Матеріали 11-я Междунар. конф. "Крым 2004": Тр. конф. — М., 2004. — 1 электрон. опт. диск (CD-ROM).
4. *Ланде Д.В*. Поиск знаний в Internet. − М.: Диалектика, 2005. − 272 с.
5. *Глушков В.М*. Основы безбумажной информатики / *В.М. Глушков*. − 2-е изд., испр. − М.: Наука, 1987. − 552 с.
6. *Ляпин С.Х*. Многоязычный поиск в электронной библиотеке и его реализация в ИС T-Libra 6.x [Электронный ресурс] / Ляпин С.Х., Куковякин А.В. // XI межд. конф. EVA-2008, Москва, 1-5 дек. 2008 г. – Режим доступа: http://conf.cpic.ru/upload/eva2008/reports/doklad_1389.doc. – Загол. с экрана.

Поступила 23.08.2010р.

УДК 621.372

Б.В.Дурняк, Ю.-Ю.М.Коростіль, С.О.Нікулін

ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ПРОЦЕСУ ЗАХИСТУ ДОСТУПУ СПЕЦІАЛІЗАЦІЇ СИСТЕМИ УПРАВЛІННЯ

Алгоритми реалізації процесу захисту спеціалізованої системи управління представляють собою досить складну структуру в силу наступних причин:

- система алгоритмів складається з алгоритмів окремих функціональних блоків,
- процес функціонування системи захисту як єдиний алгоритм повинен розглядатися як реалізація послідовності певних подій в часі,
- перехід від одного фрагменту алгоритму до іншого може обумовлюватися факторами, які не пов’язані з часом, як базовим параметром системи.

Приймаючи до уваги приведені фактори, перш ніж говорити про формування загального алгоритму функціонування, необхідно розглянути принципи функціонування окремих функціональних блоків системи захисту (SZ) та різні варіанти взаємозв’язку між окремими функціональними блоками.

Блок аналізу загроз (AZG), що входить до складу системи SZ, реалізує задачу виявлення невідомих загроз, які характеризують об’єкт захисту (OZ), і тому його робота ініціюється блоком управління системою захисту (BUSZ), при умові, що з OZ прийшла інформація про успішне завершення однієї з атак. При цьому розпізнавання факту успішного завершення атаки здійснюється відповідним Zh_i на основі даних, які сформувала система управління OZ за участю блока аналізу роботи засобу захисту $ARZh_i$ причиною можливого успішного завершення атаки можуть служити наступні

фактори:

- наявність невідомої загрози, що існувала в OZ з самого початку його функціонування або появилася в результаті певних дій зовнішніх чи внутрішніх факторів, які здійснювалися в процесі функціонування OZ в штатних режимах,
- засіб захисту, що був розміщений у відповідній точці цифрового середовища, виявився нездатним виявити відповідну атаку,
- система моніторингу засобів захисту не забезпечила відповідну точку простору моніторування у відповідний момент необхідним засобом захисту.

У першому випадку AZG виявляє початкову стадію виникнення атаки, яка відповідає процесу співпраці з загрозою, що реально полягає у використанні параметрів, які характеризують ту чи іншу частину OZ, для забезпечення реалізації наступних дій по реалізації атаки. В рамках блока AZG це реалізується шляхом моделювання тієї або іншої загрози, ціллю якої являється результат, що був досягнутий реальною загрозою. Моделювання в даному випадку розглядається як процес, який умовно можна вважати побудовою послідовності подій, що були реалізовані атакою, яка завершилася успішно. Очевидно, що одна і таж ціль може бути досягнена різними способами, що відповідають різним способам реалізації атаки. У цьому випадку блок AZG має наступні можливості, що можуть бути отримані в результаті такого моделювання:

- в результаті моделювання атаки AZG може прийти до загрози, яка не є відомою системі захисту,
- блок AZG може прийти до загрози, яка не є відомою SZ, але не єдиною успішною атакою,
- у першому випадку, коли виявлена в результаті роботи блоку $ARZh_i$, виявлена загроза є відомою, це може означати наступне:
- що процес моделювання в оберненому напрямку виявився на певному етапі помилковим,
- що система моніторингу, яка складається UM та AMZ, не забезпечила систему необхідним засобом захисту в момент появи атаки, яка використала відому загрозу,
- що атака, яка закінчилася успішно, є комплексною і використала в процесі своєї реалізації дві або більше загроз, одна з яких є відомою.

