Voice over Internet Protocol (VoIP) Security

(A Review Article)

Name: Rebaz Tahir Hamakhan

Subject: Computer Network Security

2024

Voice over Internet Protocol (VoIP) Security

(A Review Article)

Abstract

Voice over Internet Protocol (VoIP) is technology used to transmit multimedia contents through the IP network. From its first deployment it gets to spread widely in communications systems and its use has been increased remarkably. This article is based on the survey of other published works under the security of VoIP title. The first part of this article is an overview of basic VoIP networks. The basic structure of VoIP paradigm is shown. Then the mostly common used protocols, including signaling, media transport, and defence mechanisms, to run the system are presented, and then some of attacks on the security of the VoIP networks with proposed solutions to counter them have been discussed.

Keywords: VoIP, Security, Attack, Defence.

I. Introduction

In communications world, one of the most controlling and dominant technologies is the Voice over Internet Protocol (VoIP) [1]. Since its emergence in the late of 90s, VoIP had been taking over in the telecommunication systems in the world, as a modern technology for transporting multimedia (voice and video) over IP networks [2] [3]. It is the easiest way for data transmission and video conferencing, and to make a phone call through internet by sending packets through packet switched based network [1]. VoIP technology pursues packet switching. The input signal (voice, data, and video) in packet switching, turned into digital form so the other operations become simple. After this the data encoding is processed, to make more secure transmission for the digital data through the channel. The next step is transmitting the signal over the channel with the additional information on the packet block which is sequence number for reassembling the data at the receiver side. At the receiver, the reverse process is required to restore packets and reorder these packets [4].

VoIP systems are not free of threats and attacks. The aim of this article is to overview the VoIP system structure, the protocols that needed for such a system, most probable threats and attacks to VoIP networks, also to provide the security/defence mechanisms for the attacks on VoIP system.

I. Methodology and Research Objective

The descriptive method is used in this review paper; which is type of methodology based on describing previously covered areas in the study of the related field. This article depends on the identifications, explanations, and suggestions of the used techniques for securing the VoIP networks.

The objectives of this review article are to:

- show the basic structure of VoIP network
- present the protocols used for implementation of the VoIP networks, including signalling, transport, multimedia, and also defence protocols
- present the most common threats and attacks on VoIP networks, and the proposed solutions for these threats

II. Survey on VoIP Security Issues

There are many researches concerned with the study of VoIP and its security issues, all of them are based on the threats and attacks to this system. Many of these researches also draw some security designs to encounter these attacks. In this section, the main articles of the VoIP literature concerning the security, threats and attacks, are presented.

Geneiatakis et al. [5] considered that the vulnerabilities in Session Initiation Protocol (SIP) protocol lead to the most of the attacks and threats in VoIP networks, and stated that the SIP protocol requires efficient protection mechanisms. Butcher et al. [6] presented an overview to the VoIP technology, and stated security issues that VoIP infrastructure face, and also showed solutions for future research. Fernandez et al. [7] believed that while multimedia (voice and video) is converged over the packet based data communication, many issues will occur to the VoIP systems. So in [7] several security patterns to face the possible attacks are designed.

All the systems that have a connection with Internet are critically responsive to malicious code which attempts to mess up many possible hosts to cause overcrowding in the infrastructure of the network. VoIP is open to network attacks, such as denial-of-service (DoS) and distributed DoS, malicious code (viruses and Trojans), toll Fraud, eavesdropping, packet spoofing and masquerading, and VoIP spam. These attacks do not damage the infected systems only; they also damage the systems those are not infected even if they are not vulnerable [8].

