18º WRNP
Workshop RNP
15 | 16 MAIO
Belém | PA

GT-CIRD

Caracterização e Identificação Remota de Dispositivos

João Paulo de Souza Medeiros (coordenador, DCT/UFRN) <jpsm@dct.ufrn.br>
Agostinho de Medeiros Brito Júnior (c. adjunto, DCA/UFRN)
Antonio Alfredo Ferreira Loureiro (c. adjunto, DCC/UFMG)
Rommel Wladimir de Lima (c. adjunto, DI/UERN)

VISÃO GERAL

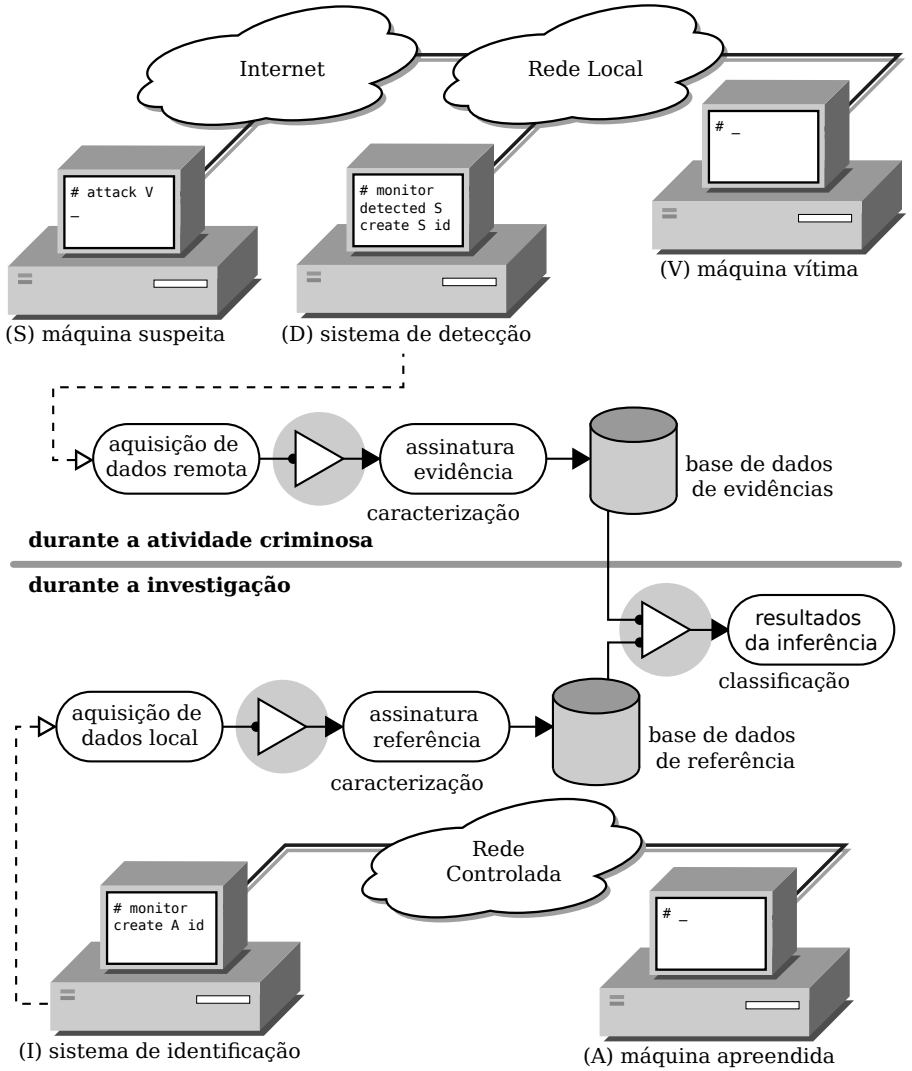
Caracterização: busca por características que possam ser utilizadas para representar (*fingerprint*) de forma eficaz algum componente (físico ou lógico) de uma máquina remota. Exemplos:

- Rede: Opções do cabeçalho IP e ICMP Timestamp;
- Transporte: Opções do cabeçalho TCP, TCP ISN (PRNG) e Timestamp; e
- Aplicação: Banner grabbing, Estrutura de Arquivos (FTP) e Grafo de Hyperlinks (HTTP).

