LUMINIȚA SCRIPCARIU
ION BOGDAN
ȘTEFAN VICTOR NICOLAESCU
CRISTINA GABRIELA GHEORGHE
LIANA NICOLAESCU

SECURITATEA REȚELELOR DE COMUNICAȚII

CASA DE EDITURĂ „VENUS” IAȘI 2008

CUPRINS

CUVÂNT ÎNAINTE

Rețelele de comunicații reprezintă o realitate cotidiană pentru fiecare dintre noi indiferent de vârstă, în toate domeniile de activitate (comercial, financiar-bancar, administrativ, educațional, medical, militar etc.), dar şi în mediul familial.

Fără a depinde de mediul fizic prin care se realizează (cablu metalic, fibră optică sau mediul wireless) sau de specificul rețelei de transmisie a informațiilor (de calculatoare, de telefonie fixă sau mobilă, de televiziune prin cablu, de distribuție a energiei electrice), securitatea comunicațiilor reprezintă un aspect esențial al serviciilor oferite, fiind critică în cazul informațiilor cu caracter secret din aplicații fianciar-bancare, militare, guvernamentale şi nu numai acestea.

“Cine? Când? De unde? Ce? De ce?” acestea sunt întrebările esențiale referitoare la securitatea comunicațiilor, care determină împreună o nouă sintagmă, “a celor cinci W” (5W – Who, When, Where, What, Why?). Cine accesează rețeaua? Când şi de unde se produce accesul? Ce informații sunt accesate şi de ce? Aceste aspecte trebuie să fie monitorizate şi securizate în funcție de importanța informațiilor, de caracterul public sau privat al rețelei de comunicații, indiferent de terminalul folosit (calculator, laptop, telefon mobil, PDA, iPOD, bancomat etc.).

Conexiunea la Internet reprezintă o facilitate dar creează de cele mai multe ori mari probleme de securitate pentru rețelele de comunicații.

Scopul serviciilor de securitate în domeniul rețelelor de comunicații vizează pe de o parte menținerea acestora în funcțiune (regula celor cinci de 9 adică 99,999 % din durata de funcționare), iar pe de altă parte asigurarea

securității aplicațiilor precum şi a informațiilor stocate pe suport sau transmise prin rețea.

Se identifică mai multe aspecte ale securității unei rețele (securizarea accesului fizic şi logic, securitatea serviciilor de rețea, secretizarea informațiilor) care se exprimă prin diverşi termeni specifici: autentificare, autorizare, asociere cu un cont de utilizator şi audit (AAAA – *Authentication, Authorization, Accounting, Auditing*), confidențialitate, robustețe.

Politica de securitate este cea care, pe baza analizei de securitate a unei rețele, exprimă cel mai bine principiile care stau la baza adoptării unei anumite strategii de securitate, implementată prin diverse măsuri specifice, cu tehnici şi protocoale adecvate.

Scopul acestei cărți este acela de a trece în revistă toate aceste aspecte, de a analiza riscuri şi vulnerabilități specifice diferitelor rețele de comunicații, precum şi o serie de soluții şi strategii, tehnici şi protocoale de securitate.

AUTORII

Capitolul I INTRODUCERE

I.1 NOŢIUNI GENERALE DESPRE REŢELELE DE COMUNICAŢII

O ***reţea de comunicaţii*** reprezintă un ansamblu de echipamente de comunicaţii (calculatoare, laptopuri, telefoane, PDA-uri etc.), interconectate prin intermediul unor medii fizice de transmisie (cablu torsadat, coaxial sau optic, linie telefonică, ghid de unde, mediul wireless), în scopul comunicării folosind semnale vocale, video sau de date, precum şi al utilizării în comun a resurselor fizice (hardware), logice (software) şi informaţionale ale reţelei, de către un număr mare de utilizatori.

Se disting diverse tipuri de reţele de comunicaţii (reţele de telefonie fixă, reţele telefonice celulare, reţele de cablu TV, reţele de calculatoare ş.a.) prin intermediul cărora se transmit informaţii sau se comunică în timp real.

Calculatoarele personale interconectate în reţele au oferit un nivel superior de performanţă în stocarea, procesarea şi transmisia informaţiilor. Ansamblul tuturor calculatoarelor interconectate între ele în cea mai largă reţea de calculatoare din lume reprezintă aşa-numitul INTERNET (INTERnational NETwork).

Conexiuni la Internet se pot realiza în prezent nu numai prin intermediul calculatoarelor, dar şi de pe alte echipamente precum telefoane mobile sau PDA-uri.

Terminalele din rețea pot fi fixe sau mobile, astfel că accesul la Internet se poate face în prezent şi din vehicule în mişcare, pe baza unor standarde definite pentru Internetul mobil.

Comunicațiile între echipamentele interconectate fizic şi logic într-o rețea se realizează pe baza protocoalelor de comunicații.

Prin **protocol** se înțelege o suită de reguli de comunicare şi formate impuse pentru reprezentarea şi transferul datelor între două sau mai multe calculatoare sau echipamente de comunicație.

Se folosesc numeroase suite de protocoale dar scopul oricărei rețele de comunicații este acela de a permite transmisia informațiilor între oricare două echipamente, indiferent de producător, de sistemul de operare folosit sau de suita de protocoale aleasă, pe principiul sistemelor deschise (*open system*).

Echipamentele de interconectare (modem, hub, switch, bridge, router, access point) sunt responsabile de transferul informațiilor în unități de date specifice (cadre, pachete, datagrame, segmente, celule) şi de conversiile de format ce se impun, precum şi de asigurarea securității comunicațiilor.

Probleme specifice de securitate se identifică atât în nodurile rețelei, precum şi pe căile de comunicație (cablu sau mediu wireless).

De asemenea, atunci când se ia în discuție securitatea comunicației, trebuie făcută distincția între procesele de comunicație în timp real care se realizează în cazul transmisiilor vocale sau video şi cele de transfer al informațiilor sub formă de fişiere. Apar riscuri mari de securitate în aplicațiile de tip „peer-to-peer” (p2p), precum Skype, în care se desfăşoară procese de comunicație în timp real, dar şi atacuri la securitatea rețelei în paralel cu acestea.

Serviciul de transfer al fişierelor este mai puțin critic din punct de vedere al timpului de rulare, ceea ce permite efectuarea unor teste de asigurare a securității sistemului.

Pentru o analiză completă a securității trebuie avute în vedere toate aspectele referitoare la o rețea de comunicații, interne şi externe, hardware şi software, factorul uman şi de tip automat, tipurile de rețea, topologiile şi mediile de transmisie, protocoalele de comunicații, aplicațiile rulate, riscurile de securitate şi, nu în ultimul rând, costurile.

Vulnerabilitățile rețelelor de comunicații şi ale sistemelor informatice actuale pot antrena pierderi uriaşe de ordin financiar şi nu numai, direct sau indirect, cum ar fi scurgerea de informații confidențiale cu caracter personal, militar sau economic.

I.2 TIPURI DE REȚELE DE COMUNICAȚII

Rețelele de comunicații se clasifică în primul rând în funcție de aplicabilitatea lor:

- De calculatoare
- Telefonice
- De comunicații mobile
- De radio şi teledifuziune
- De televiziune prin cablu
- De comunicații prin satelit.

Întrucât în continuare ne vom referi la securitatea comunicațiilor şi în deosebi a datelor transmise prin Internet, în continuare vom prezenta în

detaliu rețelele de calculatoare şi vom face referire, acolo unde este cazul, la modalitățile de utilizare a celorlalte tipuri de rețele pentru transmisii de date.

Un criteriu de clasificare a rețelelor de calculatoare este mărimea lor (Tabelul I.1):

1. rețele locale (LAN – *Local Area Network*);
2. rețele metropolitane (MAN – *Metropolitan Area Network*);
3. rețele de arie largă (WAN – *Wide Area Network*).

În cadul rețelelor locale sau de arie largă se disting şi unele subtipuri, definite de comunicațiile wireless prin unde radio, în funcție de tehnologia folosită, puterea de emisie şi aria de acoperire:

4. rețele personale (PAN –*Personal Area Network*) numite şi *piconet*, asociate tehnicii Bluetooth (BTH).
5. rețele locale wireless (WLAN – *Wireless Local Area Network*) asociate în general comunicațiilor în standard IEEE 802.11, denumite şi rețele WiFi.
6. rețele wireless de arie largă (WWAN – Wireless Wide Area Network) create pe baza tehnologiilor de arie largă (ATM – *Asynghronous Transfer Mode*, WiMax – *Worldwide Interoperability for Microwave Access* ş.a.).

Tabelul I.1

Clasificarea rețelelor de calculatoare

Ordin de mărime	Arie de acoperire	**Tipul rețelei**
1m	mică	**PAN**
10-100-1000 m	Cameră, Clădire, Campus	**LAN, WLAN**
10 Km	Oraş	**MAN, WMAN**
100-1000 Km	Țară, Continent	**WAN, WWAN**
10.000 Km	Planetă	**Internet**

Un alt criteriu de clasificare a rețelelor este cel al modului de transmisie:

- **rețele cu difuzare** către toate nodurile terminale, utilizate în general pentru arii mici de acoperire;
- **rețele punct-la-punct** cu conexiuni fizice între oricare două noduri, fără risc de coliziune a pachetelor.

Modelarea unei rețele de calculatoare se poate face pe baza teoriei grafurilor. Echipamentele terminale sau cele de comunicație sunt reprezentate ca noduri iar fiecare conexiune fizică existență între două noduri apare ca arc în graf.

Într-o rețea locală sunt interconectate mai multe calculatoare-gazdă (*host*) şi unul sau mai multe servere. De asemenea, în rețea pot fi incluse şi alte echipamente terminale (imprimante, scannere, maşini de tip xerox etc.) pe care utilizatorii le folosesc în mod partajat.

În rețelele metropolitane şi cele de arie largă un rol deosebit îl are rețeaua de transport formată din routere şi alte echipamente de dirijare a

pachetelor de date (switch cu management, bridge, access point) între diverse rețele locale.

Din punct de vedere al configurării, specificul unei rețele de arie largă este total diferit de cel al unei rețele locale. Într-o rețea locală se configurează plăcile de rețea din fiecare calculator sau alt echipament terminal conectat la rețea şi serverele locale, în timp ce într-o rețea de arie largă accentul cade pe partea de configurare a routerelor sau a altor echipamente de comunicații.

În particular, configurările pe partea de securitate sunt diferite.

Fiecare sistem de operare de pe echipamentele de tip client oferă facilități de securizare prin stabilirea grupurilor şi a drepturilor de utilizator, domenii de lucru etc.

Pe serverele din rețea se pot stabili diferite restricții referitoare la traficul intern şi extern.

Interfața de acces spre şi dinspre Internet este securizată de echipamentele de tip firewall.

Totuşi în LAN cele mai periculoase atacuri sunt cele interne iar efectele acestora pot fi minimizate prin stabilirea şi aplicarea unei politici de securitate adecvate şi a unor tehnici de securizare eficiente.

În WAN aspectele securității sunt diferite față de o rețea locală. Furnizorii de servicii de Internet sunt cei care administrează rețeaua de transport şi care aplică diferite politici şi măsuri de securitate. Responsabilitatea acestora este mult crescută deoarece numărul de utilizatori este foarte mare şi este dificil sau chiar imposibil să se administreze manual rețeaua. În acest caz se pot folosi diferite programe

sofware de securitate oferite de firme de profil, care monitorizează şi clasifică evenimentele din rețeaua de arie largă.

De exemplu, într-o rețea cu peste 100000 de echipamente terminale, numărul de evenimente înregistrate în decurs de o oră poate fi semnificativ, clasificarea acestora în funcție de natura lor şi pe mai multe nivele de gravitate permite identificarea unor atacuri cu risc sporit şi luarea măsurilor pentru obstrucționarea lor în timp util. Totul se poate face automat prin intermediul programelor software de securitate a rețelelor de comunicații.

I.3 MODELAREA REȚELELOR DE CALCULATOARE

I.3.1 MODELUL DE REȚEA ISO/OSI

Proiectarea, întreținerea şi administrarea rețelelor de comunicații se poate face mai eficient prin folosirea unui model de rețea stratificat. De asemenea, pe baza unui model stratificat se pot realiza modulele software necesare funcționării rețelei care implementează diferite funcții (codare, criptare, împachetare, fragmentare etc.).

Organizația Internațională de Standardizare ISO a propus pentru rețelele de calculatoare **modelul OSI** (*Open Systems Interconnection*) stratificat, cu şapte nivele (*Layers*) numerotate de jos în sus (Fig.I.2):

1. nivelul fizic (*Physical Layer*)
2. nivelul legăturii de date (*Data Link Layer*)
3. nivelul de rețea (*Network Layer*)

4. nivelul de transport (*Transport Layer*)
5. nivelul sesiune (*Session Layer*)
6. nivelul de prezentare (*Presentation Layer*)
7. nivelul de aplicație (*Application Layer*).

Acestor nivele li se asociază seturi de protocoale, denumite **protocoale OSI**.

Fiecare nivel are rolul de a ascunde nivelului superior detaliile de transmisie către nivelul inferior şi invers. Nivelele superioare beneficiază de serviciile oferite de cele inferioare în **mod transparent.** De exemplu, între nivelele-aplicație informația circulă fără erori (*error-free*), deşi apar erori de transmisie pe canalul de comunicație, la nivel fizic.

În figura I.2, calculatoarele A şi B sunt reprezentate pe baza modelului OSI. Transferul datelor de la A la B, respectiv de la B la A, se face pe traseele marcate cu linie continuă. Datele sunt transmise între echipamente prin legătura fizică.

Între nivelele similare ale terminalelor, comunicația se realizează pe baza unui protocol specific, denumit după numele nivelului. Cu excepția protocolului de la nivelul fizic, toate celelalte sunt asociate unor **comunicații virtuale** prin **legăturile virtuale** (*virtual path*) deoarece nu există o legătură reală între nivelele respective, datele transferându-se doar la nivel fizic, acolo unde are loc **comunicația reală (fizică)** dintre calculatoare, printr-un **circuit fizic**.

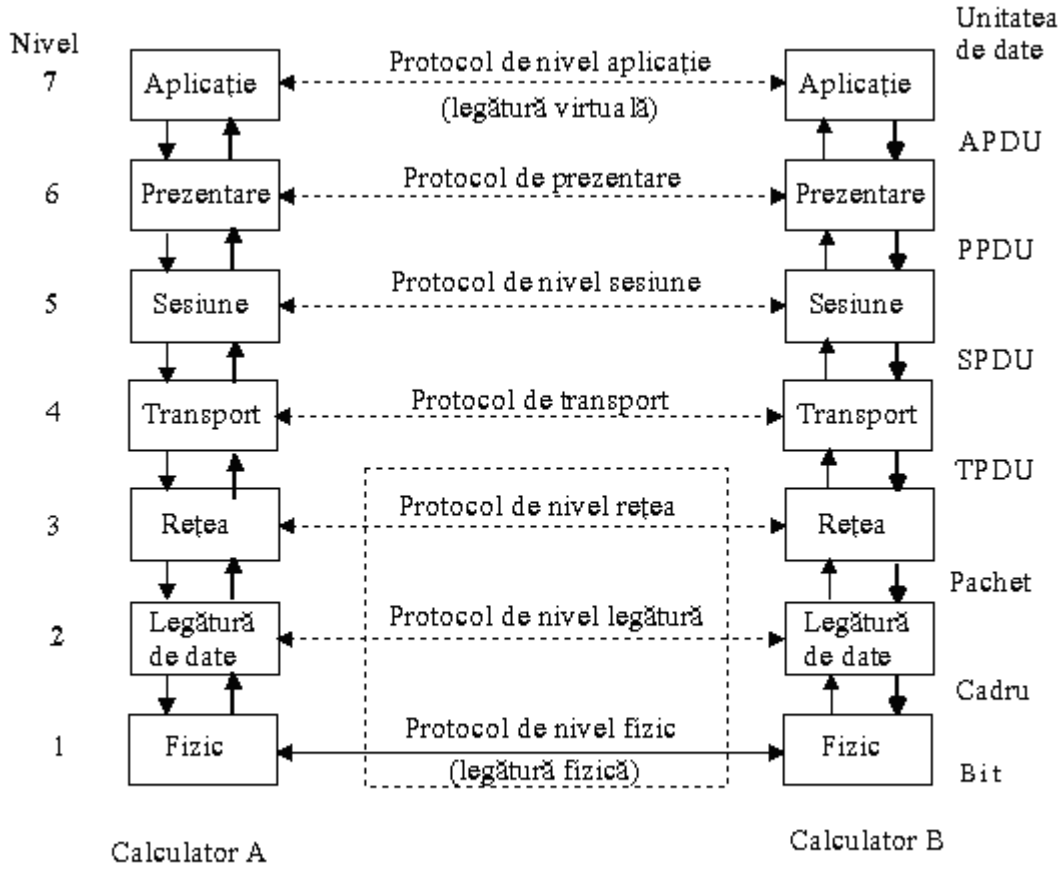

Fig. I.1 Modelul de rețea OSI și suita de protocoale OSI

Dacă cele două calculatoare nu aparţin aceleiaşi rețele, atunci protocoalele de pe nivelele inferioare (1, 2 şi 3) se aplică prin intermediul echipamentelor de comunicație (*switch, bridge, router* sau *gateway*), în **subrețeaua de comunicație** sau **de transport.**

Se observă că pe fiecare nivel se denumeşte altfel unitatea de date (DU - *Data Unit*).

Denumirea unității de date pe fiecare nivel al modelului OSI depinde de protocolul aplicat. În figura I.1, s-au folosit pentru nivelele superioare, termeni generici cum ar fi APDU (*Application Protocol Data Unit*), PPDU

(*Presentation Protocol DU*), SPDU (*Session Protocol DU*), TPDU (*Transport Protocol DU*) care vor căpăta denumiri specifice în funcție de suita de protocoale folosită într-o anumită rețea. De exemplu, în rețelele TCP/IP se folosesc termenii de **datagramă** sau **segment** pe nivelul de transport (*L4*)**.** Pe nivelul de rețea (*L3*) se foloseşte termenul consacrat de **pachet** (*packet*). Pe nivelul legăturii de date (*L2*) se transferă **cadre de date** (*frame*). La nivel fizic (*L1*) datele sunt transmise sub formă de **biți**.

La **nivel fizic**, se transmit datele în format binar (biți 0 şi 1) pe canalul de comunicație din rețea. În standardele echipamentelor care lucrează la nivel fizic, precum şi în cele ale interfețelor fizice aferente acestora, sunt specificate caracteristicile lor electrice, mecanice, funcționale şi procedurale. Natura sursei de informație (date, voce, audio, video) nu se mai cunoaşte la acest nivel ceea ce face ca procesul de comunicație să fie considerat transparent.

La **nivelul legăturii de date** circulă **cadre** de biți, adică pachete încapsulate cu antet (H - *header*) şi marcaj final (T - *trail*), care includ adresele sursei (SA - *Source Address*) şi destinației (DA - *Destination Address*) pentru a se putea expedia datele între calculatoare. Suplimentar, în cadrul de date sunt incluse: un câmp de control al erorilor, unul responsabil de sincronizarea transmisiei, un câmp de protocol etc.

În principal, nivelul legăturii de date este responsabil de detecția erorilor de transmisie a datelor prin rețea.

Pe nivelul OSI 2, se folosesc **coduri ciclice** (CRC - *Cyclic Redundancy Checking*) care au o capacitate mai mare de detecție a erorilor decât sumele de control. Pentru aplicații speciale se codifică datele în baza unei tehnici de codare pentru corecția erorilor de transmisie (Hamming,

Reed-Solomon etc.), ceea ce permite eliminarea retransmisiilor de cadre şi creşterea eficienței canalului de comunicație.

Nivelul legăturii de date este împărțit în două subnivele: LLC (*Logical Link Control*) şi MAC (*Media Access Control*) (Fig. I.2). Aceste subnivele stabilesc modalitățile de acces la mediu în cazul canalelor de comunicație cu acces multiplu şi realizează controlul traficului pentru a se evita efectele neadaptării ratelor de transmisie ale echipamentelor şi posibilitatea saturării lor (*flooding*).

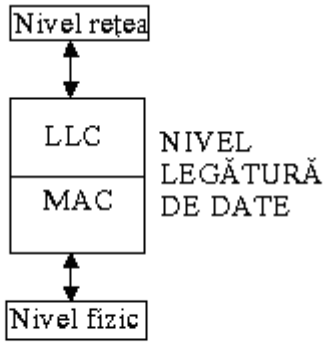

Fig. I.2 Subnivelele de nivel 2
și interconectarea cu nivelele adiacente din modelul OSI

Pe **nivelul de rețea**, se alege calea de expediere a pachetului, se realizează controlul traficului informațional din rețea şi dintre rețele, se rezolvă congestiile, eventual se converteşte formatul pachetului dintr-un protocol în altul. În unele LAN-uri, funcția nivelului de rețea se reduce la cea de stocare (*buffering*) şi retransmisie a pachetelor. În WAN-uri, la acest nivel se realizează operația de **rutare** a pachetelor, adică stabilirea căilor optime de transmisie între noduri. În Internet, se utilizează **sume de control** (*check sum*), calculate la emisie şi la recepție, prin sumarea pe verticală, modulo-2 bit cu bit în GF (*Galois Field*), a tuturor blocurilor de 16 biți din

câmpul datelor (RFC 1071). Aceste sume permit detecția erorilor simple, eventual a unor erori multiple, urmată de cererea de retransmisie a pachetului.

Nivelul de transport deplasează datele între aplicații. Acest nivel răspunde de siguranța transferului datelor de la sursă la destinație, controlul traficului, multiplexarea şi demultiplexarea fluxurilor, stabilirea şi anularea conexiunilor din rețea. De asemenea, la acest nivel mesajele de mari dimensiuni pot fi **fragmentate** în unități mai mici, cu lungime impusă, procesate şi transmise independent unul de altul. La destinație, acelaşi nivel răspunde de refacerea corectă a mesajului prin ordonarea fragmentelor indiferent de căile pe care au fost transmise şi de ordinea sosirii acestora.

Nivelul de sesiune furnizează diverse servicii între procesele-pereche din diferite noduri: transfer de fişiere, legături la distanță în sisteme cu acces multiplu, gestiunea jetonului (*token*) de acordare a permisiunii de a transmite date, sincronizarea sistemului etc. O sesiune începe doar dacă legătura între noduri este stabilită, deci este orientată pe conexiune. Nivelul sesiune este considerat ca fiind interfața dintre utilizator şi rețea.

Nivelul de prezentare se ocupă de respectarea sintaxei şi semanticei impuse de sistem, de codificarea datelor (compresie, criptare) şi reprezentarea lor în formatul standard acceptat, de exemplu, prin codarea ASCII (*American Standard Code for Information Interchange*) a caracterelor. În plus, acest nivel supervizează comunicațiile în rețea cu imprimantele, monitoarele, precum şi formatele în care se transferă fişierele.

La **nivelul aplicație** se implementează algoritmii software care convertesc mesajele în formatul acceptat de un anumit terminal de date real. Transmisia se realizează în formatul standard specific rețelei. Față de aceste

standarde de comunicație, DTE-ul real devine un **terminal virtual** care acceptă standarde de rețea specifice (de exemplu, VT100/ANSI).

Un program de aplicație pentru comunicații în rețea poate să ofere unul sau mai multe servicii de rețea, pe baza anumitor protocoale de transmisie.

Nivelele modelului OSI pot fi implementate fizic (*hardware*) sau logic (*software*). Evident nivelul fizic este implementat fizic (interfețe fizice, conectori de legătură). Nivelul legăturii de date poate fi implementat logic dar se preferă varianta fizică, aceasta asigurând viteze mari de procesare. Nivelele superioare sunt de obicei implementate logic, ca procese software, în cadrul sistemului de operare în rețea (NOS – *Network Operating System*), de cele mai multe ori inclus în sistemul de operare propriu-zis (OS – *Operating System*).

Echipamentele de comunicație din rețea se clasifică de asemenea pe baza modelului OSI.

Conectarea terminalului de date la mediul fizic de transmisie se realizează prin intermediul **interfeței fizice** cu caracteristicile specificate de nivelul fizic (de exemplu, Ethernet, RS - 232, RS - 485, E1, X.21, V.35).

Între nivelele superioare se intercalează interfețe implementate doar prin soft, denumite **interfețe logice**. De exemplu, în sistemele cu multiplexare în timp, cum ar fi sistemele de transmisie sincrone (SDH - *Synchronous Digital Hierarchy)*, un canal E1 cu 32 de canale primare trebuie partajat pentru asigurarea accesului multiplu. Utilizatorilor li se alocă anumite intervale de transmisie (*time slot*), pe baza protocolului de legătură punct-la-punct (PPP - *Point-to-Point Protocol*) prin interfețe logice *ppp.*

Echipamentele de comunicație din rețea de tip hub lucrează pe nivelul fizic.

Comutatoarele de rețea (*switch*) şi punțile de comunicație (*bridge*) sunt proiectate pe nivelul OSI 2, în timp ce routerele, configurate ca "gateway" sau "firewall", lucrează pe nivelul de rețea.

Modelul OSI este foarte general, pur teoretic, şi asigură o mare flexibilitate în cazul dezvoltării rețelelor prin separarea diverselor funcții ale sistemului pe nivele specifice. Numărul relativ mare de nivele din acest model face necesară utilizarea unui mare număr de interfețe şi a unui volum crescut de secvențe de control. De aceea, în numeroase cazuri se va folosi un număr redus de nivele. Modelul OSI nu constituie un standard, ci doar o referință pentru proiectanții şi utilizatorii de rețele de calculatoare.

I.3.2 MODELUL TCP/IP

Familia de protocoale în baza căreia se realizează comunicația în rețelele eterogene de calculatoare conectate la Internet este denumită **suita de protocoale Internet** sau TCP/IP (*Transmission Control Protocol/Internet Protocol*). De asemenea, termenul de **tehnologie Internet** semnifică suita de protocoale TCP/IP şi aplicațiile care folosesc aceste protocoale (RFC 1180).

Suita de protocoale TCP/IP gestionează toate datele care circulă prin Internet.

Modelul TCP/IP are patru nivele şi este diferit de modelul OSI (*Open System Interconnection*), dar se pot face echivalări între acestea (Fig.I.3).

Primul nivel TCP/IP de **acces la rețea** (*Network Access*) înglobează funcțiile nivelelor OSI 1 şi 2.

Al doilea nivel TCP/IP corespunde nivelului OSI 3 şi este denumit **nivel Internet** după numele principalului protocol care rulează pe acesta.

Al treilea nivel TCP/IP este cel **de transport,** echivalent ca nume şi funcționalitate cu nivelul OSI 4.

Nivelul aplicație din modelul TCP/IP include funcțiile nivelelor OSI superioare 5, 6 şi 7.

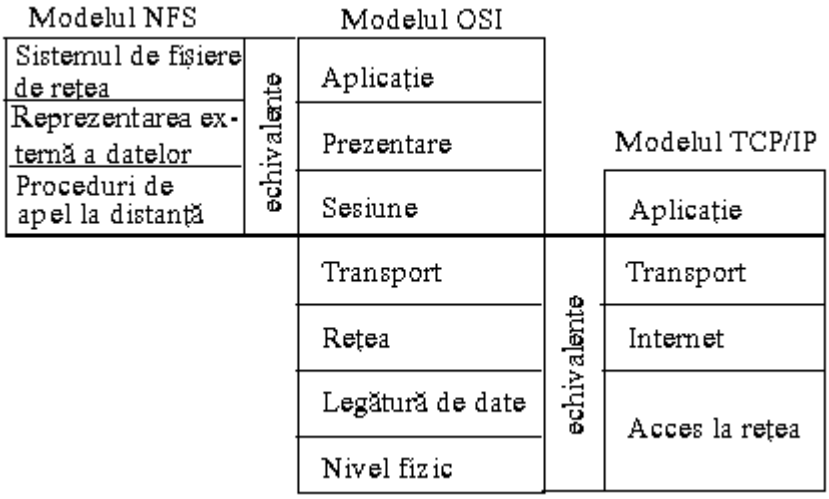

Figura I.3 Echivalențele între modelele de rețea OSI, TCP/IP şi NFS

Modelul TCP/IP şi modelul NFS (*Network File System*) alcătuiesc împreună aşa-numitul context de operare al rețelelor deschise (ONC - *Open Network Computing*).

Observație: În multe cazuri se consideră modelul de rețea TCP/IP ca având cinci nivele: fizic, legătură de date, Internet, transport şi aplicație. Acest lucru este motivat de faptul că cele două nivele inferioare au numeroase funcții care trebuie diferențiate, preferându-se discutarea lor pe nivele separate.

Suita de protocoale TCP/IP gestionează toate transferurile de date din Internet, care se realizează fie ca **flux de octeți** (*byte stream*), fie prin unități de date independente denumite **datagrame** (*datagram*).

Numele acestei suite de protocoale este dat de protocolul de rețea (IP) şi de cel de transport (TCP). Stiva de protocoale TCP/IP include mai multe protocoale deosebit de utile pentru furnizarea serviciilor Internet. Protocoalele de aplicație colaborează cu protocoalele de pe nivelele inferioare ale stivei TCP/IP pentru a transmite date prin Internet, mai precis pentru a oferi servicii utilizatorului (poştă electronică, transfer de fişiere, acces în rețea de la distanță, informații despre utilizatori etc).

Protocoalele din această familie sunt ierarhizate pe cele patru nivele ale modelului TCP/IP (Figura I.4):

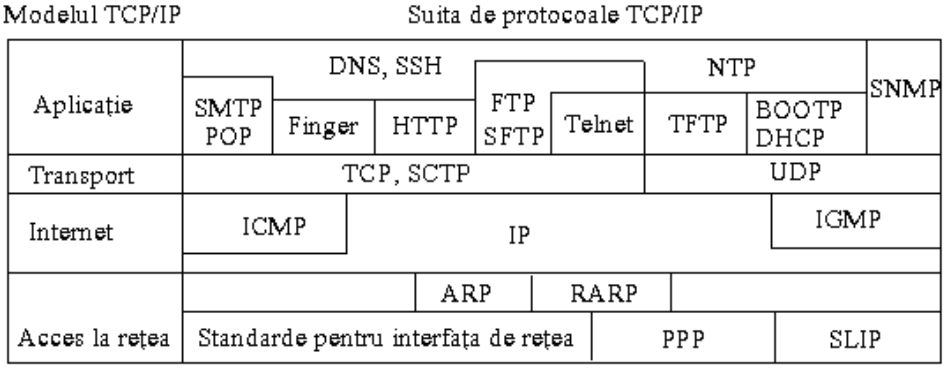

Figura I.4 Stiva de protocoale TCP/IP

Pe nivelul de acces la rețea se definesc standardele de rețele (*Ethernet, Fast Ethernet, GigaEthernet, 10GigaEthernet, Token-Bus, Token-Ring, WLAN, WIFI, Bluetooth* etc.) şi protocoalele pentru comunicații seriale PPP (*Point-to-Point Protocol*) şi SLIP (*Serial Line Internet Protocol*).

Legătura cu nivelul Internet este făcut de cele două protocoale de adresare ARP (*Address Resolution Protocol*) şi RARP (*Reverse Address Resolution Protocol*).

ARP comunică la cerere, pe baza adresei IP a unui echipament, adresa fizică (MAC) de 6 octeți a acestuia (RFC 826). Tabelele ARP sunt stocate în memoria RAM a echipamentului (calculator, router etc). Se pot face echivalări sugestive între numele unei persoane şi adresa MAC a echipamentului, respectiv între adresa poştală şi adresa IP, care permit localizarea destinației unui mesaj.

RARP furnizează la cerere adresa IP dată unui echipament cu adresa MAC, pe baza unor tabele de adrese (RFC 903).

ARP şi RARP se utilizează numai în interiorul unui LAN. Aceste protocoale nu folosesc IP pentru încapsularea datelor.

Pe nivelul Internet, se folosesc protocoalele IP (*Internet Protocol*), ICMP (*Internet Control Message Protocol*) şi IGMP (*Internet Group Management Protocol*).

Protocolul Internet este un protocol de nivel rețea prin intermediul căruia se transferă toate datele şi care stabileşte modul de adresare ierarhizat folosind în versiunea 4 adrese IP de 4 octeți, exprimați în format zecimal cu separare prin puncte (*dotted-decimal notation*), pentru localizarea sistematică a sursei şi destinației, într-o anumită rețea sau subrețea de calculatoare (RFC 791). Întrucât IP încapsulează datele provenite de pe

nivelul de transport sau de la celelalte protocoale de pe nivelul Internet (ICMP, IGMP), nivelul de rețea mai este denumit şi **nivel IP**.

Versiunea 6 a protocolului IP (IPv6) defineşte adrese de 128 de biți, respectiv 16 octeți, adică un spațiu de adrese extrem de larg, de circa $3{,}4x10^{38}$ adrese. Dimensiunea unității de date maxim transferabile (MTU – *Maximum Transfer Unit*) este considerabil mărită, de la 64 KB cât admite IPv4, la 4GB în aşa-numite „*jumbograms*". IPv6 nu mai foloseşte sume de control pe nivelul Internet, controlul erorilor revenind nivelelor legătură de date şi celui de transport. Prin utilizarea IPv6 NAT nu mai este necesar şi multe probleme legate de rutare precum CIDR (*Classless Interdomain Routing*) sunt eliminate. IPv6 include protocoalele de securitate IPsec care erau doar opționale în versiunea anterioară a protocolului IP. O altă facilitate se referă la utilizarea IPv6 pentru comunicații mobile (MIPv6 - *Mobile IPv6*) care evită o serie de probleme de rutare precum cea de rutare în triunghi. Pentru aplicarea IPv6 se preconizează adaptarea protocoalelor actuale la acesta (DHCPv6, ICMPv6 etc.)

ICMP este un protocol de nivel rețea care transportă mesaje de control, de informare sau de eroare, referitoare la capacitatea sistemului de a transmite pachetele de date la destinație fără erori, informații utile despre rețea etc (RFC 792). Protocolul ICMP comunică direct cu aplicațiile, fără a accesa TCP sau UDP.

IGMP gestionează transferul datelor spre destinații de grup, care includ mai mulți utilizatori, prin transmisii *multicast* (RFC 1112).

Tot pe nivelul de rețea operează şi protocoalele de rutare (RIP – *Routing Information Protocol*, OSPF – *Open Shortest Path First*, BGP – *Border Gateway Protocol* ş.a.).

Pe nivelul de transport se folosesc două tipuri de protocoale, cu şi fără conexiune.

TCP (*Transmission Control Protocol*) este un protocol orientat pe conexiune, asemenea sistemelor telefonice. Permite controlul traficului, confirmarea sau infirmarea recepției corecte a mesajelor, retransmisia pachetelor şi ordonarea corectă a fragmentelor unui mesaj.

UDP (*User Datagram Protocol*) este un protocol de transport fără conexiune, asemănător sistemului poştal clasic, mai puțin sigur decât TCP dar mai puțin pretențios.

SCTP (*Stream Control Transmission Protocol*), definit în RFC 4960 din 2000, este un protocol de transport asemănător TCP dar, spre deosebire de acesta, permite transmisia în paralel a mai multor fluxuri (*multi-streaming*), utilă în numeroase aplicații de tip multimedia (de exemplu, transmisia simultană a mai multor imagini dintr-o aplicație web.

