International Journal of Computer Applications Technology and Research
Volume 7–Issue 03, 114-121, 2018, ISSN:-2319–8656

Survey of Research on IP-DECT and VOIP Systems Safety and a Novel Counter-Measure Approach

Ferdi Sönmez
Department of Computer Engineering,
Istanbul Arel University, Turkey

Beytullah EROL
Department of Computer Engineering,
Istanbul Aydin University, Turkey

Abstract: One of the most preferred communication tools in the telecommunication world is telephony. Telephone exchanges that do not use the functioning Internet Protocol (IP) technology are beginning to lose importance. Instead, exchange systems that provide communication over IP have begun to be used. Although, Voice over IP (VoIP) technology provides great advantages over traditional telephone exchanges as enabling voice transmission over IP, security and safety concerns are seen as critical issues for VoIP technology and devices or software applications using this technology. VoIP security and safety is directly related with Internet security, since VoIP technology uses Internet infrastructure during communication and the data is transmitted between devices as IP packets. In this study, old-fashioned telephone exchange systems and systems using IP technology are compared at first glance. Secondly, threats, security and safety issues related to VoIP are addressed and studies consisting of identification of threats, identification of security measures, testing of these security measures, situations threaten VoIP security and vulnerabilities of VoIP technology are examined. Threat categorizations of Voice Over IP Security Alliance (VoIPSA) and the Internet Engineering Task Force (IETF) are examined. Papers on VoIP security and safety are classified according to VoIPSA and IETF threat taxonomy. Lastly, possible and novel counter-measures to those security and safety threats are proposed.

Keywords: Switchboard, IP PBX, IP Deck, VoIP Security and Safety, IP Deck Security and Safety

1. INTRODUCTION

By means of the telephone, the voice has been transmitted from one point to another using public switched telephone networks (PSTN) [1]. With the rapid progress and development of Internet Protocol (IP) technology, widespread use has led to the idea of voice transmission over packet-switched networks [2]. PBX means private branch exchange and IP PBX is the exchange system that makes data communication over IP (Internet protocol). On the other hand, while PBX is a conventional PBX system, IP PBX refers to PBX systems that communicate over IP. These IP PBX systems have many advantages over conventional PBX systems [3][4].

Voice over Internet protocol (VoIP) is a collection of technologies based on the IP protocol that enables today's circuit-switched communication services to operate on packed data networks [1]. In other words, instead of traditional telephone networks, the transmission of voice over IP-based networks by converting them into IP packets is called 'IP Telephony' [2]. In other respects, The IP-DECT (digitally enhanced cordless telephone) system can be thought of as a link (bridge) between VoIP and DECT. IP-DECT systems can be used in a number of situations where wireless connectivity is needed in IP converters or integrated communications systems [3]. Especially; IP-DECT systems provide effective advantages for users where wireless connection is required [5][6]. But even for any person, it is a practical and very advantageous solution for users to take their phone and go to another place, and respond to all their calls without being tied to the desk. Flexibility and ease of use are combined with IP-DECT technology [6]. The disadvantages of fixed phone are eliminated by IP-DECT technology and a more advantageous solution is offered [6][7].

When looked at by the IP PBX, each DECT phone sends an IP call in the context of the phone feature. Many services are provided, such as the features that the IP PBX is subscribed to, and the numbering plan [8]. All configuration and maintenance procedures are performed via the IP-DECT Base Stations, the IP-DECT Gateway and the web interface on the VoIP gateway. On account of the web interface, all the configuration and maintenance operations can be adjusted easily. Moreover, the web interface on IP-DECT base stations, IP-DECT gateways and VoIP gateways, many operations can be performed easily by manual operation in classical telephone exchange systems [8]. Another important feature is that new base stations with VoIP support can be used together with traditional base stations in the same system [9]. As an example of this advantageous situation, when a person wants to convert the traditional PBX system to the system of the new technology IP telephone server structure, the VoIP system can be seamlessly switched without losing the wireless communication system infrastructure used. Benefits of the IP-DECT system compared to traditional DECT systems [8][9]:

- Less cabling and maintenance requirements with a single main network
- Integrated telephony and data-based technologies
- Mobile freedom without being connected to a fixed location
- In other locations, there is no telephone exchange system requirement.
- One number for roaming (mobile) users
- Flexibility and usability
- Classic and new IP PBX systems can work together

Despite the advantages, VoIP carries some security problems, since the transmission is influenced by the problems that occur on the Internet. VoIP traffic consists of data stream between network devices that the interventions to the network

devices mean that the system is open to intervention from the outside. The threats to the system are a combination of protocols used, VoIP devices and software. There are different methods of attack on such systems. VoIP traffic can be intercepted, copied, blocked, slowed, or altered by malicious intent [10]. The study was organized as follows. In section two, VOIP is examined. Section 3 involves the VOIP security and safety issues and a classification of research papers. Then, in section 4, counter-measures againsts threats is summarized. Section 5 includes concluding remarks.

