International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 7; Issue 4(K); April 2018; Page No. 12022-12024
DOI: http://dx.doi.org/10.24327/ijcar.2018.12024.2104

Review Article

A REVIEW ON DISTRIBUTED DENIAL-OF-SERVICE FLOODING ATTACKS WITH DYNAMIC PATH IDENTIFIERS

Vijay N* and Munivara Prasad K

Department of Computer Science and Engineering, Sree Vidyanikethan Engineering College, Tirupati, Andhra Pradesh, India

A R T I C L E I N F O

Article History:

Received 12th January, 2018
Received in revised form 24th February, 2018 Accepted 10th March, 2018
Published online 28th April, 2018

Key words:

Inter-domain routing, security, distributed denail-of- service (DDoS) attacks, path identifiers.

A B S T R A C T

In recent years, there are increasing interests in using path identifiers (*PIDs*) as inter-domain routing objects. However, the *PIDs* used in existing approaches are static, which makes it easy for attackers to launch distributed denial-of-service (DDoS) flooding attacks. To address this issue, we present the design, implementation, and evaluation of D-PID, a framework that uses *PIDs* negotiated between neighboring domains as inter-domain routing objects. In DPID, the *PID* of an inter-domain path connecting two domains is kept secret and changes dynamically. We build a 42-node prototype comprised by six domains to verify D-PID's feasibility and conduct extensive simulations to evaluate its effectiveness and cost.

INTRODUCTION

Distributed denial-of-service (DDoS) flooding attacks are very harmful to the Internet. In a DDoS attack, the attacker uses widely distributed zombies to send a large amount of traffic to the target system, thus preventing legitimate users from accessing to network resources [1]. For example, a DDoS attack against BBC sites in Jan. 2016 reached 602 gigabits per second and "took them down for at least three hours" [3]. This attack peaked at nearly one terabit per second (Tbps) and even forced Akamai to stop offering DDoS protection to OVH [2]. Therefore, many approaches [4] have been proposed in order to prevent DDoS flooding attacks, including network ingress filtering, IP traceback, capability-based designs, and shut-up messages.

Francois, I. Aib, and R. Boutaba

Distributed denial-of-service (DDoS) attacks remain a major security problem and the mitigation of which is very hard. In computing, a denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a machine or network resource unavailable to its intended users. The early discovery of these attacks, although challenging, is necessary to (IPSs) located at the Internet service providers (ISPs) level.

Corresponding author:* **Vijay N
Department of Computer Science and Engineering, SreeVidyanikethan Engineering College, Tirupati, Andhra Pradesh, India

The IPSs form virtual protection rings around the hosts to defend and collaborate by exchanging selected traffic information. The evaluation of this work using extensive simulations and a real dataset is presented, showing its effectiveness and low overhead, as well as its support for incremental deployment in real networks.

Distributed denial-of-service (DDoS) attacks still constitute a major concern [1] even though many works have tried to address this issue in the past. As they evolved from relatively humble megabit beginnings in 2000, the largest DDoS attacks have now grown a hundredfold to break the 100 Gb/s, for which the majority of ISPs today lack an appropriate infrastructure to mitigate them [1].Most recent works aim at countering DDoS attacks by fighting the underlying vector, which is usually the use of botnets [3]. A botnet is a large network of compromised machines (bots) controlled by one entity (the master). The master can launch synchronized attacks, such as DDoS, by sending orders to the bots via a Command & Control channel. Unfortunately, detecting a botnet is also hard, and efficient solutions may require to participate actively to the botnet itself [4], which raises important ethical issues, or to first detect botnet related malicious activities (attacks, infections, etc.), which may delay the mitigation.

Here presents a new collaborative system that detects flooding DDoS attacks as far as possible from the victim host and as close as possible to the attack source(s) at the Internet service provider (ISP) level. It relies on a distributed architecture

composed of multiple IPSs forming overlay networks of protection rings around subscribed customers.

S. T. Zargar, J. Joshi, D. Tipper

Detecting Distributed Denial of Service (DDoS) flooding attacks as soon as possible before they affect the victims, identifying the sources of the attacks, and finally stopping them by blocking or rate limiting the attack traffic is the ultimate goal of current defense mechanisms. The success in detecting and responding to DDoS flooding attacks is highly dependent on the data monitored by the employed traffic monitoring mechanisms, the degree of collaboration among various domains, and the response approach employed in various domains. In this poster, we present Biodefense, which is a distributed collaborative defense mechanism whose main goal is to detect and respond to high volume DDoS flooding attacks closer to the sources of the attacks.

