Multilayer Privilege Management for Dynamic Collaborative Scientific Communities

David Chadwick[a], Theo Dimitrakos[b], Kerstin Kleese-Van Dam[c], Damian Mac Randal[b], Brian Matthews[b], Alexander Otenko[a]

[a]ISI, University of Salford
[b]CCLRC Rutherford Appleton Laboratory
[c]CCLRC Daresbury Laboratory

Abstract

1 Introduction and Motivation

Rapid advancements in Grid Computing and the convergence of Grid and Web Services, and the development of infrastructures such as the Ecology GRID (ECO 2003) and NERC DataGrid (Lawrence 2003), bring about protocols and machine-processable message/document formats that will soon enable seamless and open application-application communication. This will bring about the prospect of ad hoc integration of systems across institutional boundaries to support collaborations that may last for a single transaction or evolve over many years. We will witness on-demand creation of dynamically-evolving, scalable Virtual Organisations (VO) spanning national and institutional borders, where the participating entities pool resources, capabilities and information to achieve common objectives.

As a motivating example, consider a hypothetical environmental project where there are several research groups in different institutes collaborating on a study of complex physical phenomenon which involves simulation and on-line analysis of existing atmospheric and oceanographic data (including satellite imagery). Being a large project, it would have several work packages involving different parts of the consortia and running for different periods of time within the project timeframe. The satellite images, plus significant quantities of metadata and derived data are held in data centres. This data, collected from many sources, may be commercially sensitive, and therefore access is to be restricted to only those individually with a project-relevant need.

The data owners may want to apply varying conditions on access to their data, e.g. non-military personnel should only be given degraded versions of military sourced images, with different degradation filters applicable for different application domains. The data centres have to ensure the security and confidentiality of data and so has to control who can do what on their machines, e.g. who can carry out cross database correlations, or upload filters to be applied to images. The project, which is paying for the data access, wishes to control who is allowed to access the data and when. It needs to be able to define several authorization groups (e.g. corresponding to work packages) and specify what data is available to that group. The groups will have a specific lifetime, and individuals may join or leave the group during its lifetime, i.e. they are dynamic virtual organizations.

The data centres need to take these different authorization policies and apply them for each of the actions and units of data being accessed. This raises several challenges:

Applying multiple authorization policies to control access to resources.

Enforcing fine-grained access control at the resource.

Managing dynamic virtual organizations comprising of resources and individuals authorized to use them.

Handling the multiple authorities necessitated by distributed VOs and resources.

Handling policy conflicts where individuals may play different roles, at the same time or at different times.

In this paper we outline a new project, DyCom, which seeks to combine the results of two European projects, Grasp and PERMIS, to provide an architecture to manage the complex privileges required in such scenarios. We will describe the mechanisms developed in these projects and show how they could be combined.

2 Detailed Example

As a motivating example consider the scenario in Figure 1. As a part of the scientific project, University researcher Alice needs to perform on-line analysis and simulation of atmospheric and oceanographic in order to study and complex physical phenomenon. Using specialised services provided by different Application Service and Data Providers (ASP1, ASP2 and ASP3). Such services may include analysis tools (hosted at another institution SH1), pre-existing data sets (held by a remote data archives SH2, SH3), additional computation power outsourced to a supercomputing centre acting as ASP1. The goal is, as the analysis proceeds, to create overlaying security perimeters, protecting different virtual collaborations that may exist at a time, while ensuring the security of each member as defined by its local administrator.

Alice belongs to team of researchers assigned to a local administrator at the University. The main activities of the analysis and simulation are executed by end-to-end services CSI1 provided by ASP1, and CS2 provided by ASP2. We assume that CSI1 is using sub-services executed in house at ASP1 who is responsible for administering CSI1 and its sub-services, whereas ASP2 is effectively outsourcing some of the sub-services to different service hosts SH1 and SH2. Each administrator wants to protect its local "private" resources from the general "public" which may include hostile agents. At the same time seamless interaction between Alice and the end-to-end services, as well as CSI2 and its outsourced sub-services, is highly desirable in order to facilitate collaboration objectives, i.e., the analysis of a complex physical phenomenon.