Walsh et al. [9] explained the ways for analysing the challenges of securing VoIP, and for adopters of VoIP technology, have supplied a series of instructions. Different classes of attacks and various directions for upcoming network attacks are presented by Staniford et al. [10]. Also E. Levi [11] provided the information about malicious logics of sanity worms, which focuses their targets on the generic Web applications. The sanity worms have the ability to spread widely and they are hard to detect and prevent when they infect Web applications. The encrypted malicious software is harder to detect because for any infection it uses a different key or the malicious logic represents itself differently on each new infection [12]. Programmers are in a continuous fight to detect and prevent malicious code attacks; they have suggested a number of intrusion detection systems (IDS). Just like email systems, VoIP systems are susceptible to spam which

termed SPIT (Spam for Internet Telephony). Filtering, black listing, and callers' reputation are techniques for fighting SPIT, but all of these techniques have less effects when SPIT methods are very intelligent [13] [14].

Other attacks that could be directed to VoIP systems are DoS and Distributed Denial of Service (DDoS). DoS attacks occur when disruptive numbers of requests have been sent from a single host to a server, while DDoS attacks are sent from a number of hosts. For the network infrastructure counteract threats, researchers suggested many techniques such as sharing bandwidth and throttling. Demers et al. [15] suggested classifying packets to have both source host and packet sizes so as to minimize the disruptive traffic. Mahajan et al. [16] defined a ''pushback'' mechanism made of the review of dropped packets to find the aggregate signatures which are responsible of congestion (this will be done without separating malicious from non-malicious packets) and then filtering these signatures in a delay queue. Vargas M. Martin [17] suggested a mitigation plan at congestion time, in which the classification of packets to be in equivalent classes. The packet classification is based on how many times the packet has been forwarded.

Moreover, pharming attacks, which lead to another possible DDoS issue to VoIP systems, are evolution for less-developed attack named phishing. The contacted person, either by email or message, is asked by a Fraudulent with seemingly legal request to provide some information. Another type of pharming attack is done by misdirecting very large number of calls to a specified domain to commit a DDoS [18].

Besides what DoS and DDoS threats do to the VoIP system, there is another attack congesting VoIP system called flash-crowds. In flash-crowds, a large number of non-malicious requests have been sent to the same server suddenly. Many researchers proposed attempts to reduce flash-crowds' threat into VoIP systems. Chen et al. [19] presented a flash-crowd reduction system based on the web servers' request regulation. Jung et al. [20] discovered characteristics of flash-crowds and proposed a dynamic load-balancing algorithm design for Web caches by utilizing these characteristics.

III. Basic structure of VoIP network

There are many different forms of VoIP systems, but the basic structure of these VoIP systems has the same functionality. The basic structure is shown in Fig.1. It ensures a smooth understanding of VoIP network. The basic physical structure of VoIP systems can be divided into three categories [15] as follows:

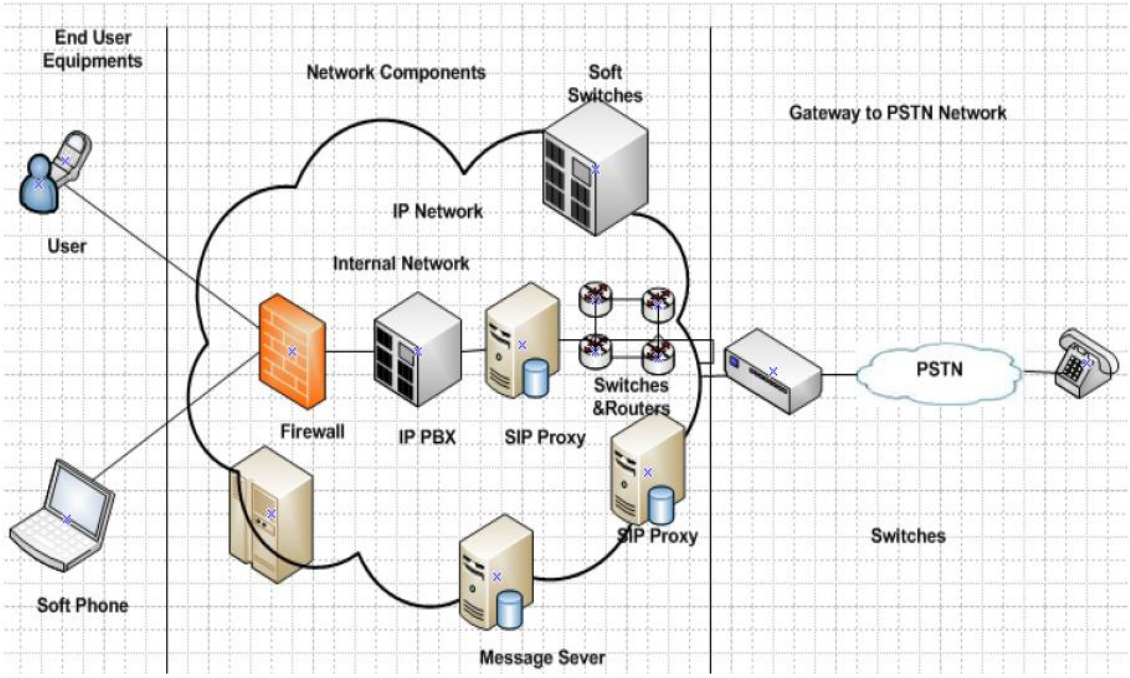

Fig.1. Basic components of VoIP network

A. End-user devices

The interface for voice users to communicate with each other is provided by end-user equipment in VoIP system. These devices consist of “VoIP phones” which have an interface similar to conventional telephone network, and “soft phones” which emulates a telephone. To communicate with the IP networks, end-user devices use TCP/IP protocol. The security of end-user equipment relies on how they are installed; they do not have built-in security features. The Dynamic Host Configuration Protocol (DHCP) server is usually responsible of automatic configuration VoIP phones. It guides the phone to the configuration server which is similar to a call processing server [15] [21]. On the other hand, a soft phone that is installed on software applications on computers and mobiles, would take the features of the VoIP phones [22].

B. Network components

The network components of VoIP system include switches, routers, and firewalls. All of these devices can be named under the main component called the IP-PBX which stands for Internet Protocol-Private Exchange Box [23]. IP-PBX is a central system that manages the calls between VoIP users and telephone through switching and routing many calls simultaneously. IP-PBX switches calls between VoIP and PSTN networks. VoIP uses the IP networks normally makes it vulnerable, the firewall provides the security features to the VoIP system [24]. The advantage of IP-PBX is that it converts voice and data, this provides the flexibility, reduction of long-term operational and maintenance cost for networks of the organizations [21].

C. VoIP gateways/gatekeepers

The device that converts voice calls in real-time between the IP network and the Public Switched Telephone Network (PSTN) in VoIP system is the gateway. The security policies of the gateways will be better if do not introduce any vulnerabilities [25]. The main functions of the gateway in VoIP are compression and decompression of voice, control signaling, call routing, and voice packetization [15] [21]. Additionally a gateway can serve as an interface with external controllers such as Gatekeepers, network management system, billing system, media gateway controllers (MGC), soft switches, and SIP proxies. Malicious attackers can take advantage of these interfaces if they have weakness potentials, so the security framework should be quick and efficient to counter any attack [15].

The gatekeeper is a centrally controlled entity that provides management functions for multimedia in a VoIP such as authentication, address mapping and bandwidth management. It also provides intelligence to the VoIP system. Services such authorization and authentication, addresses resolution, and logging of call detail record, are additional functions of the gatekeeper [25].

IV. VoIP Protocols

The traditional way for making a phone call involves dialling a sequence of digits, which are processed later by the telephone company to ring the called party, and when the call answered a connection formed. Through the call initiation, the communication over the phone is started [15]. To communicate with VoIP, the users enter the calling number, which is a number of telephone or the uniform resource identifier/or (universal resource indicator (URI)). After that based on VoIP signaling protocol a sequence of packet exchange will happen, and once the called party answers, digitization of voice signals is occurred and then divided into a stream of packets to be transmitted based on transport protocol [15].

