Preuve à divulgation nulle de connaissance

Ludovic PATEY

6 janvier 2010

Sommaire

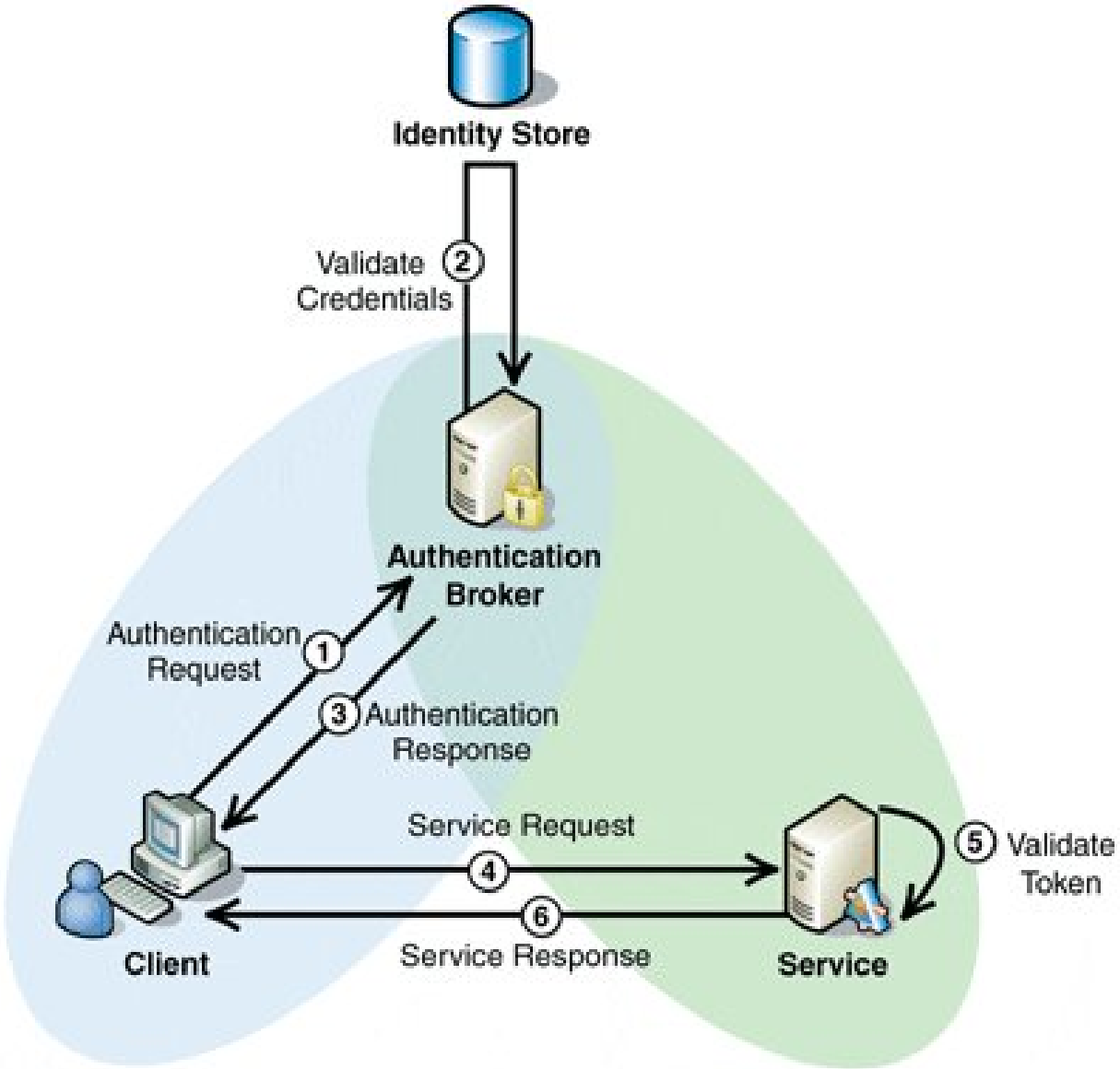
1. Introduction
2. Système de preuve interactive
3. Système de preuve à divulgation nulle de connaissance
4. Protocole de Fiat et Shamir
5. Conclusion