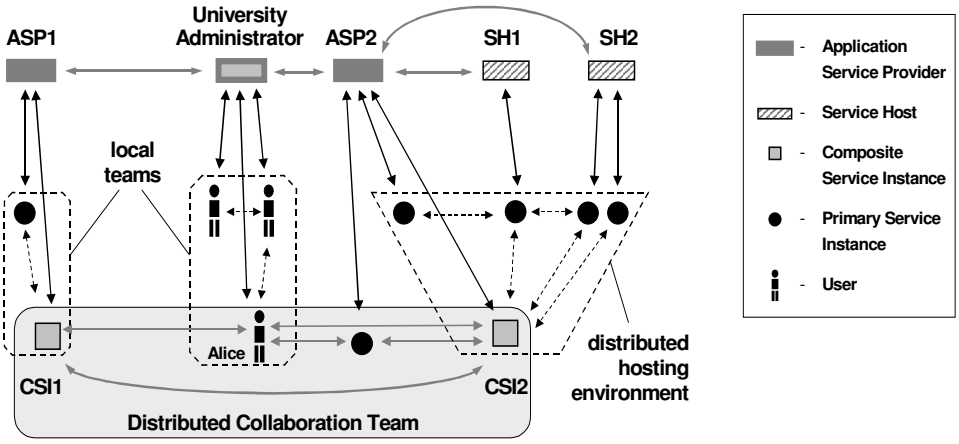

Figure 1. A motivating scenario

This scenario highlights several issues related to secure collaboration in dynamic virtual organisations:

- Collaboration of resources that are controlled by different institutions. Each institution will have their own policies on access control and conditions of use.
- Resources may be called upon to participate in the task without previous knowledge of the other participants. Trust between resources has to be established in real time on a peer-to-peer basis.
- Resources need to be protected from their collaborators and the whole collaboration team has to be protected from outsiders including other entities residing with the participating institutions.
- The same resource may interact in different contexts in groups corresponding to different collaborative project teams. A separation between those interactions has to be achieved.
- Different security conditions may be applied for different parts of the resource, including restrictions on data.
- Collaborating resources may play different roles in their organisation and various collaborations, and different (potentially conflicting) security policies may apply.
- There is no central administrative point. Security has to be achieved via devolved policy management combined with distributed enforcement.
- Complex trust relationships may hold between collaborating resources (users or services) and their managers: Trust of a resource may evolve over time based on the direct observations of its collaborators, witnessing whether it is performing as expected, given its role. Also, changes of the trust level in a manager may reflect on the trust level in the resources it manages, and vice versa.

A suitable architecture must be able to provide a security and trust management infrastructure that meets these requirements.

3 GRASP Security Infrastructure

The GRASP project (http://www.eu-grasp.net) is an industry driven European research project, exploring the use of Grid Services to support the evolution of the Application Service Provision market towards a sustainable utility computing model. GRASP is developing an architectural framework for Grid-based application service provision, a prototype realisation of this framework, and "proof-of-concept" implementations of "federated" and "many-to-many" ASP models in the e-Learning and Biomedical domains. The implementation has been developed on top of Microsoft's .NET platform and taking advantage of WSE (Web Service Enhancements) and OGSI.net components.

