Shielding the Grid World: An Overview

Christos Chrysoulas
(Corresponding author: Christos Chrysoulas)

Electrical & Computer Engineering Deapartment, University of Patras
(Email: cchrys@ece.upatras.gr)

(Received Mar. 20, 2014; revised and accepted Apri. 30, 2014)

Abstract

Continues research and development efforts within the Grid community have produced protocols, services, and tools that address the challenges arising when we seek to build scalable virtual organizations (VOs). The technologies that have evolved from the Grid community include security solutions that support management of credentials and policies when computations span multiple institutions; resource management protocols and services that support secure remote access to computing and data resources and the co-allocation of multiple resources; information query protocols and services that provide configuration and status information about resources, organizations, and services; and data management services that locate and transport datasets between storage systems and applications.

Keywords: Grid computing, Security, Web services

1 Introduction

Grid computing [1-2] 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 are possible to make use of existing solutions or can implement completely new models. In either case, research is required to understand the utility of different approaches and the techniques that may be used to implement these approaches in different environments. Grid computing is distinguished from conventional distributed computing by its focus on large-scale pervasive resource sharing, virtual and pluggable high-performance orientation. The electrical power grid's pervasiveness and reliability inspired computer scientists in the mid-1990s to explore the design and development of a new infrastructure, computational power grids for network computing. The real and specific problem that underlies the Grid concept is coordinated resource sharing and problem solving in dynamic, multi-institutional virtual organizations. The sharing is not just file exchange but rather direct access to computers, software, data, and other resources, as is required by a range of resource brokering strategies emerging in industry, science, and engineering.

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 [3], such as data integrity, confidentiality, and information privacy in potentially volatile environments.

The rest of the document is structured as follows. Section 2 presents the Grid security model. Section 3 and Section 4 discusses security binding and security associations respectively. Section 5 presents authentication in Grid systems. Section 6 gives an insight on available security standards. Security in web service is provided in Section 7 while Section 8 analyzes the grid security infrastructure. Finally Section 9 concludes the document.

2 Grid Security Model

Web services (WS) [4] is an emerging architecture that has the ability to deliver integrated, interoperable solutions. Ensuring a) integrity, b) confidentiality, and c) security of Web services through the use of a comprehensive security model is critical, both for organizations and their customers. The secure "transactions" between virtual organizations demands interoperable solutions using heterogeneous systems. For instance, the secure messaging model proposed by the

Web Services Security roadmap [5] 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 1.

