The Data Grid: Security and Privacy Issues[*]

Nicola Mezzetti and Fabio Panzieri

University of Bologna
Department of Computer Science
{nicola.mezzetti, panzieri}@CS.UniBO.it

1 Introduction

A Virtual Organisation (VO) can be thought of as a dynamical environment consisting of a set of mutually distrustful *"entities"* (e.g., users, resources, organizations) collaborating to carry out a common task. In one such an environment, the Data Grid Architecture aims to providing those entities with flexible, secure, and coordinated resource sharing.

For example, in the weather forecasting context, a common task can be that of processing metereological data, captured by a constellation of satellites.

In addition to resource sharing, the scope of the Grid is the provison of a set of protocols that can enforce an approriate security policy within a VO. To this end, the Grid incorporates an entity named *Community Authorization Service* (CAS) ([PWFK02]), i.e., a Trusted Third Party (TTP). Essentially, the CAS can enforce a specific security policy within a VO by i) maintaining full knowledge of both the VO members, and the fine-grained access control policy of the principals belonging to that VO, and ii) using this information in order to produce capabilities to enable access to resource provider services.

We wish to point out that, as the CAS is an entity *inside* a VO, it cannot be "trusted"; by definition, entities in a VO may belong to several mutually distrustful *Physical Organisations* (POs). In addition, owing to the same motivation, the CAS cannot be considered a "third party". Thus, the CAS may turn out to be a single point of failure within a VO, that can put at risk the security and privacy requirements of that VO.

In order to solve these problems, we propose a distributed authorization system that can meet privacy requirements, in terms of both anonymity and untraceability, of a VO.

2 A Trusted Authorization System

The distributed authorization system we propose allows the various POs, participating in a VO, to share the responsibility of enforcing a global security policy within that VO.

[*] This work has been partially supported by European FP5 RTD project TAPAS (IST-2001-34069).

Our authorization system is based on a failure detection mechanism that makes use of digital signatures, timestamps, and receipts. In essence, this system consists of as many local policy servers as the POs in a VO. Each of these local servers, named *Community Server* (CS), is deployed within an associated security domain. Thus, every PO is responsible for the certificates it distributes, and can check the policy compliance of inbound service requests.

The CS in a PO is a *local trusted party* within that PO, as the principals[1] belonging to the same PO trust each other[2]. In contrast, the set of CSs in a VO maintains the abstraction of a central CAS, and can support fault tolerance by exploiting the *non-repudiability*, *originality*, and *memory* properties of the building blocks out of which our authorization system is constructed.

The only global knowledge required to build our system is a resource naming service that can be located anywere in the system. This service has no control over sensible data and policy enforcement; it is named *VO Connectivity Server* (VOCS), and can be replicated without threatening the VO security features.

Our distributed authorization system can meet the *privacy* requirements of a VO by allowing each CS to assume the role of *anonymity grantor* for the principals belonging to its own PO. To this end, the CS introduces a new certificate type, termed the *pseudonym*, that hides the binding between a *nym* (i.e., a "dummy" identity), and the real identity of the principal that asked for it. The CS that generated the pseudonym maintains secret that binding, provided that the anonimous principal to which the pseudonym relates does not behave maliciously.

Finally, *untraceability* can be achieved by integrating our authorization system within the Onion Routing protocol for anonymous connections [SGR97].

References

[M02] Mezzetti, N.: A Secure and Anonymous Authorization Service for Grid Architectures. “Laurea” Degree Thesis in Computer Science, Department of Computer Science, University of Bologna (June 2002)

[PWFK02] Pearlman, L., Welch, V., Foster, I., Kesselman, C.: A Community Authorization Service for Group Collaboration, 2002 IEEE Workshop on Policies for Distributed Systems and Networks (2002)

[SGR97] Syverson, P., Goldschlag, D., Reed, M.: Anonymous Connections and Onion Routing. IEEE Symposium on Security and Privacy (1997)

[1] Entities that can play an active role.

[2] This assumption is realistic as each security domain has its own local security infrastructure and access control.