La sécurité dans les grilles

Yves Denneulin
Laboratoire ID/IMAG

Laboratoire Informatique et Distribution
CNRS CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
Institut National Polytechnique de Grenoble
INRIA INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE
GRENOBLE 1 UNIVERSITÉ JOSEPH FOURIER SCIENCES,TECHNOLOGIE,MÉDECINE

Plan

- Introduction
  - les dangers dont il faut se protéger
  - Les propriétés à assurer
- Les bases de la sécurité
  - Protocoles cryptographiques
  - Utilisation
  - Architecture PKI
- Application aux grilles
  - Propriétés particulières des grilles
  - Les points clés de l'infrastructure
    - authentification
    - autorisations d 'accès
    - illustration sur Globus et Datagrid

Les dangers

- Intrusion
  - utilisation abusive des hôtes compromis
- Vol d ’information
  - espionnage
- Usurpation d ’identité
- Déni de service
- …

Propriétés à assurer

- Confidentialité
  - stockage
  - communication
- Authentification
  - limiter l ’accès aux ressources
  - être sûr de l ’origine de l ’information
- Non répudiation
  - impossibilité de nier être à l ’origine d ’un message
- Intégrité
  - message non altéré
  - données non modifiées

Quelques éléments de base

Outils cryptographiques

- Algorithmes de chiffrement symétrique (à clé privée)
  - même clé pour le chiffrement et le déchiffrement
  - secret = clé
  - exemples : XOR, DES, AES (rijndael), IDEA, …
  - implantable efficacement en hardware
  - utilisation compliquée (secret partagé)
- Algorithmes de chiffrement asymétrique (à clé publique)
  - clé constituée de deux parties : une publique (diffusable) et une privée (secrète)
  - on chiffre avec l'une et on déchiffre avec l'autre
  - exemples : RSA, courbes elliptiques, log discret
  - fonctions mathématiques complexes => coûteux

Utilisation pour le secret

- mixage des deux
  - gestion facilitée avec les clés publiques
  - efficacité du chiffrement avec clés privées
- à l ’envoi
  1. choix d ’une clé privée (de session)
  2. chiffrement du message avec cette clé
  3. envoi du message chiffré et de la clé de session chiffrée avec la clé publique du destinataire
- à la réception
  1. déchiffrage de la clé de session avec la clé privée du destinataire
  2. déchiffrage du message envoyé en utilisant la clé de session

Utilisation pour l’authentification

- Envoi
  - Calcul de l ’empreinte (signature) du message
    - utilisation d’une fonction de hachage (MD5)
  - Chiffrement de l ’empreinte avec la clé privée de l ’émetteur
  - Envoi de l ’empreinte chiffrée + le message
- Réception
  - calcul de l ’empreinte (algorithme standard)
  - déchiffrement de l ’empreinte envoyée
  - si les deux sont égales c’est OK
- En bonus
  - non-répudiation
  - intégrité (message modifié -> hash altéré)

Secret + Authentification

- Procédure identique à la précédente
- Envoi en chiffrant avec la clé publique du destinataire

Architecture PKI

- PKI = Public Key Infrastructure
- Infrastructure basée sur les certificats pour l ’authentification des participants à une communication
- Début d’une transaction
  - A envoie sa clé publique à B
  - B envoie un challenge pour que A prouve qu ’il a la clé privée correspondante
  - idem pour B ensuite
- Comment A peut-il prouver qu ’il est bien qui il prétend être ?
  - Nécessité d ’une base de clés sur un site de confiance

Architecture PKI (2)

- Existence d ’une base de clés publiques
  - tiers de confiance
  - nécessite une communication par authentification
    - coûteux
    - peu pratique
    - peu sûr (usurpation possible à chaque vérification)
- Autre alternative : utilisation de certificats
  - contient
    - identité du porteur
  - clé publique associée
  - signée par la clé privée d ’une autorité de certification (CA)
  - contient une date d ’expiration

Authentification par certificats

- Étapes pour que A s ’authentifie auprès de B :
  - A envoie son certificat à B
  - B en vérifie la validité en utilisant la clé publique du CA
  - B envoie un challenge à A
  - A chiffre le challenge avec sa clé privée et répond à B
  - B déchiffre avec la clé publique de A
- Démarrage de la session
  - B envoie une clé de session (chiffrée) à A
- Authentification mutuelle
  - B s ’authentifie de la même manière auprès de A

