ANÁLISE E CONSTRUÇÃO DE UMA SOLUÇÃO GENÉRICA PARA CONTROLE E PERMISSÃO DE ACESSO DE USUÁRIOS PARA SISTEMAS DE INFORMAÇÃO

Pierre da Costa Viana Júnior[1], Antonio Sckendall da Silva Sousa[2]

[1]Professor do tecnólogo em Análise e Desenvolvimento de Sistemas – IFRR. E-mail: pierre@ifrr.edu.br

[2]Discente do tecnólogo em Análise e Desenvolvimento de Sistemas - IFRR. E-mail: sckendall16@gmail.com

Introdução

Atualmente autenticação e autorização em sistemas de informação são características abordadas com bastante importância por grandes organizações. Para Silva et al. (2003), a grande questão é fundamentalmente a de descobrir qual a melhor forma de autenticar alguém e essencialmente a de garantir que apenas pessoas autorizadas tenham acesso aos recursos disponibilizados.

Muitas soluções são encontradas para controlar acesso e permissões de usuário. Porém, essas soluções possuem limitações. Tais soluções não atentem a necessidades como por exemplo: definição de perfis de acesso e generalização de uma solução para sistemas desktop e web.

Com isso, esse trabalho tem como objetivo desenvolver um modelo genérico e flexível para controle e permissão de acesso de usuários de sistemas de informação, que contemple as vantagens dos modelos existentes e supra as necessidades do mercado.

Metodologia ou Desenvolvimento do Trabalho

Dada importância do levantamento bibliográfico destacada por Gil (2002), inicialmente realizou-se um levantamento literário que rebuscou o conhecimento acerca dos conceitos relacionados à segurança da informação e das principais soluções de autenticação e controle de permissões existentes.

Para o levantamento bibliográfico bem como para revisão literária, utilizou-se livros disponíveis na biblioteca do IFRR-Campus/BV além de artigos e revistas

cientificas encontradas no site DevMedia, iMasters, dentre outros encontrados no Google acadêmico. O levantamento literário e o desenvolvimento do modelo foram feitos com a utilização de um notebook. Além disso, foi utilizado a ferramenta de desenvolvimento de sistemas NetBeans 8.1, com seus principais plug-ins, o software de modelagem UML, Astah e o software Dbdesigner para modelagem do banco de dados.

Resultados e discussão

A revisão literária proporcionou a identificação das principais soluções de autenticação e autorização existentes atualmente. As soluções mais robustas são desenvolvidas com a utilização de frameworks de segurança. Entre os principias frameworks destacou-se: JAAS, JGuard, Spring Security e Apache Shiro.

O JAAS, (Java Authentication and Authorization Service), é a API padrão do JAVA para implementação de autenticação e controle de acesso de usuários. Pode ser aplicado tanto em sistemas desktops quanto web. Porém, por falta de um modelo robusto, genérico e flexível, desenvolvedores acabam por fazer suas próprias implementações gerando problemas de portabilidade e restrições no gerenciamento de usuários e permissões.

O jGuard foi desenvolvido sobre framework JAAS (Java Authorization and Authentication Service). Os mecanismos de autenticação e autorização com o jGuard podem ser configurados com a utilização de banco de dados relacional, arquivos XML, ou até mesmo serviço LDAP.

O Spring Security é um framework que além de possibilitar a implementação de autenticação e controle de acesso, também disponibiliza outros recursos de segurança. (SPRING PROJECT, 2015).

Porém, pelo fato do JGuard e o Spring Security se limitarem a aplicações WEB, ambos se caracterizam inadequados para a construção de um modelo genérico.

Conclusão

Com o levantamento bibliográfico e a análise das principais soluções existentes atualmente, concluiu-se que embora não haja um modelo de autenticação e controle de acesso genérico, frameworks de segurança dão suporte para o desenvolvimento do mesmo.

Além disso, com o estudo dos principais frameworks de segurança, constatou-se que por possibilitar a implementação de autorização e permissão de acesso tanto em sistemas desktops quanto web, além de permitir o desenvolvimento de um modelo flexível que proporcione ao usuário final a administração desse modelo, o Apache Shiro é o framework que se mostrou mais apto a ser utilizado no desenvolvimento do nosso modelo de autenticação e autorização.