https://www.uni-koblenz.de/de/informatik/iwvi/mauthe
Research Group IT- und Datensicherheit

Bachelor Thesis

Comparative Analysis of Malware-to-Image Algorithms for Malware Image Classification Focusing on Instruction Relevance

Description:

The cornerstone of traditional malware detection has been the signature-based approach, which compares byte sequences extracted from malware binaries. However, it struggles to detect unknown polymorphic and metamorphic malware, which constantly change their appearance.

To overcome these limitations, machine learning techniques, especially artificial neural networks, have been adapted for dynamic and adaptive malware detection. Convolutional Neural Networks (CNNs) have shown promising results in classifying malware represented as grayscale images. In this approach, 8-bit vectors extracted from raw malware binaries are transformed into grayscale values that capture structural characteristics of the malware.

While successful in many cases, the underlying conversion algorithms - how raw binaries are mapped to image representations - are not always well-documented. This leaves a gap in understanding how specific instructions or parts of the malware corpus may be omitted or abstracted during the transformation, potentially influencing classification accuracy.

The goal of this thesis is to experiment with different conversion algorithms, aiming to assess their impact on common classification metrics (precision, recall, and F1-score). Specifically, the thesis shall explore whether the exclusion of more or less common instructions can improve the model's ability to generalize. The thesis will involve a comprehensive opcode / byte / instruction analysis, followed by the application of CNNs, but also standard classifiers such as Random Forest, to evaluate the resulting image datasets.

Research questions:

- How do different image conversion schemes impact the final classification metrics?
- Is it beneficial to omit certain instructions or encode them differently to enhance the generalization ability of CNNs or the respective machine learning system?
- Optional: Small literature review on existing frameworks / approaches and visualizations

Recommended:

- Proficiency in working with Python and Deep Learning Frameworks (pytorch, tensorflow) or at least interest in familiarizing oneself with Deep Learning frameworks, techniques and algorithms

Contact: Alexander Rosenbaum, M. Sc. (arosenbaum@uni-koblenz.de)

Literature:

- Yang, H., Zhang, Y., Zhang, L., & Cheng, X. (2022). Malware detection based on visualization of recombined API instruction sequence. *Connection Science*, *34*(1), 2630–2651. https://doi.org/10.1080/09540091.2022.2139353
- Bensaoud, A., & Kalita, J. (2024). CNN-LSTM and transfer learning models for malware classification based on opcodes and API calls. *Knowledge-Based Systems*, *290*, 111543.
- O'kane, P., Sezer, S. & McLaughlin, K. Detecting obfuscated malware using reduced opcode set and optimised runtime trace. *Secur Inform* **5**, 2 (2016). https://doi.org/10.1186/s13388-016-0027-2

Contact: Alexander Rosenbaum, M. Sc. (arosenbaum@uni-koblenz.de)