GT-CIRD
Caracterização e identificação remota de dispositivos

EQUIPE

Coordenador
João Paulo de Souza Medeiros

Coordenadores-adjuntos
Agostinho de Medeiros Brito Júnior
Antonio Alfredo Ferreira Loureiro
Rommel Wladmir Lima

Assistentes
João Batista Borges Neto
Paulo Sérgio da Motta Pires
Mizael Clistion Souza Elias
Sebastião Emidio Alves Filho

Alunos
Maycon Jebson Dantas
Alex Medeiros de Araújo

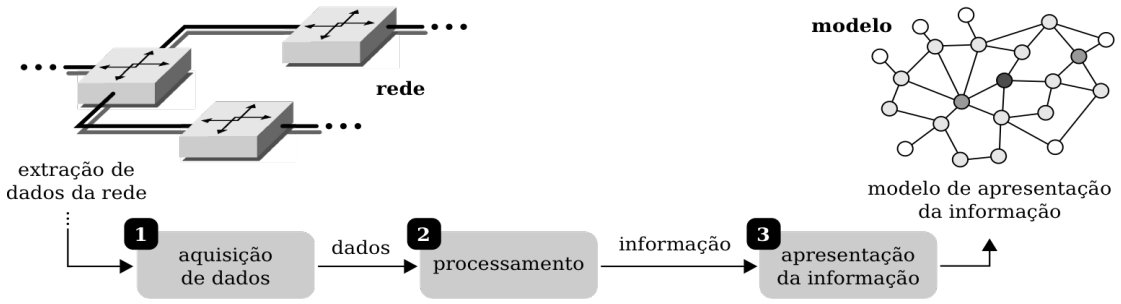
Parceiros
Universidade Federal do Rio Grande do Norte (UFRN)
Universidade Federal de Minas Gerais (UFMG)
Universidade do Estado do Rio Grande do Norte (UERN)

SITE
http://labepi.ufrn.br/project/cird/

CONTATO
pd@rnp.br

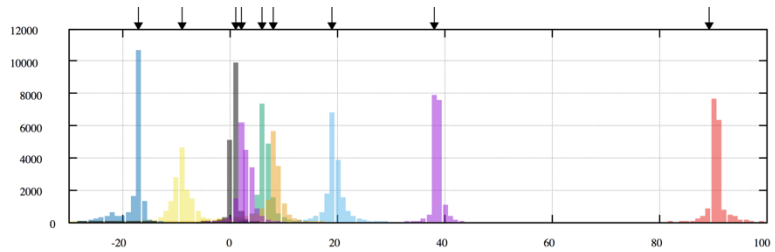
DESCRIÇÃO

O processo de caracterização e identificação de computadores possui aplicações em segurança da informação e na análise forense em redes de computadores. Um exemplo é a sua utilização em conjunto com sistemas de detecção de intrusão para caracterizar máquinas utilizadas em ataques de rede. A caracterização de dispositivos remotos é baseada na análise de dados de rede gerados pela máquina de origem e a abordagem clássica é a de explorar características peculiares das diferentes implementações dos protocolos em cada camada da pilha de protocolos. O uso de inteligência computacional pode melhorar o desempenho da identificação, principalmente, quando comparado com métodos e ferramentas clássicas. Esse projeto tem como objetivo a criação de um sistema de caracterização e classificação de assinaturas digitais para identificação de dispositivos. O processo de captura, extração e apresentação dos dados utilizados pela plataforma proposta é ilustrada na figura abaixo.



Informações como portas abertas e a rota dos pacotes são as primeiras informações extraídas pelas ferramentas. Essas informações são utilizadas em capturas subsequentes.

Uma das principais informações extraídas e apresentadas pela ferramenta é o atraso do relógio da máquina remota em relação ao da máquina que realiza a captura. A figura abaixo ilustra o resultado de um experimento feito com nove (9) máquinas.



Na figura acima, é possível verificar o atraso na unidade de microssegundos por segundo. Por exemplo, a máquina com atraso representado mais à direita, teve pacotes TCP *Timestamp* capturados e, após uma etapa de caracterização, verificou-se que seu relógio se adianta 90 microssegundos por segundo, em relação ao relógio de quem realizou a captura.

Com outros dados da camada de rede e transporte, foi possível identificar o sistema operacional da máquina remota. Isso foi possível mesmo quando a máquina remota estava sob condições em que outras ferramentas não são eficazes (e.g. utilização de NAT, PAT ou *Firewall*).

Para a camada de aplicação, foram desenvolvidas ferramentas para coletar dados de serviços que utilizam os protocolos DNS, FTP, HTTP e SSH. Para cada um dos protocolos, foram extraídas as seguintes informações:

- DNS: tabela de informações de mapeamento entre nomes e endereços;
- FTP: lista com a relação de comandos implementados pelo servidor e sua estrutura de diretórios, caso o usuário anônimo esteja habilitado;
- HTTP: grafo que representa a ligação entre as páginas e arquivos internos do servidor, além dos dados relacionados ao serviço;
- SSH: lista de chaves públicas e informações da aplicação que gerencia o serviço.

Na figura ao lado, é ilustrada a arquitetura do protótipo para captura e verificação de evidências.