2. VOICE COMMUNICATION over the INTERNET PROTOCOL

VoIP is the name given to technology that enables voice transmission over a packet-switched Internet network instead of a public switched telephone network.

2.1. VoIP and Historical Development

In VoIP, voice data is converted into IP packets and transmitted over the Internet. When the voice is converted into a packet, it is added to the voice data in the titles including the route information to be monitored by the package. Small segmented audio signals are sent over the network to a single destination [10]. In summary, audio signals are compressed while being packed, transferred over the network, and then decompressed again [11].

One of the biggest advantages of VoIP technology is that it can be negotiated at very long distances without paying a fee other than the Internet fee, or paying much below the standard telephone tariff. The development of VoIP solutions has enabled large business operators to have voice calls over existing Internet lines within their organization. VoIP can carry 5 to 10 times more voice calls over the same bandwidth compared to conventional circuit switched services [11]. In the case of voice transmission scenarios such as computer to computer, computer to telephone, computer to telephone and telephone to telephone, devices must make calls to each other, call terminations etc. There are protocols that they use when they perform business and operations. The need for different protocols to be developed by different VoIP application developers or device manufacturers needing to use a common set of protocols so that users can interact with each other [12].

2.2. VoIP Scenario

VoIP scenario takes place in five ways.

- Computer voice transmission from computer to computer.
- Computer to phone (PSTN) or telephone (PSTN) to computer
- From the phone (PSTN) to the phone (PSTN)
- Mobile VoIP
- Wireless VoIP

The conventional telephone system (PSTN) is numbered according to ITU-T E.164 recommendation. According to this numbering system, the phone numbers consist of country code, area code / national destination code (long distance code) and subscriber number [13]. In order for a phone on the PSTN network to communicate with a computer with Internet access, the computer to be dialed must have a number according to ITU-T E.164 recommendation. For instance, in the VoIP service named Wirofon offered by Turk Telekom Company, the subscriptions were given a number starting with an area code of 850.

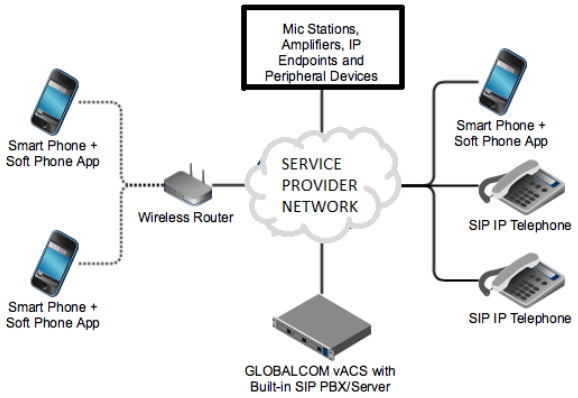

Figure 1. A Generic VoIP Scenario

Switching between the traditional telephone system (PSTN) and the VoIP system is provided by means of a gateway. The gateway is responsible for converting voice and other signaling information between the traditional telephone system (PSTN) and VoIP systems [14].

2.3. Computer to computer voice transmission

Communication from computer to computer is usually done by entering the IP address of the opposite party. Other methods such as domain name, e-mail address, member name and password can be preferred.

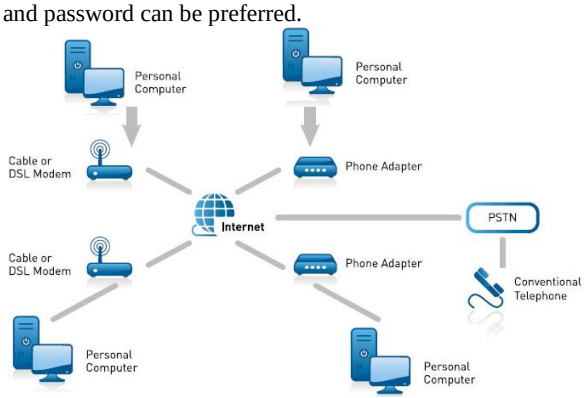

Figure 2. Computer voice transmission from computer to computer

VoIP calls can be made from mobile phone to mobile phone, as well as fixed phones and computers in PSTN network from mobile phone [14].

2.4. Mobile VoIP

Mobile VoIP has become a new VoIP scenario with the transition of mobile networks to 3G systems. While mobile networks operating with the 2G system operate with the circuit switching logic, packet switching data communication in addition to 2G has been possible with the transition to 3G [14]. Thanks to packet switching in the 3G system, bandwidth is only used during data exchange and much higher data transmission speeds are supported. With the innovations introduced by 3G technology, it supports users to make VoIP calls over the mobile network or using wireless networks [15].

