International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 3 Issue: 3 1432 - 1435

Defense Mechanisms for Bandwidth DDOS Attacks and Its Issues

Basavaraj Havale
P.G Student: I.S.E Dept.,
National Institute Engineering,
Mysore, India
bvhavale90@gmail.com

Prajakta Madankar
Assistant professor: I.S.E Dept.,
National Institute Engineering,
Mysore, India
prajakta270976@yahoo.com

Nagaveni Mallikarjun
P.G Student: I.S.E Dept.,
National Institute Engineering,
Mysore, India
nagaveni1292@gmail.com

***Abstract*—**The Development of the Information Technology enables delivery or processing information to the end-users with respect to the capacities of the Internet architecture. The evolution and development of the technology impacts the nature and conflict of war such as threats emanating from cyberspace. The Distributed Denial-of-service (DDoS) phenomenon poses a serious threat to stability and reliability of the Internet Architecture as long as there is a rise in the internet population. The DDoS attack involving large number of compromised machines affects the legitimacy service to the end-users. In this paper, we have surveyed the ongoing various approaches for mitigating DDoS attacks and operational issues, benchmark challenges and political concerns.

Keywords- *Denial of service, DDoS, BDDoS Mitigation, Operational issues, Benchmark suite, Political concern.*

*****

I. INTRODUCTION

The Development of the Internet and low-cost wireless communication has made more dependent in our daily activities. The growing demand of various services range can be communication, e-commerce, and data-storage. Users are accessing these services through mobile phones, computers, PDA, etc.

These services are indispensible in today's modern world and the credibility of providing quality service to the end-users through the internet is difficult as the numbers of users are growing rapidly. The growing demand can be satisfied through increasing the network infrastructure and these are vulnerable to various threats including Denial-of-Service (DoS).

The Distributed Denial of Service (DDoS) can be described as presence of large number of compromised computers with co-ordinated effort involving disrupting the services and thus consuming bandwidth. Thus the term Bandwidth Distributed Denial of service (BDDoS) came to light in the field of Internet. We shortly discuss the main features to differentiate between different attackers and some of the proposed mechanisms operational issues, benchmark-suite and political issues.

In Bandwidth Distributed Denial of Service, attack is carried out by many compromised machines through Zombies, puppet, and others to disrupt the legitimate traffic by consuming relatively large bandwidth eventually leads to denial of service.

In the Internet infrastructure, there is a greatest possible number or limit for the network interface bandwidth of the server when the number of data packets exceeds this limit, congestion occurs and effective responses are minimized. According to recent survey, Bandwidth Distributed Denial of Service's are the most frequently used method. According to[1],BDDoS reached volume of 100 Gbps[1] and according to[3],recently even reached 300Gbps,according to[2],these attack targeted 60-86.5% to mitigation infrastructure. The various reports demands for dynamic defense methodologies like real-time traffic monitor because, attackers are becoming more organized and sophisticated eventually resulting in-stability of network infrastructure.

To overcome problem, researchers, analysts, scholars need not be dependent on one defense-mechanism instead combining various approaches and making affordable-changes in network infrastructure may result in reducing attacker's rate.

II. DOS ATTACK CLASSIFICATION

DoS attacks can be classified into five categories [4] based on the attacked protocol level.

A. Network-based DoS attack

These include attacks that arise in the network devices due to the malformed packets from numerous puppets, zombies or bots interact with network protocol or application software. The victim's hardware like printers or other networking devices are damaged so badly that leads to replacement or reinstallation of whole system. They consume extra memory utilization, CPU processing capability eventually leading to denial of service. E.g. maxSYN attack.

B. OS level Dos attack

These include attacks on operating system with massive ICMP/IGMP protocols. The operating system gets crashed due to bug in the TCP/IP fragmentation reassembly. They relatively consume large resources by including large number of smaller requests than maximum standard size available

 ISSN: 2321-8169
1432 - 1435

towards victim eventually leading to often system crash. E.g. DNS amplification attacks.

