A survey of Attacks on VoIP networks and Countermeasures

Julius N. Obidinnu [1] and Ayei E. Ibor [2]

[1,2]Department of Computer Science,
Cross River University of Technology, Calabar, Nigeria.
Email: *obijulius@yahoo.com[1], ayei.ibor@gmail.com[2]*

Abstract

There is a fast pace of growth in the use of Voice over Internet Protocol (VoIP) networks owing to the fact that more organisations are deploying IP based voice networks. This invariably has a security concern for the payload as the traffic on IP based voice networks is exposed to threats similar to those found on regular data traffic. Realising end-to-end security has been influenced by numerous exploits targeted at VoIP networks with attendant lower rate of calls than the traditional telephone system. Although the requirements for security as well as accessibility for voice traffic are dissimilar as compared to data traffic, it is equivalently significant to protect this payload from attacks such as spoofing, eavesdropping and man-in-the-middle attacks. These security concerns, due to the flexibility of the VoIP system with corresponding convergence of the voice and data networks pose a plethora of threats to the confidentiality, integrity and availability of the services rendered on VoIP networks. In this paper, the various threats, vulnerabilities and attacks on VoIP networks as well as countermeasures for mitigation will be examined. Finally, the direction for future research work on robust solutions for attack mitigation will be highlighted.

Keywords: VoIP; Security; Threat; Vulnerability; Attack vector; Countermeasures.

1.0 Introduction

Voice over Internet Protocol (VoIP) is a network that allows users to transmit digital voice information in discrete form, in such a way that voice calls can be placed with the use of the Internet, rather than deploying the services of the traditional Public Switched Telephone Network (PSTN). Zhao & Ansari in [6] asserts that with VoIP, calls can be made using the computer, VoIP phones as well as traditional phones. The use of VoIP networks for voice calls and data transmission has been on the increase in recent years. This increase in the use of VoIP networks may be considered as a factor of flexibility for both businesses and individuals as well as lowered cost of delivering telecommunication services. This view is agreed by [8], [6], [4] and [2] who assert that cheaper call rates for local, long distance as well as international calls is one of the benefits of the VoIP technology. Telephone calls can be made with IP and Soft phones – for instance Skype and instant messages can be sent from a computer system. This trend paves way for large amount of traffic and payload being transmitted by the VoIP resulting in the increase in attacks and exploitation of the VoIP services.

As opined by [4], the popularity of the application of VoIP networks has attracted the attention of attackers, who try to have unauthorised access to transmitted data

and information in a bid to achieve financial gains or the mere fun of it.

Several attacks such as Session Initiation Protocol (SIP) flooding as described in [2] and [5], denial of service in [1], eavesdropping, spoofing and man-in-the-middle are commonplace. An insight into the unpredictable nature of what the future holds for the security of VoIP is given in [3]. These attacks pose serious challenges to the realisation of end-to-end security of VoIP networks data transmission [1]. The proliferation of these attacks largely emanate from the various weaknesses in the existing VoIP networks, as described in [7] and [4]. More so, restricted access to information on the exploits and incidents involving VoIP systems impede the growth in the development of effective defence vectors against these attacks [3].

In view of the identified weaknesses above, this paper reviews relevant literatures to provide information that will guide network and system administrators as well as security professionals to identify the existing vulnerabilities, attacks and countermeasures in VoIP networks.

Identifying Voip Security Issues: Threats and Vulnerabilities

The development of IP networks in relation to shared media communication exposes the network to security breaches.
In discussing the security issues predominant in VoIP networks, the following security components shall be identified as classified in [9]:

i. Security constraints: these include all the items for which security is considered a problem in any information infrastructure. System assets, vulnerabilities and threats fall in this category.

ii. Security requirements: these are designed to resolve (or fix) vulnerabilities as well as eradicate threats. They comprise of various mechanisms, services and the policies that need to be used to resolve the identified security problems.

iii. Security management: in addressing security, a range of decisions would be made on the tasks and operations with respect to the standards, tools and the legal policies needed to support definite business functions and processes.

