УДК 683.05

Б.В.Дурняк, О.В. Шевченко

АЛГОРИТМ ФУНКЦІОНУВАННЯ СИСТЕМИ ЗАХИСТУ

Детально розглянуті алгоритми виявлення атак у середовищі мереж зв`язку.

In detail the algorithms of exposure of attacks are considered in the environment of communication network

Функціонування системи захисту тісно зв`язано з методами реалізації атак та з рівнем небезпеки, на який може наражатися об`єкт охорони. Методи реалізації атак залежать від цілого ряду факторів:

- наявності загроз у об'єкті, що охороняється;
- рівня розвитку, міри складності системи зв`язку об'єкта, що охороняється, з зовнішнім світом;
- від характеру і доступності інформації про об`єкт;
- від наявності та цінності цілей, які можна було би визначити, для кожної з атак;
- від повноти даних, про можливі події, що пов`язані з порушенням безпеки об'єкта, якими володіє система безпеки об`єкту S^Z у рамках моделей, які використовуються об`єктом, для управління його основними процесами.

Наявність загроз є досить складним фактором. Оскільки, загроза, як така визначається лише у тому випадку, коли існує деяка властивість об`єкту, якою може скористатися певний процес і існує такий процес, який по відношенню до об`єкту, що володіє відповідною характеристикою, або особливістю, приводить до порушення або зменшення рівня безпеки системи. У зв`язку з цим, певна властивість, яка ніколи не використовується процесами, що направлені на порушення безпеки, ніколи не буде інтерпретуватися як загроза до того моменту, поки вона не буде використана атакою. Щоб вийти з такої залежності у визначені загрози, при проектуванні системи захисту S^Z необхідно поступати наступним чином:

- визначити можливі небезпеки, які можуть ініціювати активні дії у вигляді атак по відношенню до об`єкту, що охороняється;
- на основі таких небезпек проектують можливі атаки на об`єкт захисту, які представляють у вигляді послідовності подій, що можуть відбуватися на об`єкті і залежати одна від одної;
- кожна атака, що орієнтована на конкретний об`єкт і є відомою, використовує властивості, або особливості об'єкта, які не створювались спеціально у зв`язку з забезпеченням тих, чи інших функціональних можливостей об'єкта, а являються наслідком дії різних факторів, починаючи

від методів проектування системи та кінчаючи випадковими подіями, що призвели до їх виникнення; відповідні особливості ідентифікуються, як загрози;

- на основі даних, що приведені у попередніх пунктах, у рамках системи S^Z формуються моделі, які дозволяють виявляти атаки на різних стадіях їх існування та формують засоби протидії відповідним атакам;

- засоби протидії створюються таким чином, щоб кожний з засобів міг протидіяти по можливості, як можна ширшому колу типів атак.

Приведені вище фактори не завжди у повній мірі використовуються, чи приймаються до уваги, оскільки вони визначають міру захисту, яку може забезпечити відповідна S^Z. Необхідна міра захисту визначається на основі двох підходів:

- на основі оцінки втрат, до яких можуть привести успішні атаки на систему, при цьому, не розглядаються втрати зв`язані з руйнуванням системи;

- на основі аналізу атак, що мали місце по відношенню до системи, при цьому приймається до уваги кількість атак, цілі атак та інші фактори, що відображають особливості атак на об`єкт, який охороняється.

Проблеми оцінки рівня захищеності об'єкта та методи здійснення цих оцінок, у даному випадку, розглядатися не будуть. Зупинимося більш детально на алгоритмах виявлення атак, що можуть бути реалізовані на основі моделі H^{LG} та у рамках інших засобів, що використовуються у системі управління ТКС. Модель H^{LG} описує події, що можуть виконати у системі, їх зв`язок з загрозами, які відомі і існують у системі. Події $x_{ij}$, що відображені у моделі $H^{LG}$ можуть обумовлюватися не тільки атаками, а й відповідати переліку подій, що передбачаються штатними режимами роботи. Така ситуація має місце у зв`язку з тим, що атаки, які формуються у системах S^N, повинні задовольняти ряду вимог, до яких можна віднести:

- процес реалізації атаки в об`єкті повинен забезпечувати максимальну невидимість свого протікання на всіх стадіях реалізації атаки;

- процес реалізації атаки повинен, по можливості, володіти властивостями адаптації до непередбачуваних змін, при її реалізації у середовищі об`єкту атаки;

- факт досягнення атакою цілі повинен маскуватися, якщо характер атаки не являється агресивним і ціль атаки не передбачає інформування об`єкту атаки про успішне досягнення атакою цілі;

- атака повинна формуватися таким чином, щоб у мінімально можливий мірі, по закінченні атаки можна було ідентифікувати систему небезпеки S^N, що її сформувала;

- атака, по можливості, повинна бути здатною до адаптації по відношенню до цілі атаки.

Невидимість атаки для об'єкта, який атакується, є однією з ключовий властивостей атаки, оскільки у залежності від цього параметру атака може досягнути, чи не досягнути цілі, через те, що буде виявлена на стадіях зародження, чи розвитку. Основними умовами досягнення цілі атакою являються наступні:

- процес зародження атаки на процес розвитку атаки повинні реалізовуватися на основі використання невідомих об'єкту небезпек, чи на основі використання невідомих параметрів подій, що ініціюються у процесі реалізації атаки на згаданих вище стадіях;
- події, що ініціюються атакою повинні відповідати по своїх зовнішніх атаках подіям, що передбачені штатними режимами роботи системи, що атакується відповідною атакою;
- на етапах зародження та розвитку, процес реалізації атаки не повинен впливати видимим чином на поточний штатний режим роботи системи;
- тіло атаки повинно бути максимально невидимим у середовищі, в якому атака реалізується.

Властивості адаптації атак до непередбачуваних ситуацій, що можуть виникнути у процесі реалізації атаки, чи у результаті неповних даних про об`єкт, які були отримані на стадії розвитку, є близькими до властивостей вірусів, що впроваджується у інформаційну систему.

На відміну від адаптивних властивостей вірусів, адаптація процесів, що реалізують атаки повинна бути достатньо оперативною, оскільки ціль атаки може бути актуальною лише на проміжку заданого інтервалу часу. Ця особливість визначає принципову відмінність атак від вірусів, яка полягає у тому, що основною ціллю вірусів є їх проникнення у систему на необмежений час, наприклад з ціллю зміни параметрів функціонування системи. Атака, як певним чином сформована послідовність дій, що визначаються ціллю атаки, являється більш точно орієнтованою, і детально визначеною відповідною ціллю. Наприклад, атака може бути орієнтована на проведення конкретних змін в об`єкті атаки. Атака може бути орієнтована на несанкціоновану модифікацію конкретних даних, або їх несанкціоновану пересилку у систему $S^N$ і т.д. У даному випадку, під атакою будемо розуміти певного «інтруза», який у відповідності з термінологією прийнятою у галузі захисту комп`ютерних мереж представляє собою, у більшості випадків програмну компоненту сформовану у S^N і впроваджену в об`єкт, щ охороняється.

Атаки не агресивні являються більш небезпечними ніж атаки агресивні у силу того, що останні цілеспрямовані не тільки на виконання певних не-уповноважених дій, а й неспрямовані на інформування об'єкта охорони про успішне виконання дій відповідною атакою. У зв`язку з цим, система захисту $S^Z$ у значній мірі повинна орієнтуватися на виявлення неагресивних атак, оскільки їх успішна дія на об`єкт може бути не виявлена взагалі, що

завжди приводить до значно більших втрат ніж дія агресивних атак. Таким чином, система захисту S^Z повинна реалізовувати певну стратегію функціонування, у рамках якої незалежно від того, чи проявився інтруз у системі певним чином, чи ні, повинна розв`язуватися задачами пошуку у системі слідів перебування інтруза. На основі виявлення таких слідів система захисту відшукує відповідного інтруза.

Оскільки у середовищі мереж зв`язку пов`язані між собою всі засоби, включаючи комп`ютери різної функціональної орієнтації, то фізичним джерелом відповідного інтруза, являється деякий комп`ютер, або інше обладнання, що підключене до мережі. У зв`язку з цим, відповідний інтруз буде у тій чи іншій мірі вміщати інформацію про джерело своєго походження.