2.5. Wireless VoIP

Wireless VOIP is implemented with phones designed to be compatible with the 802.11x standard family and capable of connecting to the Internet without cables and communicating voice over VoIP protocols over wireless networks [14][15]. Although WLAN is designed to expand IP networks, it has also created an alternative for voice communication.

Although wireless VoIP systems have evolved in recent years, Wi-Fi VoIP phones need to be improved in terms of battery life, security support, Internet browser support [16]. Because Wi-Fi technology is not designed to consume less energy, the small batteries of Wireless VoIP phones are inadequate. Some wireless network providers (Hotspot providers) use a website to login to the wireless network for security checks [17]. If the Wi-Fi VoIP phone does not have Internet browser support, the hotspot will not be able to use the wireless network because it can not open the Internet site required for access [16][17]. Supporting up-to-date wireless encryption methods in the 802.11x standard Wi-Fi VoIP phone will enable secure voice communication [18]. As a result, the widespread deployment of the Wireless VoIP scenario needs to increase the number of devices that are capable of the above mentioned features.

2.6. Session Initiation Protocol

Session Initiation Protocol (SIP) was proposed by The Internet Engineering Task Force (IETF) as a standard for IP multimedia calls and derived from Hyper-Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) [19]. It is flexible with the text based creation of SIP and can be expanded and scaled by code changes. In addition, the ability to work with the web also allows to use with other IP applications [20]. Multimedia presentations, instant messaging applications, distributed computer applications, signaling and most important VoIP calls are the main usage areas of SIP.

One of the advantages of SIP is that it can use Internet-based protocols to complete its own signaling protocols [21]. SIP only deals with how sessions are created, edited and terminated [20]. Other features are provided through protocols such as HTTP 2.0, Session Definition Protocol (SDP), Domain Name Server (DNS), Dynamic Host Configuration Protocol (DHCP), Real-time Transport Protocol RTP, Real-time Control Transport Protocol (RTCP) [21]. The SIP protocol can detect the condition of the destination of the voice packet. If the destination does not exist at that time or is not available, the SIP protocol can detect this situation . So, it tries other ways of reaching the target. It can do address resolution, address mapping, call routing [22].

3.VOIP SECURITY and SAFETY

In IP communication technology, every application used is the target or tool to be attacked [23]. With the increasing popularity of VoIP technology in recent years, it has become inevitable to target against the attackers. Especially VoIP attacks exploiting information security attacks are increasing day by day, and weaknesses and weak points of VoIP networks are being affected too much by this [24].

VoIP technology has several differences compared to traditional PSTN technology. Especially when the configuration of the software and services can be done by both the manufacturer and the end user, it makes the system vulnerable to attack. Today, VoIP applications and users are increasing rapidly [23]. It is also a possible that hundreds of million mobile VoIP users are thought to be faced with such threads. Because of SIP's text-based structure and its architecture similar to HTTP architecture, it is possible to attack not only known attack types but also SIP-specific attacks [23]. Packet exchanges during the use of TCP and UDP during communication make it very easy to exchange messages and information. Since SIP is not its own security mechanism, it is possible to be affected by the attacks as long as no measures are taken [25]. In addition to being vulnerable to known threats and known weaknesses, complex security architectures are needed depending on VoIP specific weaknesses. Currently used security devices are insufficient in VoIP and SIP security [24]. Attacks such DoS attacks, session dropping, wiretapping, fake recording, etc. can cause VoIP network to become ineffective or leak information [26]. The Voice Over IP Security Alliance (VOIPSA) has published security weaknesses against VoIP systems in its notice posted on its web site and categorized it as follows [25].

- Social threats
- Eavesdropping threats
- Denial of service threats
- Service abuse threats
- Physical access threats
- Interruption of services threats

IETF has categorized the threats coming with a similar grouping:

- Service disruption and annoyance
- Eavesdropping and traffic analysis
- Masquerading and impersonation
- Unauthorized access
- Fraud

