

Sécurité des systèmes informatiques

L'identification

Olivier Markowitch

L'identification

Mécanisme permettant à un *vérificateur* de s'assurer interactivement de l'identité d'un *prouveur*

L'identification est nécessaire au contrôle d'accès (prévention), mais aussi à la réalisation de fichier de logging (détection et réaction)

Ambiguïté dans le vocabulaire : identification, intégrité, authentification (d'entités et de données)

Propriétés

Le vérificateur Bob ne peut réutiliser les informations reçues du prouveur, Alice, pour *impersonnaliser* cette dernière auprès de Charles (un vérificateur tiers)

La preuve de l'identité ne devrait donc pas être *transférable*

La probabilité qu'Oscar puisse se faire passer pour Alice auprès de Bob doit être négligeable

Identification faible

Identification basée sur :

- les mots de passe, éventuellement associés à S/Key
- au schéma de Lamport
- message authentication code

Identification faible

Identification basée sur :

- les mots de passe, éventuellement associés à S/Key
- au schéma de Lamport
- message authentication code : le prouveur transmet $r, h_k(r)$ où k est un secret partagé et r une valeur changeant à chaque identification

Identification forte

L'identification forte est aussi appelée *challenge-response*

Le prouveur prouve sa connaissance d'un secret au vérificateur sans pour autant le révéler

A chaque session d'identification, le vérificateur pose une question différente (un challenge) au prouveur, à laquelle ce dernier répond grâce à la connaissance de son secret (response)

Identification forte (suite)

Challenge-response basé sur :

- le chiffrement symétrique
(identification unilatérale ou mutuelle)

Identification basé sur ch. sym.

- Identification unilatérale

Identification basé sur ch. sym.

– Identification unilatérale

$$V \rightarrow P : r_V$$

Identification basé sur ch. sym.

- Identification unilatérale
 $V \rightarrow P : r_V$ (challenge)

Identification basé sur ch. sym.

- Identification unilatérale
 - $V \rightarrow P : r_V$ (challenge)
 - $P \rightarrow V : E_k(r_V)$

Identification basé sur ch. sym.

– Identification unilatérale

$V \rightarrow P : r_V$ (challenge)

$P \rightarrow V : E_k(r_V)$ (response)

Identification basé sur ch. sym.

- Identification unilatérale
 - $V \rightarrow P : r_V$ (challenge)
 - $P \rightarrow V : E_k(r_V)$ (response)
- Identification mutuelle

Identification basé sur ch. sym.

- Identification unilatérale
 - $V \rightarrow P : r_V$ (challenge)
 - $P \rightarrow V : E_k(r_V)$ (response)

- Identification mutuelle
 - $V \rightarrow P : r_V$

Identification basé sur ch. sym.

- Identification unilatérale

$V \rightarrow P : r_V$ (challenge)

$P \rightarrow V : E_k(r_V)$ (response)

- Identification mutuelle

$V \rightarrow P : r_V$

$P \rightarrow V : E_k(r_V, r_P)$

Identification basé sur ch. sym.

- Identification unilatérale

$V \rightarrow P : r_V$ (challenge)

$P \rightarrow V : E_k(r_V)$ (response)

- Identification mutuelle

$V \rightarrow P : r_V$

$P \rightarrow V : E_k(r_V, r_P)$

$V \rightarrow P : E_k(r_P, r_V)$

Identification forte (suite)

Challenge-response basé sur :

- le chiffrement symétrique
(identification unilatérale ou mutuelle)
- les fonctions à sens unique avec clés
(exemple : SKID3)

Identification sur base de MAC

- Identification unilatérale
 - $V \rightarrow P : r_V$ (challenge)
 - $P \rightarrow V : h_k(r_V)$ (response)

Identification sur base de MAC

- Identification unilatérale

$V \rightarrow P : r_V$ (challenge)

$P \rightarrow V : h_k(r_V)$ (response)

- Identification mutuelle

$V \rightarrow P : r_V$

$P \rightarrow V : r_P, h_k(r_V, r_P)$

$V \rightarrow P : h_k(r_P, r_V)$

Identification sur base de MAC

- Identification unilatérale

$V \rightarrow P : r_V$ (challenge)

$P \rightarrow V : h_k(r_V)$ (response)

- Identification mutuelle : **SKID3**

$V \rightarrow P : r_V$

$P \rightarrow V : r_P, h_k(r_V, r_P)$

$V \rightarrow P : h_k(r_P, r_V)$

Identification forte (suite)

Challenge-response basé sur :

- le chiffrement symétrique
(identification unilatérale ou mutuelle)
- les fonctions à sens unique avec clés
(exemple : SKID3)
- le chiffrement asymétrique
(exemple Needham-Schroeder)

Identification basé sur ch. asym.

