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 CentroTécnico e Científico – PUC-Rio

Rio de Janeiro, 16 de abril de 2007

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

Lista de Figuras

Lista de Tabelas

Lista de Abreviaturas

AVA - Análise de Vulnerabilidade Adaptativa
CC - Common Criteria
CERT - Computer Emergency Response Team
COBIT - Control Objectives for Information and Related Tecnologies
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