Diagnóstico de Vulnerabilidades através da Injecção de Ataques

SINO'05, Covilhã, Portugal

João Antunes[1], Nuno Neves[1],
Miguel Correia[1], Paulo Veríssimo[1],
Rui Neves[2]

[1] Faculdade de Ciências da Universidade de Lisboa
[2] Instituto Superior Técnico da Universidade Técnica de Lisboa

7 de Novembro de 2005

Conteúdo

Introdução

Vulnerabilidades

Aplicações

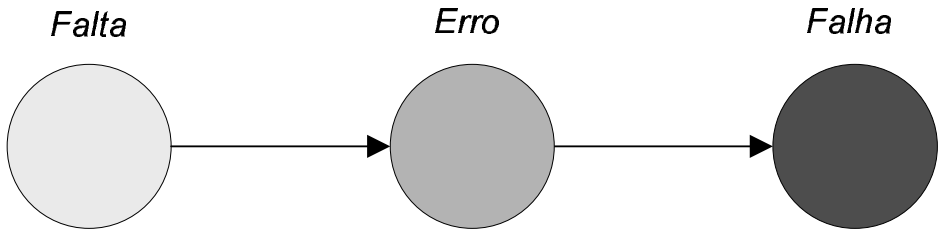
- Maior dimensão e complexidade
- Envolvimento de mais pessoas (directa e indirectamente)
  - maiores equipas de desenvolvimento
  - fonte externa (e.g., bibliotecas de terceiros)

$\Rightarrow$ Resulta na **introdução de erros**:

- em maior número
- de maior complexidade
- e as ferramentas de detecção não estão preparadas

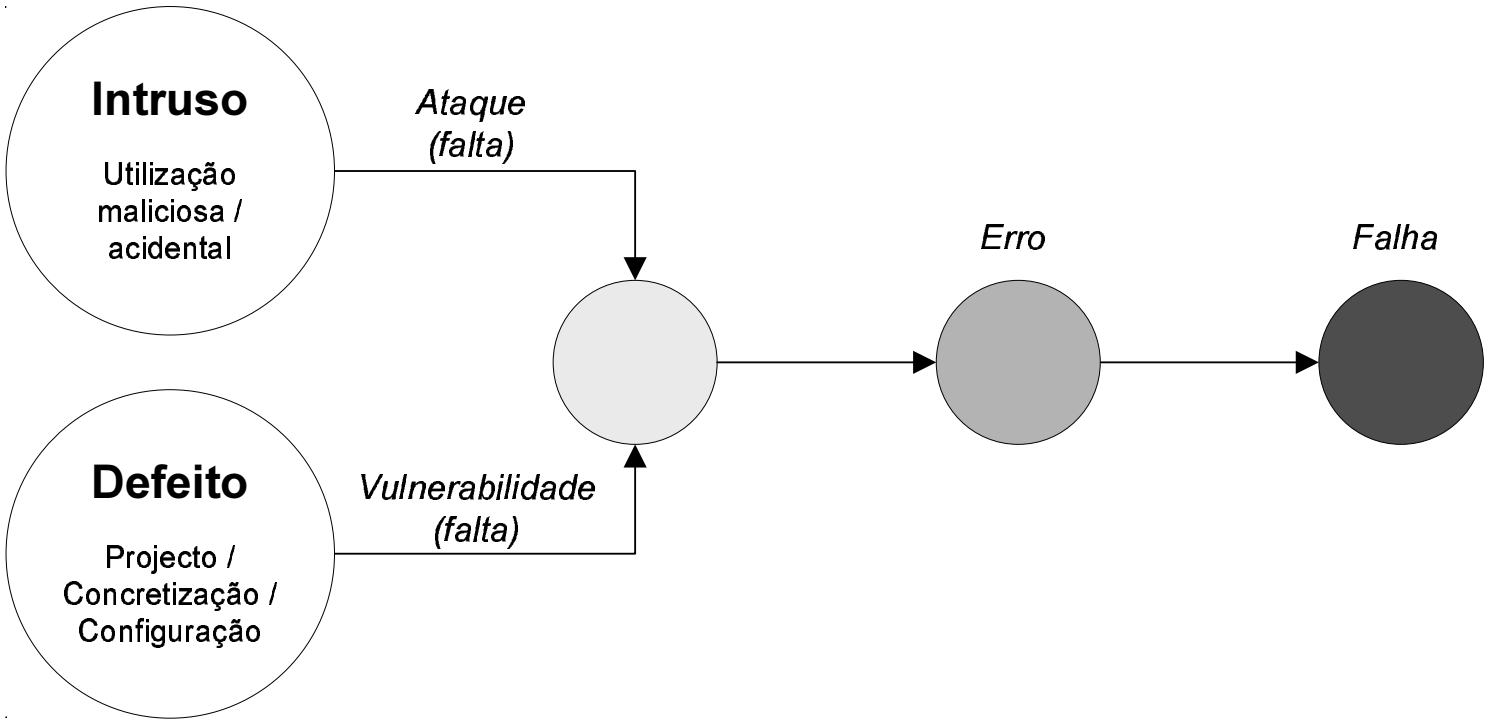
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



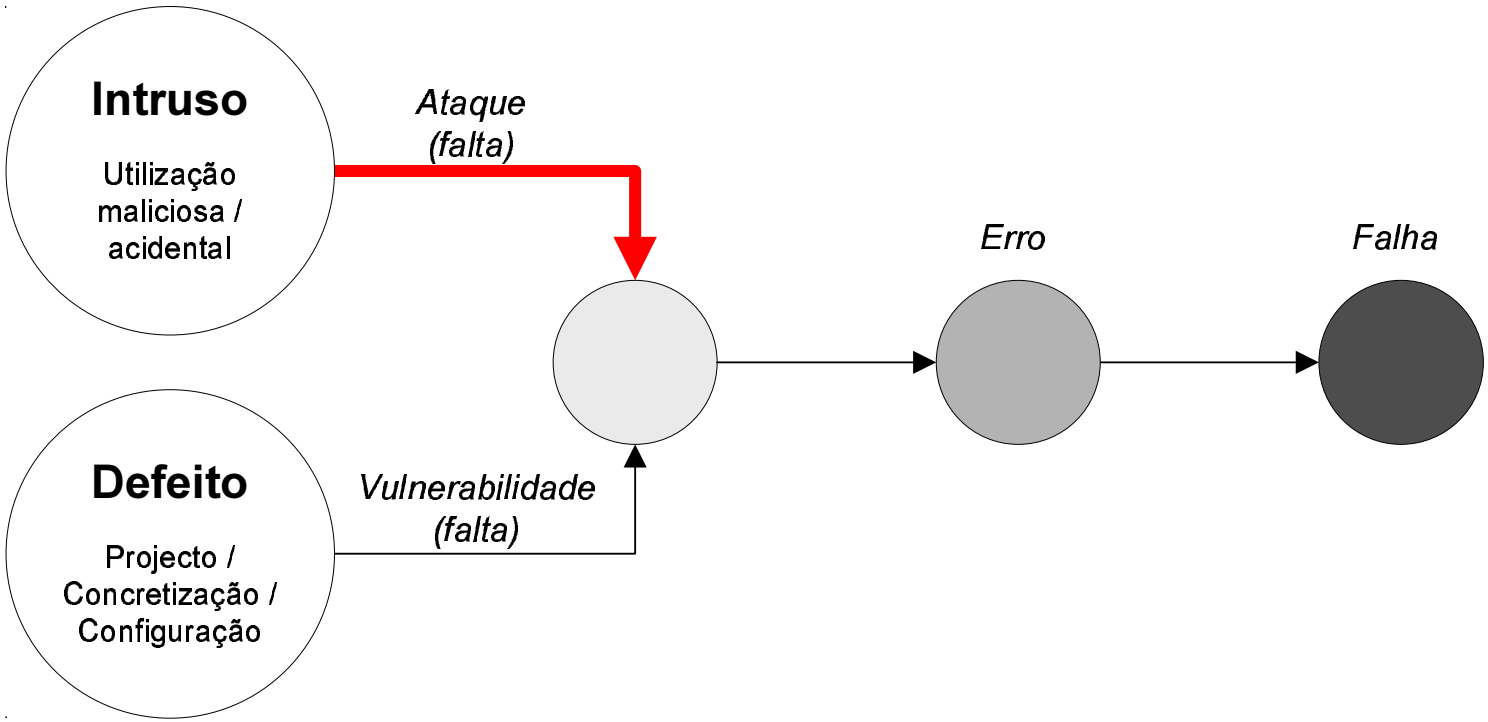
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



