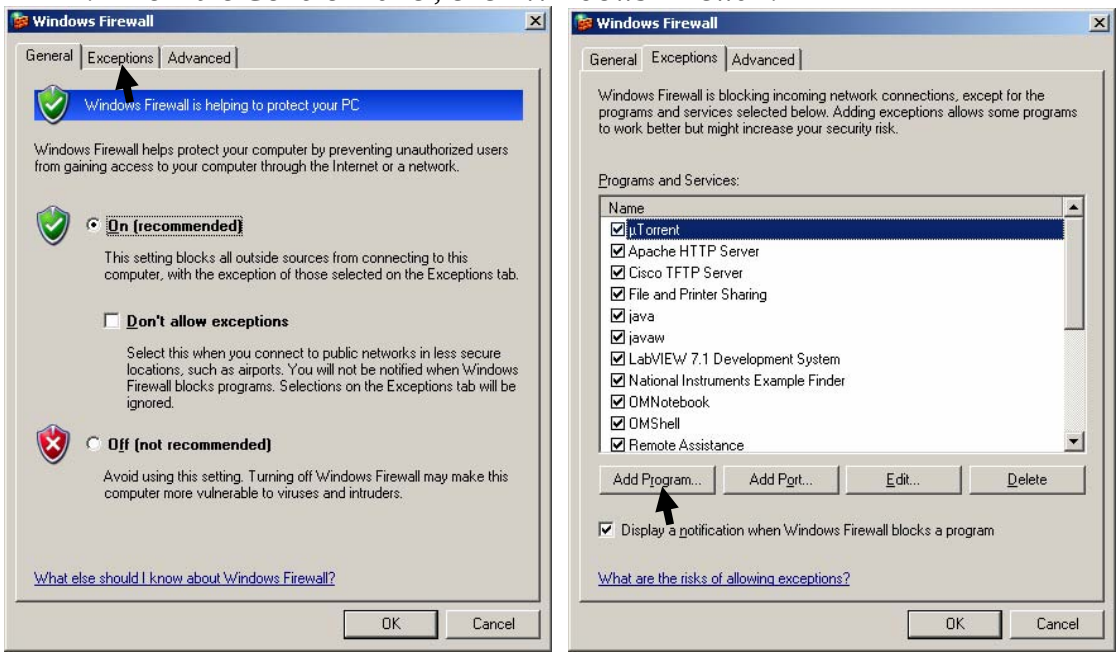
Utilizatorii de Windows XP care doresc caracteristici diferite într-un firewall pot să utilizeze, de asemenea, un firewall hardware sau unul software de la un alt

producător. În unele situații, utilizatorii avansați pot opta pentru utilizarea în rețea atât a unui firewall software cât şi a unuia hardware.

3.3.3 Verificarea stării Windows Firewall

Pentru a verifica dacă verify that Windows Firewall este pornit se efectuează următorii paşi:

1. Click **Start**, and then click **Control Panel**.
2. From the **Control Panel**, click **Windows Firewall**.

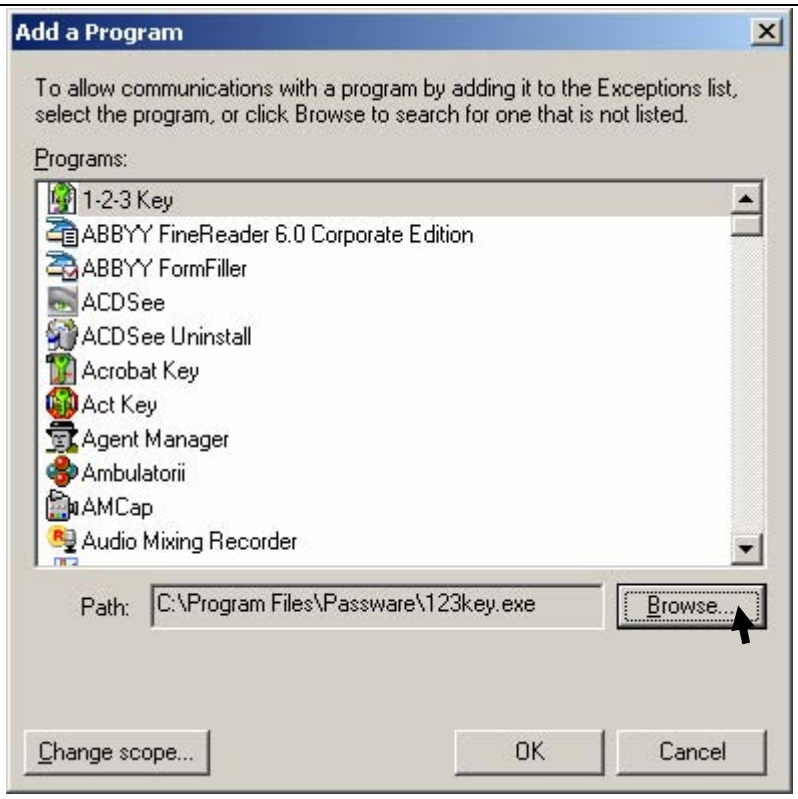


3. Dacă Windows Firewall este **On**, atunci este pornit.
4. Dacă Windows Firewall este **Off**, atunci el este închis, pentru al porni click pe **On**.

3.3.4 Adăugarea unei excepții în Windows Firewall

Uneori, Windows Firewall blochează un program care este folosit pentru conectarea la Internet. Dacă dorim ca acest program să aibă acces la Internet, putem adăuga în Windows Firewall o excepție pentru acesta, lucru care se efectuează astfel:

1. Dăm clik pe tab-ul Exceptions)figura de mai sus);
2. Clik pe Add Program …
3. în **Add a Program** dialog box, click **Browse**.



4. şi căutăm aplicația căreia dorim să-i permitem să treacă de Firewall;
5. Windows Firewall va adăuga o excepție pentru programul selectat. Şi îi va permite să se conecteze pe Internet cu un alt calculator. (de exemplu Yahoo Messenger).

3.3.5 Probleme de compatibilitate cu ISP, hardware sau software

Conexiunile la Internet ale unor distribuitori ISP nu apar în folderul Conexiuni în rețea. De exemplu, versiunile mai vechi ale programelor de conexiune AOL sau MSN nu sunt compatibile cu firewall-ul din Windows XP. Dacă vă confruntați cu această incompatibilitate, luați legătura direct cu distribuitorul ISP pentru asistență. În anumite cazuri, distribuitorii ISP furnizează un firewall personal alternativ, fie software, fie hardware.

În anumite cazuri, conexiunea pentru ISP poate apărea în folderul Conexiuni în rețea, însă nu veți vedea fila Complex în caseta de dialog Proprietăți conexiune sau nu veți vedea caseta de selectare Paravan de protecție a conexiunii la Internet. Aceasta înseamnă că software-ul de conexiune ISP nu este compatibil cu firewall-ul.

Firewall-ul poate să interfereze cu anumite programe şi utilitare de rețea de pe computer. În majoritatea cazurilor, aveți posibilitatea să corectați selectiv aceste incompatibilități reglând funcționarea firewall-ului sau cerând asistență furnizorului de software sau ISP. Uneori, o versiune nouă de software va corecta această problemă.

3.4 Desfăşurarea lucrării

Studenții vor efectua următoarele operații:

- vor verifica dacă Windows Firewall este pornit, iad dacă acesta este închis îl vor porni;
- vor adăuga o excepție pentru aplicația "Windows Messenge", a cărei locație pe hard disc este "C:\Program Files\Messenger\msmsgs.exe";

3.1 Păcălirea Firewall/IDSurilor şi ascunderea identității

Mulți pionieri ai internetului au prevăzut o rețea globală deschisă cu un spațiu universal de adrese IP permițând conexiuni virtuale între oricare două noduri. Acest lucru permite hosturilor să acționeze ca parteneri în comunicație, să servească şi să obțină informații unul de la celalalt. Oamenii pot accesa sistemele de acasă, să schimbe temperatura în casă sau să deschidă uşa pentru oaspeții grăbiți. Viziunea conectivității universale a fost înăbuşită de micşorarea spațiului de adrese şi de problemele de securitate. La începutul anilor 90, organizațiile au început implementarea firewallurilor cu scopul precis de reducere a conectivității. Rețele uriaşe au fost separate de Internetul nefiltrat prin aplicații proxy, traduceri de adrese de rețea (NAT) şi filtre de pachete. Fluxul nerestricționat de informații a făcut loc canalelor de comunicație aprobate şi supuse unor anumite reguli, precum şi controlului datelor ce trece prin ele.

Obstacolele din rețea cum ar fi firewallurile pot face din maparea rețelei o operație extrem de dificilă. Nu va deveni mai uşor din moment ce constrângerile aplicate rețelei reprezintă adesea un scop al implementării noilor echipamente în rețea. Nu e mai puțin adevărat ca Nmap oferă multe opțiuni pentru înțelegerea acestor rețele complexe şi să verifice dacă filtrele funcționează aşa cum trebuie. Chiar suportă mecanisme de depăşire a sistemelor de apărare prost implementate. Puneți-vă în pielea unui atacator şi aplicați tehnici din aceasta secțiune în rețeaua dumneavoastră. Lansați un atac sărit FTP, o scanare Idle, o fragmentare a atacului sau încercați realizarea unui tunel printr-un proxy de-al dumneavoastră.

În plus față de restricțiile rețelelor, companiile au început să monitorizeze traficul cu sisteme de detecție a intruziunilor (IDS). Toate IDSurile cunoscute sunt livrate cu reguli care să detecteze scanările Nmap deoarece acestea preced de obicei un atac. Multe dintre acestea sau transformat în sisteme de *prevenire*a intruziunilor (IPS) care blochează în mod activ traficul presupus malițios. Din păcate pentru administratorii de rețea şi vânzătorii IDSurilor, detectarea în mod corect a relelor intenții prin analizarea pachetelor este o problemă dificilă. Atacatorii cu răbdare, îndemânare şi ajutor din partea anumitor opțiuni Nmap pot în mod normal să treacă de IDS nedetectați. Între timp, administratorii au de a face cu o mulțime de alerte false când trafic inocent este greşit diagnosticat şi se emite o atenționare sau este chiar blocat.

