Globus Security Infrastructure: Uma Infra-Estrutura de Segurança para Grades Computacionais

Reinaldo Bezerra Braga[1], Felipe Sampaio Martins[1,2,*], Janine Silva da Costa[1,2,**], Rossana M. C. Andrade[1,3]

[1]CENAPAD-NE – Centro Nacional de Processamento de Alto Desempenho no Nordeste
Universidade Federal do Ceará

[2]Pós-graduação em Engenharia de Tele-Informática
Universidade Federal do Ceará

[3]Departamento de Ciência da Computação
Universidade Federal do Ceará

e-mails: {reinaldo, felipe, janine}@cenapadne.br, rossana@lia.ufc.br

1. Introdução

O *Globus Security Infrastructure* (GSI) disponibiliza um conjunto de ferramentas e bibliotecas que possibilitam o acesso seguro de aplicações e usuários aos recursos de uma grade computacional [1].

O projeto GRAD-GIGA, coordenado pelo SINAPAD, dentro da chamada RNP 01/2004, tem como objetivo a construção de uma grade de produção nacional, englobando os sete CENAPADs, utilizando o Globus Toolkit como plataforma, cuja infra-estrutura de segurança é oferecida pelo GSI.

O objetivo deste trabalho é descrever as principais características do GSI, detalhando suas funcionalidades e demonstrando como este conjunto de ferramentas torna possível uma comunicação segura em ambientes de grades.

2. Características do GSI

Com o crescimento das grades computacionais, surgiu a necessidade de se pensar em um esquema que permitisse uma comunicação segura entre elementos do ambiente, com suporte à autenticação, incluindo delegação de credenciais para os recursos [2].

Motivado por isso, a API-GSI, desenvolvida pela Globus Alliance [3], baseia-se em chaves criptografadas, certificados no padrão X.509, e *Secure Sockets Layer* (SSL) como protocolo de comunicação [4].

As características de segurança do GSI estão voltadas principalmente para a autenticação, comunicação segura, autorização e privacidade. Os elementos da grade (usuários, estações e recursos) utilizam certificados, contendo informações relativas à identificação e autenticação, assinados por um *Certificate Authority* (CA).

---

* Bolsista de mestrado financiado pela FUNCAP

** Bolsista de mestrado financiada pelo Instituto Atlântico, Convênio INST. ATLÂNTICO/FCPC PT-07

O GSI oferece duas formas de autenticação, a única e a mútua. Na autenticação única (*single sign-on*), o usuário autentica-se apenas uma única vez para, a partir de então, utilizar usuários *proxies*, que podem iniciar procedimentos no sistema e alocar recursos da grade, não importando o domínio administrativo em que ele se encontra. Tratando-se de autenticação mútua, esta utiliza SSL e envolve a troca de certificados entre os elementos da grade.

Para garantir a segurança na comunicação, o GSI implementa um conceito de Assinaturas Digitais, responsáveis pela autenticidade e integridade dos dados de origem. Essa abordagem permite prevenção de bloqueios ao envio de informações (não repúdio). Por se basear em funções *Hash*, as assinaturas digitais proporcionam uma melhoria na Assinatura Digital Simples, recebendo a entrada de dados encriptados de tamanhos variados e produzindo um tamanho fixo, o que torna a transmissão de informações não só mais segura como também mais eficiente.

Outra característica relevante é a delegação de credenciais, que se dá através da criação de usuários *proxies*. As chaves privadas e os certificados X.509, criados para cada usuário *proxy* gerado remotamente dentro da grade, devem ser assinados pela chave original do usuário credenciado.

3. Considerações Finais

Dentre os requisitos de segurança para o GRAD-GIGA, o GSI contempla os principais: *single sign-on*, interoperabilidade com soluções de segurança local, proteção e delegação de credenciais, privacidade, não-repúdio e integridade dos dados entre os centros.

Pela inexistência de um mecanismo que garanta a integridade de execução dos *jobs* faz-se necessário a implementação de um módulo que assegure a entrega correta dos *jobs* processados. Constitui-se, portanto, como trabalho futuro, o desenvolvimento de um módulo de segurança que possibilite a integridade dos *jobs* dentro de cada centro que compõe o projeto GRAD-GIGA.

4. Referências

[1] Pearlman, L., Welch, V., Foster, I., Kesselman, C., Tuecke, S., A Community Authorization Service for Group Collaboration . In: IEEE 3rd International Workshop on Policies for Distributed Systems and Networks, 2002, p. 2.

[2] Globus Alliance. GSI: Key concepts. Overview of the Grid Security Infrastructure. Disponível em <http://www-unix.globus.org/toolkit/docs/3.2/gsi/key/index.html>. Acesso em: 03 Janeiro 2005

[3] The Globus Alliance. Disponível em <http://www.globus.org/>. Acesso em: 27 Janeiro 2004.

[4] Enacts. Grid Service Requirements . EPCC e Centro de Computação Poznan para redes Enacts. Relatório setorial. Janeiro de 2002. p. 45.