O reprezentare echivalentă a suitei TCP/IP este dată în figura I.5. Protocoalele de pe nivelele superioare ale stivei beneficiază de serviciile furnizate de nivelele inferioare.

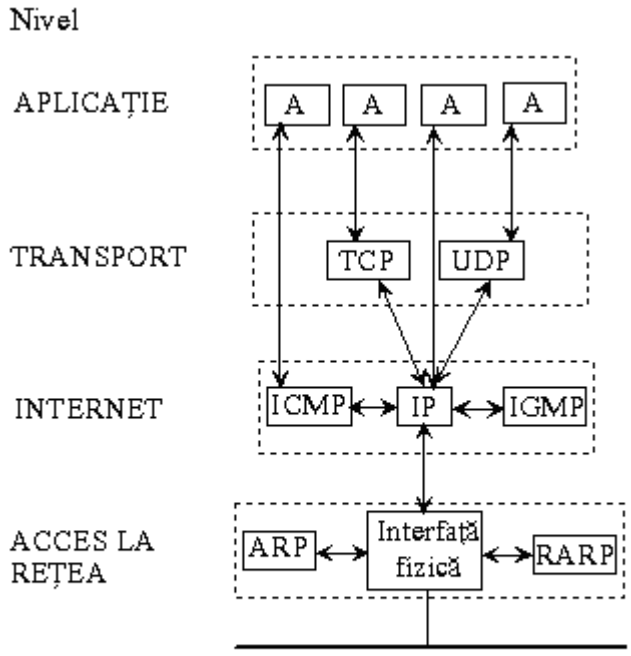

Fig.I.5 Comunicații între protocoalele
din stiva TCP/IP (A= aplicatie)

Din figura I.5, se observă că un protocol de aplicație (A) poate comunica direct cu IP, dar în acest caz este nevoie să includă funcțiile de transport în propriul program de aplicație.

Toate protocoalele care folosesc încapsularea IP şi implicit adresele de rețea sunt **rutabile**.

Utilizatorul foloseşte serviciile de rețea prin intermediul unor programe de aplicații care implementează protocoalele de comunicație pentru serviciile respective, eventual folosind interfețe grafice pentru utilizatori (GUI - *Graphic Unit Interface*).

Ca **protocoale de aplicații**, care oferă direct servicii de rețea utilizatorului, se folosesc:

SMTP (*Simple Mail Transfer Protocol*) permite diferitelor calculatoare care folosesc TCP/IP să comunice prin poşta electronică (*electronic-mail*). Acest protocol stabileşte conexiunea punct-la-punct între clientul SMTP şi serverul SMTP, asigură transferul mesajului prin TCP, înştiinţează utilizatorul despre noul mesaj primit, după care se desface legătura dintre client şi server (RFC 821).

POP (*Post-Office Protocol)* este protocolul prin care utilizatorul îşi preia mesajele din căsuța poştală proprie. Spre deosebire de versiunea POP 2, POP3 permite accesul de la distanță al utilizatorului la căsuța sa poştală.

IMAP (*Internet Message Access Protocol*) versiunea 4 (RFC 3501, RFC 2595) este echivalent ca funcționalitate cu POP3, adică permite clientului preluarea de la distanță a mesajelor de e-mail din căsuța poştală proprie. Acest protocol foloseşte portul de aplicații 143 şi este preferat în rețele largi precum cele din campusuri. IMAP4 poate utiliza SSL (*Secure Sockets Layer*) pentru transmisia criptată a mesajelor. Spre deosebire de POP3, IMAP permite conexiuni simultane la aceeaşi cutie poştală.

FTP (*File Transfer Protocol*) este un protocol de transfer al fişierelor între calculatoare, mai precis un limbaj comun care permite comunicarea între oricare două sisteme de operare (WINDOWS, LINUX/UNIX etc) folosind programe FTP pentru client şi server. FTP foloseşte două conexiuni TCP pentru transferul sigur al datelor simultan cu controlul comunicației (RFC 959).

SFTP (*Simple File Transfer Protocol*) este o versiune simplificată a FTP, bazată pe o singură conexiune TCP, care nu s-a impus însă ca performanțe.

TFTP (*Trivial File Transport Protocol*), mai puțin sofisticat decât FTP, acesta este folosit pentru transferul unor mesaje scurte prin UDP. Se

impun tehnici de corecție a erorilor întrucât UDP nu generează confirmarea de recepție corectă a mesajelor (ACK) ca TCP (RFC 783, RFC 906).

TELNET (*Virtual Terminal Connection Protocol*) este un protocol de terminal virtual care permite conectarea unui utilizator de la distanță la anumite calculatoare-gazdă, rulând programul *telnetd* al serverului. Se utilizează algoritmi de negociere cu terminalul respectiv, pentru a-i cunoaşte caracteristicile. Acesta este văzut ca un terminal virtual cu care se poate comunica de la distanță, indiferent de caracteristicile lui fizice (RFC 854, RFC 856).

FINGER (*Finger User-information Protocol*) este un protocol care permite obținerea de informații publice despre utilizatorii unei rețele.

SSH (*Secure Shell Protocol*) oferă mai multe servicii de rețea (poştă electronică, transfer de fişiere, conexiuni la distanță ş.a.) în mod securizat, folosind algoritmi de criptare.

BOOTP (*BOOTstrap Protocol*) este apelat de un utilizator pentru a-şi afla adresa IP. Acest protocol foloseşte UDP pentru transportul mesajelor. Un calculator care foloseşte BOOTP, expediază un mesaj în rețea prin broadcast (pe o adresă IP cu toți biții '1'). Serverul de BOOTP retransmite mesajul în toată rețeaua (*broadcast*) iar destinația îşi recunoaşte adresa MAC şi preia mesajul. Acest protocol nu poate lucra într-un sistem de alocare dinamică a adreselor IP, dar spre deosebire de RARP, acesta furnizează sursei atât adresa sa IP, cât şi adresele IP ale serverului şi routerului (*default gateway*) folosit de LAN (RFC 951).

DHCP (*Dynamic Host Configuration Protocol*), succesor al protocolului BOOTP, permite utilizarea unui număr limitat de adrese IP de către mai mulți utilizatori. Clientul solicită serverului DHCP o adresă IP. Acesta îi alocă o adresă dintr-un domeniu de adrese cunoscut, eventual îi

furnizează şi masca de rețea. Alocarea este rapidă şi dinamică. Deşi routerele nu suportă transmisiile broadcast solicitate de ARP şi RARP, ele permit aceste transmisii în cazul BOOTP şi DHCP ceea ce facilitează comunicațiile dintre diverse LAN-uri.

HTTP (*HyperText Transfer Protocol*), protocolul generic al serviciului de web, este folosit de utilizatorii *web* şi de serverele WWW pentru transferul unor fişiere de tip text, imagine, multimedia, în format special (*hypertext*), prin intermediul unui limbaj de editare HTML (*HyperText Markup Language*). Varianta securizată a acestuia este HTTPS (HTTP *Secure*) foloseşte pentru securizarea procesului de navigare pe web fie SSL, fie TLS (*Transport Layer Security*) care oferă protecție față de tentativele de interceptare a comunicației sau față de atacurile de tip „omul din mijloc" (*man-in-the-middle attack*). Comunicația se poate face pe portul implicit 443 sau pe orice alt port ales de utilizator.

NTP (*Network Time Protocol*) este cel mai precis protocol de timp din Internet. Acesta sincronizează ceasurile interne din două sau mai multe calculatoare, cu o precizie de 1 - 50 ms față de timpul standard oficial (RFC 1305).

SNMP (*Simple Network Management Protocol*) este folosit pentru supravegherea funcționării rețelelor bazate pe TCP/IP (controlul statistic al traficului, performanțelor, modului de configurare şi securizare) utilizând bazele de informații de management (MIB), structurate pe baza unor reguli definite de SMI (*Structure of Management Information*) conform RFC 1155. Versiunea SNMP2 prevede posibilitatea aplicării unor strategii centralizate sau distribuite de management de rețea.

IRC (*Internet Relay Chat*) este un protocol de comunicație în timp real, fie de tip conferință, cu mai mulți utilizatori, fie de comunicare în pereche de tip unul-la-unul. IRC foloseşte TCP şi opțional TLS.

Există şi alte protocoale în suita TCP/IP care oferă diverse servicii utilizatorilor din Internet. Clienții serviciilor de rețea pot fi utilizatori umani dar şi o serie de module software (programe software, protocoale, echipamente) care adresează cereri serverelor din rețea.

În general, lista serviciilor Internet disponibile pe un PC din rețea, conținând informații despre protocoalele utilizate şi porturile de aplicații asociate se găseşte într-un fişier special (SERVICES), conceput ca o bază de date.

I.3.3 MODELUL CLIENT-SERVER

Deosebit de util pentru înțelegerea proceselor de comunicații şi realizarea programelor de aplicații pentru rețea este **modelul client-server.**

Clientul este partea hardware sau software care adresează o cerere (de acces, de informare, de transfer de fişiere etc).

Serverul este partea hardware sau software care răspunde cererii clientului (Figura I.6).

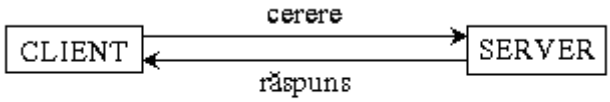

Figura I.6 Modelul client-server

Pe aceste considerente, anumite calculatoare din rețea pe care sunt instalate programe software de tip server sunt denumite simplu servere (de nume, de fişiere, de web, de poştă electronică, de bază de date etc).

Numeroase procese de comunicație din rețea, dintre echipamente sau dintre module software, au loc pe baza modelului client-server. De multe ori, rolurile de client şi de server se inversează pe durata comunicației.

Aplicația server se autoinițializează după care rămâne într-o stare de aşteptare până la primirea unei cereri de serviciu de la un proces client. Aplicația client este cea care solicită a conexiune iar aplicația server primeşte cererea şi o rezolvă. Între cele două aplicații apare o conversație virtuală ca şi cum între ele ar exista o conexiune punct-la-punct.

I.3.4 MODELUL PEER-TO-PEER

Modelul de rețea de comunicare în pereche (p2p – *peer-to-peer)* reuneşte în fiecare nod rolurile de client şi de server, rezultînd o pereche de noduri comunicante cu drepturi egale precum în telefonia clasică. Topologia de rețea de tip „plasă” (*mesh*) ilustrează foarte bine acest concept (Figura I.7).

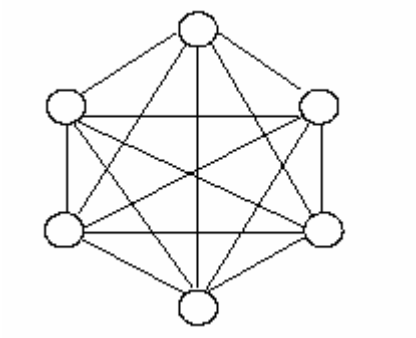

Figura I.7 Rețea de comunicații P2P

Primele rețele P2P erau folosite pentru distribuția (*sharing*) de fişiere muzicale în format mp3 (rețelele Napster, KaZaA etc.) iar în prezent aplicațiile sunt mult diversificate (mesagerie scrisă,vocală sau video, schimb de fişiere de orice tip inclusiv muzică şi filme, forumuri de discuții şi multe altele).

Din punctul de vedere al securității, aceste aplicații P2P sunt de multe ori critice, ele permițând accesul neautorizat la resursele rețelei:

- programele software folosite în comunicațiile P2P pot fi modificate de terți;
- entități cu intenții malițioase pot redirecționa pachetele spre destinații inexistente sau incorecte rezultând pierderi de pachete
- în comunicații P2P entitățile îşi pot păstra anonimatul.

I.4 INTRODUCERE ÎN SECURITATEA REȚELELOR

Informațiile, stocate sau transmise ca date în rețea, reprezintă o resursă valoroasă care trebuie controlată şi administrată strict, ca orice resursă comună. O parte sau toate datele comune pot prezenta o importanță strategică pentru organizație. Bazele de date reprezintă o aplicație majoră a rețelelor de calculatoare. Sistemul de gestiune a bazei de date SGBD trebuie să furnizeze un mecanism prin care să garanteze că numai utilizatorii autorizați pot accesa baza de date şi că baza de date este sigură. Securitatea se referă la protejarea bazei de date față de accesul neautorizat fie intenționat, fie accidental, prin utilizarea unor elemente de control bazate sau nu pe calculatoare. Considerațiile de securitate nu se aplică doar datelor conținute în baza de date. Breşele din sistemul de securitate pot afecta şi alte părți ale sistemului care la rândul lor pot afecta baza de date.

Securitatea rețelelor se referă la elementele hardware, software, persoane şi date.

Persoanele sau entitățile autentificabile şi înregistrate sunt denumite, în satndardele ISO, **parteneri**. Partenerii care au un rol activ în sistem se numesc **inițiatori**. Partenerii cu rol pasiv sunt denumiți **ținte**.

Vom considera securitatea datelor relativ la:

- furt şi fraudă,
- pierderea confidențialității,
- pierderea caracterului privat,
- pierderea integrității,
- pierderea disponibilității.

Furtul şi frauda nu sunt limitate la mediul bazelor de date ci întreaga rețea este expusă acestui risc. Pentru a reduce riscurile de furt şi fraudă se procedează la păstrarea în siguranță a documentelor privind plata salariilor, înregistrarea cantității exacte de hârtie utilizată la tipărirea cecurilor de plată şi asigurarea înregistrării corespunzătoare şi distrugerii hârtiilor rezultate ca urmare a tipăririi greşite.

Confidențialitatea se referă la necesitatea de a păstra secretul asupra unor date, de regulă numai a celor de importanță majoră pentru organizația respectivă, în timp ce **caracterul privat** se referă la necesitatea de a proteja datele referitoare la persoane individuale.

Integritatea reprezintă asigurarea faptului că datele nu au fost alterate(corupte) sau distruse în urma unui proces de atac.

Pierderea integrității datelor are ca rezultat apariția unor date care numai sunt valabile sau sunt greşite.

Disponibilitatea se defineşte ca şi caracteristică a unui sistem informatic de a funcționa fără întreruperi şi posibilitatea lui de a fi accesat oricând, de oriunde. Importanța ei este motivată de faptul că o rețea găzduieşte servere de aplicații, baze de date, echipamente de stocare, şi nu în ultimul rând oferă operabilitate utilizatorilor finali.

Pierderea disponibilității înseamnă că datele, sistemul sau ambele, nu pot fi accesate.

Este necesar ca organizațiile să identifice riscurile de securitate la care sunt expuse şi să inițieze planuri şi măsuri adecvate, ținându-se cont de costurile implementării acestora şi valoarea informațiilor protejate.

Computerele şi rețelele de calculatoare prezintă puncte slabe, intrinseci. Printre acestea se numără cele legate de protocolul TCP/IP, sisteme de operare, şi nu în ultimul rând puncte slabe datorate unui

management defectuos, şi unei politici de securitate necorespunzătoare. Administratorii rețelelor trebuie să descopere şi să contracareze punctele slabe din cadrul rețelelor de care răspund.

Se pot identifica trei tipuri de breşe de securitate care pot reprezenta o posibilă țintă în cazul unui atac:

- breşe cauzate de aspecte tehnologice
- breşe datorate unei configurări necorespunzătoare a echipamentelor şi a rețelei în general
- breşe determinate de o politică de securitate necorespunzătoare.

Evenimentele provocate până în prezent de breşele de securitate din rețelele de comunicații demonstrează că indiferent de cât de sigur pare a fi un sistem, un nivel adecvat de securitate poate fi atins doar dacă este securizat şi mediul de transmisie. Obiectivul oricărei politici de securitate este de a realiza un echilibru între o operație rezonabil de sigură, care nu obstructționează în mod nejustificat utilizatorii, şi costurile întreținerii acestora. Pericolele accidentale au ca rezultat majoritatea pierderilor din cele mai multe organizații.

Tipurile de contramăsuri față de pericolele care amenință o rețea variază, de la elemente de control fizic, până la procedura administrativă. În general, securitatea unui sistem SGBD este aceeaşi ca cea a sistemului de operare, datorită strânsei lor asocieri.

Pentru a evita problemele create de atacurile adresate securității rețelelor, trebuie adoptate măsuri adecvate fiecărui nivel OSI:

1. la nivel fizic, se impune controlul accesului fizic la rețea şi la resursele acesteia, precum şi minimizarea riscului de „ascultare pasivă” a fluxurilor de date transmise.

2. la nivel legătură, este necesară securizarea prin criptare a informațiilor.
3. la nivel de rețea, este eficientă activarea firewall-urilor şi configurarea lor pe baza principiilor exprimate în politica de securitate a rețelei. Accesul logic la sistem sau rețea se poate realiza pe baza diferitelor metode de autentificare, inclusiv pe baza unor liste de control al accesului (ACL – *Access Control List*).
4. la nivel de transport se pot folosi diferite protocoale de securitate a conexiunilor, precum SSL (*Secure Socket Layer*), sau TLS (*Transport Layer Security*).
5. la nivel de aplicație, securitatea se realizează prin jurnalizarea accesului, monitorizarea evenimentelor din rețea, clasificarea lor pe clase de risc şi aplicarea unor măsuri de limitare şi anihilare a atacurilor. Se pot folosi diferite instrumente software şi hardware pentru efectuarea unor teste de securitate asupra rețelei cu simularea atacurilor (scanarea rețelei şi a porturilor: *Nmap, Ethereal, SuperScan*; identificarea sistemelor de operare: *Xprobe;* testarea serverelor de baze de date precum *SQLping*; testarea conectivității prin *TraceRoute* sau *VisualRoute*; detecția vulnerabilităților: *Nessus, Nikto, Netcat, Zedebee, Winfo*; conexiuni de la distanță: *Remote Desktop, PsExec*; spargerea parolelor: *Brutus, Hydra, Vncrack*; instrumente de ecou de la tastatură: *Xspy*; detecția vulnerabilităților rețelelor wireless: *Netstumbler, Kismet, Airsnort, Process Explorer*; listarea, recuperarea şi protejarea resurselor: *chkrootkit, TCT - Coroner's Toolkit, IPchains, Iptables.*

   Elementele de control al securității bazate pe calculator cuprind:

- autorizarea

- autentificarea
- copiile de siguranță şi posibilitățile de refacere a sistemului
- integritatea
- criptarea.

Autorizarea reprezintă acordarea unui drept sau privilegiu care permite unei persoane să aibă acces legitim la un sistem sau la un obiect din sistem. Controlul autorizării poate fi implementat în cadrul elementelor de software şi poate reglementa nu numai sistemele sau obiectele la care are acces un utilizator, ci şi ce poate face acesta cu ele (citire, scriere, execuție).

Autentificarea este un mecanism de verificare a identității unei entități. De obicei administratorul de sistem este responsabil de acordarea permisiunilor de acces la un sistem, prin crearea unor conturi individuale. Odată ce unui utilizator i-a fost acordată permisiunea de a utiliza un sistem, acestuia îi pot fi acordate anumite privilegii. Autentificarea este vitală pentru securitatea sistemului, pentru că arată valabilitatea unui utilizator, serviciu sau aplicație. Cu alte cuvinte trebuie verificată identitatea utilizatorului care intenționează să acceseze resursele.

Autentificarea poate fi realizată pe diferite criterii:

- cunoştințe (parole, adrese fizice sau de rețea, coduri PIN, coduri de tranzacții etc.)
- posesie (carduri, chei etc.)
- proprietăți (biometrice: amprente, retină, voce; de altă natură).

Ca metode de autentificare amintim:

- parolele asociate cu nume de utilizator
- protocoale de securitate, precum SSL (*Secure Socket Layer*)
- semnături şi certificate digitale (X.509)
- carduri inteligente (*smart cards*)

- cookies.

În rețelele de comunicații cu acces nerestricționat, nu este necesară aplicarea vreunei metode de autentificare (*no-authentication*). Este cazul așa-numitelor „*free hotspot*” care oferă servicii gratuite de Internet în aeroporturi, universități, şcoli, restaurante etc.

În cazul rețelelor cu acces restricționat, se impune utilizarea unei anumite tehnici de autentificare, fie în sistem deschis (*open system authentication*), fie în sistem închis (*closed system authentication*), cu o cheie predefinită, cunoscută dinainte numai de utilizatorii autorizați (*shared key authentication*) care, în plus, dispun de un mecanism de criptare comun.

În sistem deschis, autentificarea se face la cerere, fără restricții sau pe baza unei liste de clienți. Clientul trimite ca cerere un cadru de management pentru autentificare în care este inclus identificatorul său. Serverul verifică acel cadru şi identificatorul clientului şi îl autentifică dacă identificatorul de rețea este corect. Acest mecanism de autentificare este de exemplu util pentru diferențierea rețelelor wireless care transmit în aceeaşi arie, pentru a se realiza conexiunea la rețeaua cu SSID-ul corect. Acest mod de autentificare este considerat modul implicit sau nul de autentificare în multe sisteme sau rețele (*null-type authentication*). Acest mod de autentificare permite intruşilor să intercepteze sau „să asculte” tot ce se transmite în rețea (*eavesdropping*) şi de aceea se impune în acest caz criptarea informațiilor cu caracter secret.

Autentificarea cu cheie predefinită se face la cererea clientului, pe baza unei informații secrete pe care o dețin serverul şi clientul. Serverul generează o întrebare aleatoare pe care o criptează cu cheia secretă şi o trimite clientului. Clientul criptează răspunsul la întrebare, dacă deține informația respectivă, şi o răspunde serverului. După decriptare, serverul

decide dacă răspunsul este corect, caz în care consideră autentificarea realizată. Cheia de criptare poate fi cunoscută în pereche, numai de server şi de un anumit client (*unicast key*), fie de server şi de toți clienții din rețea (*multicast or global key*).

Pentru un control mai riguros al accesului în rețea (NAC – *Network Access Control*), se poate impune ca, în vederea autentificării, clientul să ofere o serie de garanții (*credentials*) înainte de a se autentifica în vederea accesării serviciilor oferite pe un anumit port din rețea (*port based NAC*). Odată autentificat, clientul obține acces la toate serviciile oferite pe acel port. De accea, sunt necesare metode de certificare riguroase pentru a nu crea breşe în sistem.

Autentificarea se poate face şi mutual, adică ambele entități implicate într-un proces de comunicație se autentifică una față de cealaltă.

Salvarea de siguranță este procesul de efectuarea periodică a unei copii a bazei de date pe un mediu de stocare offline. Un sistem SGBD trebuie să conțină facilitatea de salvare de siguranță, care să asiste la refacerea bazei de date după o defecțiune. În general, pentru orice sistem trebuie să se realizeze copii de siguranță cu o anumită perioadă de valabilitate.

Criptarea reprezintă tehnica de codare a datelor printr-un anumit algoritm, care transformă aşa-numitul „text în clar” (*plaintext*) în date criptate din care informația nu poate fi extrasă în absența algoritmului de decodare şi a cheii de criptare, asigurându-se astfel secretul acesteia. Inițial tehnicile de criptare se aplicau doar pe texte, ulterior securizarea conținutului fiind necesară pentru multe alte tipuri de informații (financiare, date de identificare, fotografii, hărți, transmisii vocale sau video etc.).

Pentru a transmite datele în siguranță, este necesară utilizarea unui criptosistem, care include:

- cheia de criptare
- algoritmul de criptare
- cheia de decriptare
- algoritmul de decriptare.

În asigurarea securității unui sistem, atitudinea şi comportamentul oamenilor sunt semnificative. Ca urmare este necesar un control adecvat al personalului pentru evitarea unor atacuri din interiorul organizației, din rețeaua internă (*intranet*).

Securitatea rețelelor impune printre altele şi **asigurarea securității serverelor de rețea**. Majoritatea resurselor informaționale sunt accesate prin intermediul site-urilor web. Serverul de web este considerat temelia unui site deci şi al unui portal. Orice aplicație web va interacționa cu serverul şi cu ajutorul lui se va vizualiza cea mai mare parte a conținutului. Trebuie deci folosit un server de web securizat care să corespundă nevoilor aplicației care va fi implementată.

În alegerea unui server web, se au în vedere cele care permit controlul autentificării, setarea drepturilor şi permisiunilor de utilizator, folosirea scripturilor CGI (*Common Gateway Interface*). Serverul Apache este unul dintre cele mai populare servere Web, gratuit, uşor de configurat, rezultatul proiectului Apache. Serverul Apache îşi setează configurările conform cu trei fişiere:

- access.conf – controlează drepturile de acces global.
- httpd.conf - conține directive de configurare care controlează modul de rulare a serverului, locația fişierelor-jurnal (log-urilor), porturile de acces.

- smr.conf - conține directive pentru configurarea resurselor (locația documentelor web, scripturi CGI).

Configurarea serverului pentru rulare se face prin intermediul directivelor de configurare (*configuration directives*). Acestea sunt comenzi care setează anumite opțiuni. Serverul Apache rulează în unul din următoarele două moduri:

- *stand-alone* – cu performanțe superioare, pentru care în fiecare moment există un proces gata să servească o cerere de client.
- *daemon* – serverul porneşte de fiecare dată când apare o nouă cerere.

Ca şi **avantaje** ale acestui server, se pot aminti:

- oferă securitate sporită aplicațiilor prin protocolul SSL, prin criptarea mesajelor
- este uşor de configurat
- rulează pe un număr mare de platforme şi sisteme de operare.

RISCURI DE SECURITATE ÎN REȚELELE WIRELESS

- **Furtul şi frauda –** rețelele wireless pot fi detectate de la distanțe relativ mari (10 km), cu echipamente simple şi costuri reduse (antene parabolice de 18”), cu programe software adecvate (NetStumbler) disponibile pe Web (*free software*), fără posibilitatea detectării intruşilor pasivi. Folosind sisteme de operare Linux sau Macintosh, un eventual hacker se poate disimula ca şi sistem Windows, poate accesa resursele publice (*sharing*). Intruşii activi sunt aceia care apar ca şi utilizatori autorizați (*crack* MAC), ei fiind capabili să intercepteze pachetele din rețea. Este recomandată separarea resurselor care necesită securitate sporită prin configurarea unor rețele VPN şi aplicarea politicii de firewall.

- **Controlul accesului -** cele mai periculoase echipamente de accesare neautorizată a rețelei wireless sunt dispozitivele de tip PDA (*Personal Digital Assistant*), echipamente portabile de mici dimensiuni care dispun de software adecvat diverselor sisteme de operare (PocketDOS, Windows, Linux).
- **Autentificarea –** precede faza de asociere a stației cu un punct de acces (AP – *Access Point*), fiind realizată pe baza unui identificator de rețea (SSID – *Service Set Identifier*) valid. Există riscul ca într-o anumită arie geografică să funcționeze pe lângă un AP autorizat, un **AP intrus** (*counterfeiting*), eventual cu nivel de putere sporit, care încearcă să detecteze identitatea utilizatorilor autorizați din acea celulă şi cheile de criptare folosite în rețeaua wireless. Localizarea unui fals AP este dificilă şi devine practic imposibilă atunci când acest AP este mobil. Monitorizarea traficului pe teren de către organismele de control abilitate, combinată cu preluarea şi memorarea informațiilor GPS, permite crearea unor baze de date cu informații despre AP-urile autorizate, urmând ca accesarea unui AP de către client să se realizeze pe principiile unei politici de securitate aplicată la nivelul acestuia, bazată pe verificarea coordonatelor AP-ului, eventual furnizate de un **server de securitate** intermediar care pe principiul client-server răspunde afirmativ (*access granted*) sau negativ (*access denied*) cererii de acces, păstrând secretul identităților unităților din rețea pe care le deserveşte. Se impune în acest caz asigurarea securității fizice în perimetrul AP-urilor autorizate. IEEE 802.1X nu este un mecanism propriu-zis de autentificare ci este asociat cu EAP. 802.1x descrie autentificarea automată şi criptarea cu cheie modificată dinamic prin protocolul extins de autentificare (EAP - *Extensible Authentication Protocol*), localizat pe server precum şi în echipamentele-client, care acceptă autentificarea pe bază de

jetoane (*token*), parole, certificate digitale şi metodele cu cheie publică (EAP – TLS, EAP – TTLS Tunneled Transport Layer Security, LEAP - Lightweigth EAP).

- **Criptarea datelor** – este considerată o funcție opțională şi de aceea este dezactivată în varianta implicită (default) de instalare a sistemelor de operare, pentru a folosi viteza maximă de transmisie. Se efectuează în mod uzual cu chei de maximum 128 biți, relativ scurtă ca număr de caractere (16 caractere ASCII, 8 caractere UNICODE). DES suportă chei de criptare de 40 – 64 biți; 802.11b foloseşte chei de 64-128 biți. Metoda WEP (*Wired Equivalent Privacy*) aplică algoritmul simetric de criptare RC4-128 pe baza unei chei de transmisie de 104 biți, cu vectori de inițializare IV (*Initialization Vector*) de 24 de biți transmişi în clar, pentru secretizarea datelor, nu şi a antetelor de transmisie, asigurând confidențialitatea informațiilor, nu şi restricționarea accesului utilizatorilor neautorizați. Schimbarea manuală a cheilor de criptare şi posibilitatea ca mai mulți utilizatori să folosească aceeaşi cheie, cresc riscul de interceptare a cheii şi extragerea informațiilor din pachetele criptate similar. Metoda WPA (WiFi *Protected Access*) foloseşte algoritmii AES-128 şi TKIP pentru schimbarea automată a cheilor. Pentru o securitate sporită se impune criptarea cu cheie secretă a informațiilor de identificare, a cadrelor de control şi de management. Trebuie acordată o atenție sporită sistemului de generare şi gestionare a cheilor de criptare, precum şi excluderii cheilor compromise sau slabe. Dimensiunea spațiului cheilor de criptare este diminuată semnificativ prin folosirea parolelor bazate pe caractere printabile (din 26 litere mici, 26 litere mari şi 10 cifre rezultă circa $2x10^{14}$ combinații posibile de 8 caractere), eventual cu semnificații particulare şi personale de tip cuvinte uzuale, nume proprii, date de naştere etc.

- **Tehnici de protecție şi autorizare –** acordarea dreptului de acces în rețeaua wireless pe baza adreselor MAC unic alocate de producător plăcilor de rețea NIC, folosind liste de control al accesului stocate în router, AP sau în servere RADIUS, permite eliminarea riscului de asociere a unui posibil intrus în infrastructura şi evitarea emulării unei adrese MAC autorizate (MAC *spooffing*). Metodele de extensie a spectrului cu o secvență de cod pseudoaleator conferă o oarecare securitate, metoda de extensie cu secvență directă DSSS (*Direct Sequence Spread Spectrum*) fiind mai performantă decât metoda de extensie cu salturi de frecvență FHSS (*Frequency Hopping Spread Spectrum*). Prin eventuala scanare pasivă a benzii de transmisie a unui AP (*eavesdropping*) nu se pot prelua pachetele de date fără cunoaşterea codului de împrăştiere a spectrului. Caracterul periodic al secvențelor pseudoaleatoare este un inconvenient în menținerea unei redundanțe reduse a semnalului transmis, fiind necesară găsirea unor secvențe de cod mai eficiente. Monitorizarea traficului din rețea în timpul orelor fireşti de funcționare şi din afara programului permite administratorului să detecteze eventualele congestii sau intruziuni din rețea, depistarea porturilor de protocol prin care se accesează neautorizat rețeaua cu posibilitatea restricționării ulterioare a accesului. Cel mai puternic şi mai dăunător este atacul de tip "acces interzis" (DoS – *Denial of Service*) prin care se întrerupe orice comunicație în rețea folosind surse de emisie suficient de puternice în aceeaşi arie geografică. În acest caz, o soluție eficientă constă în aplicarea unei tehnici de extensie de spectru cu un câştig de extensie suficient de mare. Este de asemenea utilă monitorizarea permanentă a traficului (24/24, 7/7) şi a tuturor transmisiilor radio din aria rețelei wireless.
- **Tehnici de detecție a intruşilor IDS (***Intrusion Detection System***) –** în rețelele wireless este mai dificilă detecția intruşilor decât în rețelele cu

transmisie “pe fir”, prezența lor fiind similară unei rate de eroare a pachetelor (PER – *Packet Error Rate*) mari sau unor încercări eşuate de autentificare a unui utilizator autorizat. Se poate restricționa numărul maxim de încercări de autentificare de la distanță eşuate succesiv, dreptul de acces fiind acordat numai după reidentificarea persoanei şi a echipamentului de către administratorul de rețea.

- **Integritatea datelor –** este testată folosind diverse coduri, precum cele ciclice (CRC – *Cyclic Redundancy Checking*) şi funcțiile hash.

Odată cu dezvoltarea tot mai mult a rețelelor de calculatoare, a serviciilor oferite de acestea şi a importanței informațiilor pe care le vehiculează, a crescut şi necesitatea protejării acestora.

Comunicațiile P2P oferă o serie de facilități:

- jurnalizarea transferurilor
- autentificarea partenerilor
- mobilitatea echipamentelor
- rezistență la atacuri de tip DoS, flooding, reluarea mesajelor.
- folosirea mecanismelor anti-pollution.

Rețelele pot fi amenințate la nivel fizic, logic sau informațional, atât din interior, cât şi din exterior. Pot fi persoane bine intenționate, care fac diferite erori de operare sau persoane rău intenționate, care alocă timp şi bani pentru penetrarea rețelelor.

Există şi **factori tehnici** care determină breşe de securitate în rețea:

- anumite erori ale software-ului de prelucrare sau de comunicare;
- anumite defecte ale echipamentelor de calcul sau de comunicație;
- viruşii de rețea şi alte programe cu caracter distructiv (*worms*, *spam*);

- lipsa unei pregătiri adecvate a administratorilor, operatorilor şi utilizatorilor de sisteme;
- folosirea abuzivă a unor sisteme.

Rețelele de comunicații pot deservi organisme vitale pentru societate, cum ar fi: sisteme militare, bănci, spitale, sisteme de transport, burse de valori, oferind în acelaşi timp un cadru de comportament antisocial sau de terorism. Este din ce în ce mai greu să se localizeze un defect, un punct de acces ilegal în rețea, un utilizator cu un comportament inadecvat.

Creşterea securității rețelelor trebuie să fie un obiectiv important al oricărui administrator de rețea. Însă trebuie avută în vedere realizarea unui echilibru între costurile aferente şi avantajele concrete obținute. Măsurile de securitate trebuie să descurajeze tentativele de penetrare neautorizată, să le facă mai costisitoare decât obținerea legală a accesului la aceste programe şi date.

Asigurarea securității informațiilor stocate în cadrul unei rețele de comunicații, presupune proceduri de manipulare a datelor care să nu poată duce la distribuirea accidentală a lor şi/sau măsuri de duplicare a informațiilor importante, pentru a putea fi refăcute în caz de nevoie.

O rețea de calculatoare cu acces sigur la date presupune o procedură de autentificare a utilizatorilor şi/sau de autorizare diferențiată pentru anumite resurse.

