11.Protectie si siguranta in functionare

a) Concepte fundamentale: exemple si comparatii intre Linux si Windows, UID si SETUID la Linux, SID si jetonul de acces la Windows
Cristian Saulea
b) Functiile principale din Win32 API legate de securitate;
Constantin Adina
c) Apelurile de sistem legate de securitate la Linux
Caju Ana-Maria
d) Implementarea securitatii la Linux si Windows
Munteanu Daniel-Dumitru

SUMAR:

Concepte fundamentale: exemple si comparatii intre Linux si Windows, UID si SETUID la Linux, SID si jetonul de acces la Windows - Cristian Saulea

Functiile principale din Win32 API legate de securitate; -Constantin Adina

2.2.5.1 Polita LSA
2.2.5.2 Filtrele de parole
2.2.5.3 Serviciul de securitate a atasamentelor
2.2.6 Control parental la Windows Vista

Apelurile de sistem legate de securitate la Linux - Caju Ana-Maria

3. Apelurile de sistem legate de securitate la Linux
3. Generalitati
3.1. Securitate prin parolare si criptare
3.2. PGP si criptarea cheiei publice
3.3.1. SSL, S-HTTP si S/MIME
3.3.2 Impelmentari Linux IPSEC
3.3.3 SSH (Secure Shell) si `stelnet`
3.3.4 PAM - Pluggable Authentication Modules
3.3.5 Incapsularea criptografica IP (CIPE)
3.3.6 Kerberos
3.3.7 Shadow Passwords
3.3.8 "Crack" and "John the Ripper"
3.4 Utilizatorul, Sistemul, si Procesul de administrare
3.4.1 Utilizarea Syslog
3.4.2. Folosirea utilizatorului de administrare
3.4.3. Utilizarea procesului de administrare
3.4.4. Administrarea utilizatorilor

Implementarea securitatii la Linux si Windows - Munteanu Daniel-Dumitru

4 Implementarea securitatii la Linux si Windows

4 Generalitati
4.1 Polita de utilizare
4.2 Securitate raportata la retea
4.2.1 Servicii vulnerabile
4.2.2 Posibile tipuri de atac
4.3 Securitate sub Windows
4.4 Securitate sub Unix/Linux
4.4.1 Conturi de utilizatori+parole
4.4.2 Permisiunile sistemului de fisiere sub Linux
4.4.3 Criptare si firewall
4.4.4 software-ul pentru verificarea securitatii

1.1.Concepte generale de securitate

Prevenirea accesului neautorizat la date sensibile este esential în orice mediu care implica accesul utilizatorilor multiplii la aceleasi resurse fizice sau de retea. Un sistem de operare trebuie sa fie în stare sa protejeze fisiere, memoria si setarile de configuratie de modificarile si vizualizarile nedorite. Securitatea sistemului de operare cuprinde mecanisme evidente, precum conturi, parole si protectie la nivel de fisiere. De asemenea mai cuprinde si mecanisme mai putin evidente, precum protejarea sistemului de operare de corupere, protejarea sistemului de diverse actiuni (reboot, de exemplu) care ar putea fi folosite de utilizatori cu drepturi mai putine, protejarea modificarilor unor programe ale unor utilizatori de catre alte programe, etc.

Un utilizator reprezinta o entitate care poate executa programe sau detine fisiere. Accesul la resursele sistemului se realizeaza prin intermediul utilizatorilor înregistrati, în functie de drepturile atribuite acestora.

Din punctul de vedere al sistemului de operare UNIX, un utilizator (numit si câteodata si cont de utilizator, user sau user account) nu este neaparat o persoana. Utilizatorii pot fi ori persoane reale, ori utilizatori logici. Acestia din urma sunt rezervati pentru anumite aplicatii care efectueaza activitati specifice . De asemenea, poate exista un cont utilizator partajat de mai multe persoane dintr-un grup de lucru. În majoritatea cazurilor, însa, un utilizator înseamna o anumita persoana care poate “intra” (log in) în sistem, executa programe si utiliza sistemul.

1.2.1.UID

Din punct de vedere al sistemului de operare ,fiecare utilizator este reprezentat printr-un numar ,numit user ID (identificatorul utilizatorului),la fel cum fiecare persoana are un CNP (cod numeric personal).Desi in realiatate noi spunem “fiecare nume are asociat un CNP”,sistemul de operare gandeste invers : el recunoaste utilizatorii dupa UID (calculatorul se “pricepe” mai bine la numere,pe cand identificatorii (etichetele) te tip text sunt specific umani – vezi cazul adrese IP- DNS).Pentru ca noi sa putem opera cu nume (care sunt mai usor de retinut decat numerele),sistemul de operare ne permite sa realizam asocieri UID-nume .

UID-ul este omniprezent in sistemul de operare: in drepturile de acces la sistem,in securitatea la nivel de fisier,in drepturile asociate unui proces care ruleaza etc.El este un numar mai mic sau egal cu 2147483647;exista urmatoarele conventii:

UID	Cont	Descriere
0 – 99	Root,daemon,bin,sys etc	Conturi de system
100 – 2147483647	Useri obisnuiti	Conturi normale de utilizator
60001	Nobody	Useri neautentificati
60002	Noaccess	Introdus pentru compatibilitatea cu Solaris 2.0 si SVR4

1.2.2.GID

Utilizatorii pot fi grupati în grupuri. Acestea sunt practic colectii de utilizatori si pot contine unul sau mai multi utilizatori. Fiecare grup are asociat un identificator de grup (Group ID sau GID), folosit intern de sistem.Folositi împreuna, identificatorul de utilizator respectiv identificatorul de grup determina drepturile de acces la fisiere si la alte resurse ale sistemului. Acesti doi identificatori sunt atribuiti în mod automat la momentul crearii utilizatorului, însa pot fi modificati si ulterior.

Fisierul care memoreaza informatiile despre utilizatori în UNIX este /etc/passwd, iar cel despre grupuri este /etc/group. Parolele utilizatorilor sunt memorate criptat, într-un fisier protejat, si anume /etc/shadow.
Fisierul /etc/passwd are urmatoarea structura:

nume : parola : UID : GID : informatii : director : shell , *unde:*

• *nume - este numele utilizatorului*
• *parola - reprezinta parola criptata a utilizatorului*
• *UID - reprezinta identificatorul utilizatorului,având în mod normal valoare unica*
• *GID - este identificatorul grupului principal din care face parte utilizatorul*
• *informatii - contine în mod normal numele utilizatorului.*
• *director - reprezinta directorul home al utilizatorului, de obicei /home/nume.Fiecare utilizator detine câte un asemenea director separat, folosit pentru a depozita fisierele proprii*
• *shell - este interpretorul de comenzi folosit de utilizator*.

1.2.3 SETUID

Procesele din UNIX au doua identitati la un moment dat. Prima identitate este identificatorul de utilizator real, adica cea data de numele de cont de la conectarea utilizatorului. Uneori, pentru executia anumitor programe sau comenzi, utilizatorii trebuie sa primeasca identitatea altui utilizator; acesta este identificatorul de utilizator efectiv EUID , valabil doar pe durata executiei respectivului program. Acest transfer de identitate este acceptat de proprietarul programului, prin setarea bitului Set UID (SUID) din drepturile de acces ale fisierului executabil.

1.2.4. SU (Substitute User)

Comanda su (Substitute User) permite schimbarea identitatii unui utilizatorDaca noul nume de cont furnizat este protejat prin parola, utilizatorul trebuie sa o furnizeze; daca utilizatorul real este root, nu este necesara furnizarea parolei.

Un exemplu de bit SETUID setat :
snark:~$ ls -l /bin/login
-rwsr-xr-x 1 root bin 20164 Dec 17 12:57 /bin/login

Precum contul de root insusi, programele setuid sunt folositoare dar periculoase. Oricine poate corupe sau modifica un program setuid detinut de root poate sa-l foloseasca pentru a porni un shell cu privilegii de root. Pentru acest motiv, deschiderea unui fisier pentru scriere dezactiveaza in mod automat bitul setuid pe cele mai multe Unixuri.

1.2.5.Afisarea utilizatorilor in Linux

Comenzi referitoare la utilizatori:
• whoami - furnizeaza numele utilizatorului efectiv curent

• who - afiseaza lista sesiunilor deschise ale utilizatorilor
• w - comanda înrudita cu who, afiseaza sesiunile deschise si, pentru fiecare sesiune în parte, ultima comanda executata
• id - ofera informatii privitoare la identitatea reala a unui utilizator:
• finger [nume] - afiseaza utilizatorii conectati curent la sistem. Daca este specificat un nume de utilizator, vor fi afisate diferite informatii despre respectivul utilizator, cum ar fi numele acestuia si ultima intrare în sistem
• last [nume] - afiseaza ultimele intrari ale utilizatorilor în sistem, în ordine descrescatoare a datei. Daca este specificat un nume de utilizator, jurnalul afisat se va referi la intrari ale utilizatorului respectiv.

[1]

1.3.1.SID

In locul utilizarii numelor (care pot sau nu sa fie unice) pentru a identifica entitatile care executa diferite actiuni în sistem, Windows utilizeaza identificatori de securitate (security identifiers – SIDs). Utilizatorii au asignat câte un SID, la fel si grupurile locale si de domeniu, calculatoarele locale, domenii, membrii domeniilor. Un identificator de securitate este o valoare unica de o lungime medie care este folosita pentru a identifica o politica de securitate sau o securitate de grup intr-un mediu de operare Windows. Identificatorii cei mai cunoscuti sunt de fapt un grup de identificatori care reprezinta generic niste utilizatori sau grupuri.Valorile lor raman constante in cadrul fiecarui sistem de operare.

Aceste informatii sunt benefice pentru diagnosticarea problemelor de securitate.De asemenea este folositor pentru afisarea potentialelor probleme in editorul ACL (Access Control List).

Windowsul acorda sau respinge accesul la sistemul de operare pe baza listelor de acces (ACL) ,pe care identificatorii de securitate le folosesc pentru a identifica utilizatorul sau grupul din care face parte.Cand un utilizator se logheaza pe calculator,se genereaza un jeton de acces care contine identificatorul de securitate al grupului utilizatorului si nivelul de privilegii acordat acestuia.Cand utilizatorul face o cerere la resursele calculatorului,jetonul de acces este verificat de lista de acces,ACL,pentru a ii permite sau refuza cererea la resursa respectiva.

Formatul identificatorului de securitate este urmatorul:

S-1-5-12-7623811015-3361044348-030300820-1013

S-prefix care identifica faptul ca stringul este un SID
1- numarul reviziei
5- autoritatea de securitate Windows
12-7623811015-3361044348-030300820 –identificatorul domeniului sau al calculatorului
1013 – ID relativ (RID)
Orice grup sau utilizator care nu este creat default va avea un identificator relativ mai mare ca 1000.

Când Windows este instalat pe un calculator, programul de setup emite calculatorului un SID care este asignat conturilor locale de pe calculator. Fiecare SID al conturilor locale este bazat pe identificatorul de securitate al calculatorului la care se adauga identificatorul relativ. Identificatorii relativi pentru conturile utilizatorilor încep de la 1000 si cresc cu 1 pentru fiecare nou cont sau grup. De asemenea Windows emite câte un SID pentru fiecare domeniu nou Windows .Identificatorii de securitate ai Windows sunt bazati pe identificatorii domeniului la care se adauga

identificatorii relativi (care încep de la 1000 si cresc cu 1 pentru fiecare nou utilizator sau grup).

Windows emite si identificatori de securitate bazati pe identificatorul unui calculator sau domeniu cu identificatori relativi ficsi. De exemplu, 500 este contul administratorului, iar 501 este cel de guest.

Cativa din cei mai cunoscuti identificatori de securitate, valorile numerice si utilizarea lor:

SID	Grup	Utilizare
S-1-1-0	Everyone	Grup care cuprinde toţi utilizatorii
S-1-2-0	Local	Utilizatori locali
S-1-3-0	Creator Owner ID	Un identificator de securitate care este înlocuit cu cel al utilizatorului care a creat noul obiect. Acest identificator este utilizat pentru intrările controlului de securitate moştenit.
S-1-3-1	Creator Group ID	Identificator care este înlocuit cu identificatorul grupului din care face parte utilizatorul care a creat obiectul.

[2][3][4]

1.3.2.Jetonul de acces

Un jeton de acces este un obiect care incapsuleaza descriptorii de securitate ai unui proces.Atasati unui proces,descriptorii de securitate identifica proprietarul unui obiec,in acest caz ai unui proces,si lista de acces care specifica drepturile pe care proprietarul le are asupra obiectului.Jetonul de acces este folosit de catre windows cand un proces sau un thread incearca sa interactioneze cu un obiect al carui descriptor de securitae forteaza lista de acces.

