# CONTROLUL ACCESULUI

## I.Matrice de control

Este un model de securitate de stare in sistemele de calculatoare care caracterizeaza drepturile fiecarui subiect cu drepturile fiecarui obiect din sistem.

Starea de protectie a unui sistem de calculatoare poate fi abstractizata ca un set de obiecte O care este un set ce trebuie protejat(ex:procese,fisiere,pagini de memorie)si un set de subiecti S care constituie toate entitatile active(ex:utilizatori, procese, etc).

De asemenea exista un set de drepturi R de forma r(s,o), unde s apartine lui S, o apartine lui O si r(s,o) inclus in R.

Un drept specifica un tip de access pe care un subiect are asupra unui obiect.

Datalii matrice de access:

Subiectii sunt priviti ca obiecte; starea sistemului este reprezentata printr-o matrice; liniile sunt etichetate cu subiecti, coloanele cu obiecte.

## II.Politica de confidentialitate Bell-LaPadulla.

BLP este un modul de stare folosit pentru a intari controlul de access in aplicatiile guvernamentale si militare.

Modelul BLP se axeaza pe confidentialitatea datelor si accesul controlat la informatiile clasificate.

In acest model, entitatie sunt impartite in subiecti si obiecte.

Notiunea de "stare securizata" este definita si este demonstrat ca fiecare stare de tranzitie prezerva securitatea prin saltul de la o stare securizata la alta, demonstrand prin inductie ca sistemul satisface nivelele de securitate din model.

BLP este construit pe un concept de "masina stare" cu un set de stari intr-un sistem.Tranzitia de la o stare

la alta este definita de functiile de tranzitie.

**Proprietatile BLP:**

1.Simple Security Propriety(Proprietatea de securitate simpla): Un subiect cu un anumit nivel de access X nu poate citi un obiect de securitate Y mai mare (Y>X => no read up)

2.Propiretatea "star":Un subiect cu un anumit nivel de securitate X nu are drepturi de scriere asupra unui obiect cu un nivel de securitate mai mic (Y<X => No write down)

3.Proprietatea discreta:utilizarea unei matrici de access pentru a specifica discret controlul de access.

## III.Politica de integritate Biba:

Este un sistem de tranzitie intre stari care descrie un set de reguli de control de acces modelate sa asigure intregritatea datelor.

Datele (obiectele(??)) si subiectii sunt grupati in mai multe nivele de integritate ordonate.

Modelul este conceput in asa fel incat subiectii sa nu corupa obiectele de nivel mai mare decat ei sau subiectii sa nu fie corupti de catre obiecte de nivel mai mic.

In acest model, uitilizatorii pot crea continut (write access) doar la nivelul lor de integritate sau mai jos.

De asemenea ei pot vedea (read access) elementele de la nivelul lor sau mai sus.

Modelul Biba defineste un set de reguli de securitate similar cu cel de la BLP. Aceste reguli sunt inversele

regurilor BLP.

1.Axioma intregritatii simple:Un subiect de un anumit nivel de integritate X nu trebuie sa citeasca un obiect de nivel de intregritate Y mai mic (no read down).

2.Axioma de integritate "star":Un subiect de un nivel de integritate X nu trebuie sa detina drepturi de scriere asupra unui obiect de integritate Y mai mare (no write up).

3.Proprietatea de invocare:Un proces cu nivel mic de securitate nu poate cere access unui obiect cu un nivel mai mare de securitate, doar subiectii cu un nivel egal sau mai mic pot face asta.

## IV.Politica Zidului Chinezesc (Brewer Nash model):

Este construit pentru a furniza o securitate a informatiei bazata pe controlul de access care se poate schimba dinamic. Este conceput pentru a furniza controale care atenueaza conflictele de interes in organizatiile comerciale si este construit pe un "flow de informatii".

In acest model, nici o informatie care poate crea un conflict de interese nu poate parcurge intre subiecti si obiecte .

