УДК 681.3

МОДЕЛИРОВАНИЕ ПРОЦЕССА ФЛУД-АТАКИ НА ПОЧТОВЫЙ СЕРВЕР: ИСПОЛЬЗОВАНИЕ ВРЕДОНОСНОЙ ПРОГРАММЫ EMAIL-FLOODER

В.В. Бутузов, П.А. Паринов

В работе на основе аппарата теории сетей Петри-Маркова производиться моделирование процесса реализации флуд-атаки на почтовый сервер, с использованием вредоносной программы Email-flooder

Ключевые слова: флуд-атака, Email-flooder, сети Петри-Маркова

Рассмотрим флуд-атаку на почтовый сервер, с использованием вредоносной программы Email-flooder [1, 2].

Смоделируем данную атаку с помощью сети Петри-Маркова [3], где S_i - позиции, t_j – переходы процесса. В частности:

S_1 – злоумышленник имеет информацию для формирования команды вредоносной программе Email-flooder;

S_2– хост злоумышленника готов;

t_1– формирование комадны для управляющего сервера;

S_3 –команда для управляющего сервера готова;

S_4 – управляющий сервер готов принять команду;

t_2 – отпрака команды управляющему серверу;

S_5 – управляющий сервер принял команду для дальнейшей ее пересылке;

S_6 – устройство с вредоносной программой Email-flooder готово принять команду от управляющего сервера;

t_3 – отправка команды устройствам с вредоносной программой Email-flooder;

S_7 – устройства с вредоносной программой приняли команду;

t_4 – обработка принятой команды;

S_8 - команда обработана;

t_5 – формирование сообщений, в соответствии с принятой командой;

S_9 - сообщения для отправки сформированы;

t_6 – настройка вредоносной программы Email-flooder;

S_{10} - вредоносная программа Email-flooder настроена и готова к атаке;

S_{11} - атакуемый почтовый сервер готов принять сообщения;

t_7 – отправка сообщений и помещение их в очередь почтового сервера;

S_{12} – сообщения помещены в очередь почтового сервера;

t_8 – переполнение очереди почтового сервера;

S_{13} - пользователь не может обрабатывать поступающие сообщения.

Вид данной сети представлен на рис. 1

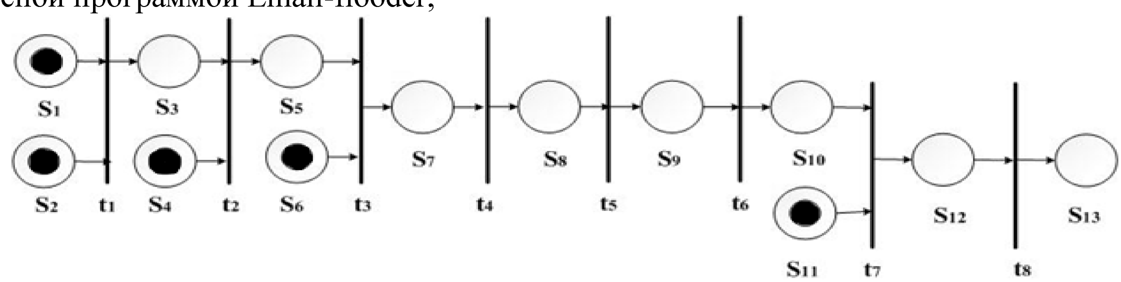

Рис. 1. Вид сети Петри-Маркова для флуд-атаки на почтовый сервер, с использованим вредоносной программы Email-flooder

Бутузов Владимир Вячеславович – ВГТУ, аспирант,
e-mail: manc@comch.ru
Паринов Павел Александрович – ВГТУ, студент,
e-mail: manc@comch.ru

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

$$
V_{S_1 t_8} = \begin{array}{c|cccccccc}
 & t_1 & t_2 & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 \\
\hline
S_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
S_2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
S_3 & S_1 t_1 \cap S_2 t_1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
S_4 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
S_5 & 0 & S_3 t_2 \cap S_4 t_2 & 1 & 0 & 0 & 0 & 0 & 0 \\
S_6 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
S_7 & 0 & 0 & S_5 t_3 \cap S_6 t_3 & 1 & 0 & 0 & 0 & 0 \\
S_8 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
S_9 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\
S_{10} & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
S_{11} & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
S_{12} & 0 & 0 & 0 & 0 & 0 & 0 & S_{10} t_7 \cap S_{11} t_7 & 1 \\
S_{13} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
$$

