CHRONOS

Etude et mise en place
d'un système d'horodatage sécurisé

http://recherche.iaai.fr/chronos

Les équipes

- Mont de Marsan : Alban Gabillon
  - JJ. Bascou, K. Bilbech(Doc)
- Toulon : Sami Harari
  - C. Prissette, L. Enel, L. Poinsot(Doc)
- Marseille : Alexis Bonnecaze
  - E. Godard, P. Liardet, T. Tanzi

Qu'est ce que l'horodatage?

- Authentification de documents électroniques
  - Signature : qui est le propriétaire?
  - Horodatage : dater le document
- Horodatage
  - D a été créé dans un intervalle de temps [t0,t1] :

  Datation absolue
  - D a été créé après D0 et avant D1 :

  Datation relative
- Principales applications
  - Commerce et notariat électroniques
  - Sécurité

Le projet CHRONOS

Buts :

- Développer la recherche dans le domaine
- Développement et déploiement d’un prototype paramétrable
- Agrément gouvernemental (LEN)
- Standards européens (EESSI,NESSIE)

Fonctionnement

- Alice construit l'**empreinte** h(D)
- Alice envoie h(D) à **l'autorité d'horodatage** (TSA)
- La TSA renvoie à Alice le certificat d'horodatage, appelé cachet, qui a été construit par lui grâce à un **protocole d'horodatage** particulier
- Le vérifieur se procure D et le cachet et utilise le **protocole de vérification** associé au protocole d'horodatage

La TSA doit être fiable, de confiance et disponible

Les risques possibles

- Défaillances matérielles ou logicielles
- Attaques malveillantes
  - Déni de service
  - Man in the middle
  - Perte de contrôle du serveur
  - Compromission de la clé

Techniques actuelles

- Les schémas de liaison

Hn

Autorité d'horodatage

Ln=(tn-1, IDn-1, Hn-1, H(Ln-1))

$S = sig_{TSS}(n, tn, IDn , Hn, Ln)$

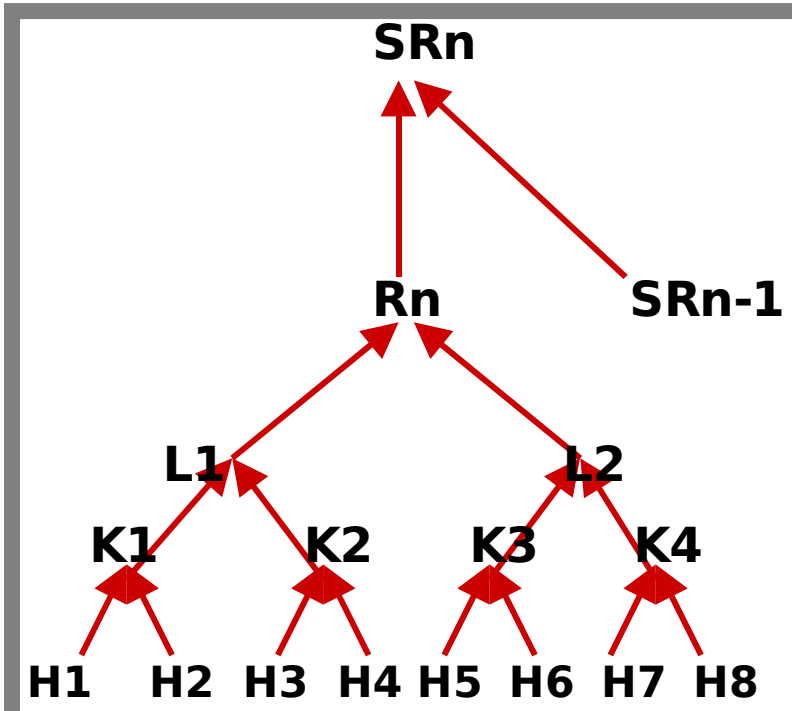
Avantage

Minimise la confiance dans la TSA

Inconvénients

- Ne répond pas à un problème de déni de service
- Nécessite de mémoriser beaucoup d'infos
- Vérification longue et délicate, dépendant linéairement du nombre de cachets

Autre schéma de liaison : par arbre binaire (Merkle, 1980)



Les requêtes reçues durant un tour sont combinées ensemble dans un arbre binaire.

