



Engenharia de Papéis e o Processo XP - Uma Proposta de Integração Através do Jogo do Planejamento

IV Simpósio Brasileiro de Sistemas de Informação

Ludmila de Almeida Pedrosa

Gustavo H. M. B. Motta

UFPB - Programa de Pós-Graduação em Informática



Agenda

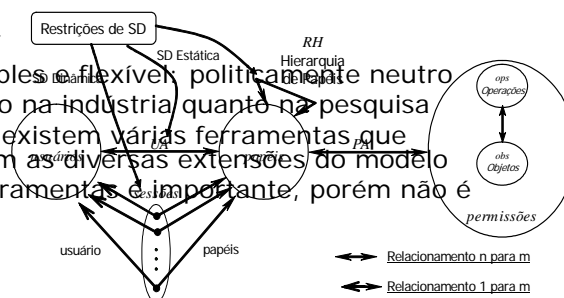
- Motivação
 - Segurança da Informação
 - RBAC
 - Engenharia de Papéis
 - eXtreme Programming – XP
- Integrando a Engenharia de Papéis ao XP
- Discussão e Conclusão

Segurança da Informação

- Necessidade da Segurança da Informação:
 - Proliferação da internet e dos sistemas web
 - Grande quantidade de sistemas distribuídos
 - Informações que trafegam na rede
 - Crescimento potencial de usuários
- Objetivo: controlar o acesso dos usuários às aplicações
- Solução:
 - Implantar algum modelo de controle de acesso
 - Modelos clássicos: carecem de necessidades das organizações atuais
 - **RBAC – Controle de Acesso Baseado em Papéis**

Controle de Acesso Baseado em Papéis

- RBAC
 - Regula o acesso dos usuários aos objetos protegidos com base nos **papéis** que eles exercem na organização
 - A autorização de acesso são associadas aos papéis
- Papel:
 - **Função de trabalho** que descreve autoridade e responsabilidade a um usuário dentro da organização
- Modelo RBAC:
 - Padrão NIST
 - Solução simples e flexível, politicamente neutro
 - Popular tanto na indústria quanto na pesquisa
 - Mercado: já existem várias ferramentas que implementam as diversas extensões do modelo
 - O uso de ferramentas é importante, porém não é essencial!



Engenharia de Papéis

- Metodologia que auxilie na definição e execução de uma política de segurança para controle de acesso:
 - Engenharia de Papéis (*Role Engineering*)
- Definição:

“Engenharia de Papéis é o **processo** de definir **papéis**, **permissões** e **hierarquia de papéis**” (*Neumann e Strembeck, 2002*)
- Benefícios:
 - Implementação do modelo RBAC com um esquema efetivo de controle de acesso
 - Simplificação da administração da política
 - Auxiliará a Engenharia de Requisitos no levantamento dos requisitos de controle de acesso.
- As abordagens atuais são apresentadas em base *ad hoc* ou tratam apenas de parte do processo
- Necessidade de levantar os requisitos de controle de acesso nas fases iniciais do processo de software

eXtreme Programming - XP

- Objetivo: engenharia de papéis de forma integrada ao processo de software
 - XP – *eXtreme Programming*
 - Flexibilidade exigida pelas organizações contemporâneas
- eXtreme Programming - XP:
 - Programação extrema: software rápido e de alta qualidade
 - Valores: comunicação, *feedback*, simplicidade e coragem
 - Práticas: 12 principais
 - **Jogo do Planejamento XP**

eXtreme Programming - XP

- Jogo do Planejamento XP:
 - **O que será feito?**
 - Requisitos e prioridades
 - **Quando será entregue?**
 - Estimativa dos *releases* – *Planejamento da Versão*
 - **Quais serão os próximos passos?**
 - Iterações – *Planejamento da Iteração*
- Motivação:
 - O Jogo do Planejamento seria suficiente para identificar os requisitos de controle de acesso?

Integrando a Engenharia de Papéis ao eXtreme Programming

- Pré-requisitos para Integração:
 - As atividades da **engenharia de papéis** adicionados ao jogo de planejamento devem estar alinhadas com as práticas XP
 - As atividades devem ser realizadas num trabalho iterativo: saídas fáceis de testar
 - Requisitos reunidos nas atividades devem ser baseados em análises de riscos:
 - *Engenharia de papéis mal feita implica em modelo RBAC indevido*
 - Não poderíamos tornar a **engenharia de papéis** e o **jogo de planejamento** pesados e centrados na documentação!

