Information Security, Fall 2007

- **Prof.Dr. Ferucio Laurentiu Tiplea**
- **Asist.Prof.Dr. Cătălin Bîrjoveanu**

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

Date: Feb 16, 2008

Examen Final – Soluţii

1. Protocolul de mai jos (datorat lui Woo şi Lam) are scopul de a mijloci autentificarea unui client A către un alt client B prin intermediul unui server S (în protocol, $\{x\}_K$ înseamnă x criptat cu K, iar K_{XY} reprezintă cheia partajată de X şi Y):

$$\begin{array}{llcl} (1) & A \rightarrow B & : & A \\ (2) & B \rightarrow A & : & N_b \\ (3) & A \rightarrow B & : & \{N_b\}_{K_{AS}} \\ (4) & B \rightarrow S & : & \{A, B, \{N_b\}_{K_{AS}}\}_{K_{BS}} \\ (5) & S \rightarrow B & : & \{A, B, N_b\}_{K_{BS}} \end{array}$$

   (a) Explicaţi modul în care funcţionează protocolul (furnizaţi cât mai multe detalii convingătoare asupra realizării obiectivului acestuia). **7p**

   Soluţie: La solicitarea de autentificare iniţiată de A la pasul 1, A primeşte un nonce ce va fi folosit ca element de verificare a identităţii (pasul 2). A răspunde cu nonce-ul primit, criptat cu cheia K_{AS} (această cheie este cunoscută doar de A şi serverul S şi, deci, exceptând S, numai A poate să producă mesajul de la pasul 3). B va verifica identitatea lui A solicitând serverului S să decripteze $\{N_b\}_{K_{AS}}$, cu cheia partajată de el cu A (pasul 4). In urma decriptării, B va accepta demonstraţia de identitate a lui A numai dacă elementul obţinut prin decriptare de către server este chiar nonce-ul ales de B la pasul 2 (aceasta deoarece, exceptând serverul, numai A ar fi putut să cripteze N_b prin $\{N_b\}_{K_{AS}}$). Serverul S este autoritate de încredere, iar comunicaţia dintre el şi B este securizată prin criptare.

   (b) Se ştie că acest protocol este vulnerabil la atac prin interpunerea unui intrus între participanţii la protocol. Prezentaţi un astfel de atac. **7p**

   Soluţie: Notăm prin $I(X)$ intrusul I ce impersonifică X. Un atac asupra protocolului Woo-Lam este următorul:

$$\begin{array}{llcl} (1) & I(A) \rightarrow B & : & A \\ (2) & B \rightarrow I(A) & : & N_b \\ (3) & I(A) \rightarrow B & : & N_b \\ (4) & B \rightarrow I(S) & : & \{A, B, N_b\}_{K_{BS}} \\ (5) & I(S) \rightarrow B & : & \{A, B, N_b\}_{K_{BS}} \end{array}$$

   Impersonificând pe A, intrusul nu criptează nonce-ul N_b la pasul 3 pentru ca apoi, prin impersonificarea serverului, intrusul să poată returna lui B chiar mesajul trimis de B, mesaj ce conţine N_b necriptat. In esenţă, intrusul evită criptarea lui N_b care ar constitui metodă de verificare a identităţii şi, ca urmare, va trebui să impersonifice serverul pentru a nu-l lăsa pe acesta să decripteze N_b cu K_{AS} (ceea ce ar produce un mesaj diferit de N_b).

2. Schema Fiat-Shamir de identificare are următoarea descriere:

   - **Stabilirea parametrilor.** Se generează două numere prime distincte p şi q, se calculează $n = pq$ şi se alege un parametru de securitate t. Numerele p şi q sunt secrete, iar n şi t sunt publice;
   - **Alegerea unei valori de identificare.** Entitatea A alege un parametru secret $s \in \mathbf{Z}_n^*$ şi face publică valoarea $v = (s^2)^{-1} \ mod \ n$ (se ştie că este intractabil a determina s cunoscând v şi n);

- **Protocolul de identificare.** Dacă A doreşte să se identifice faţă de B, atunci el va repeta de t ori următorul protocol:

  (1) A alege aleator un număr r, calculează $x = r^2 \ mod \ n$ şi trimite x lui B;

  (2) B alege aleator un bit $b \in \{0, 1\}$ şi îl trimite lui A;

  (3) A calculează $y = rs^b \ mod \ n$ şi trimite y lui B;

  (4) dacă $y^2 v^b \not\equiv x \ mod \ n$ atunci B respinge demonstraţia de identitate a lui A şi abortează protocolul.

  Dacă protocolul nu a fost abortat în nici una din cele t iteraţii atunci, după ultima iteraţie, B acceptă demonstraţia de identitate a lui A.

Arătaţi următoarele:

(a) Dacă A şi B urmează întocmai schema Fiat-Shamir, atunci B va accepta demonstraţia de identitate a lui A. **7p**

Soluţie: B acceptă demonstraţia de identitate a lui A dacă în fiecare din cele t iteraţii este verificată congruenţa $y^2 v^b \equiv x \ mod \ n$ (r, x, b şi y depind de iteraţie). Insă, dacă A şi B urmează protocolul, această congruenţă este satisfăcută deoarece:

$$\begin{aligned} y^2 v^b &\equiv (rs^b)^2((s^2)^{-1})^b \ mod \ n \\ &\equiv r^2 \ mod \ n \\ &\equiv x \ mod \ n \end{aligned}$$

(b) Dacă în două iteraţii distincte ale protocolului entitatea A generează acelaşi parametru r inversabil modulo n, iar B generează biţi diferiţi (în pasul (2)) în aceste iteraţii, atunci orice intrus care poate obţine informaţiile ce circulă între A şi B poate determina parametrul secret s al lui A în timp polinomial determinist. **12p**

Soluţie: Presupunem că, pentru un acelaşi r inversabil modulo n, la iteraţia a i-a se alege $b = 0$ şi, deci, se răspunde cu $y_0 = r \ mod \ n$, iar la iteraţia a j-a ($j \neq i$) se alege $b = 1$ şi, deci, se răspunde cu $y_1 = rs \ mod \ n$. Atunci,

$$s = y_1 y_0^{-1} \ mod \ n$$

Cum inversul modular şi înmulţirea modulară se realizează în timp $\mathcal{O}((\log n)^3)$, deducem că s se poate determina în timp polinomial determinist.

(c) Orice terţă parte C se poate identifica către B ca fiind A cu probabilitatea $1/2^t$. **17p**

Soluţie: Fie C o terţă parte ce rulează protocolul cu B, încercând să se identifice drept A.

La pasul 1, C alege arbitrar un număr y şi un bit b, calculează $x = y^2 v^b \ mod \ n$ (v este public) şi trimite x lui B. Dacă C primeşte la pasul 2 chiar bitul b, atunci el va răspunde la pasul 3 cu y şi, implicit, congruenţa $y^2 v^b \equiv x \ mod \ n$ va fi satisfăcută. Ca urmare, B nu va aborta protocolul într-o astfel de iteraţie. Dacă acest lucru va putea fi repetat de t ori în secvenţă, atunci B va accepta demonstraţia de identitate a lui C (pe care îl va crede ca fiind A). Probabilitatea ca B să aleagă la o iteraţie exact bitul b ales anterior de C este $1/2$. Probabilitatea ca aceasta să se întâmple de t ori la rând este $1/2^t$, ceea ce încheie demonstraţia.

Soluţie alternativă (teoretică): bitul 0 este trimis de t ori la rând (în practică, nici un generator aleator nu va face aceasta).

Punctajul minim la proba scrisă, pentru promovarea examenului, este de 20p.