УДК 683.05

Б.В.Дурняк, Ю.М.Коростіль, В.І.Сабат

ОСОБЛИВОСТІ РОБОТИ СИСТЕМИ ЗАПОБІГАННЯ ДІЯМ, ЩО НАПРАВЛЕНІ НА ПОРУШЕННЯ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

Системи запобігання діям, що обумовлюються та ініціюються небезпеками, які існують по відношенню до комп'ютерних систем, прийнято називати системами *IPS* (Intrusion Preventions System) [1]. Оскільки будь які дії реалізуються певними носіями, які в рамках комп'ютерних мереж можуть реалізовуватися в формі програмних елементів, в формі спеціалізованих програмних засобів, що функціонально подібні на штатні компоненти, то такі носії прийнято називати інтрузами (Intrusion) [2].

Системи *IPS* представляють собою наступний етап розвитку систем захисту комп'ютерних мереж по відношенню до систем *IDS* (Intrusion Detection System – систем виявлення інтрузів). На відміну від *IDS* , стосовно системи *IPS* не склалося загально прийнятого уявлення про *IPS* , як систему, що має свою власну структуру і достатньо чітко визначені відмінності від інших засобів захисту, в першу чергу, від *IDS* .

У відповідності з визначенням *IPS* , як системи протидії інтрузам, в *IPS* розв'язуються задачі запобігання діям інтрузів в рамках наступних методів та підходів:

- виявлення загроз, що існують в системі, яка захищається і, переважно, представляє собою локальну мережу (*LAN*), що підключена до загальної мережі, наприклад Internet;
- однією з функцій системи *IPS* є виявлення потенціальних неоднорідностей, або аномалій в мережному середовищі, суміжному по відношенню до *LAN* ; система *IPS* на основі цих даних повинна виявити причини встановлення таких аномалій і, якщо визначено, що такі причини можуть породити інтрузи, для *LAN* , що захищається, то *IPS* повинна активізувати засоби захисту таким чином, щоб вони були достатньо чутливими до інтрузів певних типів, або *IPS* повинна розширити окремі компоненти засобів захисту таким чином, щоб вони відповідний інтруз не пропустили у *LAN* ;
- реалізовувати запобігання дії інтруза, якщо на основі аналізу його в *IPS* виявиться, що він не може бути затриманим існуючою системою захисту; для цього *IPS* повинно використовувати примарні моделі об'єкту атаки, або засоби honey pot [3];
- запобігати дії інтруза, що виявлений в *IDS* , як такий, що не дійшов

до *LAN*, яка обслуговується *IPS*, але може бути орієнтованим на *LAN*, при певному розширення інтруза; запобігання, в цьому випадку, полягає у протидії можливості його доповнення, що реалізується на основі аналізу повного образу інтруза, який може описуватися конкретною сигнатурою;

- виявлення сканування *LAN*, що захищається, та інших проявів початкових етапів реалізації атак та початкових етапів формування відповідних інтрузів.

Виявлення загроз в комп'ютерних системах використовується досить широко, в основному, по відношенню до програмних складових локальних мереж, що захищаються, і відомому, як виявлення «слабих місць», переважно, в системному програмному забезпеченні. Засоби, які можна вважати орієнтованими на виявлення загроз, складають досить широкий асортимент, до якого можна віднести:

- засоби систем тестування програмного забезпечення та апаратних засобів комп'ютерних мереж,
- програмне забезпечення, що визначає надійність відповідних компонент мережі,
- засоби контролю роботи комп'ютерної мережі та її компонент,
- широкий спектр аналізаторів роботи мережі і т.д.

Вводити в склад системи *IPS* приведений асортимент засобів, для реалізації процесів виявлення загроз не доцільно, оскільки, це привело би до перевантаженості системи. Тому, в рамках *IPS* реалізується система визначення необхідності використання тих, чи інших засобів та запотребування останніх з обслуговуючих мережу ресурсів. Початкова версія системи *IPS* вміщає деякий мінімальний комплект засобів виявлення загроз, який в процесі її роботи може поповнюватися та модифікуватися.

