УДК 004.725.7

Балакін С.В.

ЗАСТОСУВАННЯ ШТУЧНИХ ІМУННИХ СИСТЕМ ПРИ ВИЯВЛЕННІ ШКІДЛИВИХ ПРОГРАМ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Національний авіаційний університет

yabal@mail.ru

Проаналізовано поведінку шкідливих і нешкідливих програмних об'єктів з метою отримання протоколу їх роботи. Розглянуто варіанти розпізнавання шкідливих програм на рівні їх виявлення і блокування. Виявлено загальні для досліджуваних програм особливості поведінки. Наведено рівняння, що описують дії даного способу базуючись на операторах штучних імунних мереж. Реалізовано запропоновану структуру виявлення шкідливих програм. Запропоновано методи підвищення виявлення шкідливих програм і атак в комп'ютерній мережі

Ключові слова: комп'ютерна мережа, протокол, виявлення, дослідження, штучна імунна мережа

Вступ

Головною проблемою в сучасному інформаційному просторі являється стрімке зростання кількості шкідливих програм і атак на комп'ютерні мережі. З переважною їх більшістю можуть впоратися антивіруси та фаєрволи, але деякі атаки можуть обійти навіть такий захист, приносячи шкоду користувачеві чи компанії. Частіше за все наявний захист спрацьовує з запізненням - тобто тоді, коли система вже була атакована й відбулась втрата даних чи контроль над певними компонентами мережі.

Розглянуто спосіб підвищення достовірності розпізнавання шкідливих програм в комп'ютерній мережі та запропоновано нові рішення наявних проблем.

Постановка проблеми

Вирішуваною проблемою виступає достовірність розпізнавання шкідливих програм в комп'ютерній мережі та вибір методів захисту. Головним завданням є моніторинг поведінки шкідливих і нешкідливих об'єктів з метою отримання протоколу їх роботи для прийняття рішення про належність чи неналежність даної програми до сімейства шкідливих програм. Виходячи з особливостей досліджуваного процесу, запропоновано оцінювати достовірність розпізнавання шкідливих програм, використовуючи аналіз протоколів роботи програм.

Дослідження в цій галузі

При виконанні поставленого завдання використовувалися методи моніторингу поведінки програмних об'єктів для отримання протоколів їх роботи. Дослідження послідовностей виклику API функцій і переданих їм аргументів. Дослідження і навчання проведено на базі процесора Intel Core 2 Duo T7300 на ОС Windows 8.

Негативні фактори, що впливають на результат роботи - достатнє, але в міру різноманітна кількість досліджуваних служб та програм на базі експериментальної системи.

Мета досліджень

Застосування даного способу розпізнавання шкідливих програм і атак в локальних і глобальних комп'ютерних мережах. Визначення актуальності використання даних програмних методів та їх ефективності. Визначити програми котрі негативно впливають на ефективність і захищеність системи й усунення їх негативних наслідків. Блокування чи обмеження функціоналу шкідливих програм.

Результат досліджень

Більшість алгоритмів маскування

кодів шкідливих програм працює з популярними аналізаторами коду, котрі використовують поведінкові методи аналізу [1]. Такі методи використовують системні виклики для свого функціонування. При відмові від аналізу коду відпаде необхідність в роботі з алгоритмами упаковування і шифрування для розпізнавання шкідливих програм.

Проблема частково вирішується за допомогою евристичних аналізаторів, що використовують поведінковий аналіз на підставі даних, отриманих від аналізу за допомогою штучних нейронних мереж, штучних імунних систем, генетичних алгоритмів, мультиагентного підходу та ін. [2, 3,4].

Для вирішення задачі розпізнавання шкідливих програм у складі евристичного аналізатора, який виконує розподіл розпізнавання на основі зваженої оцінки деякої кількості ознак, пропонується використовувати штучні імунні мережі. Модель такого евристичного аналізатора шкідливих програм складається з чотирьох блоків (рис.1).

Рис.1. Модель евристичного аналізатора

Блок моніторингу. Його функція - моніторинг поведінки шкідливих і нешкідливих об'єктів з метою отримання протоколу їх роботи (послідовностей виклику API функцій і переданих їм аргументів).