Attackers can exploit any of the vulnerabilities in these components as most of these vulnerabilities have similarities to those available on public-switched telephone networks. While threats specifically identify the attack source and means, vulnerabilities comprise security flaws (such as wrong configurations, open ports, etc), which are exploited to conduct a successful attack. This is highlighted in [10], asserting that VoIP has a range of security issues similar to most Information Technology infrastructures including the network and physical security of devices such as computers, routers, switches, servers, VoIP phones and several other devices that constitute the VoIP system. One of the most common vulnerability of the switched telephone system – avesdropping, which is achieved through the physical use of a listening device placed on the phone line, is also possible on VoIP networks. It is stated in [9] that it is possible for an attacker to use a listening device such as a packet grabber on the network when he has physical access to the TCP/IP (Transmission Control Protocol/Internet Protocol) network in order to eavesdrop a conversation between two parties.

There are other vulnerabilities, which mimic those available on most data networks. Since VoIP uses the existing platforms such as Linux and Windows operating systems, which have a wide range of attack vectors (especially the Microsoft Windows operating system) it is likely that VoIP servers (control and gateway) and the entire network are vulnerable as well. VoIP as a packet-based network requires the configuration of parameters such as IP addresses and MAC (media access control) addresses.

With a majority of the devices and programs on a VoIP such as routers, firewalls, voice terminals as well as call processing components, which are used for call placing and routing, requiring the establishment of network parameters (e.g. IP and MAC addresses) dynamically, in the event of restarting or adding a network or VoIP telephone, there is a wide attack space of vulnerable spots for intruders [9].

When security measures are to be considered, confidentiality, integrity and availability of the traffic and payload should be of high priority. As shown in figure I, every security measure should be assessed based on whether it can be compromised or not with respect to these factors. While threats to confidentiality involve the disclosure of conversation between two users (say Bob and Alice), call data such as dialled telephone numbers, duration of calls etc, threats to integrity target the alteration of the call message, call record logs, trusting the identity of the caller as well as that of the recipient. Threats to availability endanger the making or receiving of calls [10]; [9].

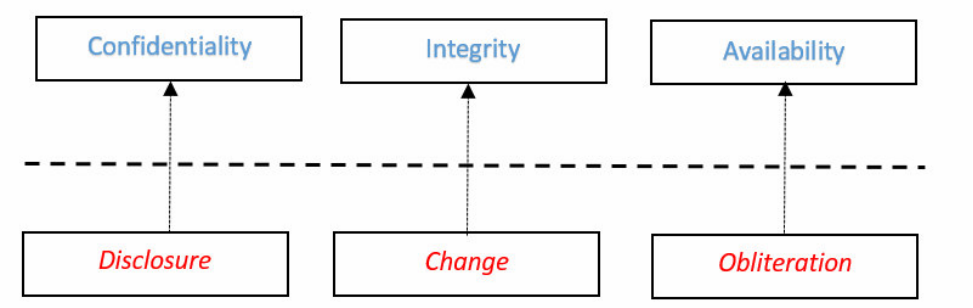

Figure 1: Threats to Confidentiality, Integrity and Availability

Exploiting vulnerabilities in a VoIP system may be due to some factors including benefits such as free access to phone services, free access to long distance services, the sheer committing of fraud by spoofing the identity of others, eavesdropping on a phone line in order to commit fraud and gaining an infamous status by frequently upsetting normal services on the VoIP network [9]. As discussed in [4], the protocols that are used to establish and manage calls can also be one of the sources of vulnerabilities in VoIP networks. This is due to the fact that the transmitted packet headers and payload may not be encrypted. Consequently, an attacker can inject specially crafted packets into the normal traffic in order to manipulate the state of devices and calls. The main threats connected with the VoIP technology as shown in [11], [9], and [12] will be briefly discussed below:

- *Eavesdropping*: this threat impacts on confidentiality. The attacker typically monitors the conversation between two VoIP end-points, that is, the signalling or data stream or both between the communicating parties is received by the attacker who may replay the conversation to extract the contents. These contents can be used to commit crime. Apart from the voice conversations, data conversations transmitted across a VoIP system are also subject to eavesdropping. Examples of these include the transmission of fax data, dual-tone multi-frequency (DTMF) data for obtaining bank and credit card passwords etc.
- *Vishing*: This involves the spoofing of both the VoIP and caller ID. Vishing is

usually concealed behind fake financial organizations, which demand confidential information such as credit card numbers from users. In contrast to phishing, it directed unsuspecting users to call a phone number for which they were asked to reveal their account information.

