ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Survey of Dos Attacks, Detections & Prevention Frameworks for SIP Proxy Server

Muthu Ganesh V, Pravin Kumar D, Vinodini M S, Abhejit S K
Assiatant Professor (Sr.Gr.), Department Of ECE, KLNCE, India
ASP, Department Of CSE, KLNCE, India
Department Of ECE, KLNCE, India
Department Of ECE, KLNCE, India

ABSTRACT: We researched the list of Voice over IP security papers, from a collection of 15 publications on Denial of Service attacks and also we categorized these papers based on their prevention mechanisms. Our objective is to identify the scope of VOIP researches in the area of DoS and to identify opportunities and numerous threats and vulnerabilities present in VoIP systems. We also discussed and analysed the scope of the results provided on those papers and also presented our comparisons among these publications. It seems that the findings in our analysis with respect to Denial of Service reported and prevented in a variety of ways for the VoIP products. Since, we identify specific problem area denial of service, which requiring attention from the research community. Our analysis reveals that the papers of the surveyed works took a lateral view of VoIP systems and that avoids few problems addressed in this area. At last, we laid roadmap for further work on understanding the mechanisms to detect and prevent Denial of Service attacks, which forms the by-product of a highly complex system-of-systems and an indication of the issues in future large-scale systems.

INDEX TERMS – VoIP, SIP, DoS,

I. INTRODUCTION

Today business scenarios are rapidly changing our day to day activities and business trends. In this dynamic environment we need to keep up to present trends. Business needs to understand the consumers and the way the products are reaching the consumers, in today's world the VoIP provides higher flexibility and more features than the traditional telephony infrastructures.VOIP is an advancedcommunication service that enables best use data over IP network.While voiceis the main aspect for communication service, video and other data capabilities(*e.g.*, collaborative editing and filesharing,calendaring) are even included in addition with these communication services [1]. The main advantages of VoIPare flexibility and low cost. The flexibility of VoIP is due to its open architectures and software-based implementations,since most open communities are focused on VoIP are numerous, while the low cost is due to competition, equipment manufacturers andnetwork-link policies, and ubiquitous consumer-gradebroadband connectivity.Because of these benefits, VoIP has seen rapid reach in both theenterprises and consumer markets. Alarge number of enterprisesare replacing their internal phone network with VoIPbasedimplementations, in order to introduce new features and benefits and toefficiently utilize the IP network equipment's rather than spending on traditional communication services. Consumers have introduced to a large number of competitors for broadband connections withdifferent features and costs, includingP2P calling (Skype), Internet-to-PSTN network bridging,and wireless VoIP. These new technologies and businessmodels are being promoted by a new generation of start-upcompanies that are challenging the traditional status quo intelephony and personal telecommunications. As a result, anumber of PSTN providers have already completed or are inthe process of transitioning from circuit-switched networksto VoIP-friendly packet-switched backbones. Since, thecommercial and consumer sectors uses these new

technologies and trends, governmentsand militaries also interested, due to cost reduction concerns and the generaldependence on Commercial off the Shelf (COTS) equipmentfor the majority of their computing needs.

Because of the need to interoperate with theexisting telephony infrastructure, the new features, and thespeed of development and deployment, VoIP protocols andproducts have been repeatedly found to contain numerousVulnerabilities. As a result, a fair amount of research has been directedtowards addressing some of these issues. However, the effort isunbalanced, with little effort spent on some highly deservingProblem areas.

This survey covers 15 VoIP security researchpapers on Denial of Service;our primarygoal is to create a roadmap of existing work in securingVoIP, towards reducing the start-up effort required by otherresearchers to initiate research in this space. A secondary goalis to identify gaps in existing research, and to help inform thesecurity community of challenges and opportunities for furtherwork.

We classify these papers according to the class of threatthey seek to address, we discussour findings, and contrast them with our own perspective of survey onVoIP vulnerabilities.

Paper Organization: Section II provides an overviewof SIP, which is the most popular VoIP technology currentlyin use. Section III summarizes the threats& vulnerabilities definedby the papers on VoIP. Next we discussed the frameworks on securing the VoIP products for both SIP servers and clients on those products. Our conclusion and future direction on denial of service is provided in the last section.

II. SIP BACKGROUND

Session Initiation Protocol (SIP), anopenly available and most widely used technology. Most researchers also focused on SIP, mainly because of its ease of use and the number of free and open-source implementations in open source community.

