SECURING SIP SERVERS FROM DDOS ATTACKS – A LITERATURE SURVEY

Abdullah Akbar [1], Shaik Mahaboob Basha [2], Syed Abdul Sattar [3]

[1] **Department of Computer Science Engineering, Jawaharlal Nehru Technological University, Hyderabad, Telangana, India**
[2] **Al Habeeb College of Engineering and Technology, Chevella, R.R. District. Telangana, India**
[3] **Royal Institute of Technology and Science, Chevella, R.R. District. Telangana, India**

Corresponding author: Abdullah Akbar, akbar.jntuphd@gmail.com

ABSTRACT: SIP servers are playing vital role in preserving multimedia, voice, data and video file storage and distribution through Voice over Internet IP services. The increase popularity of SIP servers through VOIP has attracted the attention of cyber terrorist to instigate the most damaging attacks to eavesdrop the information and compromise the servers with DDoS attacks. The recent evidences of victimization of SIP servers for the attack of DDoS through VOIP networks made this topic to be addressed with high intensity. DDoS attacks are affecting VOIP networks and SIP servers by injecting malicious virus data packets along with the normal user data sent from different locations. The proposed literature survey is focusing on measures to be taken care of to protect SIP servers from DDoS attacks with several possible novel mechanisms.

KEYWORDS: SIP Servers, DDoS Attacks, Voice, Data, Video and multimedia transmissions.

1. INTRODUCTION

Session Initiation Protocol [SIP] is popularly known as an application hand shaking protocol. This is predominantly working in association with other application protocols in managing multimedia communication sessions. SIP is widely used in VoIP technology communications to facilitate the voice and video international calls. SIP is widely used in VoIP networks because of the flexible nature to support multimedia sessions between groups of participants. SIP server plays a predominant role in transmitting the calls to the users of the network automatically where the call has to be diverted and destinated when some users of the network are busy with other calls. SIP servers are used mostly in VoIP based SIP phone system to handle the incoming and outgoing international calls associated with video and voice chat or multimedia transmission while calling. SIP facilitates the users to enjoy the video, file transfer and voice call at a time with the configuration of SIP server. SIP is setup to facilitate the users to send voice data between the phones with the help of Real-time transport Protocol to support multicast meetings and video conferences. The calls transmitted from SIP server will have a SIP address or a specific gateway which includes the branch address or exchange address. SIP servers are widely used to transfer the call, terminate call, change call parameters in mid – session to switch over to 3-way conference and other facilities while talking with other caller. SIP enables the end user to listen the ringing and lifting status of destinated phone.

SIP is playing an important role in the global telecommunication infrastructure. At the same time the significance of SIP is damaged by the disruptive attacks like Distributed Denial of Service attacks [DDoS], Spam over Internet Telephony [AOIT] and toll fraud attacks. The proposed literature survey is focusing on developing an anti-mechanism against these attacks in the SIP server in VoIP environment.

2. RELATED WORK

VoIP is a new generation international calling system with video and multimedia file accessing along with the voice calling. The security threats have not left VoIP environment and SIP servers. The previous research papers have explored new counter measures and gave raise to confidentiality, integrity and availability of SIP servers in VoIP environment [CHK15]. Predominantly sketch based change detection and prevention system is regarded as remarkable solution to notify the significant changes in massive internet traffic with the help of time series forecasting model. But this model could not withstand for high computations when the data values are retired from keys in the normal operations [SK12]. Similarly another research work has introduced Snort. This is an open source network intrusion detection and prevention system works on user defined rules. This purely meant for detecting intrusion. To give remarkably good solution for DDoS attacks with novel counter measures with the establishment of proxy SIP servers is regarded as one of the best remedies. In this system distributed

change point detection using change aggregation sub tree was predominant and used for multiple network domains. Another research work is proposed with novel intrusion detection system for SIP Servers in VoIP environment with the help of stateful detection using cross-protocol protection abstractions. RTP attacks, bye attack, fake instant messaging and call hijacking are the predominant attacks can be suppressed by SCIDIVE architecture with rule matching engine - Yu-Sung Wu et al. [Y+04]. Similarly SIP detector is identified a standalone defense-device to handle DDoS attacks. It is working on the basis of filtering techniques along with firewall, Redirect server and NAT. This solution is limited to the limited number of flooding attacks but not for large number of flooding attacks. SIP DDoS attacks can be effectively stopped by implementing Kamailio proxy server. This is an open source SIP server widely used in the world. This has to be implemented with a load balancer Abdullah Akbar et al. [ABS15].

