Journal of Engineering and Applied Sciences 7 (5): 383-386, 2012
ISSN: 1816-949X

Effective Analysis of Distributed Denial of Service Attacks Using IP Traceback Algorithm

G. Jeya Bharathi and B. Santhi
School of Computing, SASTRA University, Thanjavur, Tamil Nadu, India

Abstract: Distributed Denial-of-Service (DDoS) attacks are a major security threat to internet services. DDoS attack is a type of attack in which a multitude compromised systems attack a single target system. The flood of incoming messages to the target systems essentially forces it to shutdown. The internet routing mechanisms are memory less so the source path cannot be found. This study proposes a novel IP trace back method to trace back the original source and to detect the DDoS attacks. The proposed strategy is to use IP address to detect and track back the violations occurred in the files.

Key words: DDoS, IP trace back algorithm, file watcher, shutdown, violations, India

INTRODUCTION

Distributed Denial-of-Service (DDoS) attack is one of the most difficult security problems to address. In DDoS attacks, attackers create a huge amount of requests to victim through compromised systems with the aim of denying normal service. DDoS attack causes a great damage on the network resources. These are done internationally. It can also be done large scales also which create a massive loss of time and money. The early attacks are too well known websites such as CNN, Amazon and Yahoo (Garber, 2000). The extreme complexity of the current internet it is difficult for the victim to ascertain the attack source in a DDoS attack because the attacker routinely forges the source IP address of each attack packet. The sources of a DDoS attack is harder to retrieve because many attack sources are widely dispersed in the internet and there is no apparent feature of a DDoS stream that can be directly exploited by the victim.

Probabilistic Packet Marking (PPM) and Deterministic Packet Marking (DPM) are the two previous packet marking techniques. Probabilistic packet marking can operate only in Internet Service Provider (ISP) network. Internet service provider network is generally quite small and the sources of the attack cannot be traced back since it is located out of the ISP network. Deterministic packet marking (Gong and Sarac, 2008) requires all the internet routers to be updated and it also requires more storage for packet logging. Both of these require routers to inject marks into individual packets. The packet marking strategies has lack of scalability and extraordinary challenge on the storage space.

The main goal of this study is to use the IP address and the DNS (Domain Name System) servers to detect and trace back the violations occurred in the files and to prevent the system from the DDoS attacks on the internet. By this trace back we can avoid system thrust such as system is either slow down or stopped together and overwhelming a server. IP trace back means retrieval of the original source of any packet sent across the internet. The proposed method needs no marking on packets and therefore avoids the inherit shortcoming of packet marking mechanism.

Background of distributed denial of service attacks: Distributed Denial-of-Service (DDoS) attacks targeted on exhausting the victim's resources such as network bandwidth, computing power and operating system data structures. DDoS attack is an attack on a computer or network that prevents legitimate use of its resources. To install a DDoS attack, attackers can use different kinds of techniques to install a DDoS attack (Weaver, 2001, 2002; Kevin, 2001) such as scanning, software/backdoor vulnerability, Trojan Horse Program, Buffer Overflow and Corrupted File.

There are two categories of DDoS attacks, bandwidth and resource depletion attack (Mirkovic and Peter, 2004; Chen *et al*., 2004). Bandwidth depletion attack is on the person's usage of bandwidth. It happens in two types of attacks called flood and amplification attack. Both are used to reduce the bandwidth of the user by sending the messages to the IP address and completely down the bandwidth. Resource depletion attack means the communication is attacked by the attacker. The packets are sent will completely mix up and confuse the legal

Corresponding Author: G. Jeya Bharathi, School of Computing, SASTRA University, Thanjavur, Tamil Nadu, India

users. So, they cannot use any network till they are corrected. In this type of attacks are targeted a server or process on the victim system making it unable to process legitimate requests for service.

Related work: PPM mechanism can solve only the flooding attacks. To overcome the attacks consists of a smaller number of packets. For that Belenky and Ansari (2003) used a deterministic packet marking method. The initial router of the information source, the router embeds an IP address into a packet by dividing the routers IP into 2 segments with 17 bits. Then the victim can trace that the packets came from which router.

The PPM mechanism is to mark packets with the IP address. It is vulnerable to the attackers and the accuracy is another problem, the marked messages by the routers overwritten by the downstream routers on the attack tree. The large amounts of storing marked packets are the main drawbacks of the PPM algorithm. The randomize (Law *et al*., 2005) and the link approach is used to implement the IP trace back based on the PPM mechanism. The algorithm targets to reconstruct the marks from the markers and the PPM to make more secure. Savage *et al*. (2001) proposed the probability based packet marking method. This adds the node address at the end of the packet. It has a long path that contains an unused space in the original packet. Then researchers proposed the node sampling algorithm, it records the routers address to the packet with probability (p) on the attack path. Researchers can reconstruct the attack path based on the number of marked packets and it requires a large number of accuracy to improve. The edge sampling algorithm is used to mark the start and the end router address of an attack link and measures the distance between the two ends.