C. *Application-based attacks*

These include attacks on victim's machine by injecting malicious URLs, bugs, viruses in network applications. The server-running software is exploited by buffer overflow, large number of logs in disk space depleting its connection bandwidth. They take advantage of these cases leading to out of service. E.g. XDoS (or XML DoS)

D. *Data flooding attacks*

These include attacks on victim machine by consuming the bandwidth available through sending large amount of data packets, meaningless request. An attacker disrupting victim's network bandwidth in the connectionless scenario such as UDP flood attacks, they reduce victim's available bandwidth eventually leading to system crash, out of service. E.g.Ping flood.

E. *Protocol manipulation attacks*

These include attacks that exploit legitimate victim's protocol behavior by spoofing IP protocol. An attacker need to have strong zombie with administrative privileges thus avoid detection by manipulating source IP address, known as spoofing. They take advantage by making forged request towards victim machine to consume available resources eventually leading to denial of service. Eg:IP address spoofing.

III. DEFENSE MECHANISMS AND OPERATIONAL ISSUES

Table I: Comparison between BDDoS Defense Mechanisms [5]

Mechanism	Response	Location	Infra. Adapt.	Cooperation
Ingress Filter	filter	router	configuration	standalone
ACL	filter	router	configuration	standalone
RTBH	filter	router	configuration	inter AS (BGP)
Capabilities	rate-limiting	dst,router,src	router software	inter AS
PSP	rate-limiting	router	router software/IP fields	intra AS
Pushback	filter	router	router software	inter AS
BTT	rate-limiting	router	configuration	inter AS
RON	detour	src,cloud	end-hosts software,cloud	end-host and overlay
SOS	filter	src,cloud	end-hosts software,cloud	end-host and overlay
Scrubbing	filter	router,cloud	configuration,cloud	inter AS(BGP),cloud
QoSoDoS	break-through	src,dst	end-hosts	end-hosts
LOT	filter,rate-limiting	router	router software	inter LOT-routers

A. *Ingress and Egress Filtering*

Ingress and Egress Filtering [6] provides filtering mechanism based on certain criteria at the router to detect DDoS attack. Ingress mechanism disallows incoming IP address that does not match with legitimate traffic flow whereas Egress filtering ensures only legitimate IP address leaves at the router. If the packets pass the criteria, they are routed inside and outside of the sub-network from which they originated.

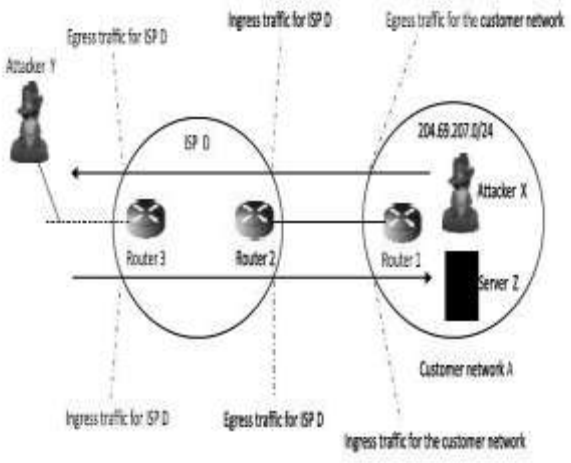

Fig 1.An Example of Ingress Filtering and Egress Filtering [6]

Sometime Ingress mechanism is ineffective for Mobile-IP using genuine IP address connecting Foreign Agent cannot get filtered and Egress filtering do wastage resources if the packet arise from same domain.

