

Examen (timp de lucru: 1h40')

1. (Controlul accesului – timp estimat: 40')

- (a) Care sunt operațiile primitive în cadrul modelului bazat pe matrici de control al accesului? **0.5p**
 (b) Ce se înțelege prin comandă în cadrul modelului bazat pe matrici de control al accesului? **0.5p**
 (c) Ce se înțelege prin sistem de protecție în cadrul modelului bazat pe matrici de control al accesului? **0.5p**
 (d) Fie structurile

```
command CREATE(process, file)
  if file does not exist
  then
    create object file
    enter own into (process, file)
  end

command CONFER_READ(owner, friend, file)
  if own in (owner, file) and
    r not in (friend, file)
  then
    create object file
    enter x into (friend, file)
  end
```

Este $\mathcal{C} = \{CREATE, CONFER_READ\}$ sistem de protecție peste mulțimea de drepturi $R = \{own, r, w\}$? Justificați răspunsul. **0.5p**

- (e) Fie comanda *JUST_CREATE* peste mulțimea de drepturi $R = \{f, m, r, w\}$ dată prin

```
command JUST_CREATE( $X_{s_1}, X_{s_2}, X_o$ )
  if  $f$  in ( $X_{s_1}, X_{s_2}$ ) and
     $m$  in ( $X_{s_2}, X_{s_1}$ )
  then
    create object  $X_o$ 
  end
```

și A matricea de control al accesului de mai jos

	Ion	Gelu	Dan	file
Ion	r	r, w, f	r, a	\emptyset
Gelu	w, m	r, w	r, a	r
Dan	r	\emptyset	\emptyset	w

Se poate aplica *JUST_CREATE*(*Ion, Gelu, personal*) asupra matricii A ? Dacă da, care este rezultatul? Justificați răspunsul. **0.5p**

- (f) Este posibil a aplica comanda *JUST_CREATE* de la punctul anterior unei matrici de control al accesului ce are doar un singur subiect? Justificați răspunsul. **0.5p**
 (g) Fie $\mathcal{C} = \{JUST_CREATE\}$ un sistem de protecție peste $R = \{f, m, r, w\}$, și fie $Q = (S, O, A)$ starea dată prin $S = \{\text{Ion, Gelu, Dan}\}$, $O = \{\text{Ion, Gelu, Dan, file}\}$ și matricea A de la punctul (e). Este Q sigură pentru dreptul f ? Justificați răspunsul. **1p**

2. (Protocolul Woo-Lam – timp estimat: 30')

Protocolul de mai jos are scopul de a mijloci autentificarea unui client A către un alt client B prin intermediul unui server S (în protocol, $\{x\}_K$ înseamnă x criptat cu K , iar K_{XY} reprezintă cheia partajată de X și Y):

1. $A \rightarrow B$: A
2. $B \rightarrow A$: N_b
3. $A \rightarrow B$: $\{A, B, N_b\}_{K_{AS}}$
4. $B \rightarrow S$: $\{A, B, \{A, B, N_b\}_{K_{AS}}\}_{K_{BS}}$
5. $S \rightarrow B$: $\{A, B, N_b\}_{K_{BS}}$

- Explicați modul în care funcționează protocolul (furnizați cât mai multe detalii convingătoare asupra realizării obiectivului acestuia). 0.5p
- Se știe că acest protocol este vulnerabil la atac prin interpunerea unui intrus între participanții la protocol. Prezentați un astfel de atac. 2.5p

3. (DNSsec – timp estimat: 30')

În Figura 1 aveți un arbore DNS (mult simplificat) în care sunt figurate zonele de autoritate (prin elipse întrerupte – nodul rădăcină este zona de autoritate pentru el). Se presupune ca nodul **example** conține

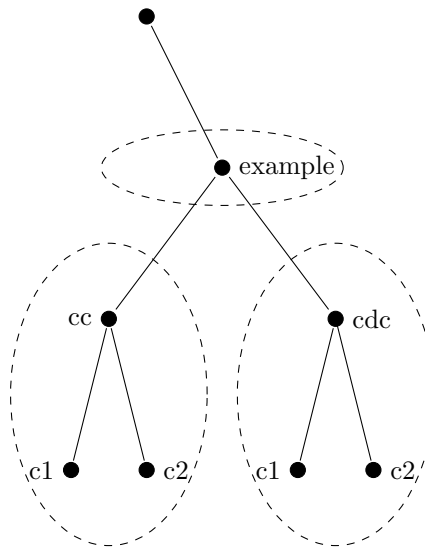


Figure 1: Arbore DNS

înregistrări de tip SOA, MX și NS, nodurile **cc** și **cdc** conțin fiecare înregistrări de tip NS și MX, iar nodurile copil a nodurilor **cc** și **cdc** conțin înregistrări de tip A. Cerințe:

- (a) Care sunt serviciile fundamentale asigurate de DNSsec? 0.25p
- (b) Arătați cum se adaugă înregistrările specifice DNSsec arborelui din Figura 1. 0.75p
- (c) Explicați cum se obțin proprietățile de securitate DNSsec pentru rezoluția **c2.cc.example** 1p
- (d) Explicați cum se obțin proprietățile de securitate DNSsec pentru rezoluția **c2.ccc.example** 1p