VILNIAUS UNIVERSITETAS
MATEMATIKOS IR INFORMATIKOS FAKULTETAS
PROGRAMŲ SISTEMŲ STUDIJŲ PROGRAMA

GAN architektūrų, tinkamų kenkėjiško kodo obfuskacijai, analizė

Analysis of GAN architectures suitable for Ethical Malware Obfuscation

Kursinis darbas

Atliko: 4 kurso 3 grupės studentas
Liudas Kasperavičius

Darbo vadovas: prof. dr. Olga Kurasova

Vilnius – 2024

Turinys

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]
- `notes/9.md` - Notes about [AKF+18]
- `notes/10.md` - Notes about [DCB+21]
- `notes/11.md` - Notes about [YPT22]
- `notes/12.md` - Notes about [CDH+16]

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.

Šaltiniai

[AKF+18] H. S. Anderson, A. Kharkar, B. Filar, D. Evans, P. Roth. *Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning*. 2018-01-30. [žiūrėta 2024-09-30]. Prieiga per internetą: https://doi.org/10.48550/arXiv.1801.08917.

[CDH+16] X. Chen, Y. Duan, R. Houthooft, J. Schulman, I. Sutskever, P. Abbeel. *InfoGAN: Interpretable Representation Learning by Information Maximizing Generative Adversarial Nets*. 2016-06-11. [žiūrėta 2024-10-07]. Prieiga per internetą: https://doi.org/10.48550/arXiv.1606.03657.

[CSD19] R. L. Castro, C. Schmitt, G. Dreo. AIMED: Evolving Malware with Genetic Programming to Evade Detection. Iš: *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, p. 240–247 [žiūrėta 2024-09-23]. ISSN 2324-9013. Prieiga per internetą: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00040.

[DCB+21] L. Demetrio, S. E. Coull, B. Biggio, G. Lagorio, A. Armando, F. Roli. Adversarial EXEmples: A Survey and Experimental Evaluation of Practical Attacks on Machine Learning for Windows Malware Detection. *ACM Trans. Priv. Secur.* 2021, tomas 24, numeris 4, 27:1–27:31 [žiūrėta 2024-09-30]. ISSN 2471-2566. Prieiga per internetą: https://doi.org/10.1145/3473039.

[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, tomas 7, p. 48867–48879 [žiūrėta 2024-09-18]. ISSN 2169-3536. Prieiga per internetą: 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. [žiūrėta 2024-09-18]. Prieiga per internetą: http://arxiv.org/abs/1702.05983.

[YPT22] J. Yuste, E. G. Pardo, J. Tapiador. Optimization of Code Caves in Malware Binaries to Evade Machine Learning Detectors. *Computers & Security*. 2022, tomas 116, p. 102643 [žiūrėta 2024-10-07]. ISSN 0167-4048. Prieiga per internetą: https://doi.org/10.1016/j.cose.2022.102643.

[KOD19] M. Kawai, K. Ota, M. Dong. Improved MalGAN: Avoiding Malware Detector by Leaning Cleanware Features. Iš: *2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. 2019, p. 040–045 [žiūrėta 2024-09-14]. Prieiga per internetą: 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, tomas 19, numeris 4, p. 579–595 [žiūrėta 2024-09-15]. ISSN 2263-8733. Prieiga per internetą: 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, tomas 73, numeris 4, p. 980–993 [žiūrėta 2024-09-15]. ISSN 1557-9956. Prieiga per internetą: 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, tomas 121, p. 102869 [žiūrėta 2024-09-14]. ISSN 0167-4048. Prieiga per internetą: 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, tomas 8, numeris 4, p. 485–491 [žiūrėta 2024-09-23]. ISSN 2352-8648. Prieiga per internetą: https://doi.org/10.1016/j.dcan.2021.11.007.