Journal of Engineering and Applied Sciences 9 (10-12): 452-456, 2014
ISSN: 1816-949X
© Medwell Journals, 2014

Analysis of Methods Organization of the Modelling of Protection of Systems Client-Server

[1]G.A. Shangytbayeva, [1]B.S. Akhmetov, [1]R.N. Beysembekova and [2]G.N. Kazbekova
[1]Kazakh National Technical University Named after K.I. Satpayev, Almaty, Kazakhstan
[2]Kazakh Russian International University, Aktobe, Kazakhstan

Abstract: The study analyzes the methods and mechanisms the protection of information, structures attacks type DoS/DDoS/DRDoS and models of their tracking computer networks. Is developed classification of mathematical models of information threats which helps effectively to solve problems of counteraction of DoS/DDoS/DRDoS attacks. And also is carried the review of model of communication of the client and the server to see key problems of the architecture steady for the specified attacks on computer networks. Are analysed known approaches and models of tracking of attacks like DoS/DDoS/DRDoS. It is noted that for tracking of the IP address of a source of attack to refusal in service it is expedient to use a method probabilistic markings of packages.

Key words: Network attacks, DoS/DdoS/DRDoS attacks, "denial of service", detection of network attacks, networks

INTRODUCTION

Among numerous attacks of malefactors on computer networks, constantly infect the internet, most widespread are interruptions and distortions of package traffic. More common attacks to today's time is the attacks directed on refusal in service of lawful services. In this case, the initiator of attacks compromises knot user by exploiting its resources to obtain full management of knot. On the compromised knots the unauthorized user carries out attacks to the next knots. The initiator of attacks directs a large number of a counterfeit traffic to knot user, consuming thus essential volume the capacity that leads to impossibility to serve a legitimate traffic (Elliott, 2000; Hautio and Weckstrom, 1999; Ferguson and Senie, 2000).

DoS (Denial of Service Attack, 2015) attacks is such a class, leading to denial of service. During such type of attack there is a raised expense of resources of the processor and reduction of capacity of a communication channel that can lead to strong delay of work all computer network, separate tasks or in general before complete cessation of tasks of the user. The most widespread method of implementation DDoS of attack is a saturation of the attacked knot a large number of external inquiries so that is attacked the equipment which is not able to respond to the requests of users or corresponds too slowly, thus becomes actually inaccessible (Bhatia *et al.*, 2014; Bhuyan *et al.*, 2015). DRDoS (Distributed Reflection Denial of Service) distributed attack directed on absorption of capacity a network. The initiator of attack provides SYN package on any of public servers with forged IP addresses of a source to the server. The recipient of SYN of a package will generate SYN/ACK and to send it in a target network. Thus, the server is used by the initiator of attacks to display packages on a target network, without sending packages directly to a target network as in a case with DdoS attack (Lee, 2000; Li Mhu *et al.*, 2008; Ioannidis and Bellovin, 2002).

Objective of the study: This research is directed on studying of methods and mechanisms of information security, structures of attacks like DoS/DDoS/DRDoS and models of their tracking in computer networks.

Literature review: In research considered the problem classification of information threats of computer information and is carried the analysis of the most widespread and theoretically reasonable classification schemes according to which all possible threats in limited number of groups are distributed. Are provided recommendations about improvement of systems of information security, classification of threats of computer information.

MATERIALS AND METHODS

Research model: To see key problems of architecture steady against attack to computer networks, at first it is expedient to consider the simplified model of communication of the client and the server (Fig. 1).

Corresponding Author: G.A. Shangytbayeva, Kazakh National Technical University Named after K.I. Satpayev, Almaty, Kazakhstan