Блок AZG для продовження виявлення загроз розглядає отримані результати у послідовності, що представлена вище. Якщо виявляється, що загроза, яка визначена в процесі оберненого моделювання є відомою, то блок AZG приймає в процесі моделювання переаналізовано фрагмент, який є помилковим. Для цього AZG, починаючи від початку моделі, який приймається в точці завершення атаки, міняє останній крок, або подію, що реалізована на цьому кроці, на альтернативну подію. Альтернативна подія в даному випадку визначається не на рівні механізму її реалізації, а на рівні

інтерпретації відповідної події в межах системи, що об'єднує OZ і SZ, яку будемо називати об'єднаною системою і будемо позначати SB=OZ U SZ, де об'єднання розглядається на рівні інтерпретації безпечного функціонування OSB. В цьому випадку одним із ключових блоків являється блок IKSZ, який вміщає інформаційні компоненти, завдяки яким стає можливим використовувати інтерпретацію тих чи інших подій. Така інтерпретація відомих подій описується семантичними словниками. Інтерпретація подій, які не були описані при формуванні SZ, формується на основі перетворень інтерпретаційних описів, що реалізуються за допомогою відповідної системи перетворень в результаті виконання обернених дій на певному етапі реалізації процесу моделювання повинно виявитися неможливим вибрати альтернативну подію для виконання альтернативного кроку. В цьому випадку також реалізується в протилежному напрямку крок відповідного процесу функціонування моделі реалізації атаки. Якщо в результаті такої процедури блок AZG приходить до загрози, що була вибрана атакою, така загроза повинна бути відмінною від тієї загрози, що визначилась блоком AZG при реалізації першого процесу моделювання. Виявлена таким чином нова загроза передається в систему моніторингу, для того щоб остання забезпечила можливість її контролю над засобами захисту, передає опис відповідної загрози в модуль IKSZ та в блок моделі небезпек MN для розширення можливостей виявлення можливих атак за допомогою блока MN. Крім того, інформація про виявлену, нову загрозу передається системі управління об'єктом, яка разом з останнім реалізується у вигляді блока OZ. Якщо в результаті реалізації процесу функціонування моделі атаки, що реалізується в напрямку, протилежному до реалізації процесу функціонування самої атаки, блок AZG прийшов до загрози, яка не є відомою для SZ, то відповідною інформацією блок AZG розпоряджається так само, як і в першому випадку.

У третьому випадку має місце ситуація, коли атака, що реалізується по відношенню до OZ, використовує кілька загроз. Прикладом такої атаки може служити атака, що використовує троянського коня, який впроваджується в систему, а потім використовується для досягнення певної цілі. В цих двох етапах реалізації однієї атаки, ціллю якої є, наприклад, несанкціоноване заволодіння інформацією, використовуються дві різні загрози. Перша загроза дозволяє здійснити несанкціоноване встановлення в системі троянського коня, і вона може полягати у недостатньому контролі вхідних даних, а друга загроза представляє собою недостатній рівень управління доступом до даних, який повинен був реалізовуватися по відношенню до всіх об'єктів, які можуть мати певний рівень захисту доступу [1, 2]. Тоді моделювання процесу її реалізації повинно складатися з двох частин. Цю ситуацію зручно інтерпретувати шляхом розподілу опису самої кінцевої цілі на дві або більше під цілей, кожна з яких знаходиться по відношенню до інших в певній детермінованій залежності, що формально описується співвідношенням

$$(C^i_1 \to C^i_2 \to \ldots \to C^i_k) \to C^*_i$$

Тоді для реалізації процесу досягнення кожної з цілей, необхідно проводити окремі процедури моделювання процесу реалізації окремих складових атак, які з точки зору способу їх реалізації можуть бути розподіленими в часі та в просторі. Це суттєво ускладнює можливі алгоритми реалізації процесів функціонування блоку AZG. Для останнього випадку необхідно визначитися з критеріями, на основі яких можна було би розпізнати тип атаки, що визначається її розподіленістю. Цю задачу можна було б розв'язувати на основі аналізу результатів дії успішності атаки.

