Grid Security-an Adaptive Technique

Anjali Kalra[1], Sarbjeet Singh[2], Sukhvinder Singh[3]
M.Tech. CSE(1st Year).
Sri Sai College of Engg. And Technology, Pathankot[1,2,3]

Abstract
Grid computing is concerned with the creation of distributed virtual organizations across multiple control domains to enable the sharing of diverse remote resources. Due to its multi-institutional nature, securing the grid is one of the main challenges in grid computing. In this paper an overview of the grid security fundamentals, requirements, models, architecture, and use patterns is provided. The major security challenges and requirements for grids, the main grid security models that address these requirements, current grid security architectures, emerging grid security services , the convergence of grid services are studied in this paper.

KeyWords:
Grid, Grid computing, grid security

1. Introduction

Grid computing [4] is the aggregation of networked connected computers to form a large-scale distributed system used to tackle complex problems. By spreading the workload across a large number of computers, grid computing offers enormous computational, storage, and bandwidth resources that would otherwise be far too expensive to attain within traditional supercomputers. High-performance computational grids involve heterogeneous collections of computers that may reside in different administrative domains, run different software, be subject to different access control policies, and be connected by networks with widely varying performance characteristics. The security of these environments requires specialized grid-enabled tools that hide the mundane aspects of the heterogeneous grid environment without compromising performance. These tools may incorporate existing solutions or may implement completely new models. Grid computing is distinguished from conventional distributed computing by its focus on large-scale pervasive resource sharing, virtual and pluggable high-performance orientation. Security is a major issue that must be resolved in order for the potential of the grid to be fully exploited. The heterogeneous nature of resources and their differing security policies are complicated and complex in the security schemes of a grid computing environment. These computing resources are hosted in different security domains and heterogeneous platforms. The major security requirement for the grid is centered on the dynamic configuration of its security services, such as data integrity, confidentiality, and information privacy in potentially volatile environments. In general, the purpose of security mechanisms is to provide protection against malicious parties. Traditional security mechanisms typically protect resources from malicious users by restricting access to only authorized users[2]. However, in many situations within distributed applications one has to protect oneself from those who offer resources so that the problem is in fact reversed. The paper is organized as- Section 2 describes the requirements of a secure grid infrastructure, section 3 describes the grid security model, section 4 describes the grid security architecture and section 5 provide details about OGSA security, section 6 concludes the whole paper.

2. Requirements of a Secure Grid Infrastructure

The security challenges faced in a grid environment can be grouped into three categories: integration with existing systems and technologies, interoperability with different hosting environments (e.g., J2EE servers, .NET servers, Linux systems), and trust relationships among interacting hosting environments. Relationship between these categories is as shown in Figure1.

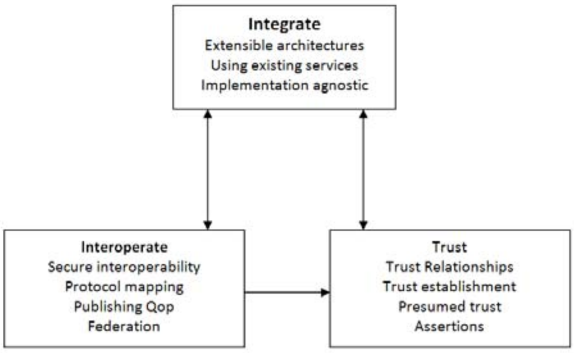

Figure1- Security Challenges in Grid Computing.

Manuscript received June 5, 2010
Manuscript revised June 20, 2010

2.1 The Integration Challenge

For both technical and pragmatic reasons, it is unreasonable to expect that a single security technology can be defined that will both address all grid security challenges and be adopted in every hosting environment. Existing security infrastructures cannot be replaced overnight. Similarly, authentication mechanisms deployed in an existing environment that is reputed secure and reliable will continue to be used. Each domain typically has its own authorization infrastructure that is deployed, managed, and supported. It will not typically be acceptable to replace any of these technologies in favor of a single model or mechanism.

2.2 The Interoperability Challenge

Services that traverse multiple domains and hosting environments need to be able to interact with each other, thus introducing the need for interoperability at multiple levels. At the *protocol level*, it is required mechanisms that allow domains to exchange messages; this can be achieved, for instance, via SOAP/HTTP. At *the policy level*, secure interoperability requires that each party be able to specify any policy it may wish in order to engage in a secure conversation and that policies expressed by different parties can be made mutually comprehensible. Only then can the parties attempt to establish a secure communication channel and security context upon mutual authentication, trust relationships, and adherence to each other's policy. At the *identity level*, mechanisms for identifying a user from one domain in another domain are required.

