Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 3, March 2017, pg.242 – 249

DDoS Attack and Review of Some Traditional and Current Techniques

Lavanya.A
(Assistant Professor, Department of Computer Technology, KG College of Arts and Science, Coimbatore
Email: lavanya.a@kgcas.com)

ABSTRACT: ***Distributed denial-of-service (DDoS) could be a rapidly growing drawback. The multitude and sort of each the attacks and the defense approaches is overwhelming. This paper is a survey on the drawback of denial-of-service (DoS) and Distributed Denial of Service (DDoS) attacks and projected ways in which to deal with it. we tend to describe the character of the matter and look for its root causes, more presenting temporary insights and steered approaches for defensive against DDoS. I point out each the positive and negative sides of every potential answer. Future work identifies and justifies open analysis problems. In conclusion we tend to provide a temporary outline of what has realistically been achieved thus way, as well as what the key missing components still. In this paper, we tend to gift a classification of out there mechanisms that are proposed in literature on preventing net services from attainable DDoS attacks and discuss the strengths and weaknesses of every mechanism.***

Keywords: DoS, DDoS, SYN, CERT, Prevention, Zombie

1. INTRODUCTION

A Distributed Denial of Service Attack or DDOS is a trial to create an online service untouchable to its meant users. Associate in nursing aggressor accomplishes this by flooding the target server with reserve network traffic within the kind of internet service requests. During this manner, the online service becomes bowed down responding to the requests and it slows down responses to valid requests from actual users.

As the name suggests these attacks are distributed, that means a bunch of computers meet multiple locations however suffering from same Trojan virus may be used. Like several alternative virus it's a computer virus that executes remote commands by the aggressor on a user's infected laptop, while not their data.

The Trojan infected user's laptop is named zombie and a network of zombies makes up a robotic network, known as a botnet. A botnet is liable for DDOS attacks. Your laptop might be a zombie i.e. a node of a bigger botnet while not your data. It's calculable that there are quite ten millions zombies worldwide.

An application level DDOS attacks the appliance layer of the online server infrastructure just like the login/registration page. Whereas Network level DDOS attacks flood the network infrastructure of an online service. Network level DDOS attack ar usually high in volume.

However. application level DDOS attacks are harder to sight as a result of the tally a typical user's activity like work in, work out, registration etc.

Either way, the DDOS attackers don't seem to be straightforward to spot as a result of they use a couple of dominant computers as handlers. They impart with zombie computers – usually via coding. Application level DDOS attacks target application vulnerabilities at the appliance / computer programs level; therefore it may be prevented by building secure applications. DDos attack mitigation needs expensive network security instrumentality. A managed international intelligence agency supplier offers this instrumentality on pay per use basis, therefore you'll be able to mitigate attacks while not finance network security hardware.

2. DDOS ATTACK VARIETIES

DDoS attacks area unit classified into the subsequent types:

2.1. Volume primarily based Attacks

This type of DDoS attack includes UDP floods, ICMP floods, and spoofed-packet floods. The DDoS attackers goal is to fill the information measure of the attacked web site, and conjointly the positioning won't settle for any response and it's measured in bits per second (Bps).

2.2. Protocol Attacks

This type of attack includes SYN floods, , Ping of Death, Smurf, fragmented packet attacks DDoS and additional. This kind of attack consumes actual server resources, or those of intermediate facility, like firewalls and cargo balancers, and this kind of attacks area unit measured in Packets per second.

2.3. Application Layer Attacks

The main goal of this kind attack is to crash the complete net server by causing the DDoS attack request to it explicit web site. It includes low-and-slow attacks, GET/POST floods and additional. This kind of attack is measured in Requests per second. This is one important type of attacks in the network. The origin server is crashed by using this type of attacks.

3. DDOS ATTACK TECHNIQUE

DDoS attack doesn't believe explicit network protocol or system weakness. It merely exploits the massive resource spatiality between the web and also the victim [7]. Since web design is open in nature, any machine hooked up to that is in public visible to a different machines hooked up to alter the communication. The hacker or offender community takes the unhealthy advantage of this open nature to get any insecure machine connected to the web.