Важливим для SZ є блок моделювання небезпек. Цей блок вміщає описи потенціальних небезпек, а також потенціальних небезпек і в його рамках реалізуються процеси генерації атак. Такий підхід є новим по відношенню до підходів, що використовуються, наприклад, в IDS і полягають у збиранні сигнатур відомих атак [3]. Цей підхід потребує великих баз даних для збереження відомих сигнатур та їх оновлення. Такий самий підхід використовується в антивірусних системах, які функціонують на основі використання еталонів відомих вірусів [4]. В рамках блоку MN існує можливість генерувати можливі атаки на основі даних про саму систему OZ та про дані, які в ній знаходяться. При цьому блок MN може отримувати від OZ дані про поточний стан рівня безпеки, який також визначає можливі способи реалізації атак таким чином, щоб вони виявилися, по можливості, найбільш успішними. Генератори атак, що реалізуються в MN вміщають всю інформацію про загрози, що існують в OZ. Очевидно, що сформовані в MN атаки використовуються засоби захисту типу honeypot, або Zh_i для розпізнавання атак, що можуть діяти на OZ ззовні. Атаки, що генеруються в MN крім параметрів, які їх описують, характеризуються також і зовнішніми по відношенню до атак параметрами. Прикладом таких параметрів можуть служити параметр активності атаки, параметр часу життя атаки та інші. Такі параметри дозволяють оптимізувати процеси розпізнавання атак засобами захисту та оптимізувати роботу системи моніторингу засобів захисту в рамках системи захисту. В рамках даної роботи приймається, що небезпеками являються інформаційні системи, що споріднені з системою, що охороняється. Це дозволяє для формування моделей небезпек і, відповідно, моделювання атак, використовувати дані, що характеризують саму систему OZ.

Окремо виділений засіб захисту для не уповноваженого доступу ZhD, призначений для захисту OZ від спроб несанкціонованого доступу до OZ зі сторони потенціальних користувачів. Відомо, що структура вхідних даних в системах доступу споживачів суттєво відрізняється від структури даних зі сторони мережі. Тому ZhD з точки зору автоматної мережі, що описує поведінку ZhD з зовнішньої точки зору, також відрізняється від засобів захисту Zh_i. Спільним між Zh_i і ZhD є те, що обидва засоби захисту використовують один і той же модуль аналізу роботи засобу захисту $ARZh_i$. Основною відмінністю ZhD від Zh_i є те, що ZhD не є розподіленим у просторі. Це означає, що OZ має обмежену кількість адрес, а приймаючи до

уваги, що OZ є спеціалізована система управління, то однією з її особливостей, які визначають її як спеціалізовану, є обмежена та фіксована кількість адрес доступу користувачів. У більшості випадків таких точок доступу не більше двох чи трьох. У зв'язку з цим по відношенню Zh_i не існує проблем моніторингу відповідних засобів захисту оскільки вони на постійній основі використовуються у визначених точках мережі в рамках нормованих процедур доступу. Єдиний зв'язок ZhD з системою процедур доступу. Єдиний зв'язок ZhD з системою моніторингу полягає у активізації окремих засобів точок доступу. Природно, що такий засіб захисту безпосередньо зв'язаний з OZ, якому знаходиться система доступу. У багатьох випадках система захисту доступу і сама система доступу розглядається як єдине ціле. Це обумовлюється тим, ідентифікація і аут ідентифікація, процедури, що реалізують захист і розглядаються як єдине ціле з двома іншими процедурами, якими може розширятися система доступу. Якщо проводити аналогію з пакетами мережі, які використовуються для зв'язку між вузлами мережі, то ідентифікатор і пароль, які служать для ідентифікації та аут ідентифікації, відповідно, то ідентифікатор і пароль аналогічні адресам, що розміщаються в пакеті. Так само як адреси визначають адреси приймача і джерела пакету, так само ідентифікатор і пароль дозволяють визначити ресурси системи, які потребує споживач та встановити ідентичність споживача. Перше можна розглядати як адресу споживача, а друге як адресу джерела, що буде використовувати відповідні ресурси.

Принципи honeypot в рамках блоку Zh_iD реалізуються наступним чином. Перш ніж передати ідентифікатор і пароль в систему доступу в OZ засіб захисту проводить аналіз параметрів потенціального споживача. Такими параметрами являються:

внутрішні параметри, що знаходяться в блоці IKSZ і характеризують персональні особливості окремого користувача, наприклад, час використання доступу, почерк користувача, якщо доступ реалізується з пультів системи, характер задач, які передбачає або планує виконувати користувач, частоту звертання до системи та ряд інших параметрів, які можуть відображати особливості OZ,

зовнішні параметри, що є додатковими у зв'язку з тим, що система, яка охороняється, є спеціалізованою, наприклад, додаткова інформація про наявність індивідуальних повноважень, додаткове підтвердження уповноважень на момент доступу споживача до системи, що реалізується в період звертання споживача до системи за доступом та ін.

