УКРАЇНА

(19) UA (11) 127724 (13) U

(51) МПК (2018.01)
H04W 12/08 (2009.01)
G06F 21/00
G06F 12/14 (2006.01)

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2017 11238**

(22) Дата подання заявки: **17.11.2017**

(24) Дата, з якої є чинними права на корисну модель: **27.08.2018**

(46) Публікація відомостей про видачу патенту: **27.08.2018, Бюл.№ 16**

(72) Винахідник(и):
Комар Мирослав Петрович (UA),
Кочан Володимир Володимирович (UA),
Саченко Анатолій Олексійович (UA),
Головко Владімір Адамовіч (BY),
Бєзобразов Сєргєй Валєрьєвіч (BY)

(73) Власник(и):
Комар Мирослав Петрович,
вул. Збаразька, 31, кв. 48, м. Тернопіль, 46010 (UA),
Кочан Володимир Володимирович,
вул. Львівська, 7, м. Тернопіль, 46009 (UA),
Саченко Анатолій Олексійович,
вул. Загребельна, 24, м. Тернопіль, 46027 (UA),
Головко Владімір Адамовіч,
ул. Воровского, 17, кв. 54, г. Брест, 224030, республика Беларусь, (BY),
Бєзобразов Сєргєй Валєрьєвіч,
ул. Московская, 267А, кв. 91, г. Брест, 224017, республика Беларусь, (BY)

(54) СПОСІБ ІЄРАРХІЧНОЇ КЛАСИФІКАЦІЇ КОМП'ЮТЕРНИХ АТАК НЕЙРОМЕРЕЖЕВОЮ ШТУЧНОЮ ІМУННОЮ СИСТЕМОЮ

(57) Реферат:

Спосіб ієрархічної класифікації комп'ютерних атак шляхом інтеграції набору нейромережевих детекторів в штучну імунну систему, яка проводить спостереження за діями абонентів в режимі реального часу та постійно донавчає нейромережеві детектори на основі параметрів мережевого з'єднання, яке виявлене як атака. При спрацюванні декількох нейромережевих імунних детекторів спочатку обчислюють поточні різниці між вхідним образом і ваговими векторами всіх нейронів кожного нейромережевого імунного детектора, потім обчислюють квадратні корені із суми квадратів цих поточних різниць, а мінімальні значення серед обчислених квадратних коренів подають на другі виходи кожного нейромережевого імунного детектора, причому на тип атаки вказує той нейромережевий імунний детектор, на другому виході якого є найменше значення квадратного кореня.

UA 127724 U

Корисна модель належить до галузі захисту інформаційно-комунікаційних систем від несанкціонованого доступу до їх ресурсів, а саме до способів і пристроїв, які забезпечують контроль та класифікацію мережевого трафіку для виявлення комп'ютерний атак.

Відомий спосіб виявлення атак, який реалізовано у патенті [1], включає до свого складу нагляд за тотальним мережевим трафіком, накопичення даних, перевірку даних за заданими правилами і вживання відповідних дій при виявлені даних, що відповідають цим правилам.

Недоліком такого способу виявлення атак є те, що він на мережевому рівні не дозволяє виявляти атаки, що спрямовані на спеціалізовані інформаційні системи для отримання несанкціонованого доступу. До того ж він не забезпечує виявлення зловживань незареєстрованими абонентами під час роботи з ресурсами інформаційної системи. А також, у зв'язку з необхідністю обробки великого обсягу даних мережевих з'єднань, даний спосіб не забезпечує своєчасного виявлення атак та реагування на них.

Аналогічне рішення передбачає використання сигнатурного аналізу для фільтрації вхідних пакетів [2, 3]. Крім недоліків попереднього способу, спосіб [2, 3] не забезпечує виявлення нових, не відомих комп'ютерних атак на інформаційні ресурси.

Спосіб виявлення атак, який реалізовано у [4], включає спостереження за трафіком пакетів даних, що надходять абоненту, перевірку цих пакетів за заданими правилами і подачу сигналу для прийняття заходів захисту від несанкціонованого доступу, коли перевірка виявляє відповідність вказаним правилам. Він орієнтований на спостереження за поведінкою зареєстрованих користувачів мереж і виявлення спроб несанкціонованого доступу до ресурсів мережі з їхньої сторони. Особливістю даного способу є те, що для виявлення спроб несанкціонованого доступу від обманно присвоєного імені іншого абонента мережі, проводять спостереження за трафіком адресованих абоненту пакетів даних, що включає постійно поновлюваний підрахунок числа пакетів, що виконується в межах серії пакетів, що надходять підряд один за одним через проміжки часу, не більші заданого значення. При цьому перевірку пакетів даних, що надходять, виконують кожен раз на відповідність заданим правилам, коли розмір чергової серії досягає критичного числа пакетів.

