Um Agente SNMP para Detecção de Intrusão Baseada na Interação de Protocolos

Edgar Meneghetti (UCS)
Luciano Paschoal Gaspary (UNISINOS)
Liane Tarouco (UFRGS)

GTS 01.2004

Roteiro da Apresentação

- Motivação
- Sistemas de Detecção de Intrusão
- Sistemas de Gerenciamento de Redes
  - Arquitetura Trace
- O Agente SNMP para Detecção de Intrusão
  - Extensões
- Conclusões e Trabalhos Futuros
- Referências

Motivação

- Muitas organizações (médio e grande porte) utilizam plataformas de gerenciamento de rede
  - Geralmente direcionadas a gerenciamento de falhas e desempenho (Tivoli, OpenView, etc)
- Segurança é tratada de forma paralela
  - Geralmente não há integração com as plataformas
  - Atividades redundantes $\rightarrow$ monitoração
  - Não há visão integrada da estrutura de TI
- Pode ser interessante integrar segurança e gerenciamento...

Desafios em Detecção de Intrusão

- Baixo índice de falsos positivos e falsos negativos
- Flexibilidade para descrever cenários de ataques
  - Sistemas programáveis através de linguagens de fácil aprendizado
  - Capacidade de monitorar ataques em todos os níveis: físico, rede, transporte e aplicação
- Capacidade de suportar alto tráfego

Sistemas de Detecção de Intrusão

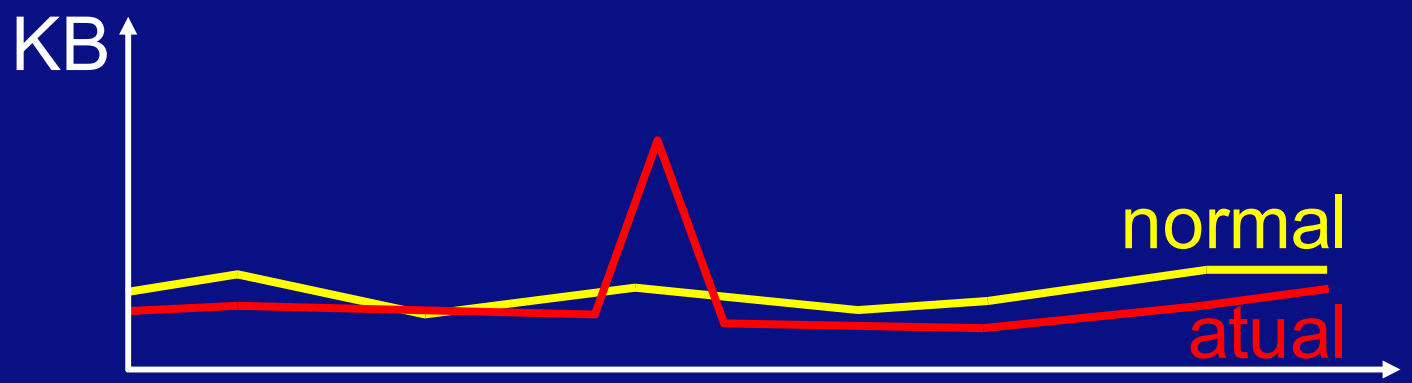
- Analisam atividades de um sistema de computação procurando evidências de comportamento malicioso
- Ao observar atividade suspeita
  - Alerta o administrador (*email*, *pager*, *pop-up*)
  - Aciona algum mecanismo de defesa (reconfiguração do *firewall*)

Sistemas de Detecção de Intrusão

- Informações podem ser coletadas de
  - Registros do sistema (*logs*)
  - Rede
- Baseiam-se em
  - Anomalia de comportamento
  - Assinaturas de ataques

Sistemas de Detecção de Intrusão

- Anomalia de comportamento
  - Identificação do comportamento “normal” do sistema
  - Comparação do estado atual com o esperado
  - Contempla ataques desconhecidos
  - Dificuldade em determinar comportamento “normal” - baseline