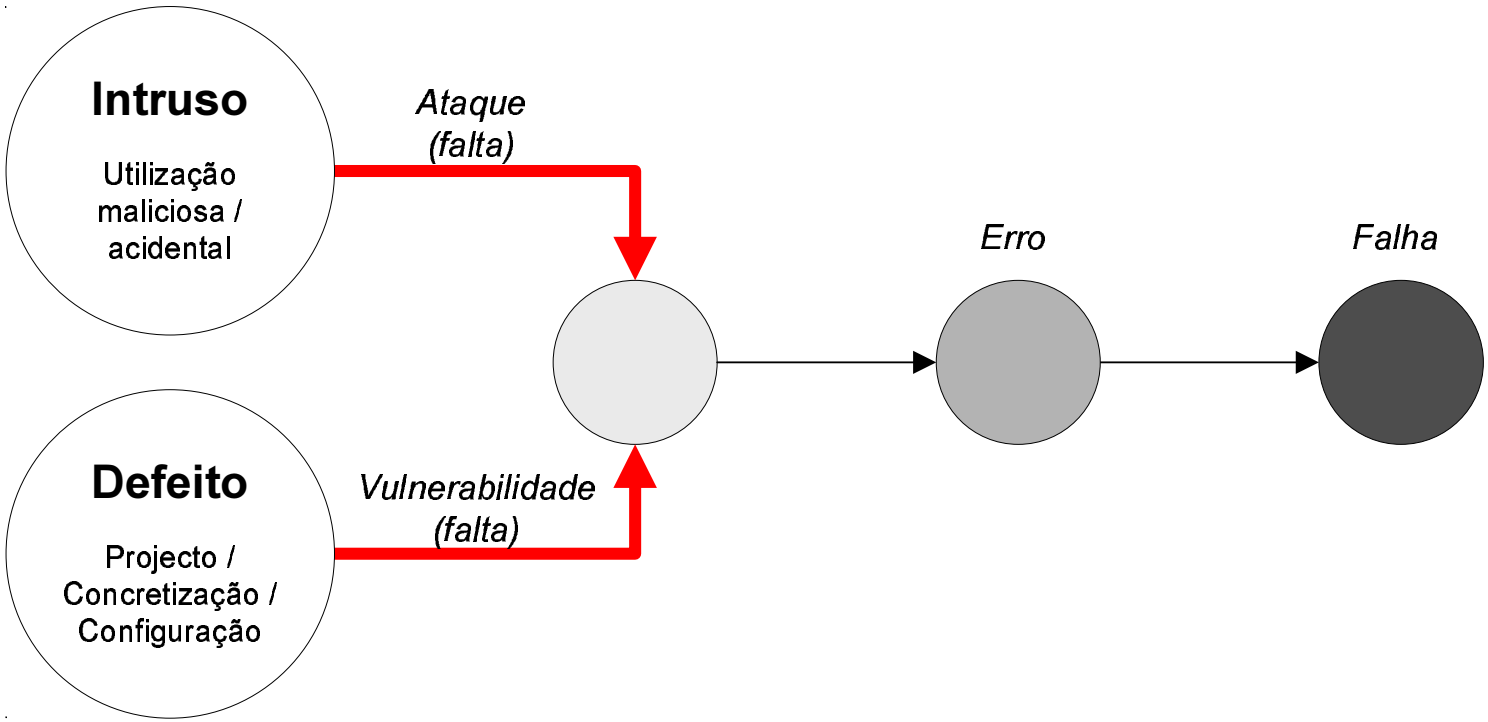
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



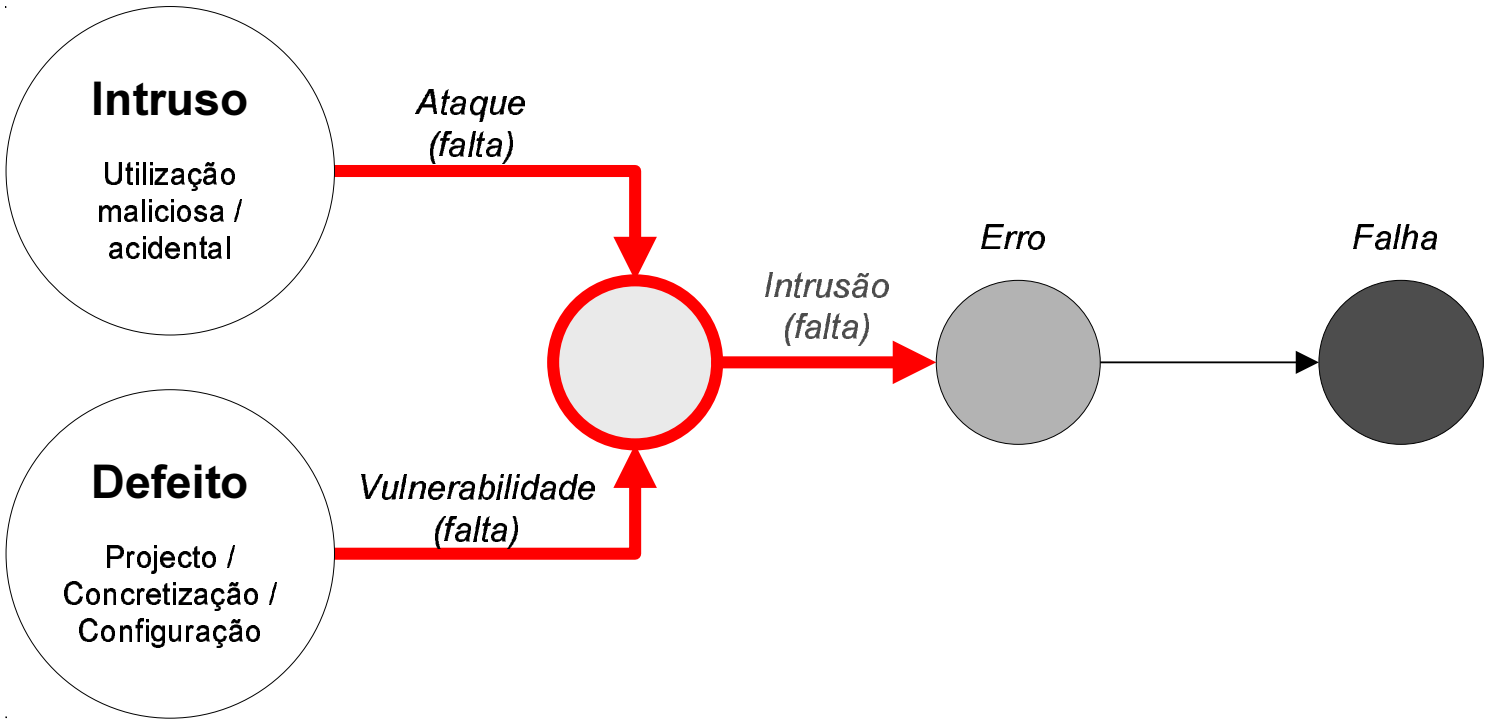
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



