UDC 004.056.57

ANALYSIS OF REALIZATION AND METHOD OF DETECTING LOW-INTENSITY HTTP-ATTACKS. PART 2. METHOD OF DETECTING SLOW HTTP ATTACKS

A. CARLSSON
Blekinge Institute of Technology
E. DURAVKIN, A. LOKTIONOVA
Kharkiv National University of Radioelectronics

Abstract *- Analysis of the implementation specifics Slow HTTP- attacks allowed to allocate a set of features, based on which is possible to detect this type of attack. The model of the web- server's behavior when implementing Slow HTTP- attack was created. The model is based on Markov chains using the machine as a means of describing the web-server transitions between states. The formulary relations allowing to calculate the probability of transition of web-server into overload condition for known values of intensities Incoming and outgoing requests were derived. Definable relations allowing to calculate the transition to web-server overload condition using the method of generating functions were withdrawn.*

Анотація *– Аналіз особливостей реалізації Slow HTTP - атак дозволив виділити набір ознак, на підставі яких можливе виявлення атак даного типу. Розроблено модель web -сервера при реалізації Slow HTTP - атаки. Модель заснована на використанні апарату Марківських кіл, як засобу опису переходів web - сервера між станами . Виведено аналітичні співвідношення, що дозволяють розрахувати ймовірність переходу web - сервера в стан перевантаження при відомих значеннях інтенсивностей надходження і обробки запитів. Виведено аналітичні співвідношення, що дозволяють розрахувати час переходу web -сервера в стан перевантаження за допомогою методу виробничих функцій.*

Аннотация *– Анализ особенностей реализации Slow HTTP-атак позволил выделить набор признаков, на основании которых возможно обнаружение атак данного типа. Разработана модель web-сервера при реализации Slow HTTP-атаки. Модель основана на использовании аппарата Марковских цепей как средства описания переходов web-сервера между состояниями. Выведены соотношения, позволяющие рассчитать вероятность перехода web-сервера в состояние перегрузки при известных значениях интенсивностей поступления и обработки запросов. Выведены зависимости, позволяющие рассчитать время перехода web-сервера в состояние перегрузки при помощи метода производящих функций.*

Introduction

The main implementation feature of DoS-attacks on network and transport layers is generating significant traffic, which allows blocking the bandwidth of attacked site. Abrupt generation of large amounts of traffic causes anomalies in statistical description. Modern IDS`s are directed towards discovering such anomalies [1].For this purpose they use wavelet analysis, regression analysis, etc. [2]

Slow HTTP-attacks differ from simple DoS-attacks by the absence of such large amounts of traffic. Thus, all means that are aimed at detecting and preventing DoS-attacks on network and transport layers are low efficient in this case.

Consequently, it is necessary to develop a mathematical model, which will formalize this type of attacks, as well as to develop an algorithm to detect it.

I. Slow HTTP-attack detection model

Investigations of this attack type`s nature showed that during implementation of such attacks the flow of attacker`s requests can be considered as the simplest one.

Parameters of http-requests (length, data reception rate, size of received data and delay between acknowledgments) are identical and constant. This fact allows describing attacked Web-server as a queuing system of M/M/N type, where N stands for maximum number of concurrent http-requests (maximum number of processes (threads) that can be run simultaneously by Web-server). For example, for Apache server it can be replaced by «MaxClients» parameter from the configuration file «http.conf».

The presence of buffer can be neglected in this case since it does not affect the fact of launching an attack, but affects only its duration. Hence, the graph of attacked web-server states can look like as shown in Fig. 1.

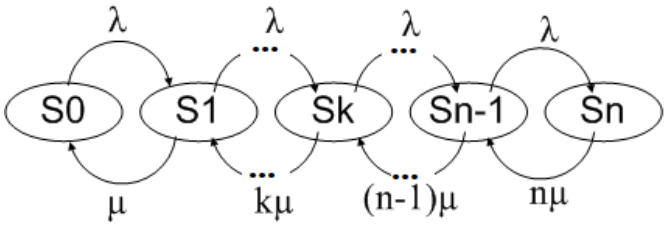

Fig. 1. Tagged graph of Web-server state transition

The states of the web-server are:

S_0 - 0 requests are being served;

S_1 - 1 request is being served;

……..

S_k - k requests are being served;

……..

S_{n-1} - n-1 requests are being served;

S_n - n requests are being served, server is overloaded.

The parameters of the model are:

n - maximum number of concurrent http-requests;

k - current number of concurrent http-requests;

λ - arrival rate of http-requests;

μ - intensity of http-request serving.

