



Universidade de Fortaleza (UNIFOR)



VIII SIMPROS

Processo de Apoio à Segurança de Software (PASS):

Uma Experiência Prática

Autor: Francisco José Barreto Nunes

Orientador: Arnaldo Dias Belchior

São Paulo - SP, 05 de dezembro de 2007

Agenda

- ◆ Introdução
- ◆ Referencial Teórico
- ◆ Pesquisa de Campo
- ◆ Processo de Apoio à Segurança de Software (PASS)
- ◆ Aplicação do Processo de Apoio (Estudo de caso)
- ◆ Conclusão

Introdução

◆ **Motivação**

- ◆ A Engenharia de Software atual, os modelos de maturidade, e as normas internacionais de processos de desenvolvimento de software ainda não enfatizam a capacidade dos sistemas de resistir a ataques, mantendo a segurança das informações manipuladas.
- ◆ A crescente complexidade e interconectividade dos sistemas, além da exigência do mercado na entrega rápida de soluções de software contribuem para um número cada vez maior de sistemas com falhas de segurança.
- ◆ Apesar da crescente importância da segurança de software, os processos de desenvolvimento são estruturados sem considerá-la.

3

Introdução

◆ **Objetivos gerais**

- ◆ Prover mais visibilidade para a segurança de software em um processo de desenvolvimento de software.
- ◆ Tratar sistematicamente vulnerabilidades, ameaças, impactos e riscos relacionados à segurança do produto de software.
- ◆ Possibilitar que ações de segurança estejam alinhadas aos objetivos estratégicos especificados para a organização.

4

Introdução

◆ Objetivos específicos

- ◆ Identificar, entre práticas, normas e modelos de segurança, atividades semelhantes que pudessem ser utilizadas para aumentar a segurança de software.
- ◆ Avaliar a abordagem de segurança de software na literatura de engenharia de software e na literatura de segurança da informação.
- ◆ Propor um processo de apoio à segurança de software que possa ser utilizado em conjunto com outros processos de software para confecção de software seguro, suprimindo algumas deficiências da segurança de software identificadas na literatura.
- ◆ Experimentar o processo de apoio proposto, relatando os resultados.

5

Introdução

◆ Restrições

- ◆ A organização onde foi realizado o estudo de caso desconhecia qualquer tipo de assunto relacionado à segurança de software.
- ◆ O estudo foi realizado com um conjunto mínimo de atividades de segurança seguindo o resultado da pesquisa de campo.
- ◆ O estudo não tratou da questão das métricas de segurança.

6

Referencial Teórico

- ◆ O Processo de Apoio à Segurança de Software proposto foi baseado nos seguintes modelos e normas de segurança:
 - ◆ SSE-CMM (System Security Engineering – Capability Maturity Model)
 - ◆ OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
 - ◆ ISO/IEC 15408 Information Technology – Security Techniques – Evaluation Criteria for IT Security
 - ◆ Part 1: Introduction and General Model
 - ◆ Part 2: Security Functional Requirements
 - ◆ Part 3: Security Assurance Requirements
 - ◆ ISO/IEC 27002 Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação

7

Referencial Teórico

SSE-CMM

- ◆ Uma ferramenta para avaliar as práticas da engenharia da segurança e definir melhorias.
- ◆ Um método pelo qual organizações possam ser avaliadas, estabelecendo a confiança na capacidade da organização, garantindo um sistema seguro.
- ◆ Um mecanismo padrão para clientes avaliarem a capacidade da engenharia de segurança de um fornecedor.

OCTAVE

- ◆ Técnica auto-orientativa de avaliação de riscos.
- ◆ Ativos, ameaças, vulnerabilidades, e impacto organizacional são analisados, permitindo a organização ajustar a estratégia de proteção de seus riscos de segurança.

8

Referencial Teórico

ISO/IEC 15408

- ◆ O desenvolvimento seguro de *software* envolve segurança no ambiente de desenvolvimento e segurança da aplicação desenvolvida (definição de requisitos e controles de segurança).

