

Segurança nas Grids

António Pereira up200703278
David Martins up200706371
Departamento Ciência dos Computadores

1 Introdução

O termo Grid refere-se a um conjunto de máquinas e recursos geridos por um middleware que proporciona aos utilizadores uma visão unificada de todo o sistema, disponibilizando vários serviços.

Desde o aparecimento do conceito de Grid [Figura 1], um dos principais desafios inerentes passa por encontrar meios que permitam pôr em prática medidas de segurança eficazes. Medidas estas que passam pela obtenção de autenticação e autorização dos utilizadores e gestão das suas tarefas, assim como, pela confidencialidade, integridade e não-repúdio dos dados.

Após a leitura de alguns artigos, iremos agora fazer um breve resumo de segurança em Grids, seguido de uma pequena avaliação.

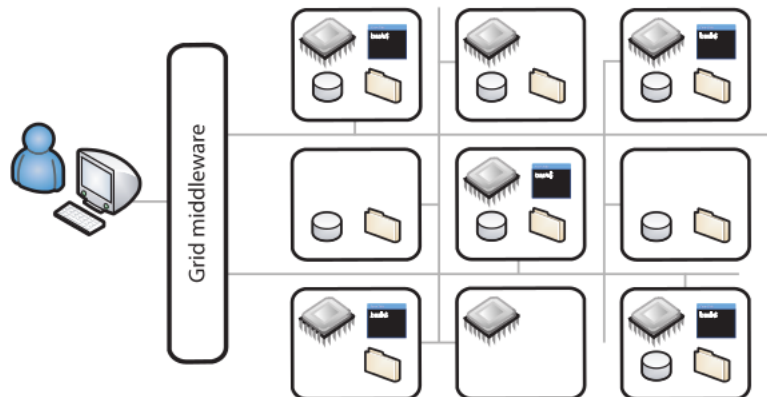


Figure 1: Conceito de Grid

2 Requisitos de Segurança de uma Grid

Sendo a segurança um ponto essencial numa Grid, esta requer esforços para superar as falhas e vulnerabilidades que possam existir. Iremos agora ver os principais pontos a ter em conta nesta área [4].

2.1 Autenticação

Numa Grid, a autenticação trata-se da parte central de segurança. Esta recorre ao uso de protocolos e certificados de modo a obter confiança entre ambas as partes. Na maioria dos casos, a autenticação é obtida através da apresentação de um determinado *token*, não podendo este ser falsificado.

2.2 Autorização

Em geral, este requisito é baseado em esquemas de autenticação, sendo que grande parte dos middlewares seguem esta premissa. Existem dois grandes métodos de autorização, podendo estes ser baseados em identidade ou em *tokens*.

2.3 Confidencialidade

É imprescindível que a troca de dados importantes seja feita de uma forma segura, de maneira a prevenir que entidades externas tenham acesso a estes. Desta forma, deve ser estabelecida uma área de segurança recorrendo a políticas e algoritmos criptográficos.

2.4 Integridade

Torna-se necessário a existência de políticas e ferramentas que protejam os dados de modificações não autorizadas e de qualquer tipo de perda que possa ocorrer.

2.5 Não-Repúdio

Uma vez que as informações de uma Grid não podem ser facilmente alteradas, torna-se necessário que quando isto aconteça, não seja possível ao autor refutar o seu acto.

2.6 Gestão

Devido à descentralização de um Grid e à grande variedade e quantidade de recursos torna-se difícil a sua administração. Como solução para este problema, o uso de certificados associados a várias políticas têm um papel fulcral nesta área.

3 Modelo de Segurança em Grids

Numa Grid é necessária a existência de um modelo de segurança, sendo o mais comum o GSI (*Grid Security Infrastructure*), modelo este utilizado pelo conhecido *Globus Toolkit* [2].

O principal objectivo do GSI consiste em usar os protocolos de autenticação e autorização existentes, de maneira a providenciar um conjunto de serviços aos fornecedores de recursos para a Grid, com o intuito de reforçar as políticas de segurança tanto locais como nas VO's (*Virtual Organizations*).

Do ponto de vista de usabilidade, para aceder à Grid e seus recursos, os utilizadores devem inserir as suas credenciais de login uma só vez (*single-sign-on*), factor este essencial para o sucesso e o crescimento das Grids. O uso do PKI (*Public Key Infrastructure*) baseado nos certificados X.509 tornou-se um modelo padrão nos middlewares de Grids como por exemplo o *Globus* e *gLite*.

Para evitar a exposição de credenciais, recorre-se a uma *proxy*, a qual usa credenciais temporárias, não pondo em risco as credenciais de longa duração do utilizador. Possibilitando também, que submissões de longa duração possam ser executadas em que o utilizador esteja presente, preservando todos os direitos.

4 Avaliação dos Artigos

Para a escrita deste relatório efectuamos a leitura de diversos artigos, nos quais são descritos os vários métodos de forma a superar as vulnerabilidades de segurança em Grids.

Nos vários artigos lidos a bibliografia é bastante diversificada e actual, de acordo com as datas em que estes foram publicados.

Em termos de organização, os artigos encontram-se bem escritos e bem estruturados. Porém o artigo [1], é bastante mais técnico e de difícil compreensão em relação aos outros. Quanto à ilustração, alguns tópicos poderiam estar melhor ilustrados para uma melhor compreensão.

O tema abordado é muito importante, não só em Grids, mas hoje em dia, em qualquer serviço *web* é necessário que segurança dos dados envolvidos.

References

- [1] *Security in grid computing: A review and synthesis*, Erin Codya, Raj Sharmana, Raghav H. RAO and Shambhu Upadhyayab, 2007
- [2] *Grid Security: Next Steps*, Andrew Martin, Po-wah Yau, 2007.
- [3] *Security in Grid Computing*, Muhammad Asif Habib and Michael Thomas Krieger, 2007.
- [4] *The review of Security issues in Grid Computing*, Saiful Adli Ismail, Zailani Mohamed Sidek
- [5] *Security for Grid Services*, Von Welch, Frank Siebenlist, Ian Foster, John Bresnahan, Karl Czajkowski, Jarek Gawor, Carl Kesselman.
- [6] *Grid Security and its use of X.509 Certificates*, Russell Lock, Prof Ian Sommerville.
- [7] *Grid Security : Authentication and Authorization*, Jong Kim, 2005.
- [8] *A Security Architecture for Computational Grids*, Ian Foster, Carl Kesselman, Gene Tsudik.