According to the mass service theory, one of two events which lead to change of web-server state can occur at the same time:

- http-request inflow, that leads to transition to a neighboring state; if server is in a state S_n, its state does not change which corresponds to denial of service;

- completion of http-request serving and transition to a state with a lower number.

The above arguments allow using the Erlang`s formula to calculate probabilities for each (k-th) state (p_k) of Web-server:

$$p_k = \frac{\frac{\alpha^k}{k!}}{\sum_k^n \frac{\alpha}{k!}^k}, \quad (1)$$

where:

$$\alpha = \frac{\lambda}{\mu}. \quad (2)$$

Expression (1) allows associating request arrival rate (λ) with request serving rate (μ) [3].

As was mentioned in [4], the feature of slow-http attacks is not a significant increase of the input stream intensity, but drop of served http-requests number with a steady input stream.

Fig. 2 shows the probability distribution of Web-server states during normal operation mode (a), and during the implementation of slow-http (slow head) attacks (b-d).

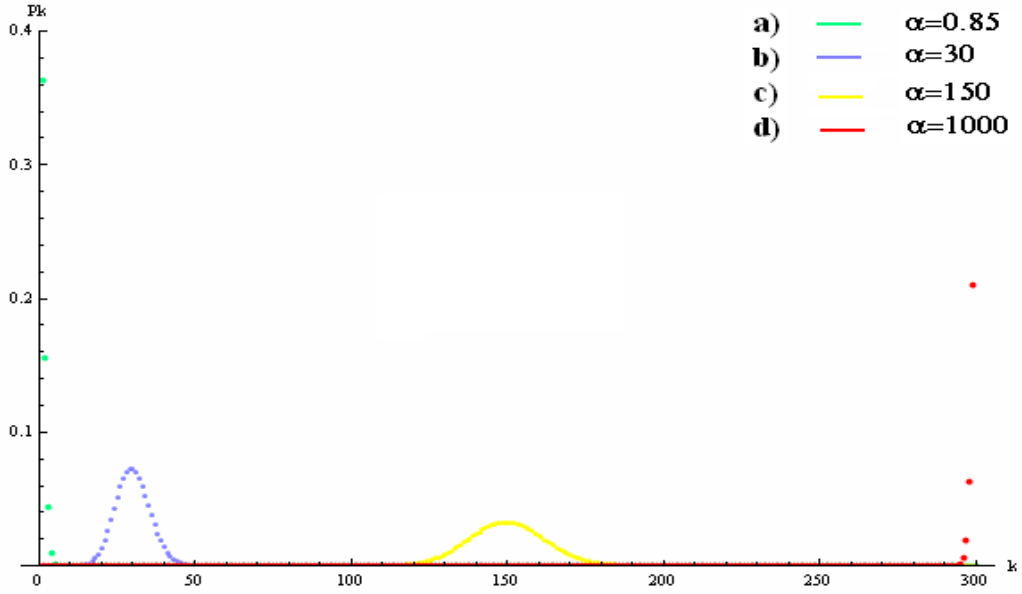

Fig. 2. Graph of web-server state distribution for different values of α

As can be seen from the graph shown in Fig. 2, probability distribution of Web-server states shifts to the right during attack implementation. Hence, slow-http attack detection system can calculate this parameter in real time and generate warnings.

The disadvantage of this approach is inability to assess the time when server status changes to "overloaded". It is proposed to use the generating functions method to overcome this problem [5].

According to this method system is represented by a set of states and characteristics of transitions between them written as: $f(p_i, t_i) = p_i z^{t_i}$, p_i - probability of transition to state i, t_i - transition time to state i.

Previously obtained web-server state model, provided in the form of a Markov chain, was displayed using the method of generating functions in order to obtain probability-time graph presented in Fig. 3.

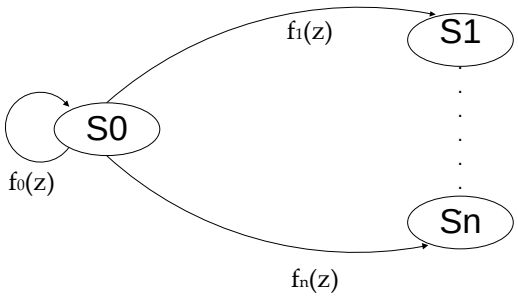

Fig. 3. Probability-time graph of Web-server state transitions

According to the methods of probability-time graph conversion, it can be converted to the form shown in Fig. 4.

