ISSN No. 0976-5697

Volume 3, No. 3, May-June 2012

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Analysis of Conflict DoS Attacks Process and Counter Measure on SIP Based VoIP Network

Md. Ruhul Islam*
Dept. of Information Technology
Sikkim Manipal Institute of Technology
Majhitar-737136, East-Sikkim, India
md_ruhul@rediffmail.com

Dr.Smarajit Ghosh
Dept. of Electrical & Instrumentation Engineering
Thapar University
Patiala-147004, Punjab, India
smarajitghosh@rediffmail.com

Nausrat Jahan Ahmed
Dept. of Applied Electronics & Instrumentation Engineering
Sikkim Manipal Institute of Technology
Majhitar-737136, East-Sikkim, India
nausratahmed@gmail.com

Abstract: Voice over Internet protocol (VoIP) is continuously developing and changing the face of business telephony. The Session Initiation Protocol (SIP) is a generally used standard in VoIP communications to setup and tear down phone calls. Amongst various online attacks hampering IT security, Denial of Service (DoS) has the most devastating effects. It has also put great difficulty over the security experts recently, in bringing out successful defense solutions. These attacks could be implemented diversely with a variety of tools and codes. Since there is not a single solution for DoS, this attack has managed to overcome on internet for nearly a decade. Denial-of Service (DoS) attack recently come out as the greatest threat to VoIP systems. Such type of attacks are difficult to detect and capable of realize vulnerabilities in protocols with low rate traffic. In VoIP based network it might be possible to collision on a DoS attack. Therefore must be happened call disruption in between sender and receiver. In this paper we aim to provide conflict of DoS attack and how to counter measure these collision of DoS in SIP based network.

Keywords: VoIP, SIP, IP PBX, DoS attack, RTP;

I. INTRODUCTION

Voice of IP (VoIP), Internet conference, and messenger are good examples of SIP-based services [1]. SIP will become a major session control protocol of Internet-based multimedia services in the near future. Denial-of-Service (DoS) attacks are explicit attempts to disable a target thereby pre-venting legal users from making use of its services. DoS attacks continue to be the main threat facing network operators. As telephony services move to Internet Protocol (IP) networks and Voice over IP (VoIP) becomes more prevalent across the world, the Session Initiation Protocol (SIP) [2] infrastructure components, which form the core of VoIP deployments, will become targets in order to disrupt communications, gain free services, or simply to make a statement. Since DoS attacks are at-tempts to disable the functionality of the target, as opposed to gaining operational control, they are much more difficult to defend against than traditional invasive exploits, and are practically impossible to eliminate. We designed and demonstrated effective resistance the collision of DoS attacks and their counter measure on a SIP-specific DoS attacks.

II. BACKGROUND

A. Overview on SIP:

The most important SIP operation is that of inviting new participants to a call. To achieve this functionality we can distinguish different SIP entities:

a. ***Proxy:*** A proxy server receives a request and then forwards it towards the current location of the callee either directly to the callee or to another server that might be better informed the location of the callee.
b. ***Redirect:*** A redirect server receives a request and informs the caller about the next hop server. The caller then contacts the next hop server directly.
c. ***User Agent:*** A logical entity in the terminal equipment that is responsible for generating and terminating SIP requests.
d. ***Registrar:*** To assist SIP entities in locating the requested communication partners SIP supports a further server type called register server. The register server is mainly consideration to be a database containing locations as well as user preferences as indicated by the user agents. SIP is used for establishing a session between two parties who support VoIP. The session setup functionality in SIP is handled by various architectural components. User-Agent Clients (UAC) and User-Agent Servers (UAS) are the hardware or software components that commence and respond to the end users requests respectively. A Proxy within a given domain handles the requests on behalf of user-agents belonging to that domain. It may require authentication from the client before it forwards any such requests. A User-Agent will typically register itself with a Registrar within its domain, and the agent's actual IP addresses are stored with a Location Server.

