

CARLOS FREUD ALVES BATISTA

Métricas de Segurança de Software

DISSERTAÇÃO DE MESTRADO

DEPARTAMENTO DE INFORMÁTICA

Programa de Pós-Graduação em Informática

Rio de Janeiro

Abril de 2007



Carlos Freud Alves Batista

Métricas de Segurança de Software

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Informática do Departamento de Informática da PUC-Rio.

Orientador: Prof. Arndt von Staa

Rio de Janeiro

Abril de 2007



Carlos Freud Alves Batista

Métricas de Segurança de Software

Dissertação apresentada como requisito parcial para obtenção do grau de mestre pelo programa de pós-graduação em Informática do Departamento de Informática da PUC-Rio. Aprovada pela Comissão Examinadora abaixo assinada.

Prof. Arndt von Staa

Orientador

Departamento de Informática – PUC-Rio

Prof. Julio Cesar Sampaio do Prado Leite

Departamento de Informática – PUC-Rio

Profa. Karin Koogan Breitman

Departamento de Informática – PUC-Rio

Prof. José Eugenio Leal

Coordenador Setorial do Centro Técnico e Científico – PUC-Rio

Rio de Janeiro, 16 de abril de 2007

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do autor e do orientador.

Carlos Freud Alves Batista

Graduou-se em Bacharelado em Informática pela Universidade Federal do Rio de Janeiro em agosto de 1996. Atualmente é analista de sistemas da Tecnologia da Informação da Petróleo Brasileiro S/A (PETROBRAS). Sua área de concentração é a implantação e a melhoria de processos de desenvolvimento de software.

Ficha Catalográfica

Batista, Carlos Freud Alves

Métricas de segurança de software / Carlos Freud Alves Batista ; orientador: Arndt Von Staa. – 2007.

102 f. : il. ; 30 cm

Dissertação (Mestrado em Informática)–Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2007.

Inclui bibliografia

1. Informática – Teses. 2. Medição. 3. Métricas. 4. Segurança. 5. Segurança de software. I. Staa, Arndt Von. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Informática. III. Título.

CDD: 004

A Deus por tudo o que tem feito e por tudo que vai fazer. Por suas promessas e por tudo que É.

Este trabalho é dedicado a minha esposa Roseane e ao meu filho Davi Lucas que em todos os momentos me cercaram de amor, incentivo, compreensão e carinho.

Agradecimentos

Ao meu orientador, professor Arndt von Staa, pelo apoio, estímulo, paciência, parceria e tempo despendido neste trabalho. Sua orientação e comentários preciosos foram fundamentais para o desenvolvimento deste trabalho.

Aos professores Julio Cesar Sampaio do Prado Leite, Karin Koogan Breitman e Simone Diniz Junqueira Barbosa por participarem da Comissão Examinadora.

Aos meu pais, pela educação, atenção e carinho de todas as horas.

Aos amigos da Petrobras pelas valiosas colaborações para a realização deste trabalho.

A todos os irmãos da Comunidade Shamah pelos momentos de oração.

Resumo

Batista, Carlos Freud A.; Staa, Arndt v. . **Métricas de Segurança de Software**. Rio de Janeiro, 2007. 102p. Dissertação de Mestrado - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro

A dependência cada vez maior da tecnologia de informação (TI) torna software seguro um elemento chave para a continuidade dos serviços de nossa sociedade atual. Nos últimos anos, instituições públicas e privadas aumentaram seus investimentos em segurança da informação, mas a quantidade de ataques vem crescendo mais rapidamente do que a nossa capacidade de poder enfrentá-los, colocando em risco a propriedade intelectual, a relação de confiança de clientes e a operação de serviços e negócios apoiados pelos serviços de TI. Especialistas em segurança afirmam que atualmente boa parte dos incidentes de segurança da informação ocorrem a partir de vulnerabilidades encontradas no software, componente presente em boa parte dos sistemas de informação. Para tornar o software fidedigno em relação à segurança, a criação e o uso de métricas de segurança serão fundamentais para gerenciar e entender o impacto dos programas de segurança nas empresas. Porém, métricas de segurança são cobertas de mistério e consideradas bastante difíceis de serem implementadas. Este trabalho pretende mostrar que hoje ainda não é possível termos métricas quantitativas capazes de indicar o nível de segurança que o software em desenvolvimento virá a ter. Necessitam-se, então, outras práticas para assegurar níveis de segurança a priori, ou seja, antes de se por o software em uso.

