Tema 2,Securitate Informației

Ionită Mihail-Cătălin,Grupa B2

December 8, 2020

1 Exercițiul 1

Fie următoarele matrici de control al accesului,unde a,b,c,d sunt considerați subiecți.

	a	b	c
a		q	
b	k		
c	k	q,k	

	a	b	c	d
a		t		
b			t	
c			q	
d				

Pentru matricea a) având definită comanda

```
command tansfer(X,Y,Z)
    if q in (X,Y)
    if K in (X,Y)
    if k in (X,Z)
    then
        enter q in (X,Z)
        delete q from (X,Y)
    end
```

a)

Vom descrie in cele ce urmeaza starea matricii de control dupa execuția comenzilor transferq(c,a,b),transferq(c,b,a)

Vom executa comanda transferq(c,a,b)

Aplicâm pentru σ(X)=c,σ(Y)=a și σ(Z)=b

- verificâm condiția σ(if q in (X,Y))=if q in (c,a) - fals
- verificâm condiția σ(if k in (X,Y))=if k in (c,a) -adevărat
- verificâm condiția σ(if k in (X,Z))=if k in (c,b) - adevărat

Cum una dintre condiții este falsă nu se va intra in blocul de instrucțiuni astfel matricea de control al accesului va arata identic cu cea inițială

	a	b	c
a		q	
b	k		
c	k	q,k	

Vom executa comanda transferq(c,b,a)
Aplicâm pentru σ(X)=c,σ(Y)=b și σ(Z)=a

- verificâm condiția σ(if q in (X,Y))=if q in (c,b) - adevărat
- verificâm condiția σ(if k in (X,Y))=if k in (c,b) -adevărat
- verificâm condiția σ(if k in (X,Z))=if k in (c,a) - adevărat
- aplicâm operațiile
  - enter q in (σ(X),σ(Z))=(c,a)
    - S_1=S
    - O_1=O
    - $A_1(c,a)$=A(c,a)$\cup$q,$A_1(x,y) = A(x,y)$ dacă x$\neq$c,y$\neq$a
  - delete q from (σ(X),σ(Y))=(c,b)
    - S_2=S_1
    - O_2=O_1
    - $A_2(c,b)$=$A_1(c,b) - \{q\}$,$A_1(x,y) = A(x,y)$ dacă x$\neq$c,y$\neq$b

Matricea de control al accesului obținută în urma execuției comenzii transferq(c,b,a) este

	a	b	c
a		q	
b	k		
c	q,k	k	

b)
Definitie:
Comanda α scurge dreptul r in starea Q dacă:

- α se poate aplica stării Q sub p substituție σ;
- prin aplicarea operațiilor comenzii α o celulă a stării Q ce nu conține r ajunge să conțină r

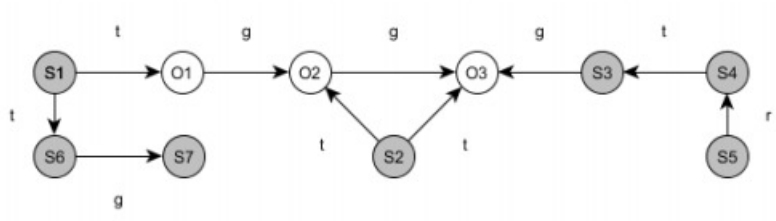
Pentru a obține un leak al dreptului q către un nou nod e creat de către nodul a vom aplica comenzile create,grant și take în următoare ordine:

1. b take q for d from c - $take\_q(b, c)$
2. a take q for d from b - $take\_q(a, b)$
3. a create t,g for new subject e - $create(a, e)$
4. a grant q for b to e - $grant\_q(a, e)$

Astfel în urma aplicării acestor comenzi în celula asociată subiectului e din matricea de control a accesului va apărea dreptul q ceea ce conform definiției este o scurgere a dreptului q.

2 Exercițiul 2

Se dă următorul graf take-grant G:



a)Există un span inițial către nodul S7 acesta fiind p'=S1 întrucât există tg-drumul S1,S6,S7

b)Pentru a verifica valoarea de adevăr a predicatului can_share(r,S4,S7,G) vom testa condițiile teoremei 23 prezentate în cadrul cursului

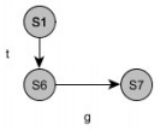
Theorem 23

Let G be a take-grant state, r a right, and x and p nodes in G. Then, $can.share(r,x,p,G)$ is true if and only if $r \in (p,x)$ or there exists a node s, two subjects p' and s', and islands $I_1, \ldots, I_n$ such that:

- $r \in_G (s,x)$;
- $p' = p$ or p' initially spans to p;
- $s' = s$ or s' terminally spans to s;
- p' is in I_1, s' is in I_n, and there is a bridge from I_j to I_{j+1}, for all $1 \leq j < n$.

Vom verifica condițiile teoremei:

1. Cazul I:
   - Există o muchie in graful G de la nodul S7 la nodul S4 etichetată cu r - fals
2. Cazul II:
   (a) Există un nod s în G,și o muchie de la s la x cu etichetată cu r - Adevărat,s=S5
   (b) Există un nod p' în G care fie este chiar p,fie are un span inițial către p, - Adevărat de la subpunctul anterior știm că există un span inițial de la nodul S7 cu p'=S1
   (c) Există un nod s' în G care fie este chiar s,fie are un span final către s - Adevărat vom conside cazul în care s=s'=S5 întrucât în sensul original nu există un span final catre s
   (d) Nodul p' aparține de o insulă I1,iar s' aparține de o insula In,iar I1 și In sunt conectate fie direct printr-un bridge,fie printr-o cale formată din mai multe bridge-urice trec prin insule intermediare - Fals,putem identifica următoarele insule:



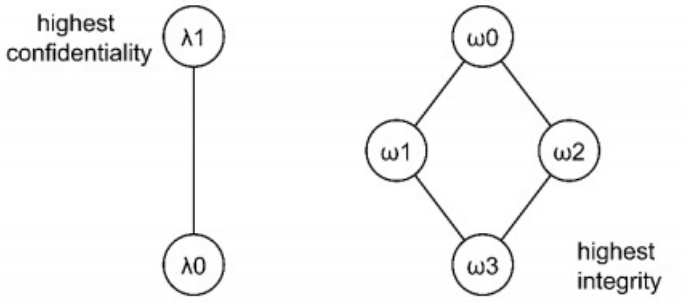
Între aceste insule nu există bridge-uri care conectează nodul p' și nodul s',care să respecte definiția structurii de bridge,anume:
Un bridge este un drum care are drept capete două noduri subiect etichetat cu una din secventele:

- (t)* direția $\rightarrow$
- (t)* direcția $\leftarrow$
- (t)*g(t)* direcțiile $\rightarrow\rightarrow\leftarrow$
- (t)*g(t)* direcțiile $\rightarrow\leftarrow\leftarrow$

Având în vedere faptul că modelul nu respectă toate condițiile teoremei 23 simultan,putem concluziona faptul că can_share(r,S4,S7,G)=false

3 Exercițiul 3

Se dau următoarea diagrame ce exemplifică modelarea a doua fluxuri de informație folosind modelele Bell-LaPadula si Biba. Combinați cele doua diagrame astfel încât direcția fluxului de informație să fie respectat în ceea ce privește clasele cu cea mai mare confidențialitate și cea mai mare integritate.



Compunerea celor două modele respectând direcția fluxului de informație este următoarea: