ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Discernmenting Denial of Service Flooding Attacks In Networks

A.Venkataraju
M.Tech Student,
Department of CSE,
Aims College of Engineering,
Mummidivaram, Amalapuram.

Md.Alisha
Associate Professor & HOD,
Department of CSE,
Aims College of Engineering,
Mummidivaram, Amalapuram.

Abstract:

Distributed Denial of Service (DDoS) flooding attacks are launched by attackers disturbing server services as well as Individual users who are active in internet. Especially attackers are targeting network Transport level DDOS flooding attacks and application level DDoS attacks. Interrupt a legitimate user's connectivity by exhausting bandwidth, router processing capacity or network resources these are essentially network transport level flooding attacks and interrupt a legitimate user's services by exhausting the server resources like sockets, CPU, memory, disk, database bandwidth, these essentially include application-level flooding attacks .monitor and DDoS detecting algorithm is proposed to prevent these attacks . Client send the data to the server at that time attacker can also send the large amount of data continuously and simultaneously to the targeted system. The target system either responds so slowly as to be unusable or sometimes crashes completely. It becomes more complicated for the defense mechanisms to recognize the original attacker developing a comprehensive defense mechanism against recognized and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention research community.

Keywords:
Attack; intrusion detection system; flood; intrusion; Denial.

INTRODUCTION:

Denial of service (DOS) flooding attacks, which are intended attempt to stop legitimate user from accessing a specific network resources. Distributed denial of service (DDOS) flooding attacks are one of the biggest concerns for security professionals. DDOS attacks are typically explicit to disrupt legitimate user's access to services. Attackers usually gain access to a large number of computers by exploiting their vulnerabilities to set up attack armies (i.e., Bonnets).

Once an attack army has been set up, an attacker can invoke a coordinated, large-scale attack against one or more targets. Especially attackers are targeting network/ Transport level DDOS flooding attacks and application level DDoS attacks. Disrupt a legitimate user's connectivity by exhausting bandwidth; router processing capacity or network resources these are essentially network-level flooding attacks. Disrupt a legitimate user's services by exhausting the server resources (e.g., sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth) these essentially include application-level flooding attacks .Client send the data to the server at that time attacker can also send the large amount of data continuously and simultaneously to the targeted system. The target system either responds so slowly as to be unusable or sometimes crashes completely. It becomes more complicated for the defense mechanisms to recognize the original attacker developing a comprehensive defense mechanism against identified and anticipated DDoS flooding attacks is a desired goal of the intrusion detection and prevention research community.

In that comprehensive classification of various DDoS defence mechanisms along with their advantages and disadvantages based on where and when they detect and respond to DDoS flooding attacks. The development of such a mechanism requires a comprehensive understanding of the problem and the techniques that have been used thus far in preventing, discernment and responding to various DDoS flooding attacks.We focus on DDoS flooding attacks and defense mechanisms in wired networked systems. Here, our goal is to categorize the existing DDoS flooding attacks and to provide a comprehensive survey of defense mechanisms categorized based on where and when they detect and respond to DDoS flooding attacks. Such a study of DDoS flooding attacks and the presented survey is important to understand the critical issues related to this important network security problem so as to build more comprehensive and effective defense mechanisms. we explore the scope of the DDoS flooding attack problem and attempts to combat it.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We categorize the DDoS flooding attacks and classify existing countermeasures based on where and when they prevent, detect, and respond to the DDoS flooding attacks. Moreover, we highlight the need for a comprehensive distributed and collaborative defense approach.Our primary intention for this work is to stimulate the research community into developing creative, effective, efficient, and comprehensive prevention, detection, and response mechanisms that address the DDoS flooding problem before, during and after an actual attack. Currently, there are two main methods to launch DDoS attacks in the Internet. The first method is for the attacker to send some malformed packets to the victim to confuse a protocol or an application running on it (i.e., vulnerability attack). The other method, which is the most common one, involves an attacker trying to do one or both of the following:

I.disrupt a legitimate user's connectivity by exhausting bandwidth, router processing capacity or network resources; these are essentially network/transport-level flooding attacks or

II.Disrupt a legitimate user's services by exhausting the server resources (e.g., sockets, CPU, memory, disk/database bandwidth, and I/O bandwidth); these essentially includeapplication-level flooding attacks .

