Échange de Clés Authentifiées Résistant aux Attaques par Dictionnaire

Mihir Bellare

mihir@cs.ucsd.edu

Dept. of Computer Science
& Engineering
UCSD

David Pointcheval

David.Pointcheval@info.unicaen.fr

GREYC
Dépt d'Informatique
Université de Caen

Plan

- Introduction
- Attaque de SPEKE
- Modèle de Sécurité
- Nouvelle Proposition
- Sécurité Exacte
- Extensions

Introduction

Authentification :

- mot de passe « classique »$\Longrightarrow$ problème du ¡¡rejeu¿¿
- protocole « zero-knowledge »
  $\Longrightarrow$ secret de longue taille à mémoriser
  $\Longrightarrow$ stockage sur un support (sécurisé)

Souhait :

mot de passe π (mémorisable) avec question–réponse
$\Longrightarrow$ danger : attaques par « dictionnaire »

Authentification Mutuelle Client–Serveur :

- symétrique : ils partagent π
- asymétrique : le client possède π, le serveur $f(\pi)$

$\Longrightarrow$ se prouvent mutuellement leur connaissance

- résistance aux attaques par dictionnaire :
  les informations échangées ne permettent pas
  à un adversaire passif ou actif de retrouver π
  par une recherche « exhaustive »et « off-line »

Échange de Clés :

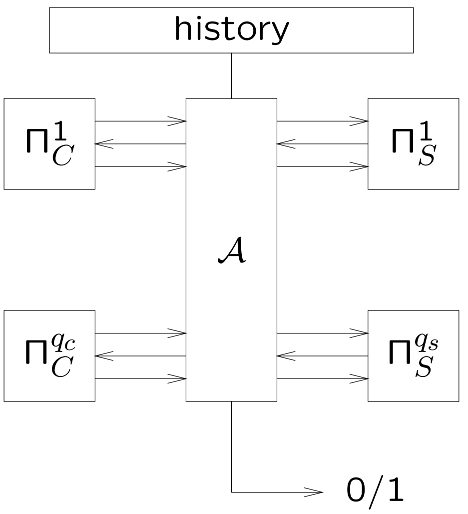
Propriété « forward secrecy » :
la compromission de π ne remet pas en cause
la confidentialité passée.

SPEKE

Client		Serveur
	g élément de $\left(\mathbb{Z}/p\mathbb{Z}\right)^\star$ d'ordre q	
$x \stackrel{R}{\longleftarrow} \mathbb{Z}/q\mathbb{Z}$ $X \longleftarrow (g^\pi)^x \bmod p$	$\xrightarrow{\quad X \quad}$	
	$\xleftarrow{\quad Y \quad}$	$y \stackrel{R}{\longleftarrow} \mathbb{Z}/q\mathbb{Z}$ $Y \longleftarrow (g^\pi)^y \bmod p$
$K \longleftarrow h(Y^x \bmod p)$ $V_1 \longleftarrow h(h(K))$	$\xrightarrow{\quad V_1 \quad}$	
	$\xleftarrow{\quad V_2 \quad}$	$K' \longleftarrow h(X^y \bmod p)$ $V_1 \stackrel{?}{=} h(h(K'))$ $V_2 \longleftarrow h(K')$
$V_2 \stackrel{?}{=} h(K)$		
	K : clé commune de session SK	

Un « faux »serveur peut obtenir $(X = (g^\pi)^x, y, Y = g^y, V_1 = h(h(h(Y^x))))$.
Alors $V_1 = h(h(h(X^{y/\pi})))$: π peut être retrouvé.

