ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Detecting DDOS Attacks by Circular Protection Network

Yamini B[1], Chithra Devi R[2]

M-tech(IT) Final Year, Information Technology, Anna University, Dr.Sivanthi Aditanar College of Engineering, Tuticorin-628215, Tamilnadu, India[1]

Asst. Professor, Information Technology, Anna University, Dr.Sivanthi Aditanar College of Engineering, Tuticorin-628215, Tamilnadu, India[2]

ABSTRACT— One of the major threat in most of the networks is the distributed denial of service and its mitigation is another important concern, this paper addresses this problem by using the firecol whose core is composed of a ring of Intrusion prevention systems(IPS) defends by exchanging only a selected traffic. In this paper, we address the problem of DDoS attacks and present the theoretical foundation, architecture, and algorithms of the circular protection network. The core is composed of intrusion prevention systems (IPSs) located at the Internet service providers (ISPs) level. The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information

KEYWORDS-: Mitigation, flooding, distributed denial-of-service (DDoS), Detection.

I. INTRODUCTION

The distributed denial of service (DDoS) attack is a serious threat to the security of Internet. Distributed DOS (DDoS) is a large-scale, coordinated attack on a victim system or network resource. Launched indirectly through many compromised computers on the Internet DDoS attack countermeasures can be categorized into four classes: prevention, detection, mitigation, and traceback, of which detecting and mitigating these kind of attack is a real challenge. Defending against DDoS attacks is challenging for two reasons. First, the number of attackers1 involved in a DDoS attack is very large. Even if the volume of traffic sent by a single attacker might be small, the volume of aggregated traffic arriving at the victim host is overwhelming. Second, attackers usually spoof their IP addresses, which make it very difficult to trace the attack traffic back to its sources. Unfortunately, detecting a botnet is also hard, and efficient solutions may require to participate actively to the botnet itself [2], which raises important ethical issues, or to first detect botnet-related malicious activities (attacks, infections, etc.), which may delay the mitigation. To avoid these issues, this paper focuses on the detection of DDoS attacks. Although non distributed denial-of-service attacks usually exploit vulnerability by sending few carefully forged packets to disrupt a service, DDoS attacks are mainly used for flooding a particular victim with massive traffic as highlighted in [1]. In fact, the popularity of these attacks is due to their high effectiveness against any kind of service since there is no need to identify and exploit any particular service-specific flaw in the victim. Hence, this paper focuses exclusively on flooding DDoS attacks. A single intrusion Prevention System is capable of detecting such attacks only if it is close to the victim hence to overcome this problem a circular network that comprises of multiple intrusion prevention system is used that forms a collaborative protection network around the node to be protected detecting the DDoS attacks, this circular protection network uses some of the metrics like maximum bandwidth it allows, entropy rate, score lists it maintains based on the previous observations to detect the attack. In addition to detecting the DDos attacks it also detects attacks caused by Botnets. This paper proceeds as follows. Section II describes the related work and the global operation of the circular protection network. This paper proceeds as follows. Section III describes the architecture and the global operation of system. The different leveraged metrics and components of the system are presented in Section III. Section IV presents explains the conclusion and future works.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. EXISTING WORK

Arbor Networks, Inc., in cooperation with the Internet security operations[17] community, has completed this fourth edition of an ongoing series of annual operational security surveys. This survey, covering a 12-month period from August 2007 through July 2008, is designed to provide data useful to network operators so that they can make informed decisions about their use of network security technology to protect their mission-critical infrastructures. It is also meant to serve as a general resource for the Internet operations and engineering community, recording information on trends and employment of various infrastructure security techniques.

Operational network securities issues—the day-to-day aspects of security in commercial networks—are the primary focus of survey respondents. As such, the results provided in this survey more accurately represent real-world concerns than theoretical and emerging attack vectors addressed and speculated about elsewhere.

The Internet[15] was originally designed for openness and scalability. The infrastructure is certainly working as envisioned by that yardstick. However, the price of this success has been poor security. For example, the Internet Protocol (IP) was designed to support ease of attachment of hosts to networks, and provides little support for verifying the contents of IP packet header fields [Clark 1988]. This makes it possible to fake the source address of packets, and hence difficult to identify the source of traffic. Moreover, there is no inherent support in the IP layer to check whether a source is authorized to access a service. Packets are delivered to their destination, and the server at the destination must decide whether to accept and service these packets. While defenses such as firewalls can be added to protect servers, a key challenge for defense is how to discriminate legitimate requests for service from malicious access attempts. If it is easier for sources to generate service requests than it is for a server to check the validity of those requests, then it is difficult to protect the server from malicious requests that waste the resources of the server. This creates the opportunity for a class of attack known as a denial of service attack.