Palavras-chave

Medição, métricas, segurança, segurança de software

Abstract

Batista, Carlos Freud A.; Staa, Arndt v. (Advisor). **Software Security Metrics**. Rio de Janeiro, 2007. 102p. MSc. Dissertation - Departamento de Informática, Pontifícia Universidade Católica do Rio de Janeiro

Today's growing dependency on information technology (IT) makes software security a key element of IT services. In recent years public and private institutions raised the investment on information security, however the number of attacks is growing faster than our power to face them, putting at risk intellectual property, customer's confidence and businesses that rely on IT services. Experts say that most information security incidents occur due to the vulnerabilities that exist in software systems in first place. Security metrics are essential to assess software dependability with respect to security, and also to understand and manage impacts of security initiatives in organizations. However, security metrics are shrouded in mystery and very hard to implement. This work intends to show that there are no adequate metrics capable of indicating the security level that a software will achieve. Hence, we need other practices to assess the security of software while developing it and before deploying it.

Keywords

Measurement, metrics, security, software security

Sumário

1 INTRODUÇÃO	15
1.1 Motivação.....	16
1.2 Proposta.....	17
1.3 Discussão e contribuições esperadas	18
1.4 Organização deste trabalho	19
2 CONCEITOS E PROPRIEDADES DESEJÁVEIS PARA UM SOFTWARE SEGURO	20
2.1 Definindo Segurança.....	20
2.2 Propriedades desejáveis para um software seguro.....	21
2.3 Relacionamento entre Fidedignidade e Segurança.....	24
2.4 Terminologias associadas com segurança e seus relacionamentos..	26
2.5 Relações entre Segurança da Informação, Segurança de Sistemas de Informação, Segurança de Software	29
2.6 O que queremos em relação ao desempenho do software quanto à questão da segurança?	33
3 MÉTRICAS DE SEGURANÇA DE SOFTWARE	36
3.1 Medição de Software.....	36
3.2 Métricas de Segurança de Software	38
3.3 Classificações de Métricas de Segurança encontradas na Literatura	40
3.4 Critérios de Avaliação.....	41
3.4.1 Modelo de avaliação de segurança a partir de boas práticas do mercado (Auditoria externa)	42

3.4.2 Modelo de avaliação de segurança a partir de práticas de segurança definidas internamente (Auditoria interna)	44
3.4.3 Modelo de maturidade da capacitação.....	45
3.4.4 Modelo de Análise de Riscos	45
3.4.5 Modelo de Eliminação de Defeitos	45
4 AVALIAÇÃO QUANTITATIVA DE SEGURANÇA DE SISTEMAS.....	46
4.1 Esforço despendido por um atacante	46
4.2 O Índice de Vulnerabilidade do Sistema.....	48
4.3 MTTI – Minimum-Time-To-Intrusion	51
4.4 Avaliação Quantitativa para Monitorar a Segurança Operacional	56
4.5 Método Wang e Wulf para Medir Segurança.....	63
4.6 Redução da Superfície de Ataque.....	74
4.7 Proposta de um Framework para medir a segurança de um software.....	78
4.8 Análise dos Métodos Apresentados	81
5 DIFICULDADES NA GERAÇÃO DE MÉTRICAS DE SEGURANÇA QUANTITATIVAS	83
5.1 Evolução de Nossa Capacidade de Tratar a Insegurança	85
5.2 Dificuldades que encontramos na busca por métricas quantitativas de segurança.....	87
5.2.1 Outros campos têm números para expressar. Qual é a equivalência para segurança do software?	87
5.2.2 Composição pode Introduzir Falhas.....	88
5.2.3 Pessoas e processos podem diminuir a segurança	88
5.2.4 Falta de embasamento teórico	89
5.2.5 O aspecto tempo	90
5.2.6 Valores Lógicos Tradicionais.....	90
5.2.7 Terminologia de segurança.....	90

5.2.8 As facilidades e recursos hoje disponíveis	90
5.2.9 Dificuldades dos Sistemas de Detecção de Invasão	91
5.2.10 A garantia da segurança após a evolução do software	91
5.2.11 A complexidade de verificar segurança em grandes sistemas	91
5.2.12 A limitação de métodos baseados em contagem de Bugs de segurança.....	92
5.2.13 Outras propriedades desejáveis podem afetar a segurança como um todo.....	92
5.2.14 Nem sempre podemos só considerar uma análise quantitativa	92
5.3 Recomendações para a Avaliação de Segurança.....	93
6 CONCLUSÕES E TRABALHOS FUTUROS	95
6.1 Trabalhos Futuros	96
7 REFERÊNCIAS BIBLIOGRÁFICAS	97

