

Examen SI 2021-2022 v.1

[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 $C = \{\text{give_r}, \text{give_t}, \text{create_n}\}$, unde comenzile sunt cele descrise mai jos, și starea $Q = \{S, O, A\}$, unde $S = \{\text{Ana}, \text{Eva}, \text{Ion}, \text{Geo}\}$, $O = \{\text{Ana}, \text{Eva}, \text{Ion}, \text{Geo}, \text{tab}, \text{PC}\}$ 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	t	\emptyset	g	\emptyset	\emptyset	x
Eva	o	\emptyset	t, x	t, o	o, t	\emptyset
Ion	d	\emptyset	d	g	g, x	t
Geo	\emptyset	o	\emptyset	o	\emptyset	r

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

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

```
command create_n (Xs1, Xs2)
  if g in (Xs1, Xs1)
  then
    create subject Xs2
    enter t into (Xs2, Xs1)
end
```

- ☐ Da, deoarece putem aplica 2 sau 3 comenzi într-o anumită ordine și niciodată dreptul t nu va fi introdus.
- ☐ Nu deoarece putem aplica comenzile give_t , give_r , create_n în această ordine și dreptul t va apărea într-o nouă celulă.
- ☐ Nu deoarece putem aplica comenzile give_r , create_n și dreptul t va fi introdus. Nicio altă variantă de comenzi nu va duce la demonstrarea nesiguranței sistemului C .
- ☐ Sistemul este nesigur deoarece putem aplica 2 sau 3 comenzi într-o anumită ordine,

- ☒ cum ar fi give_r, create_n si va aparea dreptul t.
- ☐ Da, deoarece dreptul t nu poate fi introdus.

Nume, Prenume, GRUPA *

Your answer

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

 Add file

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 următoarea variantă de MAC (utilizată în protocolul 802.11b WEP):

- (a) Fie $F(K, r)$ o PRF ce produce ca rezultat un șir binar de 32 biți, unde K este o cheie dintr-un spațiu \mathcal{K} de chei, iar r este un element generat random dintr-un spațiu \mathcal{R} (nu este necesar de a se cunoaște spațiile \mathcal{K} și \mathcal{R});
- (b) Fie $CRC32$ un cod detector de erori ce produce șiruri de 32 bits. Vom presupune că $CRC32$ este întotdeauna definit pe șirurile de intrare considerate și, 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 obține t .

Cerință: Este această schema de MAC sigură? Justificați răspunsul.

2. Putem utiliza o schemă de MAC în locul semnăturilor digitale în DNSsec? Justificați răspunsul.

Your answer



Fie modelul Bell-LaPadula $SC = \{A, B, C, D, E\}$. Cu fluxurile de informație $E \rightarrow C$, $E \rightarrow D$, $C \rightarrow A$, $D \rightarrow A$, $D \rightarrow B$, $B \rightarrow A$. Considerați următorii subiecți și obiecte, cu etichetele de confidențialitate corespunzătoare din tabelul $[\lambda]$. 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
Maria	r	-	r	r
Ionuț	r,w	-	-	r
Adi	-	w	-	-
Georgiana	w	w	w	r,w

$[\lambda]$	Subiecți	Obiecte
A		liste
B	Maria	note
C	Adi	
D	Ionuț	acte
E	Georgiana	fișe

	A,X	B,X	C,X	D,X	E,X	A,Y	B,Y	C,Y	D,Y
Maria	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Adi	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ionuț	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Georgiana	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
fișe	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
liste	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
note	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
acte	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>



Opțional. 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	t	Ø	g	Ø	Ø	x
Eva	o	Ø	t, x	t, o	o, t	Ø
Ion	d	Ø	d	g	g, x	Ø
Geo	Ø	o	Ø	o	Ø	r

Your answer

Submit

Clear form

Never submit passwords through Google Forms.

This content is neither created nor endorsed by Google. [Report Abuse](#) - [Terms of Service](#) - [Privacy Policy](#).

Google Forms

