Biblioteca de Requisitos sobre propriedades de segurança em Sistemas Computacionais

Mariana A. Gualhano[1], Ausberto S. Castro Vera[2], Roberto C. Medeiros Junior[3]

[1] IFF - Instituto Federal de Educação, Ciência e Tecnologia Fluminense, Campos dos Goytacazes, RJ

[2]UENF - Universidade Estadual do Norte Fluminense Darcy Ribeiro, CCT-LCMAT - Ciência da Computação

[3]Faculdade Redentor, Itaperuna, RJ

mariana_gualhano@hotmail.com, ascv@uenf.br, r_junior17@hotmail.com

Resumo. *Este artigo apresenta uma metodologia de elicitação e análise de requisitos baseada na construção de uma biblioteca que inclui propriedades fundamentais de segurança computacional (integridade, confidencialidade e disponibilidade). Esta construção utiliza os conceitos de domínio de requisitos e orientação a aspectos e foi auxiliada por uma ferramenta de gerenciamento de requisitos (FGR).*

1. Introdução

As Tecnologias da Informação e a Internet tornaram-se cada vez mais um elemento importante do parque computacional das organizações modernas, de tal maneira que, o desenvolvimento e gerenciamento dos sistemas de informação são cada vez mais complexos e críticos. Um aspecto preocupante em tais organizações e sistemas é o aumento da fragilidade ou falta de segurança, manifestada em custos cada vez maiores na área de segurança, gerando assim, a necessidade de estudos mais aprofundados e medidas a serem implementadas, principalmente nas primeiras etapas do processo de desenvolvimento de tais sistemas, de modo que propriedades e requisitos relacionadas com a segurança sejam implementadas também na parte inicial do processo. Estas tarefas correspondem a Engenharia de Requisitos em conjunto com a Engenharia da Segurança.

[Dubois and Mouratidis 2010] salienta a importância de considerar a segurança desde o início do desenvolvimento do sistema, de modo que requisitos de segurança possam ser definidos junto com os requisitos do sistema.

[Gurses et al. 2013] afirma que a *Engenharia de Requisitos* é uma fase fundamental da Engenharia de Software, e ressalta a importância da elicitação e análise de requisitos, explicando que se não forem feitos de forma adequada, podem afetar o sucesso do projeto. [Gurses et al. 2013] também alerta que a descoberta da maior parte dos problemas e, geralmente os mais caros e de maior impacto negativo no desenvolvimento, são originados nas etapas iniciais do desenvolvimento. Estas duas afirmações, apontam a uma nova maneira de desenvolver sistemas computacionais, priorizando boas práticas na etapa inicial do ciclo de vida do desenvolvimento (análise de requisitos).

Neste contexto, este artigo tem como objetivo apresentar uma metodologia de elicitação e análise de requisitos baseada na construção de uma biblioteca que inclui

propriedades fundamentais de segurança computacional (integridade, confidencialidade e disponibilidade). Esta construção utiliza a metodologia de domínio de requisitos e orientação a aspectos e uma ferramenta de apoio FGR (Ferramenta de Gerenciamento de Requisitos).

2. Definições básicas

A maioria das definições básicas mencionadas nesta seção, estão devidamente descritas em [Castro-Vera 2013]. Um *requisito* é uma condição ou capacidade que deve ter ou possuir um sistema, produto, serviço, resultado ou componente para satisfazer um contrato, padrão, especificação ou outro documento formalmente imposto. Requisitos incluem necessidades quantificadas e documentadas, desejos e expectativas de patrocinadores, clientes e outros stakeholder [ISO/IEC/IEEE 2010]. Por exemplo, são requisitos: banco de dados centralizados, transmissão sem fio, segurança, armazenamento em nuvem, etc.

Considerando [Pfleeger and Pfleeger 2007], [Allen et al. 2008] e [Jacobs 2011], define-se *segurança computacional* como o estudo e objetivo de três aspectos fundamentais de qualquer sistema computacional: confidencialidade, integridade e disponibilidade. Um *sistema seguro* é aquele que satisfaz os requisitos de confidencialidade, integridade e disponibilidade.

