3
Métricas de Segurança de Software

Independente do modelo de avaliação da segurança de software, esta dissertação busca um critério para medir segurança de softwares antes que estes sejam colocados em produção. Conseguimos até com certo sucesso medir insegurança, porém o que estamos buscando é como medir objetivamente se o sistema é potencialmente seguro ao analisarmos o seu projeto, código, testes, etc, isto é, antes de ser colocado em uso.

Devanbu (2000) declara que segurança é como beleza, depende do observador. O entendimento do que é belo varia de observador para observador. Apesar desta afirmação, métricas de segurança de software devem ser usadas para avaliar a segurança, eliminando a advinhação e estimativas subjetivas sobre segurança. O princípio de que uma atividade não pode ser gerenciada se ela não pode ser medida também se aplica à segurança.

A prática de medição vem sendo reconhecida há muito tempo como uma atividade crítica para o desenvolvimento de sistemas com qualidade assegurada. Segurança necessita de meios de avaliação comparáveis a aqueles empregados em outros atributos de qualidade de software, como por exemplo manutenibilidade, que é um atributo de qualidade bem entendido e que pode ser quantitativamente estimado ao avaliarmos propriedades tais como o tamanho e a complexidade.

Este capítulo tem como objetivo introduzir o tema métricas de segurança de software.

3.1 Medição de Software

A medição pode ser definida como um processo pelo qual números ou símbolos são associados a atributos de entidades do mundo real, com o objetivo

de caracterizá-la de acordo com um conjunto de regras claramente definido (Fenton, 1995). Então, a medição requer: Entidades, Atributos e Regras.

Exemplos de entidades incluem: produtos, processos, recursos, artefatos, atividades, agentes, organizações, ambientes e restrições. Entidades também podem ser conjuntos ou coleções de outras entidades.

Atributos são características ou propriedades de entidades. Assim como uma pessoa (entidade) pode ser descrita por características tais como altura, cor dos olhos, sexo, idade e anos de experiência, entidades de software podem ser descritas por atributos tais como tamanho, custo, tempo, esforço, tempo de resposta, taxa de transações, número de defeitos encontrados, etc. Um processo de medição de segurança precisa capturar os atributos relevantes de um sistema, antes de realizar uma avaliação de segurança.

As regras definem como a medição será realizada. Um processo de medição contém todos os passos a serem seguidos para a realização de medições em uma organização.

A medição é um processo que produz como resultado um conjunto de medidas. Uma medida constitui um mapeamento entre um atributo empírico e uma escala matemática. Unidades de medida são estabelecidas para convencionar como esses atributos devem ser registrados (Park et al., 1996).

Uma métrica consiste em uma unidade de medida e a correspondente medição (definição + processo) utilizada para medir ou avaliar uma determinada propriedade de uma entidade.

Um processo de medição pode ser baseado em instrumentos (Medir), pode utilizar julgamento humano baseado em algum critério definido (Avaliar) ou utilizar julgamento humano sem um critério definido (Julgar). Segurança deve ser medida, pode ser avaliada, mas nunca deveria ser somente julgada.

Segundo Park et al. (1996), uma organização de software tem bons motivos para estabelecer um programa de métricas de software. Através das métricas a organização pode:

- Conhecer seus processos, produtos, recursos, ambientes e estabelecer *baselines* para comparar com avaliações futuras.

- Avaliar se a situação de uma determinada entidade em relação às metas pré-estabelecidas está com o seu desempenho conforme esperado. Também avaliamos para verificar as metas de qualidade e para medir o impacto das melhorias de processos e tecnologia sobre processos e produtos.

- Prever para poder melhor planejar. A medição serve para obter entendimento do relacionamento entre processos e produtos e construir modelos a partir destes relacionamentos. Projeções e estimativas baseadas em dados históricos também nos ajudam a analisar riscos e fazer comparações de projetos e custos.

- Melhorar a organização ao coletar informações quantitativas que auxiliam na identificação de obstáculos, causas raiz, ineficiências, e outras oportunidades de melhoria da qualidade do produto e da performance do processo, facilitanto a melhoria nessas atividades ao aplicar ações corretivas, baseadas em medições observadas.