Tráfego DNS ao longo do dia em 172.16.1.1

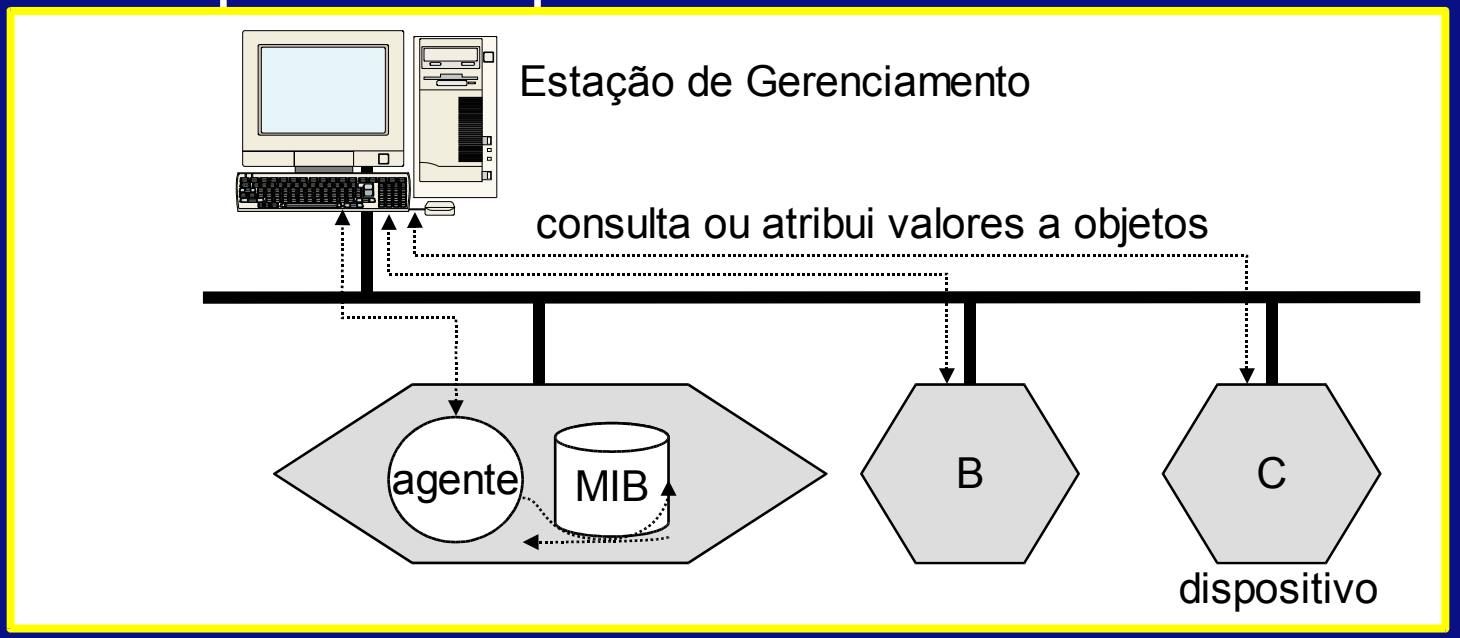
Sistemas de Detecção de Intrusão

- Assinaturas de ataques
  - Descrição dos ataques são armazenados em um BD
  - Detecção acontece quando comportamento do sistema é idêntico às assinaturas armazenadas
  - Não contempla ataques desconhecidos
  - São relativamente simples de serem modeladas
- Ataque a servidor WEB: procurar pela string

GET /scripts/..\%C0\%AF../winnt/system32/cmd.exe?/c+dir+c:

Gerenciamento de Redes

- Redes TCP/IP → Arquitetura SNMP (*Simple Network Management Protocol*)
  - Simples e amplamente difundida



