SECURITY AND CERTIFICATION ISSUES IN GRID COMPUTING

Ian Foster, Frank Siebenlist, Steven Tuecke, Von Welch
Argonne National Laboratory and The University of Chicago.
foster@mcs.anl.gov

Abstract Grid computing is concerned with the sharing and coordinated use of diverse resources in dynamic, distributed "virtual organizations." The dynamic nature of Grid environments introduces challenging security concerns that demand new technical approaches. In this brief overview, we review key Grid security issues and outline the technologies that are being developed to address those issues. We focus in particular on work being done within the context of the Open Grid Services Architecture, a new initiative aimed at recasting key Grid concepts within a service-oriented framework. This work involves a tight integration with Web services mechanisms and appears particularly relevant to the concerns of e-services.

Keywords: grid computing, Open Grid Services Architecture (OGSA), grid security, certification, global grid forum

1. INTRODUCTION

The term "Grid" is frequently used to refer to systems and applications that integrate and manage resources and services that are distributed across multiple control domains [2]. Initially pioneered in the e-science context, Grid technologies have recently generated considerable interest in the e-business context, as a result of the apparent relevance of Grid distributed management concepts and mechanisms to a variety of commercial distributed computing scenarios [6].

A common scenario within Grid computing—and, we believe, within an increasing number of e-business scenarios—is the formation of dynamic "virtual organizations" (VOs) [5] comprising groups of individuals and associated resources and services united by a common purpose but not located within a single administrative domain. The need to support the integration and management of resources within such VOs introduces challenging security issues. In particular, we have to deal with the fact that for a variety of issues relating to certification, group membership, authorization, and the like, participants in

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: 10.1007/978-0-387-35696-9_19
E. Nardelli et al. (eds.), *Certification and Security in E-Services*

such VOs represent an overlay with respect to whatever trust relationships exist between individual participants and their parent organizations.

Research in Grid computing is producing solutions to some of these problems based around not direct interorganizational trust relationships but rather the use of the VO as a bridge among the entities participating in a particular community or function. The results of this research have been incorporated into a software systems called the Globus Toolkit that is now seeing widespread use [3], and that addresses issues of single sign on, delegation [7, 8], and so forth, while supporting standard APIs such as GSS-API [9]. They are also being incorporated into standards through work on the Open Grid Services Architecture (OGSA) being conducted within the Global Grid Forum (GGF).

In the remainder of this overview article, we outline the nature of the Grid security problem, provide examples of Grid security solutions, and review work being conducted within GGF on OGSA security. We provide plentiful references to other sources for additional information.

2. GRID SECURITY AND CERTIFICATION

Figure 1 illustrates a common situation in Grid computing. Two organizations, A and B, each operate their own corporate security solutions that address certification, authentication, authorization, and so forth. Between the two organizations, however, no trust relationship exists. We now assume that an entity in subdomain A1 wishes to access a resource managed by another individual in subdomain B1 with whom he is engaged in some collaborative activity. (More specifically, as we show here, a task initiated by the first individual wishes to invoke an operation on a server located in subdomain B1.)

In principle, the establishment of such a sharing relationship should be straightforward. In practice, however, it can be difficult for at least three different reasons:

1 *Cross certification.* The entity from A1 can obtain a credential certified by some certification authority in domain A. But in the absence of a trust relationship between A and B, an entity in domain B cannot enforce policies requiring that that credential is issued by an approved certification authority. We need a means of establishing cross-certification between A and B. Or rather we need a means of establishing cross-certification among the entities participating in the VO.

2 *Mechanisms and credentials.* Assuming that the cross-certification problem is solved, we then face another problem. A and B may rely on quite different security mechanisms and credential formats.

