Policy-Based Negotiation for Grid Service Authorization

Daniel Olmedilla, Wolfgang Nejdl

Semantic Grid: The Convergence of Technologies
Dagstuhl Seminar, 4th-8th July 2005
Motivating Scenario
Grid Limitations

MyProxy Credential Repository

0a Request previously stored proxy certificate
0b Receive proxy certificate

NEESgrid Linux Cluster
1 Mutual Authentication (M.A.)
2 Alice submits a job
3 Delegate proxy certificate

GridFTP Server

M.A. : Mutual Authentication

RLS

SRB
Shake table

Alice Smith
Motivating Scenario
Grid Limitations

- Too many Credentials to keep track of
- Knowing which credential to use
- Different sites trust different CA
- No way to determine automatically which issuers are trusted

Authorization may depend on user’s properties
E.g. user’s affiliation with a project

Job must know in advance what credentials will have to be disclosed

In large projects, an account per user does not scale
Policy-Based Negotiation
Trust Negotiation

Step 1: Alice requests a service from Bob

Step 2: Bob discloses his policy for the service

Step 3: Alice discloses her policy for VISA

Step 4: Bob discloses his BBB credential

Step 5: Alice discloses her VISA card credential

Step 6: Bob grants access to the service
To gain access to a grid resource, I must satisfy its access control policy, which describes

- Which certificates must be presented to gain access to it
- Who is responsible for obtaining and presenting these certificates

If required, for sensitive resources, negotiation can be longer

- To obtain (access to) a certificate, I must satisfy its access control policy, which specifies … --and so on, recursively—
Motivating Example
Negotiating on the Grid

Alice Smith

Credential Repository

NEESgrid Linux Cluster

1. Authentication
2. Request
3. Alice membership?
4. Alice membership?
5. Alice BigQuake membership

Shake Table Access Manager

Shake table

0. Alice submits a job
6. Alice BigQuake membership
7. Access granted
8. Alice’s job Shakes the table
Implementation
Easy Integration with Current Grid Services

Service
- include one jar file containing the policy based trust negotiation engine
- minor add-ons to the service wsdl file (import one wsdl file and extend one port type) and wsd file (add one more provider and install a security descriptor)
- have a resource (if not available)
- re-deploy the service

Client
- use one jar file containing the policy based trust negotiation engine
- invoke the service as usual / or call directly for a trust negotiation process
- look for authorization exceptions and if one triggered by trust negotiation failure make simple calls to the negotiation engine
Negotiating Trust on the Grid
J. Basney, W. Nejdl, D. Olmedilla, V. Welch, M. Winslett
2nd Workshop on Semantics in P2P and Grid Computing at the 13th International WWW Conference, May 2004, New York, USA

D-GRID Infrastructure Project
- Work on AAAI / Security
- Specifically on / with MyProxy and online credential repositories
- Project starts in August/September
Thanks!

olmedilla@l3s.de - http://www.l3s.de/~olmedilla/