Existem poucos trabalhos sobre métricas de segurança, especificamente em Engenharia de Software (Langweg, 2006). Um pouco de atenção até tem sido dada a métricas focadas na segurança operacional de sistemas de informação em seu ambiente de produção, mas de uma forma geral os trabalhos ainda são poucos.

3.2 Métricas de Segurança de Software

Métricas de segurança são ferramentas para que profissionais de segurança da informação avaliem os níveis de segurança de seus sistemas, produtos e processos**,** dando a possibilidade de tratar as questões de segurança que estão enfrentando. Métricas podem ser úteis para identificar vulnerabilidades em sistemas e avaliar os seus riscos, orientando as ações corretivas de maior prioridade, aumentando o nível de maturidade sobre segurança na organização.

Com o conhecimento de métricas de segurança, um profissional de segurança da informação poderia tentar responder a perguntas como:

- As aplicações estão hoje mais, ou menos, seguras do que antes?
- Como nós saberemos quando nossos sistemas estarão seguros?
- Estamos nós seguros o suficiente?
- Treinar em segurança realmente faz diferença?

As métricas também podem ser usadas para justificar e direcionar futuros investimentos em segurança e também facilitar a prestação de contas dos governantes e melhorar a confiança dos clientes. Isto porque o investimento em segurança, aqui considerando desenvolvimento de software e ambiente de operação, não é pequeno. Além das preocupações tradicionais no desenvolvimento de software com qualidade assegurada, as equipes de desenvolvimento e operação dos sistemas se vêem obrigadas a se preocupar com conceitos que não estão acostumadas a trabalhar. Isso requer investimento em treinamentos e contratação de consultoria especializada.

Distinguir métricas significativas é crítico para o desenvolvimento de um programa de métricas de segurança efetivo, principalmente para os programas com responsabilidade direta com a administração da segurança e para aqueles que tratam diretamente com assuntos e interesses da administração da organização. As métricas verdadeiramente úteis indicam o grau para o qual as metas de segurança, como confidencialidade dos dados, está sendo alcançado e elas orientam ações que devem ser tomadas para melhorar o programa de segurança de uma organização como um todo.

Devido à impossibilidade de se medir diretamente o nível de segurança de um software, sem considerar o sistema de informação em que está inserido, diferentes fatores e conseqüências que têm efeito sobre este nível de segurança devem ser avaliados. Para que isto seja possível, as métricas de segurança devem ser obtidas em níveis diferentes dentro de uma organização, podendo ser mais detalhadas, quando coletadas ao nível de sistema de informação, ou ser

acumuladas e desdobradas em níveis mais altos progressivamente, dependendo do tamanho e complexidade de uma organização. Seja qual for o grau de detalhamento da métrica de segurança, elas devem estar fundamentadas em metas e objetivos de desempenho de segurança da organização (ITSEC, 1991).

3.3 Classificações de Métricas de Segurança encontradas na Literatura

A definição e escolha das métricas de segurança não é uma tarefa muito simples. Muitas vezes, o termo métrica de segurança é confuso e ambíguo em muitos contextos de discussão sobre segurança da informação. No ano de 2001 foi realizado um evento intitulado *Workshop on Information Security System Scoring and Ranking* (Henning, 2001) que tinha como principal objetivo discutir sobre o assunto métricas para segurança da informação de produtos e tecnologia de informação numa tentativa de minimizar estes problemas. Neste W*orkshop* foi proposta uma classificação para métricas de segurança em 3 categorias: técnico, organizacional e operacional (Figura 7). Esta classificação tem sido adotada na maioria dos trabalhos sobre métricas de segurança de software desde então.