To deploy any multimedia application such as network gaming, VoIP, or video conference, signaling protocols required to set up the sessions between end points, and a distinguished protocol to transmit the media streams. Between the endpoints of any established session, a standard protocol used to exchange the media streams.

A. Signaling Protocols

The signaling protocol has a major role making the VoIP network components to communicate with each other either by setting up a call or destroy it. A call for IP telephony can be directed between numbers of participants as the multimedia session, while signaling merged with a call is mentioned as a connection. Signaling protocol has many key roles that could be divided into four main functions which are [1];

- Session establishment in which the callee chooses to accept, reject or redirect the call.
- Finding User's location in which the caller has to indicate the location of the callee.
- Call management that gives the permission to the users to leave or join a present session.
- Session negotiation which ensures that the participating endpoints agreed on the session's set of properties.

The signaling protocol of VoIP networks can be divided into two main categories; the first is session control protocols, and the second is media control protocols. Session

control protocols have the responsibility of establishing, protecting and disjoining of call sessions. The negotiation of session parameters such as tones, bandwidth capabilities, and codecs are other responsibilities of session control protocols. H.323 and SIP protocols are the main session control protocols that deal with transporting protocols [1].

1. H.323 Protocol

H.323 is gathering many sub-protocols to set up calls, disconnect calls, recording the calls, authenticating and other functions. It is recommended by International Telecommunication Union (ITU). It uses the Transport Control Protocol (TCP) and the User Datagram Protocol (UDP) as a connection for transporting its protocols [15] [26]. This standard family of protocol provides audio, video, and data transmission bases across networks using internet protocols. Basically H.323 consists of;

- A protocol for registration, admission, and call signaling defined as H.225.
- A protocol for media session establishment and control registered as H245.
- A protocol for conferencing application recorded as T.120.
- A series of protocols to define audio codec named G.7xx.
- A series of protocols to define video codec names H.26x.

2. SIP

SIP is a signaling protocol used for instant messaging, audio, video, internet telephony and conference, online gaming and other multimedia elements. It is developed first by Institute of Electronics and Telecommunication Engineering (IETE) and Internet Engineering Task Force (IETF) defines the SIP standard as an application layer protocol. Unicast or multicast multimedia sessions are created, modified, and disconnected through SIP [15] [26]. The main framework of SIP is to establish sessions, the call details are not focused on. SIP deals with requests from clients and responses to from servers, so it is also called request-response protocol. Requests had been sent by any participant from any transport protocol, are identified by SIP user register location (URL). The determination of the end system session, the communication media and parameters of communication media, and the call response of the recipient are made by SIP. SIP will establish all call parameters, and hold all transfer and ending [27]. SIP supports TCP and UDP as transport connection, makes use of Session Description

Protocol (SDP) which gives the description of sessions and used for coding data, and Real-time Transport protocol (RTP) which delivers voice and video over IP [28].

B. Transport Protocols

The delivery of voice and video over IP network and handling the requirements of applications with real-time characteristics is set by transport protocol. Transport protocol manages the unicast and multicast multimedia data services. It consists of the RTP protocol and real-time transport control protocol (RTCP) which used by both SIP and H.323 protocols [1].

1. Real-time Transport Protocol (RTP)

RTP is prepared for stream data transfer of all real-time, and it is treated as a main voice and video transport standard in IP networks. The data transfer is enabled to multiple endpoints through IP multicast network. RTP is simple protocol and its potential is very good, but it does not make the delivery of the packets sure for the reason that real-time properties of the streams have more importance than the transport reliability [15].

2. Real-time Transport Control Protocol (RTCP)

RTCP is a protocol that works with RTP to monitor the data delivery over large multicast networks. The primary work of RTCP is data collection about the efficiency and quality of the connection. The RTCP observes jitter, one way latency, packet loss, and fraction loss. The RTCP uses the same route of RTP for its messages transport. The media gateway is collecting and responding to RTCP messages. The major drawback of RTCP is that it does not report about the late packets' arrival, but this has been overcome by adding an improvement of "Extended Reports" to RTCP, to be named as RTCP-ER [1] [15].

