International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-2 Issue-1, October 2012

Risk Mitigation of Denial of Service Attack

Ankit Pincha

Abstract— In this paper, I propose to mitigate the risk of denial of service attack. This involves identification of genuine traffic and giving it a higher priority. This results in lower priority for suspected malicious traffic. The priority of threads below the specified threshold will be discarded. Spoofed Denial of service attacks have also been taken care of thereby providing maximum security to the system by the attacker. The attacker suffers from a reduced priority of service. The reduced priority means greater response time for service request. The attacker might find his attack to be effective whereas the system might still be handling the request of genuine traffic.

Index Terms— DOS, risk, mitigation, attack, denial of service, prevention.

I. INTRODUCTION

A denial of service (DoS) attack is defined as an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. In a distributed denial-of-service, large numbers of compromised systems (sometimes called a botnet) attack a single target.

We have seen the impact of loss with DOS attack.

- With DOS attack, attacker might be able to access valuable information about your accounts and misuse them. You may not be able to access your own account, but attacker does.
- These attackers actually can cause huge revenue loss by attacking root servers, computers which are networked through broadband connection.

For example: the torrent site miniova is an interesting case. The figure shows how effective the DOS attack can be to bring the system down.

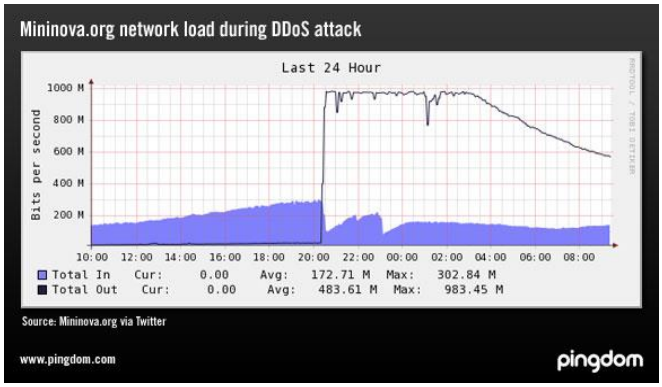

Fig 1: Example of DOS attack: miniova.org

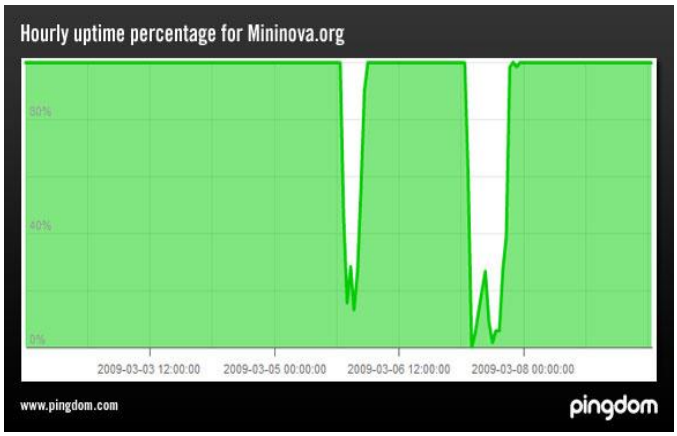

Fig 2: Hourly uptime of miniova.org

II. EXISTING SYSTEMS:

Existing systems work on rule based mechanism. They are firewall based where specified addresses are blocked, existing ports are secured etc. But, attacker can be clever enough to bypass these rules and attack the system by IP spoofing etc.

If this is the case, the system is useless and cannot be a sure solution to the increased threat of Denial of Service attack. The configurations can change but only after the damage done. This is because of their static nature without dynamism approach that needs to be sought.

III. ALGORITHM :

The following algorithm is proposed:

1. Collect the request logs(which consist of the information about all the users who have used our system)
2. Extract all IP addresses of the current request.
3. Count the number of serviced and existing threads in the system corresponding to the IP address. Also check for corresponding service response time.
4. If existing thread with the same IP is found, decrease the priority of both the incoming thread and the existing thread by 1 (in case of java) or by 10%. In java, this is used by concept called thread pooling.
5. If service request time is greater than 100% of the average service request time, decrease the priority of existing request by 1(in case of java) or by 10%.
6. If thread priority is less than or equal to 1(in case of java) or a specific threshold (in others), discard the thread and release the resources associated with the thread.