Jetonul de acces este generat de serviciul de logon cand un anumit utilizator se logheaza pe statie si credentialele oferite de catre utilizator sunt verificate in baza de autentificare,specificand drepturile pe care utilizatorul le are in descriptorul de securitate incapsulat de jeton.Jetonul este atasat fiecarui proces pornit de catre utilizator .Oricand un proces acceseaza resurse care sunt sub protectia listei de acces,Windows se uita in descriptorii de securitate ai jetonului de acces daca proprietarul acelui proces este eligibil sa acceseze acea informatie,si daca are dreptul,ca operatii poate executa (citire,scriere,executie).

Tipuri de jetoane de acces:-jetonul principal
-jetonul de impersonificare

1.3.2.1Jetonul primar

Jetonul primar poate fi asociat doar proceselor,si reprezinta subiectul de securiate al proceselor.Crearea jetonului primar si a asocierii acestora cu procese sunt operatii privilegiate ,care necesita 2 tipuri de privilegii: serviciul de autentificare care creaza jetonul,si servicil de logon care asociaza jetonul cu shelul utilizatorului.Procesele intial mostenesc o copie a jetonul procesului parinte.Jetonul de impersonificare poate fi asociat doar thread-urilor

1.3.2.2.Jetonul de impersonificare

Impersonificarea este un concept unic pt Windows,care permite aplicatiilor server sa fie temporar client in termeni de acces la obiecte securizate.Impersonificarea are 3 nivele posibile : -*identificarea* serverul inspecteaza identitatea clientului

-*impersonificarea* serverul actioneaza in numele clientului
-*delegarea* asemanator impersonificarii dar care se extinde la sisteme remote catre care serverul se conecteaza.

Clientul poate alege nivelul maxim de impersonificare ,daca este disponibil,al serverului ca un parametru al conexiunii.Delegarea si impersonificarea sunt operatii privilegiate.

1.3.2.3.Componentele unui jeton :

-un identificator
-identificatorul asociat sesiunii de logon
-identificatorul utilizatorului (acest camp este cel mai important si de sasemenea cel mai restrictiv-doar citire)
- identificatorul grupului din care face parte utilizatorul
-identificatorul grupului restrictiv(optinal).Aces set aditional de grupuri nu permite accesul,ci doar il restrictioneaza si mai mult;accesul la oun obiect este permis doar daca accesul este permis si unuia dintre aceste grupuri
-privilegiile ;ajoritatea privilegiilor sunt inactivate default. avaria
-proprietarul

[5]

2.1 Introducere in WinAPI

2.1.1 Windows API

Windows API, abreviat – WinAPI, este setul de interfete ale *aplicatiilor programabile* ale *nucleului* Microsoft disponibil in sistemele de operare Microsoft Windows. Aplicatiile programabile sunt utilizate pentru crearea rutinelor software personalizate. Interfata aplicatiilor programabile este o interfata a *codului sursa* (seventa de comenzi sau declaratii ale unui limbaj de programare, scrise intr-o forma accesibila utilizatorului uman) pe care un sistem de operare sau o biblioteca o furnizeaza pentru deservirea cererilor de servicii (cereri efectuate de catre programe). Nucleul (denumit si *kernel*) reprezinta componenta centrala a majoritatii sistemelor de operare. Intre responsabilitatile sale este inclusa administrarea resurselor sistemului (comunicatia intre componentele hardware si software).

Programele Windows, cu exceptia *consolelor de program*, interactioneaza cu Windows API indiferent de limbajul utilizat. Un program consola reprezinta un program care ruleaza in DOS sau intr-o fereastra DOS chiar si atunci cand este rulat in Windows. API (*API - Application Programming Interface*), presupune existenta unor instrumente de programare care sa permita dotarea aplicatiilor cu interfete grafice care sa respecte anumite standarde (standardele API includ - ferestre, meniuri, bare, controale, ferestre de dialog).

Arhitectura sistemelor de operare Windows este modulara si este constituita din doua niveluri principale : componente care ruleaza in *modul utilizator* si componente care ruleaza in *modul nucleu (kernel)*. Programele si subsistemele din modul utilizator sunt limitate din punctul de vedere al accesului la resurse, in timp ce in modul kernel accesul la memoria sistemului si dispozitivele externe este nerestrictionat.Accesul la un nivel inferior al sistemului Windows, de cele mai multe ori necesar pentru driverele componentelor este oferit de Windows Driver Foundation in versiunile curente de Windows.

O schema a arhitecturii Windows este urmatoarea:

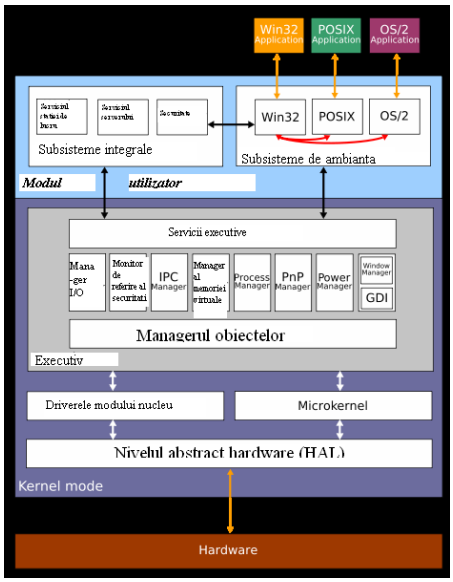

***Fig. 1** [1]*

Serviciile oferite de Windows API pot fi grupate in sapte categorii:

***1.** Servicii de baza* – ofera acces la resursele fundamentale disponibile intr-un sistem Windows. Sunt incluse urmatoarele componente:

• *sistemul de fisiere* - metoda de stocare si organizare a fisierelor calculatorului, si a informatiilor continute de acestea pentru o cautare si accesare mai rapida. Sistemul de fisiere reprezinta un set de tipuri abstracte de date care sunt implementate pentru stocarea, organizarea ierarhica, manipularea, cautarea, accesarea si recuperarea datelor;

• *procese* - procesul reprezinta o instanta a unui program care este executat in mod secvential. Programul in sine reprezinta o colectie pasiva de instructiuni in timp ce procesul reprezinta executarea propriu-zisa a instructiunilor respective;

• *accesul la registrele Windows* - acesta reprezinta un director in care sunt stocate setarile si optiunile sistemului de operare Windows. Contine informatii si setari pentru hardware, software-ul sistemului de operare, useri etc. Cand un utilizator executa modificari in setarile Control Panel, asocierile de fisiere, politicile de system sau modificari ale software-ului instalat, aceste modificari se reflecta in salvarile sin registrele Windows;

• *manipularea erorilor*.

Aceste functii sunt disponibile in kernel.exe, krnl286.exe si krnl1386.exe pentru Windows pe 16 biti si in kernel32.dll si advapi32.dll pentru Windows pe 32 biti. *[2]*

***2.** Interfata grafica* – ofera functionalitatea pentru afisarea continutului grafic pe monitoare, imprimante si alde dispozitive de iesire. Functii disponibile in gdi.exe pentru Windows pe 16 biti sau gdi32.dll pentru Windows pe 32 de biti. *[2]*

***3.** Interfata cu utilizatorul* – ofera suportul necesar utilizatorului pentru a crea si manevra fereastra de Windows si controlul de baza la consola al utilizatorului, cum ar fi butoanele si scroll-ul, semnalele de intrare date de mouse si tastatura. Functiile: user.exe pentru Windows pe 16 biti si user32.dll pentru Windows pe 32 biti. Incepand cu varianta Windows XP, controlul de baza este oferit de comctl32.dll (Common Control Library). *[2]*

***4.** Funcţii API de control prin dialog în fereastră. Biblioteca ferestrei de dialog* – ofera aplicatiilor fereastra de dialog standard pentru deschiderea sau salvarea fisierelor, alegerea culorii sau a fontului etc.

In cadrul interfetei grafice cu utilizatorul, o *fereastra de dialog* este o fereastra speciala, utilizata pentru afisarea informatiilor catre utilizator sau pentru a primi un raspuns, in cazul in care acesta este necesar. Denumirea de "fereastra de dialog" vine de la faptul ca se formeaza un dialog intre calculator si utilizator – fie pentru informarea utilizatorului, fie pentru obtinerea unor informatii de la utilizator. Functiile sunt disponibile prin commdlg.dll pentru Windows pe 16 biti si comdlg.dll pentru Windows pe 32 biti. Sunt grupate in categoria *Interfata cu utilizatorul* oferita de API. *[2]*

5. *Functii API de control comun. Libraria controlului comun* – dispune accesul la unele functii avansate de control oferite de sistemul de operare, cum ar fi: barele de stare, barele de progres, barele de unelte si tab-urile.

• *Bara de stare* este o componenta in general prezenta in partea de jos a undei ferestre Windows. De cele mai multe ori aceasta bara este divizata in mai multe sectiuni, fiecare sectiune prezentand anumite informatii. Functia principala a berelor de stare o reprezinta afisarea informatiilor despre starea curenta a ferestrei de lucru.

• *Bara de progres* reprezinta o componenta a interfetei grafice cu utilizatorul care indica progresul unei sarcini de lucru, cum ar fi download-ul sau transferul unui fisier. De cele mai multe ori, partea grafica a barei de progres este insotita de o reprezentare textuala a progresului, sub forma da procente.

• *Bara de unelte* este reprezentata printr-un rand, o coloana sau un bloc de butoane care atunci cand sunt selectate activeaza anumite functii ale programului.

Pentru Windows pe 16 biti functiile se regasesc in commctrl.dll si pentru Windows pe 32 biti in comctl32.dll *[2]*

6. *Functii de acces la nucleul Windows* – Componente ale Windows API care permit aplicatiilor sa acceseze sau modifice functionalitatile oferite de *shell-ul* sistemului de operare. *Shell-ul* este un soft care ofera o interfata pentru utilizatori. Shell-urile unui sistem de operare permit accesul la serviciile oferite de catre kernel. Acestea pot fi incadrate intr-una din categoriile *linie de comanda* sau *grafica.* Shell-ul din categoria liniei de comanda asigura interfata liniei de comanda (*CLI – Command Line Interface*) pentru sistemul de operare, in timp ce shell-ul de tip grafic asigura existenta interfetei grafice cu utilizatorul (*GUI – Graphical User Interface*).

Functiile se regasesc in shell.dll pentru Windows pe 16 biti si in shell32.dll si pentru versiuni mai noi decat Windows 95 in shlwapi.dll pentru Windows pe 32 biti. *[2]*

7. *Serviciile de retea* – ofera accesul la diferite functii ale retelei oferite de sistemul de operare. Sub-componente ale sale sunt:

• *NetBIOS* este un acronim pentru *Network Basic Input/Output System.* API-ul NetBIOS permite aplicatiilor rulate in calculatoare diferite sa comunice intr-o retea locala de calculatoarea (*LAN – Local Area Network*). NetBIOS ofera servicii legate de *nivelul sesiune* al Modelului OSI (Acesta – nivelul sesiune – ofera mecanismele pentru manevrarea dialogului dintre procesele aplicatiilor end-user).

• *Winsock* – abreviere de la *Windows Sockets API,* reprezinta specificatiile tehnice care definesc modul in care software-ul de retea ar trebui sa acceseze serviciile retelei, in mod special *TCP/IP* (*TCP/IP – Transmission Control Protocol/ Internet Protocol*). Winsock defineste o interfata standard intre o aplicatie client TCP/IP a Windows (de exemplu – un client FTP sau un client Gopher) si stiva de protocoale TCP/IP.

• *NetDDE* –reprezinta o abreviere a *Network Dynamic Data Exchange,* unde DDE reprezinta o tehnologie pentru comunicatie intre multiple aplicatii care ruleaza sub Microsoft Windows (aceasta tehnologie a fost exclusa din versiunea Windows Vista *[3]*) si OS/2 (*OS/2*

– *Operating System/2* – un sistem de operare creat si implementat de IBM). NetDDE reprezinta o extensie a DDE utilizata pentru initierea si mentinerea unei legaturi necesare pentru conversatii DDE intre aplicatii care ruleaza pe calculatoare diferite in cadrul unei retele. O conversatie DDE reprezinta interactiunea intre o aplicatie de tip client si o aplicatie de tip server.

• *RPC – Remote Procedure Call*, reprezinta tehnologia care permite unui program executarea unei subrutine sau a unei proceduri intr-o alta locatie de memorie (in general un alt calculator) fara a fi necesara scrierea explicita a codului necesar pentru efectuarea acestor operatiuni la distanta (*remote*). Adica, un programator ar trebui sa scrie acelasi cod de program indiferent daca subrutina este locala (pentru programul rulat) sau la distanta (remote).