Today, DDoS attacks are often launched by a network of remotely controlled, well organized, and widely scattered Zombies1 or Botnet computers that are simultaneously and continuously sending a large amount of traffic and/or service requests to the target system. The target system either responds so slowly as to be unusable or crashes completely. Zombies or computers that are part of a botnet are usually recruited through the use of worms, Trojan horses or backdoors. Employing the resources of recruited computers to perform DDoS attacks allows attackers to launch a much larger and more disruptive attack.

Furthermore,it becomes more complicated for the defense mechanisms to recognize the original attacker because of the use of counterfeit (i.e., spoofed) IP addresses by zombies under the control of the attacker. Distributed Denial of Service (DDoS) flooding attack, intrusion detection systems, intrusion prevention systems distributed DDoS defense, collaborative DDoS defense. our paper and provides some insights for implementing a comprehensive distributed collaborative defense mechanism against DDoS flooding attacks.

LITERATURE SURVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above considerations are taken into account for developing the proposed system.A literature review is a body of text that aims to review the critical points of current knowledge including substantive findings as well as theoretical and methodological contributions to a particular topic. Literature reviews are secondary sources, and as such, do not report any new or original experimental work. Also, a literature review can be interpreted as a review of an abstract accomplishment. Most often associated with academic-oriented literature, such as a thesis, a literature review usually precedes a research proposal and results section. Its main goal is to situate the current study within the body of literature and to provide context for the particular reader.

Network Based Define Mechanism Countering the DDoS and DoS Problems:

As proposed by Tao Peng, Analyze the design decisions in the Internet that have created the potential for denial of service attacks. On the Internet, a DoS attack aims to disrupt the service provided by a network or server The original aim of the Internet was to provide an open and scalable network among research and educational communities. In this environment, security issues were less of a concern. the number of Internet users and the users' bandwidth have kept increasing dramatically. Unfortunately, the average security knowledge for current Internet users is decreasing while attacks are becoming more and more sophisticated.The techniques that have been proposed to detect and respond to these attacks. The attack classification criteria was selected to highlight commonalities and important features of attack strategies that define challenges and dictate the design of countermeasures. One important step to combat DOS attacks is to increase the reliability of global network infrastructure. More reliable mechanisms are needed to authenticate the source of Internet traffic, so that malicious users can be identified and held accountable for their activities.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A Taxonomy of DDoS Attack And DDoS Defense Mechanisms:

As proposed by Jelena Mirkovic, Peter Reiher This presents two taxonomies for classifying attacks and defenses and thus provides researchers with a better understanding of the problem and the current solution space. The attack classification criteria was selected to highlight commonalities and important features of attack strategies, The defense taxonomy classifies the body of existing DDoS defenses based on their design decisions.Taxonomies are to be used A map of DDoS research field. Exploring new attack strategies. DDoS benchmark generation. Common vocabulary. Design of attack classification solutions. Understanding solution constrains. Identifying unexplored research areas.They will highlight new features for classification. They will also offer new design features carrying their share of benefits and weaknesses. We expect these taxonomies to offer a foundation for classifying threats and defenses in DDoS field. As the field grows, the taxonomies will also grow and be refined..

