5

Análise de Trabalhos Relacionados

Este capítulo apresenta uma análise de alguns trabalhos relevantes com abordagens distintas para elaboração de requisitos de segurança: “Elaborando requisitos de segurança através da construção de anti-modelos intencionais [10]” e “Casos de Uso de Segurança[11]”. Em seguida é apresentado um trabalho interessante com foco em elicitação de requisitos de segurança: “Elicitação de requisitos baseada em metas com políticas de segurança e privacidade em comércio eletrônico [37]”. Na seção seguinte é apresentado um trabalho mais recente de Liu, Yu e Mylopoulos: “Desenho (Design) de Segurança Baseado em Modelagem Social” [37], seguida de uma breve análise do “Common Criteria [26]”. Finalmente, é apresentado um resumo dos trabalhos analisados juntamente com o nosso trabalho.

PUC-Rio - Certificação Digital Nº 0410836/CA

5.1 . “Elaborando requisitos de segurança através da construção de anti-modelos intencionais” [10]

5.1.1 Idéia

Este trabalho baseia-se, em termos gerais, na construção, de modo iterativo e concorrente de dois modelos: (i) um modelo intencional do sistema como ele deve ser (*system-to-be*) que cobre tanto o software quanto o ambiente no qual está inserido e inter-relaciona suas metas, agentes, objetos, operações, requisitos e premissas (*assumptions*); (ii) um anti-modelo, derivado do modelo do sistema, que apresenta (através de vulnerabilidades e capacidades requeridas para satisfação de anti-metas) como os elementos do modelo original podem ser maliciosamente ameaçadas, por que e por quem.

Os requisitos de segurança são elaborados sistematicamente pela iteração dos seguintes passos: (a) instanciar de padrões associados a classes (sub-tipos) de requisitos de segurança como privacidade, integridade, autenticação; (b) derivar especificações do anti-modelo que ameacem as especificações do modelo; e (c) derivar contra-medidas alternativas para estas ameaças e definir novos requisitos através da seleção das alternativas que melhor atendam a outros requisitos de qualidade do modelo. O modelo original é então enriquecido com novos requisitos de segurança derivados como contra-medidas para o anti-modelo.

5.1.2 Background

O método é baseado em um *framework* orientado a metas [19], desenvolvido anteriormente pelo próprio Lamsweerde, para geração e resolução de obstáculos ao atendimento de requisitos e foi estendido para obstáculos maliciosos, permitindo que o processo de refinamento de obstáculos seja guiado pelas metas dos atacantes com o objetivo de derivar vulnerabilidades observáveis e ameaças que possam vir a serem implementadas. Os conceitos de *metas*, *agentes* e *papéis* existentes neste *framework* são similares aos de i*.

Neste método, metas são organizadas em hierarquias E/OU de refinamento de abstração onde as metas de nível mais alto são em geral estratégicas e envolvem vários agentes e as metas de nível mais baixo são em geral técnicas e envolvem poucos agentes. O refinamento de uma meta termina quando cada uma de suas sub-metas é passível de realização por algum agente individual. Uma meta é operacionalizada em especificações de operações necessárias para alcançá-la. *Metas flexíveis* prescrevem comportamentos preferenciais, e podem ser usadas para selecionar alternativas preferenciais em um grafo de refinamento de meta E/OU.

Propriedades do domínio são declarações descritivas sobre o ambiente, como leis físicas ou normas organizacionais.

Um *requisito* é uma meta terminal sob responsabilidade de algum agente no modelo original. Uma *expectativa* é uma meta terminal de um agente no ambiente (diferentemente dos requisitos, expectativas não podem ser realizadas pelo sistema). Um *atacante* é um agente malicioso no ambiente. Uma *anti-meta* é uma

PUC-Rio - Certificação Digital Nº 0410836/CA

meta de um atacante. Uma *ameaça* é um obstáculo intencionalmente estabelecido por um atacante. *Objetos* têm estados definidos por seus atributos e relacionamentos para outros objetos. Podem ser passivos (entidades, associações, eventos) ou ativos (agentes).

