УДК 621.396

Д.О. Даниленко, О.А. Смірнов, Є.В. Мелешко

Кіровоградський національний технічний університет, Кіровоград

Ä Î ÑË²ÄÆÅ Í Íß Ì ÅÒ Î Ä²Â ÂÈßÂËÅ Í Íß ÂÒ Î ÐÃ Í Å Í Ü Â ÒÅËÅÊ Î Ì Ó Í²ÊÀÖ²É Í² ÑÈÑÒÅ Ì È ÒÀ Ì ÅÐÅÆ²

Розглядаються методи підвищення безпеки телекомунікаційних мереж та систем, зокрема, досліджуються методи виявлення вторгнень (порушень), які функціонують із застосуванням статистичних критеріїв та аналізу відхилень від встановлених правил дій легітимних користувачів. Досліджуються математичні моделі та критерії, які застосовуються для виявлення вторгнень, аналізується архітектура розподілених систем виявлення порушень та архітектура відповідних агентів телекомунікаційної мережі.

Ключові слова: *телекомунікаційні системи та мережі, система виявлення вторгнень.*

Âñòóï

Перспективним напрямком у розвитку сучасних механізмів захисту інформаційних систем є розробка новітніх методів та програмно-технічних комплексів виявлення та запобігання вторгненням (порушенням) в телекомунікаційних системах та мережах [1 – 8].

Побудовані на їх основі системи виявлення та протидії вторгненням забезпечують додатковий рівень захисту комп'ютерних систем та використовуються для виявлення певних типів шкідливої активності, яка може порушити безпеку комп'ютерної мережі [7 – 8]. До такої активності відносяться мережеві атаки проти уразливих сервісів, атаки, що спрямовано на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення, наприклад, комп'ютерних вірусів [1 – 8].

Метою статті є аналіз та дослідження методів виявлення вторгнень (порушень), які функціонують із застосуванням статистичних критеріїв та аналізу відхилень від встановлених правил дій легітимних користувачів.

УДК 621.396

Д.О. Даниленко, О.А. Смірнов, Є.В. Мелешко

Кіровоградський національний технічний університет, Кіровоград

ДОСЛІДЖЕННЯ МЕТОДІВ ВИЯВЛЕННЯ ВТОРГНЕНЬ В ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ

Розглядаються методи підвищення безпеки телекомунікаційних мереж та систем, зокрема, досліджуються методи виявлення вторгнень (порушень), які функціонують із застосуванням статистичних критеріїв та аналізу відхилень від встановлених правил дій легітимних користувачів. Досліджуються математичні моделі та критерії, які застосовуються для виявлення вторгнень, аналізується архітектура розподілених систем виявлення порушень та архітектура відповідних агентів телекомунікаційної мережі.

Ключові слова: *телекомунікаційні системи та мережі, система виявлення вторгнень.*

Вступ

Перспективним напрямком у розвитку сучасних механізмів захисту інформаційних систем є розробка новітніх методів та програмно-технічних комплексів виявлення та запобігання вторгненням (порушенням) в телекомунікаційних системах та мережах [1 – 8].

Побудовані на їх основі системи виявлення та протидії вторгненням забезпечують додатковий рівень захисту комп'ютерних систем та використовуються для виявлення певних типів шкідливої активності, яка може порушити безпеку комп'ютерної мережі [7 – 8]. До такої активності відносяться мережеві атаки проти уразливих сервісів, атаки, що спрямовано на підвищення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення, наприклад, комп'ютерних вірусів [1 – 8].

Метою статті є аналіз та дослідження методів виявлення вторгнень (порушень), які функціонують із застосуванням статистичних критеріїв та аналізу відхилень від встановлених правил дій легітимних користувачів.

Основний розділ

Методи виявлення вторгнень

Останнім часом цей підхід до захисту інформаційних ресурсів мережі дуже швидко розвивається та поширюються, що обумовлено певними рисами, зокрема:

– якщо вторгнення буде виявлено швидко, порушника можна ідентифікувати і позбавити доступу до системи перш, ніж він встигне пошкодити або скомпрометувати інформаційні ресурси. Навіть якщо порушення буде зафіксовано надто пізно, аби перешкодити діям порушника, нанесений збиток буде мінімізований і система перейде до етапу відновлення;

– ефективна система виявлення порушень частково виконує і функції системи запобігання вторгненням;

– виявлення порушень дозволяє збирати ін.-формацію про методи вторгнення, яку згодом можна використовувати для посилення системи запобігання вторгненням.

Виявлення вторгнень ґрунтується на припущенні, що поведінка порушника відрізняється від поведінки легального користувача і відповідні відмінності можна представити в кількісному виразі. Звичайно ж, не можна чекати, що буде спостерігатися абсолютно різне використання ресурсів порушником порівняно з легальним користувачем. Правильніше припустити, що в поведінці того й іншого будуть загальні риси.

