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) Cum se realizează autentificarea şi confidenţialitatea în cadrul PGP ? Descrieţi şi modul de administrare a cheilor necesare. **15p**

   (b) Presupunem că în modul "autentificare şi confidenţialitate" în PGP inversăm operaţiile (de autentificare şi confidenţialitate). Crează aceasta vreo problemă relativ la autentificare şi confidenţialitate? Explicaţi aceasta prin comparaţie cu protocolul original. **15p**

   (c) Presupunem că operaţia de autentificare în PGP este realizată doar prin hash. Se păstrează proprietatea de autentificare? Explicaţi aceasta prin comparaţie cu protocolul original. **15p**

2. (IPsec – timp estimat: 40')
   Modul CFB de criptare a unei secvenţe binare x cu un criptosistem pentru care lungimea cheii de criptare, a blocului de intrare şi a celui de ieşire este m, funcţionează astfel:

   - se împarte x în blocuri de lungime r, $x = x_1 \cdots x_n$, unde $1 \leq r \leq m$;
   - se consideră un vector de iniţializare de lungime m;
   - se aplică următorul algoritm ce produce criptotextul y asociat lui x cu cheia K:

     $I_0 := IV$;
     $y_0 := \lambda$; (λ este şirul vid)
     $y := \lambda$;
     `for` $j := 1$ `to` n `do`
         $I_j :=$ ultimii m bits ai lui $I_{j-1}y_{j-1}$
         $z_j :=$ primii r bits ai lui $e_K(I_j)$;
         $y_j := x_j \oplus z_j$;
         $y := yy_j$;
     `end_for`

   (a) Cum se realizează decriptarea în modul CFB? **15p**

   (b) 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. Cum ? **15p**

   (c) Dacă în IPsec se utilizează modul de criptare CFB în locul modului CBC, se mai poate monta atacul de la punctul precedent ? **25p**

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