УДК 004.056

РОЗРОБКА ОЦІНКОВОЇ МОДЕЛІ ПРОГРАМНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

К.В. КОЛЕСНІКОВ, В.Ю. ШАДХІН

Київський національний університет технологій та дизайну

Розроблено модель для отримання кількісних оцінок ефективності функціонування програмної системи захисту інформації (ПСЗІ), що функціонують в призначеному для користувача режимі. Отримані в результаті оцінки можуть бути використані як для порівняння існуючих ПСЗІ, так і для аналізу змін, що вносяться до алгоритмів захисту ПСЗІ

Необхідність використання систем захисту програмного забезпечення (ПЗ) зумовлена низкою чинників, серед яких слід виділити такі: незаконне використання алгоритмів, що є інтелектуальною власністю автора, несанкціонований доступ, використання і модифікація ПЗ, незаконне розповсюдження і збут ПЗ.

Є тенденція до зростання рівня піратства, яка зберігається і нині, що збільшує фінансові втрати виробників ПЗ. У зв'язку з цим завдання розробки надійних програмних систем захисту інформації (ПСЗІ) набуває великого значення.

Розглянемо довільну програмну систему захисту інформації, що функціонує в кільці захисту ядра операційної системи. Подібна ПСЗІ з огляду на операційну систему є призначеним для користувача додатком. Таким чином, в адресному просторі ПСЗІ наявні пуасонівські категорії інформаційних потоків.

Об'єкти та методи дослідження

Стверджуватимемо, що довільна ПСЗІ, яка функціонує в призначеному для користувача режимі, буде повністю контрольованою з боку засобів аналізу, якщо засоби аналізу здатні здійснювати контроль над всіма категоріями інформаційних потоків, наявних в адресному просторі ПСЗІ в процесі її роботи [1].

Таким чином, довільна ПСЗІ буде повністю зламана, якщо може бути здійснений контроль над всіма категоріями інформаційних потоків. Здійснення подібного контролю можливе в двох випадках:

– інформаційні потоки відповідної категорії не були захищені;

– для відповідної категорії інформаційних потоків проведена успішна нейтралізація способів протидії засобам аналізу.

Для введених в роботу [2] категорій інформаційних потоків введемо такі позначення: інформаційні потоки категорій 1–3 позначатимемо F_1–F_3 відповідно. Усі ці категорії інформаційних потоків є незалежними один від одного.

При аналізі довільної ПСЗІ засобами дослідження програмного коду система захисту інформації може перебувати в таких станах (тобто процес зламу довільної ПСЗІ може бути описаний такими станами):

S_1 – ПСЗІ не зламана, засоби дослідження програмного коду успішно нейтралізуються реалізованими для інформаційних потоків категорій $F_1 - F_3$ способами протидії;

S_2 – ПСЗІ не зламана, зламані (або не були захищені) реалізовані для інформаційного потоку F_1 способи протидії, інформаційні потоки F_3 і F_2 успішно протидіють засобам аналізу;

S_3 – ПСЗІ не зламана, зламані (або не були захищені) реалізовані для інформаційного потоку F_2 способи протидії, інформаційні потоки F_1 і F_3 успішно протидіють засобам аналізу;

S_4 – ПСЗІ не зламана, зламані (або не були захищені) реалізовані для інформаційного потоку F_3 способи протидії, інформаційні потоки F_1 і F_2 успішно протидіють засобам аналізу;

S_5 – ПСЗІ не зламана, зламані (або не були захищені) реалізовані для інформаційних потоків F_1 і F_2 способи протидії, інформаційний потік F_3 успішно протидіє засобам аналізу;

S_6 – ПСЗІ не зламана, зламані (або не були захищені) реалізовані для інформаційних потоків F_1 і F_3 способи протидії, інформаційний потік F_2 успішно протидіє засобам аналізу;

S_7 – ПСЗІ не зламана, зламані (або не були захищені) реалізовані для інформаційних потоків F_2 і F_3 способи протидії, інформаційний потік F_1 успішно протидіє засобам аналізу;

S_8 – (поглинаючий стан) – програмна система захисту інформації зламана, інформаційні потоки категорій $F_1 - F_3$ контролюються засобами аналізу (зламані або не були захищені).

Таким чином, будь-яка ПСЗІ може перебувати у восьми визначених вище станах.

