Information Security, Fall 2008

- **Prof.Dr. Ferucio Laurenţiu Ţiplea**
- **Lect.Dr. Sorin Iftene**
- **Asist.Prof.Dr. Cătălin Bîrjoveanu**

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

Date: Jan 24, 2009

Examen Final – Soluţii

1. Protocolul de mai jos are ca scop stabilirea unei chei de comunicare între A şi B, utilizând un server de încredere S (e_S este cheia publică a lui S):

$$\begin{array}{llcll} (1) & A \rightarrow S & : & B, \{K_A\}_{e_S} & \text{unde } K_A \text{ este o cheie secretă generată de } A \\ (2) & S \rightarrow B & : & A & \\ (3) & B \rightarrow S & : & A, \{K_B\}_{e_S} & \text{unde } K_B \text{ este o cheie secretă generată de } B \\ (4) & S \rightarrow A & : & B, \{K_B\}_{K_A} & \end{array}$$

K_B va fi cheia utilizată în comunicare de A şi B.

(a) Arătaţi că există un atac prin care un intrus poate obţine cheia K_B. **15p**

Soluţie: Intrusul I impersonifică pe A (abreviat $I(A)$):

$$\begin{array}{llcll} (1) & I(A) \rightarrow S & : & B, \{K_I\}_{e_S} & \text{unde } K_I \text{ este o cheie secretă generată de } I \\ (2) & S \rightarrow B & : & A & \\ (3) & B \rightarrow S & : & A, \{K_B\}_{e_S} & \text{unde } K_B \text{ este o cheie secretă generată de } B \\ (4) & S \rightarrow I(A) & : & B, \{K_B\}_{K_I} & \end{array}$$

(b) Arătaţi că există un atac prin care un intrus poate impune o cheie generată de el. **15p**

Soluţie: Intrusul I impersonifică pe B (abreviat $I(B)$):

$$\begin{array}{llcll} (1) & A \rightarrow S & : & B, \{K_A\}_{e_S} & \text{unde } K_A \text{ este o cheie secretă generată de } A \\ (2) & S \rightarrow I(B) & : & A & \\ (3) & I(B) \rightarrow S & : & A, \{K_I\}_{e_S} & \text{unde } K_I \text{ este o cheie secretă generată de } I \\ (4) & S \rightarrow A & : & B, \{K_I\}_{K_A} & \end{array}$$

(c) Arătaţi că există un atac prin care un intrus poate obţine cheia K_B în timp ce A obţine şi el aceeaşi cheie de comunicare K_B. **15p**

Soluţie: Aceasta este o "combinaţie" a primelor două:

$$\begin{array}{llcll} (1) & I(A) \rightarrow S & : & B, \{K_I\}_{e_S} & \text{unde } K_I \text{ este o cheie secretă generată de } I \\ (2) & S \rightarrow B & : & A & \\ (3) & B \rightarrow S & : & A, \{K_B\}_{e_S} & \text{unde } K_B \text{ este o cheie secretă generată de } B \\ (4) & S \rightarrow I(A) & : & B, \{K_B\}_{K_I} & \\ (5) & A \rightarrow S & : & B, \{K_A\}_{e_S} & \text{unde } K_A \text{ este o cheie secretă generată de } A \\ (6) & S \rightarrow I(B) & : & A & \\ (7) & I(B) \rightarrow S & : & A, \{K_B\}_{e_S} & \\ (8) & S \rightarrow I(A) & : & B, \{K_B\}_{K_A} & \end{array}$$

2. Presupunem că ESP în modul transport încapsulează segmente TCP, iar aceste segmente sunt criptate în modul CBC. Dacă un intrus are acces (citire şi modificare) la vectorul de iniţializare IV al modului de criptare, poate acesta monta un atac cu succes? Discutaţi toate variantele posibile ce credeţi că pot conduce la atac, şi argumentaţi-le cât mai riguros. **25p**

   Notă: Structura unui segment TCP este cea de mai jos:

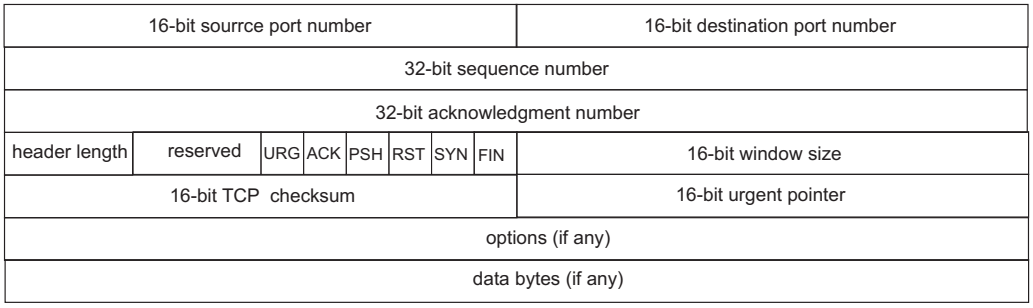

Figure 1: TCP segment format

Soluţie: (schiţă) Primii 64 bits ai headerului TCP conţin adresa destinaţie. Dacă intrusul are acces la IV (citire/modificare), atunci el poate modifica IV astfel încât să se rescrie adresa destinaţie printr-o adresă pe care el o poate controla. O astfel de modificare nu afectează modul de criptare/decriptare şi nici rezultatul decriptării, exceptând faptul că adresa destinaţie va fi cea dată de intrus. In acest fel, intrusul obţine mesajul original.

Şi modificări ale câmpurilor ce conţin numărul de secvenţă sau dimensiunea ferestrei pot cauza anomalii (chiar dacă acestea nu sunt la fel de puternice ca atacul de mai sus).

Punctajul minim la proba scrisă, pentru promovarea examenului, este de 25p.