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

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.

http://sektor.anl.ro/

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.

http://en.wikipedia.org/wiki/Security_Identifier
http://support.microsoft.com/kb/243330
http://support.microsoft.com/kb/163846

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

http://en.wikipedia.org/wiki/Token_%28Windows_NT_architecture%29