Information Security, 2015–2016

Prof.Dr. Ferucio Laurenţiu Ţiplea
Department of Computer Science
"Al.I.Cuza" University of Iaşi
Office: C 301
Tel: (0232) 201538

Date: Jan 22, 2016

Examen (timp de lucru: 1h40')

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

   (a) Care sunt operaţiile primitive în cadrul modelului bazat pe matrici de control al accesului? **0.5p**

   (b) Ce se înţelege prin comandă în cadrul modelului bazat pe matrici de control al accesului? **0.5p**

   (c) Ce se înţelege prin sistem de protecţie 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 protecţie peste mulţimea de drepturi $R = \{own, r, w\}$? Justificaţi răspunsul. **0.5p**

   (e) Fie comanda $JUST\_CREATE$ peste mulţimea 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

   şi A matricea de control al accesului de mai jos

$$\begin{array}{c} \\ \text{Ion} \\ \text{Gelu} \\ \text{Dan} \end{array} \begin{array}{c} \begin{array}{cccc} \text{Ion} & \text{Gelu} & \text{Dan} & file \end{array} \\ \begin{pmatrix} r & r,w,f & r,a & \emptyset \\ w,m & r,w & r,a & r \\ r & \emptyset & \emptyset & w \end{pmatrix} \end{array}$$

   Se poate aplica $JUST\_CREATE(Ion, Gelu, personal)$ asupra matricii A? Dacă da, care este rezultatul? Justificaţi 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? Justificaţi răspunsul. **0.5p**

   (g) Fie $\mathcal{C} = \{JUST\_CREATE\}$ un sistem de protecţie peste $R = \{f, m, r, w\}$, şi fie $Q = (S, O, A)$ starea dată prin $S = \{\text{Ion,Gelu,Dan}\}$, $O = \{\text{Ion,Gelu,Dan}, file\}$ şi matricea A de la punctul (e). Este Q sigură pentru dreptul f? Justificaţi 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 şi Y):

$$\begin{array}{lcl} 1. & A \rightarrow B & : \quad A \\ 2. & B \rightarrow A & : \quad N_b \\ 3. & A \rightarrow B & : \quad \{A, B, N_b\}_{K_{AS}} \\ 4. & B \rightarrow S & : \quad \{A, B, \{A, B, N_b\}_{K_{AS}}\}_{K_{BS}} \\ 5. & S \rightarrow B & : \quad \{A, B, N_b\}_{K_{BS}} \end{array}$$

- Explicaţi modul în care funcţionează protocolul (furnizaţi cât mai multe detalii convingătoare asupra realizării obiectivului acestuia). **0.5p**
- Se ştie că acest protocol este vulnerabil la atac prin interpunerea unui intrus între participanţii la protocol. Prezentaţi un astfel de atac. **2.5p**

Solutie: (atac asupra protocolului – I_X înseamnă că intrusul I impersonifică X)

$$\begin{array}{lcl} 1'. & I_A \rightarrow B & : \quad A \\ 2'. & B \rightarrow I_A & : \quad N_b \\ 3'. & I_A \rightarrow B & : \quad N_b \\ 4'. & B \rightarrow I_S & : \quad \{A, B, N_b\}_{K_{BS}} \\ 5'. & I_S \rightarrow B & : \quad \{A, B, N_b\}_{K_{BS}} \end{array}$$

3. (DNSsec – timp estimat: 30')
In Figura 1 aveti 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` conţine

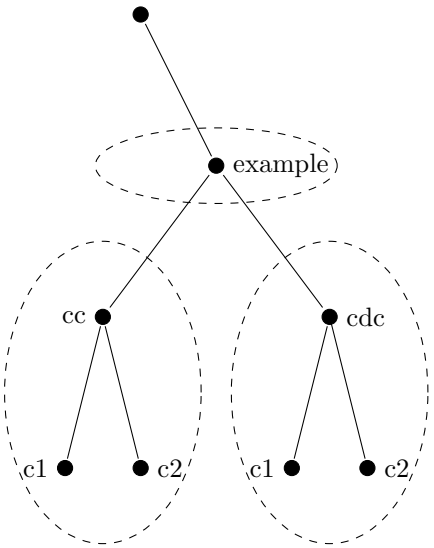

Figure 1: Arbore DNS

inregistrări de tip SOA, MX şi NS, nodurile `cc` şi `cdc` conţin fiecare înregistrări de tip NS şi MX, iar nodurile copil a nodurilor `cc` şi `cdc` conţin înregistrări de tip A. Cerinţe:

(a) Care sunt serviciile fundamentale asigurate de DNSsec? **0.25p**

(b) Arătaţi cum se adaugă înregistrările specifice DNSsec arborelui din Figura 1. **0.75p**

(c) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.cc.example` **1p**

(d) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.ccc.example` **1p**