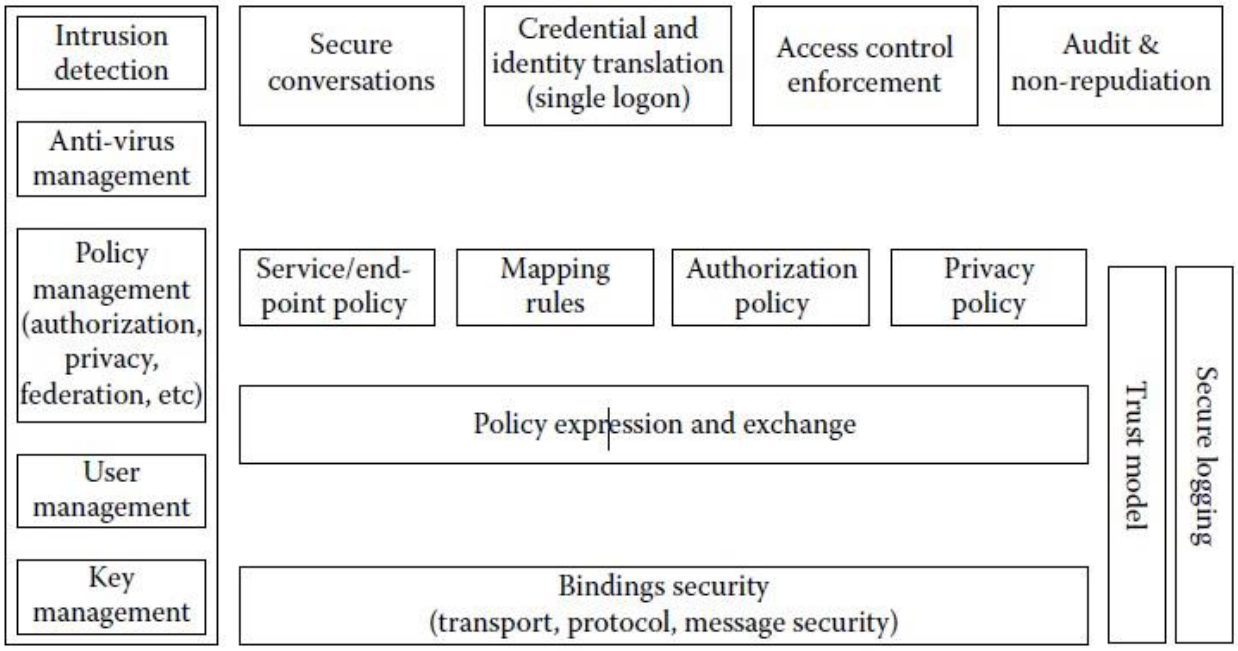

Figure 1: Grid security model components

3 Binding Security

The set of bindings to be considered includes SOAP (SOAP/HTTP, SOAP over a message queue or SOAP over any other protocol) and IIOP bindings. The security of a binding is based on the security characteristics of the associated protocol and message format. If new protocols or message formats are introduced, care should be taken to address security requirements in those bindings so that, at a minimum, suitable authentication, integrity, and confidentiality can be achieved.

HTTP is an important protocol to consider because of its transparency to firewalls and wide adoption. In the case of bindings over HTTP, requests can be sent over SSL (i.e., https) and thus SSL can provide authentication, integrity, and confidentiality. However, SSL ensures these qualities of service only among participating SSL connection end points. If a request needs to traverse multiple intermediaries (firewalls, proxies, etc.), then end-to-end security needs to be enforced at a layer above the SSL protocol.

In the case of SOAP messages, security information can be carried in the SOAP message itself in the form of security tokens defined in the WS-Security specification [5]. SOAP messages can also be integrity and confidentiality protected using XML Digital Signature and XML Encryption support, respectively. Signature and encryption bindings defined in WS-Security can be used for this purpose.

Web services can be accessed over IIOP when the service implementation is based on CORBA. In the case of IIOP, the security of the message exchange can be achieved by using the Common Secure Interoperability specification, version 2 (CSIv2). This specification is also adopted in J2EE.

In addition to, binding-level security requirements, network security solutions (e.g., firewalls, IPSec, VPN, DNSSEC, etc.) remain useful components for securing a Grid environment. Firewalls can continue to enforce boundary access rules between domains and other network-level security solutions can continue to be deployed in intradomain environments. Grid services deployment can take the topology into consideration when defining security policies. At the same time, deployment assumptions may be surfaced as policies attached to firewalls and network architecture.

The Grid security model must be able to leverage security capabilities of any of these underlying protocols or message

formats. For example, in the case of SOAP over HTTP requests, one can use WS-Security for end-to-end security functionality, HTTPs for point-to-point security, and SSL, TLS, or IPSec for other purposes. Security requirements for a given Web service access will be specified and honored based on the set of policies associated with the participating end points. For example, a policy associated with a Web service can specify that it expects SOAP messages to be signed and encrypted.

Thus, service requestors accessing that service would be required to use WS-Security to secure their SOAP requests. Addressing the security of the service bindings will address the requirements related to integrity and confidentiality of messages, achieving delegation facilities, and facilitating firewall traversal.

4 Secure Associations

A service requester and a service provider are likely to exchange more messages and submit requests subsequent to an initial request. In order for messages to be securely exchanged, policy may require the service requester and service provider to authenticate each other. In that case, a mechanism is required so that they can perform authentication and establish a security context.

This security context can be used to protect exchange of subsequent messages. As an added benefit, using the established security context will improve the performance of secure message exchanges. The period of time over which a context is reused is considered a session or association between the interacting end points. Security context establishment and maintenance should be based on a Web service context (to be) defined within Web or Grid service specifications.