Наприклад, для передачі інформації по мережі використовуються протоколи, які несуть досить повну інформацію про джерело відповідних пакетів, більш того, зміст інформації, що передається, або циркулює у мережі, може відображати особливості та прикмети джерела, що її згенерувало у мережу. З іншого боку, не уповноважена діяльність в інформаційному середовищі відслідковується, і у випадку встановлення адресату відправки по відношенню до останнього можуть використовуватись ті чи інші випереджувальні заходи, які забезпечили б неможливість повторення такої діяльності. Тому система захисту, у випадку виявлення слідів інтруза, повинна не тільки виявити останнього, а й по можливості, як можна точніше визначити джерело походження відповідного інтруза з тим, щоб організувати відповідні системні санкції по відношенню до системи небезпеки S^N .

При формуванні атаки у S^N , основою для її проведення та основою для вибору методу, чи способу її формування є наступні фактори:

- ціль атаки;
- особливості функціонування об`єкту захисту;
- загрози, на основі використання яких планується формувати відповідну атаку.

Якщо адаптація по відношенню до непередбачуваних ситуацій, що складається в об`єкті атаки реалізується на стадіях зародження та розвитку атаки, то на стадії дії атаки на об`єкт, атака повинна мати здатність адаптуватися до сформованої в S^N цілі атаки. Справа у тому, що у межах інтруза, ціль атаки безпосередньо не представлена, як окрема його компонента. Вона визначає і впливає на всі прояви його функціонування. На етапі дії на об`єкт, коли відповідна ціль безпосередньо реалізується, може виявитися, що така дія не приводить до осягнення очікуваної цілі. Наприклад, якщо ціллю інтруза являється завантаження у тіло інтруза деяких даних з ціллю їх пересилки до об`єкту S^N , то це є типова ціль для інтрузів типу троянських коней. Відповідна дія, по переписуванню даних без

додаткового їх аналізу на предмет їх ідентичності цілі атаки, може привести до того, що передані до S^N дані не будуть відповідати початковим вимогам, що окреслені ціллю.

У цьому випадку, для уникнення таких результатів дії інтруза, останній повинен адаптуватися до цілі, яка описує ознаки даних, які необхідно переслати у S^N. Такими ознаками, у найпростішому випадку, можуть служити дані, що відображають специфікацію інформації, яка розшукується інтрузом. Наприклад, такою специфікацією може служити ідентифікація даних, що описує накладну, в якій знаходять найменування товарів, їх ціна та кількість. Відповідна специфікація може представляти собою спеціальні ідентифікатори, або внутрішню структуру файлу, в якому відповідні дані розміщаються.

Досить детальний аналіз різних особливостей поведінки інтруза та особливостей його можливостей необхідний для того, щоб можна було сформувати базовий алгоритм, або ряд алгоритмів їх виявлення та протидії відповідним інтрузам, який реалізується засобами, що знаходяться у рамках системи захисту об'єкта S^Z. На рисунку 4.1. приведено фрагмент блок-схеми базової версії алгоритму виявлення та протидії деяким класам атак та інтрузам, яких будемо вважати носіями або тілом відповідних атак.

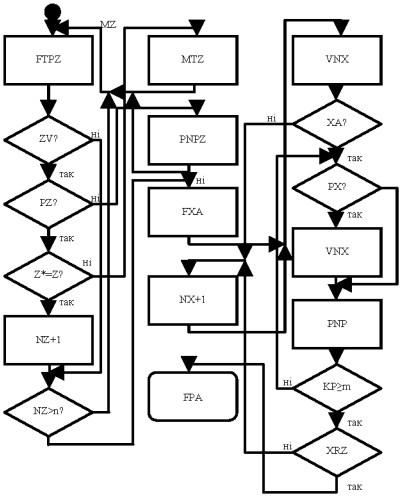

Рис. 4.1. Фрагмент блок-схеми функціонування системи захисту

На рисунку використовуються наступні скорочення:

- FTPZ – формування тестової послідовності для виявлення загрози в об`єкті, що охороняється;
- ZV – перевірка чи виявлена загроза;

- PZ – перевірка чи всі параметри загрози проаналізовані;

- Z*=Z – перевірка, чи розпізнана загроза є новою в об`єкті, що охороняється;

- NZ+1 - збільшуємо лічильник загроз, які є в об`єкті, що охороняється;

- NZ>n? - чи кількість загроз більша деякої визначеної величини;

- PNPZ - вибираємо наступний параметр загрози;

- MTZ - модифікуємо тести для нової загрози;

- FXA - формуємо умови виконання моніторингу подій;

- VNX - вибираємо чергову подію;

- XA - перевіряємо, чи подія активізована;

- PX - перевіряємо, чи черговий параметр, або причина виникнення події належить події, що аналізується на даному етапі;

- VNZ - обчислюємо величину параметра події;

- PNP - переходимо до наступного параметра події;

- KP≥m - перевіряємо, чи кількість параметрів події не перевищила визначеного значення m;

- NX+1 - переходимо до наступної події;

- XRZ - перевіряємо, чи подія, що аналізується зв`язана з загрозами, що були виявлені і проаналізовані;

- FPA - формуємо елемент профілю атаки.

Перш ніж коментувати приведену блок-схему, розглянемо загальну організацію процесу моніторування загроз та виявлення атак, що зароджуються. Основою для формування стратегії моніторування являються дані про стан обслуговування системою ТКС запитів споживачів на отримання зв`язку з абонентами. Для цього, у центральній системі управління формуються дані про параметри роботи системи ТКС у цілому. До таких параметрів відносяться наступні:

- середня кількість запитів на обслуговування μ, що поступила у систему за визначений інтервал часу (ΔT);

- середня величина затримки по наданню послуг, що визначаються запитом від користувачів (τ);

- кількість відмов у надані послуг, що наступили у процесі реалізації послуги (δ) за періоди (ΔT), та кількість відмов у наданні послуг при отриманні системою ТКС запитів на послуги зв`язку (υ);

- зміна часу обслуговування окремого запиту для різних типів послуг, що надаються у ТКС (δT);

- кількість виявлених помилок, або збоїв, що появилися у процесі виконання послуг зв`язку, для кожного окремого типу послуги (ρ).

У залежності від особливостей роботи ТКС, чи особливостей типів замовлень на надання послуг зв`язку, приведені параметри можуть бути розширені іншими параметрами, що відображають особливості предметної

області інтерпретації сфери вимог, що характерні для окремих фрагментів розподіленої системи ТКС. Приведені вище параметри аналізуються у рамках окремих фрагментів розподілу системи зв`язку. При цьому, розподіл ТКС на фрагменти здійснюється у просторі, або на основі територіального розподілу всієї ТКС та одночасно розподіл на фрагменти системи ТКС здійснюється у часі. При цьому, для розподілу ТКС у часі використовуються інтервали часу, які мають ознаки циклічності. Наприклад, якщо в якості ознаки циклічності вибрано період, що охоплює один рік, то розподіл ТКС на фрагменти може здійснюватися по ознаках пори року, по квартальному розподілу відповідного часового циклу розподілу системи ТКС і т.д. Очевидно, що ознаками для фрагментації ТКС з ціллю реалізації розподіленості системи, можуть вибиратися параметри, що характеризують процес функціонування ТКС. Наприклад, таким параметром може служити інтенсивність запитів на обслуговування. У цьому випадку, окремі фрагментації можуть бути розподіленими по відношенню до інших параметрів, наприклад, просторових параметрів. Фрагментація яка реалізується у рамках ТКС, в залежності від її ефективності, у процесі функціонування системи може змінюватися. Під ефективністю фрагментації, у даному випадку, розуміється відповідність розподілу значень параметрів, що характеризують роботу ТКС у цілому, з виділеними фрагментами. Наприклад, якщо фрагментація ТКС реалізується по просторовій ознаці, то така фрагментація є ефективною, якщо значення параметру кількості запитів на обслуговування за період часу ΔT, для даного фрагменту, знаходиться у певному діапазоні значень. Ефективність фрагментації може бути абсолютна, коли всі визначені параметри, що характеризують ТКС мають значення, розподіл яких узгоджується з фрагментацією. Ефективність фрагментації є відносною, якщо приведена відповідність не є повною. Це означає, що відповідність між значеннями параметрів та виділеними фрагментами по відношенню до різних параметрів різна. Наприклад, фрагментації φ_i відповідає розподілу значень параметра μ і υ, а розподіл значень параметра ρ даній фрагментації не відповідає. Необхідність фрагментації розподіленої системи ТКС, як і довільної іншої розподіленої системи, обумовлюється тим, що розв`язувати задачі, які пов`язані з забезпеченням необхідних параметрів процесу функціонування системи, доцільно у рамках окремих фрагментів, а не у рамках всієї системи у цілому. У даному випадку, таким параметром являється параметр рівня безпеки системи ТКС. Природно припустити, що з сторони небезпеки, або системи S^N, інтерес до ТКС може обмежуватися рамками тих, чи інших фрагментів. Наприклад, при територіальній фрагментації, у рамках певного фрагменту можуть виникати певного типу канали зв`язку між абонентами, які фізично зв`язані з певними територіями, а S^N може проявляти зацікавленість саме до тих абонентів, і відповідно до їх каналів зв`язку. Аналогічні приклади можна привести і для випадків розподілу ТКС на

