Um Modelo de Segurança em Grades Computacionais para o projeto GRAD-GIGA

Reinaldo B. Braga[1], José Bringel Filho[1], Felipe S. Martins[1,2], Rossana Andrade[1,2,3]

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

[2]Pós-Graduação em Engenharia de TeleInformática
Universidade Federal do Ceará

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

{reinaldo,bringel,felipe}@cenapadne.br, rossana@lia.ufc.br

***Abstract**. This paper describes a security model that allow reducing the possibilities unauthorized access as well as providing data privacy and integrity in a grid environment using Globus Toolkit 3.2. With intention of identifying invasion attempts and confirming grid attacks occurrence, an intrusion detection system was added as part of the model.*

***Resumo.** Este trabalho descreve um modelo de segurança que permite reduzir as chances de acesso não autorizado de usuários, bem como prover a confidencialidade e integridade dos dados transmitidos em um ambiente de grades computacionais implantado, utilizando a plataforma Globus Toolkit 3.2. Com o intuito de identificar tentativas de invasão e confirmar a ocorrência de ataques à grade, um sistema de detecção de intrusão foi adicionado como parte deste modelo.*

1. Introdução

Em Grades Computacionais, falhas na especificação das condições de segurança e controle de acesso podem acontecer, permitindo o acesso não autorizado aos recursos e as tarefas em execução na grade [Grid Stack 2005]. Tais falhas podem causar impacto em diferentes níveis, caracterizando-se desde o desgaste da imagem da organização até a perda ou exploração de informações importantes.

Neste contexto, o modelo de segurança proposto neste artigo destina-se a suprir as necessidades de segurança no sub-projeto GRAD-GIGA [SINAPAD 2005], o qual objetiva construir uma grade de produção com os recursos computacionais de alto desempenho dos sete CENAPADs (e.g. CENAPAD-NE, CESUP), que fazem parte do projeto Giga da RNP [RNP-GIGA 2005], utilizando ferramentas de domínio público. Por se tratar de um ambiente geograficamente distribuído e heterogêneo, composto por vários domínios, as políticas de segurança poderão diferir em diversos aspectos quanto as regras de acesso os recursos da grade. É necessário estabelecer um modelo de segurança único e padronizado, o que é então uma tarefa difícil, visto que cada domínio possui suas próprias características e restrições. Sendo assim este artigo apresenta um modelo de segurança a ser adotado em uma grade montada sobre a plataforma Globus

Toolkit 3.2 [Globus Alliance 2005], respeitando as políticas de segurança local de cada domínio que compõem a grade.

Este artigo está organizado da seguinte forma: na seção 2 são abordados os mecanismos de segurança existentes para os ambientes de computação em grade; a seção 3 discute as políticas de segurança dos domínios distintos que compõem a grade; a seção 4 apresenta a proposta de segurança para o projeto GRAD-GIGA; por fim, a seção 5 apresenta as considerações finais e trabalhos futuros.

2. Mecanismos de segurança para ambientes de computação em grade

A arquitetura de comunicação que interliga os CENAPADs está ilustrada na Figura 1. Para prover os requisitos de segurança do projeto GRAD-GIGA está sendo construído e desenvolvido uma infra-estrutura de segurança baseada na plataforma Globus, a qual usa as seguintes ferramentas: *Globus Security Infrastructure* – GSI [Globus Alliance 2005], *Virtual Private Network* – VPN e Sistemas *Intrusion Detection System* - IDS. Nas sub-seções seguintes estas ferramentas são detalhadas.

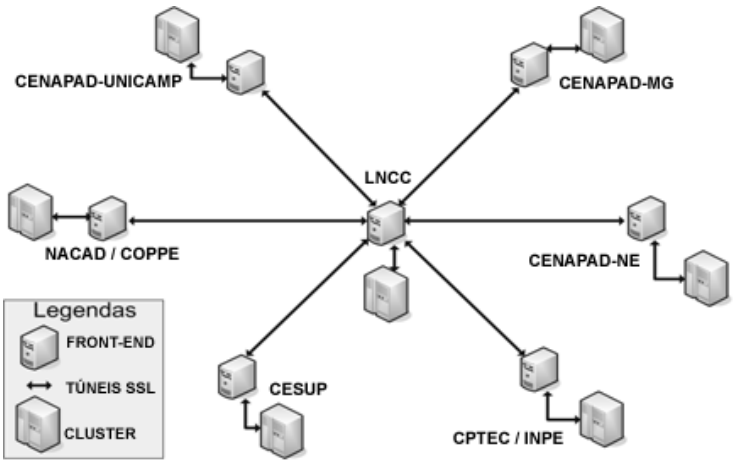

Figura 1. Arquitetura dos CENAPADs

2.1. *Globus Security Infrastructure* - GSI

A GSI, que compõe o Globus Toolkit, disponibiliza um conjunto de ferramentas destinadas a prover serviços de autenticação, autorização, não-repúdio, confidencialidade e privacidade [Pearlman et al 2002].

Para autenticar as entidades da grade (e.g., usuários, estações e recursos) são utilizados certificados digitais que seguem a especificação X.509 [Pearlman et al 2002]. Estes certificados contêm informações necessárias para identificação e autenticação das entidades. Eles são assinados por um *Certificate Authority* (CA), que exerce a função de administração e armazenamento dos certificados.

A autenticação pode acontecer de duas formas: única ou mútua. Na autenticação única o usuário da grade é autenticado uma única vez. Ao migrar para um novo domínio, a autenticação será realizada de forma transparente, através da utilização de usuários *proxy*. A autenticação mútua é realizada através da troca de chaves entre as entidades envolvidas neste processo corrente. Nesse tipo de autenticação a GSI utiliza o *Secure Socket Layer* (SSL) [Braga et al 2005], que fornece os serviços de confidencialidade e integridade dos dados.

