World Academy of Science, Engineering and Technology
International Journal of Economics and Management Engineering
Vol:12, No:1, 2018

Towards a Security Model against Denial of Service Attacks for SIP Traffic

Arellano Karina, Diego Avila-Pesántez, Leticia Vaca-Cárdenas, Alberto Arellano, Carmen Mantilla

***Abstract*—**Nowadays, security threats in Voice over IP (VoIP) systems are an essential and latent concern for people in charge of security in a corporate network, because, every day, new Denial-of-Service (DoS) attacks are developed. These affect the business continuity of an organization, regarding confidentiality, availability, and integrity of services, causing frequent losses of both information and money. The purpose of this study is to establish the necessary measures to mitigate DoS threats, which affect the availability of VoIP systems, based on the Session Initiation Protocol (SIP). A Security Model called MS-DoS-SIP is proposed, which is based on two approaches. The first one analyzes the recommendations of international security standards. The second approach takes into account weaknesses and threats. The implementation of this model in a VoIP simulated system allowed to minimize the present vulnerabilities in 92% and increase the availability time of the VoIP service into an organization.

***Keywords*—**Denial-of-service SIP attacks, MS-DoS-SIP, security model, VoIP-SIP vulnerabilities.

I. Introduction

VoIP is a technology that provides voice communication through the TCP/IP network. It is an economical alternative for telephone communication, compared to the traditional public telephone network (PSTN) [1]. A VoIP call uses two phases: signaling and data transmission. The SIP protocol is an application layer protocol, used for signaling in VoIP connections traffic, implemented in a communications network infrastructure. According to an IBM report [2], 51% of cyber-attacks are directed to SIP protocol. It is established that, in the second semester of 2016, the highest number of these attacks was carried out. The primary cause is due to the vulnerabilities of this protocol [3], as well as to the flood based on the DoS attack. These attacks are explicit attempts to disable voice transmission within an organization, thus preventing legitimate users from using their services [4].

For best security practices in VoIP communications, companies can implement security models, which allow protecting and safeguarding information, maintaining confidentiality, availability, and integrity of the services. These models will make aware a security manager of how to protect VoIP services, to the extent the possible to mitigate these types of threats and the adverse effects they cause on communication systems. Currently, there are several proposals from technology companies and industry standards that support the need to create a security model, but few focus on security in SIP protocols. According to the literature reviewed, the works of [5]-[7], developed studies to ensure a higher availability the VoIP service, and mitigate DoS attacks. But they do not present specific solutions for the SIP protocol. On the other hand, the studies of [8]-[12] analyzed the SIP signaling protocol, with a focus on security mechanisms, which constitute the basis for the proposal of our model.

Other researchers, Ormazabal et al. [4] conducted studies on the functionality and performance of the DoS prevention systems, using tools that generate attacks based on SIP traffic. The experimental results were able to detect and mitigate the spoofing and request, response and floods attacks. Also, Jouravlev [5] analyzed the main threats of DoS in a VoIP environment, as well as the best countermeasures that could be used to prevent and improve security in the VoIP environment into a company.

The study developed by Keromytis [3] presented a comprehensive analysis of VoIP security, using a set of 245 academic research publications about this topic, and classified them according to an extended version of the VoIP Security Alliance (VOIPSA) according to the threat taxonomy. Also, they provided a roadmap to identified deficiencies in the treatment of the numerous threats and vulnerabilities present in VoIP systems. They established two specific problem areas that require more attention from the research community, and these are the DoS attacks and abuse of service.

For this proposal, several components were analyzed and based on the ISO/IEC 27002 standard, which offers recommendations for the best practices in information security management. That is considered as the fundamental issue for the implementation of protection measures [13]. Also, with an ITU-T X.805 framework, the security architecture for end-to-end communication systems was defined, as well as the dimensions that guarantee the security of distributed applications [14]. Finally, the best practices proposed by companies that lead the market such as Asterisk, Cisco, and VOIPSA were reviewed.

For complementing the structure of the proposed model, it was considered the OSSTMM 2.1 methodology, composed of six sections, but only the Security issues in Communications and Security in Internet Technologies section was framed within the focus of this study [15]. At the end, it relied on the

K. Arellano is with Engineering Faculty, National University of Chimborazo, Riobamba, Ecuador (e-mail: karina.arellano@unach.edu.ec).

