УДК 621.38(62-52)

В.В. Стешин

ІНТЕЛЕКТУАЛЬНИЙ АГЕНТ В ЗАДАЧАХ МОНІТОРИНГУ БЕЗПЕКИ РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМ

Анотація: В статті розглянутий механізм захисту розподілених комп'ютерних систем розроблений на основі інтелектуальних агентів. Він дозволяє вчасно виявити та запобігти загрозі інформаційній системі шляхом порівняння поточних дій користувача з шаблоном загальних правил, сформованих адміністратором. Проведений експеримент з прогнозування активності користувача. Виявлено, що реалізація механізму прогнозування дозволяє налаштувати моніторинг системи таким чином, щоб вчасно запобігти неправомірним діям.

Ключові слова: інтелектуальний агент, розподілені комп'ютерні системи, безпека комп'ютерних систем.

Вступ

Сучасний розвиток інформаційних технологій та галузей науки потребують збільшення обчислювальних потужностей. З цією метою розробляються нові механізми комп'ютерної обробки. Існують два напрямки в дослідженні цієї теми. Перший полягає у збільшенні швидкодії робочої станції, на якій здійснюється обробка, такий варіант є надто затратним і не виправдовує себе, іншим напрямком є розробка розподілених комп'ютерних систем в основі яких лежить розподілення завдань між вузлами інформаційної системи, що збільшує швидкість обробки та видачу результату. При цьому більш важливим є кількість робочих станцій, а не їхня потужність. Розподілена комп'ютерна система також легко масштабується та забезпечує автономність її компонентів.

Однак незважаючи на переваги таких систем існує ряд невирішених питань, зокрема збереження цілісності даних та забезпечення безпеки. Оскільки дані розподіляються між робочими станціями системи виникає потреба в обмеженні доступу та контроль за виконанням операцій над ними. Безліч технологій, що забезпечують це мають обмежений набір правил, що робить комп'ютерну систему вразливою до дій користувача невідомих механізму безпеки. Погіршує також ситуацію збільшення навантаження на комп'ютерну систему та кількості завдань, які вона виконує . Наслідком цього є неефективне та несвоєчасне виявлення недозволених операцій.

Тому розробка механізмів забезпечення безпеки основаних на принципах штучного інтелекту, які б могли вчасно самостійно приймати рішення, збирати інформацію, навчатися та діяти у відповідних ситуаціях є актуальним питанням. У статті розглянутий

механізм забезпечення безпеки на основі інтелектуальних агентів, який відповідає потребам захисту розподілених комп'ютерних систем та підвищить рівень їх безпеки.

Загальні принципи побудови систем виявлення вторгнень з використанням інтелектуальних агентів

Механізм захисту на основі інтелектуального агента є гібридною системою виявлення вторгнень. Під гібридної системою прийнято розуміти систему, в якій для вирішення завдання використовується більше одного методу імітації інтелектуальної діяльності людини [5]. Гібридні інтелектуальні системи можуть поєднувати аналітичні моделі, експертні системи, штучні нейронні мережі, нечіткі системи, генетичні алгоритми, імітаційні статистичні моделі та ін. Розробка таких систем основана на об'єднанні декількох методів, як правило, з різних класів, для вирішення завдань управління та проектування.

Під терміном інтелектуальний агент розуміються сутності, що одержують інформацію через систему сенсорів про стан керованих ними процесах і здійснюють вплив на них. Такий агент може бути як програмною системою так і складною автоматизованою системою. Інтелектуальні агенти поділяються на два типи: прості інтелектуальні агенти та інтелектуальні агенти, що навчаються. У першому випадку виконується лише спостереження та виконання певних дій заданих агенту. Прикладом може бути програма з часовим таймером, що виконує запуск програм у відповідний момент. [9] В іншому випадку інтелектуальні агенти, що навчаються, володіють такими властивостями як: можливість навчатися і розвиватися в процесі взаємодії з навколишнім середовищем, пристосовуватися в режимі реального часу, швидко навчатися на основі великого обсягу даних, застосовувати нові методи вирішення проблем, володіти базою прикладів з можливістю її поповнення, мати параметри для моделювання швидкодії, пам'яті, часу і т.д., аналізувати себе та результат.