– Identification unilatérale

$$V \rightarrow P : E_{K_P}(r)$$

Identification basé sur ch. asym.

– Identification unilatérale

$V \rightarrow P : E_{K_P}(r)$ (challenge)

Identification basé sur ch. asym.

– Identification unilatérale

$V \rightarrow P : E_{K_P}(r)$ (challenge)

$P \rightarrow V : r$

Identification basé sur ch. asym.

– Identification unilatérale

$V \rightarrow P : E_{K_P}(r)$ (challenge)

$P \rightarrow V : r$ (response)

Identification basé sur ch. asym.

- Identification unilatérale

$V \rightarrow P : E_{K_P}(r)$ (challenge)

$P \rightarrow V : r$ (response)

- Identification mutuelle : Needham-Schroeder

$P \rightarrow V : E_{K_V}(r_1, P)$

Identification basé sur ch. asym.

- Identification unilatérale

$V \rightarrow P : E_{K_P}(r)$ (challenge)

$P \rightarrow V : r$ (response)

- Identification mutuelle : Needham-Schroeder

$P \rightarrow V : E_{K_V}(r_1, P)$

$V \rightarrow P : E_{K_P}(r_1, r_2)$

Identification basé sur ch. asym.

- Identification unilatérale

$V \rightarrow P : E_{K_P}(r)$ (challenge)

$P \rightarrow V : r$ (response)

- Identification mutuelle : Needham-Schroeder

$P \rightarrow V : E_{K_V}(r_1, P)$

$V \rightarrow P : E_{K_P}(r_1, r_2)$

$P \rightarrow V : r_2$

Needham-Schroeder

$$P \rightarrow V : E_{K_V}(r_1, P)$$

Needham-Schroeder

$$P \rightarrow V : E_{K_V}(r_1, P)$$

$$V \rightarrow V' : E_{K_{V'}}(r_1, P)$$

Needham-Schroeder

$$P \rightarrow V : E_{K_V}(r_1, P)$$

$$V \rightarrow V' : E_{K_{V'}}(r_1, P)$$

$$V' \rightarrow V : E_{K_P}(r_1, r_2)$$

Needham-Schroeder

$$P \rightarrow V : E_{K_V}(r_1, P)$$

$$V \rightarrow V' : E_{K_{V'}}(r_1, P)$$

$$V' \rightarrow V : E_{K_P}(r_1, r_2)$$

$$V \rightarrow P : E_{K_P}(r_1, r_2)$$

Needham-Schroeder

$$P \rightarrow V : E_{K_V}(r_1, P)$$

$$V \rightarrow V' : E_{K_{V'}}(r_1, P)$$

$$V' \rightarrow V : E_{K_P}(r_1, r_2)$$

$$V \rightarrow P : E_{K_P}(r_1, r_2)$$

$$P \rightarrow V : r_2$$

Needham-Schroeder

$$P \rightarrow V : E_{K_V}(r_1, P)$$

$$V \rightarrow V' : E_{K_{V'}}(r_1, P)$$

$$V' \rightarrow V : E_{K_P}(r_1, r_2)$$

$$V \rightarrow P : E_{K_P}(r_1, r_2)$$

$$P \rightarrow V : r_2$$

$$V \rightarrow V' : r_2$$

Needham-Schroeder corrigé

$$P \rightarrow V : E_{K_V}(r_1, P)$$

$$V \rightarrow P : E_{K_P}(V, r_1, r_2)$$

$$P \rightarrow V : r_2$$

Needham-Schroeder corrigé

$$P \rightarrow V : E_{K_V}(r_1, P)$$

$$V \rightarrow V' : E_{K_{V'}}(r_1, P)$$

$$V' \rightarrow V : E_{K_P}(V', r_1, r_2)$$

$$V \rightarrow P : E_{K_P}(V', r_1, r_2)$$

$$P \rightarrow V : \text{STOP}$$

Protocole sans apport d'information

Résolution sur mesure du problème d'identification au cours d'un *protocole de preuve interactive*

