Um Agente de Software Orientado à Monitoração de Traços de Protocolos

Ricardo Nabinger Sanchez
Ciência da Computação - bolsista renovado Pibic/CNPq
Luciano Paschoal Gaspary
Orientador

Universidade do Vale do Rio dos Sinos (UNISINOS)
Programa Interdisciplinar de Pós-Graduação em Computação Aplicada – PIPCA

Projeto Trace
http://mutuca.metropoa.tche.br

XVI Salão de Iniciação Científica – Outubro de 2004

Introdução

- Nos últimos anos a proliferação de protocolos e aplicações para redes de computadores fez com que um número expressivo de usuários as incorporasse em seu uso cotidiano
- Com isso, as ferramentas de medição de tráfego tornaram-se essenciais, sobretudo, para justificar os custos crescentes com a ampliação e manutenção da infraestrutura de rede
- As ferramentas para caracterização são especialmente importantes por detalharem os protocolos que compõem o tráfego de rede monitorado

Motivação

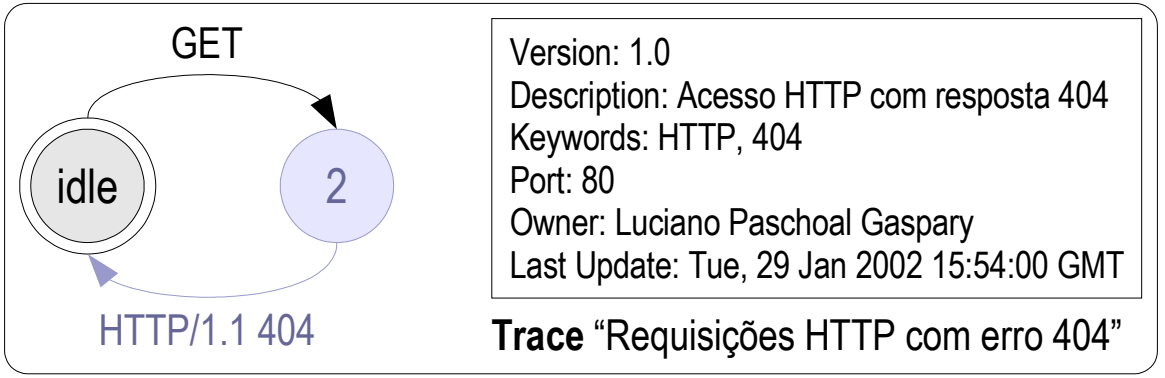
- Muitos dos problemas enfrentados atualmente em redes como falhas, baixo desempenho e insegurança, são originados no uso incorreto dos protocolos e nas implementações deficientes das aplicações
- A medição e caracterização do tráfego de rede não é mais suficiente para garantir o bom funcionamento dos protocolos e aplicações
- As ferramentas atualmente disponíveis (ntop, Snort, NeTraMet, ...) pecam em identificar eventos relacionados a falhas, desempenho e segurança
- A falta de padronização , frequentemente os administradores e gerentes de rede se vêem em meio a diversas ferramentas que não são facilmente integráveis entre si e com infra-estrutura já implantada

Alternativa Proposta

- Para amenizar esta problemática, está em desenvolvimento um agente de monitoração capaz de contabilizar seqüências de trocas de pacotes (**traços**), utilizando uma abordagem *stateful inspection*
- Essa abordagem permite identificar comportamentos de interesse para a gerência de falhas, desempenho e segurança de forma precisa, pois ao invés de avaliar os pacotes isoladamente, o agente correlaciona os pacotes pertencentes ao mesmo fluxo
- Por se tratar de uma extensão a um agente RMON2 (já desenvolvido pelo nosso grupo), as informações geradas pelo agente podem ser recuperadas a partir de qualquer plataforma de gerenciamento com suporte ao protocolo SNMP (*Simple Network Management Protocol*)

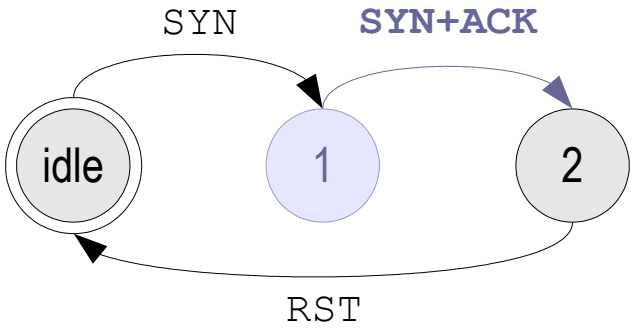
Modelando Traços de Protocolos

- A especificação dos traços de protocolos é feita utilizando a linguagem PTSL (*Protocol Trace Specification Language*), que possui uma notação gráfica, visando simplicidade e clareza, e também uma textual, onde é possível aproveitar todo o seu poder de expressão



Version: 1.0
Description: Acesso HTTP com resposta 404
Keywords: HTTP, 404
Port: 80
Owner: Luciano Paschoal Gaspary
Last Update: Tue, 29 Jan 2002 15:54:00 GMT