Global Internet threats are undergoing a profound transformation from attacks designed solely to disable infrastructure to those that also target people and organizations. Behind these new attacks is a large pool of compromised hosts sitting in homes, schools, businesses, and governments around the world. These systems are infected with a bot that communicates with a bot controller and other bots to form what is commonly referred to as a zombie army or botnet. Botnets are a very real and quickly evolving problem that is still not well understood or studied. In this paper we outline the origins and structure of bots and botnets and use data from the operator community, the Internet Motion Sensor project, and a honeypot experiment to illustrate the botnet problem today. the effectiveness of detecting botnets is studied by directly monitoring IRC communication or other command and control activity and show a more comprehensive approach is required.It [14] concludes by describing a system to detect botnets that utilize advanced command and control systems by correlating secondary detection data from multiple sources.

This frightening new class of attacks directly impacts the day-to-day lives of millions of people and endangers businesses around the world. For example, new attacks steal personal information that can be used to damage reputations or lead to significant financial losses. Current mitigation techniques focus on the symptoms of the problem, filtering the spam, hardening web browsers, or building applications that warn against phishing tricks. While tools such as these are important, it is also critical to disrupt and dismantle the infrastructure used to perpetrate the attacks. At the center of these threats is a large pool of compromised hosts sitting in homes, schools, businesses, and governments around the world. These systems are infected with a bot that communicates with a bot controller and other bots to form what is commonly referred to as a zombie army or botnet. A bot can be differentiated from other threats by a communication channel to a controller.

Botnets, i.e., networks of compromised machines under a common control infrastructure, are commonly controlled by an attacker with the help of a central server: all compromised machines connect to the central server and wait for commands. However, the first botnets that use peer-to-peer (P2P) networks for remote control of the compromised machines appeared in the wild recently. In this paper, a methodology to analyze and mitigate P2P botnets. In a case study,this system[11] examine in detail the Storm Worm botnet, the most wide-spread P2P botnet currently propagating in the wild. The system is able to infiltrate and analyze in- depth the botnet, which allows us to estimate the total number of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

compromised machines. Furthermore, two different ways to disrupt the communication channel between controller and compromised machines in order to mitigate the botnet and evaluate the effectiveness of these mechanisms.

A flooding-based distributed denial of service (DDoS) attack sends a large amount of unwanted traffic to a victim machine. Existing network-level congestion control mechanisms are inadequate in preventing service quality from deteriorating because of these attacks.This paper[13] propose a distributed framework to defend against DDoS attacks. It has three major components: detection, traceback, and traffic control.The traffic control component in detail in this paper. A distance-based rate limit mechanism is proposed to allow the traffic control component at the victim end request the defense systems at the source end to set up rate limits on the edge routers of the attack source ends. This rate limit mechanism efficiently reduces attack traffic from being forwarded to the victim. This evaluates the DDoS defense framework using the NS2 platform. The results demonstrate that the framework can effectively control attack traffic to sustain quality of service for legitimate traffic compared to the pushback technique.

Traffic differentiations are known to be found at the broadband ISPs and wireless carriers. The differentiations is essential for customers to develop edge of the Internet in ability to detect traffic effective strategies for improving their application performance.This system[9], called NetPolice, that enables detection of content- and routing-based differentiations in backbone ISPs. NetPolice is easy to deploy since it only relies on loss measurement launched from end hosts. The key challenges in building NetPoliceinclude selecting an appropriate set of probing destinations and ensuring the robustness of detection results to measurement noise. NetPolice to study 18 large ISPs spanning 3 major continents over 10 weeks in 2008. This work provides concrete evidence of traffic differentiations based on application types and neighbour ASes. identifies 4 ISPs that exhibit large degree of differentiation on 4 applications and 10 ISPs that perform previous-AS hop based differentiation, resulting in up to 5% actual loss rate differences. The significance of differences increases with network load. Some ISPs simply differentiate traffic based on port numbers irrespective of packet payload and the differentiation policies may only be partially deployed within their networks.

It also find strong correlation between performance differences and Type-of-Service value differences in the traffic. In this paper, the problem of detecting traffic differentiation in backbone ISPs. Different types of traffic may experience different performance within the same ISP network due to various reasons. An ISP may "passively" throttle the traffic from a neighbor (*e.g.*, a peer) by carrying the traffic over a low-capacity link, since it may not have the economic incentive to provision or upgrade the link . It may also "actively" prevent the traffic of an application (*e.g.*, BitTorrent) from disrupting other traffic via weighted fair queuing when the network is congested. Regardless of the actual reasons behind the performance differences, it is important for customers to be able to reason about the behaviors of their ISPs. The ability to detect traffic differentiation enables customers to develop appropriate strategies for improving their application performance.

