IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 5, May 2018

A Survey on Preventing Distributed Denial of Service Attacks and Data Security

Shabna.M[1], Aswathi.T[2]

Department of CSE, Cochin College of Engineering and Technology, Valanchery, Kerala[1]

Asst. Professor, Department of CSE, Cochin College of Engineering and Technology, Valanchery, Kerala[2]

Abstract: 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. 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 attacks in network.

Keyword: Inter-domain routing, Cryptographic techniques security, distributed denial-of-service (DDoS) attacks, Path Identifiers (PID).

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.

1.1 DPID DESIGN WITH DATA SECURITY

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.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 5, Issue 5, May 2018

1.2 PROPOSED SYSTEM DESIGN

In proposed system mainly four modules are introduced. Firstly, in Nodes Reset module, nodes are created. Nodes IP address and Mac Address is retrieved into node creating users system. Each nodes IP address and MAC address is automatically stored in the admin system. Created nodes only connected into p2p and sharing the data's into another nodes. Second,In these modules we will find the shortest path into source to destination. First choose any one shortest path .The choose path detect the any botnet means choose the another shortest path automatically. Send the data without modified into correct path. Breadth-first search (BFS) is an algorithm for traversing or searching tree or graph data structures. Third, in Attacker Module: bots are try to modify your message. The attackers IP address and MAC address is identify the this modules. Modified message also detect and stored into admin system. Last ,DES Encryption: The Data Encryption Standard (DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). Figure 1 illustrates the Proposed system with detailed view of modules. it is a use case diagram of proposed system. A use case diagram in the Unified Modeling Language (UML) is a type of behavioral diagram defined by and created from a Use-case analysis. Its purpose is to present a graphical overview of the functionality provided by a system in terms of actors, their goals (represented as use cases), and any dependencies between those use cases. The main purpose of a use case diagram is to show what system functions are performed for which actor. Roles of the actors in the system can be depicted.

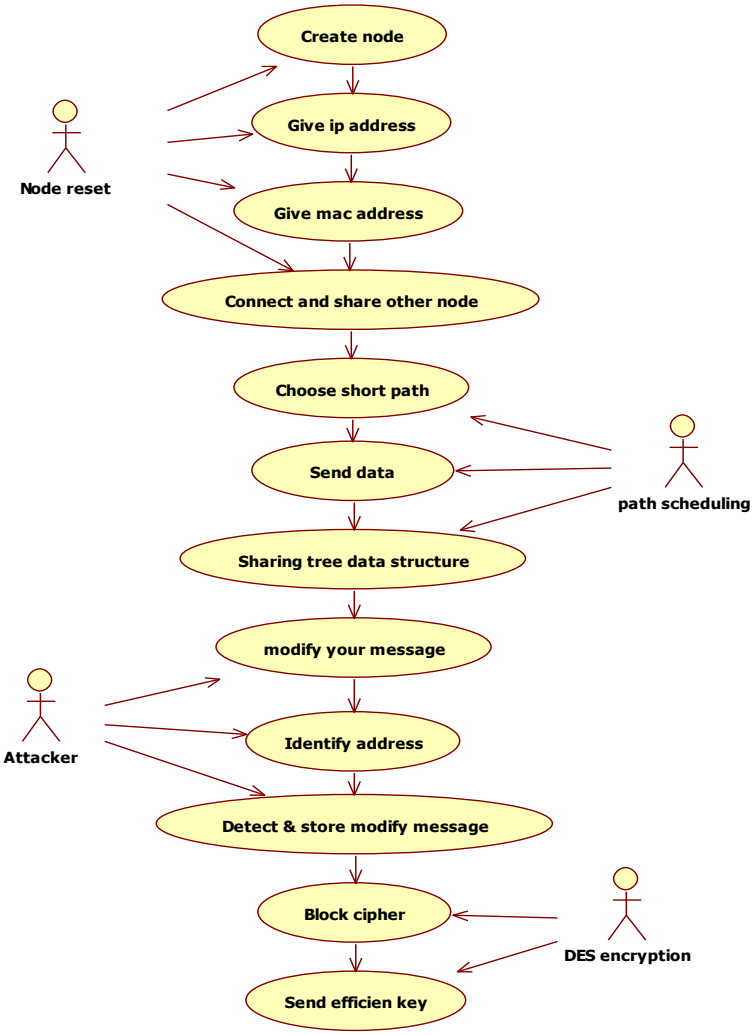

Fig 1.Use case diagram of proposed system

2. CONCLUSION

This project presented the design of DPID, 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.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.

ACKNOWLEDGEMENT

First and foremost I take immense pleasure in thanking the Management and respected principal, **Mr. Sakkariya.T**, for providing me with the wider facilities. I express my sincere thanks to **Ms. Alma Mary Margret**, Head of Department of Computer Science and Engineering, CCET for giving me opportunity to present this project research and for timely suggestions. I wish to express my deep sense of gratitude to the PG Coordinator **Mrs Jaseela Jasmin T.K** Asst professor, Department of Computer Science and Engineering, who coordinated in right path. Words are inadequate in offering my thanks to Guide **Mrs. Aswathy.T** Asst professor Department of Computer Science and Engineering, for her encouragement and guidance in carrying out the research.

REFERENCES

[1] Hongbin Luo, Member, IEEE, Zhe Chen, Jiawei Li, and Athanasios V. Vasilakos, Preventing Distributed Denial-of-Service Flooding Attacks with Dynamic Path Identifiers. *IEEE transactions on information and forensics security*,2017.
[2] H. Luo, Z. Chen, J. Cui, H. Zhang, M. Zukerman, C. Qiao," CoLoR :an information Centric internet architecture for innovations" *IEEE Network*, May 2014.
[3] 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
[4] S. T. Zargar, J. Joshi, D. Tipper "A Survey of Defense Mechanisms Against system *Distributed Denial of Service (DDoS) Flooding Attacks," IEEE Commun.Surv &Tut.* Nov. 2013
[5] P. Ferguson and D. Senie, "Network Ingress Filtering: Defeating Denial of Service of 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 the Distributed DoS Attack Prevention in Power-Law Internets," Aug. 2001
[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.*, Oct. 2006
[8] H. Wang, C. Jin, K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering,"*IEEE/ACM Trans on Netw*. 2007.
[9] Z. Duan, X. Yuan, J. Chandrashekar, "Controlling IP Spoofing through Inter domain Packet Filters," *IEEE Trans. on Depend. and Secure Computing*, Feb. 2008
[10] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical Network Support for IP Traceback," *In Proc*, Aug. 2000, Stockholm, Sweden.
[11] P. B. Godfrey, I. Ganichev, S. Shenker, and I. Stoica, "Pathlet routing," *in Proc. SIGCOMM'09*, Aug. 2009
[12] P. Jokela, A. Zahemszky, C. E. Rothenberg, S. Arianfar, P. Nikander, "LIPSIN: Line Speed Publish/Subscribe Inter- networking," *in Proc. SIGCOMM'09,* Aug. 2009
[13] T. Koponen, M. Chawla, B. C G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, I. Stoica, "A data-oriented (and beyond) network architecture," *in Proc. SIGCOMM'07,* Aug. 2007
[14] Seung-Jo Han,"The improved data encryption standard (DES) algorithm", IEEE 1996
[15]Scott beamer,david Patterson,"Direction-optimizing Breadth-First Search",IEEE Conferrence2012