УДК 681.3

МОДЕЛИРОВАНИЕ ПРОЦЕСС АТАКИ ТИПА «СЛЭШДОТ-ЭФФЕКТ»

И.В. Толкачев, Ю.Ю. Филатов

В работе на основе аппарата теории сетей Петри-Маркова производиться моделирование процесса реализации атаки типа слэшдот-эффект на компьютерные системы

Ключевые слова: слэшдот-эффект, сети Петри-Маркова

Рассмотрим компьютерную систему, которая может быть подвержена деструктивным информационным воздействиям типа «слэшдот-эффект».

Смоделируем данную атаку с помощью сети Петри-Маркова [1], где S_i - позиции, t_j– переходы процесса. В частности:

S_1 – владелец сервера имеет востребованнную информацию, размещение которой может привести к «слэшдот»-эффекту;

S_2–сервер к размещению информациии готов;

t_1– размещение информации на сервере, который будет подвержен «слэшдот»-эффекту;

S_3 – злоумышленником сформирован список популярных ресурсов, на которых будет размещена ссылка на востребованную информацию на сервере;

S_4 – сервера популярных ресурсов готовы к размещению ссылки на источник востребованной информации;

t_2 – размещение ссылок на популярных ресурсах на источник востребованной информации;

S_5 – устройства пользователей готовы для отправки запросов к серверу по интересующей ссылке;

t_3 – пользователи отправляют запросы на сервер;

S_6 – порт сервера готов для приема запросов от пользователей;

t_4 – обработка принятых запросов;

S_7 - количество пользователей, посылающих запросы на сервер, возрастает;

t_5 – превышение количества принимаемых запросов;

S_8 - время обработки сервером каждого запроса увеличивается;

t_6 – прием запросов и помещение их в очередь сервера;

S_9 – запросы помещены в очередь сервера;

t_7 – переполнение очереди сервера;

S_{10} - пользователь не может своевременно получать ответы от сервера на отправленные запросы.

Вид данной сети представлен на рисунке1.

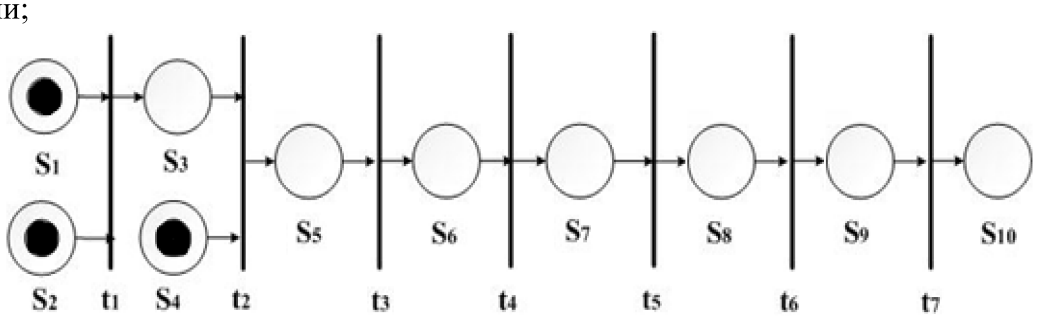

Рис. 1. Граф сети Петри-Маркова для реализации «слэшдот»-эффекта на компьютерные системы

Филатов Юрий Юрьевич – ВГТУ, студент,
e-mail: mnac@comch.ru
Толкачев Иван Васильевич – ВГТУ, аспирант,
e-mail: mnac@comch.ru

Элементы матрицы, определяющие направленности дуг графа) следующим логические функции срабатывания сети, образом:
могут быть записаны (без учета

$V_{S_1t_7}$ =

	t_1	t_2	t_3	t_4	t_5	t_6	t_7
S_1	1	0	0	0	0	0	0
S_2	1	0	0	0	0	0	0
S_3	$S_1t_1 \cap S_2t_1$	1	0	0	0	0	0
S_4	0	1	0	0	0	0	0
S_5	0	$S_3t_2 \cap S_4t_2$	1	0	0	0	0
S_6	0	0	1	1	0	0	0
S_7	0	0	0	1	1	0	0
S_8	0	0	0	0	1	1	0
S_9	0	0	0	0	0	1	1
S_{10}	0	0	0	0	0	0	1

Для данной сети Петри-Маркова имеет интегрально-дифференциальных место следующая система уравнений:

$$\Phi_{S_1t_1}(t) = \pi_{11}\int_0^t f_{S_1t_1}(\tau)d\tau,$$

$$\Phi_{S_2t_1}(t) = \pi_{21}\int_0^t f_{S_2t_1}(\tau)d\tau,$$

$$\Phi_1(t) = \int_0^t f_{S_1t_1}(\tau)\,\Phi_{S_2t_1}(t) + f_{S_2t_1}(\tau)\Phi_{S_1t_1}(t),$$

$$\Phi_{S_3t_2}(t) = \pi_{32}\int_0^t f_{S_3t_2}(\tau)\Phi_1(t-\tau)d\tau,$$

$$\Phi_{S_4t_2}(t) = \pi_{42}\int_0^t f_{S_4t_2}(\tau)d\tau,$$

$$\Phi_2(t) = \int_0^t f_{S_3t_2}(\tau)\,\Phi_{S_4t_2}(t) + f_{S_4t_2}(\tau)\Phi_{S_3t_2}(t),$$