Remarques sur les certificats

- Une norme : X509
- Contient une date d ’expiration
- Un certificat peut être révoqué
  - plus confiance en son porteur
  - clé privée correspondante compromise
- Existence d ’une liste de révocation
  - géré par le CA signataire du certificat
  - peut être administré localement
  - doit être (théoriquement) consultée à chaque tentative d ’authentification
  - en pratique, mise à jour relâchée (1 jour à 1 semaine)

Politique

- Crypto + protocoles = outils
- Le plus important est la définition d ’une politique
  - propre à chaque site/organisation
  - non technique
  - écrite en français
- Contient
  - règles à suivre par tous
  - les contraintes que doit satisfaire l ’architecture
  - des procédures de mise à jour et d ’audit
  - …

Application aux infrastructures de grilles

Laboratoire Informatique et Distribution
CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE
Institut National Polytechnique de Grenoble
INRIA
UNIVERSITÉ JOSEPH FOURIER

Particularités des grilles

- Distribution géographique forte
  - politique de sécurité hétérogène
- Grand nombre d ’utilisateurs
  - gestion d ’un nombre potentiellement important de comptes
  - nécessité d ’une politique de gestion globale
- Politique de sécurité
  - niveau de confiance limité aux utilisateurs car peuvent venir de l ’extérieur
  - différent du cas général
  - deux niveaux de politique (local, global)

Particularités des grilles (2)

- Session typique
  - soumission d'un travail
  - choix d 'un (ensemble de) site d'exécution
  - transfert des données et du code nécessaire sur les sites concernés
  - démarrage du processus (recompilation?)
  - collecte et transfert des résultats
- Grande variété d 'intervenants
  - utilisateur
  - services (démons)
  - sites distants -> nécessité d 'authentification mutuelle des parties en jeu

Particularités des grilles (3)

- Confidentialité des transferts nécessaire
  - transport par réseau non sur
- Stockage de données importantes sur disques extérieurs
- Pas de confiance systématique entre les utilisateurs
  - Exécution sur des machines sur lesquelles on n 'a pas forcément confiance
- Contrôle d 'accès toujours fait localement (efficacité)
  - indispensable pour la scalabilité
- Solution sécurité doit s 'intégrer dans un grand nombre de technos existantes
  - contrainte d 'intégration forte

Solutions existantes

- Motivations
  - Communication sûre
  - Sécurité entre des organisations existantes
    - pas de centralisation possible
    - pas de politique globale indépendante des politiques locales
  - Login unique (Single Sign On)
    - une seule authentification est nécessaire pour lancer une expérience
  - suppose la confiance entre les partenaires
- Catégories
  - système « stand alone » : Legion
  - sur-système : **Globus, Datagrid**

Zoom sur les deux problèmes principaux

- Authentification
  - utilisateur
  - ressources
  - chaque opération peut être globale -> authentification ne peut être locale (login)
- Autorisation d ’accès aux ressources
  - qu’a le droit de faire chaque utilisateur ?
    - dépend de son rôle (administrateur, …)
    - nécessite une gestion globale
  - à quels droit cela correspond sur le système local?
    - Correspondance faite au niveau local

Authentification

- But : identifier avec certitude les deux parties dans une communication
- Basée sur le chiffrement asymétrique et les certificats
  - un certificat pour chaque entité
    - utilisateur
    - services
    - ressources
- Doit être distribuée (non centralisée)
- Schéma général non possible en pratique
  - nécessite une intervention manuelle (clé privée) => pas de single sign on
  - nécessite le transfert de la clé privée des utilisateurs -> inacceptable

Délégation

- Permettre à une autre entité d ’utiliser des ressources au nom d ’un utilisateur
- Deux types
  - **délégation de droits (ex : accéder à des données)**
  - délégation de responsabilités (ex : exécuter une tâche)
- Propriétés à respecter
  - délégation restreinte (droits, temps)
  - confiance au délégué
  - révocation possible
  - efficacité

Certificat

- Servent à identifier
  - utilisateurs
  - services (au sens large)
- Contient
  - nom de l 'utilisateur/ du service
  - clé publique
  - identité du CA qui a signé
  - signature du CA
- Rappel
  - pour être utilisé dans une authentification, nécessite la clé privée

Certificats délégués

- Utilisation de certificats temporaires (GSI : Globus)
  - généré (et signé) à partir du certificat **utilisateur**
  - agissent comme des proxys du vrai certificat
  - utilisés pour l 'authentification auprès de tous les éléments du système
  - permettent le single sign on (SSO) : authentification unique pour toute une session
- Particularités
  - expire au bout de 12 à 24 heures
  - typiquement utilisé pour une session/un job
- Avantages
  - perte/vol de la clé privée moins critique
  - la clé privée du proxy peut voyager
- Standardisée (RFC)