3. RET ALGORITHM

William Conner et al. [CN15] have illustrated the counter measures to the attacks against SIP server with the implementation of Random Early termination algorithm. This algorithm is introduced to drop suspected transactions involved in ringing User Access Servers with heavy load. The Random Early Termination algorithm facilitates the SIP servers with stateful proxies to protect from DDoS attacks. The utility of Random Early termination scheme is predominant in identifying the attacks associated with incoming calls from caller to the SIP server. Before reaching SIP server a shielding mechanism can be established with the SIP proxy servers to detect the 200 IK response and delay to identify DDoS attack associated with the incoming call. Once it is identified the call will get terminated by the mechanism to protect SIP server.

4. ATTACK SYNTHESIS AND ANALYSIS MACHINE

M. Zubair Rafique et al. [RAF15] has illustrated the attack synthesis and analysis machine for SIP server to facilitate the protection from DDoS attacks and other malicious virus attacks in VoIP telephony services. This analysis tool is developed on the basis of SIP metrics. The machine is predefined with specific parameters of SIP server like Call Completion Ratio, Call Establishment Latency, Call Rejection Ratio, Number of Retransmitted requests, CPU usage, CPU interrupts rate and Interrupt handling time. The tool is configured with three vital modules like client configuration module, attack generation module and report generation module to predict the possible attacks to Open SER, Party SIP, Open SBC and MjServers.

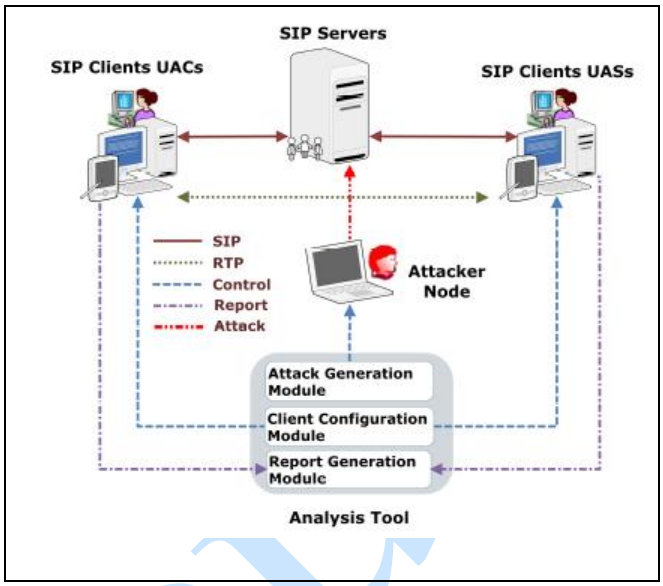

Figure 1 Attack synthesis & analysis machine

The experimental results have been obtained from all the above mentioned servers in VoIP environment and successfully obtained the results to demonstrate the effective usage of machine against the attacks. [RAF15].

Muthu Ganesh et al. [M+14] has illustrated in a research article published in 2014 International Conference on Innovations in Engineering and Technology (ICIET'14) about the detection and prevention methods for various dangerous attacks in SIP server. This paper has illustrated the ways of integration of SIP, RTP and IPSec to prevent the attacks. The attacks generally identified in the SIP server have enlisted in a table with proposed solution and criterion. This paper has illustrated the flooding attack, Multi Attribute Attack, VoIP defender intrusions, Ringing based DDoS attack, integrity attack and other possible attacks with proposed solution in a table very obviously. This paper has stressed less on DDoS attacks and more focus on different flooding attacks of SIP servers with prevention methods. [M+14]

5. DISTRIBUTED DENIAL OF SERVICE ATTACK

Distributed Denial of Service [DDoS] attacks is regarded as high threat which targets the server to thwart its services to the targeted users. Basically these types of attacks are instigated by group of hackers or cyber terrorists to compromise the services and confidential information from SIP servers. DDoS attacks give raise to the flooding at the network and transport levels. DDoS is powered

by bots. A bot is capable of performing specific functions with automatic triggering events. DDoS is configured with bots and triggered into the target computer whenever it is rebooted with the help of Zombie and infect the computer to stop the services. DDoS is associated with control channel which makes all bots to meet together in the computer network and facilitate the attacker to control over the network and manage remotely. DDoS attacks are distinguished into different types like Bandwidth Depletion Attack, Resource depletion Attack, Amplification Attack. These are used to activate flooding attacks, to create unwanted traffic and prevent the legitimate traffic to reach the attacked system. Malformed Packet Attack is also another formation of DDoS attack. This attack activate the malformed packets are to be transmitted by zombies to the attacked system to crash it.