According to CERT [1], the rapid growth of the Internet services has increased the number of possible attacks against these services. DDoS flooding attacks often originate from a group of organized and widely scattered zombies that simultaneously and continuously either (i) disrupt a legitimate user's connectivity by exhausting bandwidth, router processing capacity or network resources; or (ii) disrupt a legitimate user's services by exhausting the server resources.

In the host-based defense mechanisms, the key issues are either the lack of enough information at the sources to detect an attack in a timely fashion or inability of destinations to accurately detect and respond to the attacks before they reach the victims and wastes resources on the paths to the victims. Network-based defense mechanisms usually incur high storage and processing overhead at the routers; these overheads increase if each router performs redundant monitoring of the same traffic flows. Hence, the best alternative to traditional systems would be hybrid defense mechanisms in which defense mechanisms can be deployed at multiple locations including sources, destinations or intermediate networks.

H. Wang, C. Jin, K. G. Shin

IP spoofing has been exploited by Distributed Denial of Service (DDoS) attacks to (1) conceal flooding sources and localities in flooding traffic, and (2) coax legitimate hosts into becoming reflectors, redirecting and amplifying flooding traffic. Thus, the ability to filter spoofed IP packets near victims is essential to their own protection as well as to their avoidance of becoming involuntary DoS reflectors. Although an attacker can forge any field in the IP header, he or she cannot falsify the number of hops an IP packet takes to reach its destination. This hop-count information can be inferred from the Time-to-Live (TTL) value in the IP header. Using a mapping between IP addresses and their hop-counts to an Internet server, the server can distinguish spoofed IP packets from legitimate ones.

An Internet host can spoof IP packets by using a raw socket to fill arbitrary source IP addresses into their IP headers. IP spoofing is usually associated with malicious network behaviors, such as Distributed Denial of Service (DDoS) attacks. As one of the most difficult problems in network security, DDoS attacks have posed a serious threat to the availability of Internet services. The IP protocol lacks the control to prevent a sender from hiding the origin of its packets. Furthermore, destination-based routing does not maintain state information on senders, and forwards each IP packet toward its destination without validating the packet's true origin. Overall, IP spoofing makes DDoS attacks much more difficult to defend against.

Compared to the router-based approach, the victim-based approach has the advantage of being immediately deployable. More importantly, a potential victim has a much stronger incentive to deploy defense mechanisms than network service providers. The current victim-based approach protects Internet servers using sophisticated resource management schemes. These schemes provide more accurate resource accounting, and fine-grained service isolation and differentiation

A. C. Snoeren, C. Partridge, L. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer

The design of the IP protocol makes it difficult to reliably identify the originator of an IP packet. Even in the absence of any deliberate attempt to disguise a packet's origin, wide-spread packet forwarding techniques such as NAT and encapsulation may obscure the packet's true source. We present a hash-based technique for IP trace back that generates audit trails for traffic within the network, and can trace the origin of a single IP packet delivered by the network in the recent past. We demonstrate that the system is effective, space-efficient and implementable in current or next-generation routing hardware. We present both analytic and simulation results showing the system's effectiveness.

Tools are readily available, from covertly exchanged exploit programs to publicly released vulnerability assessment software, to degrade performance or even disable vital network services. The consequences are serious and, increasingly, financially disastrous, as can be seen by all-too-frequent headlines naming the most recent victim of an attack. Unfortunately, the anonymous nature of the IP protocol makes it difficult to accurately identify the true source of an IP datagram if the source wishes to conceal it. Many routers employ a technique called ingress filtering [9] to limit source addresses of IP datagrams from a stub network to addresses belonging to that network, but not all routers have the resources necessary to examine the source address of each incoming packet, and ingress filtering provides no protection on transit networks.

We have developed a Source Path Isolation Engine (SPIE) to enable IP traceback, the ability to identify the source of a particular IP packet given a copy of the packet to be traced, its destination, and an approximate time of receipt. SPIE therefore allows routers to efficiently determine if they forwarded a particular packet within a specified time interval while maintaining the privacy of unrelated traffic.

R. Oliveira, B. Zhang, and L. Zhang

Characterizing the evolution of Internet topology is important to our understanding of the Internet architecture and its interplay with technical, economic and social forces. A major challenge in obtaining empirical data on topology evolution is to identify real topology changes from the observed topology changes, since the latter can be due to either topology changes or transient routing dynamics. In this paper, we formulate the topology livens problem and propose a solution based on the analysis of BGP data. We find that the impact of transient routing dynamics on topology observation decreases exponentially over time, and that the real topology dynamics

consist of a constant-rate birth process and a constant-rate death process. Our model enables us to infer real topology changes from observation data with a given confidence level.