# CRIPTOGRAFIE

### I.1 Criptosisteme simetrice(cu o singura cheie, si acea cheie este secreta):

Algoritmii cu cheie secreta sunt caracterizati de faptul ca folosesc aceeasi cheie atat in procesul de criptare cat si in procesul de decriptare. Din acest motiv acesti algoritmi mai sunt cunoscuti si sub numele de algoritmi simetrici.

Pentru aplicarea lor este necesar ca inaintea codificarii/decodificarii, atat emitatorul cat si receptorul sa posede deja cheia respectiva.

In mod evident, cheia ce caracterizeaza acesti algoritmi trebuie sa fie secreta.

Criptarea simetrica prezinta avantajul rapiditatii cu care sunt realizate procesele de criptare/decriptare a mesajelor.

Succesul sistemului se bazeaza pe dimensiunea cheii. Daca are mai mult de 128 de biti este una destul de sigura, deci sigura in exploatare.

Cele 3 caracteristici ale criptarii simetrice sunt:

-Siguranta

-Rapiditatea

-Volumul mare de date de criptare

Principalul dezavantaj ale algoritmilor simetrici consta in faptul ca impun un schimb de chei private inainte de a se incepe transmisia de date. Altfel spus, pentru a putea fi utilizati este necesar de un canal cu transmisie protejat pentru a putea fi transmise cheia/cheile(secreta(e)) de criptare/decriptare.

Exemple de criptosisteme simetrice:AES, DES si fratiorul lui, 3DES(not sure about DES&3DES)

## I.2 Criptosisteme asimetrice(cu 2 chei, una publica si una secreta):

Este un criptosistem care utilizeaza o pereche de chei:o cheie publica si o cheie privata(secreta).

Cum functioneaza:

Un utilizator care detine o astfel de pereche de chei, isi publica cheia publica astfel incat oricine poate sa o foloseasca pentru a ii transmite un mesaj criptat.

Numai detinatorul cheii secrete este cel care poate decripta mesajul astfel criptat.

Matematic, cele 2 chei sunt legate, insa cheia privata nu poate fi obtinuta din cheia publica.In caz contrar, oricine ar putea decripta mesajele destinate unui alt utilizator fiindca oricine are access la cheia publica a acestuia.

O analogie este folosirea unei cutii postale.Oricine poate pune in cutie un plic, dar la plic are access doar posesorul cheii de la acea cutie postala.

Criptografia asimetrica se mai numeste si criptografie cu chei publice.

Cele 2 mari ramuri ale criptografiei asimetrice sunt:

1.Criptarea cu cheie publica-un mesaj criptat cu o cheie publica nu poate fi decodificat decat folosind

cheia privata corespunzatoare.Metoda este folosita pentru a asigura confidentialitatea.

2.Semnaturi digitale-un mesaj semnat cu cheia privata a emitatorului poate fi verificat de catre oricine

prin access la cheia publica corespunzatoare, astfel asigurandu-se autenticitatea mesajului.

## I.2.1Diferentele dintre criptosistemul simetric si cel asimetric:

Sistemele de criptare cu chei simetrice folosesc o singura cheie atat pentru criptare cat si pentru decriptare.

Pentru a putea folosi aceasta metoda atat receptorul cat si emitatorul ar trebui sa cunoasca cheia secreta.

Aceasta trebuie sa fie unica pentru o pereche de utilizatori, fapt care conduce la probleme din cauza

gestionarii unui numar foarte mare de chei. Sistemele de criptare asimetrica inlatura acest neajuns.

De asemenea se elimina necesitatea punerii de acord(emitator+receptor) asupra unei chei secrete comune, greu de transmis in conditii de securitate sporita intre cei 2 interlocutori.

## I.3 Criptare inlantuita

Mesajul circula prin mai multe noduri intre expeditor si destinatar.Un nod intermediar primeste mesajul,

il decripteaza cu aceeasi cheie care a fost criptata si il recripteaza cu o alta cheie si apoi il trimite

la urmatorul nod unde procesul se repeta cu noua cheie pana ce mesajul ajunge la destinatar.