Trace "Requisições HTTP com erro 404"

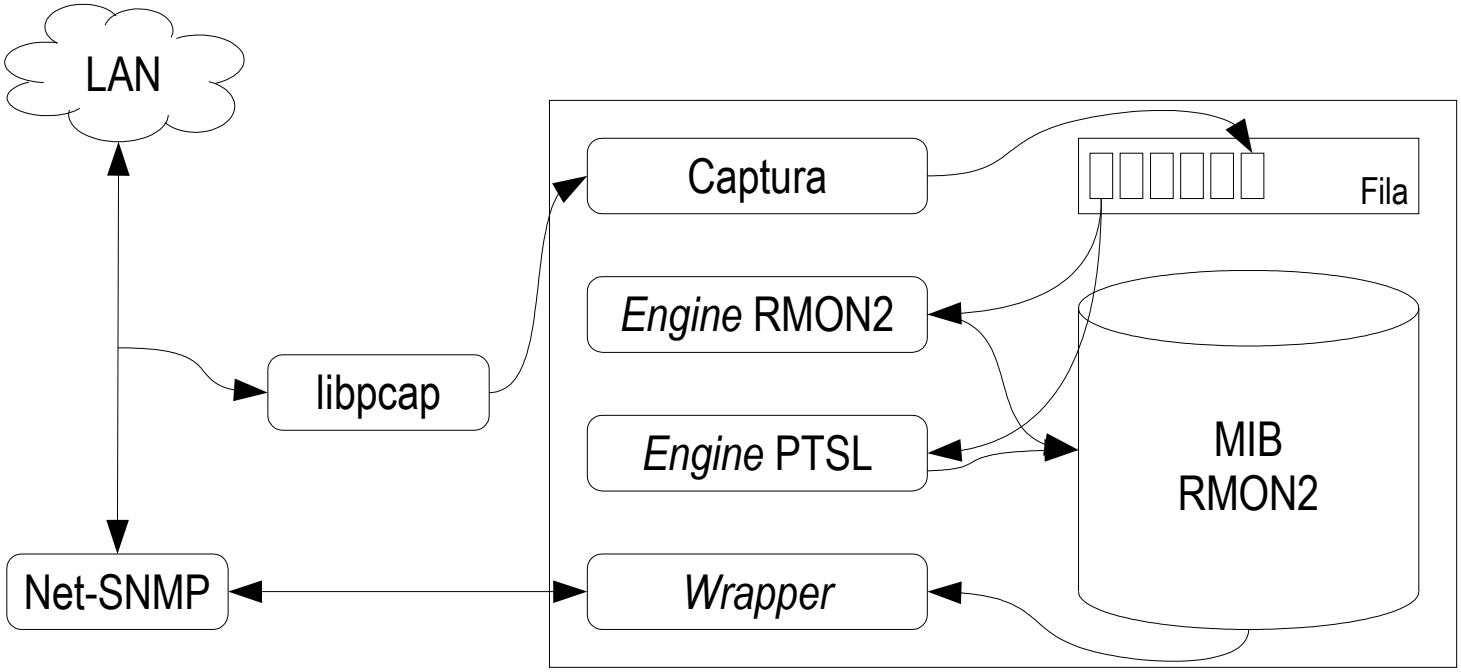


Version: 0.2
Description: *Portscan* usando 'nmap -sS'
Keywords: nmap, *portscan, stealth*
Port: *
Owner: Ricardo Nabinger Sanchez
Last Update: Sat, 29 May 2004 08:17:52 GMT

Trace "*Portscan stealth* do nmap"

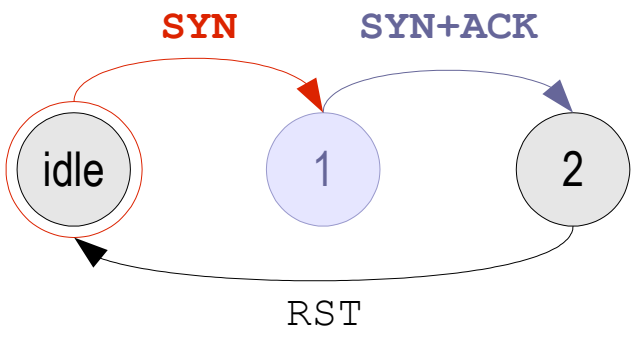
Arquitetura do Agente

- O agente é composto por módulos de **captura**, processamento de estatísticas **RMON2** e processamento de **traços de protocolos**
- O módulo *Wrapper* integra o agente ao Net-SNMP para que seja possível consultar a MIB RMON2 utilizando o protocolo SNMP



Funcionamento do Módulo PTSL

- Uma máquina cliente envia um pacote IPv4/TCP para um servidor (de qualquer aplicação), com a *flag* TCP SYN ativada
- O módulo PTSL testa os diversos traços de protocolos instalados, e verifica que houve uma evolução para um determinado traço
- Como o estado final do traço não foi atingido, o módulo armazena uma instância do traço aberto que pode ser identificado dependendo dos próximos pacotes capturados