2.3 The Trust Relationship Challenge

The VOs that underlie collaborative work within grids may form quickly, evolve over time and span organizations; as discussed before, their effective operation depends on trust. In the simple case, personal knowledge between parties in the VO allows policies to be derived from identifiable trust "anchors" (parties vouching for other parties). An example in current grid systems is the use of certificate authorities to root certificate-based identity mechanisms. For these to work, one must "know" about the trustworthiness of the certificate authority used to establish the identity of a party in order to bind it to specific usage policies. However, personal knowledge does not scale for the case on nontrivial VOs, which are most of the VOs, and it is necessary that other technologies such as reputation management [15] are in place to create and monitor relationships.

3. Grid Security Model

Ensuring the integrity, confidentiality, and security of Web services through the application of a comprehensive security model is critical, both for organizations and their customers, which is the fundamental starting point for constructing virtual organizations. The secure interoperability between virtual organizations demands interoperable solutions using heterogeneous systems. For instance, the secure messaging model proposed by the Web Services Security roadmap [7] document supports both public key infrastructure (PKI) and Kerberos mechanisms as particular embodiments of a more general facility that can be extended to support additional security mechanisms. The security of a grid environment must take into account the security of various aspects involved in a grid service invocation. This is depicted in Figure 2.

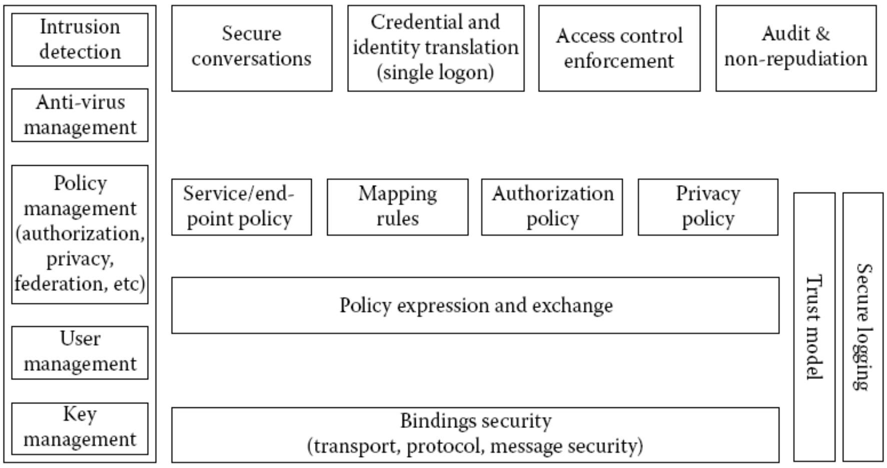
Intrusion detection
Anti-virus management
Policy management (authorization, privacy, federation, etc)
User management
Key management
Secure conversations
Credential and identity translation (single logon)
Access control enforcement
Audit & non-repudiation
Service/end-point policy
Mapping rules
Authorization policy
Privacy policy
Policy expression and exchange
Bindings security (transport, protocol, message security)
Trust model
Secure logging

Figure2- Components of grid security model.

A Web service can be accessed over a variety of protocols and message formats it supports. Each participating end point can express the policy it wishes to see applied when engaging in a secure conversation with another end point. Policies can specify supported authentication mechanisms, required integrity and confidentiality, trust policies, privacy policies, and other security constraints. Given the dynamic nature of grid service invocations, end points will often discover the policies of a target service and establish trust relationships with it dynamically. Once a service requestor and a service provider have determined the policies of each other, they can establish a secure channel over which subsequent operations can be invoked. Such a channel should enforce various qualities of service including identification, confidentiality, and integrity. The security model must provide a mechanism by which authentication credentials from the service requestors' domain can be translated into the service providers' domain and vice versa. This translation is required in order for both ends to evaluate their mutual access policies based on the established credentials and the quality of the established channel.

4. Grid Security Architecture and standards

The grid environment and technologies address seamless integration of services with existing resources and core application assets. As discussed in the Grid Security Model section, the grid security model is a framework that is extensible, flexible, and maximizes existing investments in security infrastructure. It allows the use of existing technologies such as X.509 public key certificates, Kerberos shared-secret tickets, and even password digests. Therefore, it is important for the security architecture to adopt, embrace, and support existing standards where relevant. Given grid services are based on Web services, grid security model will embrace and extend the Web services security standards proposed under the WS Security roadmap [7]. Specifically, given that OGSA is a service-oriented architecture based on Web services (i.e., WSDL-based service definitions), the OGSA security model needs to be consistent with Web services security model. The Web services security roadmap [wssecurity-roadmap] provides a layered approach to address Web services, and also defines SOAP security bindings.