SIP is a protocol developed &standardized by the Internet Engineering Task Force (IETF), and is designed to support the setup of bidirectional communication sessions including, and also to support VoIP calls. It is similar in few ways to Hypertext transfer protocol, which has a request-response structure, and also uses a mechanism based on the HTTP Digest Authentication[2] for user authentication.

SIP can be a stateful or stateless protocol, which supports interaction with multiple network components (*e.g.*, middleboxes such as PSTN bridges), andasynchronous notifications. While its finite state machine is simple, but in practice it has become quite large and complicated — an observation supported by the fact that themain SIP RFC [3] is one of the longest ever defined, with additional RFCs further extending the specification.

SIP can operate over a number of transport protocols, including TCP [4], UDP [5] and SCTP [6]. UDP is generally the preferred method due to simplicity and performance, although TCP has the advantage of supporting TLS protectionof call setup. SCTP, on the other hand, offers several advantages over both TCP and UDP, including DoS resistance [7], multi-homing and mobility support, andlogical connection multiplexing over a single channel.

In the SIP architecture, the main entities are endpoints (whether softphones or physical devices), a proxy server, a registrar, a redirect server, and a location server. Figure 1 shows a high-level view of the SIP entity interactions. The registrar, proxy and redirect servers may be combined, or theymay be separate entities operated independently. Endpoints communicate with a registrar to indicate their presence. This information is stored in the location server. A user may be registered via multiple endpoints simultaneously.

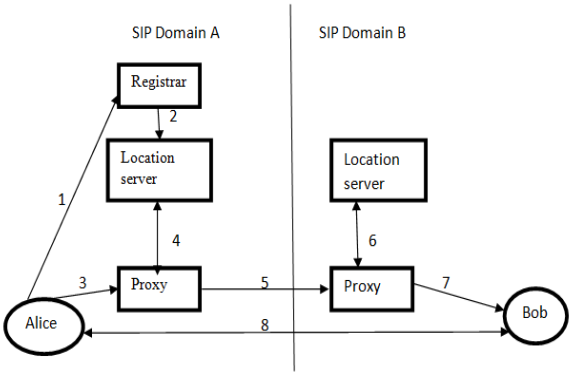

Fig 1 SIP Entity Interactions

During call setup, the endpoint communicates with the proxy which uses the location server to determine where the call should be routed to. This may be another endpoint in the same network (*e.g.*, within the same enterprise), or another proxy server in another network. Alternatively, endpoints mayuse a redirect server to directly determine where a call should be directed to; redirect servers consult with the location server in the same way that proxy servers operate during call setup. Once an end-to-end channel has been established (through oneor more proxies) between the two endpoints, SIP negotiates the actual session parameters (such as the codecs, RTP ports, *etc.*) using the Session Description Protocol (SDP) [8].

Figure 2 shows the message exchanges during a two-party call setup. Alice sends an INVITE message to

the proxy server, optionally containing session parameter information encoded within SDP. The proxy forwards this message directlyto Bob, if Alice and Bob are users of the same domain. If Bob is registered in a different domain, the message will be relayed to Bob's proxy, and from there to Bob. Note that the message may be forwarded to multiple endpoints, if Bob isregistered from multiple locations. While these are ringing (or otherwise indicating that a call setup is being requested), RINGING messages are sent back to Alice. Once the call has been accepted, an OK message is sent to Alice, containing his preferred parameters encoded within SDP. Alice responds with an ACK message. Alice's session parameter preferences may be encoded in the INVITE or the ACK message.