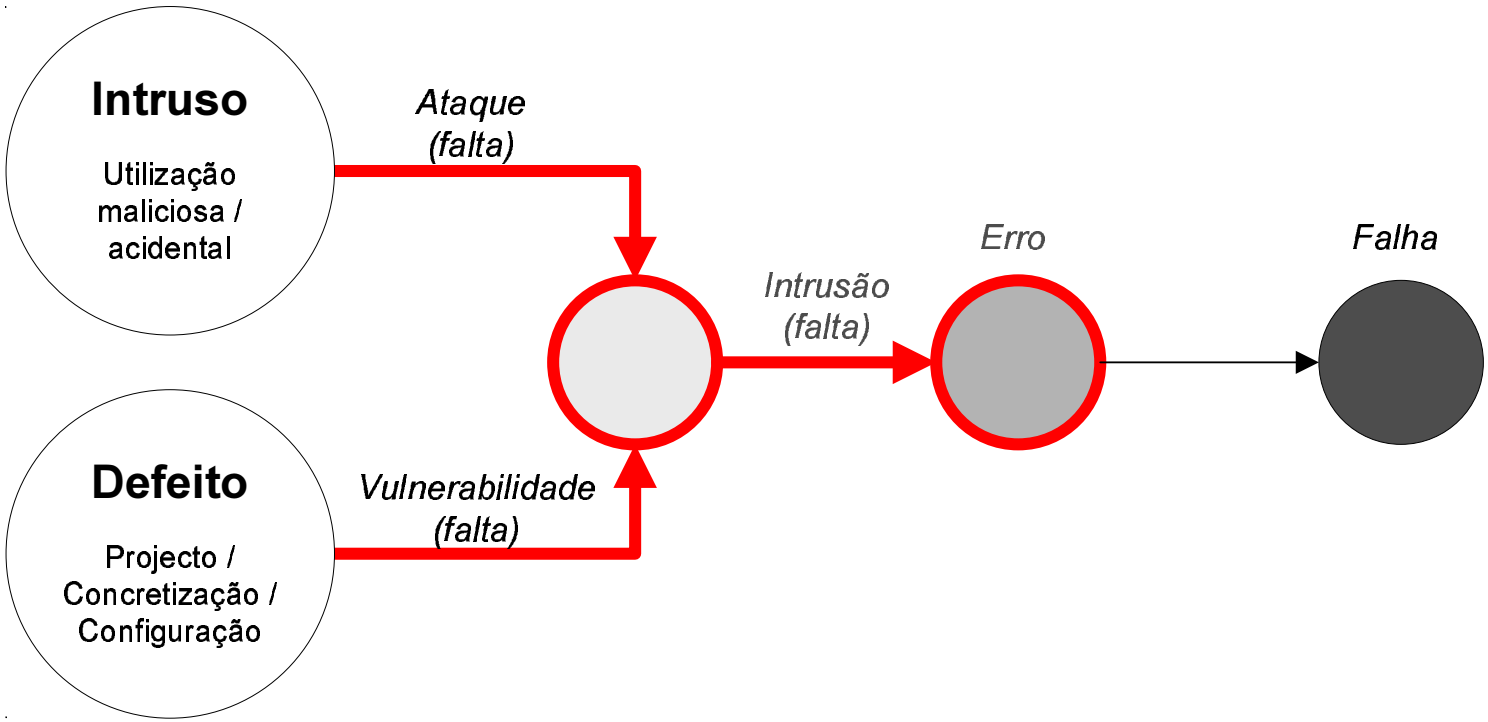
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



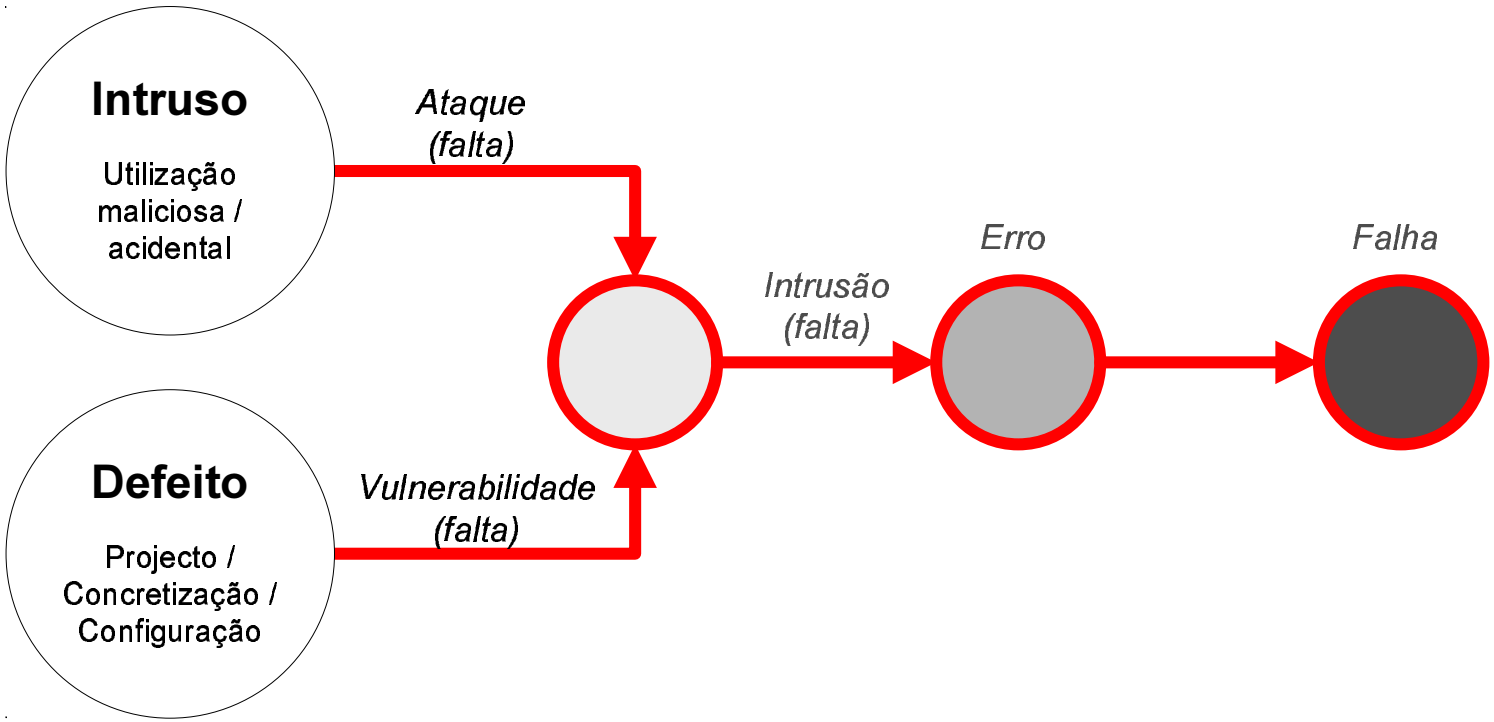
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