The discovered machine is so infected with the attack code. The infected machine will more be wont to discover and infect another machine connected so on. The offender so bit by bit prepares AN attack network known as botnet. Relying upon the offensive code the compromised machines area unit known as Masters/Handlers or zombies. Hackers send management directions to masters, that successively management zombies. The zombies beneath the management of masters/handlers transmit attack packets as shown in Fig.3.1 that converge at victim to exhaust its resources. DDoS attack primarily targets victim's procedure or communicatory resources [11], like information measure, memory, CPU cycle, file descriptors and buffers etc.

A Distributed Denial of Service attack is often characterized as an occasion within which a legitimate user or organization is bereft of bound services, like web, email or network property, that they might usually expect to possess. DDoS is essentially a resource overloading drawback.

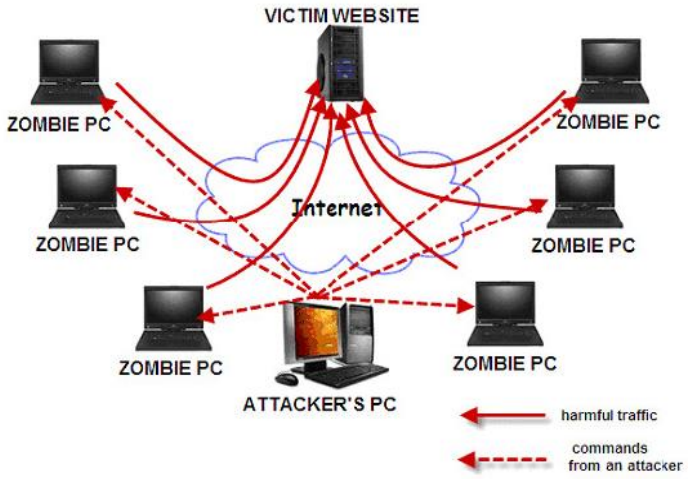

Figure 3.1 DDoS attack architecture

A Distributed Denial of Service attack is often characterized as an occasion within which a legitimate user or organization is bereft of bound services, like web, email or network property, that they might usually expect to possess. DDoS is essentially a resource overloading drawback. The resource are often information measure, memory, CPU cycles, file descriptors, buffers etc. The attackers bombard scare resource either by flood of packets or one logic packet which may activate a series of processes to exhaust the restricted resource [7]. In the Fig. 3.2 simplified Distributed DoS attack situation is illustrated. The figure shows that offender uses 3 zombie's to come up with high volume of malicious traffic to flood the victim over the web so rendering legitimate user unable to access the service.

How area unit DDoS attacks performed?

A DDoS attack is distributed in many phases. The offender initial recruits multiple agent machines.

This method is typically performed mechanically through scanning of remote machines, longing for security holes that may alter subversion.