Недоліком даного способу є те, що хоч дана система забезпечує збір даних в реальному часі, проте потім, при послідовному аналізі сеансів мережевих з'єднань, виявлення несанкціонованих дій в комп'ютерній мережі відбувається з неминучим запізненням по відношенню до початку таких дій. У багатьох випадках, запізнення з прийняттям заходів по припиненню несанкціонованих дій може приводити до непоправних наслідків і робити захист малоефективним.

Відомий також спосіб виявлення атак [5], що передбачає спостереження за діями абонентів шляхом отриманням даних з системних журналів інформаційної системи, що містять інформацію про запити абонента на доступ до ресурсів, або аналізом трафіку, який надходить від абонентів до інформаційної системи. Дані про дії абонентів перевіряються за заданими правилами. За результатами аналізу видаються сигнали для прийняття заходів захисту інформаційної системи. Для своєчасного реагування на атаку аналіз трафіку виконується безперервно, а аналіз накопичених даних виконується через невеликий інтервал часу, величина якого вибирається залежно від інтенсивності роботи абонентів з ресурсами інформаційної системи і необхідним часом реагування на виявлену атаку.

Недоліком способів, реалізованих в [1-5] є те, що вони не забезпечують в режимі реального часу виявлення всіх типів комп'ютерних атак, а в основному направлені на виявлення атак зі сторони зареєстрованих користувачів мереж, тобто окремих типів атак. Також відомі рішення не забезпечують виявлення нових, не відомих комп'ютерних атак на інформаційні ресурси.

Найближчим аналогом даного способу є спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою [6], що включає спостереження за діями абонентів, яке забезпечується безперервним аналізом трафіку, що надходить від абонентів до інформаційної системи, та видачу сигналів для прийняття заходів щодо захисту інформаційної системи. Цей спосіб відрізняється тим, що спостереження за діями абонентів та аналіз мережевого трафіку здійснюється в режимі реального часу нейромережевою штучною імунною системою, яка реалізована на основі інтеграції нейромережевих детекторів в штучну імунну систему згідно з наступними операціями: навчання з використанням навчальної вибірки, яка складається із сукупності параметрів нормальних мережевих з'єднань та параметрів комп'ютерних атак; відбір кращих детекторів з використанням тестової вибірки, які не мають помилкових спрацьовувань і характеризуються мінімальною середньоквадратичною помилкою виявлення комп'ютерних атак; функціонування нейромережевих імунних детекторів для виявлення та класифікації атак; активація нейромережевих імунних детекторів, коли мережеве з'єднання класифікується одним або кількома детекторами як комп'ютерна атака; формування

імунної пам'яті шляхом занесення в навчальну вибірку параметрів мережевого з'єднання, яке класифіковане як атака.

Однак, при використанні відомого способу [6] можуть виникати конфлікти, пов'язані з одночасним спрацюванням нейромережевих імунних детекторів, кожен з яких навчений на певному типі атак. У такому випадку виникають збої у формуванні імунної пам'яті, що в свою чергу веде до втрати під час донавчання спеціалізації нейромережевих імунних детекторів щодо виявлення конкретного типу атаки.

В основу корисної моделі поставлена задача вдосконалення способу ієрархічної класифікації комп'ютерних атак нейромережевою штучною імунною системою шляхом спостереження за діями абонентів в режимі реального часу та недопущення виникнення конфліктів, пов'язаних з одночасним спрацюванням декількох нейромережевих імунних детекторів, що дозволяє підвищити достовірність виявлення атак, а також зменшити ймовірність помилкових спрацювань, коли нормальне з'єднання класифікується як атака.

Поставлена задача вирішується за рахунок того, що ієрархічна класифікація комп'ютерних атак ведеться шляхом інтеграції набору нейромережевих детекторів в штучну імунну систему, яка проводить спостереження за діями абонентів в режимі реального часу та постійно донавчає нейромережеві детектори на основі параметрів мережевого з'єднання, яке виявлене як атака. Згідно з корисною моделлю, при спрацюванні декількох нейромережевих імунних детекторів спочатку обчислюють поточні різниці між вхідним образом і ваговими векторами всіх нейронів кожного нейромережевого імунного детектора, потім обчислюють квадратні корені із суми квадратів цих поточних різниць, а мінімальні значення серед обчислених квадратних коренів подають на другі виходи кожного нейромережевого імунного детектора, причому на тип атаки вказує той нейромережевий імунний детектор, на другому виході якого є найменше значення квадратного кореня.