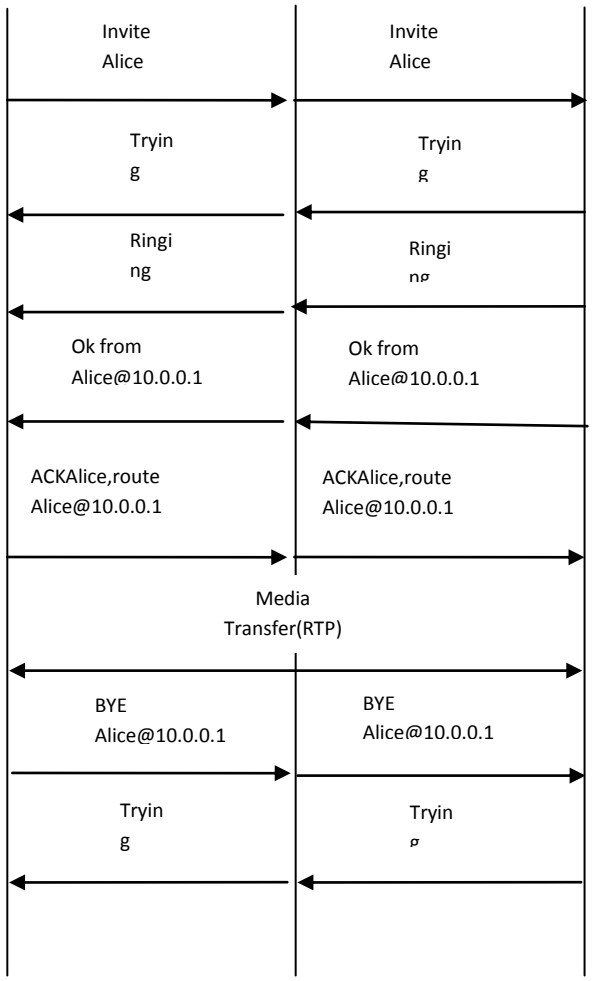

Fig 2 Message exchanges between two party call setup

Following this exchange, the two endpoints can begin transmitting voice, video or other content (as negotiated) using the agreed-upon media transport protocol, typically RTP. While the signalling traffic may be relayed through a number of SIP proxies, the media traffic is exchanged directly between thetwo endpoints. When bridging different networks, *e.g.*, PSTN and SIP, media gateways may disrupt the end-to-end nature of the media transfer. These entities translate content (*e.g.*, audio) between the formats that are supported by the differentnetworks.

Because signalling and media transfer operate independently, the endpoints are responsible for indicating to the proxies that the call has been terminated, using a BYE message which isrelayed through the proxies along the same path as the call setup messages.

The SIP supports call forwarding, conferencing, voice mail, etc. SIP traffic is typically transmitted over port 5060 (UDPor TCP), although the port can vary based on configuration parameters. The ports for the media transfers are dynamic and negotiated by SDP during call setup procedures. Typically, these have to be stateful and understand the SIP exchanges so that they can open the appropriate RTP ports for the media transfer.

For authenticating endpoints, the registrar and the proxy typically use HTTP Digest Authentication, as shown in Figure 3. This is a simple challenge-response protocol that uses a shared secret key along with a username, domain name, a nonce, and specific fields from the SIP message to compute acryptographic hash. Passwords are not transmitted in plaintext form over the network. It is worth noting that authentication may be requested at almost a a call setup.

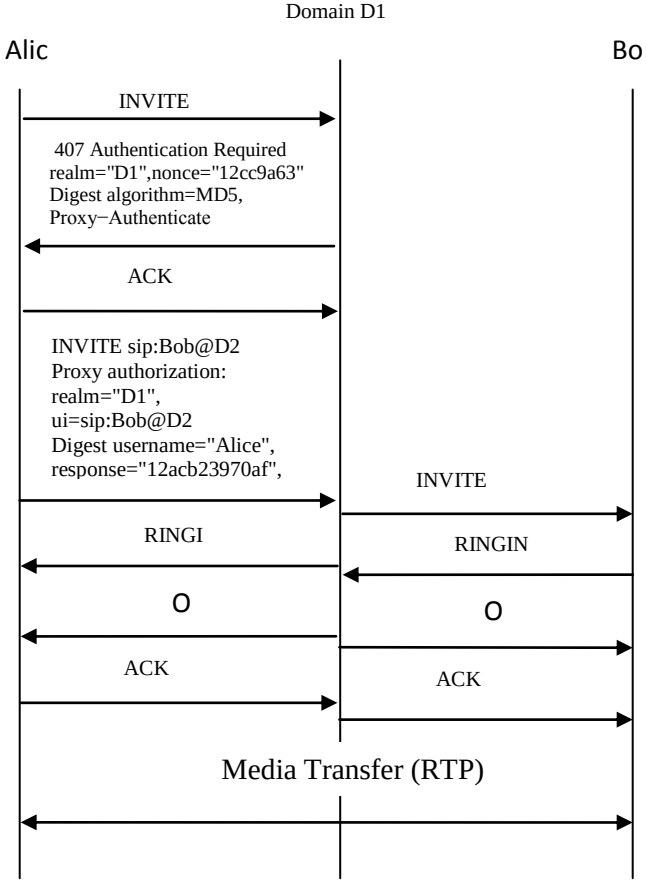

Fig 3 SIP Digest Authentication

For more complex authentication scenarios, SIP can useTCP as the transport protocol;in such cases, TLS can be used to protect the SIPmessages. TLS is required for communication among proxies, registrars and redirect servers, but only recommended between endpoints and proxies or registrars. Alternatively, IPsec [9]may also be used to protect all communications, regardless of the transport protocol. However, because few implementations integrate SIP, RTP and IPsec, it is left to system administratorsto setup and manage such configurations.