Um *domínio de requisitos* é um sistema ou conjunto de requsitos D que pode ser decomposto (particionado) em componentes D_i, de modo que:

- $D = \cup_{i=1}^{n} D_i$ (união de componentes)
- $D_i \cap D_j = \emptyset$ se $i \neq j$ (componentes disjuntas)

Apresentar esta definição como um formalismo matemático (estrutura de sistema ou conjunto) é importante pelas seguintes razões:

- *Completeza e interdependência*. O domínio como uma união de componentes denota um tipo de interdependência entre componentes (sistema): a ausência de qualquer componente do sistema torna inviável a existência de tal sistema que está sendo construído.
- *Completeza e bem-definido*. Apresenta-se um esquema formal bem definido (conjunto), onde todos os elementos são bem definidos, possuem uma propriedade comum e não existe ambiguidade.
- *Unicidade*. Cada requisito formalmente pertence a uma única componente, evitando-se desta maneira a duplicação de requisitos no mesmo domínio.

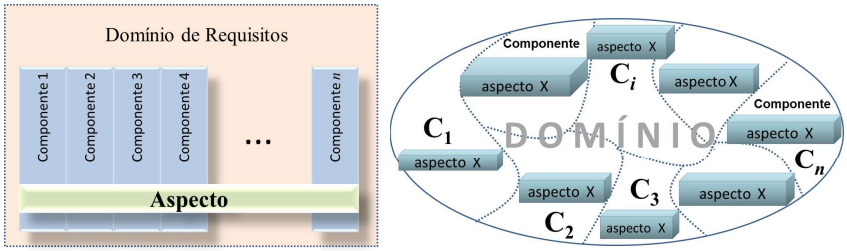

Figura 1. O conceito de *aspecto* e *domínio*

Para construir nossa metodologia para elicitação de requisitos aplicada a segurança computacional, definimos um *aspecto* como *um conjunto de requisitos que corta (cruza, é*

parte de, atravessa) todas as componentes do domínio de requisitos (como ilutsrado na Fig.1), i.e. a interseção do aspecto com cada uma das componentes do domínio, é não vazia. Os requisitos no processo de elicitação são agrupados em domínios que estão formados por componentes. Em geral, a partir de um domínio de n componentes: $C_1, C_2, C_3, ..., C_n$ pode-se estabelecer um aspecto como sendo subconjuntos não vazios de cada componente C_i. A Fig.1 (direita), ilustra o conceito de aspecto de uma forma mais realista devido a que cada componente representa conjuntos de requisitos de diferentes naturezas e tamanhos e portanto, os aspectos sobre cada componentes representam diferentes subconjuntos de requisitos.

3. O Paradigma de Desenvolvimento de Sistemas Seguros

O paradigma de desenvolvimento (utilizando biblioteca de requisitos sobre segurança), bem como a metodologia utilizada na análise de requisitos (usando domínios e aspectos) ([Castro-Vera 2013]) é ilustrada na Fig.2

