УДК 004.738 (043.3)

Даниліна Г.В., канд. техн. наук
Милокум Я.В.

СТАТИСТИЧНИЙ ПІДХІД ДО АНАЛІЗУ КОМП'ЮТЕРНИХ ПОГРОЗ

**Інститут комп'ютерних технологій
Національного авіаційного університету**

Розглянуто методи конфліктного управління захистом комп'ютерних мереж з прогнозуванням розвитку ситуації і корекцією за результатами її поточного аналізу, які пропонується використовувати у розподілених системах захисту. Пропонується перехід від детермінованих до статистичних методів аналізу погроз і статистичного синтезу систем захисту. Завдання виявлення вторгнень вирішується як завдання перевірки простий гіпотези (нормальна робота за відсутності зловмисних дій) проти складної альтернативи

Вступ

При розробці систем виявлення погроз історично застосовувалися детерміновані методи аналізу. З часом число вірусів і інших шкідливих програм зростає в геометричній прогресії. Для забезпечення роботи антивірусних програм, аналізу файлів і моніторингу комп'ютера в реальному або хоч би в квазіреальному масштабі часу потрібне все більший об'єм обчислювальних ресурсів. Теоретично верхньої межі числу вірусів не існує [1].

Основою традиційних систем виявлення вторгнень є методи аналізу сигнатур і/або аналізу протоколів. Використовуються комбіновані системи виявлення вторгнень із спільним аналізом сигнатур і протоколів, створенням правил обробки специфічного (аномального, підозрілого) трафіку і так далі Проте захист знаходиться в режимі пасивного очікування нових погроз. Ефективність детермінованих систем виявлення вторгнень з часом постійно знижується.

Головною метою роботи є аналіз метода конфліктного управління з прогнозуванням розвитку ситуації і корекцією за результатами її поточного аналізу.

Розв'язування задачі. Логічним виходом є перехід до статистичних методів аналізу погроз і статистичного синтезу систем захисту.

При вирішенні завдань статистичного аналізу і синтезу необхідно визначити деяку функцію спостережуваної реалізації випадкового процесу. Зазвичай вибирають функцію такого вигляду, за допомогою якої здійснюється редукція даних без втрати апріорної інформації. Вона називається достатньою статистикою.

Як достатні статистики використовують початкові і змішані моменти розподілу – математичне очікування, дисперсію, вищі моменти, функції кореляції і регресії. Мінімальне число характеристик процесу, якими обмежуються при аналізі достатньої статистики, залежить від необхідної точності. Воно не залежить від обсягу накопичених раніше даних, які надалі відіграють роль апріорних відомостей про результуючі характеристики випадкового процесу та статистичних гіпотез.

Як статистичні моделі погроз використовують ознаки відхилень в роботі устаткування, аномалій мережевого трафіку, сплесків активності окремих мережевих вузлів і інших аномальних явищ. Так само будують і моделі нормального функціонування комп'ютера і мережі, до складу якої він входить. У статистичній системі виявлення вторгнень класи ознак нормальної і аномальної поведінки захищаємого об'єкта постійно модифікуються з урахуванням накопиченої інформації.

Завдання виявлення вторгнень вирішується як завдання перевірки простий гіпотези (нормальна робота за відсутності зловмисних дій) проти складної альтерна-

тиви. Для вирішення лише завдання виявлення вторгнень складну альтернативу можна звести до простої. Хай $p(y|\mu,1)$ – умовна щільність вірогідності спостережуваного процесу для випадку $\theta=1$ (присутньо один або декілька ознак аномалії), залежна від параметра $\mu\in\Omega_1\subset\Omega$, який належить заданій області Ω_1. Відповідно, $p(y|\ \aleph,0)$ – умовна щільність спостережуваного процесу для випадку $\theta=0$ (ознаки аномалії відсутні), залежна від параметра $\aleph\in\Omega_2\subset\Omega$, який належить заданій області Ω_2. Параметри μ і $\aleph$ вважаються апріорі за невідомих. Область Ω_1 значень параметра μ і область Ω_2 значень параметра $\aleph$ є підпросторами спільного простору Ω спостережуваних значень і в спільному випадку є пересічними.

Байєсівське (відносно μ і $\aleph$) рішення даної задачі полягає в обчисленні відношення правдоподібності і порівнянні з порогом [2], який може вибиратися по різних статистичних критеріях. При байєсівському підході параметри μ і $\aleph$ інтерпретуються як випадкові величини з відомими апріорними розподілами, зокрема, щільністю вірогідності $p_0(\mu)$, $p_0(\aleph)$ (якщо μ, $\aleph$ – безперервні величини).