In recent years there have been a plethora of efforts in understanding the Internet AS topology and its evolution. On the empirical side, most work has focused on examining graph properties of topology snapshots and degree correlation. However there is a missing link between these two categories of work: an empirical description of the topology evolution, that is when and where AS nodes and inter-AS links are added or removed over time in reality.

The changes in the observed topology do not necessarily reflect the changes in the real topology and vice versa. Because the observed topology is normally inferred from routing or data paths, its changes can be due to either real topology changes or transient routing dynamics (e.g., caused by link failures or router crashes). Therefore the challenge is, given all the changes in the observed topology over time, how to differentiate those caused by real topology changes from those caused by transient routing dynamics, which we call the livens problem. Only after solving this problem can we provide empirical topology evolution data such as when and where an AS or an inter-AS link is added or removed from the Internet.

CONCLUSION

Preventing DDoS attacks are very important aspect in implementation and evaluation of D-PID, a framework that dynamically changes path identifiers (PIDs) of inter-domain paths in order to prevent DDoS flooding attacks, when PIDs are used as inter-domain routing objects. We have described the design details of D-PID and implemented it in a 42-node prototype to verify its feasibility and effectiveness. We have presented numerical results from running experiments on the prototype. The results show that the time spent in negotiating andDistributingPIDsare quite small (in the order of ms) and D-PID is effective in preventing DDoS attacks. We have also conducted extensive simulations to evaluate the cost in launching DDoS attacks in D-PID and the overheads caused by D-PID. The results show that D-PID significantly increases the cost in launching DDoS attacks while incurs little overheads, since the extra number of GET messages is trivial (only 1.4% or 2.2%) when the retransmission period is 300 seconds, and the PID update rate is significantly less than the update rate of IP prefixes in the current Internet. To the best of our knowledge, this work is the first step toward using dynamic PIDs to defend against DDoS flooding attacks. We hope it will stimulate more researches in this area.

References

1. Francois, I. Aib, and R. Boutaba, "Firecol: a Collaborative Protection Network for the Detection of Flooding ddos Attacks," IEEE/ACM Trans.onNetw., vol. 20, no. 6, Dec. 2012, pp. 1828-1841.
2. S. T. Zargar, J. Joshi, D. Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks," *IEEE Commun. Surv. & Tut.,* vol. 15, no. 4, pp. 2046 - 2069, Nov. 2013.
3. H. Wang, C. Jin, K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Trans. on Netw., vol. 15, no. 1, pp. 40 - 53, Feb. 2007.
4. A. C. Snoeren, C. Partridge, L. Sanchez, C. E. Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer, "Hash-Based IP Traceback," In Proc.SIGCOMM'01, Aug. 2001, San Diego, CA, USA.
5. R. Oliveira, B. Zhang, and L. Zhang, "Observing the evolution ofInternet AS topology," In Proc. SIGCOMM'07, Aug. 2007, Kyoto, Japan, pp. 313 - 324.
6. T. Benson, A. Akella, and D. A. Maltz, "Network traffic characteristics of data centers in the wild," In Proc. SIGCOMM IMC'10, Nov. 2010, Melbourne, Australia, pp. 267 - 280.
7. H. Jiang, and C. Dovrolis, "Passive estimation of TCP round-trip times,"ACM Comput. Commun. Rev., vol. 32, no. 3, pp. 75 - 88, 2002.
8. H. Luo, Z. Chen, J. Cui, H. Zhang, "An Approach for Efficient, Accurate, and Timely Estimation of Traffic Matrices," In Proc. IEEE Global Internet Symposium (GI'14), May 2014, Toronto, Canada, pp. 67-72.
9. M. Antikainen, T. Aura, M. Sarela, "Denial-of-service attacks in bloomfilter-based forwarding," IEEE/ACM Trans. on Netw., vol. 22, no. 5, pp.1463 - 1476, Oct. 2014.
10. CAIDA Ark IPv4 Routed /24 AS Links Dataset. http://www.caida.org/data/active/ipv4 routed topologyaslinks dataset.xml/.

How to cite this article:

Vijay N and Munivara Prasad K (2018) 'A review On Distributed Denial-of-Service Flooding Attacks With Dynamic Path Identifiers ', *International Journal of Current Advanced Research,* 07(4), pp. 12022-12024.
DOI: http://dx.doi.org/10.24327/ijcar.2018.12024.2104

****