A SYSTEM FOR VALIDATING AND COMPARING HOST-BASED DDOS DETECTION MECHANISMS

Nguyen Hong Son

Department of Information and Communication Technology, Post and Telecommunication Institute of Technology, Ho Chi Minh City, Viet Nam

ABSTRACT

All DDoS detection mechanisms need to be validated and compared with each other. Researchers are looking for an easy way to do these jobs and to get reliable results. The best way to do that is to build a practical system and run the mechanisms simultaneously. Based on behavior of mechanisms in the same situation, various mechanisms are evaluated and compared with each other. However, to build such a actual system is not an easy job. Currently, no more systems allow running simultaneously mechanisms for evaluating and comparing purpose. This paper proposes a system and method for running simultaneously DDoS detection mechanisms. The system helps researchers not only to validate their mechanisms reliably and quickly but also to compare mechanisms easily.

KEYWORDS

DDoS, Detection, Methodology, Practical Testing System

1. INTRODUCTION

DDoS detection is a difficult task in information security. The challenge has attracted many researchers who spend time looking for a perfect solution to the issue. In fact, hackers launch a DDoS attack by using one of two main methods: The first one is to disrupt service by exploiting vulnerable of protocols or software in servers; The second one is to exhaust bandwidth or resources of servers by filling up with a lot of requests. There are many ways to attack belonged to the methods. Thus, each detection mechanism differs from others and depends on specific attacks.

The goal of any DDoS defense mechanism is to detect attacks as soon as possible and stop them as near as possible to their sources. Several DDoS defense mechanisms were proposed in [1], [2], [3], and [26]. According to [4], DDoS defense mechanisms were categorized into network-based and destination-based. Network-based defense mechanisms often use solutions of identifying and filtering IP traffic [5], [6], [7], [8]. However, it is difficult for such identifying/filtering mechanisms to prevent application-level DDoS attacks. The only way to detect application-level DDoS attacks is to use host-based defense mechanisms. In host-based DDoS defense mechanisms proposed, researchers almost use techniques which reveals syndrome of attack for early detecting.

DOI : 10.5121/ijnsa.2015.7603

Researchers apply creatively various theories, such as calculating entropy in information theory [9], [10], [11], [12], data mining and artificial intelligent [13], [14], [15], [16], GT model in [26]. The performance of DDoS defense mechanisms were overall assessed by [17]. Confident level of a mechanism is based on four quantities: True Positive rate, False Positive rate, True Negative rate and False Negative rate. Authors usually validated their proposed mechanism by private simulation, and using a certain data set for determining the above rates. The main purpose of this paper is to propose a practical testing system together with a method to allow implementing and experimenting host-based DDoS detection mechanisms simultaneously. By using this system, researchers easy test their proposed mechanism and compare it with other mechanism in the same actual condition and in the same time. Experimental results are reliable and gotten quickly. The rest of paper is constructed as following: Section 2 overviews related works from other authors. Analyses and designs of the system are presented in section 3. Section 4 introduces method to use the system for validating and comparing mechanisms. Section 5 shows an example of using the proposed system and method to test simultaneously two mechanisms: detecting DDoS base on output from netstat command and detecting DDoS base on calculating entropy. The paper is finished by several conclusions in section 6.

2. RELATED WORKS

Researchers have spent a lot of time and effort validating their proposed DDoS defense mechanisms. Currently, authors often use a private method to do that with various means. In [19], [20], for instance, authors implement their proposed algorithm as simulation programs and run on desktop with a certain data sets for getting the four quantities. The detection mechanisms for SYN flooding were surveyed in [18]. The advantages and disadvantages of typical detection schemes are also examined and their performance are compared by using private simulation method. In other papers, authors use simulation tools, such as NS-2 or OpNet, which allows generating traffic and observing signatures for evaluating, [10], [11]. In [17], authors also categorized DDoS defense mechanisms, introduced measure parameters of performance, and compared the mechanisms by using the parameters. However, methodologies of the comparison and how to get values of parameters were not mentioned. Up to now, there have been no more researches about system and methodology for testing DDoS defense mechanisms. In [22], the authors have proposed a process that is called T&V process. It is for testing and validating activity models describing network intrusions. In the proposed T&V process, the intrusion model developer is responsible of creating the first set of models for testing and validation. The tester will create required test data to test and validate the intrusion models under test. In [24] and [23], authors analyze current testing methodologies and show how to create testing systems, and how to use them in academic and industrial evaluations.

