

ACI SI MOSAIC

25/05/2005

Yves Roudier – Institut Eurécom

2 Protocoles étudiés

- Protocole à base de crédits
 - Les cartes permettent de stocker l'argent virtuel engrangé contre des sauvegardes
 - Version optimiste: les cartes échangent de la monnaie immédiatement réutilisable + TTP en cas de protocole non terminé
 - Version pessimiste: tout argent gagné est soumis à validation préalable par un TTP
- Protocole à base de compteur
 - Compteur incrémenté à chaque service accepté et décrémenté à chaque remise de données
 - Les cartes sont bloquées à partir d'un certain nombre d'utilisations "malveillantes" (seuil de sauvegardes non délivrées)

Protocoles (suite)

- Crédits:
 - On ne peut stocker plus de données qu'on n'a de crédits (équité forte des services rendus)
 - Comment initialiser les crédits ?
 - Confiance = droits sauvegarde = crédits gagnés
- Compteurs:
 - On peut stocker autant de données que les voisins peuvent en accepter à un moment donné (plus flexible)
 - Confiance = compteur des sauvegardes correctement effectuées (géré par la carte par exemple)
 - repose sur le coût / la difficulté d'obtenir de nouvelles cartes
 - Droit à sauvegarde = compteur du nombre de données acceptées ? Autre métrique ?

Récupération des données: mobile et ad-hoc ou infrastructure fixe ?

- 2 problèmes différents
- Récupération de données avec un point d'ancrage mobile (e.g. crash système + SIM intacte)
 - Comment libérer la place sur tous les terminaux mobiles ayant participé à la sauvegarde ?
- Récupération de données avec escrow (e.g. vol du terminal mobile)
 - Comment éviter la destruction des données par le voleur (libération mémoire après récupération abusive d'une sauvegarde) ?