In SIP, a user is identified through a SIP URI in the form of user@doamin. This address can be determined to a SIP proxy that is responsible for the user's domain. To identify the actual location of the user in terms of an IP address, the user needs to register his IP address at the SIP registrar responsible for his domain. Thereby when inviting a user, the caller sends his invitation to the SIP proxy responsible for the user's domain, which checks in the registrar's database the location of the user and forwards the invitation to the callee. The callee can either accept or reject the invitation. The session initiation is then finalized by having the caller acknowledging the reception of the callee's answer. During this message exchange, the caller and callee exchange the addresses at which they would like to receive the media and what kind of media they can accept. After finishing the session establishment, the end systems can exchange data directly without the involvement of the SIP proxy. For authenticating a user SIP uses the digest authentication mechanisms, which is based on a challenge/reply approach. In the following we describe some headers included in the SIP messages and that can be misused for launching DoS attacks:

- ***e.*** ***Request-URI:*** Indicates the destination the request is being sent.
- ***f.*** ***Route:*** Determines the route a request should take. After receiving a request with such a header, the proxy is supposed to forward the message to the address indicated in this header .
- ***g.*** ***Contact:*** Indicated the exact address of a user agent. Proxies might use this header as entry for a location information cache that could be used to speed up future searches.
- ***h.*** ***VIA:*** The VIA header indicates the path taken by a request so far.

B. Overview of DoS:

Denials of Service attacks were first used to "have fun", get some kind of revenge from system operators or make complex attacks possible. IRC servers were also frequently targeted after one got snubbed on a channel. At this time networks and Internet uses were "confidential", and those attacks had very limited impact. With time and as the Internet gets more and more used as a communication channel, hacktivism becomes more and more popular. Geopolitical situations, wars, religious concerns, ecology, any motive is then good to launch attacks on companies, political organization or even national IT infrastructures. A more recent use of Denial of Service is linked to online gaming. Many servers have been victims of such attacks, generated by unhappy gamers who lost lives or their favorite weapon during game. But the very use of Denial of Service today is definitely extortion. More and more enterprises rely on their IT infrastructure. Mail, critical data and even phone are handled by the network. Very few companies can survive without their main communication channel. Furthermore the Internet is also a production tool. Search engines and gambling web sites, as an example rely entirely on their connectivity to the network.

Denial of Service (DoS) attacks intend at denying or degrading a genuine user's access to a service or network resource, or at bringing down the servers offering such services. In the last several years DoS attacks have increasingly become a major problem of computer security.

By definition a Denial-of-service attack is any explicit attempt by an attacker to deem a resource or service unavailable for legitimate users. We can identify an attack as logical or exhaustive. A logical attack is one where the attacker uses precise methods to disrupt service. Internet Denial-of-Service attacks has increased in frequency, severity and sophistication [3]. Between the years of 1989 and 1995, the number of such attacks reported to the Computer Emergency Response Team (CERT) increased by 50% per year [4]. According to a 1999 CSI/FBI survey report 32% of respondents detected DoS attacks directed against them [5]. To make things worse, reports in the last few years [6] indicate that attackers have developed tools to coordinate distributed attacks from many separate sites, which is also known as Distributed Denial of Service (DDoS) attack. There are two principal classes of attacks: logic attacks andflooding attacks [7]. Overwhelming a victim's resources by flooding it with malicious traffic is the most basic and probably the most difficult to defend against DoS attack [8]. In communication networks these attacking techniques can be applied to protocol processing functions at different layers of the protocol architecture. That is attacks can be launched on the network, transport or application layers. From a high level point of view DoS attacks can be classified into the two categories resource destruction and resource allocation. In a more detailed examination the following DoS attacking techniques can be identified:

III. COLLISION OR CONFLICT OF DOS ATTACKS PROCESS

A. Real-time Sensitivity:

Even a two packet 40 ms drop has a measurable drop in MOS scores. Jitter buffer are usually < 100ms a variation in delay of more than that results in drops .ITU specifies 150ms as the maximum end to end delay for voice. Below figure shows how end to end voice has been happen. Here the caller call to another person, at that situation at the end of receiver portion the receiver get the response late because delay of voice.

B. Peer-to-peer:

Below figure1 shows Attackers can directly flood endpoints. Any segment of network possibly can be an attack target. Here it is happen pair wise. For this situation the attacker attacks point to point.