III. DETECTION & PREVENTION METHODS

Bremler-Barr *et al.* [10] demonstrated the de-registration attacks in SIP, wherein an attacker can weaken a user by disassociating him with the proxy server and registrar server, or to even divert that user's calls to any party (including to the attacker). This attack works even when authentication is used, if the attacker can monitor the traffic between the client and the SIP proxy server. They demonstrate the attack against several SIP implementations, and proposed a protection mechanism that is similar to onetime passwords. This SOHA, SIP one way Hash function algorithm prevents this attack, by adding a header field into this SIP message. Also, it is backward compatible and no configuration required from the user or the server.

From the figure the first step in the registration is the client chooses a random number x^4. The client then puts in the X-Hash-authenticate-header a number which is equal to applying the chosen hash functions h over x for n times (i.e., *h(h(h(h(x))))*. The client choses the n, but it should be large enough.

The server stores X-Hash-Authenticate-header for all clients it receives. In the next message, the client will send a value in its header which equals to applying h over x for n-1 times.

The solution is the server applies h over this value send by the client and its result with that in the server should be identical from the previous header. If any attacker wants to reverse the hash function, h, she cannot find the next value, even if she catches the traffic between the client and server.

If the n gets close to zero, the client will send two headers in the next message. One is X-Hash-Authenticate which contains the next hash value, and another is X-Hash-Reset, which has a new hash value, by new random number x' by applying the same hash function h, for some n' number of times. When the server receives the message with both of these headers, it resets its stored hash value to the one given in the X-Hash-Reset header field.

Sengar*et al*[11]describe vFDS, an anomaly detection system that seeks to identify flooding denial of service attacks in VoIP. The approach taken is to measure abnormal variations in the relationships between related packet streams using the Hellinger distance, a measure of the deviation between two probability measures. Using synthetic attacks, they show that vFDS can detect flooding attacks that use SYN, SIP, or RTP packets within approximately 1 second of the commencement of an attack, with small impact on call setup latency and voice quality.

They considered an enterprise VoIP service which may receive hybrid packet floods for many protocols, but they analysed on (SYN)-, (INVITE)-, and RTP-related floods, belonging to transport and applications layers carrying call ontrol and audio packets as their threat models.

The vFDS, Hellinger distance is given by,

$$HD_{n+1}^{thresh.} = X * a_n + \eta * v_n$$

The SIP attributes computations and its Hellinger distance is in the figure,

A similar approach, using Hellinger distance on traffic sketches, is proposed by Tang *et al.* [**100]**[12]**,** overcoming the limitations of the previous schemes against multi-attribute attacks. Furthermore, their scheme does not require the constant calculation of an accurate threshold (defining "normal" conditions). Instead it requires sketch based data structures to aggregate high dimensional data streams into smaller dimensions.

This sketch makes our scheme flexible, since it doesn't care about the number of users in the VoIP network; the sketch derives fixed size trafficIt uses the EWMA exponential weighted moving average method to estimate the threshold, for the flooding attack in the SIP, Hellinger distance is used to profile normal traffic behaviours and detectattacks based on probability distributions defined from the sketch tables. The "estimation freeze scheme" presented shows its ability to both protect the threshold estimation from being impacted by the attacks and determine the durations of theattacks. Finally, a voting procedure is applied to assure the detection accuracy. Since we define distributions based on single SIP attributes, our scheme is fully effective to the multiattributeattack. Performance evaluation shows that the scheme preserves high detection accuracy even when the attack rate is very low

Fiedler *et al.* [13] present VoIP Defender, an open architecture for monitoring SIP traffic, with a primary focuson high-volume denial of service attacks. Their architecture allows for a variety of detection methods to be integrated, and several different attack prevention and mitigation mechanisms to be used. Key design goals include transparency, scalability, extensibility, speed and autonomous operation. Their evaluation of the prototype implementation consists exclusively of performance measurements.

