Contribution ID: **135** Type: **Oral**

Improving Grid User's Privacy with gLite Pseudonymity Service

Monday 12 April 2010 16:30 (20 minutes)

The Grid computing model provides Grid users a way to use resources that are not usually owned by their parent organizations. The use of Grid resources entails a balance between the resource owner's need to oversee and account for the resource usage and the user's privacy requirements. From the user's point of view, complete anonymity is desirable, but not possible due to requirements like traceability without user intervention. The solution we propose is the concept of a lesser degree of anonymity, pseudonymity: the use of traceable pseudonyms as user identifiers.

Conclusions and Future Work

We have presented a service implementation that enables pseudonymous Grid access, ie. the hiding of true identity of the user from the Grid resources. The service has been running in our test VO with our test online CA, and its users have been able to submit pseudonymous Grid jobs to our test cluster. However, wider deployments would allow us to gain practical experience of the system and identify problem areas. We also see Grid portals as potential pieces in the overall architecture of the system: the benefits and drawbacks need to be explored.

Detailed analysis

The security of many of today's Grid middlewares, including gLite, is based on PKI certificates. In order to interoperate seamlessly with them, the pseudonymous identities must also be modeled as standard X.509 certificates, but their subject DNs needs to be anonymized and lifetime more limited. Users obtain pseudonymous identities from the Pseudonymity Service by using their existing Grid identity for authentication and authorization. The service registers the newly issued pseudonyms to the VO's attribute authority as aliases to the users' existing certificates. This enables the users to request VO attribute assertions to be used in conjunction with the pseudonymous identity. The service uses the gLite SLCS implementation and its XML-based request-response protocol as a basis on both the server- and client-side. The service runs on a Java servlet container and uses a relational database for storing the identity mappings. It is currently compatible with online CA software supporting CMC or CMP protocols and VOMS-admin version 2.5. The Java-based command-line client tool is used for communication with the service.

Impact

After obtaining the pseudonymous certificate from the service, the user can initialize his pseudonymous Grid identity with the standard VOMS client. In the pseudonymous Grid access, the most important challenge is confidentiality: the true identity must remain hidden from the resources. In order to prevent correlation attacks, the lifetime of the pseudonymous identities should be short: ideally they are used for only one action in the Grid. As all the pseudonymous certificates must have a unique subject DN, the user authentication and authorization at the Grid resources must be based solely on the VO attributes. In fact, the bigger the group of users sharing the set of attributes is, the better individual user's identity is buried. On the other hand, big

group sizes may also reduce privacy as the whole group can access the same data in the Grid, even though the real user identities behind the pseudonyms would be different.

Keywords

Authentication, Authorization, Grid Security, Pseudonymity

URL for further information

http://tek.hip.fi/Projects/IDM/GridPseudonymity

Author: Mr MIKKONEN, Henri (Helsinki Institute of Physics HIP)

Co-authors: Dr WHITE, John (Helsinki Institute of Physics HIP); Mr HAHKALA, Joni (Helsinki Institute of Physics HIP)

Presenter: Mr MIKKONEN, Henri (Helsinki Institute of Physics HIP)

Session Classification: Security

Track Classification: Software services exploiting and/or extending grid middleware (gLite, ARC, UNICORE etc)