INTERNATIONAL JOURNAL · ENGINEERING RESEARCH

International Journal for Innovative Engineering and Management Research

A Peer Revieved Open Access International Journal

www.ijiemr.org

IJIEMR Transactions, online available on 22nd Jul 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-07

Title: **ENHANCING NETWORK SECURITY IN DISTRIBUTED DENIAL-OF-SERVICE ATTACKS THROUGH DYNAMIC PATH IDENTIFIERS**

Volume 08, Issue 07, Pages: 249–255.

Paper Authors

P.SIVALAKSHMI, B SIVAKUMAR

SIR C.V. RAMAN Institute of Technology & Science, AP, India

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ENHANCING NETWORK SECURITY IN DISTRIBUTED DENIAL-OF-SERVICE ATTACKS THROUGH DYNAMIC PATH IDENTIFIERS

P.SIVALAKSHMI[1], B SIVAKUMAR [2]
[1]PG Scholar, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, India
[2] Assistant Professor, Dept of CSE, SIR C.V. RAMAN Institute of Technology & Science, AP, India

ABSTRACT: 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, in this paper, 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 describe in detail how neighboring domains negotiate PIDs, how to maintain ongoing communications when PIDs change. 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. The results from both simulations and experiments show that D-PID can effectively prevent DDoS attacks.

1. INTRODUCTION

Distributed denial of service (DDoS)attack occur when multiple systems flood the bandwidth or resources of a targeted system usually one or more web servers .such an attack is often the result of multiple compromised systems(for example ,a botnet) flooding the targeted system with traffic. it is very harmful to the internet.it is a malicious attempt to disrupt normal traffic to a web property. IP Spoofing is the act of creating an IP packet with a forged source IP address for the purpose of hiding the true source IP address, usually for the purpose of launching special types of distributed denial-of-service (DDoS attacks).It is used for launching DDoS to mask the sender's identity by changing the IP address with numbers.

In recent years, Path identifiers (PID) are used as inter domain routing objects in network. However, the PIDs used in existing approaches are static, which makes it easy for attackers to launch distributed denial-of service (DDoS) flooding attacks. In existing systems there are two different use cases of PIDs in approaches. In the first case, pathlet routing the PIDs are globally advertised [11] As a result, an end user knows the PID(s) toward any node in the network. In the second case, LIPSIN [12] and CoLoR[13] , PIDs are only known by the network and are secret to end user. However, keeping PIDs secret to end users is not enough for preventing DDoS flooding attacks if PIDs are static. To address this issue, introduce a D-PID, 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. Security of data which shared in network can be ensured with cryptographic techniques also..DPID mechanism with data secure provide more chance to prevent DDoS attack in network.

In D-PID, two adjacent domains periodically update the PIDs between them and used for packet forwarding. Even if the attacker tries to get the PIDs to its target and sends the malicious packets successfully, these PIDs will become invalid after a certain period and the subsequent attacking will be removed. Moreover, if the attacker tries to obtain the new PIDs to launch DDoS flooding attack it not only significantly increases the attacking cost but also makes it easy to detect the attacker.this DPID with data encryption provide more security to data throughout their network path.

The basic functions of cryptography are encryption, decryption and cryptographic hashing. In order to encrypt and decrypt messages, the sender and recipient need to share a secret. Typically this is a key, like a password, that is used by the cryptographic algorithm. DPID Mechanism with cryptographic techniques provide more security in network .DES(Data encryption standard) algorithm one of the cryptographic algorithm used commonly because of its key space without any more running time and it enhance the security of the encryption algorithm, also provide bigger secret-key space and higher encrypting efficiency. There is chance of attacking data through key assigned for data .but the proposed system, DPID with data encryption and decryption will also detect that type of attack also.for routing the data from source to destination in network through a secure path which means attack free.the breadth first search algorithm and detection of attack or checking the behavior of each node is combined

