Int. J. Advanced Networking and Applications
Volume: 02, Issue: 03, Pages: 719-722 (2010)

Defending Denial of Service: State Overload Attacks

S S Nagamuthu Krishnan
(Assistant Professor, Thiagarajar School of Management, Madurai-625 005.
PhD Research Scholar, Bharathiar University, Coimbatore – 641 146, Tamilnadu, INDIA
Email: ssnkrishnan@gmail.com

Prof. (Dr).V Saravanan
Director, Department of Computer Applications, Dr. NGP Institute of Technology, Coimbatore. INDIA
Email:tvsaran@hotmail.com

----------**ABSTRACT**----------
In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting your computer and its network connection, or the computers and network of the sites you are trying to use, an attacker may be able to prevent you from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer. Several value-added services have been proposed for deployment in the Internet. IP multicast is an example of such a service. IP multicast[2] is a stateful service in that it requires routers to maintain State for forwarding multicast data toward receivers. This characteristic makes the service and its users vulnerable to denial-of-service (DoS) attacks. One type of attack aims to saturate the available buffer space for storing state information at the routers. A successful attack can prevent end systems from properly joining multicast groups. In this paper, we present a solution to state overload attacks;

Keywords - **: IP Multicast, State Overload attack.**

Date of Submission: July 01, 2010 Revised: September 13, 2010 Date of Acceptance: October 21, 2010

1. Introduction

In 1990, Deering proposed IP multicast – an extension to the IP unicast service model for efficient multipoint communication [2]. The multicast service model offered two key benefits: (1) the efficient use of bandwidth for multipoint communication and, (2) the indirections of a group address which allows for network-level rendezvous and service discovery. On the one hand, support for multicast is built into virtually every end host and IP router and the service is often deployed within enterprise networks. Several value-added services have been proposed for deployment in the Internet. These include multicast communication [2], quality-of-service support [3], content distribution networks[4], and denial-of-service (DoS) defense mechanisms[5]. These services provide users with an array of added capabilities.

Compared to the stateless nature of the traditional best effort IP packet forwarding service, some of the above mentioned value-added services introduce additional overhead into the network. When misused, this overhead can be a means to launch DoS attacks on the service or its users. In this paper, we take IP multicast[2] as an example and demonstrate how it can be misused to create DoS attacks on the service and its users. We then propose a solution to defend the IP multicast service from these attacks. IP multicast is one of the first value-added services to be developed and partially deployed in the Internet [2]. Despite the well known advantages of IP multicast in supporting multi receiver network applications, the existing multicast protocols suffer from various security flaws that have restricted the use of IP multicast on a larger scale [6], [7]. One important security threat in IP multicast is the possibility of DoS attacks against multicast-enabled routers. DoS attacks are possible because of the additional overhead required for packet forwarding.

The current protocol to build and maintain multicast trees is Protocol Independent Multicast (PIM) [8]. A PIM domain is a contiguous set of routers that all implement PIM and are configured to operate within a common boundary defined by PIM Multicast Border Routers (PMBRs). PMBRs connect each PIM domain to the rest of the Internet. Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP). This address is used as the root of a group-specific distribution tree whose branches extend to all nodes in the domain that want to receive traffic sent to the group. Senders inject packets into the tree in such a manner that they reach all connected receivers. How this is done and how the packets are forwarded along the distribution tree depends on the particular routing protocol. For all senders to reach all receivers, it is crucial that all routers in the domain use the same mappings of group addresses to RP addresses.
An exception to the above is where a PIM domain has been broken up into multiple administrative scope regions. These are regions where a border has been configured so

Volume: 02, Issue: 03, Pages: 719-722 (2010)

that a set of multicast groups will not be forwarded across that border. In this case, all PIM routers within the same scope region must map a particular scoped group to the same RP within that region.

In PIM, in response to join requests coming from multicast receivers, routers create and maintain state entries in exhaustible forwarding state buffers. This mechanism makes routers vulnerable to DoS attacks called state overload attacks [7]. State overload attacks can be classified by the intended victim of the attack, either end system or the infrastructure itself. In a directed end system attack, the objective is to thwart an end system or its subnet from sourcing or receiving multicast content. By overloading the state buffers at routers in its vicinity, a DoS attack can be executed against a multicast source (e.g. an Internet TV station) preventing new customers from joining and receiving data. In an infrastructure attack, the attack target may be a group of the core routers in the network backbone.

