ACSIJ Advances in Computer Science: an International Journal, Vol. 4, Issue 1, No.13 , January 2015
ISSN : 2322-5157
www.ACSIJ.org

ACSIJ
WWW.ACSIJ.ORG

The Innocent Perpetrators: Reflectors and Reflection Attacks

Srinivas Arukonda[1], Samta Sinha[2]
[1] Computing Science and Engineering, Galgotias University Greater Noida, Uttar Pradesh, India
Srinivas.arukonda@gmail.com

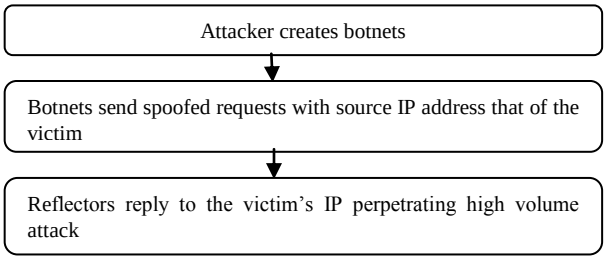
[2] Computer Science and Engineering, Galgotias University Greater Noida , Uttar Pradesh, India
Samta1sinha@gmail.com

Abstract
In this paper we make a comparable study of the various types of Reflector Denial of Service attacks popularly known as DRDoS attacks. We discuss their cause, effects, defense mechanisms proposed so far, the effectiveness of these defense mechanisms and their future relevance. We have also shown how reflection attacks are a potential threat to the cloud which is one of the most popular and highly evolving arenas in the Internet.
Keywords: *DRDoS, reflector, cloud, attacks*

1. Introduction

1.1 DRDoS Attacks

Distributed reflector denial of service attacks are DDoS attacks with a more sophisticated and lethal visage. Figure 1, [1] represents the strategy of reflector attacks. In reflector attacks the attacker tries to sabotage the victim's resources by compelling third party innocent servers or routers to launch a distributed flooding attack. Any server which responds to a request is a potential reflector [1].Reflection attack steps involve the following course of actions:



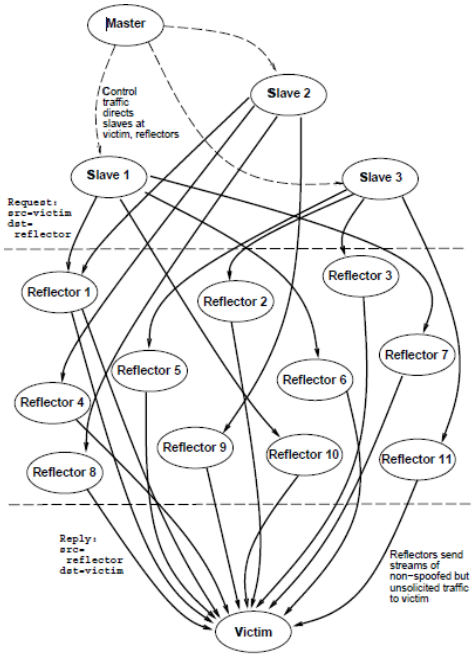


Fig 1 Representation of Reflector attack

Another variation of reflector attack is amplification attack. In case of amplification attacks the request to be sent to the reflector is so selected that the reply is many times magnified in terms of size (measured in bytes) in comparison to the request. Thus amplification means magnification of length of reply packet and sometimes magnification in bandwidth utilized in sending the request packet.

1.2. Rise of DRDoS Attacks

DRDoS came into light around 2000 and culminated with an attack on Spamhus in March 2013 which saw peaks of 300 Gbps. It intensified with 421 Gbps in the early 2014.
In Feb 2014 EU and was hit by attack up to 400Gbps abusing the Network Time Protocol. About 13 massive

SNMP attacks were observed in May 2014 bringing down popular gaming websites.

DRDoS has evolved like a giant in the Internet community devouring services as means of ransoms, for disproving government policies, stealth of passwords, bank frauds and every branch and leaf of the mighty Internet tree. Some factors that contribute to it's popularity as an attack tool include

1. Free availability of attacking tools
2. Ease of launching attack
3. Severity of damage it causes in comparison to simple attack efforts
4. Damages not only the intended server but the entire network

1.3. Related Works

Several such surveys as ours have been produced in the past [1,2,4,6].They have dealt with the attack methodologies , methods of DRDoS detection, the percentage of vulnerable reflectors in the Internet , characteristics of vulnerable reflectors, some have discussed the various defense mechanisms proposed so far. However our survey differs from them in that we present a comparative description of attack strategies, detection and defense considering recent attack domain that is cloud.