Підсистема, що забезпечує функцію виявлення загроз системою *IPS*, скорочено будемо позначати *SVZ* (система виявлення загроз). Вона функціонує на основі використання принципів активності компонент. Принцип активності компонент реалізується на основі аналізу та використання наступних вимог та умов.

Умова 1. Певний засіб переводиться в активний стан, якщо на протязі часу Δt_i він активізувався у відповідності з дисципліною роботи *SVZ*, чи з інших причин, що обумовлені алгоритмом функціонування *SVZ*.

Умова 2. Кількість активних засобів (z_i) на протязі одного Δt_i в *IPS* є обмеженою і визначається початковими умовами інсталяції *IPS*.

Умова 3. Система *IDS* використовує засоби не тільки з ресурсів локальної мережі, що охороняється, а з ресурсів всієї мережі.

Умова 4. В рамках принципу активності використовуються дисципліни динамічних пріоритетів, які визначаються ресурсам.

Умова 5. Система управління *SVZ* зв'язана з іншими системами *IPS*

двохсторонніми зв'язками, які можуть активізуватися як із сторони *SVZ* , так і із сторони інших систем *IPS* .

Умова 6. Необхідність використання певного типу z_i визначається в рамках системи *SVZ* .

Вимога 1. Системі *SVZ* в рамках всієї *IPS* призначається базове та текуче значення пріоритету активності.

Вимога 2. При виявленні загрози, *SVZ* повинна провести аналіз актуальності відповідної загрози і на основі такого аналізу реалізувати певний вид протидії цій загрозі.

Перша і друга умови призначені для вирішення проблеми можливого переповнення *IPS* засобами виявлення і контролю загроз.

Третя умова передбачає можливість використання системою *IPS* мережних ресурсів. Такі ресурси можуть передаватися в *IPS* через систему захисту, якою обладнана локальна мережа, що захищається, або можуть передаватися безпосередньо з мережі, якщо відповідний ресурс має необхідний сертифікат безпеки.

Сертифікатом безпеки можуть володіти ресурси, що призначені для широкого використання в межах мережі. Він надається довіреною стороною тим ресурсам, які пройшли перевірку на відсутність в них небезпечних несанкціонованих компонент, ресурси, які верифіковані по відношенню до опису функціонального призначення та мають визначені гарантії відповідальності. При наявності у ресурсів таких сертифікатів, появляється можливість знизити рівень захисту, що реалізується в процесах передачі та використання відповідних засобів.

Система *SVZ* , крім виявлення загроз, реалізує певний тип реакції на неї. В даному випадку, можливі наступні типи реакції на загрози:

- елімінація загрози,
- блокування загрози,
- реєстрація загрози,
- пасивна реакція на загрозу.

Елімінація загрози полягає у її ліквідації. Якщо загроза виявлена в програмному забезпеченні, то процес елімінації реалізується шляхом доповнення програмного засобу відповідним розширенням, яке реалізується автором відповідного програмного засобу, або його власником. Крім того, як і в системі *IDS* , реалізується розсилка інформації про виявлену загрозу всім функціонуючим системам *IPS* .

Блокування загрози реалізується в тому випадку, коли на основі даних, що отримані з локальної мережі, існує можливість виявити потенціальні об'єкти атаки. Наприклад, якщо в якості загрози виявлено можливість несанкціонованого відкриття нового порту, а в системі, що охороняється функціонують програмні засоби, що розв'язують деяку задачу користувача, які оперують даними, що мають статус даних з обмеженим доступом, то

необхідно оперативно перекрити можливість доступу до них. Оскільки, елімінація загрози, у відповідності з її описом, потребує часу, на протязі якого може появитися інтруз, що скористається відповідною загрозою. В даному прикладі, таким інтрузом може бути троянський кінь, з допомогою якого може бути реалізовано несанкціонований доступ до даних з обмеженим доступом. Зрозуміло, що заблокована загроза в подальшому може елімінуватися описаним вище способом, якщо це виявиться необхідним на наступних етапах роботи системи *IPS*.