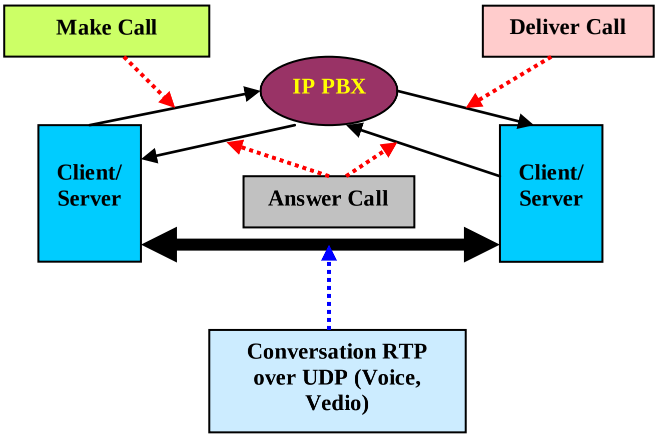

Figure 1: shows Through PBX, peer-peer attack on DoS

C. Complex Protocols:

Basically in VoIP phones are multi ported (figure 2). If we have many port that means there should be different port number as well as different protocols. In the sense so many calls could be handled by phones. In this case we have used multiple protocols with different port number. Therefore the attacker also may take chances. Complexity is friend of attacker. More ports more ways to attacks. More attacks like reflection, amplification possible. Real-time streaming Voice-over-IP applications such as SIP and H.323 and peer-to-peer applications such as Napster are examples of complex applications [9].

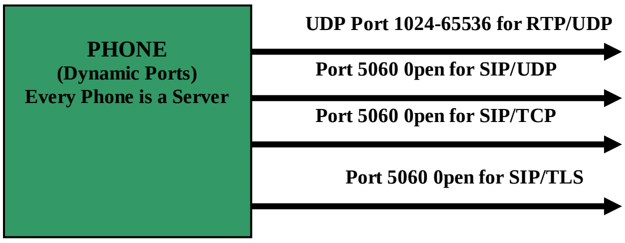
PHONE
(Dynamic Ports)
Every Phone is a Server
UDP Port 1024-65536 for RTP/UDP
Port 5060 0pen for SIP/UDP
Port 5060 0pen for SIP/TCP
Port 5060 0pen for SIP/TLS

Figure 2: shows multi port attack using DoS

D. *Application Layer:*

In application layer the attack rate is low. This thing has happened due to layer approach. Each message can result in heavy processing. Creation of complex state machines, Application layer makes the servers vulnerable low rate attacks.

A server is a process implementing a specific service, for example, a file transfer service or an email service. A client is a process that requests a service from a server by sending it a request and subsequently waiting for the server's reply. Sometimes, the terms client and server are also used refer to the machines that runs the client process and the server process respectively. In below figure 3 shows how attack happen in application layer.

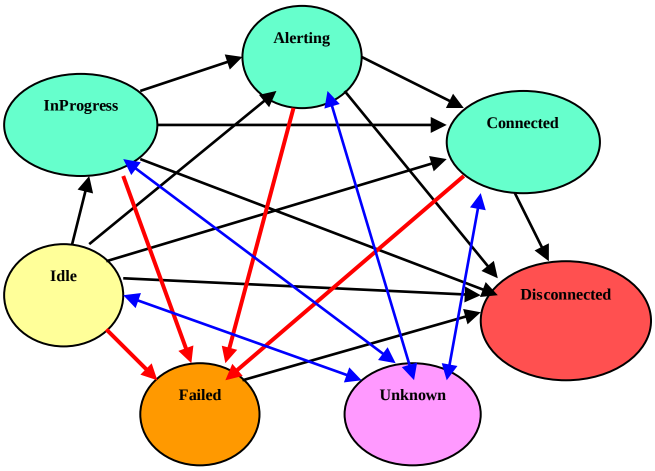

Figure 3: shows application layer attack using DoS

E. *Weak VoIP Endpoints:*

In VoIP services have to needed two ways, one is sender and another is receiver means must have starting as well as end points. So if the end points are weak, then also possible to attack. On the other hand Low CPU rate as well as the low memory space, No Security tools are used for protection on endpoint against DoS attacks.

F. *Human Interactive:*

Human interaction allows for secrecy attacks targeting users. Very low volume traffic can overwhelm users.