One basic idea to defend against state overload attacks is to rate limit the number of join requests originating from end hosts or multicast enabled subnets [7], [9]. Rate limiting can be effective against state overload attacks that involve one or more attack hosts within the same subnet. However, rate limiting without knowledge about which join requests are valid can have an adverse effect on legitimate join requests. Furthermore, it may not be effective if the attack is sufficiently distributed.

Previous research proposed solutions to defend against state overload attacks[7]. The objective of that solution is to protect multicast-enabled routers from being overloaded with unwanted state information.

In this paper, we propose a proactive solution to defend against state overload attacks. We introduce certain enhancements to the PIM join procedure to enable routers to verify the validity of a join message before creating state.

2. Protocol-Independent Multicast

Protocol-independent multicast *(PIM)*[7] gets its name from the fact that it is IP routing protocol-independent []. PIM can leverage whichever unicast routing protocols are used to populate the unicast routing table, including EIGRP, OSPF, BGP, or static routes. PIM uses this unicast routing information to perform the multicast forwarding function, so it is IP protocol-independent. Although PIM is called a multicast routing protocol, it actually uses the unicast routing table to perform the reverse path forwarding (RPF) check function instead of building up a completely independent multicast routing table. PIM does not send and receive multicast routing updates between routers like other routing protocols do.

2.1. PIM Dense Mode

PIM Dense Mode (PIM-DM) uses a push model to flood multicast traffic to every corner of the network [7]. This is a brute-force method for delivering data to the receivers, but in certain applications, this might be an efficient mechanism if there are active receivers on every subnet in the network.

PIM-DM initially floods multicast traffic throughout the network. Routers that do not have any downstream neighbors prune back the unwanted traffic. This process repeats every 3 minutes.

The flood and prune mechanism is how the routers accumulate their state information—by receiving the data stream. These data streams contain the source and group information so that downstream routers can build up their multicast forwarding tables. PIM-DM can support only source trees—(S, G) entries. It cannot be used to build a shared distribution tree.

2.2. PIM Sparse Mode

PIM Sparse Mode (PIM-SM) uses a pull model to deliver multicast traffic [11]. Only networks that have active receivers that have explicitly requested the data will be forwarded the traffic. PIM-SM is defined in RFC 2362.

PIM-SM uses a shared tree to distribute the information about active sources. Depending on the configuration options, the traffic can remain on the shared tree or switch over to an optimized source distribution tree. The latter is the default behavior for PIM-SM on Cisco routers[10]. The traffic starts to flow down the shared tree, and then routers along the path determine whether there is a better path to the source. If a better, more direct path exists, the designated router (the router closest to the receiver) will send a join message toward the source and then reroute the traffic along this path.

PIM-SM has the concept of an RP, since it uses shared trees—at least initially. The RP must be administratively configured in the network. Sources register with the RP, and then data is forwarded down the shared tree to the receivers. If the shared tree is not an optimal path between the source and the receiver, the routers dynamically create a source tree and stop traffic from flowing down the shared tree. This is the default behavior in IOS. Network administrators can force traffic to stay on the shared tree by using a configuration option (lp pim spt-threshold infinity).

PIM-SM scales well to a network of any size, including those with WAN links. The explicit join mechanism prevents unwanted traffic from flooding the WAN links.

3. Related Works

3.1. Modified PIM Join:

There have been several efforts to reduce the anonymity in loading the forward states. One way to address the problem is Modified PIM Join [1]. This approach of the modified join procedure is to ensure that before creating any state. During join forwarding, routers

do not create any forwarding state, but instead add the requisite state information to the join message before sending it upstream towards the source. Each on-tree router, Rj , appends this state information as nonce, say Nj , to the end of a nonce block in a new Join(S,G,N) message. The state information added includes the incoming interface, ij , of the join message and a secure hash of all the locally added state, Hj. If the source and the group in the Join(S,G,N) message are valid, the accumulated state information is returned by DR(S) in a new JoinACK(S,G,N) message. Each router, Rj , in the return path individually verifies the JoinACK(S,G,N) by recomputing the secure hash Hj with the relevant state information in the nonce Nj . This ensures that the received JoinACK(S,G, N) is a valid acknowledgment of the Join(S,G,N) that Rj had previously forwarded upstream. Once the verification is complete, Rj creates a forwarding entry for (S,G) with ij as the oif and IntRPF (S) as the iif for the group. Once the JoinACK reaches and is verified by DR(R), the join process is complete.