Câteodată oamenii sugerează ca Nmap nu ar trebui să ofere funcții de păcălire a regulilor firewallurilor sau de trecerea nedetectata de IDS. Argumentează prin faptul că pot fi folosite de atacatori. Problema în acest raționament este că atacatorii tot vor găsi instrumente sau patchuri pentru Nmap pentru a realiza acest lucru. Între timp, administratorii pot descoperii că munca lor este mult mai dificilă. Instalarea numai a serverelor FTP moderne, cu patchurile aplicate la zi este o metodă mult mai bună de protecție decât prevenirea distribuirii instrumentelor ce implementează atacurile sărite FTP.

Nu există nici o opțiune magică în Nmap pentru detectarea şi păcălirea firewallurilor si a sistemelor IDS. Acest lucru ia îndemânare şi experiență O prezentare detaliată este dincolo de scopul acestei lucrări de laborator, care listează doar opțiunile relevante şi descrie ce fac ele.

`-f` (fragmentează pachetele);
`--mtu` (foloseste MTU specificat – Unitatea Maxima de Transmitere)

Opțiunea `-f` face ca scanarea cerută (incluzând scanarea ping) să folosească fragmente mici de pachete IP. Ideea este împărțirea headerului TCP în mai multe pachete pentru a îngreuna misiunea filtrelor de pachete, sistemelor de detectare a intruziunilor şi a altor elemente de detectare a activității. Atenție cu aceasta opțiune! Unele programe au probleme în manevrarea acestor pachete mici. De exemplu Sniffit eşua după primirea primului fragment. Specificați această opțiune o dată şi Nmap va împărți pachetul în fragmente de opt bytes sau mai puțin după headerul IP. Astfel, un header TCP de 20 bytes va fi împărțit în 3 pachete. Două de opt bytes şi unul cu ultimii patru. Desigur, fiecare fragment are propriul header TCP. Specificați `–f` încă o dată pentru folosirea a 16 bytes pe fragment (reducând numărul de fragmente). Sau puteți specifica propriile dimensiuni cu opțiunea`--mtu`. Nu specificați şi `-f` dacă folosiți `--mtu`. Dimensiunea trebuie să fie un multiplu de 8. Pachetele fragmentate nu vor trece de filtrele de pachete şi firewallurile care interoghează toate fragmentele IP, cum ar fi opțiunea CONFIG_IP_ALWAYS_DEFRAG din kernelul Linuxului, unele rețele nu-şi pot permite pierderea de performanță cauzată de aceste configurări şi le dezactivează. Altele nu pot activa configurările de acest gen deoarece fragmentele pot intra pe rute diferite în rețea. Unele sisteme defragmentează pachetele de ieşire în kernel. Linux cu modulul de urmărire a conexiunii din iptables este un exemplu. **Realizați o scanare şi rulați în acelaşi timp un sniffer de genul Ethereal pentru a vă asigura că pachetele sunt fragmentate.** Dacă sistemul de operare vă crează probleme, încercați opțiunea `--send-eth`de sărire a nivelului IP şi de trimitere de cadre ethernet brute.

`-D <momeala1 [,momeala2][,ME (EU)],...>`(Scanare acoperita de momeli)

Face ca o scanare acoperită de momeli să fie executată, ceea ce face ca ținta să creadă că momelile specificate ca argument scanează şi ele rețeaua. Astfel IDS poate raporta 5-10 scanări de porturi de la adrese IP unice, dar nu va ştii care adresă scanează cu adevărat şi care sunt momeli inocente. Cu toate ca aceasta tehnica poate fi contrată prin urmărirea căii prin routere, ignorarea răspunsului şi alte mecanisme active, ea reprezintă o tehnică eficientă de ascundere a adresei IP.

Separați fiecare momeală prin virgule şi folosiți opțional `ME` (adică propria adresa IP) ca una dintre momeli pentru a reprezenta adevărata poziție a adresei IP reale. Daca puneți `ME` în a şasea poziție sau mai târziu, unele detectoare de scanări de porturi (cum ar fi Solar Design) pot să nici nu afişeze adresa IP reală. Dacă nu folosiți `ME`, nmap îl va pune într-o poziție aleatoare.

Rețineți faptul că țintele pe care le folosiți ca momeli trebuie să fie active sau altfel riscați să inundați cu pachete SYN ținta. În aceeaşi ordine de idei, este uşor de determinat cine face scanarea dacă o singură adresă IP este activă. E de preferat să utilizați adrese IP în loc de nume (astfel încât numele hostului dumneavoastră să nu apară în logurile DNSului țintă).

Momelile sunt folosite atât în pingul inițial (folosind ICMP, SYN, ACK sau orice altceva) şi în timpul scanării efective de porturi. Momelile sunt de asemenea folosite la detectarea sistemului de operare (`-O`). Momelile nu funcționează cu detecția versiunii sau scanarea TCP connect().

Nu folosiți prea multe momeli deoarece pot încetini scanarea şi o pot face mai puțin corectă. De asemenea, unii ISP vor filtra pachetele false, dar mulți nu restricționează pachetele IP de loc.

`-S <Adresa_IP>`(Seteaza adresa IP sursa)

În anumite circumstanțe, Nmap se poate afla în imposibilitatea determinării adresei sursă (Nmap va anunța dacă acest lucru se întâmpla). În această situație, folosiți `-S` cu adresa IP a interfeței pe care doriți să trimiteți pachetele.

Altă posibilă utilizare a acestei opțiuni este să faceți ținta să creadă că este scanata de *altcineva*. Imaginativă o companie permanent scanată de un competitor! Opțiunea `-e` va fi în general necesară pentru astfel de utilizare si `-P0` este de asemenea recomandă.

`-e <interfata>`(Foloseste interfata specificata)

Spune Nmapului ce interfață să folosească pentru trimiterea şi primirea pachetelor. Nmap ar trebui să poată determina automat acest lucru, dar vă va anunța dacă nu poate.

`--source-port <numarul_portului>;-g <numarul_portului>`(Seteaza portul sursa)

O greşeală surprinzător de des întâlnită o reprezintă configurarea relațiilor de încredere în funcție de numărul portului sursă. Este ușor de înțeles cum stau lucrurile. Un administrator instalează un nou firewall şi este apoi îngropat în plângeri din partea utilizatorilor nemulțumiți ale căror aplicații nu mai funcționează. În particular, DNSul poate fi blocat deoarece răspunsurile UDP DNS de la serverele externe nu mai pot intra în rețea. FTP este un alt exemplu. În transferurile FTP active, serverul încearcă să stabilească o conexiune înapoi la client pentru transferarea fişierului solicitat.

Soluții securizate la aceste probleme există, de obicei sub forma de proxiuri la nivelul aplicație sau module firewall care analizează protocoalele. Din păcate există şi soluții mai simple şi mai nesigure. Notând faptul că răspunsurile DNS vin de la portul 53 şi cele de la conexiunile FTP de la portul 20, mulți administratori au căzut în capcana permiterii necondiționate a traficului de la aceste porturi. Adesea ei presupun că nici un atacator nu va observa şi exploata astfel de găuri în firewall. În alte cazuri, administratorii consideră aceasta rezolvare ca una pe termen scurt până când vor implementa o soluție mai sigură. Apoi ei uită să mai facă upgradeul de securitate.

Administratorii rețelelor supraîncărcate nu sunt singurii care cad în această capcană. Numeroase produse au fost livrate cu aceste reguli nesigure. Chiar şi Microsoft are partea ei de vina. Filtrele IPsec livrate cu Windows 2000 şi Windows XP conțin o regulă implicită care permite traficul oricărui pachet UDP cu portul sursa 53 (DNS) sau 67 (DHCP).

Nmap oferă opțiunile `-gsi--source-port` (care sunt echivalente) pentru exploatarea acestei slăbiciuni. Specificați un număr ca argument şi Nmap va trimite pachete de la acel port oricând acest lucru este posibil. Nmap trebuie să folosească porturi diferite pentru anumite teste de detectare a sistemului de operare şi cererile DNS ignoră opțiunea `--source-port` deoarece Nmap se bazează pe librăriile sistemului pentru a le manevra. Multe scanări TCP, incluzând-o pe cea SYN, suportă această opțiune, la fel ca şi scanarea UDP.

`--data-length <numar>` (Adaugă un număr aleator de date la pachetul trimis)

În mod normal Nmap trimite pachete minimaliste conținând doar headerul. Astfel pachetele TCP au în general 40 bytes şi cererile de răspuns ICMP doar 28. Această opțiune adaugă un numărul dat ca argument de bytes, generați aleator, la majoritatea pachetelor trimise. Pachetele pentru detecția sistemului de operare (`-O`) nu

sunt afectate, dar majoritatea pingurilor şi scanărilor de porturi sunt. Acest lucru încetineşte viteza de scanare, dar pachetele pot fi mai puțin suspicioase.

`--ttl <valoare>`(Seteaza campul IP time-to-live – timp de viata)

Setează câmpul IP time-to-live – timp de viata – la valoarea specificată.

`--randomize-hosts`(Scaneaza hosturile in ordine aleatoare)

Spune Nmapului să aranjeze aleator grupuri de 8096 hosturi înainte de scanare. Această opțiune poate face scanarea mai puțin vizibilă pentru anumite sisteme de monitorizare a rețelei, în special când se combină cu un specificator mic de timp. Dacă vreți ca aranjarea aleatoare să se realizeze pentru grupuri mai mari, creşteți valoarea PING_GROUP_SZ din`nmap.h`si şi recompilați. O soluție alternativă o reprezintă generarea listei de IPuri ce urmează a fi scanată cu o scanre de tip lista (`-sL -n -oN`*`numefisier`*), şi să realizați aranjarea aleatoare a lor cu un script Perl, apoi să furnizați întreaga listă Nmapului cu opțiunea `-iL`.