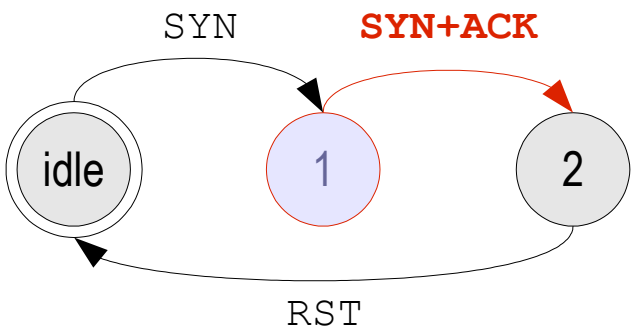


Version: 0.2
Description: *Portscan* usando 'nmap -sS'
Keywords: nmap, *portscan, stealth*
Port: *
Owner: Ricardo Nabinger Sanchez
Last Update: Sat, 29 May 2004 08:17:52 GMT

Trace "*Portscan stealth* do nmap"

Funcionamento do Módulo PTSL

- O servidor responde ao pacote inicial do cliente com outro pacote, mas desta vez com as *flags* TCP SYN e ACK ativadas
- O módulo PTSL identifica que para esse par cliente-servidor já existe uma instância de traço aberta
- Ao testar a segunda mensagem do traço, o módulo verifica que o traço evoluiu para o próximo estado, mas este não é final, então ele mantém a mesma instância do traço aberta

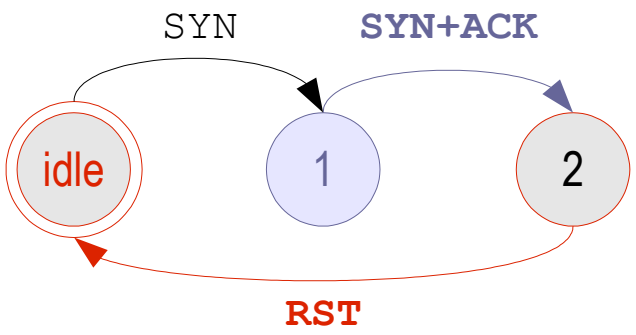


Version: 0.2
Description: *Portscan* usando 'nmap -sS'
Keywords: nmap, *portscan, stealth*
Port: *
Owner: Ricardo Nabinger Sanchez
Last Update: Sat, 29 May 2004 08:17:52 GMT

Trace "*Portscan stealth* do nmap"

Funcionamento do Módulo PTSL

- O cliente então envia um pacote com a *flag* TCP RST ativada
- Novamente, o módulo PTSL verifica que para esse par cliente-servidor já existe um traço em andamento
- Ao verificar que a última mensagem foi encontrada e o traço evoluiu completamente, o número de ocorrências **com sucesso** é atualizado na MIB RMON2
- Se o traço não finalizasse, ainda assim o módulo atualizaria a MIB RMON2, desta vez incrementando o número de ocorrências **sem sucesso**



Version: 0.2
Description: *Portscan* usando 'nmap -sS'
Keywords: nmap, *portscan, stealth*
Port: *
Owner: Ricardo Nabinger Sanchez
Last Update: Sat, 29 May 2004 08:17:52 GMT

Trace "*Portscan stealth* do nmap"

Conclusões e Trabalhos Futuros

- **Conclusões**
  - Por utilizar uma abordagem *stateful inspection*, a ferramenta se mostra bastante eficaz no contexto de segurança de redes, por ser capaz de identificar cenários complexos com grande precisão
- **Trabalhos Futuros**
  - Concluir a implementação, que já se encontra em fase de testes em ambiente controlado
  - Investigar outros cenários de aplicação da ferramenta
  - Monitoração em ambientes reais

Publicações

- **XIV Salão de Iniciação Científica, UFRGS**
  - Aumentando a Sustentabilidade de Monitoração de um Agente RMON2 a partir da Utilização de Tabelas Hash em Memória
- **Mostra de Iniciação Científica 2003, UNISINOS**
  - Aumentando a Sustentabilidade de Monitoração de um Agente RMON2 a partir da Utilização de Tabelas Hash em Memória
- **IEEE Latin American Network Operations and Management Symposium 2003 (LANOMS'2003)**
  - On the Development of IETF Monitoring MIBs for High Speed Networks
- Submetido ao **IEEE Journal on Selected Areas in Communications**
  - ID-Trace: An SNMP-based Platform for Distributed Stateful Intrusion Detection

Muito Obrigado!

Perguntas?

- Ricardo Nabinger Sanchez
  rnsanchez@cscience.org
- Luciano Paschoal Gaspary
  paschoal@exatas.unisinos.br

http://mutuca.metropoa.tche.br

TRACE Management Platform

UNISINOS

CNPq