У процесі симуляції ми бачимо як хакери атакують пристрої, як захисники реагують на ці атаки, і як пристрої можуть оновлюватися, щоб підвищити свій рівень захисту. Така 3D візуалізація допомагає краще уявити, як ці агенти працюють в реальному часі, спостерігаючи за змінами в мережі і рухами агентів, що дає вам наочне розуміння того, як працює механізм атаки та захисту.

1. Alrawi, C. Lever, M. Antonakakis, F. Monrose, Security of the Internet of Things: Vulnerabilities, Attacks and Countermeasures. November 2019IEEE Communications Surveys & Tutorials 22(1):616-644 DOI:10.1109/COMST.2019.2953364

2. Seth Tisue, Uri Wilensky. NetLogo: Design and Implementation of a Multi-Agent Modeling Environment. Center for Connected Learning and Computer-Based Modeling Northwestern University, Evanston, Illinois,

Розробка алгоритму детекції шкідливого програмного забезпечення на основі поведінкового аналізу

УДК 004.056.5 (043.2)

Артем Повозніков[1], Наталья Козаченко [2]

Національний університет «Одеська Політехніка»,

[1]9560415@stud.op.edu.ua, [2]kozachenko.n.h@op.edu.ua

В умовах стрімкого зростання кількості та складності кіберзагроз традиційні антивірусні рішення стають менш ефективними. Це обумовлює потребу у впровадженні нових методів виявлення шкідливого програмного забезпечення (ШПЗ), зокрема заснованих на поведінковому аналізі.

Мета роботи – розробка алгоритму детекції ШПЗ, який базується на аналізі аномальної поведінки програм, а не лише на сигнатурних базах.

Сигнатурні антивірусні системи залежать від оновлення баз даних загроз і часто не здатні розпізнати нові або модифіковані варіанти шкідливих програм. Натомість поведінковий аналіз орієнтується на виявлення відхилень у звичних сценаріях роботи програм, таких як аномальні зміни реєстру, нетипові запити до мережі або небажаний доступ до критичних системних ресурсів. У рамках дослідження розглянуто існуючі методи детекції шкідливого ПЗ(таблиця 1).

Таблиця 1

Порівняння методів детекції шкідливого програмного забезпечення

Критерій/ Метод	**Сигнатурний аналіз**	**Евристичний аналіз**	**Поведінковий аналіз**	**Машинне навчання**
Виявлення нових загроз	Низьке	Середнє	Високе	Високе
Рівень хибних спрацьовувань	Низький	Середній	Середній	Може бути високим

Швидкість виявлення	Висока	Висока	Залежить від реалізації	Залежить від моделі
Необхідність оновлення баз	Часте	Менш часте	Не потребує	Не потребує
Вимоги до ресурсів	Низькі	Середні	Високі	Високі
Складність реалізації	Низька	Середня	Висока	Висока

Таким чином, використання поведінкового аналізу та методів машинного навчання дозволяє істотно підвищити ефективність виявлення нових загроз у порівнянні з традиційними підходами.

Було розроблено та протестовано власний алгоритм, що включає:

1) збір даних про поведінку програм у контрольованому середовищі (sandbox),

2) екстракцію ключових поведінкових ознак,

3) навчання моделі машинного навчання для класифікації нормальної та шкідливої активності.

Для тренування моделі використовувались відкриті датасети поведінкових логів, зокрема зі спільнот VirusTotal та Cuckoo Sandbox.

Результати експериментальної перевірки показали, що запропонований алгоритм досягає точності виявлення понад 95% при мінімальному рівні хибних спрацьовувань, що свідчить про його перспективність для реального впровадження.

Таким чином, поведінковий аналіз відкриває нові можливості для раннього виявлення невідомих та складно маскованих шкідливих програм, що є важливим кроком для підвищення рівня кібербезпеки.