Lista de Figuras

Figura 1: Segurança em seu conceito mais tradicional.....	23
Figura 2: Relacionamento de Fidedignidade e Segurança (extraída de Avizienis et al., 2004)	24
Figura 3: Conceitos relacionados à segurança e seus relacionamentos. (extraída do Common Criteria , 2002)	26
Figura 4: Ameaça e vulnerabilidade (extraída de Pfleeger, 2003).....	29
Figura 5: Sistemas de Informação.....	30
Figura 6: Diferentes dimensões de segurança do sistema (extraída de Goertzel et al., 2006).....	31
Figura 7: Classificação das métricas de software encontradas em HENNING(2001)	40
Figura 8: Caracterização de Métricas de Software (extraída de HENNING, 2001).....	41
Figura 9: Histórico da Criação do <i>Common Criteria</i> . Figura extraída do artigo “ <i>Computer Security Criteria: Security Evaluations and Assessment</i> ” de 2001 da Oracle.	43
Figura 10: Visão Geral do protótipo AVA (extraída de Voas et al., 1996)	54
Figura 11: Métrica MTTI. M é o número de localizações aonde o AVA foi aplicado (extraída de .Voas et al., 1996)	55
Figura 12: Métrica MinTTI (extraída de .Voas et al., 1996)	55
Figura 13: X obtém os privilégios do nó Y	57
Figura 14: Grafo de Privilégios (extraída de Ortalo et al., 1999)	58
Figura 15: O Atacante e o caminho até o alvo.	60
Figura 16: Derivação das <i>Attack state graphs</i> a partir do Grafo de Privilégios. Figura baseada no artigo de Ortalo e co-autores (Ortalo et al., 1999)..	61
Figura 17: Exemplo de decomposição. Figura extraída do artigo “ <i>A Framework for Security Measurement</i> ” de Wang e Wulf (1997)	65

Figura 18: Exemplo da Porta (extraída do artigo “A Framework for Security Measurement” de Wang e Wulf (1997))	67
Figura 19: Funcionamento da janela em relação aos seus fatores (extraída do artigo “A Framework for Security Measurement” de Wang e Wulf (1997))	69
Figura 20: Árvore de Decomposição para uma Casa (Extraída do artigo “A Framework for Security Measurement” de Wang e Wulf (1997)).....	71
Figura 21: Hype Cycle for Cyberthreats, (extraída de Williams et al, 2006)	86

Lista de Tabelas

Tabela 1: Impacto Financeiro de Ataques de Vírus - Fonte Computer Economics, (McManus, 2006).	16
Tabela 2: Indexes de Sensitividade (S.I.s) dos componentes básicos da casa (extraída do artigo “A Framework for Security Measurement” de Wang e Wulf (1997)).	72

Lista de Abreviaturas

AVA - Análise de Vulnerabilidade Adaptativa
CC - Common Criteria
CERT - Computer Emergency Response Team
COBIT - Control Objectives for Information and Related Technologies
CTCPEC - Canadian Trusted Computer Product Evaluation Criteria
CVE - Common Vulnerabilities and Exposures
DOD - Department of Defense
EAL - Evaluation Assurance Level
EPA - Extended Propagation Analysis
FIPS - Federal Information Processing Standard
IDS - Intrusion Detect System
ISO - International Standards Organization
ITSEC – Information Technology Security Evaluation Criteria
IVS - Índice de Vulnerabilidade do Sistema
METB - Mean Effort to Breach
METF - Mean Effort to Security Failure
MITRE - Massachusetts Institute of Technology
MTTF - Mean Time to Failure
MSFR - Minimum Security Functionality Requirements
ML - Memory Less
MTTI – Minimum-Time-To-Intrusion
NIST - National Institute of Standards and Technology
NW - Normalized Weight
PS - Prioritized Siblings
SDLC - System Development Life Cycle
SI - Sensitivity Index
SP - Short Path
SSE-CMM - System Security Engineering Capability Maturity Model
TCSEC – Trusted Computing System Evaluation Criteria
TI - Tecnologia da Informação
TM - Total Memory
WL - Weakest Link
WWL - Weighted Weakest Link