Початковими станами можуть бути такі:

1. S_1 – захищені від засобів аналізу інформаційні потоки категорій $F_1 - F_3$;
2. S_2 – захищені від засобів аналізу інформаційні потоки категорій F_2, F_3;
3. S_3 – захищені від засобів аналізу інформаційні потоки категорій F_1,F_3;
4. S_4 – захищені від засобів аналізу інформаційні потоки категорій F_1,F_2;
5. S_5 – захищені від засобів аналізу інформаційні потоки категорії F_3;
6. S_6 – захищені від засобів аналізу інформаційні потоки категорії F_2;
7. S_7 – захищені від засобів аналізу інформаційні потоки категорії F_1.

Таким чином, початковий стан для цієї ПСЗІ визначається наявністю реалізованих способів протидії для відповідної категорії інформаційних потоків.

Розглянемо зв'язки між станами системи.

Для перекладу системи з полягання S_i в S_j, в системі діють пуасонівські потоки подій $\lambda_{i,j}(t)$ [2]. Настання події полягає в успішній спробі зламу алгоритмів протидії засобам аналізу для відповідної категорії інформаційних потоків. Враховуючи визначені в попередньому розділі стани, процес отримання контролю над ПСЗІ засобами аналізу можна подати у вигляді графа G (рис. 1).

Для скорочення запису приймемо таке позначення: $\lambda_{ij}(t) = \lambda_{ij}$

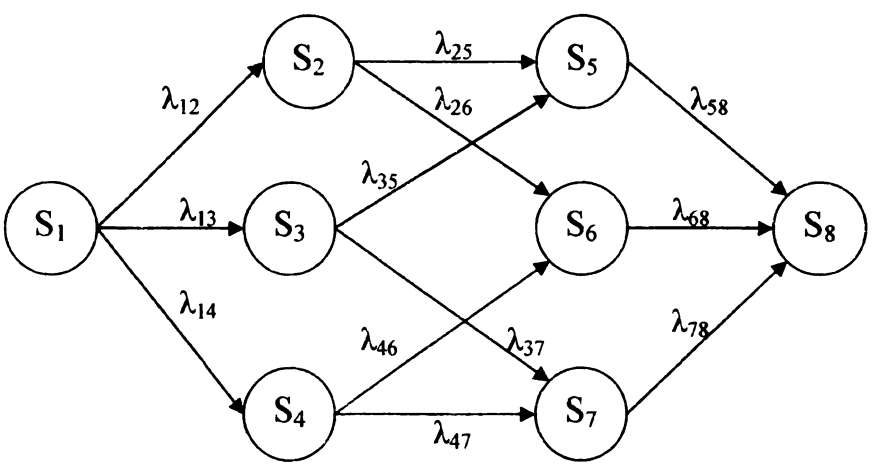

Рис.1. **Граф G**

Для перекладу ПСЗІ в стани, перехід в які характеризується нейтралізацією способів протидії потоків категорії F_1 (перехід з S_1 в S_2, перехід з S_3 в S_5, перехід з S_4 в S_6, перехід з S_7 в S_8) діє пуасонівський

потік успішних спроб нейтралізації способів протидії для F_1. Інтенсивність цього пуасонівського потоку дорівнює:

$$\lambda_1(t) = \lambda_{12}(t) = \lambda_{35}(t) = \lambda_{46}(t) = \lambda_{78}(t).$$

Для перекладу системи в стани, які характеризуються нейтралізацією способів протидії потоків категорії F_2 (перехід з S_1 в S_3, перехід з S_2 в S_5, перехід з S_4 в S_7, перехід з S_6 в S_8), діє пуасонівський потік успішних спроб нейтралізації способів протидії для F_2. Інтенсивність цього дорівнює:

$$\lambda_2(t) = \lambda_{13}(t) = \lambda_{25}(t) = \lambda_{47}(t) = \lambda_{68}(t).$$

Для перекладу системи в стани, які характеризуються нейтралізацією способів протидії потоків класу F_3 (перехід з S_1 в S_4, перехід з S_2 в S_6, перехід з S_3 в S_7, перехід з S_5 в S_8) діє пуасонівський потік успішних спроб нейтралізації способів протидії для F_3. Інтенсивність цього потоку дорівнює:

$$\lambda_3(t) = \lambda_{14}(t) = \lambda_{26}(t) = \lambda_{37}(t) = \lambda_{58}(t).$$