Реєстрація загрози реалізується в тому випадку, коли виявлена загроза не може бути використана інтрузом для атаки на текучий стан системи, що охороняється. Наприклад, якщо в системних програмних засобах виявлено можливість не санкціоновано перехоплювати управління задачами, але така ситуація є можливою лише в тому випадку, коли системні програмні засоби, наприклад, операційна система, переходить у певний режим роботи, але згідно з функціональними вимогами політики безпеки локальної мережі операційна система в цьому режимі не повинна працювати. Тоді, загроза, що виявлена, реєструється і в подальшому може бути елімінована, якщо це виявиться необхідним. Необхідність реєстрації такої загрози обумовлюється тим, що інформація про неї мусить бути передана іншим системам *IPS*, що обслуговують інші локальні мережі, для яких така загроза може бути актуальною на момент їх функціонування.

Пасивна реакція на загрозу реалізується в наступному випадку. Нехай в роботі *IPS* використовуються засоби контролю надійності системи і в результаті чергового контролю виявилося, що рівень надійності понизився по відношенню до попереднього етапу його визначення. В цьому випадку, здійснюється пасивна реакція на загрозу. Вона полягає у тому, що в *IPS* ініціюються процедури, з допомогою яких можна було би виявити причини пониження рівня надійності певних фрагментів локальної мережі.

Виявлення небезпек, що проявляються у вигляді зміни значень параметрів, які характеризують оточення мережі, яка захищається, є важливою функцією *IPS* і повністю відповідає ідеології її роботи. Прикладами таких параметрів можуть служити, перш за все, параметри, що характеризують засоби комунікації між окремими вузлами мережі. Наприклад, значна зміна навантаження на окремих трафіках, що може привести до виникнення відомої атаки *DoS* [4], зміна характеру параметрів протоколів пакетів сеансу зв'язку, або поява нетипового для контрольованого середовища типу протоколу і т.д. Всі неоднорідності, або аномалії ідентифікуються по відношенню до сеансів зв'язку, *IP* адресами протоколів та іншими параметрами, що є обов'язковими, при організації деяких сесій в мережі. На основі таких даних, в першу чергу, визначаються потенціальні джерела, з якими пов'язані виникаючі аномалії. Здійснюється локалізація відповідних джерел, які ідентифікуються, як небезпеки, що породжують, або можуть породити інтрузів.

Важливою складовою системи IPS, яку будемо називати системою виявлення небезпек і будемо позначати символами SVN, являється прогнозування породження інтрузів виявленою небезпекою. В контрольованому фрагменті мережі, яку аналізує IPS, аномалії можуть мінятися різними способами. Тому, IPS в рамках SVN повинна розв'язувати наступні задачі:

- задачу аналізу розвитку аномалії,
- задачу аутентифікації небезпеки,
- задачу визначення міри агресивності міри виявленої небезпеки,
- супровід небезпеки,
- прогнозування поведінки небезпеки.

Задача аналізу розвитку небезпеки полягає у наступному. Нехай міняється деяка сукупність параметрів мережного середовища. В SVN від IPS існують дані про можливі залежності між параметрами. Тоді, SVN реалізує моні торування зміни величин цих параметрів в часі і просторі, що визначаються визначеним періодом циклу моні торування та фрагментом мережі, який аналізується. Якщо величини відповідних змін перевищують певний поріг, або такі зміни порушують визначені співвідношення між параметрами, то SVN реєструє факт виявлення небезпеки. Після цього ініціюються процеси ідентифікації і аутентифікації відповідної небезпеки. Якщо в процесі текучого кроку моніторингу виявленої небезпеки значення параметрів, параметрів, що її проявили, повернулись у допустимий діапазон, або стали меншими заданого порогу і такі значення тримаються на протязі часу Δt_i, де $\Delta t_i > \Delta t_j$, де Δt_j - час, на протязі якого відповідні параметри перевищували заданий поріг і визначений як час, що є допустимим, з точки зору динаміки функціонування небезпек, яка пов'язується з політикою безпеки LAN, то відповідна небезпека нівелюється. Це не означає, що вона щезає зовсім, а означає, що вона на даному етапі не досліджується, хоча встановлені про неї дані залишаються в базі даних IPS.

