

Sécurisation des communications entre pairs dans MoSAIC : premières remarques

Ludovic Courtès

LAAS-CNRS

11 octobre 2006

Contexte & motivations

- **Besoins pour des mécanismes d'imputabilité** (réputation, confiance, monétaire, etc.)
 - **établir l'identité** des interlocuteurs
 - besoin d'une forme d'« **authentification mutuelle** »
 - de manière **décentralisée** (hors-ligne)

- **Se prémunir contre les modifications malintentionnées des messages**
 - **protéger les messages/requêtes** échangés
 - assurer **l'intégrité et l'authenticité** des messages

- **Protéger le contenu des communications**
 - vraiment nécessaire ? redondance avec la couche de stockage ?

⇒ Définir précisément les besoins de MoSAIC.

- **Établissement de l'individualité de pairs**
 - Objectifs
 - Notion d'individualité (*identity*)
 - Individualité des participants dans MoSAIC
 - Authentification par clef publique
- Autres besoins de sécurité
- Considérations pratiques

Objectifs

- **reconnaître** les interlocuteurs (participants MoSAIC)
- ... avec **autant de certitude que possible**
- permettre **l'imputation du comportement** de chaque participant :
 - **consommation** de ressources (prix ?)
 - **exactions** et **bonnes actions**
 - **réputation** mauvaise ou bonne
- permettre **d'adapter son comportement à l'interlocuteur**
 - « S'agit-il d'un **participant de confiance** ? »
 - « S'agit-il d'un **bon payeur** ? »

Notion d'individualité (*identity*)

Définitions

- ***identity***: « The distinct personality of an individual regarded as a persisting entity » (Wordnet)
- **individualité** : « *Caractère ou ensemble de caractères qui constituent la particularité de quelque chose ou de quelqu'un.* » (TLF)

Désigner une individualité

- Nom : **une étiquette pour désigner une individualité**
- Problème : rarement **uniques, globaux, et sûrs** (e.g., "Marco", powell@laas.fr, "192.168.1.2", /home/ludo/.emacs)
- « **nom sûr & décentralisé** » : ne peut pas être usurpé, est non ambigu
- cf. *Names: Decentralized, Secure, Human-Meaningful: Choose Two*, Bryce Wilcox-O'Hearn, <http://zooko.com/distnames.html>

Individualité des participants dans MoSAIC

Individualité d'un participant ?

- participant : le **logiciel** MoSAIC, représentant de l'utilisateur humain
- son **comportement** au cours du temps
- observation du comportement lors des **échanges électroniques**

Si tous les échanges sont signés...

- ⇒ la connaissance d'un participant est **uniquement dérivée d'échanges électroniques**
- ⇒ ces échanges sont **liés à une clef publique**
- ⇒ donc, **la clef publique est fortement liée à l'individualité du participant**
- ⇒ cf. Carl Ellison, *Establishing Identity Without Certification Authorities*, USENIX Security Symp., 1996

Authentification par clef publique

Une solution : l'authentification par clef publique/certificat

- un participant *peut* **utiliser toujours la même clef** pour être reconnu
- pour chaque participant : **information de comportement associée à chaque clef connue**

Une « brique de base » pour...

- **la réputation** : possibilité d'échange des données comportementales (cf. *SPKI/SDSI Certificate Theory*, RFC2693)
- **la gestion de ressources** : choisir qui est autorisé à consommer

- Établissement de l'individualité de pairs
- **Autres besoins de sécurité**
 - Intégrité et authenticité des messages
 - Confidentialité des messages
- Considérations pratiques

Intégrité et authenticité des messages

Les messages entre participants dans MoSAIC

- des **requêtes** de stockage/restauration
- typiquement, put et get (cf. *Storage Tradeoffs...*, EDCC-6)

Garantir l'intégrité et l'authenticité de requêtes entières

- utilisation de **codes d'authentification** (e.g., HMAC, RFC2104)
- **vérification d'un HMAC** uniquement possible par le récepteur

Confidentialité des messages

Un message

- une **requête** (put ou get)
- paramètres de la requête : **un nom et des données *chiffrées* à stocker**

Confidentialité des messages : nécessaire ?

- **confidentialité des données** : garantie par la couche de stockage
- **confidentialité de la requête** : peu d'intérêt + coûteux en énergie

Conclusion des besoins de MoSAIC

1. « **authentification mutuelle** » par clef publique
2. mise en place d'un **canal de communication sûr**
3. garantie de **l'intégrité des messages**
4. peu d'intérêt pour le **chiffrement des requêtes** (économie d'énergie)

- Établissement de l'individualité de pairs
- Autres besoins de sécurité
- **Considérations pratiques**
 - Protocoles
 - Implémentation

Protocoles

TLS (RFC2246)

- permet **l'authentification par certificats** (X.509)
- extension (*draft*) pour **l'authentification par « certificats » OpenPGP**, par Nikos Mavrogiannopoulos

Sun/ONC RPC (RFC1831)

- mécanisme d'appel de procédures distantes classique
- utilisé par NFS (entre autres)

RPCSec (RFC2203, RFC2695)

- mécanismes de sécurité pour ONC RPC
- problème : **trop centralisé** (Kerberos 5, serveur d'authentification)

Implémentation

GnuTLS

- implémente TLS
- permet **l'authentification à base de clefs publiques** OpenPGP
- **large choix d'algorithmes** (authentification, échange de clefs, chiffrement)

Sun/ONC RPC

- problème : **pas d'implémentation existante de RPC sur TLS**
- solution : **la faire** (basé sur le code de la bibliothèque C GNU, simple)

Fin

Questions ?