2. LITERATURE SURVEY

Appropriated disavowal of-administration (DDoS) assaults remain a noteworthy security issue, the alleviation of which is exceptionally hard particularly with regards to exceedingly disseminated botnet-based assaults. The early revelation of these assaults, albeit testing, is important to secure end-clients just as the costly system foundation assets. In this paper, we address the issue of DDoS assaults and present the hypothetical establishment, design, and calculations of FireCol. The center of FireCol is made out of interruption counteractive action frameworks (IPSs) situated at the Internet specialist organizations (ISPs) level. The IPSs structure virtual security rings around the hosts to guard and work together by trading chosen traffic data. The assessment of FireCol utilizing broad reenactments and a genuine dataset is introduced, demonstrating FireCol adequacy and low overhead, just as its help for gradual arrangement in genuine systems.

Circulated Denial of Service (DDoS) flooding attacks are one of the greatest worries for security professionals.DDoS flooding assaults are normally unequivocal endeavors to disrupt legitimate clients' entrance to administrations. Assailants for the most part gain accessto countless PCs by misusing their vulnerabilities to set up assault armed forces (i.e., Botnets). When an assault armed force has-been set up, an aggressor can conjure an organized, enormous scale attack against at least one targets. Building up a comprehensive defense instrument against distinguished and foreseen DDoS flooding assaults is an ideal objective of the interruption discovery and prevention look into network. In any case, the improvement ofsuch a system requires a thorough comprehension of the issue and the strategies that have been utilized up to this point inpreventing, distinguishing, and reacting to different DDoS floodingattacks.In this paper, we investigate the extent of the DDoS flooding attack issue and endeavors to battle it. We sort theDDoS flooding assaults and arrange existing countermeasures based on where and when they counteract, recognize, and react tothe DDoS flooding assaults. Besides, we feature the need fora far reaching appropriated and cooperative protection approach. Our essential expectation for this work is to animate the research community into creating innovative, powerful, proficient, and comprehensive avoidance, identification, and reaction mechanisms that address the DDoS flooding issue previously, during and after an genuine assault.

Denial of service(DoS)attack on the Internet has become a pressing problem. In this paper, we portray and evaluate route-based distributed packet filtering (DPF),a tale approach to distributed DoS (DDoS)attack prevention. Weshow that DPF achieves proactiveness and scalability, and we show that there is an intimate relationship between thee restiveness of DPF at mitigating DDoS attack and power-law arrange topology. The striking highlights of this work are two-fold.First,we demonstrate that DPFis ready to proactively filterout a significant fractionof spoofedpacket flows and forestall assault parcels from reachingtheirtargetsin the firstplace.TheIP flowsthatcannotbe proactively curtailed are extreme elysparse so thattheirorigincan be localized|i.e.,IP follow backstop within small, constant number of competitor sites.Wes how that the two proactive and reactive execution fectscan be accomplished by actualizing course bantering less than20%of Autonomous(AS)sites. Second, we show that the two complementary performance measures are subject to the properties of the underlying AS graph. In particular, we demonstrate that the power-law structure of Internet AS topology leads to network properties which are essential in facilitating the watched performance f-facts

3. EXISTING SYSTEM:

A main reason that DDoS flooding attacks proliferate is a node can send any amount of data packets to any destination, regardless whether or not the destination wants the packets. To address this issue, in the existing system, several approaches have been proposed. In the “off by default” approach, two hosts are not permitted to communicate by default. Instead, an end host explicitly signals, and routers exchange, the IP-prefixes that the end host wants to receive data packets from them by using an IP-level control protocol. The D-PID design is similar in sprit, since D-PID dynamically changes PIDs and a content provider can send data packets to a destination only when the destination explicitly sends out a GET message that is routed (by name) to the content provider. However, there are two important differences. First, the "off by default" approach works at the IP-prefix granularity, but D-PID is based on an information-centric network architecture and works at the content granularity. Second, the IP-prefixes that an end host wants to receive packets from are propagated throughout the Internet in the "off by default" approach, which may cause significant routing dynamics if the allowed IP-prefixes of end hosts change frequently. On the other hand, the PIDs are kept secret and change dynamically in D-PID. While this incurs cost since destinations need to re-send GET messages, the results presented in Sec. V show that the cost is fairly small.