$$\Phi_{S_5t_3}(t) = \pi_{53}\int_0^t f_{S_5t_3}(\tau)\Phi_2(t-\tau)d\tau,$$

$$\Phi_{S_6t_4}(t) = \pi_{64}\int_0^t f_{S_6t_4}(\tau)\Phi_{S_5t_3}(t-\tau)d\tau,$$

$$\Phi_{S_7t_5}(t) = \pi_{75}\int_0^t f_{S_7t_5}(\tau)\Phi_{S_6t_4}(t-\tau)d\tau,$$

$$\Phi_{S_8t_6}(t) = \pi_{86}\int_0^t f_{S_8t_6}(\tau)\Phi_{S_7t_5}(t-\tau)d\tau,$$

$$\Phi_{S_9t_7}(t) = \pi_{97}\int_0^t f_{S_9t_7}(\tau)\Phi_{S_8t_6}(t-\tau)d\tau,$$

где $f_{S_i t_j}(t)$ – плотность вероятности времени перемещения из состояния S_i к переходу t_j; $\Phi_{S_i t_j}(t)$ соответствующий закон распределения; π_{ij} – вероятность срабатывания перехода.

Входящие запросы носят пуассоновский характер:

- сообщения поступают с постоянной интенсивностью, т.е. поток стационарен;

- события прихода запросов на сервер независимы друг от друга. Т.е. причины обусловившие приход отдельного сообщения именно в тот, а не в другой момент, как правило, не связаны с аналогичными причинами для других сообщений[2,3]. Т.е. поток без последействия;

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями[4,5].

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

$$f_{S_i t_j} = \alpha_{ij} e^{-\alpha_{ij} t},$$

где $\alpha_{ij} = 1/\tau_{ij}$ i = 1,…,10; j = 1,…,7.

Согласно предельной теореме, для редеющих событий при последовательном разрежении стационарного ординарного потока результирующий поток с увеличением числа разрежений приближается к простейшему. Таким образом, результирующий поток является экспоненциальным, так как экспоненциальный поток и есть простейший [4].

Расчет с применением прямого и обратного преобразования Лапласа получается весьма громоздким, поэтому целесообразно применять пуассоновское приближение для плотностей распределения вероятностей времени перемещения в переходы сети Петри-Маркова. Применяя пуассоновское приближение, получим среднее время τ перемещения по сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения

$$\tau_1 = \frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}},$$

$$\tau_2 = \tau_1 + \tau_{32},$$

$$\tau_3 = \frac{\tau_{42}^2 + \tau_{42}\tau_2 + \tau_2^2}{\tau_{42} + \tau_2},$$

$$\tau_4 = \tau_3 + \tau_{53},$$

$$\tau_{5=} \tau_4 + \tau_{64} + \tau_{75} + \tau_{86} + \tau_{97},$$

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

где исходные параметры атаки принимают следующие значения:

λ – интенсивность атаки (количество сообщений/с); m– количество сообщений, которое требуется отправить жертве; τ_{11} = 350 с – среднее время формирования информации, размещение которой может привести к «слэшдот»-эффекту; τ_{21} = 3,1 с – среднее время подготовки сервера, τ_{32} = 12,5 с – среднее время формирования списка популярных ресурсов ;τ_{42} = 11,4 с – среднее время подготовки сервера популярного ресурса;τ_{53} = 6,5 с – среднее время подготовки рабочих машин пользователей;

τ_{64} = 3,8 с – среднее время подготовки сервера для обработки запросов; τ_{75} = 634 с – среднее время нарастания количества пользователей; τ_{86} = 9,1 с – среднее время появления задержки в обработке запросов; τ_{97} = 1,7 с – среднее время переноса запросов в очередь; $\tau_{10\,7}$ = m/ λс – среднее время переполнения очереди сервера.

Представленная модель, является обобщенной моделью реализации процесса «слэшдот»-эффекта на компьютерные системы.

Таким образом, полученные данные демонстрируют, что среднее время реализации «слэшдот»-эффекта и затраты на нее незначительны. Следовательно, для уменьшения последствий реализации «слэшдот»-эффекта необходимо использовать программные или программно-аппаратные средства для отслеживания резкого роста принимаемых сервером запросов и увеличения производительности сервера при регистрации такого роста.

Литература

1. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. - М: РадиоСофт. 2010. - 232 с.

2. Malda R. Free Internet Forum Software: Slashdot, Phpbb, Fluxbb, Fudforum, Beehive Forum , Phorum, 2010.- P. 10–18.

3. McFedries P. World Slashdot / McFedries P., R., Miller, February 17, 2004.- P.68-72

4. Гмурман В.С. Теория вероятностей и математическая статистика. – М.: Высшая школа, 2003. – 479 с.

5. Вентцель Е.С. Теория вероятностей и ее инженерные приложения: учеб. пособие для втузов / Е.С. Вентцель, Л.А. Овчаров. – М.: Высшая школа, 2003. – 464 с.

Воронежский государственный технический университет
Voronezh state technical university

MODELING FOR SLASHDOT EFFECT ON COMPUTER SYSTEMS

I.V. Tolkachov, Yu.Yu. Filatov

In this paper is modeling process implementation for slashdot effect on computer systems, which resulted in the dependence of the probability of a slashdot effect on the time

Key words: slashdot effect, Petri net and Markov chains