3.1. Denial of Service

Denial of Service (DoS) attacks target IP networks that can have little effect on system operation or contrarily make the system completely unusable [27]. These attacks can not be prevented by security measures, such as encryption or authentication, because the voice packets are sent to the intended user [28]. It is difficult to take action against DoS and DDoS attacks because it usually comes in the form of Syncronize (SYN) and Internet Control Message Protocol (ICMP) packets [29]. Servers and UAs will accept these packages because it is not known which package is real, and which package is destined for attack. The percentage of DoS / DDoS attacks on networks such as VoIP, which perform real-time data communication, is very high [30]. A momentary interruption can cause major distress in these systems. If the attacker performs these attacks against high-priority network devices such as media gateways, interactive voice response (IVR), virtual machine, and so on, then ultimate harm may also occur [29][30]. The management of UDP ports is crucial to this attack, which can also be faced in the way that all calls are routed to another system or firewall [31]. Another and most faced DoS attack is replay attack which is a type of attack based on re-sending data packets. The re-transmitted data packets affect the data ordering on the receiver side. As a result, the stage becomes delayed and the call quality drops [29]. A person interfering with a call between two people records some or all of the talk, then transmits the packets it receives to the recipient. The most risky part of such an attack may be that the speaker shares his personal information or approves a major operation [28]. The attacker causes the voice packets containing the acknowledgment voice of the talkers to be repeatedly transmitted to the receiver in order to confirm the undesired operations. Below are other types of DoS attacks [30][31][32]. Some of these attacks may be partially inadequate, while others may completely disable the system. There are also DoS attacks that prevent calls from being made and that prevent voice messages from being received, and that do not even allow emergency calls.

- TLS Connection Reset
- VoIP Packet Replay Attack
- Quality of Service (QoS) Modification Attack
- VoIP Packet Injection
- DoS against Supplementary Services

- Control Packet Flood
- Bogus Message DoS
- Immature Software DoS
- Packet of Death DoS

3.2. Eavesdropping

Eavesdropping takes the form of listening or recording phone calls. It is necessary to access the network in order to carry out this attack [33]. Some protocol analysis programs can be used to listen to and record SIP and RTP traffic. Details of multiple conversations can be reached with this attack [34]. This means that unprotected signaling and data packets between users are displayed. It is possible to access and store data packets on the purpose of analyzing the network traffic [35]. Another intent of the attack is to obtain verbal or written information by techniques such as social engineering [36][37].

3.3. Spoofing

Spoofing is dangerous for service providers, since accomplished by changing the settings of the signaling messages or VoIP devices [29]. Here, attackers aim to make personal or financial gain by abusing VoIP services [30]. Fraud scenarios can be implemented in VoIP applications by influencing the call flow [27]. To prevent spoofing robust and difficult to interlace intrusion detection systems shold be preffered and more complex defense mechanisms should be followed.

3.4. Man in the Middle Attack and Call Hijack

This attack covers or combination of many other attacks. It can be described as the attacker entering between two or more users in the transmission and reading or changing messages without informing them [38]. If there is no security precautions for wireless connections and if there is a SIP communication over this network, vulnerability may occur [39]. The attacker intercepts the interim messages and changes the direction as it passes over its own server. Afterwards, DoS, hijacking and many other attacks can take place in the position [37]. This attack allows an attacker to intervene between the SIP server and the SIP user agent. Any valid username or password can be registered with the SIP server without knowing it [36]. Along with recording, it opens up many attacks.

3.5. Masquerade

Attackers behave and being treated as a user or system component and gain authorization on the system entities [40][41]. This attack is intended to access another user, service, or component [42]. This creates a significant layer of attack because fraud, unauthorized access, and service disruption attacks can be performed using this method. The characteristic of this attack is that system components can mimic the identity of entity. The target of the attack may be a user, device, or network component [43]. VoIP components can be signaled by unauthorized access or remote connection, or data packets can be used at their own discretion. Masquerade attacks particularly are directed to the application layer protocols [42][44].

3.6. Classification of Studies on VoIP Threats

Now, we discuss the studies contained in the VoIPSA and IETF classification that makes up the remaining of the study. All studies are classified in Table 1.

Table 1. Research Grouping by VoIPSA and IETF Threats Classification

S/N	VoIPSA classification	References by research	IETF classification	References by research	S/N
1	*Eavesdropping threats*	[33][34][35][36][37][38]	*Service disruption and annoyance*	[25][27][28][29][30][31][32]	1
2	*Denial of Service threats*	[23][25][27][28][29][30][31][32]	*Eavesdropping and traffic analysis*	[33][34][35][36][37][38]	2
3	*Service Abuse threats*	[45][46][47][48][49][50]	*Masquerading and impersonation*	[61][62][63][64][65][66]	3
4	*Physical access threats*	[51][52][53][54][55][56]	*Unauthorized access*	[51][52][53][54][55][56]	4
5	*Interruption of services threats*	[38][39][57][58][59][60]	*Fraud*	[45][46][47][48][49][50]	5
6	*Social threats*	[61][62][63][64][65][66]			

There are many academic studies on VoIP security. These studies mostly consist of identification of threats, identification of security measures, and testing of these security measures [24][67]. Since VoIP technology is a widely used, ever-evolving and growing technology, many service providers that offer VoIP services are also working on this issue. VoIP security has been the subject of thesis studies, too. Situations that threaten VoIP security are at the top of the most researched topics [67]. In order to take measures against security attacks, it is first necessary to identify these threats [59]. Vulnerabilities arise from VoIP architecture, protocols used, signaling weaknesses, routing and termination problems of components are the basis of their work. Classification of detected security threats is another important issue. Correct detection of security threats and good classification are an important step in taking effective measures against security threats [59]. After the identification of security threats, the proposed solution to these is another research topic.