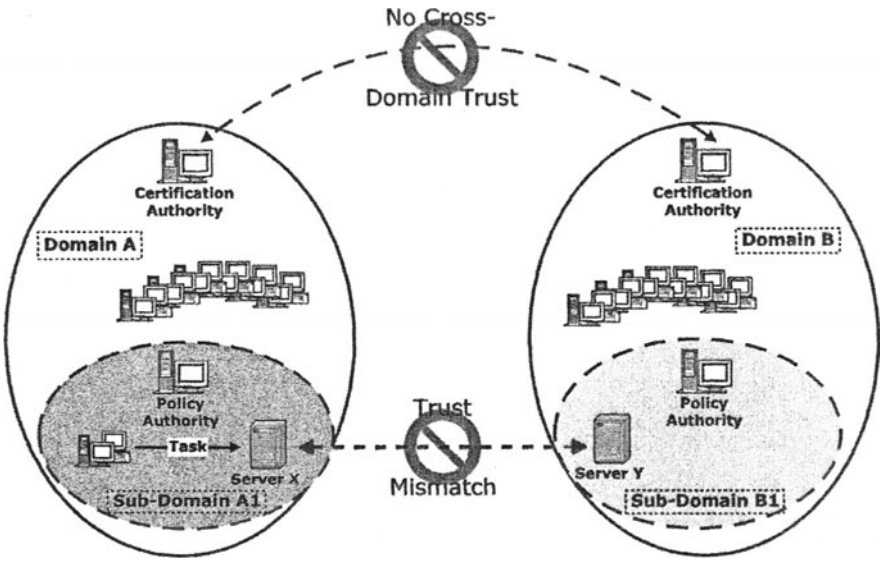

Figure 1 A representative Grid computing scenario, illustrating key certification and trust issues

3 *Distributed authorization.* Another difficulty that arises is that individual entities in one domain are not necessarily well positioned to know all foreign requestors and thus to enforce fine-grained policies based on identity or other characteristics.

4 *Other issues.* Other issues that must be addressed in the VO context include logging and auditing (how do we merge logs and perform auditing across VO resources?).

One approach to addressing these issues is to establish high-level interinstitutional agreements concerning cross-certification, mechanisms and credential formats, authorization, auditing, and so forth. These agreements can be difficult to negotiate, however, because of potentially broad legal implications, liability issues, and the inevitable engagement of central bureaucracies. In practice, many such relationships do not require involvement of upper management: as long as they are consistent with institutional policies, they can be established by organizational subunits or individuals.

These observations have motivated the adoption within Grid computing of approaches in which the virtual organization is used as a bridge and federation is achieved within the VO through mutually trusted services. As illustrated in Figure 2, entities within the VO domain rely on some mutually trusted VO

service to establish trust and use some negotiated common mechanism to negotiate access. Local policy authorities continue to play a role, serving as the final arbiters of what is allowed on a particular resource.

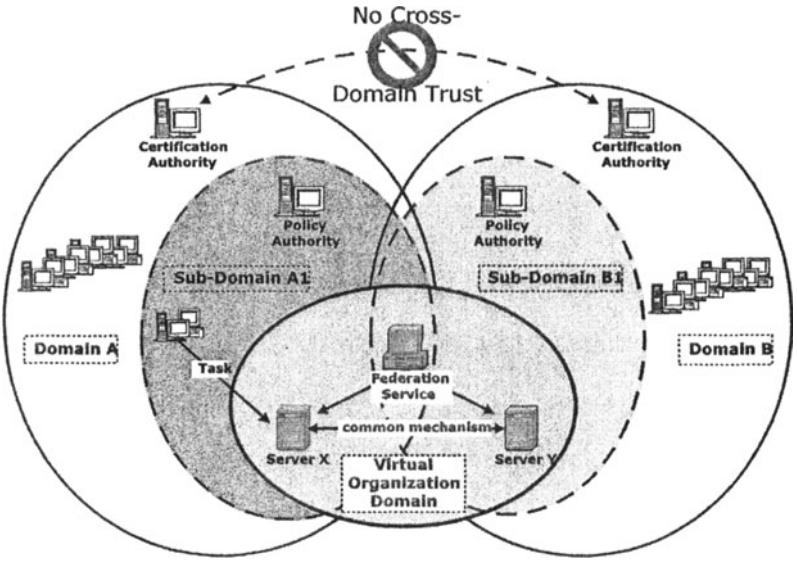

Figure 2 The use of virtual organizations as a bridging mechanism

In the following, we describe mechanisms that have been developed based on this concept to address cross-certification, common credentials and mechanisms, and distributed authorization.