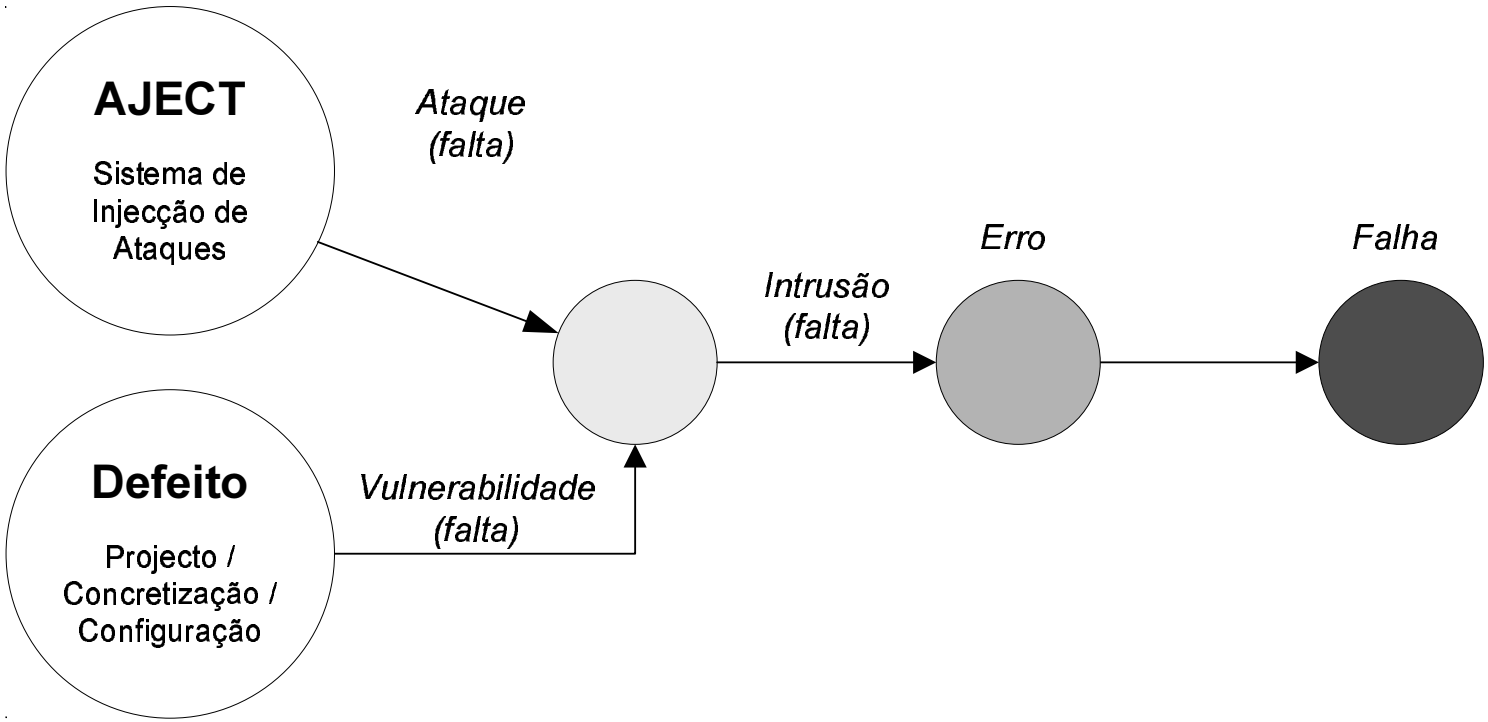
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



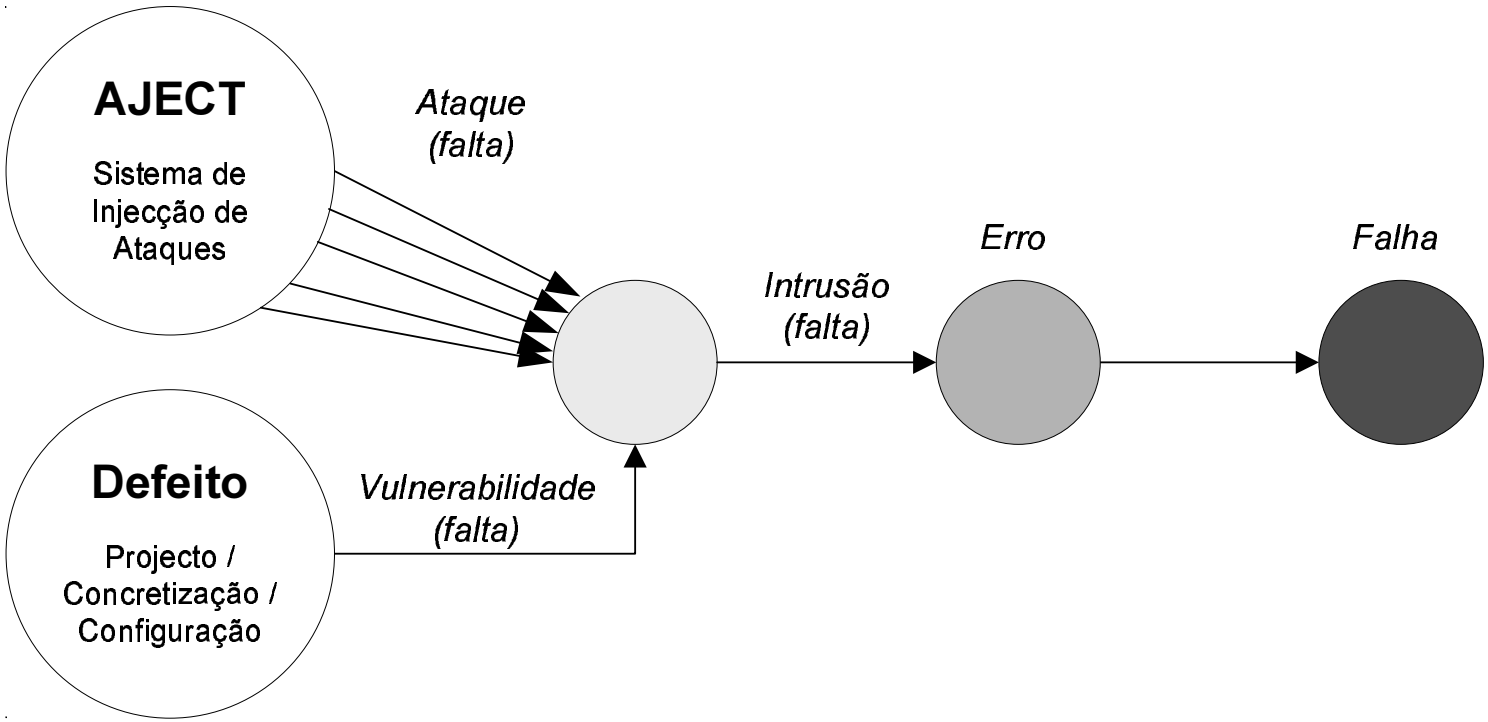
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



