A New Architecture of Grid Security System Construction*

MingChu Li, Yongrui Cui, Yuan Tian
School of Software, Dalian University of Technology
Dalian 116620, P.R. China.
Email: li_mingchu@yahoo.com
Dong Wang
School of Computer Science, Tianjin University
Tianjin 300072, China
Songyuan Yan
Coventry University, Coventry CV1 5FB, United Kingdom

Abstract

Due to the complexity of Grid computing, many new security problems have appeared in grid, and so the traditional network security practices can not meet the security demand of grid. As a result, the study of security problems in grid is important, complicated and arduous. In this paper, we propose a new approach to construct grid security systems, and analyze both the disadvantages of current existing grid security systems. Our grid security system framework is positioned as an alternative to the security framework of Open Grid Service Architecture (OGSA). Based on our analysis, we conclude that a security system in grid should be composed of two parts: security rule definitions and security rule implementation. We also discuss the advantages of our new security system architecture.

Keywords: *grid, security system, security rule definition, framework*

1. Introduction

Grids [3] have emerged as a common approach to construct dynamic, inter-domain, distributed computing and data collaborations. The Globus Toolkit[4] has been the dominant middleware for grid deployments worldwide. Grid security infrastructure (GSI)([2], [5]) is the portion of the Globus Toolkit that provides the fundamental security services needed to support grids. GSI provides libraries and tools for authentication and message protection that use standard X.509 public key certificates [6], public key infrastructure (PKI), the SSL/TLS protocol [1] and X.509 proxy certificates. GSI and proxy certificates have been used to build numerous middleware libraries and applications that have been widely deployed in large production and experimental grids. Because of the complexity of grid computing, a lot of new security problems have appeared in grid, and so the traditional network security practices can not meet the security demand of grid. Thus the study of security problems in grid is important, complicated

* Supported by Natural Science Foundation of China under Grant No. 90412007.

and arduous. Actually, current researches on information security are still decentralized, and there is no unified, overall cognition in information security. However, with the development of security and network technology, there is the deep interpenetration among various security problems. So there is the obvious trend toward the unified and the integration of some systems. For example, Firewall systems and Intrusion and Detection Systems (IDS) are integrated into one system to serve the security management of local network. A big scale of application systems also integrate various technologies such as encryption, digital signatures, authentication, data protection and so on to support security requirements and other demands. Thus these trends give us a hint that various aspects of information security have much to do with one another, and so the essence of information security needs to be studied. In this paper, we will explore the problem in grid computing environment (see Section 2). We will propose a new approach to construct grid security systems for solving grid security problems. In this paper, we analyze both the disadvantages of current existing grid security system framework and the essence of information security. Based on our analysis, we conclude that a security system in grid should be composed of two parts: security rule definition and security rule implementation, and a new framework on grid security system other than the security framework of Open Grid Service Architecture (OGSA) of Globus (see Figure 1) is putted forward. We also discuss the advantages of our new architecture.

We start with the discussion of the disadvantages of current existing security framework such as OGSA of Globus in Section 2. Section 3 discusses the necessity of constructing grid security systems. In Section 4, we provide a new architecture for grid security systems and make comparison between current security framework and new security system architecture. Section 5 includes this paper.

2. Disadvantages of Current Grid Security Architectures

It is easy to see that researchers have already considered how to implement security functions while designing grid systems. First, Grid security infrastructure (GSI) was proposed by the extension of original security protocols, and then Web Service Security (WS-Security) framework is constructed after the development of Open Grid Services Architecture (OGSA) (see Figure 1). We easily see that the designs of these frameworks follow the following two rules.

(1). Combining existing techniques and actual applications, researchers integrate various security techniques to support network security. For example, Integrating secure sockets layer (SSL) protocols to support communication security, and extending public key infrastructure (PKI) to support the authentication.

(2). The design of security framework is in accordance with grid system framework. For example, in OGSA, because the communication is based on HTTP protocols and message description is adopted by XML, researchers use SSL protocol to do intercommunication.