3.2. Overlay Based Indirection:
The second solution is overlay based architecture [1]. The idea behind this solution is to ensure that the DR(R) propagates join requests only if the source and the group being requested in the join message are known to be valid. This prevents the possibility of state overload attacks with bogus join messages. The overlay based architecture require three components in each multicast domain: 1) Overlay nodes, 2) Verification boxes (VB), and 3) Indirection boxes (IB). One or more overlay nodes are deployed per domain and are configured statically or dynamically with a database of valid (S,G) pairs within their domain. Domain names can be created such that a source address S can be translated to a domain name using a simple bootstrap or mapping algorithm. To maintain connectivity of the overlay network, overlay nodes in neighboring domains establish neighborhood relationships with each other. A routing protocol is also established on top of the overlay network to provide packet forwarding between nodes.

Verification boxes (VB) are deployed by the ISPs and network administrators at the edges of their domains. A VB is responsible for monitoring and filtering all incoming and outgoing PIM control messages from its domain. Incoming transit and outgoing messages are also verified to ensure that the final destination is valid.

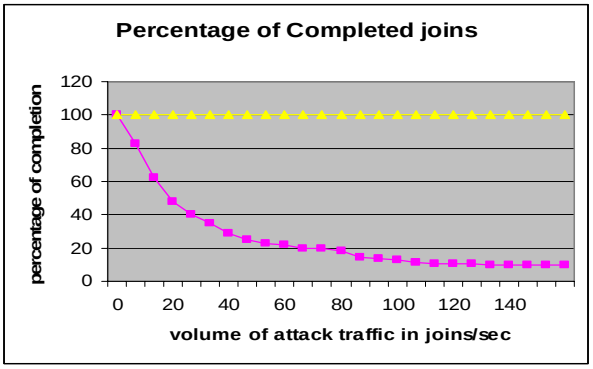
Indirection Boxes (IB) are co-located with the designated router (DR) in IP multicast domains. They use IGMP snooping to detect and redirect IGMP traffic from hosts in their domains to themselves. All IGMP messages are buffered in the IBs until the intended recipients are verified as valid.

Proposed Solution

4. Enhanced validated Group Join procedure:

The objective of the solution is to ensure that before creating any state, every router in the forwarding path can individually verify and check validity of the source and the group being subscribed to join. This verification ensures that bogus join messages sent by malicious receivers cannot create unwanted state in the routers. This can be achieved by creating unique ID which persists for that particular session; This ID is a hexadecimal one that is sent along with the group join invitation.

This hexadecimal ID should be included in the join request message. Every router between source and destination router should maintain those ID in the Routing table. Every time the join request arrived at the router, it will ensure the message and allow it to proceed from the forward state in the buffer, before creating the state in the router it again checks for the state in the buffer in order to avoid redundancy in the state buffer. If there exists a forward state in the buffer, then the new message will replace the existing state. This second level of filtration in creating the state inside the buffer avoids the bogus message to create the state at any time. It is obvious that if there is no state for the authorized join request it will create the new state. This enhanced feature of second level screening avoids the unnecessary creation of repeated state in the buffer even though the join request is from the authorized user.



The graphical analysis shows the percentage of completed joins. Upon simulation of the modified PIM join procedure, even in the increase of volume of attack traffic the percentage of completed joins remain static at an increased rate.

5. Conclusion

In this paper, we have examined DoS attacks, called state overload attacks, for a specific service, multicast which cause serious problem to the value added service in internet. We proposed a set of modifications to make it more secure against these attacks. This solution against DoS attacks without creating noticeable performance loss or latency for the end user. And the efficiency and

tolerance of the proposed solution examined and performance is showed graphically.

We believe our solution represents a valuable step to provide successful join even though the number of attackers increases. Several areas remain to be addressed in future work, such as the Random number generation for every receiver and Time based state updating.

