

Diagnóstico de Vulnerabilidades através da Injecção de Ataques

SINO'05, Covilhã, Portugal

João Antunes¹, Nuno Neves¹,
Miguel Correia¹, Paulo Veríssimo¹,
Rui Neves²

¹ Faculdade de Ciências da Universidade de Lisboa

² Instituto Superior Técnico da Universidade Técnica de Lisboa

7 de Novembro de 2005

Conteúdo

SINO'05

Introdução

Concretização

Execução

Sumário e
Conclusões

- 1 Introdução
- 2 Concretização da Ferramenta de Injecção de Ataques
- 3 Execução da Ferramenta de Injecção de Ataques
- 4 Sumário e Conclusões

SINO'05

Introdução

Vulnerabilidades
Modelo de Falhas

Concretização

Execução

Sumário e
Conclusões

Introdução

Vulnerabilidades

SINO'05

Introdução

Vulnerabilidades
Modelo de Falhas

Concretização

Execução

Sumário e
Conclusões

Aplicações

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

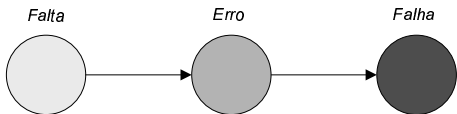
⇒ Resulta na **introdução de erros**:

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

Modelo de Faltas

SINO'05

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



Introdução

Vulnerabilidades

Modelo de Faltas

Concretização

Execução

Sumário e
Conclusões

Modelo de Faltas

SINO'05

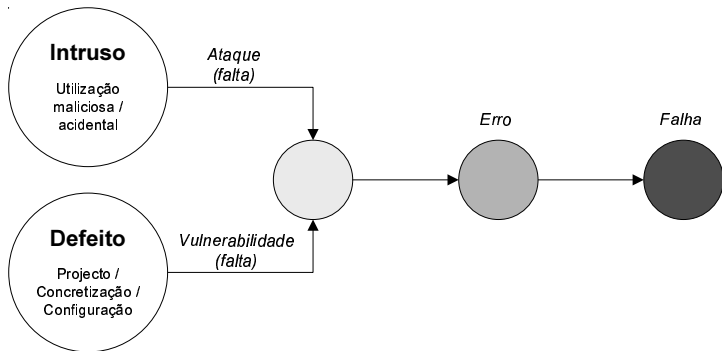
Introdução
Vulnerabilidades
Modelo de Faltas

Concretização

Execução

Sumário e
Conclusões

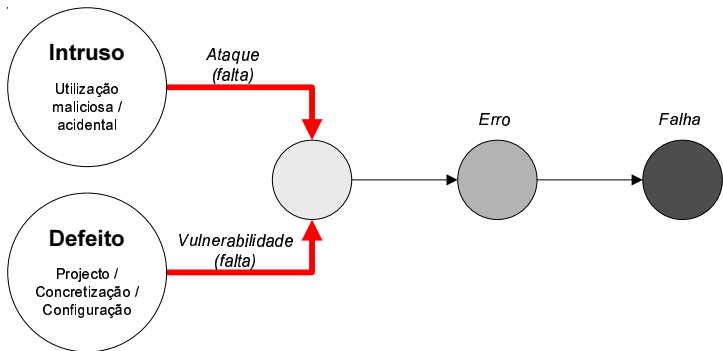
- Modelo composto de faltas AVI (Ataque, Vulnerabilidade e Intrusão)