C. Media Gateway Control Protocols (MGCP)

Media Gateway Control Protocol is used for establishing an interface between two separate VoIP gateways. MGCP is complementary protocol for both SIP and H.323 protocols. MGC server, also known as "call agent", who manages calls and holds up the provided services, is mandatory within MGCP [29].

The media gateway endpoints are unaware of the calls and do not save call states. The commands, which have sent by MGC, are executed by media gateways. There is no mechanism for synchronizing call agents within MGCP. MGCP supposes that MGCs are synchronized with each other to send orders to media gateways under their control [15] [26].

D. Defence Mechanisms/Protocols

In the previous headings, VoIP protocols have been discussed, here the focus will be on the defence mechanisms for VoIP protocols.

1. Signaling defence mechanism

a) H.235

H.323-based systems use the H.235 security framework mechanism to support expanded communications along with key exchange interfacing protocols to provide authentication, confidentiality, and integrity. For the security interests of signaling, control and media communications in the H.323-based systems, the H.235 recommends many procedures, messages, algorithms and structures. End-to-end security, unicast and multicast security are supplied and supported by H.235 mechanism; but H.235 is not a good standard for internet communications because it needs complex implementation compared to SIP-based systems [15].

b) Secure/Multipurpose Internet Mail Extensions (S/MIME)

Application protocols such as SIP are provided with end-to-end authentication, integrity, and confidentiality with the help of S/MIME. An S/MIME encryption technology encodes and represents complex content formats such multimedia messages (e.g., audio, video) and other language characters (e.g., Chinese, Greek) inside other protocols such as SIP. The S/MIME gives an authentication of sender, data confidentiality for Session Description Protocol (SDP), and information integrity within SDP parts of SIP messages. Also due to its infrastructure demands and complexity, it requires more potential to be implemented [30].

c) Internet Protocol Security (IPSec)

By producing secure subways between endpoints, IPSec gives authentication, integrity, and confidentiality for signaling and media streams. Internet Protocol's security

architecture supplies protection to the transport applications that use TCP or UDP. The requirement of IPSec infrastructure should be carefully behold for proper situations to provide a secure channel that can support SIP, RTP, UDP, TCP, etc. [31].

2. Transport Defence Mechanisms

a) SRTP

The profile mechanism for RTP to get authentication, integrity, and confidentiality for media streams (audio and video) is the secure real-time transport protocol (SRTP). SRTP protects RTP packets in both multicast and unicast applications.

Besides providing integrity, confidentiality, and authentication for media streams by SRTP, however; SRTP does not have the ability of maintaining end-to-end message integrity, confidentiality, and authentication for the media streams sent from an IP network to a PSTN network [32].

b) SRTCP

The shape of secure real-time transport control protocol (SRTCP) packet is very similar to SRTP with a small difference of having two additional headers; index of SRTCP and authentication encrypt-flag. These additional headers are encrypted because the contents and the original part of the report need to be protected for holding sensitive information [15].

3. Key Management Mechanisms

The fundamental element for protecting internet multimedia applications is the key management protocol. VoIP is an internet multimedia application; it needs a key negotiation mechanism which adds to the system powerful and extensible capabilities for unicast and multicast communications. Many key management standards exist, while the focus is on the MIKEY and ZRPT which are two key management protocols getting popular in VoIP networks.

a) MIKEY

The Multimedia Internet KEY (MIKEY) is a designed key management protocol for real-time applications, especially used to hold up SRTP. For several security protocols MIKEY affords the negotiation of security parameters and cryptographic keys.