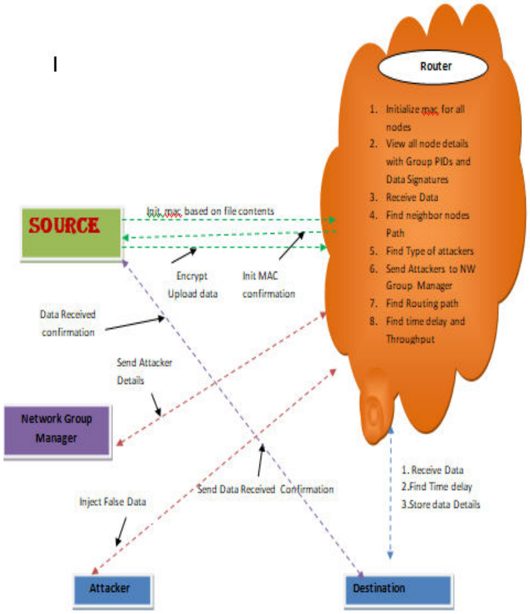
More Time Delay in Routing and less throughput. Data security is very less lack of path identifiers (PIDs)

4. PROPOSED SYSTEM:

In the proposed system, the system proposes the D-PID design by addressing the following challenges. First, how and how often should PIDs change while respecting local policies of autonomous systems (ASes)? To address this challenge, D-PID lets neighboring domains negotiate the PIDs for their inter-domain paths based on their local policies. In particular, two neighboring domains negotiate a PID-prefix (as an IPprefix) and a PID update period for every inter-domain path connecting them. At the end of a PID update period for an inter-domain path, the two domains negotiate a different PID (among the PID-prefix assigned to the path) to be used in the next PID update period. In addition, the new PID of an inter-domain path is still kept secret by the two neighboring domains connected by the path.

Distributed denial-of-service (DDoS) attacks to avoid attackers More security due to path identifiers (PIDs).

5. SYSTEM ARCHITECTURE


I
Router
1. Initialize mac for all nodes
2. View all node details with Group PIDs and Data Signatures
3. Receive Data
4. Find neighbor nodes Path
5. Find Type of attackers
6. Send Attackers to NW Group Manager
7. Find Routing path
8. Find time delay and Throughput
SOURCE
Init mac based on file contents
Encrypt Upload data
Init MAC confirmation
Data Received confirmation
Send Attacker Details
Network Group Manager
Inject False Data
Send Data Received Confirmation
1. Receive Data
2.Find Time delay
3.Store data Details
Attacker
Destination

6. IMPLEMENTATION

Source

In this module, the Source will browse an file, assign signature to all nodes, assign group PIDs to all groups (group1, group2 and group3) and then send to particular user (A, B, C, D and F). After receiving the file he will get response from the receiver. The Source can have capable of manipulating the data file and initializing keys / PIDs to all nodes before sending data to touter.

Router

The Router manages a multiple Groups (Group1, Group2, Group3, and Group4) to provide data storage service. In Group n-number of nodes (n1, n2, n3, n4…) are present, and in a Router will check all PIDs and it will select the Neighbor node path. The router also will perform the following operations such as Initialize mac for all nodes, View all node details with Group PIDs and Data Signatures, Receive Data, Find neighbor nodes Path ,Find Type of attackers, Send Attackers to NW Group Manager, Find Routing path, Find time delay and Throughput.

Group Manager

In this module, the group manager can distribute key for each and every group (Group1, Group2 and Group3) and a group each node has a pair of group public/private keys issued by the group manager. Group signature scheme can provide authentications without disturbing the anonymity. Every member in a group may have a pair of group public and private keys issued by the group trust authority (Group Manager). Only the group trust authority (Group Manager) can trace the signer's identity and revoke the group keys. If any attacker will found in a node then the group manager will identify and then send to the particular users.

