



**Herbet de Souza Cunha**

**Uso de Estratégias Orientadas a Metas  
para Modelagem de Requisitos de  
Segurança**

**Dissertação de Mestrado**

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

Orientador: Prof. Julio César Sampaio do Prado Leite

Rio de Janeiro  
abril de 2007



**Herbet de Souza Cunha**

**Uso de Estratégias Orientadas a Metas  
para Modelagem de Requisitos de  
Segurança**

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

**Prof. Julio Cesar Sampaio do Prado Leite**

Orientador

Departamento de Informática – PUC-Rio

**Prof. Arndt Von Staa**

Departamento de Informática – PUC-Rio

**Profa. Vera Maria Benjamim Werneck**

Universidade do Estado do Rio de Janeiro - UERJ

**Prof. José Eugênio Leal**

Coordenador Setorial do Centro

Técnico Científico – PUC-Rio

Rio de Janeiro, 16 de abril de 2007

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

### **Herbet de Souza Cunha**

Graduou-se em Bacharelado em Ciências da Computação pela Universidade Federal de Pernambuco em agosto de 2000. Área de interesse acadêmico: Engenharia de Software, mais especificamente a sub-área de Engenharia de Requisitos. Atualmente é funcionário da área de Tecnologia da Informação da Petróleo Brasileiro SA (PETROBRAS) atuando na área de arquitetura de informações e metadados.

#### Ficha Catalográfica

Cunha, Herbet de Souza

Uso de estratégias orientadas a metas para modelagem de requisitos de segurança / Herbet de Souza Cunha; orientador: Julio César Sampaio do Prado Leite. – 2007.

148 f. : il. ; 30 cm

Dissertação (Mestrado em Informática)– Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

Inclui bibliografia

1. Informática – Teses. 2. Requisitos. 3. Segurança. I. Leite, Julio César Sampaio do Prado. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

Para meus pais, Nalva e Milton, pelo  
incentivo e confiança.

## Agradecimentos

A Julio César Sampaio do Prado Leite pelas orientações e paciência.

A Antônio de Pádua Albuquerque Oliveira pela colaboração.

Aos amigos da Petrobras pelo incentivo e força.

A Petrobras pelo apoio.

## Resumo

Cunha, Herbet de Souza; Leite, Julio Cesar Sampaio do Prado. **Uso de estratégias orientadas a metas para modelagem de requisitos de segurança**. Rio de Janeiro, 2007. 148p. Dissertação de Mestrado - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro

Adicionar requisitos de segurança às arquiteturas de software após elas terem sido construídas é uma tarefa bastante difícil. Conceitos de segurança devem permear todo o ciclo de desenvolvimento do software, desde a engenharia de requisitos, passando por desenho (design), implementação, testes e distribuição. Este trabalho apresenta uma abordagem para modelagem de requisitos de segurança, especialmente os requisitos de confidencialidade e consistência das informações, baseada em estratégias orientadas a metas, trazendo a questão da segurança para o início do ciclo de desenvolvimento de software. São apresentados também os resultados da aplicação desta abordagem em um estudo de caso.

## Palavras-chave

Requisitos, Segurança

## Abstract

Cunha, Herbet de Souza; Leite, Julio Cesar Sampaio do Prado. **Uso de estratégias orientadas a metas para modelagem de requisitos de segurança**. Rio de Janeiro, 2007. 148p. Master degree thesis – Computer Science Department, Pontifícia Universidade Católica do Rio de Janeiro

Adding security requirements to software architectures after they are built is a hard work. Security concepts have to cross the whole software development cycle, from requirement engineering to deployment, passing by design, coding and test. This work presents an approach to security requirements modeling, mainly the information confidentiality and consistency, based on goal oriented strategies, bringing the security issues to the beginning of the software development cycle. It also presents the results of this approach in a case study.

## Keywords

Requirements, Security.

## Sumário

1 INTRODUÇÃO .....	13
2 O <i>FRAMEWORK</i> I* .....	19
3 USO DE ESTRATÉGIAS ORIENTADAS A METAS .....	33
4 ESTUDO DE CASO .....	51
5 ANÁLISE DE TRABALHOS RELACIONADOS .....	129
6 CONCLUSÃO .....	141
7 REFERÊNCIAS.....	145