`--spoof-mac <adresa mac, prefix, numele vanzatorului >`(Falsifica adresa MAC)

Cere Nmapului să folosească adresa MAC furnizată pentru toate cadrele ethernet pe care le trimite. Această opțiune implică `--send-eth` pentru a se asigura că Nmap trimite pachetele la nivelul rețea. MAC-ul specificat poate avea câteva formate. Dacă spcificați şirul “0”, Nmap alege un MAC complet aleator pentru sesiunea respectivă. Daca şirul furnizat este un număr par de digiți hexa (cu perechile separate prin caracterul “:”), Nmap va folosi respectiva adresa MAC. Dacă mai puțin de 12 digiți sunt furnizați, Nmap umple 6 bytes cu valori aleatoare. Dacă argumentul nu este nici 0, nici şir hexa, Nmap caută în `nmap-mac-prefixes` pentru a găsi un producător care să conțină şirul dat (căutare insenzitivă). Dacă o asemănare este găsită, Nmap foloseşte identificatorul unic al vânzătorului (3 bytes) şi completează cu 3 bytes aleşi aleator.

argumentele valide ale opțiunii `--spoof-mac` sunt `Apple 0`,`01:02:03:04:05:06`, `deadbeefcafe`, `0020F2`, şi `Cisco`.

4 Proxy server

4.1 Obiective:

- înțelegerea funcționării şi a rolului unui server proxy în securitatea sistemelor informatice;
- pornirea şi configurarea unui server proxy sub sistemului de operare Windows XP;
- instalarea şi configurarea WinGate.

4.2 Generalități/Definiții Server Proxy

Probabil că mulți dintre dumneavoastră, dacă vă veți hotărî să instalați un astfel de server pentru rețeaua la care sunteți conectați, veți fi puşi în fața unor decizii destul de grele, problema configurării unui astfel de sistem fiind destul de complicată. În continuare se vor prezenta câteva soluții în acest sens, pentru mai multe variante de rețea (Windows NT sau Windows 2000, Unix) pentru a vă ajuta să instalați şi să configurați cu succes un astfel de program.

4.3 Server Proxy pentru WINDOWS

Prima soluție se pretează platformelor Windows NT sau Windows 2000 şi poartă numele de Microsoft Proxy 2.0. După ce vă hotărâți să procedați la instalarea acestui proxy va trebui să validați pentru instalare (să bifați sau să debifați) opțiunile necesare pentru ca serverul să funcționeze în parametrii doriți de dumneavoastră. Recomandate sunt opțiunile de instalare a serverului propriu-zis, share-ul pentru clienții compatibili Windows NT şi Windows 9x, uneltele de administrare şi eventual documentația şi suportul pentru clienții ce folosesc Windows NT Alpha sau Windows 3.x.

Stabilirea valorii cache

Al doilea pas este configurarea cache-ului, pentru acest lucru aveți nevoie de o partiție NTFS, celelalte tipuri nefiind suportate. Puteți să nu selectați instalarea cache-ului, dar atunci nu veți beneficia decât de opțiunile de securitate ale serverului. Va trebui să specificați valoarea cache-ului, pentru calculul acesteia fiind recomandată formula 0,5xC+100MB, unde C este numărul de clienți deserviți de server.

Tabela de adrese locale

În a treia etapă va trebui să configurați tabela de adrese locale (Local Address Table - LAT). Prin intermediul acestei tabele clientul proxy va şti care sunt adresele locale din rețea în scopul de a le contacta fără a mai „trece" prin serverul proxy. Aici aveți mai multe opțiuni, puteți adăuga un interval de adrese (Add private ranges), dar trebuie avut în vedere că acestea vor fi acceptate ca fiind adrese interne referitor la Internet şi procedura trebuie executată cu atenție pentru a nu se „strecura" vreo adresă externă nedorită. De asemenea puteți încărca adresele existente în tabela de rutare (Load from NT internal Routing Table) ale tuturor adaptoarelor de rețea sau le puteți selecta doar pe cele dorite. În cazul în care există adaptoare de rețea conectate la o rețea externă trebuie să selectați „Load known address ranges from the following IP interface cards"

şi apoi să selectaţi doar dispozitivele interne. Puteţi, bineînţeles, să inseraţi sau să ştergeţi adrese specifice din LAT, cu condiţia de a nu introduce adrese IP externe.

Configurarea clienţilor

Prima dată trebuie să stabiliţi cum se vor conecta clienţii la server, aceasta făcându-se în două moduri, fie după numele de host fie după adresa IP. A treia opţiune, configurarea manuală, nu este disponibilă decât dacă reinstalaţi serverul proxy, caz în care puteţi păstra sau suprascrie configuraţia deja existentă.

Apoi este recomandat să optaţi pentru configurarea automată a browserelor Web pentru a suporta proxy, deci validarea opţiunii „Automatically configure the clients Web browser during the client setup" şi configurarea automată definită în fişierul Array.dll. Valoarea pentru portul TCP nu trebuie modificată (portul prestabilit este TCP 80). Se poate renunţa la folosirea configuraţiei existente predefinite în Array.dll, putând fi folosit un script de configurare, sau se pot modifica unele setări din Array.dll prin apelarea la configurarea avansată a clienţilor (Advanced Client Configuration) disponibilă ulterior accesării proprietăţilor (Properties). În acest punct puteţi stabili dacă browserele Web vor folosi proxy pentru serverele locale, opţiune iniţial nevalidată. De asemenea puteţi seta ca pentru anumite adrese IP conectarea să nu se facă prin intermediul proxy, adresele şi măştile lor de subreţea trebuind să le specificaţi în fereastra de mai jos. Poate să se renunţe la proxy în favoarea conectării directe pentru anumite domenii şi se poate modifica ruta de siguranţa (în cazul în care serverul proxy nu mai este funcţional se recurge la o rută alternativă care poate fi un alt proxy sau conectarea directa la Internet).

Limitarea accesului

În acest punct se stabilesc criteriile de limitare a accesului la unele protocoale sau servicii Internet. Puteţi dispune de controlul accesului pentru WinSock Proxy Service, pentru Web Proxy Service sau pentru amândouă. Iniţial, ambele sunt selectate şi e bine de ştiut că în configuraţia prestabilită nu se oferă acces nimănui din reţeaua internă către Internet prin serverul proxy. Dacă optaţi pentru configuraţia prestabilită trebuie apoi să creaţi drepturi (pentru grupuri, staţii solitare sau pentru toata reţeaua internă) privind conectarea la Internet prin intermediul serverului proxy. De asemenea se poate beneficia de opţiunea filtrării de pachete în cazul în care aţi optat pentru instalarea uneltelor de administrare. Această filtrare de pachete limitează tipul de trafic şi de conexiuni pe care utilizatorii externi le fac către reţeaua internă. Înainte de a apela la un server proxy trebuie avute în vedere configuraţia şi structura reţelei şi de software-ul de reţea de pe staţiile client folosit pentru a contacta reţeaua externă. În momentul implementării serverului se recomandă să faceţi o listă cu toate aplicaţiile TCP/IP folosite de către clienţi pentru conectarea la reţeaua externa, în special trebuie avute în vedere browserele Web folosite deoarece fiecare aplicaţie ce doriţi să folosească serve-rul proxy trebuie configurată în acest sens. Browserele cunoscute, cum sunt Internet Explorer sau Netscape, pot fi configurate automat, dar poate fi nevoie de configurare manuală pentru alte aplicaţii. Integrarea serverului proxy în reţea se află în strânsă legătură cu modul în care clienţii se conectează la Internet. De exemplu, dacă doriţi forţarea conexiunii numai prin intermediul proxy, trebuie să aveţi grijă să nu mai existe alte rute către Internet disponibile. În acest caz este esenţial să dezactivaţi opţiunea „IP forwarding" pentru serverul dumneavoastră. Acest lucru se poate face din pagina de proprietăţi pentru TCP/IP, şi în cazul în care nu dezactivaţi această opţiune serverul pe care este instalat proxy poate face rutarea de pachete fără a

mai folosi proxy. De asemenea trebuie verificate şi routerele existente ce pot oferi acces la Internet, dacă acestea există trebuie să satisfacă aceleaşi condiţii de control şi securitate oferite de proxy.

4.4 Desfăşurarea lucrării

4.4.1 Instalare şi configurare server proxy WinGate

Versiunea WinGate 6.2.1 se poate download-a şi folosi timp de 30 de zile gratuit de pe http://www.wingate.com/download.php .

Cele mai indicate moduri de instalare a WinGate sunt prezentate în figura 1, în care serverul WinGate are legătură directă la Internet sau prin intermediul unui modem sau router. Pe această interfață, Serverul are o adresă IP publică. Pentru conexiunea la rețeaua locală, poate avea o a doua interfață, conectată cu un switch pentru a permite accesul mai multor utilizatori.

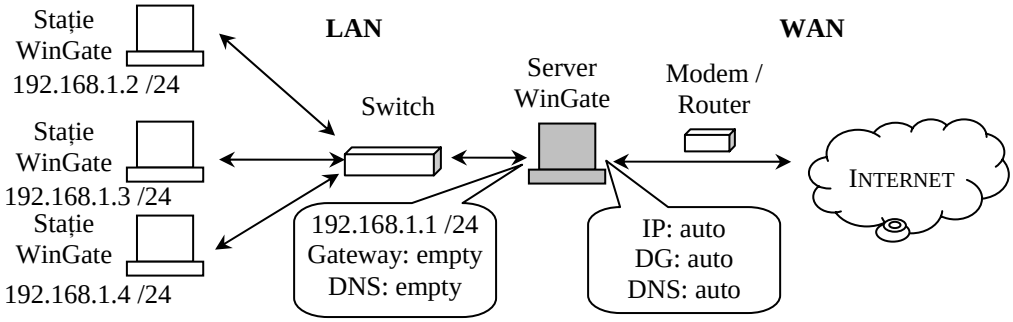


Fig. 1: Instalarea şi cofigurarea unui server proxy sub Windows.

Configurarea adaptorului pentru LAN

Placa de rețea de pe Server care va fi conectată la LAN, va fi configurată static cu un IP privat (vezi figura 1), iar câmpurile pentru Default Gateway şi DNS server for fi lăsate goale.

Configurarea adaptorului pentru WAN

Placa de rețea ce va face conexiunea cu Internetul va fi configurată astfel:

1. dacă conexiunea este realizată direct la internet, se va da un IP static Public, care este oferit de către providerul de Internet (ISP);
2. dacă conexiunea este realizată printr-un router (aşa ca în laborator), care are pe el un server de DHCP pornit, atunci IP va fi obținut automat bifând opțiunea **Obtain IP address automatically.**

Procesul de instalare

Procesul de instalare este identic oricărei aplicații sub Windows.

La instalare trebuie să optăm pentru una din variantele: Client WinGate sau Server WinGate.