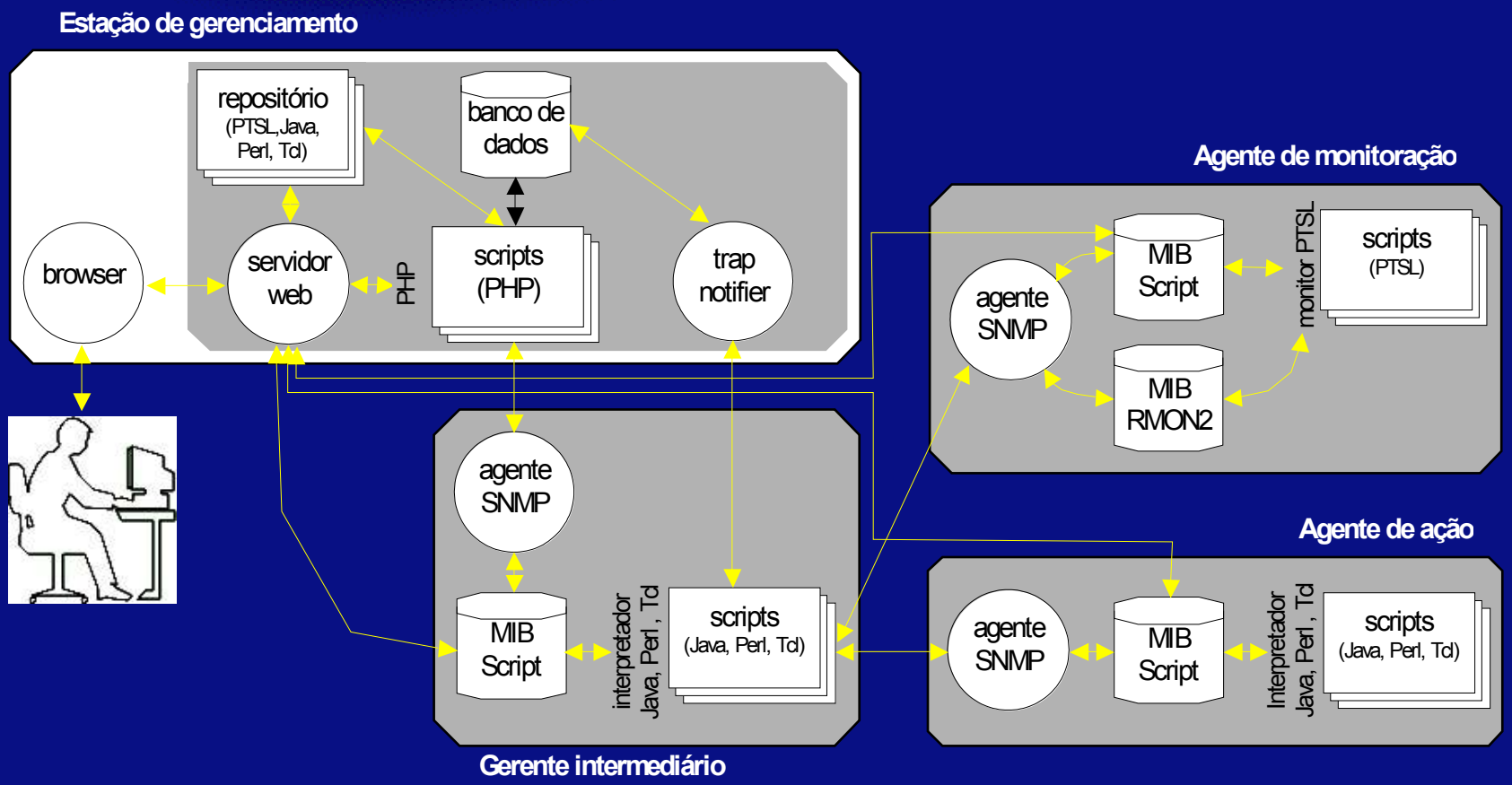
Gerenciamento de Redes

- MIBs (*Management Information Bases*) padrões
  - MIB II
    - Octetos/pacotes de entrada/saída
    - IP, ICMP, TCP, UDP, SNMP, …
  - RMON (*Remote Network Monitoring*)
  - RMON2
    - HTTP, SMTP, POP3, FTP, …
- Não existem MIBs específicas ligadas à detecção de intrusão