Доцільність використання інтелектуальних агентів в системах виявлення вторгнень очевидна. Такі характеристики дозволять розробити систему захисту основану на принципах штучного інтелекту, яка б дозволяла вчасно реагувати на загрози, що виникли в системі без участі самого користувача чи адміністратора.

Запропонований механізм забезпечення безпеки на основі інтелектуальних агентів базується на порівнянні та прогнозуванні. Поточні дії користувача порівнюються з попередніми та набором правил системного адміністратора. Залежно від результату механізм забезпечення безпеки блокує, або дозволяє виконання програм (використання ресурсів) та переходить до аналізу наступних дій користувача. Інтенсивність та частота роботи користувача з про-

грамами або ресурсами також фіксується. Ця інформація дозволяє виконати прогнозування наступних його дій.

Інтелектуальний агент виконує роль проміжної ланки між робочою станцією користувача та мережею. Всі процеси, що відбуваються в розподіленій комп'ютерній системі контролюються і опрацьовуються ним. Агент на стороні користувача виконує моніторинг його робочої станції та обмінюється інформацією з основним агентом на сервері системи. Взаємодія агентів дозволяє контролювати всю мережу незалежно від кількості вузлів у ній [8].

Особливості інтелектуального агента для вирішення задач моніторингу безпеки

Інтелектуальний агент (ІА) використовується у різноманітних випадках. В даному контексті захисту інформаційної системи можна виділити наступний набір характеристик: [1,2].

Автономія. Здатність агента діяти без прямого втручання користувачів, або інших агентів і мати деякий контроль на основі свого внутрішнього і/або зовнішнього середовища.

Співпраця. Агент має можливість взаємодіяти з іншими агентами з метою виконання завдань, які виходять за рамки можливостей конкретного агента.

Ініціативність. Здатність агента передбачити майбутню ситуацію та змінити напрямок дій, щоб уникнути небажаного результату. Проактивні агенти здатні виявити певну поведінку методом виявлення ініціативи об'єкта спостереження.

Здатність до реагування. Така поведінка означає, що агент реагує в режимі реального часу на зміни, які відбуваються в середовищі системи

Інтелект. Агент може володіти певним інтелектуальним рівнем пріоритету, починаючи від планування до самостійного навчання.

Гнучкість. Здатність агента адаптуватися до будь-якої ситуації в системі, в якій він знаходиться

Мобільність. Агент здатний переміщатися від однієї до іншої локалізації для виконання конкретного завдання, або відреагувати на конкретну подію попередньо вивчивши вимоги до властивостей та аспектів забезпечення безпеки.

Загальна архітектура інтелектуального агента

Пропонується механізм захисту розподіленої комп'ютерної системи оснований на інтелектуальних агентах, базовий з яких знаходиться на стороні адміністратора, серверного вузла, і агента на стороні користувача. У другого є унікальний зв'язок, за допомогою якого відбувається обмін інформацією з основним агентом. Даний зв'язок створюється на вимогу агента користувача і знищується при виході з системи. На рис. 1 зображено основний агент, який

взаємодіє за допомогою багатьох зв'язків з агентами на стороні користувачів.

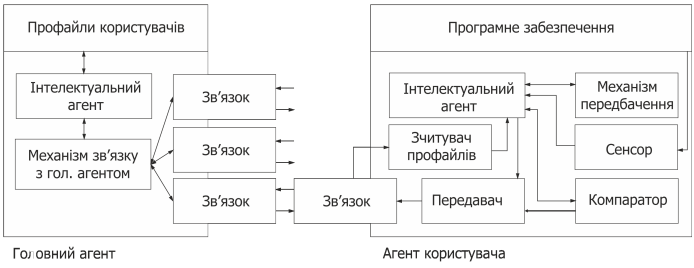

Рис. 1 – Архітектура інтелектуального агента

Розглянемо детальніше особливості реалізації представленого на малюнку 1 інтелектуального агента на стороні користувача. Він включає в себе чотири основних блоки: сенсор, передавач, зчитувач профайлів та компаратор.

Сенсор. В процесі виконання будь-яких операцій на робочій станції користувача та при вході в систему першим етапом роботи інтелектуального агента є збір інформації. За виконання даного завдання відповідає сенсор, який постійно сканує програмне забезпечення, що запущене на робочій станції користувача. Опитування активності відбувається через деякий певний період і супроводжується збором такої інформації як: індифікатор користувача, назви програм і індифікатори процесів, ресурсів та ін. Частоту сканування сенсора може змінювати системний адміністратор, або формуватися на основі даних отриманих механізмом передбачення. Даний блок дозволяє спрогнозувати майбутню активність на основі попередньої.