3. PRACTICAL SIMULTANEOUS TESTING SYSTEM

The system is designed to include the same components as practical scenarios: server running protected services, DDoS attack detection system, DDoS attacking sources and networking environment. The following features must be provided by the system: to allow deploying various DDoS attacking scenarios; to allow running more detection mechanisms simultaneously and to do it easily and quickly.

Although every DDoS detection method is different, it is proper for almost DDoS detection mechanisms to be installed on the protected service systems. The detection mechanisms were usually implemented as hidden programs that run and send reports to monitoring system regularly. Normally, a special subroutine is also created in order to process reports and to make decision of next actions. The next action may be a request sent to firewalls for dropping the related sessions. Since the proposed system is just for validating and comparing the DDoS detection capability of mechanisms, it does not include reactive actions.

To build a practical testing system from scratch is a heavy job that takes a lot of time and effort of researchers. In order to relieve the job, this paper applies advantages of Nagios open source. The functional origin of Nagios is to allow administrators monitoring performance of computer networks. Basically, Nagios was designed in two main components: Nagios server and Nagios agent. The first is always placed on monitored systems. It takes the role of monitoring station where administrators can observe entire network. The second is responsible for collecting, processing and sending related data to the monitoring station. Nagios server compares the incoming values with the configured reference values to make conclusions about performance of various parts of monitored network.

In Nagios a common platform, called Nagios core, was built for any monitoring operation. In order to monitor a certain factor, developers just make a proper plugin and add it to the platform. This paper exploited the advantage of Nagios for building the practical simultaneous testing system as mentioned above. Truly, it is not difficult to see that we can use Nagios to construct a DDoS detection system. The monitored performance factors are now replaced by DDoS attacking syndromes. The DDoS detection mechanisms would be implemented in plugins and be added to the Nagios platform. By the way, researchers can test their proposals quickly.

Another feature of Nagios is to allow simultaneously running more plugins. Thereby, we easy compare more DDoS detection mechanisms in the same attacking scenario. Data from each mechanism are logged into independent storages for comparing and evaluating latter.

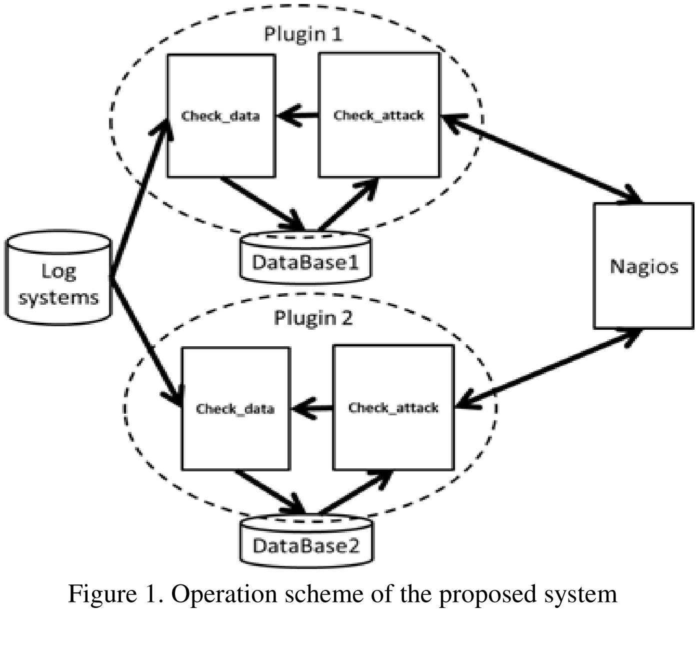

Figure 1. Operation scheme of the proposed system

In common case of testing and comparing two DDoS detection mechanisms, it should be implemented in Plugin 1 and Plugin 2. The operation scheme of the system is described in figure 1. Although every detection mechanism is different, all plugins contain two main parts: Check_data and Check_attack. Check_data gets state information of protected system from log systems and processes it. Database stores necessary information written by Check_data and is queried by Check_attack. Check-attack carries out basic calculations of detection algorithms based on data from Database. Results of the calculations are used to make a decision on trigging an alarm in Nagios server.

