International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 4, Special Issue 3 (March '2018)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

A NOVEL MECHANISM TO PREVENT DDOS TCP SYN ATTACK USING PRE-SHARED KEY

Logeswari.M,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Varsha.C,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Shruthi Kalyani.SP,
Student,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Gowri.V,
Assistant Professor,
Department of Information Technology,
Velammal Engineering College,
Chennai,Tamilnadu,India.

Abstract: The Internet usage is growing everyday along with them there is a significant increase in the security attacks of which the DDoS attack plays a major role. Hackers use different types of DDoS attacks to satisfy their purposes by crashing email servers, websites and other services provided by the Internet. TCP SYN attack which comes under DDoS attack is a great threat in the emerging cyber crime field. This paper focuses on a mechanism to prevent IP spoofing during a TCP SYN attack. The existing system checks the sender for being a blacklisted person or not and executes the prevention mechanism for the transmitted packet accordingly. Though this system prevents the website from the attacks due to IP spoofing a normal user would be blacklisted and would be denied for further service. The proposed system solves the spoofing problem by using a pre-shared key mechanism. In addition this paper proposes a mechanism by which tracing back to the sender node is possible using packet marking technique in certain cases like packet failure or for detecting the sender.

KeyWords: DDoS attack, TCP SYN attack, IP spoofing, IP trace back, Packet Marking Technique, Pre-Shared key.

I.INTRODUCTION

Internet is a global system of interconnected computer networks that use the standard Internet Protocol Suite to serve billions of users worldwide. The Internet carries a wide range of services and information services. Attacks against Internet connected systems are now common that Internet crime has become a ubiquitous phenomenon. Though a large number of preventive measures and legislations against Internet crime has been proposed and implemented, Internet crime is still growing. Computer crime encloses a broad range of illegal activities. Examples of crimes that primarily target computer networks or devices would include:

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

Among all the crimes, in this paper we focused only on denial of service (DoS).

A **denial-of-service attack** (**DoS attack**) or **distributed denial-of-service attack** (**DDoS attack**) is an attempt to make a computer resource unavailable to its intended users.

In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer. By taking advantage of security vulnerabilities or weaknesses, an attacker could take control of your computer as in Fig 1. It is one of the major cybercrime attacks currently faced. Cyber attackers aim to destroy the services provided by internet to its legitimate users. Hence DDoS attacks are increasing at a rapid pace and becoming more vulnerable to IT Security.

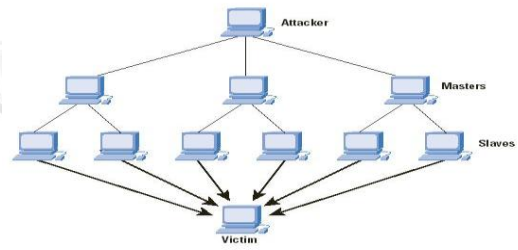

Figure1:DDoS Attack

The DDoS attacks are further classified into different types. Some of the most common DDoS attacks are

Reflected Attack

This kind of attack involves sending forge request of some type to a large number of computers that will reply to the request.

Ping of Death Attack

On the Internet, ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol.

Smurf Attack

The Smurf attack is a distributed denial-of-service attack in which large numbers of Internet Control Message

Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.

TCP SYN flood Attack

TCP SYN flood (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

UDP flood Attack

User Datagram Protocol is a session-less networking protocol. One common DDoS attack method is referred to as a UDP flood. Random ports on the target machine are flooded with packets that cause it to listen for applications on that those ports and report back with an ICMP packet.

Phlashing Attack

It is a permanent DDOS attack that damages victim system so badly that leads victim to re-install the operating system. It exploits security flaws that allows remote administration.

