Chapter 4.11
Credential Management Enforcement and Secure Data Storage in gLite

Francesco Tusa
Università degli Studi di Messina, Italy

Massimo Villari
Università degli Studi di Messina, Italy

Antonio Puliafito
Università degli Studi di Messina, Italy

ABSTRACT

This article describes new security solutions for Grid middleware, and specifically faces the issues related to the management of users' and servers' credentials, together with storing and secure data transmission in the Grid. Our work, built on Grid Security Infrastructure (GSI), provides new capabilities (i.e. smart card Grid access, and strong security file storage XML-based) to be used on top of different Grid middlewares, with a low level of changes. This work is currently implemented on gLite and accomplishes the access to Grid resources in a uniform and transparent way. These improvements enable the Grid computing toward the new processing model known as business services.

INTRODUCTION

In the last years, a huge amount of scientific computations has been performed on the Grid, thus addressing the always increasing demand for computational and storage power, and offering an infrastructure available to the scientists 24 hours-a-day. The geographically spread resources of Grid can be virtually exploited as a traditional computing system by means of a specific middleware that hides much of the complexity, giving the user impression that all the resources are available as a coherent computer center (Foster, Kesselman, & Tuecke, 2001).

Both gLite (The Enabling Grids for E-sciencE project: http://www.eu-egee.org/, 2009) and Globus (Foster & Kesselman, 1998) grid middlewares

DOI: 10.4018/978-1-4666-0879-5.ch4.11

refer to the Grid Security Infrastructure (GSI) (Foster, Kesselman, Tsudik, & Tuecke, 1998) for enabling secure authentication and communication over an insecure network. GSI is based on public key encryption (Brincat, 2001), X.509 certificates (Housley, Ford, Polk, & Solo, 1999) and the SSL (Secure Sockets Layer) communication protocol (Dierks & Allen, 1999). According to the GSI specifications, a user needs to have a trusted X.509 certificate in order to be authenticated on the Grid. The certificate must by issued by a Certification Authority (CA) (Weise, 2001).

When originally thought, the Grid was a mean to share resources among academic partners based on trusting. The current security infrastructure, exactly matches the scientists' requirements in terms of authentication needs to access the grid computational resources. Nowadays the Grid is emerging as a valid support also for commercial applications. As evidence, the European Commission (EC) is also trying to move toward the use of grid resources in business context. EC has funded a "Business Experiments in Grid Technologies" (BEinGRID: http://www.beingrid.eu/, 2009) project, to foster the adoption of the so-defined Next Generation Grid technologies by the accomplishment of several business experiments.

However, to be the Grid recognized as a key enabling technology for commercial applications, it is necessary to guarantee better services in terms of QoS, accountability (S-Sicilia Project. Bringing commercial applications to the Grid: http://ssicilia.unime.it/, 2009) and security. We focus on this latter aspect, proposing both an encrypted file storage and a user credential management system, based on smart card devices and crypto-tokens. This article aims to build an additional security layer on top of the existing security infrastructure: the integrations involve accounting mechanisms on the User Interface[1] (UI), storage encryption on the Storage Elements[2] (SE) and data computing on the Worker Nodes[3] (CE).

According to the existing authentication mechanisms of gLite, both the user X.509 certificate (i.e. the RSA public key together with the related user identity) and the related RSA private key are stored on the UI home directory on two different files: the first one contains the public key and the related user credentials while the second one holds the user private key. Both files are encoded using the Privacy Enhancement for Internet Electronic Mail (PEM) format (Linn, 1993). Thus, the user private key plays a crucial role and the fact it is stored on the file system implies that it could be potentially stolen and then employed by insider attackers (e.g. malicious system administrator). According to the traditional GSI authentication model, in order to gain access to a grid resource, a user has to employ his own RSA key-pair for generating a temporary proxy certificate (Tuecke, Welch, Engert, Pearlman, & Thompson, 2004). Once this latter is generated, it has to be digitally signed (Brincat, 2001) through the RSA private key associated to the user himself.

This is the first security issue we intend to address, proposing and implementing a new solution for storing and using the RSA private key in a more secure way than the existing one: a new credential management system has been developed exploiting smart cards to store and interact with the user's RSA key-pair. By means of the introduced tweaks, all the cryptographic operations involving the key-pair (mainly the private key) can be directly performed on the smart card, supplied with an ad hoc micro-processor, exploiting the user private key it stores (as detailed in Section "Architecture"). In order to implement the previously described features, the voms-proxy-init software module of the UI has been modified: the source code involved in the proxy certificate generation has been integrated with a new component to allow the interaction with the smart card device.

We also present an innovative solution for storing data in a secure way into the Grid, validated through a performance analysis of the costs, comparing the job execution time with and without security features. Our contribution points out