The framework, which has been introduced in this work, offers a large variety of functionalities for detection algorithms, like SIP parsing, rule management and scalability features. The architecture consists of many nodes (FSNs, Analyzers, Decider). Currently, when scaling up the system, all components have to be stopped, reconfigured and restarted to reflect the new setup. Therefore it would be desirable to add the feature of a runtime reconfiguration, so that new components can be added

Conner and Nahrstedt[14] describe a semantic-level attack that causes resource exhaustion on stateful SIP proxies by calling parties that (legitimately or in collusion) do not respond. This attack does not require network flooding or other high traffic volume attacks, making it difficult to detect with simple, network-based heuristics used against other types of denial of service attacks. They propose a simple algorithm, called *Random Early Termination* (RET) for releasing reserved resources based on the current state of the proxy (overloadedor not) and the duration of each call's ringing. They implement and evaluate their proposed scheme on a SIP proxy running in a local test bed, showing that it reduces the number of benign call failures when under attack, without incurring measurable overheads when no attack is underway.

Luo *et al.*[15] experimented the vulnerability of SIP protocol to CPU-based denial of service attacks. They usedan open-source SIP server in 4 attack scenarios: basic flooding, spoofed-nonce flooding (in this case the server is forced to check the authenticator in a received message), adaptive-nonce flooding (in this case the nonce is updated sporadically by obtaining a new id from the server), and adaptive nonce flooding with IP spoofing. These measurements show that the attacks can have a large impact on the QoS provided by the servers. They propose several countermeasures to influence against such vulnerabilities, indicating that authentication by itself cannot solve the problem and that, in some situations, it can worsen its severity. These mitigation mechanisms include lightweight authentication and the proper choice of authentication parameters, and binding of the nonce to each client addresses.

Geneiatakis and Lambrinoudakis[16] consider some of the attacks, and propose mitigation through an additional SIP header that is added in all the messages and can cryptographically validate the authenticity and integrity of control messages for each client addresses.

Ormazabal*et al.* [17]describes the architecture and methodology of a SIP-aware, rule-based application-layer firewall that can handle denial of service (and other) attacks in the signalling and media protocols. Therule matching componentuses the hardware acceleration &also achievesfiltering rate of the order of hundreds of transactions per second. The SIP-specific rules, in the SIP aware firewall combined with state validation at the endpoints, allows the firewall to communicateexactly the ports needed for communication only at the local and remote addresses involved in the transactions

Paper Title	**Published year**	**Attack Methods**	**Solution Proposed**	**Criterion**
Unregister attack in SIP[10]	Nov'06	Flooding attack	SOHA	Similar to One Time Password
Detecting VoIP floods using Hellinger Distance[11]	June'08	Multi Attribute Attack	Anomaly Detection System	Hellinger Distance
Sketch Based SIP flooding attack[12]	Nov/ Dec'09	Multi Attribute Attack	Sketch based data structure	Uses the Traffic data's to filter out unwanted data's
VoIP defender[13]	July'07	Vulnerability detection & protection	VoIP defender	Intrusion detection system
Protecting SIP servers from Ringing based DoS[14]	Dec'08	Ringing based DoS attack	Random Early Detection	MRTT(minimum ringing time threshold)
CPU based DoS attacks against SIP servers[15]	Apr'08	4 Attack methods, Basic flood, Nonce based flood, Nonce based flood with IP spoofing	Light weight authentication process	Modification of the Authentication process in SIP
A Cost	Jul	Signalli	Integrity-	Additional

Effective Mechanism to Protect SIP from Signalling attacks[16]	y'08	ng attack	Auth mechanism	Header Value in SIP message with hashing
A Secure SIP – Scalable Prevention mechanism for DoS attacks[17]	July'08	Vulnerability detection & protection	SIP aware firewall design	Dynamic pinhole filter & SIP specific filter
Performance evaluation of flooding detection mechanism[18]	June'09	Flooding attack	Bloom Filter	Only incomplete sessions are monitored, & detected session distance & Threshold to identify floods
Attack analysis & Bio inspired security framework for IMS[19]	July'08	Flooding Attack	Artificial Immune System utilizing negative selection	AIS-IDP uses learning phase to learn about normal behaviour and protection phase to use negative selection algorithm
Application of Evolutionary algorithm in detection of SIP based flooding attacks[20]	July'09	Flooding attack	It uses the different types of classifiers and analyzers	Intrusion detection framework
RTP Miner: A Real time security framework for RTP fuzzing attacks[21]	June'10	RTP fuzzing attack	Analysed the different Classifiers for different situations	Malformed packet headers and payloads
Evaluating DoS attacks against SIP based VoIP systems[22]	Nov/ Dec'09	Flooding attack-Testing 4 Open Source implementations	No Solutions proposed	Performance metrics such as call completion, rejection, latency
Comparative study of anomaly detection algorithm for detecting flooding in IMS[23]	Dec'08	Flooding attack	Analysed the accuracy of flooding attack for 3 detection methods: Adaptive threshold, Cumulative Sum, Hellinger Distance	Synthetic traffic data