The practical simultaneous testing system includes protected web server, Nagios server and many attack computers. All computers are connected together by an Ethernet switch. The system should use NRPE add-on to manage plugins in web server.

4. METHODOLOGY OF USING THE PROPOSED TESTING SYSTEM

The attacking sources of the proposed testing system are represented by a Botnet simulator which could be controlled by researchers. In order to test and validate a certain DDoS detection mechanism, researchers should properly create attacking samples which includes on/off attack-interleaved periods. Length of the periods would depend on specific attacking samples. In this paper, such attacking sample is referred to as Event Data Sample (EDS). The method of using the proposed system is briefed in figure 2. Researchers should control the Botnet for matching its action with a known specific EDS. Detection results of mechanisms are simultaneously logged, stored separately and used as one of two inputs of statistic task. The remaining input is EDS of the testing case. Thereby, it is easy to calculate four quantities: True Positive rate (TP), False Positive rate (FP), True Negative rate (TN) and False Negative rate (FN). The quantities help researchers not only to evaluate a specific mechanism but also to compare mechanisms with each other.

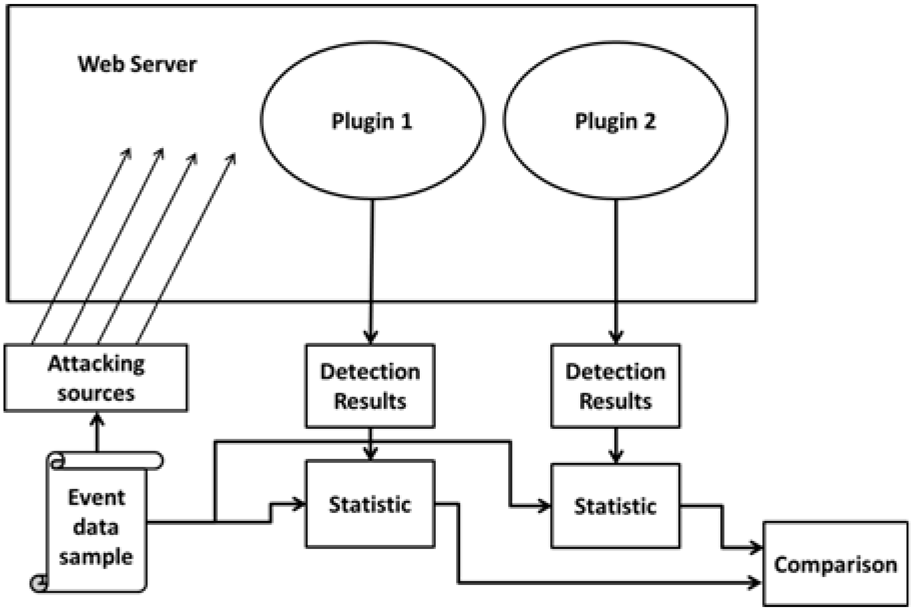

Figure 2. Method of using the proposed system

5. AN EXAMPLE OF APPLYING THE PROPOSED SYSTEM

This section illustrates an example of testing and comparing two DDoS detection mechanisms such as below:

(1) Netstat command-based mechanism: It bases on number of connections listed by netstat command. By using the command, it can count the number of half open connections in a system at that instant. If number of connections exceeds a preset threshold during of netstat command cycle, the mechanism warns administrator of a DDoS attack.

(2) Entropy-based mechanism: It bases on calculating entropy of stochastic requests in a period of time, proposed in [21]. According to the algorithm, if deviation of two values of entropy from two consecutive calculations exceeds a preset threshold, the system was under a DDoS attack.

