Detection of DDoS Attack Using Traceback Technique

M. Vimal Chander, Jayashree Padmanabhan, A. Ayyasamy and B. Persis Urbana Ivy

ABSTRACT
In this paper, we presenting a retrospect on detection of Denial of Service (DoS), DDoS attack in internet and voice-over-IP network using IP traceback mechanism. Voice over Internet Protocol (VoIP) is the innovation to transport voice correspondence over IP system. For instance, web which is fit for making telephone brings over pack trading framework. It exploits advance voice compression technique and bandwidth sharing in packet switching network. VoIP works on IP backbone hence it also vulnerable to all types of attacks and internet is susceptible with. Among these, DDoS plays a vital role and has major impact on its performance. The objective of IP trackback is to follow the way of an IP packet to its inception. DDoS is a conveyed synergistic extensive scale dos assault which assault on an extensive variety of unobtrusive. It’s very easy to implement and difficult to prevent and trace. The objective of appropriated dissent of administration assault is to deny true blue clients access to a specific asset. This is done by exploitation system weakness or adding computational system overload or by misusing a protocol. Proper network configuration made DoS attack difficult to accomplish.

INTRODUCTION
Voice over Internet Protocol (VoIP) is a family of technologies for the transmission of voice over the internet (Keromytis, D., Angelos, 2012). Voice is converted into digital signals and is transmitted as data packets. The conversion of analog voice to digital signals is done by the analog to digital converter. Voice over IP is a technology in which transmission of voice using IP technology over packet switching network. VoIP is a subnet of IP telephony which is used for transport telephone calls. So internet telephony is its main application.

Skype is one of its product which reduce communication and infrastructure cost. Main advantage is that more telephone calls are possible over a single bandwidth. But it is not free of attacks. In this paper, focus on DDoS attack which can easily change the source address of an IP packet and cause memory less feature of internet (John, A., T. Sivakumar, 2009; Snoeren, 2001). Denial of service (DoS) attack can prevent outgoing traffics or incoming traffic to network services. They utilize the weakness of computer or TCP/IP protocol.

In this paper we are additionally talking about diverse sort of DoS attacks and trace back mechanism to detect attacks. To defending against IP spoofing in which identity of sender is fake. Reconstructing the attacked path by tracing the packet back to source. Packet logging and packet marking algorithms are used for this purpose. VoIP can support file sharing, calendaring, sending fax, collaborative editing, and video. It supports dual mode telephone conversation between cellular service and Wi-Fi network, internet to PSDN network bridging, P2P calling in Skype (Gong, 2005).
DDoS Attacks in TCP/IP Protocol:

DDoS attack depends on shortcoming in TCP/IP protocol. TCP/IP network are made of packets VoIP use it to go across the networks. There are different types of DoS attack has been including over the networks as follows.

A. Flood attack:
First, attacker sends more movement to server more than it can deal with. It is difficult to prevent and the attacker have more speed than target machine (Song, et al., 2001).

B. Ping of death attack:
The attacker sends IP datagram of larger size which exceeds the standards that is sending a ping of 65,535 byte to target (Guerid, et al., 2011).

C. SYN attack:
It occurs in handshake mode of connection taking place using SYN and ACK messages. The attacker surges the accepting station with SYN messages which appears to be come from unreachable internet address and fill the SYN buffer. The target can’t send ACK messages and thus prevent other system communicate with target machine (Wei, et al., 2010).

D. Teardrop attack:
Is which confuses the target machine or hang it. Here corrupted packets are sent to target machine using packet fragmentation algorithm.

E. Smurf attack:
Which a broadcast addresses of third party is used. The attacker sent ping request to third party which is a spoofed IP address appears to be come from target machine. So the every system in the third party will send ping response to target machine.

Compromise of ddos attacks:
In DDoS attacks in make compromised systems using Trojan horse or worm or hacked (Oe, et al., 2003). And these compromised systems are controlled by client server software like tribe flood network, Trinoo, shaft.

