ACI SI MOSAIC

15/02/2005

Yves Roudier – Institut Eurécom

Première Implantation

- Choix “pragmatiques”
  - cartes à puce Javacard
  - Solution à base de TTP
- Les cartes permettent de :
  - Stocker la réputation de l’utilisateur
  - Négocier le prix de la sauvegarde
  - Stocker un log des opérations de sauvegarde
- Le TTP permet de:
  - Gérer les malveillances éventuelles (interprétation des fautes difficiles sans horloge sur les cartes)

Sauvegarde Mobile : Incitations

- Solution en 2 étapes: crédits + réputation
- Protocole d'échange équitable optimiste (offline)
  - repose sur la résilience des cartes à puce (représentant le TTP)
- Réconciliation au niveau du TTP (online)
  - repose sur la reconnection obligatoire pour
    - Récupérer les données sauvegardées
    - déchargement les données sauvegardées
    - Raffraichir sa réputation (rendu obligatoire pour continuer à profiter de l'infrastructure)

Implantation en cours

- Etat de la réalisation :
  - Protocole de base
  - log implanté sur Javacards
  - Logique du TTP pas terminée (interprétation partielle des erreurs)
  - Stockage et récupération non abordé
  - Pas encore de négociation du prix du stockage
  - réseau filaire entre 2 PCs

En prévision

- Simplification du protocole offline
- Vers une version P2P pour le TTP (sauvegarde + réputation)
  - À discuter
- Vers une version ad-hoc sans TTP
  - Comment forcer le passage par la carte à puce : chiffrement des données sauvegardées, les clés étant distribuées par les cartes