Specified communication protocols such as H.323 and SIP are also provided with independency through MIKEY, and two-way initiation key material model is a feature makes MIKEY suitable for the real-time multimedia scenes [33].

b) ZRTP

ZRTP is a key management protocol to exchange media for unicast secure real-time transport protocol (SRTP) sessions for VoIP. ZRTP does not need additional support in the signaling mechanism because it is multiplexed with RTP on the same port. The main difference between MIKEY and ZRTP is that, ZRTP uses the negotiation of keys for encryption between the two of endpoints while MIKEY uses signaling route. The two endpoints are performing key negotiation directly without involving other intermediate terminals to pass along the keying elements. ZRTP is a better choice than MIKEY in that it requires endpoint software to run and does not demand to additional component. Both MIKEY and ZRTP mechanisms do not support transmitted calls between PSTN and VoIP networks [34].

V. VoIP Security: Attacks and Proposed Solutions

The medium for transmitting voice and other which has been used by VoIP system is Internet. Since the Internet is not a secure medium, the security will be a main problem of VoIP networks which should not be ignored. Usually attackers focus on popular and famous applications and systems. One can steal the identity of a user, Denial of Service, cut off a call, and make other issues to the VoIP network [35].

A. Denial of Service (DoS)

The greatest threat to VoIP systems is Denial of Service (DoS) which can be targeted toward any element of the network directly to disrupt the functionality of the system. The number of available IP addresses bandwidth and router functions are reduced by DoS attacks. The networking capabilities of the identical components such as user's devices, media components, signaling components, billing systems, and security systems are also reduced. DoS attacks stop the servers' service. While a call processing application of VoIP system is getting DoS attack with vast amount of synchronous requests, forcing the application to be shut down and service to be disrupted, thus the service to authorized users is denied [26] [36].

DoS Proposed Solutions

Here are some countermeasures to handle DoS attacks in VoIP systems which include [26]:

- Monitoring and filtering: to look after suspicious users' lists and block them from getting any service and connection.
- Authentication: to ensure from the identity of the user before forwarding any message from his/her side through the network.
- Stateless proxy: to minimize the risk of memory exhaustion attacks, and other security checks such as authenticating users, registering third party, and filtering spam heads to be performed.
- Server design: to create the first line of defence against any DoS attacks from CPU, memory, and network connection.

B. Eavesdropping

Eavesdropping is the attempt to gather sensitive information to get ready for an attack or obtain intelligence. Eavesdropping occurs in VoIP where the attacker has the ability to monitor exchanged signaling or media contents between participant users in order to analyse communications to prepare for the future attacks [15].

Eavesdropping Proposed Solution

There are some strategies recommended to prevent eavesdropping, which are [15]:

- Installation of flawless hardware in VoIP network.
- Ensuring that unauthorized persons are restricted from the access to wiring closets.
- Any vulnerable network point (ex, reception courtesy phone) should be implemented with port-based MAC address security.
- Setting a procedure to scan the network for capturing devices which are running in disorganized mode.
- Besides having additional overhead to VoIP, encryption of VoIP traffic is another solution.

C. Masquerading

Masquerading attack is the ability of the attacker to use a fake network identity such as a user identity, device identity or service identity. The aim of the attacker is to get unauthorized access to a network and its element/s, service and service disruption, or sensitive information. The worst case of masquerading attack is when the attacker gains the control of the identity of a user in the service. Masquerading attack become easier for the attacker in case the authorization and authentication processes are not protected well [15].

Masquerading Proposed Solution

It is better to have a standard strategy that has enough effective encryption technique merged with authentication module to detect any suspected action efficiently [15].

D. Toll Fraud

Toll fraud is one of the most dangerous attacks for telecommunication provider companies and carriers. In toll fraud, the attacker gains unauthorized access to the VoIP services to get personal and financial benefits. There are many ways to achieve toll fraud, either by making changes to the signaling messages or manipulating the billing systems configuration of VoIP system [15].

Toll Fraud Proposed Solution

To prevent toll fraud, the providers and carriers of VoIP can make a proper firewall configuration and protect parts of the network including devices. The providers of VoIP network should also monitor the networks, so that they know who has the access to the network and how many times the participant gets into the network, and who is leading to network traffic type/s [15].