O rețea de calculatoare este sigură dacă toate operațiile sale sunt întotdeauna executate conform unor reguli strict definite, ceea ce are ca efect o protecție completă a entităților, resurselor şi operațiilor din rețea, reguli cunoscute sub numele de **politică de securitate**.

Lista de amenințări la adresa unei rețele constituie baza definirii **cerințelor de securitate**. Odată cunoscute acestea, trebuie elaborate regulile

conform cărora se efectuează toate operațiile din rețea. Aceste reguli operaționale se implementează prin **protocoale şi servicii de securitate**.

Pentru a realiza o rețea sigură, trebuie implementate, pe baza politicilor şi protocoalelor de securitate, unul sau mai multe **mecanisme de securitate** ("zid de foc" – *firewall*, rețele virtuale private cablate VPN - *Virtual Private Network*, rețele private ad-hoc virtuale VPAN – *Virtual Private Ad-Hoc Network*, servere de securitate şi altele).

Securitatea, ca proces, definește starea rețelei de a fi protejată în fața atacurilor. Nu se poate vorbi despre securitate în sens absolut pentru că, în realitate, orice formă de securitate poate fi compromisă. Resursele de care dispun atacatorii sunt finite şi astfel o rețea poate fi considerată sigură atunci când costurile de atac sunt cu mult mai mari decât „recompensa" obținută.

Securitatea rețelei trebuie avută în vedere încă din faza de proiectare. Adăugarea ulterioară a măsurilor de securitate conduce la costuri ridicate, precum şi la nevoia schimbărilor în arhitectura retelei.

Este foarte important ca serviciile de securitate să fie asigurate pe toate nivelele, de la nivel fizic, până la cel de aplicație pentru protecția propriu-zisă a informațiilor şi a rețelei în general.

Capitolul II PRINCIPII ALE SECURITĂȚII REȚELELOR

II.1 ASPECTE GENERALE

Ca o categorie aparte a serviciilor de rețea, serviciile de securitate sunt oferite prin intermediul diferitelor tipuri de programe sofware, fie ca module componente ale unui sistem de operare, fie ca şi facilități ale unor programe specifice, fie ca aplicații independente. Implementarea lor se poate face şi în varianta hardware, cu circuite dedicate, a căror eficiență este în general foarte ridicată. Dezavantajul metodelor hardware derivă din necesitatea achiziționării unor noi module hardware atunci când se schimbă metoda de securizare a unui sistem.

Serviciile de securitate sunt diverse :

- **Autentificarea** (*authentication*) - reprezintă un mecanism prin care se identifică un utilizator uman, un echipament sau un program sofware client sau server, prin prezentarea unor date de identificare (parolă, smart card, amprente, date biometrice etc.).
- **Autorizarea** (*autorization*) - este permisiunea acordată unui utilizator, de accesare a unor date sau programe, după ce a fost autentificat.
- **Disponibilitatea** (*availability*) – este serviciul prin care un anumit serviciu poate fi utilizat de catre grupul de utilizatori cu drept de acces. Un atac împotriva disponibilității unui sistem este cunoscut sub numele de “refuzul serviciului” (*Denial of Service* - DoS).

- **Confidențialitatea** (*confidentiality*) **–** reprezintă protecția secretului informațiilor cu caracter privat.
- **Integritatea** (*integrity*) **-** se referă la protecția datelor împotriva modificărilor neautorizate.
- **Nerepudierea** (*non-repudiation*) **–** reprezintă un mecanism de prevenire a fraudelor prin care se dovedește că s-a executat o anumită acțiune dintr-un anumit cont de utilizator fără ca posesorul său să poată nega acest lucru .

Costurile serviciilor de securitate depind de mai mulți factori:

1. mediul fizic de transmisie
2. performanțele echipamentelor din rețea
3. performanțele pachetelor software folosite (aplicații dar şi sisteme de operare)
4. nivelul de securizare a datelor propriu-zise prin criptare.

Este importantă clasificarea şi ierarhizarea datelor transferate sau stocate în rețea în vederea securizării corespunzătoare a lor.

Datele sau informațiile pot fi clasificate în mai multe tipuri, folosind diverse criterii.

Pe **criteriul de proprietate**, informațiile se împart în:

a. informații de utilizator
b. informații de rețea

Pe **criteriul importanței**, informațiile pot fi:

a. informații publice
b. informații private (cu diferite grade impuse de confidențialitate).

Pe **criteriul locației**, se pot defini următoarele categorii de date:

a. informații externe (stocate pe diferite tipuri de suport)

b. informații interne (de terminal, server sau echipament de rețea cu management).

Pe **criteriul domeniului de utilizare**, aplicațiile se împart în mai multe categorii:

a. Publicitare
b. Comerciale
c. Educaționale
d. De divertisment
e. Cu sau fără plată
f. Guvernamentale
g. Militare

Alegerea unui anumit serviciu de securitate este condiționată de natura informațiilor care trebuie protejate şi de costurile acceptate pentru această operație.

Politicile de securitate stabilesc regulile şi normele care trebuie respectate de toți utilizatorii rețelei: modul de utilizare adecvată a resurselor, de deschidere a unui cont de utilizator, modul de acces de la distanță, protecția informațiilor confidențiale, administrarea şi distribuirea parolelor, modul de conectare la Internet etc.

Alegerea unei strategii eficiente de securizare a unei rețele trebuie să aibă în vedere riscurile la care este expusă aceasta şi punctele vulnerabile pentru a adapta soluția de securitate la nevoile fiecărei rețele şi a reduce costurile, atât pe termen scurt, cât şi pe termen lung.

Securitatea la nivel fizic presupune luarea unor măsuri de securitate pentru controlul accesului la resursele fizice ale rețelei şi protecția acestora prin protecția sub cheie, folosirea cardurilor de acces, identificarea biometrică a personalului autorizat. Este necesară protecția fizică a tuturor

resurselor importante ale rețelei, precum şi amplasarea corespunzătoare a echipamentelor de rețea şi a cablurilor de legătură astfel încât să se evite degradarea lor intenționată sau accidentală.

Accesul fizic la anumite echipamente trebuie restricționat şi admis doar pe baza unor elemente de identificare (carduri de acces, insigne, recunoaşterea unor caracteristici biometrice precum fața, vocea, amprentele, geometria mâinii, irisul sau retina). Este necesară securizarea strictă a serverului pe care este stocată baza de date conținând aceste informații de identificare precum şi sistemul de transmisie al lor către terminalul de identificare, fiind preferabil ca transmisia să se realizeze „cu fir" şi chiar fibră optică, pe distanțe mici.

Securitatea la nivel logic se referă la acele metode software prin care se asigură controlul accesului logic la resursele informatice şi la serviciile rețelei. De regulă, identificarea şi autentificarea persoanelor cu drept de acces, precum şi accesul selectiv la resursele rețelei se realizează prin intermediul conturilor de utilizator şi a parolelor. În cadrul unei rețele este foarte importantă stabilirea unor reguli cu privire la păstrarea şi distribuirea parolelor, care trebuie respectate de toți utilizatorii.

Administrarea conturilor de utilizator în mod sistematic preîntâmpină eventualele posibilități de abuz manifestate ca atacuri interne asupra rețelei private (furtul, distrugerea sau modificarea unor informații).

Este total neindicată crearea unui cont general de utilizator care poate fi utilizat şi de persoane neautorizate cu un efort minim de aflare a informațiilor de autentificare. De aceea este recomandată o preautentificare a plăcilor de rețea wireless, pe baza adreselor MAC, pentru care este permis accesul în rețea.

Existența programelor de clonare a adreselor MAC scade eficiența metodei de filtrare pe baza de MAC. Cunoașterea istoricului comunicațiilor (Logs) dintr-o rețea permite identificarea acelor combinații utilizator-adresă MAC şi refuzarea accesului în cazul unor încercări repetate cu adrese diferite. Un utilizator autorizat care foloseşte un alt echipament trebuie să înştiințeze administratorul despre noua adresă pentru a putea accesa rețeaua.

Păstrarea la secret a adreselor MAC autorizate este esențială pentru succesul metodei. Stabilirea unor criterii stricte de autorizare a anumitor persoane şi echipamente pentru acces la rețeaua wireless este deosebit de importantă. Folosirea semnăturilor electronice, a certificatelor digitale precum şi a unor coduri de acces personalizate este o metodă sigură de securizare a accesului.

De asemenea, pentru un control mai strict al accesului în rețea este indicată folosirea adresării statice în locul celei dinamice prin DHCP chiar dacă acest lucru presupune gestionarea corectă a unui spațiu de adrese relativ mare.

Monitorizarea traficului din rețea şi operațiile de audit permit detecția unui eventual utilizator neautorizat (IDS – *Intrusion Detection System*) şi excluderea sa. Sistemele de alarmare în cazul unui volum mare de date transferat sau a unei încărcări excesive a procesoarelor permit de asemenea detecția intruşilor sau a unor eventuale atacuri de floodare a rețelei. Programarea corespunzătoare a firewall-ului şi configurarea unor rețele virtuale private reduc riscurile de intruziune şi de atac din exterior.

Utilizarea programelor de tip NetStumbler permite administratorului scanarea tuturor rețelelor wireless dintr-o anumită arie geografică, testarea caracterului deschis sau privat al acestora, deducerea identificatorului de rețea (SSID), a canalelor de comunicație folosite.

Chiar şi fără a se autentifica un eventual atacator poate utiliza un program de preluare de pachete (packet sniffer) realizând un atac pasiv asupra rețelei. Acesta este deosebit de eficient dacă monitorizează traficul broadcast din rețea. De aceea se recomandă folosirea echipamentelor multiport de tip switch şi nu a celor de tip hub.

Eventualele resurse partajate (*shared*) fără restricții între doi utilizatori autorizați sunt vizibile şi pentru alți clienți neautorizați care detectează rețeaua Wi-Fi şi se asociază la aceasta în mod pasiv.

Programele de tip „virus" de asemenea pot afecta rețeaua în mod distructiv.

Pentru evitarea unor astfel de riscuri, trebuie aplicate măsuri de control al accesului suficient de stricte.

Securizarea informațiilor se referă la secretizarea acestora atunci când este cazul, la asigurarea integrității datelor şi verificarea autenticității lor.

Transmiterea informațiilor în clar în aceste pachete prezintă riscul preluării lor neautorizate. Evitarea acestui risc este posibilă prin folosirea tehnicilor de criptare, respectiv prin activarea opțiunilor de secretizare a informațiilor oferite de diverse echipamente şi standarde de rețea. Performanțele acestora sunt exprimate pe diferite nivele de securizare şi sunt limitate astfel încât gradul de protecție oferit nu este întotdeauna acelaşi depinzând substanțial de costurile echipamentelor şi ale programelor software (sisteme de operare, programe de aplicații etc).

Un sistem informatic satisface proprietatea de **confidențialitate** dacă datele sale sunt protejate față de uzul neautorizat adică doar destinatarul unui mesaj poate descifra conținutul acestuia, fapt care se poate realiza prin utilizarea unor **algoritmi criptografici**. Sistemele criptografice transformă

un text în clar într-un text criptat. Sunt două tipuri de sisteme criptografice: simetrice şi asimetrice. Sistemele simetrice folosesc o singură cheie, secretă, atât pentru criptare, cât şi pentru decriptare. Criptosistemele asimetrice utilizează chei diferite. Cheile folosite la decriptate sunt secrete, pe când cele folosite la criptare sunt făcute publice. În acest fel doar destinatarul de drept al mesajului va putea descifra conținutul acestuia, presupunând că deține cheia privată de decriptare. Sistemele simetrice se mai numesc şi sisteme cu chei private, iar cele asimetrice sisteme cu chei publice. Acestea din urmă sunt mai lente şi impun folosirea unor mecanisme de distribuție sigură a cheilor.

Lungimea cheii de criptare variază şi depinde de nivelul de securitate dorit. Aceasta poate fi de exemplu de 40, 64 sau 128 de biți. Deşi creşterea lungimii cheii de criptare reduce şansele de atac brut, aceasta poate fi făcută numai în condițiile creşterii performanțelor procesoarelor (ca număr de operații pe secundă) pentru a nu întârzia transmisia.

Algoritmii matematici de criptare sunt şi ei diferiți ca nivel de robustețe la atacurile criptografice (DES, 3DES, IDEA, RC4, RSA, AES etc). Oricum, în timp, algoritmii de criptare sunt tot mai mult analizați, tot mai multe vulnerabilități ale lor sunt depistate şi variate modalități de atac asupra lor sunt găsite. Optimizarea acestor algoritmi şi proiectarea altora noi este esențială pentru eficiența operației de criptare a datelor.

DES (*Data Encryption Standard*) reprezintă un cifru bloc, cu cheie simetrică, care prin utilizarea unor operații simple de permutare şi substituție, criptează un bloc de 64 de biți, cu ajutorul unei chei tot de 64 de biți. Algoritmul de criptare diferă de cel de decriptare prin utilizarea în ordine inversă a subcheilor. Lungimea mult prea scurtă a cheii de criptare

DES îl face vulnerabil în fața atacului, ceea ce a dus la folosirea din ce în ce mai puțin a acestuia.

3DES (*Triple DES*) reprezintă varianta îmbunătățită a algoritmului DES simplu, prin creşterea domeniului cheii. Acesta aplică de trei ori algoritmul DES (cu 2 sau 3 chei distincte) ceea ce îl face mult prea lent în comparație cu alți algoritmi simetrici.

RSA (*Rivest, Shamir, Adleman*) este cel mai utilizat standard pentru criptare şi semnare care foloseşte chei publice. Securitatea algoritmului are la bază dificultatea factorizării numerelor foarte mari. În principal RSA este utilizat pentru generarea semnăturilor digitale şi criptarea unor volume mici de date deoarece este destul de lent.

IDEA (*International Data Encryption Algorithm*) este un cifru bloc simetric utilizat pentru criptarea unui bloc de date de lungime 64 de biți cu ajutorul unei chei de 128 de biți. În prezent, este considerat ca fiind unul dintre cei mai rapizi şi mai siguri algoritmi. Decriptarea se face identic ca în procesul de criptare, cu diferența utilizării unui set diferit de chei, determinat din cele utilizate la criptare.

Blowfish este un cifru bloc simetric, cu ajutorul căruia pot fi criptate/decriptate blocuri de date de 64 de biți cu ajutorul unei chei de lungime variabilă. Este un algoritm rapid, imposibil de spart în varianta de aplicare în 16 paşi. Poate înlocui DES şi IDEA. Decriptorul utilizează aceleaşi operații ca şi algoritmul de criptare însă subcheile se aplică în ordine inversa.

AES (*Advanced Encryption Standard*) este un algoritm simetric utilizat pentru criptarea unui bloc de date de lungime 128, 192 sau 256 de biți cu ajutorul unei chei cu aceeaşi lungime. Este un algoritm rapid şi uşor de implementat. Este standardul actual cu chei simetrice. Algoritmul de

decriptare AES presupune inversarea funcţiilor utilizate la criptare şi aplicarea acestora în ordine inversă.

Modalităţile de generare, transmitere şi gestionare a cheilor de criptare afectează securitatea datelor stocate sau transferate în reţea. Neutilizarea cheilor de criptare slabe sau compromise constituie o sarcină importantă a sistemului de gestionare a cheilor. Mecanismul Kerberos este indicat pentru distribuţia sigură a cheilor de criptare.

Schimbarea periodică automată a cheii de criptare reduce riscul deducerii acesteia din secvenţa de date transmisă.

Un alt serviciu de securitate, **integritatea informaţiilor,** se referă la acele metode de securitate care trebuie implementate pentru a se evita modificarea sau ştergerea fără autorizaţie a informaţiilor. Printre metodele care pot asigura integritatea datelor se numără: tehnica hash, semnăturile digitale, certificatul digital şi marcarea informaţiilor.

Tehnica hash presupune utilizarea unei funcţii de transformare prin care se obţine un cod unic de identificare a datelor. Dacă informaţiile transmise sunt modificate în timpul transmisiei, acest cod unic nu se va mai potrivi la recepţie.

Semnăturile digitale sunt o modalitate prin care se poate demonstra autenticitatea originii unui mesaj dar şi verificarea integrităţii acestuia. De asemenea, semnăturile digitale asigură non-repudierea mesajelor transmise sau a serviciilor de reţea folosite. Semnăturile digitale se realizează prin tehnici de criptare asimetrică. Ele se realizează cu ajutorul cheii private şi sunt verificate la recepţie cu ajutorul cheii publice. Există numeroşi algoritmi pentru generarea semnăturilor digitale, dintre care cel mai utilizat este RSA.

Certificatele digitale asigură autenticitatea cheilor publice de criptare. Certificatele sunt emise de către o autoritate de certificare. Aceasta trebuie să se bucure de încrederea mutuală a entităților care comunică.

Marcarea unui mesaj se realizează fie prin semnarea digitală a mesajului, fie prin atașarea unei informații specifice pentru protecția drepturilor autorului.

O rețea de comunicații poate fi **vulnerabilă la atacuri** atât din punct de vedere hardware (atacul la integritatea fizică), cât şi software (posibilitatea folosirii neautorizate a informațiilor). Printre cele mai importante categorii de atacuri se numără: atacurile locale şi cele de la distanță, atacurile pasive şi cele active.

Atacurile locale pot fi evitate prin distribuirea selectivă a drepturilor utilizatorilor în rețea, precum şi educarea corespunzătoare a acestora. I

În cazul **atacurilor de la distanță** este dificilă localizarea şi identificarea atacatorilor. Pentru evitarea atacurilor de la distanță, pentru realizarea controlului comunicației dintre o rețea publică şi una privată, se poate utiliza un *firewall*. VPN-urile reprezintă rețele virtuale private care asigură comunicarea în mod sigur prin intermediul unei rețele publice nesigure. Acestea două (firewall-ul şi VPN-urile) au în comun faptul că delimitează o zonă de apărare în care accesul este restricționat.

Atacurile pasive sunt doar atacuri de intercepție. Atacatorul nu modifică în nici un fel informațiile transferate în rețea dar le poate folosi în alte scopuri şi de aceea este necesară prevenirea ți contracararea lor.

În schimb, **atacurile active** determină modificarea, deteriorarea sau întârzierea informațiilor transferate prin intermediul rețelelor de comunicații.

Toate aceste tipuri de atacuri, pot fi evitate prin implementarea unor tehnici de securitate corespunzătoare, pe baza unor politici de securitate a rețelelor bine definite.

O categorie aparte o constituie **atacurile criptografice** care acționează asupra criptosistemelor, prin care se urmăreşte determinarea cheilor pentru decriptare sau obținerea mesajelor în clar. Cel mai cunoscut atac criptografic este atacul brut, care constă în testarea tuturor cheilor posibile pentru determinarea celei corecte.

Prin implementarea unor **tehnici de securitate** adecvate într-o rețea de comunicații se pot evita intercepția, accesarea şi falsificarea informațiilor în mod neautorizat. Cerințele de rapiditate şi funcționalitate ale rețelei afectează de multe ori deciziile privind securitatea în detrimentul protecției datelor. Neactivarea opțiunilor de securizare (WEP, WPA, WPA2, WPA-PSK) conduce la creşterea vitezei de transmisie dar permite preluarea neautorizată a informațiilor.

O metodă de reducere a interferențelor dintre canale şi de creştere a securității comunicației o reprezintă extensia spectrului semnalului transmis, de exemplu cu salturi de frecvență (FHSS) sau cu secvență directă (DSSS), pe baza unei secvențe binare pseudoaleatoare. Necunoaşterea acestei secvențe împiedică detecția semnalului util şi preluarea informației transmise.

O metodă de atac asupra rețelelor este şi cea de perturbare a comunicațiilor radio (*electronic warfare*), de exemplu prin bruiaj, cu scopul întreruperii totale a acestora. Sunt trei categorii de măsuri de protecție față de perturbațiile specifice comunicațiilor radio:

1. ECM (*Electronic Counter Measure*) pentru a opri folosirea neautorizată a unei benzi de transmisie;

2. ESM (*Electronic Support Measure*) pentru intercepția, identificarea, analiza şi localizarea atacatorilor;
3. ECCM (*Electronic Counter - Countermeasure*) pentru planificarea şi proiectarea corespunzătoare a rețelei, respectiv a serviciilor de securitate, în vederea preîntâmpinării atacurilor asupra ei.

În prima categorie, ECM, sunt incluse metodele de protecție antibruiaj, care pot folosi fie tehnici de extensie a spectrului, fie filtre adaptate pentru maximizarea raportului de puteri semnal-zgomot de bruiaj.

Ca măsuri de tip ECCM putem considera alegerea unei benzi de frecvențe licențiate, cu frecvențe mai mari pentru care analizoarele de spectru şi alte echipamente să aibă costuri suficient de mari pentru a fi inaccesibile marii majorități a hackerilor, protecția zonei de acoperire a rețelei WLAN la interferențe radio cu ecrane adecvate, de exemplu ecrane din aluminiu plasate în imediata vecinătate a unui AP pentru a creşte raportul radiațiilor față-spate şi pentru a reduce şansele celor din exterior de a intercepta (*eavesdropping*) sau de a perturba transmisia. Utilizarea antenelor directive în locul celor omnidirecționale reprezintă o soluție de restrângere a ariei în care traficul de date prin unde radio poate fi interceptat.

Prin combinarea diverselor metode de securizare a comunicațiilor (autentificare, criptare, extensie de spectru) din rețelele Wi-Fi simple sau mixte (Wi-Fi şi cablate) se asigură creşterea gradului de securitate.

În standardul IEEE 802.11n adresat sistemelor MIMO (*Multiple Input Multiple Output*) de Internet mobil, în care gradul de utilizare a serviciului de *roaming* este deosebit de mare, trebuie prevăzute măsuri adecvate şi performante de reducere a riscurilor de securitate.

Măsurile de securitate se pot aplica pe toate nivelele suitelor de protocoale folosite (în particular, TCP/IP) fiind indicată folosirea protocoalelor de securitate precum TLS (*Transport Layer Security*), SSL (*Secure Socket Layer*), HTTPS (*HyperText Transfer Protocol Secure*), IPsec (*IP security*) pentru a împiedica preluarea pachetelor şi a informațiilor secrete sau confidențiale transmise prin rețeaua publică. Serviciile oferite prin intermediul paginilor web folosind protocolul HTTPS sunt mai sigure deoarece folosesc un alt port pentru conexiunea realizată prin TCP (443) şi introduc operații de criptare între nivelul de aplicație pe care lucrează protocolul HTTP şi cel de transport corespunzător protocolului TCP.

În concluzie, putem afirma că utilizarea măsurilor de securitate este destul de costisitoare ca preț şi resurse astfel încât aplicarea lor se justifică pentru informațiile care necesită cu adevărat protecție (date de identificare, parole, informații de configurare, date confidențiale, informații cu caracter secret „mission-critical data”).

II.2 ANALIZA SECURITĂȚII REȚELEI

Analiza securității datelor într-o rețea presupune în primul rând identificarea cerințelor de funcționare pentru acea rețea, apoi identificarea tuturor amenințărilor posibile (împotriva cărora este necesară protecția). Această analiză constă în principal în trei sub-etape:

- analiza vulnerabilităților - identificarea elementelor potențial slabe ale rețelei

- evaluarea amenințărilor - determinarea problemelor care pot apărea datorită elementelor slabe ale rețelei şi modurile în care aceste probleme interferă cu cerințele de funcționare
- analiza riscurilor - posibilele consecințe pe care breşele de securitate le pot crea, gradul de admisibilitate a lor.

Următoarea etapă constă în definirea politicii de securitate, ceea ce înseamnă să se decidă:

- care amenințări trebuie eliminate şi care se pot tolera
- care resurse trebuie protejate şi la ce nivel
- cu ce mijloace poate fi implementată securitatea
- care este prețul (financiar, uman, social etc.) măsurilor de securitate care poate fi acceptat.

Odată stabilite obiectivele politicii de securitate, următoarea etapă constă în selecția serviciilor de securitate – funcțiile individuale care sporesc securitatea rețelei. Fiecare serviciu poate fi implementat prin metode (mecanisme de securitate) variate pentru implementarea cărora este nevoie de aşa-numitele funcții de gestiune a securității. Gestiunea securității într-o rețea constă în controlul şi distribuția sigură a informațiilor către toate sistemele deschise ce compun rețeaua, în scopul utilizării serviciilor şi mecanismelor de securitate şi al raportării evenimentelor de securitate ce pot apărea către administratorii de rețea.

II.3 MODELE DE SECURITATE

O rețea de calculatoare este un sistem complex cu mulți utilizatori, cu drepturi diferite de utilizare a resurselor, iar securitatea acesteia trebuie asigurată modular, pe mai multe nivele: fizic, logic şi informațional.

Modelul de securitate centrat pe informație sau pe subiect are mai multe straturi care reprezintă **nivelele de securitate** (figura II.1)**.** Acestea oferă protecție subiectului ce trebuie securizat. Fiecare nivel izolează subiectul şi îl face mai dificil de accesat în alt mod decât cel în care a fost prevăzut. Acest model este denumit sugestiv în literatura de specialitate "modelul ceapă" (*onion model*). Fiecare nivel sau strat oferă un plus de securitate informației cu caracter secret.

Nivelele de securitate din acest model au următoarele semnificații:

SF - Securitatea fizică;

SLA - Securitatea logică a accesului;

SLS - Securitatea logică a serviciilor;

SI - Secretizarea informației;

II - Integritatea informației.

Un sistem de securitate funcțional trebuie să asigure accesul la resurse prin verificarea drepturilor de acces pe toate aceste nivele, fără posibilități de evitare a lor.

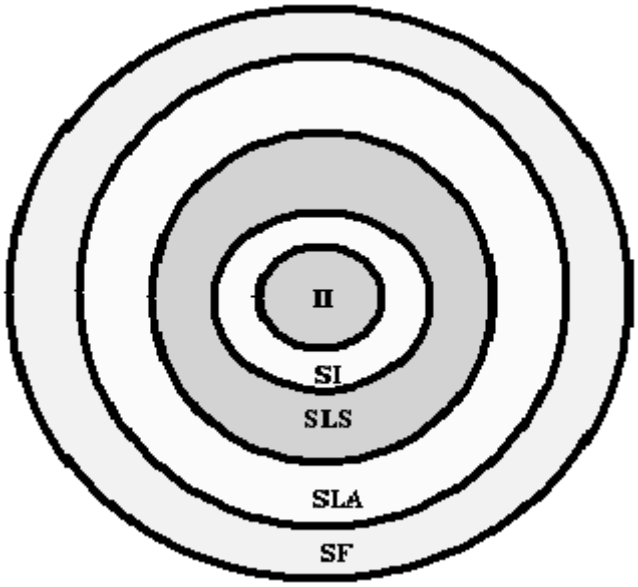

Figura II.1 Modelul stratificat de securitate

Modelul de securitate stratificat se pretează cel mai bine într-un anumit nod de rețea. Dar procesele de comunicație implică două sau mai multe noduri de rețea precum şi căile de transmisie dintre acestea. Prin urmare, securitatea trebuie urmărită în fiecare nod al rețelei dar şi pe fiecare cale sau flux de comunicație (flow) din rețea.

Pentru modelarea serviciilor de securitate din sistemele informatice, se foloseşte şi modelul distribuit de securitate, de tip „arbore” (Figura II.2).

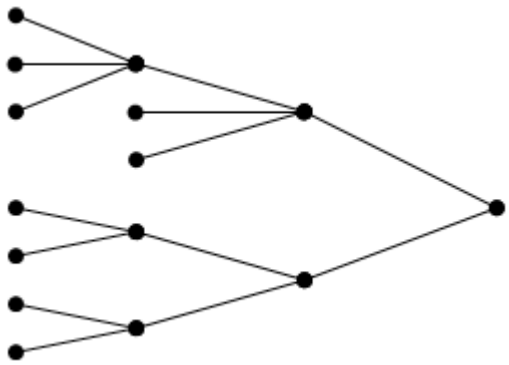

Figura II.2 Model de securitate arborescent

Modelul de securitate de tip „arbore” trebuie aplicat în cazul în care se accesează resurse distribuite pe mai multe servere din rețea. Informațiile sunt transferate de la nodul-sursă la nodul-destinație prin intermediul mai multor noduri de rețea şi pe diverse căi fizice de comunicație, „cu sau fără fir”. Gradul de securitate oferit unui proces de transfer de date în rețea va fi dat de cel mai „slab” segment al căii de transfer (nod sau canal de comunicație). De aceea, pentru reducerea riscurilor de securitate din rețea, este necesară securizarea tuturor segmentelor implicate în procesul de comunicație la gradul de securitate dorit pentru fiecare mesaj.

Clientul este reprezentat ca nod-rădăcină în diagrama de mai sus, serverele ca noduri-terminale, iar echipamentele de comunicație din rețea ca şi noduri intermediare. În fiecare nod se poate aplica primul model de securitate centrat pe subiect. Conexiunile dintre noduri sunt căile fizice de comunicație, de tip radio sau cablate. În cazul rețelelor cu topologie redundantă, de tip „plasă” (mesh) este dificil de identificat „arborele” de

comunicație dar acesta poate fi impus prin decizii de rutare strictă pe o anumită cale din rețea.

Pentru rutarea unui pachet cu un anumit grad de securitate specificat este necesară definirea unei metrici de securitate care să poată fi aplicată în graful rețelei. Spre deosebire de metricile uzuale folosite de algoritmii de rutare, metrica vizând securitatea trebuie să includă şi nivelul de securitate oferit de nodurile care delimitează un arc din graf. De asemenea, este utilă folosirea grafurilor orientate şi reprezentarea separată a căilor de transmisie de tip up-link şi down-link dintre două noduri de rețea, în cazul comunicațiilor asimetrice, cu medii şi tehnologii diferite de transmisie. Metrica de securitate se va stabili pe baza riscului de securitate pe care îl prezintă un anumit element din graful rețelei. Decizia privind ruta optimă din punct de vedere al securității transmisiei va viza reducerea riscului de securitate la nivelul impus de costurile maxim admise. Gradul de securitate al unui pachet poate fi exprimat prin biții opționali de securitate incluşi în antetul pachetului.

Modelul de securitate arborescent este deosebit de util pentru analiza atacurilor distribuite lansate în rețea din şi spre mai multe noduri, pentru a fi mai greu de identificat atacatorul şi pentru a creşte eficiența de atac.

Monitorizarea proceselor de comunicație şi a evenimentelor de securitate, simultan cu clasificarea şi ierarhizarea lor pe mai multe grade de risc pe principiul sistemelor fuzzy, permite stabilirea unei strategii de securitate optime şi aplicarea unor măsuri eficiente de contraatac folosind modelul arborescent de securitate.

În domeniul rețelelor de comunicații, s-au propus diverse modele securitate de către firmele producătoare de echipamente şi de programe

software, pentru diferite domenii de aplicabilitate care necesită protecția informațiilor cu caracter privat sau confidențial (în domeniul sănătății populației HIPAA - *Health Insurance Portability and Accountability Act*, în domeniul financiar-bancar şi de asigurări GLBA - *Gramm-Leach-Bliley Act*, precum şi în cel al plăților prin intermediul cardurilor bancare PCI DSS - *Payment Card Industry Data Security Standard* şi altele).

II.4 SECURITATEA FIZICĂ

Securitatea fizică (IRL - *in real life security*) trebuie să constituie obiectul unei analize atente în cazul rețelelor de comunicații. Aceasta cuprinde atât securitatea mediului de transmisie, cât şi a tuturor echipamentelor din rețea.

Securitatea fizică reprezintă nivelul exterior al modelului de securitate şi constă, în general, în protecția "sub cheie" a echipamentelor informatice într-un birou sau într-o altă incintă precum şi asigurarea pazei şi a controlului accesului.

Conform statisticilor 80 % din atacuri pornesc din interiorul rețelei.

Este foarte dificil să se obțină o schemă completă a tuturor entităților şi operațiilor active la un moment dat în rețea, deoarece acestea sunt sisteme complexe, cu un număr foarte mare de echipamente, în particular calculatoare (uneori de ordinul sutelor de mii sau milioanelor la nivel macro), şi cu numeroase linii de legătură. Din această cauză, rețelele de comunicații sunt aproape imposibil de administrat manual în mod eficient, ele devenind vulnerabile la diferite atacuri externe, dar şi interne.

Această complexitate este generată de:

- dispersarea geografică, uneori intercontinentală a componentelor rețelei;
- implicarea mai multor organizații în administrarea unei singure rețele;
- existența unor tipuri diferite de echipamente şi sisteme de operare;
- existența unui număr foarte mare de entități în rețea.

Personalul care se ocupă de administrarea rețelei trebuie să asigure şi să respecte măsurile de bună funcționare şi securitate fizică prevăzute de politica de securitate a rețelei:

- cablurile şi echipamentele distribuite din rețea trebuie să fie protejate prin montarea acestora pe perete, în locuri cu trafic redus pentru a se evita defectarea lor accidentală sau intenționată;
- serverele de rețea trebuie protejate de accesul fizic neautorizat al unor persoane, prin amplasarea acestora în incinte închise, cu acces restricționat;
- echipamentele din rețea trebuie protejate de anumite perturbații de tensiune din rețeaua de alimentare cu energie electrică, folosind surse de energie electrică neîntreruptibile (UPS - *Uninterruptible Power Supply*), care trebuie să asigure funcționarea neîntreruptă a celor mai importante echipamente din rețea;
- accesul fizic la componentele critice din rețea trebuie securizat folosind dispozitive cu chei, carduri sau coduri de acces, senzori de mişcare, de identificare biometrică (amprente digitale, semnatură, voce, forma mâinii, imaginea retinei sau a feței etc.);

Tehnicile de identificare biometrică sunt relativ scumpe în comparație cu cele clasice şi deseori incomode sau neplăcute la utilizare, dar se dovedesc a fi cele mai eficiente pentru securizarea accesului fizic la rețea.

Securitatea fizică poate fi asigurată prin:

- amenajarea adecvată a spațiului rețelei astfel încât să fie descurajate eventualele tentative de intruziune (IPS – *Intrusion Prevention System*);
- restricționarea, controlul şi monitorizarea video a accesului fizic;
- detectarea intruşilor (IDS – *Intrusion Detection System*) din spațiile nesupravegheate cu ajutorul sistemelor automate de alarmare (RAI – *Remote Alarm Indicator*).

Măsurile de securitate fizică a rețelei se stabilesc pe baza analizei riscurilor şi vulnerabilităților de securitate ale rețelei, pe baza politicii de securitate adoptate şi se implementează de către grupul de administrare folosind diferite produse software şi hardware.

II.5 SECURITATEA LOGICĂ

Securitatea logică se referă la protecția accesului logic la resursele şi serviciile de rețea. Aceasta se realizează prin metode şi facilități software care asigură controlul drepturilor de acces şi utilizare.

Se disting două mari nivele de securitate logică, fiecare cu mai multe subnivele:

- **securitatea logică a accesului** (SLA) care include: accesul la sistem/rețea, la contul de utilizator şi la documente (fişiere).

- **securitatea logică a serviciilor** (SLS) care cuprinde accesul la serviciile de sistem/rețea pe baza listelor de aşteptare, intrare/ieşire de pe disc, controlul şi gestionarea serviciilor (management).

Controlul serviciilor (CS) monitorizează şi raportează starea serviciilor, activează sau dezactivează serviciile oferite de sistem şi de rețea. Drepturile la servicii (DS) stabilesc cine şi cum foloseşte un anumit serviciu.

