Controlando Acesso a Recursos Distribuídos usando Contexto

Ricardo T. Macedo[1], Taís C. Appel [1], Junior M. Bandeira [2], Raul C. Nunes [2]

[1]Universidade de Cruz Alta (UNICRUZ)
Cruz Alta – RS – Brazil

[2]Universidade Federal de Santa Maria (UFSM)
Santa Maria – RS - Brasil

{rimacedo,tappel}@unicruz.edu.br, {jbandeira,ceretta}@inf.ufsm.br

Abstract. *This work shows how the contextual information-based access control mechanism can control the access to distributed resources distributed and how was its development. The software have low coupling between different programming languages, databases and operating systems and adds open standards for encoding access control policies, resulting in easy use on different domains.*

Resumo. *Este trabalho demonstra como o mecanismo de Controle de Acesso à Informação com Base em Expressões Contextuais pode controlar o acesso a recursos distribuídos e como foi seu desenvolvimento prático. A implementação possui baixo acoplamento entre diferentes linguagens de programação, bancos de dados e sistemas operacionais, e agrega padrões abertos para codificação das políticas de controle de acesso, o que facilita seu uso em diferentes domínios.*

1. Introdução

Com o avanço da tecnologia, cresce cada vez mais a necessidade de utilizar recursos e informações distribuídos nos diversos domínios. Além disso, cada vez mais computadores são interligados em rede e, neste cenário, cresce a importância dos modelos de controle de acesso (autenticação e autorização), pois é necessário garantir a integridade e confiabilidade de recursos e informações compartilhadas.

Do ponto de vista da autorização, o modelo de controle de acesso baseado em perfis (*Roled Basic Acess Control* - RBAC) [Ferraiolo e Sandhu 2001] é o mais difundido, sendo aplicado inclusive na gerência de grades computacionais [Pereira e Muppavarapu 2006]. Este modelo associa permissões de acesso a perfis ao invés de associá-las diretamente a usuários, o que proporciona mais flexibilidade ao modelo, porém não considera o contexto do acesso, ou seja, dados dinâmicos que cercam o sujeito que solicitou acesso e o objeto requisitado. Pode-se estender o RBAC através da associação de expressões contextuais nas permissões de acesso [Bandeira e Nunes 2008], expressões contextuais são informações do ambiente que formam o contexto de uma entidade, essas informações podem ser definidas como propriedades contextuais. Este trabalho demonstra como foi realizada a implementação e validação prática do

modelo RBAC estendido, bem como sua aplicabilidade para gerenciar recursos distribuídos.

2. Tecnologias utilizadas e o ambiente de testes

A implementação do modelo estendido do RBAC foi realizada através de uma arquitetura modular e com tecnologias abertas, de modo que o mecanismo não tenha dependência de sistema operacional, linguagem de programação e banco de dados. Para codificação das políticas de segurança foi escolhida a linguagem de marcação *eXtensible Access Control Markup Language* - XACML por ser um padrão aberto para especificar políticas de controle de acesso [Oasis 2009]. A linguagem de programação escolhida foi o Java em conjunto com o servidor *web GlassFish* para publicação do projeto. Na camada de persistência do SGBD utilizou-se o Hibernate [Hibernate 2009] e para a comunicação entre linguagens de programação foi adotada a tecnologia de Web Service [Skogan e Gronmo 2004].

O ambiente de testes escolhido foi o portal de um banco de dados de *Geodesastres* [Morgan 2009] do CRS/INPE, o qual possui dados que relatam desastres ambientais. Para integração do modelo foi necessária a alteração da função responsável pela verificação da segurança dos objetos antes de conceder o acesso.

3. Implantação e Testes

A implementação resultou na criação de uma camada de software que gerencia o acesso a todos os bancos de dados suportados pelo Hibernate (*Mysql, Postgres* e *Firebird*) e oferece um mecanismo baseado em contexto que absorve conceitos que permitem controle com granularidade fina, ou seja, é possível construir políticas de controle de acesso mais abrangentes que aumentam a segurança dos dados.