Avantages

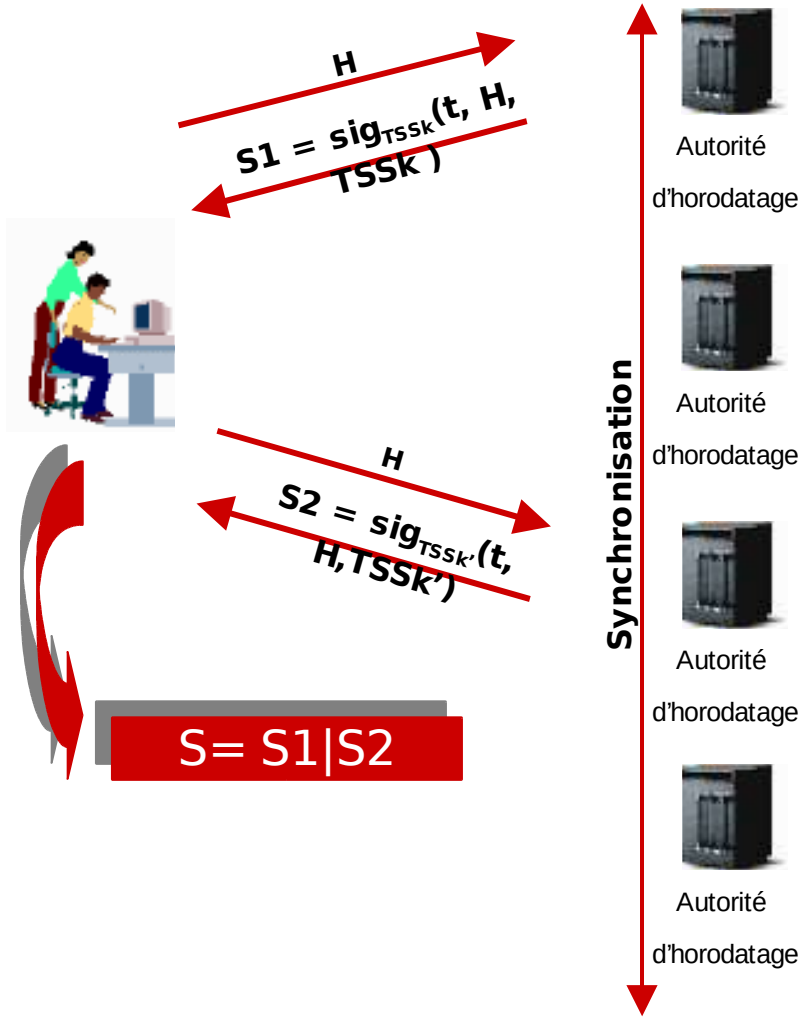
- Il faut mémoriser moins d'infos
- Vérification plus facile

Inconvénients

- Ne répond pas à un déni de service
- Le nombre de requêtes doit approcher une puissance de 2
- Temps relatif
- Publication dans un journal

S= (t, SRn, chemin de Hi à SRn, SRn-1)

Modèle Distribué (1)



Modèle distribué

n serveurs en parallèle

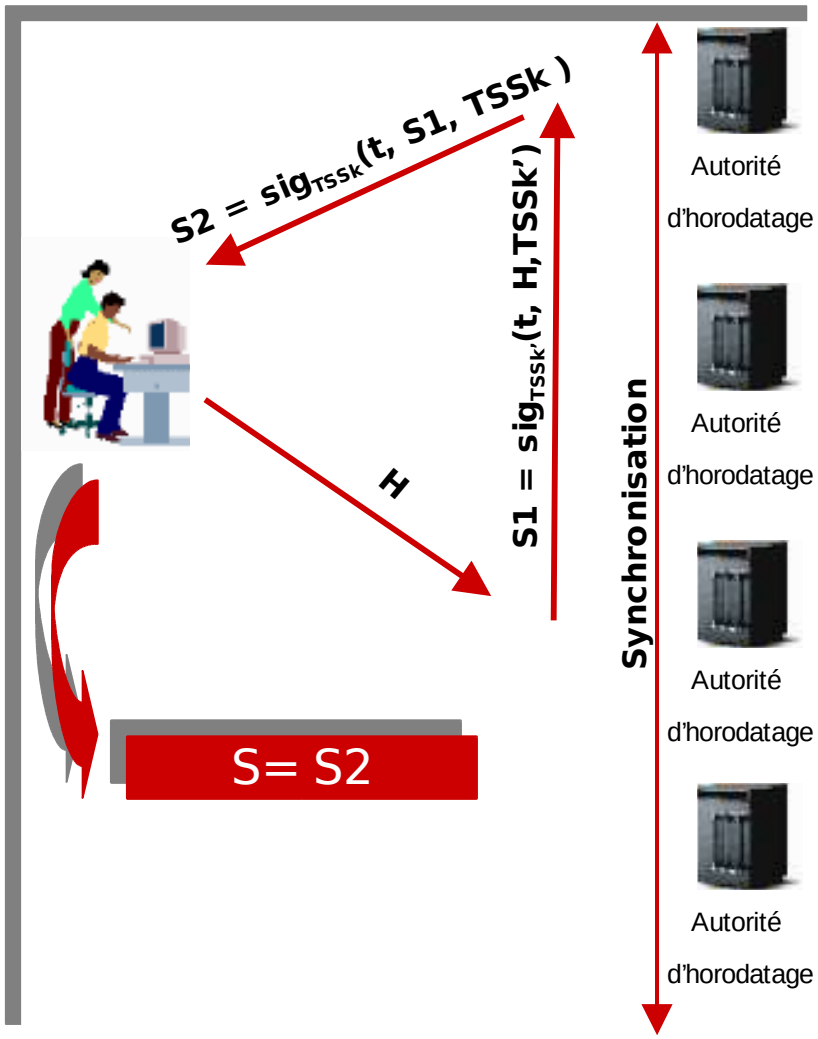
Avantages

- L'attaquant doit attaquer toutes les TSA
- Peut répondre au problème
  -de déni de service
  -de compromission de clé