D. Avila-Pesántez and L. Vaca-Cárdenas are with the Informatics and Electronic Faculty, Polytechnic School of Chimborazo, Riobamba, Ecuador (e-mail: davila@espoch.edu.ec, leticia.vaca@espoch.edu.ec).

A. Arellano is with the Electrical Engineering Department, Polytechnic School of Chimborazo, Riobamba, Ecuador (e-mail: aarellano@espoch.edu.ec).

C. Mantilla is with the Projects and Technology Transfer Department, Polytechnic School of Chimborazo, Riobamba, Ecuador (e-mail: carmen.mantilla@espoch.edu.ec).

collection techniques proposed in the book "Hacking exposed VoIP", where the ethical hacking phases are identified [16].

For the analysis of the results of this model, a case study was utilized, where a VoIP network of an organization was simulated using GNS3 version 1.4.5 [17]. It was designed according to two scenarios. First was established without implementation security mechanisms and second applying the proposed model. In the test environment, the most common attacks used with DoS were executed, and voice and availability quality performance parameters were determined. All responses to attacks were registered, which would guarantee the availability of the VoIP service.

Firstly, general information related to VoIP session and DoS SIP attack was introduced in this paper. The rest of this paper is organized as follows. Section II presents the MS-DoS-SIP model. The case study will be described in Section III. At last, the article finishes with the conclusion of the work.

II. Model MS-DoS-SIP

The proposed model was based on several components such as the OSSTMM methodology [15], which includes Footprint, Scanning, and Enumeration recognition techniques for a VoIP network. The most relevant recommendations of the ITU-T X805 and ISO / IEC 2702: 2007-2015 standards; the NIST standard [18]; the VOIPSA Alliance [19]; the VoIP Asterisk platforms [20], and security recommendations from Cisco System. These allowed determining the structure of the model, the definition of its phases and generation of security policies.

The OSSTMM methodology presents its phases according to cost and time, as shown in Fig. 1, so the practical part relied on several factors such as analysis of security sections, internet technologies, and security in communications. Because the first one is the core part, and in the second one contemplates aspects of security testing for VoIP technology, with which the model stages were defined.

Through the execution of the recognition techniques as Footprint, Scanning, and Enumeration, the security holes present in the network infrastructure were identified. It allows issuing security policies, to minimize vulnerabilities and mitigate threats. Taking into account the recommendations of ITU-T X805, which refer to "Protect the control or signaling information used in the network service", the protection of the SIP protocol was analyzed in the process of starting and maintaining the sessions of VoIP transmission. Also, the ISO/IEC 2702: 2007-2015 standard was considered in its domain 9, which deals with the Safety Communications, emphasizing the protection of VoIP traffic, encrypting, segmenting data and voice traffic, ensuring IP-PBX, using perimeter security controls. In the first practices for the implementation of a secure VoIP network, NIST proposes:

a) Develop an appropriate architecture utilizing the Speech Network Authentication, handle authentication and access control, and Implement Firewalls.
b) Perform physical inspections on the VoIP network.
c) Use Protection mechanism as specialized VoIP firewall.

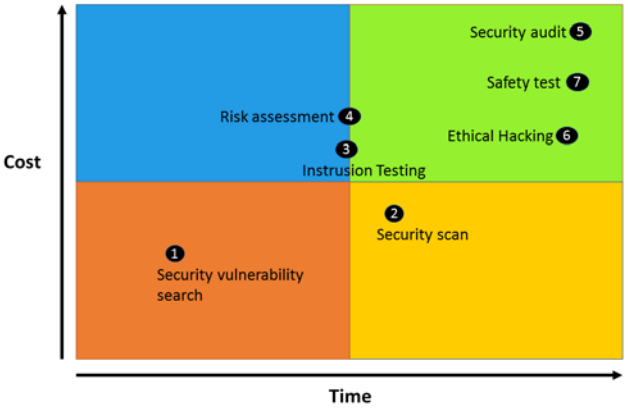

Fig. 1 Adapted OSSTMM Phases [15]

This work was complemented, with the best practices proposed by Asterisk and Cisco System. They recommend making constant updates, use monitoring tools of the VoIP network, eliminate services that are not being used, modify basic configurations, always use VLANs, secure the elements of the network VoIP, apply Firewalls, IDS, IPS, and SBC to analyze traffic and monitor any attack type. Also, VOIPSA's most important recommendations were added: identify VoIP network devices by scanning ports and protocols, perform periodic security sweeps using automatic or manual scanning, and implement Firewalls and IPS, explicitly targeting networks VoIP.