Um *obstáculo* a uma meta, em termos declarativos, é uma condição cuja satisfação pode evitar que a meta seja alcançada (satisfeita). A análise de obstáculos consiste em adotar uma visão pessimista para as metas, requisitos e expectativas que são elaboradas. O princípio é identificar tantos modos de obstruir metas, requisitos e expectativas quanto possíveis. Para resolver tais obstruções são elaborados requisitos mais completos para sistemas mais robustos.

A especificação de requisitos de segurança específicos da aplicação é obtida, através da aplicação de padrões de especificação genéricos associados às classes de segurança, da seguinte forma: (a) instanciando meta-classes como Objeto, Agentes e atributos genéricos como informação para classes sensíveis específicas da aplicação, e (b) especializando predicados como ‘Autorizado’, ‘Sob Controle’ ou ‘Usando’ pela substituição por definições específicas da aplicação.

Uma árvore de obstáculos é ancorada por meta e sua raiz é a negação de uma meta (do modelo original). Os obstáculos podem ser gerados formalmente pela regressão da negação através das propriedades do domínio e outras declarações de meta ou pelo uso de obstrução formal e refinamento de padrões.

5.1.3 Procedimento

Os passos do procedimento para construção do anti-modelo são os seguintes:

1 – Capturar as anti-metas iniciais através da negação dos padrões de especificação de metas de classe de segurança (confidencialidade, integridade, disponibilidade), instanciados para objetos sensíveis do modelo de objetos;

2 – Para cada anti-meta, elicitar potenciais atacantes que poderiam possuir a anti-meta;

PUC-Rio - Certificação Digital Nº 0410836/CA

3 – Para cada anti-meta e (para cada) classe de atacante correspondente identificada, elicitar as anti-metas de mais alto nível de abstração;

4 – Elaborar o grafo E/OU da anti-meta através de refinamento “E” (*AND*) de anti-metas por todos os ramos alternativos, com o objetivo de derivar anti-metas terminais passíveis de realização pelo atacante identificado ou por um agente do sistema atacado. Os primeiros são anti-requisitos atribuídos aos atacantes enquanto os últimos são vulnerabilidades atribuídas aos agentes do sistema.

5 – Derivar os anti-modelos de agentes e objetos da especificação de anti-metas.

6 – Operacionalizar (via refinamento E/OU) todos os anti-requisitos em termos das capacidades do correspondente atacante.

Uma vez gerados os anti-modelos intencionais, o próximo passo é considerar contra-medidas alternativas para as vulnerabilidades e anti-requisitos encontrados. Estas contra-medidas são geradas sistematicamente usando operadores como: substituição de meta; substituição de agente; enfraquecimento de meta; restauração de meta; e prevenção de anti-meta; juntamente com operadores específicos de segurança como: proteger de vulnerabilidade; neutralizar de ameaça; e evitar vulnerabilidade.

5.1.4 Semelhanças e diferenças de [10] com o nosso trabalho e [3]

A construção de anti-modelos proposta por Lamsweerde [10] tem semelhança com os passos 1 – Identificação de atacantes, 3 – Identificação de intenções maliciosas e 4 – identificação de medidas de ataque da análise de medidas de ataque; de nossa abordagem. (estes passos foram inicialmente propostos em [3]).

Anti-metas correspondem às intenções maliciosas, embora em [10] as anti-metas iniciais sejam formalmente geradas a partir da negação das metas flexíveis de segurança. Uma diferença em relação à ordem de execução dos passos é que em [10], são identificados possíveis atacantes para uma anti-meta, enquanto na

PUC-Rio - Certificação Digital Nº 0410836/CA

nossa abordagem são identificadas possíveis intenções maliciosas para um atacante.

A especificação dos requisitos em [10] é feita através da aplicação de padrões de especificação, que guarda semelhança com catálogos de requisitos não-funcionais, embora [10] refine esses padrões formalmente. A operacionalização de anti-metas (medidas de ataque) em [10] também podem ser feita formalmente.