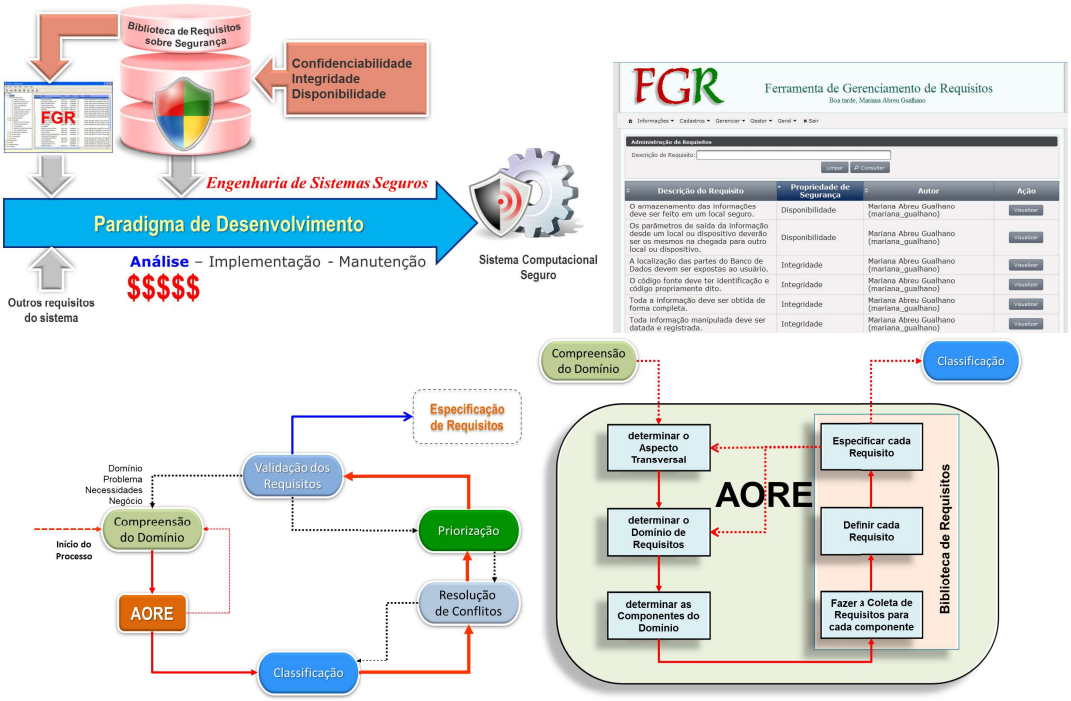

Figura 2. Paradigma de desenvolvimento, FGR e metodologia de análise de requisitos

4. Biblioteca de Requisitos

A construção de uma *biblioteca de requisitos para sistemas seguros* faz parte de um projeto de pesquisa sendo desenvolvido na UENF ([Castro-Vera 2013]), visando muitas propriedades sobre segurança computacional e considerando a metodologia de domínios e orientação a aspectos.

Primeiramente, foram escolhidos vários domínios considerados básicos ou padrão para a maioria de sistemas computacionais, entre os quais podemos mencionar:

- *Sistema computacional padrão*, com os seguintes componentes: hardware, software, banco de dados, pessoas, metodologias e documentação.

- *Ciclo de Vida da Informação*, com os componentes: obtenção, tratamento, armazenamento, distribuição e descarte da informação.
- *ERP Acadêmico*, com as componentes Gestão Acadêmica, Gestão Tecnológica, Gestão Empresarial, e Gestão Estratégica. Este domínio foi considerado como um estudo de caso aplicado a um sistema universitário ([Morelli 2013]).
- *Ciclo de Desenvolvimento*, com os componentes: definição, projeto, construção e manutenção.

Em um segundo momento foram considerados os aspectos básicos da segurança da informação (confidencialidade, integridade e disponibilidade) para cada um dos domínios escolhidos. E finalmente foram elicitados e analisados os requisitos, segundo a metodologia descrita em [Castro-Vera 2013], utilizando a ferramenta FGR. O estágio atual da biblioteca inclui aproximadamente 250 requisitos sobre segurança para qualquer sistema computacional.

5. Considerações Finais

Devido as limitações de espaço, foi apresentado apenas uma visão genérica da construção de uma Biblioteca de Requisitos baseado nas propriedades fundamentais da segurança computacional. Em razão da escassez de metodologias utilizadas para a coleta de requisitos, a metodologia proposta mostrou-se eficiente, facilitando a escolha dos requisitos, sua classificação, e a sua especificação. Uma facilidade para o levantamento de requisitos foi a utilização das ferramentas Visual Paradigm e FGR.

Referências

[Allen et al. 2008] Allen, J. H., Barnum, S., Ellison, R. J., McGraw, G., and Mead, N. R. (2008). *Software Security Engineering*. Addison-Wesley. Citado na página 2.

[Castro-Vera 2013] Castro-Vera, A. S. (2013). Engenharia de Requisitos e Segurança: uma metodologia orientada a aspectos. (Notas de Pesquisa). UENF-CCT-LCMAT-C.Computação. Citado 3 vezes nas páginas 2, 3 e 4.

[Dubois and Mouratidis 2010] Dubois, E. and Mouratidis, H. (2010). Guest editorial - security requirements engineering - past present and future. *Requirements Engeneering*, 15:1–5. Citado na página 1.

[Gurses et al. 2013] Gurses, S., Seguran, M., and Zannone, N. (2013). Requirements engineering within a large-scale security-oriented research project: lessons learned. *Requirements Eng.*, 18:43–66. Citado na página 1.

[ISO/IEC/IEEE 2010] ISO/IEC/IEEE (2010). Iso/iec/ieee 24765 - system and software engineering- vocabulary. Citado na página 2.

[Jacobs 2011] Jacobs, S. (2011). *Engineering Information Security: The Application of Systems Engineering Concepts to Achieve Information Assurance*. Wiley-IEEE Press, 1st edition. Citado na página 2.

[Morelli 2013] Morelli, C. P. G. (2013). Aplicação de uma metodologia AORE para elicitação de requisitos de segurança. TCC, UENF-CCT-LCMAT-CC. Citado na página 4.

[Pfleeger and Pfleeger 2007] Pfleeger, C. P. and Pfleeger, S. L. (2007). *Security in Computing*. Pearson Education Prentice Hall, 4th edition. Citado na página 2.