II.5.1 SECURITATEA LOGICĂ A ACCESULUI

În orice rețea de calculatoare, sistemul de securitate trebuie să determine care sunt persoanele autorizate, vizitatorii sau categoriile de utilizatori indezirabili, neautorizate.

De regulă, identificarea, autentificarea şi autorizarea persoanelor cu drept de acces se realizează prin intermediul numelor şi al parolelor de utilizator.

Parolele sunt utilizate pentru a se permite accesul la calculatoarele din rețea, fie ca utilizatori, fie în grupuri de utilizatori.

Sistemul parolelor, oricât de complex, nu oferă un nivel de securitate suficient, acesta depinzând în mod esențial de modul de păstrare a caracterului lor secret.

De cele mai multe ori, utilizatorii îşi aleg parole cu un număr mic de caractere, redundante şi cu o anumită semnificație care să le permită memorarea uşoară a acestora (nume, date importante, numere de maşină etc.) toate fiind vulnerabile în fața unor spărgători calificați care dețin deja unele informații private. Programele actuale de baleiere a seturilor de

caractere pentru atacul brut de deducere a parolei sau a codului de acces sunt destul de performante.

O greşeală comună a celor mai puțin avizați o reprezintă păstrarea parolelor sub formă scrisă, pe hârtie sau în documente electronice, de teama de a nu fi uitate.

Creşterea securității logice accesului la conturile de utilizator este posibilă prin folosirea unor parole sub forma unor combinații de caractere aleatoare, relativ lungi, schimbate periodic, accesibile doar persoanelor autorizate şi de încredere. În cazul sistemelor care vehiculează informații cu caracter secret (confidențiale sau private), parolele sunt atribuite de persoanele responsabile de securitatea sistemului, în particular, administratorul de rețea.

Având în vedere importanța parolelor în sistemul de securitate al rețelei, se impune respectarea unor reguli de alegere, gestionare şi păstrare a parolelor, stabilite în cadrul politicii de securitate:

1. Parolele sunt şiruri de caractere alfanumerice – cifre, litere mari şi mici, alte caractere, ordonate aleator. Pentru o parolă de 4 caractere trebuie încercate circa 256000 de combinații dar sistemele actuale sunt suficient de performante pentru a o deduce în doar câteva minute. Combinațiile scurte de caractere sunt vulnerabile față de “profesioniști”. Se impune alegerea unei combinații cât mai lungi, de tip “passphrase” față de care atacul brut să devină ineficient. La o astfel de combinație apare problema memorării sau a transferului ei în condiții de siguranță.
2. Parolele trebuie să fie schimbate periodic, măcar o dată la 6 luni, dar pentru informațiile deosebit de importante se impun termene şi mai scurte.

3. Parolele comune trebuie înlocuite imediat ce o persoană părăseşte un grup. De aceea este indicat ca includerea unei persoane într-un grup să se facă abia după ce s-a dovedit a fi de încredere şi stabilă.
4. Parolele trebuie să fie schimbate imediat ce apar unele bănuieli privind cunoaşterea lor de persoane neautorizate sau atunci când, din anumite motive, secretul lor a trebuit să fie dezvăluit pentru redresarea unei stari de urgenta.
5. Parolele trebuie să fie ținute minte şi nu scrise, cu excepția celor pentru situații de urgență. Fiecare parolă scrisă se păstrează într-un plic sigilat pe care sunt înscrise detalii privind echipamentul la care poate fi folosită şi numele celor autorizați să o folosească. După ruperea sigiliului, pe plic vor fi scrise data şi numele celor care au aflat parola. Plicurile cu parole se păstrează în condiții de siguranță, de către persoana responsabilă de securitatea rețelei.
6. Dacă parolele-duplicat se păstrează stocate pe calculator, astfel de fişiere trebuie să fie protejate împotriva accesului neautorizat şi create copii de siguranță. Listele cu parole pot fi memorate în formă criptată.
7. Parolele nu trebuie afişate pe echipamentele din configurația sistemului, iar la introducerea acestora de la tastatură nu trebuie să se afle persoane străine în preajmă.
8. Pentru blocarea operațiunilor de găsire a parolelor şi a codurilor de acces prin încercări repetate, de ordinul miilor, echipamentul de rețea trebuie să permită un număr limitat de încercări de introducere a acestora, uzual trei, urmat de perioade de refuz al accesului. Dacă limita a fost depăşită de către utilizator, intenția trebuie raportată administratorului de rețea, însoțită de un semnal sonor specific de

avertizare. Acesta trebuie să blocheze terminalul de la care s-au efectuat prea multe încercări eşuate şi de asemenea tot el îl va repune în funcțiune. În cazul sistemelor speciale, se recomandă şi supravegherea sălii sau a locului de unde s-a încercat accesarea prin parole eronate repetate, pentru identificarea persoanei respective.

9. Odată ce au pătruns în sistem, utilizatorilor nu trebuie să li se permită schimbarea identității cu care au efectuat deschiderea sesiunii şi nici să acceseze documente sau resurse alocate altor utilizatori. În rețelele cu un număr foarte mare de utilizatori se recomandă folosirea unor programe software pentru securizare, cu control automat al accesului în rețea, fără intervenția explicită a administratorului.
10. Dacă un terminal funcționează o perioadă lungă de timp, procesul de autentificare trebuie reluat la intervale regulate de timp pentru a se asigura că nu foloseşte altcineva sistemul. Dacă terminalul rămâne neutilizat, dar deschis şi nesupravegheat, acesta trebuie să se "încuie" (*lock*) automat după un anumit interval de timp, pentru a evita folosirea unui cont autorizat de acces de către persoane rău intenționate.
11. La deschiderea unei noi sesiuni de lucru, utilizatorului trebuie să i se aducă la cunostință când a fost accesat ultima dată sistemul cu parola respectivă, pentru a observa dacă altcineva a folosit-o între timp.
12. În cazul accesării unor resurse informaționale deosebit de importante, precum baze de date, fişiere de configurare, servere, fişiere din sistemul de operare, liste cu parole, etc. se impune **controlul dual al parolei** iar cele două persoane responsabile

trebuie să fie conştiente de riscurile şi consecințele declanşării unor operațiuni împotriva rețelei.

II.5.2 SECURITATEA LOGICĂ A SERVICIILOR

După realizarea identificării sau ”legitimării” persoanei, în urma căreia se obține accesul fizic la resursele rețelei, se realizează introducerea parolei fie direct de la tastatură, fie prin introducerea într-un echipament special a unui document care să conțină parola (de exemplu, un cititor de card), obținându-se astfel şi accesul logic la resursele rețelei.

Serverul de autentificare verifică parola pe baza unei liste pentru controlul accesului stocate într-o bază de date locală sau „la distanță”. Pe baza numelui şi parolei, utilizatorului i se permite accesul şi i se garantează respectarea privilegiilor predefinite la anumite resurse ale sistemului, cum ar fi:

- **Drept de execuție** - prin care poate lansa în execuție un program, dar nu i se permite să modifice structura acestuia;
- **Drept de citire** - prin care poate citi un fişier, dar nu îi este permisă nici o altă operațiune;
- **Drept de scriere** - prin care i se oferă posibilitatea de scriere a datelor în fişierul deschis, dar i se interzic alte operațiuni;
- **Drept de citire / scriere** - prin care poate citi fişierul şi i se oferă şi posibilitatea de scriere în el;
- **Drept de ştergere** - prin care utilizatorul poate efectua ştergerea unor date din fişiere.

Sistemele de operare actuale oferă metode de administrare a drepturilor de acces al fişierelor pentru anumiți utilizatori sau grupuri de utilizatori. Aceste sisteme au capacitatea de a controla operațiile ce pot fi realizate asupra fişierelor din sistem.

Pentru ilustrarea modului în care se pot realiza limitările la serviciile şi resursele unui sistem, se consideră drept exemplu, sistemul de operare UNIX, în care **permisiunile de acces** sunt exprimate printr-o secvență de 10 caractere formată din:

- primul caracter ilustrează tipul fişierului (”-” pentru fişier obişnuit, ”d” pentru director, ”l” pentru un link etc.);
- trei grupuri de câte trei caractere fiecare: primul grup specifică operațiile permise ”proprietarului” resursei (*owner*), cel de-al doilea triplet se referă la drepturile acordate grupului de utilizatori (*group*), iar cel de-al treilea exprimă permisiunile celorlalți utilizatori (*others*), alții decât proprietarul şi grupul căruia îi aparține acesta.

  Fiecare grup de 3 caractere are următoarea semnificație:
- primul caracter exprimă dreptul sau interdicția de citire (”r” - *read*);
- cel de al doilea caracter exprimă dreptul sau interdicția de scriere (”w” - *write*);
- cel de-al treilea caracter exprimă dreptul sau interdicția de execuție (”x” - *execute*).

Exemplu: Secvența - rwxr-xr-- înseamnă că pentru un fişier obişnuit ”proprietarul” poate realiza toate tipurile de operații, în timp ce cei din grupul său pot citi sau lansa în execuție fişierul, restul utilizatorilor fiindu-le permisă numai operația de citire.

Secvența de exprimare a drepturilor de utilizatori poate fi echivalată cu o valoare numerică octală, corespunzătoare unei secvențe de 9 biți.

Fiecare bit are semnificația corespunzătoare poziției sale, conform regulilor de mai sus, valoarea „1” exprimă dreptul de operare iar „0” interdicția de efectuare a acelei operații.

Exemplu: Dacă se exprimă în binar secvența de drepturi din exemplul anterior, se obține şirul de biți 111101100 şi secvența octală 754.

Pe tot parcursul accesării rețelei, trebuie monitorizat accesul la servicii şi resurse informaționale pentru a depista eventualele tentative sau evenimente de fraudă, prin „depăşirea” restricțiilor impuse de către utilizatorii autorizați ai rețelei. Pentru un număr mare de utilizatori activi la un anumit moment în rețea, este necesară utilizarea unor programe de securitate cu facilități de monitorizare automată a accesului la servicii şi resurse, precum şi de soluționare automată a evenimentelor de securitate, prin punerea în carantină a anumitor utilizatori şi/sau echipamente cu risc crescut, urmată eventual de restricționarea accesului şi chiar excluderea acestora din rețea. Restricțiile pot fi impuse pe diferite criterii:

- adrese de rețea
- adrese MAC
- porturi logice
- nume de utilizatori
- temporale (anumite zile şi ore)
- ierarhice, conform funcției fiecărui utilizator.

Drepturile utilizatorilor şi grupurilor de utilizatori, restricțiile care trebuie impuse şi criteriile de stabilire a acestora sunt incluse în politica de securitate a rețelei.

II.6 SECURITATEA INFORMAȚIILOR

Secretul transmisiei, confidențialitatea mesajelor şi autentificarea surselor de informație se asigură prin diverşi algoritmi de criptare a datelor.

Criptografia reprezintă o ramură a matematicii, care se ocupă cu securizarea informației, precum şi cu autentificarea şi restricționarea accesului într-un sistem informatic. În realizarea acestora se utilizează metode matematice, bazate de exemplu pe dificultatea factorizării numerelor foarte mari.

Criptarea (*encryption*) reprezintă procesul de conversie a informației obişnuite (text în clar - *plaintext* - M) într-un text neinteligibil (text cifrat - *ciphertext* - C), cu ajutorul unei chei de criptare, K_E:

$$C = E_{K_E}(M)$$

Decriptarea (*decryption*) este inversul criptării, adică, trecerea de la textul cifrat, neinteligibil, la textul original, cu ajutorul unei chei, K_D.

$$M = D_{K_D}(C)$$

Modul de operare detaliat al unui criptosistem este controlat de algoritmii folosiți pentru criptare şi pentru decriptare precum şi de secvențele-cheie.

Termenul „cheie” se referă la informația necesară pentru a cripta sau a decripta datele. Securitatea unei chei este deseori discutată în termeni de lungime sau de număr de biți ai acesteia, dar nu mărimea cheii este singura garanție a robusteții sistemului de securitate a rețelei.

Există două categorii de tehnici de criptare, definite în funcție de tipul de cheie utilizat:

- criptarea cu cheie secretă;

- criptarea cu cheie publică.

Criptosistemele mixte, care utilizează mai multe chei de transmisie, de exemplu una secretă şi alta publică, se dovedesc a fi superioare ca performanțe celor cu cheie unică.

Criptosistemele cu spectru extins care se utilizează pentru comunicații de bandă largă (*broadband communications*), în sisteme radio terestre sau prin satelit, respectiv pe fibră optică, folosesc secvențe-cheie pseudoaleatoare, care prin periodicitatea lor sunt vulnerabile în fața atacurilor statistice.

Se cunosc numeroase tehnici de criptare bazate pe algebră (Laplace), topologie matematică şi geometrie (Poincaré) sau combinatorică. Multe dintre acestea utilizează sisteme liniare, relativ uşor predictibile.

Algoritmii de criptare utilizați în prezent (DES, 3DES, RSA, MD4, MD5, SHA-1) sunt relativ robuşti față de diverse metode de atac dar devin vulnerabili din cauza lungimii finite a cheilor de criptare şi prin faptul că au fost studiați în detaliu de mult timp. De aceea, se dezvoltă noi algoritmi de criptare a datelor mai performanți, cu timp redus de procesare şi diversitate mare a cheilor de criptare, bazați pe noi teorii matematice şi fizice (criptografie cuantică, criptografie haotică). Metodele bazate pe teoria haosului pot fi aplicate cu succes pentru secretizarea transmisiei (vezi sistemul lui Baptista, simplu sau modificat) şi pot fi aplicate şi în spații multidimensionale (ca în cazul imaginilor digitale 2D şi 3D, respectiv pentru transmisii simultane de date-voce, audio-video etc).

Principiul criptografiei bazate pe teoria haosului este dat de difuzia şi confuzia parametrilor traiectoriilor generate pe baza cheii de criptare şi a mesajului transmis. La mici variații ale cheii de transmisie trebuie să apară modificări extreme ale traiectoriei din spațiul fazelor pentru sistemul

dinamic utilizat. Astfel se asigură rezistența criptosistemului față de atacurile brute bazate pe încercarea tuturor cheilor posibile de transmisie.

Traiectoriile haotice nu sunt nici periodice, nici cvasiperiodice, şi au un aspect aleator, cu un spectru de putere de tip 'zgomot alb' (de bandă largă).

Nici un calculator şi nici un program software nu poate prezice traiectoria unui sistem dinamic haotic deoarece complexitatea algoritmică a traiectoriilor este pozitivă, fiind dată de entropia K-S (Kotulski-Szczepanski) a sistemului. Pe acest fapt se bazează ideea proiectării unor tehnici eficiente de criptare a datelor pe baza teoriei haosului astfel încât entropia sistemului să crească prin codare şi să depăşească limitele capacității computaționale a criptanalistului.

Criptosistemele bazate pe haos utilizează sisteme dinamice discrete, descrise de ecuații funcționale de stare în care se utilizează o funcție ***f*** de 'dinamică a sistemului', liniară sau neliniară, extrem de sensibilă la condițiile inițiale care determină în mod unic evoluția stărilor criptosistemului şi permite decodarea necatastrofică a secvenței codate.

x[n+1] = ***f***(x[n], n) (n - variabila discretă de timp).

Se preferă utilizarea sistemelor dinamice neliniare care pot avea în regim permanent mai multe mulțimi limită, cu bazine de atracție diferite, dependente într-un mod foarte sensitiv de condiția inițială, astfel încât devine imposibilă predicția pe termen lung a stării acestora.

Pentru generarea cheilor de criptare se poate folosi funcția logistică neliniară următoare:

$$x_{k+1} = Rx_k(1-x_k), k = 0,1,2..., x_k \in (0,1),\ R \in (0,\ 4), x_0 \neq 0.$$

Se pot utiliza si alte funcții logistice neliniare (triunghiulare simetrice sau în formă de „dinți de fierăstrău”, exponențiale sau logaritmice).

Cheia de transmisie, introdusă de exemplu ca parolă de utilizator cu lungime neimpusă, este utilizată pentru inițializarea sistemului haotic care generează cheia de criptare pe toată durata transmisiei.

Reducerea lungimii cheii de transmisie determină creşterea redundanței secvenței criptate şi a riscului de deducere a ei de către criptanalist.

Pentru reducerea şanselor atacurilor criptografice, lungimea cheii de criptare trebuie să fie comparabilă cu cea a mesajului.

II.6.1 CRIPTAREA CU CHEIE SECRETĂ

Criptosistemele convenționale au fost concepute pe principiul cheii secrete, cu o funcție de criptare inversabilă cunoscută doar de utilizatori. Cheia secretă constituie punctul vulnerabil al sistemului deoarece odată aflată, securitatea tuturor informațiilor transmise este compromisă. Decriptorul aplică funcția inversă pentru deducerea secvenței originale, folosind aceeaşi cheie ca la criptare (Figura II.3).

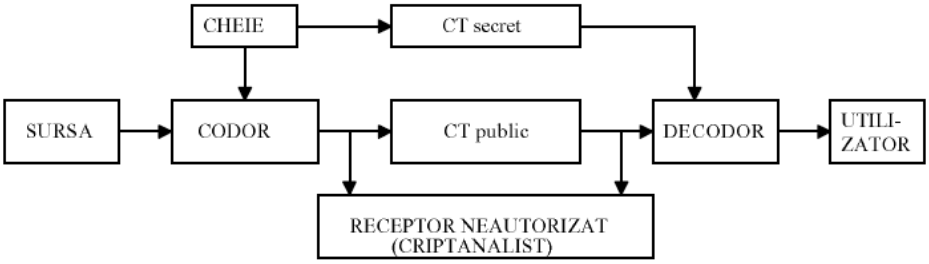

Figura II.3 Schema de principiu a unui sistem de comunicaţii
cu criptare cu cheie secretă

Criptarea cu cheie secretă, cunoscută sub numele de **criptare simetrică**, utilizează o singură cheie, K, pentru a cripta şi decripta datele.

$$K = K_E = K_D \Rightarrow C = E_K(M),\ M = D_K(C)$$

Securitatea algoritmului cu cheie secretă depinde deseori de cât de bine este păstrată sau distribuită cheia secretă.

Algoritmii cu chei secrete se împart în două mari categorii:

- **algoritmi bloc** (*block cipher*), care procesează blocuri de date de lungime fixă;
- **algoritmi de şiruri** (*stream cipher*), care procesează la un moment dat un singur bit sau simbol.

Printre avantajele criptării cu cheie simetrică se numără rapiditatea procesului de criptare şi simplitatea utilizării acestuia. Dezavantajele acestei tehnici sunt legate de necesitatea distribuirii în siguranţă a cheii secrete şi de managementul cheilor.

Printre algoritmii de criptare de tip bloc, cu cheie simetrică, se numără:

- DES - *Data Encryption Standard*

- 3DES - *Triple DES*
- IDEA - *International Data Encryption Algorithm*
- AES - *Advanced Encryption Standard*
- Blowfish

Dintre algoritmii de criptare bazați pe şiruri, se remarcă:

- RC4 - *Ron's Cipher 4*
- SEAL - *Software-Optimized Encryption Algorithm*
- Cifrurile de transpoziție (modifică ordinea simbolurilor din şir, după o anumită regulă)
- Cifrurile de substituție (se înlocuiesc litere sau simboluri, singure sau în grup, cu altele generate pe baza unor tabele de substituție).

II.6.2 CRIPTAREA CU CHEIE PUBLICĂ

Un criptosistem cu cheie publică, bazat pe funcții greu inversabile, foloseşte de fapt o funcție inversabilă într-un singur sens (*one-way function*), a cărei inversă nu poate fi calculată practic întrucât acest calcul implică depaşirea fie a capacității sistemelor de calcul utilizate, fie a timpului în care informațiile transmise sunt valabile şi considerate secrete (Figura II.4).

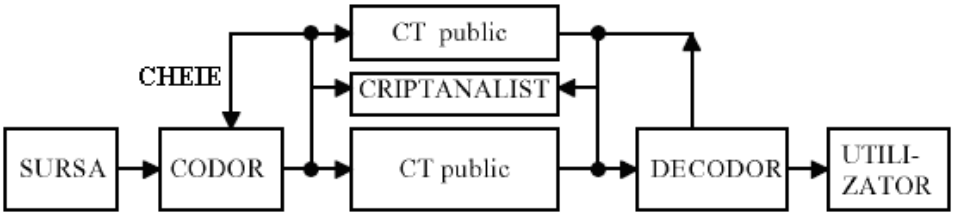

Figura II.4 Schema de principiu a unui sistem de comunicații

cu criptare cu cheie publică

Acest principiu de criptare a fost propus în 1976 de doi cercetători, Diffie şi Hellman (DH).

Criptarea cu cheie publică sau ***criptarea asimetrică*** utilizează o pereche de chei. Una dintre aceste chei, ***cheia publică*** *(*K_E*)*, este utilizată pentru criptarea informațiilor şi se caracterizează prin faptul că este distribuită în rețeaua publică de comunicații, în timp ce cealaltă cheie, numită ***cheia secretă*** *(*K_D*)*, folosită pentru decriptarea informațiilor trebuie să aibă caracter secret. Din cheia publică, este imposibil să se determine cheia secretă.

$$K_E \neq K_D \Rightarrow C = E_{K_E}(M),\ M = D_{K_D}(C)$$

Algoritmii cu cheie publică se bazează, cel mai adesea, pe complexitatea calculelor şi operațiilor care trebuie realizate. Ele pot fi utilizate pentru generarea semnăturilor digitale.

Cheile private corespunzătoare cheilor publice trebuie întotdeauna securizate şi transmise pe canale de comunicații securizate. Unul dintre mecanismele utilizate pentru stocarea cheii private este cardul inteligent (*smart card*), un dispozitiv electronic asemănător unei cărți de credit. Un card criptografic are abilitatea de a genera şi stoca chei. Acesta poate fi vulnerabil la atacuri, dar oferă o mai mare securitate față de procedeul de stocare a cheilor private pe un calculator.

Printre algoritmii cu cheie publică se numără:

- RSA - *Rivest, Shamir, Adelman*
- El Gamal
- DH - *Diffie-Hellman*.

II.6.3 MANAGEMENTUL CHEILOR

Una dintre problemele fundamentale atât în sistemele de criptografice cu cheie publică, cât şi în cele cu cheie secretă, o reprezintă modalitatea de distribuire şi păstrare în mod securizat a cheilor utilizate pentru criptare şi decriptare.

Algoritmii cu cheie secretă depind de obținerea în mod securizat a cheii de către toate părțile implicate.

Mecanismul de management al cheilor include mai multe aspecte:

- Generarea la secret a cheilor
- Distribuția securizată a cheilor
- Stocarea, eventual arhivarea cheilor în mod securizat
- Păstrarea istoricului utilizării cheilor (cine şi ce chei a folosit deja) prin procesul de audit al cheilor
- Eliminarea cheilor deja compromise.

Toate aceste procese sunt importante pentru securitatea rețelei de comunicații. Insecuritatea unui singur proces afectează siguranța transmisiilor din rețea.

Parolele implicite constituie un punct slab în securitatea rețelei sau o vulnerabilitate critică. Acestea trebuie schimbate de la prima utilizare pentru a securiza entitatea în cauză (echipament, cont de utilizator etc).

Folosirea unor parole sau chei foarte simple (secvențe de caractere identice, de exemplu “1” sau “0”, sau alte combinații simple, “abcd”, “1234”) sunt primele încercate de cei care încearcă să spargă sistemul de securitate, deci devin puncte de vulnerabilitate în sistem.

Referitor la distribuția cheilor, sistemul de poştă electronică nu este considerat un mecanism securizat de distribuire a cheilor, deoarece există terți care îl pot intercepta în tranzit.

De fapt, dificultatea de a gestiona cheile de transmisie creşte odată cu numărul de utilizatori din rețea.

O 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 dorește trimiterea unui mesaj criptat cu o cheie secretă către mai mulți destinatari, toți trebuie să primească cheia prin care să se poată decripta mesajul. Astfel, expeditorul trebuie să se asigure de faptul că toți destinatarii recepționează cheia, că aceasta nu este interceptată sau compromisă în timpul tranzitului şi că este păstrată în mod securizat la destinație. Pentru fiecare mesaj nou trimis, procesul trebuie să se repete, cu excepția faptului când se dorește reutilizarea cheii inițiale.

Reutilizarea cheii originale sporeşte şansele ca aceasta să fie compromisă, iar în cazul în care se dorește ca fiecare destinatar să aibă o cheie secretă, sistemul de distribuție nu mai este practic.

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.

Sistemul de gestiune a cheilor trebuie să le clasifice pe acestea în chei tari şi chei slabe pentru a distribui numai chei tari, şi, în plus, este necesară eliminarea cheilor deja compromise. Însă nu în toate situațiile de interceptare a cheii, rețeaua poate să sesizeze acest fapt. De exemplu, în rețelele wireless este dificil de urmărit intruşii pasivi, care “ascultă” rețeaua şi preiau pachetele din care extrag cheia de transmisie prin diferite metode de atac criptografic sau preiau vectorii de inițializare transmişi în clar.

Sunt necesare mecanisme specializate de distribuție a cheilor, astfel încât nici măcar serverul care intermediază transferul să nu cunoască secvențele-cheie folosite la criptare. De asemenea, este necesară dubla autentificare, a clienților către server şi a serverului de chei către clienți, pentru a se evita pătrunderea în rețea a unor intruşi neautorizați.

În acest sens, sunt indicate mecanisme de autentificare Kerberos sau RADIUS, precum şi metode de criptare P2P (*Peer-to-Peer*) pentru conexiuni în pereche între clienți.

II.7 INTEGRITATEA INFORMAȚIEI

Termenul de integritate a datelor sau informațiilor semnifică faptul că acestea nu pot fi create, modificate sau şterse fără autorizație.

Integritatea informației se poate asigura prin mai multe metode:

- tehnica rezumatului
- semnătura digitală
- certificatul digital
- marcarea conținutului.

Codarea fiecărui cadru de date transmis în rețea folosind un cod ciclic de verificare a redundanței (CRC) permite verificarea la recepție a integrității datelor şi rejectarea celor modificate, accidental sau cu intenție.

Rezumatul electronic permite verificarea integrității datelor stocate sau transmise şi identificarea informațiilor false sau eronate transmise în mod neautorizat.

Semnăturile digitale atestă autenticitatea informațiilor, faptul că acestea sunt transmise de surse autorizate, şi nu permit repudierea mesajelor. Autentificarea originii datelor (*message authentication*) include integritatea datelor.

Certificatele digitale se utilizează pentru autentificarea echipamentelor din rețea şi realizarea unor interconexiuni sigure. Sunt indicate în mod special în rețelele wireless, pentru a evita accesul neautorizat al unor echipamente.

Marcarea mesajelor se foloseşte pentru aplicarea dreptului de autor în cazul documentelor electronice.

II.7.1 TEHNICA HASH

Integritatea datelor reprezintă un aspect extrem de in important ce trebuie avut în vedere la comunicațiile prin intermediul rețelelor publice, întrucât aceste date pot fi interceptate şi modificate.

Pentru a preveni modificarea unui mesaj sau pentru a putea verifica dacă mesajul recepționat este identic cu cel transmis, se utilizează o tehnică specifică, **tehnica hash** sau **tehnica rezumatului**, care permite generarea unei secvențe de identificare a datelor transmise, denumită “rezumatul datelor” (*message digest*). Rezumatul unui mesaj se construieşte prin aplicarea unei funcții de transformare (funcție hash), care se caracterizează prin faptul că furnizează la ieşire un şir de date de lungime fixă, o valoare de transformare (*hash value*), atunci când la intrare se aplică un şir de date cu

lungime variabilă. Sensul unic de transformare asigură faptul că nu se pot deduce datele de intrare pe baza celor de ieşire.

Funcția hash ne asigură că datele transmise la intrarea în rețea sunt aceleaşi cu cele primite la destinație, metoda fiind oarecum asemănătoare cu suma de control (*checksum*) dintr-un segment folosită pentru controlul erorilor. În urma aplicării unei funcții hash la un pachet de date, înainte de transmisie, va rezulta o valoare fixă, care este apoi recalculată la recepție. În cazul în care cele două valori sunt identice, se trage concluzia ca datele nu au fost alterate din punct de vedere al securității. Dacă datele sunt modificate în tranzit, la destinație se va obține o altă valoare de transformare, ceea ce va indica falsificarea datelor. Prin utilizarea unei funcții hash, chiar şi o mică modificare a conținutului va crea mari diferențe între valorile hash de la transmisie şi recepție.

Funcțiile hash criptografice sunt utilizate pentru autentificarea mesajelor, controlul integrității datelor, verificarea parolelor şi realizarea semnăturilor digitale, în diferite aplicații de securitate a rețelelor de comunicații.

Funcțiile hash se clasifică în două mari categorii:

1. **Coduri de detecție modificate** (MDCs), cunoscute ca şi coduri de manipulare-detecție sau, mai puțin folosit, **coduri de integritate a mesajului** (*message integrity codes* - *MICs*). Scopul unui MDC este de a oferi o imagine (hash) reprezentativă unui mesaj şi de a facilita, cu ajutorul unor mecanisme secundare, verificarea integrității datelor cerută de aplicații specifice. MDC-urile sunt o subclasă a funcțiilor hash fără cheie, şi, la rândul lor, pot fi clasificate în:

- **funcții hash inversabile într-un singur sens** *(one-way hash functions* - OWHFs) rezistente la preimagine (*preimage resistant*),

adică pentru o valoare hash dată (H), este greu de găsit un mesaj M, astfel încât:

$$H = hash(M)$$

- **funcții hash rezistente la coliziune** *(collision resistant hash functions* - CRHFs): această proprietate se referă la faptul că este dificilă găsirea a două mesaje care să aibă aceeaşi valoare hash (o coliziune apare atunci când două mesaje distincte au aceeaşi valoare hash).

2. **Coduri de autentificare a mesajelor** *(message authentication codes* -MACs) care permit, fără ajutorul niciunui mecanism adițional, asigurarea autenticității sursei şi a integrității mesajelor. MAC-urile au funcțional doi parametrii distincți: mesajul de intrare şi o cheie secretă (subclasa de funcții hash cu cheie).

Observaţii:

1. Trebuie făcută distincția între algoritmul MAC şi utilizarea unui MDC cu o cheie secretă inclusă ca o parte din mesajul de intrare. Se presupune în general că algoritmul unei funcții hash este cunoscut. Deci, în cazul MDC-urilor, dat fiind un mesaj de intrare, oricine poate calcula funcția sa hash.
2. MAC-urile şi semnăturile digitale pot determina dacă datele au fost generate de o anumită entitate la un moment dat în trecut, dar ele nu oferă garanții în privința momentului când acestea au luat naştere. Deci aceste tehnici nu pot detecta mesajele reutilizate, ceea ce este necesar în medii în care acestea au un alt efect sau o utilizare secundară. Insă, aceste

tehnici de autentificare pot fi modificate pentru a asigura şi aceste garanții.

Pentru asigurarea integrității datelor, se folosesc algoritmii *Message Digest* (MD) şi *Secure Hash Algorithm* (SHA), ambii implementați în diferite variante de-a lungul timpului:

- SHA-1- *Secure Hash Algorithm* 1;
- MD4- *Message Digest* 4;
- MD5- *Message Digest* 5;
- RIPEMD-160 - *Race Integrity Primitives Evaluation Message Digest* - 160.

Exemplificăm folosirea funcțiilor hash prin c**onstrucția Merkle-Damgård** (Figura II.5).

O funcție hash trebuie să fie capabilă să proceseze un mesaj de lungime variabilă şi să furnizeze o ieşire de lungime fixă. Acest lucru se poate realiza prin împarţirea mesajului de intrare într-o serie de blocuri de dimensiuni egale, şi procesarea succesivă a acestora folosind o funcție ireversibilă (F). Această funcție se caracterizează prin faptul că ea converteşte cele două intrări de aceeaşi lungime, într-o ieşire de lungime egală cu una din intrările sale.

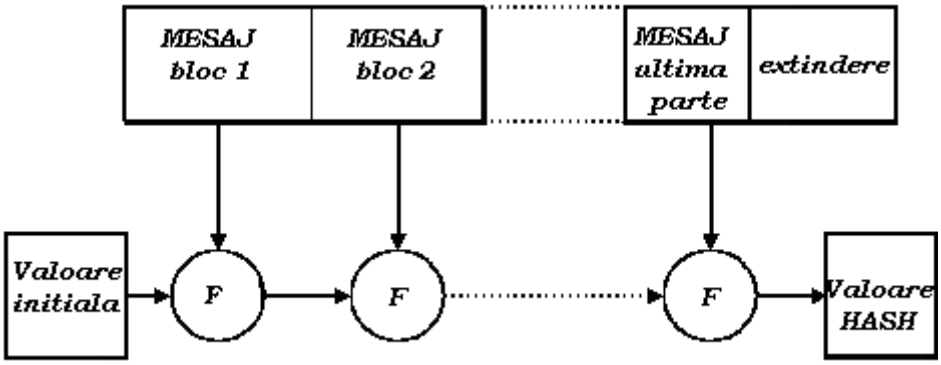

Figura II.5 Construcția Merkle-Damgård

De exemplu, dacă funcția F are o intrare de 128 de biți şi una de 256 de biți, atunci va furniza o ieşire de 128 de biți.

Funcția utilizată poate fi proiectată special pentru hashing sau construită dintr-un cifru bloc.

O funcție hash realizată folosind construcția Merkle-Damgård este rezistentă la coliziune, în aceeaşi măsura în care este şi funcția ireversibilă utilizată.

Ultimul bloc procesat trebuie să fie urmat de un alt bloc de extindere *(length-padding)*, cu ajutorul căruia este mascată lungimea reală a acestuia, lucru deosebit de important pentru securitatea construcției.

II.7.2 SEMNĂTURA DIGITALĂ

Termenul de semnătură electronică sau digitală 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 la recepție.

Semnăturile digitale sunt un tip de criptare asimetrică, asemănătoare semnăturilor de mână, ce sunt utilizate pentru a identifica un individ într-o manieră legală. Ele pot identifica persoana care a semnat o tranzacție sau un mesaj, dar spre deosebire de semnăturile de mână, poate ajuta în verificarea faptului că un document sau o tranzacție nu a fost modificată față de starea originală din momentul semnării.

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 aparține persoanei a cărei semnătură apare în mesaj, fără drept de repudiere.

Incapacitatea de a nega faptul că un mesaj sau o tranzacție a fost executată (semnată, în acest caz) se numeşte **nerepudiere**.

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 referitoare la identitatea utilizatorului.

Schema unei semnături digitale constă din 3 algoritmi:

- **algoritmul de generare a cheii** - furnizează aleator o pereche de chei, o cheie de verificare cu caracter public K_P şi o cheie pentru semnătură cu caracter privat K_S .

- **algoritmul de semnare** - produce o semnătură *S* cu ajutorul cheii private K_S pentru mesajul de intrare *M*.
- **algoritmul de verificare a cheii V** - pentru un mesaj de intrare *M*, o cheie de verificare K_P şi o semnătură *S*, acceptă sau respinge mesajul.

