Restanțe/măriri SI 2021-2022 v.1

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_d, give_take, give_read, give_find}, unde comenzile sunt cele descrise mai jos - variabilele S1, S2, S3 sunt în S și O1, O2 în O - și starea Q = {S,O,A}, unde S = {Mara, Ina, Geo, Ela}, O = {Mara, Ina, Geo, Ela, tel, PC, obj} și 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	t	Ø	f	Ø	s	r	t
Ina	r	Ø	Ø	Ø	f	Ø	r
Geo	Ø	f	Ø	r	Ø	Ø	r
Ela	r	f	Ø	Ø	Ø	Ø	t

```
command give_d (S1, O1, O2)
        if t in (S1, O2) and
          r in (S1, O1)
        then
          enter d into (O1, O2)
end
-----------------------------------------------------------------
command give_take (S1, O1, O2, O3)
        if t in (S1, O1) and
          r in (O3, O1)
        then
          enter t into (S1, O3)
end
-----------------------------------------------------------------
command give_read (S1, S2, O1, O2)
        if t in (S2, O2) and
          r in (S1, O2) and
          r in (S1, O1)
        then
          enter r into (S2, O1)
end
-----------------------------------------------------------------
command give_find (S1, S2, S3, O1)
        if d in (S1, O1) and
          t in (S2, O1) and
          r in (S3, S3) and
          r in (S1, S3)
        then
          enter w into (S1, S3)
          enter f into (S1, S2)
end
```

Răspunsul dvs.

[BLP-Biba - 15pct] Fie modelul Bell-LaPadula SC = {A, B, C, D, E}. Cu fluxurile de informație E → A, E→ D, D → C, D → B, C → A, B → A. 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	w	r	r	-
Ion	w	r,w	-	w
Liviu	w	-	r	r
Elena	w	-	-	w

[λ]	Subiecți	Obiecte
A	Ana	cărți
B	Ion	acte
C	Liviu	filă
D		CD
E	Elena	

	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

Nu trimiteți parole prin formularele Google.