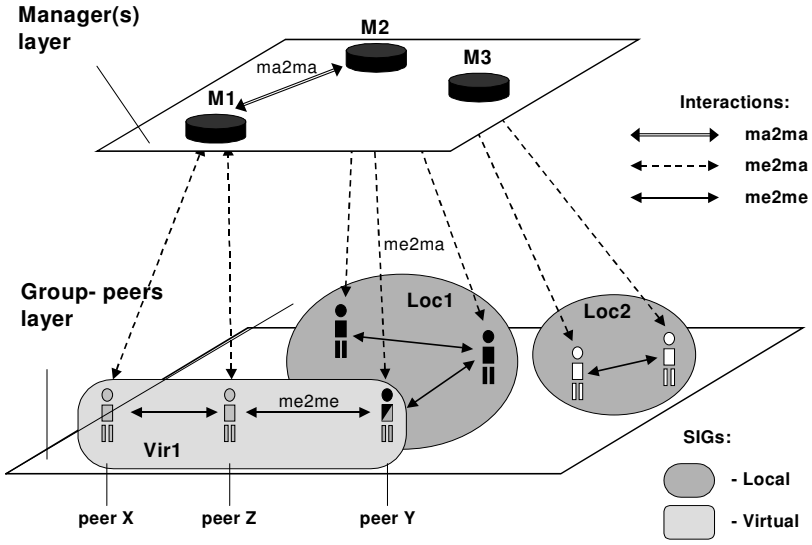

Figure 2. Types of interactions and communities within the GRASP Security Infrastructure

The Security Infrastructure being developed within GRASP is based on secure collaboration groups which can be dynamically altered in terms of membership and policy constraints. The interaction model integrates a layered peer-to-peer model (between collaborating resources and between managers administering resources), with a centralised community management model (between members and their local managers) and a master/slave model (between security managers and enforcement agents). This is depicted in Figure 2. It supports on-demand creation and management of dynamic virtual collaborations in the form of secure groups of peers (user agents, services, resources, etc.) that cut across geographical and organisational boundaries. This architecture has been developed with two main goals in mind:

- Enabling communication within dynamically created collaboration groups, that is: secure, scalable, accountable, robust and independent of network topology.
- Enforcing security perimeters, which adapt to the highly dynamic evolution of a collaboration group (in terms of membership and security policy).

These goals are addressed via:

- Certificates to manage group membership and privileges.
- Role based security policies describing permissions, prohibitions and obligations within the collaboration teams, set by, and negotiated between, the community managers.
- Mechanisms for end-entity enforcement of the security policies that protects individual members within a collaboration group and the collaboration group as a whole.

This security architecture caters for enforcement at each end-point by creating a shell protecting each peer. This extends the notion of a distributed firewall by introducing further layers of control for group authentication and role-based access to service instance data and operations that are enforced (at the middleware layer) by a perimeter protecting each individual service, as depicted in Figure 3.

Security perimeters for each peer contribute to the formation of a distributed security perimeter protecting a community. Security enforcement is controlled by the local security administrator of each member and it is coordinated by the administrator of the whole virtual group around which the distributed perimeter is established. For more on the GRASP Security Infrastructure and its foundation, see Dimitrakos 2002/3/4, Djordjevic 2004a/b, Ritrovato 2004).