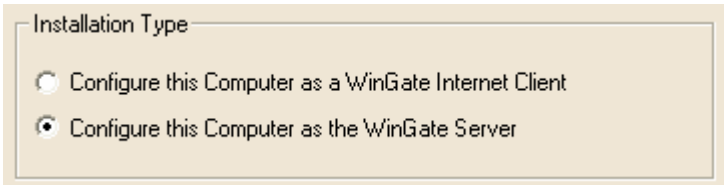


Fig.2: Alegerea tipului instalării: Server sau Client WinGate.

WinGate Server va fi instalat doar pe un singur calculator, cel care va face legătura la Internet.

Ferestrele care se deschid în procesul de instalare sunt următoarele:

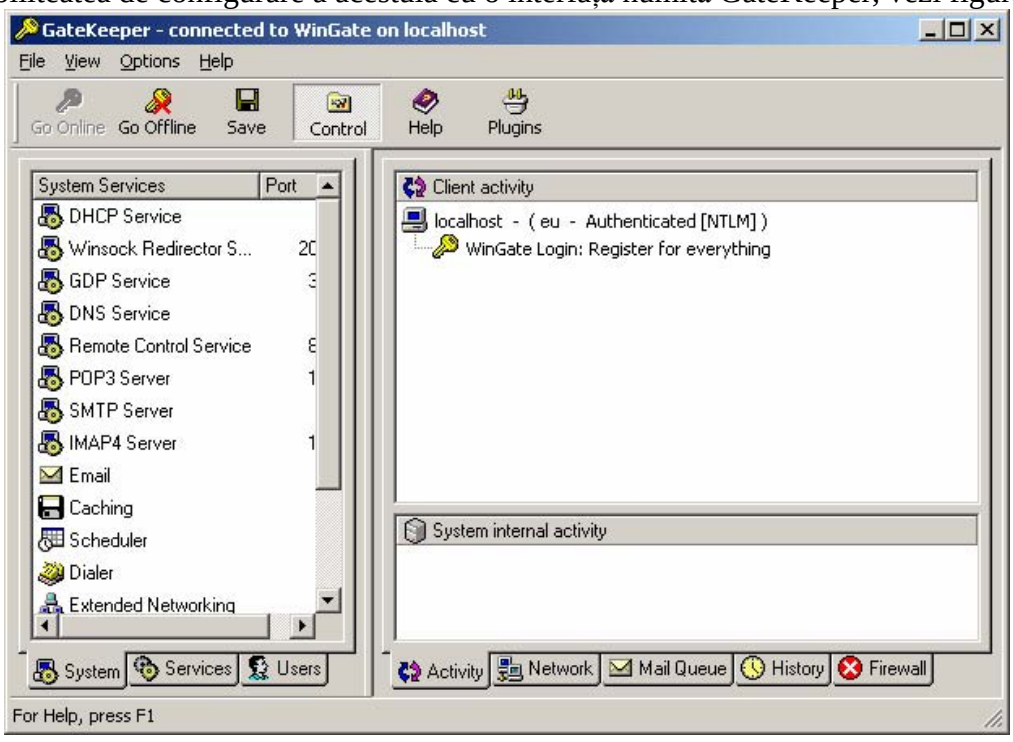
1. Install directory
2. Important
3. NT Users and Authentication
4. Email
5. ENS
6. Auto Update
7. Activate WinGate
8. Begin Installation
9. Installation Completed

Procesul Post-instalare

Odată ce WinGate Server a fost instalat, sunt câteva setări care trebuie făcute pentru a ne asigura de corectitudinea funcționării WinGate.

1. WinGate Engine - este instalat şi rulează ca serviciu numit Qbik WinGate Engine, şi poate avea trei stări de funcționare: stating, running şi stopped.

2. GateKeeper – oferă toate funcționalitățile lui WinGate pentru a opera şi oferă posibiliteatea de configurare a acestuia cu o interfață numită GateKeeper, vezi figura 2.



Conexiunea la rețea

După conectarea la GateKeeper, următorul pas este şă se verifice dacă WinGate a descoperit şi clasificat corect conexiunea la rețea, lucru care se face astfel:

1. se selectează tab-ul **Network** de pe partea dreaptă a GateKeeper;
2. în secțiunea **network connection** vor fi afişate toate interfețele descoperite de WinGate;
3. dublu click pe interfața care conectează WinGate Server la rețeaua locală;

4. în fereastra de dialog ce se deschide se alege General tab;
5. se verifică dacă interfața este setată pe **Auto** sau **Internal (trusted provate network)**;

Interfața Modem / Router – Internet

1. în fereastra Network connection, dublu click pe interfața care conectează Serverul WinGate la Modem, Router sau direct la Internet;
2. în **General** tab, se selectează butonul radio **External (untrusted network)**;
3. click **OK** pentru a salva modificările.

Astfel, această interfață va fi tratată de WinGate Server drept conexiunea externă care va fi folosită pentru accesarea Internetului.

Testarea conectivității cu clienții

Odată conectați la GateKeeper şi realizate setările pentru conexiunile la rețea, trebuie verificat că toate gazdele din LAN au acces la Internet.

Implicit, oricine are acces la Internet prin WinGate, până când vor fi definite restricții. Utilizatorii pot fi urmăriți în Activity tab.

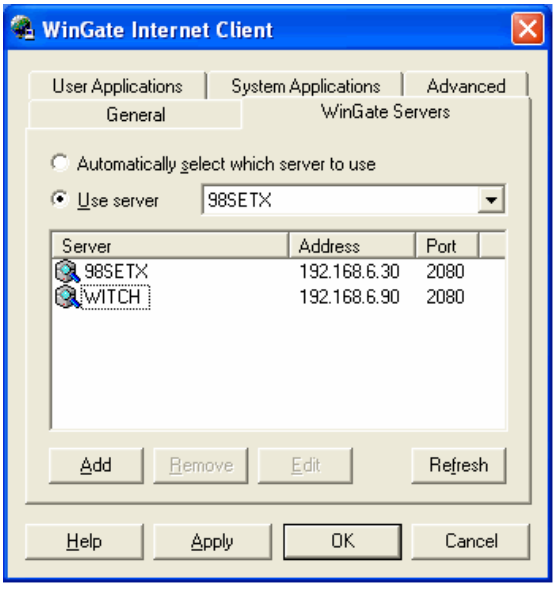
4.4.2 Instalare şi configurare Client proxy WinGate

Pe stațiile din rețea, care se vor conecta la Internet prin Proxy, se va instala aplicația Client proxy WinGate, lucru realizabil prin selectarea în procesul de instalare a opțiunii Client, vezi figura 2.

WinGate Internet Client (WGCI) este un apllet care odată instalat pe stația client, ne ajută să comunicăm cu toate cererile de navigare pe Internet adresate către Winsock Redirector Service de pe WinGate Server.

Când o aplicație bazată pe Winsock, cum ar fi un browser internet sau un program de e-mail, emite o cerere către o maşină client de pe Internet, WGIC va intercepta cererea şi o va trimite la Winsock Redirector Service de pe WinGate Server care va trata cererea conform setărilor clientului.

Appletul WGIC permite definirea modului în care Winsock Redirector Service de pe WinGate Server va trata cererea unei aplicații client/server care rulează pe maşina clientului.



Appletul WinGate Internet Client

Pentru a lansa în execuție appletul WGIC:

Start → Programs → WinGate Internet Client → **WinGate Internet Client Applet**

şi va apare fereastra de mai sus.

WGIC va găsi automat orice server WinGate din rețea, atâta timp cât WinGate

server rulează şi are serviciul GDP pornit. Serviciul GDP este special proiectat să permită maşinilor WGID să detecteze prezența serverelor WinGate din rețea.

În exemplul din figura de mai sus, sunt două servere WinGate, 98setx şi Witch, care au fost detectate în rețea. Se poate seta appletul WGIC care din cele două servere să fie folosit, manual sau automat.

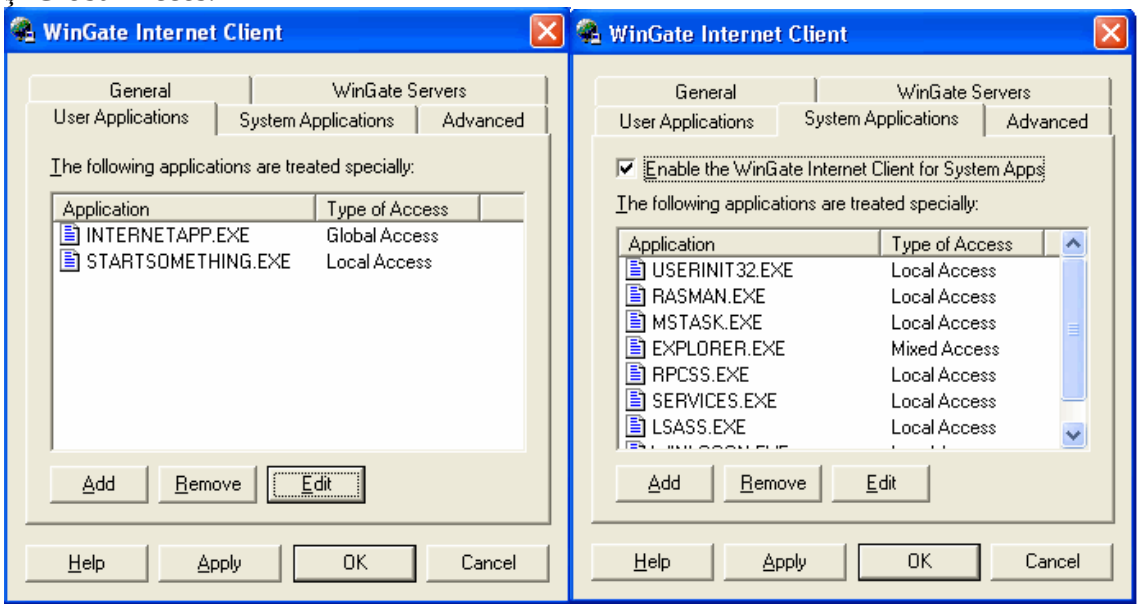
- **Server** – este numele din rețeaua Windows a PC-ului pe care rulează WinGate;
- **Address** – este adresa IP privată a Serverului WinGate;
- **Port** – este portul TCP pe care **Winsock Redirector Service** rulează pe serverul WinGate, **WGIC** foloseşte Winsock redirector Service pentru a oferi conectivitate la Internet prin WinGate, Implicit, WinGate foloseşte portul 2080 pentru a primit cererile WGIC.