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

$$\Phi_{S_1 t_1}(t) = \pi_{11} \int_0^t f_{S_1 t_1}(\tau) d\tau,$$

$$\Phi_{S_2 t_1}(t) = \pi_{21} \int_0^t f_{S_1 t_1}(\tau) d\tau,$$

$$\Phi_1(t) = \int_0^t f_{S_1 t_1}(\tau)\, \Phi_{S_2 t_1}(t) + f_{S_1 t_1}(\tau) \Phi_{S_1 t_1}(t),$$

$$\Phi_{S_3 t_2}(t) = \pi_{32} \int_0^t f_{S_3 t_2}(\tau) \Phi_1(t-\tau) d\tau,$$

$$\Phi_{S_4 t_2}(t) = \pi_{42} \int_0^t f_{S_4 t_2}(\tau) d\tau,$$

$$\Phi_2(t) = \int_0^t f_{S_3 t_2}(\tau)\, \Phi_{S_4 t_2}(t) + f_{S_4 t_2}(\tau) \Phi_{S_3 t_2}(t),$$

$$\Phi_{S_5 t_3}(t) = \pi_{53} \int_0^t f_{S_5 t_3}(\tau) \Phi_2(t-\tau) d\tau,$$

$$\Phi_{S_6 t_3}(t) = \pi_{63} \int_0^t f_{S_6 t_3}(\tau) d\tau,$$

$$\Phi_3(t) = \int_0^t f_{S_5 t_3}(\tau)\, \Phi_{S_6 t_3}(t) + f_{S_6 t_3}(\tau) \Phi_{S_5 t_3}(t),$$

$$\Phi_{S_7 t_4}(t) = \pi_{74} \int_0^t f_{S_7 t_4}(\tau) \Phi_3(t-\tau) d\tau,$$

$$\Phi_{S_8 t_5}(t) = \pi_{85} \int_0^t f_{S_8 t_5}(\tau) \Phi_{S_7 t_4}(t-\tau) d\tau,$$

$$\Phi_{S_9 t_6}(t) = \pi_{96} \int_0^t f_{S_9 t_6}(\tau) \Phi_{S_8 t_5}(t-\tau) d\tau,$$

$$\Phi_{S_{10} t_7}(t) = \pi_{10\,7} \int_0^t f_{S_{10} t_7}(\tau) \Phi_{S_9 t_6}(t-\tau) d\tau,$$

$$\Phi_{S_{11} t_7}(t) = \pi_{11\,7} \int_0^t f_{S_{11} t_7}(\tau) d\tau,$$

$$\Phi_4(t) = \int_0^t f_{S_{10} t_7}(\tau)\, \Phi_{S_{11} t_7}(t) + f_{S_{11} t_7}(\tau) \Phi_{S_{10} t_7}(t),$$

$$\Phi_{S_{12} t_8}(t) = \pi_{12\,8} \int_0^t f_{S_{12} t_8}(\tau) \Phi_4(t-\tau) d\tau,$$

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 сообщения носят пуассоновский характер:

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

- события прихода сообщений 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. Т.е. поток без последействия;

-сообщения приходят по одному, а не парами, тройками и т.д, так как сервер в один момент времени способен обработать только одно сообщение. Т.е. поток сообщений приходящий на сервер является ординарным.

Таким образом, даже, если брать по отдельности разные каналы коммутации, из которых идут ординарные потоки сообщений на почтовую систему, и даже, если они имеют последействие, то при их сложении получится поток, в котором последействие ослабевает. Результирующий входящий поток также будет ординарным и без последействия, то есть, относиться к типу пуассоновского [4].

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,…,13; j = 1,…,8.

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 [3].

