BIOSCIENCES BIOTECHNOLOGY RESEARCH ASIA, November 2014. Vol. **11**(Spl. Edn.), p. 173-176

Flood-attacks Within the Hypertext Information Transfer Protocol: Damage Assessment and Management

Alexandr Grigorevich Ostapenko, Maxim Vasilyevich Bursa Grigorii Alexandrovich Ostapenko and Denis Olegovich Butrik

Voronezh State Technical University, Russian Federation,
394026, Voronezh, Moskovsky Prospect, 14, Russian

doi: http://dx.doi.org/10.13005/bbra/1457

(Received: 27 September 2014; accepted: 10 October 2014)

The paper reviews an analytic damage function for information telecommunication systems to which DDoS-attacks with HTTP-flood are directed. The modification of this function at different stages of an attack is reviewed according to the actions of the attacker and the attacked. The paper also provides methods for controlling the damage function by acting on its parameters. To choose a method to control the damage the paper suggests using management efficiency based on the integrated assessment of damage.

Key words: Damage, attack, flood, management.

To conduct a risk analysis of the attacked system the damage function[1-4] should be set, which describes a negative event that occurs as a result of the destructive impact.

The considered type of DDoS-attacks[1, 3, 5] aims to exhaust the resources of the attacked system, and thereby make it unavailable. The feature of this attack is that the attackers will send hard-configured requests to computers, thus it will slow down the computer work of the victim[3, 6, 7]. Thereby, the damage will depend on the number of received messages.

Consider the change in damage at every stage of the realization of DDoS-attacks of the type HTTP-flood. Figure 1 depicts the moment of success attack characterizing the dependence of the number of incoming requests *m* received by the resource from time *t*. It shows that at the time point t_0, the intensity of attack exceeds the intensity of request processing λ_0 by a critical value m_{cr}, after which the attack is determined as successful[3, 4, 8-11].

$$m_{cr} = (\lambda_a + \lambda_n - \lambda_0)\, t_0, \qquad ...(1)$$

where: λ_n-the intensity of useful requests processing.

At the time of the success attack the damage function will be as follows:

$$u(t) = (\lambda_a + \lambda_n - \lambda_0)t \qquad ...(2)$$

After a successful attack the waiting queue of the victim starts to overflow. Until the time t_p after which the attacked begins to take actions, there is a risk to lose some resources of the attacker – the denial of infected computers.

* To whom all correspondence should be addressed.

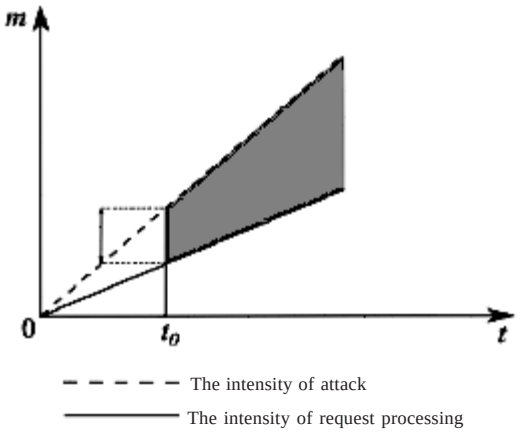

Fig. 1. The dependence of the number of incoming requests from time in the moment of success attack t_0

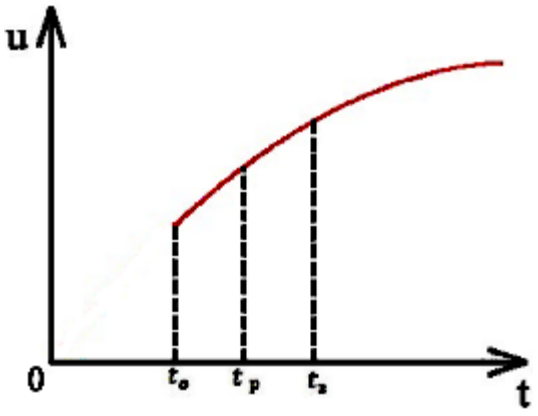

Fig. 2. Graph of damage function until the activating of the attacked system's protections means

Thus, the intensity of attack λ_a may vary as follows:

$$\lambda'_a = \lambda_a - \lambda_{in}\lambda_i^t, \quad ...(3)$$

where: λ_{in} – the intensity of denial by infected computers; $\lambda_i t$ – the number of requests sent by infected computers (multiplied by λ_{in} we get the intensivity of requests, which could receive messages to the attacked resource at normal functioning of infected computers).

The value λ'_a shows the change in intensity of attack due to disconnection of infected computers sending spam requests [3].