4. COUNTER-MEASURES

VoIP security is directly related with Internet security, since VoIP technology uses Internet infrastructure during communication and the data is transmitted between devices as IP packets. There are many security mechanisms and methods developed against the attacks as counter-measures. In this section, we examined the security measures used in VoIP security, briefly. These security measures aim to provide effective and efficient security at each layer.

In order for a system to be secure, it must have at least three qualities or obey CIA triad [25] rules and domain specific ones [24][26]. These are;

- Confidentiality: The transmitted data means that only authorized users can access it. Ensuring that SIP signaling is done in a secure environment and that it is not affected by attacks such as wiretaps is essential. An attacker who can view SIP messages can easily listen to each unencrypted conversation [40]. To avoid this unwanted situation, messages must be encrypted. IPsec (Internet Protocol Security), developed to meet the security needs of the IP protocol, must be used to prove the authenticity of the communication, to ensure its privacy.
- Integrity: Protecting the data transmitted of stored against external factors, ensuring data integrity, means that only authorized users or malicious software change the data. Integrity principle, which provides user authentication, is used to protect the trusted sources. An attacker who is involved in an untrusted system without any situation of being caught or noticed can change different contents. It is desired to avoid this situation with integrity. SIP authentication prevents this from being altered by an unauthorized attacker. IPsec must be used to prove the authenticity of the communication, to ensure its integrity.
- Availability: It is defined as the time when the users defined in the system are at the request of the service and the service availability. Delays over acceptable level are undesirable for SIP networks. Any delay in real-time VoIP infrastructure can cause troubles. For example, a user who makes an invite request will cancel the request if the request does not take a certain period of time. However, the other user message will be delayed and the request message will be sent to the requesting user after the request is canceled. Another example is service disruption attacks which are intended to affect network components [40]. Spam Through Internet Telephony (SPIT) is examined as a service disruption attack which aims to prevent availability phones [41].
- Authentication: the user and the server must trust the credentials passed. In the request message, the called party must trust the requested information in the response message to the caller information sought.
- Rejection: The user who sent the message should not deny that it sent this message. This feature, which is used as an attack countermeasure, avoids the complexity and allows the attacker to distinguish between the attacker and the attacker.

5. CONCLUSION and RECOMMENDATIONS

IP telephone exchange systems are better than conventional telephone exchange systems in many respects, such as usability and security. As in all systems, there are security problems in IP based systems as well. Here, the security issues that IP-based systems may encounter, are addressed. Activating the https protocol will be of great benefit to users. This protocol, which means secure hyper text transfer communication, can be used to prevent the attacker from being infiltrated into the network and seizing the data, while being more protected than the classic http protocol against attack. Activating IP-based filtering is also an important factor. For example, accepting connections that only have a certain IP will not accept other connections. Another method is to restrict the number of users connected to the devices. Lastly, in order to make a system more secure, it must have at least three qualities or obey CIA triad rules and domain specific ones. In this study, 45 publications on IP DECK and VoIP security have been examined and classified by VoIPSA and IETF threat taxonomy. Vulnerabilities arise from VoIP architecture, protocols used, signaling weaknesses, routing and termination problems of components are the basis of their work. As a future hope and work, this study will help to conduct other VoIP security and counter-measures research and we will pay much attention on counter-measure research that after a comprehensive analysis of them we plan to develop a novel counter-measure or defense approach for recent threats or threats which have big and resident effects.

6. REFERENCES

[1] Bestak, R., Vranova, Z., & Ondryhal, V. (2011). Testing of Transmission Channels Quality for Different Types of Communication Technologies. Digital Information and Communication Technology and Its Applications, pp.13-23.

[2] Frieden, R. (2013). The mixed blessing of a deregulatory endpoint for the public switched telephone network. *Telecommunications Policy*, *37*(4), pp.400-412.

[3] Abid, F., Izeboudjen, N., Bakiri, M., Titri, S., Louiz, F., & Lazib, D. (2012). Embedded implementation of an IP-PBX/VoIP gateway. In Microelectronics (ICM), 2012 24th International Conference on, pp. 1-4.

[4] Kulin, M., Kazaz, T., & Mrdovic, S. (2012). SIP server security with TLS: Relative performance evaluation. In Telecommunications (BIHTEL), 2012 IX International Symposium on, pp. 1-6.