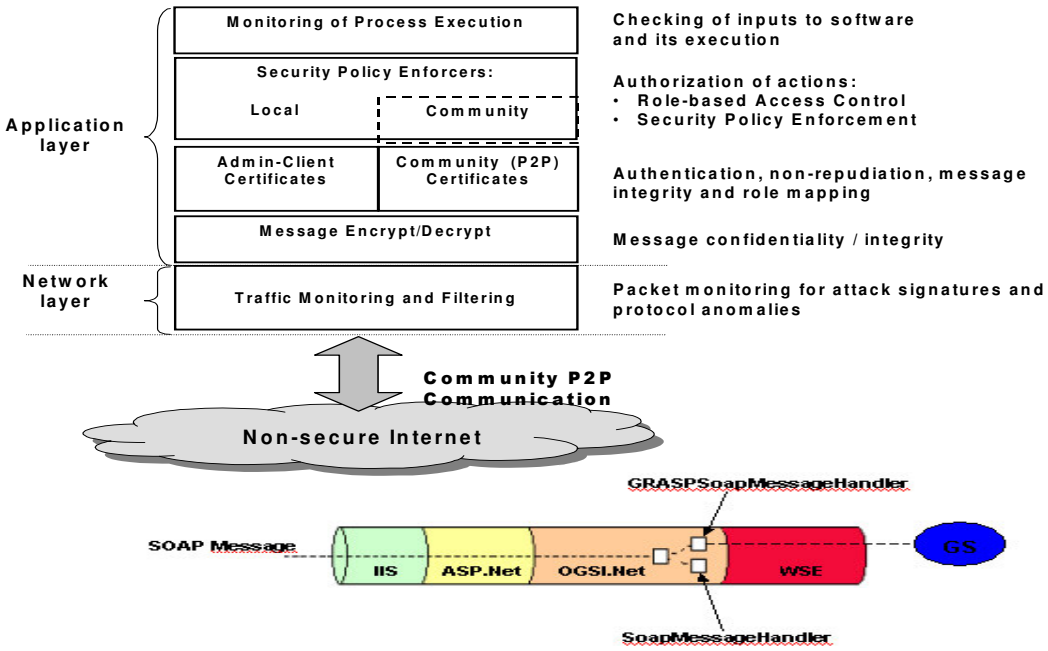

Figure 3. Overview of the GRASP distributed security enforcement architecture

The current implementation of the GRASP Security Infrastructure realizes the distributed enforcement and community management models of this architecture. Although the implementation allows for Attribute Certificates (AC) capturing role information relating to security policies, and for incorporation of an executable containing policy enforcement configuration code, a fully-fledges policy management mechanism and high level policy description language is currently absent.

4 PERMIS

PERMIS is a role-based Privilege Management Infrastructure (PMI). Policies are written in XML and stored embedded in X.509 attribute certificates (ITu-T 2001) in an LDAP directory. Application gateways comprise an application dependent enforcement function (AEF) and application independent decision function (ADF). The interface between the AEF and the PERMIS ADF comprises a decision request and a decision response. This is implemented as either a Java API or as SAML (Oasis 2004) request/response messages, depending upon the choice of the application. A decision request currently comprises: the name of the user, the name of the target, and the action being requested, along with optional environmental parameters such as the time of day. PERMIS makes its access decisions according to the policy retrieved from the policy AC at initialisation time, and the role ACs of the user retrieved at decision time. The PERMIS system structure is illustrated in Figure 4.

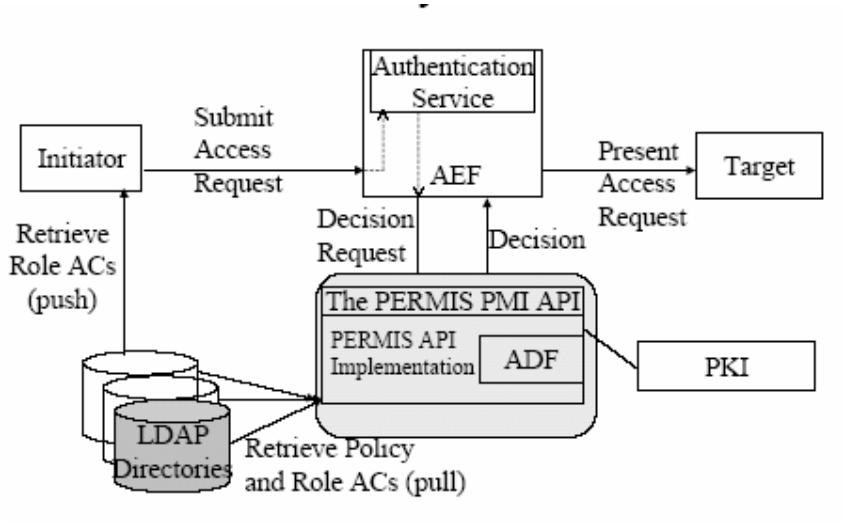

Figure 4: PERMIS API System Structure

5 System integration challenges

5.1 Data Grid Technologies

For a data grid infrastructure to be easy to use and resilient, it will have to support diverse access criteria both within the metadata and the software. However, traditional Grid software solutions showed a lack of stable tools addressing a substantial fragment of the required policy space. By integrating the dynamic community management architecture developed within the GRASP European project and the access control capabilities of PERMIS on top of the current data grid implementations, we expect to provide a reference implementation of a powerful and flexible access control enhancement on top of one of the data grid implementations.

