Sécurité sur la grille

C. Loomis (CNRS/LAL)

Agenda

- Les besoins et les contraintes
- Les différents composants
- Les certificats
- Les Virtual Organizations
- Les proxies

Système de sécurité

- **Le système de sécurité doit permettre d'établir des relations de confiance entre les différents acteurs**
  - Les administrateurs des sites
  - Les utilisateurs
  - Les organisations virtuelles et actuels
- **Défi : La grille est un grand système largement distribué**
  - Des milliers d'utilisateurs
  - Plus de 300 sites dans le monde

Contraintes

- **Evolutif :**
  - Les acteurs ne peuvent pas connaître toutes les autres
  - Performance doit être acceptable
  - Permettre l'accès de personnes de différents pays
- **Utilisation doit être « simple » :**
  - Sinon, les gens ne l'utilisent pas
  - Equilibre difficile entre sécurité et utilisation simple
  - Doit permettre une délégation des droits utilisateurs à certains services (soumission de jobs, transfert de fichiers…)

Fonctionnalités Essentielles

- **Authentification**
  - Qui est qui ?
- **Autorisation**
  - Qui a le droit ?
- **Comptabilité (Accounting)**
  - Combien de ressources sont fournis/utilisées ?
- **Audit sécurité**
  - Qui fait quoi et quand ?

Grid Security Infrastructure

- **GSI : un standard pour les logiciels de grille de calcul**
  - Conçu par le projet Globus aux E.U.
  - Utilisé par (presque) toutes les grandes grilles
- **Basé sur « Public Key Infrastructure » (PKI)**
  - Chaque entité a une clé publique et une clé privée
  - Format : X509v3
- **Principales fonctionnalités :**
  - Single sign-on : le mot de passe n'est donné qu'une seule fois
  - Délégation : une personne (ou un service) peut autoriser un autre service à agir en son nom
  - Authentification mutuelle : le destinataire et l'émetteur s'authentifient

Certificat = Passeport Grille

- **Un certificat n'est qu'une pièce d'identité !**
  - Ne donne aucun droit en soi
- **Un certificat peut être émis pour :**
  - Une personne physique (certificat personnel)
  - Une machine (certificat de hôte)
  - Un programme (certificat de service) : pas (encore) utilisé

- **La clé publique (certificat)**
  - Signée après vérification de l'identité du destinataire
  - Publiée sur le réseau
- **La clé privée**
  - Chiffré et protégée par un mot de passe
  - Conservée sur le poste de l'utilisateur ou sur la machine

Autorités de Certfication (CA)

- **Rôle essentiel dans l'établissement de la confiance**
  - En charge de « signer » les certificats
  - Doit vérifier l'identité de l'utilisateur avant de signer un certificat
- **Une ou plusieurs par pays ou région (~90)**
  - Définir les normes et procédures minimaux
  - Etablit des relations de confiance entre les CAs
- **Pour la France, seuls les certificats de la CA « GRID-FR » sont acceptés sur la grille.**

Authentification

- **Authentification c'est fait par les certificats signés.**

- **Principales informations :**
  - Le sujet (DN) du certificat identifie de façon unique un utilisateur ou une machine → username
  - La période de validité du certificat (en général une année)
  - Les utilisations autorisées du certificat (extensions X509v3)

- **Deux formats différents**
  - PKCS12 : un seul fichier pour la clé privée ET la clé publique
  - PEM : deux fichiers, 1 pour la clé privé, 1 pour la clé publique

  - Utilisez PKCS12 (~/.globus/usercert.p12 ET usercred.p12)

Organisations Virtuelles

- **Organisations Virtuelles (VOs)**
  - Ensemble d'individus ayant des buts communs
  - Membres de la VO répartis en sous-groupes
  - Membres peuvent avoir plusieurs rôles (un seul a la fois)
  - Appartenance à une VO détermine les ressources accessibles
  - Un utilisateur peut appartenir à plusieurs VOs
- **Les utilisateurs sont regroupés par :**
  - Expériences : biomed, alice, atlas, esr, …
  - Projets : embrace, gridpp, auvergrid, …
  - Laboratoires : vo.lal.in2p3.fr, vo.u-psud.fr, cppm, …
- **Liste des VOs existantes :**
  - http://cic.gridops.org/index.php?section=home&page=volist

Autorisation

- **Les VOs déterminent l'autorisation d'une personne dans la grille.**

- **Droits par service et par site sur la base de :**
  - L'identité de l'utilisateur
  - La VO à laquelle appartient l'utilisateur
  - Le(s) groupe(s) de la VO auquel appartient l'utilisateur
  - Le rôle de l'utilisateur
- **L'administrateur d'une VO :**
  - Décide qui peut être un membre de cette VO
  - Repartit les membres dans des groupes et sous-groupes
  - Définit les « rôles » de ses membres
- **L'administrateur d'un site :**
  - Décide quelles VOs le site supporte
  - Met en place le contrôle d'accès défini par la VO
- **Un service orienté « autorisation » : ARGUS**
  - Permet un contrôle central (mapping, bannissement)

Délégation

- **Les utilisateurs ne peuvent pas autoriser chaque transaction dans la grille :**
  - Trop de jobs dans la grille
  - Les jobs ne sont pas forcément localisés sur un seul site
  - Un job peut avoir besoins d'utiliser d'autres services
- **Doit être possible de déléguer les droits d'accès aux jobs et aux services grilles :**
  - Certains services (WMS, FTS, CREAM CE) ont besoin d'agir au nom de l'utilisateur avec d'autres services
  - La clé privée du certificat est une information sensible et ne peut être transmise aux services grilles
  - Création d'un certificat de courte durée : « proxy »

Proxy

- **Nouveau certificat :**
  - Signé par le certificat d'utilisateur
  - Période de validité beaucoup plus courte que le certificat utilisateur
  - Valable pour une VO avec éventuellement un groupe/ rôle spécifique
  - Le fichier contenant le proxy est envoyé avec le job et permet d'agir avec les droits de l'utilisateur

- **Durée :**
  - Courte : voms-proxy-init --voms VO, -info, -destroy
  - Longue : myproxy-init, -info, -destroy, -get-delegation

Autres Services

- **Comptabilité**
  - Pas vraiment la sécurité mais basée sur l'authentification
  - Base des données centralisée pour l'utilisation (par VO)
    - http://www3.egee.cesga.es/gridsite/accounting/CESGA/egee_view.html
  - Les quotas ne sont pas (encore) implémentés
- **Les services grilles génèrent un « log » des actions**
  - Pour comprendre qui fait quoi et quand
  - Pour comprendre le fonctionnement du système
  - Les administrateurs doivent garder pendant une période définie

Récapitulatif

- **Les grilles basées sur gLite utilise la « Grid Security Infrastructure » comme système de sécurité.**
- **Authentification**
  - Réseau des CAs signent les certificats des entités
  - Le certificat est le « passeport grille » pour les utilisateurs
- **Autorisation**
  - Gérée par les Organisations Virtuelles
  - Mise en place par les administrateurs des sites
- **Proxy**
  - Contient les VOs, groupes, et rôles de l'utilisateur
  - Permet une délégation de droits aux services grilles et aux jobs