Якщо протягом перевірок, що реалізуються в блоці Zh_iD, не виявлено ознак спроб несанкціонованого доступу, ідентифікатор і пароль передаються в систему доступу OZ. Якщо виявиться, що система доступу OZ не розпізнала користувача по ідентифікатору та паролю, то ця інформація передається ARZhi і останній проводить аналіз стану засобу Zh_iD. Якщо Zh_iD виявив ознаки несанкціонованого доступу, то ідентифікатор і пароль не передаються у блок доступу OZ, але Zh_iD не відмовляє користувачу у

доступі, а починає реалізовувати процес імітації співпраці з користувачем наступним чином. Перш за все, ZhiD передає в OZ інформацію про пароль і ідентифікатор для перевірки системою доступу OZ чи відповідний користувач є зареєстрованим в OZ. Якщо він зареєстрований, то OZ передає інформацію про його повноваження в ZhD, в якій знаходять дані, про те чим останній може користуватися в OZ. На основі цих даних ZhD реалізує процеси імітації надання відповідних ресурсів, але при цьому ініціює діалог, який пов'язаний з одержанням системою додаткових даних про споживача та його додаткові запотребування та інші дані, які дозволяють виявити небезпеку, що активізувала відповідний доступ у вигляді користувача. Цей алгоритм реалізується через OZ з використанням блоку MN, в якому відповідна модель небезпеки або її наближення може бути сформовано обернений зв'язок між MN і засобом ZhD в цьому випадку реалізується через систему, яка охороняється та блок управління системою захисту BUSZ.

Якщо користувач, що звернувся до OZ через Zh_iD, виявився незареєстрованим в системі доступу OZ, то Zh_iD імітує діалог, який орієнтовано на виявлення додаткових даних про користувача, які виявилися необхідними у зв'язку із змінами в системі доступу OZ. Формування такого діалогу в кожному конкретному випадку пов'язане з особливостями поточного стану системи доступу, в якій можуть мінятися повноваження користувачів на основі внутрішніх процесів, які керують рівнями доступу до різних ресурсів, в процесі функціонування OZ. Виходячи з приведеного вище, можна стверджувати, що основною відмінністю між засобом захисту типу Zh_i і Zh_iD є те, що у першому випадку засіб захисту імітує співпрацю системи OZ з першоджерелом пакетів на основі відомих даних про систему OZ, а в другому випадку Zh_iD імітує співпрацю з користувачем, який виявився несанкціонованим, пропонуючи йому надавати в процесі діалогу додаткову інформацію про себе, яка дозволила би ідентифікувати небезпеку. В другому випадку ZhD повинно таким чином формувати діалог з несанкціонованим користувачем, щоб останній, по можливості, не запідозрив факт його виявлення як несанкціонованого користувача. Цього можна досягнути за рахунок того, що в рамках такого діалогу зі сторони засобу Zh_iD будуть формуватися такі запити, які тісно пов'язані з особливостями системи OZ або відповідні запити зі сторони Zh_iD відповідають інформації, якою диспонує несанкціонований користувач, про систему, що охороняється.

В загальному, можна стверджувати, що використання систем захисту або окремих засобів захисту, які реалізують принципи ідеології honeypot, реалізують не тільки захист інформаційних об'єктів, що характерно для всіх інших засобів захисту, і реалізують виявлення небезпек, що породжують відповідних інтрузів. Виявлення небезпек є принциповим для технології honeypot, оскільки інформація про них дозволяє формувати моделі небезпек. На основі таких моделей стає можливим розв'язання задач прогнозування виникнення атак по відношенню до OZ, а останнє дозволяє упереджувати можливість їх дії на об'єкт охорони.

Принципово новим блоком, що використовується в рамках системи захисту типу SZh є блок BAAP, який вміщає базові алгоритми аналізу подій, що відбуваються або можуть виникнути в середовищі системи захисту. Необхідність цього блоку обумовлюється наступними факторами:

- блоки, що реалізують засоби захисту Zh_i, ZhD, в процесі роботи можуть адаптуватися, що приводить не тільки до зміни значень параметрів, що використовуються алгоритмами цих блоків, а й до зміни самих алгоритмів, наприклад, алгоритмів виявлення повного циклу інтрузів,
- блоки, які приймають участь у реалізації процесів захисту, наприклад, блоки системи моніторингу засобів захисту в середовищі мережі також можуть змінюватися, наприклад, такі зміни можуть полягати у модифікації алгоритмів моніторингу і т. д.