Identificação: utilização de métricas e métodos de comparação de assinaturas (*fingerprint*) com o objetivo de classificar de forma singular máquinas remotas. Exemplos:

- Regressão linear e distância angular;
- Espaço de fase e distância entre conjunto de pontos; e
- Árvores/grafos e distância entre grafos.

Objetivo: criação de assinaturas (*fingerprint*), potencialmente singulares, de máquinas remotas utilizadas em ataques virtuais e demais atividades criminosas.

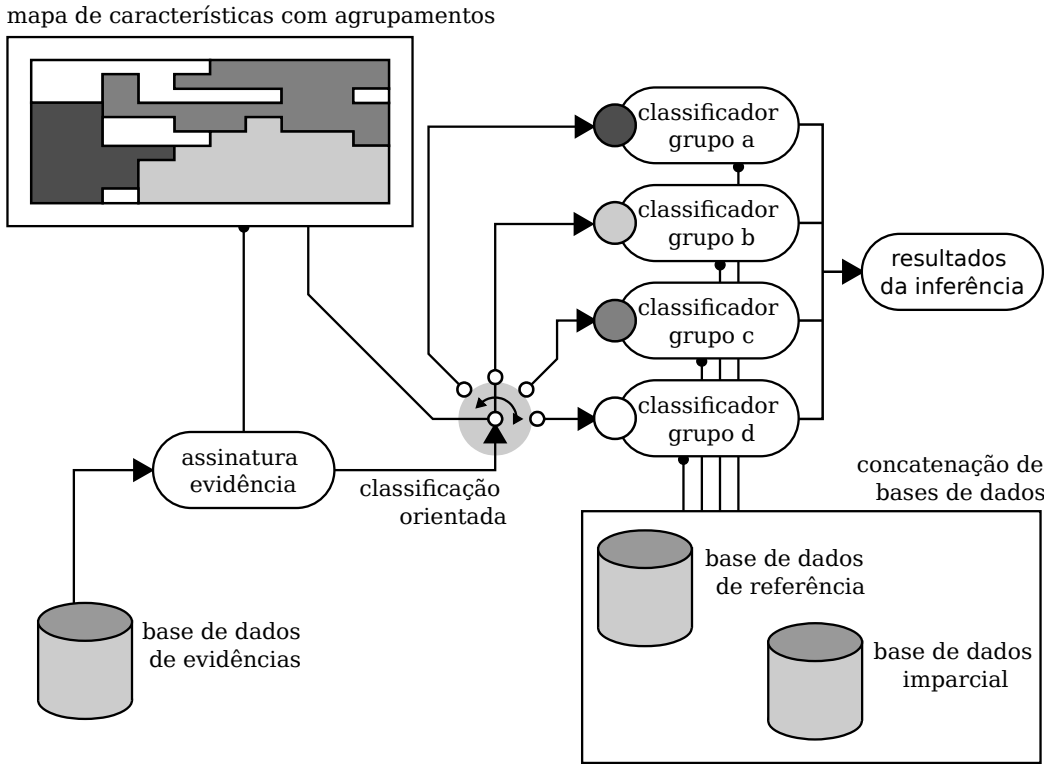


NOSSA ABORDAGEM

Caracterização: utilização de algoritmos de mineração de dados, extração de cararacaterísticas e aprendizado de máquina, com o objetivo de identificar dados que possam tornar a criação de uma assinatura (*fingerprint*) potencialmente singular.

Identificação: utilização de algoritmos e técnicas de aprendizado de máquina para criação de classificadores especializados. Exemplo: projeto de classificadores especializados em discriminar assinaturas (*fingerprint*) de máquinas com implementação similar da pilha TCP/IP do sistema operacional.

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



Objetivo: criação de assinaturas (*fingerprint*) e classificadores para cada uma das camadas (rede, transporte e aplicação) e para dados potencialmente singulares (e.g. desvio de relógio) identificados em cada uma delas.