Information Security, 2016-2017

Instructor: Prof.Dr. Ferucio Laurenţiu Ţiplea
Department of Computer Science
Alexandru Ioan Cuza University of Iaşi
Office: C 301
Tel: (0232) 201538

Date: Jan 30, 2017

Examen

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

   (a) Care sunt operaţiile primitive în cadrul modelului bazat pe matrici de control al accesului? **5p**

   (b) Ce se înţelege prin comandă în cadrul modelului bazat pe matrici de control al accesului? **5p**

   (c) Ce se înţelege prin sistem de protecţie în cadrul modelului bazat pe matrici de control al accesului? **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. **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. **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. **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. **5p**

2. (IPsec – timp estimat: 40')

   (a) Descrieţi, succint dar clar, elementele ce stau la baza arhitecturii $IPsec$ (asociere de securitate, AH, ESP, moduri de utilizare pentru datagrame IPv4). **15p**

   (b) Modul de criptare CBC al unei secvenţe $P_1 \cdots P_n$ cu vectorul de iniţializare $IV = C_0$ este dat prin $C_i = e_K(P_i \oplus C_{i-1})$, pentru orice $1 \leq i \leq n$. Ce implicaţii, la destinaţie, are apariţia unei erori în transmisia unui bloc C_i ? **10p**

   (c) Modul de criptare PCBC al unei secvenţe $P_1 \cdots P_n$ cu vectorul de iniţializare $IV = C_0$ este dat prin $C_1 = e_K(P_1 \oplus C_0)$ şi $C_i = e_K(P_i \oplus P_{i-1} \oplus C_{i-1})$, pentru orice $2 \leq i \leq n$. Ce implicaţii, la destinaţie, are apariţia unei erori în transmisia unui bloc C_i ? **10p**

3. (Timp estimat: 40')
   Problema *Cinei criptografilor* se formulează astfel. Trei criptografi, C_1, C_2 şi C_3 au luat cina şi, la sfârşit, au fost anunţaţi că cineva a plătit. Cum masa putea fi plătită de un criptograf (şi doar de unul) sau de o persoană externă, criptografii hotărăsc să afle dacă cina a fost plătită de un extern sau de unul dintre ei dar, în cel de-al doilea caz, să nu se divulge identitatea acestuia. Pentru aceasta ei procedează conform următorului protocol, notat $DC(3)$:

   - fiecare criptograf C_i alege random un bit şi îl comunică în mod secret criptografului din stânga sa (criptografii sunt asezaţi la o masă circulară în ordinea C_1, C_2, C_3, de la stânga la dreapta);
   - fiecare criptograf C_i alege încă un bit astfel: bitul 0 dacă nu a plătit masa, şi 1, altfel;
   - fiecare criptograf C_i publică suma modulo 2 ($\oplus$) a celor 3 bits cunoscuţi, notată z_i.

   In urma desfăşurării protocolului şi analizei sumei $z_1 \oplus z_2 \oplus z_3$, criptografii deduc dacă masa a fost plătită de unul dintre ei sau de un extern. In plus, din punctul de vedere al unui criptograf ce nu a plătit masa, oricare din ceilalţi doi criptografi ar fi putut să o plătească, cu egală probabilitate (în ipoteza în care unul dintre ei a plătit-o).

   (a) Justificaţi corectitudinea concluziei criptografilor (presupunând că criptografii sunt oneşti în cadrul protocolului $DC(3)$). **10p**

   (b) Generalizaţi problema de mai sus la cazul a $n \geq 3$ criptografi (protocolul va fi notat $DC(n)$). **5p**

   (c) In cadrul protocolului $DC(n)$, $n \geq 3$, presupunem că criptografii C_{i-1} şi C_{i+1} bănuiesc că C_i a plătit masa. Dacă C_{i-1} şi C_{i+1} îşi pun în comun o parte din informaţiile lor private, pot ei stabili dacă C_i a plătit sau nu? Justificaţi răspunsul. (în cadrul notaţiei de mai sus, dacă $i = 1$ atunci $i - 1$ va fi considerat n, iar dacă $i = n$ atunci $i + 1$ va fi considerat 1). **10p**

   (d) Protocolul $DC(n)$ are dezavantajul că dacă un criptograf a plătit masa dar cel puţin un alt criptograf C_i nu este onest în publicarea valorii reale (corecte) z_i, atunci concluzia desprinsă de criptografi poate fi eronată. Justificaţi aceasta. **5p**

Punctajul minim la proba scrisă, pentru promovarea examenului, este de 50p.