Towards More Flexible and Increased Security and Privacy in Grids

Willy Weisz
University of Vienna
Institute for Scientific Computing, VCPC

Certification Authority

UNICORE SUMMIT 2006, Dresden
30 – 31 August, 2006

Contradictory requirements

Users want

- systems they can trust to protect the integrity and privacy of the information they own

Administrators want to

- preserve integrity of their systems

But Grid users want

- flexibility and easy access of Grid resources
- easy authorisation procedures

Identification, Authentication and Authorisation on Travels

Identification item:

- ID card or Passport

Authentication:

- Visual (future: computer assisted) comparison of holder and ID Document (RFID stored) picture

Authorisation:

- Come and go when and where you want (EU style)
- Visa – whole country or only special regions, any or only restricted number of border crossing points

Identification, Authentication and Authorisation in Organisations

Security of operations through:

- Identification of all:
  - Employees and co-operating entities (actors)
  - Resources
  - Allowed activities
- Definition of
  - which actor
  - is allowed to do what
  - using which resource
- Works fine in small organisations
- Impractical in large, distributed ones

Authorisation in Organisations

Therefore:

- Definition of Attributes for
  - Actors (roles, functions, hierarchy level etc.)
  - Resources
  - Possibly also for actions

- Definition of authorisation
  - Which type of actor
  - May perform which (type of) action
  - Using resources with which attributes

Mapping of attributes to Entities at the “local” level

Authorisation in Collaborations

Collaborations must:

- Honour the authorisation matrix of each partner
- Define
  - Attributes for the collaboration
  - Map them to individual entities allowed to participate in it
  - Define a collaboration specific authorisation matrix

Organisations on the Grid

Organisations on the Grid are a special type of collaborations:

- They share resources
- They are geographically often wide apart
- Their partners meet over the Internet rather than in face-to-face
- They are called Virtual Organisations (VO)

Identification and Authentication on the Grid

Identification and Authentication using an X.509 Public Key Infrastructure (PKI)

Identification using a Trusted Third Party:

- the Certification Authority
- issuing an X.509 certificate to an end entity

Authentication:

- Entity proves to possess the private key corresponding to the identifying certificate

Identification and Authentication on the Grid

Entities with certificates:

- Consumers/requestors (human and others)
- Hardware resources
- Applications
- Services

Trust in PKIs

Relying parties trust that:

- CAs issue certificates that conform to a set of minimal requirements related to:
  - Identity vetting
  - Secure storage and handling of the CA's private key
  - Procedures
  - Accessibility of revocation information
  - Any other item listed in the CP/CPS documents

Trust in PKIs

Relying parties trust that:

- Users protect their private key from unauthorised access and use by
  - Storing them in a secure container only accessible to the owner
    - In a file protected by restrictive access rights and a secure system
    - On a secure token (SmartCard, USB token, HSM …) – the only truly secure key store
  - Encrypting it with a “good” passphrase or PIN only known to the owner

CAs and their Federation

CAs exist:

- Within organisations
- For VOs (e.g. UNICORE CA)
- to serve a regional (national) community

Relying parties trust certain CAs to issue trustable certificates

CAs can create Federations:

- Recognise that their minimal security requirements are compatible
- Give relying parties trust in the certificates issued by CAs they don't know

Authorisation based on Identity

Discretionary Access Control – DAC

Overwhelmingly used in

- Operating systems
- Grid middlewares
  - UNICORE
  - Globus Tool Kit

Authorisation based on Identity

After identification and authentication a consumer

- is mapped to an O/S identity
- enjoys “almost help-yourself party”

Authorisation is

- too coarse grain
- not suitable for e.g. database systems

Grid mostly unfit for use of federated databases

- Neither OGSA-DAI nor GGF DAIS-WG have yet tackled security aspects of gridified databases

High-Security Authorisation

Entities (consumers and resources) classified according to clearance levels

Mandatory Access Control – MAC

Read access to objects of lower clearance level (Read Down)
Write access to objects of higher clearance level (Write Up)

Consumer may need to lower temporarily her/his/its clearance level to become able to write an object

Too restrictive a scheme for most Grid environments

Role-Based Access Control - RBAC

RBAC preferred authorisation scheme if

- DAC is too weak
- MAC is too restrictive

Allows

- more fine-grained access rights than DAC
- easy adaptation to an entity's role change
- definition of hierarchical role scheme like MAC

Attribute-Based Access Control - ABAC

Allows even more flexibility than RBAC

- Attribute relations are less static than consumer-resource authorisation relations in RBAC

Roles are but one of the possible attributes

$\Rightarrow$RBAC is subset of ABAC

User Database at the Grid Resource Site

Comprehensive lists of allowed consumer entities for

- UNICORE – the UUDB at the V-site
- Globus – the gridmap-file on the Globus host

Gridmap-file

- Manageable remotely by VO management system (e.g. VOMS)
- Doesn't store X.509 certificates

UUDB

- Only maintainable from local site
- Stores certificates – which have a limited life-time!
- Doesn't scale well with expanding and changing VOs

