MAC5701 – Tópicos em Ciência da Computação
Plano de Estudos

Stefan Neusatz Guilhen
sneusatz@ime.usp.br

Controle de acesso baseado em papéis e certificados de atributos X.509

Orientador: Prof. Dr. Francisco Carlos da Rocha Reverbel
Departamento de Ciência da Computação

Universidade de São Paulo
- São Paulo, SP – 2005 -

1 Introdução

A grande maioria dos sistemas desenvolvidos atualmente tem como requisito algum tipo de controle de acesso às informações a aos recursos que são de grande importância. Primeiro, usuários devem se identificar ao sistema utilizando algum mecanismo de autenticação. Depois de identificado, o usuário deve somente poder acessar recursos para os quais ele tem permissão de acesso.

O RBAC [1] ou *Role-Based Access Control* é um mecanismo para controle de acesso baseado em papéis. Ele define um conjunto de papéis, que geralmente representam posições profissionais como gerente, administrador, diretor, etc, e atribui a cada papel um conjunto de permissões ou privilégios, que representam as ações que eles podem executar. Esse mecanismo simplifica de maneira significativa o gerenciamento de controle de acesso para um grande número de usuários, uma vez que tipicamente o número de papéis que os usuários podem desempenhar é muito inferior ao número de usuários em si.

Diversos serviços de segurança e *middlewares*, como servidores de aplicação, utilizam o RBAC como mecanismo de autorização e controle de acesso. Entretanto, a maioria dessas aplicações não utiliza uma maneira padronizada para mapear os usuários de uma aplicação aos seus respectivos papéis.

Recentemente, o comitê X9 da *U.S. American National Standards Institute* (ANSI) desenvolveu uma infra-estrutura de gerenciamento de privilégios, ou PMI [2],[3], que utiliza os certificados de atributos X.509 para armazenar o conjunto de privilégios de um usuário. Esses certificados estabelecem, dessa forma, uma estrutura padronizada para fazer o mapeamento entre os usuários e seus papéis.

O uso dos certificados de atributos como estrutura para implementar o RBAC facilita o gerenciamento distribuído dos privilégios de um usuário, pois mais de uma entidade pode emitir certificados contendo informações a respeito dos privilégios de um mesmo usuário, cada uma se preocupando com uma área diferente de aplicação. Por exemplo, uma entidade pode emitir certificados contendo informações sobre os papéis do cidadão no sistema eleitoral (eleitor, mesário, etc) enquanto outra pode emitir certificados contendo os atributos de sua carteira de motorista, identificando a sua autorização para dirigir determinados tipos de veículos.

2 Objetivos

Atualmente, a especificação de segurança de EJB não define um modo padronizado de implementar o mapeamento entre os usuários do sistema e seus respectivos papéis. Isso nos dá liberdade de utilizar os certificados de atributos X.509 como estrutura de armazenamento dos papéis dos usuários em um servidor de aplicação J2EE. Desse modo, o plano de estudos desenvolvido tem como objetivo analisar a viabilidade de implementar o mecanismo de controle de acesso utilizando certificados X.509 para componentes EJB implantados em um servidor de aplicação.

Esse mecanismo poderia ser configurado com os endereços dos repositórios de certificados de atributos das entidades nas quais o servidor confia, promovendo o gerenciamento distribuído dos privilégios dos usuários, algo que é especialmente útil em ambientes distribuídos e grades. Para isso, o seguinte roteiro de estudos deve ser seguido:

- estudar a PMI – *privilege management infraestructure*, definida pelo comitê X9 da ANSI – com atenção especial ao conteúdo e à aplicabilidade dos certificados de atributos.

- analisar os modelos *push* e *pull* de distribuição de certificados de atributos e observar os prós e contras de cada modelo [4].

- estudar algumas infra-estruturas de controle de acesso já implementadas [5],[6], observando como cada uma implementa seu mecanismo de autorização.

- estudar como a arquitetura J2EE ou Java 2 *Enterprise Edition* especifica [7] a política de controle de acesso aos componentes EJB (*Enterprise Java Beans*) implantados em um servidor de aplicação.

3 Referências

[1] R.S. Sandhu, E.J. Coyne, H.L. Feinstein, C.E. Youman, *Role based access control models*, IEEE Comput. 29, 1996.

[2] ITU-T Rec. X.509 ISSO/IEC 9595-8, *The Directory: Public-key and Attribute Certificate Frameworks*, 2001.

[3] *An Internet Attribute Certificate Profile for Authorization*, abril de 2002, http://www.ietf.org/rfc/rfc3281.txt

[4] J. Crampton, H. Khambhammetu, *Authorization and Certificates: Are we pushing when we should be pulling? Proceedings of the IASTED International Conference on Communication, Network, and Information Security*, p 62-66, 2003

[5] D.W. Chadwick, A. Otenko, *The PERMIS X.509 role based privilege management infrastructure*, Future Generation Computer Systems, Volume 19, Edição 2, Fevereiro 2003, p 277-289.

[6] *Akenti Authorization Infrastructure*. http://dsd.lbl.gov/Akenti

[7] *Enterprise Java Beans Specification*, Chapter 21 – Security Management, novembro de 2003. http://java.sun.com/j2ee/1.4/docs/index.html