Apăsând butonul Add, se deschide fereastra de mai jos, prin care se pot adăuga manual Servere WinGate.

Aplicații Utilizator – User Application

Acest tab permite configurarea modului în care WGIc va trata aplicațiile clientului care vor rula pe maşina WGIC.

Tipurile de acces pe care le pot avea aplicațiile sunt: Local Acces, Mixed Acces şi Global Acces.



System Aplication – sun listate aplicațiile sistemului şi modului de acces al acestora.

Majoritatea aplicațiilor listate au Local Access, care închide WGIC pentru anumite aplicații. În general, lista implicită nu necesită să fie modificată.

4.4.3 Modurile de lucru ale Winsock Redirection Application

Aplicațiile care rulează pe un computer pot fi împărțite în două categorii:

- **Aplicațiile client** – majoritatea aplicațiilor care cer o conexiune exterioară cu alte computere aflate pe Internet (în afara propriei rețel) pentru a obține anumite servicii.
  De exemplu, navigatorul web se conectează la un computer pe care rulează un server web şi cere să-i trimită o pagină web în limbaj HTML. Similar este şi serviciul de e-mail POP3.
- **Aplicații Server** – aceste aplicații ascultă datele de intrare venite de la alte computere şi oferă servicii către computerele cu care sunt conectate.

Modurile Aplicație

- **Local Access Mode**
  Dacă setăm aplicația unui client la Local Access în WGIC, se suspendă Winsock Redirector Service din WinGate de tratare a cererilor aplicațiilor.
  Aplicațiile din modul de acces local vor fi ignorate de WGIC şi astfel trebuie să posede o metodă de conexiune alternativă pentru aşi completa cererile. Acest mod face accesul local ideal pentru aplicațiile clienților care vor rula prin WGIC.
  În multe cazuri se doreşte utilizarea vitezei şi simplicității WinGate NAT pentru aplicațiile client (acest lucru necesită doar o conexiune aut către Internet). Orice aplicație care vrem să folosească NAT trebuie setată să ruleze în Local Acces Mode.
- **Mixed Access Mode**
  Acest mod este sigur dar funcțional doar pentru aplicațiile server. Acest mod permite întotdeauna aplicațiilor să facă orice conexiune către exterior cu Winsock redirector Service, dar va permite accesul doar a computerelor din aceeaşi rețea. Este mai apropiat pentru aplicațiile server gen Intranet Web sau Ftp servers. Se numeşte mixt, deoarece oferă o aplicație cu conectivitate atât globală cât şi locală.
  Modul de acces mixt este alocat automat oricărei aplicații server care încearcă să asculte pe un port sistem (orice mai mic de 1024). Acesta este un mecanism de siguranță al WGIC, care necesită în mod explicit setarea aplicații în Modul global de Acces pentru a fi vizibilă pe Internet.
- **Global Access Mode**
  Acest mod este utilizat când avem un server de aplicație ce rulează pe WGIC în spatele serverului WinGate, care are trebuie să primească cereri de pe Internet (server Web sau Ftp).
  O aplicație server poate asculta liber pe porturi sub 1024. Dar din motive de securitate a rețelei, configurația implicită pentru WGIC nu va permite nici unei aplicații să asculte porturi sub 1024. Dacă rulați un server cu un port sun 1024 şi doriți să fie accesibil computerelor din Internet trebuie configurat în mdoul de acces global.
  De obicei, serverul Web ascultă pe portul 80 iar un server FTP pe portul 21.

http://www.youngzsoft.net/ccproxy/

5 Proxy server Squid pe sistem de operare Linux

5.1 Obiective:

- înțelegerea funcționării şi a rolului unui server proxy în securitatea sistemelor informatice;
- pornirea şi configurarea unui server proxy sub sistemului de operare Linux;

5.2 Generalități/Definiții Server Proxy

Probabil că mulți dintre dumneavoastră, dacă vă veți hotărî să instalați un astfel de server pentru rețeaua la care sunteți conectați, veți fi puşi în fața unor decizii destul de grele, problema configurării unui astfel de sistem fiind destul de complicată. În continuare se vor prezenta câteva soluții în acest sens, pentru mai multe variante de rețea (Windows NT sau Windows 2000, Unix) pentru a vă ajuta să instalați şi să configurați cu succes un astfel de program.

5.3 Configurarea Squid pentru Linux

Squid este un Web proxy destinat pentru a rula sub sistemele Unix, este un software open-source foarte capabil, ce oferă foarte multe opțiuni administratorilor ce se decid să-l utilizeze, cu condiția de a fi instalat şi configurat corespunzător pentru a satisface necesitățile rețelei. Vom încerca să prezentam un ghid conținând cele mai importante aspecte privind configurarea acestui server, clasate pe domeniul de interes.

Opțiuni de rețea

Setarea portului la care Squid va face apel pentru a primi cereri HTTP se face cu comanda http_port. Valoarea predefinită a acestui port este 3128. Pentru a suprascrie în fişierul de configurare (squid.conf) valoarea portului se apelează opțiunea „-a” în linia de comandă, adică #/usr/local/squid/bin/squid -a <numar_port>.

Comanda http_port înlocuieşte vechea „tcp_ incoming_address”.

Pentru setarea portului prin care Squid trimite şi primeşte mesaje ICP de la cache-urile vecine se foloseşte comanda icp_ port. Valoarea predefinită pentru acesta este 3130, iar pentru suprascriere se utilizează opțiunea „-u”: #/usr/local/squid/bin/squid -u <numar_port>.

Pentru a se alătura unui grup multicast ca să primească mesaje multicasting ICP se foloseşte mcast_groups <Adresa_IP>. La aceasta opțiune se recurge doar dacă doriți să primiți mesaje multicast, şi predefinit Squid nu este setat pentru a primi astfel de mesaje. Pentru conectarea la distanță cu alte servere şi pentru comunicarea cu alte cache-uri folosind HTCP sau CARP este utilizată comanda tcp_outgoing_address <Adresa_IP>. Valoarea inițială este 255.255.255.255.

Pentru a primi mesaje ICP de la alte cache-uri se setează udp_incoming_address <Adresa_IP>, a cărui valoare predefinită este 0.0.0.0., iar pentru a trimite pachete ICP către celelalte cache-uri se foloseşte udp_outgoing_address <Adresa_IP>, a cărui valoare este implicit 255.255.255.255.

Următoarea secțiune se ocupă de cazul în care se implementează mai multe cache-uri Squid, şi anume de opțiunile de configurare ale algoritmului de selecție a cache-urilor vecine.

Pentru specificarea celorlalte cache-uri în ierarhie se apelează la comanda cache_peer. Aceasta se desfăşoară pe cinci câmpuri, primul este numele sau IP-ul cache-ului vecin ales, al doilea indică tipul de relație cu acesta, al treilea setează portul HTTP al serverului destinație iar al patrulea setează portul pentru ICP. Ultimul câmp este opțional, conține unul sau mai multe cuvinte cheie ce vor fi specificate mai jos. Linia de comanda ar fi cache_peer <IP_number><relatie> <port_HTTP> <port_ICP> [<cuvant_cheie_1> <cuvant_cheie_2> ... <cuvant_cheie_n].

Relația în care cache-ul curent se poate afla cu celelalte cache-uri este parent (parinte), sibling (pe acelaşi nivel) sau multicast (pentru grup multicast). Cuvintele cheie sunt proxy-only (pentru a nu salva local obiectele găsite în cache-ul vecin), weight=n (ce setează „gradul" părintelui, valoarea implicită pentru n este 1, cu cât n este mai mare cu atât creşte gradul de importanță al cache-ului specificat), ttl=n (pentru a seta un timp de viață al unui mesaj ICP pentru un grup multicast), no-query (pentru vecinii ce nu suporta ICP), default (în cazul în care cache-ul avut în vedere este văzut ca „ultimă soluție"), round-robin (în cazul în care se doresc a fi folosite mai multe linii cache_peer), multicast-responder (ce priveşte cache-ul în cauză ca fiind un membru al unui grup multicast, iar mesajele ICP nu vor fi trimise direct către acesta dar răspunsurile ICP de la el vor fi acceptate), closest-only (pentru a primi doar mesajele Closest_Parent_Miss şi nu First_Parent_Miss), no-digest (pentru a nu apela la acest vecin), no-netb-exchange (prin care se renunță la cerințele ICMP RTT de la acest vecin), no-delay (pentru a nu permite accesul acestui vecin să influențeze întârzierile), login=user:password (în cazul în care cache-ul părinte necesită autentificare), connect-timeout=nn (pentru a specifica timpul de aşteptare pentru realizarea conexiunii cu acest vecin, valoarea nn implicită fiind 30). De avut în vedere, dacă ați compilat Squid pentru a suporta HTCP, că se va proceda la conectarea TCP pe portul 4827, nefiind nici o opțiune de a schimba aceasta valoare.

Pentru a limita domeniile pentru care se va apela la cache-urile vecine se foloseşte cache_peer_domain. Linia de comandă este cache_peer_domain cache _host domain [domain ...]. Dacă înainte de numele domeniului introduceți „!" se produce negarea domeniului în cauză. Se pot introduce oricâte domenii doriți, în cazul mai multora apelul se va opri la primul ce va da răspuns pozitiv. De exemplu comanda cache_peer_domain parent.my.net.edu va trimite pachetele către serverul local doar dacă obiectul căutat există pe un server în domeniul .edu.
Este posibilă şi modificarea tipului de vecin pentru unele domenii specifice. Puteți trata câteva domenii diferit față de tipul specificat în cache_peer. De exemplu neighbor_type_domain cache.mycache.com sibling .com .net.

Tot în cadrul comenzilor folosite pentru mai multe cache-uri intră şi icp_query_timeout, maximum_icp_ query_timeout, mcast_icp_query_timeout, dead_peer_timeout ce sunt urmate de o valoare reprezentând numărul de milisecunde atribuite operațiunilor specificate în linia de comandă, operațiuni pe care nu le vom mai explica, titlul lor fiind destul de sugestiv.

