УДК 691.3

К ВОПРОСУ МОДЕЛИРОВАНИЯ ПРОЦЕССА РЕАЛИЗАЦИИ АТАК ПОСРЕДСТВОМ КОМПЬЮТЕРНЫХ ЧЕРВЕЙ

Ю.Г. Пастернак, Н.Н. Корнеева, К.В. Дегтярева

Предлагается модель реализации атаки сетевым вредоносным обеспечением типа IM-Worm с помощью сети Петри – Маркова

Ключевые слова: IM-Worm, сети Петри – Маркова

IM черви (IM-Worm) - черви, которые используют интернет-пейджеры (так называемых «червей, передающихся по сетям мгновенного обмена сообщениями»). Такие компьютерные черви используют один единственный способ распространения – рассылку пользователям из контакт-листа жертвы сообщений, содержащих ссылку на файл, расположенный на стороннем веб-сервере [1].

Смоделируем с помощью сети Петри – Маркова атаку на информационно-телекоммуникационную систему сетевым вредоносным обеспечением типа IM-Worm. Для моделирования выбран данный математический аппарат, так как он в наибольшей степени отражает процесс распространения во времени почтового червя. Приведем необходимые для моделирования обозначения:

S_i – позиции, t_j – переходы:

S_1 - создание списка жертв;

S_2 - подготовка червя в сообщении;

S_3 - готов к внедрению;

t_1 - подготовка к атаке;

t_2 - проникновение в систему;

S_4 - сообщение прочитано/передано;

t_3 - активация;

S_5 - инфицирование системы;

t_4 - поиск жертв;

S_6 - создание списка для рассылки;

t_5 - подготовка к рассылке;

S_7 - рассылка сообщений / распространение копий.

Вид данной сети представлен на рис. 1.

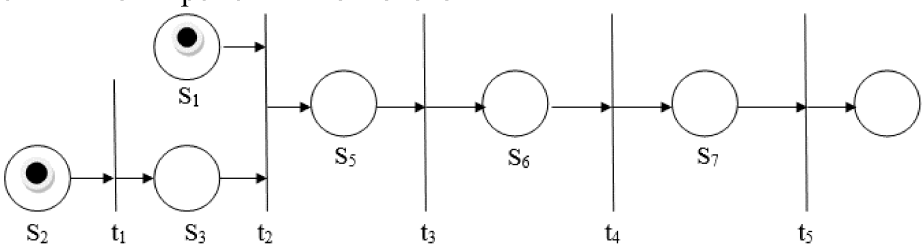

Рис. 1. Вид сети Петри-Маркова для модели атаки IM-Worm

В этой сети позиции не имеют инцидентные дуги, поэтому вероятности перемещения из них в переходы равны единице.

Для данной сети Петри – Маркова имеет место следующая система интегрально-дифференциальных уравнений, в которой $f_{S1t2}(t)$ – плотность вероятности перемещения из состояния S_i к переходу t_j, $\Phi_{S1t2}(t)$ - соответствующий закон распределения, π_{ij} - вероятность срабатывания перехода, причем вероятности срабатывания всех переходов на данной траектории не зависят от времени. Вероятность перемещения по всей сети рассчитывается по формуле

$$\pi_{рез} = \prod_{d_{ij}} \pi_{ij},$$

где d_{ij} - все полушаги сети.

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид:

$$f_{Sitj} = \lambda_{ij} e^{-\lambda ijt}.$$

Пастернак Юрий Геннадьевич – ВГТУ, д-р техн. наук, профессор, e-mail: mnac@comch.ru

Корнеева Наталья Николаевна – ВГТУ, студент, e-mail: mnac@comch.ru

Дегтярева Ксения Викторовна – ВГТУ, студент, e-mail: mnac@comch.ru

$$\Phi_{S1t2}(t) = \pi_{12} \int_0^t f_{S1t2}(\tau) d\tau;$$

$$\Phi_{S2t1}(t) = \pi_{21} \int_0^t f_{S2t1}(\tau) d\tau;$$

$$\Phi_{S3t2}(t) = \pi_{32} \int_0^t f_{S1t2}(\tau) \Phi_{S2t1}(t - \tau) d\tau;$$

$$\Phi_1(t) = \int_0^t f_{S1t2}(\tau) \Phi_{S3t2}(\tau) + f_{S3t2}(\tau) \Phi_{S2t1}(\tau) d\tau;$$

$$\Phi_{S4t3}(t) = \pi_{43} \int_0^t f_{S4t3}(\tau) \Phi_1(t - \tau) d\tau;$$

$$\Phi_{S5t4}(t) = \pi_{54} \int_0^t f_{S5t4}(\tau) \Phi_{S4t3}(t - \tau) d\tau;$$

$$\Phi_{S6t5}(t) = \pi_{65} \int_0^t f_{S6t5}(\tau) \Phi_{S5t4}(t - \tau) d\tau.$$

Согласно предельной теореме, для решающих событий при последовательном разрежении стационарного ординарного потока результирующий поток с увеличением числа разрежений приближается к простейшему. Таким образом, результирующий поток и есть простейший. Для расчета плотностей распределения вероятностей времени перемещения в переходы сети Петри – Маркова целесообразно применить пуассоновское приближение. Тогда получим среднее время τ перемещения по Петри – Маркова из начальной позиции до конечного перехода:

$$\tau_1 = \tau_{21} + \tau_{32},$$

$$\tau_2 = \frac{\tau_{12}^2 + \tau_{12} \times \tau_1 + \tau_1^2}{\tau_{12} + \tau_1},$$

$$\tau_3 = \tau_2 + \tau_{43} + \tau_{54} + \tau_{65},$$

$$\tau = \frac{\tau_{12}^2 + \tau_{12} \times (\tau_{21} + \tau_{32}) + (\tau_{21} + \tau_{32})^2}{\tau_{12} + \tau_{21} + \tau_{32}} + \tau_{43} + \tau_{54} + \tau_{65}.$$

Формула вероятности принимает вид:

$$P(t) = 1 - e^{-\frac{t - \tau_a}{\tau}}.$$

Таким образом, с помощью сети Петри – Маркова было проведено моделирование процесса распространения сетевых червей класса «IM-Worm».

Литература

1. Остапенко Г.А., Риски распределенных систем: методики и алгоритмы оценки и управления / Г.А. Остапенко, Д.О. Карпеев, Д.Г. Плотников, Р.В. Батищев, И.В. Гончаров, П.А. Маслихов, Е.А. Мешкова, Н.М. Морозова, С.А. Рязанов, Е.В. Субботина, В.А. Транин // Информация и безопасность. 2010. Т. 13. №4. С. 485–530.

Воронежский государственный технический университет
Voronezh State Technical University

CONSTRUCTION OF MATHEMATICAL MODELS OF REALIZATION OF ATTACKS BY MALICIOUS SOFTWARE TYPE IM-WORM

Yu.G. Pasternak, N.N. Korneeva, C.V. Degtyareva

A model of the implementation of network attacks by malicious software type IM-Worm using Petri net - Markova

Key words: IM-Worm, Petri net - Markova