Modelo de Faltas

SINO'05

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



Introdução

Vulnerabilidades

Modelo de Faltas

Concretização

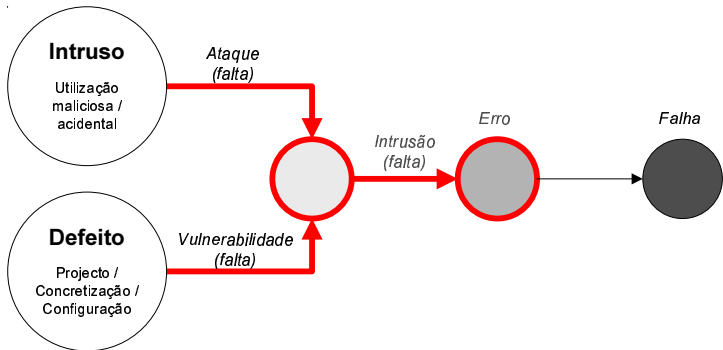
Execução

Sumário e
Conclusões

Modelo de Falhas

SINO'05

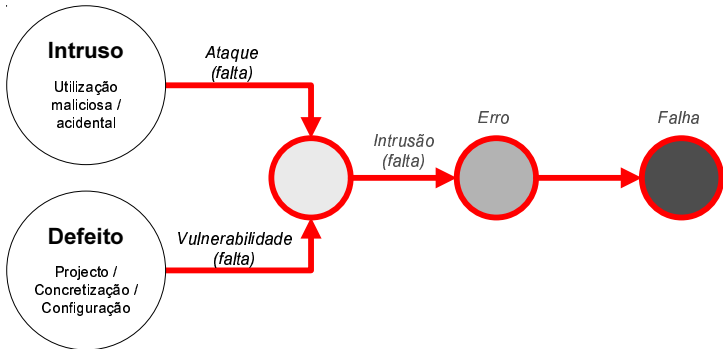
- Modelo composto de faltas AVI (Ataque, Vulnerabilidade e Intrusão)



Modelo de Falhas

SINO'05

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



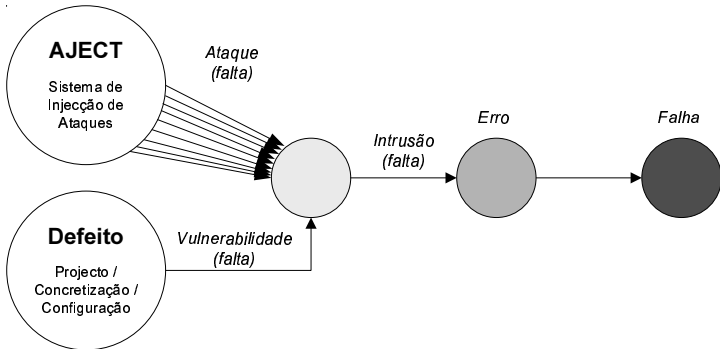
Introdução
 Vulnerabilidades
Modelo de Falhas
 Concretização
 Execução
 Sumário e
 Conclusões

Modelo de Falhas

SINO'05

Introdução
Vulnerabilidades
Modelo de Falhas
Concretização
Execução
Sumário e
Conclusões

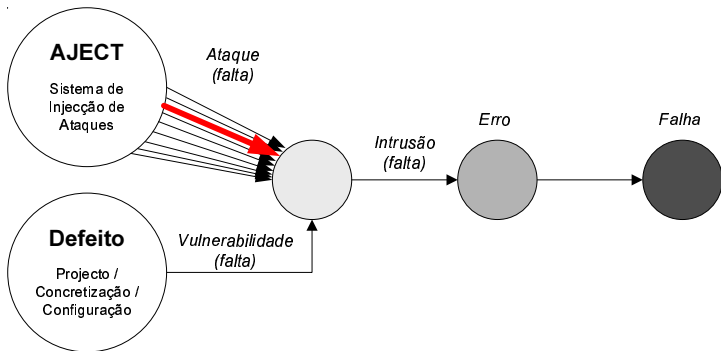
- Modelo composto de faltas AVI (Ataque, Vulnerabilidade e Intrusão)