O altă comandă este hierarchy_stoplist ... , prin care se renunța la apelarea vecinilor pentru anumite şiruri de caractere ce apar în URL-uri. De exemplu, hierarchy_stoplist asp jsp va verifica fiecare URL primit să vadă dacă există aceste cuvinte, iar dacă acestea apar nu se va apela la vecini ci se va contacta direct serverul apărut in URL.

Ultima şi poate cea mai importantă opțiune de pe acest nivel este no_cache. Prin aceasta linie de comandă se forțează apelarea directă a anumitor obiecte. Se face apel la

lista de control a accesului, deci vor exista de fapt două linii de comandă. Starea prestabilită este:

acl QUERY urlpath_regex cgi-bin \?

no_cache deny QUERY

Acl-ul QUERY asigură că URL-ul conținând cgi-bin nu va fi apelat prin cache.

Opțiuni ce afectează dimensiunea cache-ului

Aceste opțiuni setează valoarea memoriei folosite pentru parametrii cache-ului. Acestea sunt cache_mem (predefinit 8MB), cache_swap_low şi cache_swap_ high (parametri ce procedează la înlocuirea obiectelor din cache funcție de procentajul de utilizare a cache-ului, valoarea low prestabilită este 90 iar high 95), maximum_object_size, minimum_object_size şi maximum_object_size_in_ memory (cu valori date în bytes), ipcache_size (implicit 1024), ipcache_low şi ipcache_high (procentaje ce marchează limitele cachingului adreselor de IP, pentru low prestabilit 90, pentru high 95), şi setul cache_replacement_policy şi memory_replacement _policy ce stabileşte modul în care obiectele vor fi înlocuite în cache când este nevoie de spațiu.

Acest parametru poate fi LRU, GDSF (Greedy-Dual Size Frequency), LFUDA (Least Frequently Used With Dynamic Aging).

În următoarea secțiune ne vom ocupa de instrucțiunile ce privesc controlul accesului. Prima comandă din acest set este acl, şi se foloseşte pentru a defini o listă de acces.

Sintaxa este acl ... | „fisier”.

Sunt mulți parametri pentru , unul este src (mod prin care se specifica adresa IP). Sintaxa unei astfel de instrucțiuni este acl src IPaddress/netmask. Aproximativ acelaşi lucru se obține şi cu dst ca parametru, cu diferența ca se face referire la ServerIPaddress. Pentru controlul unui domeniu specific se pot folosi ca parametri srcdomain, dstdomain (când se specifică explicit domeniul) sau srcdom_regex, dstdom_regex pentru a căuta un domeniu al cărui nume conține şirul de caractere existent în comandă. Se poate căuta şi în URL, cu parametrii url_regex sau urlpath_regex, cu diferența că primul caută şirul de caractere în întreg URL-ul pe când cel de-al doilea îl caută doar în secțiunea ce nu conține protocolul sau numele de host. Aceste căutari sunt key-sensitive, lucru ce trebuie luat în calcul.

Accesul poate fi controlat şi prin adresa portului serverului destinație, cu parametrul port. Sintaxa este acl port <numar_port>. De asemenea se pot lua în calcul şi protocolul de transfer utilizat prin parametrul proto (urmat de tipul de protocol, de exemplu HTTP, FTP), sau metoda prin care se formulează cerința prin opțiunea method (urmată de tipul metodei, de exemplu GET, POST). Se poate configura astfel încât să verifice browserul de la care vin cerințele (prin opțiunea browser), de exemplu comanda acl browser MOZILLA se va referi la cerințele ce vin de la browserele ce conțin MOZILLA în antet.

Prin parametrul ident se pot forma liste bazate pe identitatea utilizatorilor, prin combinarea cu alte comenzi, de exemplu prin comanda acl friends ident dan adi gigi nicu combinată cu http_access allow friends şi urmată de http_ access deny all. Ca şi în cazurile anterioare există parametrul ident_regex ce face o căutare (după grupul de caractere specificat) în setul de nume al utilizatorilor.

Setul de parametri proxy_auth şi proxy_auth_regex asigură autentificarea utilizatorilor via procese externe. Aceşti parametri necesită un program extern de autentificare să verifice combinațiile <nume_utilizator> + <parola>.

Comanda http_access garantează sau neagă accesul HTTP bazându-se pe listele de acces definite. Sintaxa este http_access , unde parametrul poate fi allow (aprobă accesul) sau deny (neagă accesul), de exemplu http_access allow manager localhost. Este foarte important ca ultima linie a unui set de comenzi http_access să fie deny all, deoarece după stabilirea regulilor de acces, dacă acesta nu e negat atunci este garantat, deci specificați cât mai multe reguli de acces (funcție de ce aveți nevoie) iar la sfârşit nu uitați linia http_access deny all. Fără această ultima linie accesul va fi stabilit de varianta implicită, care este allow. După acelaşi sistem lucrează şi comanda icp_access, cu aceeaşi parametri, allow sau deny, comanda referindu-se la ICP. Comanda miss_access forțează cache-urile vecine vizate să devină cache de acelaşi nivel şi nu părinți, folosind aceiaşi parametri. De exemplu miss_access allow clientlocal înseamnă că doar grupul specificat are voie să primească mesaje MISS, ceilalți clienți pot primi doar HIT-uri. Valoarea implicită este miss_access allow all.

Se mai poate seta cache_peer_access, comandă similară cu cache_peer_domain, dar ce oferă mai multă flexibilitate folosind elementele acl. Mai există ident_lookup_access, tot cu opțiunile de allow sau deny, comandă ce conține o lista de elemente acl şi prin care puteți, de exemplu, să recurgeți la secvențe de identificare pentru cerințele ce aparțin stațiilor folosite de mai mulți utilizatori Unix, dar nu pentru celelalte stații. Implicit nu se recurge la secvențe de identificare pentru nici o cerință. De asemenea se poate garanta sau restricționa accesul ținând cont de dată şi oră.

Setarea parametrilor administrativi

Primul dintre aceşti parametri este cache_mgr <persoana>, el poate fi configurat în scopul setării persoanei care va primi mesaj în cazul „căderii" cache-ului. Valoarea implicită a câmpului <persoana> este webmaster.

Prin comenzile cache_effective_user <utilizator> şi cache_effective_group <grup> se pot seta numele utilizatorului sau grupului în cazul în care cache-ul rulează ca root. Valoarea implicită a parametrului din expresie este nobody. În cazul în care cache-ul nu rulează ca root se pastrează numele curent de utilizator. De asemenea de notat că, dacă nu se rulează ca root, nu puteți seta pentru http_port o valoare mai mică decât 1024.

Dacă vreți să precizați un nume special de host în mesajele de eroare, definiți visible_hostname . Altfel valoarea implicită este cea returnată de gethostname (). Acest lucru este important în cazul în care aveți mai multe cache-uri şi primiți erori în legătură cu IP-forwarding. Dacă doriți să aveți mai multe stații cu acelaşi nume vizibil de host, trebuie să setați pentru fiecare un nume unic diferit prin unique_hostname , pentru a se putea detecta buclele la forwarding.

Unele servere cache pot funcționa ca servere Web şi viceversa. Acestea acceptă cerințele în ambele formate, în formatul Web standard, unde se dau doar calea şi fişierul dorit, şi în formatul proxy specific, unde este necesar întregul URL. Proiectanții Squid-ului au decis să nu îl lase să funcționeze în acest fel, pentru a reduce numărul de probleme ce pot apărea şi a scădea complexitatea codului. Totuşi, dacă se adaugă un layer de translație în Squid, se pot accepta şi înțelege cerințele de tip Web, deoarece formatul este în esență acelaşi. Layer-ul adițional rescrie cerințele Web, prin schimbarea serverului şi portului destinație. Această cerință rescrisă este apoi tratată ca una normală, serverul destinație e contactat iar datele sunt scrise în cache. Acest lucru dă Squid-ului o alura de Web server. Lucrul este necesar pentru caching transparent, Squid poate fi configurat să intercepteze cerințele Web cu scopul de a aduce datele cerute în

cache, lucru ce nu se poate face fără „traducerea” din format Web în format cache. Comanda httpd_accel_host <IPAdress>|virtual setează numele de host pentru serverul „accelerat”, în cazul în care dați adresa de IP a acestuia, iar dacă doriți să realizați o procedura de caching transparent al traficului, trebuie să folosiți opțiunea „virtual” în locul adresei IP. Foarte important, în momentul în care recurgeți la httpd_accel_host, se dezactivează proxy-caching-ul şi ICP-ul, dar dacă vreți în continuare să beneficiați de aceste opțiuni, setați httpd_accel_with_ proxy normal on. Setarea portului se face cu httpd_accel_port <portnumber>. Cerințele „accelerate” pot fi transmise doar către un port, nu există o tabelă ce asociază host-urile accelerate cu un port destinație, deci acesta trebuie specificat. Nu există valoare predefinită pentru numărul portului, acesta trebuie să corespundă cu cel din squid.conf în cazul în care preluați informațiile de pe stația locală, iar dacă vreți să le transmiteți către un set de servere din background în cele mai multe cazuri folosiți portul 80, portul implicit pentru Web. Pentru suportul de port virtual setați numărul portului pe 0. Dacă aveți un singur server în background spre care doriți să transmiteți informația, setați httpd_accel_single_host pe on, dacă aveți mai multe astfel de servere, lăsați pe default (off) şi folosiți o unealtă de redirecționare pentru a mapa cerințele către serverele de rigoare.

O cerința HTTP include un antet de host, care este de fapt numele de host ce apare în URL. Squid poate fi un accelerator pentru servere HTTP diferite folosindu-se de acest antet, dar Squid nu verifică valoarea antetului de host şi astfel se deschide o importantă gaură în securitate. Este recomandat să nu folosiți httpd_ accel_uses_host_header decât dacă sunteți foarte în temă cu ceea ce faceți. Din păcate sunteți obligați să activați această opțiune dacă doriți să rulați Squid ca proxy transparent, altfel serverele virtuale ce au nevoie de antetul de host nu vor fi cache-uite eficient.