Таким чином, чим більш грубо інтерпретуватиметься поведінка порушника, тим вищою буде імовірність "помилкових спрацьовувань", тобто визнання легальних користувачів порушниками. В той же час прагнення позбавитися помилкових спрацьовувань шляхом суворої інтерпретації поведінки порушника веде до ситуацій, коли порушники залишаються невиявленими.

Отже, виявлення правопорушника (легального користувача, що виконує несанкціоновані операції) є складним завданням, оскільки в даному випадку нелегітимна поведінка може майже не відрізнятися від легітимної. Поведінку правопорушника можна виявити, якщо правильно визначити клас умов, при яких відбувається несанкціоноване використання ресурсів.

Проведений аналіз та дослідження показали, що в сучасних телекомунікаційних системах та мережах застосовуються наступні методи виявлення та протидії несанкціонованим вторгненням (рис. 1). На сьогоднішній день застосовуються методи виявлення вторгнень із застосуванням математичного апарату математичної статистики, тобто із застосуванням статистичних відхилень, та процедур розробки набору правил поведінки користувачів та аналізу відповідних відхилень їх дії від встановлених правил.

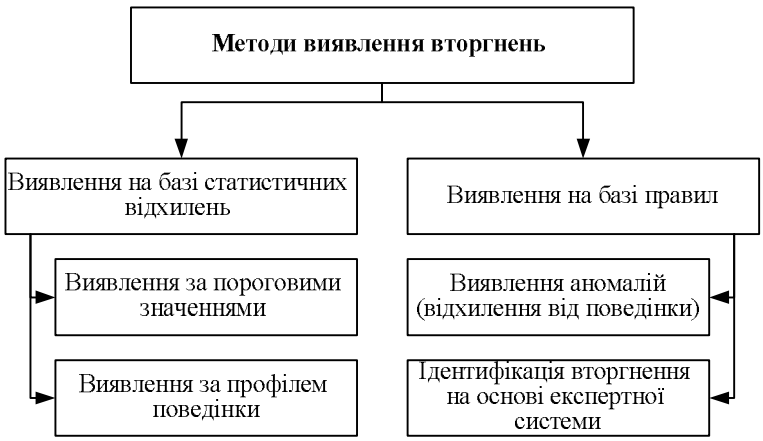

Рис. 1. Класифікація методів виявлення вторгнень

Розглянемо відомі методи виявлення вторгнень в телекомунікаційні системи та мережі, які наведено на рис. 1, обґрунтуємо шляхи їх подальшого розвитку.

Виявлення на базі статистичних відхилень

Це виявлення передбачає збір даних, що характеризують поведінку легальних користувачів, протягом певного часу. Потім ці дані аналізуються із застосуванням статистичних методів, щоб з високим ступенем точності визначити, відповідає поведінка певного користувача поведінці легального користувача чи ні.

По суті, в підході, заснованому на статистичних методах, робиться спроба визначити нормальну або очікувану поведінку, тоді як в підході, заснованому на правилах, робиться спроба виявити фактичну поведінку.

Щодо типів порушників, визначених вище, виявлення статистичних аномалій є ефективним відносно імітаторів, які навряд чи стануть наслідувати поведінку легального користувача, під ім'ям якого

входять в систему. В той же час, ця методика практично непридатна для правопорушників. Проти такого типу атак ефективніший підхід, заснований на використанні правил, що дозволяють розпізнати окремі події й їх послідовності, які в певному контексті означають вторгнення. На практиці в системі реалізується певна комбінація обох підходів, що забезпечує ефективне протистояння широкому спектру порушень.

Основним засобом виявлення порушень є контрольний запис (audit record), в якому повинні записуватися певні операції, що виконуються користувачами для подальшого застосування цих записів як початкових даних системи виявлення порушень. Найчастіше застосовують наступні дві стратегії.

Системні контрольні записи (native audit records). Практично всі операційні системи, розраховані на велику кількість користувачів містять програми для збору інформації про дії, що виконуються користувачами. Перевага використання цієї інформації полягає у відсутності додаткового програмного забезпечення. Недолік пов'язаний з тим, що системні контрольні записи можуть не містити необхідної інформації або можуть містити її в невідповідній формі.

Спеціальні контрольні записи (detection-specific audit records). Можуть бути розроблені і застосовані спеціальні засоби збору інформації, які генерують записи, що містять дані, необхідні тільки для роботи системи виявлення порушень. Перевагою такого підходу є незалежність від постачальника системи і можливість розповсюдження на різні платформи. Як недолік слід зазначити додаткове навантаження на систему у зв'язку з необхідністю виконання двох програм ведення контрольних записів.