The damage until the activating of protections means will be equal to:

$$u(t) = (\lambda_n + \lambda_a - \lambda_p\lambda_i^t - \lambda_0)t \quad ...(4)$$

Graphical representation of the damage (4) is shown in Figure 2.

When an attack is detected, it is necessary to take actions to minimize and eliminate the damage. Considering the features of DDoS-attacks of the type HTTP-flood, namely hard access to database server, to prevent this kind of attacks it is necessary to create mirror database that is stored on the server's hard disk drives, and add new clusters united in RAID arrays. RAID 0[6, 7] should be used for maximum productivity.

RAID 0 allows increasing the memory bandwidth by several times due to additional physical disks. Stored on all disks are the same files, and requests to them proceed evenly.

The period of time $(t_p - t_r)$ is required for all of these procedures, where t_p – the activating time of protective means, and t_r – the reaction time of the victim to the attack.

Following the adoption of measures to resist the attack, the system begins to process requests that have been collected in the waiting queue with an intensity exceeding than the intensity of the attack.

At time t_n the waiting queue becomes less than the critical value m_{cr}, the damage equals to zero.

The analytic expression of the damage function with increasing productivity (adding capacity to processing requests):

$$u(t) = \begin{cases} (\lambda_n + \lambda_a - \lambda_p\lambda_i t - \lambda_o)t, t_0 \le t \le t_p, \\ (\lambda_n + \lambda_a - \lambda_p\lambda_i t - q\lambda_o)t, t_p < t \le t_n. \end{cases} \quad ...(5)$$

The option viewing above to deal with the attack is fairly simple. Increasing productivity through the RAID array, we lose much of the system reliability. If one of the hard disk drives fails, then all the disks will fail. Next, consider the situation with filtering HTTP traffic.

After detecting an attack, there is a need to produce a package of measures to detect unacceptable requests; identifying them, we can write an algorithm in the firewall settings to not reach treatments GET or complex structured requests on port 80 (HTTP-port) to the HTTP-server. Determine the percentage of the filtered network traffic as *x*. Such a way to deal with the attack type HTTP-flood is the most effective, but it requires more time to implement[5].

Expression of damage considering

filtering of network traffic will be as follows:

$$u(t)=\begin{cases}(\lambda_n+\lambda_a-\lambda_p\lambda_i t-\lambda_o)t, t_0\le t\le t_p,\\((\lambda_n+\lambda_a-\lambda_p\lambda_i t)(1-x)-q\lambda_o)t, t_p<t\le t_n.\end{cases} \quad ...(6)$$

The received expression of the damage can be normalized with the maximum value of the damage. The maximum value of the damage takes at the point t_m. To find the value , the derivative of (6) should be found and set equal to 0:

$$t_m=\frac{(\lambda_n+\lambda_a)(1-x)-q\lambda_o}{2\lambda_p\lambda_i(1-x)}.$$

The normalized damage takes the form:

$$\overline{u(t)}=\begin{cases}\dfrac{(\lambda_n+\lambda_a-\lambda_p\lambda_i t-\lambda_o)t}{\dfrac{((\lambda_n+\lambda_a)(1-x)-q\lambda_o)^2}{4\lambda_p\lambda_i(1-x)}}, t_0\le t\le t_p,\\[2ex]\dfrac{((\lambda_n+\lambda_a-\lambda_p\lambda_i t)(1-x)-n\lambda_o)t}{\dfrac{((\lambda_n+\lambda_a)(1-x)-q\lambda_o)^2}{4\lambda_p\lambda_i(1-x)}}, t>t_p.\end{cases} \quad ....(7)$$

In order to get rid of unaccepted requests, it is necessary to conduct a range of measures to identify the IP-addresses belonging to unsuspicious victims which send malicious HTTP requests to web-sites[2, 3, 5].

Figure 3 shows how the damage function changes depending on the amount of filtered traffic network:

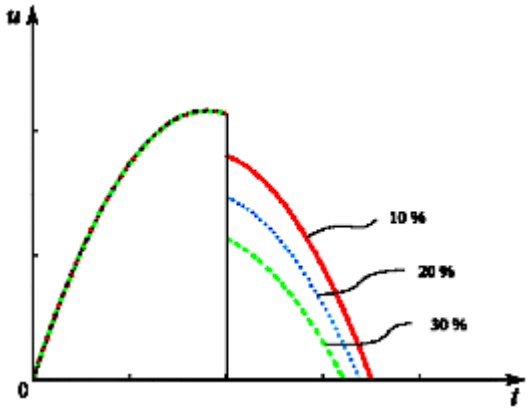

Fig. 3. Changing of the damage function with activating of filtered traffic network