Manuscript published on 30 October 2012.
***** Correspondence Author (s)
Ankit Pincha, Information Technology, Sardar Patel Institute Of Technology,Mumbai, India.

7. Identify the address of the intermediate routers of the above identified hosts. The best and most common way is to attempt to ping the target host's IP address using and incremental Time to Live identifier in the IP header. These addresses will be stored in database. This will then be used to identify malicious clients when they spoof their IP address or MAC address.
8. If any of the subsequent requests follows the network path of previous malicious request, special logs are for these clients are created to monitor them stringently. These logs are monitored by a specialist, and if need arises, blacklisting of the path is done.
9. Repeat the above procedures till the server is running to prevent Denial of service attack.

IV. Benefits of Proposed Approach over Existing Solutions

The above proposed algorithm has various benefits over existing approaches:

Proposed system (priority based)	Filtering approach (existing solution)
The attacker's thread decreased priority means greater availability of system to genuine users.	The existing system just accepts or discards the packet.
Response time for the attacker increases. Hence, the attacker might be under the impression that the system is successfully bogged down whereas on the contrary it is usable to genuine clients.	Not possible with existing approach
The malicious client will be monitored if he goes for further attacks in future. Hence, attacking once might expose him to failure of attacks in future.	The malicious attacker can bypass the filters set.
The genuine clients will not suffer because their traffic is negligible compared to an attacker employing DOS attack. As it deals with relative reduction of priority, the priority of attacker will decrease more than the genuine client.	Suffers from various drawbacks like genuine traffic might suffer from rules developed and attacker bypassing the filters.

Table1: Comparison of proposed system and existing solution.

V. Spoofing Scenario:

If IP address and MAC addresses are spoofed, the intermediate routers which are authentic can be used to strictly monitor the traffic. These authentic routers will have their specific suffix for their identification. Any traffic generating from these routers will be monitored due to an attack suspect.

VI. Result of Developed Prototype

DOS attack was launched using LOIC (TCP flooding). This was done to simulate DOS attack. The result is as shown below:

Table 2: Results of prorototype

Scenario	**Response time before DOS mitigation system**	**Response time after DOS mitigation system**
Request flooding from 8 clients using LOIC over LAN	20-24 sec	5-8 sec
Request flooding from 8 clients using LOIC over world wide web	15-18 sec	10-12 sec

VII. Conclusion

The proposed system has shown motivating results and the approach is successful to acceptable extent to mitigate the risk of DOS. Hence the algorithm developed looks promising and reliable. This approach can be studied with heavy research methodology to help mitigate the problem which has been a huge threat for years together.

Acknowledgment

I dedicate this paper to my mother. She has played an immense role and has been the guiding light. She has been my strength throughout.

My father has been a constant inspiration and motivated me at every juncture to work hard.

I would like to thank Prof Ambavde, Prof. Kailas Devadkar, Prof Sheetal Chaudhari and HOD Prof. Radha Ma'am, without which this paper would not have been possible. Prof Radha (currently pursuing PHD at JNTUH) and Prof Kailas were a friend, mentor and a guide. They aroused interest of network security which motivated me for this research.

References

[1] http://support.microsoft.com/kb/162326
[2] http://searchsoftwarequality.techtarget.com/definition/denial-of-service
[3] http://www.denial-of-service-attacks.com/what-is-direct-denial-of-service.html
[4] http://cr.yp.to/syncookies.html
[5] http://www.ddosattacks.net/2012/07/25/five-ways-to-protect-against-distributed-denial-of-service-ddos-attacks/
[6] http://royal.pingdom.com/2009/03/10/the-anatomy-of-a-ddos-attack/?isalt=0
[7] Internet Denial of Service: Attack and Defense Mechanisms by Jelena Mirkovic, Sven Dietrich, David Dittrich, Peter Reiher

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

Ankit Pincha: I have done my engineering from Sardar Patel Institute of Technology. I have been a Microsoft Student Partner, and have given many talks on Microsoft Technologies. I have also completed IBM DB2 certification. At college level, won coding competitions, organized events. My research interest in this topic triggered when I realized how ubiquitous denial of service attack has become and how no effective methods have yet been developed.