- *Denial of Service (DoS):* According to]13], in DoS, an attacker is able to disrupt normal services on a phone system. The aftermath may be not being able to make or receive calls on the entire network, or in some cases a specific range of phone numbers may be targeted. DoS impacts on availability and may include performance latency, physical intrusion, loss of external power supply and the exhaustion of resources on the network.

- *Toll fraud:* an attacker accesses a VoIP network in order to place illegal international or intercontinental calls. This impacts on the integrity of data as weak passwords and usernames can be exploited by hackers.

- *Alteration of Voice Stream:* this is otherwise known as a man-in-the-middle (MITM) attack as shown in figure 2. It impacts on the confidentiality and integrity of communication between two parties. In this scenario, the attacker can listen and alter the conversation between two parties. In doing this, the attacker can replay previously captured conversation in a bid to trick the receiver to listen to a different message from the one transmitted by the sender. Altering a conversation with contents such as 'power on' to 'power off' or 'stop' to 'start' would have great impact on the outcome of the conversation. Alteration of voice streams could allow an attacker to exploit an interactive voice response phone system. Assuming an attacker has initially intercepted the financial password such as a PIN (personal identification number) of a victim and used it to withdraw funds from an account, the attacker could use the man-in-the-middle attack to replay a pervious balance when the victim places a call to the interactive voice response system requesting for an account balance. This may give the victim wrong information thereby making him believe that there were no withdrawals of funds on his account

.

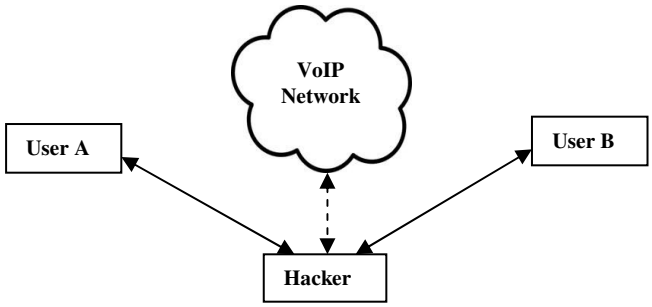

Figure 2. Man-in-the-middle (MITM) attack

- *Call redirection:* Butcher et al in [9] discusses that this feature of the VoIP system allows a user to redirect his call to a location of his choice. If compromised, this feature poses a potential security risk as the attacker can conveniently redirect the phone number of the victim to any location he chooses. In this way, the attacker can impersonate the victim when he redirects the victim's calls to his phone.

- *Masquerading:* this is a situation where an attacker is able to impersonate a VoIP Server. The attacker can then trick the victim to forward requests to this server. This can reveal a lot of confidential

information to the attacker while providing no services to the victim.

- *Spam over Internet Telephony (SPIT):* Scatá & Corte in [11] described SPIT as a variant of email spam that can be considered as a social threat. SPIT involves the generation of unsolicited communications such as unwanted calls, unsolicited advertisements, which are used to perturb users and can also include telemarketing calls, which are meant to influence users in the sale of products. In [10], SPIT is identified as a potential risk to subscribers in terms of the usage of bandwidth and cost.

- *Physical access threats:* As opined by [7] and [12], the threats such as physical access include illegal access to VoIP equipment or access made to the network's physical layer. It is highlighted in [11] that physical threat can compromise entry systems using lock and key, surveillance and alarm systems, as well as allow intruders to make unauthorized changes to configurations and intentionally shut down power systems.