1. Saxe, J., Berlin, K. Deep neural network-based malware detection using two-dimensional binary program features // Proceedings of the 10th International Conference on Malicious and Unwanted Software (MALWARE), IEEE, 2015.

2. Anderson, H. S., Roth, P. Ember: An open dataset for training static PE malware machine learning models // arXiv preprint arXiv:1804.04637, 2018.

3. Gandotra, E., Bansal, D., Sofat, S. Malware analysis and classification: A survey // Journal of Information Security, 2014.

4. Mohaisen, A., Alrawi, O., Mohaisen, M. AMAL: High-fidelity, behavior-based automated malware analysis and classification // Computers & Security, 2015.

5. VirusTotal. [Електронний ресурс]. URL: https://www.virustotal.com/ (дата звернення: 05.05.2025).

6. Cuckoo Sandbox. [Електронний ресурс]. URL: https://cuckoosandbox.org/ (дата звернення: 05.05.2025).

7. Stiborek, J., Rehák, M., Pevný, T. Anomaly-based network intrusion detection: Techniques, systems and challenges // Computers & Security, 2018.

8. Kolosnjaji, B., Zarras, A., Webster, G., Eckert, C. Deep learning for classification of malware system call sequences // Australasian Joint Conference on Artificial Intelligence, Springer, 2016.

9. Yuan, B., Lu, X., Xie, M. Malware detection based on deep learning of behavior graphs // Journal of Computer Virology and Hacking Techniques, 2020.

10. Ucci, D., Aniello, L., Baldoni, R. Survey of machine learning techniques for malware analysis // Computers & Security, 2019.

Застосування нейронних мереж для аналізу побічних каналів (side-channel attacks)

УДК 004.4:056.57

Олександр Полевод
Національний університет «Чернігівська політехніка»,
oleksandr.polevod23@gmail.com

Актуальність досліджень у галузі інформаційної безпеки зумовлена стрімким розширенням використання криптографічних засобів захисту конфіденційних даних. Попри стабільність теоретичних моделей сучасних криптоалгоритмів, їх реальні програмно-апаратні реалізації нерідко зазнають загроз, пов'язаних із побічними каналами (side-channel)[1]. Побічні канали можуть надавати додаткову інформацію про внутрішній стан системи внаслідок вимірювання часових затримок, електромагнітного випромінювання, енергоспоживання, шуму тощо. Застосування методів глибинного навчання дозволяє суттєво підвищити ефективність атак на основі побічних каналів, адже нейронні мережі добре справляються з масивними та «зашумленими» даними, виявляючи приховані закономірності.[2]

Основна мета роботи полягає у дослідженні можливостей застосування глибинних нейронних мереж для проведення атак на основі побічних каналів та оптимізації методів виявлення криптографічних витоків. Зокрема, робота має на меті визначити найефективніші архітектури нейронних мереж і методи обробки сигналів, які б дозволили зменшити обсяг необхідних вимірювань, підвищити точність відновлення секретних ключів та сприяти розробці нових методів захисту від подібних атак.

Класичні методи аналізу побічних каналів ґрунтуються на використанні статистичних чи кореляційних підходів (Differential Power Analysis, Correlation Power Analysis тощо)[1]. Вони вимагають ретельної підготовки наборів даних та візуального/евристичного пошуку оптимальних характеристик сигналу. Проте з ускладненням апаратних реалізацій (наприклад, систем на кристалі, які поєднують декілька криптографічних ядер одночасно) та суттєвим зростанням рівня шуму ці підходи стають дедалі менш ефективними. Натомість, використання нейронних мереж надає змогу автоматично виявляти найінформативніші ознаки (features) у сигналах, що дає змогу успішно відтворювати секретні ключі або інші конфіденційні дані з меншими вимогами до попередньої обробки.[3]

Дослідження базується на застосуванні різних підходів машинного навчання. Зокрема, найефективнішими виявилися згорткові (Convolutional Neural Networks, CNN) та рекурентні нейронні мережі (Recurrent Neural