E. Spam over Internet Telephony (SPIT)

SPIT is an unwanted, previously recorded, automated, bulk telephone calls made within VoIP network. The same principle of email spam used for SPIT, but SPIT is more severe than email spam because this type of attack demands a real-time defence mechanism. To explain how SPIT is working, a pre-recorded voice will be sent to many VoIP users within a short time. Due to its depressed costs, SPIT will become a good medium for spammers certainly. The users' privacy and security will be a target to attackers when their IP telephony number is known [26].

SPIT Proposed Solution

Some proposed mechanisms are set to overcome SPIT attacks which are [26]:

- Blacklisting approach; in which let all the coming calls to be from known IP addresses.
- VoIP providers also come up with security measurements for blocking doubtful callers.
- The receivers must be informed not to uncover any important information to the attackers.

VI. Conclusion

For its fast expansion inside communications networks, VoIP technology became a widely used technology for multimedia transmitting including voice and video. Any one may understand VoIP network requirements briefly through a simple explanation of its structure. The VoIP networks require protocols to perform; the basic and widely used mechanisms such as signaling, transport, multimedia, and defence protocols. In order to answer the question related to security issues, some of the attacks targeting the VoIP systems are explained with proposed solutions to encounter and overcome these attacks.

References

[1] S. Jalendry and V. Shradha, "A detail review on voice over internet protocol (voip)," *Int. J. Eng. Trends Technol,* vol. 23, no. 4, pp. 161-166, 2015.

[2] P. Patrick, "voice over IP Security," *Cisco Press,* no. ISBN-10: 1-58705-469-8, 2008.

[3] T. Peter and T. Ari, "Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures," *Addison-Wesley Professional,* no. ISBN-10: 0-321-43734-9, 2007.

[4] A. K. MADHESHIYA, K. S. KALE, S. K. YADAV and J. R. VALVI, "Voice over Internet Protocol (VoIP): A Brief Review," *IRE Journals,* vol. 1, no. 10 | ISSN: 2456-8880, pp. 15-18, 2018.

[5] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambrinoudakis, S. Gritzalis, S. Ehlert and D. Sisalem, "Survey of security vulnerabilities in session initiation protocol," *IEEE Communications Surveys and Tutorials,* vol. 8, no. 1-4, pp. 68-81, 2006.

[6] D. Butcher, X. Li and J. Guo, "Security Challenge and Defense in VoIP Infrastructures," *IEEE Transactions on systems, man and cybernetics,* vol. 37, no. 6, pp. 1152-1162, 2007.

[7] E. B. Fernandez, J. C. Palaez and M. M. Leonardo-Petrie, "Security Patterns for VoIP Networks," in *International Multi- Conference on Computing in the Global Information Technology*, ISBN: 0-7695- 2798-1, 2007.

[8] M. Bishop, COMPUTER SECURITY: RT AND SCIENCE, New Jersey: Addison-Wesley, 2003.

[9] T. J. Walsh and D. R. Kuhn, "Challenges in securing voice over IP," *IEEE Security & Privacy,* vol. 3, no. 3, pp. 44-49, 2005.

[10] S. Staniford, V. Paxson and N. Weaver, "How to Own the Internet in your spare time," in *Proc. 11th USENIXSecurity Symp.*, San Francisco, USA, 2002.

[11] E. Levi, "Worm propagation and generic attacks," *IEEE Security & Privacy,* vol. 3, no. 2, pp. 63-65, 2005.

[12] C. Nachenberg, "Computer virus-antivirus coevolution," *Comm. Of the ACM,* vol. 40, no. 1, pp. 46-51, 1997.

[13] S. L. Pfleeger and G. Bloom, "Canning spam: Proposed solutions to unwanted email," *IEEE Security & Privacy,* vol. 3, no. 2, pp. 40-47, 2005.

[14] K. Wang and S. J. Stolfo, "Anomalous payload-based network intrusion detection," in *Proc. Of the 7th Int'l Symp. on Recent Advances in Intrusion Detection*, Sophia Antipolis, France, 2004.