- *Social threats:* Social threats are classified in [7] as those threats, which target humans. Such threats include wrongly configured parameters, bugs or bad protocol communications in VoIP system that may allow a malicious user to impersonate legal parties. This can provide a basis for a more severe attack scenario such as service theft, phishing, or spam.
- *Service interruption:* this threat involves the inability to access VoIP services due to non-intentional circumstances such as loss of power, exhaustion of resources from over-subscription and call quality degradation due to the decline of performance standards [7].
- *Call hijacking and spoofing:* In this scenario, a phone's identity (phone number), which is associated with a device can be spoofed by an attacker in a bid to place or receive calls thereby impersonating the victim. As examined in [9], all an attacker needs to do is to setup his VoIP phone device so that the identity of the victim's device is used. On the successful completion of the attacker's device registration on the phone system, incoming calls to the victim's phone number would be redirected to the attacker's phone. Impersonating a victim in this way can lead to divulging and altering confidential information including bank or credit card details since most banking applications may rely on caller identity to authenticate a customer. This impact greatly on integrity.

3.0 Attacks On Voip Networks

The vulnerabilities in VoIP networks can be exploited by attackers. The consequences of exploiting these vulnerabilities including interruption of media services through the flooding of traffic, having access to confidential and classified information when call signals or contents are intercepted, impersonating servers hence being able to hijack calls, and identity spoofing resulting in the free use of services as well as the placement of fraudulent calls are highlighted in [8]. This invariably will impact the security of users underpinned by confidentiality, integrity and availability. To this effect, the various attacks on VoIP networks will be discussed below:

- *Signal protocol tampering*: this attack is targeted at the call set up process. It involves the attacker being able to monitor and capture the packets during call set up. The attacker, through this process, can alter the data stream fields. This will enable him to place VoIP calls devoid of a VoIP phone. Coulibaly & Liu in [7] explained that this malicious user may also be able to place expensive calls which the IP-

PBX (Internet Protocol Private Branch Exchange) can connect to another user.

- *Repudiation attacks*: in this attack, a conversation between two parties can be denied by one party.
- *Registration hijacking of session initiation protocol (SIP)*: In a VoIP network, establishing, modifying and terminating user sessions can be handled by SIP, which is an application layer control protocol. As demonstrated in [7], [9] and [4], SIP as well as other VoIP protocols requires the registration of a user agent (UA/IP phone) with the control node of a SIP proxy/registrar so that inbound calls are directed by the proxy to the phone. An attacker, who is aware of this process, can perform Registration hijacking by impersonating a valid UA to the registrar. This allows the attacker to modify the genuine registration to his own address. As a consequence, inbound calls sent to the valid UA will be redirected to the rogue UA resulting in loss of calls to the targeted UA. Victims in this category may include individual and/or group of users as well as a media gateway or voice mail system identified as a high traffic resource. If this attack is successful, inbound calls will be affected and the rogue UA can record the contents of calls.

i. IP Spoofing: this attack involves using an internal or external trusted IP address to impersonate a trusted computer. In [7], it is asserted that IP spoofing attacks can be used as the pivot for other attacks such a Denial of Service (DoS) attack in which case the hacker is able to hide his identity with the use of spoofed source addresses. This may result in the spoofing of the address of the IP-PBX, when adequate defence mechanisms are not put in place causing the entire voice segment to be flooded with UDP (user datagram protocol) packets.

Message Modification of SIP: Since a SIP message does not have an inbuilt mechanism for checking the integrity of the message sent, it is possible that an attacker is able to intercept and make modifications to a SIP message using a man-in-the middle (MITM) attack such as IP spoofing, MAC (media access control) spoofing, or SIP registration hijacking. In doing so, the attacker can make changes to all or some of the attributes of the message thus impersonating the caller or being able to redirect a call to another destination without the knowledge of the caller [9].