The notion of a context is tightly coupled with the bindings. Many existing protocols (e.g., IPSEC, SSL, IIOP) and mechanisms (e.g., Kerberos) already support secure association contexts. For example, in the case of IIOP, context establishment is based on the CSIv2 specification. In the case of SOAP, the context can be carried and secured as part of the SOAP messages.

WS-Secure Conversation will describe how a Web service can authenticate service requestor messages, how service requestors can authenticate service providers, and how to establish mutually authenticated security contexts. WS-Secure Conversation will be designed to operate at the SOAP message layer so that the messages may traverse a variety of transports and intermediaries. Therefore, in the case of SOAP bindings, the Grid security model should adopt WS-Secure Conversation to establish security contexts and exchange messages securely. Alternatively, depending on the constraints of a VO's other technologies (e.g., SASL, BEEP, etc.) may be used. Therefore, the mechanism used to establish security contexts between end points will be based on the bindings used as well as the policy associated with the end points.

Facilitating secure association is required to establish the identity of a requestor to the service provider (and vice versa) so that the service provider (and service requestor) can satisfy the requirements to authenticate the identity on the other end and then enforce authorization and privacy policies based on the established identity. The identities of the requestor and service provider are required for auditing purposes, so that audit logs will contain information about accessing identity.

5 Authentication in Grid Systems

A computational Grid has been defined as "a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities." Typically, Grid resources are provided by various organizations and are used by people from diverse sets of organizations. A Grid may support (or define) a single virtual organization or it may be used by more than one virtual organization. Individual pieces of hardware may be used in more than one Grid, and people may be members of more than one virtual organization. The different resources in a Grid may have different access policies, including how they authenticate and authorize users. If no common or overlapping authorizations exist among the resources, however, they do not form a usable Grid.

Users, hosts, and services need to be able to authenticate themselves in the Grid environment. Experience in using Grids for remote computations has demonstrated the need for unattended user authentication in addition to interactive authentication. Unattended authentication of users is needed when a user is making frequent requests to remote servers and does not want to repeatedly type in a pass phrase and when a long-running job may need to authenticate itself after the user has left. Servers specific to a single host mays need to be started at system boot time and run with their own or the host's identity. Some services may need to be started periodically on many different hosts and be able to authenticate themselves with a known identity.

Basically, authentication between two entities on remote Grid nodes means that each party establishes a level of trust in the identity of the other party. In practical use an authentication protocol sets up a secure communication channel between the authenticated parties, so that subsequent messages can be sent without repeated authentication steps,

although it is possible to authenticate every message. The identity of an entity is typically some token or name that uniquely identifies the entity.

6 Relationship to Security 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 [5].

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 provides a layered approach to address Web services, and also defines SOAP security bindings. Figure 2 illustrates the layering of security technology and standards that exist today and how they fit into the Grid security model.