2.2. *Virtual Private Network* - VPN

No caso da utilização de VPN, o estabelecimento de um túnel de comunicação seguro é implementado através do IPSec, que utiliza três algoritmos: *United States Data Encryption Standard* (USDES), *Data Encryption Standard* (DES) e *Triple Data Encryption Data* (3DES) [HP Invent 2002].

Além do serviço de confidencialidade, o IPSec fornece os serviços de integridade e autenticidade dos dados transmitidos através da inserção do cabeçalho *Authentication Header* (AH) em todos os pacotes, o qual possui informações que permitem verificar a integridade e prevenir ataques de *replay*.

2.3. *Intrusion Detection System* - IDS

Os IDSs implementam mecanismos de segurança que permitem a detecção de cenários de intrusão, no momento em que eles ocorrem ou não [Wanner and Weber 2001].

Um sistema IDS funciona seguindo duas técnicas distintas: a técnica de detecção de mau uso e a de detecção baseado em anomalias. Na primeira modalidade, o funcionamento consiste na utilização de padrões de ataques conhecidos para se descobrir tentativas de invasão no momento em que eles ocorrem. Na segunda técnica, é realizado com o estudo do tráfego da rede e dos dados dos usuários, em busca de anomalias no sistema. Nesta técnica existe um problema de descoberta da origem dos ataques, já que esta detecta apenas as anomalias na rede.

3. Políticas de Segurança

Para implementar políticas de segurança em cada organização virtual de uma grade, as estações servidoras da grade devem utilizar um *firewall* que implemente, no mínimo, o seguinte conjunto de regras restritivas descritas na Tabela 1, respeitando todas as políticas locais adotadas em cada centro.

Tabela 1. Regras a serem implementadas no *firewall*.

Tráfego	**Estado**
Pacotes de saída	Liberado
Portas (Globus) 8080,2119,22, 7512	Liberado
Redes (RFC 1918, nulas, loopback)	Bloqueado
Demais portas	Bloqueado

4. O Modelo de Segurança para o GRAD-GIGA

De acordo com as soluções apresentadas anteriormente, as estratégias que provêem autenticidade, confidencialidade, integridade e não-repúdio são a GSI e VPNs.

Ao utilizar VPN, um túnel seguro é estabelecido entre cada *Front-End* pertencente a uma organização virtual (veja a Figura 1). Desta forma, os dados que trafegam por esse túnel estão protegidos contra acesso indevido, de forma transparente às aplicações que executam nas camadas superiores. Embora o estabelecimento de VPNs proteja o tráfego de dados entre os CENAPADs, a sua utilização ocasiona *overhead* na comunicação de outros serviços que não requerem proteção.

Já na utilização da GSI, a proteção é realizada no nível de aplicação através do protocolo SSL/TLS. Por ser parte do Globus, a GSI não oferece problemas de integração ou incompatibilidade com os *Front-Ends*. Na Figura 1 pode ser observado o ambiente de computação em Grade utilizando a GSI para a provisão da confidencialidade e integridade na transmissão dos *jobs*.

5. Considerações Finais

Tendo em vista as vantagens da GSI apresentadas acima, este documento propõe a sua utilização para a provisão da confidencialidade e integridade na transmissão dos *jobs* em um ambiente de grades. Sugere-se ainda a utilização de um *firewall*, como o IPTables [Netfilter 2005], que implementa regras no nível de Kernel do sistema.

Além da GSI e da adoção de políticas de segurança, este artigo propõe ainda a utilização de ferramentas IDS visando aumentar segurança e confiabilidade da grade computacional. O IDS Snort [Snort 2005], por exemplo, mostra-se eficiente como ferramenta de detecção de intrusão, à medida que protege o *Front-End* Globus da arquitetura de grade do projeto GRAD-GIGA.

6. Referências

Braga, R., Andrade, R., Martins, F., Costa, J., "Globus Security Infrastructure: a security infrastructure for computational grids". In: III Workshop Grid e Aplicacões (WCGA 2005), 2005, p. 2.

Globus Alliance. Globus Toolkit 3.2: Documentation. Disponível em <http://www-unix.globus.org/toolkit/docs/3.2. Acesso em: 03 Janeiro 2005

Grid Stack: Grid Computing. Disponível em <http://www-128.ibm.com/developerworks/grid>. Acesso em: 22 Junho 2005

HP Invent. Authentication Header (AH). Disponível em < http://docs.hp.com/en/J4256-90009/ch01s02.html>. Acesso em: 24 Fevereiro 2005

Netfilter: firewalling, nat, and packet mangling for linux. Disponível em <http://www.iptables.org>. Acesso em: 22 Junho 2005

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.

RNP-GIGA. Subprojetos de P&D do Projeto Giga. Disponível em <http://www.rnp.br/pd/giga/subprojetos.html>. Acesso em: 24 Junho 2005

SINAPAD. Sistema Nacional de Processamento de Alto Desempenho. Disponível em <http://www.lncc.br/sinapad/projetos.php> Acesso em: 24 Junho 2005

Snort. Disponível em <http://www.snort.org>. Acesso em: 22 Junho 2005

Wanner, P. and Weber, R., "Ferramenta de Injeção de Falhas para Avaliação de Segurança em Rede". Disponível em <http://www.ppgia.pucpr.br/~maziero /pesquisa/wseg/2003/04.pdf>. Acesso em: 24 Fevereiro de 2005.