Modèle de Sécurité



- l'adversaire observe « passivement » q_p authentifications
- l'adversaire interagit
  - q_c fois avec le client
  - q_s fois avec le serveur

  avec 3 types de questions :
  - de façon « normale »
  - demandant de « révéler » la clé de session en cours
  - demandant une « devinette » : il lui est retourné a,
    - soit la clé de session,
    - soit une clé aléatoire
- il doit deviner ce que a représente avec un avantage non-négligeable :

$$\Pr[\mathcal{A} \to 1 \mid a = SK] - \Pr[\mathcal{A} \to 1 \mid a = r].$$

Nouvelle Proposition

Client		Serveur
	p et q grands premiers tels que $p = 2q + 1$	
	g élément de $\left(\mathbb{Z}/p\mathbb{Z}\right)^\star$ d'ordre q	
	$E_k : \langle g \rangle \longrightarrow \langle g \rangle$, pour tout $k \in \mathcal{K}$	
	$h : \{0,1\}^\star \longrightarrow \{0,1\}^\ell$	
$x \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ $X \longleftarrow g^x \bmod p$ $Z_1 \longleftarrow E_\pi(X)$	$\xrightarrow{\quad Z_1 \quad}$	
		$y \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$ $Y \longleftarrow g^y \bmod p$ $Z_2 \longleftarrow E_\pi(Y)$ $K \longleftarrow X^y \bmod p$ $V_2 \longleftarrow h(K, X, Y, 2)$
	$\xleftarrow{\quad Z_2, V_2 \quad}$	
$K \longleftarrow Y^x \bmod p$ $V_2 \stackrel{?}{=} h(K, X, Y, 2)$ $V_1 \longleftarrow h(K, X, Y, 1)$	$\xrightarrow{\quad V_1 \quad}$	
		$V_1 \stackrel{?}{=} h(K, X, Y, 1)$
	$SK = h(K)$: clé commune de session	

Sécurité Exacte

Notations :

- $Q = q_c + q_s$
- $S = \#\{\text{mots de passe}\}$

Résultat :

Après Q interactions,
$\mathcal{A}$ ne peut répondre à la « devinette »
avec un avantage supérieur à Q/S (environ).

Conséquences

- Les observations « passives »ne révèlent rien
- chaque attaque « active »ne permet à l'attaquant que d'éliminer, de la liste des mots de passe possibles, le mot de passe essayé
  $\Longrightarrow$ ce résultat est optimal.

Remarques

- La compromission d'une clé de session ne met pas en danger le système (ni passé, ni futur)
  = « révélation »de clé de session
- La compromission du mot de passe π ne met pas en danger les clés de session antérieures
  L'Hypothèse Diffie-Hellman les protège.

Diffie-Hellman

Calculatoire

Étant donnés $X = g^x$ et $Y = g^y$,
il est difficile de calculer $Z = g^{xy}$

Décisionnel

Il est difficile de distinguer les distributions suivantes :

$\mathcal{D} = \{(X = g^x, Y = g^y, Z = g^{xy}) \,|\, x, y \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}\}$

$\mathcal{R} = \{(X = g^x, Y = g^y, Z = g^z) \,|\, x, y, z \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}\}$

Preuve du Résultat (idée)

Modèle de l'Oracle Aléatoire

- h est une fonction aléatoire
- E_k est une permutation aléatoire pour toute clé

Méthode

utiliser un attaquant $\mathcal{A}$ contre notre schéma
pour construire un distingueur Δ entre $\mathcal{R}$ et $\mathcal{D}$:
avantage de $\mathcal{A}$, $\varepsilon \geq Q/S + \alpha$
$\Longrightarrow$ avantage de Δ supérieur à $\alpha/4$
(avec des temps d'exécution similaires)

Distinction entre $\mathcal{R}$ et $\mathcal{D}$

- Soit (A, B, C) un triplet provenant de $\mathcal{R}$ ou de $\mathcal{D}$
- Toutes les interactions sont simulées
  en dérivant les triplets (X, Y, K) du triplet (A, B, C) :
  $x, y \xleftarrow{R} \mathbb{Z}/q\mathbb{Z}$,
  $X \longleftarrow A \cdot g^x$, $Y \longleftarrow B \cdot g^y$ et $K = C \cdot A^y \cdot B^x \cdot g^{xy}$
- $\mathcal{A}$ gagne si
  - il renvoie un message chiffré par E_π } S
  - il pose une question $(K, X, Y, *)$ à h } S
  - il répond correctement à la « devinette ». } $\overline{\text{S}}$
- Lorsque $\mathcal{A}$ gagne, Δ répond 1 $(= \mathcal{D})$
  Sinon, il lance une pièce