Un algoritm de criptare care poate fi utilizat pentru semnăturile digitale este algoritmul RSA, în care, generarea unui mesaj semnat se realizează cu o funcție exponențială, într-un câmp algebric finit:

$$S = M^d \bmod N$$

N este dimensiunea câmpului şi se obține ca produs de două numere prime foarte mari.

M este mesajul care trebuie semnat şi transmis.

d este exponentul cheii private (semnătura este generată cu ajutorul cheii private).

La recepție se verifică dacă este adevărată relația:

$$M = S^e \bmod N$$

e reprezintă exponentul cheii publice (decriptarea mesajului semnat se face cu ajutorul cheii publice).

Acestă metodă nu este prea sigură din punct de vedere al atacurilor, o soluție în acest sens ar fi, aplicarea unei funcții hash, înaintea algoritmului RSA. Astfel la emisie se va realiza operația:

$$S = H^d \bmod N$$

Iar la recepție:

$$H = S^e \bmod N$$

Valoarea hash H rezultată este comparată cu valoarea hash a mesajului şi dacă sunt egale, atunci se confirmă faptul că mesajul provine într-adevăr de la persoana autorizată.

În concluzie, funcțiile hash, cu sau fără cheie, pot fi utilizate pentru securizarea accesului la rețea, pentru criptarea datelor şi verificarea integrității acestora.

II.7.3 CERTIFICATUL DIGITAL

Accesul neautorizat reprezintă o problemă tuturor rețelelor wireless, în particular WiFi.

Pentru a avea un control asupra persoanelor care accesează rețeaua şi asupra resurselor accesate de acestea (*who and what?*) este necesar un mecanism de control selectiv al accesului, pe bază de credite personale.

O semnătură digitală în sine nu oferă o legătură puternică cu o persoană sau o entitate.

Pentru a avea garanția că o cheie publică utilizată pentru a crea o semnătură digitală aparține într-adevăr unui anumite persoane şi că acea cheie este încă validă, este necesar un mecanism care să stabilească o legătură între cheia publică şi utilizatorul real. Acest serviciu de autenticitate este oferit de **certificatele digitale**.

Certificatele digitale pot fi generate folosind chei publice sau chei private.

Infrastructura cu chei publice (*PKI - Public Key Infrastructure*) este mecanismul prin care o cheie publică este “legată” de un anumit utilizator printr-un certificat digital de identificare.

Sistemul PKI corelează informațiile despre utilizator cu o anumită cheie publică, astfel încât cheile publice să poată fi utilizate ca o formă de identificare.

Sistemul PKI se ocupă de crearea, distribuția, stocarea centralizată, revocarea şi actualizarea certificatelor digitaleprin intermediul cărora se asigură servicii de bază de securitate precum autentificarea utilizatorilor, confidențialitatea şi integritatea informațiilor, ajutând de asemenea la implementarea serviciului de nerepudiere.

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** (*CA - Certificate Authority*). O autoritate de certificare semnează un certificat în calitate de garant pentru identitatea persoanei căreia îi aparține certificatul respectiv.

Toate certificatele revocate sau anulate sunt trecute într-o **listă de revocare a certificatelor** (*CRL - Certificate Revocation List*).

Cel mai întâlnit standard pentru certificatele digitale este ITU-T X.509, standard pentru infrastructura cu chei publice (PKI). Acesta specifică, printre altele, formatul standard al certificatelor digitale, precum şi un algoritm de validare a certificatelor.

Elementele unui certificat digital definite de acest standard sunt următoarele:

- versiunea certificatului (*certificate version*) - care indică formatul unui certificat;

- numărul de serie (*serial number*) - un număr unic generat de către autoritatea de certificare, utilizat pentru a se ține evidența certificatelor;
- numele emitentului (*issuer name*) - specifică numele autorității de certificare;
- perioada de valabilitate (*period of validity*)
- numele proprietarului certificatului (*subject*);
- cheia publică şi algoritmul cheii publice (*subject's public key info*);
- un câmp opțional utilizat pentru a identifica emitentul certificatului sau autoritatea de certificare (*issuer unique identifier*);
- un câmp opțional pentru identificarea subiectului (*subject unique identifier*);
- un câmp opțional utilizat pentru extensii (*extensions*), care poate cuprinde: alte denumiri ale subiectului, informații pentru utilizarea cheilor şi punctele de distribuție a listelor de revocare a certificatelor (*CRL*);
- algoritmul folosit pentru semnarea certificatului (*certificate signature algorithm*);
- semnătura (*signature*).

O problemă a certificatelor digitale o reprezintă 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, printre care se numără compromiterea cheii, compromiterea autorității de certificare sau o schimbare a autorității de certificare.

Numeroase metode de autentificare sunt bazate pe PKI, iar certificatele pot fi stocate pe carduri inteligente (*smart cards*), fie în fişiere, în registrele sistemului. Prin folosirea cardurilor de acces, utilizatorul nu

este obligat să reţină sau să introducă de fiecare dată un volum mare de informaţii de identificare, ci numai o simplă secvenţă PIN (*Personal Identification Number*).

Utilizatorilor autentificaţi în reţea pe bază de certificate digitale, în sistem PKI, li se asigură un grad mare de securitate, la nivel de aplicaţii (*application-level security*), cu posibilitatea semnării şi codării mesajelor folosind certificate de criptare (*encryption cerificates*).

Certificatele digitale sunt utilizate şi în autentificarea mutuală dintre client şi server, fiecare prezentând un certificat propriu.

PKI este un sistem complex şi robust de securizare, recomandat doar pentru comunicaţiile care necesită un grad foarte mare de securitate (*mission-critical*), precum cele guvernamentale.

II.7.4 MARCAREA

În literatura de specialitate pot fi întâlnite diferite definiţii pentru marcarea documentelor.

Marcajele sunt acele elemente distinctive, greu de reprodus, care asigură autenticitatea unui document şi, eventual identificarea autorului. Astfel de elemente de marcare se utilizează din cele mai vechi timpuri pe bancnote şi monede pentru a nu putea fi falsificate.

Marcajele pot fi vizibile sau ascunse, transparente (*watermark*).

Marcajele pentru imaginile digitale sunt tratate ca manipulări ale celor mai puţin semnficativi biţi din eşantioanele de imagine (*LSB - Least Significant Bits*), coduri ascunse de marcare, texturi invizibile, constrângeri secrete în domenii de transformare etc.

Marcajele sunt generate în mod privat şi pot fi detectate folosind chei private sau publice, în funcție de întrebuințarea lor.

Marcajul pentru protejarea dreptului de autor (*copyright*) denumit şi ştampilă invizibilă, conține o informație specifică proprietarului legal sau este un semn aleator de unicitate pentru respectivul proprietar.

Protejarea informațiilor prin marcare se realizează astfel:

- fiecare proprietar de copyright deține un număr unic sau un set de numere care constituie cheia privată a marcajului;
- folosind cheia privată şi un algoritm public sau privat, proprietarul dreptului de autor modifică datele digitale care sunt marcate;
- folosind un algoritm de detecție, proprietarul de copyright poate verifica sau decoda modificările făcute de el însuşi.

Marcajele de autenticitate a produselor digitale sunt de fapt semnăturile digitale. Autenticitatea face referire la un produs original cu privire la originalitatea conținutului, numele autorului, data la care a fost creat, proprietarul dreptului de autor etc. Marcarea cu ajutorul semnăturii digitale asigură autenticitatea sursei din care provine un produs digital sau un mesaj transmis în rețea şi elimină riscul ca acesta să fie un fals.

II.8 POLITICI DE SECURITATE

Principiile care stau la baza asigurării securității unei rețele de comunicații sunt exprimate, sub forma unui set de reguli şi practici, în aşa-numita politică de securitate a rețelei.

Politica de securitate se aplică tuturor persoanelor care într-un fel sau altul au acces la resursele rețelei, la orice nivel începând cu cel fizic şi indiferent de scop (utilizare, administrare, întreținere, fraudă, atac).

În primul rând, trebuie stabilite necesitățile fiecărei categorii de utilizatori cu privire la resursele rețelei şi drepturile de acces, din interiorul sau din exteriorul acesteia, folosind structura cablată sau accesul wireless la rețea. De asemenea, trebuie stabilit care dintre utilizatori au cu adevărat nevoie de acces la rețeaua publică de Internet. Toate aceste aspecte sunt tratate în cadrul **politicii de acces**.

Criteriile după care se stabilesc grupurile de utilizatori, dreptul de a avea un cont de acces în rețea, condițiile de activare şi de dezactivare a conturilor, persoanele cu drept de administrare reprezintă **politica de conturi** a rețelei.

Conexiunea la Internet şi la rețeaua publică în general reprezintă o breşă în securitatea oricărei rețele deoarece pe aici acționează atacurile lansate din afara rețelei. Sunt necesare principii clare de securizare a interfețelor dintre rețeaua publică şi cea privată. Principiile conform cărora se securizează căile de acces la Internet şi se acordă drepturi în acest sens alcătuiesc **politica de acces la Internet** (I-AUP - *Internet Acceptable Use Policy*).

Accesul, fizic şi logic, pe diferite echipamente de comunicație din rețea trebuie restricționat corespunzător importanței acestora în buna funcționare a rețelei. Trebuie luate măsuri de prevenire a tentativelor de acces neautorizat.

Folosirea metodei de autentificare pe bază de nume de utilizator şi parolă implică aplicarea unor principii de acceptare, gestionare şi schimbare a parolelor în cadrul **politicii de management a parolelor**.

Drepturile de acces la rețea trebuie diferențiate în ceea ce priveşte accesul la documente şi drepturile asupra acestora (citire, scriere, modificare sau ştergere). Prin politica de securitate se stabilesc drepturile utilizatorilor referitor la accesul la informații şi fişiere în general, strategia care trebuie adoptată în vederea asigurării respectării acestora, garanțiile de respectare a politicii de securitate de către toți utilizatorii (de exemplu, clauze de confidențialitate din contractele semnate de utilizatori). Toate aceste aspecte reprezintă aşa-numita **politică de utilizare adecvată a resurselor rețelei**.

Formularea politicii de securitate a unei rețele trebuie făcută clar, cu cât mai multe detalii, astfel încât să nu apară interpretări diferite ("be as specific as possible").

Cunoaşterea în detaliu a tuturor echipamentelor care se conectează la rețea şi a garanțiilor pe care le oferă fiecare utilizator constituie premiza unor decizii juste cu privire la privilegiile sau restricțiile care se impun în fiecare caz în parte (**politica de conectare**).

Refuzul accesului la rețea pentru acele entități pentru care se dovedeşte intenția de atac, prin monitorizarea traficului, constituie o măsură de forță majoră, necesară menținerii funcționării rețelei în condiții de siguranță.

Vulnerabilitățile de securitate sunt cauzate de diverşi factori, printre care neactualizarea (*update*) sistemelor de operare, programelor antivirus sau a altor programe sau module de securitate (*software patches, firmware upgrades, authentication routines, encryption algorithms, intrusion detection systems*). Periodic se impune instalarea celor mai noi versiuni de software, actualizarea bazelor de date cu semnăturile viruşilor noi apăruți sau ale altor forme de atac recent identificate.

De asemenea, periodic, personalul implicat în asigurarea securității rețelei trebuie instruit pentru a cunoaşte eventualele noi riscuri la care este expusă rețeaua şi procedurile care trebuie urmate pentru soluționarea problemelor.

Trebuie stabilite reguli pentru asigurarea securității pe toate nivelele: fizic, de acces logic, de acces la servicii, de acces la informații.

Toate configurările implicite trebuie schimbate din momentul punerii în funcțiune a echipamentului şi nu mai trebuie să se revină niciodată la acestea.

Periodic trebuie revizuite configurările diferitelor echipamente din rețea pentru a stabili dacă ele corespund nevoilor de securitate ale rețelei de la un anumit moment, inclusiv parole, liste de control al accesului, adrese MAC, chei de criptare.

În cazul rețelelor wireless, trebuie aplicate tehnici de site survey pentru măsurarea ariei de acoperire a fiecărui echipament AP (*Access Point*) şi a nivelului de semnal în afara zonei de interes, pentru a stabili posibilele locații ale unor intruşi. Reducerea nivelului la emisie precum şi a ariei de acoperire prin ecranarea anumitor pereți sau folosirea unor antene directive conduce la micşorarea riscurilor de atac asupra rețelei wireless.

Criptarea informațiilor se impune ca măsură ultimă de asigurare a secretului transmisiei, în situația în care un intrus reuşeşte să descarce pachete din rețeaua privată. De asemenea, criptarea reprezintă o măsură de siguranță în ceea ce priveşte secretul unor informații cu caracter special, care poate fi atacat de persoane din exteriorul dar şi din interiorul rețelei. Principiile de securizare a informațiilor sunt incluse în **politica de protecție a informațiilor**.

Rețelele VPN (*Virtual Private Network*) reprezintă o bună soluție de securitate, adoptată cu precădere de companii cu mai multe sedii răspândite într-o arie geografică largă. Accesul de la distanță prezintă de cele mai multe ori riscuri mari de securitate cauzate de tentative de atac ale unor persoane din afara companiei fiind necesară securizarea pe baza unor principii clare privind drepturile şi restricțiile de acces de la distanță (*remote access*) şi tacticile de securitate care trebuie adoptate conform **politicii de acces de la distanță**.

Politici de securitate specifice se pot stabili pentru fiecare serviciu de rețea în parte (poştă electronică, transfer de fişiere, aflarea informațiilor despre utilizatorii rețelei etc).

Regulile de securitate pot avea caracter obligatoriu sau facultativ rezultând mai multe categorii de prevederi de securitate:

- **prevederile obligatorii,** rezultate ca efect al acordurilor, al regulamentelor şi al legilor, exprimate detaliat, cu cât mai multe elemente specifice, în funcție de domeniul de utilizare, au rolul de a oferi siguranță şi încredere într-o rețea de comunicații sau o anumită entitate (server, serviciu, program etc).
- **prevederile recomandate,** deşi neobligatorii, sunt motivate de consecințele grave ale neaplicării lor. Pentru o securitate cât mai bună a rețelei, acestea trebuie considerate ca şi obligatorii deşi costurile implementării lor sunt în general mari. De exemplu, nu este obligatorie rularea programelor de tip antivirus şi nici instalarea tuturor patch-urilor de securitate din sistemele de operare. Toate acestea implică unele costuri suplimentare (preț, memorie de sistem, timp de procesare) dar într-o rețea fiecare nod nesecurizat corespunzător poate fi o poartă de acces pentru atacatori.

- **prevederile informative** au rolul de a atenționa (*warning*) utilizatorii asupra existenței unor vulnerabilități (de exemplu, neactualizarea listelor cu viruşi pentru programele antivirus), asupra riscurilor şi consecințelor breşelor de securitate ale sistemelor şi rețelelor.

Politica de securitate se exprimă sub forma unui document în care sunt incluse: motivele şi obiectivele aplicării acesteia, autoritatea competentă care o aprobă, autori, referințe, data elaborării, proceduri, măsuri de compatibilitate, consecințele neaplicării.

Din păcate, nu există un sistem de securitate sigur 100 %, dar prin definirea unei politici de securitate se încearcă găsirea celei mai bune căi de evitare a riscurilor la care este supusă rețeaua de comunicații.

Capitolul III ATACURI ASUPRA REȚELELOR DE COMUNICAȚII

III.1 VULNERABILITĂȚI ALE REȚELELOR

O rețea sigură este aceea în ale cărei resurse se poate avea încredere, adică furnizează servicii corecte şi de calitate.

Deoarece o rețea de comunicații este un sistem complex, eterogen, cu foarte mulți utilizatori, ea reprezintă o zonă convenabilă pentru diferite atacuri. De aceea, securitatea reprezintă un obiectiv operațional vital al oricărei rețele de comunicații.

Rețelele de calculatoare ale diferitelor organizații sunt utilizate atât pentru realizarea comunicațiilor dintre angajați, cât şi pentru comunicații externe, astfel încât acestea nu mai pot fi izolate şi trebuie securizate la nivelul interfețelor de acces dintre rețeaua publică şi cea privată.

Comunicațiile realizate prin rețelele publice sunt expuse riscurilor de interceptare, de furt sau de falsificare a informațiilor, de disfuncționalități tehnice manifestate fie prin calitate slabă a transmisiei, fie prin întreruperi.

În funcție de vulnerabilitățile rețelei de comunicații pe care le pot exploata, atacurile se pot manifesta pe mai multe planuri:

- accesare neautorizată a rețelei sau a unor resurse ale acesteia din interiorul organizației sau din afara acesteia,
- tentative de perturbare sau de întrerupere a funcționării rețelei la nivel fizic (prin factori mecanici, de întrerupere a unor cabluri sau scoatere din funcțiune a unor echipamente din rețea; factori electrici,

de bruiaj în cazul rețelelor radio, semnale de interferență în rețelele cablate),

- tentative de întrerupere sau de încărcare excesivă a traficului din rețea prin transmiterea unui număr foarte mare de pachete către unul sau mai multe noduri din rețea (*flooding*),
- atacuri soft asupra echipamentelor de rețea care concentrează şi dirijează fluxurile în noduri critice (switch, router, access point etc.) prin modificarea fişierelor de configurare şi a drepturilor de acces stabilite de personalul autorizat,
- modificarea sau distrugerea informației, adică atacul la integritatea fizică datelor,
- preluarea şi folosirea neautorizată a informațiilor, adică încălcarea confidențialității şi a dreptului de autor.

Astfel, trebuie avute în vedere, cu prioritate, două aspecte principale legate de securitatea rețelelor:

- integritatea şi disponibilitatea resurselor unei rețele, fizice sau logice, indiferent de defectele de funcționare, hard sau soft, de perturbații sau de tentative de întrerupere a comunicațiilor.
- caracterul privat al informațiilor (*privacy*), exprimat ca fiind dreptul individual de a controla sau de a influența care informație referitoare la o persoană poate fi memorată în fişiere sau în baze de date din rețea şi cine are acces la acestea, rețeaua fiind responsabilă de împiedicarea încercărilor ilegale de sustragere a informațiilor, precum şi de încercările de modificare ale acestora. Informația este vulnerabilă la atac, în orice punct al unei rețele, fie stocată pe diferite maşini (stații de lucru, servere) din rețea, fie în procesul de transmisie de la sursă la destinația finală.

Vulnerabilitățile rețelelor se manifestă pe toate nivelele OSI, fiind necesară adoptarea unor măsuri de securitate adecvate fiecărui nivel şi fiecărui model de rețea în parte.

III.2 TIPURI DE ATACURI

Atacurile asupra rețelelor de comunicații pot fi clasificate după mai multe criterii.

Ținând cont de locul de unde se execută, atacurile pot fi:

- **locale** (*local*)
- **de la distanță** (*remote*).

O altă clasificare a atacurilor adresate rețelelor de comunicații, în funcție de modul în care acționează acestea, ca sursă şi destinație, atacurile pot fi **centrate** pe o singură entitate (de exemplu, este atacat un anumit server din rețea de pe un singur echipament) sau pot fi **distribuite** (lansate din mai multe locații sau către mai multe maşini simultan).

Atacurile distribuite sunt cele mai performante deoarece este dificilă identificarea şi localizarea autorilor, iar efectele lor sunt maximizate prin atacarea rețelei în mai multe noduri simultan.

După modul de interacțiune a atacatorului cu informația obținută în urma unui atac reuşit, se disting două categorii de atacuri: **pasive** şi **active**. Este greu de spus care dintre acestea are un risc mai mare. La o primă vedere, s-ar crede că cele mai periculoase sunt atacurile active. Dar să nu uităm atacurile pasive prin care se preiau chei de criptare fără ca serverul de

chei să îşi dea seama care sunt cheile compromise. Toate informațiile criptate cu acele chei devin astfel complet neprotejate.

O categorie aparte de atac asupra informațiilor stocate sau transmise în rețea o reprezintă **atacurile criptografice**, prin care se încearcă extragerea informației din mesajele criptate.

Un tip aparte de atac îl reprezintă aşa-numitul **atac etic** lansat periodic chiar de personalul de administrare a rețelei, simulare de atac menită a testa securitatea rețelei şi a descoperi vulnerabilitățile acesteia.

Cu toate că nu există soluții care să fie capabile să protejeze rețeaua împotriva oricărui tip de atac, există unele sisteme de securitate care pot reduce substanțial şansele şi efectele atacurilor. Se impune dezvoltarea unei politici de securitate adecvate fiecărei rețele în parte, aplicarea ei simultan cu educația utilizatorilor şi adoptarea unor soluții de securitate, software sau hardware, potrivite vulnerabilităților şi riscurilor de atac specifice fiecărei rețele.

III.2.1 ATACURI LOCALE

Atacurile locale presupun spargerea securității unei rețele de calculatoare de către o persoană care face parte din aceasta, adică de către un utilizator local.

Acesta dispune de un cont şi de o parolă de utilizator care îi dau drept de acces la o parte din resursele sistemului. De asemenea, persoana respectivă poate să aibă cunoştințe despre arhitectura sistemului de securitate al rețelei, putând astfel lansa atacuri mult mai periculoase.

Atacatorul, de la calculatorul propriu, va putea să-şi sporească privilegiile şi în acest fel să acceseze informații la care nu are drept de acces. De asemenea va putea să încarce programe care să scaneze rețeaua şi să găsească punctele vulnerabile ale rețelei.

Obținerea de drepturi de administrator (*admin, root*) reprezintă țelul atacatorilor.

Riscul de atac local poate fi redus în diferite moduri:

- acordarea utilizatorilor locali privilegiile minim necesare efectuării sarcinilor zilnice, potrivit funcției şi rolului fiecăruia în companie;
- monitorizarea activităților din rețea pentru a sesiza eventualele încercări de depăşire a atribuțiilor, eventual şi în afara orelor de program;
- impunerea de restricții de acces pe cele mai importante echipamente din rețea;
- distribuirea responsabilităților mari între mai mulți angajați.

Din nefericire, majoritatea sistemelor de protecție sunt inutile dacă mai mulți indivizi din interiorul rețelei cooperează pentru a învinge măsurile de securitate ale acesteia. De aceea, în vederea acordării unor privilegii de utilizare a resurselor rețelei, utilizatorii trebuie ierarhizați pe mai multe nivele de încredere, în funcție de vechimea în rețea, comportamentul acestora şi gravitatea unor evenimente de securitate în care au fost implicați.

III.2.2 ATACURI LA DISTANȚĂ

Atacul la distanță (*remote attack*) este un atac lansat împotriva unei rețele de comunicații sau a unui echipament din rețea, față de care atacatorul nu deține nici un fel de control.

Accesul de la distanță la resursele unei rețele este mai riscant decât accesul din rețeaua locală prin simplul fapt că în Internet sunt câteva miliarde de utilizatori ceea ce face ca numărul posibililor atacatori externi să fie mult mai mare decât al celor interni. Prin aplicarea unei politici de securitate corecte şi a unor soluții de securitate performante, riscul atacurilor locale poate fi minimizat.

Atacul de la distanță se poate realiza în trei etape:

Prima etapă este una de informare în care atacatorul trebuie să descopere informații despre:

- administratorul retelei
- echipamentele din rețea şi funcțiile acestora
- sisteme de operare folosite
- puncte de vulnerabilitate
- topologia rețelei
- politici de securitate etc.

Această etapă este considerată un atac în sine, denumit **atac de recunoaştere** (*reconnaissance*), şi constă în maparea neautorizată a unui sistem informatic, a serviciilor şi a vulnerabilităților lui. Este un pas precedent oricărui atac informatic, prin care se identifică porturi deschise, serviciile active, sisteme de operare, aplicații rulate, versiuni de software. Pe baza acestor informații, atacatorul poate pregăti un atac eficient.

Atunci când calculatorul-țintă deține o soluție de securitate, eforturile de atac sunt diminuate.

În funcție de dimensiunea şi arhitectura rețelei din care face parte calculatorul-țintă, folosind programe de scanare se pot obține informații despre numele şi adresele IP ale calculatoarelor dintr-o anumită arie.

Dar cea mai mare importanță o are colectarea informației despre administratorul de rețea din care provine ținta. Aceasta va aduce cele mai multe informații utile atacatorului. Dacă se determină când, cum şi cât îi ia administratorului de sistem sau persoanei responsabile de securitatea rețelei, să detecteze un eventual atac, atacatorul va iniția atacurile în afara acestor perioade, cu parametrii care să îi asigure succesul.

2. A două etapă este una de testare care presupune crearea unei clone a țintei şi testarea atacului asupra acesteia, pentru a se vedea modul în care reacționează. Realizând aceste experimente pe un calculator-clonă, atacatorul nu atrage atenția asupra sa pe durata simulării iar şansele atacului real, care va fi lansat ulterior, vor fi foarte mari. Dacă se fac experimente direct pe ținta reală, pentru atacator există riscul să fie detectat şi se pot alege cele mai eficiente contramăsuri.

3. Etapa a treia constă în lansarea atacului asupra rețelei. Pentru a avea cele mai mari şanse, atacul trebuie să dureze puțin şi să fie efectuat în intervalele când ținta este mai vulnerabilă.

Observație: Atacurile combinate, în care una sau mai multe persoane furnizează informații din interiorul rețelei şi altele din exterior lansează atacul de la distanță folosind acele informații, sunt extrem de periculoase, din punctul de vedere al atacatorului. În aceste cazuri, mascarea atacului este foarte bună iar şansele sistemului de securitate al rețelei de a reacționa la timp şi eficient sunt din cele mai mici.

III.2.3 ATACURI PASIVE

Atacurile pasive sunt acele atacuri în cadrul cărora intrusul doar observă rețeaua, canalul de comunicație, adică monitorizează transmisia şi, eventual, preia semnalul sau pachetele de date fiind denumite şi **atacuri de intercepție** (Figura III.1).

Atacurile pasive pot fi de două feluri:

- de citire şi înregistrare a conținutului mesajelor, de exemplu, în serviciul de poştă electronică;
- de analiză a traficului.

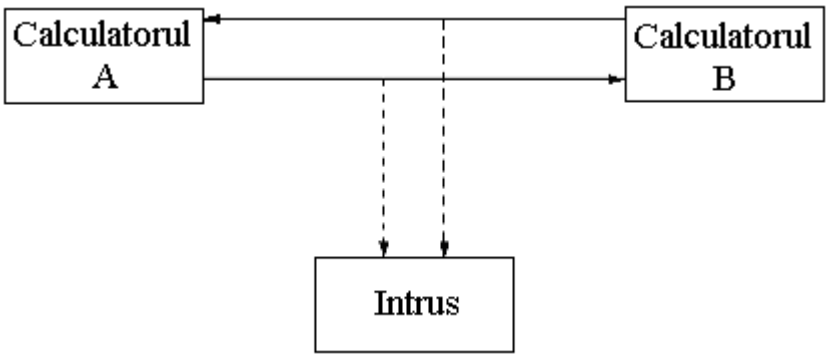

Figura III.1 Model de atac pasiv

Atacul pasiv de simplă observare sau de „ascultare" a traficului (*eavesdropping*) poate fi simplu realizat în rețelele wireless cu echipamente de radiorecepție acordate pe frecvența de lucru a rețelei.

Interceptarea pachetelor transmise în rețea (*packet sniffing*) reprezintă de asemenea un atac pasiv deosebit de periculos deoarece intrusul este conectat la rețeaua de comunicație (de exemplu, pe un port la unui

switch nesecurizat fizic) are acces logic la rețea şi poate prelua din pachete informațiile transmise în clar.

Referitor la atacurile pasive, se observă că:

- nu produc distrugeri vizibile (de exemplu, nu blochează rețeaua, nu perturbă traficul, nu modifică datele)
- încalcă regulile de confidențialitate prin furtul de informații
- observă modificările din rețea (noi echipamemente introduse, schimbarea configurărilor etc.)
- sunt avantajate de rutarea pachetelor prin noduri de rețea mai puțin protejate, cu risc crescut
- sunt greu sau chiar imposibil de detectat.

De aceea, se dezvoltă sisteme de prevenție şi detecție a intruziunilor în rețea, fie ca soluții software, fie cu echipamente dedicate (de exemplu, prin măsurători de câmp radiat pentru stabilirea ariei de acoperire a unei rețele wireless).

Din acest punct de vedere, rețelele optice sunt cel mai bine protejate fiind practic imposibilă interceptarea traficului fără a se sesiza prezența intrusului. Riscurile cele mai mari de atac pasiv, de intercepție a informațiilor din rețea (date propriu-zise sau de identificare) apar în rețelele wireless. Rețelele cablate, cu cabluri cu conductoare metalice, sunt vulnerabile la atacuri pasive în nodurile de comunicație de tip hub sau switch.

Atacurile pasive nedetectate care au ca finalitate preluarea cheilor de criptare reprezintă un risc major pentru rețea, întrucât prin necunoaşterea cheilor compromise se creează breşe în sistemul de securizare a informațiilor prin criptarea traficului.

III.2.4 ATACURI ACTIVE

Atacurile active au ca scop furtul sau falsificarea informațiilor transmise ori stocate în rețea, reducerea disponibilității rețelei prin supraîncărcarea acesteia cu pachete (*flooding*), perturbarea sau blocarea comunicațiilor prin atac fizic sau logic asupra echipamentelor din rețea şi a căilor de comunicații (Figura III.2).

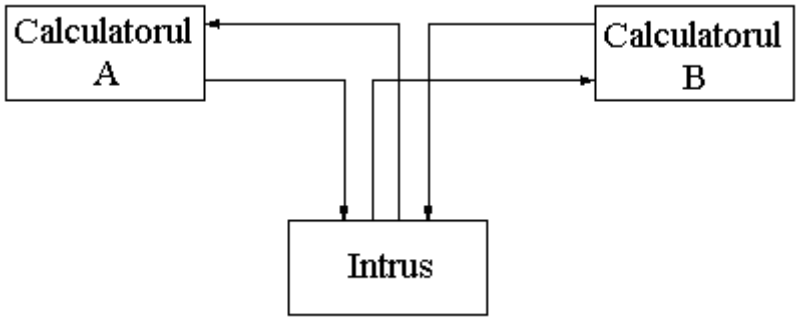

Figura III.2 Model de atac activ

S-au identificat până în prezent mai multe tipuri de atacuri active:

Mascarada (*masquerade*) este un atac în care o entitate din rețea (client, server, utilizator, serviciu) pretinde a avea o altă identitate pentru a prelua informații confidențiale (parole de acces, date de identificare, chei de criptare, informații despre cărți de credit şi altele).

Multe dintre atacurile de acest tip pot fi evitate prin adoptarea unor politici de securitate adecvate, care presupun responsabilizarea utilizatorilor, implementarea unor metode de acces robuste, folosirea unor metode de autentificare cât mai eficiente.

Un tip aparte de atac de mascare sau de falsă identitate se produce atunci când atacatorul activează în rețeaua wireless un echipament neautorizat de tip AP (*counterfeiting*) care reuşeşte să preia date valide de identificare ale utilizatorilor autorizați, în scopul folosirii lor ulterioare pentru accesare neautorizată a rețelei asupra căreia s-a produs atacul.

Un alt tip de atac constă în **modificarea mesajelor** (*message alteration*)**,** adică mesajul transmis este interceptat, întârziat, iar conținutul său este schimbat sau reordonat pentru modificarea datelor precum schimbarea unor valori în fişiere, în particular în înregistrări financiar-bancare, în diverse programe software astfel încât acestea să producă efecte diferite de cele pentru care au fost gândite. Un astfel de atac se întâlneşte în rețelele wireless 802.11b bazate pe WEP, cu vulnerabilități ale mecanismului de criptare. Atacatorul reuşeşte să intercepteze pachetele, să decripteze datele şi să modifice informațiile, după care le criptează din nou, cu acelaşi algoritm, şi corectează CRC-ul pentru ca datele modificate să fie considerate valide la destinație. Acest tip de atac este denumit şi **atac subtil,** fiind extrem de dificil de depistat.

Falsificarea datelor şi a mesajelor este posibilă şi prin atacul de tip **“omul-din-mijloc”** (*man-in-the-middle attack*) când atacatorul se află într-un nod intermediar dintr-un link de comunicare şi poate intercepta mesajele transmise de sursă substituindu-le cu mesaje proprii, cu informații false.

Refuzul serviciului (DoS *Denial-of-service attack*), lansat eventual în varianta distribuită (DDoS – *Distributed Denial-of-Service*), constă într-o supraîncărcare a serverelor cu cereri din partea atacatorului şi consumarea resurselor, astfel încât acele servicii să nu poată fi oferite şi altor utilizatori. Ca urmare a acestui atac, conexiunile existente se închid, fiind necesară reautentificarea utilizatorilor. Atacatorul profită de acest moment pentru a

intercepta date de identificare valide, informații despre rețea şi conturi de utilizare autorizată.

In general, atacurile DoS se realizează fie prin forțarea calculatorului-țintă să aloce toate resursele pentru a răspunde cererilor transmise într-un număr tot mai mare de către atacatori până la epuizarea resurselor, fie prin perturbarea şi chiar întreruperea comunicației dintre client şi server (de exemplu, a celor wireless prin diferite tehnici de bruiaj), astfel încât serverul să nu mai poată furniza serviciile sale clientului.

Reluarea unui mesaj sau a unui fragment din acesta (*replay*) este un atac lansat cu scopul de a produce un efect neautorizat în rețea (autentificarea atacatorului folosind informații de identificare valide, transmise de un utilizator autorizat al rețelei). Sistemul de gestionare a resurselor şi de monitorizare a accesului poate depista intenția de acces fraudulos de pe un anumit nod din rețea şi, pe baza politicii de securitate, poate să îl treacă în carantină, pe o perioadă de timp limitată în care se verifică existența atacului, şi ulterior să îi interzică total accesul în rețea pe baza adresei fizice, a celei de rețea sau de pe un anumit cont de utilizator de pe care s-a produs atacul. Acest atac poate avea ca efect erori de de management de rețea, interzicerea accesului clientului la anumite resurse, neplata unor servicii de rețea. De cele mai multe ori acest atac este considerat pasiv, dar dacă se iau în considerare efectele pe care le poate avea, inclusiv interceptarea şi distrugerea informațiilor transmise prin rețea, este mai indicată includerea lui în categoria atacurilor active.

O schemă simplă de clasificare a atacurilor este dată în figură:

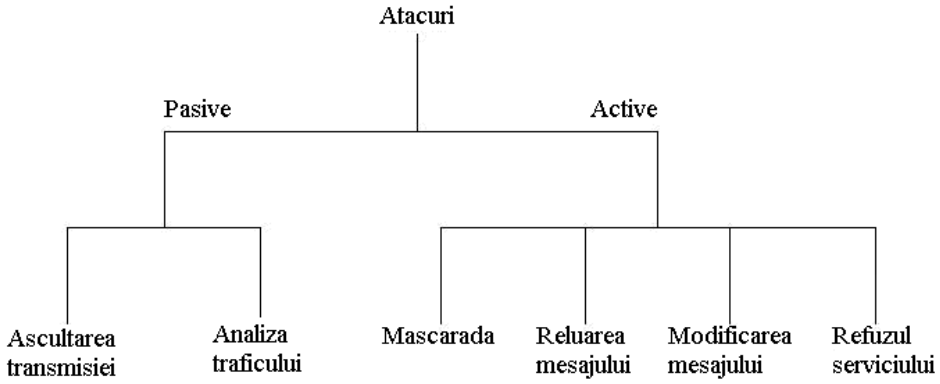

Figura III.3 Clasificarea atacurilor

Repudierea serviciului (*repudiation*) este un alt tip de atac asupra rețelelor de comunicații care se produce atunci când o entitate sau un utilizator refuză să recunoască un serviciu deja executat. Nerepudierea serviciului (*non-repudiation*) este foarte importantă în aplicațiile cu plată care necesită servicii de taxare (*billing*). Dacă utilizatorul neagă folosirea serviciului şi refuză plata acestuia, furnizorul trebuie să dispună de dovezi solide care să împiedice repudierea serviciului în context legal.