A figura 1 demonstra o modelo de controle de acesso gerenciando as requisições de acesso. Note que a aplicação recebe requisições de acesso de usuários aos recursos compartilhados e delega ao mecanismo de controle de acesso a responsabilidade de decidir com base na informação contextual (representada pelos blocos azuis associados ao usuário e objeto) se o sujeito terá ou não direito sobre o recurso que está solicitando acesso. Outro fator relevante ilustrado é o percurso realizado pelo software entre suas camadas: coleta informações contextuais através da camada de persistência e, com base nos dados recebidos da persistência, cria uma requisição XACML que será confrontada com as políticas de acesso. O resultado do confronto gera uma resposta XACML contendo a decisão de acesso, que é encaminhada para a aplicação.

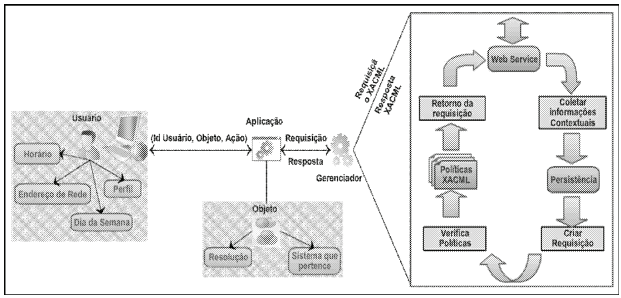

Figura 1 - Ambiente gerenciado pelo Modelo de Controle de Acesso

A representação das expressões contextuais no software proposto encontra-se tanto na criação da requisição XACML, onde são agregadas as propriedades contextuais que formam os tipos de contextos do usuário e objeto, quanto nas políticas de segurança que agregam informações contextuais específicas que devem ser satisfeitas para conceder o acesso. Por exemplo, a localização pode ser uma propriedade contextual tanto do objeto quanto do sujeito na criação de uma expressão contextual.

Durante os testes realizados no portal do INPE foram criadas políticas de controle de acesso que envolveram propriedades contextuais associadas às entidades de contexto usuários e objetos. Notou-se a viabilidade do mecanismo para: controlar o acesso a dados em sistemas distribuídos; representar regras de negócios de domínios heterogêneos; flexibilidade na construção de expressões contextuais associadas às requisições, devido à forma que o mecanismo representa informações contextuais; e flexibilidade na construção de políticas XACML, devido ao padrão de codificação usado nas requisições e políticas ser aberto.

4. Conclusão

Para prestar um serviço com maior rapidez, agilidade e facilidade, muitas organizações optam por dispor acesso on-line a informações internas, aumentando o risco de que dados confidenciais sejam descobertos por pessoas não autorizadas. Este trabalho descreve a implementação de um modelo de controle de acesso baseado em contexto, onde além da conferência da associação entre usuários, perfis e permissões, são identificados e verificados os contextos associados aos sujeitos e objetos.

A implementação do modelo e sua utilização junto a um banco de dados com informações sobre geodesastres, demonstrou que o controle de acesso a dados usando informações de contexto possibilita representar regras de negócios mais eficazes (mais detalhados). Como resultado tem-se um software de controle de acesso que oferece flexibilidade na construção de expressões contextuais associadas a regras de acesso, permitindo a edição de políticas de controle de acesso mais ricas.

Referências

Ferraiolo, F.; Sandhu, S. (2001) "Standard for Role-Based Access Control", In: *Advances in Computer Science*. Information and System Security.

Pereira, A. L.; Muppavarapu, V. (2006) **"**Role-Based Access Control for Grid Database Services Using the Community Authorization Service"**.** In: IEEE Transactions on Dependable and Secure Computing, v.3, n.2, April.

Bandeira, J.; Nunes, R. C.; Oliveira, M. A. F. (2008) "Controle de acesso à informação com base em expressões contextuais". Resende-RJ, Simpósio de Excelência em Gestão e Tecnologia,.

Hibernate. (2009) Página oficial do Hibernate. Disponível em: http://www.hibernate.org/. Acessado em Out.

Morgan, Jolvani. (2009) Banco de dados para o Núcleo de Pesquisa e Aplicação de Geotecnologias em Desastres Naturais e Eventos Extremos do Centro Regional Sul de Pesquisas Espaciais do INPE. CRS/INPE, Rel Técnico.

Oasis. (2009) eXtensible Access Control Markup Language (XACML) Version 1.0. Disponível em: http://www.oasis-open.org. Acessado em Out.

Skogan, David; Gronmo, Roy; SOLHEIM, Ida. (2004) Web Service Composition in UML. In: The 8th International IEEE Enterprise Distributed Object Computing Conference (EDOC) Monterey, California.