IV. DIFFERENT COUNTER MEASURE TECHNIQUES OVER COLLISION OF DOS ATTACK

A. *Detecting Attack:*

In case of DoS we have to monitor source, because amount of traffic came from a single source. Therefore DoS Detection is possibly the simplest way to protect from attack and is done based on large amounts of traffic from a single source. But in case of DDoS detection is required on the destination or the victim of attack and detects maximum number of spikes in traffic. In other way learning the details of message headers and detecting any mismatches allows fingerprinting to detect spoofind. I case of Stealth DoS is requirement is different. In this situation, behavior learning in different time slots, based on time of day and day of week, and ability to monitor even slight deviations from learnt behavior.

B. *Identifying Attacker:*

To solve attack on DoS, have to identify first. This is the simplest as part of detecting attack; the source of attack is easily identified, except it is being spoofed. On other hand in case of DDoS it's depend upon the number of zombies attackers may be or may not be able to identify, but it's based on volume. Spoofing in this case the number of random sources can be as high as the address space in theory, new sources of traffic or cookie based techniques are used. But if we take in case of Stealth DoS, the attacks are very low volume, identifying an attacker is difficult, it is best to verify all traffic and then allow only verified traffic

C. *Equations Justifying Attacks:*

DoS: Once the attacker is identified blocking attacker than it is quite straightforward.

DDoS: To identify the blocking attacker is possible when limited number of zombies is possible. The operation of a network of compromised machines, containing remotely controlled "Zombie" attack programs, is directed and coordinated by a "Zombie Master" central control agency [10]. All systems connected to the Internet can be affected by denial-of-service attacks [11]. In case of three way handshake protocols, the attack target sends back cookies and hides state inside the cookie and waits for handshake to complete before allocating resources, in case of spoofing and simple script zombies attack is let down. On detecting a fingerprint mismatch re-authentication can be triggered blocking spoofing attacks.

D. *Stealth DoS:*

Whenever multimedia session establishment required at that case message exchange may take an active part in different network[12].In case of three way handshake protocols, the attack target sends back cookies and hides state inside the cookie and waits for handshake to complete before allocating resources. In case of spoofing and simple script zombies attack is disappointed.

E. Reflection:

Instead of sending attack requests directly to the targeted victim, a reflected DoS attack sends requests that use victim's address as the source address to reflectors that will in turn send their replies to the victim [13]. A reflector can be any host that will return a packet if sent a packet. Web servers, DNS servers, and routers are examples of a reflector. Web servers and DNS servers will return SYN ACKs or RSTs in response to SYN or other TCP packets, and routers return ICMP Time Exceeded or Host Unreachable messages in response to particular IP packets. Eliminating IP address spoofing does not address the reflected attack problem entirely, due to the application-level reflectors such as recursive DNS queries and HTTP Proxy requests [14]. Eliminating IP address spoofing does not address the reflected attack problem entirely, due to the application-level reflectors such as recursive DNS queries and HTTP Proxy requests [13][14]. So Drop unwarranted responses or messages invalid for the state.

F. Recursive Amplification:

For this type of DDoS attack, the attacker can send the broadcast message directly, or the attacker can use the agents to send the broadcast message to increase the volume of attacking traffic. If the attacker decides to send the broadcast message directly, this attack provides the attacker with the ability to use the systems within the broadcast network as zombies without needing to infiltrate them or install any agent software. For this case Drop unwarranted responses or messages invalid for the state. Flexible policies have to implement specific messages, headers.

G. Source Monitoring:

Source monitoring is also one of the important methods to catch the attacker. In this case non conformant traffic call observes all the traffic. If the traffic gets any enormous attacker, than they would find and try to solve.

H. Destination Monitoring:

In this case monitoring technique will be applicable on destinations. It is only possible when get confirmation of behavior on that particular path. If it is possible, then also protect the end point.

I. Behavior Learning:

If we get bad behavior on the network at that time we have to observe using the normal traffic. After finding the attacker, it's possible to protect the end point.

J. Cookie Verification:

In case of cookie verification blocks spoofed DDoS came at very high rates. In this situation blocks are scripts. Here the main thing is happened like first the attacker makes call and send to phone server, on the same time the phone system send address (spoofed) without any verification. But in receiver side don't know where it's come from. After this one more call came but this time it's came from caller via internet and again send the address. when server send the address, after verification its back with valid response, then server give or allow to call and its gone through protected end point.