F. Agent-Handler Model:
In Agent-Handler Model DDoS attack consists of clients, handlers, and agents as shown in Fig. 1.

![Fig. 1: DDoS Agent-Handler Attack Model.](image)

The Client is used by the attacker to communicate with the Internet to connect with the other network for the preparation of the attack. The handlers are programming bundles is available in the current frameworks all through the Internet that the programmer uses to correspond in a roundabout way with the agents (Alenezi, 2011). The operators programming exists in traded off frameworks that will in the end complete the attack on the casualty framework. The attacker will speak with any number of handlers to plan which operators are up and running, when to calendar attacks, or when to redesign agents.

The attacker puts the handler programming in system server which can deal with the substantial measure of activity. The communication takes place through Transmission control protocol, UDP and ICMP between attacker and handler. The clients in the existing don’t know that their system is going to take part in the DDoS
attack. While the client system is participating in the attack their bandwidth and performance is reduced. So, that the DDoS occupies their bandwidth and performance and attacks the target (Malliga, S., A. Tamilarasi, 2007).

G. IRC-Based DDoS Attack Model:
Web Relay Chat (IRC) is a multi-client, on-line talking framework which permit their clients to make open, private and mystery channels. Open channels where different clients can visit and share messages and documents. Open channels permit clients of the channel to see all the IRC names and messages of clients in the channel. Private and mystery channels are set up by clients to correspond with just other assigned clients.

An IRC-based DDoS assault system is like the Agent-Handler DDoS assault model aside from that rather than utilizing a handler project introduced on a system server, an IRC correspondence channel is utilized to associate the customer to the agents. Using of an IRC channel; aggressors utilizing this kind of DDoS assault structural engineering have extra advantages.

1) Advantages
a) IRC servers tend to have vast volumes of movement making it less demanding for the aggressor to conceal his vicinity from a network administrator
b) The attacker no more needs to keep up a rundown of operators.
c) IRC organizes likewise give the advantage of simple record sharing

Control of Ddos Attacks:
After compromised, systems are controlled by client server software which is called DDoS attack tools like tribe flood network, Trinoo, shaft etc.

H. Trinoo:
It was the first DDoS tool to be discovers .Trinoo were UDP based tool and password protected. In Trinoo the attacker controls the servers through password. The server system controls multiple daemons system. Trinoo is utilized to keep framework administrators or programmers from capturing. The fundamental point of interest is it begins the assault against focus as fast as others furthermore numerous assaults can be propelled from a solitary order.

I. Tribe Flood Network (TFN):
TFN enhanced on some of the shortcomings of trinoo by including different types of assaults that could be mounted against the victim site. Organized like trinoo with assailants, customers (bosses) and daemons. Initial framework bargain permits the TFN projects to be introduced. It utilizes ICMP to convey which makes it harder to channel and square. TFN doesn't validate the wellspring of the ICMP parcels so you could flush out the customers.

J. Stacheldracht:
Stacheldracht consolidates the components of trinoo and unique TFN. It includes encryption of correspondence in the middle of assailants and bosses. It includes programmed upgrades of the agents. The components used in this are masters, attackers and daemon. It could mount ICMP, UDP, SYN floods & Smurf. It encodes the association in the middle of attacker and master not at all like TFN.

K. Mstream:
Mstream is a point – point DDoS attack tool. The attacker and handler communicate through TCP – 6723/tcp, 12754/tcp, 15104/tcp. The handler and agent are communicated through UDP – 7983,6838 and agent and handler through UDP-9325,6838. It is a slightest complex of the assault devices. It utilizes one kind of attack just (i.e.) ACK surge (Stefan Savage, 2001).

L. Shaft:
Shaft can switch handle servers and ports. Here the assailant utilizes a telnet project to converse with handlers. The communication between client and handler through TCP-20432, Handler and agent through UDP-18753, Agent and handler through UDP-20433. It can move handlers and ports makes IDS guard more troublesome (Lee, et al., 2004).

