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: Feb 15, 2017

Examen

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

   (a) Care sunt operaţiile primitive în cadrul modelului take-grant de control al accesului ? (Specificaţi clar în cadrul fiecărei operaţii tipul părţilor implicate în aceasta (subiect/obiect)). **10p**

   (b) Ce se înţelege prin comandă în cadrul modelului bazat pe matrici de control al accesului? **10p**

   (c) Arătaţi că orice sistem de protecţie take-grant poate fi simulat printr-un sistem de protecţie bazat pe matrici de access al controlului, prin păstrarea proprietăţii de siguranţă (dacă un drept este sigur într-un sistem atunci el este sigur şi în celălalt). **25p**

2. (Distribuţia cheii, IPsec – timp estimat: 40')
   Considerăm următoarea schemă de distribuţie a cheii pentru n utilizatori. Administratorul (TA) alege un număr prim $p > n$, trei coeficienţi $a, b, c \in \mathbf{Z}_p$ (distincţi doi câte doi) şi formează polinomul

   $$f(x, y) = a + b(x + y) + cxy \ mod \ p.$$

   TA distribuie fiecărui utilizator U polinomul

   $$g_U(x) = f(x, r_U) \ mod \ p = a_U + b_U x \ mod \ p,$$

   unde $r_U \in \mathbf{Z}_p$ este un parametru public ales random de U. Polinomul g_U este secret al lui U.
   Doi utilizatori U şi V vor comunica prin intermediul cheii

   $$K_{UV} = g_U(r_V) = f(r_U, r_V) = f(r_V, r_U) = g_V(r_U) = K_{VU}$$

   ce o pot calcula independent.

   (a) Arătaţi că schema este rezistentă la atac de coaliţie 1 (niciun utilizator nu poate determina, cu probabilitate ne-neglijabilă polinomul secret al altui utilizator). **(15p)**

   (b) Este schema rezistentă la atac de coaliţie 2 ? (Justificaţi răspunsul). Dacă schema nu este rezistentă la atac de coaliţie 2, modificaţi-o astfel încât aceasta să fie rezistentă la atac de coaliţie 2. **(20p)**

   (c) Descrieţi o modalitate prin care componenta IKE a protocolului IPsec poate fi modificată prin includerea schemei de la punctul precedent, şi studiaţi securitatea ei. Discutaţi apoi avantajele şi dezavantajele acestei noi metode în comparaţie cu metoda IKE standard. **(20p)**

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