УКРАЇНА

(19) UA (11) 74822 (13) U

(51) МПК (2012.01)
H04W 12/08 (2009.01)
G06F 21/00
G06F 12/14 (2006.01)

ДЕРЖАВНА СЛУЖБА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2012 05349**

(22) Дата подання заявки: **28.04.2012**

(24) Дата, з якої є чинними права на корисну модель: **12.11.2012**

(46) Публікація відомостей про видачу патенту: **12.11.2012, Бюл.№ 21**

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

(73) Власник(и):
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ,
вул. Львівська, 11, м. Тернопіль, 46020 (UA)

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

(57) Реферат:

Спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою, що включає спостереження за діями абонентів, яке забезпечується безперервним аналізом трафіку, що надходить від абонентів до інформаційної системи, видачу сигналів для прийняття заходів захисту інформаційної системи, при якому 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 стадіями: 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.

UA 74822 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'ютерних атак.

Відомий спосіб виявлення атак, який реалізовано у рішенні [1], включає до свого складу нагляд за тотальним мережевим трафіком, накопичення даних, перевірку даних за заданими правилами і вживання відповідних дій при виявленні 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 з метою 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.

Спосіб виявлення атак, який реалізовано у рішенні [2] 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 відносно до початку таких дій. У багатьох випадках, запізнення з прийняттям заходів по припиненню несанкціонованих дій може приводити до непоправного збитку і робити захист малоефективним.

Прототипом запропонованого способу є спосіб виявлення атак, який реалізовано у [3], що передбачає спостереження за діями абонентів, яке забезпечується 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 виконується видача сигналів 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 [1-3] є те, що вони не забезпечують в режимі реального часу виявлення всіх типів комп'ютерних атак, а в основному направленні на виявлення атак зі сторони зареєстрованих користувачів мереж. Також відомі рішення не забезпечують виявлення нових, не відомих комп'ютерних атак на інформаційні ресурси.

В основу корисної моделі поставлена задача вдосконалення способу виявлення комп'ютерних атак нейромережевою штучною імунною системою шляхом спостереження за діями абонентів та аналізу мережевого трафіку в режимі реального часу, що дозволяє нейромережевим детекторам самоорганізовуватися, розвиватися еволюційним шляхом, адаптуватися до невідомих комп'ютерних атак з метою їх виявлення та класифікації, а також підвищити точність виявлення атак та зменшити ймовірність помилкових спрацювань, коли нормальне з'єднання класифікується як атака.

Поставлена задача вирішується за рахунок того, що спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою, що включає спостереження за діями абонентів, яке забезпечується безперервним аналізом трафіку, що надходить від абонентів до інформаційної системи, видачу сигналів для прийняття заходів захисту інформаційної системи, згідно з корисною моделлю, вводиться те, 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 стадіями: 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.

Спосіб виявлення комп'ютерних атак нейромережевою імунною системою можна представити у вигляді наступної послідовності кроків:

1. Генерація нейромережевих імунних детекторів. На цьому кроці відбувається створення нейронних мереж з початковою ініціалізацією вагових коефіцієнтів.

2. Навчання імунних детекторів. На даному етапі згенеровані нейронні мережі піддаються процесу навчання. Навчання нейронної мережі здійснюється на основі контрольованого конкурентного навчання відповідно до правила "переможець бере все". Навчальна вибірка формується наступним чином: нехай N - множина з'єднань, що належать до певного типу мережевих атак, а M - множина з'єднань, що належать до класу нормального трафіку. З них випадковим чином формується множина вхідних образів для навчання і-то детектора.

$$X_i = \begin{bmatrix} X_i^1 \\ X_i^2 \\ \dots \\ X_i^L \end{bmatrix} = \begin{bmatrix} X_{i1}^1 & X_{i2}^1 & \dots & X_{in}^1 \\ X_{i1}^2 & X_{i2}^2 & \dots & X_{in}^2 \\ \dots & & & \\ X_{i1}^L & X_{i2}^L & \dots & X_{in}^L \end{bmatrix}$$

Відповідно, множина еталонних образів

$$e_i = \begin{bmatrix} e_i^1 \\ e_i^2 \\ \dots \\ e_i^L \end{bmatrix} = \begin{bmatrix} e_{i1}^1 & e_{i2}^1 & \dots & e_{in}^1 \\ e_{i1}^2 & e_{i2}^2 & \dots & e_{in}^2 \\ \dots & & & \\ e_{i1}^L & e_{i2}^L & \dots & e_{in}^L \end{bmatrix},$$

де L - розмірність навчальної вибірки.