A. Security Model Proposed

The Security Model was called MS-DoS-SIP, and it focuses on DoS attacks on SIP traffic. It proposes four stages of action, which administrators or IT Security professionals can apply. The phases are shown in Fig. 2 and must be developed cyclically, since each step will depend on the previous one, creating a constant loop of analysis, on the VoIP network of the organization. The execution of the phases will depend on the technologies, protocols, and devices used since not all devices have security systems mentioned in this study.

Phase 1. The first step is to know the VoIP infrastructure, using the information that is available on the network. If the data has been regarding correctly, and in detail, it allows guaranteed access to the systems that use the VoIP service. Therefore, it is essential to comprehend in depth what kind of information the attacker can acquire and to take actions that minimize the possible damage. Through software tools, the elements of the VoIP network are identified (topology, map, IP addressing, signaling protocols), and all hardware and software devices that make up the communications network (softphones, operating systems, configuration, and device characteristics). Their vulnerabilities could be established using port scanning software and protocols discovery tools.

Phase 2. The vulnerabilities and security flaws commonly used are established to cause damage to the VoIP infrastructure based on SIP, and the impact that it could cause. Table I shows the list of vulnerabilities and the impact on the VoIP service, which are usually identified in the VOIP networks and the effect on the availability of the service was

rated. Furthermore, based on the work of Endler & Collier [14], the primary threats were determined and classified, which affect the availability of the VoIP service more critically. The probability of occurrence and the degree of severity of the consequences are analyzed, considering the potential damage caused by the execution carried out successfully. In Table II, data allow in this stage to identify with certainty, which are the vulnerabilities detected in the communication network, and the possible attacks of which can probably be a victim.

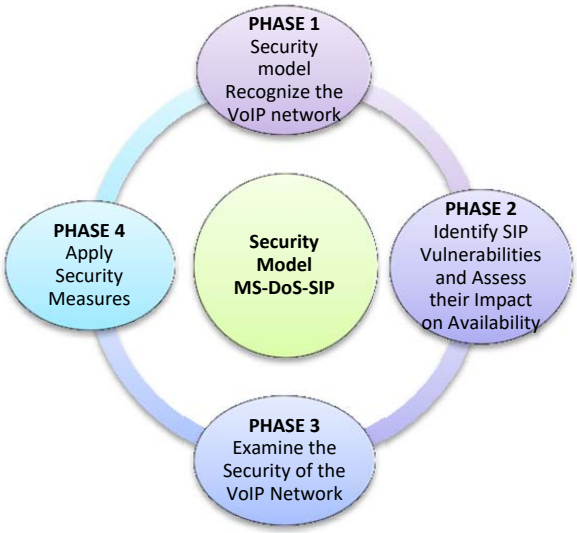

Fig. 2 Stages of the proposed MS-DoS-SIP Model

TABLE I
VULNERABILITIES AND IMPACT IN VOIP INFRASTRUCTURE [16]

VULNERABILITIES AND SECURITY FAILURES	IMPACT LOW (1)	MEDIUM (2)	HIGH (3)
Homogeneous Network		x	
Lack of Network Segmentation		x	
Weak password			x
Unnecessary open ports			x
Known Ports			x
Unnecessary enabled services			x
Weak configurations			x
Low bandwidth		x	
Limited availability of resources		x	
Lack of Authentication			x
Absence of SIP Firewall			x
Lack of Security Systems (IDS / IPS / SBC)			x
Lack of Updates and patching		x	
Enlisted SIP devices enabled			x
Scanning permissions in SIP-enabled user			x
SSH protocol unprotection			x
Unlimited concurrent request permission			x
SIP phones enabled TFTP, DCHP, TELNET		x	
Absence of Audits and Logs		x	

Phase 3. VoIP service interruptions are considered, which are not necessarily caused by attacks or intruders. For this, there are specific symptoms to find, in the identification of a DoS attack. A security review of the VoIP network is carried out, with the aim of recognizing clues, which may warn of a possible DoS attack, for example:

a) the network was working much slower than usual.
b) the service was not available.
c) a considerable number of requests were received.

Probably, the system is a victim of a DoS attack. Network monitoring is done through tools such as PRTG (they allow tracking of SIP traffic like HOMER5), as well as the analysis control and of logs through the File2ban application.