Snoeren *et al*. (2001, 2002) proposed a method by logging packets or digests of packets at routers. The packets are digested using bloom filter at all the routers. Based on these logged information, the victim can trace back the leaves on an attack tree. The methods can even trace back a single packet. However, it also places a significant strain on the storage capability of intermediate routers.

Deterministic Packet Marking (DPM) strategy was proposed by Dean *et al*. (2002). There is no more marking for the packets only the router writes its own IP address into the outgoing IP packet header. For encoding trace back information they used the algebraic approach. Their idea is that for any polynomial f(x) of degree d in the prime field GF (p), f(x) can be recovered given f(x) evaluated at d+1 unique point.

MATERIALS AND METHODS

Proposed method: There are many tricks to infect the healthy files. The attackers redesign the desktop icons and modify them such files. In this study proposes a novel trace back algorithm for DDoS attack that is based on address of the user. A novel IP trace back algorithm is used to detect the DDoS attack occurred in the web server by an unauthorized user and then to trace back the violations occurred in the files.

Trace back the attack: If the DDoS attack is found, the IP watcher is used to detect the DDoS attack. Researchers can trace the file that the IP address causes the attack with the help of log entry. While tracing the file which is being attacked, this trace back mechanism can replace the original file in place of the affected one. Thus, the IP trace back mechanism is used to prevent the file from the attack.

IP traceback algorithm

Algorithm:

```
Start the process
Analyze the files to be kept secure
Count the number of file in the list
For i = 1 to count
{
Store the files in the Home Directory
Assign each file with a log ID
Store the file in the database with the ID
}
While (time period to keep the file secure)
{
Watch the file
Identify the file log ID
New-id = file.log iD
For i = 1 to count
{
   If (File (i).old-ID == New-iD) then
      The file is secure. Leave it from any modification
   Else
      Restore the original file from the backup directory.
  }
 }
Stop the process
```

First step of the algorithm is to get the list of file names that must be kept secure from the attacks. Then count the number of files in the list. Assign unique ID for each file in the home directory and then kept the files in the database.

Each time when the user accesses the file, the file watcher identifies the log ID for that file and then compares it with original log ID which is kept in the database. If both log IDs are found to be same then the file watcher identifies that the file is the original file and leave the file from further replacement. Otherwise,

the file is replaced by the original file which is stored in the backup directory. Thus, the file watcher watches the file and prevents the file from attacks. Thus, the proposed algorithm is sufficient to satisfy the requirements of preventing the file from attacks.

RESULTS AND DISCUSSION

Experimental analysis: Figure 1 shows the log entry details of a file when the particular file is accessed by the user.

By this, if any user accessed the files in any other system, it will creates a details of the users IP address, request time, response time, date and requested files are stored in database. Figure 2 shows the file watcher which is used to keep track of all the w.w.w. files. The file watcher is used to check whether there is any DDoS attack is there on a particular file.

Figure 3 shows the blocked list of the DDoS attacked files. While replacing the file, the user who attacks the file is treated as an unauthorized user and to prevent the user from continuous accessing of the web server, their IP address is added in the blocked kist.

Figure 4 shows the access being denied for the items in the blocked list. The clients having the IP address in blocked list, the web server cannot able to provide any response to that client. Hence, the user right is prohibited.