2.1.2 Versiuni Windows API

Microsoft Windows reprezinta numele mai multor familii de sisteme de operare ale Microsoft. Primul mediu de operare introdus de Microsoft s-a numit Windows si a fost lansat in noiembrie 1985, aparut ca o adaugire la MS-DOS datorita interesului crescut pentru interfata grafica cu utilizatorul.

• *SO Windows pe 16 biti* – versiunile initiale ale Windows au fost gandite in principal ca interfete grafice cu utilizatorul, acestea ruland peste MS-DOS. Variantele pe 16 biti beneficiau totusi de format propriu de fisiere executabile si drivere propirii (pentru imprimanta, mouse, tastatura, sunet, video) pentru aplicatii. In comparatie cu MS-DOS, Windows permite utilizatorilor rularea in paralel a mai multor aplicatii grafice, datorita cooperarii multitasking. Windows a implementat o tehnica ce ii permite rularea aplicatiilor de dimensiune mai mare decat memoria disponibila – segmentele de cod si resursele sunt manevrate in memorie si eliberate cand memoria disponibila devine o problema, si segmentele de date sunt incarcate in memorie cand o anumita aplicatie elibereaza procesorul, in general in asteptarea acestor informatii. Versiunile de Windows pe 16 biti: *Windows 1.0 (1985), Windows 2.0 (1987), Windows/286 (1988).*

• *SO Windows pe 32 biti* – a introdus nucleul in mod protejat si monitorizarea masinii virtuale. S-a imbunatatit grafica, in principal datorita memoriei virtuale si a driverelor componentelor incarcabile virtual, ceea ce a permis impartirea dispozitivelor arbitrare intre ferestrele DOS. Datorita acestui aspect, aplicatiile Windows au putut fi rulate in modul protejat pe 16 biti, ceea ce a oferit accesul la mai multi megabytes de memorie, desi rulau in continuare in acelasi spatiu de adrese unde memoria segmentata oferea un grad ridicat de protectie. Versiunile de Windows pe 32 biti: *Windows 95 (1995, 1996, 1997), Windows 98(1998)* si *98 SE (1999), Windows Me(2000), Windows NT 3.1 (1993)* si *NT 4.0 (1996).*

• *SO Windows pe 64 biti* – Windows NT a putut suporta diferite platforme inainte ca *x86* sa devina dominant. Versiunile NT intre 3.1 si 4.0 puteau suporta procesoare pe 64 biti (cum ar fi DEC Alpha si MIPS R4000), desi sistemul de operare le trata ca si procesoare pe 32 biti. Cu introducerea arhitecturii Intel Itanium, referita ca IA-64, Microsoft a eliberat versiuni noi de *Windows 2000* pentru a o sprijini. Versiunile Itanium de Windows XP si Windows Server 2003 au fost eliberate în acelasi timp cu x86 (pe 32 biti). Pe 25 aprilie 2005, Microsoft a eliberat *Windows XP* Professional x64 Edition si versiunile x64 de *Windows Server 2003* pentru a sprijini arhitectura AMD64 Intel64 (sau x64 în terminologia Microsoft). Microsoft a renuntat la sprijinul pentru versiunea Itanium de Windows XP în 2005. *Windows Vista* este prima versiune de Windows pe care Microsoft a eliberat-o simultan pe 32 si 64 biti

Aproape orice noua versiune de Microsoft Windows a introdus adaugiri pentru WinAPI. Totusi, acest nume nu a fost schimbat indiferent de versiunea de Windows, si schimbarile care

au survenit, totusi, au fost limitate de schimbarile arhitecturale si de platforma pentru Windows.

Win16 – reprezinta API pentru primele versiuni ale Microsoft Windows, pe 16 biti. Initial au fost referite doar ca Windows API, dar au fost redenumite pe parcurs pentru a se face distictia de noua versiune pe 32 biti. Functiile principale sunt reunite in kernel.exe (sau krnl286.exe sau krnl368.exe), user.exe si gdi.exe. In ciuda extensiei utilizate ".exe", acestea sunt de fapt librarii cu referinte dinamice.

Win32 - reprezinta API pentru versiunile moderne de Windows pe 32 biti. API este format din functii implementate in sistem, *DLL*. *DLL - Dynamic link library* - este implementarea Microsoft a conceptului de biblioteci in comun în Microsoft Windows si OS/2. Aceste biblioteci au de obicei extensia DLL sau OCX(pentru biblioteci continand controale ActiveX). Formatul fisierelor pentru DLL-uri sunt aceleasi ca pentru fisierele Windows EXE - *Portable Executable(PE)* pentru Windows pe 32-biti si *New Executable (NE)* pentru Windows pe 16-biti. DLL-urile pot sã continã coduri , informatii si resurse, sau orice combinatie intre acestea. Functiile principale Win32 sunt reunite in kernel32.dll, user32.dll si gdi32.dll. Win32 a fost introdus odata cu lansarea Windows NT. In Windows NT 4.0 si succesorii sai, apelurile Win32 sunt executate de doua module, csrss.exe (Client/Server Runtime Server Subsystem) in modul utilizator si win32k.sys in modul kernel.

Win32s – este o extensie a familiei Windows 3.1x. Win32s a fost implementat ca un subset al Win32(*terminatia "s" vine de la "subset").* Win32s este un mediu de executie al aplicatiilor pe 32 biti pentru sistemul de operare Windows 3.11. El permite unor aplicatii pe 32 biti sa fie rulate intr-un sistem de operare pe 16 biti utilizand apelurile de proceduri.

Win32 pentru Windows pe 64 biti – anterior cunoscut sub numele de Win64, este versiunea API pentru variante de Windows pe 64 biti: Windows XP Professional x64 Edition, Windows Server 2003 x64 Edition(pentru procesoare x86-64) si Windows XP 64-bit Edition si Windows Server 2003 pentru seriile Itanium. *Itanium* reprezinta numele brand-ului pentru procesoarele Intel pe 64 biti care au implementat arhitectura *Intel Itanium.* Arhitectura Itanium este diferita de arhitectura x86 prin faptul ca aceasta se bazeaza pe paralelismul instructiunilor, compilatorul stabilind care sunt instructiunile care vor fi rulate in paralel. Aceasta modificare ii permitea procesorului sa execute pana la sase instructiuni intr-un ciclu de ceas, dar compilatorul trebuia sa tina evidenta dependentelor dintre instructiuni in timpul executarii intrucat nu exista un hardware dedicat care monitorizeze acest aspect.

2.1.3 Suportul oferit de compilator

Pentru a putea dezvolta software care utilizeaza Windows API, un compilator trebuie sa fie capabil sa importe si manevreze DLL-uri si obiecte-COM specifice Microsoft.

• *DLL - Dynamic link library* - este implementarea Microsoft a conceptului de biblioteci in comun în Microsoft Windows si OS/2. Aceste biblioteci au de obicei extensia DLL sau OCX(pentru biblioteci continand controale ActiveX). Formatul fisierelor pentru DLL-uri sunt aceleasi ca pentru fisierele Windows EXE - *Portable Executable(PE)* pentru Windows pe 32-biti si *New Executable (NE)* pentru Windows pe 16-biti. DLL-urile pot sã continã coduri , informatii si resurse, sau orice combinatie intre acestea.

• *COM – Component Object Model* – este o platforma pentru componentele software, introdusa de Microsoft in 1993. Aceasta este utilizata pentru activarea comunicarii interproces si a crearii dinamice de obiecte in orice limbaj de programare care suporta aceasta tehnologie.

Compilatorul trebuie sa accepte limbajul C sau C++ si sa manipuleze fisierele IDL(Interface Definition Language) sau antetul fisierelor care contin in interiorul lor nume de functii API. *IDL – Interface Definition(Description) Language* este un limbaj specific utilizat pentru a descrie interfata software a unei componente, permitand totodata comunicarea intre componente software care nu sunt scrise in acelasi limbaj (de exemplu – componente scrise in C++ si componente scrise in Java). IDL-urile sunt utilizate in mod curent in cadrul apelurilor de proceduri la distanta (remote), in acest caz masinile aflate la capetele lantului de comunicare putand utiliza sisteme de operare (sau limbaje) diferite. Aceste conditii esentiale (compilator, unelte, librarii si antete) sunt cunoscute sub numele de Platforma Microsoft SDK. Initial doar compilatoarele Borland si compilatoarele familiei Microsoft Visual Studio puteau asigura aceste cerinte, mentionate anterior.

Astazi, proiectele MinGW si Cygwin ofera un astfel de mediu bazat pe colectia de compilatoare GNU, folosind o colectie de fisiere de antet pentru a face legatura cu DLL-urile Microsoft posibila. “LCC-Win32” este un compilator C grauit pentru utilizari in scopuri non-comerciale, intretinut de Jacob Navia.

Compilatorul specific Windows este necesar pentru manipularea erorilor. Sistemul este folosit in mod dual: asigura un substrat pe care poate fi implementata manipularea erorilor si modul in care nucleul anunta aplicatiilor conditiile exceptionale aparute, cum ar fi deservirea unui pointer invalid sau depasirea stivei.

2.2 Securitate

In vederea asigurarii protectiei documentelor dintr-un sistem, s-a recurs la alocarea de drepturi utilizatorilor/grupurilor de utilizatori pe baza utilizarii unui *username (nume de utilizator)* si a unei *parole*. Utilizatorii care incearca sa acceseze documentele protejate sunt *autentificati* conform unei liste de *autorizare*. *Autentificarea* – este procesul de verificare a identitatii digitale a unui emitator din cadrul unei comunicatii (de exemplu, o cerere de logare in sistem). Emitatorul ce se doreste a fi autentificat poate fi reprezentat de un utilizator al unui calculator, un calculator propriu-zis sau un program. *Autorizarea* – este procesul (componenta a unui sistem de operare) care protejeaza resursele unui calculator permitand utilizarea acestora numai de catre consumatorii care au primit drepturi de utilizare. Resursele sunt reprezentate de fisiere individuale, programe, componente ale calculatorului sau functionalitati oferite de catre anumite aplicatii. Exemple de consumatori de resurse pot fi – utilizatori umani, programe sau alte componente ale calculatorului.

2.2.1 SDK(Software Development Kit) pentru managementul de alocare a drepturilor asupra unui director activ

SDK poate fi utilizat de aplicatii pentru a impune termenii folositi in criptari digitale, indiferent de formatul si continutul lor.

Scopul *directorului activ – Active Directory (DA)* este asigurarea serviciilor de autentificare si autorizare centralizate pentru computerele ce utilizeaza medii Windows. Directorul activ stocheaza informatii si setari intr-o baza de date centrala.

Managementul de alocare a drepturilor – RMS (Rights Management Services) este o tehnologie Microsoft Windows utilizata pentru a proteja documente, cum ar fi email-uri, documente Word sau pagini web. *RMS* este utilizat pentru a limita accesul la documentele protejate doar pentru utilizatorii autorizati. Este utilizata o arhitectura de tip client-server pentru a gazdui managementul de alocare a drepturilor asupra unui director activ. Clientul RMS este necesar atat pentru crearea continutului protejat cat si pentru accesarea acestuia.

Continutul RMS protejat este criptat si contine o polita de utilizare in care sunt definite drepturile pe care orice utilizator/grup de utilizatori le detine asupra acestuia. Tipuri de drepturi – permisiune de citire a documentului, copiere, printare, salvare, editare.

2.2.1.1 Scenarii in care se foloseste:

• dezvoltatorii in domeniul reclamelor publicitare digitale/producatorii de software vor sa limiteze accesul la desenele lor la doar un grup restrans de utilizatori din cadrul diviziei de cercetare fara a fi necesare parole.

• o firma de avocatura doreste sa previna ajungerea in exterior a unor mail-uri confidentiale

• o firma din domeniul designului de pagini web vrea sa permita accesul la imaginile expuse/create de catre acea firma la o rezolutie proasta in mod gratuit, sau la o rezolutie foarte buna – contra cost.

• Proprietarii unei librarii cu documentatii online vor sa detecteze identitatea vizitatorilor si vor sa le permita acestora descarcarea de fisiere cu drept de vizualizare sau printare, totul pe baza de parola.