A Novel Approach for Defending Against Distributed Denial of Service Attacks:

As proposed by Ruiliang Chen, Jung-Min Park, presents a novel countermeasure against Distributed Denial-of-Service (DDoS) attacks that we call the router port marking and packet filtering (TRACK), which includes the functions of both IP trackback and packet filtering. Unfortunately, finding effective solutions is a very challenging task this is due to several reasons. First, the Internet is an open platform. Second, in a DDOS attack, the number of zombie machines involved in an attack can reach several hundred or even several thousand. Third, IP source addresses are often forged (i.e., "IP spoofing") to amplify DDOS attacks and hide the actual attack source. Our simulation results show that TRACK has several advantageous features, which include: requires low communication and computation overhead, and is capable of supporting gradual deployment.

Ref 4: To Filter Or To Authorize: Network-Layer Dos Defense Against Multimillion-Node Botnets:

As proposed by X.liu,X.yang and Y.lu presents the design and implementation of a filter-based DoS defense system (StopIt) and a comparison study on the effectiveness of filters and capabilities.

Central to the StopIt design is a novel closed-control, open-service architecture: any receiver can use Stop It to block the undesired traffic it receives..We compare StopIt with existing filter-based and capability based DoS defense systems under simulated DoS attacks of various types and scales. Our results show that StopIt outperforms existing filter-based systems, and can prevent legitimate communications from being disrupted by various DoS flooding attacks. It also outperforms capability-based systems in most attack scenarios, but a capability-based system is more effective in a type of attack that the attack traffic does not reach a victim, but congests a link shared by the victim.

RELATED WORK:

The objective of IP trace back schemes is to find the origin of attack packets, or malicious clients. They can be further classified those of probabilistic packet marking and packet logging. Stefan Savage et al. [Sava00] proposes the very first packet marking scheme that adopts probabilistic packet marking for IP traceback, but its computation complexity of path reconstruction for multiple attackers is too high (O(n8), n is the number of attackers) to be practical. In [Song01] this problem is solved by assuming the pre-knowledge of upstream router map of the victim, which itself, however, is non-trivial. An algebraic method for trace back presented in significantly reduces the computation complexity of path reconstruction. However, it requires collecting considerably more packets for path reconstruction. Michael Go odrich [Good02] presents a scheme using large checksum cords to link message fragments, and the cords serve both as associative addresses and data integrity verifiers. The idea of checksum cords is similar to the XOR field in TRACK; therefore it also obviates the complex computation on matching multiple fragments. However, in [Good02] 12-bit additional space is used for cords and virtually nothing is left for other data coding. As a result, 8-bit ToS field is also used for the scheme and even more fragments are needed to be collected.

ALGORITHM:

In this chapter, we propose the algorithms for find the original attacker and login details of the user. First, we propose the algorithm for monitoring the system which was required for performing the login details of the users Next, we propose the algorithm for discernment the attacker site.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Following algorithms are used to monitor the application & network layer attacks.

Monitoring Algorithm:

- Input: system log
- Extract the request arrivals for all sessions, page viewing time and the sequence of N requested objects for each user from the system log.
- Compute the entropy of the requests per session using the formula:
- H(R) = -j Pj(rj) log Pj(rj)
- Compute the trust score for each and every user based on their viewing time and accessing behavior.

Detection Algorithm:

Input the predefined entropy of requests per session and the trust score for each user.

- Define the threshold related with the trust score (Tts)
- Define the threshold for allowable deviation (Td)
- For each session waiting for detection
- Extract the requests arrivals
- Compute the entropy for each session using (4)
- Hnew(R) = -j Pj(rj) log Pj(rj)
- Compute the degree of deviation:
- D = |Hnew(R)| - |H(R)|
- If the degree of deviation is less than the allowable threshold (Td), and user's trust score is greater
- than the threshold (Tts), then
- Allow the session to get service from the web server
- Else
- The session is malicious; drop it.

EXISTING SYSTEM:

Classification of various DDOS defense mechanism where and when they detect and respond to DDOS flooding attacks. More nodes in the Internet should be involved in preventing, detecting, and responding to DDoS flooding attacks. The main challenge in order to achieve this goal is that there should be some economic incentives among different service providers in order to achieve highly cooperative defense mechanisms.

