Controlul Accesului Mandatat. Modelele Bell-LaPadula, Biba

Breviar Teoretic

Problema:

Fie T, D, H - subiecţi (utilizatori sistem), P - obiect (fişier). T deţine fişierul confidenţial P (are drepturi o, r, w), D are drept de citire (r) asupra lui P, H nu are drept de citire asupra lui P. D creează un nou fişier CP (are drepturile o, r, w asupra lui CP), copiind conţinutul lui P in CP, şi ii acordă lui H drept de citire asupra lui CP. Astfel, H poate citi CP şi implicit P atât timp cât D actualizează CP la fiecare modificare a lui P.

Alt scenariu (fără colaborarea lui D - trojan horse): H programează editorul să salveze o copie a fişierului P asupra căruia să aibă drept de citire.

Soluţie: la DAC trebuie adăugat MAC (Mandatory Access Control).

Modelele MAC respectă axiomele lui Denning

Fie $IF = (SC, \rightarrow, \oplus)$ un model IF (information flow).

A1. SC finită;

A2. $\rightarrow$ ordine parţială (reflexivă, antisimetrică, tranzitivă);

A3. $\rightarrow$ are cel mai mic element;

A4. $\oplus$ (operator combinare) - reprezintă supremum ($A, B \in SC$, $A \rightarrow A \oplus B$, $B \rightarrow A \oplus B$).

Modelul Bell-LaPadula

- matrice de control al accesului (poate fi modificată de subiecţi)
- etichete de securitate (λ) asociate subiecţilor, obiectelor - nu pot fi modificate;

Condiţii necesare:

- simple-security (no read-up):

  s poate citi o doar dacă $\lambda(s) \geq \lambda(o)$ ($\lambda(o) \rightarrow \lambda(s)$) (flux de la obiect la subiect);

- $*$-property (no write-down): s poate scrie o doar dacă $\lambda(s) \leq \lambda(o)$ ($\lambda(s) \rightarrow \lambda(o)$) (flux de la subiect la obiect - interzice unui program secret să scrie intr-un document public; un utilizator secret care doreşte să scrie intr-un document public trebuie să se logheze ca utilizator public);

Dezavantaj: un subiect public poate distruge date confidenţiale; se poate utiliza proprietatea strong-$*$ (s poate scrie o doar dacă $\lambda(s) = \lambda(o)$).

Problema reluată:
Asociem următoarele etichete de securitate:
$\lambda(T) = S$, $\lambda(D) = S$, $\lambda(H) = U$, cu $U \rightarrow S$.
T creează P, $\lambda(P) = S$. D creează CP, $\lambda(CP) = S$.
H nu poate citi indirect P, CP ($\lambda(H) \not\geq \lambda(P)$).

Modelul Biba

- model de integritate;
- integritate obiect: are in vedere gradul de incredere pt informaţia din obiect precum şi eventualele probleme ce pot apare in urma modificărilor neautorizate;
- integritate subiect: nivel de incredere pt subiecţi relativ la operaţiile de ştergere, modificare, adăugare informaţie.
- model dual Bell-LaPadula;

Condiţii necesare:

- simple integrity (no read-down)

  s poate citi o doar dacă $\omega(s) \leq \omega(o)$;

- integrity $*$-property (no write-up)

  s poate scrie o doar dacă $\omega(s) \geq \omega(o)$.

Combinare BLP, Biba

- etichete independente pt confidenţialitate, integritate;
- laticele au clasele de securitate maximală in direcţii diferite ($\lambda_L \to \lambda_H$, $\omega_H \to \omega_L$);

Rezultă (grafic pe slide curs):

- s poate citi o doar dacă:
  $\lambda(s) \geq \lambda(o)$ şi $\omega(s) \geq \omega(o)$;
- s poate scrie o doar dacă:
  $\lambda(s) \leq \lambda(o)$ şi $\omega(s) \leq \omega(o)$;

Exerciţii

Exemplu 1 Se dă următorul model Bell-LaPadula:

$SC = \{Public, Confidential, Secret, TopSecret\}$;

$Public \rightarrow Confidential, Confidential \rightarrow Secret, Secret \rightarrow TopSecret.$

Se dau următoarele subiecte şi obiecte cu etichetele λ corespunzătoare (Tabelul 1):

λ	Subiecte	Obiecte
TopSecret	General	CodNuclear
Secret	Colonel	PoziţieArmată
Confidential	Maior	NrUnitArmată, NrUnitNucleare
Public	Soldat	CostProgramNuclear, CostArmată

Table 1: Funcţia de etichetare λ (Exerciţiul .)