II.RELATED WORKS

In this paper, they present two new schemes,"**The advanced marking scheme and the authenticated marking scheme**", which allow the victim to trace-back the approximate origin of spoofed IP packets. Some of the existing mechanisms and their pit falls were discussed below. Packet Marking Technique [1] is an initial approach of tracing back source node in case of ddos attacks but it failed in case of IP spoofing by the attacker node. Wang and Reiter proposed the web referral architecture for privileged service (WRAPS) [2] which has the structure of web graph to prevent DDoS attack and authenticate the user with referral hyperlink. Another approach was introduced to detect the application DoS attacks on backend servers called group testing based approach [3].Another DDoS attack prevention architecture known as secure overlay services (SOS), was presented in [4]. The authors claim that SOS can successfully decrease the probability of the attacks using filtering close to the secure edge and randomness close to the front edge. Hop count based [5] is one of the solutions proposed to counter DDoS attacks. In this method an assumption that systems in the current internet architecture are located max with the hop count of 255.

While there are multiple techniques to detect and prevent DDoS attacks the existing method CS_DDoS detects and prevents the website from the TCP SYN attack. This method is highly accurate and efficient in working but it suffers from serious problems like

i. Tracing back to the sender is a difficult task.
ii. Though the method prevents the website from being attacked but due to IP spoofing the normal user would be denied of access.

III.PROPOSED SOLUTION

The proposed solution mainly concentrates in defending the IP spoofing by providing pre-shared key mechanism and helps in identifying the sender using a packet marking technique. This study overcomes the initial limitation of previous proposals by constructing the backup path using failure resiliency algorithm which is faster enough to construct the alternative path from sender node to destination node. The solution proposed for the pre-shared key mechanism is making use of the Egress router which is directly attached to the attacker and it must be used in order to forward the packet.

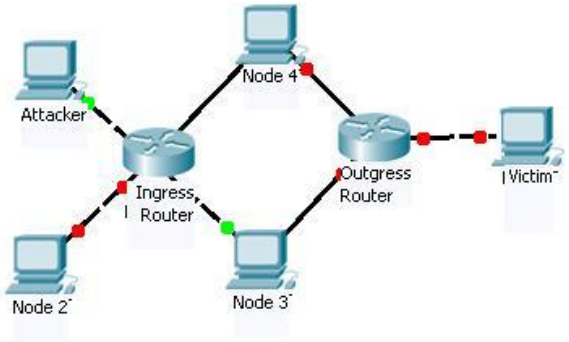

Figure2: Network Model

So, it is assumed that a secured authentication mechanism is provided between attacker and the egress router. The above mentioned mechanism makes use of pre-shared key which is considered as one of the finest secured wireless authentication mechanism as in Fig.2

Initially the Sender node need to get registered with the ingress router in order to send its packets through the network and later using pre shared key mechanism it gets authenticated by ingress router (Eg). This key is assigned by the router to all the nodes uniquely which was in the domain of router. The sender node encrypts its initial packet with this key and sends a TCP/SYN packet to the ingress router. This makes the burden of authenticating further packets coming from the same sender node to be reduced

This process involves the following steps and their notations are explained in Table.1

1.) Na - - -> Eg
Sender Node sends the request for sending packet to destination node.

2.) Eg - - - > Na
Ingress Router now will send challenge response acknowledgement to sender node

3.) Na - - - > Eg
Sender Node sends the decrypted value of hash code using its pre shared key.

4.) Eg - - - > Na
Ingress router verifies the code, if matches it then authenticates sender node and accepts the data packets that will be forwarded in the network.

Table.1: Notations

Notation		Meaning
Ns		Sender node
Nd		Destination node
Eg		Egress router
Og		Ogress router
Hcs		Hash code generated

		by sender
Hcr		Hash code generated by Eg
Sk		Shared key

If the sender node is considered to be an attacker node and targets destination node with reflector attacks then the outgress router fails back to trace the original source of packets in case of IP spoofing. But, through pre-shared mechanism it can overcome this problem. Though the sender node changes its IP it can't change the pre-shared key generated by its ingress router. This makes the sender node not to send data packets again to the same victim using different IP. If it tries to do, it will get easily identified with its pre-shared key.

IV.CONCLUSION

Methods to defend IP spoofed DDOS attacks is not yet proved. Lot many new proposals getting evolved with slight modifications and security advances. Our proposal over comes this problem by using a pre shared key mechanism. This solution proves that even though attacker node changes its IP address but it can't change the pre shared key exchanged between it and ingress router which is used for authentication. So, the attacker node can't target the victim using IP Spoofing mechanism. Our future enhancement is to implement this idea in Cloud Environment.