Introduction

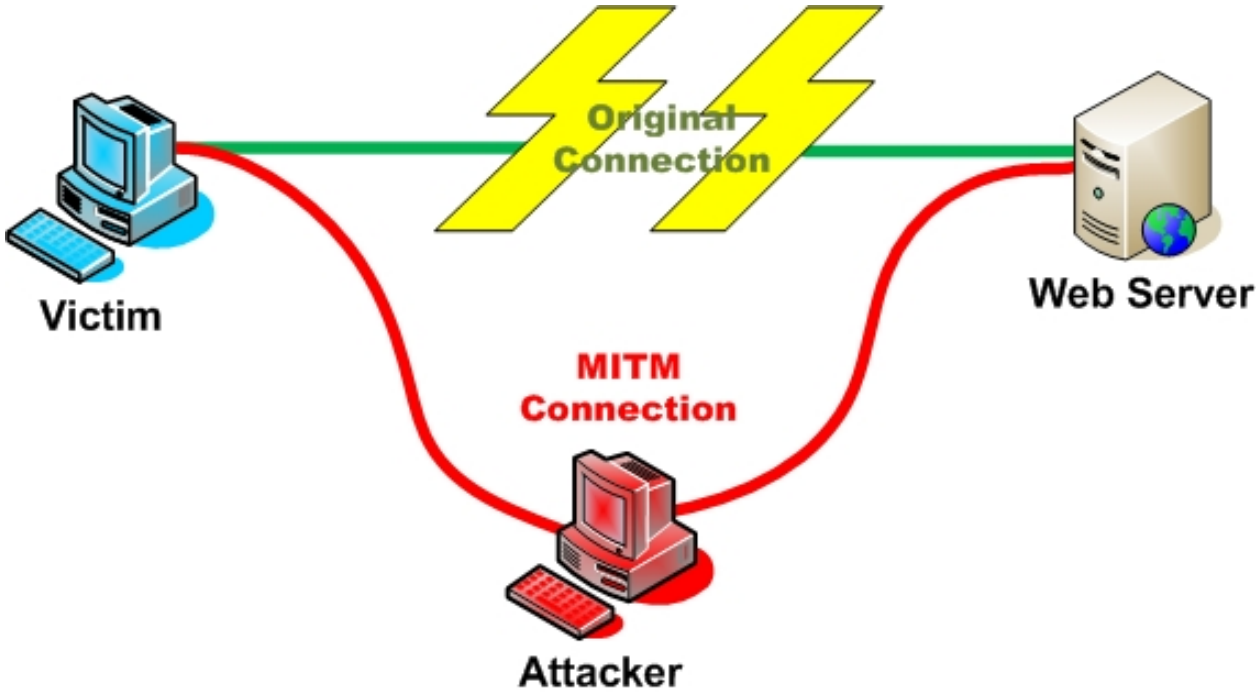
Contexte historique :

- Développement des nouvelles technologies
- Nécessité de sécuriser les communications
- Prouver son identité à une entité non fiable

Exemple : l'authentification



Exemple : l'authentification. Man in the middle



On est dans la m..élasse

Nécessité de trouver une solution qui

- permette de prouver la connaissance d'un secret
- ne dévoile pas le contenu du secret

... les système de preuve interactives de connaissances à divulgation nulle de connaissance.