We know that current security framework in Globus is based on Web Service Security, and provides users with security functions as a kind of security service. This framework proposes the constitute mode of security functions in grid system, but not give out any full description for security system. That is, the security component

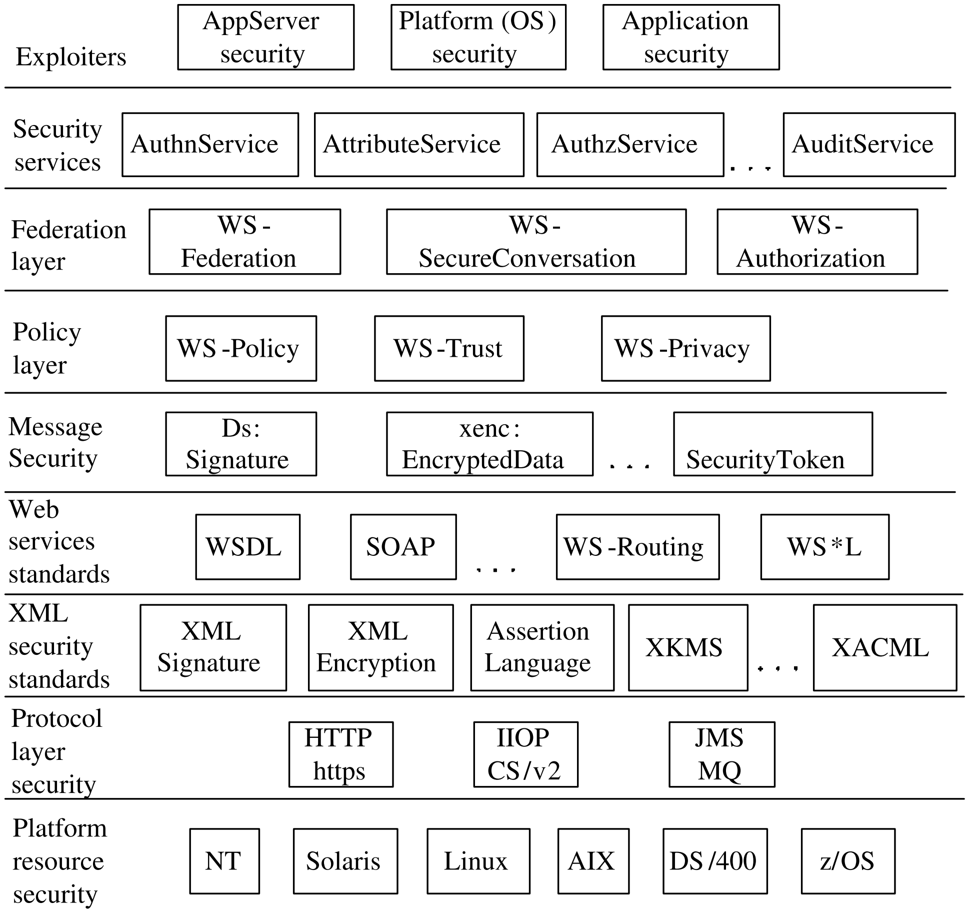

Figure 1. OGSA security framework

is dispersed to distributed systems, and security functions are not organized to form an independent system. Thus such architecture has following three disadvantages.

A. **Weak extension**. Because the security framework has high cohesion with grid architectures, its architecture is not easy to be extended when grid framework changes.

B. **Conflict**. Because different security function executes independently, there is no unified organized manner and cooperative mechanism with each other. Thus, as soon as several security functions need to be executed, conflict may occur.

C. **Insufficient transparency**. Transparency in current grid systems is not enough for users. When security functions need to be increased strongly, users may not know how to make correct choices or effectively use security functions. As a result, security leak may happen.

From the discussion above, building a security system is urgently needed for grid systems.