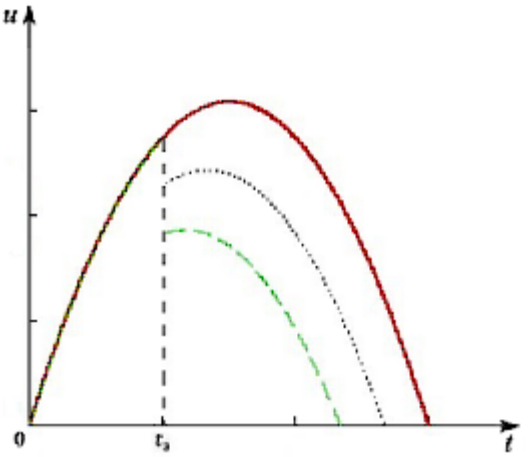

Fig. 4. Change in the damage function with increasing productivity of processing requests

Increasing productivity of proceeding requests can also reduce the quantitative value of the damage. When connecting subsidiary hard disk drives or network interfaces, queue of unaccepted requests will be processed faster. Figure 4 shows the change in the values of damage due to different amounts of subsidiary hard disk drives.

CONCLUSION

Thus, the expression (7) is received, which allows assessing the damage in an arbitrary moment of time at the known values of the intensity of attack of the type HTTP-flood λ_0, the intensity of the processing requests λ_i, the moment of success of the attack t_0, the moment of activating protecting measures t_p, the moment of neutralizing attacks t_n, the intensity of denial of infected computers from messages/requests λ_p, the number of requests sent by infected computers $\lambda_i t$, the number of subsidiary databases q, the percentage of unnecessary network traffic x.

Findings

The analytical form of the damage function for information telecommunication systems which is a subject to DDoS-attacks of the type HTTP-flood is received, allowing to conduct multiple calculations and optimization of damage

until solving management problem. The algorithm is proposed by which it is possible to increase the system security and select the most effective means of protecting information against attack[8-11].

REFERENCES

1. Hussain, A., J. Heidemann and C. Papadopoulos. A framework for classifying denial of service attacks, Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications – SIGCOMM '03. New York, USA, 2003; 99-110.
2. Ostapenko, G.A., D.G. Plotnikov, O.Y. Makarov, N.M. Tikhomirov and V.G. Yurasov, Analytical Estimation of the Component Viability of Distributed Automated Information Data Systems. *World Applied Sciences Journal,* 2013; **25**(3): 416-420.
3. Ostapenko, G.A., L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov and K.V. Simonov, Analytical Models of Information-Psychological Impact of Social Information Networks on Users. *World Applied Sciences Journal,* 2013; **25**(3): 410-415.
4. Bencsáth, B. and M.A. Rónai, Empirical analysis of denial of service attack against SMTP servers. Proceedings of the 2007 International Symposium on Collaborative Technologies and Systems. IEEE, 2007; 72-79.
5. Ostapenko, A.G., S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak and L.G. Popova, Denial of Service in Components of Information Telecommunication Systems Through the Example of "Network Storm" Attacks. *World Applied Sciences Journal,* 2013; **25**(3): 404-409.
6. Bencsáth, B. and M.A. Rónai. Empirical Analysis of Denial of Service Attack Against SMTP Servers. Laboratory of Cryptography and Systems Security (CrySyS) Department of Telecommunications. *International Journal of Computer Science and Security* (IJCSS), **6**(4): 537-550.
7. Kalashnikov, A.O., Y.V. Yermilov, O.N. Choporov, K.A. Razinkin and N.I. Barannikov, Ensuring the Security of Critically Important Objects and Trends in the Development of Information Technology. *World Applied Sciences Journal,* 2013; **25**(3): 399-403.
8. Novikov, D.A. and A.O. Kalashnikov, Information risk management in innovational Russia, Volume 16, Part 3. Voronezh: Voronezh State Technical University, 2013; 319-322.
9. Parinov, A.V. and A.A. Seregin, Chances and risks of innovative projects in the information field. Information and Security Journal, Volume 16, Part 4. Voronezh: Voronezh State Technical University, 2013; 588-591.
10. Deshin, A.E., I.A. Ushkin and O.N. Choporov, Integral assessment of the overall risk in the synthesis of ITCS on the basis of risk parameters of its components. Information and Security Journal, Volume 16, Part 4. Voronezh: Voronezh State Technical University, 2013; 510-513.
11. Radko, N.M., L.V. Parinova, Y.G. Pasternak, K.A. Razinkin and N.M. Tikhomirov, Several assessments of risks, chances and survivability of systems in terms of information epidemics. *Information and Security Journal*, 2013; **16**, Part 4. Vorone