[5] Plosz, S., Moldovan, I., Trinh, T. A., Foglar, A. (2010). Design and Implementation of a Practical Smart Home System Based on DECT Technology. In International Conference on Energy-Efficient Computing and Networking, pp. 104-113, Springer, Berlin, Heidelberg.

[6] Coisel, I., & Sanchez, I. (2014). Practical interception of DECT encrypted voice communication in unified communications environments. In Intelligence and Security Informatics Conference (JISIC), 2014 IEEE Joint, pp. 115-122.

[7] Vergados, D. D. (2010). Service personalization for assistive living in a mobile ambient healthcare-networked environment. Personal and Ubiquitous Computing, 14(6), 575-590.

[8] Soloducha, M., Raake, A., Kettler, F., Rohrer, N., Parotat, E., Waeltermann, M., & Voigt, P. (2016). Towards VoIP quality testing with real-life devices and degradations. In *Speech Communication; 12. ITG Symposium; Proceedings of*, pp. 1-5.

[9] Bestak, R., Vranova, Z., & Ondryhal, V. (2011). Testing of Transmission Channels Quality for Different Types of Communication Technologies. *Digital Information and Communication Technology and Its Applications*, pp.13-23.

[10] Bhalla, M. R., & Bhalla, A. V. (2010). Generations of Mobile Wireless Technology: A Survey. *International Journal of Computer Applications*, *5*(4), pp.26-32.

[11] Al-Saadawi, H., & Varol, A. (2017). Voice over IP forensic approaches: A review. In Digital Forensic and Security (ISDFS), 2017 5th International Symposium on, pp. 1-6.

[12] Facchinetti, T., Ghibaudi, M., Goldoni, E., & Savioli, A. (2010). Real-time voice streaming over IEEE 802.15. 4. In Computers and Communications (ISCC), 2010 IEEE Symposium on, pp. 985-990.

[13] Mealling, M., & Faltstrom, P. (2004). The E. 164 to uniform resource identifiers (URI) dynamic delegation discovery system (DDDS) application (ENUM).

[14] Wang, X., Patil, A., & Wang, W. (2006). VoIP over wireless mesh networks: challenges and approaches. In *Proceedings of the 2nd annual international workshop on Wireless Internet* (p. 6)..

[15] Boucadair, M., Borges, I., Neves, P. M., & Einarsson, O. P. (2011). *IP Telephony Interconnection Reference: Challenges, Models, and Engineering*. CRC Pres.

[16] Murty, R., Padhye, J., Chandra, R., Wolman, A., & Zill, B. (2008, April). Designing High Performance Enterprise Wi-Fi Networks. In NSDI, 8, pp. 73-88.

[17] Gibson, J. D., & Wei, B. (2004). Tandem voice communications: digital cellular, VoIP, and voice over Wi-Fi. In *Global Telecommunications Conference, 2004. GLOBECOM'04 IEEE* , 2, pp. 617-621.

[18] Ganguly, S., & Bhatnagar, S. (2008). *VoIP: wireless, P2P and new enterprise voice over IP*. John Wiley & Sons.

[19] Tzerefos, P., Smythe, C., Stergiou, I., & Cvetkovic, S. (1997, November). A comparative study of simple mail transfer protocol (SMTP), post office protocol (POP) and X. 400 electronic mail protocols. In *Local Computer Networks, 1997. Proceedings., 22nd Annual Conference on*, pp. 545-554.

[20] Gardner M. T., Frost V.S., Petr D.W. (2003). Using optimization to achieve efficient quality of service in voice over IP networks. In *Performance, Computing, and Communications Conference, 2003. Conference Proceedings of the 2003 IEEE International*, pp. 475-480.

[21] Ormazabal, G., Nagpal, S., Yardeni, E., & Schulzrinne, H. (2008). Secure sip: A scalable prevention mechanism for dos attacks on sip based voip systems. *Principles, systems and applications of IP telecommunications. Services and security for next generation networks*, pp. 107-132.

[22] Durkin, J. F. (2003). *Voice Enabling the Data Network: H. 323, MGCP, SIP, QoS, SLAs, and Security*. Cisco Press.

[23] Yüksel, M , Öztürk, N. (2017). SIP Attacks and Security Methods. International Journal of Informatics Technologies, 10 (3), pp. 301-310.

[24] Keromytis, A. D. (2012). A comprehensive survey of voice over IP security research. *IEEE Communications Surveys & Tutorials*, 14(2), pp. 514-537.

[25] Hanifan, Y., & Bandung, Y. (2013). Designing VoIP security system for organizational network. In *ICT for Smart Society (ICISS), 2013 International Conference on*, pp. 1-5.

[26] Lazzez A., Slimani T. (2013).“Deployment of VoIP Technology:QoS Concerns”, International Journal of Advanced Research in Computer and Communication Engineering, 2(9),pp. 65-74.