Modelo de Falhas

SINO'05

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



Modelo de Falhas

SINO'05

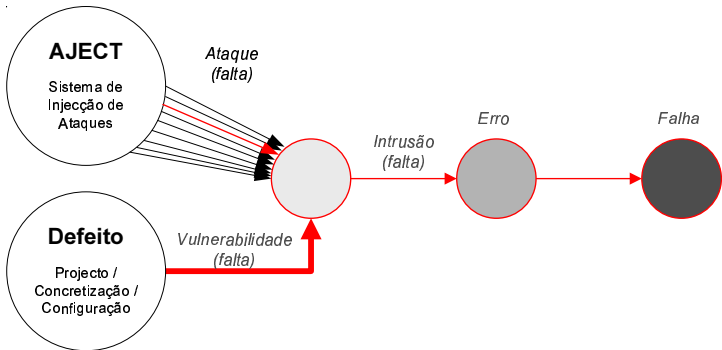
Introdução
Vulnerabilidades
Modelo de Falhas

Concretização

Execução

Sumário e
Conclusões

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



SINO'05

Introdução

Concretização

Arquitectura do
AJECT

Injecção

Monitorização

Execução

Sumário e
Conclusões

Concretização da Ferramenta de Injecção de Ataques

Arquitectura do AJECT

SINO'05

Introdução

Concretização

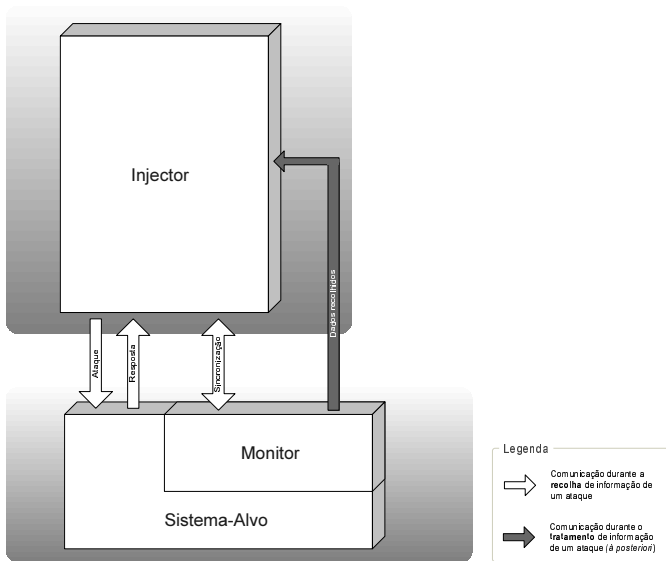
Arquitectura do AJECT

Injecção

Monitorização

Execução

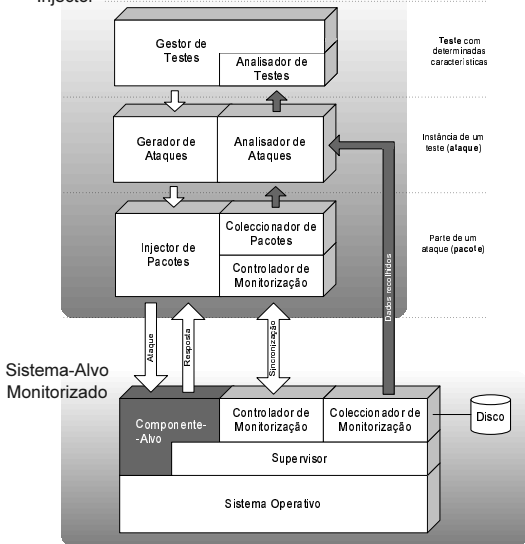
Sumário e Conclusões



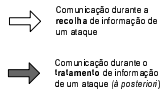
Arquitectura do AJECT (detalhe)