Phase 4. Finally, once the symptoms and vulnerabilities detected in the network have been identified, security measures are applied. For example, network segmenting, changing standard ports, updating and patching software, implementing TLS, configuring Firewalls SIP, Iptables, Session Border Controller (SBC), which allow mitigating the vulnerabilities and risks that the VoIP infrastructure can suffer within an organization.

TABLE II
VOIP SECURITY THREATS- DOS

Attack	Popularity	Impact	Risk estimation
Malformed SIP Messages	Occasionally	Intolerable	Important
Floods INVITE to SIP Proxies (Using inviteflood Tool)	Frequently	Extremely Intolerable	Very Important
Floods INVITE to SIP Phone (Using inviteflood Tool)	Very Frequently	Intolerable	Very Important
Flood Register	Frequently	Intolerable	Important
Elimination Register	Frequently	Slightly Intolerable	Important
SynFlood DoS	Very Frequently	Intolerable	Important

III. CASE STUDY

For the proposed case study, a simulated test scenario was designed using GNS3 version 1.4.5. It allowed establishing the appropriate VoIP network technology and infrastructure. A telephone exchange server was implemented with Elastix 2.5, four SIP clients with the Zoiper softphone, which allows simulating IP telephones in computers, and Express Talk (non-commercial version). Also, one router and four multilayer switches were configured. Finally, virtual machines with Kali Linux and Windows 10 were used to execute the attacks. Fig. 3 shows the scenario presented in this simulation.

When developing the first three stages of the security model proposed, in the test scenario, 13 vulnerabilities were found, which are described in Table III. After establishing these vulnerabilities, treatment was given with the implementation of the proposed security model.

In this study, the SIP-specific attacks that affect VoIP availability were established, such as Flooding and Fuzzing-based attacks: INVITE Flood to Proxy, INVITE Flood to Phones, Malformation in INVITE messages, Elimination of Registration of SIP and SYN flood users, as shown in Table IV.

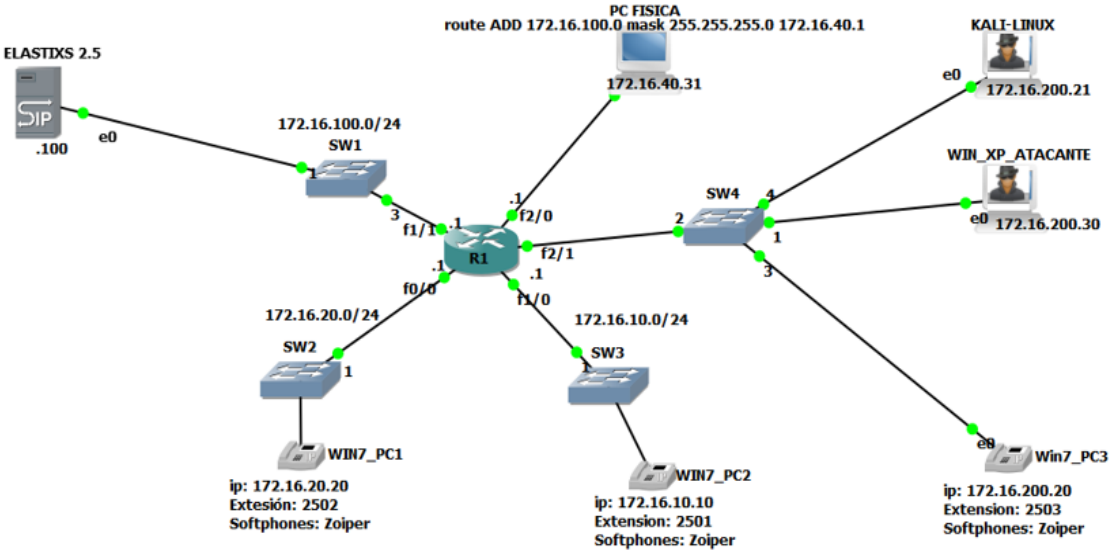

Fig. 3 Interconnection diagram established for the test scenario

TABLE III
VULNERABILITIES LOCATED IN THE TESTING SCENARIO

◦	Vulnerability
1	Unnecessary ports opened
2	Enlisted SIP-enabled devices
3	Scanning permissions in SIP-enabled user
4	Weak Configurations
5	Insufficient Network Segmentation
6	Use of default ports
7	Unnecessary enabled services
8	Insufficient Authentication/Authorization
9	Absence of Firewall
10	Lack of Security Systems
11	Lack of Updates and patching VoIP systems
12	Unsafe SIP terminals
13	SSH protocol unprotection