Кожен контрольний запис містить наступні поля:

– **Subject (суб'єкт).** Ініціатор дії. Суб'єктом, звичайно, є користувач терміналу, але це може бути і процес, що виконується для користувача або групи користувачів. Всі дії здійснюються по командах, які дає суб'єкт. Суб'єкти можуть бути згруповані в класи по рівнях доступу і ці класи можуть перетинатися;

– **Action (дія).** Операція, що виконується суб'єктом по відношенню до об'єкту, наприклад реєстрація входу в систему, читання, уведення-виведення даних, виконання програм;

– **Object (об'єкт).** Рецептори дій. Прикладами об'єктів є файли, програми, повідомлення, записи, термінали, принтери, а також структури, створені користувачами або програмами. Коли рецептором дії є суб'єкт (наприклад, при отриманні електронної пошти), цей суб'єкт теж розглядається як об'єкт. Об'єкти можуть бути згруповані по типах і відповідно до типу об'єкту і умов оточення. Наприклад, дії в базі даних можуть реєструватися як на рівні бази даних в цілому, так і на рівні окремих записів;

– **Exception-Condition (виняткова ситуація)**. Указує тип виняткової ситуації, якщо вона виникла при виконанні команди повернення;

– **Resource-Usage (використання ресурсу)**. Список кількісних показників, в якому кожен елемент указує об'єм використання того або іншого ресурсу (наприклад, число надрукованих або відображених на екрані рядків, число прочитаних або створених записів, час використання процесора, число задіяних каналів введення-виведення, тривалість сеансу зв'язку);

– **Time-stamp (позначка дати-часу**). Унікальна позначка дати і часу, яка вказує на момент виконання дії.

Більшість дій, що виконуються користувачем, складаються з набору елементарних операцій. Наприклад, копіювання файлу означає виконання команди користувача, що припускає отримання права доступу і створення копії плюс читання з одного файлу, плюс запис в інший файл. Розглянемо команду:

COPY GAME.EXE TO <Library>GAME.EXE, ініційовану користувачем Serg з метою копіювання виконаного файлу *GAME* з поточного каталогу в каталог *<Library>*. У цій ситуації можуть генеруватися наступні контрольні записи:

Serg	execute	<Library>COPY.EXE	0	CPU=00002	11058721678
Serg	read	<Serg>GAME.EXE	0	RECORDS=0	11058721679
Serg	execute	<Library>COPY.EXE	write-viol	RECORDS=0	11058721680

У прикладі процес копіювання був завершений аварійно, оскільки користувач Serg не має права запису в каталозі *<Library>*.

Розкладання дій користувача на елементарні операції має наступні переваги.

Оскільки об'єкти в системі є додатками, що захищаються, використання елементарних операцій дозволяє простежити за всіма діями, які виконуються з даним об'єктом. Система може виявляти спроби порушення контролю доступу (за відсутності відхилень від норми виняткових ситуацій) і виявляти успішні випадки таких порушень (за відсутності відхилень від норми в наборі об'єктів, доступних даному суб'єкту).

Принцип створення контрольних записів для кожного об'єкту і кожної дії спрощує модель та її реалізацію.

Зважаючи на просту і одноманітну структуру спеціальних контрольних записів, відносно просто одержати відповідну інформацію або її частину шляхом копіювання з наявних системних контрольних записів в спеціальні контрольні записи.

Виявлення за пороговими значеннями (threshold detection). Даний підхід припускає визначення незалежних від конкретного користувача порогових значень, що характеризують частоту виникнення різних подій. Цей метод припускає ведення обліку частоти виникнення подій певного типу за певний інтервал часу. Якщо частота перевищує значення, яке вважається розумним, система розглядає цей інцидент як вторгнення порушника.

Аналіз порогових значень в чистому вигляді стає дуже грубим і неефективним методом виявлення, навіть, у разі атак середньої складності. Необхідно правильно визначити і порогові значення, і тимчасові інтервали. Оскільки користувачі працюють по-різному, просте використання порогових значень призведе або до численних помилкових спрацьовувань (false positive), або до численних помилкових неспрацьовувань (false negative). Проте, простий детектор перевищення порогових значень може бути корисним в сукупності з іншими складнішими методами.

Виявлення за профілем поведінки (profile-based detection). Створюється профіль активності користувача і за допомогою цього профілю виявляються відхилення в поведінці користувача, що реєструється в системі під даним ім'ям.

Виявлення за профілем поведінки будується на вивченні попередньої поведінки, користувача або групи користувачів і порівнянні цієї поведінки з поточною поведінкою на предмет виявлення значних відхилень. Профіль може складатися з набору параметрів, так що відхилення по одному з параметрів може бути недостатнім для того, щоб генерувати системну тривогу.

Даний підхід спирається на аналіз вмісту контрольних записів. Контрольні записи забезпечують введення для функції виявлення порушень наступним чином. По-перше, розробник повинен вирішити, яке число параметрів необхідно відстежувати в поведінці користувача. Щоб виявити профіль активності типового користувача, можна провести аналіз контрольних записів впродовж деякого періоду часу. По-друге, вміст поточних записів служить як початкові дані, по яких виявляються порушення. Таким чином, пропонована модель виявлення порушень припускає аналіз поступаючих контрольних записів поведінки на предмет відхилення цієї поведінки від звичайного.