Din aceeaşi categorie a atacurilor active, fac parte şi **programele cu scopuri distructive** (*virus*, *worm*, *spy*, *spam*) care afectează securitatea echipamentelor şi a informațiilor din rețea, fie prin preluarea unor informații confidențiale, fie prin distrugerea parțială sau totală a datelor, a sistemului de operare şi a altor programe software, şi chiar prin distrugeri de natură hardware. Răspândirea acestor programe în rețea se face prin diverse servicii de rețea mai puțin protejate (de exemplu, unele sisteme de poştă electronică, de sharing de fişiere, de mesagerie în timp real etc.) sau prin intermediul mediilor de stocare externe (CD, DVD, *removable disk*) atunci când mecanismele de transfer de fişiere nu sunt verificate cu programe

specializate de detectare a virușilor şi a viermilor de rețea. De asemenea, rularea unor programe de protecție a sistemelor, de tip antivirus sau antispy, devine de cele mai multe ori ineficientă dacă acestea nu sunt corect configurate şi nu dispun de liste actualizate (*up-date*) cu semnăturile celor mai noi viruşi sau ale altor elemente de atacare a rețelei.

Viruşii de rețea (*viruses*) sunt programe inserate în aplicații, care prin automultiplicare pot determina saturarea completă a spațiului de memorie şi blocarea sistemului. Pătrunderea unui virus într-o rețea de comunicații o face vulnerabilă la orice formă de atac, tentativă de fraudă sau de distrugere. Infectarea se poate produce de oriunde din rețea. Cei mai mulți viruşi pătrund în sistem direct din Internet, prin serviciile de download, atunci când se fac up-date-uri pentru driverele componentelor sau pentru diferite programe software, inclusiv pentru sistemul de operare. Virușii rescriu porțiuni din fişiere de un anumit tip, nu infectează fişierele deja infestate pentru a nu-şi irosi resursele, sunt transportați de fişierele gata infectate. Serviciile gratuite oferite de diferite servere din Internet maschează de multe ori sursele de viruşi de rețea. De aceea, este indicată folosirea up-date-urilor oferite numai de firme consacrate, surse autentice de software, cu semnături recunoscute ca fiind valide de către sistemele de operare. De asemenea, prin verificarea periodică a sistemului de operare se pot depista la timp anumite erori sau modificări ale programelor (*sofware bugs*) şi se poate folosi soluții de refacere (*restore, backup*).

Bombele software au la bază proceduri sau porțiuni de cod-sursă incluse neautorizat în anumite aplicații, care sunt activate de un anumit eveniment predefinit: lansarea în execuție a unui program, deschiderea unui document sau fişier ataşat transmis prin poşta electronică, o anumită dată calendaristică (1 aprilie, vineri 13 etc.), accesarea unui anumit site web etc.

Viermii de rețea (*worms*) au de asemenea efecte de blocare sau de distrugere a datelor şi a rețelei ca şi viruşii şi bombele software. Principalele diferențe față de acestea sunt acelea că îşi schimbă permanent locația fiind dificil de detectat şi că nu se multiplică singuri. Cel mai renumit exemplu este viermele Internet-ului care reuşit să scoată din funcțiune un număr mare de servere din Internet în noiembrie 1988.

Trapele (*backdoors*) reprezintă căi de acces la sistem rezervate, folosite în mod normal pentru proceduri de întreținere (*maintenance*) de la distanță. Din cauza faptului că permit accesul nerestricționat la sistem sau pe baza unor date simple de identificare, acestea devin puncte vulnerabile ale rețelei care fac posibil accesul neautorizat al unor intruşi în rețea.

Calul Troian (*trojan horse*) este o aplicație care, pe lângă funcția de utilizare declarată, realizează şi o funcție secretă. Un astfel de program este dificil de observat deoarece nu creează copii. De exemplu, se înlocuieşte codul unui program normal de autentificare pe bază de nume de utilizator şi parolă, printr-un alt cod care, în plus, permite copierea într-un fişier a numelui şi parolei pe care utilizatorul le introduce de la tastatură. Contramăsurile folosite în acest caz constau în rularea programelor antivirus cu liste de semnături cât mai complete şi prin folosirea unor protocoale de comunicații şi programe securizate pentru accesarea serviciilor de Internet (HTTPS, anumite browsere de Internet, programe securizate de e-mail, ftp, telnet etc).

Rețelele botnet reprezintă un atac extrem de eficient din Internet. Atacatorii îşi creează o rețea din calculatoare deja compromise de o aplicație de tip *malware*, numite şi computere *bot*, pe care le comandă un *botmaster*. Prin intermediul acestei rețele şi al programelor de aplicații de Internet (de exemplu, e-mail, chat IRC – *Internet Relay Chat*), sunt lansate

diverse atacuri (*spam, spyware, adware, keylogger, sniffer,* DDoS ş.a.). Aceste rețele acumulează o putere de procesare extrem de mare consumând resursele calculatoarelor cooptate pentru execuția aplicațiilor.

În general, atacurile distribuite în rețea sunt dificil de urmărit şi de anihilat.

Controlul rețelelor *botnet* se poate face centralizat, peer-to-peer sau aleator. Pentru combaterea acestor rețele, este necesară întreruperea căilor de comandă şi control al lor (C&C – *Command and Control*).

În modul centralizat, serverul C&C poate fi oricare stație cu capacitate mare de procesare pe care sunt rulate aplicații de chat sau http. Prin intermediul acestuia se transmit comenzi către celelalte stații „*bot*" (în număr foarte mare, de ordinul sutelor). Canalele de comunicații folosite de atacatori sunt protejate de aceştia, de exemplu prin parole.

Rețelele *botnet* P2P sunt şi mai dificil de detectat pentru că identificarea şi anihilarea unei stații „*bot*" nu afectează restul rețelei. Acest tip de rețea poate incorpora până la 50 de calculatoare. Distribuția mesajelor C&C este mai dificilă şi se face cu oarecare întârzieri.

Deşi experimental, modul C&C aleator se dovedeşte a fi cel mai eficient şi prin implementarea acestuia, rețelele *botnet* vor fi foarte greu de distrus.

III.3 ATACURI CRIPTOGRAFICE

Atacurile criptografice se aplică direct mesajelor cifrate în vederea obținerii informației originale în clar şi/sau a cheilor de criptare şi de decriptare.

Prin definiție, **criptanaliza** este știința spargerii cifrurilor. **Criptanalistul** este persoana care se ocupă cu criptanaliza mesajelor cu caracter secret.

Scopul metodelor de criptanaliză este descoperirea mesajelor în clar (M) şi/sau a cheii (K) din mesajul criptat (C).

Se cunosc mai multe tipuri de atacuri criptografice:

- brut (*brute force*), prin încercarea tuturor combinațiilor posibile fie de chei de criptare, fie de simboluri din text pentru deducerea textului în clar (de exemplu, la metodele de criptare prin substituția sau transpoziția literelor din mesaje de tip text).
- asupra textului criptat (*cipher text attack*) interceptat, prin analiza căruia se încearcă găsirea textului original sau a cheii de criptare.
- asupra unui text în clar cunoscut (*known plain-text attack*), pentru care s-a aflat criptograma şi pe baza căruia se face o extrapolare pentru deducerea iterativă a altor porțiuni din mesaj.
- asupra unor texte criptate alese (*chosen cipher-text attack*), pentru care se obțin criptogramele asociate unor texte folosind algoritmi de criptare cu chei publice şi se urmăreşte aflarea cheilor de decriptare.

Observații:

1. Interceptarea mesajelor criptate se realizează printr-un atac de tipul „omul din mijloc”.
2. Un intrus se poate conecta la un server care oferă cheile publice de criptare prin atacuri de tip mascaradă autorizându-se ca o altă entitate.
3. Atacul brut devine ineficient atunci când lungimea cheii este suficient de mare încât numărul de încercări pe care trebuie să îl facă

un criptanalist depăşeşte capacitatea de procesare a celor mai performante sisteme de calcul iar durata de procesare criptanalitică este mai mare decât perioada de valabilitate a informațiilor transmise criptat. În medie, numărul de încercări necesare până la găsirea cheii corecte este egal cu jumătate din dimensiunea spațiului cheilor. Fiecare combinație încercată trebuie verificată dacă generează text în clar. Prin urmare timpul de atac este relativ mare.

4. Un alt tip de atac, cu conotații sociale şi psihologice, este acțiunea de "cumpărare" a cheii, adică aflarea cheii fără nici un efort de criptanaliză, prin alte mijloace decât cele tehnice (şantaj la adresa persoanelor care o dețin, furt sau scurgeri de informații de la persoane sau din documente scrise sau în fomat electronic etc.). Acest procedeu este unul dintre cele mai puternice atacuri lansate la adresa unor surse din interiorul rețelei. Pentru preîntâmpinarea lui este utilă responsabilizarea personalului, eliminarea breşelor de securitate a documentelor, eventual dubla criptare a datelor astfel încât secretul lor să nu depindă de o singură persoană.
5. Atacul de tip "întâlnire" (*meet-in-the-middle attack*) a fost dezvoltat pentru criptosistemele cu dublă criptare. Acesta presupune criptarea unui text în clar cunoscut cu fiecare cheie posibilă la un anumit capăt şi compararea rezultatului cu ceea ce se obține prin decriptarea textului criptat aferent. Aparent timpul de atac este crescut exponențial, dar în realitate se constată doar o dublare a acestuia.

   Ca şi metode de criptanaliză, s-au dezvoltat următoarele:

- **Metoda diferențială:** este folosită pentru spargerea algoritmilor cu cheie secretă, pe baza unei perechi de texte criptate, obținute prin

criptarea unei perechi de texte în clar şi analiza diferenţelor dintre acestea.

- **Metoda liniară:** foloseşte texte în clar cunoscute şi textele criptate asociate încercând pe baza lor aproximarea liniară a cheii de criptare.
- **Metoda combinată, diferenţial-liniară:** aplică ambele procedee menţionate anterior pentru spargerea cifrurilor.

La data apariţiei criptanalizei diferenţiale, algoritmul DES era singurul care rezista la toate formele de atac cunoscute. Între timp, capacitatea procesoarelor a crescut vertiginos şi spargerea DES este o chestiune de minute. A devenit necesară creşterea complexităţii algoritmului. S-a propus algoritmul Triple DES, cu cheie de criptare mai lungă, dar nici acesta nu s-a dovedit a fi suficient de sigur şi s-a impus proiectarea unor noi algoritmi.

Ca regulă generală, un algoritm este considerat sigur dacă cea mai puţin costisitoare metodă prin care poate fi atacat (ca timp de procesare, spaţiu de memorie, preţ) este atacul brut.

Capitolul IV PROTOCOALE ŞI SERVERE DE SECURITATE

Protocoalele de securitate a rețelelor de comunicații sunt definite pentru a stabili modul în care sunt oferite serviciile de securitate.

Aceste protocoale de securizare a comunicațiilor pot lucra pe diferite nivele ale modelului OSI:

- pe nivelul legăturii de date: protocoale de tunelare, precum L2TP (*Layer2 Tunnelling Protocol*) care, deşi definit pe acest nivel, operează de fapt pe nivelul OSI 5, de sesiune.
- pe nivelul de rețea: IPsec (*IP Security*) oferă servicii de autentificare, de control al accesului, de confidențialitate şi integritate a datelor.
- pe nivelul de transport: TLS (*Transport Layer Security*), SSL (*Secure Socket Layer*), protocolul Handshake de autentificare mutuală a clienților şi serverelor şi negocierea algoritmilor de criptare înaintea desfăşurării propriu-zise a transmisiei datelor.
- pe nivelul de aplicație: SSH (*Secure Shell*), PGP (*Pretty Good Privacy*), S/MIME (*Secure Multipurpose Internet Mail Extension*) şi altele.

Descrierea protocoalelor de securitate se va face în funcție de serviciile de securitate oferite şi de arhitectura folosită pentru aplicațiile de rețea.

De cele mai multe ori, se definesc suite de protocoale de securitate (IPsec, KERBEROS, SESAME şi altele).

Implementarea suitelor de protocoale de securitate în rețelele de comunicații se face cu mai multe servere de rețea dedicate diferitelor servicii:

- servere de autentificare
- servere de certificare
- servere de distribuție a cheilor de criptare
- servere de gestiune a cheilor de criptare etc.

IV.1 IPSEC

Serviciile de securitate a rețelelor de comunicații sunt implementate pe baza protocoalelor de securitate în diferite soluții tehnice, hardware şi software.

Există diferite metode de asigurare a securității transmisiei într-o rețea prin operații de autentificare a utilizatorilor, criptare a mesajelor, filtrare a traficului etc.

Protocoalele de securitate din Internet se aplică pe diferite nivele (fizic, legătură, rețea, aplicație). Fiecare poate oferi unul sau mai multe servicii de securitate.

Se pot utiliza programe software specializate pentru asigurarea securității transmisiei datelor în rețea.

Primele măsuri de securitate a rețelelor defineau asociații de securitate (SA - *Security Association),* adică grupuri de utilizatori autorizați să folosească o anumită rețea, denumită **rețea virtuală privată** (VPN - *Virtual Private Network).* Ca o extensie a acestora, în rețelele wireless se

pot configura rețele private virtuale ad-hoc (VPAN – *Virtual Private Ad-Hoc Networks*).

În prezent, în rețelele de arie largă bazate pe TCP/IP se poate utiliza suita de protocoale de securitate IPsec *(Internet Protocol Security Facility),* care realizează criptarea şi autentificarea pachetelor IP cu performanțe superioare sistemului inițial SA. VPN pot fi configurate în mod adecvat să aplice protocoalele de securitate din suita IPsec.

Gradul de protecție a pachetelor IP şi cheile de criptare utilizate de IPsec se stabilesc prin mecanismul IKE (*Internet Key Exchange)* descris de protocolul cu acelaşi nume, care se aplică împreună cu protocolul ISAKMP (*Internet Securiţy Association and Key Management Protocol),* Astfel IPsec beneficiază de serviciile ISAKMP/IKE.

IPsec oferă următoarele servicii de securitate pe nivelul IP al rețelelor TCP/IP:

- integritatea conexiunii - asigură faptul că în procesul de comunicație nu intervin entități neautorizate care să modifice datele sau să genereze mesaje false în rețea;
- autentificarea sursei de date - permite identificarea sursei şi asigurarea autenticității mesajelor;
- criptarea datelor - asigură confidențialitatea mesajelor transmise şi imposibilitatea preluării neautorizate a informațiilor;
- protecția la atacuri în rețea - detectează pachetele repetitive, replici ale aceluiaşi pachet, care se transmit la infinit în rețea şi pot produce blocaje sau saturarea rețelei *(flooding).*

IPsec asigură mai multe ***servicii de securitate***: autenticitatea pachetelor şi integritatea conexiunii (AH - *Authentication Header*), criptarea şi/sau autenticitatea pachetelor (ESP - *Encapsulating Security Payload*) şi

mecanisme pentru stabilirea parametrilor conexiunii (SA- *Security Association*).

Autentificarea sursei se face pe baza protocolului AH *(IP Authentication Header)* din suita IPsec (RFC 2401, RFC 2402). Acest protocol asigură integritatea conexiunii şi a datelor transmise, precum şi autenticitatea mesajelor. AH asigură securitatea integrală a pachetelor IP, inclusiv a antetelor de securitate ataşate ulterior acestora.

Serviciile de securitate sunt asigurate şi de protocolul ESP de încapsulare a pachetelor IP (*IP Encapsulating Securiţy Payload),* care stabileşte operații de criptare a datelor şi de autentificare a sursei de informații (RFC 2406).

ESP oferă servicii de securitate numai protocoalelor de pe nivelele superioare celui de rețea, excluzând antetele de securitate ulterior adăugate pachetelor.

Protocoalele AH şi ESP pot fi implementate prin diverşi algoritmi software şi se pot aplica fie individual, fie ambele simultan, în funcție de gradul de securitate impus pachetelor IP (RFC 2403, RFC 2404).

IPsec asigură securitatea comunicației dintre două calculatoare-gazdă, dintre două echipamente de comunicații (de exemplu, rutere) sau dintre un DTE şi un DCE.

Un router sau un server pe care sunt activate protocoalele de securitate IPsec se numeşte poartă de securitate (*securiţy gateway)* sau "zid" de protecție *(firewall).*

În general, asigurarea securității unei transmisii se realizează la ambele capete ale căii de comunicație, cu două echipamente care folosesc IP sec lucrând în pereche *(IPsec peers).*

Cele două protocoale de securitate (AH sau ESP) pot acționa în două moduri:

1. **modul de transport** (*transport mode*) - protocolul de securitate intervine în pachetul IP şi adaugă un antet de securitate imediat după antetul IP (cu sau fără opțiuni exprimate) dar antetul IP inițial (header-ul) nu se modifică, doar datele transmise sunt securizate (criptate şi/sau autentificate). Prin folosirea protocolului AH, adresele IP ale sursei, respectiv destinației, nu pot fi modificate pe parcurs deoarece acest lucru ar duce la modificarea valorii hash. ESP oferă protecție minimă protocoalelor de nivel superior, în timp ce AH securizează total pachetul, inclusiv antetul IP. Acest mod de operare se utilizează pentru schimbul de pachete între calculatoarele-gazdă (*host-to-host*).

2. **modul de tunelare** *(IP tunneling)* - întregul pachet (date şi antete) este securizat. Se introduc două antete de securitate în fiecare pachet, înainte *(outer header)* şi după *(inner header)* antetul EP. Antetul extern specifică perechea de entități între care se creează tunelul IP şi se aplică măsurile de securitate pe baza IPsec. Antetul intern precizează destinația finală a pachetului pentru realizarea rutării. ESP protejează numai pachetul transmis prin tunelul IP, în timp ce AH asigură şi securitatea antetului exterior ataşat. De regulă acest mod de operare se utilizează între porți de securitate care execută împachetarea şi despachetarea mesajelor (*gateway-to-gateway*).

Configurarea echipamentelor dintr-o rețea în vederea aplicării IPsec se realizează de către o persoană cu drepturi depline de stabilire a securității rețelei *(security officer)*, în trei etape:

1. crearea grupurilor de securitate (SA) şi stabilirea drepturilor şi atribuțiilor acestora;

2. configurarea legăturilor dintre SA-uri şi stabilirea ierarhiilor de priorități, folosind ISAKMP/IKE (RFC 2408, RFC 2409);
3. stabilirea modalităților de clasificare a pachetelor IP şi de acțiune asupra lor (permite sau interzice accesul în rețea, aplică procedurile de securitate conform IPsec).

Aceste configurații referitoare la IPsec sunt stocate în bazele de date pentru securitatea rețelei (SPD - *Security Policy Database),* la care are acces doar administratorul de rețea.

Prin SA înțelegem o conexiune simplex definită pe o pereche IPsec, pentru securitatea traficului doar într-un sens, folosind un singur protocol de securitate (AH sau ESP).

Pentru transmisiile duplex se defineşte câte un SA pentru fiecare sens de comunicație cu rețeaua *(inbound/outbound traffic).*

Dacă la unul din capetele canalului de comunicație definit de SA, se găseşte un echipament de securitate *(security gateway; firewall),* atunci este obligatoriu ca acel SA să lucreze în modul de tunelare pentru a evita problemele create prin fragmentarea pachetelor şi de existența căilor multiple de rutare.

Un SA este identificat prin trei parametri:

1. un număr aleator denumit identificator de securitate (SPI - *Security Parameter Index);*
2. adresa **IP de destinație;**
3. **protocolul de** securitate (AH sau ESP).

Dacă este necesară utilizarea ambelor protocoale de securitate în Internet (AH şi ESP), atunci se creează şi se configurează legăturile dintre două sau mai multe SA.

Regulile de securitate aplicate într-o rețea folosind IPsec sunt memorate în SPD. Acestea stabilesc trei moduri posibile de acțiune asupra pachetelor IP:

1. se aplică pachetului, serviciile de securitate conform IPsec;
2. se interzice accesul pachetului în rețea *(deny);*
3. se acordă permisiunea de acces în rețea, fără aplicarea măsurilor de securitate IP (*bypass IPsec).*

Modul de acțiune asupra unui pachet IP se stabileşte pe baza antetelor conținute de acesta, prin operația de clasificare a pachetelor, în funcție de diverşi factori de selecție:

- adresa IP a sursei;
- adresa IP a destinației;
- portul-sursă;
- portul-destinație;
- protocolul de transport;
- numele utilizatorului sau al sistemului;
- gradul de prioritate a informațiilor conținute în pachet.

Aplicarea măsurilor de securitate IPsec asupra unui pachet (autentificare, criptare, compresie), se realizează pe baza mecanismului ISAKMP/TKE prin care se generează şi se transmit între părți cheile de criptare utilizate de SA în diferite sesiuni, memorate într-o bază de date proprie ISAKMP ca atribute ale SA.

În rețelele TCP/IP, se utilizeazează diverşi algoritmi de criptare, uzuali fiind cei cu cheie publică (RSA, Diffie-Hellman, DES, 3DES etc).

De exemplu, protocolul SSH, utilizat pentru transferul securizat al fişierelor şi al mesajelor prin sistemul de poştă electronică din Internet, foloseşte diverşi algoritmi de criptare cu cheie publică. Operația de

autentificare se bazează de asemenea pe secvențe de tip 'cheie de transmisie'.

IV.1.1 PROTOCOLUL AH

Protocolul AH (*Authentication Header*) asigură autenticitatea mesajelor şi a tuturor informațiilor adiționale incluse în pachet precum şi integritatea pachetului de date, prin aplicarea funcților hash. AH împiedică modificarea ilegală a pachetelor, multiplicarea sau întârzierea datelor (*anti-replay security*).

Diagrama unui pachet AH este prezentată în figura IV.1.

Biții 0 - 7	8 – 15	16 - 23	24 - 31
Antetul următor	Lungimea pachetului	Câmp REZERVAT	
Identificatorul de securitate			
Numărul de secvență			
Informația de autenticitate			

Figura IV.1 Diagrama unui pachet AH

Semnificațiile câmpurilor sunt următoarele:

- antetul următor (*next header*) - identifică protocolul de transfer al datelor;

- lungimea pachetului AH (*payload length*) exprimată în cuvinte de 32 de biți;
- câmp rezervat cu toți biții 0, care poate fi utilizat ulterior în alte scopuri;
- Identificatorul de securitate (SPI - *Security Parameters Index*) identifică asociația de securitate (SA - S*ecurity Association*) implementată în acest pachet;
- Numărul de secvență (*sequence number*) - reprezintă un număr monoton crescător, folosit pentru a evita atacurile de reluare a datelor (*replay attacks*);
- Informația de autenticitate (*authentication data*) - conține valoarea de verificare a integrității (ICV - *Integrity Check Value*) sau codul de autentificare a mesajului (*MAC - Message Authentication Code*), necesare pentru verificarea autenticității pachetului.

IV.1.2 PROTOCOLUL ESP

Protocolul ESP (*Encapsulating Security Payload*) asigură autenticitatea, integritatea şi confidențialitatea pachetelor de date. Spre deosebire de protocolul AH, antetul pachetului IP nu este protejat de ESP. Confidențialitatea datelor este asigurată prin criptare.

Diagrama unui pachet ESP este dată în figura IV.2.

Pachetul ESP conține următoarele câmpuri:

- Identificatorul de securitate (SPI - *Security Parameters Index*) al asociației de securitate implementate (SA);

Biții 0 - 7	**8 - 15**	**16 - 23**	**24 - 31**
Identificatorul de securitate			
Numărul de secvență			
Mesaj transmis (câmp de lungime variabilă)			
	Expandare (0-255 octeti)		
		Lungimea câmpului de expandare	Antetul următor
Informația de autentificare (câmp de lungime variabilă)			

Figura IV.2 Diagrama unui pachet ESP

- Numărul de secvență (SN - *Sequence Number*), număr generat dintr-un şir monoton crescător, folosit pentru a preveni atacurile de reluare;
- Informația transmisă (*payload data*) – mesajul de pe nivelul de transport (în mod transport) sau IP (în mod tunel) care este protejat prin criptare;
- Expandare (*padding*)- câmp folosit împreună cu unele cifruri-bloc pentru a acoperi lungimea totală a blocului;
- Dimensiunea câmpului de expandare (*pad length*) – exprimată în octeți;
- Antetul următor (*next header*), identifică protocolul de transfer al datelor;

- Informația de autentificare (*authentication data*) - câmpul conține valoarea de verificare a integrității (ICV – *Integrity Check Value*).

La trecerea pachetului de date prin diferite tunele şi porți de securitate, acestuia îi sunt adăugate şi alte antete. Un antet se aplică unui pachet la începutul fiecărui tunel. După verificare, la ieşirea din tunel, antetul este eliminat.

IV.1.3 ASOCIAȚII DE SECURITATE

Un concept de bază, care apare în mecanismele IP pentru autentificare şi confidențialitate, este asociația de securitate (SA - *Security Association*). SA este o relație unidirecțională între o sursă şi o destinație care asigură servicii de securitate traficului efectuat pe baza ei. Pentru un schimb securizat bidirecțional, sunt necesare două asociații de securitate.

Serviciile de securitate pot fi asigurate de o asociație de securitate, fie pentru utilizarea protocolului AH, fie pentru protocolul ESP, dar nu pentru ambele. Dacă este necesară utilizarea ambelor protocoale de securitate în Internet (AH şi ESP), atunci se creează şi se configurează legăturile dintre două sau mai multe SA-uri.

O asociație de securitate este definită în mod unic de trei parametri:

- **Identificatorul de securitate** constă într-un şir de biți cu semnificație locală, inclus în antetele AH şi ESP pentru a permite destinației să selecteze SA-ul pentru procesarea pachetului recepționat;
- **Adresa IP de destinație** este adresa nodului de destinație al asociației de securitate, care poate fi un calculator-gazdă (*host*) sau

un echipament de comunicație al rețelei (router, firewall, access point);

- **Identificatorul protocolului de securitate** indică pentru care protocol, AH sau ESP, lucrează SA.

IV.1.4 APLICAȚII ALE IPSEC

IPsec oferă posibilitatea unei comunicări sigure în rețelele de arie largă (WAN), în aplicații precum:

- **Definirea rețelelor virtuale private** (VPN – *Virtual Private Network*), în care uzual IPsec este configurat să folosească protocolul ESP în modul tunel pentru furnizarea confidențialității. Pentru o organizație cu mai multe rețele locale, aflate în diferite locații, traficul intern rețelelor locale nu este securizat în timp ce traficul între acestea utilizează IPsec pentru securizare. IPsec este activat în echipamentele de acces la rețeaua de arie largă, de exemplu în gateway, router sau firewall. Operațiile de criptare/decriptare şi de autentificare executate de IPsec sunt transparente pentru stațiile de lucru şi serverele din rețelele locale.
- **Accesul securizat de la distanță** prin rețeua publică de Internet la un sistem în care este implementat protocolul IPsec. Se poate apela la un furnizor de Internet (ISP - *Internet Service Provider*) pentru a obține accesul securizat la o rețea privată.
- **Îmbunătățirea securității aplicațiilor** distribuite care au o serie de mecanisme de securitate incluse.

Principala caracteristică a IPsec care îi permite să securizeze o gamă atât de largă de aplicații distribuite (e-mail, transfer de fisiere, acces Web etc.), este faptul că pentru întregul trafic IP se pot utiliza mecanismele de criptare şi/sau autentificare.

IV.2 PROTOCOLUL KERBEROS

Kerberos este un protocol de autentificare şi de control al accesului în rețele, pentru aplicații distribuite.

A fost proiectat pe baza modelului client-server şi asigură autentificarea mutuală, adică atât utilizatorul cât şi serverul se autentifică unul față de celălalt.

Denumirea protocolului a fost preluată din mitologia greacă, de la câinele cu trei capete pe care îl chema Kerberos. Similar, protocolul cu acelaşi nume implică trei entități: clientul, serverul şi centrul de distribuție a cheilor (KDC – *Key Distribution Center*). Protocolul impune existența unei terțe părți de încredere, KDC, intermediară în aplicația client-server. Acestea nu trebuie neapărat să îşi acorde reciproc încredere, ci ambele trebuie să aibă încredere în KDC.

KDC are două părți:

- un server de autentificare (*Authentication Server* - AS);
- un server de alocare a tichetelor (*Ticket Granting Server* - TGS).

Mesajele protocolului Kerberos sunt protejate împotriva atacurilor de ascultare (*eavesdropping)* şi de reluare a mesajelor (*replay*).

Kerberos utilizează tehnici simetrice de criptare şi oferă un sistem de mesaje criptate numite **tichete**, care asigură în mod securizat încrederea reciprocă dintre două entități din rețea. Utilizând Kerberos, parolele nu mai sunt transmise prin rețea, nici măcar criptate. În cazul în care un tichet Kerberos este interceptat acesta rămâne protejat deoarece este criptat cu algoritmi robuşti de criptare.

Odată ce o entitate-client obține un tichet către un anume server, tichetul este păstrat pe calculatorul local până la expirare, făcând astfel din Kerberos un sistem de autentificare foarte eficient. Depinde de implementare, dar în mod uzual un tichet Kerberos expiră după opt ore.

KDC deține o bază de date cu toate cheile secrete. Fiecare entitate din rețea, fie client, fie server, deține o cheie secretă, cunoscută doar de ea şi de KDC. Această cheie constituie dovada identității unei entități.

Pentru o comunicare sigură între două entități din rețeaua publică, KDC generează o **cheie a sesiunii**.

Pentru a înțelege principiul de funcționare a protocolului, trebuie introduse următoarele noțiuni:

- Serverul TGS (*Ticket Granting Server*) oferă tichete de tip sesiune pentru accesarea altor resurse. De obicei, TGS rulează în KDC.
- Tichetul TGT (*Ticket Granting Ticket*) reprezintă un jeton de validare a unui tichet Kerberos care atestă faptul că o entitate a fost deja autentificată şi ne asigură că utilizatorii nu mai trebuie să reintroducă parola după un login inițial, până la expirarea tichetului.
- Tichetul de sesiune ST (*Session Ticket*) reprezintă un jeton de sesiune care permite accesul la resurse protejate. Pentru accesarea oricărei aplicații care utilizează Kerberos este necesar un tichet de sesiune valid.

Procesul de autentificare Kerberos se desfăşoară în mai mulți paşi:

Utilizatorul unui sistem client, utilizând un username si o parolă sau un smart card, se autentifică față de server-ul de autentificare (AS din KDC);

- AS emite clientului un tichet de tip TGT pe care îl utilizează pentru a accesa TGS.
- TGS emite un tichet de sesiune (ST) către client.
- Clientul prezintă acest tichet serviciului de rețea accesat. Tichetul de sesiune dovedeşte atât identitatea utilizatorului către serviciu, cât şi a serviciului față de client.

Observații:

- Faptul că se utilizează un server central, furnizarea serviciului se poate întrerupe (DoS) atunci când acesta nu mai funcționează, deoarece nimeni nu îl mai poate apela. Această situație poate fi evitată dacă se utilizează mai multe servere Kerberos.
- Având în vedere că toate cheile secrete ale utilizatorilor sunt stocate în serverul central, compromiterea acestuia poate duce la compromiterea tuturor cheilor.
- Kerberos necesită sincronizarea entităților apelante cu server-ul iar dacă acestea nu sunt sincronizate, atunci procesul de autentificare nu poate avea loc. Se impune să nu existe o diferență de timp mai mare de 10 minute. În practică, se poate utiliza protocolul *NTP* (*Network Time Protocol*) pentru realizarea sincronizării.

Serviciul de autentificare extinsă Kerberos v5 (RFC 1510) se bazează atât pe mecanismul de autentificare cu nume şi parolă, cât şi pe sistemul de criptografie cu chei publice (PKC – *Public Key Cryptosystem*).

IV.3 PROTOCOLUL SESAME

Protocolul SESAME (*Secure European System for Applicxations in a Multivendor Environment*) este rezultatul unui proiect al Asociației Fabricanților Europeni de Calculatoare (ECMA – *European Computer Manufacturer Asociation*) propus pentru optimizarea şi extinderea protocolului Kerberos pentru controlul distribuit al accesului în rețea.

SESAME foloseşte interfața de aplicații GSS-API (*Generic Security Services Application Program Interface*) care ascunde detaliile de securitate lucrând în mod transparent față de utilizatori.

SESAME modifică modul de implementare a algoritmilor de criptare DES, RSA şi MD5 adoptat de protocolul Kerberos, precum şi funcțiile de dispersie.

SESAME foloseşte o tehnică de autorizare şi control al accesului similară celei aplicate de protocolul Kerberos, cu autentificare a clientului de către AS. Suplimentar, este necesară şi autentificarea de către un server de privilegii (PAS – *Privilege Attribute Server)* care eliberează un certificat de privilegii (PAC – *Privilege Attribute Certificate*) după prezentarea unei dovezi de autenticitate. Certificatul este semnat cu cheia privată a serverului emitent. În certificat se specifică identitatea şi rolul utilizatorului, grupul organizațional căruia îi aparține, permisiuni şi restricții impuse, condiții de utilizare a certificatului.

După obținerea certificatului, clientul se adresează serverului KDS (*Key Distribution Center Server*), conform RFC 3634, pentru obținerea tichetului de serviciu.

Se observă că protocolul SESAME se aplică pas-cu-pas prin mai multe procese succesive de comunicație client-server.

În versiunile mai noi ale protocolului, aceste procese de comunicație cu serverele AS, PAS şi KDS sunt rulate pe un server de securitate a domeniului SESAME (DSS – *Domain Security Server*) pe care este instalată o bază de date care gestionează toate informațiile de securitate din domeniu (SMIB – *Security Management Information Base*). Fiecare domeniu dispune de o autoritate locală de înregistrare a utilizatorilor (LRA – *Local Registration Authority*) de la care se obțin informații de la autoritatea de certificare (CA – *Certificate Authority*), prin intermediul agenților de certificare (CAA – *CA Agent*) (Figura IV.3). Certificatele sunt criptate cu chei publice pe baza mecanismului de autentificare X.509 fiind necesar un mecanism de gestionare şi de distribuție a cheilor publice în rețea.