Базові алгоритми аналізу подій представляють собою в певному сенсі початкові та еталонні версії основних алгоритмів, що використовуються в блоках системи захисту, які в процесі функціонування можуть модифікуватися. Блок типу BAAP виконує не тільки функції, що полягають у збереженні еталонних алгоритмів, в ньому зберігаються також системи перетворень алгоритмів та компонент, які в процесі роботи системи можуть мінятися. Такі системи представляють собою системи правил виводу, що використовуються при перетвореннях системи логічних функцій, що використовуються в засобах типу Zh_i і являються внутрішнім формальним описом процесів формування нового стану автомату та формування вихідного слова автомату, яке є елементом повідомлення для небезпеки, що ініціювала атаку, яка була розпізнана засобом, що імітує для небезпеки, факт її співпраці з системою, яка охороняється.

У випадку обслуговування блока інформаційних компонент IKSZ блок BAAP вміщає систему правил перетворень тестових інформаційних компонент, що використовуються в процесах опису цілого ряду компонент, які досить важко в більшості випадків неможливо описати формально з необхідною мірою точності представлення відповідного фактору.

Виходячи з приведеного вище, можна стверджувати, що вміст блоку BAAP являється в найбільшій мірі незмінним по відношенню до інших компонент системи захисту.

Всі блоки системи захисту доцільно розглядати як окремі функціонально орієнтовані системи, що розв'язують певні задачі, які умовно можна розглядати незалежними одна від одної. До таких функціонально орієнтованих систем можна віднести наступні сукупності блоків:

- система захисту OZ від інтрузів, що можуть попасти в OZ зі сторони мережі, яка реалізує процеси захисту на основі ідеології honeypot, складається з блоків Zh_i, AZh_i, $ARZh_i$,
- система моніторингу засобів захисту в середовищі мережі, в яку входить Zh_i, до неї відносяться наступні блоки: UM і UMZ,
- система інформаційного за складається забезпечення складається з

блоків IKSZ і BAAP,

- система управління SZ складається з блоку BUZS і ініціюється системою, що представляє собою OZ. В цьому розумінні будемо в цю систему включати OZ.

1. *Зайцев О. В.* ROOTKITS, SPYWARE, KEYLOGGERS & BACKDOORS: обнаружение и защита. — СПБ.: БХВ. Петербург, 2006.
2. *Соколов А. В., Шаньгин В. Ф.* Защита информации в распределенных корпоративных сетях и системах. — М. ДМК, 2002.
3. *Козлов Д. А., Парандовский А. А., Парандовский А. К.* Энциклопедия компьютерных вирусов. — М.: «Соломон-Р», 2001.
4. *Смит Р. Э.* Аутидентификация: от паролей до открытых ключей. — М.: Издательский дом «Вильямс», 2002.

Поступила 16.08.2010р.

УДК 629.52.7.

О.А. Машков, д.т.н., профессор, ВАК Украины; В.Р. Косенко

ОСОБЛИВОСТІ МОДЕЛЮВАННЯ НЕШТАТНИХ (АВАРІЙНИХ) СИТУАЦІЙ В ІНФОРМАЦІЙНО-КЕРУЮЧИХ КОМПЛЕКСАХ ДИНАМІЧНИХ ОБ'КТІВ КЕРУВАННЯ

Методика виявлення відмов в інформаційно-керуючих комплексах, заснована на використанні «оновлюючих» процесів

Виділимо із загальної задачі виявлення відмов окремий клас задач керування рухом динамічного об'єкта, що містить інформаційно-керуючий комплекс (ІКК), у яких відмови моделюються у вигляді адитивних ефектів у рівняннях стану та спостереження.

Позаштатний стан ІКК моделюється одним з наступних рівнянь:

$$X(k+1) = \Phi(k+1, k)X(k) + W(k) + \vartheta\,\delta(k+1, m); \quad (1)$$

$$X(k+1) = \Phi(k+1, k)X(k) + W(k) + \vartheta\,1(k+1, m); \quad (2)$$

$$Y(k) = H(k)X(k) + U(k) + \vartheta\,\delta(k, m); \quad (3)$$

$$Y(k) = H(k)X(k) + U(k) + \vartheta\,1(k, m), \quad (4)$$

де ϑ – невідомий вектор, що характеризує величину відмови,

m – невідомий момент її виникнення.

Рівняння (1), (2) описують широке коло моделей відмов, пов'язаних зі зміною динаміки об'єкта за рахунок появи стрибків або зрушень у компонентах вектора стану. Рівняння (4) можна застосовувати для моделювання окремих рідких аномальних вимірів, а рівняння (70) – для опису раптових зрушень (зсувів), що з'являються в інформаційно-