- *Malformed Messages and SIP Command*: Gruber et al in [14], identified two categories of malformed messages. These include structure and syntax malformed messages. Although structure malformed messages conform to the RFC 3261 syntax and as such do not infringe on the rule of the SIP protocol, the complexity of the message increases the time the parser uses to execute the message. This can lead to buffer overflow when a VoIP system is poorly implemented. On the other hand, syntax malformed messages violate the RFC 3261 syntax so that parsers are not able to classify the messages received. Consequently, the testing of the SIP parser with every input possible may become difficult. As argued in [9], this vulnerability if exploited by an attacker can allow him send packets with malformed command to vulnerable nodes. This may disrupt normal services to that node.
- *Identity theft*: this type of attack allows a malicious user to acquire a valid identity from a legitimate user of the VoIP system. Some variants of identity theft including brute force and dictionary attacks are described in [14]. In the brute

force attack, the attacker is able to transmit random mishmash of characters to the SIP proxy and the message response sent back to the attacker may allow him steal the valid identities of other users. However, in the dictionary attack, the attacker carefully sends a list of words to the SIP proxy with possible names and passwords. The response message from the proxy enables him to identify likely accounts.

ii. *Service theft*: this attack is targeted at the service provider in a bid for an attacker to make free fraudulent calls. Loopholes in the configuration of the VoIP system can allow a malicious user to bypass the billing system, abuse the use of the resources on the VoIP network and/or user resources. Furthermore, Zhang & Huang in [15] argues that the consequences of service theft can include degradation in the performance of the VoIP system and increase in the expenses incurred by the operator in the delivery of quality services. However, Coulibaly & Liu in [7] states that service theft can result in toll fraud where an attacker can place or make calls using an unattended IP phone, spoofing the identity of a valid user of the phone or by placing a rogue IP phone on the network or breached gateway.

- *Cancel/Bye SIP attack*: In this attack scenario, a SIP message can be crafted by an attacker such that the payload of the message contains the Cancel or Bye command. This message is then sent to the target (an end-node or phone). When a constant stream of these packets is sent to the target phone, it may disrupt services on the end-node so that the phone may not be able to make or receive calls. If the attack space is increased to include more phones, it can lead to a distributed denial of service (DDoS) [9], [2].
- *Session initiation protocol (SIP Redirect attack*: An attack on a SIP redirect server will allow a malicious user to redirect calls meant for a victim to a number chosen by him. This is because a server application used by SIP is able to receive phone or proxy requests and give back a redirect response with information on where to retry the request. The possibility of redirecting a call to a different phone can allow the attacker to disable the phone network by redirecting all the phone numbers of users to a non-existing device [9].
- *Real-time Transport Protocol (RTP) payload attack*: a malicious user can use a man-in-middle (MITM) attack to intercept and modify (or inspect) the payload of an RTP media stream message. As stated in [6], [15] and [9], the encoded voice message between two nodes (callers) is conveyed by the RTP protocol. This protocol extends the functionality of the User Datagram Protocol (UDP) through the addition of sequencing information. This means that an attacker who can inspect the payload of the message is able to eavesdrop on the conversation between two callers. Also, if an attacker can modify the message, then he would be able to alter the meaning of the conversation by injecting his own message or in another case introduce noise to degrade the quality of the message. This is further clarified in [7] that a hacker who uses the tcpdump tool can easily locate the IP and Media Access Control (MAC) address of the phone he intends to target for an attack. The use of an Address Resolution Protocol (ARP) spoofing tool could allow an attacker to successfully impersonate a local gateway as well as the IP phone on a particular network segment. This may result in a malicious user being able to intercept a call by using a phone with a spoofed MAC address, which he can insert

into the voice segment to assume the identity of the target phone.

- *Tampering attack on the Real-time Transport Protocol (RTP)*: The RTP packet has two fields in its header that can be manipulated by an attacker. These fields are the sequence number and the timestamp fields. The attacker can successfully alter the sequence of the packet and make the conversation meaningless or cause the phone (node) receiving the packet to go offline [9].
- Other attacks similar to those obtainable in data networks include Transmission Control Protocol (TCP) SYN flood, TCP or UDP replay, Physical attack on VoIP infrastructure, Dynamic Host Configuration Protocol (DHCP) starvation, Trivial File Transfer Protocol (TFTP) server insertion, Internet Control Message Protocol (ICMP flood, Buffer Overflow attack, Operating System attack, Viruses and Malware and Call Detail Recording (CDR) Database attack [9].

