S-Process: Um Processo para Desenvolvimento de Aplicações Seguras

Ryan Ribeiro de Azevedo[1], Silas Cardoso de Almeida[1], Eric Rommel Galvão Dantas[1], Wendell Campos Veras [1], Daniel Abella[1], Rodrigo G. C. Rocha[1]

[1]Centro de Informática – Universidade Federal de Pernambuco (CIn-UFPE)
Caixa Postal 50.740 – 540 – Recife – PE – Brasil

{rra2,ergd,wcv,rgcr}@cin.ufpe.br, {silas.sca, abellad}@gmail.com

1. Introdução

Existem diversos aspectos de segurança que uma aplicação deve satisfazer, sendo três destes aspectos considerados centrais ou principais segundo [NBR ISO/IEC 27002 2005]: Confidencialidade, Integridade e Disponibilidade. Pode-se ainda adicionar a esses aspectos centrais conceitos básicos quanto a usuários, tais como: Autenticação, Autorização, Controle de Acesso e Não-Repúdio.

Grande parte dos desenvolvedores não estão prontos para produzirem aplicações seguras devido à falta de práticas e processos de Engenharia de Software adequados nas corporações. As empresas ainda estão preocupadas com *firewalls* e *Intrusion Detect Systems*. Para desenvolver aplicações seguras e de boa qualidade, os processos de desenvolvimento devem considerar aspectos de segurança em todas as suas etapas, ao invés de considerarem a segurança apenas durante a fase de desenvolvimento, obtendo assim, resultados com qualidade reproduzível. Estudos publicados pelo NIST (http://www.nist.gov/index.html) indicam que 75% dos ataques *Web* ocorrem ao nível das aplicações, indicam que 92% das vulnerabilidades estão em aplicações.

O processo proposto neste artigo visa garantir que os aspectos mencionados acima sejam considerados. Seu objetivo é auxiliar os responsáveis no gerenciamento e desenvolvimento de aplicações onde segurança é um fator crítico, a exemplo de aplicações financeiras e *e-commerce*. Tem por maior finalidade auxiliar times de desenvolvimento a desenvolverem aplicações seguras com alta qualidade e entregues no prazo especificado. Assim temos o S-Process, um processo de desenvolvimento de aplicações seguras, simplificado e apoiado em práticas de metodologias como XP, RUP e *Agile Modeling*. As demais seções deste artigo estão estruturadas da seguinte forma: a Seção 2 foca na proposta em desenvolvimento e resultados parciais. Por fim, na Seção 3 apresentam-se as considerações finais e trabalhos futuros.

2. S-Process

O S-Process é dividido em sete fases e em *deliverables*, com objetivos e etapas bem definidos. O fluxo básico com as fases do processo proposto é apresentado na Figura 1. A primeira fase do processo consiste na **Definição de Papéis-S**. Assim como o XP (http://www.xprogramming.com/), o S-Process relaciona papéis com responsabilidades explícitas a serem desempenhadas por cada um dos participantes em um projeto, atividade esta, realizada na primeira fase do processo proposto.

A segunda fase do processo, **Levantamento de Requisitos-S**, consiste em criar um relatório inicial de investigação para construir o *business case*, extrair requisitos funcionais e não-funcionais de segurança a partir de políticas de segurança, SLAs – (Acordos de Nível de Serviço), leis como *Sarbanes-Oxley* (SOX http://www.soxlaw.com) aplicadas na corporação e *user stories* definidas pelo cliente. Na terceira fase, **Análise de Riscos-S**, identifica-se todas as ameaças de segurança, a exemplo de problemas técnicos, naturais e de ação humana. Para cada ameaça são identificados sua probabilidade de ocorrência, seu impacto no negócio e o custo para mitigar o risco. A fase **Análise-S** consiste em prover realismo ao mundo ideal de requisitos, determinando a viabilidade de projetar e implementar a aplicação atendendo ao conjunto de requisitos levantados na segunda fase.

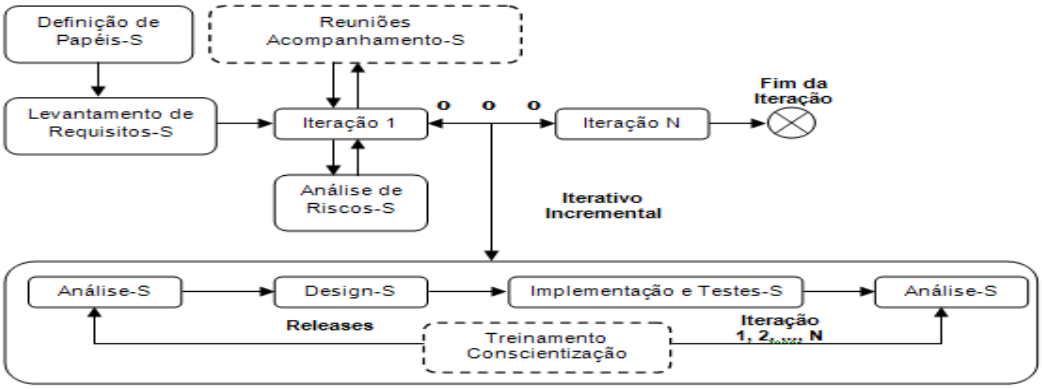

Figura 1. Fluxo e fases do S-Process.

A fase **Design-S** consiste em formular o *design* de componentes de segurança necessários para satisfazer os requisitos, definir ambientes para um desenvolvimento seguro, desenvolver a forma e tipos de testes. Na fase **Implementação e Testes-S,** é iniciada a escrita do código. É fundamental construir uma infra-estrutura que possibilite o desenvolvimento seguro e a manutenção da integridade do código em ambiente pré-piloto. Para a fase **Implantação-S** (*Deployment*) deve-se migrar a aplicação do ambiente de desenvolvimento para o ambiente de produção, atribuindo responsabilidades aos *migration owners*. Nesta fase, ainda, deve-se limpar ambientes obsoletos de informação de segurança sensível e deixar ambientes de produção seguros.

3. Conclusões e Trabalhos Futuros

Este artigo apresentou de forma sucinta um processo para desenvolvimento de aplicações seguras baseado em uma sequência de etapas selecionadas e definidas, auxiliando assim os responsáveis por manter a segurança das aplicações e desenvolvedores em ambientes computacionais onde se requer alto grau de segurança. Atualmente o S-Process encontra-se em validação por uma equipe de desenvolvimento de software em um determinado projeto.

Referências

NBR ISO/IEC 27002, 2005 “Código de Prática para a Gestão da Segurança da Informação” ABNT.