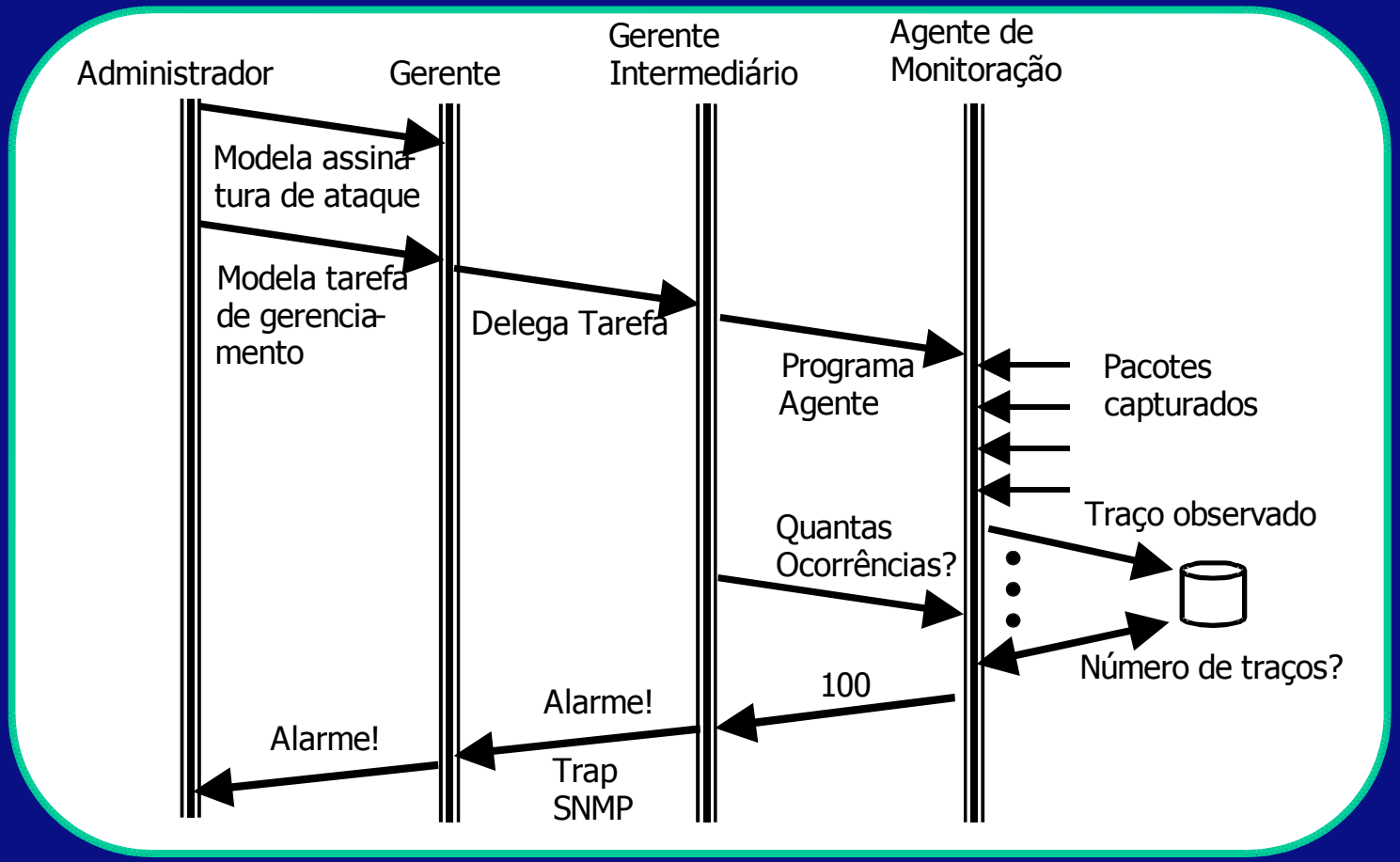
Arquitetura de Gerenciamento Trace

- A plataforma de gerenciamento Trace é uma estensão da infra-estrutura centralizada de gerenciamento SNMP
- Através de um modelo em 3 camadas, suporta o gerenciamento distribuído de protocolos de alto nível, serviços e aplicações de rede
- O agente SNMP para detecção de intrusão é uma extensão do agente de monitoração