For instance, large content providers strive to ensure their Internet applications outperform those offered by their competitors. If a content provider knows the average loss rate of its traffic traversing a particular ISP is twice that of its competitor, it may want to negotiate better service level agreements (SLA) with that ISP. Small customers will also benefit from such differentiation information. For instance, they may change port numbers or encrypt packets to circumvent content-based differentiation employed by their ISP. Most ISPs do not reveal the details of their network policies and configurations. Realizing this problem, this paper aims to develop an endhost based system that can detect traffic differentiation.

Recent spates of cyber-attacks and frequent emergenceof applications affecting Internet traffic dynamics have made it imperative to develop effective techniques that can extract, and make sense of, significant communication patterns from Internet traffic data for use in network operations and security management. This paper[3], present a general methodology for building comprehensive behavior profiles of Internet backbone traffic in terms of communication patterns of end- hosts and services. Relying on data mining and entropy-based techniques,the methodology consists of significant cluster extraction, automatic behavior classification and structural modeling for in-depth interpretive analysed and validation is done using data sets from the core of the Internet.

The NetShield security system was developed at USC to defend against network worms and flood attacks. The system[5] prevents malicious hackers from orchestrating DDoS flooding attacks on any IP-based public network. This

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

article presents new packet filtering and anomaly detection techniques developed with the NetShield system. All packets from each IP source are counted and timed during their life cycles. Special IP counters and timers are used to support the filtering process. Attack profile datamining is used to support protocol anomaly detection of flood attacks. This work uses an alarm-matrix model to assess the effectiveness of the attack/alarm verification and packet filtering processes.

III.CIRCULAR PROTECTION NETWORK

To avoid these issues, this paper focuses on the detection of DDoS attacks and not their underlying vectors. Although nondistributed denial-of-service attacks usually exploit vulnerability by sending few carefully forged packets to disrupt a service, DDoS attacks are mainly used for flooding a particular victim with massive traffic as highlighted in. In fact, the popularity of these attacks is due to their high effectiveness against any kind of service since there is no need to identify and exploit any particular service-specific flaw in the victim.

Hence, this paper focuses exclusively on flooding DDoS attacks. A single intrusion prevention system (IPS) or intrusion detection system (IDS) can hardly detect such DDoS attacks, unless they are located very close to the victim. However, even in that latter case, the IDS/IPS may crash because it needs to deal with an overwhelming volume of packets (some flooding attacks reach 10–100 Gb/s). In addition, allowing such huge traffic to transit through the Internet and only detect/block it at the host IDS/IPS may severely strain Internet resources.

Module Description:

- Topology Creation
- IPS Service
- Detect DDoS

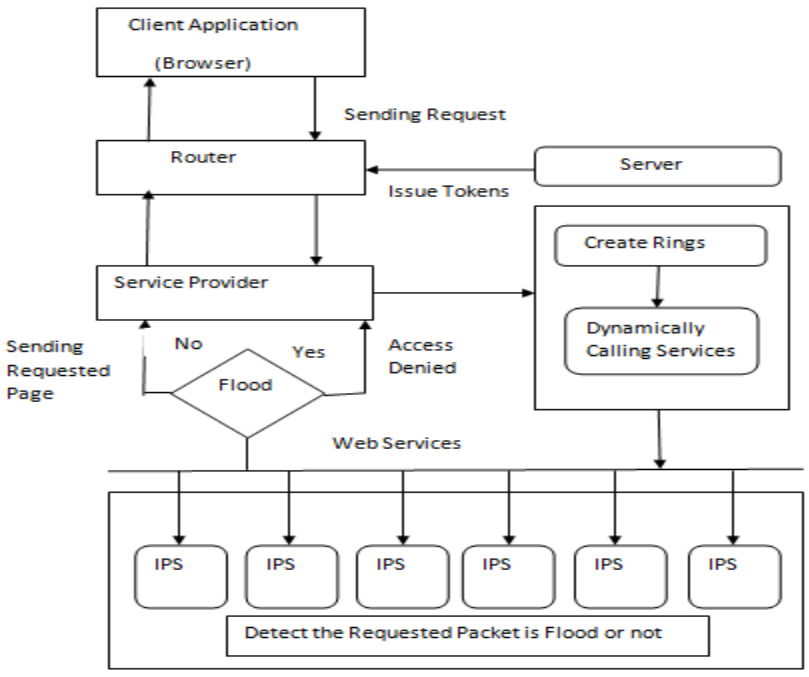

Figure 4.1 ARCHITECTURE

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Topology Creation:

The ring level of a FireCol-enabled router (IPS) is regularly updated based on the degree of stability of IP routing. This is done using a two phase process. First, the router sends a message RMsg to the protected customer containing a counter initialized to 0. The counter is incremented each time it passes through a FireCol-enabled router. The customer (or first-level FireCol router) then replies to the initiating router with the value of its ring level. This procedure is optimized through aggregation when several routers are requesting a ring-level update.

