Method of Slow-Attack Detection

Ievgen Duravkin, Anastasiya Loktionova
Telecommunication Systems Departament
Kharkiv National University of Radioelectronics
Kharkiv, Ukraine
duravkin_evgen@mail.ru

Anders Carlsson
Blekinge Institute of Technology
Karlskrona, Sweden

Abstract — **The analysis of realization low-intensity HTTP-attacks was performed. Were described scenarios of Slowloris, Slow POST and Slow READ attack. Features of this type of attacks in comparison with low-level attacks such as "denial of service" were selected: they do not require a large number of resources from the attacking machine, and they are difficult for the detection, since their parameters are similar to legitimate traffic. For each type of attacks the characteristic features were highlighted. Parameters of http-request, which assume the detection of this type attacks highlighted. The analysis of mathematical tools of building the models for the systems for these types of attacks detection on the basis of the obtained parameters was performed.**

Keywords: Denial of service, network attack, Slow-http, web-server.

I. Introduction

The analysis statistics of companies, which provides network protection was shown a significant increase in the volume and complexity of DOS- attacks for the last few years.

Main feature of Slow DOS attacks is similarity of attacker and legitimate traffic. Unlike ordinary DoS attacks, Slow HTTP does not fill the bandwidth, but depletes application layer (web-server) resources (memory, CPU time). Consequently, existing DOS-attack detection systems are ineffective for detecting Slow-HTTP attacks.

At present, there are several mechanisms to protect web-servers from Slow-HTTP attacks:

- •using programs like «Flying frog», based on the monitoring of HTTP-traffic and real-time event analysis;
- • creating rules that limit the number of simultaneous stream switch the same IP-address;
- •query caching;
- •using filters like DDoS GUARD.

However, these mechanisms have partial solutions that cannot protect server in its entirety.

Specialized means of protection against DOS-attacks base their work on the analysis of traffic and detecting anomalies in its structure. According to this approach the traffic characteristics in normal operation are build and the search for network anomalies on the observed range is done. In this case, the traffic anomaly is a deviation of characteristics from the statistical values, which were collected from the profiles. Deviation value equal larger than a predetermined threshold will activate the an alarm.

Thus, it became necessary to develop a systematic approach, which can detect the fact of attack, identify it source and protect server before the denial of service.

II. The Base Structural Components of Management System

Traditional approach of DOS attack detection is based on using of statistical methods, the vivlet analysis, the signature methods, the cluster analysis, etc. These methods allow effectively recognize and deal with avalanche DDoS-attacks of network and transport layers, aimed at filling the channel capacity (Smurf, UDP-flood, etc.) and the excess of the normal load of individual nodes (SYN-flood, Teardrop, Ping of death etc.).

At the same time, these approaches are ineffective for the detection of low-intensity DOS-application level attacks, which are characterized by the absence of anomalies in the traffic characteristics. To distinguish the traffic generated during such attacks from legitimate traffic is quite difficult. Consequently, the use of the signature method is not effective too. The specified class of attacks is relatively young, but statistics show that the proportion of low-intensity attacks is growing from year to year. As a rule, low-intensity attacks lead to the failure of web-servers, and at the same time they can be adapted to influence any application layer system.

The proposed method for the detection slow-http attacks based on the assessment of web-server utilization and predicting the time of its transition to a state of overload.

Analysis of the specifics in implementation slow-http attacks showed that in their implementation the increase of input stream of requests is almost not observed, at the same time there is a sharp increase in service time of requests.

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 «Max-Clients» 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.

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.

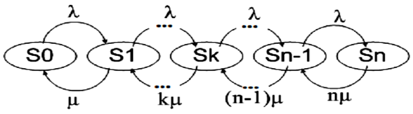

Fig. 1. Tagged graph of Web-server state transition

Formalization of request handling process by web-server as a queuing system with type M/M/N will assess the probability of transition to an overload condition. The description of web-server as queuing system with no queue is defined by the fact that the presence of waiting buffer in web-server has no effect on for its availability during the attack, and it only affects the duration of the attack. The task of the developed model is the detection of the attack, instead of calculation of its duration.

Channels for service in this case are the streams that run by web-server. The intensity of the transition from state m to $m+1$ is determined by the intensity of incoming requests for service in the opposite direction - the intensity of service requests. Number of states of the model (channels for the service (N)) corresponds to the number of threads that can be executed by the server. This parameter is specified in the configuration files of web-servers.

During normal operation mode, the intensity of the inbound and outbound flow of requests is balanced in such system; therefore, the probability of system to change its state to the final state P(N) tends to 0. At the same time, from beginning of the attack there is a sharp increase in the service time of each request that with the same intensity of the input stream will lead to an increase in P (N).

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).

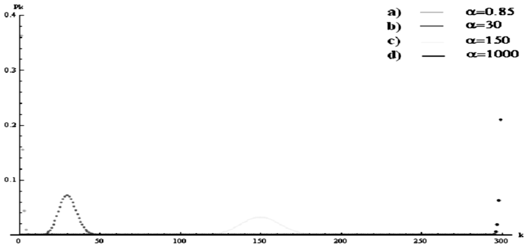

Fig. 2. Graph of web-server state distribution for different values of α

For predicting the time of transition into an overload condition have been used the apparatus of time-probability graphs and the method of generating functions.

According to this method system is represented by a set of states and characteristics of transitions between them written as: 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.

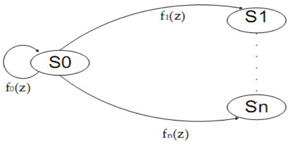

Fig. 3. Probability-time graph of Web-server state transitions

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

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

where: $t_i = \frac{1}{\lambda}\cdot k_i$.

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

III. Conclusions

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.

The process of attack detection is implemented based on a Markov model the behavior of the web server, the model parameters are the statistical characteristics of incoming, outgoing traffic, as well as the dynamics of resource use web server.

Feature of the implementation SlowHTTP attack is to use one source of the attack. Formation of traffic statistics with reference to IP-based source and destination addresses enables identification of intruders, and thus block the malicious traffic.

The advantage of the proposed system is that it allows you to detect an attack to the server status of failure, which makes it possible to implement security mechanisms in a timely manner.

References

[1] Denial of Service Attack - Prevent DoS Attacks with Palo Alto Networks [Online]. Available: 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*, Springer New York, 1997, pp. 333-347.

[3] A. Carlsson, E.V. Duravkin, A.S. Loktionova. (2013). Analysis of realization and method of detecting low-intensity HTTP-attacks. *Problemy telecomunicatsij* [Online]. no. 3, pp. 61–70. Available: http://pt.journal.kh.ua/2013/3/1/133_carlsson_attack.pdf.

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

[5] Ian Muscat. (2014). *How to mitigate Slow HTTP DoS Attacks in Apache HTTP Server* [Online]. Availible: http://www.acunetix.com/blog/web-security-zone/articles/slow-http-dos-attacks-mitigate-apache-http-server.