Еталонні вихідні значення для і-го детектора формуються наступним чином:

$$e_{i1}^k = \begin{cases} 1, \text{якщо } X_i^k \in N \\ 0, \text{інакше} \end{cases},$$

$$e_{i2}^k = \begin{cases} 1, \text{якщо } X_i^k \in M \\ 0, \text{інакше} \end{cases}.$$

В результаті навчання нейромережевого імунного детектора створюється множина цих детекторів, тобто для виявлення атаки певного типу в даному випадку використовується не один навчений нейромережевий імунний детектор, а декілька.

У загальному випадку, методику створення та навчання нейромережевих імунних детекторів можна представити в наступному вигляді:

1. Створюємо нейромережевий детектор з випадковою ініціалізацією вагових коефіцієнтів.

2. Випадковим чином з набору параметрів мережевих з'єднань вибираємо N з'єднань, що належать до певного типу мережевих атак і M з'єднань, що належать до класу нормального трафіку.

3. Послідовно подаємо вибрані параметри з'єднань на нейронну мережу, і в залежності від поданих даних та даних на виході нейронної мережі коригуємо вагові коефіцієнти. Вагові коефіцієнти коригуються відповідно до наступного:

а) обчислюється Евклідова відстань між вхідним образом і ваговими векторами нейронних елементів шару Кохонена

$$D_i = |X - \omega_1| = \sqrt{(X_1 - \omega_{1i})^2 + (X_2 - \omega_{2i})^2 + (X_n - \omega_{ni})^2},$$

де $i = \overline{1,m}$.

b) визначається нейронний елемент-переможець з номером k

$$D_k = \min_i D_i.$$

с) проводиться модифікація вагових коефіцієнтів нейрона-переможця відповідно до наступних виразів:

$$\omega_{ck}(t+1) = \omega_{ck}(t) + \gamma(X_c - \omega_{ck}(t)).$$

Якщо при подачі на вхід мережі параметрів мережевої атаки переможцем є один з перших f нейронів нейронної мережі або при подачі на вхід мережі параметрів нормального з'єднання переможцем є один з l останніх нейронів мережі Кохонена. В іншому випадку:

$$\omega_{ck}(t+1) = \omega_{ck}(t) - \gamma(X_c - \omega_{ck}(t)).$$

4. Процес повторюється, починаючи з пункту 3 для всіх вхідних образів. Навчання нейронної мережі проводиться до бажаного ступеня узгодження між вхідними і ваговими векторами, тобто доти, поки значення сумарної квадратичної помилки не стане рівним нулю:

$$E_i = \frac{1}{2}\sum_{k=1}^{L}\sum_{j=1}^{2}\left(Y_j^k - e_j^k\right)^2,$$

де Y_j^k - j-е вихідне значення нейромережевого детектора для k-го вхідного образу, e_j^k - j-е еталонне значення для k-го еталонного образу.

5. Весь процес повторюється доти, поки кількість навчених імунних детекторів не стане рівним заданому значенню F.

Таким чином, створюється набір детекторів для аналізу мережевого трафіку з метою виявлення комп'ютерних атак. Але, перед тим як виконувати аналіз мережевого трафіку, навчені детектори необхідно перевірити на коректність класифікації з метою запобігання виникненню помилкових спрацьовувань. Для цього всі навчені детектори проходять стадію відбору.

3. Відбір імунних детекторів. Для мінімізації виникнення помилкових спрацьовувань, коли нормальне з'єднання приймається за мережеву атаку, всі навчені нейромережеві імунні детектори проходять перевірку на коректність класифікації. Для цього, на нейронну мережу подається заздалегідь створена тестова вибірка, що складається з параметрів нормального з'єднання. Якщо і-й детектор класифікує одне з тестових з'єднань як атаку, то він знищується, а замість нього генерується і навчається новий детектор. Якщо і-й детектор не генерує помилкові спрацьовування на тестовій вибірці, то він вважається коректним і допускається до аналізу мережевого трафіку.