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

- Visão Geral do Processo:

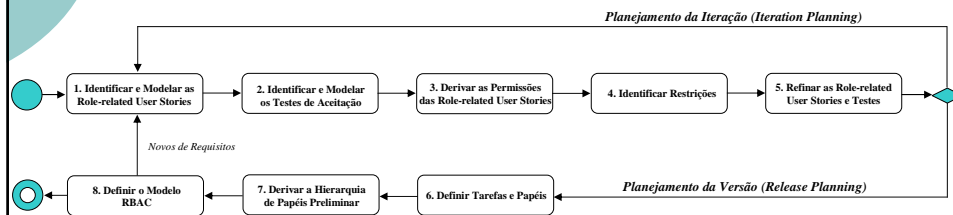


Figura 1: Visão Geral da extensão do Planejamento do Jogo para o Controle de Acesso Baseado em Papéis

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

1. Identificar e Modelar as *Role-related User Stories*

- Executada em paralelo a identificação dos requisitos funcionais
- Artefato de Saída:
 - *Role-related User Storie* (Estórias dos requisitos de controle acesso)

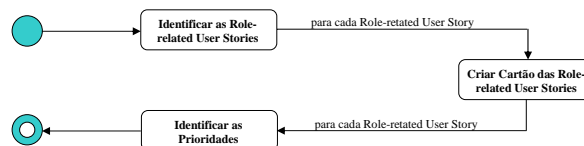


Figura 2: Sub-Processo de Modelagem das Role-related User Stories

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

2. Identificar e Modelar os Testes de Aceitação

- Prática XP:
 - Testar sempre
 - Escrever testes com antecedência
- Artefato de Entrada:
 - *Role-related User Stories*
- Artefato de Saída:
 - Cartão de Teste de Aceitação (*Criamos o que foi pedido?*)

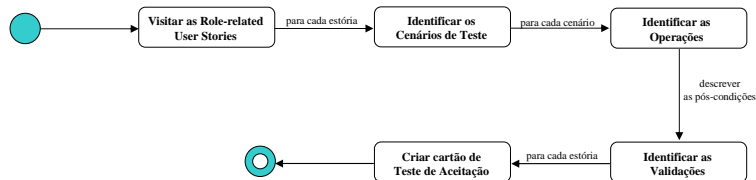


Figura 3: Sub-Processo de Modelagem dos Testes de Aceitação

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

3. Derivar permissões das *Role-related User Stories*

- Com identificar permissões?
 - Através das ações realizadas pelos sujeitos: o que faz!
- Artefatos de Entrada:
 - *Role-related User Stories e Cartões de Testes*
- Artefato de Saída:
 - Catálogo de Permissões
 - *Permissões: formadas por pares <operação, objeto>*

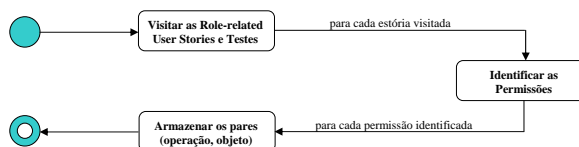


Figura 4: Sub-Processo de Derivação de Permissões

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

4. Identificar Restrições

- Quais tipos de restrições?
 - Ex: separação de responsabilidades, cardinalidades, etc.
- Com identificar restrições?
 - Através das ações não realizadas pelos sujeitos
- Artefatos de Entrada:
 - Catálogo de Permissões e Cartões de Testes
- Artefato de Saída:
 - Catálogo de Restrições

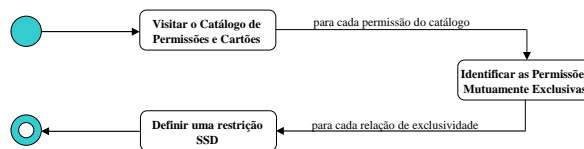


Figura 5: Sub-Processo de Identificação de Restrições

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

5. Refinar as *Role-related User Stories* e os Testes de Aceitação

- Atividades principais:
 - Derivação
 - Generalização
- Artefatos de Entrada:
 - *Role-related User Stories*
 - Cartões de Testes
- Artefatos de Saída:
 - *Role-related User Stories (revisadas)*
 - Cartões de Testes (*revisados*)

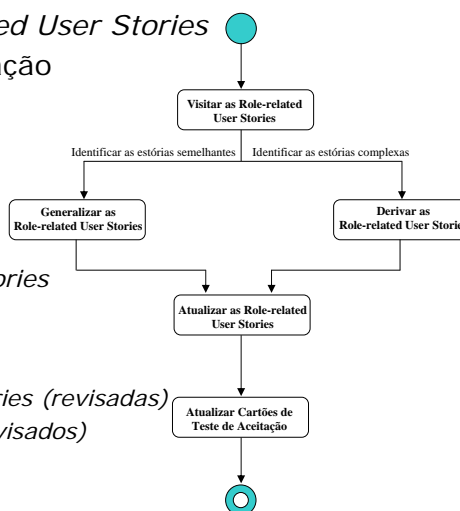


Figura 6: Sub-Processo de Refinamento

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

6. Definir Tarefas e Papéis

- Elementos são combinados p/ executar uma tarefa completa
- Artefatos de Entrada:
 - Catálogo de Permissões, *Role-related User Stories* e Cartões de Testes
- Artefatos de Saída:
 - Papéis e Associações Papéis-permissões