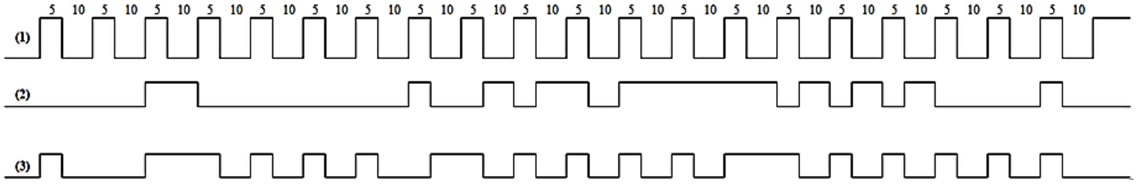

Figure 3. The testing case 1_(1) EDS1, (2) Behavior of netstat command-based mechanism (3) Behavior of entropy-based mechanism.

As mentioned above, two plugins were developed, named check_byNetstat and check_byEntropy, and added into Nagios agent in web server. Several EDSs were also specified for testing. The first EDS, called EDS 1, includes chains of 5 seconds of attack interleaved by 10 seconds of non attack, as described in figure 3. By collecting detection results from the proposed testing system, statistics of four quantities TP, FP, TN and FN are illustrated in figure 4.

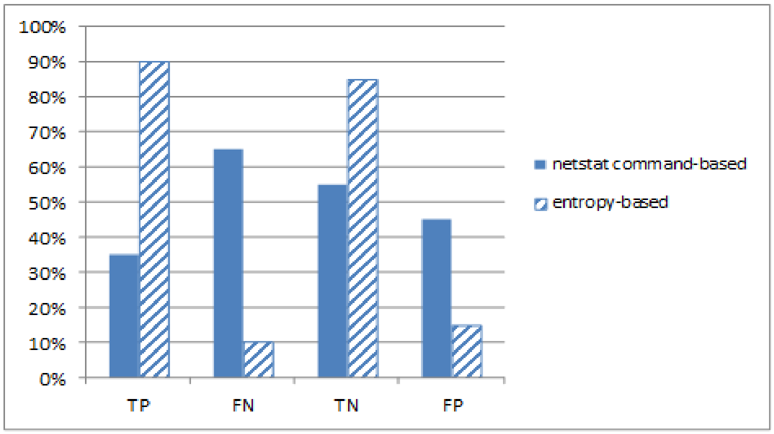

Figure 4. Results of testing for the case of using EDS1.

In the second testing case, EDS 2 includes chains of 10 seconds of attack interleaved by 10 seconds of non attack, as described in figure 5. It extends periods of attack longer than in case of EDS 1.

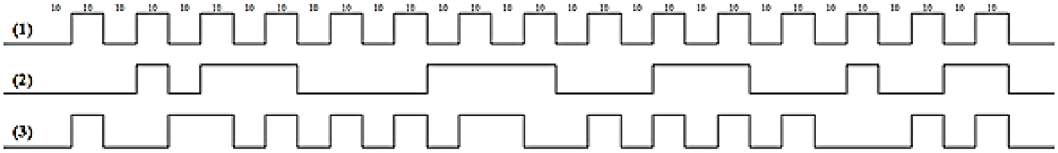

Figure 5. The testing case 2_(1) EDS2, (2) Behavior of netstat command-based mechanism (3) Behavior of entropy-based mechanism.

The statistics of four quantities TP, FP, TN and FN in the case of using EDS 2 are illustrated in figure 6.

Figure 4 shows that the TP and TN of the netstat command-based mechanism are very low, TP rate of 35% and TN rate of 55%. Conversely, the entropy-based mechanism reaches high rate of TP and TN with 90% and 85%, respectively. Rates of error indication of entropy-based mechanism are also smaller than the rates of netstat command-based mechanism. In the case of using EDS2, period of attacking time is longer than the period in EDS1. In this case, the rates of correct indication of netstat command-based mechanism improved in value with TP rate of 60% and TN rate of 67%, as shown in figure 6. However, rates of FP and FN of netstat command-based mechanism were still greater than those of entropy-based mechanism. The entropy-based mechanism remains the correct indications of TP and TN in high rate. Thus, entropy-based mechanism is better than netstat command-based mechanism.