Problems:

•It becomes more complicated for the defense mechanisms to recognize the original attacker.

•Disrupt a legitimate user's services by exhausting the server resources.
•Disrupt a legitimate user's connectivity by exhausting bandwidth, router
•processing capacity or network resources

PROPOSED SYSTEM:

To combining source address authentication, capability mechanisms and filtering mechanisms could be the most creative, effective, efficient and comprehensive prevention, detection and response mechanisms that the DDoS flooding problem before, during and after an actual attack .

Advantages:

•Aims to detect and respond (i.e., filter) to the attack traffic at the source and before it wastes lots of resources
•Easier and cheaper than other mechanisms in detecting DDoS attacks because of their access to the aggregate traffic near the destination hosts
•Aims to detect and respond to (i.e.,filter) the attack traffic at the intermediate networks and as close to source as possible.

IMPLEMENTATION:

Server:

Server module acts as the Intrusion Detection System. It consists of Effective Technique. In addition there is also Message Log, where all the alerts and messages are stored for the references. This Message Log can also be saved as Log file for future references for any network environment.

Client:

Client module the client can enter only with a valid user name and password. If an intruder enters with any guessing passwords then the alert is given to the Server and the intruder is also blocked In this client module the client can be able to send data. Here, whenever data is sent Intrusion Detection System checks for the file. If the size of the file is large then it is restricted or else the data is sent.

Attacker:

Attacker module attacker generates various types of attacks like sniffing, spreading virus, malware.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

These are identified by the MA approach and HIDS technique which is deployed in server.

MA Approach:

- The system is divided into independent layers that will help in efficiency and performance.
- The number of alerts will be reduced and the system will work in offline and online modes.
- The number of missing attack instances is extremely low or even zero in some of our experiments.
- If there is no intrusion, user will be logged in.
- The intrusions will be detected in user level, packet level & process level.
- When certain input is given the IDS will recognize the type of attack and pass it to all the subsequent layers.

Host-based intrusion detection system:

We designed and implemented a host-based intrusion detection system, which uses pattern matching and BP neural network as its detection methods. Firstly, the HIDS uses log files as its primary sources of information, and through three steps of pre-decoding log file, decoding log file, and analysis log file, it can effectively identify various intrusions. Secondly, based on BP neural network analysis technology and through establishment of system behavior characteristics profile in advance, the HIDS can identify intrusions by comparison with threshold.

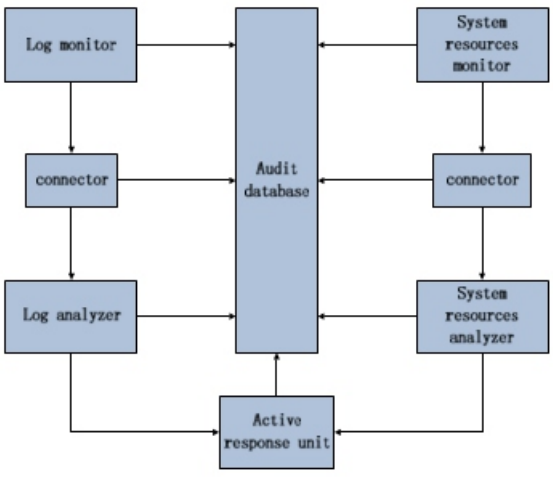

Figure1: Host-based intrusion detection system

1)Log monitor

Monitoring the log file, once the log change, log monitor will send events to the log analyzer immediately. Generally, we need to monitor three kinds of event logs: application log, security log and system log. We can add three XML nodes in the following configuration file.The node "localfile" represents the local file when system initialization. The node "location" represents file path in the disk. The node "log format" represents what type of the log. Log type includes event log, firewall log, SQL log. when initialize the HIDS, it will automatically load the above log files that need to be monitored. When finished the initialization work, the HIDS will open a demon, and the demon will check every log files to find whether there is changes in the log file. If there really exits a change, then the demon will report to the log analyzer.

