VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ STUDIJŲ PROGRAMA

Analysis of GAN architectures suitable for Ethical Malware Obfuscation

GAN architektūrų, tinkamų kenkėjiško kodo obfuskacijai, analizė

Research Paper

Author: 4 kurso 3 grupės studentas
Liudas Kasperavičius

Supervisor: prof. dr. Olga Kurasova

Vilnius – 2024

Contents

Notes

- `notes/1.md` - Notes about [NDI+23]
- `notes/2.md` - Notes about [ZCY+24]
- `notes/3.md` - Notes about [ZHZ+22]
- `notes/4.md` - Notes about [KOD19]
- `notes/5.md` - Notes about [HT17]
- `notes/6.md` - Notes about [FWL+19]
- `notes/7.md` - Notes about [ZZY+22]
- `notes/8.md` - Notes about [CSD19]

Introduction

The introduction describes the aim of the work, the relevance of the topic, and the expected results. The introduction should not be a summary of the content. The length of the introduction should be 1–2 pages.

Results

The results and conclusions section must clearly present the main results of the work (something analyzed, something created, something implemented) and provide conclusions (comparisons of methods for solving the examined problems, recommendations, and highlights of innovations).

Conclusions

1. The conclusions section compares the methods for solving the examined problems, offers recommendations, and highlights innovations.
2. Conclusions are presented in a numbered (possibly hierarchical) list format.
3. The conclusions of the work must correspond to the aim of the work.

References

[CSD19] R. L. Castro, C. Schmitt, G. Dreo. AIMED: Evolving Malware with Genetic Programming to Evade Detection. In: *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. 2019, pp. 240–247 [visited on 2024-09-23]. ISSN 2324-9013. Available from: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00040.

[FWL+19] Z. Fang, J. Wang, B. Li, S. Wu, Y. Zhou, H. Huang. Evading Anti-Malware Engines With Deep Reinforcement Learning. *IEEE Access*. 2019, volume 7, pp. 48867–48879 [visited on 2024-09-18]. ISSN 2169-3536. Available from: https://doi.org/10.1109/ACCESS.2019.2908033.

[HT17] W. Hu, Y. Tan. *Generating Adversarial Malware Examples for Black-Box Attacks Based on GAN*. 2017-02-20. [visited on 2024-09-18]. Available from: http://arxiv.org/abs/1702.05983.

[KOD19] M. Kawai, K. Ota, M. Dong. Improved MalGAN: Avoiding Malware Detector by Leaning Cleanware Features. In: *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. 2019, pp. 040–045 [visited on 2024-09-14]. Available from: https://doi.org/10.1109/ICAIIC.2019.8669079.

[NDI+23] H. Nguyen, F. Di Troia, G. Ishigaki, M. Stamp. Generative Adversarial Networks and Image-Based Malware Classification. *Journal of Computer Virology and Hacking Techniques*. 2023, volume 19, number 4, pp. 579–595 [visited on 2024-09-15]. ISSN 2263-8733. Available from: https://doi.org/10.1007/s11416-023-00465-2.

[ZCY+24] F. Zhong, X. Cheng, D. Yu, B. Gong, S. Song, J. Yu. MalFox: Camouflaged Adversarial Malware Example Generation Based on Conv-GANs Against Black-Box Detectors. *IEEE Transactions on Computers*. 2024, volume 73, number 4, pp. 980–993 [visited on 2024-09-15]. ISSN 1557-9956. Available from: https://doi.org/10.1109/TC.2023.3236901.

[ZHZ+22] F. Zhong, P. Hu, G. Zhang, H. Li, X. Cheng. Reinforcement Learning Based Adversarial Malware Example Generation against Black-Box Detectors. *Computers & Security*. 2022, volume 121, p. 102869 [visited on 2024-09-14]. ISSN 0167-4048. Available from: https://doi.org/10.1016/j.cose.2022.102869.

[ZZY+22] E. Zhu, J. Zhang, J. Yan, K. Chen, C. Gao. N-Gram MalGAN: Evading Machine Learning Detection via Feature n-Gram. *Digital Communications and Networks*. 2022, volume 8, number 4, pp. 485–491 [visited on 2024-09-23]. ISSN 2352-8648. Available from: https://doi.org/10.1016/j.dcan.2021.11.007.