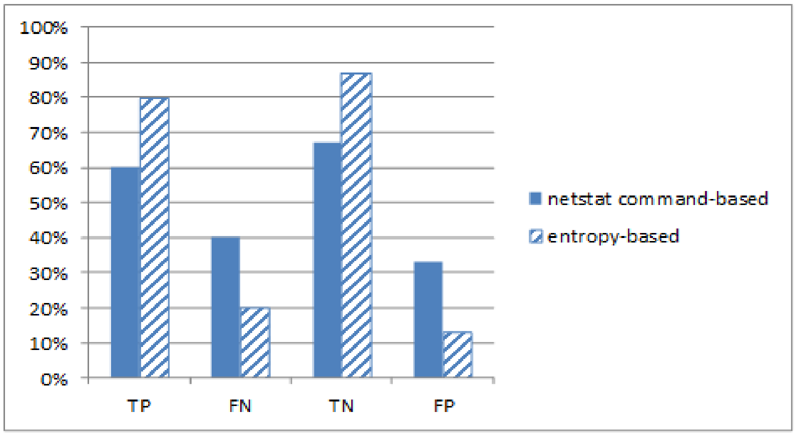

Figure 6. Results of testing for the case of using EDS2.

Above experimental results show that the system has different behaviors with various mechanisms. Also, the behavior of a detection mechanism varies depending on specific EDSs. This said that the system also help to test detection ability of a mechanism with various attack workloads.

6. CONCLUSIONS

A system and methodology for validating and comparing host-based DDoS detection mechanisms were presented. This is a practical system with real attack sources. The proposed system and methodology is a useful tool not only for validating separately a certain DDoS detection mechanism but also comparing more mechanisms simultaneously. It costs researchers a little of time and effort. All of things researchers having done are to implement algorithm of mechanism as a proper plugin and place it into Nagios agent in the protected server. The results of testing on the system show that entropy-based mechanism is better than netstat command-based mechanism, and completely matching with results of prior simulations. The system always gives reliable results because this is a practical testing system.

REFERENCES

[1] J.Mirkovic, P. Reiher; "A taxonomy of DDoS attack and DDoS defense mechanisms"; ACM SIGCOMM Computer Communications Review, vol. 34, no. 2, pp. 39-53, April 2004.

[2] T. Peng, C. Leckie, K. Ramamohanarao; "Survey of network-based defense mechanisms countering the DoS and DDoS problems"; ACM Comput. Surv. 39, 1, Article 3, April 2007.

[3] RioRey; "Taxonomy of DDoS Attacks"; RioRey Taxonomy Rev 2.3 2012, 2012. [online] http://www.riorey.com/x-resources/2012/RioRey Taxonomy DDoS Attacks 2012.pdf.

[4] Saman Taghavi Zargar, James Joshi,David Tipper; "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks"; Communications Surveys & Tutorials, IEEE ,Volume 15, Issue 4, 2013.

[5] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao; "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks"; IEEE Trans. On Dependable and Secure Computing, vol. 3, no. 2, pp. 141-155, 2006.

[6] S. Changhua, Jindou, F., Lei, S., & Bin, L.; "A Novel Router-based Scheme to Mitigate SYN Flooding DDoS Attacks"; in IEEE INFOCOM (Poster), Anchorage, Alaska, USA, 2007.

[7] M. Abliz; "Internet Denial of Service Attacks and Defense Mechanisms"; University of Pittsburgh, Department of Computer Science, Technical Report. TR-11-178, March 2011.

[8] Cheng, J., Yin, J., Liu, Y., Cai, Z., Wu, C.; "DDoS attack detection using IP address feature interaction"; Proceedings of the 1st International Conference on Intelligent Networking and Collaborative Systems, Barcelona, Spain, pp. 113–118. IEEE CS, 4-6 November 2009.

[9] Krishan Kumar, Joshil, Kuldip Singh; "A Distributed Approach using Entropy to Detect DDOS Attacks in ISP Domain"; International conference on signal processing, communications and networking 2007, Chennai: IEEExplore Digital Library Press , pp. 331 – 337, 22-24 Feb. 2007.