Furthermore, since the GRASP security infrastructure is built using popular and stable "of-the-shelf" technologies and the PERMIS privilege management infrastructure is based on open standard web technologies, we expect the resulting enhancement to be reusable by a variety of domains beyond environmental science.

5.2 GRASP

There are four major changes to the current GRASP security infrastructure which are required to support the proposed infrastructure.

- *Integration with PERMIS.* The local and community security administrators will have to be enhanced to use PERMIS to manage their security policies and to evaluate authorisations for requests from other group members. There are two parts to this. Firstly, the GRASP security administrators will have to be modified to use the PERMIS ACL, and to register these policies in the PERMIS LDAP server. Secondly they will also have to be modified to take advantage of PERMIS decision making mechanisms for allowing or denying a particular action by a particular user with a particular role. Though the GRASP security infrastructure has basically been designed to support a policy management such as those provided by PERMIS, in current implementations decision making is hard-wired to the application, and therefore inflexible.
- *Control of human administrators.* When remote administrators are allowed to assign roles (in the form of X.509 ACs) to members of their domain, the VO administrator may want to limit the scope of their powers. The latter needs to be able to set an assignment policy.

- *Recognition of authority* (Otenko 2003) among different GRASP local security group administrators may also be necessary in order to allow the integration of the local PMI under the jurisdiction of each security administrator by providing a means to one local security administrator to understand the attributes set by another administrator, and exploit the relationship between them in the context of a virtual group that incorporates resources under both administrators. This feature has already been proposed in the DyVOSE project in Glasgow, and we would expect to use it, if provided.
- *Integration into the data centres.* The GRASP security infrastructure relies on local security administrators on the resource site to enforce the relevant security policies. These local security administrators will have to be integrated with the existing security mechanisms in place at the data centres, GRASP has been implemented on top of OGSI.net, so is OGSI compliant. Therefore in theory existing data grid wrappers could be minimally enhanced to invoke existing GRASP security services. However, in practice it will be necessary to co-locate the local security administrators with the wrappers and this implies that the GRASP security services will have to be re-implemented. The group administrators could remain as OGSI.net services, but for consistency they will also be re-implemented on a GT3 (or GT4) platform

5.3 PERMIS

To support this approach the following changes need to be made to PERMIS

- *Separation of duties* is needed to stop users with conflicting roles (potentially in different project teams) from accessing any of the conflicting resources. Separation of duties can be implemented by upgrading the PERMIS policy to list the conflicting roles, and to say which targets are forbidden to the role holders. When PERMIS operates in pull mode this will implement *static* separation of duties (since the user's roles are statically stored in the LDAP directories used by PERMIS). However, when a user operates PERMIS in push mode, and only presents different subsets of roles to PERMIS on different login sessions, this *dynamic* separation of duties is more difficult to enforce. It will require PERMIS to keep a secure audit trail (called retained ADI in the ISO 10181-3 Access Control Framework [ITU-T 1995]) and to review this when making separation of duties decisions.
- *Policy control is needed on authorities* who allocate ACs to their users, to finely control the users to whom they are allowed to confer privileges. Without this fine-grained control at the allocating sites, the target site would need to have a much more complicated and finely tuned policy. In applications such as the ones being run by the data centre, coarse grained control is easier to manage at the target sites, with fine grained control at each of the allocating sites. This will be achieved by building a PERMIS decision engine into the Privilege Allocator and Bulk Loader tools that are part of the current PERMIS NMI release. These tools currently have no restrictions built into them, and their administrators can freely allocate any ACs to any users, the assumption being that the target site will determine which ACs are trusted. In the enhanced infrastructure, target SOAs and/or trusted site SOAs will be able to set PERMIS allocation policies on the privilege allocating tools.
- *Conditional decision making* will need to be implemented so as to restrict user access to one project only up to when another project becomes active. The PERMIS decision engine already supports conditional decision making, by allowing plug-in condition evaluating objects to be added to it. This project will build one such plug-in for PERMIS.