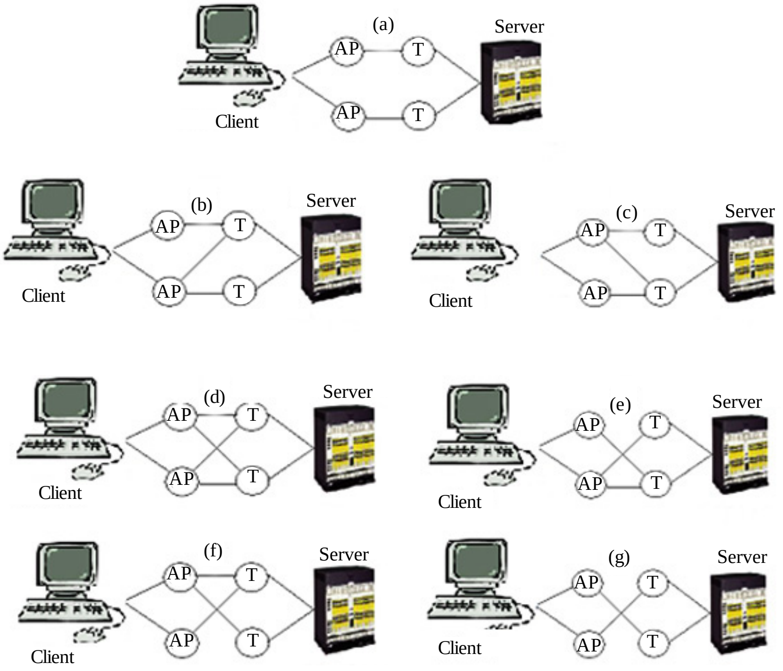

Fig. 1: Model of communication client and server: AP: access point; T: points of destination

Usually, entry points in computer networks is much more, than appointment points for example, 10-1. However in our model, we will be limited to two entry points and two points of appointment. The lines connecting the entry point and the destination point, simulate communication between them in computer networks (Bu *et al*., 2004).

Stability of a network is understood as ability of a network to provide alternative communication at destruction or to attempts to destroy at least one way between the client and the server. In our model in Fig. 1 the design d) is the most stable. The stability index on the computer networks is determined by a Eq. 1:

$$\Pi_c = \frac{n_3}{n_e} \tag{1}$$

Where:

n_3 = No. of communications

n_e = Quantity of components

Under the security is understood as ability of a network to provide as little as possible collisions (collisions) of compromises.

Wang and Chien suggested analytical model for definition of influence of compromises and DoS attacks to knots and preservation of secret and existence on them of a resource, the secrecy of server locations. In their researches considered the stability for work and/or reliability. Also was considered stability as the probability of blocking is described probabilistic model of compromise and blocking DoS-attacks (Hussain *et al*., 2003; Wang and Chien, 2003; Yu *et al*., 2014).

In this research, only attacks of DoS and a compromise were considered. Researchers consider the worst case when probability of DoS of attack it is equal 1 and also is taken into account the case when all knots of access have the same probability of being compromised (John, 1997; Lee, 2000; Li *et al*., 2008).

RESULTS

Data analysis: In order to keep track of DoS/DDoS/DRDoS attack on the network nodes, it is advisable in computer networks consider in the form of structure of the attacked T tree where T is a tree root user V and each node in the network T corresponds to router X. From the point of view of the user of V, the tree of T is under a tree of a much bigger universal tree of U (Fig. 2).

The purpose of tracking of attack to refusal in service consists in definition of routers of a tree of T. The initiator of attacks is modelled by determinant of threat to network knots and uses them for the distributed attack of DDoS. The initiator of attacks knows algorithm of trace and distorts IP headings of packages. In this case, attack of DDoS consists of a stream of many counterfeit packages directed to the user. Thus it is rather difficult to find routers of a tree of attack of T. If the initiator of attack

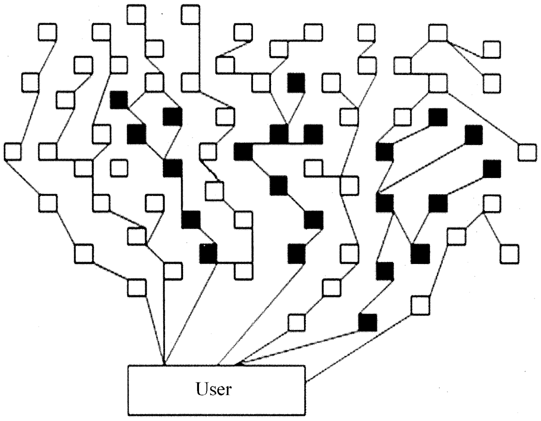

Fig. 2: Universal tree U and the tree T attacks: T an attack tree nodes; U components of the universal tree

knows the router IP address in the network internet, it can attract routers not only from a tree of attack of T. As on the internet there is a large number of routers from the practical point of view, the problem of IP tracking is reduced to the correct identification of internal knots of a tree of U as formation of routing of a tree of attack of T. For the ordinary user of the V computer networks it is important to trace attack to denial in service (Dean *et al*., 2001; Ozcelik and Brooks, 2014).