Усереднивши умовну щільність вірогідності $p(y|\mu,1)$ і $p(y|\ \aleph,0)$. по апріорній вірогідності $p_0(\mu)$ і $p_0(\aleph)$ відповідно, отримаємо умовну щільність вірогідності

$$p(y|1)=\int_{\Omega_1} p(y|\mu,1)p_0(\mu)d\mu \qquad (1)$$

і

$$p(y|0)=\int_{\Omega_2} p(y|\aleph,0)p_0(\aleph)d\aleph \qquad (2)$$

які залежать від невідомого параметра, що приймає лише одне з двох значень ($\theta=0$ і $\theta=1$), тобто до випадку перевірки простий гіпотези проти простий альтернативи.

В разі дискретних параметрів μ і $\aleph$ замість інтеграції по формулах (1, 2) обчислюється лінійна згортка умовної вірогідності $p(y|\mu,1)$ і $p(y|\aleph,0)$ з вагами, рівними апріорній вірогідності параметрів μ і $\aleph$.

За відсутності апріорних даних про вигляд і параметри розподілів $p_0(\mu)$ і $p_0(\aleph)$ використовують небайєсівські методи – мінімаксний (щодо деяких найменш сприятливих апріорних розподілів) або метод максимуму правдоподібності (при простій функції втрат і унімодальної щільності вірогідності спостережуваного процесу).

Проаналізуємо зв'язок цілей вторгнення і якісних властивостей апріорної інформації. Цілі вторгнення можна розділити на дві крупні, порівняно самостійні групи.

1. Скритне знімання інформації або впровадження вірусів і інших шкідливих програм. Супротивник намагається максимально потай проникнути в комп'ютер, що атакується, зняти інформацію, що його цікавить, і вийти, знищивши всі сліди вторгнення. Виявлення вторгнення можливо тільки по непрямих ознаках: аномалії в роботі ЕОМ, не відповідна ситуації активність периферійних пристроїв, несподіваний обмін даними із зовнішньою мережею й т.д. Короткострокові наслідки для роботи ЕОМ як самостійного суб'єкта або функціонального вузла деякої розподіленої системи практично не фіксуються.

2. Вторгнення з метою модифікації (знищення, порушення цілісності) інформації, внесення помилок або повного виводу з ладу операційної системи, реалізації атак типа *Denial of Service* і ін. Попередньо супротивник також намагається зібрати максимально можливий обсяг інформації про наявність уразливостей у системі захисту об'єкта, що атакують, (сканування портів, пошук слабких місць у програмному забезпеченні). Вторгнення

виявляється безпосередньо по явних впливах на ЕОМ, починаючи від проявів вірусної активності, виснаження ресурсів ЕОМ і забивання каналів обміну даними або іншими порушеннями працездатності, аж до повного останова об'єкта, що атакують.

В термінах радіоелектронної боротьби вивчення об'єкту, що атакується, можна трактувати в першому випадку як попередню розвідку, в другому – як старанну. Використовуючи добре розроблені методи захисту від радіоелектронної розвідки і придушення [3, 4], можна розробити ефективні методи протидії на основі статистичної теорії виявлення і розпізнавання. Завдання розпізнавання мети вторгнення є вельми важливим і актуальним.

Система розпізнавання – це складна динамічна система. Вона включає не лише пристрої реалізації алгоритмів обробки, але і експертів, за якими залишається остаточне рішення. У нашому випадку це адміністратори локальних мереж і оператор/провайдер сегменту глобальної мережі, оператор корпоративної або регіональної мережі. Система розпізнавання є суто спеціалізованою і призначеною для роботи лише у складі спільної системи захисту мережі.

Розробка системи розпізнавання пов'язана з вирішенням певної послідовності завдань.

Першим завданням є детальне вивчення об'єктів – аномалій мережевого трафіку, аномалій роботи комп'ютера або сервера, які підлягають розпізнаванню. Ступінь детальності цього вивчення залежить від потрібної ефективності роботи системи розпізнавання. Результатами вивчення об'єктів розпізнавання повинні бути обгрунтований вибір принципу класифікації й визначення кількості об'єктів. Головним завданням розпізнавання образів – об'єктів системи захисту комп'ютерної мережі – є розрізнення зловмисника від всіх інших об'єктів в зоні дії системи захисту, які не представляють загрози і є лише джерелами помилкових тривог.

