Os Desafios da Segurança no Desenvolvimento com Métodos Ágeis

Rafael Dreher
OWASP Porto Alegre Chapter - Co-founder
Security Consultant @ Dell
dreher@owasp.org

OWASP
Education Project

The OWASP Foundation
http://www.owasp.org

Agenda

- Introdução.
- Conceitos básicos: Scrum e XP.
- Desafio 1: Segurança x Agilidade
- Desafio 2: Introduzindo Segurança - Fazendo o básico...
- Desafio 3: Aprimorar a Segurança - Inserindo complexidade...
- Conclusão.

Conceitos Básicos...

- Manifesto Agile
  - Publicado em 2001.
  - Modificar os conceitos de construção de software.
  - Foco em:
    - **Indivíduos e interações** mais que processos e ferramentas
    - **Software em funcionamento** mais que documentação abrangente
    - **Colaboração com o cliente** mais que negociação de contratos
    - **Responder a mudanças** mais que seguir um plano

Conceitos básicos...

- Metodologias Ágeis são baseadas em práticas que focam princípios como:

Conceitos básicos...

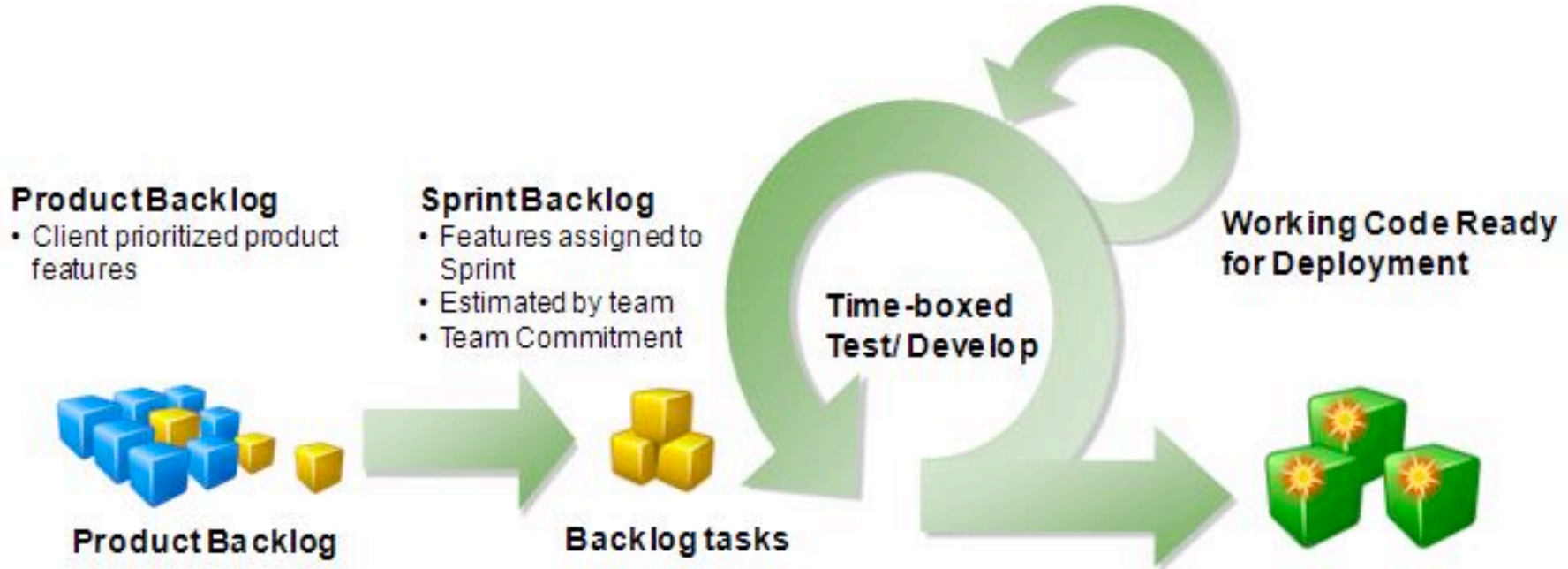
- Metodologias Ágeis são baseadas em práticas que focam princípios como:

Metodologia Scrum

- é um processo ágil para gerenciar e controlar o trabalho de desenvolvimento, melhorar a comunicação entre os times, detectar e remover qualquer impeditivo para o desenvolvimento e entrega de um produto.
  - Princípios:
    - Scrum Meeting;
    - Backlog Management;
    - Impediment Management;
    - Sprint.
    - Roles:
      - Product Manager
      - Scrum Master (Same as PM)
      - Developers

Metodologia Scrum

Metodologia Scrum



Sprint Planning Meeting
- Review Product Backlog
- Estimate Sprint Backlog
- Commit

Daily Scrum Meetings
- Done since last meeting
- Plan for today
- Roadblocks/Accelerators?

Sprint Review Meeting
- Demo features to all
- Retrospective on the Sprint Adjustments

Time-boxed "Sprint" Cycles

Metodologia Scrum

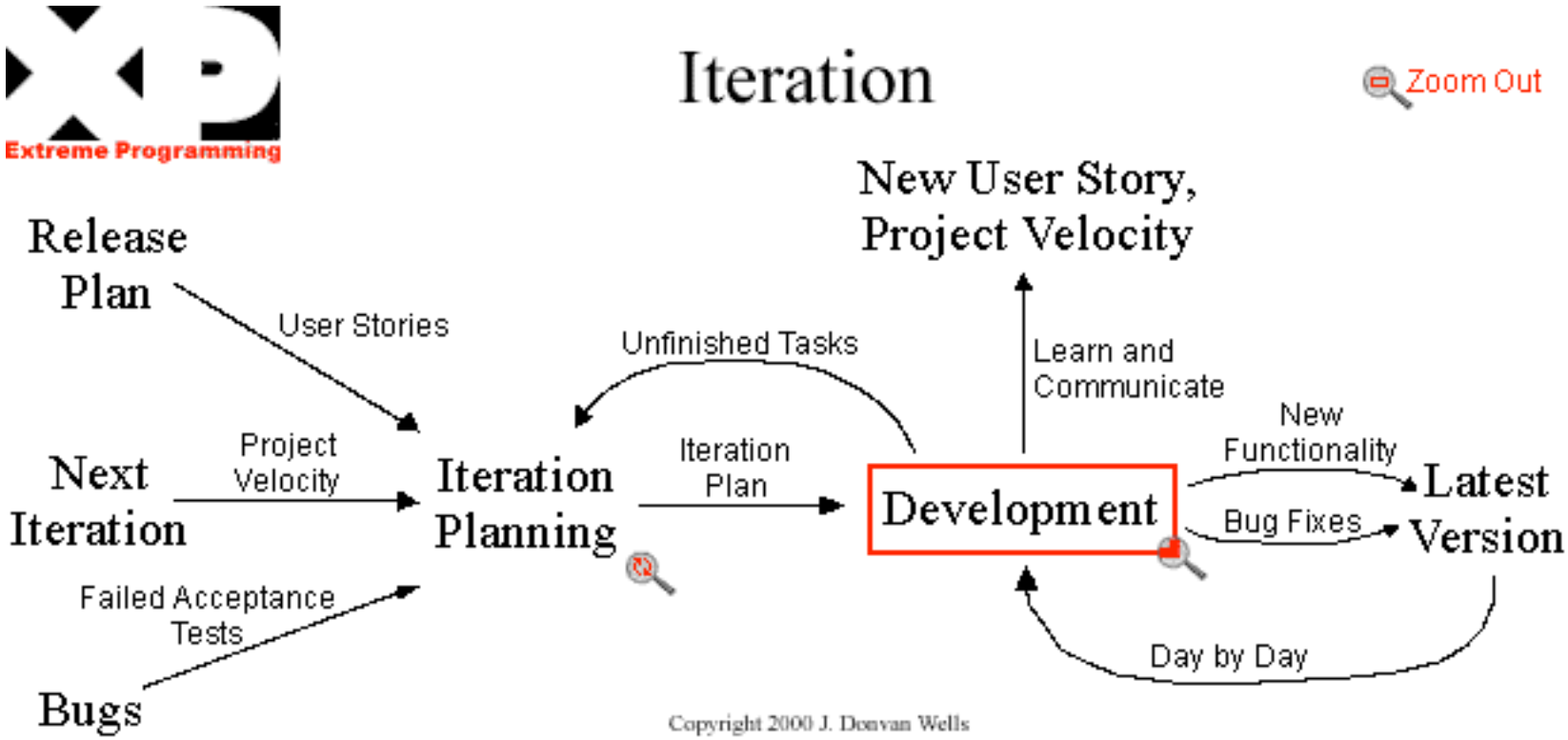
- Dividida em 3 processos principais:
  - Pre-game (Planejamento)
    - Planning (backlog), Risk Management, Cost Management, Release Dates (Roadmap);
    - Architecture, High Level Design, Refine Architecture to support changes.
  - Sprint (Desenvolvimento)
    - Pre defined time box to develop activities (Sprint time);
    - No fixed time for Srpint. The team needs to find its pace;
    - Develop activities like: code, wrap, review and adjust.
      - This is a way to implement continuous improvement in a daily basis.
  - Closure (Entrega)
    - Prepare the product for production release;
    - Training, Documentation, Final testing and Marketing.

