

- Prof.Dr. Ferucio Laurentiu Tiplea
- Asist.Prof.Dr. Cătălin Birjoveanu

Department of Computer Science
 “Al.I.Cuza” University of Iași
 C 301
 Tel: (0232) 201538

Date: Feb 16, 2008

Examen Final – Soluții

1. Protocolul de mai jos (datorat lui Woo și 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 și Y):

- (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) $S \rightarrow B$: $\{A, B, N_b\}_{K_{BS}}$

- (a) Explicați modul în care funcționează protocolul (furnizați cât mai multe detalii convingătoare asupra realizării obiectivului acestuia). 7p

Soluție: La solicitarea de autentificare inițiată de A la pasul 1, A primește un nonce ce va fi folosit ca element de verificare a identității (pasul 2). A răspunde cu nonce-ul primit, criptat cu cheia K_{AS} (această cheie este cunoscută doar de A și serverul S și, 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). În urma decriptării, B va accepta demonstrația de identitate a lui A numai dacă elementul obținut 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 creeze N_b prin $\{N_b\}_{K_{AS}}$). Serverul S este autoritate de încredere, iar comunicația dintre el și B este securizată prin criptare.

- (b) Se știe că acest protocol este vulnerabil la atac prin interpunerea unui intrus între participanții la protocol. Prezentați un astfel de atac. 7p

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

- (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) $I(S) \rightarrow B$: $\{A, B, N_b\}_{K_{BS}}$

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 conține N_b necriptat. În esență, intrusul evită criptarea lui N_b care ar constitui metodă de verificare a identității și, 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 și q , se calculează $n = pq$ și se alege un parametru de securitate t . Numerele p și q sunt secrete, iar n și t sunt publice;
- **Alegerea unei valori de identificare.** Entitatea A alege un parametru secret $s \in \mathbf{Z}_n^*$ și face publică valoarea $v = (s^2)^{-1} \bmod n$ (se știe că este intractabil să determine s cunoscând v și n);

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

- (1) A alege aleator un număr r , calculează $x = r^2 \bmod n$ și trimite x lui B ;
- (2) B alege aleator un bit $b \in \{0, 1\}$ și îl trimite lui A ;
- (3) A calculează $y = rs^b \bmod n$ și trimite y lui B ;
- (4) dacă $y^2 v^b \neq x \bmod n$ atunci B respinge demonstrația de identitate a lui A și abortează protocolul.

Dacă protocolul nu a fost abortat în nici una din cele t iterații atunci, după ultima iterație, B acceptă demonstrația de identitate a lui A .

Arătați următoarele:

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

Soluție: B acceptă demonstrația de identitate a lui A dacă în fiecare din cele t iterații este verificată congruența $y^2 v^b \equiv x \bmod n$ (r, x, b și y depind de iterație). Inșă, dacă A și B urmează protocolul, această congruență este satisfăcută deoarece:

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

- (b) Dacă în două iterații distincte ale protocolului entitatea A generează același parametru r inversabil modulo n , iar B generează biți diferiți (în pasul (2)) în aceste iterații, atunci orice intrus care poate obține informațiile ce circulă între A și B poate determina parametrul secret s al lui A în timp polinomial determinist. 12p

Soluție: Presupunem că, pentru un același r inversabil modulo n , la iterația a i -a se alege $b = 0$ și, deci, se răspunde cu $y_0 = r \bmod n$, iar la iterația a j -a ($j \neq i$) se alege $b = 1$ și, deci, se răspunde cu $y_1 = rs \bmod n$. Atunci,

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

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

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

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

La pasul 1, C alege arbitrar un număr y și un bit b , calculează $x = y^2 v^b \bmod n$ (v este public) și trimite x lui B . Dacă C primește la pasul 2 chiar bitul b , atunci el va răspunde la pasul 3 cu y și, implicit, congruența $y^2 v^b \equiv x \bmod n$ va fi satisfăcută. Ca urmare, B nu va aborta protocolul într-o astfel de iterație. Dacă acest lucru va putea fi repetat de t ori în secvență, atunci B va accepta demonstrația de identitate a lui C (pe care îl va crede ca fiind A). Probabilitatea ca B să aleagă la o iterație 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 demonstrația.

Soluție 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.