ISO/IEC 27002

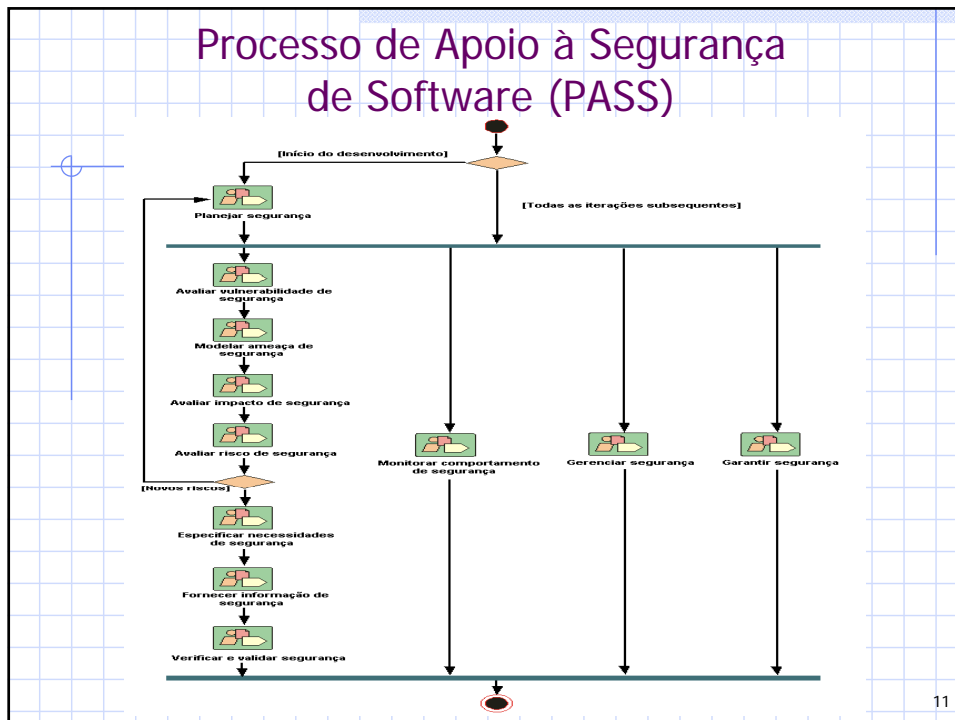
- ◆ Objetiva preservar a confidencialidade, integridade e disponibilidade das informações.
- ◆ Propõe um conjunto de controles a serem implementados. Esses controles garantem que objetivos estabelecidos para a segurança serão satisfeitos.

9

Pesquisa de Campo

- ◆ Avaliou a importância de 40 atividades de segurança no processo de software.
- ◆ Avaliou a relevância de 24 aspectos com capacidade de influenciar a utilização de um processo seguro.
- ◆ 42 especialistas participaram:
 - ◆ 31 especialistas em processo de desenvolvimento.
 - ◆ 24 especialistas em segurança da informação.

10



Processo de Apoio à Segurança de Software (PASS)

◆ Papéis e responsabilidades

◆ *Engenheiro de Segurança:*

- ◆ Especializa e instancia o processo de apoio para os objetivos do projeto, alinhado com metas e planos da organização, e monitora se os projetos satisfazem os objetivos de segurança.

◆ *Auditor de Segurança:*

- ◆ Avalia a aderência do processo de apoio nos projetos de software, em termos de resultados das atividades, dos artefatos produzidos, verificando a conformidade das ações dos projetos ao processo estabelecido.

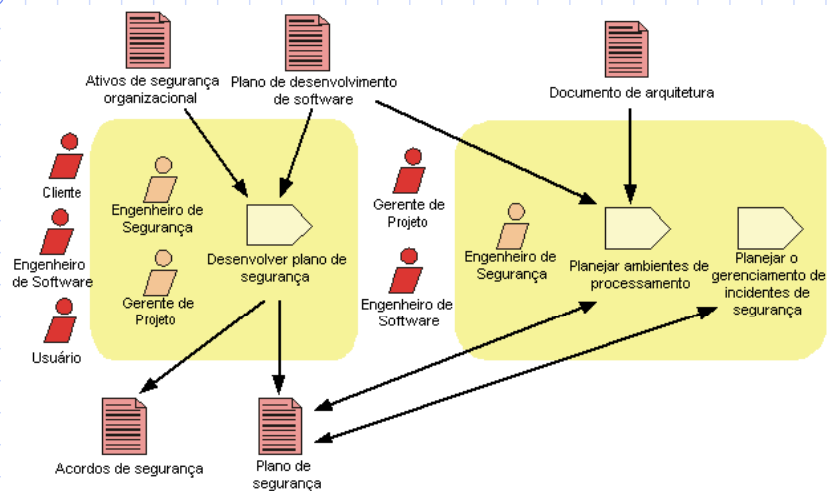
Processo de Apoio à Segurança de Software (PASS)