V.REFERENCES

[1]. Akyuz.T and I.Sogukpinar, 2009. Packet Marking with Distance based probabilities for IP trace back. Proceedings of the first International Conference on Networks and Communication, Dec.27-29, Chennai, pp.433-438.

[2]. X. Wang and M. K. Reiter, ''Using Web-referral architectures to mitigate denial-of-service threats, '' IEEE Trans. Depend. Sec. Comput. , vol.7, no.2, pp. 203–216, Apr. 2010.

[3]. Y. Xuan, I. Shin, M. T. Thai, and T. Znati, ''Detecting application denial of service attacks: A group testing based approach, ''IEEE Trans. Parallel Distrib. Syst., vol. 21, no. 8, pp. 1203–1216, Aug. 2010.

[4]. A. D. Keromytis, V. Misra, and D. Rubenstein, ''SOS: An architecture for mitigating DDoS attacks,'' IEEE J. Sel. Areas Commun., vol. 22, no. 1, pp. 176–188, Jan. 2004. KrishnaKumar.B, P.K.Kumar and R.Sukanesh, 2010. Hop count based packet processing approach to counter DDoS attacks. Proceedings of the International Conference on Recent Trends in Information Telecommunication and Computing, Mar 12-13, Kochi, Kerala, pp: 271-273.

[5]. M. Moradi and M. Zulkernine, ''A neural network based system for intrusion detection and classification of attacks,'' in *Proc. IEEE Int. Conf. Adv. Intell. Syst.-Theory Appl.*, Nov. 2004, pp. 1 – 6.

[6]. R. Jalili, F. Imani-Mehr, M. Amini, and H. R. Shahriari, ''Detection of distributed denial of service attacks using statistical pre-processors and unsupervised neural networks,'' in *Proc. Int. Conf. Inf. Secur. Pract. Exper.*, 2005, pp.192–203.

[7]. A. Kuzmanovic and E. W. Knightly, ''Low-rate TCP-targeted denial of service attacks: The shrew vs. the mice and elephants,'' in *Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun.*, 2003, pp. 75–86.

[8]. P. A. Laplante, J. Zhang, and J. Voas, ''what's in a name? Distinguishing between SaaS and SOA,'' *IT Prof.*, vol. 10, no. 3, pp. 46– 50, May 2008.

[9]. I. M. Khalil, A. Khreishah, and M. Azeem, ''Cloud computing security: A survey,'' *Computers*, vol. 3, pp. 1–35, 2014.

[10]. J. Yu, H. Lee, M.-S. Kim, and D. Park, ''Traffic flooding attack detection with SNMP MIB using SVM,''*Comput. Commun.*, vol.31, pp.4212–4219, Nov. 2008.

[11]. A. Chonka, Y. Xiang, W. Zhou, and A.Bonti, ''Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks,'' *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1097–1107, 2011.

[12]. K. Lu, D. Wu, J. Fan, S. Todorovic, and A. Nucci, ''Robust and efficient detection of DDoS attacks for large scale Internet, ''*Comput. Netw.*, vol.51, no. 18, pp. 5036–5056, 2007.

[13]. W. Dou, Q. Chen, and J. Chen, ''A confidence-based filtering method for DDoS attack defense in cloud environment,'' *Future Generat. Comput. Syst.*, vol. 29, no. 7, pp. 1838– 1850, 2013.

[14]. R. Guo, H. Yin, D. Wang, and B. Zhang, ''Research on the active DDoS filtering algorithm based on IP flow,'' *Int. J. Commun., Netw. Syst. Sci.*, vol. 7, pp. 600–607, Sep. 2009.

[15]. P. Wang, H.-T. Lin, and T.-S. Wang, ''An improved ant colony system algorithm for solving the IP trace back problem,'' *Inf. Sci.*, vol. 326, pp. 172–187, Jan. 2016.