Прикладами параметрів, які виявляються корисними при виявленні порушень за профілем поведінки, є наступні.

Лічильник (counter). Невід'ємне ціле число, значення якого можна збільшувати, але не зменшувати, до тих пір, поки це значення не буде переустановлене в результаті дії програми управління. Звичайно підрахунок числа певних подій, що спостерігалося, ведеться протягом деякого проміжку часу. Прикладами можуть бути число спроб входу в систему, зроблених користувачем протягом однієї години, число викликів певної команди протягом сеансу роботи користувача або число неправильно введених паролів протягом однієї хвилини.

Датчик (gauge). Невід'ємне ціле число, значення якого може як збільшуватися, так і зменшуватися. Звичайно датчик призначений для реєстрації поточного значення деякої характеристики об'єкту. Прикладами є число логічних з'єднань, встановлених застосуванням користувача, або число вихідних повідомлень, поставлених в чергу призначеним процесом.

Інтервальний таймер (interval timer). Довжина періоду часу між двома послідовними подіями. Наприклад, довжина періоду часу між двома послідовними спробами реєстрації по одному і тому ж обліковому запису.

Показник використання ресурсу (resource utilization). Обсяг споживання ресурсу за певний проміжок часу. Прикладами є число сторінок, віддрукованих за час сеансу роботи, або загальний час виконання певної програми.

З цими кількісними показниками можна використовувати різні тести, для з'ясування правомірності поточної діяльності користувача. При цьому можна використовувати наступні методи:

– метод середніх значень і середньоквадратичних відхилень;
– метод багатовимірної моделі;
– метод марківських процесів;
– метод часових рядів;
– операторний метод.

Найпростіший статистичний тест полягає в розгляді середніх значень і середньоквадратичних відхилень параметрів за певний період часу. Результати характеризують середню поведінку і його відхилення від середньої. Використовувати середні значення і середньоквадратичні відхилення можна для широкого спектру лічильників, таймерів і показників використання ресурсів. Але значення цих параметрів самі по собі звичайно дають дуже приблизну оцінку, щоб використовувати їх безпосередньо в цілях виявлення вторгнення.

Метод багатовимірної моделі ґрунтується на використанні кореляції між двома або декількома змінними. Поведінку порушника можна характеризувати з більшою надійністю, розглядаючи такі ко-

реляції (наприклад, часу використання процесора і ресурсів або частоти входу до системи і тривалість сеансу роботи).

Метод марківських процесів служить для визначення імовірності переходів між різними станами. Наприклад, ця модель дозволяє з'ясувати характер зв'язку між певними командами.

Метод часових рядів заснований на аналізі інтервалів часу з метою виявлення подій, які проходять або дуже швидко, або дуже поволі. При цьому для того, щоб охарактеризувати тимчасові аномалії, теж можна застосувати різні статистичні перетворення.

Нарешті, операторна модель базується, швидше, на визначенні того, що вважається таким, що виходить за рамки звичайної поведінки користувача, а не на автоматичному аналізі вмісту збережених контрольних записів. Звичайно встановлюються чітко певні межі, і вихід за ці межі розглядається як підозра на вторгнення в систему. Цей підхід краще всього працює тоді, коли поведінка порушника характеризується певними типами його дії. Наприклад, велике число спроб входу до системи і реєстрації за короткий період часу дозволяє зробити висновок про спробу вторгнення. Як приклад використання розглянутих вище параметрів і моделей розглянемо табл. 1.

Таблиця 1

Критерії, використовувані для виявлення порушень

Критерій	Модель	Тип порушень, що виявляються
Вхід до системи і сеанс роботи користувача		
Частота входів до системи по днях і годинах	Середні значення і середнє квадратичне відхилення	Порушники, найімовірніше, намагаються увійти до системи в неробочий час
Частота входів до системи з різних місць	Так само	Порушники можуть входити до систем з таких місць, де відповідний користувач буває дуже рідко або не буває ніколи
Тривалість сеансів роботи	Так само	Значні відхилення можуть означати роботу імітатора
Об'єм даних, що пересилаються в певне місце	Так само	Дуже великі об'єми даних, передані на видалені вузли, можуть означати просочування важливої інформації
Показник використання ресурсів в час сеансу	Так само	Показники завантаження процесора або пристроїв введення-виводу, що виходять за рамки звичайних, можуть означати роботу порушника
Час, що пройшов з моменту останнього входу до системи	Операторна модель	Спроба вторгнення до системи по "нічийному" обліковому запису
Число введень неправильних значень пароля при реєстрації	Так само	Спроби проникнення до системи за допомогою вгадування пароля
Невдалі спроби входу до системи з певних терміналів	Так само	Спроби вторгнення до системи
Виконання команд або програм		
Частота запуску програм	Середні значення і середнє квадратичне відхилення	Може вказувати на присутність порушника, який пробує доступні йому команди, чи на легального користувача, що дістав доступ до привілейованих команд
Використання ресурсів програмами	Так само	Значення, що виходить за рамки звичайного, може означати впровадження вірусу або троянського коня, які у фоновому режимі виконують операції, що збільшують завантаження системи введення-висновку або процесора
Число відмов виконання	Операторна модель	Може означати спроби легального користувача одержати привілеї вищого рівня
Доступ до файлів		
Частота виконання операцій читання, запису, створення, видалення	Середні значення і середнє квадратичне відхилення	Частота, що виходить за рамки звичайної, операцій доступу до файлів для читання і запису може означати присутність імітатора або проглядання ресурсів
Підрахунок невдалих спроб читання, запису, створення	Операторна модель	Можуть виявляти користувачів, які постійно намагаються дістати несанкціонований доступ до файлів

