УДК 004.056.57, 004.492, 004.89

Р. М. Кучерешко
Західноукраїнський національний університет, Україна

СИСТЕМА ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ ДЛЯ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМ

R. M. Kuchereshko

DECISION SUPPORT SYSTEM BASED ON FUZZY LOGIC FOR MALWARE DETECTION

На сьогоднішній день існує багато засобів захисту інформації, зокрема і в мобільних пристроях, що працюють на програмному і апаратному рівнях. Сучасні системи захисту інформації знаходяться на високому рівні і демонструють добрі результати. Мобільні пристрої застосовуються для широкого кола завдань і є зручним засобом для вирішення багатьох питань. Цим обумовлена висока швидкість зростання функціональних можливостей мобільних пристроїв. На тлі цієї тенденції існує проблема комплексного захисту інформації. Зловмисники мають сьогодні у своєму арсеналі безліч різних засобів і активно використовують їх для досягнення своїх протиправних цілей.

У ОС для мобільних пристроїв ефективно можуть використовуватися «класичні» методи, що добре зарекомендували себе. Вони засновані на сигнатурному аналізі і ефективно працюють за наявності відповідної сигнатури у відповідній базі, але для того, щоб вона там з'явилася, необхідно певний час, що може послужити ключовим моментом для застосування нових шкідливих програм.

Вищевикладене примушує розробників у сфері ОС для мобільних пристроїв проводити аналіз поведінкового характеру для виявлення шкідливих програм. Розробка комплексних засобів захисту дозволяє виявляти шкідливі програми як на рівні поведінки, так на сигнатурному рівні .

Об’єднання нечіткого логічного висновку і експертних оцінок є одним з перспективних підходів до організації систем динамічного аналізу шкідливих програм з метою підвищення надійності захисту інформації [1-3].

Система виявлення шкідливих програм реалізована із застосуванням машини опорних векторів [4] і системи підтримки прийняття рішень на основі нечіткої логіки по алгоритму Мамдані [5-8].

Машина опорних векторів навчається і тестується на вибірці, в якій кожному класу складені вектори поведінки програм, потім виконує класифікацію на два класи virus і ok. За допомогою системи підтримки прийняття рішень на основі даних результату роботи машини опорних векторів і додаткових критеріїв здійснюється виведення остаточного результату в процентному співвідношенні. Система виявлення шкідливих програм є об’єднанням двох методів. В якості вхідних даних використовується розроблена експериментальна вибірка, отримана шляхом аналізу роботи системи в цілому.

Навчання машини опорних векторів для класифікації програм проходить в два етапи. На першому етапі проводиться навчання на експериментальній вибірці машини опорних векторів, внаслідок чого вона стає здатною коректно розподіляти по класах програми. Навчальна вибірка включає список доступних 152 дозволів на запуск і використання ресурсів, необхідних для роботи програми, а також виявлених 12 ознак, властивих поведінці програм. Таким чином, були складені вектори поведінки як шкідливих, так і безпечних програм. До складу навчальної вибірки увійшли 67 складених векторів програм. Тестова вибірка включала 33 вектори програм з внесенням змін з метою ускладнити завдання виявлення шкідливих програм.

На другому етапі формалізуються додаткові ознаки і задаються у вигляді функцій приналежності для системи підтримки прийняття рішень. До складу функцій приналежності також входить результат класифікації машиною опорних векторів. Потім формується база

правил для коректного функціонування системи підтримки прийняття рішень. На підставі усіх ознак і результатів роботи машини опорних векторів отримуємо результат, виражений у відсотках.

Алгоритм функціонування системи складається з наступних кроків:

- формування вектору ознак з програми;
- подається вектор ознак програми (шкідлива або безпечна програма) на вхід SVM-класифікатора;
- здійснюється класифікація машиною опорних векторів на два класи virus і ok;
- результат класифікації і додаткові ознаки, задані у вигляді функцій, подаються блоку «система підтримки прийняття рішень»;
- на підставі правил проводиться аналіз результатів;
- виводиться результат у відсотках.

Таким чином, модель системи виявлення шкідливих програм має у своєму складі два блоки: машина опорних векторів, яка здійснює класифікацію з високою ефективністю, і система підтримки прийняття рішень на основі нечіткої логіки, яка дозволяє підвищити точність класифікації машиною опорних векторів з урахуванням перешкод і дати точний результат. Таким чином, можна здійснювати виявлення шкідливих програм при їх відсутності у базі сигнатур, спираючись на поведінку, властиву шкідливим і безпечним програмам.

Література:

1. Dubchak L., Komar M. Speedy procesing method of fuzzy data for intelligent systems of intrusion detection. Projekt interdyscyplinarny projektem XXI wieku: Processing, transmission and security of information. Bielsko-Biala, 2017. T. 2. Pp. 65-74.

2. Komar M., Kochan V., Dubchak L., Sachenko A., Golovko V., Bezobrazov S., Romanets I. High performance adaptive system for cyber attacks detection. The 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications : Proceedings (Bucharest, Romania, September 21-23, 2017). Bucharest, 2017. Vol. 2. Pp. 853-858.

3. Комар М., Саченко А., Кочан В. Підвищення безпеки системи виявлення вторгнень на основі використання апаратних засобів. Сучасні проблеми інформатики в економіці, управлінні, освіті та подоланні наслідків Чорнобильської катастрофи : матер. XV-го міжнар. наук. семінару, Київ – оз. Світязь, 4-8 липня, 2016. С. 271-275.

4. Nello Cristianini, John Shawe-Taylor. An Introduction to Support Vector Machines and Other Kernel-based Learning Methods. - Cambridge University Press, 2000.

5. Ross T.J. Fuzzy Logic with Engineering Applications. McGraw-Hill Inc.(USA). 1995. 600 p.

6. Рутковская Д., Пилиньский М., Рутковский Л. Нейронные сети, генетические алгоритмы и нечеткие системы. М.: Телеком. 2006. 382 с.

7. Штовба С.Д. Обеспечение точности и прозрачности нечеткой модели Мамдани при обучении по экспериментальным данням. Проблемы управления и информатики. 2007. №4. С. 102-114.

8. Dubchak L., Vasylkiv N., Kochan V., Lyapandra A. Fuzzy Data Processing Method. The 7th IEEE International Conference Intelligent Data Acquisition and Advanced Computing Systems : Technology and Applications : Proceedings (Berlin, Germany, September 12-14, 2013). Berlin, 2013. Vol. 1. Pp. 373-375.