eXtreme Programming

- XP foca em comunicação, com uma disciplina rigorosa;
- XP roles: Customer, Developer, Tracker and Coach;
- Guided by values: Communication, Courage, Feedback, Respect and Simplicity;
- Creators: Kent Beck, Ron Jeffries, Ward Cunningham.

eXtreme Programming

eXtreme Programming



Desafio 1: Segurança x Agilidade

- O maior desafio para se incluir segurança em qualquer processo é não alterar a natureza do mesmo.
- No desenvolvimento com métodos ágeis, como o nome já diz, não podemos alterar a natureza ágil do processo.
- A segurança deve ser inserida de modo transparente, de modo que não sejam efetuadas mudanças bruscas na metodologia.
- KISS = Keep It Simple Stupid. :-)

Desafio 2: Introduzindo Segurança

- Seguindo os preceitos de não alterar a natureza da metodologia, alguns controles podem ser inseridos de forma transparente, entre eles:
  - Revisão da arquitetura;
  - Revisão de código-fonte;
  - Testes de segurança;
  - Revisão final de segurança.

Desafio 3: Aprimorando a Segurança

- O princípio básico, não importa a metodologia, é treinar todos os envolvidos no projeto para pensar de forma segura.
- Cultura de segurança é um ponto de controle.
- Um dos maiores desafios da Segurança da Informação, em qualquer projeto, é ensinar o time a pensar de forma segura.

Desafio 3: Aprimorando a Segurança

- Todos os controles inseridos até agora focam no aspecto técnico da aplicação.
- E os aspectos funcionais de segurança?
- Como garantir que aplicação tenha o comportamento esperado e que não seja possível fazer uso privilegiado da mesma, subvertendo-a?

Desafio 3: Aprimorando a Segurança

- No contexto das metodologias ágeis, "User Stories" definem os requisitos e os recursos que um software terá.
- Escrever requisitos de segurança na forma de "User Stories" é uma maneira de garantir que estes sejam implementados de forma funcional no software.
- Envolve um trabalho em conjunto do Analista de Segurança da Informação com o Desenvolvedor.

Conclusões

- Segurança não é plug-and-play, especialmente em metodologias ágeis.
- Alguns controles técnicos são fáceis de ser adaptados de uma metodologia para outra.
- Mudanças mais profundas, exigem uma mudança de pensamento e de cultura.
- Segurança continua sendo uma atividade compartilhada do time de projeto com o Analista de Segurança da Informação.
- O Analista de Segurança da Informação trabalha como consultor, apoiando o projeto.

Perguntas?


AppSec Brasil '11
1st Global Appsec Latin America Conference
Porto Alegre - Rio Grande do Sul

Obrigado!