В табл.. 1 зібрані повідомлення про різні критерії, що враховуються в системі виявлення порушень IDES, використовуваній в Станфордському дослідницькому інституті (SRI – Stanford Research Institute).

Головна перевага використання статистичних профілів полягає в тому, що для їх застосування не потрібно наперед знати про всі вади в системі захисту. Програма-детектор з'ясовує, яка поведінка є "нормальною", а потім виявляє відхилення. Даний підхід не засновано на характеристиках системи і відомостях про її уразливість, тому відповідна реалізація легко переноситься з однієї системи на іншу.

Виявлення на базі правил

Припускає розробку набору правил, на основі яких ухвалюється рішення про те, що даний тип поведінки є поведінкою порушника. Передбачають відстеження подій, що відбуваються в системі, і застосування набору правил, за якими можна винести висновок, чи є дана поведінка підозрілою чи ні.

Виявлення аномалій. Розробляються правила, що дозволяють виявити відхилення від поведінки, які спостерігались раніше.

Виявлення аномалій схоже по підходам і можливостям на методи виявлення статистичних аномалій. При використанні бази правил аналіз збережених контрольних записів проводиться з метою виявлення характеристик типової поведінки і автоматичного генерування правил, що описують таку поведінку. Правила можуть представляти поведінкові шаблони користувачів, програм, привілеїв, тимчасових інтервалів, терміналів і т.п. Потім спостерігається поточна поведінка, і кожна транзакція перевіряється по набору правил на предмет її відповідності одержаним раніше поведінковим шаблонам.

Як і при виявленні статистичних аномалій, виявлення аномалій, заснованих на правилах, не вимагає знання вразливих місць захисту системи. Схема спирається на спостереження за поведінкою користувачів і на припущення, що в майбутньому ця поведінка не повинна істотно змінитися. Щоб цей підхід виявився ефективним, буде потрібна достатньо велика база правил.

Ідентифікація вторгнення. Підхід на основі використання експертної системи, що виявляє підозрілу поведінку.

Ідентифікація подолання захисту заснована на абсолютно іншому підході, пов'язаному з технологією експертних систем. Основною межею таких систем є використання правил для ідентифікації відомих видів вторгнень або вторгнень, побудованих на відомих недоліках системи захисту. Можна визначити і правила для ідентифікації підозрілої поведінки, навіть якщо поведінка не виходить за рамки типової. Звичайно правила, вживані в таких системах, залежать від конкретного типа машини і операційної системи.

Крім того, такі правила генеруються експертами, а не в результаті автоматичного аналізу контрольних записів. Найчастіше проводиться опитування системних адміністраторів і аналітиків системи захисту, для отримання відомих сценаріїв і подій, що несуть загрозу безпеці системи, яка захищається. Таким чином, успіх даного підходу залежить від професіоналізму тих, хто бере участь у виробленні системи правил.

Простий приклад типів правил, які можуть при цьому використовуватися, можна знайти в системі NDIX – одній з перших систем евристичних правил, за допомогою яких можна визначити ступінь підозрілості тієї або іншої діяльності.

Приклади таких евристичних правил описані нижче.

– Користувачі не повинні читати файли, що знаходяться в особистих каталогах інших користувачів.

– Користувачі не мають права записувати інформацію у файли, що належать іншим користувачам.

– Користувачі, які постійно працюють з системою, часто при новому вході до системи відкривають ті ж файли, які вони використовували раніше.

– Користувачі рідко відкривають дискові пристрої безпосередньо, а використовують для цього утиліти вищого рівня, пропоновані операційною системою.

– Користувачі не повинні відкривати декілька сеансів роботи з однією і тією ж системою одночасно.

– Користувачі не копіюють системні програми.

Схема ідентифікації вторгнень, реалізована в системі IDES, заснована на описаній вище стратегії. Контрольні записи у міру їх появи перевіряються по базі правил.