## II.Functii Hash

Este considerata o functie practic imposibil de inversat(adica este imposibil de a recrea datele de input

folosind DOAR valoarea ei hash). Aceste functii "one-way" sunt denumite "the workhorses of modern criptography".

O functie hash ideala are patru componente principale:

-Este usor de creat o valoare hash pentru orice mesaj.

-Este imposibil(irealizabil in practica[infeasible{look it up on the internet}]) sa generam un mesaj caruia

ii cunoastem doar functia lui hash.

-Este imposibil(irealizabil in practica[infeasible{look it up on the internet}]) sa modificam mesajul fara sa

ii schimbam hash-ul.

-Este imposibil(irealizabil in practica[infeasible{look it up on the internet}]) sa gasim doua mesaje diferite

cu acelasi hash.

## III. MAC(Message authentication code)

Este o informatie folosita pentru autentificarea unui mesaj.MAC-urile sunt generate folosind o cheie simetrica determinista numita MAC functions.

## III.1 Nested MAC

Este o functie hash cu 2 chei.

Pasii generarii Nested MAC-ului:

Pas 1:Mesajul este compresat folosind o functie hash(H) in cascada folosind cheia K2

Pas 2:Se preia outputul de la pasul 1 si se foloseste drept input pentru o functie de compresie(h) impreuna cu cheia K1

## III.2 Hash MAC

Details here,sry it's too fucked up with formulas so i can't explain it too well:

http://en.wikipedia.org/wiki/Hash-based_message_authentication_code

O posibila explicatie:Mesajul creat la NMAC se mai cripteaza o data cu o functie Hash pentru a obtine un

HASH MAC.

HMAC este sigura doar daca NMAC este sigura.

# PROTOCOALE DE SECURITATE

## I.IPSec

Internet protocol security este o suita de protocoale pentru securizarea comunicatiilor peste stiva TCP/IP.

Aceasta suita se bazeaa pe folosirea functiilor matematice si a algoritmilor de criptare si autentificare pentru a asigura confidentialitatea, integralitatea si non-reproducerea informatiilor din fiecare pachet IP transmis pe retea.

IPsec este la ora actuala una dintre cele mai folosite metode de transmisie securizata a datelor pe internet.

IPsec se afla pe nivelul 3 a stivei TCP/IP si la nivelul 3 a stivei ISO-OSI ceea ce face posibila securizarea

tuturor datelor care folosesc stiva TCP/IP.

IPsec are o arhitectura de tip end-to-end, compatibila atat cu stiva IPv4 cat si cu IPv6, unde integrarea

functiilor de securizare este nativa, inca de la proiectarea stivei pe 128 de octeti.

[Detailed crap]Modelul IPsec este descris in mod oficial de catre IETF printr-o serie de documente RFC.

Prin suita IPsec pot fi securizate comunicatiile intre 2 sau mai multe calculatoare independente, intre 2 sau mai multe subretele aflate in spatele unui gateway care se ocupa cu folosirea functiilor criptografice, pentru fiecare subretea aflata in administrarea sa precum si intre un calculator independent si o subretea aflata in spatele unui gateway. IPsec se bazeaza pe proprietatile criptografice ale unor modele precum RSA sau DSA si a algoritmilor de criptare si autentificare, cum sunt DES,3DES,AES,MD5,SHA1.

# II.SSL&TLS

## II.1 SSL

Secure Socket Layer este o tehnologie standard pentru creearea unei conexiuni sigure intre server si client (ex:intre un webserver[website] siun browser sau intre un mailserver si clientmail[Outlook]) SSL permite informatiei sensitive(ex:credit card number, social security number si login credientials) sa fie transmisa in mod securizat.

In mod normal, data transmisa intre browser si webserver este plaintext fiind vurnelabila la atacuri de interceptionare.Daca un atacator receptioneaza toate datele transmise intre client si erver, el le poate folosi cu usurinta.

## II.2 TLS

Transport Layer Security si predecesorul sau, SSL sunt desemnate pentru a prevede o comunicare securizata pe internet.