2.2.1.2 Vedere de ansamblu din punct de vedere administrativ:

Incepand cu Windows Server 2008, managementul de alocare a drepturilor asupra unui director activ implementeaza un script API usor de utilizat, pentru a facilita automatizarea managementul resurselor si serviciilor. Figura prezinta nivelele infrastructurii la care se pot efectua task-uri de management:

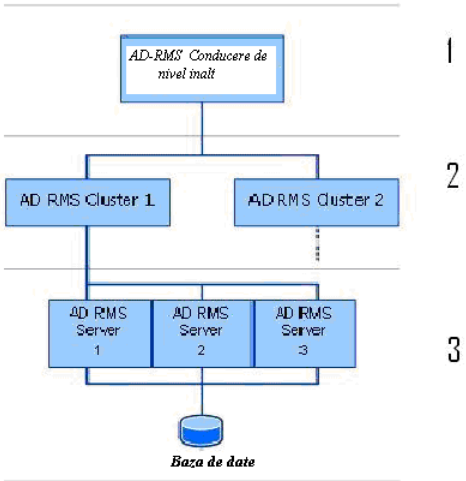

***Fig. 2** [4]*

***1 – Conducerea de nivel inalt:** manipuleaza mai degraba servicii decat componente sau computerele care le implementeaza.*

***2 – Managementul clusterelor:** administreaza componentedin calculator, organizate in clustere.*

***3 – Managementul calculatorului:** administreaza componente tinute in computere individuale.*

2.2.1.3 Arhitectura de conducere:

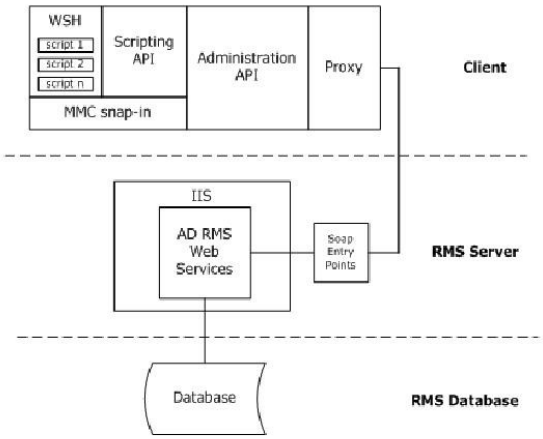

***Fig. 3** [5]*

Dupa cum se poate observa si din figura, componente arhitecturale sunt instalate la clienti, unul sau mai multe servere RMS (*Rights Management Services*) si cel putin un server ce tine baza de date.

Serverul de management de alocare de drepturi contine:

• Servicii web: functionalitatea nucleului este implementata ca un set de servicii web de tip ASP.NET al Microsoft, care ruleaza sub Microsoft Internet Information Services (IIS). Serviciile includ: administrare, certificare de conturi si licentiere.

• Interfete SOAP: fiecare serviciu este expus clientului prin intermediul unui punct de intrare SOAP (Simple Object Access Protocol)

Clientii au in componenta urmatoarele:

• Proxy de servicii web: clientii folosesc proxy-ul pentru a comunica cu un serviciu web tinut pe serverul RMS.

• Administrare API: Acest API este un nivel abstract aflat deasupra proxy-ului serviciilor web care expune functii de administrare clientului. API contine obiecte private si publice si este implementat si instalat in cache-ul asamblorului global. (GAC – Global Assembly Cache)

• MMC Snap-in: Snap-in este tipul primar de unealta de management care asigura un set de functionalitati necesar pentru administrarea tehnologiei sau aplicatiilor intr-o consola MMC(Microsoft Management Console).
Snap-in are acces la toate functiile implementate de administrarea API.

• Programarea API: Programarea managementului de alocare a drepturilor asupra unui director activ este expusa prin intermediul unui obiect COM care trebuie creat din administrarea API.

• Programe personalizate: se pot crea programe(scripturi) personale care sa automatizese task-urile administrative. Scripturile sunt gazduite in Windows Script Host (WSH) pe calculatorul client.

Serverul ce gazduieste bazele de date ruleaza urmatoarele baze de date:

• configurare

• logare

• directoarele de servicii

2.2.2 Autentificarea

Autentificarea este procesul prin care sistemul valideaza informatiile de utilizare transmise de catre utilizator. Userul si parola transmise de catre utilizator sunt comparate cu o lista de astfel de informatii autorizate, si daca exista o potrivire intre aceste informatii, accesul este permis in functie de permisiunea oferita userului respectiv prin lista de acces. Tehnologiile de autentificare Microsoft includ: LSA Authentication, Credentials Management, Smart Card Authentication, Network Provider, Security Support Provider Interface (SSPI), Winlogon, and GINA.

2.2.2.1 Modul de conducere a scrisorilor de acreditare(Credential Management) – dezvoltatorii care scriu pentru Microsoft pot folosi interfata de aplicatie programabila (API) pentru conducerea scrisorilor de acreditare incluzand functiile interfetei cu utilizatorul pentru a obtine si gestiona informatii de acreditare cum sunt utilizatorul si parola. Aceste functii utilizeaza interfete de tipul interfetei cu utilizatorul a Windows-ului. Sunt incluse optiuni suplimentare ce permit completarea informatiilor initiale ale utilizatorului. O *scrisoare de acreditare* reprezinta un atestat de calificare, de competenta sau de autorizare. Scrisorile de acreditare sunt utilizate in sistemele informatice pentru a se controla accesul la informatii sau alte resurse, iar forma cea mai comuna de prezentare este combinatia *numar de cont(utilizator) / parola*.

2.2.2.2 Modul de autentificare LSA (Local Security Authority) – descrie componentele pe care aplicatiile le folosesc pentru autentificarea si logarea utilizatorilor in sistemul local. De asemenea se ocupa de modul in care sunt create si apelate pachetele de autentificare si cele de securitate. *LSA* este un proces al sistemului de operare Microsoft Windows responsabil de respectarea politelor de securitate in cadrul sistemului. Cu ajutorul LSA se verifica logarea utilizatorilor la un calculator/server Windows, se administreaza modificarea parolelor de acces, si se creeaza log-urile de acces.

Modelul de autentidicare LSA - functionalitati:

• Autentificare LSA suporta pachete de autentificare modificabile. Acest lucru le permite utilizatorilor sau comerciantilor independenti de software (ISV – independent software vendors) sa modifice sau inlocuiasca rutinele de autentificare in vederea completarii autentificarii standard oferite de Microsoft. In timp ce pachetele de autentificare oferite de Microsoft necesita informatii de logare sub forma de username si parola, pachetele suplimentare de autentificare pot lua si alte forme pentru informatiile de logare, cum ar fi informatiile cardurilor ATM sau numarul personal de identificare (PIN). Un pachet personalizat de autentificare poate fi utilizat pentru implementarea unui nou protocol de securitate.

• LSA suporta pachete personalizate de securitate. Aceasta functionalitate a autentificarii este accesata utilizand aceeasi interfata ca pachetele de autentificare de sine statatoare, in timp ce functionalitatea providerului suportului de securitate este accesat utilizand interfata proprie SSPI - *Security Support Provider Interface*. Setul de functii suport al LSA permite accesul la functii de securitate avansate, cum ar fi crearea de token-uri si conducerea suplimentara a scrisorilor de acreditare.

• Fiecare clasa de logare a componentelor instalate pe un sistem poate avea propriul proces de logare. Clasele de componente in general include componente cum ar fi cititoarele de smart card-uri. Totusi, in scopul LSA, retelele conectate sunt tratate tot ca niste

componente ale sistemului. Prin creare, sistemele de operare Windows folosesc un proces de logare care suporta usernameul si parola introduse in mod interactiv de la tastatura.

2.2.2.3 Modelul de autentificare SSPI(Security Support Provider Interface) – permite unei aplicatii sa utilizeze diverse modele de securitate disponibile pe un calculator sau intr-o retea fara a schimba interfata cu securitatea sistemului. SSPI nu stabileste scrisori de acreditare in timpul logarii deoarece este in general o operatiune privilegiata de care se ocupa sistemul de operare. Un provider de suport de securitate (SSP – Security Support Provider) este continut intr-un DLL care implementeaza SSPI creand unul sau mai multe pachete de securitate disponibile aplicatiilor. Fiecare pachet de securitate contine maparea intre apelurile de functii SSPI ale unei aplicatii si functiile reale ale unui modle de securitate. Pachetele de securitate sunt suportate de un protocol de securitate cum ar fi autentificarea *Kerberos* si administratorul LAN. Interfata SSPI este disponibila in modul kernel si in modul utilizator. Pentru a folosi functionalitatea SSPI in modul kernel, trebuie instalat Windows Installable File System DDK.

2.2.2.4 Pachetele de securitate personalizate: Pentru a implementa noi protocoale de securitate care sa fie integrate cu Windows Server si sistemele de operare Windows, se foloseste API-ul pachetelor de securitate personalziate si functiile LSA. Acestea suporta dezvoltarea combinata de SSP-uri personalizate(SSP – Security Support Provider), care permit servicii de autentificare non-interactiva si schimb securizat de mesaje pentru aplicatiile client/server.

2.2.3 Autorizarea

Autorizarea este dreptul oferit unui utilizator pentru a folosi sistemul si data stocata pe acesta. Autorizarea este in general setata de administratorul de sistem si verificata de calculator prin intermediul unei forme de identificare a utilizatorului, cum ar fi numarul de cod sau parola. Tehnologiile de autorizare Microsoft include Administratorul Autorizatiilor (AM – Authorization Manager) si Authz API.

Controlul accesului de tip client/server:

O aplicatie de tip server ofera servicii clientilor. De exemplu, un server ar putea efectua urmatoarele servicii pentru un client:

- salvarea si oferirea informatiilor dintr-o baza de date privata
- acces la resursele de retea
- pornirea proceselor in contextul securitatii disponibile clientului, pe calculatorul server

Un server protejat controleaza accesul la serviciile sale. Windows ofera suportul pentru oferirea urmatoarelor functii de securitate:

- logarea unui client pe server
- conectarea la resursele de retea in contextul securitatii disponibile clientului
- crearea descriptorilor de securitate pentru protejarea obiectelor private
- verificarea unui descriptor de securitate pentru a vedea daca se permite accesul la un client
- verificarea faptului c aun set de privilegii sunt activate in token-ul unui client
- generarea mesajelor audit in logul evenimentelor de securitate pentru inregistrarea tentativelor unui client de a accesa obiecte sau utiliza privilegii.

2.2.4 Criptarea

Criptarea reprezinta utilizarea unor coduri cu scopul convertii datei astfel incat numai un anumit rezipient sa fie capabil sa o descifreze, folosind o cheie. Tehnologiile de criptare Microsoft includ CryptoAPI 2.0, Cryptographic Service Providers (CSP), CryptoAPI Tools, CAPICOM, WinTrust, administrarea certificatelor si dezvoltarea unei infrastructuri de chei publice perzonalizate.

2.2.4.1 Data codata si decodata:

Pentru a putea transmite datele de-a lungul unui mediu de comunicatie cum ar fi de exemplu o linie telefonica, data trebuie serializata, adica trebuie convertita intr-un sir de unuri (“*1”*) si zerouri(“*0”*) care se transmit serial de-a lungul liniei. Acest lucru trebuie facut astfel incat computerul care receptioneaza data sa o poata converti inapoi in formatul sau original. Serializarea este realizata cu ajutorul protocolului de comunicare, si este controlata atat software cat si prin transmisia hardware. Sunt mai multe nivele la care se face coversia datelor. Un exemplu este in figura:

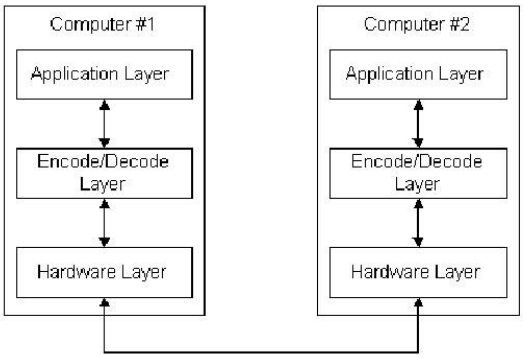

***Fig. 4** [6]*

In figura se exemplifica cum nivelul aplicatie al calculatorului #1 transmite data ce urmeaza sa ajunga la calculatorul #2 catre nivelul de codare/decodare. Acesta codeaza data intr-un sir de biti. La cel mai jos nivel, nivelul hardware, se convertesc bitii intr-un sir serial de unuri si zerouri care este transmis de-a lungul liniei catre calculatorul #2. Nivelul hardware al calculatorului #2 converteste unurile si zerourile inapoi in biti, si ii transmite mai sus catre nivelul de codare/decodare pentru a fi decodati, abia poi fiind transmisi catre nivelul aplicatie, aflat mai sus.