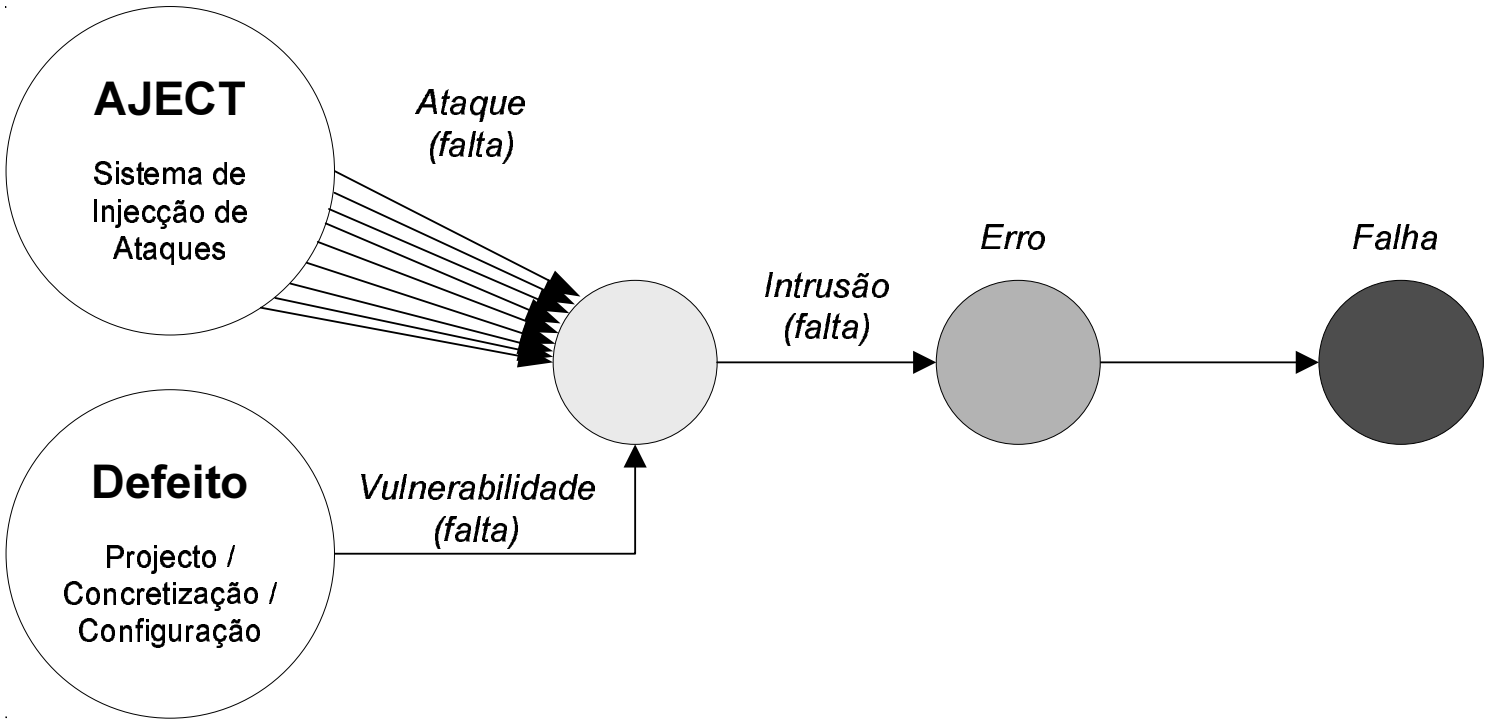
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



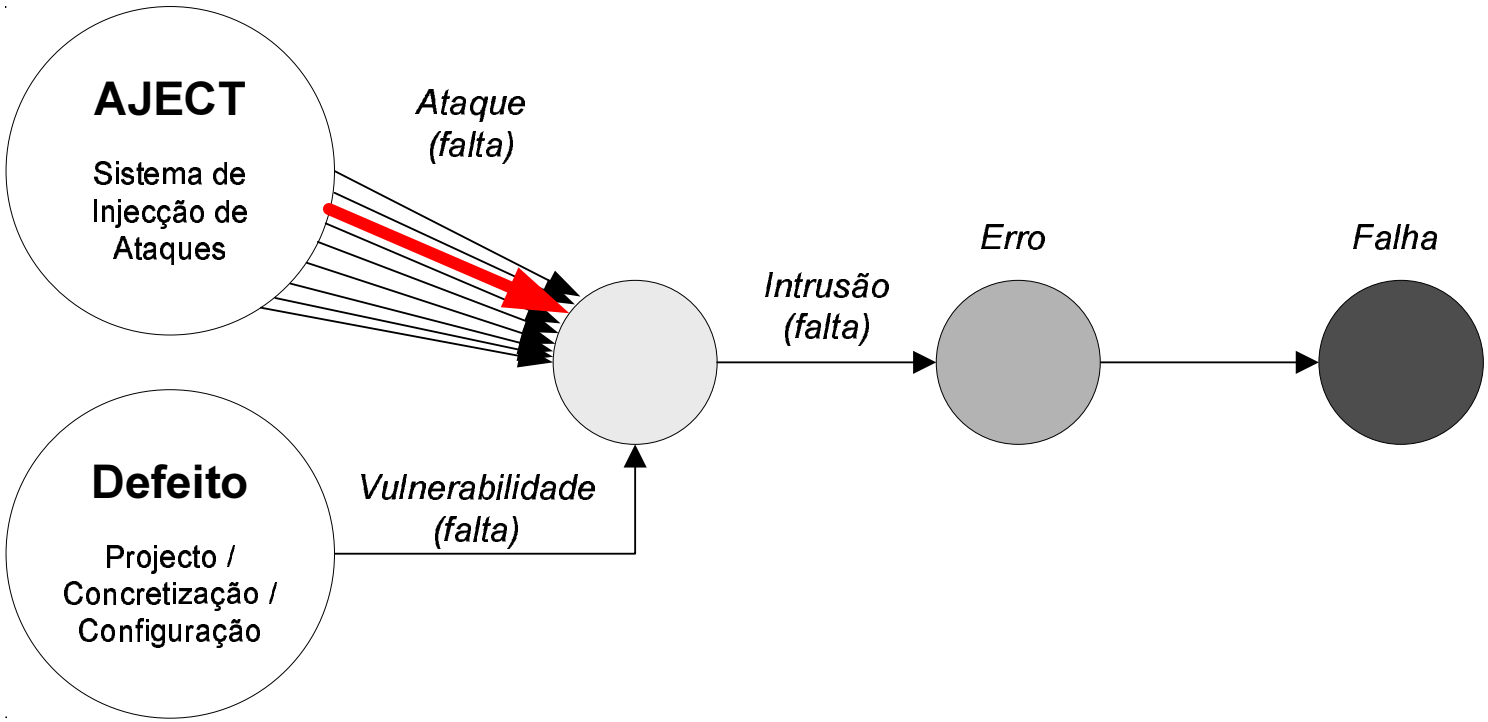
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



