Defence Against Dos Attacks Using a Partitioned Overlay Network.

Muhammad Usman Saeed
iResearch, Interactive Group, Islamabad, Pakistan

Abstract - *According to general statistics, around thousands of DOS and DDOS attacks have been carried out in the years 2009 and 2010. Choosing this problem for research was because everything in the industrial or mechanical sector is now controlled over the network through applications thus, securing these networks against DOS attacks is very important because once compromised it can cause a major damage to the infrastructure. This paper's idea revolves around the fact that hiding the network nodes mitigates DOS attack. This paper further extends the idea of node hiding with the architecture of a junkyard network where the suspected traffic will be routed and another overlay network which would contain the legitimate traffic to the proper destination.*

Keywords: Denial of service, Network, Overlay, Security, Flood

1. Introduction

Denial of Service (DOS) attacks are a major issue in today's network. DOS attacks are the attacks in which millions of packets, either normal or malformed are sent to a server. Thus resulting in denial of service. Most of the security experts are working on ways to mitigate DOS attacks but due to the complexity and limitation of the underlying network DOS mitigation is the biggest problem nowadays.

Overlay networks are logical networks which basically are used to support an underlying network. Applications of overlay networks include Virtual private networks, P2P networks etc. Many techniques which use overlay are devised to counter act a DOS attack.

DOS attacks include Smurf Attack [12], UDP DOS attacks [13] , SYN floods [14]. In a SYN flood attack the attacker can send many SYN requests to the client .Thus as a result the target system's memory increases to a very critical point thus the system goes into a state of Denial of service.

In a UDP flood attack thousands of UDP packets are aimed towards a target host thus crashing the target system.

Nowadays internet has become the lifeline for many crucial systems such as industrial, military. And due to the open nature of the internet it is vulnerable to many attacks including DOS attacks. As the systems are so crucial a microsecond of delay or interruption causes millions of worth of damage. Thus DOS attack defense is very important. Thus there is a need that more and more DOS attack prevention strategies may be devised so that the interruption or Denial of service problem may be reduced.

Sequence of the paper is as following:

An overview of what work is done related to this topic is given in Section 2. Section 3 gives the detail of what our proposed idea is and how we have planned the design and how it is implemented and in Section 4 conclusion of the whole discussion is given. Next section to 4 which is section 5 gives the future directions of our research which means that what can be added. The last section i.e. section 6 lists the references.

2. Related work

Many techniques have been devised so far for the defense against DOS attacks which include reactive techniques, proactive techniques.

These include ingress filtering [2], Source Trace back [3,4] , rate control techniques [6,7]. Location hiding mechanisms are widely used for the defense against DOS attack [5,8,9].The overlay protection layer was also devised to prevent DOS attacks [1].

The source trace back and ingress filtering comes in Reactive approach. Where as rate control, and location hiding comes in Proactive approach. Location hiding works on the principle that if the network nodes are hidden from the attacker then it means that the attacker can not attack on those nodes. That is for instance there is a hidden nodes network and one entry point, though the attacker can attack on the entry point but he/she won't know the location or the IP of other nodes let alone the target webserver. Overlay networks can be used as a mean for the location of a network device to be hidden. Overlay network is the only public interface for anyone to access the web server.

In an ingress filtering technique the routers have an ingress address range and the routers check the source IP of the incoming packet and if the address is out of the range of the ingress range, the packets are dropped.

There are many Chord [16] based overlay network Architectures, designed to defend against DDOS attacks and DOS attacks. Chord is a highly adaptive routing protocol used for the overlay networks.

Further more HOURS [10] using hierarchal overlay layers achieved DOS resilience in an open service hierarchy. Secure Overlay service (SOS) [8] and WEBSOS [5] were introduced for the protection of web servers against DDOS attacks. The OPL (overlay protection layer) [1] is uses an

overlay protection layer to help web servers / Applications communicate with each other even when there is a DOS attack in progress. And its goal is to distinguish between authorized and unauthorized traffic. In the paper "Deployable overlay network for defense against distributed SYN flood attacks" [11], an overlay method is described which defends against Distributed SYN flood attack. An Integrated notification architecture based on Overlay Networks against DDOS attacks on converged networks [15] also explains an overlay approach to how create a resilient network to fight against DDOS attacks in Converged Networks.

