Information Security, Fall 2015

- **Prof.Dr. Ferucio Laurenţiu Ţiplea**

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

Date: Feb 12, 2016

Examen Final (Restanţă)

1. ($IPsec$)

   (a) Descrieţi, succint dar clar, elementele ce stau la baza arhitecturii $IPsec$ (asociere de securitate, AH, ESP, moduri de utilizare pentru datagrame IPv4). **3p**

   (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? **1p**

   (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? **1p**

2. Presupunem că mesajele transmise prin SSL sunt prelucrate astfel:

   - mesajul este imparţit în blocuri, $B_1, \ldots, B_m$ (fiecare cu cel mult 2^{14} octeţi);
   - pentru fiecare bloc B_i se realizează:
     - se aplică un MAC blocului B_i rezultând X_i;
     - se criptează X_i cu un criptosistem simetric în modul CBC rezultând Y_i;
     - se adaugă un header SSL rezultând Z_i;
     - se transmite Z_i printr-un segment TCP.

   Criptarea primului bloc X_1 se face astfel:

   - se împarte X_1 în blocuri de 64 sau 128 bits (în funcţie de criptosistem), $X_1 = x_1^1 \cdots x_1^{l_1}$;
   - se generează $Y_1 = y_1^1 \cdots y_1^{l_1}$, unde $y_1^1 = e_k(x_1 \oplus y_0)$, y_0 este un vector iniţial, iar $y_1^j = e_K(x_1^j \oplus y_1^{j-1})$, pentru orice $j > 1$.

   Criptarea celorlalte blocuri $X_i = x_i^1 \cdots x_i^{l_i}$ $(i > 1)$ se face ca şi pentru X_1 dar cu deosebirea că y_0 este ales ca fiind $y_{i-1}^{l_{i-1}}$ (ultimul criptotext din blocul anterior).

   (a) Arătaţi că un intrus care are acces la blocurile Y_1 şi X_2 dar nu la X_1, poate decide efectiv dacă un anumit sub-bloc x_1^j coincide sau nu cu un mesaj x^* (de aceeaşi lungime cu x_1^j) ales de intrus (remarcă: funcţia de criptare este injectivă). **2p**

   (b) Dacă un sub-bloc x_1^j conţine o parolă mică, poate fi utilizat rezultatul anterior pentru montarea unui atac prin ghicirea parolei? (puteţi presupune că intrusul poate monta un atac de plaintext ales). **1.5p**

   (c) Cum poate fi îmbunătăţit protocolul pentru a nu mai avea loc proprietatea de la (a)? **1.5p**