dRBAC – Controle de Acesso para Sistemas Distribuídos

Marcos T. Souza[1], Marcio A. L. Silva[1], Tereza C. M. B. Carvalho[1]

[1]Laboratorio de Arquitetura e Redes de Computadores – Escola Politécnica da Universidade de São Paulo (POLI-USP)
Av. Prof. Luciano Gualberto, travessa 3, n.158, sala C1-46, São Paulo, SP, Brasil

{mtork, msilva, carvalho}@larc.usp.br

1. Introdução

A multiplicidade de recursos, operações e relações encontradas em ambientes distribuídos impõe desafios para a arquitetura de arcabouços de controle de acesso e para o modelo implementado por este. O modelo *Role Based Access Control* (RBAC) possui a vantagem de ter sido desenvolvido com o intuito de lidar com essa multiplicidade, possibilitando a criação de autorizações granulares e facilitando o gerenciamento de um grande número de usuários através da utilização de papéis. Considerando-se as vantagens mencionadas, propõe-se uma arquitetura distribuída que implementa este modelo, possibilitando a sua utilização em ambientes distribuídos.

2. dRBAC – *distributed Role Based Access Control*

A premissa adotada por este arcabouço é de que o sistema de controle de acesso que pretende atender a demanda (requisições de acesso) de um sistema distribuído, deve ele próprio se tornar um sistema distribuído. Dada esta necessidade, i.e., de atendimento das requisições feitas ao longo do sistema distribuído e por todos os usuários que o utilizam, a distribuição do sistema de controle de acesso permite que as principais características de um sistema distribuído (i.e. resiliência e escalabilidade) não sejam subordinadas ou anuladas por um sistema centralizado (de controle de acesso).

2.1. Arquitetura

Para a construção deste arcabouço será utilizada a arquitetura básica de sistemas de controle de acesso, que é composta por um monitor de referência (MR) e uma base de autorização [Beznosov 2000]. Além destes componentes, dada a sua relevância para o arcabouço de controle de acesso, também será especificado uma base de usuários.

Uma vez estabelecidos os componentes do arcabouço, é proposta a seguinte abordagem para se obter as características desejadas (de um sistema distribuído): o MR é alocado junto a cada um dos elementos do sistema distribuído, e as bases de dados (de autorização e de usuários) são descentralizadas, de modo a preservar as mesmas características (do ponto de vista arquitetural) do resto do sistema.

A figura 1 permite a visualização da interação entre os componentes acima discriminados, i.e., o MR e as bases de dados. O MR é responsável por obter e processar as informações das bases de dados e assim determinar se uma operação deve ou não ser realizada. A sua implementação na forma de uma simples biblioteca de processamento de dados permite a sua rápida recuperação em caso de erros (não há estados para serem validados ou dados a serem consolidados).

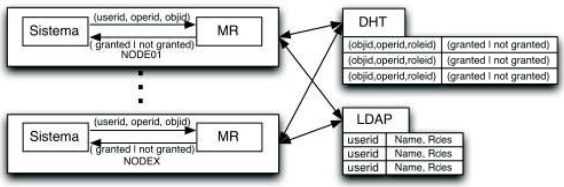

Figure 1. Arquitetura do Arcabouço

A primeira base de dados, a base de usuários, é construída através de um serviço de diretórios, o qual suporta diversas arquiteturas, inclusive a requerida neste caso: descentralizado e com inúmeras replicações. A segunda base de dados, a base de autorização, é desenhada para possuir apenas tabelas na primeira forma normal (1NF), permitindo a utilização de um serviço do tipo *Distributed Hash Table* (DHT) *(i.e. key, value store)*. As principais características deste serviço são exatamente aquelas exigidas em um sistema distribuído: escalabilidade e resiliência. A utilização de chaves do tipo (papéis x objeto x operação) garante o máxima uso do espaço de chaves e, por conseguinte, que a carga imposta ao sistema será distribuída entre os elementos do serviço DHT.

3. Comparação

Com o objetivo de suprir as exigências dos ambientes distribuídos, o modelo RBAC foi expandido [Chen 2008] e implementado [Freudenthal 2002] [Juntapremjitt 2000] de diversas formas. No entanto, a abordagem sugerida aqui tenciona apenas a expansão da arquitetura (i.e. para uma arquitetura distribuída), permitindo a utilização de qualquer modelo RBAC, expandido ou não.

4. Conclusão

Embora o arcabouço aqui descrito não forneça, *a priori*, uma solução para ambientes de múltiplos domínios de segurança, o modelo RBAC utilizado pode ser estendido para um dos modelos mencionados. A arquitetura construída atende aos requisitos de um sistema distribuído (i.e. resiliente e escalável), permitindo que a implementação de um controle de acesso robusto e eficiente não se torne um ponto de contenção para a utilização de sistemas distribuídos genéricos em sua plenitude.

Referências

Chen, G., Gu, J. and Chen, J. (2008) "An Extended Access Control Model based On Role And Department", In: International Seminar on Future BioMedical Information Engineering, IEEE Computer.

Beznosov, K., Deng, Y. (2000) "Engineering access control for distributed enterprise applications", In: Florida International University.

Freudenthal, E., Pesin, T., Port, L., Keenan, E., e Karamcheti, V. (2002) "dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments", In 22 nd International Conference on Distributed Computing Systems, IEEE Computer.

Juntapremjitt, S., Fugkeaw, S. e Manpanpanich, P. (2008) "An SSO-capable Distributed RBAC Model with High Availability across Administrative Domain", In 22nd International Conference on Advanced Information Networking and Applications – Workshops, IEEE Computer.