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

1. Protocolul de mai jos are ca scop obţinerea unei chei simetrice de comunicare între A şi B şi, totodată, obţinerea de către A a unui ticket de la B prin care ulterior se va putea autentifica către B. Cheia este distribuită de un server de încredere S (N_a, N_b şi N_b' sunt nonce-uri, K_{AS} este o cheie partajată de A şi S, K_{BS} este o cheie partajată de B şi S, K_B este o cheie cunoscută doar de B, iar T_B este o stampilă de timp generată de B):

$$\begin{array}{lll}
(1) & A \rightarrow B & : A, N_a \\
(2) & B \rightarrow S & : A, N_a, B, N_b \\
(3) & S \rightarrow B & : \{N_b, A, K_{AB}\}_{K_{BS}}, \{N_a, B, K_{AB}\}_{K_{AS}} \qquad (K_{AB} \text{ este generată de } S) \\
(4) & B \rightarrow A & : \{N_a, B, K_{AB}\}_{K_{AS}}, \{T_b, A, K_{AB}\}_{K_B}, N_b', \{N_a\}_{K_{AB}} \\
(5) & A \rightarrow B & : \{N_b'\}_{K_{AB}}
\end{array}$$

K_{AB} va fi cheia utilizată în comunicare de A şi B, iar $\{T_b, A, K_{AB}\}_{K_B}$ este ticketul eliberat de B lui A pentru autentificare ulterioară.

Atunci când A se autentifică către B, el va aplica următorul protocol de autentificare (N_a' şi N_b'' sunt nonce-uri):

$$\begin{array}{lll}
(1') & A \rightarrow B & : N_a', \{T_b, A, K_{AB}\}_{K_B} \\
(2') & B \rightarrow A & : N_b'', \{N_a'\}_{K_{AB}} \\
(3') & A \rightarrow B & : \{N_b''\}_{K_{AB}}
\end{array}$$

(a) Arătaţi că un intrus poate folosi protocolul de autentificare pentru a cripta orice mesaj mic (de dimensiunea unui nonce) cu cheia partajată doar de A şi B (fără a cunoşte această cheie). **15p**

Soluţie: Intrusul I impersonifică pe A (abreviat $I(A)$) şi alege mesajul M pe care îl doreşte criptat cu K_{AB}:

$$\begin{array}{lll}
(1') & I(A) \rightarrow B & : M, \{T_b, A, K_{AB}\}_{K_B} \\
(2') & B \rightarrow I(A) & : N_b'', \{M\}_{K_{AB}}
\end{array}$$

(b) Arătaţi că, în ipoteza în care B acceptă să ruleze protocolul de autentificare cu mai mulţi clienţi în acelaşi timp (inclusiv cu un acelaşi client de mai multe ori în paralel), atunci un intrus se poate autentifica cu succes. **15p**

Soluţie: Intrusul I impersonifică pe A (abreviat $I(A)$) în două rulări ale protocolului de autentificare (prima rulare are eticheta $r1$, iar a doua, $r2$):

$$\begin{array}{lll}
(r1.1') & I(A) \rightarrow B & : N_I, \{T_b, A, K_{AB}\}_{K_B} \\
(r1.2') & B \rightarrow I(A) & : N_b'', \{N_I\}_{K_{AB}} \\
(r2.1') & I(A) \rightarrow B & : N_b'', \{T_b, A, K_{AB}\}_{K_B} \\
(r2.2') & B \rightarrow I(A) & : N_b''', \{N_b''\}_{K_{AB}} \\
(r1.3') & B \rightarrow I(A) & : \{N_b''\}_{K_{AB}}
\end{array}$$

(a se observa modul de interpletire a celor două rulări).

(c) Cum poate fi prevenit atacul de la (b)? **15p**

Soluţie: O modalitate de prevenire a atacului de la (b) ar fi ca B să nu permită ca un nonce utilizat într-o rulare să fie folosit şi în alta. De exemplu, nonce-ul N_b'' din prima rulare este utilizat în cea de a doua rulare pentru ca intrusul să îl obţină criptat şi să poată apoi încheia prima rulare a protocolului cu succes.

2. Presupunem că ESP în modul transport încapsulează pachete UDP, 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 pachet UDP este cea de mai jos:

16-bit sourrce port number	16-bit destination port number
UDP length	16-bit UDP checksum
data bytes (if any)	

Figure 1: UDP packet format

Ultimele două câmpuri au următoarea semantică:

- UDP length = the number of bytes comprising the combined UDP header information and payload data;
- UDP checksum = a checksum to verify that the end to end data has not been corrupted by routers or bridges in the network or by the processing in an end system.

Soluţie: (schiţă) Primii 64 bits ai headerului UDP 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 câmpului "UDP length" 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.