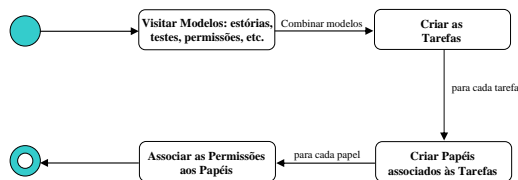


Figura 7: Sub-Processo de Definição de Tarefas e Papéis

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

7. Derivar a Hierarquia de Papéis Preliminar

- Objetivo: procurar os papéis que possuam as mesmas permissões que outros papéis
- Artefatos de Entrada:
 - Papéis e Permissões
- Artefatos de Saída:
 - Hierarquia de Papéis Preliminar e Catálogo de Permissões (Atualizado)

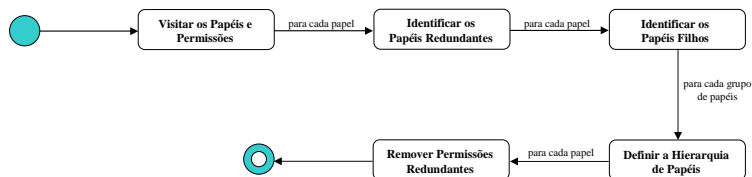


Figura 8: Sub-Processo de Derivação da Hierarquia de Papéis Preliminar

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

8. Definir o Modelo RBAC

- Objetivo: remover os papéis redundantes; definir novos papéis e restrições; mesclar as hierarquia de papéis -> Modelo RBAC

- Entradas:

- Hierarquia de Papéis preliminar
- Catálogo Restrições
- Catálogo Permissões

- Artefato de Saída:

- Modelo RBAC

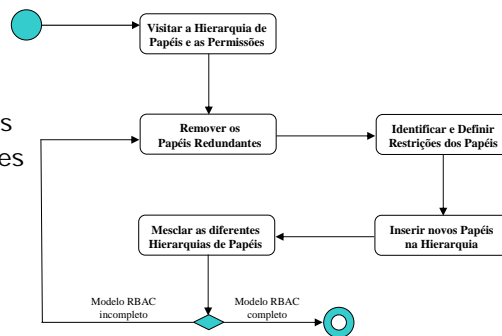
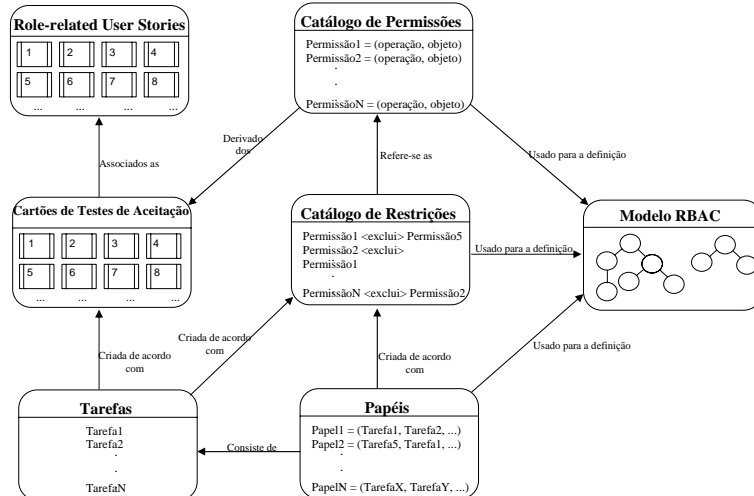


Figura 9: Sub-Processo de Definição do Modelo RBAC

Proposta da Integração: Jogo do Planejamento x Engenharia de Papéis

o Modelo de Inter-relações dos Artefatos:





Discussão e Conclusão

- Objetivo Alcançado:
 - Integração entre a engenharia de papéis e o jogo do planejamento XP
- Trabalho Atual:
 - Estudo de Caso – Projeto da Arrecadação On-line
- Trabalhos Futuros:
 - Encontrar os pontos de conflito entre os métodos ágeis e a engenharia de papéis
 - Aplicar o processo da engenharia de papéis proposto a um processo de desenvolvimento de software “tradicional”



FIM

Ludmila Pedrosa
ludmila.pedrosa@simplestec.com.br