6
Conclusão

Este capítulo apresenta uma avaliação da aplicação da abordagem proposta no nosso trabalho, as nossas contribuições e propostas para trabalhos futuros.

6.1 Avaliação

A aplicação do processo evoluído (Figura 3.3) proposto em nosso trabalho mostrou-se satisfatória no estudo de caso do *Expert Committe*, alcançando os objetivos traçados inicialmente, principalmente documentar o *rationale* da escolha da alternativa para operacionalização e possibilitar o rastro dos requisitos de segurança de alto nível até sua operacionalização (como são refinados em requisitos de nível de abstração menor; como são operacionalizados).

O objetivo de documentar o *rationale* da escolha da alternativa para operacionalização dos requisitos de segurança foi alcançado através dos modelos elaborados durante a execução do Passo 5 (Análise de Segurança) – Análise de medidas de defesa, apresentada na seção 4.2.

O rastro desde os requisitos de segurança de alto nível até sua operacionalização é possível, como pode ser verificado no exemplo do rastro do requisito de segurança do artigo revisado apresentado na tabela 6.1, a seguir.

Os resultados apresentados pela aplicação no estudo de caso se mostraram positivos. Acreditamos que também seja possível obter resultados positivos na aplicação do processo em outros casos.

Rastro do requisito: Segurança do Artigo Revisado	
Refinamento:	- **Confidencialidade interna** [Artigo Revisado]; - **Confidencialidade externa** [Artigo Revisado]; - **Consistência** [Artigo Revisado]
Vulnerabilidades relacionadas:	- Dependência de recurso Artigo Revisado (Organizador da Conferência x Autor); - Dependência de tarefa Revisar Artigo (Organizador da Conferência x Revisor); - Dependência de recurso Revisões com Conflito (Resolvedor de Conflito x Organizador da Conferência); - Dependência de recurso Resultado da Revisão (Autor x Organizador da Conferência).
Aplicação (Situações/Cenários):	Revisão de Artigos (‘*Article Reviews*’); Resolução de Conflitos (‘*Conflicts Solution*’); Recepção das Versões Finais (‘*Camera Ready Reception*’)
Atacantes:	- Atacante do Revisor; - Atacante do *Chair*; - Atacante do Autor; - Atacante do Membro do Comitê;
Intenções maliciosas dos atacantes:	- Revisões serem fraudadas (Atacante do Revisor, Atacante do *Chair*); - Revisões serem roubadas (Atacante do Revisor, Atacante do *Chair*, Atacante do Membro do Comitê) - Informação ser corrompida (Vírus, Internet Cracker); - Informação ser descoberta (Internet Hacker)
Alternativas de operacionalização p/ **Confidencialidade Interna**:	Usar chave de identificação; Usar regra de validação de acesso; Autenticar com senha - Autenticar com senha simples; - Autenticar com múltiplas senhas;
Alternativa escolhida p/ **Confidencialidade Interna**:	Usar chave de identificação; Usar regra de validação de acesso; Autenticar com senha simples;
Justificativa da escolha p/ **Confidencialidade Interna**:	Não ferir a usabilidade
Alternativas de operacionalização p/ **Confidencialidade Externa**:	Criptografar - Usar chave de 64Bits - Usar chave de 128Bits
Alternativa escolhida p/ **Confidencialidade Externa**:	Usar chave de 128Bits
Justificativa da escolha p/ **Confidencialidade Externa**:	Priorizar Segurança em relação ao Desempenho
Alternativas de operacionalização p/ **Consistência**	Usar chave de identificação; Usar regra de validação de acesso; Autenticar com senha - Autenticar com senha simples; - Autenticar com múltiplas senhas; Usar função *hash*; Informação ser copiada: - Usar mídia de DVD (para cópia); - Usar mídia magnética;
Alternativa escolhida - **Consistência**:	Usar chave de identificação; Usar regra de validação de acesso; Autenticar com senha simples; Usar função *hash*; Usar mídia de DVD (para cópia)
Justificativa da escolha p/ **Consistência**:	Não ferir a usabilidade

Tabela 6-1 - Rastro do requisito: Segurança do Artigo Revisado

Embora o estudo de caso tenha sido focado apenas nos requisitos de confidencialidade e consistência, acreditamos que a abordagem proposta possa ser aplicada também para requisitos de disponibilidade, com alguns cuidados especiais que discutiremos na seção trabalhos futuros, mais adiante.

6.2 Contribuições

A principal contribuição de nosso trabalho foi a evolução do processo proposto em [3], com a inclusão de passos específicos definição de SDsituation, definição de cenários, refinamento de atores (legítimos e atacantes) e definição de requisitos não-funcionais. Além dos passos em si, nosso trabalho propôs o uso de heurísticas para elaboração destes novos passos, como as heurísticas propostas em [4] para definição de SDsituations e definição de cenários, as propostas em [7] para o refinamento de requisitos não-funcionais, e as heurísticas propostas em nosso trabalho para o refinamento de atores.

Com estas contribuições, no estudo de caso conseguimos lidar melhor com a complexidade (para análise) dos modelos produzidos pelo framework i*, usando uma estratégia “dividir para conquistar”; apresentamos um entendimento melhor dos atores e suas relações; tornamos explícito o processo de definição dos requisitos não-funcionais, em especial, os de segurança; e, apresentamos os requisitos através de cenários, que evoluíram ao longo do processo desde a versão inicial (elaborada na primeira execução do passo 5, onde os requisitos de segurança apareciam apenas como restrições destes cenários) até a versão detalhada apresentada ao final do processo (onde os cenários apresentavam os requisitos de segurança integrados aos demais requisitos com as respectivas escolhas de operacionalização). Acreditamos que estes cenários detalhados representem uma forma mais adequada para validação pelos usuários e demais interessados que os modelos SD e SR.

Por fim, acreditamos que estes benefícios possam ser obtidos também na aplicação do processo evoluído em casos reais e em outros estudos de caso.

6.3 Trabalhos Futuros

Como trabalhos futuros, esperamos aplicar o processo evoluído, apresentado no capítulo 3, para elaboração dos requisitos de segurança em casos reais e outros estudos de caso com o objetivo de validá-lo.

Acreditamos que seja possível aplicar o processo evoluído também à elaboração de requisitos de disponibilidade. Para tanto, é necessário modelar cuidadosamente atores e recursos de infra-estrutura presentes no ambiente, uma vez que a disponibilidade de uma aplicação dependente destes atores e recursos. Por exemplo, a aplicação depende de recursos de hardware para ser rodada; de recursos a serem disponibilizados e/ou tarefas a serem desempenhadas pelo sistema operacional, por servidores de aplicação e por servidores *web*; e, de uma infra-estrutura de rede que possibilite a comunicação entre os atores. Consequentemente, a disponibilidade dos recursos, das tarefas, satisfação de metas e 'satisfação a contento' de metas flexíveis (acordadas com outros atores) dependerá sensivelmente da infra-estrutura do ambiente em que a aplicação se encontre.

O desenvolvimento futuro de uma ferramenta de modelagem integrada é necessário para viabilizar o uso eficiente do processo proposto. Em geral, os elementos usados como nós nos modelos i* (atores, metas, tarefas e recursos) aparecem em mais de um diagrama. Uma ferramenta integrada pode contribuir imensamente para manutenção da consistência dos modelos gerados.

Outro trabalho futuro a ser desenvolvido é modelar os requisitos de segurança com o objetivo de transformá-los em aspectos, justamente por serem os requisitos de segurança (e sua operacionalização) candidatos naturais a aspectos.