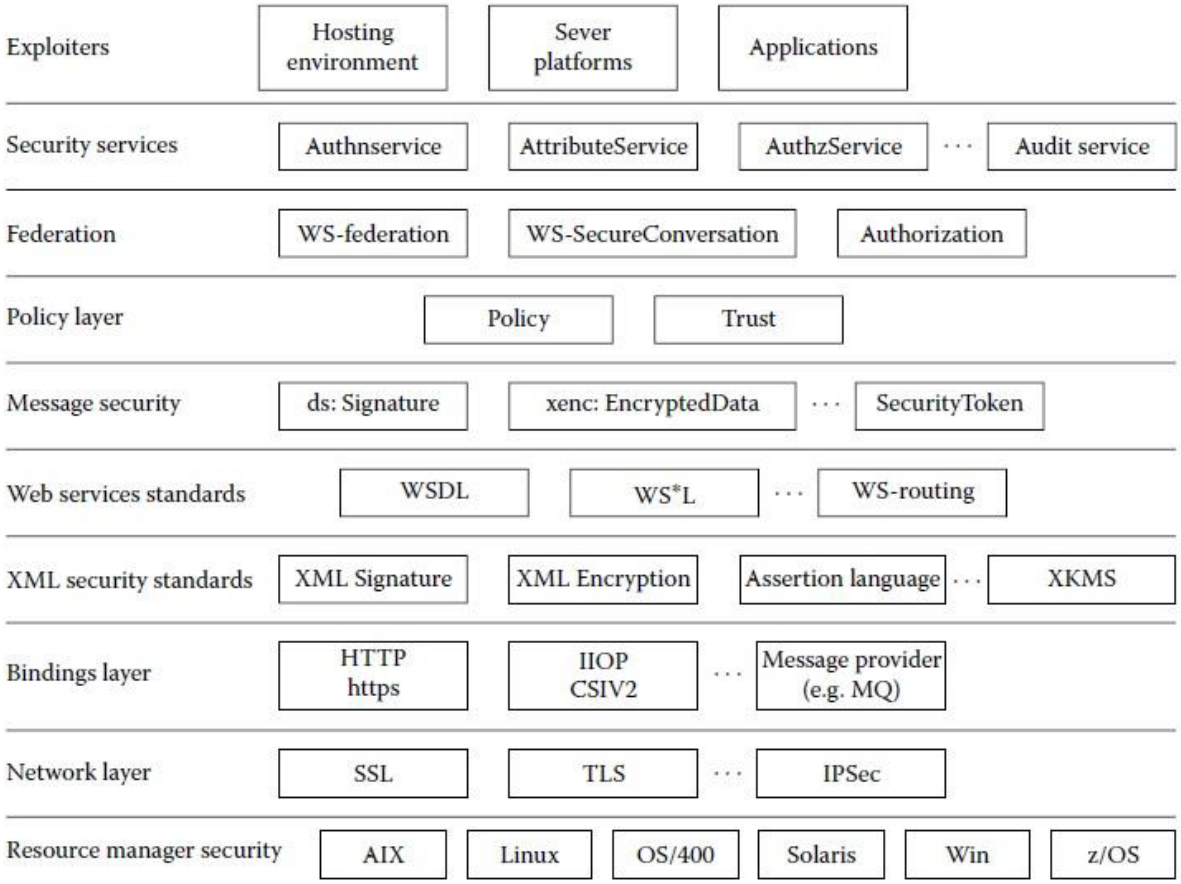

Figure 2: Building blocks for grid security architecture

7 What about Security in Web Services

Web services offer an interoperable framework for stateless, message-based, and loosely coupled interaction between software entities. These entities can be spread across different companies and organizations, can be implemented on different platforms, and can reside in different computing infrastructures. Web services expose functionality via XML messages, which are exchanged through the SOAP protocol. The interface of a Web service is described in detail in an XML document using the "Web Service Description Language" (WSDL).

In order to provide security, reliability, transaction abilities, and other features, additional specifications exist on top of

the XML/SOAP stack. The creation of the specifications is a cross-industry effort, with the participation of standardization bodies such as W3C and OASIS. A key element in the Web services specifications is the so-called combinability. Web services specifications are being created in such a way that they are mostly independent of each other; however, they can be combined to achieve more powerful and complex solutions. In this section we describe some individual specifications, specifically focusing on those dealing with secure and reliable transactions.

8 Grid Security Infrastructure

In grid computing environments, the mutual authentication and information service are serious issues. Before their applications are running, the users need to choose hosts based on security, availability, and many other aspects. The GSI (Grid Security Infrastructure) is designed as one very important part of the Globus grid toolkit. The GSI uses public key cryptography (also known as asymmetric cryptography) as the basis for its functionality.

The primary motivations behind the GSI are the need for secure communication (authenticated and perhaps confidential) between elements of a computational Grid and the need to support security across organizational boundaries, thus prohibiting a centrally managed security system. Finally, a fundamental issue is to support "single sign-on" for users of the Grid, including delegation of credentials for computations that involve multiple resources and/or sites.

GSI, which is designed to solve the security in the Globus system, is based on RSA encystations algorithm and employs a standard (X.509v3) for encoding credentials for security principals, and thus enables secure authentication and communication over open network. At the same time GSI enables Interoperable with local security solutions without changing anything. The Grid Security Infrastructure (GSI) is a specific implementation of an OGSA-based Grid security architecture that include as part of the Globus Toolkit Version 5 (GT5).