Un principiu de design software acceptat este utilizarea abstractizarii, adica descrierea unei probleme sau a unui obiect in termeni generali ai acestuia (parametri generali) mai degraba decat detalierea resurselor necesare rezolvarii problemei, sau a detaliilor unui obiect.

Majoritatea protocoalelor de comunicatie de folosesc de abstractizare. Obiectele de la nivelele superioare sunt definite in mod abstract si sunt destinate implementarii folosindu-se obiecte de la nivelele inferioare. De exemplu, un serviciu de la un nivel ar putea cere transferarea unor obiecte abstractizate intre calculatoare. Un nivel inferior poate utiliza reguli de codare pentru a transforma obiectul abstractizat intr-un sir de unuri si zerouri.

2.2.4.2 Criptarea si decriptarea datelor:

Criptarea este procesul translatarii datei sub forma textuala (*plain text data*) intr-o forma ce pare a fi aleatoare si fara un inteles aparent. Decriptarea este procedeul inver, de transformare a datei criptate inapoi in forma sa textuala.

Pentru criptarea unei date de dimensiuni mai mari, este utilizata criptarea simetrica. Cheia simetrica este utilizata atat in timpul procesului de criptare cat si in timpul decriptarii. Scopul oricarui algoritm de criptare este acela de a face textul cat mai greu de descifrat. Chiar si utilizarea unei chei de 40 biti presupune existenta a mai mult de un miliard de variante posibile de criptare.

2.2.4.3 Cryptographic Service Providers:

Un CSP(*Cryptographic Service Provider*) contine implementarea unor standarde si a unor algoritmi de criptare. In forma sa minima, contine un DLL care implementeaza functii in CryproSPI (SPI – System Program Interface). Majoritatea CSP contin implementarea tuturor functiilor sale.

2.2.4.4 Criptarea API – generatia urmatoare:

Criptarea API – noua generatir (*CNG – Cryptography API, Next Generation*) va inlocui pe termen lung forma actuala, CryptoAPI. CNG se doreste a fi extensibila la mai multe nivele. Se considera ca ea va fi utila dezvoltatorilor de aplicatii care vor permite utilizatorilor crearea si schimbarea documentelor intr-un mediu sigur, cu atat mai mult utilizandu-se un mediu de transmisiune mai putin sigur cum este Internetul. Acesti dezvoltatori ar trbui sa fie familiari cu limbajul de programare C si C++ si mediul de programare de baza al Windows-ului.

CNG poate fi momentan utilizat pe Windows Server 2008 si Windows Vista.

2.2.5 Administrarea securitatii

Tehnologiile de administrare pot fi utilizate pentru administrarea politei LSA si a politei de filtrare a parolei (*password filter*), cerrea de abilitate a programelor din surse externe ai a serviciul de securitate al atasamentelor care extinde sunctionalitatea uneltei de configurare a securitatii.

Tehnologiile de administrare Microsoft includ polita LSA API, Filtrarea Parolelor API, si Serviciul de Securitate al Atasamentelor API. Aceste tenologii permit programatorilor dezvoltarea de aplicatii care administreaza sisteme si aplicatii.

2.2.5.1 Polita LSA – LSA este un subsistem protejat al Windows-ului care pastreaza informatii despre toate aspectele referitoare la securitatea locala a unui sistem. LSA ofera servicii de translatare intre nume si identificatori de securitate (SID – Security Identifiers).Pentru variantele de Windows Me/95/98 LSA nu face parte din sistem.

2.2.5.2 Filtrele de parole – ofera un mod de implementare de polite pentru parole si de schimbare a notificarii. Cand se efectueaza o cerere de schimbare a parolei, LSA face un apel catre filtrul de parole inregistrat in sistem. Fiecare filtru de parole este apelat de doua ori, prima data pentru a valida noua parola apoi, dupa ce toate filtrele au validat noua parola, pentru a notifica filtrele ca schimbarea s-a produs. Procesul este ilustrat in figura:

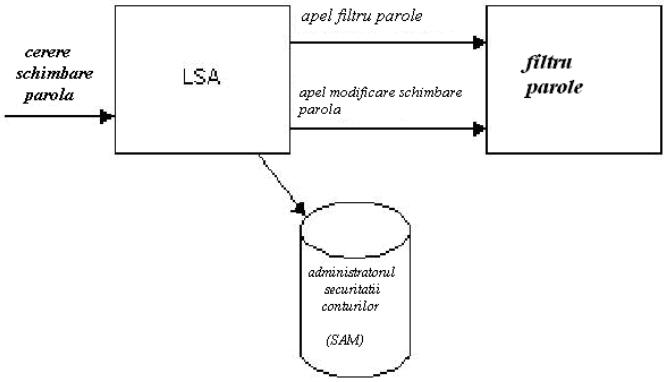

***Fig. 5** [7]*

Notificarea de schimbare a parolei este utilizata pentru sincronizarea schimbarii parolei cu conturile din baze de date externe. Pentru Windows NT 3.5 si versiuni anterioare acesteia, notificarea de schimbare a parolei nu este disponibila. Filtrele valideaza noua parola si indica daca aceasta respecta forma standard mentionata de polita.

Functiile din Safer API ofera oricarei aplicatii care lanseaza un program dintr-o sursa externa posibilitatea de a cere permisiunea inainte de a fi lansat in executie programul respectiv. Aceste functii pot fi apelate inaintea incarcarii sau rularii executabilului. Pentru Windows Me/95/98/2000/NT aceste functii din Safer API nu sunt disponibile.

2.2.5.3 Serviciul de securitate a atasamentelor – este un set de unelte al Consolei de Administrare Microsoft (MMC – Microsoft Management Console) care simplifica configurarea si analiza securitatii sistemului. Ttusi, unele servicii au specializat cerintele de configurare care depasesc setarile de securitate oferite in mod standard. Pentru manevrarea acestor cerinte se poate extinde funtionalitatea uneltelor prin scrierea unui atasament care se ocupa de taskuri specifice de securitate.

De exemplu, Spooler este un serviciu Windows NT care defineste obiecte private, care trebuie securizate, de exemplu imprimantele. Aceasta functionalitate nu este sub managementul setului standard de unelte si necesita un atasament care sa configureze si analizeze obiectele de tip imprimanta.

Cand un utilizator schimba configuratia existenta, snap-in –ul Securitatii Configuratiei stocheaza noua informatie si apoi transmite cererea catre Motorul Securitatii Configuratiei. Motorul proceseaza cererea si seteaza serviciile in noua configuratie. Daca cererea afecteaza o setare standard de securitate, este procesata de catre motor. Daca respectiva cerere are un specific de servicii, atunci motorul apeleaza motorul atasament potrivit operatiei respective:

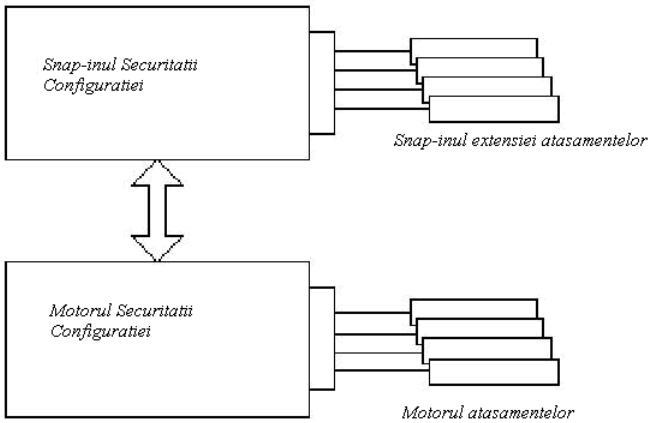

***Fig. 6** [8]*

2.2.6 Control parental la Windows Vista

Windows Vista ofera functii de control parental pentru monitorizarea si/sau limitarea accesului utilizatorilor la pericolele online si continuturi inadecvate. Tehnologia controlului parental la Windows Vista intentioneaza sa asiste parintii vigilenti pentru asigurarea acestora ca numai materialele aprobate pot sa parvina utilizatorilor acelui computer.

Utilizarea caluclatorului pentru activitati online sau offline deschide o noua lume pentru culegerea de informatii, dar totodata reprezinta un nou risc datorita hotiilor sau accesului facil la informatiilor cu continut explicit din cadrul site-urilor web, mesajelor, fisierelor download-abile, jocurilor sau fisierelor audio/video multimedia. Filtrele care pot fi setate de catre utiliator pot fi: blocarea pop-up-urilor, administrarea cookies-urilor, filtre anti-spam, administrarea listei de prieteni din mediul virtual si setari permise sau blocate pentru site-uri web.

Impunerea controlului parental este diferita de folosirea unor filtre setate de catre utilizator. Politele setate de catre parinte trebuie fortate sa functioneze independent si sa nu poata fi modificate decat din contul de administrator.

3. Apelurile de sistem legate de securitate la Linux

3 Generalitati

Securitatea in Linux este foarte importanta. Deoarece Linux este un sistem de operare destinat in primul rand retelelor, el este gandit sa functioneze prin acordarea de permisii fisierelor si directoarelor, si utilizatori cu drepturi restrictionate.

Cel mai puternic utilizator este root-ul, avand drepturi depline asupra sistemului.

Cele mai importante reguli de securitate:

- Se recomanda sa se utilizeze o parola de minim 8 caractere, compusa din litere, cifre, si

care sa nu reprezinte un cuvant, o data de nastere sau un nume. Pentru protejarea parolei de root se mai folosesc sistemele de securizare shadow si MD5. MD5 este un algoritm complex de incriptare a parolei. Shadow este un sistem prin care parolele retinute in fisierul /etc/passwd sunt transferate intr-un fisier numit /etc/shadow;

- Sa nu se instaleze programe care nu sunt necesare;

- Creearea unui utilizator obisnuit pentru folosirea sistemului. Acesta se logheaza pe root doar atunci

cand este absolut necesar;

- Folosirea ultimei versiuni a programelor;
- Pentru un sistem stabil, ar trebui sa se foloseasca versiunea stabila de kernel (cea care contine a 2-a

cifra para, ex 2.2.x, 2.4.x). Este bine ca ultimul kernel sa fie stabil si sa se foloseasca toate patch-urile;

- Creearea partitilor: ar trebui sa se creeze partitii pentru fiecare din directoarele /home, /var/cache,

/usr/local, /boot si /tmp;

- Se vor folosi programe de control la distanta doar in caz de necesitate.

3.1. Securitate prin parolare si criptare

Caracteristica cea mai importanta a securitatii este parolarea. Cele mai multe din distributiile Linux de azi, includ programe `passwd care nu vor lasa utilizatorul sa seteze o parola usor de ghicit. Exista mai multe metode de criptare a datelor, cu ajutorul unor algoritmi numiti DES` (Data Encryption Standard-Standard de Codare a Datelor) pentru criptarea parolelor. Parola criptata este stocata in `/etc/passwd sau /etc/shadow. Cand se introduce parola, ea este codata din nou si comparata cu parolele din fisier. Daca se potrivesc, fiind aceeasi parola, utilizatorul primeste accesul. Cei mai multi algoritmi nu sunt reciproci, adica nu exista posibilitatea de a lua parola criptata din continutul /etc/passwd sau /etc/shadow.`
Atacurile brute ca "Crack" sau "John the Ripper" pot gasi foarte usor parola, daca ea este una aleatoare. Modulele PAM folosesc o altfel de codare pentru parole (MD5 sau altele). Se poate folosi Crack pentru a verifica periodic baza de date in care se pot gasi parole nesigure.

3.2. PGP si criptarea cheiei publice

Criptarea cheii publice, utilizata pentru PGP, foloseste o cheie pentru codare si una pentru decodare. Codarea obisnuita foloseste o singura cheie, pentru codare si decodare; aceasta cheie trebuie cunoscuta in ambele parti si transferata dintr-o parte in alta, in mod sigur.

Criptarea cheii publice foloseste doua chei separate: o cheie publica si o cheie privata, pentru a usura necesitatea sigurantei de transmitere a cheii criptate. Fiecare cheie publica este disponibila oricarei persoane pentru a realiza criptarea, si simultan, fiecare persoana detine o cheie privata pentru a decripta mesajele cu cheia publica corespunzatoare.

Linux suporta PGP (Pretty Good Privacy). Versiunile 2.6.2 si 5.0 sunt printre cele mai bune vesiuni. Versiuni PGP:

- PGP 2.3a:

Acesta este PGP clasic. Poate fi utilizat la probleme de incompatibilitate in timpul procesarii cheilor si mesajelor generate cu versiuni 2.6.x sau mai recente sau cand se utilizeaza chei mai

mari de 1280 biti. Versiunea PGP 2.3a nu este utilizata in afara granitelor Statelor Unite datorita unor restrictii.

