1
Introdução

Com a crescente importância da *World Wide Web* (WWW) nos últimos anos em setores da educação, do governo, financeiro e nos negócios, a segurança na *Web* tem um papel vital para o sucesso da Web Semântica [Denker et al., 2005]. Recursos *Web* precisam ser protegidos de acessos não autorizados e agentes de software que acessam recursos online em nome de um usuário precisam estar seguros sobre a privacidade dos dados a serem descobertos. Desta forma, mecanismos para o controle de acesso são relevantes para as tecnologias usadas na *Web* semântica.

O controle de acesso é um mecanismo de segurança que consiste em determinar se um usuário tem o direito de usar um dado recurso do sistema, e de que forma, isto é, "quem pode fazer o que". Sandhu et al. (1996) definem controle de acesso como sendo o processo de limitar o acesso a recursos de um sistema a somente entidades autorizadas, podendo estas entidades ser pessoas, processos ou outros sistemas.

Mecanismos de controle de acesso são importantes para preservar a confidencialidade e a integridade da informação. Confidencialidade refere-se à necessidade de manter a informação segura e privada, enquanto que integridade refere-se ao conceito de proteger a informação de ser alterada de forma imprópria por usuários não autorizados.

Na literatura existem diversos métodos de desenvolvimento de aplicações hipermídia, tais como, HDM (*Hypermedia Design Model*) [Garzotto et al., 1993], RMM (*Relationship Management Methodology*) [Isakowitz et al., 1995], WebML (*Web Modeling Language*) [Ceri et al., 2000], UWE (*UML-based Web Engineering*) [Koch e Kraus, 2002], OOHDM (*Object-Oriented Hypermedia Design Method*) [Schwabe e Rossi, 1998] e o SHDM (*Semantic Hypermedia Design Method*) [Lima, 2003]. A maioria dessas abordagens especifica aplicações *web* com diferentes modelos para conteúdo, navegação, e apresentação. No entanto, nenhum destes métodos possui um modelo que contemple a descrição das diretivas relacionadas ao controle de acesso de forma integrada com os outros modelos dos métodos de *design* de aplicações *web*.

Portanto, este trabalho tem o objetivo de integrar o controle de acesso no projeto de aplicações na *Web* semântica. Uma arquitetura de software para o controle de acesso foi projetada e implementada, e dois novos modelos foram adicionados. O primeiro descreve políticas de acesso em forma de regras, e o segundo provê a especificação de conceitos relacionados ao controle de acesso, tais como, sujeito, papel do sujeito, permissão, objeto e operação. O modelo RBAC (*Role-based Access Control model*) foi escolhido devido ao seu grande uso em aplicações do mundo real [Ferraiolo et al., 2007] e considerável estudo acadêmico [Finin et al., 2008].

Tais modelos podem ser aplicados em métodos de desenvolvimento de aplicações que tenham a noção de operação do domínio. Em especial, o método SHDM (*Semantic Hypermedia Design Method*) [Lima, 2003] foi estendido para a inclusão desses modelos de controle de acesso. SHDM é um método para o projeto de aplicações hipermídia para a *web* semântica. Este método é uma evolução do OOHDM (*Object-Oriented Hypermedia Design Method*) [Schwabe e Rossi, 1998] através da adição de mecanismos da *Web* Semântica.

A arquitetura de controle de acesso foi implementada no ambiente de desenvolvimento de aplicações na Web Semântica – Synth [Bomfim, 2011]. O Synth é um ambiente de desenvolvimento desenvolvido em linguagem Ruby que dá suporte à construção de aplicações modeladas segundo o método SHDM, fornecendo um conjunto de módulos capazes de receber como entrada os artefatos gerados na execução das etapas do método SHDM e produzir como saída uma aplicação hipermídia descrita por esses artefatos.

Esta dissertação foi dividida em seis capítulos e mais as considerações finais descritos, resumidamente, a seguir:

No capítulo 2, são apresentados brevemente os principais fundamentos teóricos necessários para o desenvolvimento desta dissertação.

No capítulo 3, são mostradas as primitivas do modelo de controle de acesso usadas neste trabalho. É apresentado também uma arquitetura de software para o sistema de controle de acesso que foi implementado.

No capítulo 4, o método SHDM é apresentado com ênfase para as mudanças introduzidas neste trabalho, mais especificamente no Projeto Comportamental.

No capítulo 5, o ambiente de desenvolvimento Synth será mostrado, como também a sua arquitetura e o seu ambiente de autoria que foram estendidos para a inclusão de um novo módulo de controle de acesso.

No capítulo 6, um exemplo de aplicação modelada segundo o método SHDM e construída com apoio do ambiente de desenvolvimento Synth é apresentado, enfatizando-se as tarefas que descrevem as primitivas de controle de acesso da aplicação.

E, por último, uma comparação entre os trabalhos relacionados, as contribuições geradas com desenvolvimento desta dissertação e sugestões de trabalhos futuros são apresentados no capítulo 7.