Every DOS Defense mechanism has its strengths and weaknesses None of the defense mechanism gives protection without any tradeoffs.

3. Junkyard Overlay Network

We propose an architecture which caters two problems. One is the problem at hand , that is Resistance against a DOS attack. The other can be included into the future work that is resistance against port scanning. The architecture proposed consists of an overlay network which forms the entry point to an application site. But the overlay network is further divided into two partitions, A normal overlay network and a junkyard overlay network. The overlay access point allows the traffic to enter into the overlay network. The overlay access point acts as a proxy and also as an intrusion prevention system. The communication between the overlay access point and the sub overlay network's access points is encrypted and authenticated using special signature.

The functionality of the architecture is that when the DOS attack is once detected the suspected traffic is tunneled to the junkyard network where it is then dropped. Where as the legitimate traffic is sent through another overlay network which is connected to the Application Site . Figure 1 shows the Upper level view of the proposed architecture.

The decision as to how DOS is detected can be done on the basis of rate assessment. That is if the rate of the packets is very high or greater then a specific threshold then the defense mechanism is activated and the packets start going towards the junkyard network.

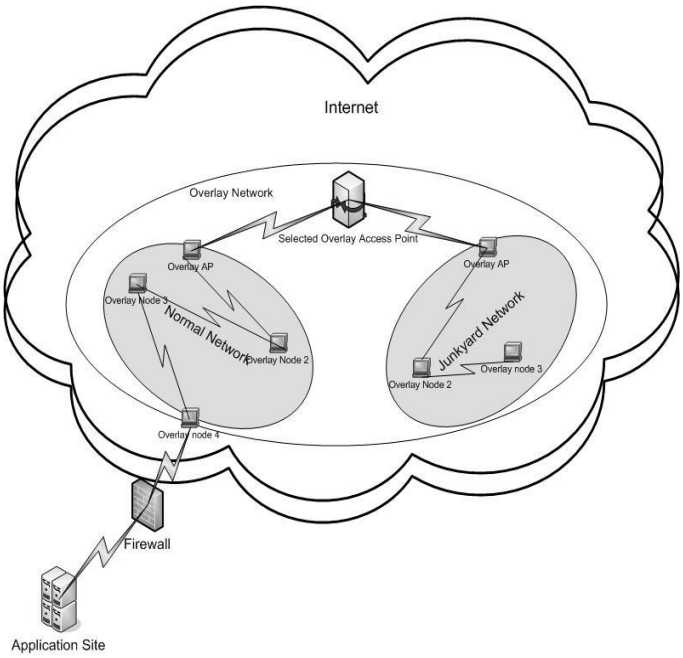

Figure 1. The packets from the internet enter through the overlay access where its decided whether the traffic is legitimate or not. Then are routed according to the decision , to the entry nodes of the Normal Overlay network or the Junkyard overlay network.

Now to solve the problem, that if the Overlay access point is attacked or flooded then what would happen? As soon as the packets hit the overlay access point and DOS is detected, the access point will shut itself down but before shutting itself down it chooses another OAP (Overlay Access Point) in the vicinity and sends a NOTIFY message containing the IP of the new OAP, to OAPs of both the partitions that is the Normal and the junkyard, telling them about the new assigned OAP. The OAPs of both the partitions send REG message to the new OAP where the authentication takes place and once registration is ok the OAP responds with REG_OK message. Figure 2 shows the scenario.

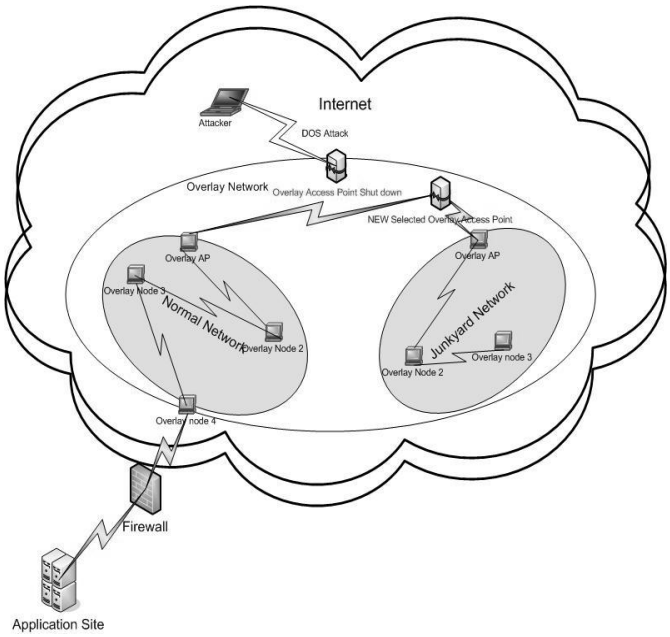

Figure 2. The attacker sends a DOS attack onto the OAP , It shuts itself down and a new OAP is selected and the communication continues.