A escolha entre as alternativas é guiada pela prioridade dos demais requisitos de qualidade (embora não fique claro em [10] como estes outros requisitos são afetados por, ou afetam, estas escolhas).

Uma diferença relevante é que requisitos funcionais e não-funcionais são modelados da mesma forma em [10] enquanto em i* os requisitos não-funcionais (metas flexíveis) distinguem-se claramente dos demais requisitos.

PUC-Rio - Certificação Digital Nº 0410836/CA

5.2 “Casos de Uso de Segurança” [11]

5.2.1 Idéia

A idéia geral é que casos de uso de segurança (*security use cases*), usados para analisar e especificar requisitos de segurança, podem ser derivados dos casos de mau uso (*misuse cases*), estes últimos usados para analisar e especificar ameaças. Assim como casos de uso (*use cases*) e casos de mau uso, os casos de uso de segurança são apresentados de forma descritiva, numa seqüência de passos. O rastro dos requisitos pode ser feito nos dois sentidos entre casos de uso, casos de mau uso e casos de uso de segurança.

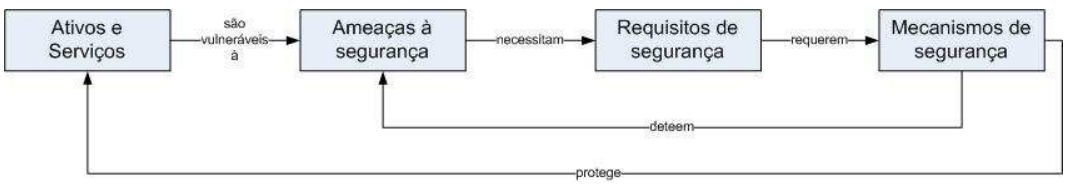

Figura 5.1 - Abordagem de casos de uso de segurança, linhas gerais, capturada de [11]

5.2.2 Semelhanças e diferenças de [11] com o nosso trabalho e [3]

No tipo de abordagem usado em [11], baseadas em anti-requisitos, a questão intencional não vem à tona. Tanto as motivações dos atacantes, quanto as motivações dos atores do sistema não são abordadas. Estas questões são centrais tanto no nosso trabalho e em [3], como também em [10].

Não está claro em [11] como os requisitos de segurança são desdobrados em mecanismos de segurança, nem há menção a escolha de alternativas para 'satisfação a contento' dos requisitos de segurança, deixando abertas lacunas mencionadas por Giogini em [28]: 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.

Estas lacunas prejudicam o rastro dos requisitos de segurança e deixam encoberto o *rationale* da escolha de alternativas.

A apresentação em forma descritiva dos requisitos de segurança, juntamente com os demais requisitos, aparece em [11] em virtude dos casos de uso de segurança serem descritos de forma parecida a de casos de uso e casos de mau uso. Em nosso trabalho, esta forma descritiva aparece em virtude da introdução do passo 5 – Definição de cenários.

PUC-Rio - Certificação Digital Nº 0410836/CA

5.3 "Elicitação de requisitos baseada em metas com políticas de segurança e privacidade em comércio eletrônico" [37]

5.3.1 Idéia

Este trabalho segue uma filosofia semelhante aos demais trabalhos com abordagem orientada a metas. O processo usado, em linhas gerais, é composto dos seguintes passos:

1. identificação dos atores envolvidos (*stakeholders*);
2. elicitação das metas do sistema;

3. atribuição de valores para as metas;
4. refinamento das metas;
5. operacionalização das metas;
6. avaliação de riscos;
7. criação de políticas de segurança e privacidade;
8. avaliação de conformidade com políticas existentes.

5.3.2 Semelhanças e diferenças

Este trabalho traz como principais diferenciais em relação aos demais trabalhos com a mesma abordagem a atribuição de valores para as metas e a avaliação de riscos, e em menor grau a avaliação de conformidade com políticas existentes.