фрагменти, що виділені відносно такого параметру як час і т.д.

Завдяки реалізації фрагментації та її узгодження з інтегральними параметрами системи стає можливим оптимізувати стратегії моніторування системи ТКС. Приймаючи до уваги її розподіленість та фізичні розміри, моніторування такого типу системи без врахування її можливої фрагментації може привести до недопустимого ускладнення всього процесу. У зв`язку з важливістю процесів фрагментування розподіленої системи ТКС та можливість динамічної зміни фрагментів, розглянемо формальні методи опису процесів фрагментації та процесів визначення їх узгодженості з інтегральними параметрами системи зв`язку. Оскільки фрагментація системи зв`язана з параметром, по якому така фрагментація проводиться, або з деяким фактором, який може описуватися рядом параметрів, то формально фрагментація може описуватися наступним співвідношенням, яке задається у вигляді:

$$\left[F\left(S^k\right) = f\left(S^k, y_1, \ldots, y_m\right)\right] \rightarrow \left\{\varphi_1\left(S^k\right), \ldots, \varphi_n\left(S^k\right)\right\} \qquad (1)$$

де S^k - система ТКС, $F\left(S^k\right)$ - розподілена система ТКС, яка розділена на фрагменти, або фрагметована S^k, y_i - параметри, що характеризують вибраний фактор, по якому реалізується фрагментація. Наприклад, якщо фактором фрагментації являється простір, то він описується, щонайменше двома параметрами, що визначають координати окремих точок у цьому просторі. Теоретично, можна говорити про багатофакторну фрагментацію, коли окремі фрагменти $\varphi_i\left(S^k\right)$ описуються кількома факторами. У цьому випадку, відповідний розподіл системи S^k на окремі фрагменти буде представляти собою структуру, яка більш важко інтерпретувати у рамках традиційної предметної області W_i. У рамках даної роботи, багатофакторна фрагментація розподіленої системи розглядатися не буде.

Очевидно, що при реалізації фрагментації деякої системи, необхідно визначатися з алгоритмами розподілу системи на окремі фрагменти, або функціями, за допомогою яких можна було би визначити параметри окремого фрагменту і тим самим у рамках всієї системи виділяти окремі фрагменти. Ця задача може розв`язуватися у рамках наступних підходів: шляхом формування аналітичних функцій визначення значень параметрів окремих фрагментів, або за допомогою конструктивних алгоритмів розподілу деякої системи по вибраних ознаках на окремі частини.

1. *Козлов Д.А., Парандовский А.А., Парандовский А.К.* Энциклопедия компьютерных вирусов. - М.: СОЛОН, 2001.
2. *Кивристи А.* Новые подходы к обеспечению информационной безопасности сети. / Компьютер-Пресс, №7, 2000.

Поступила 15.01.2009р.