2. Attack Strategies

In table1 we present a comparison of the vulnerabilities abused in various types of recently abused protocols in DRDoS attacks and their possible amplification factors.
Here Bandwidth Amplification Factor is represented by BAF and N is the number of reflectors.

Table 1: Protocols and Vulnerabilities for reflector attacks

ATTACK TYPE	***VULNERABLITY ABUSED***	***BAF***	***USE OF THE PROTOCOL***
NTP Reflection	A "get monlist" spoofed request with victim's address is channeled to vulnerable NTP server.	556.9	For synchronizing time in the Internet. Administrators can query about no of connected clients
DNS Reflection	A spoofed DNS name resolution query which results in large sized reply like DNSSEC,ANY,EDNS is channelized to open DNS servers or authoritative name servers	28-54	For mapping domain names to IP addresses and vice versa
SNMP (v1 and v2)Based Reflection	Botnets channelize a spoofed SNMP "GetBulkRequest" query with default community string which when matches with that of devices listening for SNMP query are replied to the intended victim	6.3	Used by system administrator to know the status of various devices on remote hosts of his network, which includes Internet camera, firewalls, routers and so on .
SSDP Based	SOAP (employed for delivering control messages in UPnP devices) is forged to create amplified replies	30.8	SSDP permits networked devices such as personal computers, internet gateways, Wi-Fi access points to discover each others' presence on network and establish functional network service for data sharing, communication and entertainment[11]
Smurf	A spoofed ICMP request packet is broadcast on a network.	N	ICMP protocol is used for error detection and control on a network
KAD	Sybils (peers forging multiple identities) reply to IP of the intended victim	16.3	It is a peer to peer DHT routing protocol
Bit torrent	Tracker, the central server is compromised and several peers are instructed to connect to victim at the same time during announce time.	3.8	Is a peer to peer file sharing system used for sharing large files on the Internet
CHARGEN	Adversary spoofs the IP address of the victim and redirects CHARGEN traffic towards it.	358.8	It is used for testing, debugging and management of network
TCP SYN	SYN requests with spoofed IP of victim is sent to various servers which in turn reply with SYN ACK message to victim	N	For initiating connection in connection oriented networks before message transfer

3. Attack Detection:

The approach for detection of reflection attacks consists of the following two major aspects.
Identification that the system is under attack as soon as possible

Differentiating between flash crowd and DDoS attack traffic

3.1. Distinguishing Between Flash Crowd and Attack Traffic

Detecting reflector attacks is rendered more difficult due to legitimate nature of attack traffic. The high volume of traffic generated by the reflector are innocent reply packets which are not even spoofed this type of traffic may appear occasionally on websites therefore differentiating between flash crowds and attack traffic is a significant aspect of DRDoS detection scheme. Several approaches have been proposed and we will be discussing a few recent ones.

In one of the approaches for discriminating between flash crowd and DDoS attack traffic in cloud environment[2]a credit based approach is employed where users are assorted into three classes which are well reputed, reputed and ill reputed based on credit. For detection of attack traffic they exploit the fact that malware possessing systems behave in likeness.

Another approach for differentiating flash crowds and attack traffic [3] uses concept of entropy variation in Internet Threat Monitors (ITMs), where ITMs are dispersed throughout the Internet for analyzing traffic attributes and periodically sending them to specialized data centers for evaluation.

They also propose to prioritize private users' (registered) request for monitoring over that of public (unregistered) users'.

Among other approaches is the one which proposes a parametric [4]distinction between flash crowd and DDoS traffic with parameters into consideration like rate of incoming traffic, change in rate of new IP address, and distribution of requests among source IP address .

3.2 DRDoS Detection Schemes

Many schemes have been proposed for Detecting reflector attacks. We will discuss some recent ones.

Due to the large scale DRDoS attacks scalable systems for dealing with attack traffic are difficult to obtain so Hadoop is being widely proposed by many researchers recently. Hadoop is a cost effective and easy implementable set of tools and has the capability of handling multi-tera bytes of data. In one of the papers Hadoop based platform [5] called MATATABI has been proposed. They have dealt with DNS amplification attacks, NTP reflection attacks.

Since reflector DDoS attacks are distributed, strong recommendations for distributed that is collaborative detection and defense schemes have been made. One such scheme has been proposed by [7] where reflectors keep an eye on traffic activity on the network. They use soft computing technique namely machine learning algorithm to detect abnormality in the network traffic. If any such activity is observed the reflector sends a warning message to intended victim wherein the warning includes details about the threat so observed.