Спочатку обчислюють поточні різниці між вхідним образом і ваговими векторами всіх нейронів $\left(x_1 - w_{1j}\right)$ кожного нейромережевого імунного детектора, потім обчислюють квадратні корені із суми квадратів цих поточних різниць $\left(x_1 - w_{1j}\right)$.

Далі визначають мінімальні значення серед обчислених квадратних коренів $\left(x_1 - w_{1j}\right)$ і ці значення подають на другі виходи кожного нейромережевого імунного детектора. Причому, на тип атаки вказує той нейромережевий імунний детектор, на другому виході якого є найменше значення квадратного кореня.

Таким чином, запропоновані операції способу дають можливість проводити однозначну ієрархічну класифікацію комп'ютерних атак. Тому конфлікти, пов'язані з одночасним спрацюванням нейромережевих імунних детекторів, кожен з яких навчений на певному типі атак не виникають. Це дозволить коректно донавчати нейромережеві імунні детектори і, відповідно, коректно формувати імунну пам'ять. В результаті спеціалізація нейромережевих імунних детекторів зростає і вони краще виявляють відповідні типи атак.

Запропонований спосіб, в порівнянні з найближчим аналогом, дає можливість підвищити достовірність виявлення атак, а також зменшити ймовірність помилкових спрацювань, коли нормальне з'єднання класифікується як атака.

Джерела інформації:

1. Патент США US 5796642 A від 18.08.1998 р.

2. Способ защиты информационно-вычислительных сетей от компьютерных атак / О.Е. Куликов, В.А. Липатніков, Р.В. Максимов, О.А. Можаєв // Патент Російської Федерації RU 2285287, заявл. 04.04.2005, реєстраційний номер 2005109585/09.

3. Спосіб запобігання комп'ютерним атакам у мережі за допомогою фільтрації вхідних пакетів / І.А. Жуков, С.В. Балакін // Патент на корисну модель № 110330, G06F 12/14 (2006.01). № u201602196; заявл. 09.03.2016; опубл. 10.10.2016, Бюл. № 19.

4. Способ обнаружения удаленных атак в компьютерной сети / И.О. Вильчевский, В.С. Заборовский, В.Е. Клавдиев, В.А. Лопота, А.В. Маленкова // Патент Російської Федерації RU 2179738 C2 від 24.04.2002 р., МПК7 G06F 12/14, 11/00.

5. Спосіб виявлення віддалених атак на інформаційну систему / С.А. Криштоп, М.Ф. Логвиненко, В.Я. Пєвнєв, О.А., Серков, Г.Л. Чурюмов // Деклараційний патент на корисну модель України № 9182, G06F 12/14. № u200501204; заявл. 10.02.2005; опубл. 15.09.2005, Бюл. № 9.

6. Спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою / М.П. Комар, А.О. Саченко, В.А. Головко, С.В. Безобразов // Патент України на винахід №109640, МПК(2012) H04W 12/08, G06F 21/00, G06F 12/14. № a201205350; заявл. 28.04.12; опубл. 25.09.15, Бюл. № 18.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб ієрархічної класифікації комп'ютерних атак шляхом інтеграції набору нейромережевих детекторів в штучну імунну систему, яка проводить спостереження за діями абонентів в режимі реального часу та постійно донавчає нейромережеві детектори на основі параметрів мережевого з'єднання, яке виявлене як атака, який **відрізняється** тим, що при спрацюванні декількох нейромережевих імунних детекторів спочатку обчислюють поточні різниці між вхідним образом і ваговими векторами всіх нейронів кожного нейромережевого імунного детектора, потім обчислюють квадратні корені із суми квадратів цих поточних різниць, а мінімальні значення серед обчислених квадратних коренів подають на другі виходи кожного нейромережевого імунного детектора, причому, на тип атаки вказує той нейромережевий імунний детектор, на другому виході якого є найменше значення квадратного кореня.

Комп'ютерна верстка Л. Ціхановська

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

ДП “Український інститут інтелектуальної власності”, вул. Глазунова, 1, м. Київ – 42, 01601