



Mairon de Araújo Belchior

**Modelo de Controle de Acesso no Projeto de Aplicações
na Web Semântica**

Dissertação de Mestrado

Dissertação apresentada como requisito parcial
para obtenção do título de Mestre pelo Programa
de Pós-Graduação em Informática da PUC-Rio.

Orientador: Prof. Daniel Schwabe

Rio de Janeiro
Outubro de 2011



Mairon de Araújo Belchior

**Modelo de Controle de Acesso no Projeto de Aplicações
na Web Semântica**

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Informática do Departamento de Informática do Centro Técnico e Científico da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Daniel Schwabe

Orientador

Departamento de Informática – PUC-Rio

Prof. Fernando Silva Parreiras

Departamento de Informática – FUMEC

Prof. Edward Hermann Haeusler

Departamento de Informática – PUC-Rio

Prof. José Eugenio Leal

Coordenador Setorial do Centro

Técnico Científico - PUC-Rio

Rio de Janeiro, 10 de outubro de 2011

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

Mairon de Araújo Belchior

Graduou-se em Ciência da Computação pela Universidade de Fortaleza (UNIFOR) em 2008. Participou de diversos trabalhos de iniciação científica e projetos de pesquisa. Possui interesse acadêmico e profissional nas áreas de Engenharia de Software, Linguagens de Programação e tecnologias para Web Semântica.

Ficha Catalográfica

Belchior, Mairon de Araújo

Modelo de controle de acesso no projeto de aplicações na Web semântica / Mairon de Araújo Belchior; orientador: Daniel Schwabe. – 2011.

110 f : il. ; 30 cm

Dissertação (mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Informática, 2011.

Inclui bibliografia

1. Informática – Teses. 2. SHDM. 3. Modelo de controle de acesso. 4. RBAC. 5. Web semântica. 6. Ontologias. I. Schwabe, Daniel. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

CDD:004

Este trabalho é dedicado ao meu pai Arnaldo Dias Belchior (*in memorium*)
por tudo que me proporcionou.

Agradecimentos

Ao meu orientador, professor Daniel Schwabe, pela sua atenção, seu apoio, entusiasmo, por todo conhecimento transmitido e pela sua orientação segura.

Aos professores Fernando Parreiras e Edward Hermann por terem aceitado prontamente participar da Comissão examinadora.

Aos meus colegas do laboratório TecWeb: Thiago Nunes e Maurício Bomfim por todo apoio concedido durante o desenvolvimento desta dissertação. Ao Percy e Renato, pela amizade. A todos os amigos e colegas da PUC-Rio.

A todos os professores e funcionários do Departamento de Informática da PUC-Rio, pelos ensinamento, atenção e ajuda.

A CAPES e a PUC-Rio pelo auxílio concedido.

Às minhas tias, em especial Luciana e Dayne, pelo apoio e incentivo recebidos.

Aos meus pais, Arnaldo e Fátima, pelo amor, incentivo e preocupação. Obrigado pela minha educação e por terem me ensinado a ser uma pessoa melhor. Obrigado, pai, por tudo!

Ao meu irmão, Arnaldo Segundo, pela compreensão.

À minha namorada Ingrid pelo seu carinho, companhia e amor.

A Deus por todas as bênçãos concedidas e por mais uma conquista.

Resumo

Belchior, Mairon de Araújo; Schwabe, Daniel. **Modelo de Controle de Acesso no Projeto de Aplicações na Web Semântica**. Rio de Janeiro, 2011. 110p. Dissertação de Mestrado - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