- PGP 2.6ui:

Aceasta este o veriune neoficiala a versiunii PGP 2.3a ce corecteaza problemele de incompatibilitate mentionate mai sus.Aceasta nu e o versiune 2.6.x deoarece are la baza resurse ale versiunii 2.3a

- PGP 2.62ui:

Versiune ce are la baza resurse 2.6ui, este o modificare care incearca sa fie compatibila cu cele mai noi inovatii introduse in versiunile 2.6.x.

- MIT PGP 2.6.2:

Este ultima versiune oficiala a PGP. Mesajele sale pot fi citite si de versiuni anterioare versiunii 2.5 si utilizeaza libraria de codare RSAREF. Este ilegal transportul in afara Statelor Unite ale Americii, dar odata transportate, ele se pot utiliza gratis.

- PGP 2.6.3i:

Versiune ce se bazeaza pe resurse MIT PGP 2.6.2 care au fost modificate pentru utilizare internationala.Una din schimbarile introduse este stergerea librariei de codare RSAREF, mentionata mai sus. Utilizarea acestei versiuni in Statele Unite ale Americii este ilegala.

- PGP 5.0

PGP 5.0 (anterior cunoscuta ca PGP 3.0) este o versiune complet noua a PGP. Aceasta versiune adauga noi optiuni, inclusiv suport pentru alti algoritmi de criptare ca RSA si IDEA. Ea va include si o interfata GUI pentru a simplifica utilizarea ei.

3.3.1. SSL, S-HTTP si S/MIME

- *SSL:* - SSL, sau Secure Sockets Layer (Nivelul de Securitate al Socket-urilor), este o metoda de

criptare dezvoltata de Netscape pentru a asigura securitate in Internet. Aceasta suporta instalarea mai multor protocoale de criptare si asigura autentificare client-server. SSL opereaza la nivelul transport, creeaza un canal cu date criptate prin care se cripteaza mai multe tipuri de date.

- *S-HTTP:* - S-HTTP este un alt protocol care asigura servicii de securitate in Internet. A fost

proiectat pentru confidentialitate, autentificare, integritate si pentru siguranta maxima, prin suportul a unor chei de administrare multiple, si algoritmi de criptare prin negociere intre partile implicate in fiecare tranzactie. S-HTTP este limitat pentru un software specific ce il implementeaza si cripteaza fiecare mesaj individual.

- *S/MIME:* - S/MIME, sau Secure Multipurpose Internet Mail Extension, este o criptare standard

utilizata pentru criptari electronice de mail si pentru alte tipuri de mesaje din Internet. Este un standard dezvoltat de RSA.

3.3.2 Impelmentari Linux IPSEC

IPSEC este o alta implementare pentru Linux, fiind este creeat de IETF in vederea unei comunicari criptate, sigura la nivelul retelei IP si pentru asigurarea autentificarii, integritatii, controlului de acces si confidentialitatii.

Universitatea Arizona dezvolta implementarea x-kernel Linux, folosind un obiect bazat pe o schema pentru implementarea retelei de protocoale, numita x-kernel.Altfel spus, x-kernel este o metoda de trecere a mesajelor la nivelul nucleu (kernel), ce face implementarea mai usoara.

O alta implementare IPSEC este Linux FreeS/WAN IPSEC. Afirmatia de pe site-ul lor: "Aceste servicii construiesc tunele sigure prin retele nesigure. Orice trece printr-o retea nesigura este criptat de poarta masinii IPSEC si decriptata de alta poarta la celalalt capat. Rezultatul este o retea virtuala privata, VPN. Aceasta este o retea care este efectiv privata desi include masini pe diferite site-uri, conectate de Internetul nesigur."

3.3.3 SSH (Secure Shell) si `stelnet`

Programele *`ssh`* and *`stelnet`* lasa utilizatorul sa acceseze sisteme aflate la distanta si care au conexiuni criptate.
`openssh` este un set de programe folosite pentru o inlocuire sigura pentru *`rlogin`*, *`rsh`* si *`rcp`*. Acesta foloseste cheia publica pentru a cripta comunicatia intre doi utilizatori, dar si pentru a-i autentifica. Poate fi folosita pentru a accesa un alt calculator aflat la distanta sau pentru a copia datele intre doua calculatoare, prevenind atacurile “omul la mijloc”(sesiunea hijacking) si atacurile DNS. Acesta va realiza o compresie de date pe conexiuni si o comunicatie sigura X11 intre cele doua calculatoare.
SSLeay este o implementare gratis a protocolului Netscape's Secure Sockets Layer. Acesta include numeroase aplicatii, ca telnet securizat, un modul pentru Apache, baze de date, si diferiti algoritmi ce includ DES, IDEA si Blowfish.
Folosind aceasta biblioteca, s-a creeat o inlocuire sigura *telnet*, care face criptarea peste conexiunea telnet.Opus lui SSH, *stelnet* foloseste SSL, protocolul Secure Sockets Layer dezvoltat de Netscape.
SRP este o alta implementare securizata telnet/ftp.

3.3.4 PAM - Pluggable Authentication Modules

Versiunile cele mai noi de Linux: Red Hat Linux si distributiile Debian Linux se combina cu o schema de autentificare unificata, numita PAM. PAM da posibilitatea de a schimba metodele cerintele de autentificare si incapsuleaza toate autentificarile locale, fara sa le mai recompileze
Cu PAM putem realize urmatoarele:
- alta criptare decat DES pentru parole;
- se fixeaza limite de resurse pentru toti utilizatorii, astfel incat ei sa nu poata realizeze atacuri (numarul proceselor, marimea memoriei, etc);
- permite parolele cu umbra;
- accesul in anumite momente, a anumitor utilizatori, din anumite locuri.

La numai cateva ore de la instalare si configurare, se pot preveni foarte multe atacuri inainte ca ele sa aibe loc. De exemplu, se utilizeaza PAM pentru a dezinstala folosirea sistemelor mari, fisierele *`.rhosts`* `din directoarele` *home*, adaugand urmatoarele linii la */etc/pam.d/rlogin:*

```
#
# Disable rsh/rlogin/rexec for users
#
login auth required pam_rhosts_auth.so no_rhosts
```

3.3.5 Incapsularea criptografica IP (CIPE)

Scopul principal al acestui software este sa asigure o facilitate pentru securitatea (impotriva traficului, si a mesajelor false) subretelelor interconectate peste o retea nesigura, cum ar fi Internetul.
CIPE cripteaza datele de la nivelul retea. Pachetele care circula intre calculatoare, pe retea, sunt de asemenea criptate. Masina care realizeaza cripatrea se afla plasata langa driver-ul care trimite si primeste pachetele.
Aceasta este opus lui SSH, care cripteaza data de conexiune, la nivelul socket. O conexiune logica intre programele care ruleaza pe diferite calculatoare este deasemenea criptata.
CIPE poate fi folosita in tunele, pentru a creea retele virtuale private, Virtual Private Network, VPN. Nivelul cel mai de jos al criptarii are avantajul ca poate fi facut sa lucreze transparent intre doua retele conectate in VPN, fara sa schimbe ceva in aplicatia software. CIPE foloseste metode in care multe lucruri pot fi parametrizate (ca de exemplu alegerea algoritmului de criptare actual utilizat) si sunt o alegere fixa de instalare.Acest lucru limiteaza flexibilitatea, dar permite o implementare simpla.

3.3.6 Kerberos

Sistemul de autentificare este dezvoltat Kerberos de Athena Project la MIT. Cand un utilizator se conecteaza, Kerberos autentifica acel utilizator (cu ajutorul unei parole) si asigura utilizatorul ca isi poate dovedi identitatea catre alte servere si calculatoare aflate in jurul retelei.
Aceasta autentificare este apoi folosita de programe ca *rlogin* pentru a lasa utilizatorul sa acceseze alt calculator fara o parola. Aceasta metoda de autentificare poate fi folosita de sistemul de mail pentru a garanta ca mail-ul este livrat corect si pentru a garanta ca cel care trimite este cel care trebuie sa fie.

Kerberos si celelalte programe care vin cu el, previn utilizatorii de a insela sistemul dandu-se drept altcineva. Din pacate, instalarea Kerberos inseamna modificarea sau inlocuirea a numeroase programe standard.

3.3.7 Shadow Passwords

Shadow passwords inseamna mentinerea informatiei parolei criptate, secret, de alti utilizatori. Versiuni recente ale Red Hat si Debian Linux folosesc shadow passwords, dar pe alte sisteme, parolele criptate sunt stocate in fisierele */etc/passwd* doar pentru citire, ele neputand fi modificabile.

3.3.8 "Crack" and "John the Ripper"

Daca pentru vreun motiv, programul *passwd* nu forteaza ghicirea parolelor, se poate rula un program *password-cracking* pentru a se asigura ca toti utilizatorii de parole sunt in siguranta.
Programele *password cracking* lucreaza pe baza unei idei simple: se incearca fiecare cuvant in dictionar si apoi variante ale acelor cuvinte, criptate fiecare si verificate cu parola criptata. Daca se potrivesc, atunci se stie care este parola
Programele “Crack” si “John the Ripper” utilizeaza mult CPU, dar se poate vedea daca un atacator intra si le ruleaza si il instiinteaza pe utilizator ca parola este gresita.

3.4 Utilizatorul, Sistemul, si Procesul de administrare

Toate sistemele Linux suporta procese de sistem mari, utilizator si sistem de administrare.
Administratorul de securitate ar trebui sa aiba in vedere urmatoarele:

- Conectare
- Informatii de autorizare
- Informatii de autentificare
- Comenzile utilizatorilor pentru rulare
- Restartarea si inchiderea sistemului
- Inregistrari de trenzactie ale retelei

3.4.1 Utilizarea Syslog

Programul sistemului numit *syslog* este folosit pentru evenimentele de acces ca: mesaje kernel, mesaje login, logout, mesaje generale de sistem, etc.

Se poate vedea unde se acceseaza distributia, prin accesarea fisierului */etc/syslog.conf*. Acest fisier */usr/sbin/syslogd* precizeaza locul in care se acceseaza diferitele mesaje.

Fisierele de acces sunt modificate de intrus pentru a-si acopri urmele, dare le ar trebui verificate pentru intamplari caudate. Se poate observa ca intrusul incearca sa castige intrarea sau sa exploateze un program, pentru a obtine un cont in radacina (root). Intrarile de acces ar trebui observate inainte ca intrusul sa le observe si sa le modifice.

Facilitatea "authpriv" ar trebui separata de alte date de acces, incluzand incercarea de a comuta utilizatorii, folosind `/bin/su`,incercarile de acces si alte informatii.

Stocarea datelor de acces securizat

Datele de acces sunt stocate intr-un loc sigur, un server dedicat, din interiorul retelei protejate. Odata ce masina a fost compromisa, datele de acces devin nefolositoare, pentru ca au fost modificate de intrus. Este asemanator unui caz criminalistic.Aceasta ajuta daca data de acces a fost stocata la distanta, indica momentul cand radacina a fost castigata , asa incat acele accese inainte de acest punct, au fost bune.

syslogd poate fi configurat astfel incat sa trimita automat date de acces catre server-ul central *syslogd*, dar acestea se trimit in forma de text, lasand intrusul sa poata vedea datele asa cum sunt transferate. Intrusul poate dezvalui informatii despre retea care nu sunt destinate publicului. De aceea, exista *syslog*, pentru a cripta datele odata ce sunt trimise. s*yslog* accepta si intrari de retea care pretind ca sunt locale, dar care nu indica originea adevarata.

Daca este posibil, configurati *syslogd* pentru a trimite o copie a celei mai importante date, pentru a securiza sistemul. Acesta va preveni intrusul, acoperindu-i urmele si stergandu-i accesul, *su, ftp, etc.*

3.4.2. Folosirea utilizatorului de administrare

Utilizatorul de administrare poate fi folosit pentru gasirea de informatii, despre cine foloseste sistemul la un moment de timp. Integritatea acestei informatii nu poate fi verificata integral, odata ce calculatorul a fost exploatat. Ea poate fi utila doar pentru a depista un anumit utilizator care a accesat sistemul, ora la care a accesat, cand sistemul a fost rebooted, etc.

Exista posibilitati de a procesa aceasta informatie, cu ajutorul: *last*(1), *who*(1), *ac*(1), *utmpdump*(1).