Destination

In this module, there are an n-numbers of receivers are present (A, B, C, D and F). All the receivers can receive the data file from the service provider. The service provider will send data file to router and router will connect to all groups and send to the particular receiver, without changing any file contents. The user can only access the data file. For the user level, all the privileges are given by the NGM authority and the Data users are controlled by the NGM Authority only. Users may try to access data files within the router.

Attacker

In this module, the attacker can attack the node in three ways Passive attack, DOS attack and Impression attack. Dos attack means he will inject fake Group to the particular node, Passive attack means he will change the IP address of the particular node and Impression attack means he will inject malicious data to the particular node.

7. CONCLUSIONS

In this paper, we have presented the design, 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 and distributing *PIDs* are 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] J. Francois, I. Aib, and R. Boutaba, "Firecol: a Collaborative Protection Network for the Detection of Flooding ddos Attacks," *IEEE/ACM Trans. on Netw.*, vol. 20, no. 6, Dec. 2012, pp. 1828-1841.

[2] OVH hosting suffers 1Tbps DDoS attack: largest Internet has ever seen. [Online] Available: https: //www.hackread.com/ovh-hostingsuffers-1tbps- ddos-attack/.

[3] 602 Gbps! This May Have Been the Largest DDoS Attack in History. http://thehackernews.com/2016/01/biggest-ddos-attack.html.

[4] 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.

[5] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks that Employ IP Source Address Spoofing," *IETF Internet RFC 2827*, May 2000.

[6] K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," In *Proc. SIGCOMM'01*, Aug. 2001, San Diego, CA, USA.

[7] A. Yaar, A. Perrig, D. Song, "StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense," *IEEE J. on Sel. Areas in Commun.*, vol. 24, no. 10, pp. 1853 - 1863, Oct. 2006.

[8] 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.

[9] Z. Duan, X. Yuan, J. Chandrashekar, "Controlling IP Spoofing through Interdomain Packet Filters," *IEEE Trans. on Depend. and Secure Computing*, vol. 5, no. 1, pp. 22 - 36, Feb. 2008.

[10] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," In *Proc. SIGCOMM'00*, Aug. 2000, Stockholm, Sweden.

[11] 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.

[12] M. Sung, J. Xu, "IP traceback-based intelligent packet filtering: a novel technique for defending against Internet DDoS attacks," *IEEE Trans. On Parall. and Distr. Sys.*, vol. 14, no. 9, pp. 861 - 872, Sep. 2003.

[13] M. Sung, J. Xu, J. Li, L. Li, "Large-Scale IP Traceback in High-Speed Internet: Practical Techniques and Information-Theoretic Foundation," *IEEE/ACM Trans. on Netw.*, vol. 16, no. 6, pp. 1253 - 1266, Dec. 2008.

[14] Y. Xiang, K. Li, W. Zhou, "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics," *IEEE Trans. on Inf. Foren. and Sec.*, vol. 6, no. 2, pp. 426 - 437, May 2011.

[15] H. Ballani, Y. Chawathe, S. Ratnasamy, T. Roscoe, S. Shenker, "Off by default!," In *Proc. HotNets-IV*, Nov. 2005, College Park, MD, USA.

[16] A. Yaar, A. Perrig, and D. Song, "SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks," In *Proc. IEEE Symposium on Security and Privacy*, May 2004, Oakland, CA, USA.

[17] B. Parno, D. Wendlandt, E. Shi, A. Perrig, B. Maggs, and Y. Hu, "Portcullis: Protecting connection setup from denial-of-capability attacks," In *Proc. SIGCOMM'07*, Aug.2007, Kyoto, Japan.

[18] X. Yang, D. Wetherall, and T. Anderson, "TVA: A DoS-Limiting Network Architecture," *IEEE/ACM Trans. on Netw.*, vol. 16, no. 3, pp. 1267 - 1280, Jun. 2008. IEEE Transactions on Information Forensics and Security,Volume:12,Issue:8,Issue Date:Aug.201715

[19] X. Liu, X. Yang, and Y. Lu, "To Filter or to Authorize: Network-Layer DoS Defense Against Multimillion-node Botnets," In *Proc. SIGCOMM' 08*, Aug. 2008, Seattle, WA, USA.