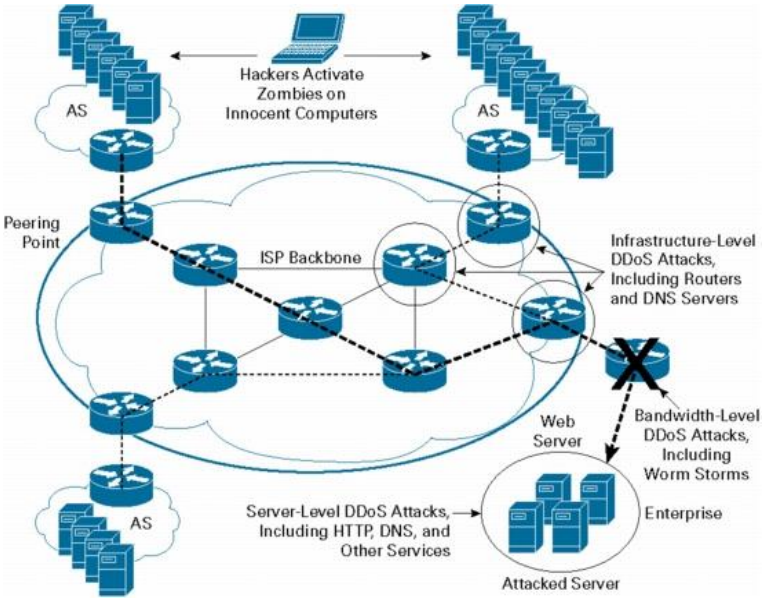

Figure 3.2 DDoS attack scenario

The discovered vulnerability is then exploited to interrupt into recruited machines and infect them with the attack code. The exploit/infect part is usually machine-driven, and also the infected machines are often used for more achievement of recent agents. Another recruit/exploit/infect strategy consists of distributing attack computer code beneath disguise of a helpful application (this computer code copies area unit. This distribution is often performed, for example, by causing E-mail messages with infected

attachments. Subverted agent machines area unit won't to send the attack packets. Attackers usually hide the identity of subverted machines throughout the attack through spoofing of the supply address field in attack packets.

3.1. Forms of attacks or DDoS attack classification:

In terms of the amount of malicious entities concerned in AN attack, we have a tendency to distinguish: Uni-source attacks – launched by and originating from one source; Distributed attacks – originating from multiple coordinated sources, though not essentially involving quite one malicious user.

3.2 DDoS attack taxonomy

The mobile ad hoc network has the following features

- It is separated from centralized network administration.
- Self-configuring nodes are also routers and bridges.

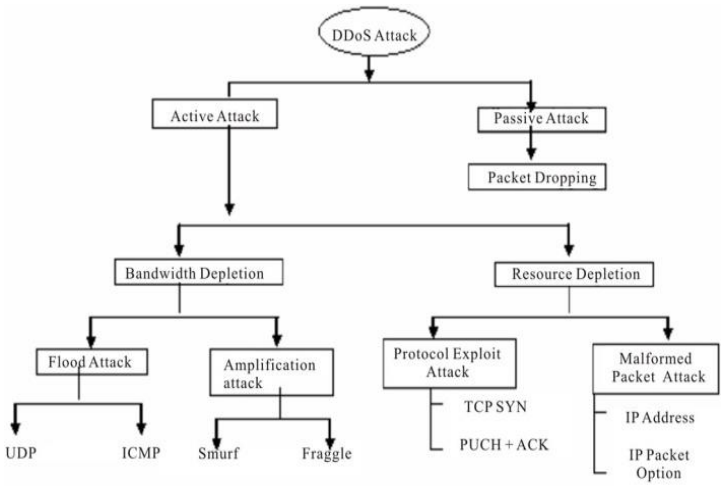

Figure 3.3 DDoS attack Types

- Self-healing during permanent re-configuration.
- Scalability incorporates the accumulation of more nodes.
- Mobility allows ad hoc networks produced on the flutter in any situation where there are numerous wireless devices.
- Flexible ad hoc can be provisionally setup at anytime, in any place.
- Lower getting-started costs due to distributed administration.

Vulnerabilities of the Mobile Ad Hoc Networks. Because mobile ad hoc networks (MANET) have more vulnerabilities and it is more crucial than the established wired networks, security is much more complex to maintain in the mobile ad hoc network than in the wired network, we discuss the various vulnerabilities that survive in the mobile ad hoc networks.

Need of Secure Boundaries

Nodes inside MANET have no restriction for nodes to connect, link, isolate and go in or outside of the network.

Dynamic Topology

The nodes are varying and joining the mobile network. It is unfeasible to record the freed accomplished by nods in a dynamic network.

Malicious from Compromised nodes Inside the Network Mobile ad hoc networks are highly at risk to routing attacks because of their dynamic topology and need of any infrastructure in the network. Each mobile nodes are autonomous units that can in join or

out join the network with independence, it is difficult for the nodes themselves to work out some efficient policies to prevent the malicious behaviors from all the nodes and it will get connect of the behavioral diversity of different nodes.