4. Функціонування імунних детекторів. Детектори, які допущені до аналізу мережевого трафіку утворюють систему виявлення мережевих атак. Весь трафік, що одержується комп'ютером, спочатку аналізується сукупністю імунних детекторів, і, якщо жоден з детекторів не виявляє аномалію, то трафік обробляється операційною системою і відповідним програмним забезпеченням. Кожен детектор має час життя, протягом якого він аналізує мережевий трафік. Якщо по закінченні виділеного часу детектор не виявив аномалію, він знищується, а на його місце приходить новий детектор. Механізм наділення детекторів часом життя дозволяє позбавлятися від детекторів, які хоч і пройшли успішно стадії навчання та відбору, проте через свою структурну особливості (набір вагових коефіцієнтів) є малопридатними.

5. Активація імунних детекторів. Під активацією детекторів розуміється виявлення детектором мережевої атаки. У випадку, коли мережеве з'єднання класифікується одним або кількома детекторами як мережева атака, відбувається його блокування, тобто воно не допускається до обробки операційною системою і спеціалізованим програмним забезпеченням. Також видається повідомлення користувачу про спробу атаки на комп'ютерну систему.

6. Формування імунної пам'яті. При виявленні і блокуванні мережевої атаки доцільним є збереження її параметрів з метою вивчення та детального аналізу. Справа в тому, що імунні нейромережеві детектори навчаються на обмеженому наборі даних, які не можуть включати в себе всі ймовірні мережеві атаки. Для того, щоб підвищити якість виявлення, а також наділити систему виявлення вторгнень гнучкістю і дозволити їй адаптуватися під сучасні реалії, параметри мережевого з'єднання, що класифіковане як атака зберігаються і заносяться в навчальну вибірку, тим самим поповнюючи її актуальними даними. Детектори, які будуть створюватися з метою замінити "застарілі" імунні детектори будуть вже навчатися також і на нових даних, що значно дозволить збільшити якість виявлення. Крім цього, створюється нова нейронна мережа, яка навчається виключно на даних, виділених з виявленої мережевої атаки, і яка вводиться в систему аналізу мережевого трафіку. Це дозволить більш точно виділити дану атаку при повторній подібній атаці на комп'ютерну систему з боку зловмисника. Сукупність детекторів імунної пам'яті буде зберігати в собі інформацію про всі мережеві атаки, направлені

в минулому на комп'ютерну систему, і забезпечувати високий рівень реагування на повторні спроби атак.

Таким чином, інтеграція нейромережевих детекторів у штучну імунну систему дозволила розробити гнучку систему виявлення мережевих атак, здатну адаптуватися до зміни тенденцій розвитку методів організації комп'ютерних атак, виділяти основні характеристики виявлених мережевих атак і навчати на нових даних нейромережеві детектори з метою підвищення якості захисту інформаційних ресурсів. Більш того, детектори імунної пам'яті здатні надійно виявляти повторні спроби атак і зберігають інформацію про такі спроби.

Запропоноване технічне рішення в порівнянні з прототипом дає можливість нейромережевим імунним детекторам самоорганізовуватися, розвиватися еволюційним шляхом та адаптуватися до невідомих комп'ютерних атак, а також підвищити точність виявлення атак та 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. Патент Російської Федерації RU 2179738, МПК7 G06F12/14, 11/00. "Способ обнаружения удаленных атак в компьютерной сети". Опубліковано 20.02.2002 г.

3. Деклараційний патент на корисну модель України UA 9182, МПК G06F12/14. "Спосіб виявлення віддалених атак на інформаційні системи". Опубліковано бюл. № 9, 15.09.2005 р.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Спосіб виявлення комп'ютерних атак нейромережевою штучною імунною системою, що включає спостереження за діями абонентів, яке забезпечується безперервним аналізом трафіку, що надходить від абонентів до інформаційної системи, видачу сигналів для прийняття заходів захисту інформаційної системи, який **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 стадіями: 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.

Комп'ютерна верстка Л. Купенко

Державна служба інтелектуальної власності України, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут промислової власності", вул. Глазунова, 1, м. Київ – 42, 01601