6 Project Status

The above approach to providing access control has bee accepted as the basis of a new JISC funded project, DyCom, between the University of Salford and CCLRC. This is proposing to prototype the architecture within existing NERC funded environmental data grid projects. The resulting implementation and guidance will then be packaged and released to the wider academic community for use in similar project within other domains.

In another project (SIPS), Salford is proposing to modify the PERMIS interface to directly support Shibboleth, so that the SHAR can pass either attributes or ACs directly to PERMIS, or the SHAR can be completely bypassed and the handle passed to PERMIS from the SHIRE. We are assuming that the SIPS development will progress in parallel with this one and be ready to use when this proposal needs it.

References

Dimitrakos, Mac Randal, Wesner, Serhan, Ritrovato, Laria (2004a). *"Overview of an architecture enabling Grid based Application Service Provision"*. 2nd European Across Grids Conference, Nicosia, Cyprus, Jan. 2004

Dimitrakos, Ritrovato, Serhan, Valles, Wesner (2003a) The Grid for e-collaboration and Virtual Organisations *in* P. Cunningham , M. Cunningham and P. Fatelnig (Eds.) Building the Knowledge Economy: Issues, Applications, *Case Studies. IOS Press 2003*

Dimitrakos, Mac Randal, Yuan, Gaeta, Laria, Ritrovato, Serhan, Wesner, Wulf (2003b) *An Emerging Architecture Enabling Grid-based Application Service Provision*. Proc. 7th International Enterprise Distributed Object Computing Conference. EDOC2003. IEEE Computer Society

Dimitrakos, Djordjevic, Matthews, Bicarregui, Phillips (2002). *Policy-Driven Access Control over a Distributed Firewall Architecture*. Policy 2002: 3rd International Workshop on Policies for Distributed Systems and Networks IEEE Computer Society.

Djordjevic, Dimitrakos, Philips (2004a) *An Architecture for Dynamic Security Perimeters of Virtual Collaborative* Organizations Networks Proceedings of the 9th IEEE/IFIP Network Operations and Management Symposium (NOMS 2004). IEEE Communications Society

Djordjevic, Dimitrakos (2004b). *Towards Dynamic Security Perimeters for Virtual Collaborative Networks*. Proceedings of Trust Management:: Second International Conference. Lecture Notes in Computer Science, Vol. 2995, 2004.

ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996 "Security Frameworks for open systems: Access control framework"

ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8: 2001, Information technology – Open Systems Interconnection – Public-Key and Attribute Certificate Frameworks.

OASIS (2004) *Security Assertion Markup Language v.2.0 (SAML)*, OASIS working draft, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Otenko (2003) *Policy-Based Privilege Management Using X.509 (The PERMIS Project)* PhD thesis submitted to University of Salford, June 2003

Ritrovato, Laria, Wesner, Serhan, Dimitrakos, Mac Randal (2004). *Trust, Security and Contract Management Challenges for Grid-based Application Service,Provision* Proceedings of Trust Management:: Second International Conference. Lecture Notes in Computer Science, Vol. 2995, 2004.

Lawrence, Cramer, Gutierrez, Kleese van Dam, Kondapalli, Latham, Lowry, O'Neill, Woolf. (2003) The NERC Datagrid Prototype. AHM 2003, Nottingham, September 2003.

ECO(2003) Ecological Datagrid, http://www.escience.cclrc.ac.uk/web/projects/hydrology_data_grid