Другим завданням є складання деякого словника ознак, які використовуються для апріорного опису класів об'єктів, що підлягають розпізнаванню. Ознаки об'єктів можуть бути логічними і описуватися детермінованими якісними висловлюваннями або кількісними величинами, які попадають у конкретний інтервал значень. Якщо ознаки є чисто випадковими і розподілені по якомусь (у загальному випадку – невідомому) числу класів або по всіх класах об'єктів з певним законом розподілу, потрібно використовувати статистичні методи. Ознаки об'єктів, які підлягають розпізнаванню, слід трактувати як імовірнісні також тоді, коли результати вимірів їх числових значень отримані з такими помилками, що по цих результатах неможливо віднести об'єкт до того або іншого класу з прийнятною якістю. Тому логічно вважати, що деякі ознаки будуть віднесені до детермінованих або до стохастичних залежно від апріорних даних і якості вимірювальних пристроїв. Якщо апріорна щільність вірогідності тієї або іншої ознаки має настільки малу дисперсію, що розподіл можна вважати за дельтоподібний, таку ознаку слід віднести до логічних (детермінованим).

На практиці найчастіше має місце ситуація, коли ознаки об'єктів різних класів частково перекриваються. В цьому випадку навіть для ознак логічного (детермінованого) типа неможливо достовірно, з вірогідністю, рівній одиниці, розрізнити класи об'єктів, що мають такі ознаки. Відповідно, потрібно використовувати статистичний підхід [5].

Процедура вибору ознак для розпізнавання є істотно неформальною. Зазвичай ознаки об'єктів виражають у вигляді впорядкованого набору параметрів X_1, X_2 ..., X_N, безперервних або дискретних [7]. Само безліч об'єктів розбивають на M окремих класів k_1, k_2 ..., k_M, які в спільному випадку можуть бути такими, що перекриваються. Це еквівалентно встановленню в деякому функціональному просторі ознак S_g підпросторів s_{gi}, $i = 1,2,\ldots,M$. Якщо об'єкт з певними ознаками нале-

жить до класу k_j, то відповідний елемент, яким представляється об'єкт в ознаковому просторі, належить області s_{gi}. Для детермінованих ознак класи об'єктів описуються на мові ознак функціональними залежностями, а для стохастичних ознак – умовною щільністю вірогідності значень параметрів ознак за умови, що об'єкти належать класу k_j, і апріорною вірогідністю $P_{pr}(k_j)$ того, що об'єкт, пред'явлений для розпізнавання, належатиме до того ж класу k_j.

Сформульоване вище завдання розпізнавання в термінах теорії перевірки статистичних гіпотез [6] визначається як перевірка простий гіпотези $h_1 = \{k_1\}$ проти складної альтернативи $H_0 = \{k_{01}, k_{02}, \ldots, k_{0N}\}$. У даному випадку k_1 – клас об'єктів, які представляють загрозу (зловмисники), а $k_{01}, k_{02}, \ldots, k_{0N}$ – класи об'єктів, які не представляють загрози для системи захисту, але є перешкодами для системи розпізнавання. На рис. 1 зображено умовний розподіл підпросторів ознак об'єктів, які можуть потрапити в зону дії системи і підлягають розпізнаванню.

Безліч об'єктів, явищ, ситуацій складає певний набір класів. Елементи цієї безлічі мають вельми різноманітну фізичну природу, що створює певні труднощі як при описі, так і при виділенні інформаційних параметрів ознак конкретного представника класу. Для подолання труднощів термінологічного характеру будемо, слідуючи роботі [7], називати ознаки класів «сигналами». Цей термін є звичним як для фахівців з електроніки і комп'ютерної техніки, так і для фахівців із статистичної теорії виявлення. Крім того, всі пристрої обробки інформації, у тому числі і комп'ютеризовані пристрої розпізнавання, оперують саме з електричними сигналами як матеріальними носіями інформації.

Відповідно і сигнал, який з'являється в результаті спроби несанкціонованого доступу зловмисником, називатимемо корисним сигналом, а сигнали сторонніх об'єктів – перешкоджаючими сигналами або просто перешкодами.

Сигнали, які поступають на вхід пристрою розпізнавання, по класифікації теорії виявлення і оцінювання [2] є сигналами з невідомими параметрами. По суті, і корисні, і перешкоджаючі сигнали є дискретними випадковими процесами, інколи – з адитивними регулярними компонентами.

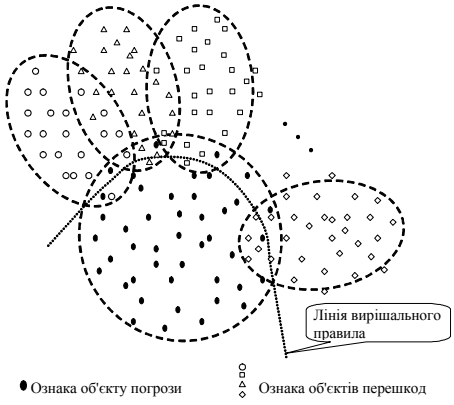

Рис. 1. Розподіл підпросторів ознак об'єктів

Щоб виключити або хоч би понизити залежність ефективності вживаних алгоритмів виявлення (розпізнавання), від абсолютних значень невідомих параметрів сигналів і перешкод, необхідно розробити методи нормування сигналів щодо цих параметрів. Таке завдання є одній з ключових для побудови алгоритму розпізнавання екстремальних ситуацій комп'ютерної мережі.