◆ Características

- ◆ Adequa-se ao ciclo de vida iterativo incremental, e seus subprocessos são compostos por um conjunto de atividades.
- ◆ Cada atividade é descrita em termos de propósito, tarefas, artefatos de entrada, artefatos de saída, e atores envolvidos.
- ◆ É possível utilizar apenas um subconjunto dos subprocessos e ou atividades propostos, adaptá-los e ou incluir novas atividades específicas (Especializar o processo).
- ◆ A partir do processo de apoio especializado para a organização, poderá haver então instanciação desse processo para a execução dos projetos de software.

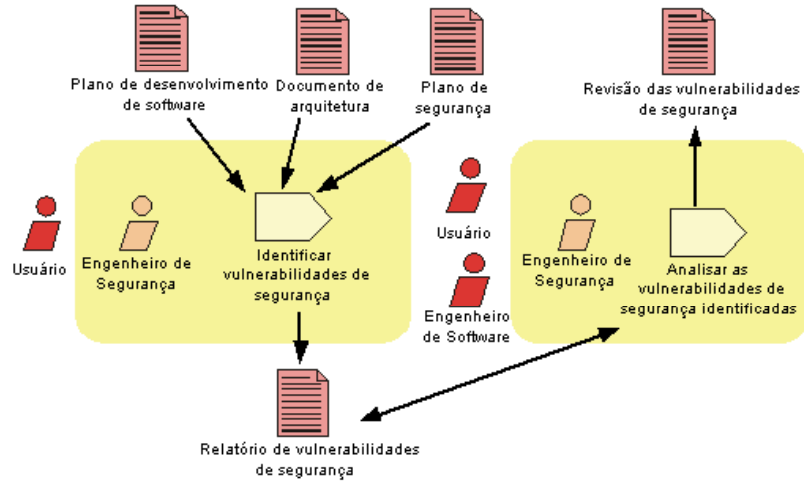
13

Subprocesso Planejar Segurança



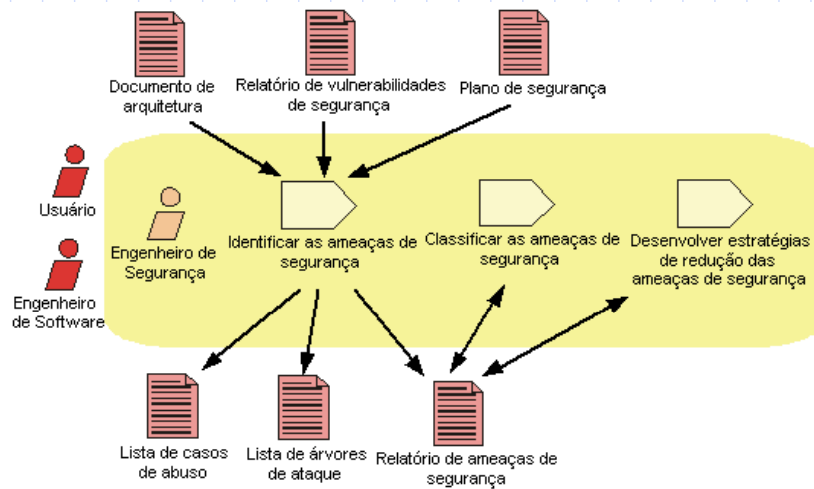
14

Subprocesso Avaliar Vulnerabilidade de Segurança



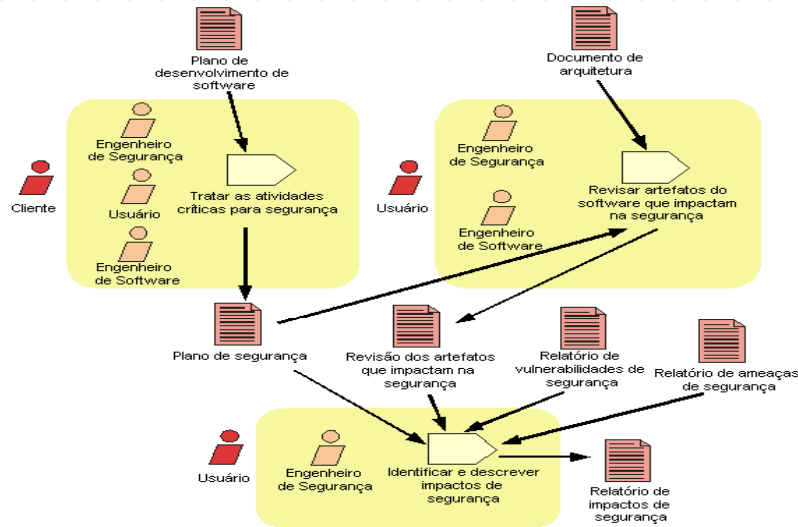
15

Subprocesso Modelar Ameaça de Segurança



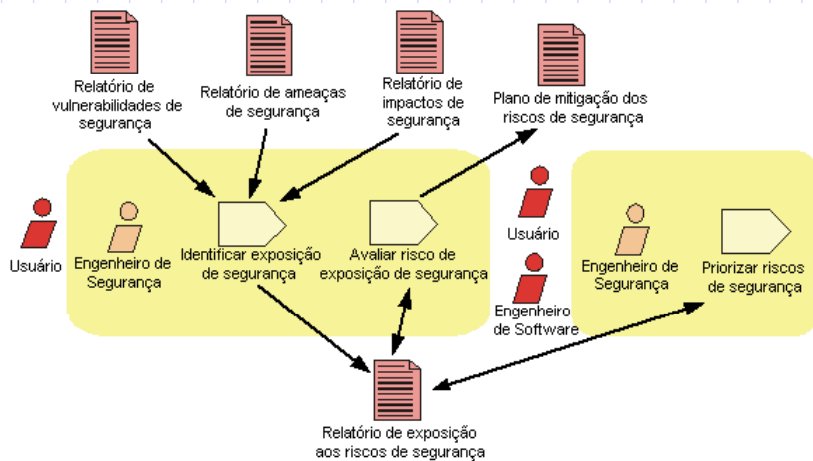
16