Managing Authorisations for VOs

VOs should move

- From concentrating on identities and their rights to access resources
- To policies based on roles and attributes defined
  - for their organisational constituency
  - for the co-operation in the VO

Policies change less frequently than entities in a VO

Attribute Authorities

A consumer may have attributes or assume roles

- in his/its organisation
- in the VO

Information on attributes/roles is published and signed by an Attribute Authority (AA) of

- the individual organisation
- the VOs

The same structure is also responsible for resource attribute publishing

Privacy - Anonymity

It may be important (or required by law) that

- the identity of a requester be anonymised for the time of the resource usage
- but be traceable at some later time (e.g. for accounting or feedback)

Possible by mapping the identity to a “general user” with attributes that will permit the traceback on a need-to-know basis

Authorisation

Authorisation driven by policies

Policy = Set of rules based on identities and attributes of consumer and resources

A policy may require a third party permission

- e.g. by the patient whose Electronic Health Record is retrieved to a doctor or an insurance

Third party must also be

- authenticated
- and its attributes taken into account

UNICORE Security

Production UNICORE has strong but very inflexible security infrastructure

Authentication is based on certificates stored in the UUDB
$\Rightarrow$No Proxies

Co-operation with Globus (GRIP project)

- unidirectional (UNICORE $\rightarrow$ Globus)
- with proxies traversing UNICORE agents as an encrypted blob (encrypted private keys are travelling!)
- to be activated when passing the job to a Globus site

Explicit Trust Delegation - ETD

Trust attribute issued by the end-user

- to a UNICORE agent
- to allow it to authorise actions on behalf of the end-user

EDT needed to dynamically create sub-jobs after the job has been submitted by the end-user

First(?) use of an attribute in UNICORE with the end-user acting as AA

Proposed Authorisation architecture

For any subject and target of a request

- a complete policy or set of policies must be defined by a Source of Authority (SOA) also called Policy Administration Point (PAP)
- decisions to allow or deny the request have to be derived using these policies

The client agent sends the request including authentication data and the attributes of the requestor to a Policy Enforcing Point (PEP).

The PEP hands the request over to a Policy Decision Point (PDP)

Proposed Authorisation architecture

The PDP

- applies the policy rules
- taking all information on identity and attributes
- may ask Policy Information Points (PIP), e.g. AAs, for more information if needed
- hands the decision – accept or deny the request – to the PEP

The PEP

- enforces the PDP decision
- enforces a default decision if the PDP was unable to decide

Attribute Collection

Attribute collection by

- the User Client
- the PDP

Collection by the User Client is

- more scalable
- easy at least for attributes defined in the requesters organisation

Attribute Collection

Attributes stored in different databases

Therefore need for

- standard protocols to transport attributes
- creation of plugins to the databases to handle the protocols

Existing standards for protocol:

- X.509 Attribute Certificates using the ASN.1 format
- XML coded Security Assertion Markup Language (SAML)

Authorisation

Replace monolithic UUDB by plugins implementing the authorisation architecture just discussed

ETD will have rules in the PDP

Formulation of policies in standard language

- e.g. eXtended Access Control Markup Language (XACML)
- easy to learn for simple policy models
- Usable for expressing complex rule sets

Looking outside the UNICORE world

Some software projects developed tools to implement some of the ideas of the proposed Authorisation architecture

They were aimed at Web Services or the Globus Toolkit

VOMS

- Manages VOs
- Users can ask to be added to VO
- Administrators accept or deny requests
- At the lowest sophistication level generates gridmap-file
- Performs only PIP functions; PDP functions assumed by Globus Gatekeeper

Shibboleth

- Federated authorisation infrastructure for Web Single SignOn across organisational boundaries
- Uses SAML v1.1 for the exchange of attributes
- Passes authorisation information in form of opaque handles
  - Provides anonymity
  - Without loosing capability for traceback to user

GridShib

- Integrates Shibboleth with Grid technology provided by Globus Tool Kit version 4 (GTK 4)
- Need to efficiently map Shibboleth's opaque handle with the DN of the X.509 certificate used by GTK 4

PERMIS

- Privilege Management Infrastructure
- Provides full policy-based authorisation service
- Policies written in XML
- Supports RBAC

GridShibPERMIS

Combines

- strength of Shibboleth as an Identity and Attributes Provider
  - GridShib provides the PIP
- the Grid Infrastructure of GTK 4
  - provides the X.509 based authentication
- Policy-based authorisation provided by PERMIS
  - acts through its interface “GridShibPERMIS Context Handler” as PDP in the GTK 4 Authorisation Framework

Conclusion for UNICORE/GS

Overhaul security infrastructure

New Security Infrastructure Model based on the PIP-PDP-PEP architecture using identity and attributes for policy-driven authorisation

Use existing standards and pieces already available to the Grid Community

For further contacts

Willy Weisz

weisz@vcpc.univie.ac.at

http://www.vcpc.univie.ac.at

http://www.austriangridca.at