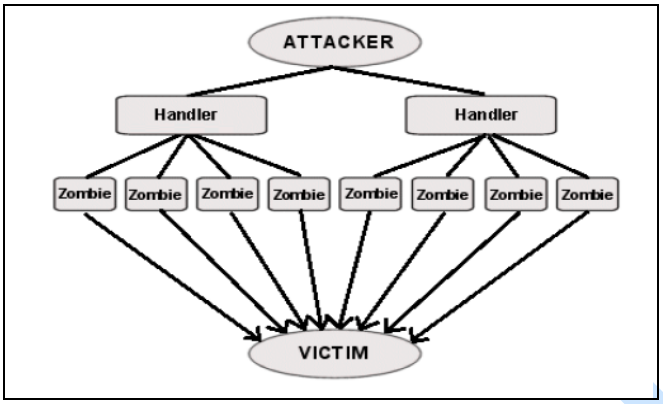

Figure 2 Architecture of DDoS Attacks

DDoS Attack architecture reveals the secret services of attacker. The attacker will take shelter behind the layers of the zombies sent to victim computer. The attacker will start the attacking from his location and malicious virus code will be injected and acts as a handler. This handler will act according to the instructions of the attacker. Once the handler is formed in the network the targeted system will be influences by the software called bots or zombies and make the targeted system as an agent. The network will be affected by the DDoS attack and convert all the client systems into agents. The final task would be victimizing SIP server under attack and compromise it.

DDoS attacks are enriched in the internet market with the implementation of tools to produce to do the destruction work to the SIP servers. The power tools which produce DDoS attacks are Trinoo, TFN, TFN2K, Stacheldraht, Shaft, Mstream, Knight and Trinity. These tools are widely used by the cyber terrorists to give rise to the TCP and UDP flooding and other flooding viruses to infect SIP servers and its network [GJM10].

6. THE ADMEASURES FOR DDoS

The research works have been investigated to find the suitable admeasures to DDoS attacks and protect the SIP servers. The following measures have been developed in research studies.

7. DEFENCE ARCHITECTURE

The research work published in Computer Communications 31 (2008) 2443–2456 has suggested an architecture to facilitate the protection to the SIP Servers from DDoS attacks. Sven Ehlert et al. [E+08] have advised to update the firewall settings and extend the awareness of DDoS for VoIP. The network should be enriched with the Denial of Service prevention capabilities. The following defence mechanism architecture is suggested in the solution.

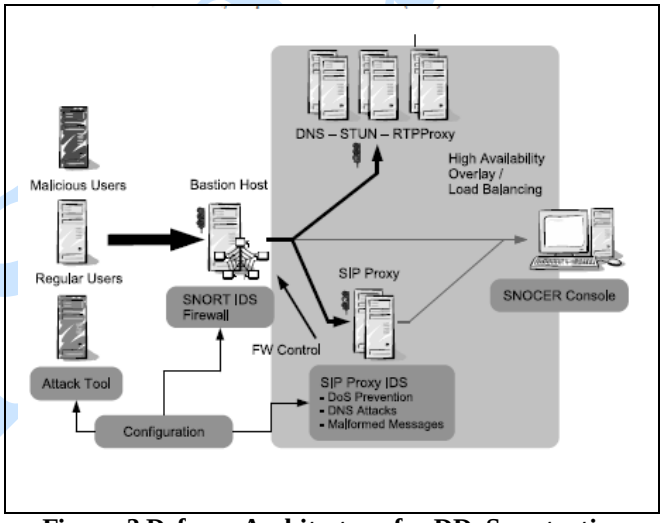

Figure 3 Defense Architecture for DDoS protection

In this architecture Enhanced protected SIP proxy is developed with Deep Packet Inspection module is deployed. An administrative console is developed to detect the intrusion. The architecture is rich with SIP proxy, RTP proxy to establish high availability overlay. The architecture is developed to give protection for flooding defense, DNS blocking defence and malicious messages defence [E+08].

8. DDoS PREVENTION MECHANISM

B. B. Gupta et al. [GJM15] have suggested the prevention of DDoS in different classifications. These are namely General Techniques like disabling unused services, installing latest security patches, Disabling IP broadcast, establishing firewalls, global defense infrastructure and IP hopping. The filtering techniques like ingress egress filtering with inbound and outbound routers establishment, router based packet filtering, history based packet filtering to give

priority to the frequent packets in case of congestion of attack, and capability based packet filtering to provide destination control for better traffic control. Secure overlay service has to be established in VoIP environment to allow the authenticated traffic and stop the suspicious and unauthorised traffic in the network. Finally the prevention mechanism suggested is Source Address Validity Enforcement to alert the routers to update the expected source IP address on each link and IP packet. If any other IP addressed packet is intruded, it should be filtered and stopped [GJM10].

The set of admeasures have been suggested in a research work against DDoS attacks in SIP servers. Defense mechanism against network transport level DDoS flooding attacks are suggested with source based mechanism. The source based mechanism should be developed to prevent network customers from generating DDoS flooding attacks through different tools available in the market place. These should be abolished. The destination based mechanism should be implemented at edge routers or the access routers of VoIP environment. IP Traceback mechanism with packet marking and link testing are useful to filter the unwanted traffic in the network. Management Information Base can help victims to identify the attacked computers with DDoS attacks. It can be possible to identify the computers with ICMP, UDP and TCP packets statistical patterns and parameters [ZJT15].