Gestion des clés privées des utilisateurs

- Stockage centralisé (poste de travail, FS partagé)
  - OK si l 'utilisateur ne bouge pas
- Solutions matérielles
  - clé USB
  - carte à puce
  - coûteux, nécessite infrastructure
- Création d 'un espace de stockage commun (datagrid)
  - accès à une clé validée par un mécanisme d 'authentification (mot de passe, Kerberos, …)
  - certificats proxy générés sur le site même
  - permet d 'automatiser la régénération de certificats

Autorisation d'accès aux ressources

- 5 entités différentes jouent un rôle
  - utilisateur
  - proxy utilisateur
  - processus
  - ressource (possède un certificat pour l'authentification mutuelle)
  - proxy ressource
- Domaine de confiance : Virtual Organization (GSI)
  - peut être de nature
    - physique (un site)
    - logique (une expérience)
  - il existe une notion de rôles dans une VO
    - administrateur
    - participant

Détermination des droits

- Choix des droits
  - information sur l 'utilisateur et la session
  - informations sur les services (objets)
  - politique de sécurité locale
- Cœur du problème
  - correspondance entre les droits dans les VOs et les droits locaux
  - gestion globale nécessaire
  - mais les droits locaux doivent être gérés en local
    - chaque site veut avoir le plein pouvoir sur ses machines

Les groupes

- Utilisation de groupes
  - correspondent à des catégories d 'utilisateurs
  - équivalent aux groupes Unix
  - dépendent de
    - la VO dont l 'utilisateur fait partie
    - son rôle dans cette VO
- À chaque session
  - les groupes dont l 'utilisateur est membre sont stockés dans un certificat
  - utilisation du certificat temporaire (proxy)

Solution Globus

- CAS (Community Authorization System)
  - contient une BD avec utilisateurs et groupes
  - contient les informations sur les objets protégés
  - serveur
- Utilisation
  - contacté à chaque (première) demande d 'accès à un objet
  - prend la décision seul : oui/non à partir du proxy certificat de l 'utilisateur
- Critiques
  - scalabilité ?
  - pas de contrôle possible en local (où la ressource est stockée)

Solution Datagrid

- Virtual Organization Membership Service (VOMS)
  - gestion des autorisations dans le cadre des VOs
  - gestion distribuée
  - définit les correspondances entre VOs et RP (resource providers)
    - dépend du rôle de l 'utilisateur dans la VO (géré par la VO)
    - dépend de ce que peut faire l 'utilisateur sur la ressource (géré en local par les sites)
  - crée le certificat qui permet l 'accès à la ressource
- Utilisation d 'un SGBDR
  - stockage des informations sur les utilisateurs (appartenance au VO)
  - centralisé pour l 'instant (jan 2003), distribué à terme

Solution Datagrid (2)

- Scénario
  - après authentification : obtention d ’un certificat
  - à partir de ce certificat obtention des « capabilities » en utilisant le service d ’autorisation
  - tentative d ’accès à un objet
    - extraction des ACL (Access Control List) de cet objet
    - comparaison avec les capabilities pour savoir si l ’accès est accordé
    - ACL local -> décision prise en local

Confidentialité des données

- Transfert
  - utilisation possible de canaux chiffrés
  - solution technique standard (SSL)
- Stockage
  - permanent
    - rien n ’est fait pour l ’instant
    - facile à mettre en place « à la main »avec des solutions classiques
  - temporaire
    - difficile : les données doivent être en clair pour pouvoir être manipulées
    - confiance mutuelle obligatoire entre les participants
    - solution?
      - Algorithmique travaillant directement sur les données chiffrées -> sujet de recherche

Confiance mutuelle

- Gestion des comptes
  - correspondance utilisateur grilles <->utilisateurs locaux (unix, NT)
    - peut être faite par site : un site-> un utilisateur
    - peut être faite par expérience : une manip-> un utilisateur
  - solution technique Globus
    - fichier grid_access contient les correspondances
    - Datagrid : fichier construit automatiquement à partir des annuaires LDAP et d ’une liste « noire »

Sources

- The security architecture for open grid services (www.ogsa.org)
- Datagrid: Security requirements and testbed 1 security implementation
- **Datagrid: Security Design**
- Projet E-toile : État de l ’art sécurité dans les grilles