Subprocesso Avaliar Impacto de Segurança



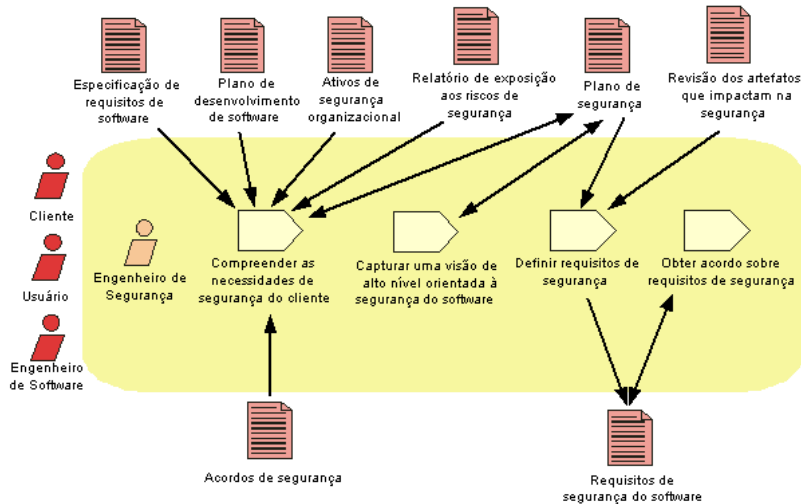
17

Subprocesso Avaliar Risco de Segurança



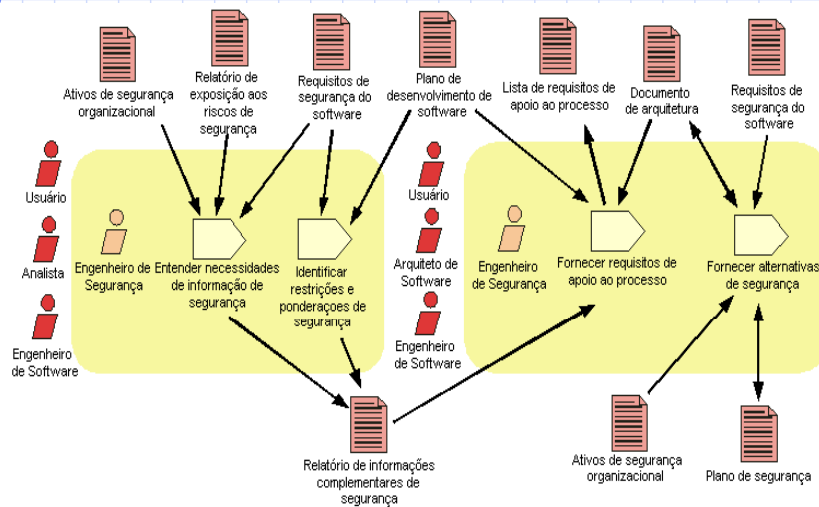
18

Subprocesso Especificar Necessidades de Segurança



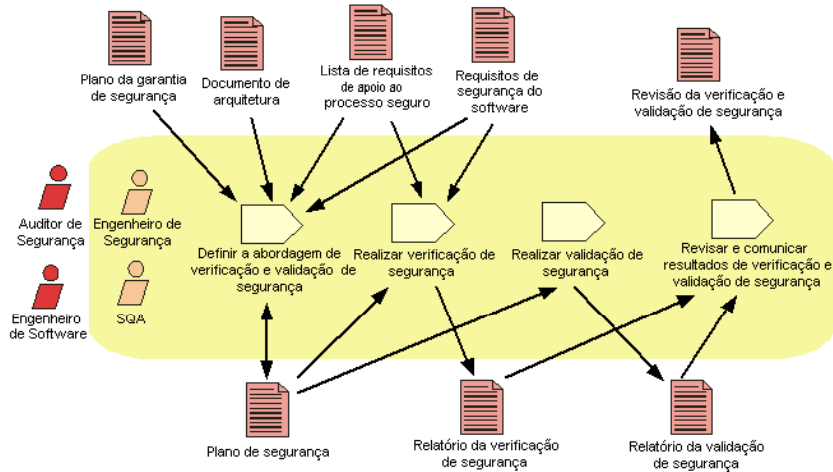
19

Subprocesso Fornecer Informação de Segurança



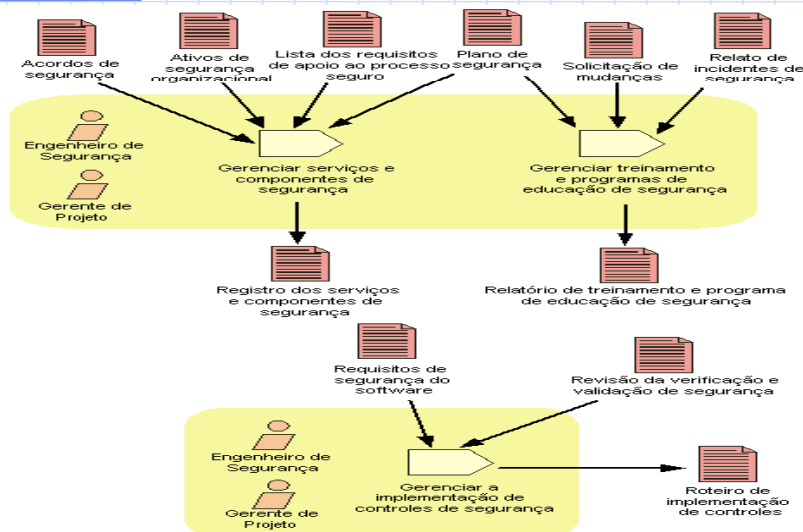
20

Subprocesso Verificar e Validar Segurança



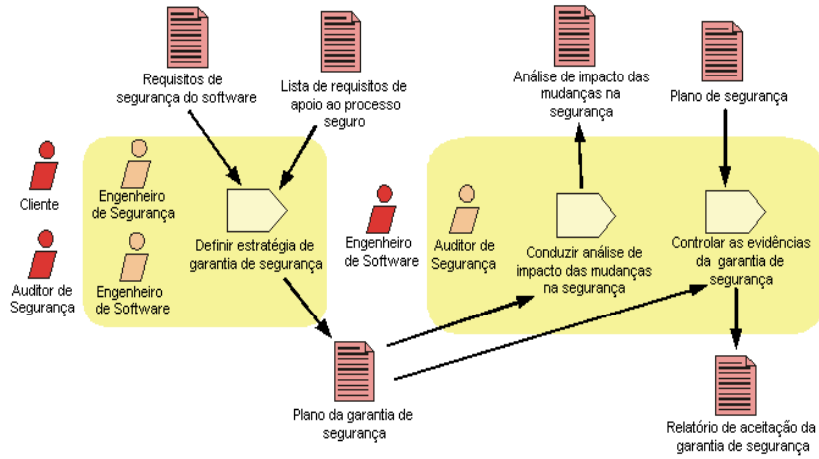
21

Subprocesso Gerenciar Segurança



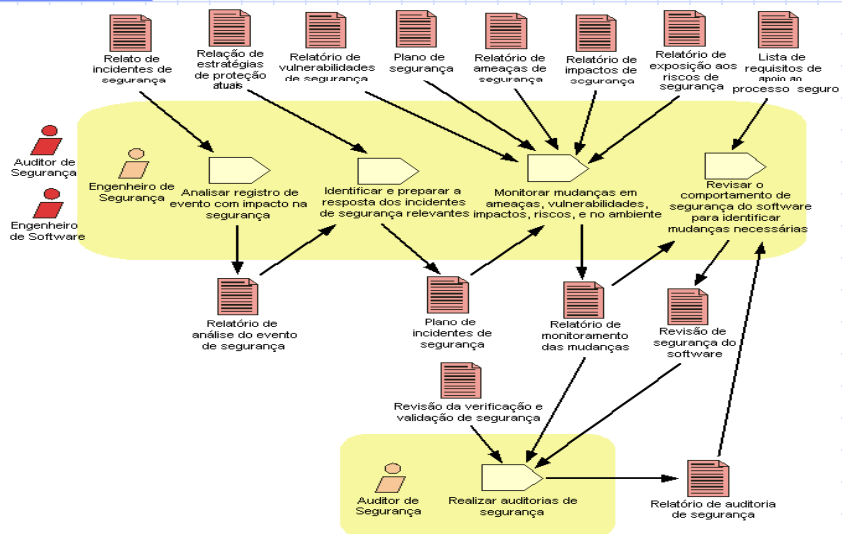
22

Subprocesso Garantir Segurança



23

Subprocesso Monitorar Comportamento de Segurança



24

Aplicação do Processo de Apoio

- ◆ Método de pesquisa
 - ◆ Buscou-se aplicar o processo de apoio em projeto de sistema considerado crítico.
 - ◆ A criticidade é em relação ao impacto negativo que um incidente de segurança causaria à organização.
 - ◆ Buscou-se avaliar como a proposta se aplicava no projeto.