Таким чином, в ПСЗІ, що функціонує в призначеному для користувача режимі, представленою графом G, діють потоки подій з трьома різними інтенсивностями:

1) $\lambda_1(t)$ – інтенсивність потоку успішних спроб нейтралізації способів протидії засобам аналізу інформаційних потоків класу F_1;
2) $\lambda_2(t)$ інтенсивність потоку успішних спроб нейтралізації способів протидії засобам аналізу інформаційних потоків класу F_2;
3) $\lambda_3(t)$ - інтенсивність потоку успішних спроб нейтралізації способів протидії засобам аналізу інформаційних потоків класу F_3.

Граф G з урахуванням введених позначень інтенсивностей інформаційних потоків набуває вигляду, представленого на рис. 2. Для скорочення запису приймемо таке позначення: $\lambda_i(t) = \lambda_i$

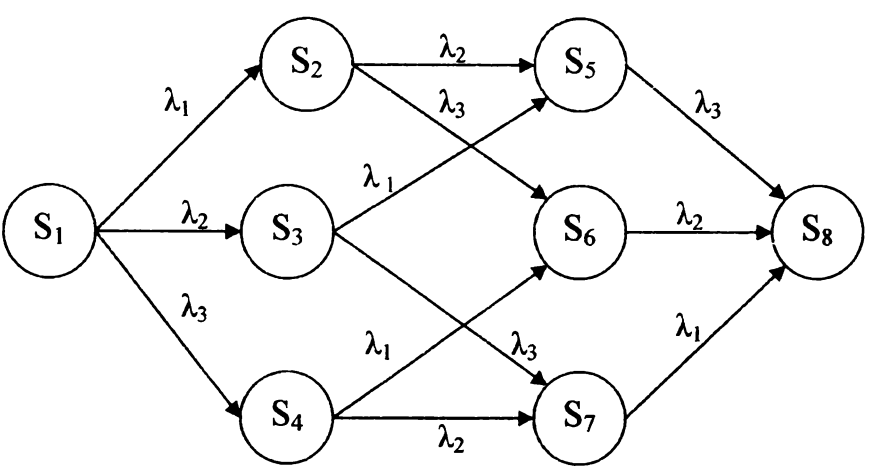

Рис.2. **Граф G_1**

Процес отримання контролю засобами аналізу над програмною системою захисту інформації, що функціонує в призначеному для користувача режимі, може бути представлений за допомогою графа, наведеного на рис. 2.

Покажемо, що процес «зламу» програмної системи захисту інформації, який функціонує в призначеному для користувача режимі, представлений графом G_1 на рис. 2 і може бути описаний за допомогою теорії марківських процесів з дискретними станами і безперервним часом [3,4]:

1) система містить кінцеву безліч станів;
2) умовна вірогідність перебування системи в будь-якому із станів не залежить від того, коли і як система прийшла в цей стан;
3) потоки подій, що переводять систему із стану в стан, є пуасонівськими (ординарні, стаціонарні, без післядії).

Оскільки процес, що протікає в системі, представленій на рис. 2, є марківським, то його можна представити за допомогою рівнянь Колмогорова [4–6].

Система рівнянь Колмогорова, що описує граф G_1, набуде такого вигляду:

$$\begin{aligned}
\frac{dp_1(t)}{dt} &= -p_1(t)*(\lambda_1(t)+\lambda_2(t)+\lambda_3(t));\\
\frac{dp_2(t)}{dt} &= p_1(t)*(\lambda_1(t)-p_2(t)*(\lambda_2(t)+\lambda_3(t));\\
\frac{dp_3(t)}{dt} &= p_1(t)*\lambda_2(t)-p_3(t)*(\lambda_1(t)+\lambda_3(t));\\
\frac{dp_4(t)}{dt} &= p_1(t)*\lambda_3(t)-p_4(t)*(\lambda_1(t)+\lambda_2(t));\\
\frac{dp_5(t)}{dt} &= p_2(t)*\lambda_2(t)+p_3(t)*\lambda_1(t)-p_5(t)*\lambda_3(t);\\
\frac{dp_6(t)}{dt} &= p_2(t)*\lambda_3(t)+p_4(t)*\lambda_1(t)-p_6(t)*\lambda_2(t);\\
\frac{dp_7(t)}{dt} &= p_3(t)*\lambda_3(t)+p_4(t)*\lambda_2(t)-p7(t)*\lambda_1(t);\\
\frac{dp_8(t)}{dt} &= p_5(t)*\lambda_3(t)+p_6(t)*\lambda_2(t)+p_7(t)*\lambda_3(t).
\end{aligned} \qquad (1)$$

