# 1
# Introdução

O objetivo deste capítulo é estabelecer o contexto da pesquisa realizada. Ao longo deste capítulo serão apresentadas: a motivação da pesquisa, o objetivo, trabalhos relacionados, conceitos utilizados e, por fim, um resumo da organização da dissertação.

## 1.1 Motivação

Existe um consenso tanto na comunidade acadêmica quanto nas empresas, que a segurança dos sistemas de software é importante. A sociedade moderna depende criticamente de uma variedade destes sistemas de software [21]. Com a popularização da internet, o número de incidentes de segurança reportados tem crescido rapidamente nos últimos anos [23]. A falha de um software pode provocar danos de abrangência variada, desde uma simples quebra do mecanismo de proteção de cópias de um 'jogo' até um desastre provocado por uma entrada não autorizada no sistema de controle de uma planta de usina nuclear. Em virtude disto, desenvolvedores de software devem pensar não apenas nos usuários, mas também nos adversários [21].

Os 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. É bem entendido pelos desenvolvedores de software que adicionar requisitos de qualidade (não-funcionais), inclusive requisitos de segurança, às arquiteturas de software após estas serem feitas é difícil ou impossível [21]. É fundamental, portanto, que tais requisitos sejam endereçados o mais cedo possível.

Giorgini [28] destaca ainda a importância de se capturar requisitos de segurança de alto nível, e de tornar claros os motivos do uso de mecanismos de proteção como criptografia e autorização de acesso.

## 1.2 Objetivo

Nosso trabalho apresenta uma abordagem orientada a metas para definição (elicitação, modelagem e análise) de requisitos de segurança específicos de aplicação. Através desta abordagem, são construídos modelos intencionais para os requisitos do domínio e para os requisitos de segurança.

A elaboração destes modelos, juntamente com a documentação complementar proposta, tem por objetivo atacar os seguintes pontos:

- ⇒ Elicitar os requisitos de segurança de alto nível;
- ⇒ Inter-relacionar os requisitos de segurança com os demais requisitos;
- ⇒ Tornar explícita a motivação dos requisitos de segurança (por que eles foram incorporados aos demais requisitos);
- ⇒ Identificar atacantes potenciais;
- ⇒ Identificar possíveis intenções maliciosas dos atacantes;
- ⇒ Identificar ameaças (medidas de ataque);
- ⇒ Identificar pontos de vulnerabilidade do sistema;
- ⇒ Avaliar alternativas para operacionalização;
- ⇒ Documentar o *rationale* da escolha da alternativa para operacionalização;
- ⇒ 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);

⇒ Descrever os requisitos de segurança de uma forma que facilite sua validação.

O escopo desta dissertação está delimitado em requisitos de segurança (*security*). Não é objetivo desta dissertação abordar fidedignidade (*dependability*) nem seguridade (*safety*).

## 1.3 Trabalhos Relacionados

A elicitação, modelagem e análise de requisitos de segurança específicos da aplicação é uma área que vinha sendo pouco explorada pela engenharia de requisitos até recentemente, como afirma Lamsweerde em [10]. Entretanto, recentemente esta área vem recebendo mais atenção da comunidade científica com alguns trabalhos publicados nos últimos anos. Uma parte considerável dos trabalhos recentes nesta área pode ser agrupada em dois segmentos:

(i) abordagens baseadas em anti-requisitos, como *Security Use Cases* [11], *Eliciting security requirements by misuse cases* [12] e *Misuse Cases: Use Cases with Hostile Intent* [24];

(ii) abordagens baseadas em estratégias orientadas a metas para elaboração dos requisitos de segurança, como *Security and Privacy Requirements Analysis within a Social Setting* [3], *Security Design Based on Social Modelling* [37], *Elaborating security requirements by construction of intentional anti-models* [10], *Intentional Modeling to Support Identity Management* [16], *Handling Obstacles in Goal Oriented Requirements Engineering* [19], *Requirement Elicitation Based on Goals with Security and Privacy Policies in Electronic Commerce [36]* e *Security and Trust Requirements Engineering* [28].

