# Detecção de Intrusão mediante Sistemas Imunológicos Artificiais

**Gustavo dos Santos Vieira, Renato B. Machado, Cristiano A. de Souza**

Laboratório de Pesquisa em Segurança Computacional – LaPSeC,
Universidade Estadual do Oeste do Paraná – Campus Foz do Iguaçu

{guustavov, renatobobsin, cristianoantonio.souza10}@gmail.com

## Objetivos

Entre as diversas aplicabilidades de Sistemas Imunológicos Artificiais (SIA), a sua utilização na área de detecção de intrusão tem se mostrado uma abordagem promissora (MACHADO, 2005). Deste modo, o objetivo deste trabalho é definir a arquitetura de um Sistema de Detecção de Intrusão (SDI) baseado em SIA utilizando métodos de Inteligência Artificial (IA) em sua "caixa de análise" para *Cloud Computing*.

## Métodos e Procedimentos

O SDI proposto baseia-se na padronização *Common Intrusion Detection Framework* (STANIFORD-CHEN et al., 1998), apresentando quatro componentes principais: geradores de eventos, analisadores de eventos (caixa de análise), base de dados de eventos e unidades de contramedida. Neste modelo, além das estratégias comumente adotadas na "caixa de análise" considerando padrões de ataques já conhecidos (assinaturas), propõe-se a inclusão de métodos tradicionais de IA, por meio de implementações disponíveis na aplicação WEKA[1]. Deste modo, o método de inteligência do SDI baseado em SIA (MACHADO, 2005) será adequado, visando abranger a detecção de variações dos ataques conhecidos. Os métodos de IA a serem avaliados serão Redes Neurais Artificiais (RNA) e K-*Nearest Neighbor* (KNN), aplicando a base de assinaturas do SDI Snort[2] para suas calibrações.

Para mensurar a eficiência das abordagens em análise, serão utilizados ataques clássicos de *Cloud Computing* por meio das ferramentas LOIC[3], Scapy[4], Iperf[5] e Netsniff-ng[6]. Por fim os métodos serão submetidos à avaliação estatística, considerando os índices de acertos, falsos positivos e falsos negativos, utilizando-se o ambiente computacional e matemático R[7].

## Resultados

Como resultados, mediante estudo da literatura e reuniões com especialistas, obteve-se o delineamento do modelo arquitetural, experimental e de dados de um SDI baseado em SIA, nos quais a classificação dos eventos monitorados é realizada com o auxílio de métodos de IA.

## Conclusões

A utilização de SIA na detecção de intrusão em redes de computadores é crescente, porém apresenta algumas limitações. Sendo assim, conclui-se que há carência de trabalhos que visem minimizar tais deficiências por meio de novas abordagens. Deste modo, a incorporação de métodos de IA é promissora e as experimentações a serem realizadas caracterizam importantes contribuições.

## Referências Bibliográficas

MACHADO, R. B. Uma abordagem de detecção de intrusão baseada em sistemas imunológicos artificiais e agentes móveis. Universidade Federal de Santa Catarina, 2005.

KAHN, C. Common Intrusion Detection Framework (CIDF). 1998. Acessado em 08/08/2016. Disponível em: < http://gost.isi.edu/cidf/>

[1] http://www.cs.waikato.ac.nz/ml/weka/
[2] https://www.snort.org/
[3] http://loic.sourceforge.net/
[4] http://www.secdev.org/projects/scapy/
[5] https://iperf.fr/
[6] http://netsniff-ng.org/
[7] https://www.r-project.org/