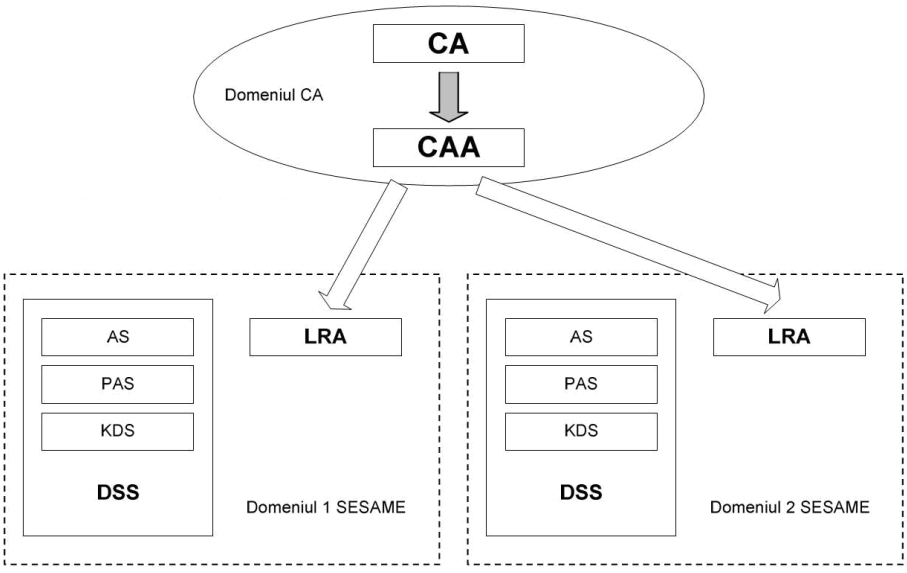

Figura IV.3 Domenii de securitate SESAME

În domeniul CA, serverele comunică în modul asincron. Serverul CA operează offline, în timp ce serverul CAA este online. Comunicația dintre LRA şi CAA se realizează în mod sincron.

Arhitectura SESAME include suplimentar (Figura IV.4):

1. sponsorul clientului care furnizează o interfață de aplicații US (*User Sponsor*).
2. modulul APA (*Authentication Privilege Atribute*) care asigură transparența serviciilor de securitate oferite de SESAME
3. managerul de context SACM (*Secure Association Context Manager*) prin care se asigură autentificarea mutuală client-server.
4. managerul cheilor publice PKM (*Public Key Manager*)
5. modulul de validare a certificatelor PVF (PAC *Validation Facility*)
6. componenta de audit realizează doar înregistrări ale evenimentelor de securitate astfel încât acestea să nu poată fi modificate de aplicațiile-proces. Analiza de audit nu cade în sarcina sistemului SESAME.
7. Facilitatea de suport criptografic (CSF – Cryptographic *Support Facility*) implementează algoritmi criptografici utilizați fie de componentele SESAME sau de alte aplicații. Algoritmii utilizați în curent de SESAME sunt DES-CBC, RSA, MD5 şi DES-MD5. CSF a fost proiectat astfel încât algoritmii să poată fi înlocuiți iar mărimile cheilor ajustate în funcție de legislația locală. Din motive de control al exportului, versiunea publică a sistemului SESAME foloseşte un simplu XOR pentru a cripta datele.

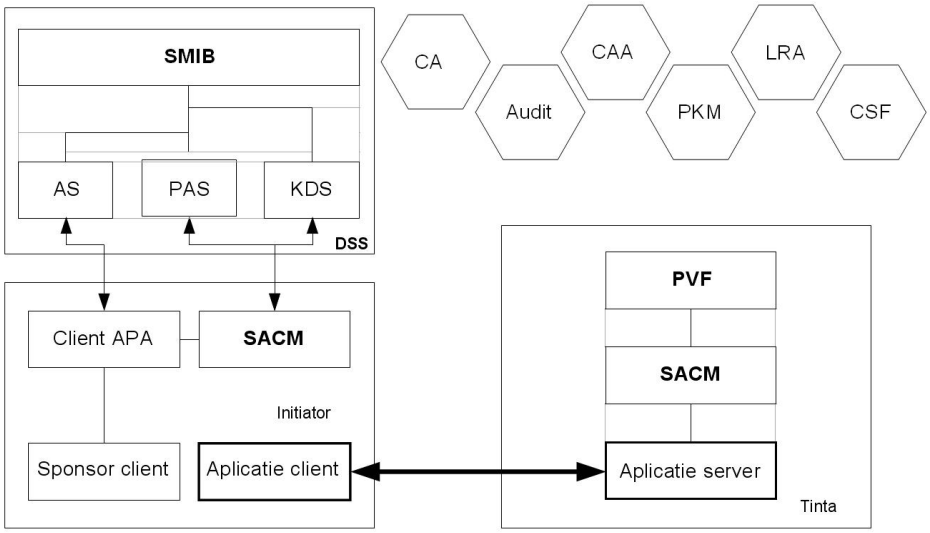

Figura IV.4 Arhitectura sistemului SESAME

SESAME foloseşte o ierarhie de chei cu două niveluri:

- O cheie simplă - stabilită şi utilizată între un SACM inițiator şi PVF-ul SACM-ului țintă, pentru a proteja PAC-urile corespunzătoare precum şi informațiile de stabilire a cheilor.
- O cheie de dialog - derivată din cheia simplă cu o funcție de dispersie cu sens unic (*one-way function*). Scopul acesteia este de a proteja datele schimbate într-un context de securitate.

Pentru protecția integrității şi a confidențialității se pot stabili chei de dialog separate, permițând ca mecanisme cu puteri de criptare diferite să fie utilizate conform cu legislația locală.

SESAME este proiectat pentru sisteme deschise, cu echipamente de la diferiți producători (*multi-vendor*), pentru servicii de autentificare, de confidenţialitate şi integritate a datelor, de autorizare şi control al accesului în aplicații distribuite în rețea.

IV.4 PROTOCOLUL RADIUS

RADIUS *(Remote Authentication Dial In User Service*) este un protocol de autentificare, autorizare şi gestionare a conturilor de utilizator (*AAA- Authentication, Authorization, Accounting*) care asigură controlul accesului la resursele unei rețele. RADIUS este utilizat de furnizorii de servicii Internet (ISP- *Internet Service Provider*) şi de alte organisme care administrează accesul la Internet sau la rețelele interne.

Un pachet RADIUS (Figura IV.5) conține următoarele câmpuri:

- Cod (*type*) - specifică tipul pachetului RADIUS (1B);
- Identificator (*identifier*) - prin care se realizează legatura dintre cerere şi răspuns (1B);
- Lungime (*length*) - indică lungimea întregului pachet, minimum 20 B, maximum 4096 B (2B);
- Autentificator (*authenticator*) - reprezintă informația prin care este autentificat răspunsul server-ului RADIUS (16 B);
- Atribute (*attributes*) - câmp de lungime variabilă care conține lista tuturor informațiilor necesare pentru un anumit tip de serviciu. Un atribut este format din trei câmpuri: nume, lungime şi valoare.

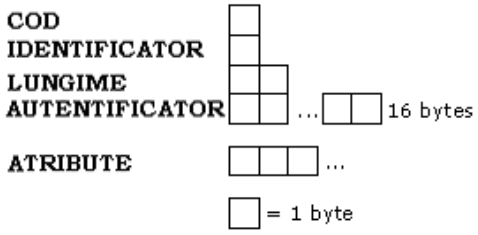

Figura IV.5 Structura pachetului RADIUS

Atributele pot fi împărțite în patru categorii:

- atribute de management ale protocolului RADIUS;
- atribute de identificare şi autentificare a utilizatorului;
- atribute de autorizare care arată tipul serviciului furnizat utilizatorului;
- atribute de gestionare a contulurilor care indică modul de utilizare a serviciului.

Serverele RADIUS utilizează conceptul AAA pentru a administra accesul în rețea, în trei paşi:

1. **Autentificarea clientului**

Clientul cere permisiunea de accesare a resurselor rețelei unui server de acces la rețea (NAS - *Network Access Server*). NAS trimite server-ului RADIUS o cerere de acces (*access request*), prin care solicită autorizația de a permite accesul. Aceasta cerere include şi o formă de identificare a clientului, un nume de utilizator şi o parolă sau un certificat digital, furnizate de acesta. În plus, cererea poate include alte informații cunoscute de NAS, cum ar fi: adresa de rețea (*MAC- Media Access Control*), numărul de telefon, informații cu privire la conexiunea fizică dintre NAS şi client.

2. **Autorizarea**

Cererea de acces inițiată de NAS este procesată de server-ul RADIUS. Acesta caută într-o listă internă de conturi, contul utilizatorului pentru a verifica informațiile despre acesta. Identitatea utilizatorului este verificată şi, opțional alte informații cu privire la cererea acestuia.

Server-ul RADIUS poate furniza unul dintre următoarele răspunsuri:

- Acces respins (*Access-Reject*) utilizatorului, la toate resursele rețelei pentru care a adresat cererea, pentru că nu s-a dovedit identitatea acestuia sau contul acestuia nu este recunoscut sau activ.
- Acces permis (A*ccess-Accept*) utilizatorului. Atributele autorizației sunt trimise către NAS de serverul RADIUS, inclusiv limitarea timpului de acces sau a cantității de informație şi restricțiile de securitate referitoare la controlul accesului şi adresele de rețea ataşate.
- Răspuns (*Access-Challenge*) prin care se cer informații suplimentare de la client, cum ar fi de exemplu o a doua parolă.

3. Gestionare cont

Atunci când se acordă accesul la rețea, unui utilizator, de către NAS, un mesaj de inițiere a contului (*accounting start*) este trimis de NAS server-ului RADIUS pentru ai semnala acestuia că un utilizator a accesat rețeaua. Acest mesaj de obicei conține: identitatea utilizatorului, adresele de rețea şi ID-ul unic al sesiunii deschise de utilizator.

Periodic NAS poate trimite mesaje intermediare (*interim accounting*) către RADIUS pentru a-l înştiința cu privire la starea unei sesiuni active. În final, când sesiunea se încheie, NAS trimite un mesaj de încheiere server-ului RADIUS (*accounting stop*) cu informații cu privire la timpul, data, motivul deconectării şi alte informații cu privire la accesul utilizatorului la rețea.

Pentru protectia parolelor trimise între NAS şi server-ul RADIUS, se pot utiliza tunele IPsec, pentru criptarea traficului. De regulă, se utilizează pentru criptarea informațiilor algoritmul RSA.

Serverul RADIUS a fost implementat în sistemul de operare MS Windows 2000 ca server IAS (*Internet Authentication Service*) care realizează centralizat operațiile de autentificare, autorizare, audit şi de cont (AAAA) pentru conexiuni prin dial-up sau VPN, de acces la servicii de la distanță sau la cerere, cu echipamente fabricate de un producător unic (*single vendor*) sau de mai multe firme producătoare (*multi-vendor*).

IV.5 PROTOCOLUL DIAMETER

Odată cu creşterea numărului de utilizatori şi al punctelor de acces, a numărului de servicii şi a complexității acestora, protocolul RADIUS nu a mai putut îndeplini toate cerințele AAA. A fost nevoie de un nou protocol, capabil să îndeplinească toate noile probleme apărute în controlul accesului şi să mențină flexibilitatea, pentru dezvoltări ulterioare.

DIAMETER (“diametru”) nu este un protocol nou, ci o versiune îmbunătățită a protocolului RADIUS (“rază”).

DIAMETER utilizează o arhitectură *peer-to-peer*, astfel încât fiecare calculator-gazdă care foloseşte acest protocol poate juca atât rolul de client, cât şi pe cel de server.

Un dispozitiv care primeşte o cerere de conectare la rețea, se va comporta ca server de acces la rețea (NAS – *Network Access Server*), care, după colectarea datelor despre client (nume de utilizator, parolă, certificat digital ş.a.), trimite o cerere de acces (*access request*) serverului DIAMETER. Acesta, pe baza informațiilor primite, autentifică utilizatorul. Dacă procesul de autentificare se face cu succes, privilegiile de acces ale

utilizatorului sunt incluse într-un mesaj de răspuns, care este trimis înapoi serverului NAS.

Mesajele serverului DIAMETER (figura IV.6) sunt de mai multe tipuri şi se deosebesc prin codul de comandă din fiecare pachet. Schimbul de mesaje DIAMETER se face sincron, adică fiecare cerere are propriul răspuns, însoțit de acelaşi cod de comandă.

Codul de comandă stabilește tipul mesajului, dar informația propriu-zisă este transportată printr-un set de AVP-uri (AVPs - *Attribute-Value-Pairs*). Aceste AVP-uri conțin detalii cu privire la autentificarea unui utilizator, autorizarea şi gestionarea conturilor, dar şi informații cu privire la rutarea pachetelor şi securitatea acestora între două noduri DIAMETER.

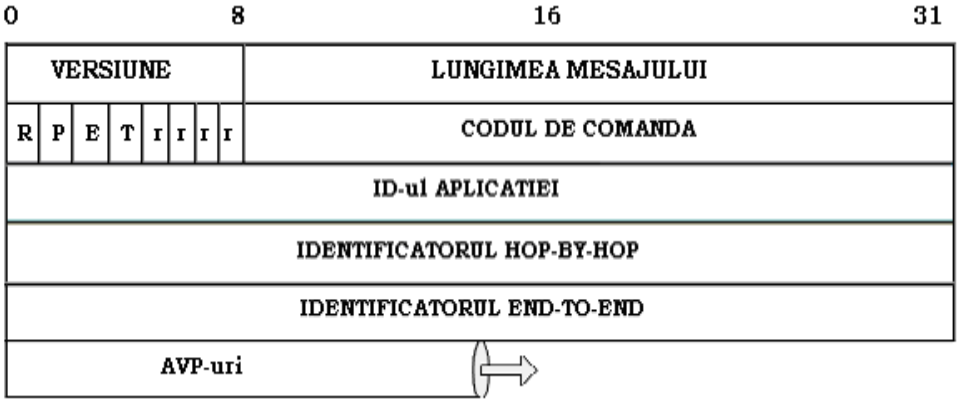

Figura IV.6 Structura pachetului DIAMETER

Un pachet DIAMETER include câmpurile:

- Versiune (*version*) - indică versiunea de protocol.
- Lungime a mesajului (*message length*) - indică lungimea întregului pachet.
- Biți de comandă (*command flags*):
  - R (*request*) - indică dacă mesajul este o cerere sau un răspuns.

- P (*proxiable*) - arată dacă mesajul trebuie redirecționat sau procesat local;
- E (*error*) - indică o eroare a protocolului;
- T (*re-transmitted message*) - arată daca mesajul a mai fost transmis;
- r (*reserved*) - biți rezervați.

- Codul de comanda (*command code*) - face legatura dintre tipul mesajului-cerere şi tipul mesajului-răspuns;
- Identificatorul aplicației (application ID) - identifică aplicația pentru care a fost trimis mesajul;
- Identificatorul *hop-by-hop* - asigură legatura dintre cerere şi răspuns;
- Identificatorul *end-to-end* - detectează mesajele duplicat.

AVP reprezintă o metoda de încapsulare a informațiilor în mesajele DIAMETER. Antetul AVP, de minimum 8 octeți, are următoarea structură:

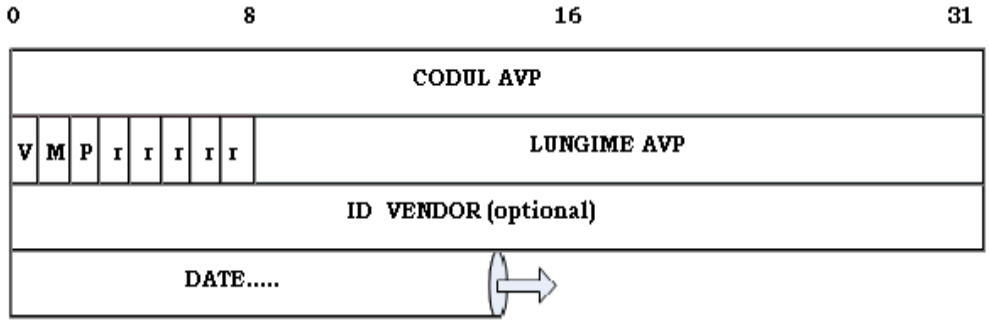

Figura IV.7 Structura AVP

Semnificațiile câmpurilor:

- Codul AVP împreună cu identificatorul producătorului (ID *Vendor*) - identifică unicitatea atributului.

- Bitul V - arată prezența câmpului opțional ID Vendor (de obicei este 0);
- Bitul P - indică necesitatea criptării pentru securitatea *end-to-end*;
- Bitul M - trebuie să ia valoarea 1, pentru ca mesajul să nu fie respins;
- Lungime AVP - indică lungimea totală a mesajului AVP;
- Date – este câmpul care conține informații specifice atributului.

Protocolul DIAMETER poate furniza aplicațiilor două tipuri de servicii: autentificare şi autorizare, cu opțiunea de gestionare a conturilor, sau numai gestionarea conturilor.

În cazul **serviciului de autentificare si autorizare**, deschiderea unei sesiuni se realizează prin trimiterea unui mesaj serverului NAS, care la rândul său trimite o cerere de autentificare serverului DIAMETER cu un identificator unic de sesiune (*session-ID*). Serverul DIAMETER poate include în mesajul de răspuns un AVP care să indice "timpul de viață" al autorizației (exprimat în secunde) după care utilizatorul trebuie să fie reautentificat. După expirarea timpului, serverul DIAMETER închide sesiunea, eliberează toate resursele alocate acesteia. În timpul sesiunii, pot fi inițiate cereri de reautentificare şi reautorizare, menite să verifice dacă utilizatorul mai foloseşte serviciul. Mesajele de închidere a unei sesiuni pot fi inițiate atât de NAS, cât şi de serverul DIAMETER.

În cadrul **serviciului de gestionare a conturilor**, se au în vedere numărul mesajelor, starea unei sesiuni active, modul de trimitere al mesajelor etc.

Erorile protocolului DIAMETER se împart în două categorii:

- **Erorile de protocol** - se referă la problemele apărute în transportul mesajelor (de exemplu, informații de rutare greșite, întreruperi temporare ale unor căi de comunicație din rețea).
- **Erorile de aplicație** – cauzate de modul de implementare a protocolului.

Ca avantaje ale protocolului DIAMETER suplimentare față de RADIUS, se pot aminti:

- mesajele de eroare care specifică problema apărută
- utilizarea mesajelor de confirmare
- blocarea trimiterii repetate a unui mesaj (*no-replay*)
- garantarea integrității mesajelor (securitate de tip end-to-end).

DIAMETER este un protocol *"peer-to-peer"* şi nu client-server, aplicabil în rețelele de mari dimensiuni, recomandat atât în rețelele cablate, cât şi în cele wireless sau hibride.

IV.6 PROTOCOLUL DE AUTENTIFICARE EXTINSĂ (EAP)

Protocolul de autentificare extinsă (EAP – *Extensible Authentication Protocol*) este utilizat în sistemele de autentificare cu cheie globală, pentru transmisia criptată a acesteia în rețea.

EAP este utilizat în rețelele wireless în standard IEEE 802.11.

Pentru autentificare mutuală se foloseşte pe nivelul de transport protocolul TLS (*Transport Layer Security*) care asigură integritatea comunicațiilor şi schimbul sigur de chei între nodurile rețelei. Acest

protocol solicită reautentiifcarea şi reautorizarea de fiecare dată când se trece din rețeaua wireless într-o rețea cablată sau o altă rețea wireless cu un nivel de securitate mai mic.

Fiecare stație care doreşte să se conecteze la rețeaua wireless, trimite către AP un mesaj de tip EAP Start pentru începerea procesului de autentificare. AP-ul îi răspunde cu o cerere EAP (EAP *Request*) pentru a-i afla identitatea după care îi trimite un mesaj de deschidere a conexiunii cu acel AP (EAP *Start Connected*). Stația răspunde AP-ului (EAP *Response*) cu un mesaj în care este inclus fie identificatorul cererii dacă nu este nici un utilizator activ la acel moment fie numele utilizatorului activ. AP-ul trimite acest răspuns serverului de autentificare care va adresa prin TLS sau codat MD5 o interogare de verificare (*challenge*) a identității clientului. Această cerere este transmisă criptat, cu o cheie unică de sesiune (*unicast key*) deoarece serverul de autentificare nu admite chei globale pentru transmisie. AP-ul intermediază comunicația client-server. Clientul transmite răspunsul conținând garanțiile sale (*credentials*) serverului de autentificare şi dacă acestea sunt valide, se creează un mesaj „Succes”, după care trimite AP-ului mesajul de răspuns pentru client în care se transmite cheia criptare generată pe baza cheii de sesiune EAP-TLS. AP-ul generează aleator o cheie globală de criptare sau o alege dintr-un set predefinit de chei, pe care o prezintă serverului de autentificare. După confirmarea recepției acestui mesaj, AP-ul transmite clientului răspunsul (EAP *Key Message*) cu cheia de transmisie criptată cu cheia de sesiune dată de server. Toate cheile de sesiune folosite de clienții unui AP, sunt stocate de acesta în liste speciale. Fiecare client extrage prin decriptare cheia globală din mesajul trimis de AP. După aceea, AP-ul generează din cheia de sesiune EAP-TLS şi transmite clientului cheia de criptare pe care o va folosi pentru transmisie ca şi cheie unică de sesiune

(*unicast session key*). Placa de rețea (NIC – *Network Interface Card*) a clientului este programată pentru a folosi această cheie pentru toate transmisiile efectuate prin acel AP. Se adresează apoi o cerere de DHCP pentru alocarea unei adrese pe baza căreia se conectează clientul la rețeaua aleasă.

Similar se pot folosi variante îmbunătățite ale protocolului EAP cu tunelare (EAP-TTLS sau LEAP – Lightweight EAP).

Capitolul V TEHNICI DE SECURITATE

V.1 INTRODUCERE

Importanța aspectelor de securitate în rețelele de comunicații a crescut odată cu extinderea aplicațiilor cu caracter privat, de genul celor financiar-bancare, realizate prin intermediul acestora (plăți electronice, tranzacții între conturi, licitații electronice, comerț electronic etc). În cazul operării cu informații confidențiale, este important ca avantajele de partajare şi comunicare aduse de rețelele de comunicații să fie susținute de facilități de securitate substanțiale.

În urma implementării unor tehnici de securitate într-o rețea, informațiile nu vor mai putea fi accesate sau interceptate de persoane neautorizate (curioase sau rău intenționate) şi se va împiedica falsificarea informațiilor transmise sau utilizarea clandestină a anumitor servicii destinate unor categorii aparte de utilizatori ai rețelelor.

În condițiile în care există numeroase interese de spargere a unei rețele, este evident că proiectanții resurselor hard şi soft ale acesteia trebuie să ia măsuri de protecție serioase împotriva unor tentative rău intenționate. Însă metodele de protecție luate împotriva “inamicilor” accidentali, se pot dovedi inutile sau cu un impact foarte redus asupra unor adversari redutabili, cu posibilități materiale considerabile.

Pentru implementarea securității unei rețele este importantă utilizarea unor tehnici specifice:

- protecția fizică a dispozitivelor de rețea şi a liniilor de transmisie la nivel fizic;

- proceduri de blocare a accesului la nivelul rețelei;
- transport securizat al datelor în spațiul public prin tunele securizate sau VPN-uri (Virtual Private Network);
- aplicarea unor tehnici de criptare a datelor.

Fără o politică de securitate riguroasă, diversele mecanisme de securitate pot fi aproape ineficiente întrucât nu ar corespunde strategiei şi obiectivelor pentru care a fost proiectată rețeaua.

Măsurile de securitate prevăzute în politica de securitate pot să vizeze mai multe aspecte:

- Renunțarea la setările implicite şi configurarea adecvată a echipamentelor din rețea (stații de lucru, servere, routere, AP): parole, chei de criptare, funcții de reset, funcții de conectare şi de reconectare automată şi de la distanță, liste de control pe baza adreselor MAC şi a cheilor publice, agenți SNMP din versiunile mai noi de protocol.
- Reînnoirea parolelor şi a setărilor implicite în general, care pot constitui vulnerabilități ale sistemului de securitate. Se poate folosi un generator automat de parole, eventual combinat cu mecanismul de autentificare cu doi factori în care parola este combinată fie cu codul PIN al unui dispozitiv de acces hardware (smart card), fie cu un alt cod de acces. Nu întotdeauna se justifică măsuri de control al accesului atât de severe.
- Stabilirea caracteristicilor de criptare trebuie făcută pe cel mai performant nivel oferit de un standard dacă nu sunt probleme de compatibilitate cu sisteme de comunicație mai vechi. De exemplu, în cazul comunicațiilor wireless care folosesc WEP, opțiunile referitoare la cheile de criptare sunt: niciuna, cheie publică de 40 de

biți şi cheie publică de 104 biți. Interconectarea unui echipament care foloseşte o cheie de 128 de biți cu unul care utilizează WEP, devine astfel imposibilă.

- Controlul funcției de resetare este foarte important pentru că o persoană care are acces fizic la un echipament, îl poate readuce la configurările implicite prin acționarea butonului de resetare după care are acces direct la rețea.
- Utilizarea listelor de acces (ACL – *Access Control List*) cu filtrare pe bază de adrese fizice (MAC – *Media Access Control*) şi cu adrese statice de rețea (DHCP dezactivat), cu limitarea domeniului de adrese alocabile, pot împiedica accesul neautorizat la rețea.
- În cazul rețelelor wireless, este utilă dezactivarea opțiunii de transmitere prin braodcast a identificatorului setului de servicii (SSID – *Service Set Identifier*) astfel încât o simplă cerere de identificare a rețelelor wireless dintr-o zonă, să fie ignorată de AP-ul respectiv. Atacatorul trebuie să lanseze în acest caz un proces de scanare activă a rețelei care însă îi desconspiră prezența.
- Maximizarea intervalului de baliză poate de asemenea să ascundă temporar un AP, fiind mai greu de depistat.
- Schimbarea canalului implicit folosit de AP în rețeaua wireless poate fi utilă în cazuri de interferență cu alte echipamente care transmit în aceaşi arie geografică. Se recomandă o separare de minimum 5 canale.

Aplicarea principiilor de securitate enunțate trebuie realizată cu ajutorul unor tehnici eficiente de control al accesului logic la rețea şi la servicii, atât pentru utilizatorii din intranet, cât şi pentru cei din afară.

Securitatea trebuie asigurată de la prima cerere de stabilire a unei conexiuni între două echipamente de comunicație, urmând ca măsuri specifice de securizare să se aplice ulterior la nivel de aplicație, în funcție de privilegiile de acces la servicii pe care le are solicitantul, utilizator sau proces software.

A devenit o cerință imperativă în rețelele de comunicații, implementarea contramăsurilor pentru accesul procedurilor automate de tip client, care sunt deosebit de eficiente în aflarea codurilor de acces, precum şi în lansarea unor atacuri de saturare a serverelor şi a rețelei. Se folosesc, de exemplu, solicitări de recunoaştere a unor litere sau cifre, cu forme deosebite sau marcate cu un simbol, care nu pot fi rezolvate prin proceduri automate de recunoaştere a formelor ci numai de utilizatorii umani.

V.2 FIREWALL

Un firewall („zid de protecție”) joacă un rol semnificativ în procesul de securitate al unei rețele de calculatoare. Ca firewall se poate folosi un dispozitiv dedicat sau o aplicație software care controlează procesul de comunicație dintre rețeaua internă şi cea externă, prin aplicarea politicii de securitate a rețelei protejate.

Un router poate fi configurat ca firewall. De asemenea, unele sisteme de operare, precum Windows XP (*eXPerience*), includ opțiunea de activare a unui firewall intern care aplică anumite reguli şi constrângeri privind accesul pe diferite interfețe ale sale.

Firewall-ul interconectează rețeaua publică şi o rețea privată, asigurând securitatea datelor vehiculate intern în rețea şi protecția rețelei private față de eventualele atacuri externe (Fig.V.1).

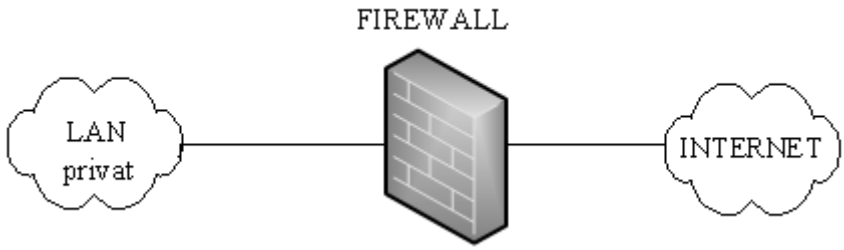

Fig. V.1 Conectarea unei rețele private la Internet
prin intermediul unui firewall

Un firewall are minimum două interfețe:

- Interfața publică prin care se realizează conexiunea dintre firewall şi rețeaua publică (în particular, Internet-ul);
- Interfața privată prin care se interconectează firewall-ul la rețeaua privată.

Firewall-ul protejează rețeaua privată de atacurile externe şi restricționează accesul din afară la resursele acesteia.

Întrucât firewall-ul reprezintă singura conexiune dintre rețeaua privată şi cea publică, la nivelul său se poate monitoriza şi jurnaliza traficul de pachete şi se verifică drepturile de acces ale utilizatorilor din afara rețelei interne (prin operația de *login*)

În prezent, se utilizează două tipuri de firewall:

1. **Poartă de aplicații** (*Application Gateway*) - varianta tradițională de firewall.

Orice conexiune între două rețele se face prin intermediul unui program de aplicații (*proxy*). O sesiune deschisă în rețeaua privată este încheiată de proxy, după care acesta creează o nouă sesiune spre nodul de destinație prin care serverul proxy adresează cererile de la nodurile interne, în numele său, în rețeaua externă.

Programul proxy se bazează pe particularitățile suitei TCP/IP şi este restrictiv pentru alte suite de protocoale. Execuția acestui program necesită resurse relativ mari din partea CPU.

La nivelul firewall-ului sunt admise numai acele protocoale pentru care sunt configurate aplicații proxy specifice. Cadrele bazate pe alte tipuri de protocoale sunt automat rejectate.

2. Modul de inspecție dependent de stare (*Stateful Inspection*) sau de **filtrare dinamică a pachetelor**, denumit şi mod de control al accesului în funcție de context (CBAC - *Context-Based Access Control*).

În această tehnologie, se preiau pachetele de date şi se citesc antetele introduse de protocolul de rețea (IP) şi de cele corespunzătoare nivelelor OSI şi TCP/IP superioare, până la nivelul de aplicație.

Firewall-ul verifică fiecare pachet care urmează să fie transferat şi acordă dreptul de acces în funcție de adresele sursei şi destinației, precum şi de serviciul solicitat.

Acțiunile firewall-ului pot fi de mai multe tipuri:

1. acceptare (*Accept, Allow*) a pachetelor, condiționată sau necondiționată de un set de reguli.
2. respingere (*Reject*) a pachetelor care nu corespund regulilor de securitate cu trimiterea unui mesaj nodului emitent.
3. blocare (*drop, deny, blackhole*) sau interzicere a accesului pachetelor în rețea, fără înştiințarea expeditorului.

În practică, se configurează şi firewall-uri transparente, care transferă cadrele între cele două sesiuni fără analiza prealabilă a informațiilor pe care acestea le conțin.

Acest tip de firewall CBAC realizează controlul fluxului cu memorie, astfel încât echipamentul este capabil să recunoască acele pachete transmise din rețeaua publică (*extranet*) ca răspuns la o cerere adresată de un nod din rețeaua internă (*intranet*), prin monitorizarea sesiunilor TCP. În paralel, se rejectează toate pachetele transmise din rețeaua publică în cea internă, dar care nu provin din traficul inițiat intern.

Prin acest concept, se asigură o procesare rapidă şi eficientă a traficului de informații dintre Internet şi rețelele private, perfect adaptată noilor aplicații Internet şi realizată cu resurse hardware relativ reduse.

Implementarea firewall-ului cu routere se face prin filtrarea dinamică a pachetelor şi controlul traficului pe baza regulii care stabileşte că:

- orice pachet transmis din rețeaua internă către o destinație externă este transferat de firewall necondiționat, cu excepția cazurilor în care se impun constrângeri;
- transferul oricărui pachet din rețeaua publică spre o destinație din rețeaua privată este blocat de firewall, cu excepția cazurilor în care se admite accesul acestora în mod explicit, prin configurarea adecvată a interfețelor publice referitor la accesul din exterior.

Interfețele firewall-ului sunt deschise numai pe durata sesiunii inițiate de un utilizator cu drept de acces.

Firewall-ul interceptează orice conexiune stabilită prin TCP şi o continuă numai după verificarea prealabilă a legăturii. Acest lucru previne

atacurile din exterior asupra rețelei private, prin distrugerea cadrelor transmise prin TCP fără drept de acces.

Firewall-ul poate fi configurat în vederea limitării accesului utilizatorilor din rețeaua internă în cea publică.

Se poate controla accesul pe diferite porturi de protocol. Este indicată închiderea unor porturi neutilizate de utilizatorii proprii pentru a nu lăsa căi de acces eventualilor atacatori.

Mesajele generate prin ICMP pot fi transferate sau blocate de firewall în funcție de modul de configurare a acestuia.

Pentru evenimentele semnificative care apar la nivelul firewall-ului se pot trimite mesaje de înştiințare către nodurile de destinație accesate.

Echipamentele de tip firewall admit diverse protocoale de aplicație: FTP, NETBIOS, GRE, OSPF, RSVP (*ReSerVation Protocol*), VDOnet's VDOLive, Microsoft's NetShow etc.

Firewall-ul protejează rețeaua privată față de **atacurile externe** de tip "inundare" cu pachete (*flooding*), cu pachete PING ilegale sau ICMP generate în număr excesiv, atacuri Smurf cu pachete având adresa IP din spațiul de adrese alocat rețelei private, de cele mai multe ori fiind chiar adresa de broadcast a acesteia, scanare a porturilor.

Firewall-ul permite controlul şi monitorizarea accesului (*Logging Facility*) în rețeaua privată dar numai pentru sesiunile create pe baza protocolului Internet, nu şi pentru alte suite de protocoale (Appletalk, DECnet, IPX/SPX).

Politica de securitate aplicată de firewall stabileşte regulile pe baza cărora se admite sau se blochează transferul pachetelor între rețeaua privată şi cea publică.

Un firewall devine activ numai după ce au fost configurate cel puțin o interfață publică şi una privată şi s-au stabilit regulile de acces la nivelul acestora.

Traficul între două interfețe ale firewall-ului nesupuse politicii de securitate se desfăşoară normal, fără restricții.

Transferul pachetelor de la o interfață nesecurizată către una securizată este automat blocat.

Firewall-ul controlează traficul de pachete pe baza adreselor fizice sau IP, a porturilor de aplicație şi chiar a zilei sau orei la care se accesează rețeaua.

Politica de securitate se aplică pe baza **listelor de acces** stocate în routere sau în servere RADIUS (*Remote Authentication Dial In User Service*).

Firewall-ul lucrează ca server de control al accesului (*Network Access Server*) care foloseşte serviciile unui server RADIUS care gexstionează baza de date cu informații despre utilizatorii rețelei (nume de utilizatori şi parole), modul de configurare a rețelei (adrese IP, măşti de rețele şi de subrețele etc), precum şi despre sesiunile stabilite anterior, sub forma unui istoric al evenimentelor din rețea.

Firewall-ul este clientul RADIUS care adresează cererea de autentificare către serverele RADIUS, pentru accesarea listelor de acces. Acestea sunt fişiere de tip 'text' (.txt), codate ASCII, care includ liste de adrese IP sau MAC.