IP spoofing is the root cause of all reflector attacks and schemes for dealing with spoofing continue to be proposed. A novel scheme for IP trace back has been proposed in one of the papers [6].They tend to generate fingerprint based on the static characteristics of packet and first eight bytes of the payload. They use response 1, Nonce of secure neighbor protocol as parameters to the network model for the traceback system they have designed.

4. Defense Mechanisms:

DRDoS attackers in recent incidents especially from 2013 till date have been found to abuse vulnerabilities in old preexisting protocols like NTP, DNS SNMP and so on. Therefore the most practical solution adapted by the Internet community is patching the vulnerabilities in these protocols by disabling certain features for common users, by bringing on more secure versions or disabling the support of the protocol completely from their products (O.S etc.). Some of such adaptive techniques recommended for vulnerable protocols include:

In case of NTP it is recommended [8] that NTP server should use version 4.2.7 p26 or later versions, out of date NTP daemons should be updated, BCP 38 must be implemented on the network.

In case of DNS [9] recommends restricting recursion and disenabling the property of sending additional delegation information

In case of SNMP as suggested by [10] end user devices must not be configured with SNMP on or public SNMP community string by default in general. General public must be encouraged to disable SNMP

Similarly in case of SSDP as per [11] unwanted WAN based UPnP requests or prevent UPnP access from Internet at all.

4.1. Defense Approaches Proposed :

Because all of the practices recommended above are not mandatory in the heterogeneous Internet world there is always a chance that users will overlook these suggestions. Researchers therefore keep on proposing better and better defense mechanisms. Since DRDoS attacks can be described as sophisticated DDoS attacks some solutions are equally applicable for both of them. We will be discussing a few recent ones below:

In [12] an extensive study of seven UDP based vulnerable protocols has been carried out. Their exposure about the various amplification vulnerabilities can be very helpful in fighting against amplification attacks. They have scanned the entire IPV4 address space to monitor and classify

amplification vulnerable devices. They have also depicted how TCP handshake can be abused for amplification. Finally they provide a mechanism to find out whether or not a network is vulnerable to spoofing.

In another approach in [13] a scheme for defending against DNS amplification attacks called T-DNS has been proposed. They suggest employing connection oriented DNS service. For the purpose of imposing security and privacy they recommend the use of Transport Layer Security and for dealing with security issues that arise due to size limitation imposed by UDP they propose TCP.

Another paper [14] recommends a method called soft control to detect IP spoofing hence protecting proxy based networks from reflector attacks. They try to perform behavior remolding and try to convert attack traffic into comparatively legitimate one before discarding them in entirety. They also propose for a change in HTTP to identify which is attacker traffic rather than attempting to key out innocent traffic.

Soft computing has been beaming as a defense aid in DDoS and DRDoS attacks since long. A similar soft computing technique fuzzy logic has been used in [15] as a defense mechanism against DDoS and they assert it can be applicable to DRDoS attacks as well. Parameters depicting traffic pattern in data center is used for developing a statistical hybrid fuzzy system for defending against DDoS. They also take into consideration the fact that during attack entropy of source IP address changes as traffic to destination converges.

5. DRDoS: A Potential Threat To Cloud

One of the most thriving and evolving branches of the Internet tree is loud computing. Cloud computing is a model for enabling ubiquitous, convenient, on demand network access to a shared pool of configurable resources (n/w, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management efforts and service providers interaction[17].
Cloud's popularity is swelling day by day pulling the giants of the technology world like Microsoft, Amazon, Google and innumerable others as well as small scaled companies towards itself. The same magnetizing popularity has drawn the attention of attackers towards cloud. Several DDoS attacks have already been made and several papers regarding the issue of DDoS attacks in cloud computing.

5.1. Vulnerabilities That Are Potential Threats To Cloud Computing

In this section we have pointed out some vulnerability in cloud computing environment which can be used by attackers to launch DRDoS attacks.
According to a report published in [16] on July 2014 UPnP forum is planning to use cloud to connect the Internet of Things (IoT) to home devices thus enhancing their capabilities. Thus with the use of UPnP devices there is high chances of attackers abusing SSDP protocol vulnerability in unprotected home devices to launch reflector attacks.
Cloud providers employ [18]DNS to route client requests to servers thus rendering them vulnerable to the most prominent DRDoS attacks in recent times namely DNS amplification attacks.

Like all big organizations cloud providers automate the task of their network management using vivid large software products. However the protocol which is the building block of any network management software namely SNMP is a potential vulnerability that can be exploited by attackers.