Задача аутентифікації даних, небезпеки полягає ґрунтується на визначенні наступних факторів, що її характеризують:

- виявлення джерела, що ініціює зміну параметрів оточення, яка проявляється у виникненні аномалій,
- встановлення характеру, або типу інтруза, який може бути сформований відповідним джерелом,
- задача визначення величини ризику реалізації успішної атаки відповідним інтрузом.

Перша задача розв'язується на основі аналізу адрес IP, що розміщаються в мережних протоколах. Виходячи з аналізу різних типів атак [5], відомо, що для багатьох атак є характерним маскування адрес реального

джерела небезпеки. Прикладом таких маскувань для різновидності атак *DoS* може служити використання технологічних протоколів, що приводить до можливості «зомбування» хостів в мережі. По характеру змін значень параметрів аномалій, *IPS* приймає рішення про вибір методів взаємодії з потенціальними кандидатами в джерела небезпек, або псевдо джерелами небезпек, для встановлення реальних джерел небезпеки в мережі. Така взаємодія може полягати у виявленні троянських коней, у випадку використання небезпеками методу бомбування хостів. В залежності від способу реалізації атаки, який припускається як можливий системою *SVN* або системою *IPS* в цілому, приймається відповідне рішення про необхідний спосіб взаємодії з небезпекою.

Встановлення типу інтруза здійснюється на основі динаміки змін параметрів аномалій. Оскільки відповідні зміни обумовлюються окремими ініціативними діями небезпеки, що проявляються в мережі як ті чи інші події, то можна говорити про виникнення певних сукупностей подій. Як відомо, реалізація атак на об'єкти мережі інтерпретується як послідовність подій, що тим чи іншим способом пов'язується з об'єктом атаки. Тому, на сьогоднішній час, переважна кількість атак описується у вигляді послідовності подій певного типу. Принциповою відмінністю *IPS* від традиційного підходу до розпізнавання типу інтруза, як носія атаки, полягає у тому, що в *IPS* розв'язується задача не ідентифікації окремих сигнатур атаки, а розв'язується задача розпізнавання атак по наближених сигнатурах, які можна вважати сигнатурами варіації інтрузів.

Задача визначення величини ризику реалізації успішної атаки небезпекою, з одного боку, являється складною, а з другого боку, ця задача безпосередньо зв'язана з оцінкою рівня безпеки локальної мережі, що охороняється системою *IPS* Тому, засоби розв'язування цієї задачі не тільки вироджуються у окрему систему, що входить в *IPS*, а й може мати відношення до інших систем локальної мережі.

1. *Rash M.Jrebaugh A., Clark G., Pinkard B., Babbin J.* Zapobieganie I aktywne przeciwdzialanie intruzom. W.: Mikom, 2005.
2. *Amrozo E.* Wykrywanie intruzow. Wprowadzenie do monitorowania, korelacji, tropienia, pulapek o reagowania w Internecie. W.: RM, 1999.
3. *Piotrowski M.* Krolicza nora. Ochrona sieci komputerowych za pomoca technologii honey pot. W.: Mikom, 2007.
4. *Анин Б.* Защита компьютерной информации. СПб.-Санкт-Петербург, 2000.
5. *Касперски К.* Техника и философия хакерских атак. М.: СОЛОН-Р, 1999.

Поступила 12.01.2009р.