Avantage de $\mathcal{A}$:

$$\varepsilon = Adv = \mathsf{Pr}[\mathsf{S}] \cdot Adv[\mathsf{S}] + \mathsf{Pr}[\overline{\mathsf{S}}] \cdot Adv[\overline{\mathsf{S}}]$$

$(A, B, C) \longleftarrow \mathcal{R}$

- $\mathcal{A}$ renvoie un chiffré par E_π avec probabilité égale à (environ) Q/S ;
- $\mathcal{A}$ pose une question $(K, X, Y, *)$ à h avec probabilité inférieure à q_h/q
- $\mathcal{A}$ répond à la « devinette »avec probabilité 1/2

$(A, B, C) \longleftarrow \mathcal{D}$

- $\mathcal{A}$ répond à la « devinette »avec avantage ε.

Échange de Clés Authentifiées Résistant aux Attaques par Dictionnaire

$$\begin{aligned}
\mathsf{pr}[1] &= \mathsf{pr}[\mathsf{S}] + \mathsf{pr}[\overline{\mathsf{S}}] \times \begin{pmatrix} (\mathsf{pr}[1 \,|\, SK \wedge \overline{\mathsf{S}}] + \frac{1}{2} \cdot \mathsf{pr}[0 \,|\, SK \wedge \overline{\mathsf{S}}]) \cdot \mathsf{pr}[SK \,|\, \overline{\mathsf{S}}] \\ + \; (\mathsf{pr}[0 \,|\, r \wedge \overline{\mathsf{S}}] + \frac{1}{2} \cdot \mathsf{pr}[1 \,|\, r \wedge \overline{\mathsf{S}}]) \cdot \mathsf{pr}[r \,|\, \overline{\mathsf{S}}] \end{pmatrix} \\
&= \mathsf{pr}[\mathsf{S}] + \frac{1}{2} \times \mathsf{pr}[\overline{\mathsf{S}}] \times \left(\frac{3}{2} + \frac{1}{2} \cdot (\mathsf{pr}[1 \,|\, SK \wedge \overline{\mathsf{S}}] - \mathsf{pr}[1 \,|\, r \wedge \overline{\mathsf{S}}]) \right) \\
&= \frac{3}{4} + \frac{1}{4} \times \left(\mathsf{pr}[\mathsf{S}] + \mathsf{pr}[\overline{\mathsf{S}}] \cdot \mathsf{Adv}[\overline{\mathsf{S}}] \right)
\end{aligned}$$

$$\begin{aligned}
\mathsf{pr}_{\mathcal{R}}[1] &\leq \frac{3}{4} + \frac{1}{4} \cdot \mathsf{pr}_{\mathcal{R}}[\mathsf{S}] \leq \frac{3}{4} + \frac{1}{4} \cdot \left(\frac{Q}{S} + \frac{q_h}{q}\right) \\
\mathsf{pr}_{\mathcal{D}}[1] &\geq \frac{3}{4} + \frac{1}{4} \cdot Adv \geq \frac{3}{4} + \frac{1}{4} \cdot \varepsilon
\end{aligned}$$

Avantage de $\triangle$: $Adv_\triangle \geq \frac{1}{4} \cdot \left(\varepsilon - \frac{Q}{S} - \frac{q_h}{q} \right)$.

Extensions

Authentification Mutuelle Asymétrique

- Le client possède π
- Le serveur possède $v = f(\pi)$

Technique :

- Preuve mutuelle de connaissance de v
- Le client prouve sa connaissance de π tel que $v = f(\pi)$ (Signature ajoutée au dernier tour).

Exemple :

- π : mot de passe
- $x_S = h(\pi, S)$, secret de C lié au serveur S
- $y_S = g^{x_S}$, secret de $S \longrightarrow \pi_S = h(y_S)$
- Preuve mutuelle de connaissance de π_S
- Au dernier tour, C ajoute une signature de X, Y, K avec sa clé secrète x_S liée à la clé publique y_S (signature Schnorr)

Conclusion

- authentification mutuelle symétrique/asymétrique
- résistance aux attaques par dictionnaire
- mise en accord de clé « forward secrecy »

Utilité :

- mise en accord de clé « sure »
  basée sur la connaissance d'un simple mot de passe
- remplacerait avantageusement Kerberos