Arquitetura de Gerenciamento Trace



Arquitetura de Gerenciamento Trace



O Agente de Monitoração

- É um agente SNMP
- Pode ser usado para realizar **detecção baseada em assinaturas de ataques e em anomalia de comportamento**
- Recebe especificação de ataques descritos em PTSL (*Protocol Trace Specification Language*)
- Monitora a ocorrência dos ataques descritos
- Atualiza uma MIB RMON2 estendida

A Linguagem PTSL

- A linguagem foi concebida para monitoração de protocolos de alto nível
- Possibilita a descrição de ataques através da construção de uma máquina de estados
  - Estados e transições entre o cliente e o servidor
  - Modelagem natural
  - Notação gráfica e textual
  - Maior granularidade do que considerar apenas pacotes da rede

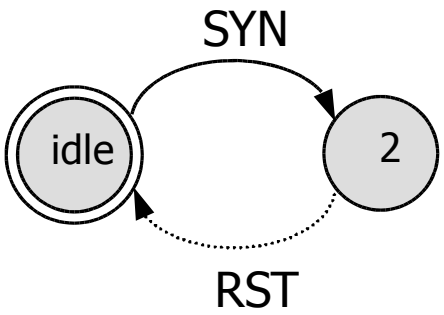
A Linguagem PTSL

- Alguns exemplos de cenários:
  - Varreduras de portas
  - Land
  - Sondagem de serviços RPC
  - Excesso de falhas de *login*

Varredura de Portas em PTSL

- Esta assinatura descreve a ocorrência de varredura de portas utilizando a técnica de envio de pacotes TCP com a flag SYN ligada e a respectiva resposta do alvo (TCP RST)

Trace "Varredura de Portas"

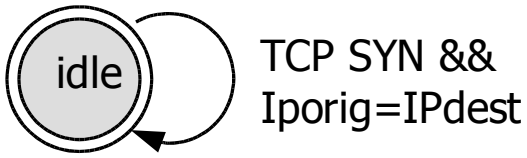


Version: 1.0
Description: Varredura de Portas por SYN/RST.
Key: varredura, portas, SYN, RST
Port:
Owner: Edgar Meneghetti
Last Update: Thu Jan 10 09:37:57 BRST 2002

Land em PTSL

- Assinatura que procura pacotes com endereços IP de origem e destino iguais
- Causava DoS em alguns sistemas operacionais mais antigos

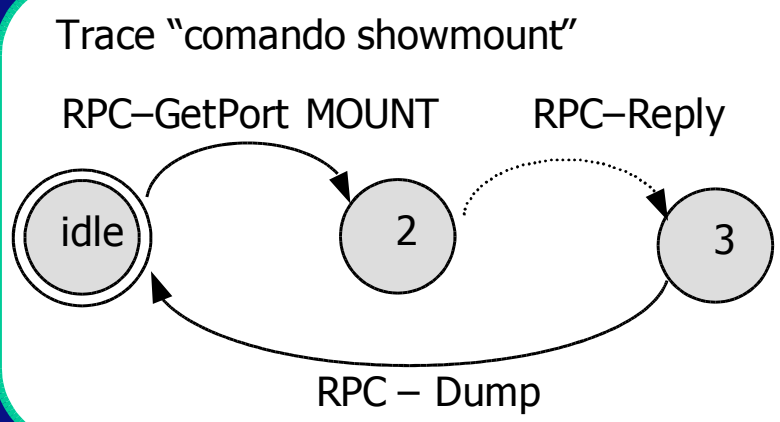
Trace "Ataque LAND"



Version: 1.0
Description: Ataque LAND.
Key: LAND,TCP, Windows
Port:
Owner: Edgar Meneghetti
Last Update: Thu Jan 10 09:37:57 BRST 2002