Якщо виявляється збіг, відбувається збільшення рейтингу підозри (suspicion rating) користувача. Якщо збіги спостерігаються для достатньо великого числа правил, рейтинг перевищує заданий поріг і система генерує звіт про виявлену аномалію.

Підхід IDES заснований на перевірці контрольних записів. Слабкою стороною цього підходу є недостатня гнучкість.

Наприклад, можна реалізувати такий сценарій вторгнення, коли система генерує ряд послідовностей контрольних записів, які слабо або майже непомітно відрізняються від інших. При цьому укласти такі відхилення в рамки наявних правил зовсім непросто.

Розподілені системи виявлення порушень

До недавнього часу всі роботи зі створення системи виявлення порушень були зосереджені навколо окремо взятої обчислювальної системи. Проте типовій організації потрібно забезпечити захист ро-

зподіленого комплексу обчислювальних вузлів, об'єднаних локальною мережею або засобами міжмережевої взаємодії. Звичайно, можна захистити кожен окремий вузол, використовуючи в кожному з них свою систему виявлення порушень, але ефективніший захист досягається шляхом координації і взаємодії систем виявлення порушень в мережі. Таким чином, формулюються наступні головні питання, що виникають при проектуванні розподіленої системи виявлення порушень.

Розподіленій системі виявлення порушень, можливо, доведеться мати справу з різними форматами контрольних записів. У гетерогенному середовищі різні системи використовують різні системи створення контрольних записів, тому для виявлення порушень ці системи можуть мати різні формати для створюваних контрольних записів.

Деякі вузли мережі повинні бути місцем накопичення і аналізу даних, що поступають до них від всіх інших систем в мережі. Тому сирі контрольні або вже оброблені дані повинні передаватися по мережі. Тобто, необхідно забезпечити цілісність і конфіденційність цих даних. Цілісність не дозволить порушнику маскувати свою діяльність шляхом зміни переданої контрольної інформації. Конфіденційність потрібна тому, що контрольна інформація може виявитися дуже важливою з точки зору підтримки працездатності системи.

Система може мати як централізовану, так і децентралізовану архітектуру.

У першому випадку передбачається наявність одного центру, де накопичуються і аналізуються всі контрольні дані. Це спрощує завдання узгодження звітів, що поступають, але створює потенційно "вузьке місце", відмова якого може привести до виходу з ладу всієї системи.

При використанні децентралізованої архітектури є декілька аналітичних центрів, проте при цьому потрібно координувати їх діяльність і організувати обмін інформацією між ними.

Хорошим прикладом розподіленої системи виявлення порушень є система, яка представлена на рис. 2.

На цьому рисунку показана загальна архітектура цієї системи, що складається з наступних трьох основних компонентів.

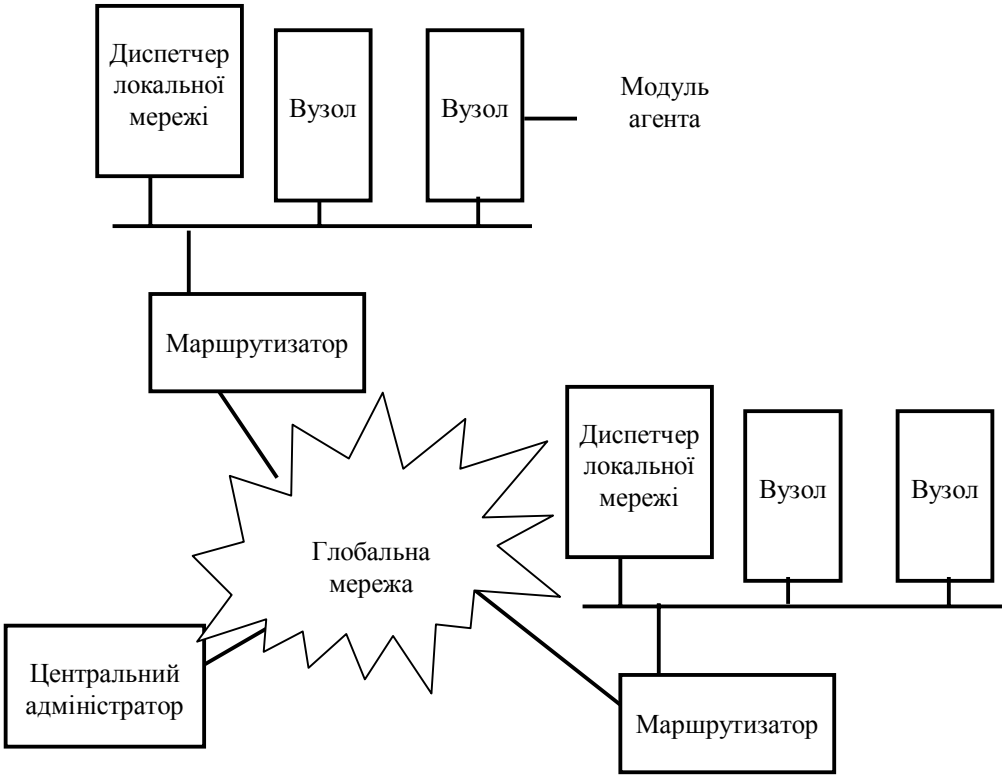

Рис. 2. Архітектура розподіленої системи виявлення порушень

Модуль агента вузла. Модуль збору контрольної інформації, що виконується у фоновому режимі в системі, за якою ведеться спостереження. Метою модуля є збір даних про події, що мають відношення до захисту вузла і передача цих даних модулю центрального адміністратора.