3.3 What makes DDoS attacks possible?

Current Inter-net style focuses on effectiveness in moving packets from the supply to the destination. This style follows the end-to-end paradigm: the intermediate network provides the clean minimum, best-effort packet forwarding service, departure to the sender and also the receiver the preparation of advanced protocols to attain desired service guarantees like quality of service, reliable and strong transport or security. The end-to-end paradigm pushes the complexness to finish hosts, departure the intermediate network straightforward and optimized for packet forwarding. There's one unfortunate implication. If one party in two-way communication (sender or receiver) misbehaves, it will do discretionary injury to its peer. Nobody within the intermediate network can step in and stop it, as a result of net isn't designed to police traffic. One consequence of this policy is that the presence of scientific discipline spoofing one. Another is DDoS attacks. The net style raises many security problems concerning opportunities for DDoS attacks.

Internet security is extremely mutually beneficial. DDoS attacks are unremarkably launched from systems that are subverted through security-related compromises. In spite of however well secured the victim system is also, its susceptibleness to DDoS attacks depends on the state of security within the remainder of the worldwide net[10].Internet resources are restricted. Every net entity (host, network, service) has restricted resources that may be consumed by too several users. Intelligence and resources aren't collocated. An finish-to-end communication paradigm light-emitting diode to storing most of the intelligence required for service guarantees with end hosts, limiting the number of process within the intermediate network so packets might be forwarded quickly and at negligible value. At identical time, a need for big outturn light-emitting diode to the planning of high information measure pathways within the intermediate network, whereas the tip networks endowed in exactly the maximum amount information measure as they thought they could would like.

Thus, malicious shoppers will misuse the abounding resources of the unwitting intermediate network for delivery of diverse messages to a less provisioned victim. Answerableness isn't implemented.IP spoofing provides attackers a robust mechanism to flee count ability for his or her actions, and generally even the means that to move attacks (reflector attacks [11], like the Smurf attack [12]).Control is distributed. Net management is distributed, and every network is run consistent with native policies outlined by its house owners. The implications of this are several. There's no thanks to enforce international preparation of a selected mechanism or security policy, and because of privacy considerations, it's typically not possible to analyze cross-network traffic behavior.

4. SUGGESTED GENERAL REMEDIAL APPROACHES

Naturally, like all kinds of security breach, there are general approaches for handling the attack–eliminating it utterly, mitigating the results of the attack on the victim, and discouraging the wrongdoer. Those don't have to be compelled to be exclusive to 1 another, however will and may be used as complementary, whenever doable.

we are going to inspect every strategy individually in additional detail, considering the variability of solutions projected in literature and mentioning what we expect area unit the sturdy and weak sides of every.

4.1 Eliminating the chance of attack:

This is out and away the foremost fascinating strategy for "defending" against any reasonably security attack. Sadly, the problems area unit rather sophisticated and extremely rarely will a threat be utterly eliminated. A lot of typically that not, this might be the case with scams, that extremely solely have transient effects.

4.1.1 Allowing connections solely to sure shoppers.

This is clearly the foremost conservative approach to communication and per se it's the very best degree of averting security threats. Such an answer is excusable for preparation solely in closed and special -purpose (e.g. military) environments. It's inherently unsuitable associated incompatible to an open communication system like the net. A renowned downside with closed environments is that outside intrusions area unit each not expected and ordinarily not anticipated. So, the amount of state for a security breach, ought to it ever occur, is incredibly low and therefore the injury grows proportionately high.

4.1.2 Out-of- band communication.

This is not a unique plan, particularly within the phone network field. The concept is that management and information signals would travel physically on separate wires and so any interference and potential confusion is excluded. This wasn't the case with the phone networks in Sixties, once in -band communication was in use. One may whistle into the phone receiver and underneath bound favorable circumstances (the right wavelength and amplitude) the signal, that very was simply information, may be understood as an impact signal (e.g. a free decision, etc.).Schneider claims that out -of-band communication wouldn't solely alleviate the present issues with denial of service attacks, however conjointly aid in defeating alternative inherent celebrated security issues within the net

4.2. Mitigating the impact of the attack on the victim:

While the utmost goal is to avoid being attacked, once and if this happens it's extremely desirable to be ready to sustain some level of (degraded) performance throughout the high load, even before the particular detection of associate degree attack. The subsequent approaches try and attain this goal in numerous ways in which

4.2.1. Securing all computers on a network:

Achieving that will render the existence of zombies' not possible associate degreed thus an offender would be reduced to having the ability to mount solely a uni-source attack. Additionally, scientific discipline trace back schemes would directly cause the attacker's weapon machine that successively would each scale back the management overhead within the post-mortem tracing method and function a rational motive for the offender to start out within the initial place.