De exemplu, folosind comanda */usr/bin/last* se vor afisa informatii despre sistem:

```
root     tty1                      Fri Jul  3 21:02   inca are acces
reboot   system boot               Fri Jul  3 21:01
dave     ttyp2        localhost    Wed Jul  1 23:11 - 23:11  (00:00)
```

david ttyp2 localhost Wed Jul 1 22:47 - 22:47 (00:00)
Comanda *last*(1) care afiseaza o lista a ultimilor utilizatori care acceseaza sistemul, si comanda *lastb*(1), care listeaza utilizatorii care au avut accesul esuat, (desi exista */var/log/btmp*),ambele consulta fisierul */var/log/wtmp*,care contine urmatoarele informatii :

- Tipul accesului
- ID-ul procesului de acces
- Numele echipamentului tty
- ID-ul initial sau ttyname prescurtat
- Numele utilizatorului
- Numele calculatorului pentru accesul la distanta
- Starea de iesire a procesului
- Ora la care a avut loc intrarea
- Adresa IP a calculatorului aflat la distanta

Fisierul */var/run/utmp* este consultat pentru a afla cine este in sistem (cu comanda *who*(1)). Totusi, pot exista mai multi utilizatori care folosesc simultan sistemul, pentru ca nu toate programele folosesc accesul *utmp*. Acest fisier este in general redus dupa boot-area fiecarui sistem, de unul din fisierele*:/etc/rc.d/rc.**. Trebuie avut in vedere daca acest fisier sa fie sau nu scris decat de utilizatorii din radacina.

3.4.3. Utilizarea procesului de administrare

Acest pachet include mai multe programe de administrare a functiilor la nivelul kernel, incluzand:

- accton (8) – Sfarsitul procesului de administrare
- accttrim (8) – A reduce marimea fisierului de administrare
- lastcomm (1) – Afisarea ultimelor comenzi, executate in ordine inversa

3.4.4. Administrarea utilizatorilor

Avand control asupra resurselor si datelor la care utilizatorii au acces, este o parte esentiala de mentinere a securitatii. Linux asigura permisiuni de acces, parole, adaugare si stergere de utilizatori, etc.
Cateva exemple de programe pentru administrarea utilizatorilor si a grupurilor:

- chage (1) – schimba parola utilizatorului la data expirarii
- groups (1) – Scrie grupurile in care se afla un utilizator
- newusers (8) – Aduce la zi si creeaza utilizatori noi
- passwd (1) – Aduce la zi jetonul de autentificare a utilizatorului
- nologin (5) – Previne conectarea la sistem a utilizatorilor care nu sunt in radacina
- su (1) – Ruleaza o carcasa cu un utilizator inlocuitor si un ID grup
- useradd (8) – Creeaza un nou utilizator sau aduce la zi infomatii despre noul utilizator
- userdel (8) – Sterge un cont al utilizatorului si fisierele aflate in legatura cu acestea
- usermod (8) – Modifica contul unui utilizator
- chgrp (1) – Schimba dreptul de propietate al grupului de fisiere
- chown (1) – Schimba dreptul de propietate al utilizatrorului si al grupului de fisiere
- gpasswd (1) – Administreaza fisierul /etc/group
- groupadd (8) – Creeza un nou grup
- groupdel (8) – Sterge un grup
- groupmod (8) – Modifica un grup

- groups (1) – Listeaza grupurile in care se afla un utilizator
- grpck (8) – Verifica integritatea unor grupuri defisiere verify integrity of group files
- pwconv (8) – Converteste in si din shadow passwords
- pwunconv (8) - Converteste in si din shadow passwords
- grpconv (8) - Converteste in si din shadow passwords
- grpunconv (8)- Converteste in si din shadow passwords
- vipw (8) – Scrie parole sau fisiere grup
- vigr (8) - Scrie parole sau fisiere grup

Implementarea securitatii la Linux si Windows

4 Generalitati

Pentru inceput cred ca ar fi util sa dzvoltam conceptul de securitate in general. Acesta poate imbraca diverse forme in functie de unghiul sub care il privim si cum este interpretat. Sunt o multitudine de factori ce influenteaza aceste lucruri printre care cei mai importanti ar fi:
-tipul de activitate emergent securitatii impuse
-tipul de informatii cu care se lucreaza
-filozofia manageriala ce guverneaza activitatile

4.1 Polita de utilizare

[1] Unul din primele lucruri care trebuiesc clarificate inca de la inceput ar fi polita de utilizarea acceptata(acceptable use policy -AUP), prin care sa se specifice obiectivele de securitate tintite(interzicerea accesului la anumite adrese de internet, conturi de utilizator cu diferite grade de prioritati, gradul de acces la reteaua interna, dreptul de instalare/dezinstalare de produse software etc).

O polita de securitate ar trebui sa se concentreze asupra urmatoarelor aspecte :

-accesul fizic la echipamente si la componente

-conturile de utilizatori(parole, username, nivel de autorizare)

-securitatea sistemului de fisiere(permisiuni la nivel de proprietar, utilizator, grup etc)

-protectia fata de virusi

-accesul la distanta

-copii de rezerva ale datelor

-plan de recuperare in eventualitatea unor dezastre

-audit

(O parte a acestor elemente le vom dezbate ulterior la nivel tehnic Windows-Linux)

4.2 Securitate raportata la retea.

Avand in vedere cresterea exponentiala de care se bucura serviciile online si nevoia de comunicare tot mai acerba o foarte mare atentie ar trebui data amenintarilor ce vin din "din retea"(atat interna cat si externa). Toate sistemele de operare ofera suport pentru stiva de protocoale TCP/IP (pe care se bazeaza si internetul) si acesta este un prim punct de pornire in

a gasi vulnerabilitati in aceste sisteme de operare ce pot fi ulterior exploatate.

4.2.1 Servicii vulnerabile

[2] Din aceasta perspectiva o subsidiara FBI (National Infrastructure Protection Center -NIPC) impreuna cu SANS Institute au publicat o lista cu cele mai vulnerabile 10 servicii in lumea LINUX/UNIX care cuprinde:

- BIND Domain Name System
- Remote Procedure Calls (RPC)
- Apache Web Server
- General UNIX Authentication Accounts with No Passwords or Weak Passwords
- Clear Text Services
- Sendmail
- Simple Network Management Protocol (SNMP)
- Secure Shell (SSH)
- Misconfiguration of Enterprise Services NIS/NFS
- Open Secure Sockets Layer (SSL)

4.2.2 Posibile tipuri de atac

In lumea reala exista o multitudine de forme prin care se poate ataca o masina din exterior, prin "retea". Cele mai importante ar fi Denial of service(DoS) constau in atacarea sistemului tinta cu o abundenta de cereri ilegitime, astfel incat sa nu mai poata raspunde cererilor legitime. Asfel de exemple ar fi:

-"ping of death": trimiterea de echo request ICMP de dimensiuni foarte mari care ar fi blocat unele sisteme.

- "land": alterarea IP-ului a sursei asflel incat sa fie identic cu cel al destinatiei pentru pachetele SYN request sistemele atacate blocandu-se in incercare de a deschide o conexiune cu ele insesi. Si s-au raportat atacuri in deosebi la sistemele de operare: Windows 95/NT, BSD Unix si Solaris, dar care ulterior si-au imbunatit codul oferind protectie la astfel de atacuri.

-Tear drop: profita de facilitatea de segmentare a packetelor IP, astfel incat trimite informatii eronate facand imposibila reasamblarea la destintie ducand intr-un final la blocarea sistemului. Atacuri s-au inregistrat la sistemele Windows 95/NT/2000 si la unele distributii de Linux.

-Smurf: lanseaza un volum mare de ping requests si altereaza campuri din header-ul IP inlocuind adresa IP sursa cu adresa IP a statie pe care doreste sa o atace, astfel toate replay-urile vor fi trimise spre statia atacata, congestionand-o.

[3]Pe langa DoS alte amenintari mai poti fi:

-Spoofing: A introduce ilegal date intr-un fisier sau un pipe

-Tampering: a impedica anumite parti ale unei tranzactii de a se realiza

-Repudiation: a impedica auditul prin blocarea accesului la log-uri

-Information Disclosure: "ascultarea" de informatii pe socheturi sau pipes.

-Elevation of privilege: executarea de cod arbitrar

4.3 Securitate sub Windows

[4] In viziunea windows ierarhizarea resurselor de sistem impreuna cu elementele care joaca un rol important in asigurarea securitatii pe nivelul respectiv este:

-Nivelul Retea: criptografie, filtrare+firewall

-Nivelul Date: configurarea protectiei datelor

-Nivelul Aplicatie: protectia memoriei

- Nivelul Platforma: fisiere, socketuri, pipes, liste de control al accesului(ACL)

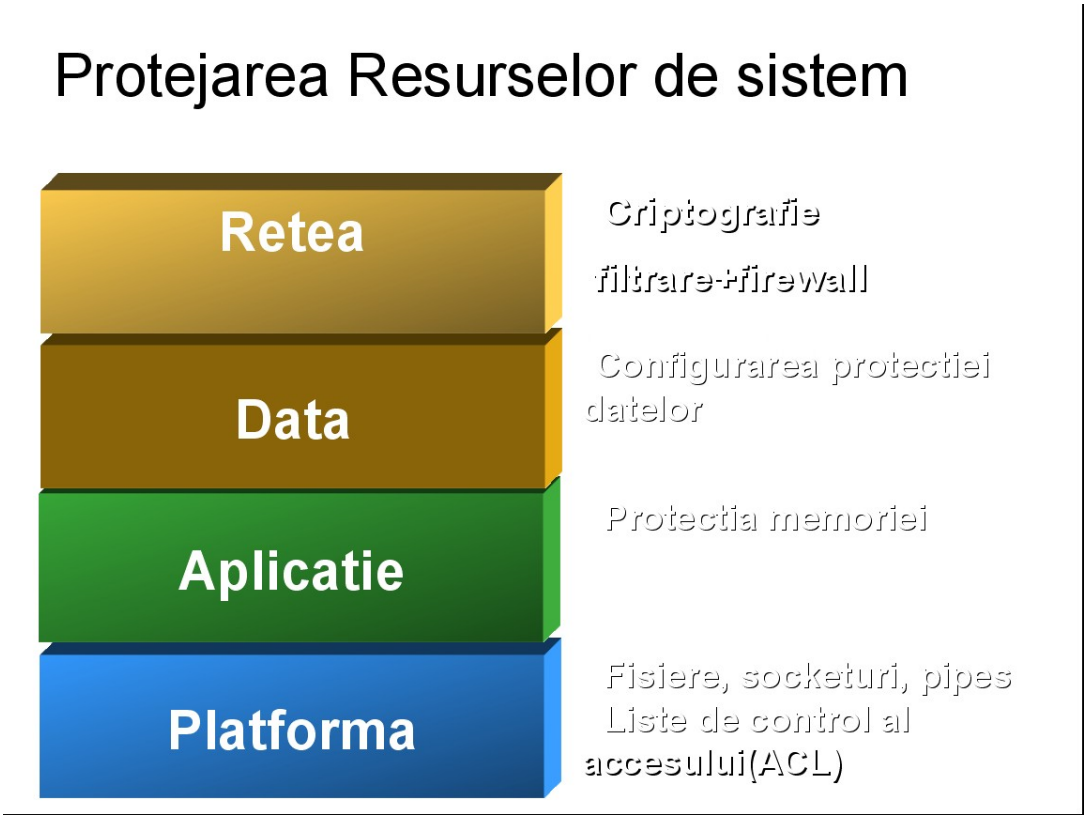

FIG 4.3[4]

[5] Pentru o abordare mai tehnica a problemei vom incerca sa analizam putin mai aprofundat modul si mijloacele prin care sistemul de operare Windows implemeneaza securitatea. In acest sens vom enumera si analiza componentele centrale si bazele de data care participa la acest concept:

>Monitorul rederential de securitate(**Security reference monitor (SRM)**)
\Windows\System32\Ntoskrnl.exe : responsabil cu definirea structurii de date a jetonului de acces

realizand verificarea accesului pe obiecte, manipuleaza privilegii, generand mesaje de audit de securitate.
>Subsistem autoriatar de securitate local: **Local security authority subsystem (Lsass)** \Windows\System32\Lsass.exe : este responsabil pentru polita de securitate locala, autentificarea userilor, si de a trimite mesaje de audit de securitate Event log-ului.

>Baza de date a politei LSASS : **Lsass policy database** se gaseste in registrii sub HKLM/SECURITY si include informatii precum: cine are permisiune sa acceseze sistemul si "cum", cine are anumite privilegii, si ce tip de audit de securitate se va face.

>Servicul manger al conturilor: **Security Accounts Manager (SAM) service :** un set de subrutine responsabiule cu managementul bazei de date care contine numele utilizatorilor si grupurilor definite pe sistemul local. Ruleaza in procesul Lsass si este implementat sub: \Windows\System32\Samsrv.dll.