Блок порівняння. Він приймає протоколи роботи декількох програм з блоку моніторингу і порівнює їх. Результатом роботи буде безліч однакових фрагментів (ознак) у протоколах різних програм одного сімейства.

Бібліотека ознак. Цей блок зберігає виявлені блоком порівняння ознаки і веде їх статистику. На основі статистики ознакам присвоюється рейтинг, що характеризує частоту появи ознаки. Знайдений в протоколах всіх програм фрагмент матиме найбільший рейтинг, а фрагмент знайдений в найменшій кількості програм - найменший.

Блок прийняття рішень. Функція даного компонента - прийняття рішення про належність чи неналежність даної програми до сімейства шкідливих програм.

Блок моніторингу моделює штучне оточення для роботи програм. На вхід блоку надходить об'єктний файл, який запускається

на виконання в штучно створеному середовищі. Під час виконання запущених функцій програми обробниками, ведеться збір даних і формується протокол. По завершенню виконання програми сформований протокол подається на вихід блоку для подальшої обробки.

Блок порівняння реалізує ряд алгоритмів, спрямованих на виявлення

загальних для досліджуваних програм особливостей поведінки. На вхід блоку надходять протоколи роботи виконуваних файлів, отримані від емулятора. На виході необхідно отримати безліч загальних фрагментів для всіх протоколів, які були подані на вхід. Обробка відбувається в два етапи:

Фільтрація вхідних протоколів і очищення їх від даних, які не несуть інформацію про події, що пов'язані з діями

над файловою системою, системним реєстром, процесами або роботою в інтернет [5].

Після фільтрування протоколи порівнюються для знаходження в них спільних фрагментів (обидві послідовності повинні бути однакової довжини).

Бібліотека ознак являє собою сховище даних, у якому містяться фрагменти протоколів у зручному для обробки форматі [6]. Фрагменти являють собою масиви структур, кожна з яких призначена для зберігання ключової інформації про API функції – тип функції й значення найбільш важливих аргументів.

Для кожної збереженої ознаки $x_f, f = \overline{1, L_f}$ підраховується рейтинг тієї, що зустрічається R_f :

$$R_f = \frac{X_f}{F}$$

де X_f - кількість знайдених об'єктів з даною ознакою; F - загальна кількість об'єктів.

Блок прийняття рішень є основним компонентом евристичного аналізатора, який призначений для розпізнавання як шкідливих програм певного сімейства, так і не шкідливих і здатний виконувати класифікацію вхідних векторів на дві групи. Він може бути реалізований різними технологіями штучних імунних мереж. Модель штучної імунної мережі, запропонована Н. Ерне [7], надає більше можливостей по організації взаємодії популяцій імунних об'єктів (рис. 2).

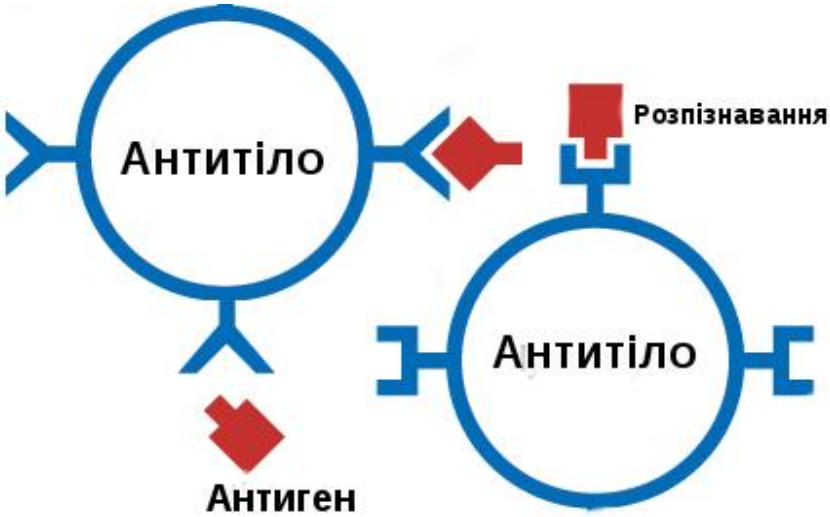

Рис. 2. Принцип мережевої взаємодії антитіл

В даній моделі антитіла і їх клони являють собою регульовану мережу клітин, що взаємодіють не тільки з антигенами, а й між собою. При цьому взаємодія між антитілами відбувається не тільки при їх стимуляції антигенами, а й за відсутності чужорідних об'єктів. Дана модель заснована на припущенні про взаємодію лімфоцитів між собою шляхом встановлення зв'язків між їх антитілами [8,9].