Inconvénients

- Vérification coûteuse en temps
- Charge du réseau
- Coût du système qui doit être réparti sur plusieurs réseaux

Modèle Distribué (2)



Les cachets sont liés

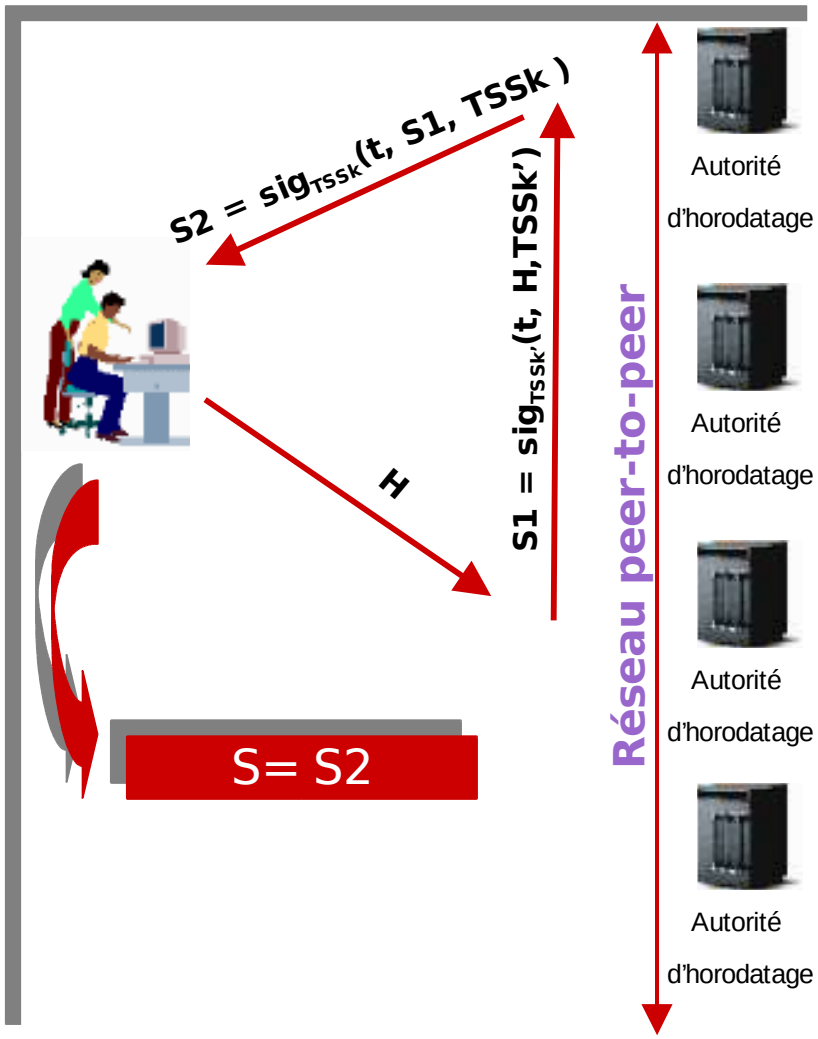
Avantage :
- Facilité d'utilisation

(un seul cachet est retourné)

Inconvénients
- Déni de service possible
- Prise de contrôle de la TSA
- Publication régulière de la racine de l'arbre de Merkle des documents

Autre modèle distribué

Modèle Distribué (3)



Modèle distribué

Les cachets sont liés et publiés sur un réseau *peer-to-peer*

Avantage **:**

- Facilité d'utilisation : pas de publication dans un journal
- Confiance répartie

Inconvénients :

complexité des protocoles

- Temps de latence
- Preuves de correction

Autres Projets

- Cuculus (surety.com)
  - Schémas de liaison
  - Un seul serveur
  - Publication hebdomadaire dans le New York Times
- Prokopius (U. Stanford)
  - Schémas de liaison
  - Algorithmes distribués: accord byzantin et signatures à seuil
  - Simulation : 42 h pour ~ 150 noeuds
  - Preuves à compléter...

Chronos

- Des compétences diversifiées (*cryptographie, génération aléatoire, réseaux, base de données, codages, algorithmique distribuée,...*)
- Approche distribuée pour l'horodatage
- Garantie de niveau de sécurité et de temps de latence
- Implantation et déploiement d'un prototype sur les trois sites