2.1. CROSS CERTIFICATION

Consider the two domains illustrated in Figure 3. We assume that domain A uses Kerberos mechanisms for certification, authentication, and so forth, while domain B uses some other scheme. We also assume a lack of trust relationships between domains A and B.

Figure 3 illustrates a particular implementation of a VO bridging solution to these two problems, based on the use of (a) a bridging certification service (the Kerberos-CA service) and (b) standard X.509 credentials and Grid Security Infrastructure (GSI) mechanisms [4]. The KX509 service and the Globus Toolkit provide commonly used open source implementations of these two functions, respectively.

In brief, participants in the VO agree to use X.509 credentials and GSI protocols as common interorganizational mechanisms. This provides common

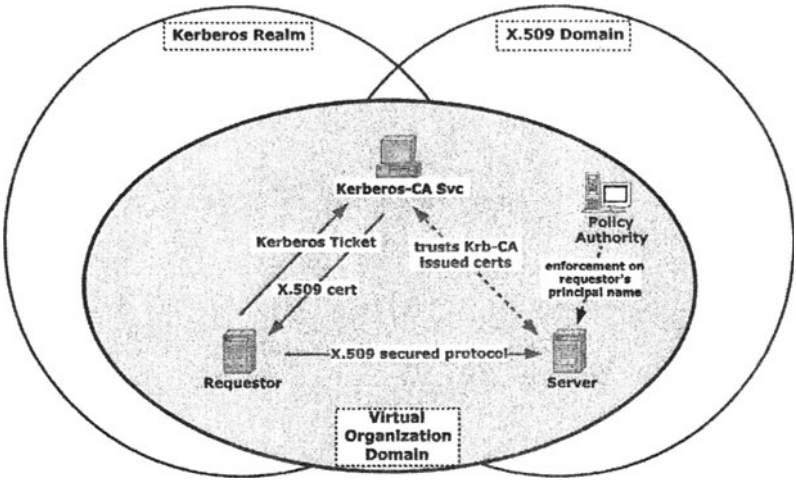

Figure 3 A concrete realization of bridging, in which KX509 is used as a bridging certification service, and X.509 and GSI as common mechanisms

formats for wire-level compatibility for authentication; however, it does not address the issue of interorganization trust. The two organizations still have disjoint entities providing certification of identities. To address the cross-certification requirement, they also agree to trust a VO service, the Kerberos-CA service, as a means of gatewaying from domain A's Kerberos credentials to VO X.509 credentials. An entity in A1 that wishes to issue a request to an entity in B1 must thus first issue a Kerberos-authenticated request to the Kerberos-CA service to obtain an (short-lived) X.509 credential that asserts the requestor's Kerberos principal name. The A1 entity (the requestor) can then present this credential to the entity in B1. The latter entity has a trust relationship with the Kerberos-CA service and can thus verify the authenticity of the credential (e.g., by checking the signature chain) prior to applying VO policies (based on the requestor's Kerberos principal name) and/or local policies to determine whether the request should be granted.

2.2. DISTRIBUTED AUTHORIZATION

A simplistic implementation of the system just described has the disadvantage that each resource in the VO must know all foreign requestors if fine-grained policy is to be applied. A solution to this problem is to outsource fine-grained policy administration to a trusted third party within the VO domain who can more easily maintain information about all requestors. The local domain can, of course, continue to maintain and apply coarse-grained policy.