Therefore, the problem of IP trace is reduced to minimization of volume of an additional traffic on the Internet that is a necessary condition for tracking of attack to Denial in service.

If V' the part of routers on the internet carries out algorithm of tracking in this case, it is possible to determine a set of routers of a tree by section $T\cap U'$. Besides, the user needs to define a router of a tree of attack of T and quickly enough to reconstruct a tree of attack of T.

Filtering and step by step tracing of attack to Denial of Service. In certain cases, the user can use templates of filtering DDoS/DRDoS-packets on a firewall. Also, the user can use trace approach where traces attack DoS while they are in the active status. This approach is based on a towage method and this decision is supported now by vendors of routers. In this approach, the administrator gets access to routers which are located closer to the user and by statistical data of the analysis and the general network topology defines the following router of T attack trees. This method repeats on router inputs until attack is the active. In case of application of this method of tracing, it is necessary to take measures for coordination of actions between network administrators. Similar approach is used scientists of Burch and Cheswick for execution of trace by iterative algorithms of internet users to research influence of attack to the incoming traffic. Owing to iterative nature of such approach limited opportunities of trace in large-scale DDoS/DRDoS attacks (Burch and Cheswick, 2000; Jenshiuh *et al*., 2007).

Tracing of attacks on the basis of ICMP of messages. In the alternative approach based on ICMP messages, each router of X with some probability q (for example, q = 1/20000) for each packet of P, sends additional ICMP packets to the destination. The main idea of such approach is that during attack DDoS/DRDoS enough packets of attacks causes message ICMP from routers in T attack tree so that the user can define T router from this message. However, the main lack of such approach is that is created the additional network traffic in the absence of DDoS/DRDoS of attacks on a network.

Registration approach. Some researchers use registration approach for tracing of IP addresses. In this method, on routers all packets which are processed by them register. Then the full log of all routers which packets faced on the way to the destination is formed. Scientists of Stone (2000) and Baba and Matsuda (2002) in the operations analyze information on registration of packets on routers and offer registration of packets on routers. A lack of such approach is that in case of its use it is necessary to store in addition on routers all information on packets.

DISCUSSION

Having analysed approaches to methods of tracking of attacks for a problem of trace of IP addresses an alternative method is probabilistic markings of packages. This approach is appropriate to apply during the attack or after an attack. In a method, probabilistic markings of packages is not generated the additional network traffic and is stored information on routers or package size increases.

For tracking of the IP address of the initiator of attack to refusal in service it is expedient to use a method probabilistic markings of packages. It is known that in this method each router probabilistically enters the local information on a package transit to final knot (Apiecionek *et al*., 2015). Thus, the user with a high probability can restore a full way of passing of packages, checking marking. In algorithm, probabilistic markings of packages each router incidentally defines probability of marking which rewrites information in the field of marking, destroying markings of the passable routers (Kznetsov *et al*., 2002).

CONCLUSION

Based on results of the carried-out analysis of attacks to system the client server, it is established that such attacks to today's time is the attacks directed on refusal in service of lawful services. Attacks like DoS/DDoS/DRDoS compromise knots in computer networks used their computing resources for realization of algorithm of attack. It is shown that for prevention attack to denial of service it is necessary to develop expanded classification of known information threats and to analyse structures of DoS/DDoS/DRDoS of attacks.

On the basis of the carried analysis of the last publications it is shown that modern methods of tracking of attacks to refusal in service of system the client server are far from perfect and demand further development. For effective tracking of the IP address of a source of attack it is expedient to be based on a method probabilistic packet marking.

Are received that for tracking of a source of attack during attack type of DoS/DDoS/DRDoS or after realization it is expedient to carry out probabilistic markings of packages on routers. It is proved that at realization of attack with application by her initiator of a large number of the compromised knots of a network and counterfeit indicators of marking of packages it is necessary to investigate methods and means of counteraction to attack based on marking of packages with different probability of their marking on various routers.