Un protocole de preuve interactive peut être consistant (complete) et significatif (sound), le protocole est alors appelé *preuve de connaissance*

Protocole sans apport d'information

Un protocole de preuve interactive est consistant si, étant donné un prouveur et un vérificateur honnêtes, le vérificateur accepte la preuve du prouveur avec une probabilité proche de 1

Un protocole de preuve interactive est significatif si la probabilité de réussir à convaincre à tort un vérificateur est négligeable, et sinon (si cette probabilité n'est pas négligeable) cela implique que le faux prouveur connaît le secret du prouveur qu'il impersonnalise

Protocole sans apport d'information

Un protocole de preuve de connaissance peut respecter la propriété *d'apport nul de connaissance* (zero-knowledge property), le protocole est alors dit *simulable*

Un protocole de preuve de connaissance respecte la propriété d'apport nul de connaissance s'il existe un algorithme polynomial en temps, appelé le simulateur qui, sans interactions avec le prouveur, peut produire des outputs résultant de l'assertion à prouver qui sont indistinguables des outputs qui seraient issus des interactions avec le prouveur. Le protocole est alors dit simulable

En pratique

Protocoles d'identification de :

- Fiat-Shamir (basé sur le problème de la factorisation)
- Guillou-Quisquater (basé sur le problème RSA)
- Schnorr (basé sur le problème du logarithme discret)

Fiat-Shamir : les prémices

Une autorité :

- choisit deux premiers secrets p et q (RSA)
- calcule la valeur publique $n = pq$

Chaque prouveur :

- choisit un s secret tel que $s \in [1, n - 1]$ est premier avec n
- calcule la valeur publique $v = s^2 \pmod n$

Fiat-Shamir : l'identification

1. le prouveur choisit un nombre aléatoire r dans l'intervalle $[1, n - 1]$, calcule $x = r^2 \pmod n$, et envoie x au vérificateur
2. le vérificateur choisit un bit e aléatoire et l'envoie au prouveur
3. le prouveur calcule $y = r \cdot s^e \pmod n$ et l'envoie au vérificateur
4. si $y \neq 0$ et si $y^2 \equiv x \cdot v^e \pmod n$ alors le vérificateur accepte l'identification

Ces étapes sont réalisées t fois de suite

Fiat-Shamir : consistant

Le prouveur envoie :

$$y \equiv rs^e \pmod{n}$$

La vérification :

$$y^2 \equiv r^2s^{2e} \pmod{n}$$

$$y^2 \equiv xv^e \pmod{n}$$

Fiat-Shamir : significatif

Si un opposant arrive à s'identifier, de manière répétée, avec une probabilité non négligeable alors ce n'est pas en devinant e . Il arrive donc à construire des réponses y ayant « la bonne forme ».

Supposons que cet opposant construise, lors de deux identifications, deux réponses, y_1 et y_2 , à deux questions distinctes, $e_1 = 1$ et $e_2 = 0$, en utilisant le même r dans la construction de la réponse.

Nous avons : $y_1 = rs$ et $y_2 = r$, et donc $\frac{y_1}{y_2} = s$ le secret.

Fiat-Shamir : simulable

Le simulateur choisit aléatoirement un y et calcule :

- $x = y^2 \pmod n$ pour répondre à la question $e = 0$, et
- $x = y^2 v^{-1} \pmod n$ pour répondre à la question $e = 1$.

Nous avons ainsi une simulation basée sur une connaissance préalable des questions (des challenges).

Fiat-Shamir : exemple

Soit $n = 11 \cdot 7 = 77$.

Soient $s = 31$ et donc $v \equiv 31^2 \equiv 37 \pmod{77}$.