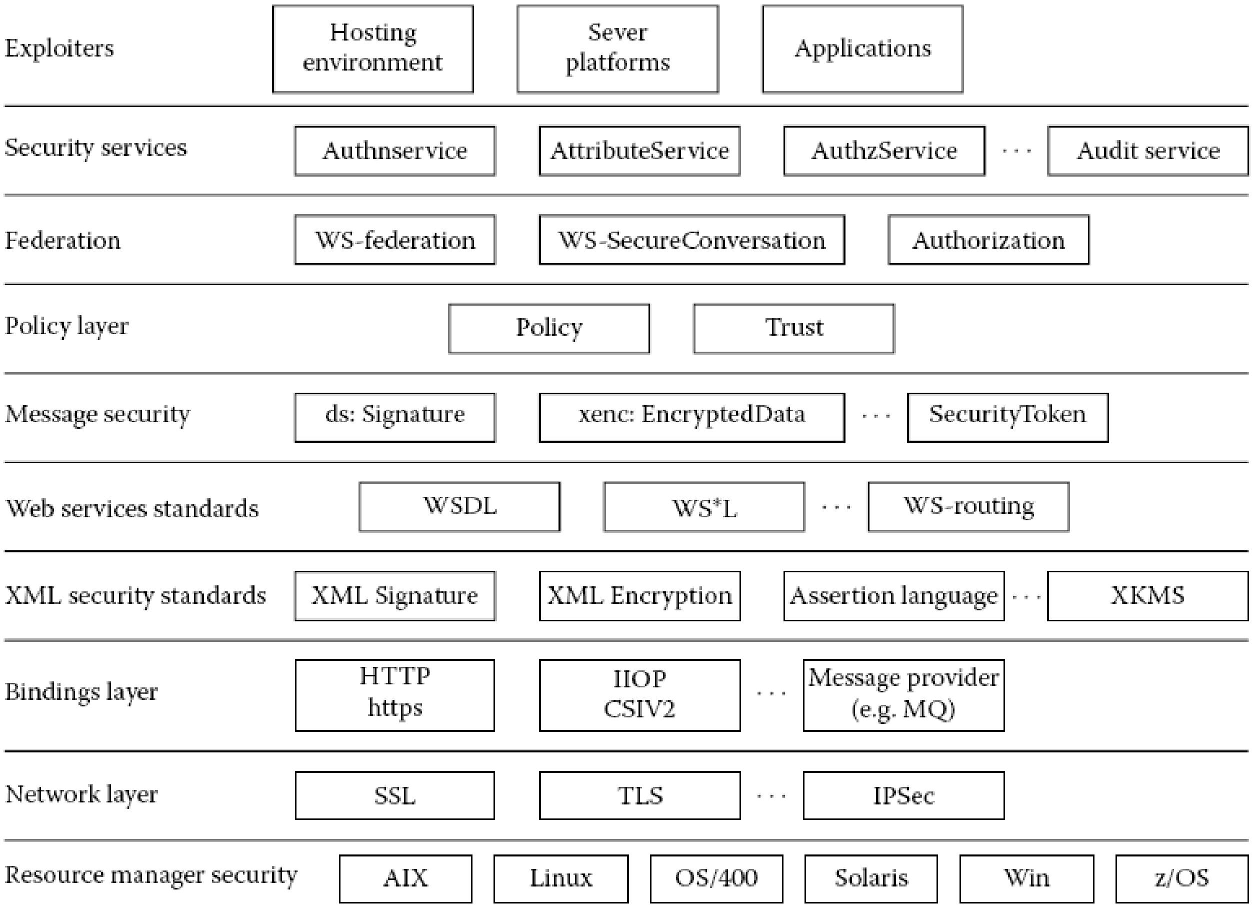

Figure3- Grid Security architecture.

5. OGSA Security

An OGSA infrastructure may use a set of primitive security functions in the form of services themselves. Following are the security services suggested by OGSA:

- An authentication service: An authentication service is concerned with verifying proof of an asserted identity.
- Identity mapping service: The identity mapping service provides the capability of transforming an identity that exists in one identity domain into an identity within another identity domain. The identity mapping service is not concerned with the authentication of the service requestor; rather it is strictly a policy-driven name mapping service.
- Authorization service: The authorization service is concerned with resolving a policy-based access control decision. The authorization service consumes as input a credential that embodies the identity of an authenticated service requestor and for the resource that the service requestor requests, resolves based on policy, whether the service requestor is authorized to access the resource.
- VO policy service: The VO policy service is concerned with the management of policies. The aggregation of the policies contained within and managed by the policy service comprises a VO's policy set.
- Audit service: The audit service, similar to the identity mapping and authorization services, is policy driven. The audit service is responsible for producing records, which track security-relevant events.
- Profile Service: The profile service is concerned with managing a service requester's preferences and data that may not be directly consumed by the authorization service. This may be service requester specific personalization data.
- Privacy Service: The privacy service is primarily concerned with the policy-driven classification of personally identifiable information (PII).