[27] Farley, R., & Wang, X. (2012). VoIP Shield: A transparent protection of deployed VoIP systems from SIP-based exploits. In *Network Operations and Management Symposium (NOMS), 2012 IEEE*, pp. 486-489.

[28] Akbar M. A. and M. Farooq, “Application of Evolutionary Algorithms in Detection of SIP based Flooding Attacks,” in Proc. Genetic and Evolutionary Computation Conference (GECCO), 2009.

[29] Ouchani, S., Jarraya, Y., & Mohamed, O. A. (2011). Model-based systems security quantification. In *Privacy, Security and Trust (PST), 2011 Ninth Annual International Conference on*, pp. 142-149.

[30] Sengar, H., H. Wang, D. Wijesekera, and S. Jajodia, “Fast Detection of Denial-of-Service Attacks on IP Telephony,” in Proc. 14th IEEE International Workshop on Quality of Service (IWQoS), pp. 199–208, 2006.

[31] Hentehzadeh, N., Mehta, A., Gurbani, V. K., Gupta, L., Ho, T. K., & Wilathgamuwa, G. (2011). Statistical analysis of self-similar Session Initiation Protocol (SIP) messages for anomaly detection. In *New Technologies, Mobility and Security (NTMS), 2011 4th IFIP International Conference on* (pp. 1-5).

[32] D. Geneiatakis and C. Lambrinoudakis, “A Lightweight Protection Mechanism against Signaling Attacks in a SIP-based VoIP Environment,” Telecommunication Systems, vol. 36, pp. 153–159, 2007.

[33] Azfar, A., Choo, K. K. R., & Liu, L. (2014). A study of ten popular Android mobile VoIP applications: Are the communications encrypted?.

In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, pp. 4858-4867.

[34] Wright C. V., Ballard L., Monrose F.N. and Masson G.M. "Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?," in Proc. 16th USENIX Security Symposium, pp. 1–12, 2007.

[35] Zhang R., Wang X., Farley R., Yang X., and X. Jiang, "On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers," in Proc. 4th International ACM Symposium on Information, Computer, and Communications Security (ASIACCS), pp.61–69, 2009.

[36] Guo J.-I., Yen J.-C., and Pai H.-F. "New Voice over Internet Protocol Technique with Hierarchical Data Security Protection," IEE Proc. — Vision, Image and Signal Processing, 149, pp. 237–243, 2002.

[37] Talevski A., Chang E., Dillon T. "Secure Mobile VoIP," in Proceedings of International Conference on Convergence Information Technology, pp. 2108–2113, 2007.

[38] Reynolds B. and Ghosal D. "STEM: Secure Telephony Enabled Middlebox," in IEEE Communications Magazine, 40(10), pp. 52-58, 2002.

[39] Cretu G. F., A. Stavrou, M. E. Locasto, S. J. Stolfo, and Keromytis A. D. "Casting out Demons: Sanitizing Training Data for Anomaly Sensors," in Proc. IEEE Security and Privacy Symposium, pp. 81–95, 2008

[40] Seo, D., Lee, H., & Nuwere, E. (2013). SIPAD: SIP–VoIP anomaly detection using a stateful rule tree. *Computer Communications*, *36*(5), pp. 562-574.

[41] Geneiatakis d., T. Dagiuklas, C. Lambrinoudakis, G. Kambourakis, and Gritzalis S. "Novel Protecting Mechanism for SIP-based Infrastructure against Malformed Message Attacks: Performance Evaluation Study," in Proc. 5th International Conference on Communication Systems, Networks and Digital Signal Processing (CSNDSP), pp. 261–266, 2006.

[42] Gritzalis, D., Marias, G., Rebahi, Y., Soupionis, Y., & Ehlert, S. (2011). SPIDER: A platform for managing SIP-based Spam over Internet Telephony (SPIT). *Journal of Computer Security*, *19*(5), pp.835-867.

[43] Kolan P., Dantu R. "Socio-technical Defense Against Voice Spamming," ACM Transactions on Autonomous and Adaptive Systems (TAAS), 2, 2007.

[44] Madhosingh A. "The Design of a Differentiated SIP to Control VoIP Spam," Masters Thesis Report SPIT, CAPTCHA, Florida State University, Computer Science Department, 2006.

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

[46] Hunter P. "VOIP the Latest Security Concern: DoS Attack the Greatest Threat," Network Security, 11, pp. 5–7, 2002.

[47] Batchvarov A. "Security Issues and Solutions for Voice over IP Compared to Circuit Switched Networks," tech. rep., INFOTECH Seminar Advanced Communication Services (ACS), 2004

[48] Geneiatakis D., Kambourakis G., Lambrinoudakis C., Dagiuklas T. and Gritzalis S. "SIP Message Tampering: THE SQL code INJECTION attack," in Proc. 13th IEEE International Conference onSoftware, Telecommunications and Computer Networks (SoftCOM), 2005.