9 Conclusions

Grid computing has really distinct security themes in comparison to other traditional computing systems. The most important security problems [7] include, but not limited to the following ones: a) Impact on Local Host: Grid computing involves running an alien code in the host system. This external code can hamper jobs running locally, and compromise local data security, b) Vulnerable Hosts: Clients using the grid remain in danger from the local hosts. The major vulnerabilities include the local hosts shutting down resulting in denial of service, viruses, or other malware in the local host affecting the entire process, and local hosts compromising client data integrity and confidentiality, c) Interception: One major security risk with grid computing is an attacker intercepting the resources and data in the grid. The attack can take various forms such as a distributed denial-of-service (DDOS) attack, and d) Packet Losses: Interruption of nodes during the routing process to send packets from source to destination decreases total packet delivery and loss or corruption of data.

The extent of security risks when using smart grid depends on the intellectual property put in the hosted environment

Most of the security issues regarding the a grid system can be solved with the use of a monitoring agency that deals with: a) the monitoring of the resource, b) the creation, management and negotiation of trust among the different actors in the grid and c) the establishment of an authorization system in order to authorize user access to specific resources.

The user running an application on a remote machine in the grid-computing network requires assurance of the machine retaining its integrity, to ensure that proprietary application remains safe. The local host requires a similar assurance regarding the client data and processes that run on the host. While the safeguards of a traditional system aim at protecting the system and data from its users, the security orientation of grid systems need to go a step ahead and also protect applications and data from the system where the computation takes place.

Grid computing security requires strong authentication and restrictions on local execution from remote systems. Some of the solutions can be: a) Secure grid communication using public key cryptography, b) Authentication or verifying identity of the participant, c) Single sign on in order to reduce the number of times a user needs to enter password, d) Filtering and auditing of data, and e) Erasing of data after use.

The gains resulting from grid computing already surpass the security risks, and since security problems find nowadays easy and realistic solutions, grid computing is becoming more and more a commonplace.

References

[1] I. Foster, C. Kesselman and S. Tuecke, "The anatomy of the Grid enabling scalable virtual organizations". International Journal of Supercomputer Applications, vol. 15, pp.200-222, 2001.

[2] I. Foster, C. Kesselman, J. M. Nick and S. Tuecke, "The physiology of the grid, an open grid services architecture for distributed systems integration", Open Grid Service Infrastructure WG, Global Grid Forum, 2002. www.globus.org/alliance/.

[3] Y. Xiao, "State-of-the-art security in grid computing". in Security in distributed, grid, mobile and pervasive computing. Auerbach, New York, pp.207-236, 2007.

[4] N. Nagaratnam, P. Janson, J. Dayka, A. Nadalin, F. Siebenlist,V.Welch, S. Tuecke, and I. Foster. "Security architecture for open grid Services", GWD-I (draft-ggf-ogsa-sec-arch-01), July, 2002.

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

[6] 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.

[7] "A Look at Security Problems with Grid Computing", Accessed 22/4/2014 http://www.brighthub.com/environment/green-computing/articles/94587.aspx

Christos Chrysoulas received his PhD in Electrical & Computer Engineering from the Electrical & Computer Engineering Dept., University of Patras, Greece in 2009. He received his Diploma in Electrical & Computer Engineering from the Electrical & Computer Engineering Dept., University of Patras, Greece in 2003. Since 2009, he is working as an Adjunct Professor, in the Technological Educational Institute of Patras, HELLAS. He is teaching in the Informatics & MM Department and in Museology and Museography Department. From July 2013 he is with the CISTER Research Center as a Research Associate. His research interests include Computer Networks, High Performance Communication Subsystems Architecture and Implementation, Wireless Networks, New Generation Networks Architectures, Resource Management and Dynamic Service Deployment in New Generation Networks and Communication Networks, Grid Architecture, Semantics. During the last year he is intensively working in the Smart Grid area, as a system architect expert. He is also interested in Cyber physical systems. Christos Chrysoulas has published more than 10 technical papers in these areas. He has also participated as Senior Engineer in European Research Projects.