Système de preuve interactive

Modèle : Machine de Turing

Nécessité d'une modélisation des entités... les machines de Turing.
Formellement, un 7-uplet $(\Sigma, Q, \sigma, \delta, \Delta, q_0, F)$ où

- Σ est un ensemble de symboles appelé *alphabet*, comprenant un symbole particulier noté $\#$.
- Q est un ensemble non vide fini d'états.
- $\sigma : Q \times \Sigma \to \Sigma$ est une fonction d'*impression*.
- $\delta : Q \times \Sigma \to Q$ est une fonction de *transition*.
- $\Delta : Q \times \Sigma \to \{-1, 1\}$ est une fonction de *déplacement*.

Une machine de Turing dispose en outre d'un ruban de mémoire infinie.

Machine de Turing interactive

Variante de la machine de Turing :

- Un ruban des données initiales, accessible en lecture seule.
- Un ruban de travail, accessible en lecture et écriture.
- Un ruban aléatoire ω_M suivant une distribution uniforme.
- Un ruban de communication IN, en lecture seule.
- Un ruban de communication OUT en écriture seule.

Machine de Turing interactive

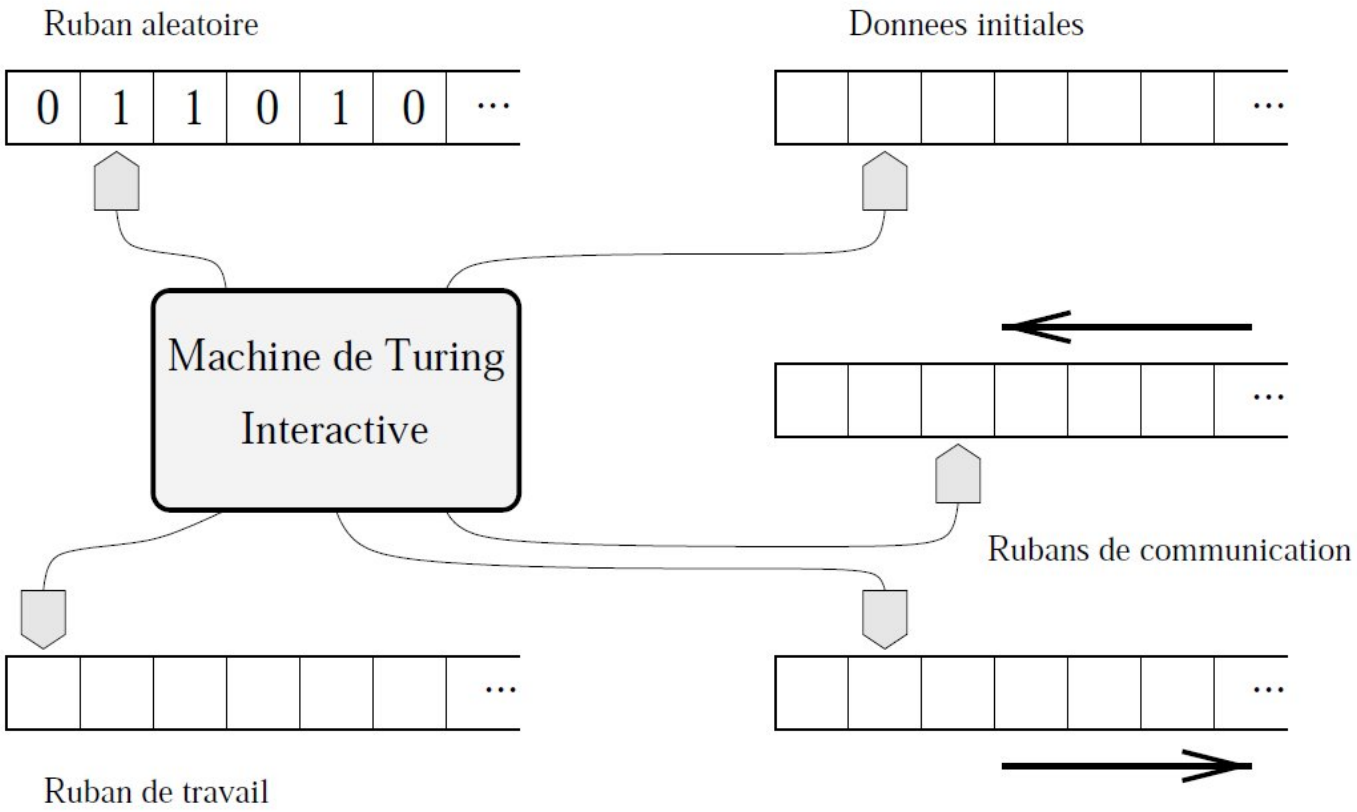


FIGURE: Machine de Turing interactive

Le ruban aléatoire

Le ruban aléatoire contient un ensemble infini de symboles différents de #, ce qui n'est pas sensé être le cas avec les rubans d'une machine de Turing normale.

Protocole interactif

Protocole interactif :

- Deux machines de Turing interactives
- Actives tour à tour
- Rubans de communication partagés
- Le vérifieur *accepte* ou *rejette* la preuve

Protocole interactif

La machine B (vérifieur) doit agir en temps polynomial.

Preuves de connaissance

- Ruban supplémentaire contenant le secret
- La machine A (prouveur) doit également être polynomiale

Système de preuve interactive de connaissance

Définition

*Un **système de preuve interactive de connaissance** est un protocole interactif entre un prouveur A et un vérifieur B tel que :*