3. Necessity of Building Security Systems in Grid

As we know, a grid computing system is built on the foundation with large scale distributed, dynamic change resources. Resources and users in grid may belong to different trusted domain, and resource nodes in grid are distributed in Internet. Thus grid security needs two kinds of services: one is to guarantee the security inside the grid system itself; the other is to guarantee the security outside the grid system. If the two kinds of security problems interweave together, the situation would become more complicate. In such circumstance, if we could build a grid security system, we would put all security problems into the grid security system so that the complicated problem can be simplified. On the other hand, if we could build a grid security system, we would make integrity of various security functions and use unified standards inside the system so that the association of various security taches become tighter and so some security leaks are reduced. As a result, the grid system can obtain more perfect security support from the security system.

Again, with the building of security systems, we can make the security system low coupling with other systems in grid systems, which will benefit the extension of security functions in the future.

4. A New Architecture of Security System in Grid

In section, we provide our new security system architecture (see Figure 2), and make comparison between current security framework and our new security system architecture (see Table 1). From the discussion in Sections 2 and 3, we see that building a security system is urgently needed for grid system, and the security system should provide overall support for grid security. Thus we need to explore the architecture for the security system. Based on the essence of information security, the problems in information security remain with the management ones of using message permission by users, where the management functions involve two aspects: the permission enactment of message processing by users, and putting in practice of permission policies by concrete security techniques. Thus we should follow the two aspects to build our security system, and also need to consider the characteristics of grid system architecture so that our security system can provide security support for static status and dynamic status. Thus we provide the following new security system architecture in grid (see Figure 2). In order to understand our architecture better, we now explain them as follows.

In our grid security system (see Figure 2), the bottom layer is called *basic security constitute elements.* It consists of *security algorithms, security data and certificate infrastructure.* The *security algorithms* involve various basic information security algorithms such as encryption/decryption algorithms, private key generation algorithms, digital signature algorithms, certificate generation services, and so on. The security data are the various ones which are used to achieve security functions, such as symmetric secret keys, public keys, private keys, pseudo-random numbers and certificates. *Certificate infrastructure* is the PKI system which is used to do authentication in grid. *Security middleware* is based on the basic security constitute elements, and provides static services and dynamic services. The static services are the ones which can be directly used in applications by users, such as encryption, the generation of certificates. They consist of two parts: invocation interfaces of security services and security function composition. The component of security functions composition can integrate different security functions so that it can provide more security support for users. For example, users can call the services of the transmitted data secret and the data integrity to achieve the encryption of the transmitted data

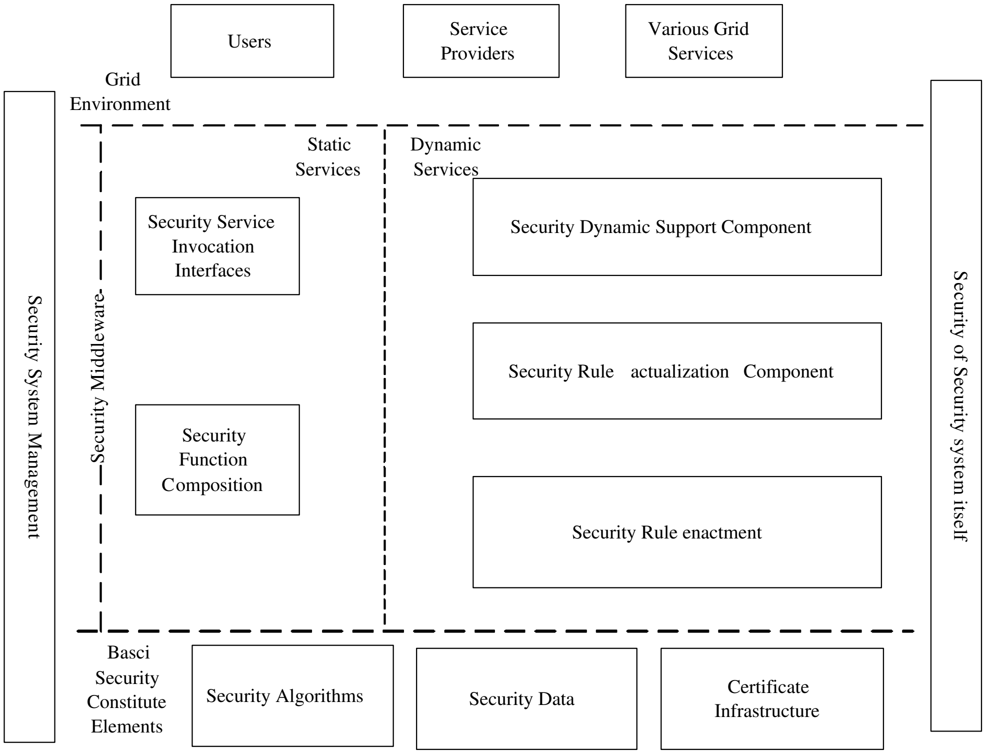
Users
Service Providers
Various Grid Services
Grid Environment
Security System Management
Security Middleware
Static Services
Dynamic Services
Security Service Invocation Interfaces
Security Function Composition
Security Dynamic Support Component
Security Rule actualization Component
Security Rule enactment
Security of Security system itself
Basci Security Constitute Elements
Security Algorithms
Security Data
Certificate Infrastructure