Ar mai fi multe de spus, există multe alte opțiuni de configurare, pentru suportul de programe externe, pentru modul în care obiectele sunt păstrate sau eliminate din cache, se pot stabili timpii de aşteptare pentru efectuarea anumitor operațiuni (de genul conectare, identificare, citire a datelor etc.), şi de asemenea o secțiune foarte importantă se ocupă de configurarea fişierelor în care sunt tipărite activitățile de rutină, erorile ce apar în rețea (aşa numitele fişiere log sau simplu log-uri). Informațiile din aceste fişiere reprezintă cea mai importantă sursă pentru un administrator, cu ajutorul datelor existente acolo se pot remedia problemele apărute şi se poate face rețeaua „sa meargă” în parametrii doriți.

Chestiunea cea mai importantă în alegerea şi configurarea unui proxy este modul în care doriți ca acesta să se integreze în rețeaua dumneavoastră. Înainte de a alege şi instala un firewall şi un proxy trebuie să stabiliți şi să creați o balanță între necesitățile de securitate şi performanțele dorite ale rețelei, precum şi gradul de instruire al utilizatorilor. În ultimii ani numărul de atacuri pe Internet a crescut îngrijorător, dar trebuie luată în calcul şi natura „liber pentru toata lumea” a Internetului, care a ajuns ce este azi tocmai din această cauză, deci „fragmentarea” lui cu o pleiadă de algoritmi de autentificare, parole şi chei, firewall-uri şi alte elemente de acest gen îi limitează oarecum orizontul şi nu este întotdeauna cea mai potrivită soluție.

5.4 Desfăşurarea lucrării

Serverul Squid este derivat din proiectul **Harvest** început de ARPA, fiind dezvoltat în continuare de National Laboratory for Applied Network Research. Suportă protocoalele http, https, ftp şi gopher.

Squid ne poate ajuta să limităm utilizarea bandwidth-ului disponibil, pentru a reduce cheltuielile sau a nu supraîncărca rețeaua.

Acest lucru e posibil datorita faptului că:

- păstrarea paginilor web, imaginilor şi altor tipuri de fişiere pe hard-disk. În caz că cineva se adresează la una şi aceeaşi pagină - ea nu va mai fi accesată de pe internet, ci luată din cash. Cu ajutorul acestei funcții poate fi economisită în mediu 30% din bandă (depinde şi de site-urile vizitate, şi de alți parametri).
- în afară de aceasta putem folosi funcția **delay pool** pentru a limita accesul către unele site-uri (de exemplu care conțin în url cuvântul porno) sau interzice download-ul unor anumite tipuri de fişiere.

Downloadăm sursele de pe site-ul oficial - **www.squid-cache.org**

1.Instalare –

```
tar -xjvf squid-2.5.STABLE3.tar.bz2
cd squid-2.5.STABLE3
CC="gcc" \
CFLAGS="-O3 -march=i686 -funroll-loops -fomit-frame-pointer" \
./configure \
--prefix=/usr \
--exec-prefix=/usr \
--bindir=/usr/sbin \
--libexecdir=/usr/lib/squid \
--sysconfdir=/etc/squid \
--enable-delay-pools \
--enable-cache-digests \
--enable-poll \
--disable-ident-lookups \
--enable-truncate \
--enable-xmalloc-statistics \
--enable-linux-netfilter \
--enable-stacktraces && make all && make install
```

2. Pentru a creşte performanța squid, e nevoie de o partiție, sau dacă nu e posibil - cream un director cache.

```
mkdir /cache
```

Cel mai potrivit ar fi alocarea squid-ului un hard disk SCSI.

Adăugăm userul squid şi grupul squid, fără shell (pentru a nu rula proxy serverul ca root)

```
groupadd squid
useradd -d /cache -s /sbin/nologin -g squid squid
chown -R squid:squid /cache
```

Cream directorul /var/log/squid , cu proprietarul – squid

```
mkdir /var/log/squid
chown squid:squid /var/log/squid
```

3. Configurare:

În continuare voi prezenta structura minima a fişierului **/etc/squid/squid.conf**

```
########################################################
# Portul şi adresa ip pe care va aştepta conexiuni squid
http_port 192.168.1.1:8080
# Directorul în care se va află cache-ul şi dimensiunea lui în Mb
#(în cazul de mai jos - 6000 mb)
cache_dir ufs /cache 6000 16 256
# Userul şi grupul sub care va rula serverul squid
cache_effective_user squid
cache_effective_group squid
#Portul pe care squid va trimite şi primi cereri către cache a altor proxy servere vecine
#Dacă nu mai avem alte proxy, specificăm 0
icp_port 0
# Cream acl-urile (acess control list):
acl all src 0.0.0.0/0.0.0.0
acl localhost src 127.0.0.1/8
acl lan src 192.168.1.0/24
#clienții proxy serverului nostru
#Paginile ce se creează dinamic vor fi accesate direct de la sursă
hierarchy_stoplist cgi-bin php asp ?
# Obiectele create dinamic nu vor fi salvate în cache
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
# Permitem accesul de la maşina locală (dacă este cazul)
http_access allow localhost
# Permitem calculatoarelor din rețeaua locala să utilizeze proxy serverul
http_access allow lan
# Interzicem celorlalți să acceseze squid-ul
http_access deny all
# Specificăm unde squid va păstra logurile
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
# Pidul procesului
pid_filename /var/run/squid.pid
########################################################
```

Aceasta este configurația minimă pentru ca squid să ruleze. Inițializăm cache-ul prin comanda:

squid -f /etc/squid/squid.conf –z

Dacă primiți un mesaj de tipul:

2003/08/11 20:30:28| aclParseIpData: WARNING: Netmask masks away part of the specified IP in '127.0.0.1/8'

nu va speriați , nu este o eroare, ci o avertizare.

Prima dată pornim squid-ul cu comanda:

squid -NDCd1

pentru a vedea eventualele mesaje de eroare. Dacă totul e ok - avem mesajul:

2003/08/11 20:30:29| Ready to serve requests.

Squid este gata pentru a accepta conexiuni.

Adăugam în scripturile de inițiere şi oprire a sistemului ca squid să pornească , respectiv să oprească la startul şi oprirea calculatorului. Şi să nu uităm să închidem portul 8080 pentru conexiuni dinafară cu ajutorul firewall-ului, şi să-l lăsăm deschis pentru clienții din rețea.

6 Open VPN

6.1 Obiective:

- înțelegerea şi familiarizarea cu noțiunea de rețea virtuală privată;
- familiarizarea cu noțiunea de tunnel între două sisteme pe Internet;
- instalarea şi configurarea OpenVPN

6.2 introducere în OpenVPN

OpenVPN este o soluție open-source pentru rețele virtuale private, bazată pe standardul SSL. Poate funcționa în regim de server ce acceptă conexiuni multiple sau în regim direct între doi clienți. Implementat la nivelul 2 şi 3 OSI, OpenVPN utilizează pentru autentificare şi criptare protocolul SSL/TLS (SSL = *Secure Sockets Layer*), prin intermediul bibliotecilor OpenSSL şi acceptă diferite metode de autentificare bazate pe certificate, smart-card, chei unice şi alte metode. Legătura tip tunel ce încapsulează traficul IP între două subrețele sau adaptoare Ethernet se realizează prin intermediul unui singur port, fie folosind protocolul TCP/IP fie UDP. Aplicația suportă tunele între adrese IP dinamice, traversarea NAT şi Ethernet bridging.

Unul din marile avantaje ale acestui program este uşurința configurării atât la nivel de client cât şi la nivel de server, depăşind din acest punct de vedere implementările IPSec din Linux şi Windows.

Un alt avantaj este portabilitatea, fiind asigurat suportul pentru următoarele platforme: Linux, Windows 2000/XP, OpenBSD, FreeBSD, NetBSD, Mac OS X şi Solaris. Implementările VPN folosind ca nivel de autentificare SSL/TLS au devenit din ce în ce mai populare recent, iar OpenVPN este una din cele mai bune soluții din acest domeniu.

Printre dezavantajele acestei aplicații se numără un overhead relativ mare determinat de folosirea SSL, o implementare mai puțin ergonomică sub sistemul de operare Windows şi o oarecare instabilitate în condițiile folosirii pe conexiuni nesigure, cu timpi de latență mari, anumite probleme fiind observate în special pe conexiuni wireless la distanță mare.

Aplicația este dezvoltată în regim open-source, putând fi folosită sub licența GPL[1] sau sub licență comercială în cazul în care se doreşte încorporarea ei în alte produse care nu sunt distribuite tot sub licență GPL sau o licență compatibilă.

6.3 Aplicație experimentală

Studenții vor realiza rețeaua din figura 1, vor instala OpenVPN şi vor configura un tunel între un server VPN şi un Client VPN urmând paşii descrişi în continuare.

Unul dintre sisteme va fi configurat cu rol de server, celalalt cu rol de client. Primul lucru pe care trebuie sa il facem este sa descarcam OpenVPN-Windows Installer de la adresa http://openvpn.net/release/openvpn-2.0.9-install.exe si sa il instalam pe cele doua sisteme in directorul C:\Program Files\OpenVPN.

[1] GPL – General Public Licence – Licență Publică Generală

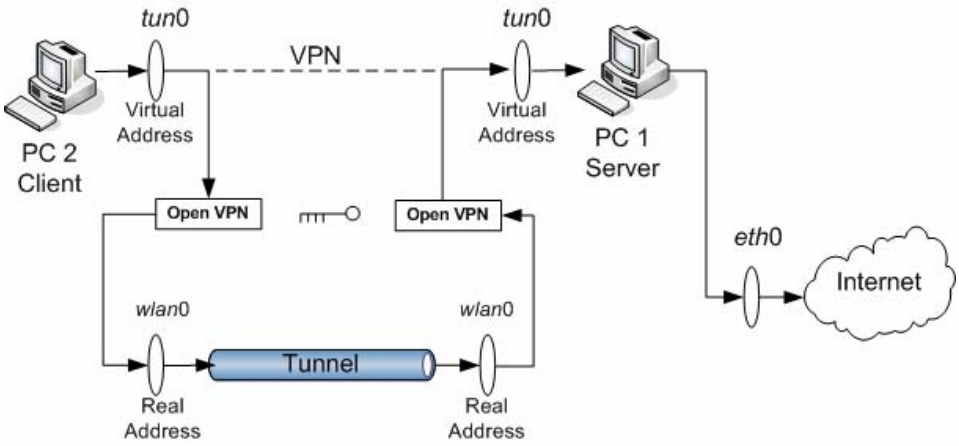


Fig.1: Virtual Private Network rulează printr-un tunel, iar end-point-urile acestuia sunt adresele IP reale ale Clientului PC2 şi Serverului PC1

6.3.1 Pe sistemul server

mergem în Start -> Run , scriem CMD şi dăm enter. În fereastra care se deschide tastăm:

cd C:\Program Files\OpenVPN\easy-rsa
copy vars.bat.sample vars.bat

Editam apoi vars.bat cu comanda edit vars.bat şi modificăm parametrii după nevoile noastre.