- *pour tout entier k et pour tout I suffisamment grand tel que $P(I, S)$ est satisfiable, A disposant d'un témoin S convainc B avec une probabilité supérieure à $1 - |I|^{-k}$, les probabilités étant calculées sur le contenu des rubans aléatoires ω_A et ω_B (on dit que la preuve est **consistante**).*

$$\forall k \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall I \in \{I / \exists S\ P(I, S) \wedge |I| \geq n_0\}$$

$$\text{Pro}\left[A \text{ connaissant } S \text{ convainc } B\right] \geq 1 - \frac{1}{|I|^k}$$

Système de preuve interactive de connaissance

Définition

Et tel que :

- *pour tout entier k, il existe une machine de Turing probabiliste agissant en un temps polynomial en fonction de $|I|$ notée M telle que, pour toute machine de Turing interactive $\tilde{A}$ et pour tout entier k', si $\tilde{A}$ convainc B avec une donnée initiale I suffisamment grande avec probabilité supérieure à $|I|^{-k}$, alors M produit S tel que $P(I,S)$ en interrogeant $\tilde{A}$ avec une probabilité supérieure à $1-\frac{1}{[I]^k}$ (on dit que la preuve est **significative**).*

$$\forall k \in \mathbb{N}\ \exists M \forall \tilde{A}\ \forall k' \in \mathbb{N}\ \exists n_0 \in \mathbb{N}\ \forall I \in \{I/|I| \geq n_0\}$$

$$\text{Pro}\left[\tilde{A} \text{ convainc } B \text{ dela connaissance de } S \text{ tel que } P(I,S)\right] \geq \frac{1}{|I|^k}$$

$$\Rightarrow \text{Pro}\left[M \text{ produit } S \text{ tel que } P(I,S)\right] \geq 1 - \frac{1}{|I|^{k'}}$$

Système de preuve interactive de connaissance

Ne requiert pas qu'aucune information ne soit transmise au vérifieur.

Divulgation nulle de connaissance

Système de preuve interactive à divulgation nulle de connaissance.

Indistinguabilité de variables aléatoires

Définition

Soient $U(m)$ et $V(m)$ deux familles de variables aléatoires paramétrées par les mots d'un langage $\mathcal{L}$.