B. *Pushback Architecture*

In Pushback Architecture [7], idea is to mitigate rate-limiting at upstream routers by a pushback message involving a rate-limiting value along the path to destination, As DDoS attacks are considered traditionally as Congestion-Control problem, the Pushback Architecture allows fair use of available resources mitigating Bandwidth Consumption attacks

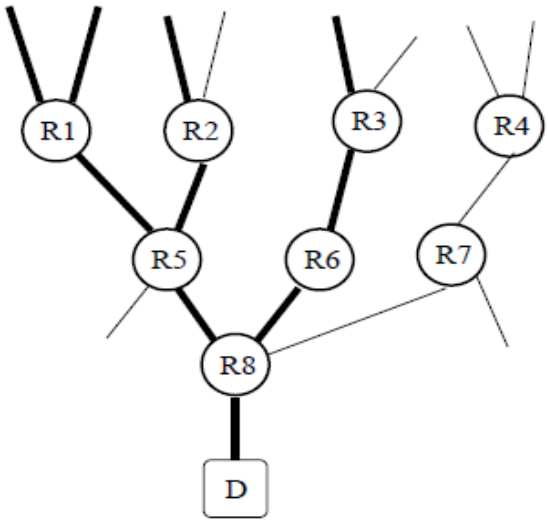

Fig 2. A DDoS Attack In Progress. [7]

Under DDoS attack the packets arriving at routers along the path of destination involves dropping of packets from illegitimate flows using end-to-end congestion control algorithms. The pushback is not suitable against uniformly distributed attacks.

C. Secure Overlay Services (SOS)

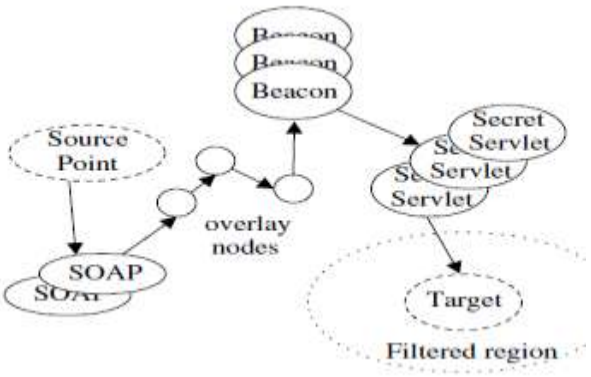

Fig 3: Basic SOS Architecture. [8]

The SOS architecture [8] provides user's authorized flow of packets through the overlay network using combination of nodes to the target. This Architecture involves intensive filtering across nodes or links to prevent illegitimate traffic flow mitigating the attacks.

Secure overlay Services (SOS) Architecture is a distributed system, does not require modification of current infrastructure. However the presence of overlay infrastructure, updated software and protocols related to client and server is required and not suitable for public server systems.

D. Stateless Internet Flow filter (SIFF)

SIFF, a Stateless Internet Flow Filter[9], which provides an end-host to selectively stop individual flows from reaching its network without including ISP's collaboration and secure overlay infrastructure to mitigate DDoS flooding problem.

Stateless Internet Flow filter(SIFF) provides features such as Client/Server privileged communication, Recipient controlled privileged flows, Limited spoofing of source addresses, No end-host/ISP or inter-ISP cooperation, No intra-ISP cooperation, No intra-ISP cooperation, Small-constant state at routers small, per-packet processing at routers, Backward Compatibility. However, SIFF must deal with marking space in the IP header, routers mark at every packet and short-term route stability.

IV. BENCHMARKS

DDoS defense includes typical benchmark suite [10] contains typical attack scenarios and comprehensive suite that influence defense's performance. It facilitates interaction of select feature instead of performing exhaustive testing in multi-dimensional space.
Keeping in mind that our existing methods have some limitations because they rely on limited number of traces available to public, as both defense and attacks evolve, designing these benchmark suites is an on-going approach for evaluating proposed DDoS defenses.

The major technical challenges for designing a benchmark suite are as follows (1) To generate typical test suites, gathering enough trace and topology data (2) Designing and understanding comprehensive manageable test cases understanding through the interaction between the traffic, topology and resources (3) Evaluating each application by a success criteria (4) To define a short, meaningful collection result strategies, (5) To update benchmarks.