Fig 5 Attack Methods and Proposed Solutions

In a specific session, by decomposing and analysing the content and meaning of SIP signalling message headers. They experimented&evaluated the behaviour of their prototype with a distributed testbed involving synthetic benign and attack traffic generation for each client involved in the test bed.

Geneiatakis*et al.* [18]uses counting Bloom filters to detect messages between the User Agents that are part of a denial of service attack in SIP by determining the number of traffic flows where if normal number of pending sessions for a given system are counted and their configurations based on profiling, to estimate the flooding attack and are resolved by the Bloom's filter.

Awais*et al.* [19]describes an anti-DoS architecture which is based on bio-inspired anomaly detection using Artificial Immune System for IDP. They compare their scheme againstsignature based algorithms using synthetic traffic. Akbar and Farooq[20] conduct a comparative evaluation of several evolutionary and non-evolutionary machine learning algorithms using synthetic SIP traffic datasets with different levels of attack intensities and durations. They conclude that different algorithms and settings are best suited for different scenarios.[21]applies anomaly detection techniques to identify Real Time Protocol fuzzing attacks which seeks to cause server crashes through malformed packet headers and payloads **.** They investigated several different classifiers, analyzing their accuracy in both training and testing datasets and performance in different scenarios for different classifiers using synthetic RTP traces.

Rafique*et al.* [22]analyzes the strength and trustworthiness of SIP proxy servers under DoS attacks. They introduce a number of synthesized attacks against four well-known open source SIP proxy servers (OpenSER, PartySIP, OpenSBC, and MjServer). Their experimental results showed that the ease in SIP servers can be overloaded with call requests, causing such performance metrics as Call Completion Rate, Call Establishment Latency, Call Rejection Ratio and number of Retransmitted Requests to deteriorate rapidly as attack volume increases, sometimes with as few as 1,000 packets/second. As an extreme case of such attacks large volumes of INVITE messages can even cause certain implementations to crash. While valuable in documenting

the susceptibility to such attacks, this work proposes no defence strategies or directions.

Akbar *et al.* [23] conduct an analysis of three anomaly detection algorithms for detecting flood attacks in IMS: adaptive threshold, cumulative sum, and Hellinger distance. They use synthetic traffic data to determine the detection accuracy of these algorithms in the context of a SIP server being flooded with SIP messages.

V CONCLUSION & FUTURE WORK

We have tabulated a survey of 15 publications on the topic of VoIP security, categorizing them according to the attack threat models. We tabulated this survey against the analysis on VoIP security vulnerabilities. Weidentified a specific area, denial of service as being not focused much in the research efforts directedat them,which is relative to their status in the vulnerabilitysurvey. Furthermore, we presented the consolidated attack models and their prevention frameworks as being proposed by all the analysed papers in tabular form. We believe thatthis work will simplify the task of taking up research in VoIPsecurity in denial of service in specific.

REFERENCES

[1] Keromytis, A.D., "A Comprehensive Survey of Voice over IP Security Research," *Communications Surveys & Tutorials, IEEE*, vol.14, no.2, pp.514, 537, Second Quarter 2012.

[2] J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, and L. Stewart, "*HTTP Authentication: Basic and Digest Access Authentication*." RFC 2617 (Draft Standard), June 1999.

[3] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "*SIP: Session Initiation Protocol*." RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853, 4320, 4916, 5393.

[4] J. Postel, "*Transmission Control Protocol*." RFC 793 (Standard), Sept.1981. Updated by RFCs 1122, 3168.

[5] J. Postel, "*User Datagram Protocol*." RFC 768 (Standard), Aug. 1980.