 - ◆ Método de coleta de dados
 - ◆ Análise da documentação do projeto do sistema.
 - ◆ Entrevistas não estruturadas com membros da equipe.
 - ◆ Observação direta.

25

Aplicação do Processo de Apoio

- ◆ Características da organização
 - ◆ Administração pública.
 - ◆ Tecnologia como atividade meio.
 - ◆ 30 profissionais de desenvolvimento (Plataforma J2EE).
 - ◆ Metodologia baseada no PMBOK e RUP.
- ◆ Características do projeto
 - ◆ Novo sistema web de auditoria e segurança:
 - ◆ Controla acesso aos demais sistemas da organização através de perfis no qual o usuário se enquadra.
 - ◆ Estabelece padrões para a criação, alteração e manutenção das senhas.
 - ◆ Permite configuração de dados para auditoria.
 - ◆ 4 semanas.
 - ◆ 3 membros da equipe de projeto, sendo 2 dedicados.

26

Aplicação do Processo de Apoio

- ◆ Aplicaram-se apenas as atividades melhor avaliadas na pesquisa de campo.
- ◆ Procurou-se identificar as necessidades de segurança desejadas com o sistema de auditoria e controle de acesso.
- ◆ Foi avaliada conjuntamente a aplicabilidade e o impacto do PASS nas atividades da metodologia de desenvolvimento de software da organização.

27

Aplicação do Processo de Apoio

- ◆ Peculiaridades importantes na especialização do PASS
 - ◆ Atividades propostas no processo de apoio precisaram ser ajustadas.
 - ◆ É importante existir uma prática direcionada para a identificação dos ativos de informação do software.
 - ◆ Não havia uma base de conhecimento/histórica de erros e problemas nos sistemas da organização que permitisse identificar com maior brevidade possíveis vulnerabilidades e ameaças de segurança.
 - ◆ Maior tempo para realizar avaliação de vulnerabilidades e a modelagem das ameaças devido à inexperiência da equipe.
 - ◆ Necessidades de treinamento, incluindo curso de programação segura em Java.