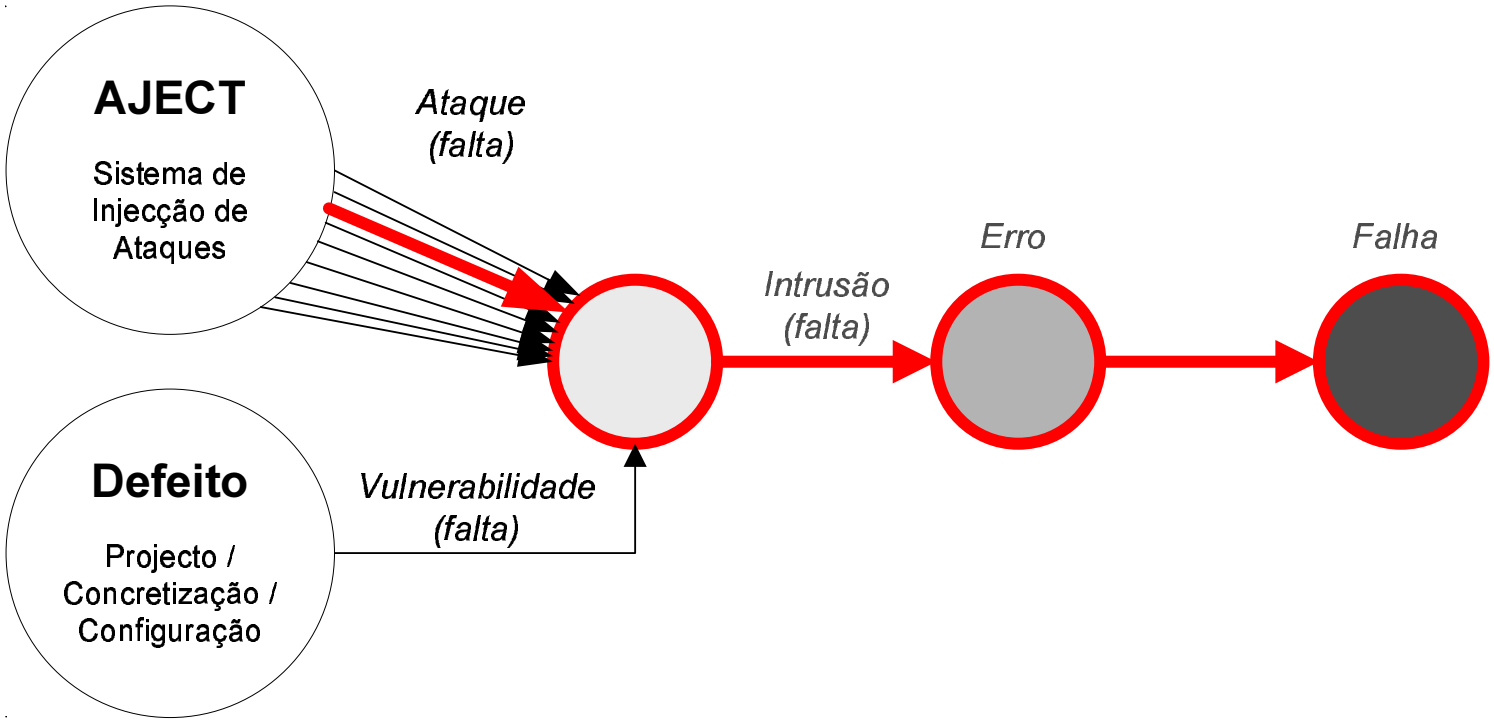
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



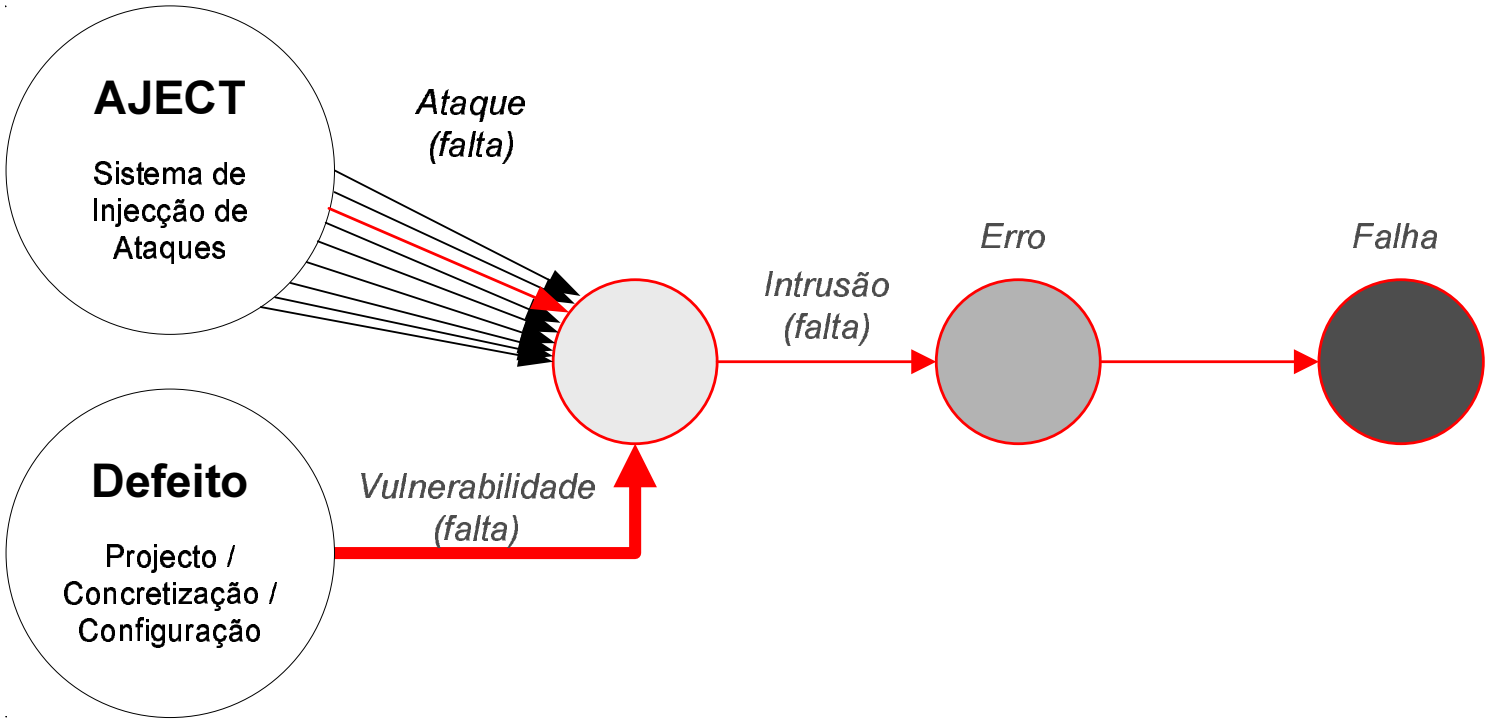
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)



