1
Introdução

A construção de um software fidedigno é um dos grandes desafios a ser alcançado por todos aqueles que desenvolvem software. Entre as várias questões relacionadas à fidedignidade do software, o desenvolvimento de software seguro apresenta-se como uma área desafiadora e de interesse cada vez maior por parte das empresas e dos pesquisadores (Redwine, 2004).

Apesar de todo o investimento realizado contra as ameaças à segurança da informação, a quantidade de ataques a empresas e seus aplicativos vem aumentando mais rapidamente do que a nossa capacidade em poder enfrentá-los. Profissionais da indústria de informática concordam que um software inseguro é uma das principais causas de falhas de segurança, que freqüentemente levam a inúmeros problemas nos negócios das empresas (Lanowitz, 2005). Segundo o relatório *IT Security Study: The Current State of IT Security Budgets, Management Practices, and Security Incidents da Computer Economics* (McManus, 2006), só o impacto dos ataques de vírus do computador no mundo já atingiu a cifra de $111 bilhões de dólares se somarmos os gastos de 1995 até 2005, como pode ser observado na tabela 1 a seguir.

Ano	Valor
2005	$14.2 Bilhões
2004	$ 17.5 Bilhões
2003	$ 13.0 Bilhões
2002	$ 11.1 Bilhões
2001	$ 13.2 Bilhões
2000	$ 17.1 Bilhões
1999	$ 13.2 Bilhões
1998	$ 6.1 Bilhões
1997	$ 3.3 Bilhões
1996	$ 1.8 Bilhão
1995	$ 500 Milhões

Tabela 1: Impacto Financeiro de Ataques de Vírus - Fonte Computer Economics, (McManus, 2006).

Diante deste grande desafio de se produzir software fidedigno em relação à segurança da informação, como podemos garantir que o investimento das empresas em segurança da informação está tendo o retorno desejado, particularmente, aquele investimento realizado para garantir um software seguro, isto é, em níveis aceitáveis de segurança?

Mas como avaliar a segurança de um software? É realmente possível hoje medir se um software é seguro ou não? Se possível, como fazer isso?

1.1 Motivação

Várias pesquisas indicam que com o passar dos anos a segurança de informação vem crescendo em prioridade para muitas organizações (Henning, 2001; Davis, 2004 ; Lanowitz, 2005; Goertzel et al., 2006). A preocupação com a segurança de computador está se tornando crescentemente, não só em relação ao investimento a ser aplicado em segurança, mas também em relação ao retorno deste investimento num momento em que as áreas de TI vem sendo orientadas a reduzirem seus custos.

Diante dos relatórios freqüentes com notícias sobre falhas de segurança sérias, principalmente nos softwares, gerentes de segurança e profissionais de TI estão sendo, mais do que nunca, pressionados a demonstrar a efetividade dos seus programas de segurança.

Como forma de justificar o investimento em segurança, cada vez mais as organizações estão reconhecendo a importância de um programa de métricas de segurança, porém há pouca informação disponível ao redor da prática "O como fazer?" para estabelecer um programa com métricas confiáveis (Bellovin, 2006). Como resultado, métricas de segurança são envoltas em mistério e são consideradas muito difíceis de serem implementadas (Henning, 2001).

Como os gastos com segurança continuam subindo (McManus, 2006), os analistas da indústria afirmam que as iniciativas de métricas de segurança serão críticas para entender o impacto dos programas de segurança.

Mas avaliar a segurança de um software não é uma tarefa fácil. Se não conseguimos medir segurança, então como podemos melhorá-la? (Bellovin, 2006)

Ao melhorar a segurança em um software, queremos que o software resista a ataques deliberados ou acidentais, impedindo a divulgação de dados confidenciais a quem não tem direito, registrando as tentativas de agressão e acidentes e que disponibilize informações que facilitem localizar as brechas de segurança e as faltas na sua implementação. Em suma, um software mais fidedigno quanto aos seus requisitos de segurança.

1.2 Proposta

A proposta desta dissertação é mostrar que hoje ainda não dispomos de métricas confiáveis para medir o nível de segurança de um software. Para a realização deste trabalho, esta proposta de dissertação propõe:

1. Conceituar segurança, descrevendo as principais propriedades relacionadas com o tema.

2. Descrever os princípios para avaliações de segurança de software e a

importância das métricas de segurança de software.

3. Apresentar os principais métodos de avaliação quantitativa de segurança hoje existentes, apontando as suas falhas.

4. Apresentar algumas dificuldades na geração de métricas de segurança quantitativas.

5. Propor áreas de pesquisa para o estudo de métricas de segurança de software.

1.3 Discussão e contribuições esperadas

Segundo Redwine (2004), nem no mundo físico, nem em Engenharia de Software a segurança pode ser garantida por completo. Apesar disto, um bom programa de métricas deve ser adotado para obtermos evidências estatísticas de que um processo produz software seguro ou que um software possui um nível de segurança adequado. Um programa de métricas pode ajudar a uma organização a ter respostas a perguntas como:

1. Qual o retorno do investimento em segurança nas aplicações?

2. Qual é a capacidade e a competência dos recursos em trabalhar com segurança?

3. As ações de segurança estão baseadas em boas práticas conhecidas e em acordo com padrões aplicáveis e com requisitos legais?

4. Como os riscos de segurança estão sendo gerenciados?

5. Qual é a performance alcançada por nossos sistemas em termos de gerenciamento de ameaças, de vulnerabilidades, de responder a eventos e de retomar e controlar perdas?

Esta é uma iniciativa importante porque muitas empresas enfrentam hoje, além do próprio problema do aumento do número de incidentes contra suas políticas de segurança da informação, exigências de leis governamentais tais como

a *Sarbanes-Oxley*[1] (Tipton, 2004), que preconizam uma maior segurança das aplicações utilizadas por estas instituições.

Os resultados deste trabalho podem ser utilizados para a melhoria de práticas hoje utilizadas no desenvolvimento e na manutenção de softwares.

1.4 Organização deste trabalho

No segundo capítulo serão apresentados conceitos básicos sobre segurança importantes para o entendimento e elaboração do trabalho.

O terceiro capítulo apresenta o conceito de métricas de segurança de software, descrevendo a sua importância e os principais métodos para avaliação de segurança de software.

No quarto capítulo são apresentados alguns métodos para avaliação quantitativa de segurança presentes na literatura, suas vantagens e desvantagens. Uma comparação entre os métodos também é apresentada ao final deste capítulo.

No quinto capítulo são apresentadas as dificuldades hoje encontradas na geração das métricas de segurança de software e o porquê de até hoje não conseguirmos definir com sucesso tais métricas.

[1] Sarbanes-Oxley - lei americana que busca aperfeiçoar os controles financeiros das empresas e apresentar eficiência na governança corporativa. A lei visa garantir a transparência na gestão financeira das organizações, credibilidade na contabilidade, auditoria e a segurança das informações para que sejam realmente confiáveis, evitando assim fraudes, fuga de investidores, etc.