SINO'05

Injector



Legenda



Injecção de Ataques

SINO'05

Introdução

Concretização

Arquitectura do
AJECT

Injecção

Monitorização

Execução

Sumário e
Conclusões

- 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

SINO'05

Introdução

Concretização

Arquitectura do
AJECT

Injecção

Monitorização

Execução

Sumário e
Conclusões

- 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

SINO'05

Introdução

Concretização

Arquitectura do
AJECT

Injecção

Monitorização

Execução

Sumário e
Conclusões

- 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

SINO'05

Introdução

Concretização

Arquitectura do
AJECT

Injecção

Monitorização

Execução

Sumário e
Conclusões

- 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

SINO'05

Introdução

Concretização

Arquitectura do
AJECT

Injecção

Monitorização

Execução

Sumário e
Conclusões

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

SINO'05

Introdução

Concretização

Execução

Tipos de Testes

Execução do AJECT

Aplicação-Alvo

Sumário e

Conclusões

Execução da Ferramenta de Injecção de Ataques

Tipos de Testes

SINO'05

Introdução

Concretização

Execução

Tipos de Testes

Execução do AJECT

Aplicação-Alvo

Sumário e

Conclusões

- Testes de sintaxe
- Testes de valor

Tipos de Testes

SINO'05

Introdução

Concretização

Execução

Tipos de Testes

Execução do AJECT

Aplicação-Alvo

Sumário e

Conclusões

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

SINO'05

pacote exemplo

[A: 1] [B: 0 – 1000]

Introdução

Concretização

Execução

Tipos de Testes

Execução do AJECT

Aplicação-Alvo

Sumário e

Conclusões

Teste de valor

[1] [0]

[1] [-1]

[1] [1]

[1] [1000]

[1] [999]

[1] [1001]

[1] [1000000000000000]

[1] [-1000]

...

Execução do AJECT

SINO'05

Introdução

Concretização

Execução

Tipos de Testes

Execução do AJECT

Aplicação-Alvo

Sumário e
Conclusões

```
Multi-Gnome-Terminal - [ 2-jantunes@aject1: /home/jantunes/Projects/Monitor ]
1-Shell
> ping
ping OK
> injected
injected QUIT jantunes
< reply (42 bytes)
< -ERR Unknown AUTHORIZATION state command
> ATTACK: 4
> opening
opening OK
> ping
ping OK
> injected
injected r1qFHLGdcXsoIxVBwclVuUDhsMbhUDvrnfVeJKyDwkhSMFevNrxurguTbYTHqeTRgdNvHyddLIagDM
dLGYwCwVubImdupubVvuLYsPiLD0mEHlCKJjixUjIRuhjLkIiviCuiNinNyYUvppusDxpLW0LiuxYeekNlv0TLCB5
CNFclRvUEwMLHxmqdJSHnerqHDAWkf jantunes
< reply (42 bytes)
< -ERR Unknown AUTHORIZATION state command
<monitor> ATTACK: 1
<monitor> ... monitoring ...
<tor> ... launched /home/jantunes/bin/yahoopops (pid = 15184)
<tor> ... not monitoring ...
<tor> ATTACK: 2
<tor> ... monitoring ...
<monitor> ... launched /home/jantunes/bin/yahoopops (pid = 15194)
<monitor> ... not monitoring ...
<monitor> ATTACK: 3
<monitor> ... monitoring ...
<monitor> ... launched /home/jantunes/bin/yahoopops (pid = 15206)
<monitor> ... not monitoring ...
<monitor> ATTACK: 4
<monitor> ... monitoring ...
<monitor> ... launched /home/jantunes/bin/yahoopops (pid = 15212)
<monitor> ... not monitoring ...
```

Conteúdo do pacote injectado

Ataque e respectiva monitorização

Resposta da aplicação-alvo

Aplicação-Alvo

SINO'05

Introdução

Concretização

Execução

Tipos de Testes

Execução do AJECT

Aplicação-Alvo

Sumário e

Conclusões

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)

SINO'05

Introdução

Concretização

Execução

**Sumário e
Conclusões**

Conclusão

Trabalho Futuro

Sumário e Conclusões

Conclusão

SINO'05

Introdução

Concretização

Execução

Sumário e
Conclusões

Conclusão
Trabalho Futuro

Desafios

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

Conclusão

SINO'05

Introdução

Concretização

Execução

Sumário e
Conclusões

Conclusão

Trabalho Futuro

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

A desenvolver

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