[15] S. Phithakkitnukoon, R. Dantu and E. A. Baatarjava, "VoIP security – attacks and solutions," *Information Security Journal: A Global Perspective,* 2008.

[16] R. Mahajan, S. M. Bellovin, S. Floyd, J. Joannidis, V. Paxson and S. Shenker, "Controlling high-bandwidth aggregates in the network," *ACMSIGCOMM Computer Communication Review,* vol. 32, no. 3, pp. 62-73, 2002.

[17] M. V. Martin, "A Monitoring system for mitigating fast propagating worms in the network infrastructure," in *Proc. IEEE Canadian Conf. on Electrical and Computing Eng.*, Saskatoon, Canada, 2005.

[18] P. C. Hung and M. V. Martin, "Security issues in VoIP applications," in *Canadian Conference on Electrical and Computer Engineering*, IEEE, 2006.

[19] X. Chen and J. Heidemann, "Flash crowd mitigation via adaptive admission control based on application-level measurement," *Technical Report ISI-TR-557,* 2002.

[20] J. Jung, B. Krishnamurthy and M. Rabinovich, "Flash crowds and denial of service attacks: Characterization and implications for CDNs and web sites," in *Proc. ofthe 11th International World Wide Web Conference*, Honolulu, USA, 2002.

[21] O. O. Ayokunle, "Integrating Voice over Internet Protocol (VoIP) technology as a communication tool on a converged network in Nigeria," *International Journal of Information and Communication Technology Research,* vol. 2, no. 11, 2012.

[22] M. Desantis, "Understanding Voice over Internet Protocol (VoIP)," *US-CERT,* 2008.

[23] Ramachandran, "VoIP Security: asserting the trust boundary," *The Global Voice of Information Security ISSA Journal,* pp. 8-13, 2006.

[24] W. Chou, "VoIP network security," *IT Professional magazine,* vol. 9, no. 5, p. 42–46, 2007.

[25] R. Dhamankar, "Intrusion Prevention: The Future of VoIP Security," *White paper by Tripping Point,* 2005.

[26] S. S. Kumar, R. Singh, R. Chauhan and A. Singh, "A Review Paper: Security on Voice over Internet Protocol from Spoofing attacks," *International Journal of Advanced Research in Computer and Communication Engineering,* vol. 1, no. 3, 2012.

[27] H. Schulzrinne and J. Rosenberg, "A Comparison of SIP and H. 323 for Internet Telephony," in *In Proc. International Workshop on Network and Operating System Support for Digital Audio and Video*, 1998.

[28] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Spark and E. Schooler, "SIP: session initiation protocol," 2002.

[29] A. Karim, "VoIP Performance Over different service Classes under Various Scheduling Techniques," *Australian Journal of Basic and Applied Sciences,* vol. 5, no. 11, pp. 1416-1422, 2011.

[30] B. Ramsdell, "Secure/multipurpose Internet mail extensions (S/MIME) Version 3.1 Message Specification. RFC 3851," 2004.

[31] S. Kent and R. Atkinson, "Security architecture for the Internet protocol. RFC 2401," 1998.

[32] M. Baugher, McGrew, D. Nashund, E. Carrara and K. Norman, "The secure real-time transport protocol (SRTP). RFC 3711," 2004.

[33] J. Arkko, E. Carrara, F. Lindholm, M. Nashund and K. Norrman, "MIKEY: Multimedia Internet KEYing. RFC 3830," 2004.

[34] P. Ziemmermann, "ZRTP: Media path key agreement for secure RTP," 2008.

[35] H. Dawood, "IPv6 Security Vulnerabilities," *International Journal of Information Secirity Science,* vol. 1, no. 4, pp. 100-105, 2012.

[36] A. Kumar, "An overview of voice over internet protocol (voip)," *Rivier college online academic journal,* vol. 2, no. 1, 2006.