9. COLLABORATIVE DETECTION SYSTEM

Yu Chen et al. [CHK15] have suggested a collaborative detection system for DDoS attacks over multiple network domains. The collaborative detection system should be implemented at traffic anomaly detection at superflow level. This implementation will enable the traffic monitoring and anomaly detection will be implemented low cost. The second domain is Distributed change-point detection. In this mechanism the collaborative routers should be deployed for distributed change-point detection and alert correlation and aggregation. A hierarchical alert and detection decision making system should be implemented to simplify the alert correlation and global detection procedures. The fourth domain is novelty of Secure Infrastructure Protocol implementation in the form of Trust-negotiating SIP protocol to secure inter-server communications [CHK15].

CONCLUSION

Distributed Denial of Service attacks are regarded as high level damaging and controlling virus like attacks in SIP server network configured by VoIP. The present literature review has discussed in detail about the DDoS origin, configuration and tools to promote. The present paper has discussed the SIS protocol based servers in VoIP configuration and the possible attacks. The paper has concentrated on DDoS attacks and the preventive measures to the attacks. The paper has illustrated different anti-DDoS attacks mechanism & specific architectural and preventive measures.

REFERENCES

[ABS15] **Abdullah Akbar, S. Mahaboob Basha, Syed Abdul Sattar** - *Leveraging the SIP Load balancer to detect and mitigate DDos attacks*, ICGCIoT 2015.

[CN15] **William Conner, Klara Nahrstedt** - *Protecting SIP Proxy Servers from Ringing-based Denial-of-Service Attacks*, published and accessed in 2015 from www.ideals.illinois.edu/bitstream/handle/2142/11469/.

[CHK15] **Yu Chen, Kai Hwang, Wei-Shinn Ku** - *Collaborative Detection of DDoS Attacks over Multiple Network Domains*, IEEE Transactions on Parallel and Distributed Systems, TPDS-0228-0806, 2015.

[E+08] **Sven Ehlert, Ge Zhang, Dimitris Geneiatakis, Georgios Kambourakis, Tasos Dagiuklas, Jirí Markl, Dorgham Sisalem** - *Two layer Denial of Service prevention on SIP VoIP infrastructures*, Elsevier B.V., 2008.

[GJM10] **B. B. Gupta, R. C. Joshi, Manoj Misra** - *Distributed Denial of Service Prevention Techniques*, International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010.

[J+05] **R. Jalili, F. Imani-Mehr, M. Amini, H. R. Shahriari** - *Detection of distributed denial of service attacks using statistical pre-processor and unsupervised neural networks*, Information Security Practice and Experience, pp. 192-203, Springer Berlin Heidelberg, 2005.

[LLG10] **Jin Li, Yong Liu, Lin Gu** - *DDoS attack detection based on neural network*, Aware Computing (ISAC),

2010 2nd International, Symposium on, vol., no., pp.196, 199, 1-4 Nov. 2010.

[M+14] **Muthu Ganesh V., Pravin Kumar D., Vinodini M. S., Abhejit S. K.** - *Survey of Dos Attacks, Detections & Prevention Frameworks for SIP Proxy Server*, International Journal of Innovative Research in Science, Engineering and Technology Volume 3, Special Issue 3, March 2014.

[RAF15] **M. Zubair Rafique, M. Ali Akbar, Muddassar Farooq** - *Evaluating DoS Attacks Against SIP-Based VoIP Systems*, accessed in 2015 from www.startrinity.com/VoIP/Resources/sip22.pdf

[SK12] **Stanek J., Kencl L.** - *SIP Protector: Defense architecture mitigating DDoS flood attacks against SIP servers*, 2012 IEEE International Conference on Communications (ICC), pp.6733-6738, 10-15 June 2012.

[VCM15] **Raghav Vadehra, Nitika Chowdhary, Jyoteesh Malhotra** - *Impact Evaluation of Distributed Denial of Service Attacks using NS2*, International Journal of Security and Its Applications Vol.9, No.8 (2015), pp.303-316, 2015.

[Y+04] **Yu-Sung Wu, Bagchi S., Garg S., Singh N.** - *SCIDIVE: a stateful and cross protocol intrusion detection architecture for voice-over-IP environments*, 2004 International Conference on Dependable Systems and Networks, pp.433-442, 28 June-1 July 2004.

[ZJT15] **Saman Taghavi Zargar, James Joshi, David Tipper** - *A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*, IEEE Communications Surveys & Tutorials, 2015.