1. Soient $r = 21$, $x \equiv 21^2 \equiv 56 \pmod{77}$

$P \rightarrow V : 56$

2. Soit $e = 1$

$V \rightarrow P : 1$

3. $y \equiv rs^e \equiv 21 \cdot 31 \equiv 35 \pmod{77}$

$P \rightarrow V : 35$

4. $y^2 \equiv 35^2 \equiv 70 \pmod{77}$ et

$xv^e \equiv 56 \cdot 37 \equiv 70 \pmod{77}$

Guillou-Quisquater : les prémices

Une autorité :

- choisit deux premiers secrets p et q
- calcule la valeur publique $n = pq$
- choisit le paramètres de sécurité public b : un premier de 40 bits
- calcule a secret tel que $a \cdot b \equiv 1 \pmod{\phi(n)}$
- calcule u sur base de l'identité du prouveur :
$$u = (h(ID_{\text{prouveur}}))^{-a} \pmod{n}$$
- transmet u au prouveur

Guillou-Quisquater : l'identification

1. le prouveur choisit aléatoirement $k \in [0, n - 1]$, calcule $\gamma = k^b \pmod n$ et envoie γ et $ID_{prouveur}$ au vérificateur
2. le vérificateur calcule $v = h(ID_{prouveur})$, choisit un nombre aléatoire $r \in [0, b - 1]$ et envoie r au prouveur
3. le prouveur calcule $y = k \cdot u^r \pmod n$ et envoie y au vérificateur
4. si $\gamma \equiv v^r \cdot y^b \pmod n$, le vérificateur accepte l'identification

Guillou-Quisquater : consistant

Notons $h_{ID_P} = h(ID_{prouveur})$

Le vérificateur vérifie :

$$v^r y^b \equiv (h_{ID_P})^r k^b u^{rb} \pmod{n}$$

$$v^r y^b \equiv (h_{ID_P})^r \gamma (h_{ID_P})^{-rab} \pmod{n}$$

$$v^r y^b \equiv (h_{ID_P})^r \gamma (h_{ID_P})^{-r} \pmod{n}$$

$$v^r y^b \equiv \gamma \pmod{n}$$

Quillou-Quisquater : significatif

Un opposant qui arrive à s'identifier avec une probabilité non négligeable construit des réponses y ayant « la bonne forme ». Supposons que cet opposant produise deux réponses distinctes et correctes, y_1 et y_2 , aux questions distinctes r_1 et r_2 , et ce sur base du même k . Nous avons alors :

$$\gamma \equiv v^{r_1} y_1^b \equiv v^{r_2} y_2^b \pmod{n}$$

$$v^{r_1 - r_2} \equiv \left(\frac{y_2}{y_1}\right)^b \pmod{n} \text{ (avec } r_1 > r_2\text{)}$$

Calculons $t = (r_1 - r_2)^{-1} \pmod{b}$
(car $0 < r_1 - r_2 < b$ et b premier)

$$v^{(r_1 - r_2)t} \equiv \left(\frac{y_2}{y_1}\right)^{bt} \pmod{n}$$

Notons $(r_1 - r_2)t = lb + 1$ donc : $v \equiv \left(\frac{y_2}{y_1}\right)^{bt} v^{-lb} \pmod{n}$

Soit $c = b^{-1} \pmod{\phi(n)}$ et calculons $v^c \equiv \left(\frac{y_2}{y_1}\right)^{cbt} v^{-cbl} \pmod{n}$

Nous obtenons : $u^{-1} \equiv \left(\frac{y_2}{y_1}\right)^t v^{-l} \pmod{n}$

Et donc : $u \equiv \left(\frac{y_1}{y_2}\right)^t v^l \pmod{n}$

Guillou-Quisquater : simulable

Le simulateur connaît r , v et b . Il choisit aléatoirement y et calcule :

$$\gamma \equiv v^r y^b \pmod{n}$$

Nous avons ainsi une simulation basée sur une connaissance préalable des questions r (des challenges).

Guillou-Quisquater : exemple

Soient $n = 7 \cdot 11 = 77$, $b = 37$ et
 $h(ID_{\text{prouveur}}) = 23$.