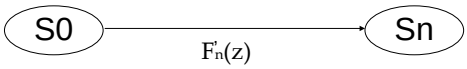

Fig. 4. Transformed probability-time graph of Web-server state transition

Generating function of this graph is:

$$F_n'(z) = (\sum_{i=1}^{n} P_i z^{t_i})(1 - P_0 z^{t_0})^{-1}. \quad (3)$$

Transit time to the overloaded state of attacked server can be determined using this expression:

$$\overline{T}_n = \left.\frac{dF_n'(z)}{dz}\right|_{z=1} = \frac{(\sum_{i=1}^{n} P_i t_i)\cdot -(1-P_0) + \sum_{i=1}^{n} P_i P_0 t_0}{(1-P_0)^2}, \quad (4)$$

where:

$$t_i = \frac{1}{\lambda}\cdot k_i. \quad (5)$$

Fig. 5 shows the dependence of transit time to the overloaded state of Web-server on intensity ratio of the input and output streams.

The analysis of this dependence shows that it is non-linear and therefore, for effective prevention of such attacks, detection system must be activated before α reaches the value of 500. After this value, an abrupt acceleration of server overload occurs, and server cannot continue to serve users [6].

Conclusion

Implementation model of Slow HTTP-attacks, developed using Markov chains and queuing systems theory, allowed to obtain the initial data for attack detection model that uses the method of generating functions.

Such attack detection model allows measuring the transition time to overloaded condition of attacked system. This can be used for attack prevention algorithms.

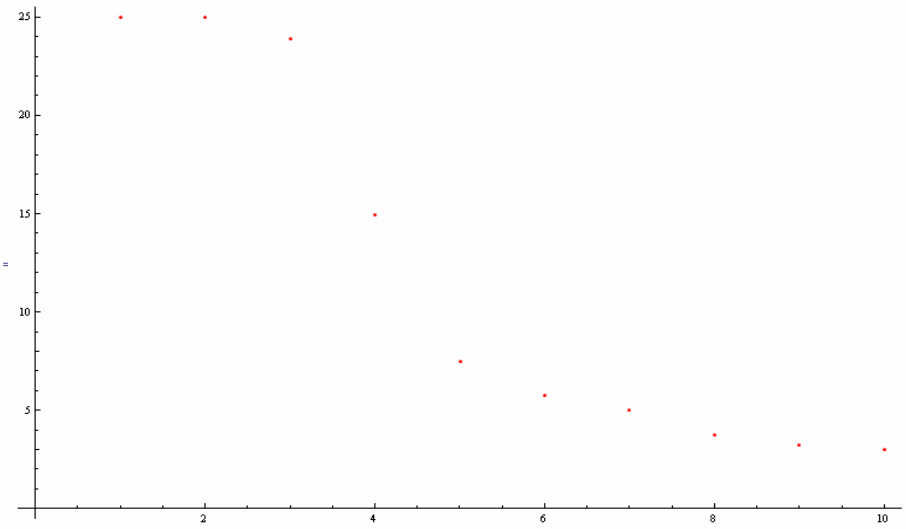

Fig. 5. The dependence of transit time to the overloaded state of Web-server on intensity ratio of the input and output streams.

However, this model has some drawbacks, such as:

- the inability to track the location of attacker`s host;
- the absence of legitimate traffic distinguishing mechanism in case of a bad client`s link or during high user activity.

These disadvantages are the prerequisites for further improvement of the model. The improvement of this method is planned at the next stage of research, which will eliminate the above disadvantages and allow further using the model as low intensity attack detection system on application layer or as an additional tool for existing IDS-systems.

References

1. Denial of Service Attack - Prevent DoS Attacks with Palo Alto Networks [Electronic resource]. – Access mode: https://www.paloaltonetworks.com/resources/learning-center/what-is-a-denial-of-service-attack-dos.html

2. *Scargle J.D.* Wavelet and Other Multi-resolution Methods for Time Series Analysis. // Statistical Challenges in Modern Astronomy II / Ed. G.J.Babu and E.D.Feigelson. – Springer New York, 1997. – P. 333-347.

3. *Венцель Е.С.* Теория вероятностей. – М.: Наука, 1969. – 576 с.

4. *Carlsson A.* Analysis of realization and method of detecting low-intensity HTTP-attacks [Електронний ресурс] / A. Carlsson, E.V. Duravkin, A.S. Loktionova // Проблеми телекомунікацій. – 2013. – № 3 (12). – С. 61–70. – Режим доступу: http://pt.journal.kh.ua/2013/3/1/133_carlsson_attack.pdf.

5. *Albert R. Meyer, Ronitt Rubinfeld* Generating Functions // Mathematics for Computer Science. – 2005. – P. 9-12.

6. *Ian Muscat.* How to mitigate Slow HTTP DoS Attacks in Apache HTTP Server [Electronic resource]. – Access mode: http://www.acunetix.com/blog/web-security-zone/articles/slow-http-dos-attacks-mitigate-apache-http-server.