6. Conclusion

This paper describes various security requirements and challenges of a grid i.e. integration, interoperability and trust relationship challenges and the relationship between them. The security architecture and the grid security model are also described in this paper. Security services of grid by OGSA architecture are authentication, authorization, identity mapping, VO policy, audit, profile and privacy services are also described in this paper.

References

[1] N. Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist,V.Welch, S. Tuecke, and I. Foster. Security Architecture for Open Grid Services.

[2] I. Foster, C. Kesselman, G. Tsudik, and S. Tuecke. Proc. A Security Architecture for Computational Grids. 5th ACM Conference on Computer and Communications Security Conference, pp. 83–92, 1998.

[3] I. Foster, C. Kesselman, J. Nick, and S. Tuecke. The Physiology of the Grid: An Open Grid Services Architecture for Distributed Systems Integration. January, 2002.

[4] C. Lai, G. Medvinsky, and B.C. Neuman, Endorsements, Licensing, and Insurance for Distributed System Services. In Proc. 2nd ACM Conference on Computer and Communication Security, 1994.

[5] N. Sklavos and P. Souras, Economic Models and Approaches in Information Security for Computer Networks, International Journal of Network Security (IJNS), Science Publications, Vol. 2, No. 1, January, pp. 14–20, 2006.

[6] N. Sklavos and O. Koufopavlou, Access Control in Networks Hierarchy: Implementation of Key Management Protocol, International Journal of Network Security (IJNS), Science Publications, Vol. 1, No. 2, September, pp. 103–109, 2005. State-of-the-Art Security in Grid Computing 237

[7] I. Foster, C. Kesselman, and S. Tuecke. International J. Supercomputer Applications, The Anatomy of the Grid: Enabling Scalable Virtual Organizations, 2001.

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

[9] The SSL Protocol Version 3.0. http://home.netscape.com/eng/ssl3/draft302.txt.

[10] RFC 2246: The TLS Protocol. ftp://ftp.isi.edu/in-notes/rfc2246.txt.

[11] The Common Object Request Broker: Architecture and Specification, Version 2.3.1. The Object Management Group (OMG), http://www.omg.org/cgi-bin/ doc?formal/99-10-07.

[12] Common Secure Interoperability Version 2 Final Available Specification. The Object Management Group (OMG), http://www.omg.org/cgi-bin/doc?ptc/2001-06-17.

[13] Java 2 Platform, Enterprise Edition, v1.5 (J2EE). http://java.sun.com/j2ee.

[14] The Platform for Privacy Preferences 1.0 (P3P1.0) Specification, W3C Recommendation 16 April 2002, http://www.w3.org/TR/P3P/.

[15] S. Tuecke, K. Czajkowski, I. Foster, J. Frey, S. Graham, and C. Kesselman. Grid Service Specification. Draft 2, 6/13/2002, http://www.globus.org.

[16] M.D. Abrams, M.V. Joyce. Trusted Computing Update. Computers and Security, 14(1):57–68, 1995.

[17] R. Alfieri et al. VOMS: An Authorization System for Virtual Organizations. In Proceedings of 1st European Across Grids Conference, Santiago de Compostela, 2003. Available from: http://gridauth.infn.it/docs/VOMS-Santiago.pdf.

[18] A.E. Arenas, I. Djordjevic, T. Dimitrakos, L. Titkov, J. Claessens, C. Geuer-Pollman, E.C. Lupu, N. Tuptuk, S.Wesner, and L. Schubert. TowardsWeb Services Profiles for Trust and Security in Virtual Organisations. IFIP Working Conference on Virtual Enterprises PRO-VE05, Valencia, Spain, 2005.

[19] S. Boeyen et al. Liberty Trust Models Guidelines. In J. Linn (editor), Liberty Alliance Project. Liberty Alliance, draft version 1.0, 2003.

[20] M. Brady, D. Gavaghan et al. eDiamond: A Grid-Enabled Federated Database for Annotated Mammograms. In F. Berman, G. Fox, T. Hey (editors), Grid Computing: Making the Global Infrastructure a Reality, Wiley, 2003.