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:

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

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

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

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

$$\tau_5 = \frac{\tau_{63}^2 + \tau_{63}\tau_4 + \tau_4^2}{\tau_{63} + \tau_4},$$

$$\tau_{6=}\ \tau_5 + \tau_{74} + \tau_{85} + \tau_{96} + \tau_{10\,7},$$

$$\tau_7 = \frac{\tau_{11\,7}^2 + \tau_{11\,7}\tau_6 + \tau_6^2}{\tau_{11\,7} + \tau_6},$$

$$\tau \quad = \tau_7 + \tau_{12\,8}.$$

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

где исходные параметры атаки принимают следующие значения:

λ – интенсивность атаки (количество сообщений/с); m – количество сообщений, которое требуется отправить жертве; τ_{11} = 0,2 с – среднее время формирования команды; τ_{21} = 3,1 с – среднее время подготовки хоста злоумышленника, τ_{32} = 0,5 с – среднее время отправки команды управляющему серверу; τ_{42} = 3 с – среднее время подготовки управляющего сервера; τ_{53} = 5,5 с – среднее время рассылки команды устройствам с вредоносной программой Email-flooder; τ_{63} = 3 с – среднее время подготовки устройств с вредоносной программой Email-flooder; τ_{74} = 1,2 с – среднее время обработки принятой команды; τ_{85} = 13,1 с – среднее время формирования сообщений; τ_{96} = 1,7 с – среднее время настройки вредоносной программы Email-flooder; $\tau_{10\,7}$ = 0,5– среднее время на отправку сообщений жертве; $\tau_{11\,7}$ = 3 с – среднее время на подготовку атакуемого почтового сервера принять сообщение; $\tau_{12\,8}$ = m/ λ с – среднее время переполнения очереди почтового сервера.

Рассмотрим зависимость вероятности реализации атаки от времени и интенсивности атаки, примем количество сообщений, которое требуется отправить жертве m = 100000.

Зависимость вероятности реализации флуд-атаки на почтовый сервер, с использованием вредоносной программы Email-flooder от времени и интенсивности атаки приобретает вид, представленный на рис. 2.

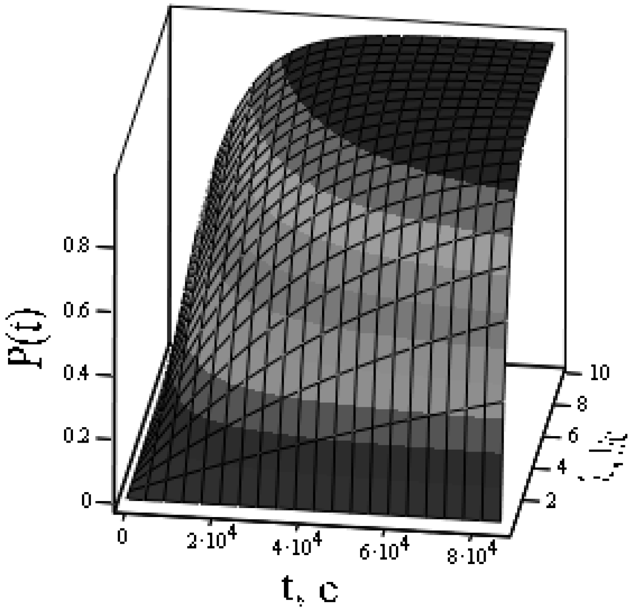

Рис. 2. Зависимость вероятности реализации флуд-атаки на почтовый сервер, с использованием вредоносной программы Email-flooder, от времени и интенсивности атаки

Представленная модель, является обобщенной моделью проведения флуд-атаки на почтовый сервер с использованием вредоносной программы Email-flooder.

Таким образом, полученные данные демонстрируют, что среднее время реализации флуд-атаки и затраты на нее незначительны. Следовательно, для уменьшения опасности реализации флуд-атаки необходимо использовать программные или программно-аппаратные средства для фильтрации нежелательных сообщений.

Литература

1 Информационный портал по безопасности http://www.securelist.com/

2 Касперски К.. Записки исследователя компьютерных вирусов. - Издательство: Питер, 2005. – 316 с.

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

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

Воронежский государственный технический университет
Voronezh state technical university

MODELING FLOOD ATTACKS ON MAIL SERVERS USING MALWARE EMAIL-FLOODER

V.V. Butuzov,P.A. Parinov

In this paper is modeling process implementation of flood attacks on the mail server, using malware Email-flooder, which resulted in the dependence of the probability of an attack on the time

Key words: flood attack, Email-flooder, Petri net and Markov chains