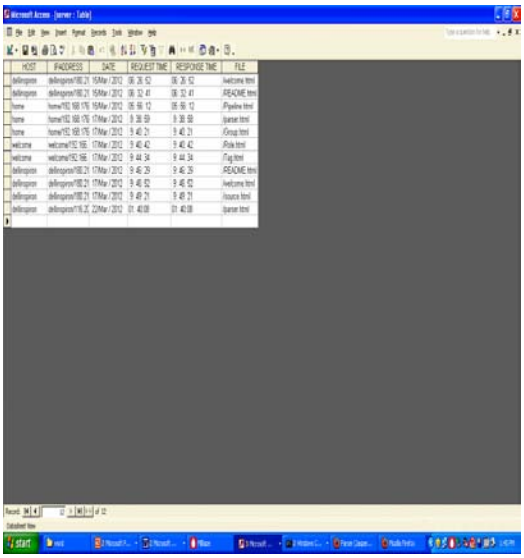

Fig. 1: Log entry

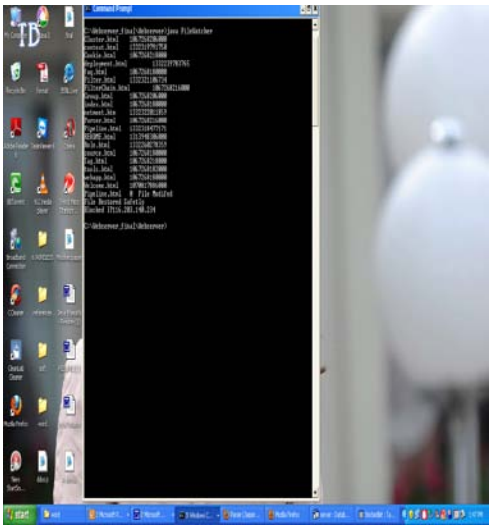

Fig. 2: File watcher

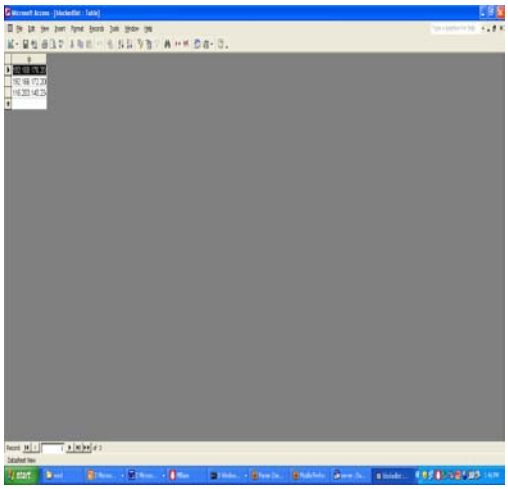

Fig. 3: Blocked list

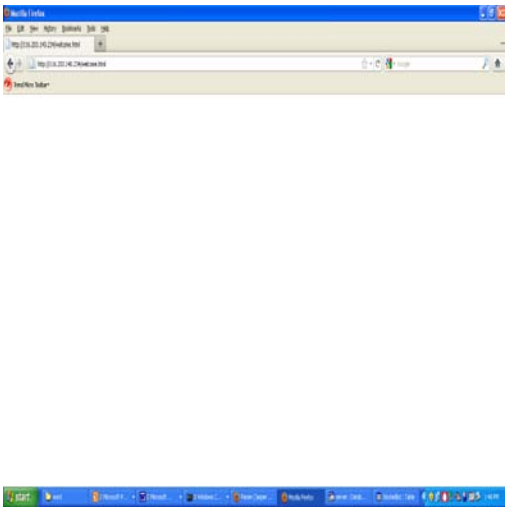

Fig. 4: Blocked IP address

CONCLUSION

This study focuses on detection of DDoS attacks in networks. Here a novel IP trace back algorithm is proposed to achieve a much more effective mechanism to prevent the system from the DDoS attack. The files that are attacked are being traced and the original non attacked files are replaced in its place. Hence, the DDoS attack is prevented. Due to this the malfunctioning of the system like frequent shutdown, system processing will be slow, overwhelming a server are prevented. Thus, the accuracy and efficiency of the system is met here.

REFERENCES

Belenky, A. and N. Ansari, 2003. IP traceback with deterministic packet marking. Commun. Lett. IEEE., 7: 162-164.

Chen, L.C., T.A. Longstaffv and K.M. Carley, 2004. Characterization of defense mechanisms against distributed denial of service attacks. Comput. Secur., 23: 665-678.

Dean, D., M. Franklin and A. Stubblefield, 2002. An algebraic approach to IP traceback. ACM Trans. Inform. Syst. Secur., 5: 119-137.

Garber, L., 2000. Denial-of-service attacks rip the internet. IEEE Comput., 33: 12-17.

Gong, C. and K. Sarac, 2008. A more practical approach for single-packet ip traceback using packet logging and marking. Proceeding of the IEEE Transactions on Parallel and Distributed Systems, Volume: 19, October 19-23, 2008, Rochester, New York, pp: 1310-1324.

Kevin, T., 2001. Tutorial-Virus Malicious Agents. University of Calgary, Alberta, Canada.

Law, T.K.T., J.C.S. Lui and D.K.Y. Yau, 2005. You can run, but you can`t hide: An effective statistical methodology to trace back DDoS attackers. IEEE Trans. Parallel Distributed Syst., 16: 799-813.

Mirkovic, J. and R. Peter, 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Comput. Commun. Rev., 34: 39-53.

Savage, S., D. Wetherall, A. Karlin and T. Anderson, 2001. Practical network support for IP traceback. IEEE/ACM Trans. Network., 9: 226-237.

Snoeren, A.C., C. Partridge and L.A. Sanchez, 2001. Hash-based IP traceback. Proceedings of the ACM SIGCOMM 2001 Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, August 27-31, 2001, San Diego, California, USA., pp: 3-14.

Snoeren, A.C., C. Partridge, L.A. Sanchez, C.E. Jones and F. Tchakountio *et al*., 2002. Single-packet IP traceback. IEEE/ACM Trans. Network., 10: 721-734.

Weaver, N., 2001. Warhol worms: The potential for very fast internet plagues. http://www.iwar.org.uk/comsec/resources/worms/warholworm.

Weaver, N., 2002. Potential strategies for high speed active worms: A worst case analysis. http://www.ccert.edu.cn/upload/2/1.pdf.