O modelo *Role-based Access Control* (RBAC) fornece uma maneira para gerenciar o acesso às informações de uma organização, reduzindo-se a complexidade e os custos administrativos e minimizando-se os erros. Atualmente existem diversos métodos de desenvolvimento de aplicações na Web Semântica e na Web em geral, porém nenhum dos modelos produzidos por estes métodos abrange a descrição de diretivas relacionadas ao controle de acesso de forma integrada com os outros modelos produzidos por estes métodos. O objetivo desta dissertação é integrar o controle de acesso no projeto de aplicações na Web Semântica (e na Web em geral). Mais especificamente, este trabalho apresenta uma extensão do método SHDM (Semantic Hypermedia Design Method) para a inclusão do modelo RBAC e de um modelo de políticas baseada em regras de forma integrada com os outros modelos deste método. O método SHDM é um método para o projeto de aplicações hipermídia para a web semântica. Uma arquitetura de software modular foi proposta e implementada no Synth, que é um ambiente de desenvolvimento de aplicações projetadas segundo o método SHDM.

Palavras-chave

SHDM; Modelo de Controle de Acesso; RBAC; Web Semântica; Ontologias.

Abstract

Belchior, Mairon de Araújo; Schwabe, Daniel (Advisor). **An Access Control Model for the Design of Semantic Web Applications.** Rio de Janeiro, 2011. 110p. MSc. Dissertation – Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro.

The Role-based Access Control (RBAC) model provides a way to manage access to information of an organization, while reducing the complexity and cost of security administration in large networked applications. Currently, several design method of Semantic Web (and Web in general) applications was proposed, but none of these methods produces an specialize and integrated model for describing access control policies. The goal of this dissertation is to integrate the access control in design method of Semantic Web applications. More specifically, this work presents an extension of SHDM method (Semantic Hypermedia Design Method) in order to include RBAC model and an rule based policy Model integrated with the other models of this method. SHDM is a model-driven approach to design web applications for the semantic web. A modular software architecture was proposed and implemented in Synth, which is an application development environment according to SHDM method.

Keywords

SHDM; Access Control Model; RBAC; Semantic Web; Ontology

Sumário

1	Introdução	16
2	Fundamentos	19
2.1.	Controle de Acesso	19
2.2.	Role-based Access Control model	20
2.2.1.	Modelo RBAC Nuclear	21
2.2.2.	Modelo RBAC Hierárquico	25
2.3.	ACL (Access Control List)	25
2.4.	Linguagem de Política	26
2.5.	Linguagens de Regra na <i>Web Semântica</i>	27
2.5.1.	SWRL	28
2.5.2.	N3Logic	29
2.6.	SHDM	30
2.7.	Synth	31
2.8.	Trabalhos Relacionados	31
3	Modelo de Controle de Acesso no Projeto de Aplicações na <i>Web Semântica</i>	42
3.1.	Modelo de Controle de Acesso	42
3.1.1.	Definição da Hierarquia de Papéis (rbac:subRole)	44
3.1.2.	Definição dos Sujeitos (rbac:Subject)	44
3.1.3.	Definição dos Objetos (rbac:Object)	44
3.1.4.	Definição dos Possíveis Papéis (rbac:role)	45
3.1.5.	Definição das Ações (rbac:Action)	45
3.1.6.	Definição das Permissões (rbac:permitted)	46
3.1.7.	Regras em N3Logic Traduzidas em OWL 2	47
3.1.8.	Definição da propriedade rbac2:relatedOperation	48
3.1.9.	Execução do modelo RBAC	48
3.1.9.1.	Perguntas de Autorização	50
3.2.	Modelo de Regras para as Políticas	50
3.3.	Modelo de ACL da W3C	52