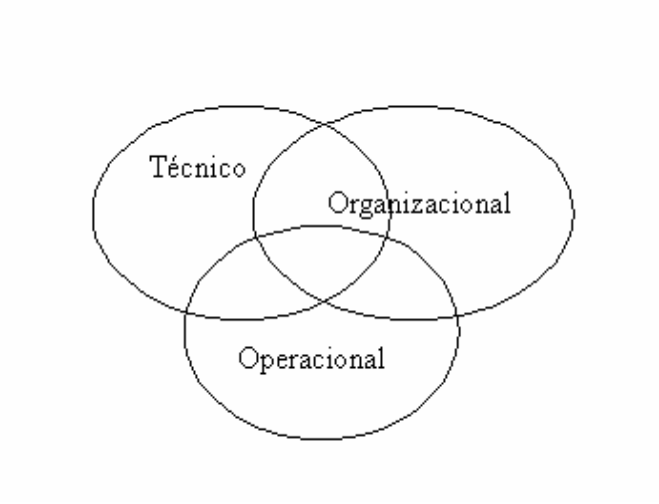

Figura 7: Classificação das métricas de software encontradas em HENNING(2001)

Na categoria técnica estão incluídas as métricas empregadas para avaliar a qualidade do software e do hardware. Estas métricas são usadas para descrever

e/ou comparar objetos técnicos. (exemplo: algoritmos, produtos ou modelos). Métricas organizacionais avaliam processos e programas de segurança. Métricas operacionais são utilizadas para avaliar sistemas e práticas operacionais em relação aos princípios de segurança.

Neste mesmo *Workshop* Deborah Bodeau do MITRE sugeriu uma caracterização interessante para métricas de segurança da informação. Ela apresentou uma abordagem para métricas de segurança de software que leva em consideração o tipo de objeto que será mensurado, o porquê da necessidade de medi-los, e para quem estamos medindo. Sua caracterização está representada na Figura 8 a seguir (Henning, 2001):

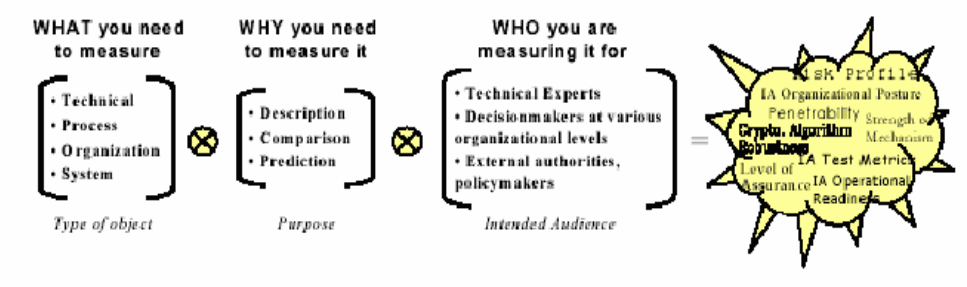

Figura 8: Caracterização de Métricas de Software (extraída de HENNING, 2001)

3.4 Critérios de Avaliação

Encontramos na literatura critérios qualitativos e quantitativos para a avaliação de um software em relação à segurança. Segundo Bayuk (2000), os modelos de avaliação de segurança se enquadram em uma das cinco categorias a seguir: Avaliação de segurança a partir de boas práticas do mercado (Auditoria externa), Avaliação de segurança a partir de práticas de segurança definidas internamente (Auditoria interna), Modelo de Maturidade da Capacitação, Análise de riscos e eliminação de defeitos.

3.4.1 Modelo de avaliação de segurança a partir de boas práticas do mercado (Auditoria externa)

O modelo de avaliação de segurança a partir de boas práticas do mercado (auditoria externa) assume que existem "melhores práticas" disponíveis sobre como proteger um determinado tipo de ambiente ou produto. Este modelo mede a segurança ao comparar o nível de controle gerencial sobre o ambiente do sistema. O resultado final é uma lista de fragilidades de segurança, ou defeitos, que devem ser corrigidos para que os sistemas operem em um nível aceitável de riscos de segurança. Enquadram-se neste tipo de avaliação o ITSEC, TCSEC, ISO 9000, ISO 17799, Common Criteria, COBIT, etc.