Передавач. Після першого опитування сенсором передавач дає запит до основного агента на отримання профайла користувача. Дана операція забезпечується зв'язком між основним агентом та агентом користувача. Зауважимо, що даний процес є паралельним і не заважає в отриманні профайлів іншим агентам користувачів.

Зчитувач профайлів. Отриманий профайл поступає на зчитувач профайлів, там обробляється і отримані дані поступають на компаратор. Профайли користувачів попередньо створюється адміністратором системи для кожного вузла окремо на основі загальних профілів та доданих правил взятих з окремих моделей поведінки. Вони містять інформацію про минулу та поточну активність користувача, яка постійно доповнюється новими записами. Таким чином забезпечується накопичення знань про користувача де, коли і з чим він працював.

Структурно поведінка користувача складається з:

1. Інформації про програми з якими працює, працював користувач;
2. Шлях по якому ці програми виконувалися;
3. Каталог та файли з якими користувач працює, або працював.

Компаратор. Виконання активних дій інтелектуального агента відбувається після порівняння профайла користувача з інформацією отриманою від сенсора. Якщо поточна поведінка не відповідає дозволеній поведінці записаній в профайлі компаратор відправляє через передавач основному агенту повідомлення, що містить ідентифікатор користувача, тип помилкової поведінки. Таким помилковим типом поведінки може бути наприклад неавторизований доступ до директорії, відкриття файлу недозволеною програмою та ін. Далі виконуються наступні дії:

1. Відправлення попереджувального повідомлення системному адміністратору, або користувачу;
2. Виключення програмного забезпечення, яке спровокувало помилкову поведінку;
3. Запобігання запуску програмного забезпечення надалі до моменту внесення коректив в профайл користувача.

Другий та третій етапи можуть відбуватися локально та паралельно, тобто на робочій станції користувача підчас інформування адміністратора. Це забезпечує своєчасне реагування механізму захисту інформаційної системи на загрозу.

Далі приймається рішення адміністратором системи, якщо процес є дозволеним тоді в профайл користувача вноситься відповідна інформація та дається дозвіл на виконання операції. В іншому випадку процес блокується і про це повідомляється користувача.

Архітектура мульти-агентного управління безпекою

Для забезпечення безпеки у розподіленій комп'ютерній системі було запропопоновано використання архітектури мульти-агентного управління безпекою. Вона виглядає як сукупність автономних та інтелектуальних агентів, розташованих в конкретних мережевих вузлах. Ці агенти співпрацюють і спілкуються між собою з метою виконання завдань ефективного виявлення вторгнення, а отже досягти більшої ефективності у захисті системи в загалом [3].

Основні характеристики архітектури безпеки є гнучкість, адаптивність і розподіл механізмів безпеки. Мульти-агент на основі архітектури управління безпекою складається з чотирьох основних компонентів, як показана на наступному малюнку.

Механізм створення інтелектуальних агентів (МІА). Являє собою середовище, в якому створюються, ініціалізуються і контролюються засоби управління безпекою інтелектуальних агентів.

Дане середовище також служить точкою доступу для адміністраторів системи.

Інтелектуальний агент (ІА). Являє собою інтелектуальний агент, який збирає, фільтрує інформацію, щодо управління і здійснює діяльність по забезпеченню безпеки в комп'ютерній системі.

Середовище виконання інтелектуальних агентів. Являє собою набір компонентів, необхідних для виконання і міграції інтелектуальних агентів.

Робоча станція адміністратора системи. Являє собою інтерфейс за допомогою якого адміністратор безпеки (людина) взаємодіє з архітектурою. Адміністратор безпеки повинен вказати політику безпеки, щоб застосувати її та створити екземпляр ІА. Для цих операцій адміністратору безпеки наданий необхідний доступ до механізму створення інтелектуальних агентів та агента управління. [6,7]