A avaliação de riscos é dividida em três sub-atividades: (i) identificação de ameaças e vulnerabilidades; (ii) estimativa da probabilidade de ocorrência e (iii) escolha da estratégia de mitigação do risco. A sub-atividade de identificação de ameaças e vulnerabilidade responde também pela identificação das fontes de ameaça (atacantes), motivação (intenções maliciosas) e ações (medidas de ataque). A estimativa da probabilidade de ocorrência é feita de forma qualitativa, usando uma escala com três valores: alto, médio e baixo. A escolha da estratégia de mitigação do risco é feita pela adição de uma nova meta ou sub-meta em resposta ao risco identificado ou através de um novo refinamento de meta visando adicionar uma restrição ou atenuar o risco identificado. Embora não esteja muito claro, essa meta serve para definição dos requisitos não-funcionais (modelados como metas), em função dos riscos identificados.

A partir deste ponto (após a avaliação de riscos) há dois caminhos a serem seguidos: avaliação da conformidade com as políticas de segurança e privacidade da organização, caso elas existam, com o objetivo de garantir que os requisitos sejam implementados de acordo com estas políticas; ou, a criação de novas políticas de segurança e privacidade para implementação destes requisitos.

PUC-Rio - Certificação Digital Nº 0410836/CA

As políticas de segurança e privacidade neste trabalho têm significados semelhantes ao que as alternativas de operacionalização têm no nosso: políticas de segurança e privacidade são normas de como os requisitos de segurança devem ser implementados, como por exemplo, políticas de identificação e autenticação.

Este trabalho traz alguns pontos interessantes não explorados em nosso trabalho. A atribuição de valores às metas é bastante interessante, e pode ser usada na priorização dos requisitos não-funcionais para escolha da alternativa de operacionalização. A avaliação de riscos, com a atribuição de um valor para o risco (ou para ameaça) é outra idéia interessante. O valor para o risco fornece um parâmetro para avaliação, ainda que de forma subjetiva ou qualitativa, do quanto se deseja investir para garantir a segurança. Em alguns casos, em virtude do impacto proporcionado e da probabilidade do risco vir a se concretizar, pode ser considerado satisfatório apenas "impedir parcialmente" (*weakly deny*) a satisfação da intenção maliciosa de algum atacante em vez de "impedir completamente" (*deny*) a sua satisfação.

PUC-Rio - Certificação Digital Nº 0410836/CA

5.4 "Desenho (*Design*) de Segurança Baseado em Modelagem Social" [37]

Neste trabalho mais recente (publicado em 2006) Liu, Yu e Mylopoulos apresentam, de forma mais resumida, um processo idêntico ao apresentado em [3]. Este processo, focado na definição dos requisitos específicos de segurança, é composto pelos seguintes passos: (i) identificação de atores e objetivos; (ii) identificação de atacantes; (iii) avaliação das conseqüências de ataques; e (iv) identificação de contramedidas alternativas.

O passo (ii) identificação de atacantes é mais elaborado que em [3], com o estabelecimento de um par de fronteiras de confiança para o sistema: uma interna e outra externa. A idéia é que os atores dentro da fronteira interna de confiança, ou além da fronteira externa, não constituem fontes de ameaça ao sistema uma vez que atores dentro dos limites destas fronteiras são considerados confiáveis. Com isto o 'espaço de procura' por atacantes é delimitado por estas fronteiras. Em

nossa proposta não usamos fronteiras de confiança para delimitar o ‘espaço de busca’ por possíveis atacantes.

Nossa abordagem apenas segmenta os atacantes em “internos” e “externos”. São considerados atacantes “internos” os atacantes derivados dos atores legítimos, com as mesmas habilidades e capacidades, porém com intenções maliciosas; enquanto os demais atacantes, que possam ameaçar o sistema sem possuir capacidades e habilidades semelhantes aos atores legítimos são considerados atacantes “externos”.

Tanto neste novo trabalho, como em [3], Liu, Yu e Mylopoulos consideram a possibilidade de ataques acidentais como, por exemplo, mau funcionamento de software, desentendimento de instrução dos usuários ou execução imprópria de instruções. Os ataques acidentais seriam ataques não intencionais.