6. Future Work

Our focus on this paper has been primarily performance oriented. In our solution we assign a unique ID for the each members, and a further work can be to create a Random Hexadecimal for forming the group. And this work can be extended by enhancing this solution with the Time based state updating concept i.e. we can remove the unwanted states in the buffer which persists for longer time. This can be achieved by having counter variable for each state loaded in the buffer.

Acknowledgement

M Srinivasan, Faculty Member, Thiagarajar School of Management, Madurai, Tamilnadu. P.Kathirvel, G.Balaji, S.G.P Devaraj, R.Dilip, G.Ilaiyaraja, Thiagarajar School of Management, Madurai, Tamilnadu.

References

[1] Jinu Kurian, Kamil Sarac, Kevin Almeroth "Defending Network-Based Services against Denial of Service Attacks" International Journal of Network Security, Vol.9, No.2, PP.186-200, Sept. 2009

[2] K. Almeroth, "The evolution of multicast: From the MBone to interdomain multicast to Internet2 deployment," IEEE Network, vol. 14, pp. 10–20, January/February 2000.

[3] S. Shenker and J. Wroclawski, "General Characterization Parameters for Integrated Service Network." Internet Engineering Task Force (IETF), RFC 2215, September 1997.

[4] B. Krishnamurthy and C. Wills, "On the use and performance of content distribution networks," in Proceedings of ACM SIGCOMM Internet Measurement Workshop, (San Fransisco, USA), November 2001.

[5] S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Practical network support for IP traceback," in Proceedings of ACM SIGCOMM, (Stockholm, SWEDEN), August 2000.

[6] C. Diot, B. Levine, B. Lyles, H. Kassem, and D. Balensiefen, "Deployment issues for the IP multicast service and architecture," IEEE Network, vol. 14, pp. 78–88, January/February 2000.

[7] P. Savola, R. Lethonen, and D. Meyer, "PIM-SM Multicast Routing Security Issues and Enhancements," October 2004. Internet Engineering Task Force (IETF) draft, work in progress.

[8] D. Estrin et al., "Protocol Independent Multicast Sparse-Mode (PIMSM): Protocol Specification." Internet Engineering Task Force (IETF) RFC 2362, June 1998.

[9] M. Handley and A. Greenhalgh, "Steps towards a DoS-resistant Internet Architecture," in Proceedings of ACM SIGCOMM workshop on Future Directions in Network Architecture, (Portland, OR, USA), August 2004.

[10]http://www.cisco.com/en/US/docs/internetworking/technology/handbook/IP-Multi.html

[11] http://tools.ietf.org/html/draft-ietf-pim-v2-dm-03

Authors Biography

S S Nagamuthu Krishnan, Assistant Professor, Thiagarajar School of Management, Madurai, Phd. Research Scholar, Bharathiar University, Coimbatore. Mr. S S Nagamuthu Krishnan has got his Bachelor's degree in Physics from Madurai Kamaraj University during the year 1995 and MCA degree from Bharathiar University during the year 1998. He has obtained his MPhil in Computer Science from Bharathiar Universitym in the year 2007. He has got more than 10 years of academic experience. His areas of interest are Object Oriented Analysis and Design, Computer Security, Data Structures & algorithms and Networking. He serves as Assistant professor and Coordinator- MCA in Thiagarajar School of Management, a B-School in Madurai. He is also pursuing his research leading to Ph. D. in Network Security.

Dr. V Saravanan obtained his Bachelor's degree in Mathematics from University of Madras during 1996 and Masters Degree in Computer Applications from Bharathiar University during 1999. He has completed his PhD in Computer Science in the Department of Computer Science and Engineering, Bharathiar University during 2004. He specialized on automated and unified data mining using intelligent agents. His research area includes data warehousing and mining, software agents and cognitive systems. He has presented many research papers in National, International conferences and Journals and also guiding 3 researchers leading to their PhD degree. He has totally 10 years experience in teaching including 3 years as researcher in Bharathiar University. He is the member of Computer Society of India, Indian Association of Research in Computing Sciences and many professional bodies. At present, he is the director of Department of Computer Applications, Dr. NGP Institute of Technology, Coimbatore.