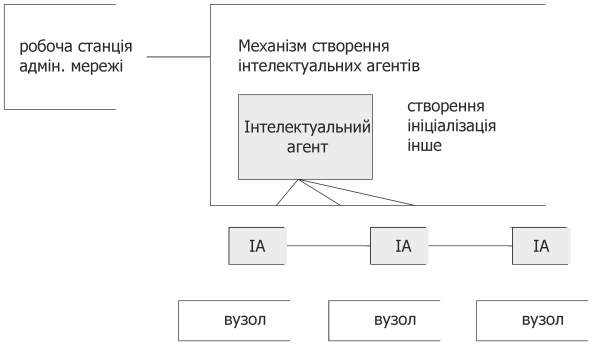

Рис. 2 – Архітектура мульти-агентного управління безпекою

Управління діяльністю в системі визначається її адміністратором і відображає політику безпеки [4]. Таким чином в середовищі мережі знаходяться безліч ІА, що співпрацюють один з одним з метою забезпечення глобальної безпеки управління, як показано на малюнку 2. Механізм мульти-агентного управління безпекою є розширенням функціонування архітектури інтелектуального агента. В цій архітектурі визначаються два типи ІА головний, ІА другорядні Другорядний ІА відповідає за управління безпекою свого домену локально, що може складатися з декількох вузлів. Є також декілька другорядних ІА, які виконують певний аналіз, перш ніж інформувати головний ІА коли вони підозрюють про атаку чи загрозу. Головний ІА відповідає за координацію завдань другорядних ІА і зіставлення інформації отриманих від них. Головний агент в свою чергу робить власний аналіз, щоб підтвердити, або ви-

явити напад і вжити необхідних заходів (наприклад, інформувати співробітника служби безпеки, заблокувати на певний період виконання джерела загрози). Перш ніж відправляти свої доповіді до головного ІА другорядні ІА можуть виконати обмін інформацією, для уточнення поточної ситуації.

Кінцевою ланкою архітектури є зовнішній агент, який виконує роль управління та контроль за будь-якого роду діяльності, що відбувається в мережі.

Експерименти та результати

Для визначення ефективності захисту GRID систем за допомогою інтелектуальних агентів на етапі прогнозування майбутньої активності та поведінки користувача отриманої на основі методу ковзаючого середнього попередньої його активності були проведені експерименти.

У ході експерименту використовувався спеціальний програмний комплекс та розподілена комп'ютерна система під управлінням Windows NT зі швидкістю мережі 10 / 100 Mb / s. для тестування роботи даної моделі. Механізм забезпечення безпеки реалізовано на мові програмування Java SDK, що в даному випадку є найзручнішою з точки зору об'єктно-орієнтованого програмування та створення потоків для забезпечення низькоприорітетного виконання моніторингу системи.

Експеримент був проведений на основі трьох робочих станцій підключених в мережу протягом п'ятдесяти годин. На кожній з них використовувався набір програм: MS Word, MS Excel, MS Outlook, MS Internet Explorer і середовище розробки C++. Обмеженість використання інших засобів та ресурсів не враховується оскільки моніторинг системи виконується на основі вище вказаного списку. Також неважливо коли та яку кількість екземплярів програм запущено підчас роботи в системі. Тобто в експерименті беруть участь лише програми з легального списку дозволених програм. Вони виконуються всіма користувачами, а інші програми доступні локально лише у межах їхніх систем і не являються доступними для інших вузлів.

Часовий період експерименту для виконання прогнозування був взятий у проміжок в 1 годину. Таким чином результати були зафіксовані 50 раз. Значення активності при цьому відповідає відношенню часу протягом якого використовувалися програми до часового періоду експерименту тобто в 1 год. Реальний час моніторингу системи при цьому співпадає з реальним часом спостереження.

В ході експерименту виконувалась оцінка таких параметрів, як Y_{t+1} – майбутня активність користувача, яка обчислювалась за формулою отримання середнього ковзаючого 1.

$$Y_{t+1} = \frac{1}{T+1}[Y_t + Y_{t-1} \dots Y_{t-T}] \quad (1)$$

де T – тимчасовий ряд, що дорівнює кількості попередніх прогнозувань і може змінюватися від 1 до n, Y_t – поточна активність користувача, Y_{t-1} – минула активність користувача, Y_{t-T} – остання активність користувача в тимчасовому ряді. Ми спеціально взяли алгоритм оцінки майбутньої активності користувача на певному проміжку, а не на основі всього часу спостереження оскільки в даному випадку результат прогнозування являється більш точним.

