Examen SI 2021-2022 v.0

boogyman1989@yahoo.com Schimbați contul

Numele și fotografia asociate cu contul dvs. Google vor fi înregistrate când încărcați fișiere și trimiteți acest formular. Numai adresa de e-mail pe care o introduceți face parte din răspunsul dvs.

*Obligatoriu

Adresă de e-mail *

Adresa dvs. de e-mail

Nume, Prenume, GRUPA *

Răspunsul dvs.

[MCA - 45pct] Fie sistemul de protecție C = {give_read, give_write, give_wg, give_find}, unde comenzile sunt cele descrise mai jos - variabilele X, Y sunt în S iar Xo1, Xo2 în O - și starea Q = {S,O,A}, unde S = {Mara, Ina, Geo, Ela}, O = {Mara, Ina, Geo, Ela, tel, PC, obj} iar A este reprezentată prin matricea de acces de mai jos. Sistemul de protecție C este sigur relativ la dreptul f și starea Q? Justificați riguros. *

	Mara	Ina	Geo	Ela	tel	PC	obj
Mara	d	d	t	Ø	f	Ø	t
Ina	Ø	Ø	Ø	f	r	Ø	t
Geo	d,f	Ø	f	Ø	r	g	Ø
Ela	Ø	s	Ø	Ø	d	t	g

```
command give_read (X, Xo1, Y, Xo2)
        if s in (Y, Xo1) and
          w in (X, Xo1)
        then
          enter r into (Y, Xo2)
end
-----------------------------------------------------------
command give_write (X, Xo1, Xo2)
        if t in (Xo1, Xo2) and
          r in (X, Xo2)
        then
          enter w into (Xo1, Xo2)
end
-----------------------------------------------------------
command give_wg (X, Xo1, Y, Xo2)
        if r in (Y, Xo1) and
          t in (X, Xo2)
        then
          enter g into (Y, Xo1)
          enter w into (X, Y)
end
-----------------------------------------------------------
command give_find (X, Xo1, Xo2, Xo3)
        if r in (Xo2, Xo1) and
          t in (X, Xo1) and
          w in (X, Xo3)
        then
          enter f into (X, Xo2)
end
-----------------------------------------------------------
```

Răspunsul dvs.

[BLP-Biba - 15pct] Fie modelul Bell-LaPadula SC = {A, B, C, D, E}. Cu fluxurile de informație A → B, A→ C, C → D, B → D, D → E, A → E. Considerați următorii subiecți și obiecte, cu etichetele de confidențialitate corespunzătoare din tabelul [λ]. Combinând laticea BLP cu o latice Biba cu 2 clase, T (omega high) și W (omega low), atribuiți etichete de integritate pentru a obține drepturile din tabelul de [drepturi]. Atașați imaginea cu laticile combinate și cu eventuale explicații în rubrica [BLP-Biba]. *

[drepturi]	cărți	acte	filă	CD
Ana	r w	w	w	w
Ion	r	r	-	-
Liviu	r	-	w	w
Elena	r	r	-	r

[omega]	Subiecți	Obiecte
T	Liviu, Ana, Elena	cărți, acte, CD
W	Ion	filă

	A,T	B,T	C,T	D,T	E,T	A,W	B,W	C,W	D,W	E,V
Ana	○	○	○	○	○	○	○	○	○	○
Ion	○	○	○	○	○	○	○	○	○	○
Liviu	○	○	○	○	○	○	○	○	○	○
Elena	○	○	○	○	○	○	○	○	○	○
cărți	○	○	○	○	○	○	○	○	○	○
acte	○	○	○	○	○	○	○	○	○	○
filă	○	○	○	○	○	○	○	○	○	○
CD	○	○	○	○	○	○	○	○	○	○

[BLP-Biba - 10pct] upload la imaginea cu laticile combinate și explicații.

Adăugați un fișier

[Crypto - 30pct] Pentru exercițiul de mai jos scrieți rezolvarea în câmpul aferent. Numai în caz de strictă necesitate, atașați un fișier cu rezolvarea în câmpul [Crypto]. *

Considerăm următoarea variantă de MAC:

(a) Presupunem că $m = m_1 \cdots m_\ell$ este un mesaj împărţit în blocuri de lungime egală;

(b) Fie F_K o PRF (cu cheia K generată random);

(c) Pentru fiecare i de la 1 la ℓ calculăm

$$t_i = F_K([i]_s \parallel m_i)$$

unde $[i]_s$ este reprezentarea binară a lui i pe s biţi (s este dat, fixat, şi presupunem că toţi întregii de la 1 la ℓ se pot reprezenta pe s biţi);

(d) Tagul mesajului m, cu cheia K, va fi

$$MAC_K(m) = t_1 \oplus \cdots \oplus t_\ell$$

Cerinţă: Este această schemă de MAC sigură? Justificaţi răspunsul.

Răspunsul dvs.

[Crypto] - opțional upload fișier cu rezolvarea exercițiului de departajare (nu mai mult de 5MB).

Adăugați un fișier

Trimiteți Goliți formularul