TLS permite aplicatiilor client-server sa comunice pe retea intr-un mod care previne interceptarea si manipularea datelor transmise.

Datorita faptului ca protocoalele pot opera cu sau fara TLS este necesar pentru client sa indice faptul ca vrea o conexiune TLS cu serverul.Se cunosc 2 solutii pentru aceasta problema:

1.Se foloseste un port diferit pentru TLS(ex:443 pentru HTTPS)

2.Clientul cere serverului sa schimbe conexiunea astfel incat sa se poate folosi TLS.

De indata ce clientul si serverul se pun de acord pentru a folosi TLS ei negociaza o conexiune folosind

procedura handshake, clientul si serverul cad de comun acord asupra anumitor parametri folositi pentru

securitatea conexiunii:

*Handshakeul incepe cand clientul se conecteaza la un server TLS si prezinta o suita de cifre(chipers)

si functii hash.

*Din lista, serverul alege un cifru si o metoda hash care are support pentru ele si il notifica pe

client asupra alegerii luate.

*Serverul trimite clientului ID-ul lui sub forma unui certificat digital. De obicei certificatul contine:

-numele serverului

-CA(certificate authority)

-cheie publica de criptare.

*Clientul poate(la alegerea lui) sa contacteze serverul care a emis CA si sa primeasca inapoi un mesaj de confirmare inainte de a trece la pasii urmatori.

*Pentru ca sa se genereze o cheie de sesiune, clientul cripteaza un numar random cu cheia publica a serverului si trimite rezultatul(criptat) la server.

*Serverul decripteaza rezultatul cu cheia sa privata.

*Folosind aceste date, ambele parti genereaza o cheie material pentru criptare si decriptare valabila pe perioada sesiunii.

## III.DNSsec

Domain Name System Security este o suita de specificatii pentru a securiza anumite tipuri de informatii venite de la DNS care sunt folosite de catre retelele IP.

Este un set de extensii la DNS care aprovizioneaza clientii DNS(resolvers) cu autentificarea originii de unde provin datele DNS si Integritatea.

DNSsec NU poate verifica disponibilitatea sau confidentialitatea.

## IV. PGP & S/MIME

## IV.1 PGP

Pretty Good Privacy este stadardul de criptare si decriptare a datelor care pune la dispozitie intimitate criptograffica si autentificare pentru comunicarea datelor.

PGP este folosit de obicei pentru semnaturi digitale, criptarea si decriptarea textelor, emailuri, fisiere si pentru a mari securitatea comunicatiilor prin email.

Cum functioneaza:

PGP foloseste o serie de combinatii de hashing, compresare de date, cheie simetrica si o cheie publica, fiecare pas foloseste unul din algoritmii suportati.

Pasii pentru CRIPTARE(my personal fucking cooking recepie taken from an immage on wikipedia):

1.Se genereaza o cheie random, K.

2.Se cripteaza datele care trebuiesc transmise(D) cu cheia random, rezultatul fiind un text criptat (DC).

3.Cripteaza cheia K cu cheia publica care a fost receptionata de la server rezultatul fiind o cheie criptata(KC).

4.Se creeaza un mesaj criptat(MC) care contine:DC si KC.

5.Se transmite MC la server.

Pasii pentru DECRIPTARE:

1.Se separa Data Criptata(DC) de cheia criptata(KC) din mesajul criptat(MC).

2.Se decripteaza KC folosind cheia privata a serverului, rezultand cheia K.

3.Se foloseste chia K ca sa decriptezi DC rezultand Data(D) care a fost transmisa.

## IV.2 S/MIME

Secure/Multi Purpoise Internet Mail Extensions este standardul pentru criptarea cu cheie publica si semnarea MIME.

Functii:

S/MIME prevede urmatoarele servicii criptografice pentru posta electronica:

-autentificare

-integritatea mesajelor

-non-reproducerea de origine(folosind semnaturi digitale)

-intimitate si securitatea datelor