2) System resources monitor

Monitoring the use of system resources, and sends the status of the system resources utilization to the system resources analyzer at regular time.

3) Connector

The connector is responsible for receiving messages from log monitor and system resources monitor, and sending these messages to log analyzer and system resources analyzer.

4) Log analyzer

Receiving events from the log monitor, match with the rule base to determine whether there is invasion, if there is invasion occurrence, report to the active response unit.

5) System resources analyzer

Receiving events form the system resources monitor, to calculate whether the abnormal state of current resources use and thus to determine whether the status is invaded, if it find there is invasion, report to the active response unit.

6) Active response unit

Receiving events from the log analyzer and system resources analyzer, decided to perform what kind of operation. Usually, the normal operations include notifying users, auditing, disconnecting from network and so on.

7) Audit database

Recording the entire process of intrusion detection, and the attack situation, prepare for use when necessary.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSION:

We have presented a comprehensive classification of various DDoS defense mechanisms along with their advantages and disadvantages based on where and when they detect and respond to DDoS flooding attacks. An ideal comprehensive DDoS defense mechanism must have specific features to combat DDoS flooding attacks both in real-time and as close as possible to the attack sources.

FUTURE WORK:

We strongly believe that combining source address authentication, capability mechanisms, and filtering mechanisms could be the most effective and efficient way to address the DDoS flooding attacks in a distributed cooperative/ collaborative DDoS defense mechanism. More development and deployment of distributed defense mechanisms from researchers and service providers respectively is what we expect to see in the near future.

REFERENCES:

[1]Autonomous Agents for Intrusion Detection, http://www.cerias.

[2]purdue.edu/research/aafid/, 2010.

[3]CRF++: Yet Another CRF Toolkit, http://crfpp.sourceforge.net/, 2010.

[4]KDD Cup 1999 Intrusion Detection Data, http://kdd.ics.uci.edu/ databases/kddcup99/kddcup99.html, 2010.

[5]Overview of Attack Trends, http://www.cert.org/archive/pdf/ attack_trends.pdf, 2002.

[6]Probabilistic Agent Based Intrusion Detection, http://www.cse.sc. edu/research/isl/agentIDS.shtml, 2010.

[7]SANS Institute—Intrusion Detection FAQ, http://www.sans.org/ resources/idfaq/, 2010.

[8]7 T. Abraham, IDDM: Intrusion Detection Using Data Mining Techniques, http://www.dsto.defence./gov.au/publications/ 2345/DSTO-GD-0286.pdf, 2008.

[9]R. Agrawal, T. Imielinski, and A. Swami, "Mining Association Rules between Sets of Items in Large Databases," Proc. ACM SIGMOD, vol. 22, no. 2, pp. 207-216, 1993.

[10]9 N.B. Amor, S. Benferhat, and Z. Elouedi, "Naive Bayes vs. Decision Trees in Intrusion Detection Systems," Proc. ACM Symp. Applied Computing (SAC '04), pp. 420-424, 2004.

[11]10. J.P. Anderson, Computer Security Threat Monitoring and Surveillance, http://csrc.nist.gov/publications/history/ande80.pdf, 2010. 11. R. Bace and P. Mell, Intrusion Detection Systems, Computer Security Division, Information Technology Laboratory, Nat'l Inst. of Standards and Technology, 2001.

[12]12. D. Boughaci, H. Drias, A. Bendib, Y. Bouznit, and B. Benhamou, "Distributed Intrusion Detection Framework Based on Mobile Agents," Proc. Int'l Conf. Dependability of Computer Systems (DepCoS-RELCOMEX '06), pp. 248-255, 2006.

[13]13 Y. Bouzida and S. Gombault, "Eigenconnections to Intrusion Detection," Security and Protection in Information Processing Systems, pp. 241-258, 2004.