Chapter 10
Security Standards and Issues for Grid Computing

Athanasios Moralis
National Technical University of Athens, Greece

Vassiliki Pouli
National Technical University of Athens, Greece

Mary Grammatikou
National Technical University of Athens, Greece

Dimitrios Kalogeras
National Technical University of Athens, Greece

Vasilis Maglaris
National Technical University of Athens, Greece

ABSTRACT

Security in grid environments that are built using Service Oriented Architecture (SOA) technologies is a great challenge. On one hand, the great diversity in security technologies, mechanisms and protocols that each organization follows and on the other hand, the different goals and policies that these organizations adopt, comprise a complex security environment. Authenticating and authorizing users and services, identity management in a multi-organizational scenario and secure communication define the main context of the problem. In this chapter, we provide an overview of the security protocols and technologies that can be applied on a Web Service (WS) based grid environment.

INTRODUCTION

A Grid is a large-scale generalized network system that offers computing resources across multiple organizations and administrative domains. For the transport of the data across the grid nodes and the interaction of the users with the grid resources, mechanisms should be utilized to assure those. The Web Services (WSs) based on the Service Oriented Architecture (SOA) provide this.

SOA provides the basic paradigm for building software applications that can be applied in today's complex and heterogeneous environments. SOA is the first integration and architec-

DOI: 10.4018/978-1-61350-113-9.ch010

tural framework that uses services available in the web and promotes loose coupling between software components, thus resulting in reusable components. SOA uses as basic building blocks the services. A service is an implementation of a well-defined business functionality. Following this strict approach, this kind of services can then be consumed by clients in different applications or by business processes. SOA in general does not impose any style of services. However, the de-facto standard is using WS Architecture to realize a SOA architecture. WSs are based on various eXtensible Markup Language (XML) standards such as Simple Object Access Protocol (SOAP), Universal Description, Discovery and Integration (UDDI), Web Services Description Language (WSDL) and designed to support interoperable machine-to-machine interaction over a network.

The wide acceptance that WSs meet is largely due to the need of integration heterogeneous applications across different systems belonging to different organizations across the Internet. WS Technologies enable more dynamic, loosely-coupled and synchronous or asynchronous interactions between both inter-domain and intra-domain applications. WSs expose in a standardized way to external clients the application's interface, with the use of WSDL, hiding in most cases the application's internal complexity. As they are often used over the Internet, for mission-critical transactions with the possibility of dynamic, short-term relationships, security is a major concern. This elevates the value of securing them against a wide range of attacks, both internal and external. The main security issues that have to be addressed are authentication, authorization, confidentiality, data integrity, non-repudiation, single sign on, delegation, trust and identity mapping.

To meet these security requirements, some WS compatible mechanisms have been defined, i.e. WS Security Specifications (Rosenberg & Remy, 2004), that apply at the message level and provide ways to transfer security tokens and credentials thus generally achieving end-to-end (from client to service) security functionality.

Specific consortiums have been constituted to address and provide standards for these kinds of WS related issues (Singhal, 2007). Major standardization initiatives, among them, are the World Wide Web Consortium (W3C) and the Organization for the Advancement of Structured Information Standards (OASIS). These organizations try to standardize WS specifications (including WS Security Specifications) and provide a common and global framework so that organizations and applications can interoperate in heterogeneous environments. Principal developers of the WS Security (O' Neill, 2003) standards are the IBM, Microsoft, VeriSign that have submitted the WS Security Specification to OASIS and it was approved.

The rest of the chapter is organized as follows. In the following section we provide the basic background, covering the WSs Security (WSS) standard. The next section describes the additional standards that complement the WSS, along with related issues that each standard may have. The two last sections provide the future directions while they conclude the chapter.

BACKGROUND

Traditionally, communications have been protected at the network layer by adopting technologies such as the Secure Socket Layer (SSL) or the Transport Layer Security (TLS) (Dierks & Rescorla, 2006) and the Internet Protocol Security (IPSec) (Kend & Atkinson, 1998).

SSL/TLS is a connection oriented protocol that offers several security features including authentication, data integrity and data confidentiality. SSL/TLS enables point-to-point secure sessions. Similarly, IPSec is a network layer standard for transport security that provides secure sessions with host authentication, data integrity and data confidentiality. Both of these technologies are