Модуль агента диспетчера локальної мережі. Робота цього модуля аналогічна роботі модуля агента вузла, але даний модуль аналізує потік даних локальної мережі, теж передаючи одержані ним дані модулю центрального адміністратора.

Модуль центрального адміністратора. Приймає повідомлення, що поступають від агентів вузлів і агента диспетчера локальної мережі, обробляє ці повідомлення, з'ясовуючи їх кореляцію і намагаючись виявити порушення.

Схема розроблялася з тим, щоб бути незалежною від операційної системи і конкретних реалізацій системи контролю.

На рис. 3. показана схема загального підходу, що застосовувався в цьому випадку. Агент переглядає кожен контрольний запис, породжений системою реєстрації контрольних параметрів відповідної системи.

Записи, що не мають інтересу з погляду захисту, фільтруються. Записи, що залишилися, перетворяться в стандартний формат контрольного запису головного вузла (HAR – host audit record). Потім набір шаблонів, який використовував логічний модуль аналізує одержані записи на предмет виявлення підозрілих дій. Перш за все, агент проводить пошук в записах подій, що представляють інтерес з точки зору безпеки незалежно від їх зв'язку з минулими подіями.

Прикладами таких подій є відмови в доступі до файлів, доступ до системних файлів і зміна параметрів контролю доступу до файлів.

На наступному рівні пошуку агент шукає послідовності подій, відповідних вже відомим спробам злому (так звані сигнатури).

Нарешті, агент намагається знайти аномалії поведінки окремих користувачів, ґрунтуючись на профілі кожного користувача, що містить відомості про число виконуваних програм, число файлів, до яких отримано доступ, і т.п.

Якщо виявляється підозріла активність, центральному адміністратору надсилається повідомлення.

Модуль центрального адміністратора включає експертну систему, здатну виявляти взаємозалежність одержаних даних. Модуль центрального адміністратора може також запитати у окремих вузлів копії їх записів HAR, щоб порівняти їх із записами інших агентів.

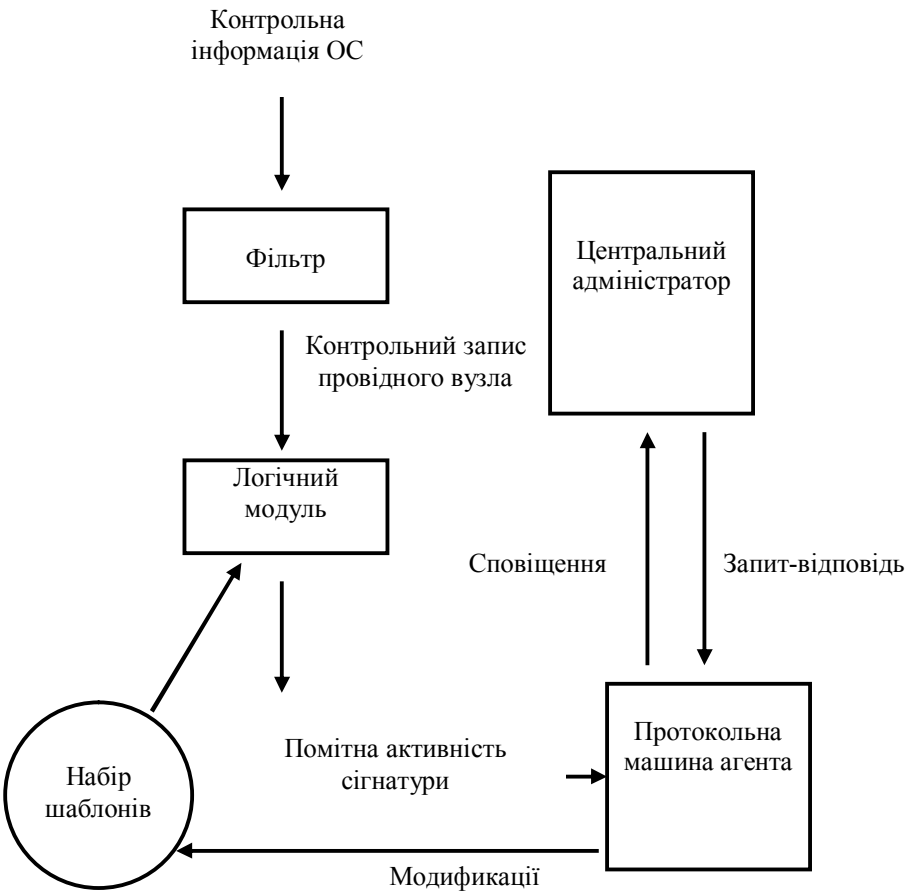

Рис. 3. Архітектура агента

Модуль агента диспетчера локальної мережі теж надає зібрані їм дані модулю центрального адміністратора.

