7
Conclusão

7.1.
Comparação com os Trabalhos Relacionados

Mühleisen et al. (2010) desenvolveram um sistema de controle de acesso que permite fazer o uso de regras definidas em uma linguagem criada pelos próprios autores baseada no SWRL (*Semantic Web Rule Language*). No entanto, essa linguagem não está relacionada com um modelo de controle de acesso, como o RBAC, e também esse sistema não está integrado a uma lista de controle de acesso (ACL).

Hollenbach, Presbrey e Berners-Lee (2009) desenvolveram um sistema de controle de acesso baseado em ACL. Porém, esse sistema não oferece suporte ao uso de regras de controle de acesso.

Finin et al. (2008) apresentaram duas abordagens para expressar os componentes do modelo RBAC usando a linguagem OWL (*Web Ontology Language*). Os autores usaram a linguagem N3Logic para modelar alguns componentes do RBAC. A principal desvantagem dessa abordagem é que para cada decisão da autorização, é necessário fazer uma nova execução da máquina de inferência, tornando o processo de autorização custoso. Além disso, essas abordagens não são integradas a uma ACL.

Ferrini e Bertino (2009) modelaram o RBAC usando também a linguagem OWL e as políticas de controle de acesso usando a linguagem XACML de forma integrada. Esta abordagem permite fazer inferências baseadas em OWL DL, porém não faz uso de linguagem de regras, como N3Logic ou SWRL, e nem faz integração com uma ACL.

Knechtel et al. (2008) mostram uma abordagem para modelar uma extensão do modelo RBAC, chamado RBAC-CH, usando a linguagem OWL. RBAC-CH é um modelo de controle de acesso que estende o modelo RBAC adicionando uma hierarquia de classes de objeto. Para a avaliação da política usando essa abordagem, a máquina de inferência baseada em OWL é executada uma única vez, e, em tempo de execução, as informações inferidas podem ser diretamente lidas para que a autorização possa ser decidida,

podendo estas informações ser armazenadas em uma ACL. No entanto, os autores não levaram em consideração as restrições estáticas e dinâmicas do modelo RBAC e nem fizeram o uso de regras para a construção de políticas.

7.2. Contribuições

O método SHDM (*Semantic Hypermedia Design Method*) não possui um modelo especializado que contemple a descrição de diretivas relacionadas ao controle de acesso de forma integrada com os outros modelos deste método. Este trabalho teve o objetivo de integrar um modelo de controle de acesso no método SHDM e estender o ambiente de desenvolvimento Synth para a inclusão deste novo modelo.

As principais contribuições deste trabalho foram:

- Inclusão do modelo de controle de acesso baseado em papel (RBAC) no método SHDM. Este modelo é composto de primitivas responsáveis pela descrição de conceitos relacionados ao controle de acesso, tais como, sujeito, papel, permissão, objeto e operação;
- Inclusão do modelo de políticas para a descrição de políticas de autorização em forma de regras de controle de acesso usando a linguagem N3Logic. O uso de linguagens de regras para a web semântica tais como, N3Logic e SWRL, permite a criação de políticas de autorização mais complexas;
- Integração do modelo de ACL da W3C com modelo RBAC junto com o modelo de políticas baseado em regras;
- Projeto e implementação de uma arquitetura de software modular para o controle de acesso de forma que os componentes sejam independente de tecnologia de implementação;
- Extensão da etapa de projeto comportamental para a adição das primitivas do modelo de controle de acesso baseado em papel e do modelo de políticas de forma integrada com o modelo de operações;
- Extensão do ambiente de desenvolvimento Synth para a adição do módulo de controle de acesso responsável por gerar as decisões de autorização.

7.3. Trabalhos Futuros

Podemos destacar como sugestões de trabalhos futuros os seguintes tópicos:

- Extensão do modelo de políticas para lidar com as políticas dinâmicas.
- Extensão da arquitetura do sistema de controle de acesso para fazer a reavaliação somente das políticas que são afetadas pela mudança na base de dados. Isso evita que todas as políticas sejam reavaliadas sempre que um recurso do domínio da aplicação for alterado.
- Estender o modelo de ACL para poder representar qual papel do usuário uma permissão está relacionada. Esta extensão permitirá que o resultado da consulta de autorização seja dado de acordo com o papel usado pelo usuário na aplicação;
- Otimizar as consultas feitas na tarefa de geração da ACL;