Sondagem de Serviços RPC em PTSL

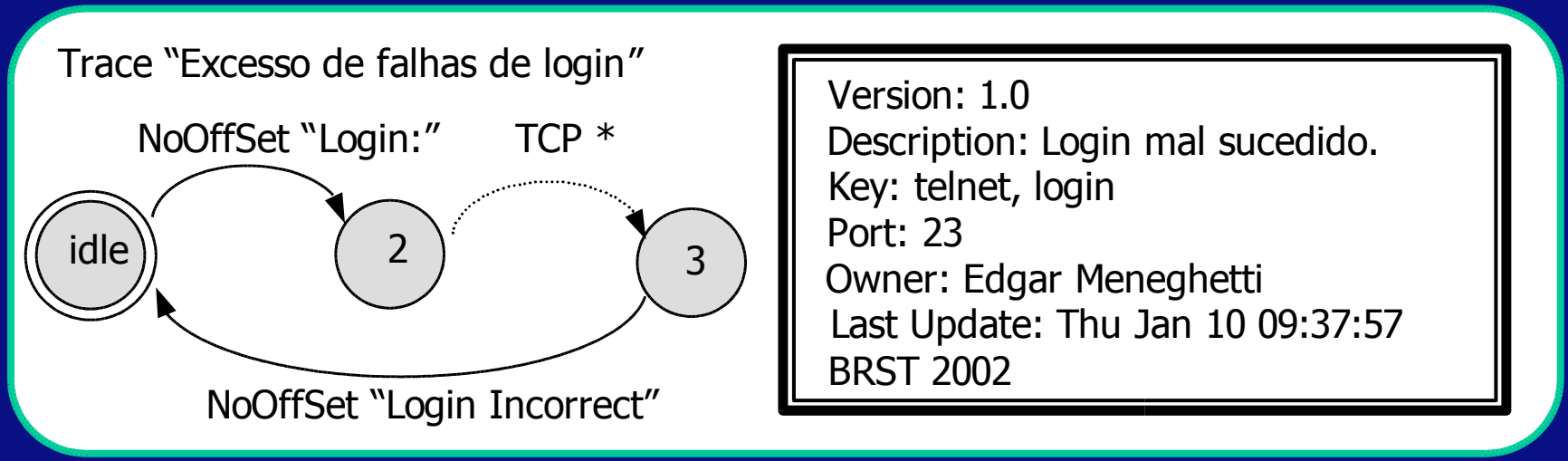
- Esta assinatura detecta o uso do comando “showmount”, que exibe os diretórios exportados por máquinas remotas



Version: 1.0
Descriptio n: Utilização do comando showmount.
Key: RPC, showmount.
Port:
Owner: Edgar Meneghetti
Last Update: Thu Jan 10 09:37:57

Excesso de Falhas de Login em PTSL

- Assinatura que evidencia tentativas de *login* mal sucedidas



Localização de Campos em PTSL

- BitCounter: localiza sequências de bits em um determinado encapsulamento e posição
  - BitCounter Ethernet 48 4 0010 "More Fragments"
- FieldCounter: localiza sequências de caracteres
  - FieldCounter Ethernet/IP/TCP 0 HTTP/1.1 "Versão do protocolo"
- NoOffSet: localiza sequências de caracteres em posição livre
  - NoOffSet Ethernet/IP/TCP /etc/passwd “Tentativa de ler senhas”