- *Si, pour tout $m \in \mathcal{L}$, on ne peut pas distinguer deux distributions, quelles que soient la taille des échantillons et la puissance de calcul du juge, on dira que les variables aléatoires sont* ***parfaitement indistinguables****.*
  D'un point de vue formel :

$$\forall m \in \mathcal{L}\ U(m) = V(m)$$

Indistinguabilité de variables aléatoires

Définition

- *Si, pour tout $m \in \mathcal{L}$, on ne peut pas distinguer deux distributions en ne voyant qu'un nombre polynomial d'éléments, on dira que les variables aléatoires sont* ***statistiquement indistinguables****.*

$$\sum_{\alpha \in \{0,1\}^*} |\Pr[U(m) = \alpha] - \Pr[V(m) = \alpha]| \leq \frac{1}{|m|^k}$$

- *Si, pour tout $m \in \mathcal{L}$, on ne peut pas distinguer en temps polynomial (et par conséquent en ne voyant qu'un nombre polynomial d'éléments) deux distributions, on dira que les variables aléatoires sont* ***calculatoirement indistinguables****.*

Variables aléatoires approximables

Définition

Une famille de variables aléatoires $U(m)$ sur un langage $\mathcal{L}$ est dite ***parfaitement*** *(resp.* ***statistiquement***, ***calculatoirement****)* ***approximable*** *s'il existe une machine de Turing M non-déterministe, fonctionnant un un temps moyen polynomial, telle que $U(m)$ et $M(m)$ soient parfaitement (resp. statistiquement, calculatoirement) indistinguables.*

Vue du vérifieur

Le vérifieur accède à

- la donnée I sur le ruban de données initiales
- toutes les interactions de la preuve (Historique H)

Nous pouvons définie la vue $\text{Vue}_{A,\tilde{B}}$

Système de preuve à divulgation nulle de connaissance

Définition

Un système de preuve interactif (A, B) *de connaissance du prédicat* $P(I, S)$ *est dit* ***parfaitement*** *(resp.* ***statistiquement, calculatoirement)*** ***à divulgation nulle de connaissance*** *si pour tout vérifieur* $\tilde{B}$*, la famille de variables aléatoires* $\text{Vue}_{A,\tilde{B}}(I, H)$ *est parfaitement (resp. statistiquement, calculatoirement) approximable sur* $\mathcal{L} = \left\{(I, H) | I \in L \text{ et } |H| \leq |I|^k\right\}$ *pour tout entier* k *fixé.*

Protocole de Fiat et Shamir

FIGURE: Protocole de Fiat et Shamir

Protocole de Fiat et Shamir

Paramètre : n un entier
Donnée secrète : $S \in \mathbb{Z}_n{}^*$
Donnée initiale : $I = S^2 \bmod n$

Répéter ℓ fois :

Prouveur		Vérifieur
$r \in_R \mathbb{Z}_n{}^*$		
$x = r^2 \bmod n$	$\xrightarrow{x}$	
	$\xleftarrow{e}$	$e \in_R \{0, 1\}$
$y = r \times S^e \bmod n$	$\xrightarrow{y}$	vérifier $y^2 \stackrel{?}{=} x \times I^e \bmod n$

FIGURE: Protocole de Fiat et Shamir

Le système de preuve et les probas

La preuve est probabiliste : $\frac{1}{2^l}$

Que se passerait-il

- si e était déterministe ?
- si on retournait les deux résultats

De la théorie à une application pratique

Application directe pour l'authentification

Conclusion

Les systèmes de preuve interactive de connaissance à divulgation nulle de connaissance sont

- longs à prononcer
- à résultat probabiliste
- directement applicables à la vie quotidienne

Pour aller plus loin


A. Fiat and A.Shamir. *How To Prove Yourself : Practical Solutions to Identification and Signature Problems* (1987).


Guillaume Poupard. *Authentification d'Entités, de Messages et de Clés Cryptographiques : Théorie et Pratique*. Thèse de Doctorat de l'École Polytechnique, 2000.


Oded Goldreich. *Foundations of Cryptography : Basic Tools*. 2007