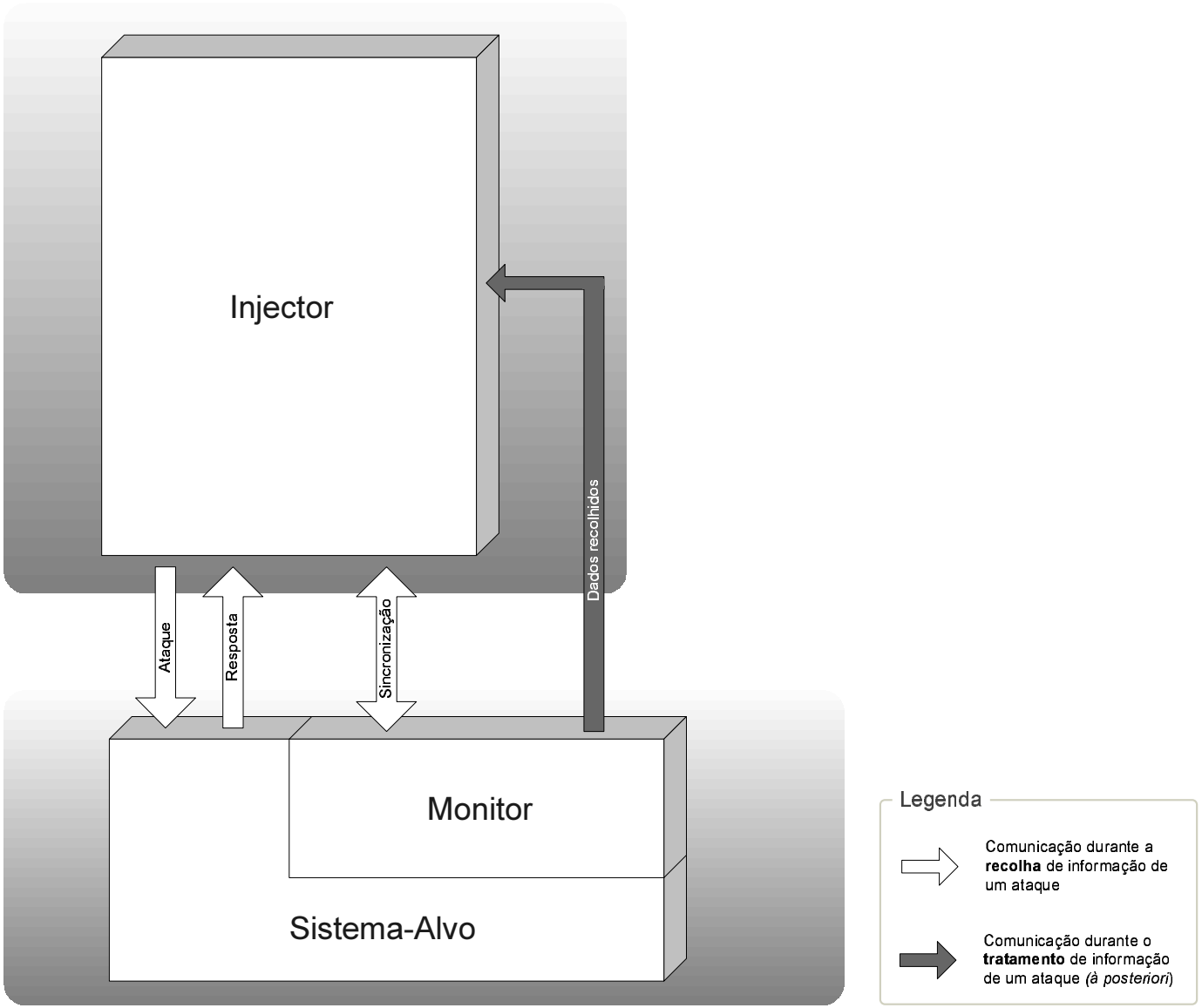
Modelo de Faltas

- Modelo composto de faltas AVI
  (Ataque, Vulnerabilidade e Intrusão)

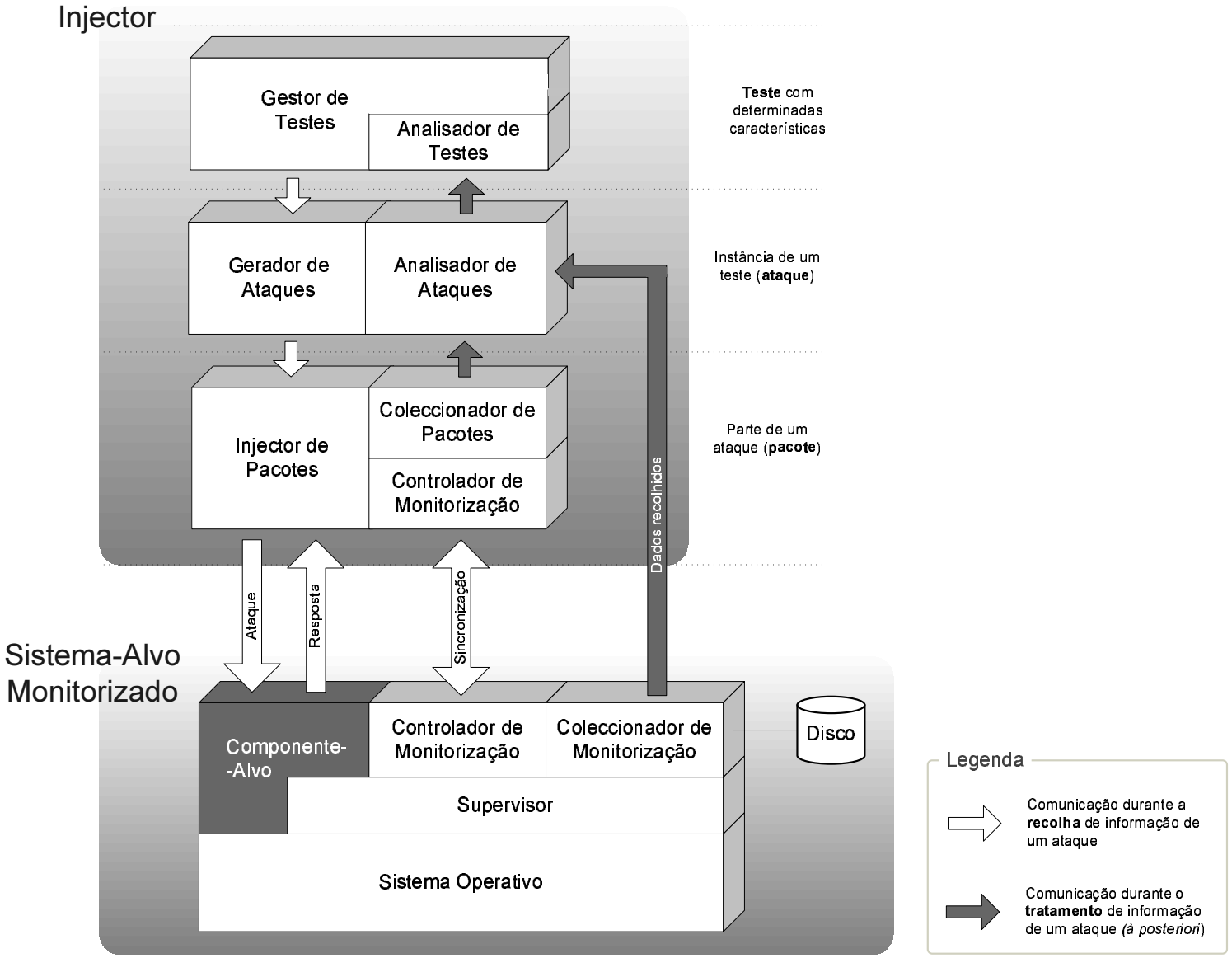


Concretização da Ferramenta de Injecção de Ataques

Arquitectura do AJECT



Arquitectura do AJECT (detalhe)



Injecção de Ataques

1. Testes geram ataques (compostos por pacotes)
2. Inicialização (início de ataque)
   - Sincronização do ataque
   - Monitor reinicializa condições de teste
   - Estabelec. de comunic. entre Injector e Aplicação-Alvo
3. Ataque (injecção de ataque)
   - Envio dos pacotes (do ataque) à Aplicação-Alvo
   - Recepção e registo das respostas
   - Supervisão da Aplicação-Alvo
4. Finalização (fim de ataque)
   - Fim de sincronização do ataque
   - Registo do ataque
   - Remoção dos efeitos do ataque