>Baza de data SAM: memorata in registri sub:HKLM\SAM: o baza de data care pe sistemele ce nu functioneaza ca controlari de domeniu contine definitii ale utilizatorilor si grupurilor locale impreuna cu parolele si restul atributelor. Pe sistemele ce functioneaza in categoria mai sus mentionata SAM memoreaza contul de recuperare al administratorului si parolele.

>Directorul activ: **Active Directory :** implementat in \Windows\System32\Ntdsa.dll si ruleaza in procesul Lsass : o baza de date ce contine informatii despre obiectele din interiorul unui domeniu cum ar fi utilizatori, grupuri sau chiar statii. Parole si informatii despre privilegii sunt memorate in directorul activ si raspandite catre acele statii dintr-un domeniu care au fost desemnate drept cotrolere ale domeniului.

>Pachetele de autentificare: include librariile de legaturi dinamice (DLL-urile) si implementeaza politica de autentificare specifica windows Un DLL de autentificare este responsabil de a verifica daca un anumit nume de utilizator si parola corespund si daca da, sa returneze Lsass-ului informatii de securitate despre utilizator generad pe baza acestora un jeton.

>Procesul de logare : **Logon process (Winlogon)** \Windows\System32\

Winlogon.exe : Responsabil de a raspunde lui SAS si de a conduce sesiuni de logare intereactive.

>Autentificare si identificare gragica: **Graphical Identification and Authentication (GINA)** \Windows\System32\Msgina.dll : Un DLL ce ruleaza in porcesul Winlogon si care este folosit de acesta pentru a obtine informatii despre numele utilizatorului si parola.

>Serviciul de logare in retea **Network logon service (Netlogon)** (\Windows\System32\

Netlogon.dll : seteaza un canal sigur catre un controller dedomeniu prin care se trimit cereri sigure(logare interactive sau autentificarea validarii prin LAN Manager))

>Driverul de device de securitate din kernel: **Kernel Security Device Driver (KsecDD)** \Windows\System32\Drivers\Ksecdd.sys

o librarie de kernel cu funtii care implementeaza interfetele procedurilor de apelare locale (LPC) si alte module de securitate din kernel (Encrypting File System (EFS)) utilizate pentru a comunica cu LSASS in modul utilizator

4.4 Securitate sub Unix/Linux

[6] In ceea ce priveste echipamentele cu sisteme de operare Linux(unix like) componentele principale prin intermediul carora putem opera la nivel de securitate sunt:

-conturi de utilizatori+parole

-permisiunile sistemului de fisiere

-controlul accesului la distanta

-software-ul pentru verificarea securitatii

4.4.1 Conturi de utilizatori+parole

Oricine care doreste sa acceseze orice fel de resursa pe un sistem Unix trebuie sa detina un cont de acces. In lumea unix-like exista 2 tipuri de conturi: ***root(superuser)*** in realitate administratorul si conturi de utilizatori.

Root-ul este cel care exista de la incpu intr-un sistem linux si care area acces la toate fisierele/directoarele din sistem.Este similar cu **contul de Administrator** in windows NT/2000 sau **contul de admin** in Novell NetWare. Acesta poate crea noi utilizatori, managiui sistemul de fisiere, instala software si executa task-uri administrative de nivel inalt.

Fiecare cont este identificat printr-un login id si parola: Login id tre sa fie unic in sistem si tre sa aiba maxim 32 de caractere, iar parola trebuie sa aibe cel putin 6 caractere.Aceste informatii sunt referite in principal de 2 fisiere: **/etc/shadow** si **/etc/passwd**.

/etc/passwd: contine informatii pentru identificarea utilizatorului. Este consultat de fiecare data cand cineva incearca sa acceseze sistemul. contine ingrgistrari formate din 7 capmuri pentru fiecare utilizator reprezentand: username, indicator pentru parola(determina cautarea in **/etc/shadow**), UID, GID, alte informatii pentru verificare utilizatorului, calea absoluta catre directorul rezident al utilizatorului, shell-ul utilizatorului cu rol de interpretor de comenizi.

/etc/shadow : contine parolele criptate astfel incat sa nu fie posibila citirea lor in text clar, si daca un utilizator "uita" parola aceasta nemaiputnad fi recuperata ci doar schimbata de catre root.

4.4.2 Permisiunile sistemului de fisiere sub Linux:

Din punctul de vedere al sistemelor de fisiere Unix-like sunt definite 3 tipuri de utilizari:

-propritari: cei care au creaz fisierul/directorul

-grup: cei care fac parte din grupurile in care este membru si proprietarul

-restul: ceilalti utilizatori care nu intra in primele 2 categorii

Permisiunile asociate cu acesti utilizatori sunt:

-citire: fisierele poate fi afisat sau copiat

directoarele pot fi listate

-scriere: continmutul fisierelor poate fi modificat

directoare: fisierele din interior pot fi adaugate sau sterse

-executie:fisiere pot fi executate

directoare: pot fi explorate prin intermediul comenzii "find".

-nici o permisiune: interzice permisiunea.

De asemenea la crearea unui fisier sau director exista un set de permisiuni default: pentru un fisier(creat cu comanda **touch**) permisiunile vor fi de citire/scriere pentru proprietar respenctiv si de citire pentru grup si restul utilizatorilor. Pentru crearea unui director (cu comanda **mkdir**-similar **dos**) setul de permisiuni default va fi: citire/scriere/executie pentru proprietar , respectiv citire/executie pentru grup si resutul utilizatorilor. In cazul in care se doreste schimbarea acestor permisiuni default comanda folosita este **chmod** cu urmatoarea sintaxa:

chmod mode numefisier , unde mode este alcatuit din trei campuri:

*who :cui i se aplica comnada(proprietar, grup, restul sau toti)

*op: operatorul care va fi folosit(=,+,-)

*permisiuni: citire, scriere, executie.(aplicate in modul octal sau simbolic)

Alte comenzi utile ar fi schimbarea proprietarului sau a grupului de care apartine un fisier/director. Proprietarul se modifica cu **chown** (in linux poate fi executat doar de root iar in solaris atat de root ca si de proprietarul curent al dierului/directorului) iar grupul cu comanda **chgrp** (in linux poate fi executat doar de root iar in solaris atat de root ca si de proprietarul curent al dierului/directorului).

Un alt set de comezi ce ar fi utile in implementarea securitatii ar fi:

#**who:** afiseaza toti utilizatorii care sunt logati la momentul curent in sistem(nume, terminal, momentul logarii, numele masinii gazda)

#**finger:** afiseaza aceleasi informatii ca si who dar mai detaliate si poate primi ca parametru un utilizator pentru a extinde informatiile despre cel in cauza.

#**who i am:** afiseaza RUID(real user id)

#**id:** afiseaza EUID(effective user id)

#**su:** primeste ca parametru numele utilizatorui cu care se doreste logarea

4.4.3 Criptare si firewall

[7] Adesea conceptul de firewall este inteles gresit fiind asociat cu un produs software de cele mai multe ori, dar el se poate prezenta si sub forma hardware. Principalul sau rol este acela de a impedica pachetele IP “rau intentionate” sa treaca de el. Multe sisteme de operare au incorporate astfel de firewall-uri(de exemplu Windows XP care in schimb datorita interfetei grafice limiteaza flexibilitatea utilizatorului in a personalizarea functiilor). In Linux datorita posibilitatii de a lucra in CLI flexibilitatea este mult mai mare(ex:comanda **iptables**)

Cea mai des intalnita forma de firewall este sub forma de filtre de pachete. Acestea sunt denumite adesea liste de control al accesului (ACL). Un ACL incepe prin definirea unui set de regului ce pot face parte din mai multe criterii: IP sursa/destinatie, portul TCP/UDP sursa/destinatie, protocolul de nivel 7 in stiva OSI(HTTP, FTP etc).

Servicii de tip proxy: sistemul ce ruleaza acest tip de servicii primeste cereri de la clienti si le rezolva in locul acestora, protejandu-i asfel de contactul direct cu exteriorul retelei. De exemplu Microsoft implementeaza acest tip de servicii cum ar fi Microsoft Proxy Server 2.0.

NAT(Network Address Translation): ruleaza de obicei pe un gateway si consta in modificarea pachetelor IP prin inlocuirea adresei IP sursa cu o adresa predefina din spaitul public. In interiorul retelei se poate aplica o schema de adresare privata.

Criptare: procesul de transformare a informatiei cu scopul ca ea sa nu poate fi inteleasa decat de catre destinatar. Algoritmii cu care se realizeaza criptarea sunt de 2 feluri: cu cheie simetrica(DES-vechi si vulnerabil, Blowfish, RC-245, 3DES, IDEA, AES) sau cu cheia asimetrica(RSA, EIGamal)

[8]OpenSSL este cea mai folosita biblioteca de functii criptografice in lumea Unix like.Aici este inclus is un utilitar in linia de comanda, ce permite accesul la functiile criptografice: **openssl comanda optiuni.** Unele din comenzile posibile sunt:

*dgst: algoritmi de digest

*enc: algoritmi simetrici

*genrsa: generare de chei RSA

*rsa: vizualizare/manipulare chei RSA

*dsaparam si dsa: generearea parametrilor/managementul cheilor DSA.

*dhparam:generarea parametrilor Diffie-Hellman

*passwd: generare de hash-uri de parole

4.4.4 software-ul pentru verificarea securitatii

Asmodeus: analizator de securitate in retea si un scaner de porturi pentru Windows si care este capabil chiar de a scana mai multe sisteme.

Satan(Security Administrator Tool for Analyzing Networks): analizor de securitate in retea pt UNIX similar cu Asmodeus dar depasit functional.

Saint(The Security Administrator`s Integrated Network Tool): o versiune imbunatatita a Satan.

Strobe(strobe-classb): folosit pentru scanarea de relee de mail deschise pentru retele de clasa B.

Ogre: scaner de vulnerabilitati in servicii pentru Windows NT. Foarte folositor pentru Netbios si Microsoft Internet Information Services (IIS).

Mscan: scaner pentru detectarea culnerabilitatilor in serviciile usuale din lumea Unix: DNS, NFS, Statd, X and finger.

Nmap: un puternic scaner de porturi pentru Unix care poate scana mai multe statii define prin adrese IP, domenii etc.

BackOffice: un server ce ruleaza in background “supervizand” conexiunile client ce administreaza sistemul de la distanta.(similar: Netbus, SubSeven)

Trinoo, Stacheldraht, tribe flood network (TFN), Mstream, Carko, Wormkit – unelte impotriva atacurilor DoS.

Bibliografie:

1.Saulea cristian:

[1]http://sektor.anl.ro/
[2]http://en.wikipedia.org/wiki/Security_Identifier
[3]http://support.microsoft.com/kb/243330
[4]http://support.microsoft.com/kb/163846
[5]http://en.wikipedia.org/wiki/Token_%28Windows_NT_architecture%29

2.Constantin Adina:

[1] http://upload.wikimedia.org/wikipedia/commons/5/5d/Windows_2000_architecture.svg
[2] http://en.wikipedia.org/wiki/Microsoft_Windows#Versions
[3] http://blogs.msdn.com/nickkramer/archive/2006/04/18/577962.aspx
[4] http://msdn2.microsoft.com/en-us/library/bb403233(VS.85).aspx
[5] http://msdn2.microsoft.com/en-us/library/bb403232(VS.85).aspx
[6] http://msdn2.microsoft.com/en-us/library/aa382003(VS.85).aspx
[7] http://msdn2.microsoft.com/en-us/library/ms721882(VS.85).aspx
[8] http://msdn2.microsoft.com/en-us/library/ms722456(VS.85).aspx

3.Caju Ana-Maria:

http://tldp.org/HOWTO/Security-HOWTO/password-security.html

4.Munteanu Daniel-Dumitru:

[1],[2]: Network Operating systems(IT Essentials II: Network Operating Systems v3.0/Modulul14 Security**) - Cisco curriculum**

[3]: Microsoft.TeachingObjects.ThreatModeling/ Threat Modeling
http://www.academicresourcecenter.net/curriculum/pfv.aspx?ID=6632

[4]: Microsoft.TeachingObjects.ResourceManagement/Resource Management
http://www.academicresourcecenter.net/curriculum/pfv.aspx?ID=6638

[5]: WindowsInternalsBook4thEdition-Chapter 8 Security. Security System Components(pg 488)

[6]: Unix/Linux Fundamental – Cisco curriculum

[7]: Curs Firewall+Criptografie (curs realizat de Ionut Morar)
[8]: http://en.wikipedia.org/wiki/Transport_Layer_Security