28

Aplicação do Processo de Apoio

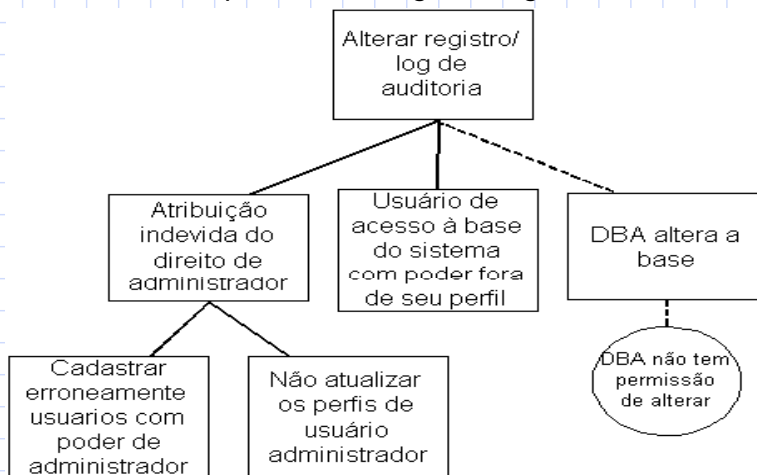
◆ Exemplo de vulnerabilidades de segurança identificadas:

Vulnerabilidade	Descrição	Criticidade
01. Falha na operação de cadastro dos usuários dos sistemas	A ineficiência no controle para cadastrar os usuários dos sistemas pode ocasionar atribuições incorretas de poder	Médio
02. Falha na operação de cadastro de ações	A ineficiência no controle para cadastrar as ações dos usuários dos sistemas pode ocasionar atribuições incorretas de direito sobre os sistemas	Médio
03. Falha no processo de autenticação	A utilização de critérios de autenticação ineficientes pode causar acessos indevidos e roubo de informações. Aconselha-se usar mecanismos de autenticação padrões de mercado para sistema/funções mais críticos	Alta
04. Falha na função de validação da senha	Permitir que usuários criem senhas de fácil descoberta comprometerá a segurança do acesso aos sistemas	Alta

29

Aplicação do Processo de Apoio

◆ Árvore de ataque "Alterar registro/log de auditoria":



30

Aplicação do Processo de Apoio

◆ Requisitos de segurança acordados:

Identificação	Descrição
RSS.01	Impedir criação de senhas inseguras
Toda e qualquer criação ou alteração de senha, seja realizada pelo sistema ou pelo usuário, deve seguir, no mínimo, as regras que estabelecem a norma interna de elaboração de senhas. Sempre e quando o usuário compor senhas que não respeitem tais regras, o sistema não permitirá sua criação, solicitando ao usuário a elaboração de outra senha. A criação só será efetivada quando respeitar as regras impostas.	
RSS.02	Impedir acesso indevido ao sistema
Os acessos do sistema devem ser seguros com autenticação e validação de perfil a fim de evitar: (i) Envio incorreto da senha inicial gerada pelo sistema, (ii) Pessoas estranhas acessem algum sistema se passando por usuários válidos, (iii) Roubo, alteração ou qualquer outra ação que comprometa as informações dos usuários, (iv) O usuário do sistema acessa outras informações além daquelas atribuídas ao seu grupo, (v) Cadastro de informações incorretas. Revisões periódicas dos usuários e seus grupos/perfis poderiam reduzir acessos indevidos.	
RSS.03	Impedir alteração nos registros de auditoria
Os registros (log) das ações realizadas pelos usuários e pelo administrador do sistema serão armazenados para consulta e estes registros não devem ser alterados ou apagados por estes usuários ou pelo administrador.	

31

Aplicação do Processo de Apoio

- ◆ Os requisitos de segurança identificados no projeto piloto foram organizados segundo as necessidades de segurança e com apoio de árvores de ataque
- ◆ Após a atividade "Obter acordos sobre requisitos de segurança" relativa aos requisitos de segurança identificados, foram realizadas verificações e validações de segurança.
- ◆ Apenas um número pequeno de testes de segurança foi conduzido em obediência às restrições de prazo para o projeto.
- ◆ Após realização das verificações e validações de segurança, a implantação do PASS foi dada por concluída.

32

Aplicação do Processo de Apoio

- ◆ Principais problemas na condução desse processo
 - ◆ Dificuldades de entendimento e assimilação do processo de apoio. Isto demandou um maior tempo para a execução do projeto piloto.
 - ◆ Obstáculos para organizar e alinhar as atividades do processo de apoio com as atividades da metodologia de desenvolvimento de sistemas da organização.
 - ◆ Necessidade de recursos adicionais para o processo de apoio e de ajustes, como forma de garantir a eficácia de sua aplicação.