[49] McGann S. and Sicker D. "An Analysis of Security Threats and Tools in SIP-Based VoIP Systems," in Proc. 2nd VoIP Security Workshop, 2005.

[50] Rebahi, Y., Nassar, M., Magedanz, T., & Festor, O. (2011). A survey on fraud and service misuse in voice over IP (VoIP) networks. *Information Security Technical Report*, *16(1)*, pp.12-19.

[51] Kolias, C., Kambourakis, G., & Maragoudakis, M. (2011). Swarm intelligence in intrusion detection: A survey. *computers & security*, *30*(8), pp.625-642.

[52] Geneiatakis D., Lambrinoudakis C., Kambourakis G. "An OntologyBased Policy for Deploying Secure SIP-based VoIP Services,"Computers and Security, 27, pp. 285–297, 2008

[53] Sisalem D., S. Ehlert, D. Geneiatakis, G. Kambourakis, T. Dagiuklas, J. Markl, M. Rokos, O. Botron, J. Rodriguez, and Liu J. "Towards a Secure and Reliable VoIP Infrastructure," Tech. Rep. Deliverable D2.1, SNOCER COOP-005892, 2005.

[54] Sher M. and Magedanz T. "Protecting IP Multimedia Subsystem (IMS) Service Delivery Platform from Time Independent Attacks," in Proc. 3rd International Symposium on Information Assurance and Security (IAS), pp. 171–176, 2007

[55] Armoogum, S., & Mohamudally, N. (2014, May). Survey of practical security frameworks for defending SIP based VoIP systems against DoS/DDoS attacks. In *IST-Africa Conference Proceedings, 2014* (pp. 1-11). IEEE.

[56] Rieck K., S. Wahl, P. Laskov, P. Domschitz, and Muller K.-R. "A Self-learning System for Detection of Anomalous SIP Messages," in Proc. 2nd Internation Conference on Principles, Systems and Applications of IP Telecommunications. Services and Security for Next Generation Networks: Second International Conference, (IPTComm), pp. 90–106, 2008.

[57] Bessis T., Rana A. and Gurbani V.K. "Session Initiation Protocol (SIP) Firewall for Internet Multimedia Subsystem (IMS) Core," Bell Labs Technical Journal, 2010.

[58] Sengar H., Wijesekera D., Wang H., and Jajodia S. "VoIP Intrusion Detection Through Interacting Protocol State Machines," in Proc. International Conference on Dependable Systems and Networks (DSN), pp. 393–402, 2006.

[59] Geneiatakis D., G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and Gritzalis S. "A Framework for Detecting Malformed Messages in SIP Networks," Computer Networks: The International Journal of Computer and Telecommunications Networking, 51, pp. 2580-2593, 2007.

[60] Mehta A., N. Hantehzadeh, V. K. Gurbani, T. K. Ho, J. Koshiko, and Vishwanathan R. "On the inefficacy of Euclidean classifiers for detecting self-similar Session Initiation Protocol (SIP) messages," in Proc. 12th IFIP/IEEE International Symposium on Integrated Network Management (IM), 2011 .

[61] Tu, H., Doupé, A., Zhao, Z., & Ahn, G. J. (2016, May). SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pp. 320-338.

[62] Cao F., Ha B., Padmanabhan R., A. Yuan, and Tran K., S. Phithakkitnukoon and R. Dantu "Defense Against SPIT Using Community Signals," in Proc. IEEE International Conference on Intelligence and Security Informatics (ISI), 2009.

[63] Banerjee N., S. Saklikar, and Saha S. "Anti-vamming Trust Enforcement in Peer-to-peer VoIP Networks," in Proc. International Conference on Communications and Mobile Computing (IWCMC), pp. 201–206, 2006.

[64] Haberler M. and Lendl O. "Secure Selective Peering with Federations," in Proc. 3rd Workshop on Securing Voice over IP, 2006.

[65] Quittek J. S. Niccolini, S. Tartarelli, and Schlegel R. "Prevention of Spam over IP Telephony (SPIT)," NEC Technical Journal, 1(2), pp. 114–119, 2006.

[66] Kolan P., R. Dantu, and Cangussu J.W. "Nuisance of a Voice Call," ACM Transactions on Multimedia Computing, Communications and Applications (TOMCCAP), 5(6), pp. 1–22, 2008.

[67] Ehlert, S., Geneiatakis, D., & Magedanz, T. (2010). Survey of network security systems to counter SIP-based denial-of-service attacks. *Computers & Security*, *29*(2), pp.225-243.