UM AGENTE DE SOFTWARE ORIENTADO À MONITORAÇÃO DE TRAÇOS DE PROTOCOLOS

Universidade do Vale do Rio dos Sinos – UNISINOS
Centro de Ciências Exatas e Tecnológicas

Ricardo Nabinger Sanchez (bolsista) – rsanchez@exatas.unisinos.br
Luciano Paschoal Gaspary (orientador) – paschoal@exatas.unisinos.br

Por que monitorar traços de protocolos?

Atualmente, 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. 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 de forma isolada, o agente correlaciona pacotes que pertençam a um mesmo fluxo de comunicação.

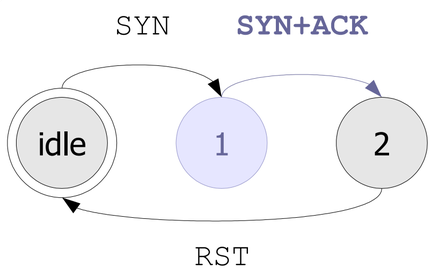
Objetivo Principal

Implementação de um agente de monitoração de acordo com os padrões propostos pelo IETF. Por se tratar de uma extensão a um agente RMON2 já desenvolvido, as informações geradas pelo agente podem ser recuperadas a partir de qualquer plataforma de gerenciamento com suporte ao protocolo SNMP.

Modelagem dos Traços de Protocolos

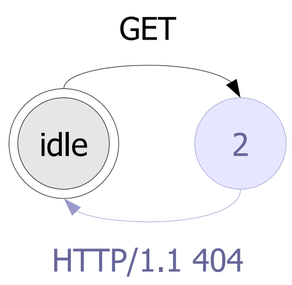
Os traços de protocolos são modelados utilizando a linguagem PTSL ("Protocol Trace Specification Language"), que possui tanto uma notação gráfica quanto textual. A diferença das notações reside no poder de expressão de cada uma delas, sendo que na textual pode-se aproveitar todo poder de expressão da linguagem.

Exemplos de Traços Modelados Usando a Linguagem PTSL



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"



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 "Requisição HTTP com erro 404"

```
Trace "Portscan stealth do nmap"
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

MessagesSection
  Message "SYN"
    MessageType: client
    BitCounter Ethernet/IP/TCP 110 1 1 "Flag SYN"
  EndMessage
  Message "SYN+ACK"
    MessageType: server
    BitCounter Ethernet/IP/TCP 107 1 1 "Flag ACK"
    BitCounter Ethernet/IP/TCP 110 1 1 "Flag SYN"
  EndMessage
  Message "RST"
    MessageType: client
    BitCounter Ethernet/IP/TCP 109 1 1 "Flag RST"
  EndMessage
EndMessagesSection
StatesSection
  FinalState idle
  State idle
    "SYN" GotoState 1
  EndState
  State 1
    "SYN+ACK" GotoState 2
  EndState
  State 2
    "RST" GotoState idle
  EndState

EndTrace
```

```
Trace "Requisição HTTP com erro 404"
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

MessagesSection
  Message "GET"
    MessageType: client
    FieldCounter Ethernet/IP/TCP/http
        0 GET "Requisição GET"
  EndMessage

  Message "404"
    MessageType: server
    FieldCounter Ethernet/IP/TCP/http
        1 404 "Resposta 404"
  EndMessage
EndMessagesSection

StatesSection
  State idle
    "GET" GotoState 1
  EndState

  State 1
    "404" GotoState idle
  EndState
EndTrace
```

http://mutuca.metropoa.tche.br

http://www.unisinos.br

http://www.cnpq.br