TABLE IV
SIP ATTACKS ESTABLISHED IN THE SCENARIO

Threats	Attack
Fuzzing	Malformed SIP Messages
Flooding	Floods INVITE to SIP Proxies (using inviteflood Tools)
Flooding	Floods INVITE to SIP Phones (using inviteflood Tools)
Signaling Handling	Elimination Register

SIP Flooding attacks occur when IP telephones generate requests or responses to send to a specific server, called a victim. As a result, the server is busy receiving excessive SIP messages within a short time, affecting general services. INVITE Flood is considered one of the most common flood attacks, both for servers and terminals. As well as message malformation attacks are a fuzzing type threat that modifies fields in the INVITE message. It sends INVITE messages with contents not foreseen by the protocol, causing the terminals to malfunction or stop working entirely.

The vulnerability used in the User Registry Elimination attack is the lack of authentication in the REGISTER message. The attacker sends a REGISTER request to the registration server indicating the identity of the user, with the contact field "Contact: *" and the value "Expire" = zero, being able to eliminate any other record of the user's address.

For the development of the tests, the number of packets sent in each attack was established, and the Endler & Collier [16] recommendation was considered, which determines the sending of 1,000,000 packets to a target to experience DoS attacks based on Flooding and Fuzzing. In contrast, for the penetration test, the proposed values are 500,000 and 2,000,000 packets. Also, to establish specific parameters regarding the VoIP service, surveys were applied to public and private institutions. The survey yielded relevant results against the use of VoIP service and the importance of always keeping it available, since, 100% of the surveyed organizations rated as high the impact that the loss of availability of the VoIP service in their Institution would produce. Likewise, 90% of the institutions said that the average time that an IP telephone call lasts is in the interval of 1 minute to 10 minutes. Therefore, for the experiments of this study, three times were established referring to the duration of IP calls for each scenario, considering calls of 3 minutes, 5 minutes and 8 minutes, respectively. Finally, the attacks with the values of established packets were executed.

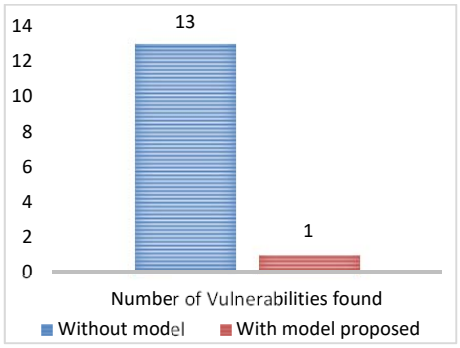

Fig. 4 Vulnerabilities Identified in the Test Scenarios

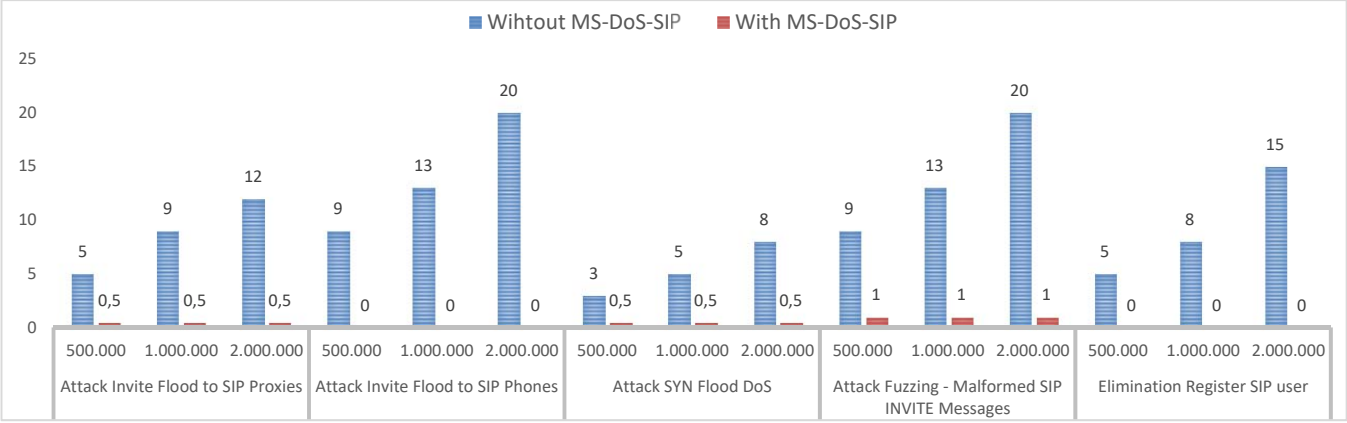

Fig. 5 VoIP Service Interruption Time (mins)