33

Como implantar segurança de software?

- ◆ Sugestões:
 - ◆ Formalizar conjunto mínimo de requisitos de segurança.
 - ◆ Preparar programa de conscientização (níveis estratégico, tático e operacional).
 - ◆ Selecionar ação segundo as estratégias e necessidades do negócio:
 - ◆ Normalmente, inicia-se com práticas de programação segura.
 - ◆ Testes de segurança e análise estática de código.
 - ◆ Análise de riscos.
 - ◆ Para cada ação, fazer projeto piloto e homologar.

34

Conclusão

◆ Contribuições

- ◆ Demonstração que a segurança de um software deve ser projetada e incorporada às soluções desde o início de seu desenvolvimento.
- ◆ Estruturação de um processo, constituído de atividades de segurança, para desenvolver software mais seguro, dentro de um contexto de ciclo de vida iterativo/incremental.
- ◆ Alinhamento com os requisitos da ISO/IEC 15408, ISO/IEC 27002, OCTAVE e do SSE-CMM.

35

Conclusão

◆ Contribuições

- ◆ Auxiliou equipe de projeto a visualizar e corrigir problemas de segurança ocorridos ao longo do processo de desenvolvimento.
- ◆ Proposição de artefatos de apoio à execução do Processo de Apoio à Segurança de Software.
- ◆ Evidenciou a existência de uma barreira cultural a ser quebrada para utilizar práticas de segurança de software no ciclo de vida de desenvolvimento.

36

Conclusão

◆ Considerações adicionais

- ◆ Ainda não há padrões de segurança largamente aceitos para o processo de desenvolvimento de software.
- ◆ A utilização do PASS pode implicar inicialmente na adição de mais recursos e investimentos, que podem variar conforme o projeto.
- ◆ Contudo, essa adição de recursos poderá vir a resultar em produtos mais confiáveis e seguros, que busquem garantir integridade, disponibilidade e confidencialidade das informações e, por conseguinte, clientes mais satisfeitos.
- ◆ A aplicação de técnicas e métodos de segurança de software não garante a prevenção de um software sem erro.

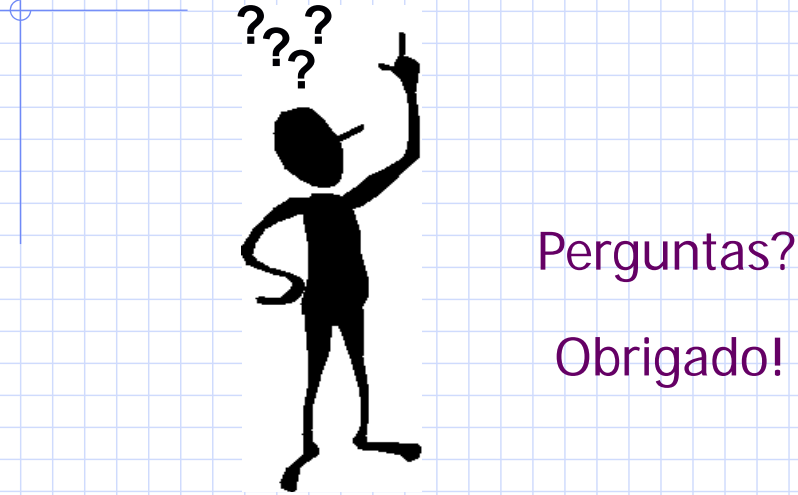
37

Conclusão

◆ Trabalhos futuros

- ◆ Aplicar o PASS em sua completude em outro projeto de desenvolvimento de sistemas.
- ◆ Agregar ao processo proposto padrões de segurança (security patterns).
- ◆ Melhorar as atividades relacionadas com a identificação das necessidades de segurança e com a definição de requisitos, propostas nesse trabalho, através da aplicação dos estudos com o UMLSec.
- ◆ Elaborar um conjunto consistente de métricas de segurança para medir o progresso e eficácia do processo, e a adequação do sistema aos requisitos de segurança.

38



Perguntas?
Obrigado!

39



Universidade de Fortaleza (UNIFOR)



VIII SIMPROS

**Processo de Apoio à Segurança de Software (PASS):
Uma Experiência Prática**

Autor: Francisco José Barreto Nunes
Orientador: Arnaldo Dias Belchior

São Paulo - SP, 05 de dezembro de 2007

40