Especificação da máquina de estados

1 Version: 1.0

2 Description: Varredura de Portas por SYN/RST.

3 Key: varredura, portas, SYN, RST

4 Port:

5 Owner: Edgar Meneghetti

6 Last Update: Thu Jun 10 09:37:57 BRST 2003

7 MessagesSection

8 Message “SYN”

9 MessageType: client

10 // OffsetType Encapsulation FieldNumber Verb Description

11 BitCounter Ethernet/IP 110 1 0 “Campo SYN/TCP”

12 EndMessage

Especificação da máquina de estados

13 Message “RST”

14 MessageType: client

15 // OffsetType Encapsulation FieldNumber Verb Description

16 BitCounter Ethernet/IP 109 1 1 “Campo RST/TCP”

17 EndMessage

18 EndMessagesSection

Especificação da máquina de estados

19 StatesSection

20 FinalState idle

21 State idle

22 “SYN”' GotoState 2

23 EndState

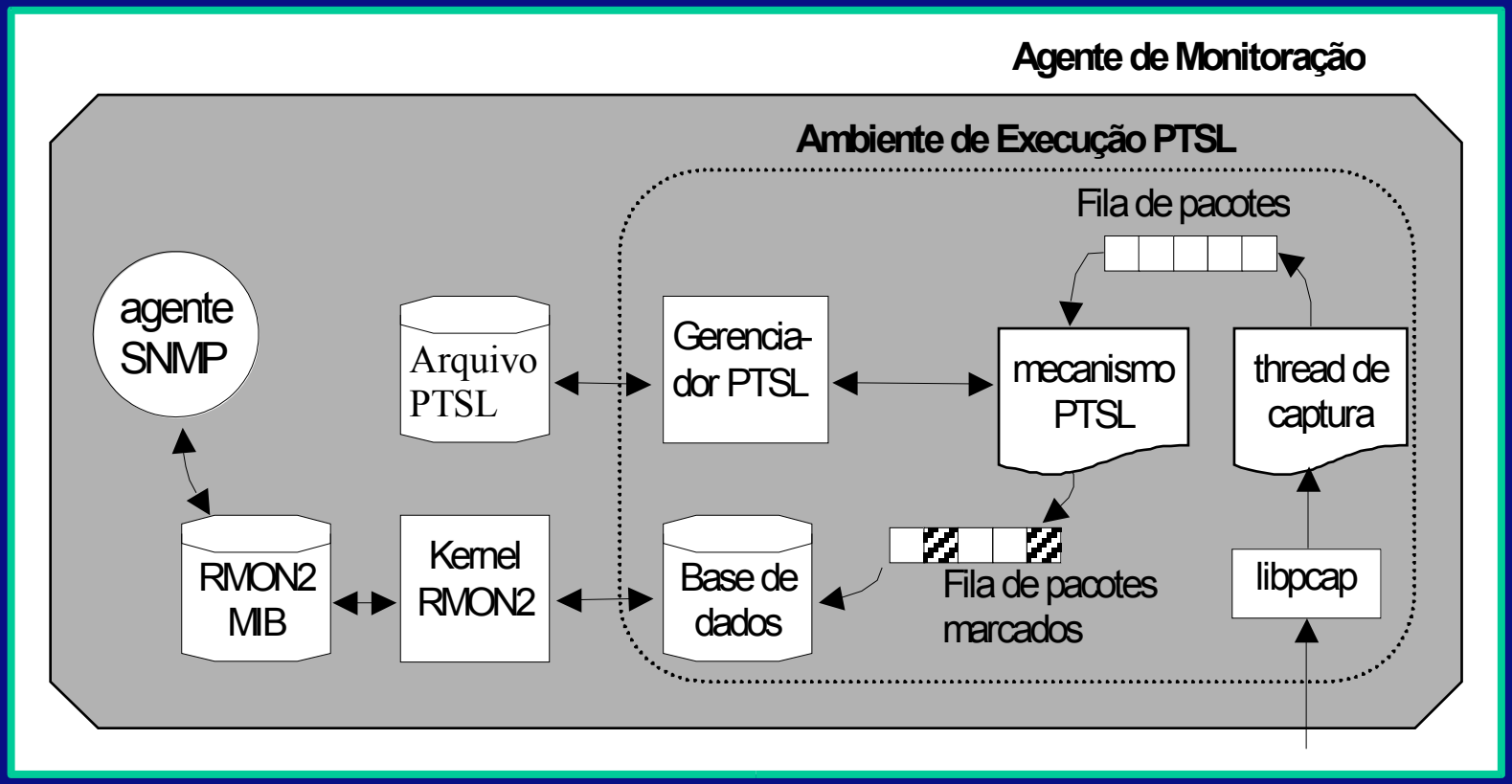
24 State 2

25 “RST” GotoState idle

26 EndState

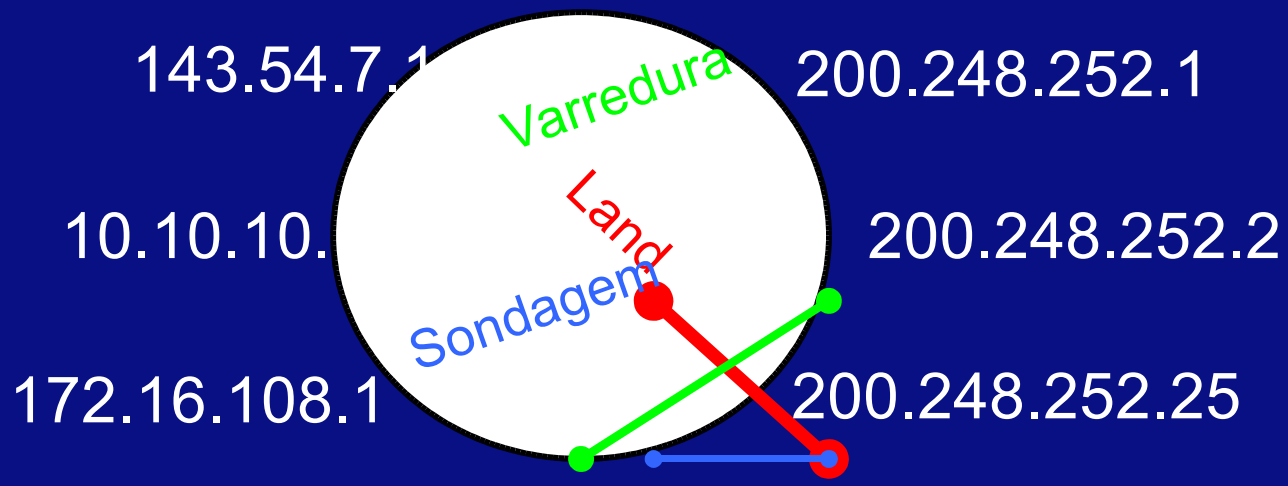
27 EndStatesSection

Arquitetura do Agente de Monitoração



Dados Armazenados pelo Agente

- A contagem de traços é feita de forma indireta, através da contagem de pacotes (*packets*) presentes em cada traço (para manter a semântica de RMON2)
  - Um traço com 3 estados ocorrido 5 vezes teria 15 pacotes contabilizados na MIB RMON2



Dados Armazenados pelo Agente

- Grupo ProtocolDir da MIB RMON2

ether2.ip

ether2.ip.tcp

ether2.ip.tcp.smtp

ether2.ip.varredura portas