Listele de acces bazate pe adrese IP includ adrese IP individuale, eventual numele calculatoarelor-gazdă, domeniul de adrese IP al unei rețele şi eventual unele comentarii care facilitează administrarea acestor liste.

Listele de acces cu adrese fizice includ adrese MAC individuale ale componentelor rețelei, eventual numele stațiilor şi comentarii ajutătoare.

Numărul maxim de liste de acces care pot fi stocate pe un router, precum şi dimensiunile acestora este în general limitat.

Pentru un spațiu de adrese extins se preferă utilizarea unui server RADIUS care să gestioneze eficient aceste liste, pentru a reduce întârzierile de trafic produse de routere.

În acest caz, routerul devine un simplu client RADIUS care adresează cererea de autentificare către serverul RADIUS şi primeşte un răspuns din partea acestuia.

Firewall-urile pot opera pe diferite nivele:

- nivel OSI 2 (pe subnivelul MAC): filtrarea cadrelor
- nivel OSI 3 de rețea: filtrarea pachetelor
- nivel OSI 4 de transport: filtrarea pachetelor cu opțiunea de inspecție a stării pentru a cunoaşte caracteristicile următorului pachet aşteptat în vederea evitării multor atacuri.
- nivel de aplicație (*application level firewall*) când se comportă ca server proxy pentru diverse protocoale care ia decizii privind aplicațiile şi conexiunile stabilite în rețea.

Observații:

1. Filtrarea dinamică a pachetelor se realizează la nivelul firewall-ului prin politica de securitate dar şi prin procedeele de translare a adreselor private în adrese publice (NAT – *Network Address Translation*; ENAT - *Enhanced NAT*). Pentru a evita dubla filtrare a pachetelor în routere, se dezactivează serviciul NAT pe durata activării firewall-ului.

2. Se poate monitoriza activitatea firewall-ului, mai precis evenimentele care se desfăşoară la nivelul său:

- accesarea adreselor de e-mail;
- desfăşurarea sesiunilor Telnet de acces de la distanță în rețeaua privată;
- comunicarea pe porturi asincrone (de exemplu, interfețe seriale);
- accesarea agenților SNMP.

O aplicație de tip firewall are şi o serie de limitări:

- nu poate interzice importul/exportul de informații dăunătoare vehiculate prin diferite servicii de rețea (de exemplu, prin poşta electronică);
- nu poate interzice scurgerea de informații pe alte căi, care ocolesc firewall-ul (*dial-up*);
- nu poate proteja rețeaua privată de informațiile aduse pe suporturi mobile (USB flash memory, dischetă, CD - *Compact Disc*, DVD - *Digital Versatil Disc* etc.);
- nu poate preveni efectul erorilor de proiectare ale aplicațiilor care realizează diverse servicii (*bugs*).
- Firewall-urile pot fi implementate în formă:
- dedicată oferind un nivel sporit de securitate
- combinată cu alte servicii de rețea, în router sau gateway sau într-un simplu calculator.

Eficiența unui firewall depinde de politica de securitate aplicată şi de modul de configurare. De cele mai multe ori este indicată restricționarea totală a traficului, urmată de deschiderea acelor porturi şi admiterea acelor

aplicații care se justifică prin politica de securitate şi după o verificare a activității lor pe o anumită perioadă de timp după activare. Verificarea eficienței firewall-ului se poate face cu aplicații software care oferă servicii de testare a vulnerabilităților de securitate (precum *Shields Up*).

V.3 SISTEME DE DETECȚIE A INTRUŞILOR

Sistemele de detecție a intruşilor (IDS – *Intrusion Detection System*) sunt o completare a activității unui firewall în procesul de securitate a unei rețele de comunicații şi constau în soluții pasive de analiză, clasificare şi raportare a evenimentelor de rețea nedorite.

Cele mai frecvente atacuri lansate din Internet asupra serverelor de rețea sunt de tip „refuz al serviciului” (DoS) corelate cu acțiuni de „inundare” a rețelei (*flooding*) cu un număr mare de pachete de diferite tipuri (ping. TCP syn ş.a.). Dar se impune şi limitarea atacurilor pasive de interceptare a pachetelor conținând informații cu caracter secret în scop de furt sau de falsificare a acestora.

Atacurile asupra rețelelor de comunicații pot fi lansate pe diferite căi, de exemplu prin serviciul de e-mail sau prin intermediul aplicațiilor p2p, şi pot viza aplicații cu caracter critic precum cele de tranzacții financiar-bancare sau de comerț electronic pentru care pierderile sunt substanțiale şi se exprimă în mari sume de bani.

De aceea, investițiile în soluțiile de securitate a comunicațiilor se dovedesc a fi necesare şi eficiente ca raport preț-pierderi.

Sistemele IDS detectează atacurile asupra rețelei, alertează personalul de administrare şi eventual declanşează acțiuni de răspuns, cum ar fi plasarea în carantină a anumitor procese până la clarificarea situației. Bineînțeles că pot să existe şi alarme false dar procedurile aplicate în primă fază nu vor face decât să întârzie anumite transmisii.

Soluțiile IDS monitorizează traficul, identifică evenimentele cu risc de securitate, le clasifică pe mai multe clase de risc şi le raportează sistemului de securitate.

Spre deosebire de un firewall care are un caracter activ, de permitere sau de blocare a pachetelor pe diferite criterii prevăzute în politica de securitate a rețelelor, IDS-ul operează pasiv în rețea, analizează traficul, identifică tentativele de atac pe baza semnăturilor aplicațiilor şi anomaliile de trafic, alertează serviciul de administrare pentru a recurge în timp util la contramăsuri dar nu blochează atacurile.

Problemele de securitate pot fi rezolvate manual doar în rețele de mici dimensiuni. În rețelele mari, cu zeci şi sute de mii de noduri, soluționarea evenimentelor cu risc de securitate trebuie realizată în mod automat, prin soluții software adecvate care procesează în timp real informațiile referitoare la traficul neautorizat de pachete şi care ia decizii de acțiune fără intervenția factorului uman de administrare. Apar în acest caz probleme de clasificare a evenimentelor într-un număr relativ redus de clase de risc pentru a putea observa atacurile distribuite asupra rețelei. Acestea pot fi tratate pe baza teoriei sistemelor fuzzy iar în procesele de decizie se pot folosi algoritmi optimi de procesare a informației.

Soluțiile IDS pot fi aplicate fie la nivel de rețea, pentru controlul accesului în rețea (NAC – *Network Access Control*), fie la nivel de calculator-gazdă (*Host IDS*).

Serviciul de detectare a intruşilor realizează la nivelul unui echipament din rețea următoarele funcții:

1. inspectarea fluxului de pachete
2. identificarea semnăturilor de atac
3. alertarea serviciului de securitate
4. activarea unor acțiuni de răspuns automate.

În general, orice IDS detectează şi procesele de scanare a rețelei (de exemplu, *Nmap*) care preced de obicei un atac, astfel fiind posibilă preîntâmpinarea acestora prin soluții active de prevenire a intruziunilor (IPS – *Intrusion Prevention System*).

V.4 VPN - REȚELE PRIVATE VIRTUALE

Un VPN este o ***rețea de comunicații privată***, folosită de obicei în cadrul uneia sau mai multor organizatii, pentru a comunica în mod confidențial, prin intermediul unei rețele publice.

Mesajele din traficul VPN pot fi transmise prin intermediul infrastructurii unei rețele publice de date, precum Internet-ul, folosind protocoalele standard, sau prin intermediul unei rețele private a furnizorului de servicii Internet.

VPN-ul este o soluție eficientă din punctul de vedere al costurilor, pentru ca diferite organizații să poată asigura accesul la rețeaua internă pentru angajații şi colaboratorii aflați la distanță, şi pentru a permite confidențialitatea datelor schimbate între punctele de lucru aflate la distanță.

Multe din programele-client ale VPN- ului pot fi configurate în aşa fel încât să ceară dirijarea întregului trafic printr-un ***tunel***, atâta timp cât conexiunea VPN este activă, sporind astfel siguranța conexiunii. Atâta vreme cât conexiunea VPN este activă, accesul din afara rețelei sigure se face prin acelaşi firewall, ca şi cum utilizatorul ar fi conectat din interiorul rețelei private. Acest fapt reduce riscurile unei posibile accesări din partea unui atacator, de interceptare şi de urmărire a pachetelor.

Un tunel reprezintă o conexiune ”punct-la-punct” între două calculatoare sau două rețele pentru care se utilizează diferite protocoale de rutare prin care se stabileşte calea pe care este trimis pachetul de la sursă la destinație.

Termenul de VPN descrie două modalități de abordare a problemei rețelelor private care au ca suport o rețea publică, din punctul de vedere al accesibilității:

1. VPN-uri realizate între mai multe rețele locale (LAN-*to*-LAN VPNs, cunoscute şi sub denumirea de *Site-to-Site* VPNs) care conectează la un nod central mai multe LAN-uri diferite aflate la mare distanță unele față de altele dar care fac parte din acelaşi intranet, astfel încât să asigure conectivitatea între ele.
2. VPN-uri de acces de la distanță (*Remote Access VPNs*) care asigură accesul de la distanță la o rețea privată, de exemplu pentru utilizatorii de Internet mobil.

Se pot folosi diverse tehnologii de implementare a VPN-urilor (Figura V.2). Alegerea uneia anume depinde de criteriile impuse prin politica de securitate a rețelei.

Prin aplicarea algoritmilor de criptare pe un anumit nivel OSI, informațiile de pe toate nivelele de deasupra sunt protejate.

Se pare că nivelul de rețea este cel mai indicat a fi securizat, deoarece este independent de nivelul-aplicație şi de cel fizic, în acest fel asigurându-se o flexibilitate sporită.

Aplicarea serviciilor criptografice la nivel de aplicație nu este o soluție eficientă din cauza diversității aplicațiilor rulate care implică schimbarea algoritmului de criptare de la caz la caz (voce, imagine, date).

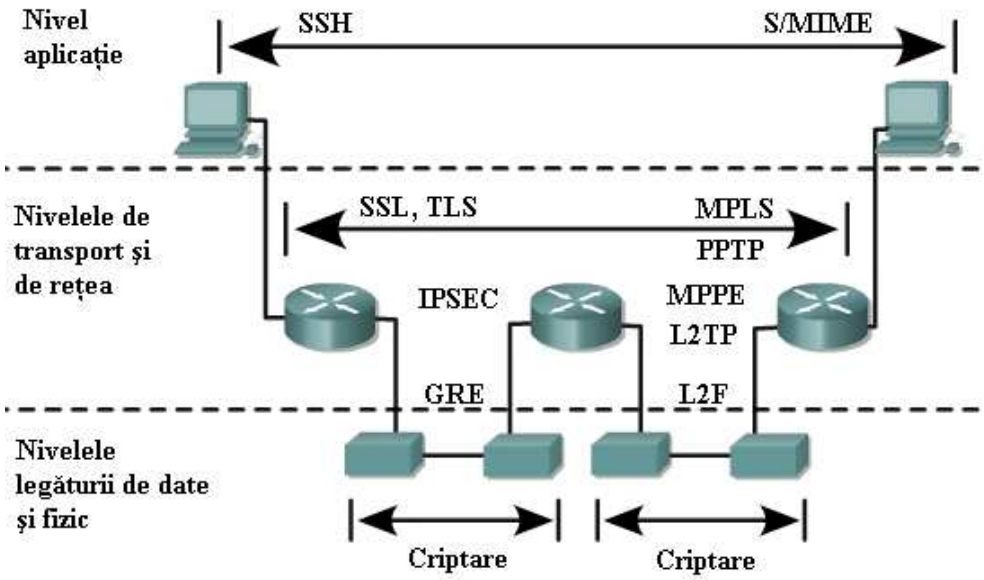

Figura V.2 Protocoale folosite pentru VPN

La nivelul de transport, s-au impus mai multe protocoale de securitate:

1. SSL (*Secure Socket Layer*) asigură autentificarea şi integritatea aplicațiilor bazate pe protocolul TCP, dar are ca dezavantaj major lipsa de flexibilitate şi dependența de nivelul-aplicație.

2. TLS (*Transport Layer Security*) s-a dezvoltat ca o alternativă la SSL care rezolvă majoritatea inconvenientelor acestuia.

În ceea ce priveşte protecția nivelului legăturii de date, problemele cele mai stringente apar la capitolul costuri de implementare, întrucât implică securizarea fiecărei legături în mod separat.

Un protocol de tunelare este protocolul prin care se stabileşte un tunel între două entități din WAN, despărțite de o infrastuctură publică, pentru care se asigură integritatea datelor vehiculate.

Se folosesc diferite protocoale de tunelare, diferențiate prin traficul care îl pot susține:

- GRE (*Generic Routing Encapsulation*) recomandat pentru rețele multiprotocol (IP, AppleTalk, DecNet). Cadrele sunt împachetate cu antete IP şi transmise prin rețeaua publică.
- IPSEC (*Internet Protocol Security*) care permite doar trafic IP.
- PPTP (*Point-to-Point Tunneling Protocol*)
- L2F (CISCO *Layer 2 Forwarding*)
- L2TP (*Layer 2 Tunneling Protocol*)
- MPLS (*Multiprotocol Label Switching*).

Protocoalele de tunelare VPN asigură funcțiile de autentificare şi de criptare. Autentificarea permite atât clienților, cât şi serverelor VPN, identificarea corectă a utilizatorilor de resurse. Criptarea asigură protecția informațiilor transportate prin tunelul VPN.

MPPE (*Microsoft Point-to-Point Encryption*) este un protocol de criptare a datelor pe legături PPP în cadrul rețelelor virtuale private. MPPE foloseşte algoritmul RC4, cu chei de sesiune de 40, 56 sau 128 de biți. Cheia de criptare poate fi schimbată la fiecare pachet. MPPE nu realizează compresia datelor şi, de aceea, pentru creşterea eficienței sale, se foloseşte

împreună cu protocoale de compresie (MPPC - *Microsoft Point-to-Point Compression*, CCP - *Compression Control Protocol* un subprotocol al PPP).

Avantajele folosirii unui VPN sunt numeroase:

- conectivitate geografică extinsă sub forma unei rețele globale;
- îmbunătățirea securității căilor de comunicații pe care datele sunt transmise necriptat;
- reducerea costurilor operaționale în comparație cu cele de securizare a comunicațiilor prin rețeaua publică de arie largă;
- reducerea timpului de acces şi a costurilor de transport pentru utilizatorii aflați la distanță;
- simplificarea topologiei rețelei în anumite cazuri.

ABREVIERI

A

AAA	Authentication, Authorization, Accounting
AAL	ATM Adaptation Layer
AC	Access Control
ACK	ACKnowledge
ACL	Access Control List
ACS	Advanced Connectivity System
ACU	Automatic Calling Unit
ADIF	Accounting Data Interchange Format
ADPCM	Adaptive Differential Pulse Coded Modulation
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption System
AGP	Advanced Graphics Card
AH	Authentication Header
AM	Amplitude Modulation
AMI	Alternative Mark Inversion
ANSI	American National Standards Institute
AODI	Always On/Demand ISDN
AP	Application Processor/ Access Point
APDU	Application Protocol Data Unit
API	Application Program Interface
ARP	Address Resolution Protocol
ARPA	Advanced Research Project Agency
ARPANET	Advanced Research Projects Agency Network
AS	Authentication Server/ Autonomous System
ASCII	American Standard Code for Information
ASIC	Application Specific Integrated Circuit
ASN	Autonomous System Number

ATA	Advanced Technology Attachment
ATM	Asynchronous Transfer Mode
AU	Attachment Unit
AUI	Attachment Unit Interface
AVP	Attribute-Value Pairs
AWGN	Additive White Gaussian Noise

B

BACP	Band Allocation Control Protocol
BAP	Band Allocation Protocol
BATE	Baseband Adaptive Transversal Equalizer
BB	Base Band
BCD	Binary Coded Decimal
BCP	Bridging Control Protocol
BECN	Backward Explicit Congestion Notification
BER	Bit Error Rate
BGP	Border Gateway Protocol
BIP-L	BIPhase-Level
BIOS	Basic Input-Output System
B-ISDN	Broadband ISDN
BOOTP	BOOTstrap Protocol
BOP	Byte Oriented Protocol
BNC	Bayonet Nut Connector
BPI	Baseline Privacy Interface
bps	bits-per-second
BPSK	Binary Phase Shift Keying
BR	Bridge-Router
BRA	Basic Rate Access
BRI	Basic Rate Interface
BS	BackSpace

BSA	Basic Service Area
BSC	Basic Station Controller
BSS	Basic Service Set
BTC	Basic Transceiver
BTH	Bluetooth
BUS	Broadcast Unknown Server

C

C/N	Carrier-to-Noise Ratio
CA	Certificate Authority
CBAC	Context-Based Access Control
CBR	Constant Bit Rate
CCK	Complementary Code Keying
CD	Compact Disc
CD	Carrier Detect
CDDI	Copper Distributed Data Interface
CDE	Common Desktop Environment
CDFS	Compact Disk File System
CDMA	Code Division Multiple Access
CELP	Code Excited Linear Prediction
CES	Circuit Emulation Service
CHAP	Challenge-Handshake Authentication Protocol
CIDR	Classless InterDomain Routing
CIR	Committed Information Rate
CISC	Complet Instruction Set Computing
CLP	Cell Loss Priority
CM	Cable Modem
CMI	Coded Mark Inversion
CMOS	Complementary Metal Oxid Semiconductor
CMTS	Cable Modem Termination Sysem
CODEC	COder-DECoder

COFDM	Coded OFDM
COMSEC	Comunications Security
CP	Communication Processor
CPCS	Common Part Convergence Sublayer
CPU	Central Processing Unit
CR	Carriage Return
CRC	Cyclic Redundancy Checking
CRL	Certificate Revocation List
CS	Checksum / Convergence Sublayer
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNET	Computer Science Network
CSS	Card and Socket Specification
CTS	Clear-To-Send
CU	Central Unit

D

3DES	Triple Data Encryption System
DA	Destination Address
DAS	Dual Attachment Station
DB	Database
DC	Differential Cryptanalysis
DCE	Data Circuit Terminal Equipment
DCL	Data and Control Logic
DDN	Defense Data Network
DEC	Digital Equipment Corporation
DES	Data Encryption Standard
DH	Diffie-Helmann
DHCP	Dynamic Host Configuration Protocol
DIR	Desired Information Rate

DL	Down Link
DLC	Data Link Control / Data Link Connection
DLCI	Data Link Connection Identifier
DLL	Dynamic Link Library
DMA	Direct Memory Access
DNS	Domain Name System
DNS	Domain Name System
DoCSIS	Data over Cable Service Interface
DoD	Department of Defense
DoS	Denial of Service
DOS	Disk Operating System
DPEs	Data Packet Encodings
DPMA	Demand Priority Media Access
DPP	Demand Priority Protocol
DPSK	Differentially Phase Shift Keying
DS	Distribution System
DSAP	Destination Service Access Point
DSB-AM	Double Side Band Amplitude Modulation
DSL	Digital Subscriber Line
DSP	Digital Signal Processing
DSR	Data Set Ready
DSSS	Direct Sequence Spread Spectrum
DTE	Data Terminal Equipment
DTR	Data Terminal Ready
DU	Data Unit
DVMRP	Distance Vector Multicast Routing Protocol

E

EAP	Extensible Authentication Protocol
EBCDIC	Extended Binary Coded Decimal Interchange Code

ECP	Encryption Control Protocol
ED	Ending Delimiter
EGP	External Gateway Protocol
EGRP	Enhanced IGRP
EIA	Electronics Industries Association
EISA	Extended Industry Standard Architecture
E-mail	Electronic mail
EMI	ElectroMagnetic Interference
EMS	Element Management System
ENAT	Enhanced Network Address Translation
ENCO	ENcryption & COmpression
ENQ	ENQuire
ESA	Extended Service Area
ESS	Extended Service Set
ESP	IP Encapsulating Security Payload
ETH	Ethernet
EUNET	EUropean NETwork

F

FAQ	Frequently Asked Questions
FAT	File Allocation Table
FC	Fragment Control / Frame Control
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FDMA	Frequency Division Multiple Access
FEC	Forward Error Correction
FF	Form Feed
FHSS	Frequency Hopping Spread Spectrum
FIFO	First-In First-Out

FIN	Final flag
Finger	Finger User-information Protocol
FI	Fragment Identification
FM	Frequency Modulation
FR	Frame Relay
FS	File System / Frame Status
FSK	Frequency Shift Keying
FTP	File Transfer Protocol / Foil Twisted Pair

G

Gbps	Giga bits-per-second
GbE	Gigabit Ethernet
GF	Galois Field
GFC	General Flow Control
GIF	Graphic Interchange Format
GMSK	Generalized Minimum Shift Keying
GRE	Generic Routing Encapsulation
GUI	Graphic Unit Interface

H

H	Header / Host
HAL	Hardware Abstraction Layer
HDBn	High Density Bipolar Code no.n
HDD	Hard-Disk Drive
HDLC	High-level Data Link Control
HEC	Header Error-Control
HID	Host IDentifier
HL	Header Length

HPFS	High-Performance File System
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HTTP Secure

I

I/O	Input/Output
IANA	Internet Assigned Number Agency
I-AUP	Internet Acceptable Use Policy
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
ICS	Internet Connection Sharing
ICV	Integrity Check Value
ID	IDentifier
ID	IDentifier
IDE	Integrated Digital Electronics
IDEA	International Data Encryption Algorithm
IDEA	International Data Encryption Algorithm
IE	Internet Explorer
IEEE	Institute of Electrical and Electronic Engineers
IER	Interrupt Enable Register
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGRP	Internal Gateway Routing Protocol
IKE	Internet Key Exchange
INTERNET	INTERnational NETwork
InterNIC	Internet Network Information Center
Intranet	Internal Local Web Servers
IP	Internet Protocol / Initial Permutation
IPCP	Internet Protocol Control Protocol
IPES	Improved Proposed Encryption Standard

IPng	IP next generation
IPsec	Internet Protocol Security Facility
IPX	Internetwork Packet eXchange
IR	Infra Red
IRC	Internet Relay Chat
IRDA	Infra Red Data Access
IRQ	Interrupt ReQuest
ISA	Industry Standard Architecture
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISI	InterSymbol Interference
ISO	International Standards Organisation
ISOC	Internet SOCiety
Iso-Ethernet	Isochronous Ethernet
ISP	Internet Service Provider
ISTE	Integrated Services Terminal Equipment
ITU	International Telecommunication Union

J

JPEG	Joint Photographic Experts Group

K

kbps	kilo bits-per-second
KDC	Key Distribution Center

L

L2F	Layer 2 Forwarding

L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LAPB	Link Access Procedure Balanced
LAPD	Link Access Protocol for D-channel
LASER	Light Amplification by Stimulated Emissions of Radiation
LC	Linear Cryptanalysis
LCN	Logical Channel Number
LCP	Link Control Protocol
LES	LAN Emulation Server
LF	Line Feed
LFSR	Linear Feedback Shift Register
LLC	Logical Link Control
LMI	Local Management Interface
LoS	Line of Sight
LPC	Local Procedure Call
LSB	Least Significant Bit
LST	Link State Technology

M

Mbps	Mega bits-per-second
MA	Multiple Access
MAC	Message Authentication Code/Media Access Control
MAN	Metropolitan Area Network
Manchester	Biphase-L Coding
MAU	Multistation Access Unit
MCA	Micro Channel Architecture
MD5	Message Digest 5
MG	Media Gateway
MGCP	Media Gateway Control Protocol
MIB	Management Information Base

MII	Media Independent Interface
MIME	Multipurpose Internet Mail Extension
MIMO	Multiple-Input Multiple Output
MIOX	Multiprotocol Interconnect Over X.25
MLID	MultiLink Interface Driver
MMF	MultiMode Fiber
MNP	Microcom Networking Protocol
MPEG	Movie Photographic Experts Group
MPLS	MultiProtocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MRC	MultiRate Coder
MRRU	Maximum Receive Reconstructed Unit
MRU	Maximum Received Unit
MS-DOS	Microsoft Disk Operating System
MSB	Most Significant Bit
MSC	Mobile Switching Center
MSK	Minimum Shift Keying
MSR	Modem Status Register
MTA	Message Transfer Agent
MTU	Maximum Transfer Unit

N

N	Network
NAK	Not AcKnowledge
NAS	Network Access Server
NAT	Network Address Translation
NAV	Network Allocation Vector
NBF	NetBEUI Frame
NCB	Network Control Block
NCP	Netware Core Protocol / Network Control Protocol

NDIS	Network Driver Interface Specification
NetBeui	Network BIOS extended user interface
NetBIOS	Network Basic Input/Output System
NFS	Network File System
NIC	Network Interface Card
NID	Next IDentifier
NLPID	Network Layer Protocol IDentifier
NOC	Network Operating Center
NOS	Network Operating System
NM	Network Mask
NMM	Network Management Module
NMS	Network Management Station
NN	Netscape Navigator
NNI	Network - Network Interface
NPM	Network Protocol Module
NT	Network Termination
NTFS	NT File System
NTP	Network Time Protocol
NUL	Null
NVT	Network Virtual Terminal

O

OAEP	Optimal Asymmetric Encryption Padding
ODI	Open Data-link Interface
OFDM	Orthogonal Frequency Division Multiplexing
ONC	Open Network Computing
OOK	On-Off Keying
OQPSK	Offset Quadrature Phase Shift Keying
OS	Operating System
OSI	Open System Interconnection

OSPF	Open Shortest Path First
OUI	Organizational Unique Identifier

P

P2P	Peer-to-Peer
PAD	Packet Assembly/Disassembly
PAM	Pulse Amplitude Modulation
PAN	Personal Area Network
PAP	Password Authentication Protocol
PAP	Password Authentication Protocol
PBX	Public Branch eXchange
PC	Personal Computer
PC1	Permuted Choice 1
PCI	Peripheral Component Interconnect
PCM	Pulse Coded Modulation
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PDN	Public Data Networks
PDU	Protocol Data Unit
PER	Packet Error Rate
PERL	Practical Extraction and Reporting Language
PES	Proposed Encryption Standard
PG	Protective Ground
PGP	Pretty Good Privacy
PHP	Personal Home Page/HyperText Preprocessor
PI	Protocol Interpreter
PING	Packet InterNetwork Groper
PKI	Public Key Infrastructure
PMD	Physical Medium Dependent
PMP	Point - to - Multipoint

PnP	Plug and Play
PoE	Power-over-Ethernet
POP	Post-Office Protocol
PP	Point-to-Point
PPDU	Presentation Protocol Data Unit
PPP	Point-to-Point Protocol
PPSN	Public Packet Switched Network
PRA	Primary Rate Access
PRI	Primary Rate Interface
PS	Postscript
PSH	Push flag
PSK	Phase Shift Keying/Pre-Shared Key
PSTN	Public Switched Telephony Network
PSU	Power Supply Unit
PTY	Payload TYpe
PVC	Permanent Virtual Circuit

Q

QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPRS	Quadrature Partial Response Signal
QPSK	Quadrature Phase Shift Keying

R

RADIUS	Remote Authentication Dial In User Service
RAI	Remote Alarm Indication
RAM	Random Access Memory
RARP	Reverse Address Resolution Protocol

RAS	Remote Access Service
RCC	Routing Control Center
RFI	Radio Frequency Interference
RJ	Registered Jack
RFC	Request For Comments
RFI	Radio Frequency Interference
RG	Radio Guide
RI	Ring Indicator
RIP	Routing Information Protocol
RISC	Reduced Instruction Set Computing
RLL	Run-Length Limited
RLP	Resource Locator Protocol
RMON	Remote Monitoring
PnP	Plug-n-Play
ROM	Read-Only Memory
RPC	Remote Procedure Call
RS	Reed-Solomon
RSA	Rivest, Shamir, Adleman
RSMI	Removable Security Interface
RST	Reset flag
RSVP	ReSerVation Protocol
RTCP	Real Time Control Protocol
RTF	Rich Text Format
RTP	Real Time Protocol
RTS	Request-To-Send
RxD	Data Receiving
RC4	Ron’s Cipher 4
RIPEMD	Race Integrity Primitives Evaluation Message Digest

S

S/MIME	Secure Multipurpose Internet Mail Extension
SA	Source Address / Security Association
SADB	Security Association Database
SAM	Security Account Manager
SAP	Service Access Point / Service Advertising Protocol
SAPI	Service Access Point Identifier
SAR	Segmentation And Reassemble
SAS	Single Attachment Station
SATA	Serrial ATA
SC	Simplex Connector
SCSI	Small Computer System Interface
ScTP	Screened Twisted Pair
SD	Starting Delimiter
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SDSL	Single-line Digital Subscriber Line
SEAL	Software-Optimized Encryption Algorithm / Simple Efficient Adaptation Layer
SFSK	Sinusoidal Frequency Shift Keying
SFTP	Simple File Transfer Protocol
SG	Signal Ground / Signaling Gateway
SHA1	Secure Hash Algorithm 1
SID	Subnetwork Identifier
SLA	Service Level Agreement
SLIP	Serial Line Internet Protocol
SMB	Server Message Block
SMF	Single-Mode Fiber
SMI	Structure of Management Information
SMP	Symmetric Multiprocessing
SMTP	Simple Mail Transfer Protocol

SN	Sequence Number
SNA	Service Network Architecture
SNAP	SubNetwork Access Protocol
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
SNTP	Simple Network Time Protocol
SPD	Security Policy Database
SPDU	Session Protocol Data Unit
SPI	Security Parameters Index
SPI	Service Parameter Index
SPX	Sequenced Packet eXchange
SRM	Security Reference Monitor
SS	Socket Services / Spread Spectrum
SS-7	Signaling System no.7
SSAP	Source Service Access Point
SSH	Secure SHell Protocol
SSI	Security System Interface
ST	Session Ticket
STA	Station Adapter / Spanning-Tree Algorithm
STP	Shielded Twisted Pair/Spanning Tree Protocol
SVC	Switched Virtual Circuit
SYN	Synchronize flag

T

TA	Terminal Adapter
Tbps	Tera bits-per-second
TC	Transmission Convergence
TCL	Tool Command Language
TCM	Trellis Coded Modulation
TCP	Transmission Control Protocol

TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TE	Terminal Equipment
Telnet	Virtual Terminal Connection
TFM	Tamed Frequency Modulation
TFTP	Trivial File Transport Protocol
TGS	Ticket Granting Server
TGT	Ticket Granting Ticket
TIA	Telecommunication Industry Association
TIME	Time of Day Protocol
TL	Total Length
ToS	Type of Service
TPDU	Transport Protocol Data Unit
TRI	Telephony Return Interface
TSM	Telephony Signaling Module
TTL	Time-To-Live
TTY	TeleTYpe
TxD	Data Transmission

U

UA	User Agent
UART	Universal Asynchronous Receiver- Transmitter
UCAID	University Corporation for Advanced Internet Development
UDP	User Datagram Protocol
UL	Up-Link
UNI	User-Network Interface
UPS	Uninterruptible Power Supply
URG	Urgent flag
URI	Uniform Resource Identifier

URL	Uniform Resource Locator
URN	Uniform Resource Name
USB	Universal Serial Bus
UTP	Unshielded Twisted Pair
USENET	USEr NETwork

V

V/FoIP	Voice/Fax-over-IP
VBR	Variable Bit Rate
VCI	Virtual Channel Identifier
VLAN	Virtual Local Area Network
VoATM	Voice-over-ATM
VoDSL	Voice-over-Digital Subscriber Line
VoFR	Voice-over-Frame Relay
VoIP	Voice-over-IP
VoN	Voice-over-Network
VoP	Voice-over-Packet
VPAN	Virtual Private Ad-hoc Network
VPI	Virtual Path Identifier
VPN	Virtual Private Network
VSB	Vestigial Side Band
VT	Virtual Terminal / Vertical Tab
VxD	Virtual Device Driver

W

WAN	Wide Area Network
WDMA	Wavelength Division Multiple Access
WEP	Wired Equivalent Privacy

WFQ	Weighted Fairly Queuing
WiFi v	Wide Fidelity
WiMax	Worldwide Interoperability for Microwave Access
WINS	Windows Internet Name Service
WLAN	Wireless Local Area Network
WM	Wireless Medium
WPA	WiFi Protected Access
WWW	W3 / World Wide Web

X

XML	Extendable Markup Language
XPSN	X.25 Packet Switched Network

BIBIOGRAFIE

[1] Barker C. William, “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher”, Publicație specială NIST 800-67, May 2004
http://csrc.nist.gov/publications/nistpubs/800-67/SP800-67.pdf

[2] Frankel Sheila, Kent Karen, Lewkowski Ryan, Orebaugh D. Angela, Ritchey W. Ronald, Sharma R. Steven, “Guide to IPsec VPNs - Recommendations of the National Institute of Standards and Technology”, Publicatie specială NIST 800-77, Dec. 2005, http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf

[3] http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/13.pdf

[4] http://www.zeroshell.net/eng/kerberos, Fulvio Ricciardi, “The Kerberos protocol and its implementations”, Nov. 2006

[5] Klander Lars, “Anti-hacker. Ghidul securității rețelelor de calculatoare”, ALL Educational, Bucureşti, 1998

[6] Liu Jeffrey, Jiang Steven, Lin Hicks, “Introduction to Diameter”, Jan. 2006
http://www.ibm.com/developerworks/wireless/library/wi-diameter

[7] Menezes J. Alfred, Van Oorschot C. Paul, Vanstone A. Scott, “Handbook of Applied Cryptography”, CRC Press, Oct. 1996

[8] Oprea Dumitru, “Protecția şi securitatea informațiilor”, Ed. Polirom, Iaşi, 2003

[9] Päivi Savola, “Mobility support in RADIUS and Diameter”, May, 28, 2003

[10] Paterson G. K., Yau K.L. Arnold, “Cryptography in Theory and Practice: The Case of Encryption in IPsec”, Nov. 2005, http://eprint.iacr.org/2005/416.pdf

[11] Patriciu V.V., “Criptografia şi securitatea rețelelor de calculatoare cu aplicații în C şi Pascal”, Ed. Tehnică, Bucureşti, 1994

[12] Scripcariu Luminița, “Bazele rețelelor de calculatoare”, Ed. Cermi Iaşi, 2005

[13] Tanenbaum S. Andrew, “Rețele de calculatoare”, Ed. Computer Press Agora, 1997

[14] Thomas J., Elbirt A.J., “Understanding Internet Protocol Security”, Electrical and Computer Engineering Department, University of Massachusetts Lowell, One University Avenue, Lowell, MA 01854, USA, 2006
http://faculty.uml.edu/aelbirt/IPsec.pdf

[15] *** http://en.wikipedia.org/

[16] *** http://www.securizare.ro/content/view/147/36 “Reguli de securizare pentru rețea”, 2004

[17] *** http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, “Announcing the ADVANCED ENCRYPTION STANDARD (AES)”, Publicația de procesare a standardelor 197, Nov. 2001

[18] *** http://docs.hp.com/en/T1428-90011/T1428-90011.pdf, Interlink Networks: “Introduction to Diameter”, Feb. 2002

[19] *** http://technology.berkeley.edu/policy/admsecpol.html, “Admin Apps and Data Security Policy”, 2008