[10] Shui Yu, Wanlei Zhou, Robin DOSs; "Information Theory Based Detection Against Network Behavior Mimicking DDOS Attacks"; Communications Letters, IEEE Vol. 12(4), pp. 318 -321, April 2008.

[11] Shui Yu, Wanlei Zhou; "Entropy-Based Collaborative Detection of DDOS Attacks on Community Networks"; Sixth Annual IEEE International Conference on Pervasive Computing and Communications, Hong Kong IEEE CS Press, pp.566 – 571, 17-21 March 2008.

[12] Giseop No, Ilkyeun Ra; "Adaptive DDoS Detector Design Using Fast Entropy Computation Method"; The Fifth IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011.

[13] Hwang, K., Dave, P., Tanachaiwiwat, S. NetShield; "Protocol anomaly detection with datamining against DDoS attacks"; Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection, Pittsburgh, PA, pp. 8–10. Springerverlag. , 8-10 September, 2003.

[14] R. Jalili, F. ImaniMehr; "Detection of Distributed Denial of Service Attacks Using Statistical Pre-Prossesor and Unsupervised Neural Network"; ISPEC, Springer-Verlag Berlin Heidelberg, pp.192-203, 2005.

[15] Y. C. Wu, H. R. Tseng, W. Yang, R. H. Jan; "DDoS detection and traceback with decision tree and grey relational analysis"; International Journal of Ad Hoc Ubiquitous Computing., vol. 7, no. 2, pp. 121-136, 2011.

[16] Wang, J., Phan, R. C. W., Whitley, J. N., Parish, D. J.; "Augmented attack tree modeling of distributed denial of services and tree based attack detection method"; Proceedings of the 10th IEEE

International Conference on Computer and Information Technology, Bradford, UK, 29 June-1 July, pp. 1009–1014. IEEE CS, 2010.

[17] Saman Taghavi Zargar, James Joshi, David Tipper; "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks"; IEEE Communications Surveys & Tutorials, Feb. 2013.

[18] Mehdi Ebady Manna, Angela Amphawan; "Review Of Syn-Flooding Attack Detection Mechanism"; International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[19] Giseop No, Ilkyeun Ra; "Adaptive DDoS Detector Design Using Fast Entropy Computation Method"; The Fifth IEEE International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, 2011.

[20] Ragendhu.T.R,. S.Subashini.; "An Efficient DDoS Attack Detection Technique using Trace Back Approach"; International Journal On Engineering Technology and Sciences – IJETS™ ISSN (P): 2349-3968, ISSN (O): 2349-3976 Volume 2 - Issue 5, May 2015.

[21] S. Renuka Devi, P. Yogesh; "Detection Of Application Layer DDoS Attacks Using Information Theory Based Metrics"; CCSEA, SEA, CLOUD, DKMP, CS & IT 05, pp. 217–223, DOI : 10.5121/csit.2012.2223, 2012.

[22] Marko Maattaa,Tomi Raty; "Testing and Validating Activity Models for Network Intrusion Detection"; International Conference on Computer & Information Science (ICCIS), Kuala Lumpur, Malaysia, 2012

[23] Stefano Zanero; "Flaws and frauds in the evaluation of IDS/IPS technologies"; 19th Annual Conference of the Forum for Incident Response and Security Teams, 2007

[24] Renaud Bidou; "How to test an IPS"; [online]
http://www.iv2-technologies.com/HowToTestAnIPS.pdf

[25] Majid Alshammari, Christian Bach; "Defense Mechanisms for Computer-Based Information Systems"; International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013.

[26] G Dayanandam, T V Rao, S Pavan Kumar Reddy, Ravinuthala Sruthi; "Password Based Scheme and Group Testing for Defending DDOS Attacks"; International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.3, May 2013.

AUTHORS

Son Nguyen Hong, received his B.Sc. in Computer Engineering from Ho Chi Minh City University of Technology, his M.Sc. and PhD in Communication Engineering from the Post and Telecommunication Institute of Technology Hanoi. His current research interests include communication engineering, network security, computer engineering and cloud computing.