3.4. Arquitetura de Software Modular para Controle de Acesso	53
3.5. Arquitetura de Implementação	55
3.6. Descrição do Sistema de Controle de Acesso	56
3.7. Políticas Estáticas e Dinâmicas	57
4 Modelo de Controle de Acesso no SHDM	59
4.1. O Método SHDM	59
4.1.1. Etapas	59
4.1.2. Levantamento de Requisitos	60
4.1.3. Modelagem de Domínio	61
4.1.4. Projeto Navegacional	61
4.1.5. Projeto Comportamental	63
4.1.6. Projeto de Interface	66
4.1.7. Implementação	66
5 Implementação do Modelo de Controle de Acesso no Synth	67
5.1. Synth	67
5.2. Arquitetura do Synth	67
5.3. Sequência de Colaboração entre os Módulos do Synth	69
5.4. Ambiente de Autoria	71
5.4.1. Sujeitos	72
5.4.2. Objetos	73
5.4.3. Papéis e Hierarquia de Papéis	75
5.4.4. User-Role Assignments	76
5.4.5. Permission-Role Assignments	77
5.4.6. Políticas	79
5.4.7. Gerador de todas as Permissões	82
5.4.7.1. Definição das Regras para Gerar as ACLs	84
5.4.8. Consulta de Permissões	85
5.5. Pré-condição da Operação	86
5.6. Custo Computacional	87
6 Um exemplo: Controle de Acesso em um Sistema de Gestão de Trabalhos em Conferências	89
6.1. Descrição do Cenário	89
6.2. Ontologia de Domínio	91
6.3. Definição das Primitivas do Modelo de Controle de Acesso	93

6.4. Políticas de Controle de Acesso Implementadas	95
6.5. Telas da Aplicação	100
7 Conclusão	104
7.1. Comparação com os Trabalhos Relacionados	104
7.2. Contribuições	105
7.3. Trabalhos Futuros	106
8 Referências Bibliográficas	107

Lista de figuras

Figura 1 – Relacionamento entre os usuários, os papéis e as permissões	22
Figura 2 – Componente estático e dinâmico do modelo RBAC nuclear	23
Figura 3 – Web Access Control (WAC) (Fonte: http://esw.w3.org/WebAccessControl/Vocabulary)	33
Figura 4 – Ontologia RBAC da primeira abordagem do RowIBAC	36
Figura 5 – Ontologia RBAC da segunda abordagem do RowIBAC	38
Figura 6 – Ontologia RBAC. (Fonte: Ferrini et al., 2009)	40
Figura 7 – Vocabulário do modelo de controle de acesso	43
Figura 8 – Vocabulário do modelo de regras para as políticas	51
Figura 9 – Vocabulário do modelo de ACL (Fonte: http://esw.w3.org/WebAccessControl/Vocabulary)	53
Figura 10 – Arquitetura Conceitual do Sistema de Controle de Acesso	54
Figura 11 – Arquitetura de Implementação do Sistema de Controle de Acesso	55
Figura 12 – Exemplo de UID como apresentado por [Vilain, 2002]	60
Figura 13 – Exemplo de modelo de contextos navegacionais	62
Figura 14 – Vocabulário do modelo de operações	63
Figura 15 – Visão conceitual da arquitetura do Synth	69
Figura 16 – Colaboração entre os módulos do Synth	71
Figura 17 – Tela de listagem de sujeitos	72
Figura 18 – Tela de criação de um sujeito	73
Figura 19 – Tela de listagem de objetos	74
Figura 20 – Tela de criação de um objeto	74
Figura 21 – Tela de listagem de papéis	75
Figura 22 – Tela de criação de um papel	76
Figura 23 – Tela de listagem de associações entre o papel e o sujeito	77
Figura 24 – Tela de criação de associação entre um papel e o sujeito	77
Figura 25 – Tela de listagem de associações entre o papel com a ação e o objeto	78
Figura 26 – Tela de criação de associação entre um papel com uma ação e um objeto	79
Figura 27 – Tela de listagem de políticas	80

Figura 28 – Tela de edição de uma política	81
Figura 29 – Tela da geração da ACL	82
Figura 30 – Tela de consulta de permissões	86
Figura 31 – Tela de edição da pré-condição de uma operação	86
Figura 32 – Tempo para fazer consultas de permissão na ACL	87
Figura 33 – Tempo de reavaliar todas as políticas quando ocorre uma mudança na base	88
Figura 34 – Hierarquia de papéis do sistema de conferências	94
Figura 35 – Tela do índice “AllPerson”	101
Figura 36 – Tela de <i>Login</i> através do protocolo OpenID	101
Figura 37 – Tela de acesso a um nó no contexto “AllPerson”	102
Figura 38 – Tela do índice “AllPublications”	102
Figura 39 – Tela de criação de uma nova revisão	103
Figura 40 – Tela de acesso a um nó no contexto “AllPublication” mostrando uma mensagem “Access Denied” quando o usuário tentou visualizar uma revisão ao clicar em "ReviewA"	103

