Examen SI 2021-2022 v.2

Switch account

The name and photo associated with your Google account will be recorded when you upload files and submit this form. Only the email you enter is part of your response.

* Required

Email *

Your email

[MCA] Fie sistemul de protecție C = {give_ot, give_d, give_g}, unde comenzile sunt cele descrise mai jos, și starea Q = {S,O,A}, unde S = {Ana, Eva, Ion, Geo}, O = {Ana, Eva, Ion, Geo, tab, PC} și A este reprezentată prin matricea de acces de mai jos. Sistemul de protecție C este sigur relativ la dreptul t și starea Q? Alegeți răspunsul cel mai complet. *

	Ana	Eva	Ion	Geo	tab	PC
Ana	o	Ø	Ø	Ø	d	t
Eva	Ø	p	t	x,w	g	Ø
Ion	p	o	Ø	p	o	Ø
Geo	Ø	o	t	Ø	Ø	w

```
command give_ot (Xs1, Xs2, Xo)
        if t in (Xs2, Xs1) and
          d in (Xs2, Xo)
        then
          enter o into (Xs2, Xs1)
          enter t into (Xs2, Xo)
end

-------------------------------------------------

command give_d (Xs1, Xs2, Xo)
        if g in (Xs2, Xs1) and
          o in (Xo, Xs1)
        then
           enter d into (Xo, Xs1)
end

-------------------------------------------------

command give_g (Xs1, Xs2)
        if o in (Xs1, Xs2) and
           t in (Xs2,Xs1)
        then
          enter g into (Xs1, Xs2)
end
```

- Da, deoarece putem aplica comenzile give_ot, give_d și give_g iar dreptul t va fi introdus intr-o celula favorabila.
- Nu deoarece putem aplica comenzile într-o anumită ordine și astfel demonstrăm nesiguranța sistemului.
- Nu deoarece putem aplica comenzile give_ot, give_g și dreptul t va fi introdus. Nicio altă variantă de comenzi nu va duce la demonstrarea nesiguranței sistemului C.
- Da, sistemul este sigur deoarece putem aplica 2 sau 3 comenzi într-o anumită ordine,

cum ar fi give_d, give_g sau give_d, give_ot, give_g si va aparea dreptul t.

Da, deoarece dreptul t nu poate fi introdus.

Nume, Prenume, GRUPA *

Your answer

Fie modelul Bell-LaPadula SC = {A, B, C, D, E}. Cu fluxurile de informație E → C, E→ D, C → A, D → A, D → B, B → A. Considerați următorii subiecți și obiecte, cu etichetele de confidențialitate corespunzătoare din tabelul [λ]. Combinând laticea BLP cu o latice Biba cu 3 clase, X (omega high), Y și Z (omega low), atribuiți etichete de integritate pentru a obține drepturile din tabelul de [drepturi]. *

[drepturi]	acte	liste	note	fișe
Oana	r	-	r	-
Adi	-	w	-	w
Ionuț	r	w	w	-
Maria	w	w	w	-

[λ]	Subiecți	Obiecte
A		liste
B	Oana	note
C	Adi	fișe
D	Ionuț	acte
E	Maria	

	A,X	B,X	C,X	D,X	E,X	A,Y	B,Y	C,Y	D,Y
Oana	○	○	○	○	○	○	○	○	○
Adi	○	○	○	○	○	○	○	○	○
Ionuț	○	○	○	○	○	○	○	○	○
Maria	○	○	○	○	○	○	○	○	○
fișe	○	○	○	○	○	○	○	○	○
liste	○	○	○	○	○	○	○	○	○
note	○	○	○	○	○	○	○	○	○
acte	○	○	○	○	○	○	○	○	○

Pentru cele două exerciții de mai jos scrieți rezolvarea în câmpul aferent exercițiului. Numai în caz de strictă necesitate, atașați un fișier cu rezolvarea în câmpul [CRYPTO]. *

1. Considerăm urmatoarea variantă de MAC (utilizată in protocolul 802.11b WEP):
   (a) Fie $F(K, r)$ o PRF ce produce ca rezultat un şir binar de 32 biţi, unde K este o cheie dintr-un spaţiu $\mathcal{K}$ de chei, iar r este un element generat random dintr-un spaţiu $\mathcal{R}$ (nu este necesar de a se cunoaşte spaţiile $\mathcal{K}$ şi $\mathcal{R}$);
   (b) Fie $CRC32$ un cod detector de erori ce produce şiruri de 32 bits. Vom presupune că $CRC32$ este întotdeauna definit pe şirurile de intrare considerate şi, în plus, are proprietatea
   $$CRC32(m_1) \oplus CRC32(m_2) = CRC32(m_1 \oplus m_2);$$
   (c) Tagurile pentru un mesaj m cu o cheie K se definesc prin:
   - $r \leftarrow \mathcal{R}$ (se generează random r din $\mathcal{R}$);
   - $t := F(K, r) \oplus CRC32(m)$;
   - Tagul este perechea (r, t);

   (d) Un tag (r, t) pentru un mesaj m este acceptat dacă prin recalculare se obţine t.

   Cerinţă: Este această schema de MAC sigură? Justificaţi răspunsul.
2. Putem utiliza o schemă de MAC în locul semnăturilor digitale în DNSsec? Justificaţi răspunsul.

Your answer

Optional puteți menționa alegerea parametrilor pentru demonstrarea stării de siguranță a sistemului de protecție C. Aici vom scrie comenzile instanțiate în exact ordinea favorabilă exercițiului [MCA].

	Ana	Eva	Ion	Geo	tab	PC
Ana	o	Ø	Ø	Ø	d	t
Eva	Ø	p	t	x,w	g	Ø
Ion	p	o	Ø	p	o	Ø
Geo	Ø	o	t	Ø	Ø	w

Your answer

[CRYPTO] - opțional upload fișier cu rezolvarea exercițiilor de criptografie (nu mai mult de 5MB).

Add file

Submit Clear form

Never submit passwords through Google Forms.