Precizaţi care dintre următoarele afirmaţii sunt adevărate. Justificaţi răspunsul.

a) Generalul poate calcula costurile totale (armată şi program nuclear);

b) Maiorul poate calcula numărul total de unităţi nucleare şi armate;

c) Colonelul poate calcula numărul total de unităţi nucleare şi armate.

d) Colonelul poate modifica poziţia armatei;

e) Maiorul poate modifica costul programului nuclear.

f) Soldatul poate modifica codul nuclear.

Exemplu 2 Descrieţi un model Biba şi atribuiţi etichetele de integritate corespunătoare subiectelor şi obiectelor de la Exemplul astfel încât, după combinarea lui cu modelul Bell-LaPadula de la Exemplul (caz de combinare 3), codul nuclear să poată fi modificat doar de către General.

Rezolvare:

Considerăm următorul model Biba: $SC = Trusted, Untrusted$, $\omega_H = Trusted$, $\omega_L = Untrusted$.

Combinare (Figura 1)

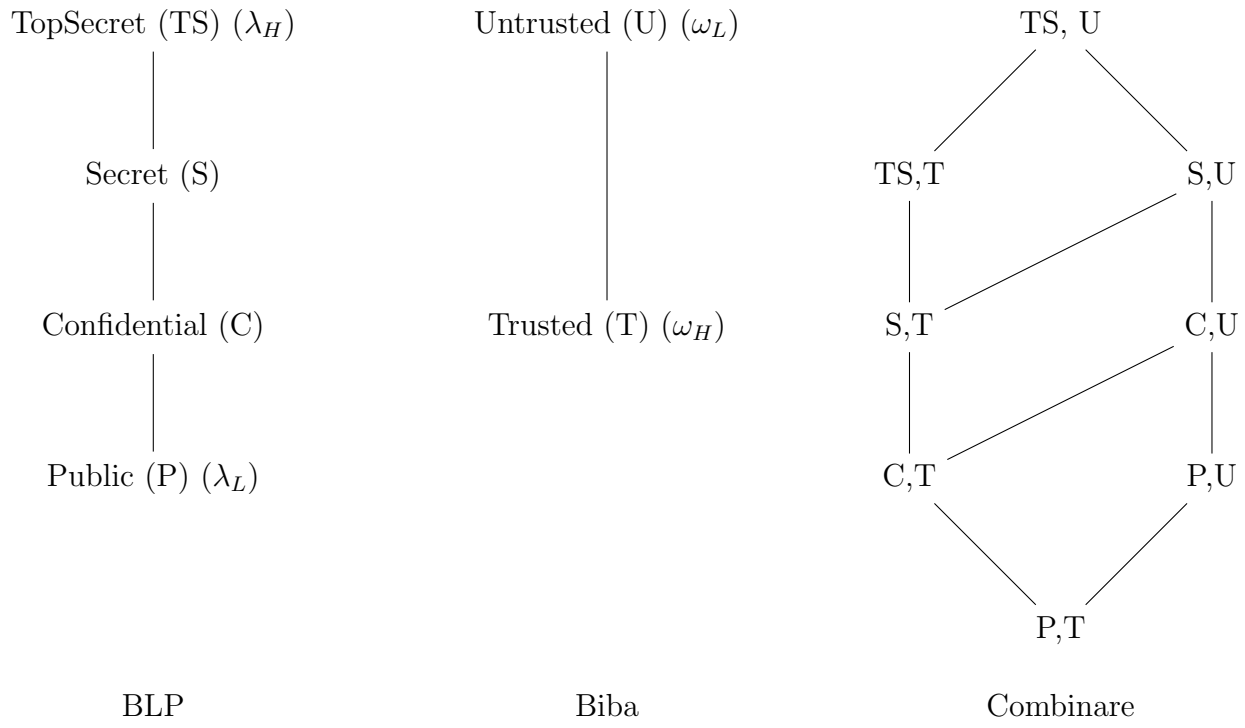


Figure 1: Combinare Exemplu 2

$\omega(General) = \omega(CodNuclear) = Trusted$,
$\omega(Maior) = \omega(Colonel) = \omega(Soldat) = Untrusted$.

- General poate scrie CodNuclear:
  $\lambda(General) = TS = \lambda(CodNuclear)$;
  $\omega(General) = T = \omega(CodNuclear)$;
- Colonel (Maior, Soldat) nu poate scrie CodNuclear:
  $\lambda(Colonel) = S, \lambda(CodNuclear) = TS$;
  $\omega(Colonel) = U, \omega(CodNuclear) = T$;
  (S, U) incomparabil in modelul combinat faţă de (TS, T).
  Analog pentru ceilalţi subiecţi.

Exerciţiul 4

Modelele Bell-LaPadula, Biba

Se dă următorul model Bell-LaPadula:

$SC = \{High, Medium1, Medium2, VeryLow\}$,

$VeryLow \rightarrow Medium1$, $VeryLow \rightarrow Medium2$, $Medium1 \rightarrow High$, $Medium2 \rightarrow High$.

Se consideră următoarele subiecte şi obiecte, cu etichetele de confidenţialitate precizate în Tabelul 4.1.

λ	Subiecte	Obiecte
High	$User_1$	$File_1$
Medium2	$User_2$	$File_2$
Medium1	$User_3$	$File_3$
VeryLow	$User_4$	$File_4$

Table 4.1: Funcţia de etichetare λ (Exerciţiul **??**.)

a) Completaţi tabelul de mai jos (Tabelul 4.2) cu valorile $-$, r, w, r, w, unde:

- $-$: subiectul $User_i$ nu are nici un drept (nu poate scrie, nici citi) asupra obiectului $File_j$;
- r: subiectul $User_i$ poate doar citi obiectul $File_j$;
- w: subiectul $User_i$ poate doar scrie obiectul $File_j$;
- r, w: subiectul $User_i$ poate citi şi scrie obiectul $File_j$;

b) Descrieţi un model simplu Biba, ataşând etichete de integritate (ω) pentru subiectele şi obiectele date şi combinaţi modelul Biba cu modelul Bell-LaPadula dat astfel incât să fie respectate drepturile din următorul tabel (4.3):

S/O	$File_1$	$File_2$	$File_3$	$File_4$
$User_1$				
$User_2$				
$User_3$				
$User_4$				

Table 4.2: Tabel drepturi Subiecte → Obiecte pentru Exerciţiul **??**.

S/O	$File_1$	$File_2$	$File_3$	$File_4$
$User_1$	r, w	$-$	$-$	$-$
$User_2$	w	w	$-$	$-$
$User_3$	$-$	$-$	r, w	r
$User_4$	$-$	w	w	r, w

Table 4.3: Tabel drepturi Subiecte → Obiecte pentru Exerciţiul **??**, punctul b).

Rezolvare:

a) Tabelul (cf. reguli BLP):

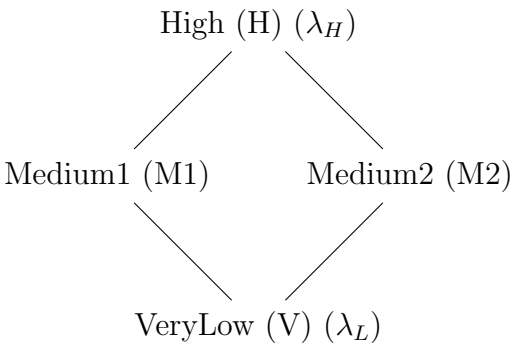
S/O	$File_1$	$File_2$	$File_3$	$File_4$
$User_1$	r, w	r	r	r
$User_2$	w	r, w	$-$	r
$User_3$	w	$-$	r, w	r
$User_4$	w	w	w	r, w

b) Model Biba: doua clase de integritate: $Trusted = \omega_H$, $Untrusted = \omega_L$.

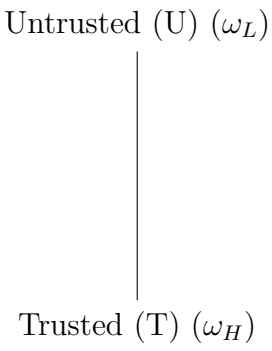
Combinare (Figura 4.1):

Etichete integritate:

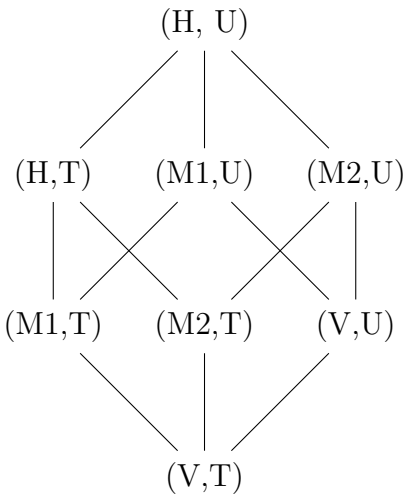
ω	Subiecte	Obiecte
Trusted	$User_1$, $User_2$	$File_1$
Untrusted	$User_3$, $User_4$	$File_2$, $File_3$, $File_4$



BLP



Biba



Combinare

Figure 4.1: Combinare modele BLP, Biba - caz 3