These are a few vulnerabilities which are a potential threat to cloud computing environment. Though many more exist and still more are likely to be devised by attackers in near future.

6. Conclusions

From our survey it is quite clear that despite several good defense mechanisms proposed so far the DRDoS menace is thriving at its fullest.
We also depict the DRDoS attacks as a potential danger to the popular cloud computing domain. It follows that we must continue to look for better ways to combat this evil lest it should continue to cause damage to Internet services and infrastructure.

References

[1] Tao Peng and Christopher Leckie and Kotagiri Ramamohanarao, "Survey of Network Based Defense Mechanisms countering the DOS and DDoS Problem", ACM Transactions on Computational Logic, Vol. 2, No. 3, September 2000
[2] N.Jeyanthi, Hena Shabeeb and Mogankumar P.C., "Credit Based Methodology To Detect And Discriminate DDoS Attack From Flash Crowd In A Cloud Computing Environment", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, September 2013
[3] K.M Prasad, A.R.M. Reddy, K.V. Rao, "Discriminating DDoS Attack traffic from Flash Crowds on Internet Threat Monitors (ITM) Using Entropy variations", African Journal of Computing & ICT , Vol . 6, No. 3. Pp -53-62 , June 2013
[4] Sajal Bhatia, George Mohay, Alan Tickle, Ejaz Ahmed, "Parametric Differences Between a Real-world Distributed

Denial-of-Service Attack and a Flash Event", 6th International Conference on Availability, Reliability and Security, 22-26 August 2011, Vienna University of Technology, Vienna.
[5] Hajime Tazaki, Kazuya Okada, Yuji Sekiya and Youki Kadobayashi, "MATATABI: Multi-layer Threat Analysis Platform with Hadoop", In Proceedings of International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS 2014). Wroclaw, Poland. September, 2014., downloaded from http://www.necoma-project.eu/
[6] Yogesh Kumar Meena and Aditya Trivedi, "A Novel Protocol for IP Traceback to Detect DDoS Attack", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012
[7] Wei Wei, Feng Chen, Yingjie Xia and Guang Jin" A Rank Correlation Based Detection against Distributed Reflection DoS Attacks "Communication Letters, IEEE (Volume 17, Issue 1) January, 2013
[8] Alert (TA14-013A)NTP Amplification Attacks Using CVE-2013-5211 Original release date: January 13, 2014 | Last revised: February, 2014
[9] The Continuing Denial of Service Threat Posed by DNS Recursion (v2.0) US-CERT 2006
[10] SNMP Reflected Amplification DDoS Attack Mitigation A Broadband Internet Technical Advisory Group, Technical Working Group Report, 2014
[11] PLXsert Threat Advisory SSDP Reflection DDoS Attacks TLP:AMBER, GSI ID:1079
[12] Marc Kührer, Thomas Hupperich, Christian Rossow, and Thorsten Holz,, "Exit from Hell? Reducing the Impactof Amplification DDoS Attacks", in the Proceedings of the23rd USENIX Security Symposium. August 20–22, 2014
[13] Liang Zhu, Zi Hu and John Heidemann,"T-DNS:Connection-Oriented DNS to Improve Privacy and Security", SIGCOMM'14, August 17–22, 2014, Chicago, IL, USA. ACM 978-1-4503-2836-4/14/08.
[14] Yedu Krishnan.R, A.Anbumani ," Protecting Proxy Based Network From DDoS Attackers With IP Spoofing Detection", IJCSMC, Vol. 3, Issue. 4, April 2014, pg.320 – 327
[15] N.Ch.S.N. Iyengar, Arindam Banerjee and Gopinath Ganapathy, "A Fuzzy Logic based Defense Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 6, No. 3, December 2014
[16] [Online] www.upnp.org
[17] The NIST Definition of Cloud Computing . Special Publication 800-145
[18] Ken Birman, Gregory Chockler, Robbert van Renesse," Towards A Cloud Computing Research Agenda", ACM SIGACT News, 2009 downloaded from cornell.edu

Srinivas Arukonda is currently working as Asst. Professor at Galgotias University.He done his M.Tech from Indian institute of Information Technology,Gwalior,MP and done B.tech from JNTU Kakinada AP.He was worked as Asst Professor at Manav Rachna International University(2010-2012) and Currently working as Asst Professor at Galgotias University(2012 onwards).His major area of interest is Computer Networks and Cloud Compouting.

Samta Sinha is a post graduate researcher at Galgotias University Greater Noida. Her research is focused on DDoS and DRDoS attacks identification and defense.