ether2.ip.tcp.ataque serv IIS

Dados Armazenados pelo Agente

- Tabela alMatrixSD da MIB RMON2

Src Addr	Dst Addr	Protocol	Packets	Octets
125.120.10.200	172.16.108.25	Acesso invalido a servico TCP	250	53256
125.120.10.100	172.16.108.25	Acesso invalido a servico TCP	20	3204
172.16.108.1	172.16.108.2	Comportamento anomalo TCP	4	4350
172.16.108.32	172.16.108.2	Comando rpcinfo	8	7300

Validação do Agente

- Utilizando o cenário proposto pelo Lincoln Laboratory (MIT), foram realizadas comparações entre o agente de monitoração e o IDS Snort
- No tráfego de fundo foi incluído acessos legítimos ao serviço em ataque (sadmind, da SUN)
- O Snort apresentou muitos falsos positivos, ao passo que o agente de monitoração indicou apenas a ocorrência dos traços programados (do ataque)
  - http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index.html

Conclusões e Trabalhos Futuros

- Objetivos alcançados:
  - Baixo índice de falsos positivos e falsos negativos
  - Flexibilidade para descrever cenários de ataques
- O desempenho do agente ainda deve ser melhorado (em andamento)
- Geração de uma versão para distribuição (licença GPL)
- O agente RMON2 já está disponível para download

Informações para Contato

- Edgar Meneghetti
  eamenegh@ucs.br
- Luciano Paschoal Gaspary
  paschoal@exatas.unisinos.br

- Página do projeto Trace
  http://prav.unisinos.br/~trace/