Агент диспетчера локальної мережі контролює з'єднання між вузлами, використані служби і рівень трафіку.

Цей агент реєструє всі помітні події, наприклад різка зміна завантаження мережі, використання служб захисту і мережеві операції типу rlogin.

Таким чином, архітектурні рішення, показані на рис. 2 і 3, виявляються достатньо загальними і гнучкими, щоб лягти в основу машинно-незалежного підходу, що дозволяє створити реалізацію, масштабовану від системи виявлення порушень на рівні окремого вузлу до рівня всієї мережі, дозволяючи на основі порівняння активності окремих вузлів виявляти підозрілі дії, які інакше залишалися б непоміченими.

Висновки

Проведені дослідження показали, що одним із ефективних шляхів захисту інформаційних ресурсів телекомунікаційних мереж та систем є розробка та впровадження систем виявлення та протидії вторгненням.

Перспективним напрямком подальших досліджень є обґрунтування математичних моделей та критеріїв, за якими виконується аналіз та обробка даних щодо поведінки окремих користувачів та інформаційних процесів, розробка на їхній основі програмно-технічних комплексів виявлення та протидії вторгненням в телекомунікаційні мережі та системи.

Список літератури

1. *Mihai Christodorescu, Somesh JhaTesting. Malware Detectors. Proceedings of the ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA'04), Boston, Massachusetts, USA, July 11-14, 2004, 11p.*

2. *McAfee AVERT. Virus information library [Електрон. ресурс]. – Режим доступу: http://us.mcafee.com/virus Info/default.asp.*

3. *Symantec Antivirus Research Center. Expanded threat list and virus encyclopedia. Published online at http://securityresponse.symantec.com/avcenter/venc/data/ cih.html.*

4. *West Coast Labs. Anti-virus Checkmark level 2. Published online at http://www.check-mark.com/checkmark/ pdf/Checkmark_AV2.pdf.*

5. *Сайт symantec.com [Електрон. ресурс]. – Режим доступу: http://www.symantec.com/security_response/ definitions.jsp.*

6. *Сайт av-test.org[Електрон. ресурс]. – Режим доступу: http://www.av-test.org/down/papers/2004-02_vb_ outbreak.pdf.*

7. *K. Brunnstein. "Heureka-2" AntiVirus Tests. Virus Test Center, University of Hamburg, Computer Science Department, Mar. 2002. [Електрон. ресурс]. – Режим доступу: http://agn-www.informatik.uni-hamburg.de/vtc/ en0203.htm.*

8. *Джей Бил. и др. Snort 2.1. Обнаружение вторжений. – М.: ООО «Бином-Пресс», 2006. – 656 с.*

Надійшла до редколегії 9.01.2012

Рецензент: д-р техн. наук, проф. О.О. Кузнецов, Харківський університет Повітряних Сил ім. І. Кожедуба, Харків.

ИССЛЕДОВАНИЕ МЕТОДОВ ВЫЯВЛЕНИЯ ВТОРЖЕНИЙ В ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ И СЕТИ

Д.А. Даниленко, А.А. Смирнов, Е.В. Мелешко

Рассматриваются методы повышения безопасности телекоммуникационных сетей и систем, в частности, исследуются методы выявления вторжений (нарушений), которые функционируют с применением статистических критериев и анализа отклонений от установленных правил действий легитимных пользователей. Исследуются математические модели и критерии, которые применяются для выявления вторжений, анализируется архитектура распределенных систем выявления нарушений и архитектура соответствующих агентов телекоммуникационной сети.

Ключевые слова: *телекоммуникационные системы и сети, система выявления вторжений.*

THE METHOD STUDY OF THE REVEALING THE INVASIONS IN TELECOMMUNICATION SYSTEM AND NETWORK

D.A. Danilenko, A.A. Smirnov, E.V. Meleshko

Are considered methods of increasing to safety of the telecommunication networks and systems, in particular, are researched methods of the revealing the invasions (the breaches), which function with using the statistical criterion and analysis of the detours from installed rules action legitimate of the users. They Are Researched mathematical models and criteria, which are used for revealing the invasions, is analysed architecture of the portioned systems of the revealing the breaches and architecture corresponding to agent to telecommunication network.

Keywords: *telecommunication systems and network, system of the revealing the invasions.*