Figure 2. A new grid security system architecture

and the protection of data integrity. The static services provide the security services for grid users, services providers and specific grid services by invoking the interfaces of security services.

Dynamic services are to automatically provide the services of common security safeguard by grid security systems. Common security safeguard is to assure reasonable allocation of permission among users and various trusted domains so that the data can be accessed only if it is permitted by grid security, the processes can be invoked only if permitted, and communication can be made only if permitted.

The realization of dynamic security services is associated with system architectures and running mechanism. In order to support the dynamic security services of the system, we must analyze security requirements of the system and then enact the corresponding permission polices, and then implement these rules by various security techniques. Finally, the support of dynamic security services in running is provided by the dynamic security support components. The dynamic security support components are associated with grid system constitutes, and achieve the monitoring and dynamic control of entities' actions, and can automatically adopt different security measure according to the different change of permission status among entities.

In order to assure normal run in grid security systems, we need to provide the management mechanism in invocation, maintenance and so on for grid security systems. At the same time, we also need to warrant the security of the system itself.

In order to understand the advantages of our new security system architecture better, we make com-

	Current Grid Security Framework	New Grid Security System Architecture
Constitute Mode	Embedding into grid system framework	As an independent system, it interacts with grid system
System Coupling	High	Low
Extensible	Weak	Strong
Dynamic Security Support	NOT	YES
Overall Security Management	NOT	YES
Integrate existing Techniques	YES	YES
Cooperative with other Components?	YES	Yes

Table 1. The Comparison between the current grid security framework and the new security system architecture

parison between the current grid security framework and our new security system architecture in Table 1.

5. Summary

The implementation and operation of secure services running on a large-scale grid leads to many challenges on security. Our project is developing a new security system to handle various security problems. The security problems in grid are very important issues. How to construct a security system is also an important task in the future. Because of the high complexity of grid computing system, grid needs to build an unified security system to support all security functions, which resides in grid systems, is independent with other systems and has good cooperative relation with other systems. In this paper, we make some exploration for constructing a grid security system. Our security system architecture has many advantages over current security framework.

References

[1] T. Dierks and C. Allen, The TLS protocol version 1.0, RFC 2246, IETF, 1999.

[2] I. Foster, C. Kesselman, G. Tsudik and S. Tuecke, A security architecture for computaional grids, ACM conference on computers and security, 1998, 83-91.

[3] I. Foster, and C. Kesselman, Computational Grids, The Grid: Blueprint for a New Computing Infrastructure (I. Foster and C. Kesselman eds), Morgan Kaufmann, 1999, 2-48.

[4] I. Foster, and C. Kesselman, Globus: A Toolkit-Based Grid Architecture, The Grid: Blueprint for a New Computing Infrastructure (I. Foster and C. Kesselman eds), Morgan Kaufmann, 1999, 259-278.

[5] J. Joseph and C. Fellenstein, Grid computing, IBM press, Prentice Hall, 2004

[6] R. Housley, W. Polk, W. Ford and D. Solo, Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, RFC 3280, IETF, April 2003