4.0 Countermeasures and Defence Vectors

The mitigation of attacks on VoIP networks requires effective countermeasures and defence vectors, which should be geared towards protecting the network infrastructure, resources and users from unauthorised access and abuse. This section will examine the most pertinent countermeasures as discussed in [9], [13], and [11], which should be implemented to prevent attacks on VoIP networks from being successful. It is noteworthy to mention here that one of the

defence vectors against most VoIP attacks is port authentication based on the 802.1x protocol standards. This is emphasised by Butcher et al in [9], stating that with port authentication, a device, which must connect to the wired or wireless network, must be authenticated by a central authority. Access is only granted to the device when it is identified by the authenticating authority as a valid device. On the other hand, access is denied if the device is identified as a rogue device and as such can prevent an attacker from adding his device to the network or having access to the network at any point in time. Also, [16] presented a system called VoIP Shield that can mitigate attacks on a VoIP system by protecting the end user and the proxy server against the manipulation of SIP packets for malicious intent. However, this system does not seem to be able to block an attack on the Domain Name System (DNS) though it was able to mitigate the exploitation of the SIP protocol by a malicious user. The attacks discussed above and their countermeasures will be represented in Table I below :

Table I. Countermeasures for VOIP attacks

VoIP Attack	**Countermeasure and defence vectors**
Signal protocol tampering	Using strong authentication to validate network users as well as encrypting transmitted packets can help prevent against this attack. The use of Virtual Private Networks (VPNs) such as Internet Protocol Security (IPSec) tunnel based VPNs can help provide high end security to mitigate this attack.
Repudiation attacks	This attack can be prevented through the use of non-repudiation techniques such as digital certificates to authenticate the origin of data to be from a trusted party.
Registration hijacking of session	Use of Transport Layer Security (TLS). TLS should be used to

initiation protocol (SIP)	establish an authenticated secure connection between the User Agent (UA) and control node.
IP Spoofing	Port authentication and the separation of VoIP and non-VoIP traffic using Virtual Local Area Networks (VLANs)
SIP message modification	Transport Layer Security (TLS) should be implemented to protect the UDP and TCP transport mechanisms. This will in turn protect the SIP message and as such an attacker will not be able to read or modify the SIP message nor identify the parties participating in the call.
Malformed messages and SIP command	The use of a strong authentication mechanism to prevent an attacker from being able to transmit malformed messages and SIP commands to a user (node or phone). Providing end-to-end encryption in which the users engaged in a conversation can first of all exchange a secret key pair that will be used to encrypt the transmitted message such as the use of IPSec based encryption (end-to-end) can help prevent this attack.
Identity theft	Use of cryptography and authentication mechanisms such as IPSec (Internet Protocol Security) to properly validate users before allowing them access to the resources on a network.
Service theft	Hardening the network gateway with the use of firewalls, use of VPN and authentication protocols.
Cancel/Bye SIP attack	Addition of strong authentication to the message exchange between the User Agent (UA) and the control node will allow the UA to identify and verify the origin of the Bye command. A Bye/Cancel command from a trusted node should have a valid certificate.
Session Initiation Protocol (SIP) Redirect attack	Use of strong passwords for authentication over Transport Layer Security (TLS) is one way to prevent against this attack. Other methods include port authentication, separation of VoIP and non-VoIP traffic using VLANs and signalling authentication with IPSec.
Real-time Transport Protocol (RTP) payload attack	Encryption of transmitted packets through the use of the Secure Real-time Transport Protocol (SRTP) – RFC 3711. In this way, eavesdropping on packets as well as the modification of the packet contents will be prevented. This attack can also be prevented by using port authentication and VLANs for VoIP traffic.
RTP tampering	One effective way to

	prevent RTP tampering is by separating the traffic of VoIP from the normal data traffic on a network. Implementing a Virtual Local Area Network (VLAN) for VoIP traffic different from the data traffic will increase the difficulty for an attacker to have access or modify the VoIP traffic.

5.0 Discussion and Conclusion

The fast pace of growth witnessed by the VoIP network came with corresponding security issues. In this paper, the various threats, vulnerabilities and attacks on the VoIP traffic and payload were identified. The future of VoIP requires adequate countermeasures to curtail the number of attacks targeted at this network. Some of these countermeasures were discussed in this paper. The optimisation of security in VoIP networks should be a research focus owing to the fact that this network has found widespread use with increased bandwidth demand and reliability issues. As more and more users deploy this network for low cost communication, there is the likelihood of more security breaches for its transmitted contents as well as its infrastructure.