IV. POLITICAL ISSUES

In the Twenty-first century, the growth of the Information and Communication Technology (ICT) are inherently dual-use in nature the same technology that supports flow of information in matter of few seconds providing robust e-commerce activities can also be used to threaten peace, security of the nations.

The sphere of political targeted attacks are growing, given the fact that the internet has become major communication tool for raising voice from various groups involving political parties, news-media, opposition and others. The targeted victims may also involve major ecommerce-sites, financial firms, government-assets.

Historically the political issues [11] can be,

- Revenge, fame, money, activism, Ideological belief, Intellectual challenge, patriotism.
- Several Govt. officials involving in crimes, corruption in published articles, recordings.
- To engage as proxies in disrupting online activities of individuals, groups, organizations on behalf of others.
- Disrupting activities of politicians, groups thus the integrity of fair-elections.

These political issues can be also aroused due to the fact that some organizations, officials are hesitant to provide details of Security-related incidents making them to public. Thus professionals, researchers involving in these studies may struggle to improve defense mechanisms without knowing the causes affecting them, and thus intensifying future attacks.
The governments, political targets infrastructure must co-operate with third party system for continuity and deployment, training of commercial tools available to overcome these attacks. Further collaboration among like-minded partners is important measure to improve information security.

V. CONCLUSION AND FUTURE ENHANCEMENT

Due to the Internet usage expand, vulnerability to crucial information Structure is growing rapidly. Bandwidth Distributed Denial of Service (BDDoS) attacks poses such a serious threat results in unavailability of service leading to disastrous effects in future. Combining various Defense mechanisms like source-address authentication, filtering mechanisms, capability mechanisms provide effective and efficient to address BDDoS Threats. The Development of these attacks, classification of defense mechanisms is an ongoing approach may still include additional weakness, can be overcome by effective communication, coordination among

Researchers, Scholars,Anylsts and uniform legal measures to cyber-crime with multi-nationals.

REFERENCES

[1]. Arbor Networks. Worldwide Infrastructure Security ReportsSeries(2005-2012). Http://Www.Arbornetworks.Com/Report.
[2]. P.T.Inc. "Prolexic Attack Report, Q3 2011–Q42012,"
[3]. M. P. Cloud flare. The Ddos That Almost Broke The Internet.Http://Blog.Cloudflare.Com/The-Ddos-That-Almost-Broke-The-Internet.
[4]. Christos Douligeris, Aikaterini Mitrokotsa, Ddos Attacks And Defense Mechanisms: Classification And State-Of-The-Art, Department Of Informatics, University Of Piraeus, 80 Karaoli And Dimitriou Str, Piraeus 18534, Greece, October 2003.
[5]. Moti Geva, Amir Herzberg, Yehoshua Gev ,Bandwidth Distributed Denial Of Service :Attacks And Defenses, Computer Science Department, Bar-Ilan University Ramat Gan 5290002, Israel.
[6]. Hakem Beitollahi,Geert Deconinck Katholieke, Analyzing Well-Known Countermeasures Against Distributed Denial Of Service Attacks.,Universiteit Leuven, Electrical Engineering Department, Kasteelpark Arenberg 10, Leuven, Belgium.
[7]. John Ioannidis,Steven M. Bellovin, Implementing Pushback: Router-Based Defense Against Ddos Attacks,AT&T Labs Research.
[8]. Angelos D,Vishal Misra,Keromytis Dan Rubenstein,SOS: An Architecture For Mitigating Ddos Attacks.
[9]. Abraham Yaar,Adrian Perrig,Dawn Song,SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks, Carnegie Mellon University.
[10]. Jelena Mirkovic, Erinc Arikan,and Songjie Wei, Benchmarks for DDoS Defense Evaluation.
[11]. Jose NAZARIO, Politically Motivated Denial of Service Attacks Arbor Networks, USA.