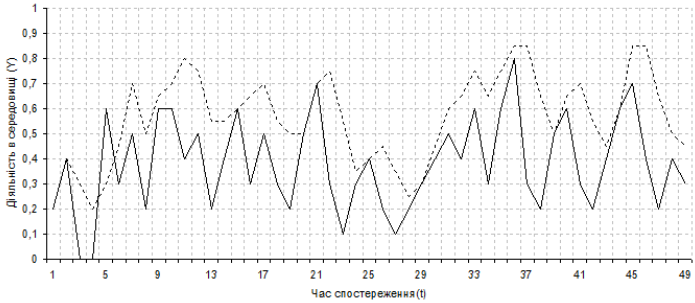

Рис. 3 – Залежність реальної та прогнозованої активності користувача на протязі часу

де 2 – реальна активність користувача, 1 – прогнозована активність користувача.

Отримані на малюнку 3 графіки ілюструють результати прогнозування механізму забезпечення безпеки протягом всього часу експерименту. Як бачимо результати прогнозування наближуються до результатів оцінки поточної активності користувача. У випадку коли користувач перестав використовувати захищений ресурс, або в нашому випадку програми, спостерігається спад графіка прогнозування майбутньої активності користувача. Лише при повторному звертанні до системи показник активності збільшуються, як і збільшується результат прогнозування.

Можна замітити, що на перших годинах експерименту спостерігається перетин двох графіків. Дана ситуація не є важливою оскільки моніторинг системи виконуються постійно, результати прогнозування впливають лише на частоту моніторингу системи.

Застосування даного методу дозволяє налаштувати механізм забезпечення безпеки згідно даних прогнозування активності користувача таким чином, щоб вчасно провести аналіз його дій та запобігти загрозі у випадку недозволеної ситуації.

Висновок

Засоби забезпечення безпеки в GRID системах є важливою складовою їхнього безперебійного функціонування. Багато запитань,

щодо безпеки вирішуються на локальному рівні, але коли користувач використовує ресурси та програми розподіленої комп'ютерної системи постає питання про захист та постійний моніторинг коректності його дій. Запропонований механізм забезпечення безпеки на основі інтелектуального агента не заміщає стандартних засобів забезпечення безпеки а доповняє їх. Він має здатність адаптуватися в будь-якій системі, навчатися, реагувати на загрози в режимі реального часу та завдяки можливості прогнозування передбачати майбутню ситуацію в системі.

Проведений експеримент на основі програмного комплексу механізму забезпечення безпеки ІА доказав готовність реагувати на зміну активності користувача системи, що дозволяє підвищити рівень безпеки у всій системі за рахунок постійного моніторингу дій користувача, порівняння інформації з даними його профайла і відповідно реагувати у випадку виконання недозволених операцій.

Библиографический список

1. S.Corley and al. The Application of Intelligent Agent Technologies to Network and Service Management.// Proc. of 15th IS&N Conference, Antwerpen, Belguim, May 2008.
2. R. Oliveira. Network Management with Knowledge of Requirements: Use of Software Agents.// PhD Thesis.
3. M. Wooldridge, An Introduction to MultiAgent Systems, John Wiley & Sons Ltd, 2002, paperback, 366 pages, ISBN 0-471-49691-X.
4. В.Е. Мухин, А.Н. Волокита. Разработка и реализация политики безопасности в распределенных компьютерных системах.// Управляющие системы и машины, N 3, 2010. – с. 78 – 85.
5. Колесніков А.В. Гібридні інтелектуальні системи: Теорія і технологія розробки. - СПБ: Вид-во СПбГТУ, 2001. - 711 с.
6. Нвана Х. Програмні агенти: Огляд. Knowledge Engineering Review, Vol.11, No.3, 205-244
7. Вулдрідж М., Дженнінгс Н. Інтеллектуальнве агенти: теорія і практика . Knowledge Eng. Rev., Vol. 10 (2), pp. 115-152, 1995
8. Розподілені комп'ютерні системи як складові інформаційних інфраструктур / В.П. Горбулін, О.Г. Додонов, О.С. Горбачик, М.Г. Кузнєцова // Реєстрація, зберігання і оброб. даних. — 2008. — Т. 10, № 4. — С. 19-24. — Бібліогр.: 9 назв. — укр.
9. N. Kasabov, Introduction: Hybrid intelligent adaptive systems. International Journal of Intelligent Systems, Vol.6, (1998) 453—454

Отримано 05.02.2013