Застосування умови [6] нормування дозволяє скоротити число рівнянь системи на одиницю. Умова нормування має такий вид:

$$\sum^{8} p_i(t) = 1.$$

Відповідно до умови нормування перепишемо $p_1(t)$ таким чином:

$$p_1(t) = 1 - p_2(t) - p_3(t) - p_4(t) - p_5(t) - p_6(t) - p_7(t) - p_8(t) = 1 - \sum^{8} p_i(t). \qquad (2)$$

Після застосування умови нормування, яка правильна у будь-який момент часу t, отримаємо вираз (2).

Після підстановки виразу (2) в систему рівнянь (1),отримаємо систему рівнянь (3):

$$\frac{dp_2(t)}{dt} = \left(1 - \sum_{i=2}^{8} p_i(t)\right) * \lambda_1(t) - p_2(t) * (\lambda_2(t) + \lambda_3(t));$$

$$\frac{dp_3(t)}{dt} = \left(1 - \sum_{i=2}^{8} p_i(t)\right) * \lambda_2(t) - p_3(t) * (\lambda_1(t) + \lambda_3(t));$$

$$\frac{dp_4(t)}{dt} = \left(1 - \sum_{i=2}^{8} p_i(t)\right) * \lambda_3(t) - p_4(t) * (\lambda_1(t) + \lambda_2(t)) \$$$$

$$\frac{dp_5(t)}{dt} = p_2(t) * \lambda_2(t) + p_3(t) * \lambda_1(t) - p_5(t) * \lambda_3(t); \quad (3)$$

$$\frac{dp_6(t)}{dt} = p_2(t) * \lambda_3(t) + p_4(t) * \lambda_1(t) - p_6(t) * \lambda_2(t);$$

$$\frac{dp_7(t)}{dt} = p_3(t) * \lambda_3(t) + p_4(t) * \lambda_2(t) - p_7(t) * \lambda_1(t);$$

$$\frac{dp_8(t)}{dt} = p_5(t) * \lambda_3(t) + p_6(t) * \lambda_2(t) + p_7(t) * \lambda_1(t).$$

Висновки

Отримана система рівнянь дозволяє визначати вірогідність злому програмних систем захисту інформації в довільні моменти часу.

Розроблена модель дає можливість отримувати кількісні оцінки для даних ПСЗІ, що функціонують в призначеному для користувача режимі. Отримувані оцінки можуть бути використані як для порівняння існуючих ПСЗІ, так і для аналізу змін, що вносяться до алгоритмів захисту ПСЗІ. Отриману кількісну оцінку можна розглядати як вірогідність того, що ПСЗІ не буде зламана за певний проміжок часу. Для отримання оцінки використовується система рівнянь (3). Розроблена математична модель відповідає результатам проведених експериментів і може застосовуватися для будь-яких програмних систем захисту інформації, призначених для роботи в режимі користувача.

ЛІТЕРАТУРА

1. Безруков Н. Н. Компьютерная вирусология. – К.: УРЕ, 1991.
2. Бурдаев О.В., Иванов М.А., Тетерин И.И. Компьютерная вирусология. Изд-во КУДИЦ. – 2002. – 320 с.
3. Вентцель Е.С. Теория вероятностей: Учеб. для вузов. – 6-е изд. стер. – М.: Высш. шк., 1999. – 576 с.
4. Вентцель Е.С, Овчаров Л.А. Теория случайных процессов и ее инженерные приложения. - Учеб. пособие для втузов. – М.: Высшая школа. 2000. – 383 с.
5. Лукацкий А.В., Цаплев Ю.Ю. Системы обнаружения атак. Стратегия выбора // Internet Security System, Inc., 1999.
6. Тимченко А.А., Колесников К.В., Шадхин В.Е. Системный анализ критериев и параметров проектирования системы защиты // Радіоелектронні і комп'ютерні системи, 2006, №2. – с. 63–65.

Надійшла 17.11.2008