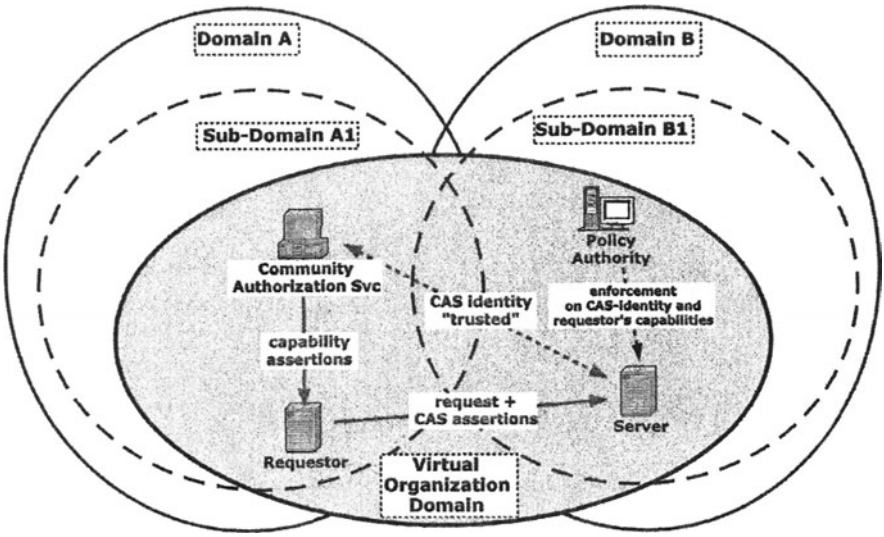

Figure 4 Community authorization service

This idea is implemented by the Community Authorization Service (CAS) [12]. (Neuman proposed, but did not implement, a similar idea [11].) As depicted in Figure 4, a VO wishing to access a CAS-enabled resource in the VO first issues a request to the VO CAS server. The CAS server consults its policy rules regarding the user and, if access is granted, returns a capability credential. This credential is presented to the resource by the user and is used by the resource to establish fine-grained policy. The resource then needs to apply only coarse-grained policy rules based on the CAS identity, although it can of course still apply other local policy.

3. OPEN GRID SERVICES ARCHITECTURE

The preceding discussion introduced some representative Grid security issues and technologies such as GSI, KX509, and CAS that are being used to address these issues. Those technologies represent the current state of the art and are being used extensively in various Grid projects.

Nevertheless, research and development efforts continue within the Grid community with the goals of continuing to expand functionality (e.g., for more general policy specification and enforcement and for auditing) and exploiting standards emerging from the Web services security (WS security) initiative. Working within the context of the Open Grid Services Architecture (OGSA),

these efforts are expected to produce input to the WS Security process and new profiles and service definitions that build on WS Security standards.

OGSA represents a refactoring, refinement, and repackaging of current Grid protocols to better expose various useful elements, incorporate new functionality, embrace a service-oriented model, and leverage emerging Web services technologies. OGSA leverages experience gained with the Globus Toolkit to define conventions and WSDL interfaces for a Grid service, a (potentially transient) stateful service instance supporting reliable and secure invocation (when required), lifetime management, notification, policy management, credential management, and virtualization. OGSA also defines interfaces for the discovery of Grid service instances and for the creation of transient Grid service instances.

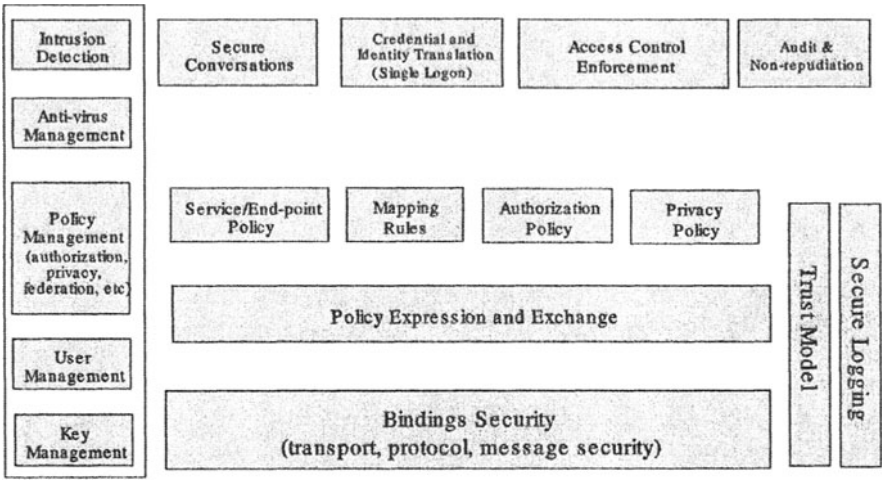

Figure 5 An early view of issues to be addressed within the OGSA security domain

Current goals for OGSA security work are outlined within an architecture document and roadmap that are being developed within the Global Grid Forum. Figure 5, taken from [10], summarizes the key components as currently conceived. The current drafts of these documents focus on defining possible relationships between OGSA security mechanisms and emerging WS Security mechanisms [1]. Thus, they identify a set of required services and indicate for each whether it is definitely provided by WS Security specifications, is expected to be provided by future WS Security specifications, or requires the definition of standardized profiles and/or mechanisms, and/or extensions to WS Security specifications. It is expected, however, that other technologies—for