Injecção de Ataques

1. Testes geram ataques (compostos por pacotes)
2. Inicialização (início de ataque)
   - Sincronização do ataque
   - Monitor reinicializa condições de teste
   - Estabelec. de comunic. entre Injector e Aplicação-Alvo
3. Ataque (injecção de ataque)
   - Envio dos pacotes (do ataque) à Aplicação-Alvo
   - Recepção e registo das respostas
   - Supervisão da Aplicação-Alvo
4. Finalização (fim de ataque)
   - Fim de sincronização do ataque
   - Registo do ataque
   - Remoção dos efeitos do ataque

Injecção de Ataques

1. Testes geram ataques (compostos por pacotes)
2. Inicialização (início de ataque)
   - Sincronização do ataque
   - Monitor reinicializa condições de teste
   - Estabelec. de comunic. entre Injector e Aplicação-Alvo
3. Ataque (injecção de ataque)
   - Envio dos pacotes (do ataque) à Aplicação-Alvo
   - Recepção e registo das respostas
   - Supervisão da Aplicação-Alvo
4. Finalização (fim de ataque)
   - Fim de sincronização do ataque
   - Registo do ataque
   - Remoção dos efeitos do ataque

Injecção de Ataques

1. Testes geram ataques (compostos por pacotes)
2. Inicialização (início de ataque)
   - Sincronização do ataque
   - Monitor reinicializa condições de teste
   - Estabelec. de comunic. entre Injector e Aplicação-Alvo
3. Ataque (injecção de ataque)
   - Envio dos pacotes (do ataque) à Aplicação-Alvo
   - Recepção e registo das respostas
   - Supervisão da Aplicação-Alvo
4. Finalização (fim de ataque)
   - Fim de sincronização do ataque
   - Registo do ataque
   - Remoção dos efeitos do ataque

Monitorização de Ataques

- Dependente do SO (rastreio de processos)
- Consiste na:
  - observação do estado da Aplicação-Alvo
  - registo da supervisão

Execução da Ferramenta de Injecção de Ataques

Tipos de Testes

- Testes de sintaxe
- Testes de valor

Tipos de Testes

pacote exemplo

[A] [B] [C]

Teste de sintaxe

[B] [C]

[A] [C]

[A] [B]

[A] [A] [B] [C]

[A] [B] [A] [C]

[A] [B] [C] [A]

...

Tipos de Testes

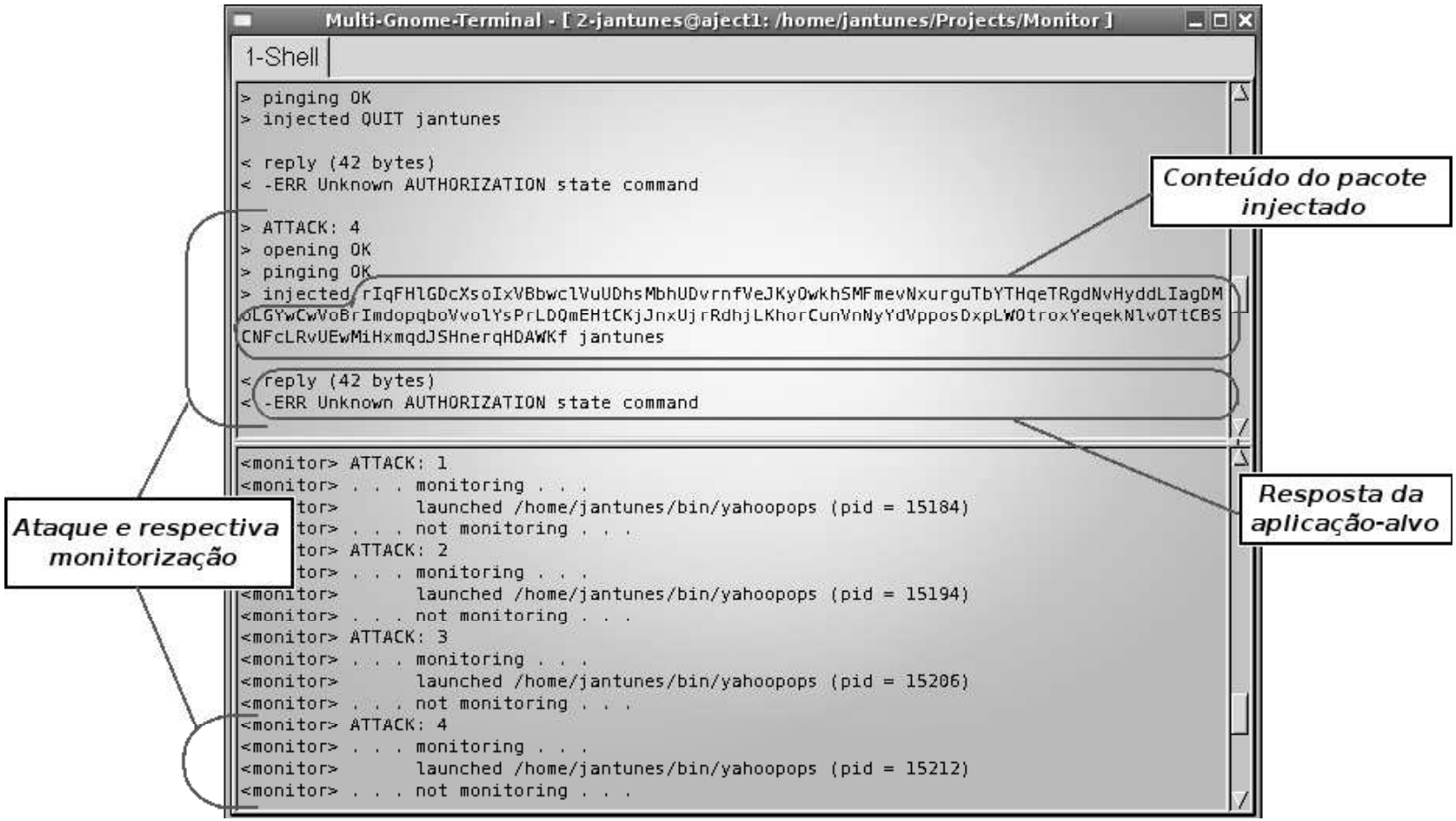
pacote exemplo

[A: 1] [B: 0 – 1000]

Teste de valor

[1] [0]
[1] [-1]
[1] [1]
[1] [1000]
[1] [999]
[1] [1001]
[1] [100000000000000]
[1] [-1000]
...

Execução do AJECT



Aplicação-Alvo

YPOPs!

- Permite descarregar e-mail de uma conta *Yahoo!*
  - servidor POP3 local que medeia a comunicação com o *Yahoo!*

Vulnerabilidade

- Teste de valor permitiu detectar vulnerabilidade de *buffer overflow*
- Vulnerabilidade descoberta em Setembro de 2004 (BugTraq nº 11256)

Sumário e Conclusões

Conclusão

Desafios

- Sistema modular e independente
- Representação do protocolo-alvo e dos tipos de dados
- Representação e geração de testes/ataques
- Mecanismos de supervisão

Conclusão

Resultados

- Sistema de detecção de vulnerabilidades
  - Modularidade
  - Independência
    - Injector $\longleftrightarrow$ Plataforma
    - Injector $\longleftrightarrow$ Sistema-Alvo Monitorizado
    - Monitor $\longleftrightarrow$ Aplicação-Alvo (depende apenas do SO)
    - Injector e Monitor $\longleftrightarrow$ Testes
- Detecção com sucesso de uma vulnerabilidade na Aplicação-Alvo

Trabalho Futuro

A desenvolver

- Testes (maior quantidade e complexidade)
- Maior automatização na análise de vulnerabilidades
- Simplificação da especificação do protocolo-alvo