18º WRNP
Workshop RNP

15 | 16 MAIO
Belém | PA

# GT-CIRD
# Caracterização e Identificação Remota de Dispositivos


**EQUIPE**

**Coordenador**
João Paulo de Souza Medeiros
*Universidade Federal do Rio Grande do Norte (DCT/UFRN)*

**Coordenador Adjunto**
Agostinho de Medeiros Brito Júnior
*Universidade Federal do Rio Grande do Norte (DCA/UFRN)*
Antonio Alfredo Ferreira Loureiro
*Universidade Federal de Minas Gerais (DCC/UFMG)*
Rommel Wladmir Lima
*Universidade do Estado do Rio Grande do Norte (DI/UERN)*

**Assistente**
Paulo Sérgio Motta Pires
*Universidade Federal do Rio Grande do Norte (DCA/UFRN)*
João Batista Borges Neto
*Universidade Federal de Minas Gerais (DCC/UFMG)*


**PARCEIROS**
- Universidade Federal de Minas Gerais (UFMG)
- Universidade do Estado do Rio Grande do Norte (UERN)

**SITE**
labepi.ufrn.br


**CONTATO**
jpsm@dct.ufrn.br


## Descrição

O processo de caracterização e identificação de computadores possui várias aplicações em segurança da informação. Na análise forense em redes de computadores, por exemplo, tal processo pode ser usado em conjunto com sistemas de detecção de intrusão para caracterizar máquinas utilizadas em ataques de rede (e.g., negação de serviço). 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 (enlace, rede, transporte e aplicação). Em trabalhos recentes é demostrado que o uso de inteligência computacional pode melhorar o desempenho de identificação quando comparado a métodos e ferramentas clássicas. Este projeto tem como objetivo a criação de um sistema de caracterização e classificação de assinaturas digitais para identificação de dispositivos. A utilização da plataforma proposta é ilustrada na Figura 1.

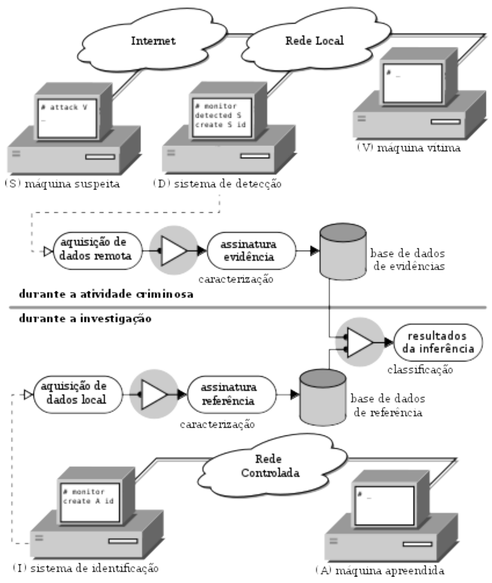


**Figura 1:** Proposta de sistema de caracterização e classificação de assinaturas digitais para identificação de dispositivos.

O desafio está em tornar possível a identificação de impressões digitais de dispositivos em rede e criar representações singulares por meio de um processo de caracterização eficaz. Propõe-se a utilização de classificadores especializados para serviços, sistemas operacionais e dispositivos da máquina que possuem características semelhantes. Isso pode ser feito projetando um classificador para cada grupo de Impressões digitais similares. Esse conceito de agrupamento é exemplificado na Figura 2 utilizando impressões digitais de diferentes sistemas operacionais. Com base em grupos definidos por alguma medida de similaridade, uma evidência pode ser classificada utilizando o algoritmo mais adequado. Esse processo de classificação guiada por agrupamento é ilustrado na Figura 3.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| IOS | IOS | IOS | SonicOS | AIX | FreeBSD | Mac OS | Mac OS | FreeBSD | FreeBSD |
| IOS | IOS | QNX | SonicOS | FreeBSD | FreeBSD | FreeBSD | FreeBSD | FreeBSD | FreeBSD |
| IOS | IOS | QNX | SCO OS | BSD/OS | IRIX | IRIX | FreeBSD | FreeBSD | HP-UX |
| Windows | Windows | NetBSD | NetBSD | NetBSD | OpenBSD | OpenBSD | OpenBSD | Solaris | Solaris |
| Windows | Windows | IBM OS | IBM OS | Minix | OpenBSD | Linux | OpenBSD | Solaris | Solaris |
| Windows | Windows | IBM OS | IBM OS | NetWare | Linux | Linux | Linux | Linux | Solaris |
| Windows | Windows | Windows | Windows | Linux | Linux | Linux | Linux | Linux | Linux |
| Windows | Windows | Windows | Linux | Linux | Linux | Linux | Linux | Linux | Linux |
| Windows | Windows | Windows | Linux | Linux | Linux | Linux | Linux | Linux | Linux |
| Windows | Windows | Symbian | Linux | Linux | Linux | Linux | Linux | Linux | Linux |

**Figura 2:** Exemplo de agrupamento com base no sistema operacional

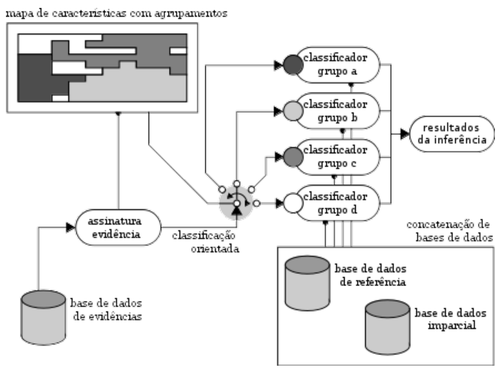


**Figura 3:** Proposta de sistema composto de classificação de assinaturas guiada por agrupamento.

A proposta é utilizar os diferentes métodos de caracterização presentes na literatura, e criar classificadores especialistas a fim de maximizar a possibilidade de criação de impressões digitais singulares. Em adição, deve-se considerar ativos da rede que possam influenciar na validade dos dados capturados, como por exemplo: Network Address Translation (NAT), firewalls e protocol scrubbers.

Para avaliação do protótipo, será utilizado um ambiente similar ao apresentado na Figura 1. Demonstrada a viabilidade técnica do protótipo, planeja-se em uma segunda fase do projeto a criação de um serviço de caracterização, classificação e armazenamento de assinaturas.

RNP MINISTÉRIO DA DEFESA MINISTÉRIO DA CULTURA MINISTÉRIO DA SAÚDE MINISTÉRIO DA EDUCAÇÃO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES BRASIL GOVERNO FEDERAL