M. Tribe Flood Network 2000:
It was gone for Solaris, Linus and Microsoft Windows NT operating System. Master and agent are the components used in TFN2K. The master and agent are communicated through encrypted communication. It utilizes TCP.SYN, UDP, ICMP/PING assaults against casualties. Difficult to recognize on the grounds that all control correspondence is unidirectional, utilizes TCP, UDP, ICMP arbitrarily (Thing, L.L., 2004).
Threats and traceback mechanisms:

Denial of service threads in VoIP: the main aim is to deny the legitimated user in accessing the VoIP network or connectivity. DoS attacks in VoIP occur by flooding the target machine with unnecessary SIP call which degrades the service. The call processing may drop or halts. The main aim of attacker is to get the remote control of the system (Chen, et al., 2003).

Spamming over internet telephony as we know the spam messages carry viruses or spywares. Each VoIP account has its own IP address. The spammer sends hundreds of voicemail to IP address and it gets clogged. It is a social threat (Wang Yu, et al., 2003).

Eavesdropping, modification threats in VoIP by stealing the credentials like password or username a third party gain a third party gain control over the voicemail and all the information of victim. Hackers listen the signaling or content of that session. The attacker can also modify the session. Call tempering in which the attacker can intentionally tamper the call by adding noise packets in communication stream which degrade the quality of service.

Vising by VoIP is called voice phishing in which fake third parties try to get identity of victim. Physical threats affecting VoIP include the unauthorized physical access to VoIP equipment, performance degradation and power loss due to weather cause inaccessible VoIP services.

N. IP Traceback Mechanisms Embrace:

Ingress filtering includes blocking the packet from attacker by configuring the router. The router has capacity to distinguish the legitimate user and illegitimate user by examining the source address of every packet. Link testing is trace back techniques which examine the upstream router from the router closet to victim till the router carrying the attacker traffic are found. Link testing includes input debugging and controlled flooding. Logging technique which helps in determining the path traversed by the packet using data mining technique. It is easy method to find the attacker but drawback is that it add enormous resources requirement.

ICMP trace back techniques which use internet control message protocol are used to trace out the attack path. Every packet enable edge sampling algorithm with low probability and generate ICMP trace back message which consist of next and previous hops and time field.

Advanced marking and authenticating marking as fragmented marking scheme proposed by savage et al[]. This methodology has low system and switch overhead. It supports an efficient authentication of routers marking. It reconstructs the attack path efficiently with low false positive.

Packet marking algorithm: Here the mark is the signature or identity of a router. In addition to forwarding it also insert a mark. Deterministic packet marking (DPM) the router mark the entire packet using IP address of router. So the casualty can reproduce the assault way utilizing it. Downside is that because of extra usefulness the switch will back off.

Probabilistic Bundle Checking (PBC) is proposed for accomplishing trace back of DOS assault. DOS assault can be counteracted if the mock source IP location is follow back to beginning to discover the attacker. But in PPM only some packets are marked by the router so the attacker can mislead by marking their original packet. Hash based IP trace back system is additionally called Source Way Disengagement Motor (SWDM). After examining the single packet the router can create queries to reconstruct its path. But the attacker can attack the queries and response communication and thus affect its performance.

Flexible Deterministic Packet Marking (FDPM) is a version of DPM. It is more efficient than DPM and adds flexible features to trace back mechanism. In TOPO based trace back mechanism bloom filter utilize the immediate predecessors topology information to trace back. It is single packet IP trace back mechanisms which reduce unnecessary queries. Topology Based Packet Marking (TBMP) is an approach against anti IP spoofing technique. It focuses on the path traversed by the packet and strengthens packet marking principle

Conclusion:

We surveyed various IP trace back techniques which are applicable to VoIP networks. Since the VoIP network not free from DoS attacks, IP trace back mechanism like link testing, packet logging, packet marking, ICMP trace back, advanced marking and authenticated marking, packet marking algorithm, deterministic packet marking, probabilistic bundle checking and hash based IP trace back are applicable to VoIP. In future we are trying to implement advanced marking and authenticated marking scheme in VoIP which help to prevent more attacks with less network and router overhead.

REFERENCES


Malliga, S., A. Tamilarasi. 2007. “A defensive mechanism to defend against DoS/DDoS attacks by IP traceback with DPM”. In International Conference on Computational Intelligence and Multimedia Applications, 4: 115-119. IEEE.