O marco inicial da avaliação de segurança ocorreu quando o governo norte-americano publicou a norma TCSEC – *Trusted Computing System Evaluation Criteria* (DOD, 85), também conhecido como *Orange Book*, para a avaliação de segurança de dispositivos de segurança (criptografia, *firewalls*, etc.). Com relação a software, o foco do TCSEC (DOD, 85) consistia na definição dos requisitos de segurança necessários para a garantia da confidencialidade das informações. Na época, o grande cliente comprador de segurança era o governo dos Estados Unidos e o sigilo de informações sensíveis era o grande requisito que deveria ser atendido.

Em 1991, uma comissão européia formada por França, Alemanha, Holanda e Reino Unido, publicou uma norma para certificação de segurança intitulada ITSEC – *Information Technology Security Evaluation Criteria* (ITSEC, 1991), baseada no TCSEC (DOD, 85), tornando-se depois de fato um padrão europeu voltado tanto para a avaliação de produtos como de sistemas. Diferente do TCSEC, o ITSEC separava funcionalidade de segurança de garantia de segurança.

Em 1992 o *National Institute of Standards and Technology* (NIST) publicou o *Minimum Security Functionality Requirements for Muiti-user Operating Systems* (MSFR, 1992) que tinha como objetivo apresentar um conjunto mínimo de requisitos funcionais de segurança para sistemas operacionais multi-usuário, especialmente aqueles relacionados com o a garantia da qualidade do processo de desenvolvimento dos fornecedores de software nos Estados Unidos. Estes

requisitos eram baseados no TCSEC e, futuramente, seriam parte do novo o novo *Federal Information Processing Standard* (FIPS), que substituiria o TCSEC (Orange Book).

Em 1993, o governo canadense juntou as normas TCSEC e ITSEC e criou o *Canadian Trusted Computer Product Evaluation Criteria* (CTCPEC,1993) com o mesmo objetivo.

Com tantas normas de certificação, as empresas multinacionais acabaram tendo problemas ao ter que certificar seus produtos perante cada órgão de governo, o que gerava enormes custos de certificação. Para resolver este problema, os países envolvidos na definição destas normas encaminhou para a ISO uma proposta de consolidação de todos estes critérios para avaliação de segurança em um único critério. A ISO acatou a idéia e posteriormente apresentou a Norma ISO 15.408:1999, dando-lhe o nome de *Common Criteria*. Os sete órgãos de governo responsáveis pelos critérios comuns (*The Common Criteria Project Sponsoring Organizations*) continuam proprietários do *Copyright*, porém cederam os direitos de uso para a ISO (figura 9).

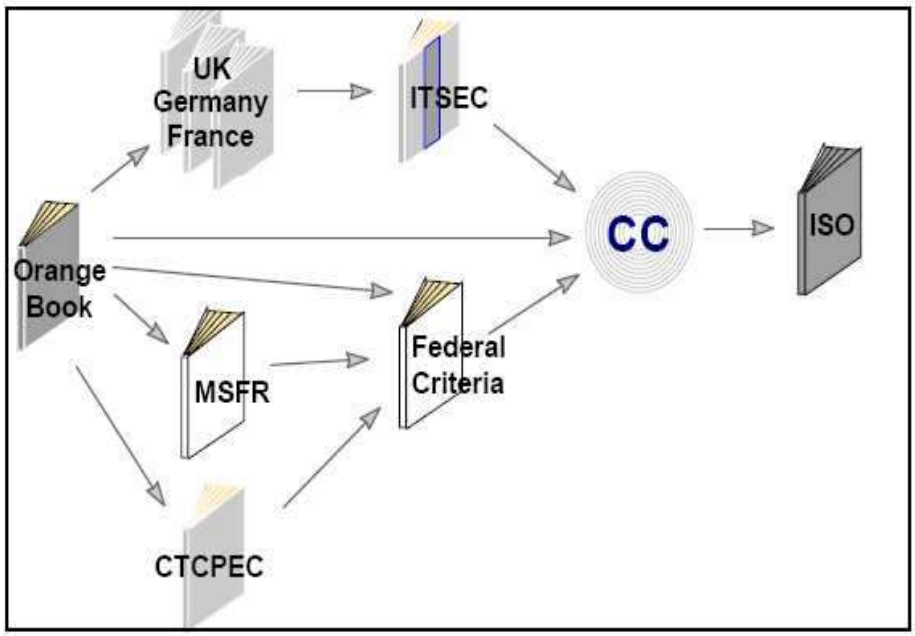

Figura 9: Histórico da Criação do *Common Criteria*. Figura extraída do artigo *"Computer Security Criteria: Security Evaluations and Assessment"* de 2001 da Oracle.