REFERENCES

Apiecionek, L., J.M. Czerniak and W.T. Dobrosielski, 2015. Quality of services method as a DDoS protection tool. Advances in Intelligent Systems and Computing, 323: 225-234.

Baba, T. and S. Matsuda, 2002. Tracing network attacks to their sources. IEEE Internet Computing, 6 (2): 20-26.

Bhatia, S., D. Schmidt, G. Mohay and A. Tickle, 2014. A framework for generating realistic traffic for Distributed Denial-of-Service attacks and flash events. Computers and Security.

Bhuyan, M.H., D.K. Bhattacharyya and J.K. Kalita, 2015. An empirical evaluation of information metrics for low-rate and high-rate DDoS attack detection. Pattern Recognition Letters, 51: 1-7.

Bu, T., S. Norden and T. Woo, 2004. Trading resiliency for security: Model and algorithms. In Proc. 12th IEEE International Conference on Network Protocols, pp: 218-227.

Burch, H. and B. Cheswick, 2000. Tracing anonymous packets to their approximate source. In Usenix LISA (New Orleans) Conference, pp: 313-322.

Dapeng, G., Y. Shicai and Y. Wenzhi, 2009. Research on composed packet marking for IP Traceback Algorithm. Computer Eng., 35: 115-117.

Dean, D., M. Franklin and A. Stubblefield, 2001. An algebraic approach to IP traceback. In Network and Distributed System Security Symposium (NDSS), pp: 3-12.

Denial-of-Service Attack, 2015. In Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Denial-of-service_attack.

Elliott, J., 2000. Distributed denial of service attack and the zombie ant effect. IT professional, pp: 55-57.

Ferguson, P. and D. Senie, 2000. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing (RFC2827). The internet Society.

Hautio, J. and T. Weckstrom, 1999. Denial of service attacks. http://www.hut.Fi/u/tweckstr/hakkeri/DoS paper.html.

Hussain, A., J. Heidemann and C. Papadopoulos, 2003. A framework for classifying denial of service attacks. Proc. ACM SIGCOMM. Karlsruhe, Germany, pp: 99-110.

Ioannidis, J. and S.M. Bellovin, 2002. Implementing pushback: Router-based defense against DDoS attacks. In Proceedings of Network and Distributed System Security Symposium. The Internet Society.

Jenshiuh, L., L. Zhi-Jian and C. Yeh-Ching, 2007. Dynamic probabilistic packet marking for efficient IP traceback. Proc. The International Journal of Computer and Telecommunications Networking, Elsevier North-Holland Press, pp: 866-882.

John, D.H., 1998. An analysis of security incidents on the internet. Ph.D. thesis, Carnegie Mellon Univerisity.

Kuznetsov, V., A. Simkin and H. Sandstom, 2002. An evaluation of different IP traceback approaches. Proc. The 4th International Conference on Information and Communications Security, pp: 37-48.

Lee, G., 2000. Denial of service attacks rip the internet. Computer, pp: 12-17.

Li, Muh., Li Min and X. Jiang, 2008. DDoS attacks detection model and its application. WSEAS Trans. Computers, 7 (8): 1159-1168.

Ozcelik, I. and R. Brooks, 2014. Deceiving entropy based DoS detection. Computers and Security, 48: 234-245.

Park, K. and H. Lee, 2000. A proactive approach to distributed DoS attack prevention using route-based distributed filtering. Tech. Rep. CSD-00-017, Department of Computer Sciences, Purdue University.

Stoica, L. and H. Zhang, 1999. Providing guaranteed services without per flow management. Proc. the Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, ACM press, pp: 81-94.

Stone, R., 2000. Center Track: An IP overlay network for tracking DoS floods. In Proc. of 9th USENIX security symposium.

Wang, J. and A.A. Chien, 2003. Using overlay networks to resist denial of service attacks. Submitted to ACM conference on computer and communucation security.

Yu, S., Y. Tian, S. Guo and D.O. Wu, 2014. Can we beat DDoS attacks in clouds? IEEE Transactions on Parallel and Distributed Systems.