IPS Service:

The FireCol system maintains virtual rings or shields of protection around registered customers. A ring is composed of a set of IPSs that are at the same distance (number of hops) from the customer. Each FireCol IPS instance analyzes aggregated traffic within a configurable detection window. The metrics manager computes the frequencies and the entropies of each rule. A rule describes a specific traffic instance to monitor and is essentially a traffic filter, which can be based on IP addresses or ports. Finally, the collaboration manager is only invoked for the few selected candidate rules based on resource-friendly metrics.

Detect DDoS:

We claim that detecting a flooding attack can be confirmed only if the traffic it generates is higher than the customer's capacity. Hence, the IPS where the alert is triggered has to initiate a ring level communication to calculate the average traffic throughput for subsequent comparison with the subscriber's capacity. Finally if the Packet Rate is larger than the threshold value the packet is addressed by Flooding Packets, so the user denied. Otherwise the corresponding response is send by the IPS.

IV. CONCLUSION

Thus the Circular Protection Network system could effectively detect and mitigate DDoS attacks by means of detection and mitigation algorithms based on the history based filtering methods and other filtering parameters. The future work includes the filtering by increasing the ring numbers and the parameters considered for filtering.

REFERENCE

[1] P. Barford and D. Plonka. Characteristics of network traffic anomalies. In Proceedings of the 1st ACM SIGCOMM Internet Measurement Workshop, pages 69.74, New York, Nov. 1.2 2001. ACM Press.
[2] CERT/CC. CA-2003-20 W32/blaster worm. http:// www.cert.org/advisories/CA-2003-20.html.
[3] K. Xu, Z.-L. Zhang, and S. Bhattacharyya, "Internet traffic behavior profiling for network security monitoring," IEEE/ACM Trans. Netw.,vol. 16, no. 6, pp. 1241–1252, Dec. 2008.
[4] A. Akella, S. Seshan, and A. Shaikh. An empirical evaluation of wide-area internet bottlenecks. In IMC, 2003.
[5] K. Hwang, S. Tanachaiwiwat, and P. Dave, "Proactive intrusion defense against DDoS flooding attacks," in Proc. Int. Conf. Adv. Internet, Process., Syst., Interdiscipl. *Res.*, 2003 [Online]. Available: http://gridsec.usc.edu/hwang/papers/IEEES&P414Final.pdf
[6] CISCO. Remote triggered black hole _ltering. ftp:// ftp-eng.cisco.com/cons/isp/security/.
[7] CISCO. Unicast reverse path forwarding enhancements for the ISP-ISP edge. ftp://ftp-eng.cisco.com/ cons/isp/security/URPF-ISP.pdf.
[8] CISCO. Using CAR during DoS attacks. http: //www.cisco.com/warp/public/63/car_rate_limit_icmp.html.
[9] Y. Zhang, Z. M. Mao, and M. Zhang, "Detecting traffic differentiation in backbone ISPs with NetPolice," in Proc. ACM SIGCOMM Conf. Internet Meas., 2009, pp. 103–115.
[11]T. Holz, M. Steiner, F. Dahl, E. Biersack, and F. Freiling, "Measurements and mitigation of peer-to-peer-based botnets: A case study on storm worm," in Proc. USENIX LEET, 2008, Article no. 9.
[12] J. Ioannidis and S. M. Bellovin. Implementing pushback: Router-based defense against DDoS attacks. In Proceedings of NDSS, San Diego, February 2002. The Internet Society.
[13]Y. You, M. Zulkernine, and A. Haque, "A distributed defense framework for flooding-based DDoS attacks," in Proc. 3rd ARES,Mar. 2008, pp. 245–252.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

[14] E. Cooke, F. Jahanian, and D. Mcpherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in Proc. SRUTI, Jun. 2005, pp. 39–44.
[15]T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network- based defense mechanisms countering the DoS and DDoS problems," Comput. Surv., vol. 39, Apr. 2007, Article 3.
[16] S. Savage, D.Wetherall, A. Karlin, and T. Anderson. Practical network support for IP traceback. In Proceedings of the 2000 ACM SIGCOMM Conference.
[17] A. Networks, Arbor, Lexington,MA, "Worldwide ISP security report",Tech. Rep., 2010.