Таким чином, розпізнавання антигену здійснюється не поодиноким антитілом або клоном, а організованою мережею лімфоцитів і їх антитіл. Математична модель імунної мережі - це мережа, в якій антигени та антитіла описуються бінарними рядками, а визначення афінності проходить наступним чином:

$$Aff_{ij} = \sum_{k=1}^{m_g} [G \left(\sum_{n=1}^{l} e_i(n+k) \right) * + * p_j(n) - s_1 \right)$$

де " *+*" – додатковий XOR оператор;

k – відхилення, що вимірюється в бітах, між паратопами і епітопами клітин;

$e_i(n) - n$ - й біт в епітопі;

$p_j(n) - n$ -й біт в паратопі;

s – поріг від $G(x) = x$ при $x > 0$ і $G(x) = 0$ в протилежному випадку.

Афінності імунних об'єктів використовуються в диференціальному рівняння для моделювання динаміки зміни антитіл. Для вихідної кількості N антитіл

$\{x_1, \ldots, x_n\}$ і n антигенів $\{y_1, \ldots, y_n\}$, зміна отриманих клітин описується наступним чином:

$$\frac{dx_i}{dt} = c\left[\sum_{j=1}^{N} aff_{ji}x_i x_j - k_1 \sum_{j=1}^{N} aff_{ji}x_i x_j + \sum_{j=1}^{n} aff_{ji}x_i y_j\right] - k_2 x_i$$

де $\sum_{j=1}^{N} aff_{ji}x_i x_j$ – стимуляція для зв'язків типу «антитіло-антитіло»;

$k_1 \sum_{j=1}^{N} aff_{ji}x_i x_j$ – придушення антитіл у зв'язках типу «антитіло-антитіло»;

$\sum_{j=1}^{N} aff_{ji}x_i y_j$ – стимуляція антитіла у зв'язках типу «антитіло -антиген»;

k1 – нормуючий коефіцієнт між стимуляцією і придушенням;

$k_2 x_i (k_2 > 0)$ – «кінцевий вираз», що видаляє кількість x_i антитіл;

c – величина продукування стимульованих антитіл.

При виявленні і розпізнаванні антигену відбувається стимуляція мережі антитіл, в результаті чого обмежена кількість антитіл, що характеризуються високою афінністю до антигену, формують популяцію клонів. Після цього сформовані клони піддаються мутації для отримання більш детальної інформації про антиген. Для редагування популяції клонів і антитіл в даній моделі використовується механізм супресії (стиснення мережі). При цьому механізм супресії може використовувати як принципи моделі клонального відбору, так і мережеві принципи редагування кількості антитіл, при яких з популяції видаляються антитіла, що характеризуються низькою афінністю до інших стимульованих антитіл.

Редагування популяції антитіл і безлічі мутованих клонів в даній моделі відбувається за допомогою виклику оператора супресії. В процесі супресії відбувається визначення афінності між антитілами та клонами, що відповідає принципу мережевої взаємодії імунних об'єктів. Використання оператора супресії виключає використання клонального відбору і старіння. Слід зазначити, що при організації супресії можуть використовуватися принципи ЄІС, використовувані в роботі оператора клонального відбору або старіння антитіл.

В даний час існує декілька основних методів, що реалізують принципи моделі імунної мережі: методи aiNET, opt-aiNET і метод RLAIS. Дані методи використовуються для вирішення завдань розпізнавання та аналізу даних і є базовими по відношенню існуючих імунних методів на основі моделі штучних імунних мереж.

Вибір значень параметрів даних операторів впливає на швидкість збіжності і час обчислень на кожному поколінні імунних алгоритмів, а також на властивість імунних алгоритмів знаходити глобальне рішення, не зупиняючись в точках локальних екстремумів. Навчена імунна мережа представляється множиною антитіл пам'яті і матрицею їх афінностей. Множина інтерпретує внутрішні відображення антигенів, подані на вхід мережі. Матриця описує зв'язки між антитілами, і показує загальну структуру імунної мережі. Маючи матриці афінності антитіл пам'яті, можна визначити структуру імунної мережі, а також належність кожного антитіла до відповідного класу. Шляхом вимірювання афінностей антитіл з множини клітин пам'яті до антигенів з навчального набору можна визначити, які з антитіл розпізнають антигени, відповідні шкідливі програми з даного сімейства, а які розпізнають нешкідливі (або шкідливі програми інших сімейств). Таким чином, здійснюється ідентифікація отриманих кластерів.