[6] L. Ong and J. Yoakum, "*An Introduction to the Stream Control Transmission Protocol (SCTP)*." RFC 3286 (Informational), May 2002.

[7] M. Handley, E. Rescorla, and IAB, "*Internet Denial-of-Service Considerations*." RFC 4732 (Informational), Dec. 2006.

[8] M. Handley, V. Jacobson, and C. Perkins, "*SDP: Session Description Protocol*." RFC 4566 (Proposed Standard), July 2006.

[9] S. Kent and K. Seo, "*Security Architecture for the Internet Protocol*." RFC 4301 (Proposed Standard), Dec. 2005.

[10] A. Bremler-Barr, R. Halachmi-Bekel,and K. Kangasharju, "*Unregister Attacks in SIP*," in *Proc. 2nd IEEE Workshop on Secure Network Protocols*, pp. 32–37, November 2006.

[11] H. Sengar, H. Wang, D. Wijesekera, and S. Jajodia, "*Detecting VoIP Floods Using the Hellinger Distance*," *IEEE Trans. Parallel Distrib.Syst.*, vol. 19, pp. 794–805, June 2008.

[12] J. Tang, Y. Cheng, and C. Zhou, "*Sketch-based Flooding Detection Using Hellinger Distance* SIP," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, pp. 1–6, November/December 2009.

[13] J. Fiedler, T. Kupka, S. Ehlert, T.Magedanz, and D. Sisalem, "*VoIP Defender: Highly Scalable SIP-based Security Architecture*," in *Proc.1st International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, pp. 11–17, July 2007.

[14] W. Conner and K. Nahrstedt, "*Protecting SIP Proxy Servers from Ringing-based Denial-of-Service Attacks*," in *Proc. 10th IEEE International Symposium on Multimedia (ISM)*, pp. 340–347, December 2008.

[15] M. Luo, T. Peng, and C. Leckie, "*CPU-based DoS Attacks Against SIP Servers*," in *Proc. IEEE Network Operations and Management Symposium (NOMS)*, pp. 41–48, April 2008.

[16] D. Geneiatakis and C. Lambrinoudakis, "*A Cost-Effective Mechanism for Protecting SIP Based Internet Telephony Services AgainstSignaling Attacks*," in *Proc. IMS and Mobile Multimedia Workshop*, July 2008.

[17] G. Ormazabal, S. Nagpal, E. Yardeni, and H. Schulzrinne, "*Secure SIP:A Scalable Prevention Mechanism for DoS Attacks on SIP Based VoIP Systems*," in *Proc. 2nd International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*, pp. 107–132, July 2008.

[18] D. Geneiatakis, N. Vrakas, and C. Lambrinoudakis, "*Utilizing Bloom Filters for Detecting Flooding Attacks against SIP Based Services*," Computers and Security, vol. 28, pp. 578–591, October 2009.

[18] D. Geneiatakis, N. Vrakas, and C. Lambrinoudakis, "*Performance Evaluation of a Flooding Detection Mechanism for VoIP Networks*," in *Proc. 16th International Workshop on Systems Signals and Image Processing*, pp. 1–5, June 2009.

[19] A. Awais, M. Farooq, and M. Y. Javed, "*Attack Analysis & Bio-inspired Security Framework for IP Multimedia Subsystem*," in *Proc. GECCO Conference Companion on Genetic and Evolutionary Computation*, pp. 2093–2098, July 2008.

[20] M. A. Akbar and M. Farooq, "*Application of Evolutionary Algorithms in Detection of SIP based Flooding Attacks*," in *Proc. Genetic and Evolutionary Computation Conference (GECCO)*, July 2009.

[21] M. A. Akbar and M. Farooq, "*RTP-Miner: A Real-time Security Framework for RTP Fuzzing Attacks*," in *Proc. 20th International Workshop on Network and Operating Systems Support for Digital Audio and Video (NOSSDAV)*, June 2010.

[22] M. Z. Rafique, M. A. Akbar, and M. Farooq, "*Evaluating DoS Attacks Against SIP-Based VoIP Systems*," in *Proc. IEEE Global Telecommunications Conference (GLOBECOM)*, November/December 2009.

[23] M. A. Akbar, Z. Tariq, and M. Farooq, "*A Comparative Study of Anomaly Detection Algorithms for Detection of SIP Flooding in IMS*," in *Proc. International Conference on Internet Multimedia Services Architecture and Applications (IMSAA)*, December 2008.