The indicators that were analyzed in the tests are latency, jitter and packet loss. Since these are the parameters that directly affect the quality of the VoIP service. The latency values were established: less than 150 ms; Jitter: less than 50 ms; and packet loss: less than or equal to 3% of the volume of data transmitted. For this analysis, the Wireshark tool was used. Finally, the most relevant indicator is the Time of Interruption of the VoIP Service, which allowed to know the exact time in which the VoIP service stopped being available in the network, through the PRTG Network Monitor tool, as shown in Fig. 4.

The experimental results obtained from the tests in each scenario were analyzed and compared, allowing to demonstrate the improvement in the prevention of attacks of each solution proposed in the MS-DoS-SIP Security Model. When applying the model, in the number of identified vulnerabilities, it was reduced by 92% concerning the scenario without security measures.

For the indicator: Time of non-availability of the VoIP service, it is established that with the implementation of the Security Model, the availability time of the VoIP service is increased; in such a way, that users can make use of it, without any setback (Fig. 5).

Finally, it was demonstrated that by applying the MS-DoS-SIP Security Model, to mitigate DoS attacks in SIP traffic in VoIP services, vulnerability to DoS attacks was reduced, increasing the availability of VoIP service in Corporate LAN.

IV. Conclusions

The MS-DoS-SIP Security Model proposed, aimed at DoS attacks in SIP traffic, is a support to the application process of security mechanism in a VoIP system. It helps to ensure that appropriate countermeasures are applied, at the moment of seeking to mitigate DoS attacks. This methodology is based on proposals such as OSSTMM and Hacked Exposed VoIP, which allow having a clear idea and a standard work reference. Besides, the safety recommendations of ISO/IEC 2702: 2007-2015 standard were considered, where the protection of VOIP traffic is emphasized through encryption, traffic segmentation and the use of perimeter security controls. Moreover, it suggests that the SIP protocol should be protected with the use of TLS connections [21], NIST; placing an appropriate architecture and use specialized firewalls in VoIP. Also, it must be periodically examined the security of the network, by scanning ports in protocols.

The application of the Model MS-DoS-SIP, in a simulated VoIP network environment, through practical scenarios, managed to minimize by 92% the vulnerabilities established in this study, in comparison with the same situation without security mechanisms. By significantly reducing weaknesses, it was possible to achieve service interruption times of a few seconds, thus ensuring the continuity of VoIP system within an organization.

Nowadays, it is highly recommended a deep researcher, regarding the techniques and tools used by the attackers, to update the proposed Security Model. In future work, it is advised to take into consideration the use of an event correlation system in VoIP systems, and new security updates, to be one step ahead in the emergence of future threats and vulnerabilities in this type of service.

References

[1] D. Golait and N. Hubballi, "Detecting Anomalous Behavior in VoIP Systems: A Discrete Event System Modeling," *IEEE Transactions on Information Forensics and Security*, vol. 12, pp. 730-745, 2017.

[2] *Security Intelligence*. Available: https://securityintelligence.com/hello-youve-been-compromised-upward-attack-trend-targeting-voip-protocol-sip/, (Accessed: 15/11/2017).

[3] A. D. Keromytis, "A comprehensive survey of voice over IP security research," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 514-537, 2012.

[4] G. Ormazabal, S. Nagpal, E. Yardeni, and H. Schulzrinne, "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, 2008.

[5] I. Jouravlev, "Mitigating Denial-Of-Service Attacks On VoIP Environment," *International Journal of Applied Management and Technology*, vol. 6, 2008.

[6] M. V. Martin and P. C. Hung, "Towards a security policy for VoIP applications," in *Electrical and Computer Engineering, 2005. Canadian Conference on*, 2005, pp. 65-68.

