Information Security, 2014–2015

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

Date: Jan 29, 2015

Examen (timp de lucru: 1h40')

1. (sisteme de protecţie – timp estimat: 40')
   (a) Ce este un sistem de protecţie peste o mulţime de drepturi? (definiţi toate conceptele ce intervin în explicarea conceptului de sistem de protecţie) **1.5p**
   (b) In ce constă problema siguranţei sistemelor de protecţie? **1p**
   (c) Ce cunoşteţi despre dificultatea rezolvării algoritmice a problemei siguranţei sistemelor de protecţie? **0.5p**
   (d) Ce este o listă de control al accesului? **0.25p**
   (e) Ce este o listă de capacităţi? **0.25p**
   (f) Ce înţelegeţi prin acces discreţionar şi acces mandatar? **0.5p**

2. (PGP – timp estimat: 30')
   (a) Ce servicii oferă PGP? **0.5p**
   (b) Cum se realizează autentificarea în PGP? **0.5p**
   (c) Cum se asigură confidenţialitatea în PGP? **1p**
   (d) Cum se realizează autentificarea şi confidenţialitatea, împreună, în PGP? **1p**
   (e) Explicaţi modul de formare şi utilizare a inelelor de chei in PGP. **1p**

3. (Managementul cheii – timp estimat: 30')
   Considerăm următoarea metodă de partajare a unei parole $K \in \mathbf{Z}_m$ la n participanţi:
   (a) se aleg random $n-1$ numere $a_1, \ldots, a_{n-1} \in \mathbf{Z}_m$ şi se distribuie (pe un canal secret) la $n-1$ participanti;
   (b) celui de al n-lea participant i se distribuie $(K - \sum_{i=1}^{n-1} a_i)\ mod\ m$.

   Arătaţi urmatoarele:
   (a) Dacă $m > n$ atunci schema este rezistentă la atac de coaliţie $n-1$ (dacă $n-1$ participanţi pun în comun secretele lor parţiale, atunci ei nu obţin nici o informaţie suplimentară asupra cheii partajate); **1.25p**
   (b) Cerinţa ca m să fie prim ar îmbunătăţi schema? Justificaţi răspunsul. **0.25p**
   (c) Rezultatul de la (1) se mai păstrează dacă $m \leq n$? Justificaţi răspunsul. **0.5p**