## Lista de Figuras

Figura 2.1 - Tipos de dependência.....	23
Figura 2.2 - Elos de decomposição de tarefa.....	24
Figura 2.3 - Elos meios-fim.....	26
Figura 2.4 - Meta-modelo elaborado em UML para <i>Strategic Actor</i> (SA) proposto em [13] .....	29
Figura 3.1 - Visão geral da Engenharia de Requisitos, adaptada de [30] .....	34
Figura 3.2 - Processo de definição de requisitos usando <i>i*</i> de Liu, Yu e Mylopoulos [3] .....	35
Figura 3.3 - Fluxograma do processo evoluído a partir do processo de Liu, Yu e Mylopoulos [3] .....	39
Figura 4.1 - Modelo SD do <i>Expert Committee</i> , reusado de [4] .....	56
Figura 4.2 - Diagrama de <i>SDSituations</i> do <i>Expert Committee</i> , adaptado de [4] .....	59
Figura 4.3 - Modelo SD do <i>Expert Committee</i> – versão revisada.....	63
Figura 4.4 - Diagrama de <i>SDSituations</i> do <i>Expert Committee</i> , adaptado de [17] .....	64
Figura 4.5 - Modelo SA – Atores legítimos .....	72
Figura 4.6 - Modelo SA – Atacantes.....	74
Figura 4.7 - Modelo SD Refinado .....	75
Figura 4.8 - Modelo SR: Researcher x Coodinator.....	77
Figura 4.9 - Modelo SR: Conference Organizer (Chair) x Coordinator - modelo complementar de [17] .....	78
Figura 4.10 - Modelo SR: Author x Conference Organizer (Chair) - modelo complementar de [17] .....	80
Figura 4.11 - Modelo SR: Reviewer x Conference Organizer (Chair) - modelo adaptado de [17].....	82
Figura 4.12 - Modelo SR: Conflicts Solver (Committee Member) x Conference Organizer (Chair) - modelo complementar de [17].....	85
Figura 4.13 - Intenções maliciosas dos atacantes internos.....	87
Figura 4.14 - Intenções maliciosas dos atacantes externos.....	88
Figura 4.15 - Tipos de requisitos não-funcionais, baseado em [7] .....	94
Figura 4.16 - Refinamento de segurança por tipo, baseado em [7].....	95
Figura 4.17 - Refinamento de consistência por tópicos.....	96
Figura 4.18 - Refinamento de confidencialidade por tópicos.....	96

Figura 4.19 - Adição de metas flexíveis de segurança às situações de submissão de artigo e recepção de versão final .....	98
Figura 4.20 - Adição de metas flexíveis de segurança à situação de revisar artigo.....	99
Figura 4.21 - Adição de metas flexíveis de segurança à situação de resolução de conflito .....	100
Figura 4.22 - Medidas de ataque dos atacantes externos.....	101
Figura 4.23 - Medidas de ataque dos atacantes internos.....	103
Figura 4.24 - Alternativas de operacionalização para confidencialidade e consistência.....	105
Figura 4.25 - Análise de medidas de defesa - confidencialidade interna [artigo revisado].....	106
Figura 4.26 - Análise de alternativas: 'usar autenticação com cartão' e 'usar autenticação biométrica' .....	107
Figura 4.27 - Análise de alternativas: 'usar senhas múltiplas'.....	108
Figura 4.28 - Análise de alternativas: 'usar senha simples'.....	109
Figura 4.29 - Escolha da alternativa: 'usar senha simples' .....	110
Figura 4.30 - Análise de medidas de defesa para confidencialidade externa (artigo revisado) .....	112
Figura 4.31 - Análise de alternativas: 'usar chave de 64bits' .....	113
Figura 4.32 - Análise de alternativas: 'usar chave de 128bits' .....	114
Figura 4.33 - Escolha da alternativa: 'usar chave de 128bits .....	115
Figura 4.34 - Análise de medidas de defesa para consistência (artigo revisado).....	117
Figura 4.35 - Escolha de alternativa: 'usar mídia de DVD' .....	118
Figura 4.36 - Operacionalização de confidencialidade interna e externa e consistência na 'submissão de artigo' .....	119
Figura 4.37 - Operacionalização de confidencialidade interna e externa e consistência na 'resolução de conflito' .....	120
Figura 4.38 - Votação aberta na 'resolução de conflito' .....	121
Figura 5.1 - Abordagem de casos de uso de segurança, linhas gerais, capturada de [11] .....	133

## Lista de Tabelas

Tabela 4-1 - Identificação de Atores – versão inicial .....	54
Tabela 4-2 - Identificação de Atacantes – versão inicial .....	55
Tabela 4-3 - Identificação de Atores – versão revisada .....	62
Tabela 4-4 - Identificação de Atacantes – versão revisada.....	62
Tabela 4-5 - Identificação de vulnerabilidades .....	66
Tabela 5-1 – Resumo de características dos trabalhos analisados .....	139
Tabela 6-1 - Rastro do requisito: Segurança do Artigo Revisado.....	142