K. Use of RTP:

To select RTP can also protect, but it will happen on block wise. So in this case attacker can't attack on whole, they will attack pair basis. Deterministic low latency and low jitter will be under attack. Restrict the impact of attack to one domain. If the attack happened in pair wise than it will recover quickly, because attack is happen block wise. DNS has been named as a major factor in the generation of massive amounts of network traffic used in Denial of Service (DoS) attacks [15]. Various incidents in the Internet have been already reported in the literature [10] as flooding attacks targeting either on the provided service or on the underlying network infrastructure. The most severe among them is presented in [16]-[18] and is known as Reflection Distributed DoS (RDDoS).

V. CONCLUSION

DoS attacks by their very nature are difficult to defend against and will continue to be an attractive and effective form of attack. Denial of service attacks is a dangerous problem to solve. This type of inborn problem root is public Internet together which difficulty to recognize "friends" from "enemies". There is large area of "unwanted attacks". If we want access or use to server resources than it is good but misbehaving implementation is bad.

VI. REFERENCES

[1] H.Schulzrinne,S.Casner,R.Frederickand V. Jacobsonm, "RTP: A Transport Protocol for Real-Time Applications", Category: Standards Track RFC 1889, January, 1996.

[2] Rosenberg.J, Schulzrinne.H, Camarillo.G, Johnston. A, Peterson.J, Sparks.R, Hand- ley.M, Schooler.E: SIP: Session Initiation Protocol, Category: Standards Track, RFC 3261 (June 2002).

[3] Computer Emergency Response Team. "Denial-of-Service Developments", CERT Advisory CA-2000-01, http://www.cert.org/advisories/, CA-2000-01.html, January 3, 2000.

[4] J. D. Howard, "An Analysis of Security Incidents on the Internet", PhD thesis, Carnegie Mellon University, August 1998.

[5] Computer Security Institute and Federal Bureau of Investigation, "CSI/FBI Computer Crime and Security",Survey, Computer Security Institute Publication, March 1999.

[6] Y. Chen."Toward a quantitative understanding of DoS".Class Proposal,University of California, Berkeley,USA, http://www.cs.berkeley.edu/~yanchen/course /261_proposal.html, 2000.

[7] D. Moore, G. Voelker, S. Savage. " Inferring Internet Denial-of-Service Activity", In Proceedings of the 10th USENIX Security Symposium, pages 9-22, August 2001.

[8] Jiri Kutha, "Comparison of Service Creation Approaches for SIP", International SIP conference, March 2000.

[9] P. Srisuresh, J. Kuthan, J. Rosenberg: “Middlebox Communication Architecture and framework”, Internet Draft, IETF, February 2001.

[10] Gibson: “Distributed Reflection Denial of Service”, on-line tutorial, http://grc.com/dos/drdos.htm, 22 Feb,2002.

[11] Houle, Waver:“Trends in Denial of Service Attack Technology”,CERTreport,http://www.cert.org/archive/pdf/DoS_trends.pdf, October 2001,

[12] 3GPP: “Signaling flows for the IP multimedia call control based on SIP and SDP", Technical Specification 3GPP TS 24.228,Technical Specification Group Core Network; 3rd Generation Partnership Project, 2003.

[13] Paxson, V.“An analysis of using reflectors for distributed denial-of-service attacks”, Newsletter: ACM SIG- COMM Computer Communication Review ,volume 31, issue 3, july 2001,page 38-47.

[14] V. Paxson. “An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks”. White Paper, AT&T Center for Internet Research at ICSI, International Computer Science Institute Berkley, USA, 2001.

[15] J.Damas, F.Neves, “Preventing Use of Recursive Nameservers in Reflector Attacks”, Category: Best Current Practice , http://www.ietf.org/rfc/rfc5358.txt,october 2008.

[16] Glenn C., George Kesidis, G.Brooks, R. R. and Suresh Rai, “Denial-of-Service Attack-Detection Techniques” IEEE Internet computing 2006.

[17] Peng.T, Leckie.C and Kotagiri. R, "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems", Journal: ACM Computing Surveys,volume 39,issue 1,2007,article no.3.

[18] Mirkovic.J, Sven Dietrich, David Dittrich, Peter Reiher, ”Internet Denial of Service: Attack and Defense Mechanism”, First Edition, Prentice Hall,2004.