Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Computação Inteligente

Título: Aplicação de Inteligência Artificial Auto explicável na Detecção de *Malware* em *Smartphones*

Orientador – Sidney Marlon Lopes de Lima (sidney.lima@ufpe.br)

Descrição:

A massificação de dispositivos móveis, associada à ampla disponibilidade de aplicativos, transformou o ambiente *Android* em um grande alvo para ciber-criminosos. Conforme identificado por Bai et al. (2020), *malwares* para *Android*, especialmente *trojans* bancários, têm adotado comportamentos cada vez mais sofisticados e adaptativos, explorando permissões sensíveis e interações legítimas com a API do sistema. Embora antivírus tradicionais ainda sejam amplamente utilizados, estudos como o de Lima et al. (2023) evidenciam que essas ferramentas falham em detectar ameaças modernas como ataques *fileless* e variantes polimórficas, que frequentemente escapam dos métodos baseados em assinatura. Adicionalmente, pesquisas como as de Zhang et al. (2021) e Pimenta et al. (2024) destacam que a eficácia de modelos baseados em *Deep Learning* pode ser ampliada quando se explora a estrutura e o comportamento do *malware* em múltiplas dimensões; inclui-se análise estática, dinâmica e agrupamento por famílias. O projeto proposto tem como objetivos desenvolver um modelo autoexplicável de aprendizado baseado em redes neurais ou técnicas híbridas com mecanismos de interpretabilidade. Nesse contexto, a técnica de *Transfer Learning* surge como uma solução promissora, permitindo o reaproveitamento de modelos de *Deep Learning* previamente treinados em grandes bases de dados para tarefas relacionadas, como a classificação de *malwares*. Conforme demonstrado por Prima et al. (2020), modelos originalmente treinados para reconhecimento de imagens, podem ser adaptados com sucesso para a classificação de *malware*. A expectativa é que a incorporação de *Transfer Learning* no pipeline de detecção fortaleça a justificativa para um modelo mais eficiente e escalável, alinhado às melhores práticas recentes da literatura.

Materiais e Habilidades necessárias

- Familiaridade com técnicas de redes neurais artificiais visando reconhecimento de padrão.
- Conhecimentos sólidos nas linguagens Python e Matlab.
- Ao menos um HD externo particular com capacidade mínima de 1 TB.

Referências Bibliográficas

BAI, Chongyang; HAN, Qian; *et al*. DBank: Predictive Behavioral Analysis of Recent Android Banking Trojans. IEEE Transactions on Dependable and Secure Computing, [S. l.], 2020. https://doi.org/10.1109/TDSC.2020.3000797.

Lima, S.M.L., Silva, S.H.M.T., Pinheiro, R.P. *et al.* Next-generation antivirus endowed with web-server Sandbox applied to audit fileless attack. Soft Computing 27, 1471–1491 (2023). https://doi.org/10.1007/s00500-022-07447-4

Zhang, N., Tan, Y.-a., Yang, C., Li, Y. (2021). Deep learning feature exploration for Android malware detection. Applied Soft Computing Journal, 102, 107069.

https://doi.org/10.1016/j.asoc.2020.107069.

Pimenta, T.S.R., Ceschin, F. Gregio, A. 2024. ANDROIDGYNY: Reviewing Clustering Techniques for Android Malware Family Classification. Digit. Threat. Res. Pract. 5, 1, Article 3 (March 2024), 35 pages. https://doi.org/10.1145/3587471.

PRIMA, B. BOUHORMA, M. Transfer learning for malware detection using pretrained convolutional neural networks. Journal of Computer Virology and Hacking Techniques, v. 18, p. 273–287, 2022. https://doi.org/10.1016/j.asoc.2020.107069.