4.2.2. Ingress filtering.

This approach is describe details in next section targeted at reducing or fully eliminating the power to forge supply addresses, that if accomplished would ultimately end in abundant easier tracing back to truth supply of associate attack and in and of itself would function a major deterrent for offender.

4.2.3 Client "puzzles" before committing resources.

The idea, recently projected by 2 RSA researchers, is to distribute science puzzles to purchasers (whether real of fake) once the server comes fraught from high load [20]. Resources are solely committed to connections that the purchasers have with success solved and submitted their puzzles inside a timeout amount.

This strategy would serve 2 purposes: damping (i.e. spacing) the consumer requests and permitting the server to control the amount of purchasers establishing connections with it by causing out tougher puzzles (depending on the load conditions and actual variety of resource slots available), and therefore experiencing sleek degradation in performance.

The main disadvantage of consumer puzzles, admitted by the authors themselves is that the demand for special client-side code (either engineered into the browser or distributed in some completely different way). Another disadvantage, remarked by Schneider [21] is that consumer puzzles though cheap as associate approach for addressing uni-source attacks, fall to distributed denial of service attacks, since generation and distribution of consumer puzzles may be a denial of service attack in its title. Overall, it appears that the approach is viable, however ought to solely be used with caution and together with different such promising approaches

4.2.4 Use increasingly stronger authentication:

The idea here is to once more avoid committing server resources early, attempting to instead incrementally gain confidence within the identity of the consumer and solely "promising" resources, proportionate to the amount of assurance the server has at anybody purpose throughout the communication . Beginning with weak authentication initial (e.g. a cookie) and upon receiving feedback (i.e. consumer responding and following the requested steps), the server increasingly chooses stronger authentication up to the purpose of doing a rich authentication (e.g. digital signature), at that purpose the important oral communication might begin. Note that "strong authentication from the beginning would be a hook for denial of service attacks".

This approach in itself doesn't forestall malicious parties from launching attacks; however it considerably raises the bar for doing that, creating the attackers work tougher by initial having to eliminate the weaker authentication. In contrast to the approaches

for fully eliminating the threat of attacks, those for truly addressing it are in our opinion quite cheap and realistic, albeit none of them offers an entire set of strategy on the way to mitigate denial of service attacks.

5. CONCLUSION AND FUTURE SCOPE

Complete elimination of denial of service threats is unworkable given the present web infrastructure. Internet, being associate open setting with no limits set in stone on the amount of users, is inherently susceptible to attacks of the denial of service sort. There are no thanks to predict the parameters of the biggest doable flood. Within the phone network the infrastructure is ready and it is known what the provisions ought to be so as to cut back the risks to acceptable levels. Such a provision is hardly conceivable within the web, as it is. Mentioned approaches and methods may well be combined to supply numerous levels of mitigation of attacks and deterrence for the attackers, however complete set of tools for defense area unit presently not on the market each within the educational and industrial communities. One doable high-investment resolution can be during a new web wherever answerability has higher price. Such associate approach would be extremely fascinating and standard among the businesses doing commerce on the web. Whereas short-run defenses may well be found within the literature, there's a involve longer-term ways against denial of service attacks. A distributed kind of DoS attack known as DDoS attack that is generated by several compromised machines to coordinately hit a victim. DDoS attacks area unit adversarial and perpetually evolving. Once a selected reasonably attack is with success countered, a small variation is intended that bypasses the defense and still performs a good attack.