No nosso trabalho, preferimos abordar o assunto de forma um pouco diferente, não considerando este tipo de acidente como ataque, justamente por não ser intencional. Porém, do mesmo modo que Liu, Yu e Mylopoulos, nos preocupamos em observar as vulnerabilidades do sistema a estes tipos de acidentes.

Os demais passos apresentados em [37] são semelhantes aos apresentados em [3], discutidos anteriormente no capítulo 3.

PUC-Rio - Certificação Digital Nº 0410836/CA

5.5 “Common Criteria” [26]

O “Common Criteria” não é um trabalho na linha de definição de requisitos de segurança, uma vez que não propõe como elicitar, modelar e analisar estes requisitos. É um trabalho voltado mais especificamente para uma sub-atividade da análise: a verificação. O “Common Criteria” propõe uma série de critérios para avaliação da segurança de um software. Estes critérios, muitas vezes, são alternativas para operacionalização de requisitos de segurança que um software ou

componente deve ter para ser considerado seguro, como por exemplo, o uso de mecanismos de autenticação e criptografia.

Em nossa avaliação, este tipo de trabalho é bastante útil para atividade de verificação, ou ainda como fonte para elicitação de alternativas de operacionalização para requisitos de segurança de software. No entanto, deixa em aberto lacunas da modelagem (como os requisitos não-funcionais são modelados, como se integram aos demais requisitos) e não é muito claro em relação à escolha das alternativas disponíveis.

5.6 Resumo

A tabela 5.1, a seguir, apresenta um resumo das principais características dos trabalhos analisados neste capítulo e de nosso trabalho. Estes trabalhos são frutos de um esforço relativamente recente da comunidade acadêmica sobre em tratar os requisitos de segurança durante a atividade de modelagem.

PUC-Rio - Certificação Digital Nº 0410836/CA

Resumo de características dos trabalhos analisados			
Trabalho Analisado	**Ponto de partida**	**Idéia chave**	**Diferencial**
Elaborando requisitos de segurança através da construção de anti-modelos intencionais [10]	Anti-metas geradas através da negação das metas originais	Construção de anti-modelos para os anti-requisitos a partir da negação do modelo de requisitos	A geração de obstáculos para a construção do anti-modelo pode ser feita formalmente.
Casos de Uso de Segurança [11]	"Casos de mau uso" (*misuse cases)*	Os casos de uso de segurança são derivados a partir dos "casos de mau uso"	Expressos de forma descritiva, semelhante aos casos de uso
Elicitação de requisitos baseada em metas com políticas de segurança e privacidade em comércio eletrônico [37]	Elicitação das metas dos atores	As metas são elicitadas e refinadas até sua operacionalização, avaliando-se a conformidade da operacionalização com as políticas de segurança existente ou criando-se novas políticas	Atribuição de valor às metas, tratamento de riscos mais apurado e uso de políticas de segurança.
Desenho (*Design*) de Segurança Baseado em Modelagem Social [37]	Elicitação das metas dos atacantes (intenções maliciosas)	Construção de modelos intencionais, incluindo atacantes e suas metas	Estabelecimento de um par de fronteiras de confiança para restringir o espaço de busca por atacantes
Common Criteria [26]	Critérios estabelecidos na própria norma	Conjunto de boas práticas e critérios para aferição de segurança	Foco na atividade de verificação.
Uso de estratégias orientadas a metas para modelagem de requisitos de segurança	Elicitação das metas dos atacantes (intenções maliciosas)	Construção de modelos intencionais, incluindo atacantes e suas metas	Uso de *SDsituations* para lidar com a complexidade dos modelos e cenários para apresentação dos requisitos de segurança.

Tabela 5-1 – Resumo de características dos trabalhos analisados

PUC-Rio - Certificação Digital Nº 0410836/CA

PUC-Rio - Certificação Digital Nº 0410836/CA