While a number of solutions have been deployed, measures should be put in place to harden the security layers of VoIP networks during communication and data exchange particularly in the areas of authentication and encryption. The adoption of Secure Real-Time Transport Protocol (SRTP), IPSec and Transport Layer Security (TLS) for encryption and authentication should continue to evolve into more secure and robust solutions in the future of VoIP networks. In this way, the quality and integrity of the transmitted packets and payload will be ensured, thereby enhancing the overall reliability of the network.

References

[1] P. Gupta and V. Shmatikov, "Security analysis of voice-over-IP protocols," in *Computer Security Foundations Symposium, 2007. CSF '07. 20th IEEE,* 2007, pp. 49-63.

[2] Jin Tang, Yu Cheng and Yong Hao, "Detection and prevention of SIP flooding attacks in voice over IP networks," in *INFOCOM, 2012 Proceedings IEEE,* 2012, pp. 1161-1169.

[3] R. do Carmo, M. Nassar and O. Festor, "Artemisa: An open-source honeypot back-end to support security in VoIP domains," in *Integrated Network Management (IM), 2011 IFIP/IEEE International Symposium on,* 2011, pp. 361-368.

[4] Lin Liu, "Uncovering SIP vulnerabilities to DoS attacks using coloured petri nets," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on,* 2011, pp. 29-36.

[5] A. Lahmadi and O. Festor, "A Framework for Automated Exploit Prevention from Known Vulnerabilities in Voice over IP Services," *Network and Service Management, IEEE Transactions on,* vol. 9, pp. 114-127, 2012.

[6] Hong Zhao and N. Ansari, "Detecting covert channels within VoIP," in *Sarnoff Symposium*

(SARNOFF), 2012 35th IEEE, 2012, pp. 1-6.
[7] E. Coulibaly and Lian Hao Liu, "Security of voip networks," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on,* 2010, pp. V3-104-V3-108.
[8] M. Ibrahim, M. T. Abdullah and A. Dehghantanha, "VoIP evidence model: A new forensic method for investigating VoIP malicious attacks," in *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on,* 2012, pp. 201-206.
[9] D. Butcher, Xiangyang Li and Jinhua Guo, "Security Challenge and Defense in VoIP Infrastructures," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on,* vol. 37, pp. 1152-1162, 2007.
[10] N. Ekekwe and A. Maduka, "Security and risk challenges of voice over IP telephony," in *Technology and Society, 2007. ISTAS 2007. IEEE International Symposium on,* 2007, pp. 1-3.
[11] M. Scatá and A. L. Corte, "Security analysis and countermeasures assessment against spit attacks on VoIP systems," in *Internet Security (WorldCIS), 2011 World Congress on,* 2011, pp. 177-183.
[12] A. D. Keromytis, "A Comprehensive Survey of Voice over IP Security Research," *Communications Surveys & Tutorials, IEEE,* vol. 14, pp. 514-537, 2012.
[13] D. Sisalem, J. Kuthan and S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms," *Network, IEEE,* vol. 20, pp. 26-31, 2006.
[14] M. Gruber, F. Fankhauser, S. Taber, C. Schanes and T. Grechenig, "Security status of VoIP based on the observation of real-world attacks on a honeynet," in *Privacy, Security, Risk and Trust (Passat), 2011 Ieee Third International Conference on and 2011 Ieee Third International Conference on Social Computing (Socialcom),* 2011, pp. 1041-1047.
[15] Yan Zhang and Huimin Huang, "VOIP voice network technology security strategies," in *Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011 2nd International Conference on,* 2011, pp. 3591-3594.
[16] R. Farley and Xinyuan Wang, "VoIP shield: A transparent protection of deployed VoIP systems from SIP-based exploits," in *Network Operations and Management Symposium (NOMS), 2012 IEEE,* 2012, pp. 486-489.