Nas abordagens baseadas em anti-requisitos, a âncora são os anti-requisitos. Um *anti-requisito* é um requisito de um usuário malicioso que subverte um requisito existente [27]. Nestas abordagens, em linhas gerais, os anti-requisitos são derivados a partir dos requisitos da aplicação. Firesmith vai além, em [11], derivando os requisitos de segurança dos anti-requisitos.

Nas abordagens baseada em estratégias orientadas a metas, as intenções são a âncora. Para os anti-requisitos, as intenções maliciosas dos atacantes são a âncora. Para os requisitos de segurança, as intenções dos atores do sistema são a âncora. Nestas abordagens, em linhas gerais, os anti-requisitos são derivados como alternativas para satisfação das intenções maliciosas dos atacantes e os requisitos de segurança como contra medidas de defesa dos atores do sistema.

No capítulo 5, é apresentada uma análise mais rica de alguns dos trabalhos mais relevantes.

## 1.4 Conceitos

No contexto desta dissertação, serão utilizados os seguintes conceitos:

- ⇒ **Requisito Não-Funcional (NFR)**: em engenharia de software, um requisito de software que descreve não o que o software deve fazer, mas como o software irá fazer isso, por exemplo, requisitos de desempenho do software, requisitos de interface externa do software, restrições da arquitetura (*design constraints*) do software, e atributos de qualidade do software. Requisitos não-funcionais são difíceis de testar; consequentemente eles são geralmente avaliados subjetivamente [29].

- ⇒ **Requisito Funcional**: um requisito de software/sistema que especifica uma função que o software/sistema ou componente do software/sistema deve ser capaz de desempenhar. Estes são os requisitos de software que definem o comportamento do sistema, isto é, o processo fundamental ou transformação que os componentes de software e hardware desempenham em entradas para produzir saídas [29].

- ⇒ **Confidencialidade**: ausência de revelação (*disclosure*) não-autorizada de informação [14].

⇒ **Consistência**[1]: ausência de alterações impróprias (não-autorizadas) do sistema.

⇒ **Integridade**: composição dos atributos de exatidão, consistência e completeza [7].

⇒ **Segurança (*security*)**: composição dos atributos de confidencialidade, integridade e disponibilidade [14].

⇒ **Fidedignidade (*Dependability*)**: habilidade de evitar falhas de serviço que sejam mais freqüentes ou mais severas que o aceitável [14].

⇒ **Disponibilidade**: prontidão para o serviço correto. [14]

⇒ **Seguridade (*Safety*)**: ausência de conseqüências catastróficas para o(s) usuário(s) e para o ambiente [14].

⇒ **Serviço correto**: serviço (entregue) que implementa as funções do sistema [14].

⇒ **Operacionalização**: técnica de desenvolvimento usada na arquitetura (*design*) ou implementação do sistema alvo para ajudar a 'satisfazer a contento' os requisitos não-funcionais [7]. Em outras palavras, é uma técnica para desdobrar os requisitos não-funcionais em requisitos funcionais.



## 1.5 Organização da dissertação

Esta dissertação apresenta uma abordagem orientada a metas para definição (elicitação, modelagem e análise) de requisitos de segurança específicos de aplicação.

[1] Em [14], consistência (e não integridade) é definida como "a ausência de alterações impróprias (não-autorizadas) do sistema. Nós optamos por considerar, como Chung et al [7], consistência como um sub-tipo de integridade, com o mesmo significado dado a integridade em [14].

No capítulo 2 é apresentado um breve resumo do *framework* i* [1] (um *framework* de modelagem intencional) que usamos para modelar os requisitos em nosso trabalho. Neste capítulo também são apresentadas duas extensões ao *framework* original propostos por Yu, que usamos em nossa abordagem.

O capítulo 3 apresenta a abordagem proposta em nosso trabalho para definição dos requisitos de segurança, baseada em um trabalho prévio de Liu, Yu e Mylopoulos [3].

No capítulo 4, é apresentado um estudo de caso com o exercício, passo a passo, da abordagem proposta em nosso trabalho.

O capítulo 5 apresenta uma análise de alguns trabalhos relevantes com abordagens distintas para definição de requisitos de segurança, situando-os em relação ao nosso trabalho.

No capítulo 6 são apresentadas as conclusões e contribuições do nosso trabalho, além das expectativas em relação a trabalhos futuros.