Пристрій, що розпізнає, призначений для роботи при неповній апріорній інформації про класи сигналів, повинен володіти здібністю до заповнення бракуючих відомостей за результатами аналізу сигналів, що поступають на його вхід. Накопичення цих відомостей здійснюється на етапі навчання пристрою, що розпізнає, в процесі якого воно пристосовується до конкретних умов розпізнавання. Розрізняють два види або режими розпізнавання.

У режимі навчання з вчителем, який часто називається просто навчанням, на вхід пристрою, що розпізнає, подається

деяка тренувальна або повчальна вибірка сигналів $X_1,\dots X_N$ і одночасно повідомляється дійсна приналежність кожного з них $\gamma_1,\dots\gamma_N$. Оскільки приналежність сигналів, що входять в повчальну вибірку, відома, те поповнення бракуючих відомостей для кожного класу може здійснюватися незалежно, що дозволяє вирішувати задачу навчання порівняно простими методами. Після того, як навчання закінчене, що розпізнає пристрій може здійснювати класифікацію сигналів, що знов поступають $X_{N+1}, X_{N+2},\dots$. Вирішення про приналежність *i*-го сигналу в цьому випадку залежить не лише від самого сигналу, але і від всієї інформації, що вчинила в процесі навчання, тобто

$$g_i = g\left(X_i; X_N,\dots,X_1;\gamma_N,\dots,\gamma_1\right),\ i > N$$

Значно цікавішим в принциповому і важливішим в теоретичному відношенні є режим самонавчання пристроїв, що розпізнають. Він відрізняється від режиму навчання тим, що повчальна вибірка сигналів, що поступає на вхід, не супроводиться жодними вказівками про їх дійсну приналежність, і всю бракуючу апріорну інформацію про класи пристрій повинен витягувати самостійно, без допомоги ззовні. Очевидно, що пристрої, що розпізнають, призначені для роботи в режимі самонавчання, є гнучкішими. Вони незамінні в тих багаточисельних реальних ситуаціях, коли дійсна приналежність сигналів, що поступають, невідома із самого початку, або коли умови розпізнавання відрізняються для різних конкретних варіантів рішення задачі і потрібне дуже часте «перенавчання» пристрою.

В самонавчальних пристроях кожен сигнал, що поступає на вхід, служить одночасно і для поповнення бракуючих апріорних відомостей, тому рішення g_i, що приймається самонавчальним пристроєм для сигналу X_i, є функцією всіх сигналів, що поступають до *i*-го моменту:

$$g_i = g\left(X_i, X_{i-1},\dots,X_1\right).$$

Висновки

В умовах безперервного зростання потенційних погроз, організації атак розподіленого типа логічним виходом з ситуації, що склалася, є у відповідь організація розподілених систем активного захисту – угрупувань, що включають чимале число лояльних партнерів і що працюють погоджено під управлінням ієрархічної системи управління об'єктами захисту.

Для запобігання існуючим і прогнозованим погрозам, успішного віддзеркалення атак на початковому етапі їх організації недоцільно застосовувати адаптивні системи захисту із-за їх постійного запізнювання, як мінімум, на один крок. У розподілених системах захисту пропонується використовувати методи конфліктного управління з прогнозуванням розвитку ситуації і корекцією за результатами її поточного аналізу.

Список літератури

1. *F. Cohen*. Computer Viruses: theory and experiments // DOD/NBS 7th Conference on Computer Security (1984); Computers and Security, 1987. – vol. 6#1. – P. 22–35.

2. *Сосулин Ю.Г.* Теория обнаружения и оценивания стохастических сигналов. – М.: Советское радио, 1978. – 320 с.

3. Защита от радиопомех. Под ред. Максимова М.В. / М.В. Максимов, М.П. Бобнев, Б.Х. Кривицкий и др. – М.: Советское радио, 1076. – 496 с.

4. *Комиссаров Ю.А., Родионов С.С.* Помехоустойчивость и электромагнитная совместимость радиоэлектронных средств. – К.: Техника, 1978. – 208 с.

5. Вопросы статистической теории распознавания. / Барабаш Ю.Л., Варский Б.В., Зиновьев В.Т., Кириченко В.С., Сапегин В.Ф. – М.: Советское радио, 1967. – 400 с.

6. *Леман Э.* Проверка статистических гипотез. – М.: Наука, 1979. – 408 с.

7. *Миленький А.В.* Классификация сигналов в условиях неопределенности. – М.: Советское радио, 1975. – 328 с.