Lista de quadros

Quadro 1 – Exemplo de um arquivo ACL.	34
Quadro 2 – Associação das permissões de acesso aos papéis	37
Quadro 3 – Regra em N3Logic definindo a hierarquia de papéis	38
Quadro 4 – Exemplo da definição de uma hierarquia de papéis	44
Quadro 5 – Exemplo da definição dos sujeitos (rbac:Subject)	44
Quadro 6 – Exemplo da definição dos objetos (rbac:Object)	45
Quadro 7 – Exemplo da definição dos possíveis papéis para os sujeitos que são recursos das classes myconference:Reviewer e myconference:SeniorReviewer	45
Quadro 8 – Exemplos da definição das ações (rbac:Action)	46
Quadro 9 – Exemplo da definição da propriedade rbac2:object para a ação rbac:createReview	46
Quadro 10 – Exemplo da definição da propriedade rbac2:object para a ação rbac:editReview	46
Quadro 11 – Exemplo da definição das permissões (rbac:permitted)	47
Quadro 12 – Definição da hierarquia de papéis usando regras em N3Logic	47
Quadro 13 – Especificação em RDF das propriedades rbac:role, rbac:activeRole e da hierarquia de papéis usando a propriedade <i>Chain Axiom</i> da linguagem OWL 2	48
Quadro 14 – Exemplo da definição da propriedade rbac2:relatedOperation	48
Quadro 15 – Regra em N3 para a ativação do papel	49
Quadro 16 – Regra em N3 para verificar se uma ação possui um objeto	49
Quadro 17 – Regras em N3 que decidem sobre a permissão de execução de uma ação	49
Quadro 18 – Exemplo de consulta de permissão de acesso	50
Quadro 19 – Exemplo de código de uma política de controle de acesso em N3Logic	52
Quadro 20 – Regra para a definição dos possíveis papéis para os sujeitos que são recursos da classe myconference:Reviewer	76
Quadro 21 – Alterações nos modelos do Synth quando ocorre a associação entre um papel e uma ação	79

Quadro 22 – Regra de geração dos recursos da ACL	84
Quadro 23 – Exemplo de política que define um conflito ao criar uma revisão do próprio artigo	95
Quadro 24 – Exemplo de política que define que o revisor só pode criar revisões de artigos que foram alocados para ele	95
Quadro 25 – Exemplo de política que define um conflito ao criar uma revisão de um artigo de um autor que trabalhe na mesma instituição que a sua	96
Quadro 26 – Exemplo de política que define que o autor só pode visualizar os contextos "AllPublication" e "AllReviews"	96
Quadro 27 – Exemplo de política que declara que o autor só pode visualizar as revisões dos artigos que ele mesmo submeteu	97
Quadro 28 – Exemplo de política que define um conflito ao criar uma revisão de um artigo de um autor que já trabalhou junto	97
Quadro 29 – Exemplo de política que define que o revisor só pode visualizar as revisões de artigos que ele já tenha revisado.	98
Quadro 30 – Exemplo de política que define que o revisor sênior só pode visualizar as revisões de artigos que foram alocados para ele	99
Quadro 31 – Exemplo de política que define que o revisor só pode editar uma revisão que ele tenha criado	99
Quadro 32 – Exemplo de política que define que o autor só pode fazer o <i>download</i> de um artigo que ele mesmo submeteu	100
Quadro 33 – Exemplo de política que define que o autor só pode visualizar o status da revisão dos artigos que ele submeteu	100

Lista de tabelas

Tabela 1 – Exemplo de ACL	26
Tabela 2 – Associações definidas entre o papel com a ação e o objeto	94