[7] L. Shan and N. Jiang, "Research on security mechanisms of SIP-based VoIP system," in *Hybrid Intelligent Systems, 2009. HIS'09. Ninth International Conference on*, 2009, pp. 408-410.

[8] J. Lee, K. Cho, C. Lee, and S. Kim, "VoIP-aware network attack detection based on statistics and behavior of SIP traffic," *Peer-to-Peer Networking and Applications*, vol. 8, pp. 872-880, 2015.

[9] M. Z. Rafique, M. A. Akbar, and M. Farooq, "Evaluating DoS attacks against SIP-based VoIP systems," in *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, 2009, pp. 1-6.
[10] U. U. Rehman and A. G. Abbasi, "Security analysis of VoIP architecture for identifying SIP vulnerabilities," in *Emerging Technologies (ICET), 2014 International Conference on*, 2014, pp. 87-93.
[11] S. Ehlert, D. Geneiatakis, and T. Magedanz, "Survey of network security systems to counter SIP-based denial-of-service attacks," *Computers & Security,* vol. 29, pp. 225-243, 2010.
[12] O. Gavilanez, F. Gavilanez, and G. Rodriguez, "Audit Analysis Models, Security Frameworks and Their Relevance for VoIP," *arXiv preprint arXiv:1704.02440,* 2017.
[13] *International Organization for Standardization. Glosario de términos.* Available: http://www.iso27000.es/glosario.html. Accessed: 01/12/2017).
[14] UIT-T. *X.805: Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*. Available: https://www.itu.int/rec/T-REC-X.805-200310-I/es. (Accessed: 15/11/2017).
[15] OSSTMM. *Open Source Security Testing Methodology Manual*. Available: http://www.isecom.org/research/osstmm.html. (Accessed: 01/12/2017)
[16] D. Endler and M. Collier, *Hacking exposed VoIP: voice over IP security secrets & solutions*: McGraw-Hill, Inc., 2006.
[17] *GNS3*. Available: https://gns3.com/news/article/gns3-1-4-5-released-2. (Accessed: 15/11/2017).
[18] *National Institute of Standars and Technology. U.S. Departament of Commerce*. Available: https://www.nist.gov/. (Accessed: 15/11/2017).
[19] *VOIPSA*. Available: http://www.voipsa.org/. (Accessed: 15/11/2017).
[20] *ASTERISK*. Available: https://community.asterisk.org/t/asterisk-security-best-practices/. (Accessed: 15/11/2017).
[21] S. Salsano, L. Veltri, and D. Papalilo, "SIP security issues: the SIP authentication procedure and its processing load," *IEEE network,* vol. 16, pp. 38-44, 2002.

Karina Arellano was born in Riobamba, Ecuador. She got the Master of Science in Telematic Security from Polytechnic School of Chimborazo in 2016. Then, she joined as a full-time instructor on the Engineering Faculty at The National University of Chimborazo, Riobamba, Ecuador. Her current research interests include Network Security and Quantum Security.

Diego Avila-Pesantez was born in Cuenca, Ecuador in 1971. He received his master in Applied Informatics from Polytechnic School of Chimborazo, (ESPOCH) and B.S. in Computer Science degree from Catholic University of Cuenca. He is currently a Ph.D. student at San Marcos National University. Also, he is assistant professor at ESPOCH. His major research areas include Computer Network, Serious Games, and Virtual & Augmented Reality.

Leticia Vaca-Cárdenas was born in Riobamba, Ecuador in 1976. She received her Master in University Pedagogy and Educative Research from University of Loja, (UNL) and B.S. in Computer Science degree from Polytechnic School of Chimborazo, (ESPOCH). She got her Ph.D. in Science and Technology of the Complex Systems from University of Calabria (UNICAL), Italy. Her research areas include Computer Science, Educational Robotics, Serious Games and Virtual Environments.

Alberto Arellano was born in Riobamba, Ecuador in 1971. He received his master in Applied Informatics and B.S in Electronic Engineering from Polytechnic School of Chimborazo, (ESPOCH). His major research areas include Network Security and Wireless Sensor Network (WSN).

Carmen Mantilla was born in Riobamba, Ecuador. She received B.S. in Electronic Engineering and M.S. in Telematic Security from Polytechnic School of Chimborazo (ESPOCH) in 2010 and 2016, respectively. Now, she is working in Projects and Technology Transfer Department at ESPOCH. Her research areas include Telematic Security and Quantum Security.