Nous avons $a \equiv b^{-1} \equiv 13 \pmod{60}$ ($\phi(n) = 60$) et
 $u \equiv 23^{-13} \equiv 23^{60-13} \equiv 23^{47} \equiv 67 \pmod{77}$

1. Soient $k = 11$, $\gamma \equiv 11^{37} \equiv 11 \pmod{77}$
 $P \rightarrow V : 11$
2. Soit $r = 13$
 $V \rightarrow P : 13$
3. $y \equiv 11 \cdot 67^{13} \equiv 11(67^6)^2 67 \equiv 44 \pmod{77}$
 $P \rightarrow V : 44$
4. $h(ID_{\text{prouveur}})^r y^b \equiv 23^{13} 44^{37} \equiv 11 \pmod{77}$
et $\gamma = 11$

Schnorr : les prémices

Une autorité choisit :

- un grand premier public p d'au-moins 512 bits
- un grand facteur premier public q de $p - 1$ (d'au-moins 140 bits)
- un élément public $\alpha \in \mathbb{Z}_p^*$ d'ordre q
- un paramètre public de sécurité t tel que $q > 2^t$

Chaque prouveur choisit aléatoirement un secret $a \in [0, q - 1]$ et calcule $v = \alpha^{-a} \bmod p$ qui est publique

Schnorr : l'identification

1. le prouveur choisit aléatoirement $k \in [0, q - 1]$, calcule $\gamma = \alpha^k \pmod{p}$ et envoie γ au vérificateur
2. le vérificateur choisit aléatoirement $r \in [1, 2^t]$ et l'envoie au prouveur
3. le prouveur calcule $y = k + a \cdot r \pmod{q}$ et envoie y au vérificateur
4. si $\gamma \equiv \alpha^y \cdot v^r \pmod{p}$, le vérificateur accepte l'identification

Schnorr : consistant

Le vérificateur vérifie :

$$\alpha^y v^r \equiv \alpha^k \alpha^{ar} \alpha^{-ar} \pmod{p}$$

$$\alpha^y v^r \equiv \alpha^k \pmod{p}$$

$$\alpha^y v^r \equiv \gamma \pmod{p}$$

Schnorr : significatif

Un opposant qui arrive à s'identifier avec une probabilité non négligeable construit donc des réponses y ayant « la bonne forme ». Supposons que cet opposant produise deux réponses distinctes et correctes, y_1 et y_2 , aux questions distinctes r_1 et r_2 , et ce sur base du même k .

Nous avons alors :

$$\gamma \equiv \alpha^{y_1} v^{r_1} \equiv \alpha^{y_2} v^{r_2} \pmod{p}$$

$$\alpha^{y_1 - y_2} \equiv v^{r_2 - r_1} \pmod{p}$$

$$y_1 - y_2 \equiv a(r_1 - r_2) \pmod{q}$$

Comme $|r_1 - r_2| < 2^t$ et q est un premier $> 2^t$, nous avons $\text{pgcd}(r_1 - r_2, q) = 1$ et donc :

$$a \equiv (y_1 - y_2)(r_1 - r_2)^{-1} \pmod{q}$$

Schnorr : simulable

Le simulateur connaît r , α et v . Il choisit aléatoirement y et calcule :

$$\gamma \equiv \alpha^y v^r \pmod{p}$$

Nous avons ainsi une simulation basée sur une connaissance préalable des questions r (des challenges).

Schnorr : exemple

Soient $p = 31$, $q = 5$, $g = 3$ un générateur de \mathbb{Z}_{31}^* ,
 $t = 3$, $a = 3$ et $ID_{\text{prouveur}} = 11$

Soit α un élément de \mathbb{Z}_{31}^* d'ordre q :

$$\alpha \equiv g^{\frac{p-1}{q}} \equiv 3^6 \equiv 16 \pmod{31}$$

Nous avons $v \equiv 16^{-3} \equiv 16^{30-3} \equiv 8 \pmod{31}$

1. Soient $k = 2$ et $\gamma \equiv 16^2 \equiv 8 \pmod{31}$

$$P \rightarrow V : 8$$

2. Soit $r = 4$

$$V \rightarrow P : 4$$

3. $y \equiv 2 + 3 \cdot 4 \equiv 4 \pmod{5}$

$$P \rightarrow V : 4$$

4. $\alpha^y v^r \equiv 16^4 8^4 \equiv 8 \equiv \gamma \pmod{31}$