example, SAML, and specifications being developed within the Project Liberty Alliance—may also have a significant role to play. One task to be addressed by the OGSA Security working group within the Global Grid Forum is to develop an understanding of where other technologies should be used in this overall Grid security work.

4. SUMMARY

Research and application studies in Grid computing have been investigating for some time various issues that are fundamental to e-services. In particular, these studies have addressed the need to provide security and certification services for dynamically formed groups of services, resources, and people—what are often called virtual organizations. The basic technical approach adopted has been to use the virtual organization as a bridging mechanism among its participants.

Existing Grid technologies provided by the Globus Toolkit and related technologies address basic issues of cross-certification, standard credential formats, standard security mechanisms, and community authorization. These technologies have seen widespread adoption within the e-science community and are also starting to see use in industry.

Current work focused on the development of an Open Grid Services Architecture appears even more relevant to e-services, because of its strongly service-oriented architecture and its adoption of Web services technologies. This work is moving quickly within the Global Grid Forum, and both open source and commercial implementations are appearing.

Acknowledgments

Other major contributors to the work on Grid security described here include Carl Kesselman, Sam Meder, Laura Pearlman, Nataraj Nagaratnam, Philippe Janson, John Dayka, and Anthony Nadalin. This work was supported in part by the Mathematical, Information, and Computational Sciences Division subprogram of the Office of Advanced Scientific Computing Research, U.S. Department of Energy, under Contract W-31-109-Eng-38; by the National Science Foundation; by the NASA Information Power Grid program; and by IBM.

References

[1] Security in a Web Services World: A Proposed Architecture and Roadmap. http://www-106.ibm.com/developerworks/library/ws-secmap/, 2002.

[2] I. Foster, and C. Kesselman. Computational Grids. In I. Foster and C. Kesselman, editors, *The Grid: Blueprint for a New Computing Infras-*

tructure. Morgan Kaufmann, 1999.

[3] I. Foster, and C. Kesselman. *The Grid: Blueprint for a New Computing Infrastructure*, chapter The Globus Toolkit, pages 259–278. Morgan Kaufmann, 1999.

[4] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke. A Security Architecture for Computational Grids. In *ACM Conference on Computers and Security*, pages 83–91. ACM Press, 1998.

[5] I. Foster, C. Kesselman, and S. Tuecke. The Anatomy of the Grid: Enabling Scalable Virtual Organizations. *International Journal of Supercomputer Applications*, 15(3), 2001. http://www.globus.org/research/papers/anatomy.pdf.

[6] I. Foster, C. Kesselman, J. Nick, and S. Tuecke. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. http://www.globus.org/research/papers/ogsa.pdf, February 2002.

[7] M. Gasser, and E. McDermott. An Architecture for Practical Delegation in a Distributed System. In *Proc. 1990 IEEE Symposium on Research in Security and Privacy*. 1990.

[8] T. Hardjono, and T. Ohta. Secure End-to-End Delegation in Distributed Systems. *Computer Communications*, 17(3):230–238, 1994.

[9] J. Linn. Generic Security Service Application Program Interface. *Internet RFC 1508*, 1993.

[10] N. Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist, V. Welch, I. Foster, and S. Tuecke. The Security Architecture for open Grid Services. Technical report, Global Grid Forum, 2002.

[11] B.C. Neuman. Proxy-Based Authorization and Accounting for Distributed Systems. In *13th International Conference on Distributed Computing Systems*. 1993.

[12] L. Pearlman, V. Welch, I. Foster, C. Kesselman, and S. Tuecke. Community Authorization Service for Group Collaboration. In *Proceedings of the IEEE 3rd International Workshop on Policies for Distributed Systems and Networks*. 2002.