Information Security, 2016–2017

Instructor: Prof.Dr. Ferucio Laurenţiu Ţiplea
Department of Computer Science
Alexandru Ioan Cuza University of Iaşi
Office: C301
Tel: (0232) 201538

Date: Jan 30, 2017

Examen

1. (Politici de securitate – timp estimat: 40')

   (a) Descrieţi modelul Bell-LaPadula (explicaţi clar fiecare notaţie utilizată). **10p**

   (b) Descrieţi modelul Biba (explicaţi clar fiecare notaţie utilizată). **10p**

   (c) In Figura 1 aveţi două latici de clase de securitate. Utilizaţi una dintre ele pentru a ilustra modelul Bell-LaPadula, iar cealaltă pentru modelul Biba.

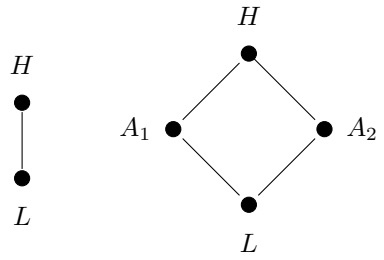

Figure 1: Latici de securitate

5p

   (d) Combinaţi modelele de la punctul anterior într-un singur model şi explicaţi-l. **10p**

2. (DNSsec – timp estimat: 40')
   In Figura 2 aveţi 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 că nodul `example` conţine 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? **3p**

   (b) Care sunt înregistrările introduse de DNSsec? **8p**

   (c) Arătaţi cum se adaugă înregistrările specifice DNSsec arborelui din Figura 2. **8p**

   (d) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.cc.example` **8p**

   (e) Explicaţi cum se obţin proprietăţile de securitate DNSsec pentru rezoluţia `c2.ccc.example` **8p**

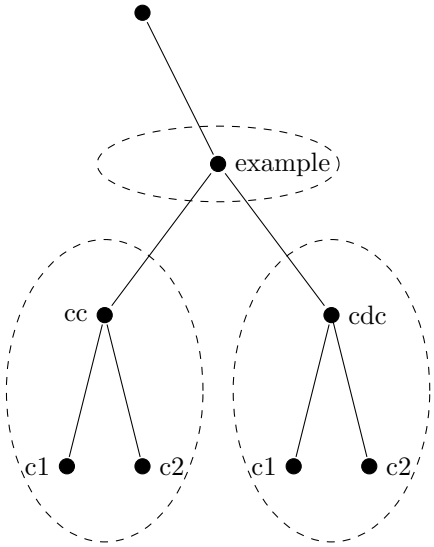

Figure 2: Arbore DNS

3. (IPsec – timp estimat: 40')
   Descriem mai jos un posibil atac asupra modului de operare CBC în IPsec. In acest mod, o secvenţă de blocuri $x = x_1 \cdots x_n$ se criptează cu o cheie K prin $y = y_1 \cdots y_n$, unde $y_1 = e_K(x_1 \oplus x_0)$, x_0 este un vector de iniţializare dat, iar $y_{i+1} = e_k(x_{i+1} \oplus y_i)$ pentru orice $i \geq 1$.

   Constatăm că dacă alterăm un bit în y_2, atunci acelaşi bit va fi alterat în x_3 (la decriptare) deoarece $x_3 = y_2 \oplus d_K(y_3)$. Presupunând că primii 32 biţi din x_3 vor trebui să conţină adresa IP destinaţie, atacantul poate modifica primii 32 biţi ai lui y_2 astfel încât, prin decriptare, primii 32 de biţi ai lui x_3 să conţină adresa atacantului.

   (a) Detaliaţi atacul de mai sus arătând clar cum se poate modifica y_2 (presupunem că atacantul are acces la mesajul criptat). **10p**

   (b) Presupunem că în IPsec modul de criptare CBC se înlocuieşte cu modul de criptare OFB unde $y_i = e_K^i(x_0) \oplus x_i$, pentru orice $i \geq 1$.
   Mai funcţionează atacul de la (a) în acest caz ? **10p**

   (c) Presupunem că în IPsec modul de criptare CBC se înlocuieşte cu modul de criptare CFB unde $y_0 = x_0$ şi $y_i = e_K(y_{i-1}) \oplus x_i$, pentru orice $i \geq 1$.
   Mai funcţionează atacul de la (a) în acest caz ? **10p**

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