Assim como os padrões que lhe deram origem, o *Common Criteria* tem por objetivo ser a base para avaliação das propriedades de segurança dos sistemas de computação. O *Common Criteria* permite comparações entre produtos fornecendo um conjunto de requisitos de segurança e medidas de garantia de segurança aplicadas a eles durante a avaliação. Ao final da avaliação de dois produtos, é possível comparar as funções de segurança e os níveis de garantia de segurança fornecido por ambos, de forma a possibilitar a escolha do produto que mais se adequa às necessidades da organização. Logo, o mais importante é que a norma ISO 15408 define diferentes níveis de confiança e garantias na avaliação (do EAL0 ao EAL7). Ela é formada por um conjunto de três volumes, onde o primeiro discute definições e metodologia, o segundo lista um conjunto de requisitos de segurança e o terceiro descreve as metodologias de avaliação.

Diferentemente da ISO 17799, o *Common Criteria* é uma norma para definir e avaliar requisitos de segurança de sistemas e não de organizações, enquanto que a ISO 17799 é uma norma que aborda a segurança da informação da organização.

Todas essas normas são usadas para avaliações qualitativas de segurança.

3.4.2 Modelo de avaliação de segurança a partir de práticas de segurança definidas internamente (Auditoria interna)

O modelo de avaliação de segurança a partir de práticas de segurança definidas internamente (Auditoria interna) assume que a organização adota um conjunto de controles definidos internamente (política de segurança) com o intuíto de proteger os ativos de sistemas de informação. A avaliação fornecer então informações (medidas) que comprovam ou não a eficácia dos controles de segurança adotados. A comparação é realizada com auditorias de anos anteriores ou com ambientes de TI similares na organização. Esta é uma abordagem qualitativa de segurança.

3.4.3 Modelo de maturidade da capacitação

Este modelo, em uma abordagem qualitativa, assume que organizações devem se comprometem em proteger seus ambientes adotando formalmente um processo que garanta esta segurança. Conforme as práticas são estabelecidas e cumpridas, o nível de maturidade em segurança da organização aumenta. O SSE-CMM (*System Security Engineering Capability Maturity Model*) avalia um processo de gerenciamento de segurança, atribuindo um nível de maturidade (de 1 a 5), que representa o quão bem a organização cumpre todas as práticas.

3.4.4 Modelo de Análise de Riscos

Análise de riscos, em suas diferentes formas, pode ser considerado um modelo útil de medição de segurança. O modelo de análise de riscos mais empregado assume que existe um fator "valor monetário" que representa o quanto deverá custar para proteger um ativo. A partir da análise de riscos, calcula-se o quanto se gastar para que o risco não ocorra. O modelo assume que se nenhum dinheiro é gasto em segurança, nenhuma segurança será alcançada. Outras abordagens podem ser também usadas. (horas sem operação, reputação, etc).

3.4.5 Modelo de Eliminação de Defeitos

Esta é uma abordagem quantitativa de segurança.que assume a existência de um parâmetro mensurável, inerente ao ambiente de tecnologia da informação, que reflete o seu perfil de segurança. Quanto mais próximo do "zero defeitos", mais seguro o software. Por exemplo, no código contamos o número de bugs encontrados (ou corrigidos ao partir de uma versão para a próxima) e no nível de sistema contamos o número de vezes em que uma versão de um sistema é mencionada nos avisos do CERT®, *Computer Emergency Response Team*, nos boletins de segurança da Microsoft ou no Mitre (Common Vulnerabilities and Exposures - CVEs).