Though there are some tradeoffs that, like any system our system can also generate false positives in theory that is. But as the junkyard network is totally isolated from the normal legitimate network, even if the legitimate traffic is recognized after it has been sent to the junkyard overlay, there won't be any way to send it to the normal network because of the lack of any interface between Normal and junkyard network.

4. Conclusion

This paper showed the design of how the overlay network could be partitioned in order to minimize the load on the network and also to mitigate flooded packets targeted at a single host. The partition [junkyard] was used because detection is easy if the filtering is applied on a gateway of any target network. But it is difficult to detect whether filtering is in place or not if the filtering is done after 3 or four hop from the gateway going inside the network. Thus the proposed technique can one , form location hiding [5,8,9] as well as the factor of deception. Similarly if the gateway of the target network is under a DOS attack, the network automatically changes the overlay access point.

5. References

[1] Beitollahi, H.; Deconinck, G. An Overlay Protection Layer against Denial-of-Service Attacks.Parallel and Distributed Processing, 2008. IPDPS 2008. IEEE International Symposium on Volume , Issue , April 2008

[2]. P. Ferguson and D. Senie. Network ingress filtering: defeating denial of service attacks which employ ip source address spoofing. In Proceedings of the IETF,RFC2267, January 1998

[3] S. Savage, D. Wetherall, A. karlin, and T. Anderson. Network support for ip traceback. ACM/IEEE Transactions on Networking, 9(3):226–237, June 2001.

[4] A. Snoeren. Hash-based ip traceback. In Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIG-COMM'01), pages 3–14, 2001.

[5] A. Stavrou and et al. Websos: An overlay-based system for protecting web servers from denial of service attacks. The International Journal of Computer and Telecommunications Networking, 48(5):781–807, August 2005.

[6] A. Garg and A. N. Reddy. Mitigation of dos attacks through qos regulation. In Proceedings of the 10th IEEE International Workshop on Quality of Service, 2002.

[7] K. Yau, C. Lui, and F. Liang. Defending against distributed denial of service attacks with max-min fair server-centric router throttles. In Proceedings of the IEEE International Workshop on Quality of Service (IWQoS'02), 2002.

[8] A. Keromytis, V. Misra, and D. Rubenstein. Sos: Secure overlay services. In Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'02), August 2002.

[9] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana. Internet indirection infrastructure. In Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIG-COMM'02), 2002

[10] Yang, H., Luo, H., Yang, Y., Lu, S., Zhang, L.: HOURS: Achieving DoS Resilience in an Open Service Hierarchy. In: Proc. of DSN, pp. 83–92, 2004

[11] Ohsita, Y. Ata, S. Murata, M , Deployable overlay network for defense against distributed SYN flood attacks , ICCCN 2005. Proceedings. 14th International Conference on Publication Date: Oct. 2005

[12] "CERT advisory CA-1998-01 smurf IP Denial-of-Service attacks." , Jan. 1998.
http://www.cert.org/advisories/ CA-1998-01.html

[13] "CERT advisory CA-1996-01 UDP port Denial-of-Service attack.".
http://www.cert.org/advisories/CA-1996-01.html.

[14] "CERT advisory CA-1996-21 TCP SYN flooding and IP spoof- ing attacks.", Sept. 1996
http://www.cert.org/advisories/CA-1996-21.html

[15] Mihui Kim, Jaewon Seo, and Kijoon Chae , Integrated Notification Architecture Based on Overlay Against DDoS Attacks on Convergence Network , IFIP International Federation for Information Processing 2007

[16] Ion Stoica, Robert Morris, David Karger, M. Frans Kaashoek, Hari Balakrishnan , Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications , SIGCOMM'01, August 27-31, 2001, San Diego, California, USA.

.[17] http://asert.arbornetworks.com/2010/12/the-internet-goes-to-war/