Să presupunem că avem în **vars.bat** următoarele:

```
@echo off
set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl.cnf
set KEY_DIR=keys
set KEY_SIZE=1024
set KEY_COUNTRY=RO
set KEY_PROVINCE=RO
set KEY_CITY=Bacau
set KEY_ORG=SorinPopa
set KEY_EMAIL=sorinpopa@ub.ro
```

Copiem fişierul **openssl.cnf.sample** în **openssl.cnf** cu comanda:
copy openssl.cnf.sample openssl.cnf
Rulăm următoarele comenzi:

```
vars
clean-all
build-ca
```

Urmează generarea certificatului şi a unei chei private pentru server:
build-key-server server

Generăm certificatele şi cheia pentru client:
build-key client

Este important ca Common Name pentru client să fie diferit de Common Name pentru server.

Generăm parametrii Diffie Hellman :

build-dh

În directorul C:\Program Files\OpenVPN\config facem un fişier **server.ovpn** în care scriem:

```
mode server
port 1194
proto udp
dev tun
ca "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\server.crt"
key "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\server.key"
dh "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\dh1024.pem"
tls-server
ifconfig 10.8.0.1 10.8.0.2
ifconfig-pool 10.8.0.3 10.8.0.5 # IP range clients
ifconfig-pool-persist ipp.txt
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
mute 20
```

Putem să pornim OpenVPN cu această configurație dacă dăm click dreapta din explorer pe fişierul **server.ovpn** şi alegem opțiunea **Start OpenVPN on this config file** sau îl putem porni ca şi serviciu din **Start -> Control Panel -> Administrativ Tools -> Serices -> OpenVPN Service** unde dăm start sau putem seta pe Automatic la Startup Type pentru a fi pornit odată cu sistemul de operare.

6.3.2 Pe sistemul client

trebuie să mergem în directorul

C:\Program Files\OpenVPN\easy-rsa şi să cream directorul **keys** în care copiem de pe server fişierele:

```
ca.crt
client.crt
client.key
```

În directorul **C:\Program Files\OpenVPN\config** facem un fişier **client.ovpn** în care scriem:

```
client
dev tun
```

```
proto udp
remote xxx.yyyy.zzzz.vvvv 1194 #se înlocuieşte xxx.yyy.zzz.vvv cu ip server
resolv-retry infinite
nobind
persist-key
persist-tun ca "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\ca.crt"
cert "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\client.crt"
key "C:\\Program Files\\OpenVPN\\easy-rsa\\keys\\client.key"
comp-lzo .
verb 3
```

Putem să pornim **OpenVPN** cu această configurație dacă dăm click dreapta din explorer pe fişierul **client.ovpn** şi alegem opțiunea **Start OpenVPN on this config file** sau îl putem porni ca şi serviciu din **Start -> Control Panel -> Administrativ Tools -> Serices -> OpenVPN Service** unde dăm start sau putem seta pe Automatic la Startup Type pentru a fi pornit o dată cu sistemul de operare

După ce am pornit atât serverul cât şi clientul (fără a avea un mesaj de eroare) putem să verificăm funcționalitatea tunelului creat.

Astfel, pe server mergem în Start - Run şi tastam CMD. În fereastra deschisă introducem comanda:

ipconfig

Vom obține mai multe informații printre care vom regăsi şi cele din imaginea de mai jos:

```
   Connection-specific DNS Suffix  . :
   IP Address. . . . . . . . . . . . : 10.8.0.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.252
   Default Gateway . . . . . . . . . :
```

Pe sistemul configurat ca şi client la comanda **ipconfig** obținem informații printre care trebuie să se regăsească și următoarele:

```
  Connection-specific DNS Suffix  . :
  IP Address. . . . . . . . . . . . : 10.8.0.2
  Subnet Mask . . . . . . . . . . . : 255.255.255.252
  Default Gateway . . . . . . . . . :
```

Conexiunea între cele două sisteme o putem verifica cu utilitarul **ping**. Atenție la configurarea firewall-ului pentru a permite ICMP Echo Request şi ICMP Echo Replay atât pe sistemul server cât şi client.

De pe sistemul configurat ca şi server, care are ip-ul 10.8.0.1 vom da ping în 10.8.0.2 (client)

```
C:\>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:

Reply from 10.8.0.2: bytes=32 time=6ms TTL=128
Reply from 10.8.0.2: bytes=32 time=3ms TTL=128
Reply from 10.8.0.2: bytes=32 time=3ms TTL=128
Reply from 10.8.0.2: bytes=32 time=6ms TTL=128

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 6ms, Average = 4ms
```

De pe sistemul configurat ca şi client, care are ip-ul 10.8.0.2 vom da ping în 10.8.0.1 (server):

```
C:\>ping 10.8.0.1

Pinging 10.8.0.1 with 32 bytes of data:

Reply from 10.8.0.1: bytes=32 time=3ms TTL=128
Reply from 10.8.0.1: bytes=32 time=7ms TTL=128
Reply from 10.8.0.1: bytes=32 time=6ms TTL=128
Reply from 10.8.0.1: bytes=32 time=7ms TTL=128

Ping statistics for 10.8.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 7ms, Average = 5ms
```

Bibliografie

1. Anderson R. – Security Engineering : A Guide to Building Dependable Distributed Systems, NY 2001;
2. Andress, M. – *Surviving Security: How to Integrate People, Process and Technology*, SAMS, Indianapolis, 2002, pp. 59-63.
3. Davis D. – "*The Problems Catch Up With The Solution*", in *Card Technology*, April 2003;
4. Denning D.E. – *Information Warfare and Security*, Addison-Wesley, Reading, Massachusetts, 1999;
5. King, C.M., Dalton, C.E., Osmanaglu, T.E. – *Security Arhitecture: Design, Deployment& Operations*,Osborne/McGraw-Hill, New York, 2001, pp. 18-26
6. Krutz R.L, Vines R.D. – *The CISSP Prep Guide – Mastering the Ten Domains of Computer Security*, Wiley & Sons, Inc. New York, 2001;
7. Schwartan W. – *Information Warfare*, 2nd Edition , Thunder's Mouth Press, New York, 1996;
8. Simmons G.J. – "The Prisoners' Problem and the Subliminal Channel", in Proceedings of Crypto '83, Plenum Press 1984;
9. Renesse R. – *Optical Document Security*, 2nd ed., Artech House, 1997;
10. Renesse R. – "Verifying versus Falsyfying Banknotes", in Optical Security and Counterfeit Deterrence Techniques II, (1998);
11. U.S. Department of Energy – "*Identification of Classfied Information*", Office of Clasification, December 1991;
12. Tuomas Aura, Pekka Nikander, Jussipekka Leiwo - *DoS-resistant Authentication with Client Puzzles.* Proceedings of the Cambridge Security Protocols Workshop 2000, LNCS, Cambridge, UK, April 2000, Springer-Verlag
13. G. B. Agnew, R. C. Mullin, S. A. Vanstone - *Improved Digital Signature Scheme based on Discrete Exponentiation*, Electronic Letters, Vol. 26, 1990
14. K. Alagappan - *SPXInstallation*, Digital Equipment Corporation, February 1991
15. K. Alagappan, J. Tardo - *SPX Guide - A Prototype Public Key Authentication Service*, Digital Equipment Corporation, February 1991
16. K. Alagappan - *Telnet authentication: SPX (RFC 1412)*, Digital Equipment Corporation, 1993
17. F. Bauspiess, H. J. Knobloch - *How to Keep Authenticity Alive in A Computer Network*, Proceedings of EUROCRYPT' 89, Springer-Verlag, Berlin, 1990
18. S. M. Bellovin, M. Merritt - *EncryptedKey Exchange: Password-Based Protocols Secure Against Dictionary Attacks*, Proceedings of the IEEE Symposium on Security and Privacy, IEEE Computer Society Press, Los Alamitos, CA, 1992
19. S. M. Bellovin, M. Merritt - *Augumented EncryptedKey Exchange*, Proceedings of the 1st ACM Conference on Communications and Computing Security, November 1993
20. Steven M. Bellovin, Michael Merritt - *Limitations of the Kerberos Authentication System*, AT&T Bell Labs

21. Th. Beth - *Efficient Zero-Knowledge Identification Scheme for Smart Cards*, Proceedings of EUROCRYPT '88, Springer-Verlag, Berlin, 1989
22. Th. Beth, H. J. Knobloch, M. Otten - *Verifiable Secret Sharingfor Monotone Access Structures,* Proceedings of the 1st ACM Conference on Communication and Computing Security, November 1993
23. Th. Beth, H. J. Knobloch, M. Otten, G. J. Simmons, P. Wichmann -*Towards Acceptable Key Escrow System,* Proceedings of the 2nd ACM Conference on Communication and Computing Security, November 1994
24. T. Beth, H. J. Knobloch, S. Stempel, P. Wichmann -*Authentifikationsdienst SELANE - Modularisierung und Einsatz,* Report 94/3, Univeristy of Karlsruhe, EISS, 1994
25. Leitner Achim, "Rețele WLAN sigure, cu un tunel OpenVPN criptat", Linux Magazin, nr. 22, iunie 2005;
26. OpenVPN: *http:// openvpn. sourceforge. Net*
27. Biblioteca LZO: *http:// www. oberhumer. com/opensource/ lzo/*
28. Proiect OpenSSL: *http:// www. openssl. org/*
29. Driver TUN/ TAP: *http:// vtun. sourceforge. net/ tun/*
30. Thomas T., *Primii paşi în securitatea reţelelor*, Corint, Bucureşti, 2005.
31. www.squid-cache.org
32. http://www.wingate.com/download.php
33. http://www.youngzsoft.net/ccproxy/
34. http://www.securekit.com/
35. www.digimarc.com
36. www.digimarc-id.com
37. www.aris-techni.fr/

Cuprins

Aplicații practice