У режимі розпізнавання на вхід вже навченої штучної імунної мережі подається вектор даних, що являє собою но-

вий антиген, з яким навчена мережа раніше не стикалася. Вимірявши афінності даного антигену до антитіл, що містяться в пам'яті цієї мережі, можна визначити, до якого кластеру віднести даний антиген, і таким чином винести вердикт про приналежність або неналежність антигену до множини шкідливих програм досліджуваного сімейства

Попри високу точність отриманих результатів, умови при проведенні дослідження не були ідеальними. Це пов'язано з неможливістю тестування методу з усіма відомими програмами. Поставлена задача виявлення шкідливих програм виконана. Однак існує ряд факторів, які необхідно використовувати в проведених розрахунках для отримання більш точних даних. Також доцільним є опрацювання більшої кількості шкідливих програм для розширення діапазону можливих рішень на виході евристичного аналізатора.

Висновки

Представлено модель розпізнавання шкідливих програм і атак в комп'ютерній мережі на основі штучних імунних систем. Основною проблемою при проведенні дослідження було коректне виявлення саме шкідливих дій через те, що іноді вони можуть маскуватись як дії користувача для приховання своєї діяльності.

Запропоновано оцінювати достовірність розпізнавання шкідливих активностей, використовуючи аналіз протоколів роботи програм. У такий спосіб не упускаються шкідливі дії, але з іншого боку можуть блокуватися деякі програми та утиліти користувача.

Наведено рівняння, що описують дії даного способу базуючись на операторах штучних імунних мереж. За їх допомогою можна реалізувати запропоновану структуру виявлення шкідливих програм за описаною схемою евристичного аналізатора, котрий відповідає за коректне опрацювання всіх даних і гарантує отримання відповідних результатів. Сформульовано шляхи підвищення достовірності виявлення шкідливих програм і атак в комп'ютерній мережі.

Проведені дослідження показують доцільність використовуваних інструментів. Даний підхід ефективний при виявленні й запобіганні несанкціонованих дій в комп'ютерній мережі.

Список літератури

1. Ситник В.Ф. Основи інформаційних систем: Навч. посіб. - 2-ге вид., перероб. і допов // К.: КНЕУ, 2001. – 420 с.

2. Стивен Норткат, Джуди Новак. Обнаружение нарушений безопасности в сетях, 3-е издание: Пер. с англ. – М.: Изд. дом "Вильямс", 2003. – 448 с.

3. Щерба М.В. Система анализа устойчивости распределенных компьютерных сетей к атакам // Омский научный вестник, 2012. – 286 с.

4. Милославская Н.Г., Толстой А.И. Интрасети: Обнаружение вторжений: учеб/пособие для вузов // Юнити-Дана, 2001. – 592 с.

5. Таненбаум Э. Компьютерные сети. // СПб.: Питер, 2008. – 848 с.

6. Іванов В.Г., Карасюк В.В., Гвозденко М.В. Основи інформатики та обчислювальної техніки: Навч. посіб. // Юрінком Інтер, 2004. – 328 с.

7. N.K. Jerne, Idiotypic networks and Other Preconecived Ideas // Immunological review, Vol. 79, 1984. – P. 5–24.

8. Балакин С.В. Выявление компьютерных атак с помощью мониторинга сетевых объектов // Информационные технологии и системы управления, №25, 2015. – С. 35-38.

9. Пат. 110330 Україна, МПКG06F 12/14. Спосіб запобігання комп'ютерним атакам в мережі за допомогою фільтрації вхідних пакетів / І.А. Жуков, С.В. Балакін ; власник Нац. Авіаційний Університет. – № 201602196 ; заявл. 09.03.2016 ; опублік. 10.10.2016, Бюл. № 19. – 6 с.

Статтю подано до редакції 30.05.2017