In this paper, I coated a summary of the DDoS drawback, available. Defense challenges and principles, and a classification of obtainable DDoS hindrance mechanisms. This provides higher understanding of the matter and allows a security administrator to effectively equip his arsenal with correct hindrance mechanisms for fighting against DDoS threat. The most drawbacks are that there are a unit stills several insecure machines over the web which will be compromised to launch large-scale coordinated DDoS attack.

REFERENCES

[1] Akamai‘s Prolexic Quarterly Global DDoS Attack Report Quarter 1 of 2014

[2] Computer Emergency Response Team, “CERT advisory CA-2000.01 Denial of service developments”, Jan 2000. (http://www.cert.org/advisories/CA-2000-01.html)

[3] The Standard Performance Evaluation Corporation, “SpecWeb96benchmarkresults”, 1998.(http://www.specbench.org/osg/web96/results).

[4] John D. Howard, “An analysis of security incidents in the Internet”, PhD thesis, Carnegie Mellon University, 1998.

[5] Arbor’s ninth Annual Worldwide Infrastructure Security Report (WISR), released march ,2014

[6] K. Kumar, R.C. Joshi and K. Singh, “An Integrated Approach for Defending against Distributed Denial-of-Service (DDoS) Attacks”, iriss, 2006, IIT Madras

[7] J. Mirkovic, P. Reiher, “A Taxonomy of DDoS Attack and DDoS defense Mechanisms,” ACM SIGCOMM Computer Communications Review, Volume 34, Issue 2, pp. 39-53, April 2004.

[8] B. Wang, H. Schulzrinne, “Analysis of Denial-of-Service Attacks on Denial-of-Service Defensive Measures”, GLOBECOM 2003, pp. 1339-43

[9] CERT CC. Trends in Denial of Service Attack Technology, October 2001.http://www.cert.org/archive/pdf/DoS trends.pdf.

[10] V. Paxson. An analysis of using reflectors for distributed denial-of-service attacks. ACM Computer Communications Review (CCR), 31(3), July 2001.

[11] CERT CC. Smurf attack. http://www.cert.org/advisories/CA-1998-01.html.

[12] Oliver Spatscheck and Larry Peterson, “Defending against denial of service in Scout”, In proceedings of 3rd USENIX/ACM Symposium on OSDI, pp.59-72, Feb 1999.

[13] Charalampos Patrikakis, Michalis Masikos and Olga Zouraraki, “The Internet Protocol-Vol 7, Number 4”.

[14] 15.Jelena Mirkovic,Sven Dietrich,David Dittrich,Peter Reiher, “Internet Denial of Service: Attack and Defenses Mechanisms

[15] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, “Practical network support for IP trace back”, Technical report UW-CSE-00/02/01, In submission to SIGCOMM’00, Feb 2000

[16] Roger M. Needham, “Denial of service: an example”, Communications of the ACM, vol.37, No.11, pp.42-46, Nov 1994.

[17] Li Gong and Paul Syverson, “Fail-stop protocols: An approach to designing secure protocols”, 1998.

[18] Vern Paxson, “Bro: a system for detecting network intruders in real-time”, in proceedings of the 7th USENIX Security Symposium, San Antonio, TX, Jan 1998.

[19] Ari Juels and John Brainard, “Client puzzles: A cryptographic countermeasure against connection depletion attacks”, In proceedings of the 1999 Networks and distributed system security symposium (NDSS’99), Internet society, Mar 1999.(http://www.isoc.org/ndss99/proceedings)

[20] Bruce Schneier, “Distributed denial of service attacks”, Crypto-gramnewsletter(http://www.counterpane.com/crypto-gram-0002.html#DistributedDenial-of-ServiceAttacs)

[21] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson, "Practical network support for IP trace back", Technical report UW-CSE-00/02/01, In submission to SIGCOMM'00, Feb 2000
[22] X. Geng, A.B. Whinston, Defeating Distributed Denial of Service attacks, IEEE IT Professional 2 (4) (2000) 36–42.
[23] Felix Lau, Rubin H. Stuart, Smith H. Michael, and et al., "Distributed Denial of Service Attacks," in Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics, Nashville, TN, Vol.3, pp.2275-2280, 2000.

