A Set of Policies and Guidelines for Deploying Safer VoIP Solutions

Amelia Araneo, Eric Gamess, and Dedaniel Urribarri

***Abstract*—Attacks on networks which implement VoIP could lead to the degradation of the IP PBX performance, the interception of conversations, the theft of important and confidential information, and the generation of large expenses in any organization, if they do not have the correct security mechanisms. VoIP is based on existing layers and protocols and therefore inherits their security issues. In relation to signalization, different protocols have been proposed for VoIP. However, the Session Initiation Protocol (SIP) tends to be the favorite one because it is standardized by the IETF and has many features. Similarly to any other Internet protocol, SIP is susceptible to security threads, and can be involved in different kinds of attacks. In this paper, we propose three basic scenarios, representing common fundamental network architectures for VoIP, from which more complex systems can be built. We also establish a set of policies and guidelines focused on the aforementioned architectures, in order to mitigate security threads and provide more effective solutions for existing vulnerabilities in VoIP.**

***Index Terms*—Security, risk mitigation, VoIP, attacks, SIP, Elastix, Kali Linux.**

I. Introduction

VoIP (Voice over IP) is a technology that carries voice, previously digitalized and compressed, over data networks without the need of a conventional telephone infrastructure. As it rises in popularity, there is a growing concern about safety in VoIP solutions. VoIP relies upon other protocols and therefore inherits their security issues. That is, most of the important threats against VoIP are the classical well-known issues that affect common data networks. Hence, many of the attacks against VoIP networks are focused toward the hardware and software of VoIP devices, especially against the OS (Operating System) or the firmware. Even if just few users are concerned by the security of the voice system they use at work, it is fundamental to mitigate the security threads of those systems.

In this paper, we introduce three basic scenarios for VoIP. They can be used as elementary building blocks for large telephony solutions based on TCP/IP. For each of the scenario, we propose a set of policies and guidelines to mitigate security issues. Our work is focused on SIP [1]-[3] (Session Initiation Protocol) for the signaling protocol, and Elastix [4]-[6] as the IP PBX software.

Manuscript received January 14, 2017; revised March 18, 2017.

Amelia Araneo and Dedaniel Urribarri are with the School of Computer Science, Central University of Venezuela, Los Chaguaramos, Caracas, Venezuela (e-mail: aaraneo7@gmail.com, dedanielu@gmail.com).

Eric Gamess is with the Department of Mathematical, Computing, & Information Sciences, Jacksonville State University, Jacksonville, AL, USA (e-mail: egamess@jsu.edu).

The rest of this paper is organized as follows: we discuss related work in Section II. We introduce the three basic test scenarios, which can be used as building blocks of complex VoIP systems, in Section III. Section IV presents common attacks against VoIP solutions, while Section V gives important policies and guidelines to mitigate them. Finally, Section VI concludes the paper and gives directions for future work in this area.

II. Related Work

Many of the works done in the area are general, and not targeted to a specific IP PBX and signaling protocol. For example, in their study, Kuhn, Walsh, and Fries [7] made an introduction to VoIP technologies and solutions. They explained that the cornerstone to make VoIP more secure is to use all the security mechanisms available for data networks, such as firewalls, encryption, VPNs (Virtual Private Networks), SRTP [8] (Secure Real Time Protocol), among others. In [9], the authors presented ten important security issues, with a special emphasis over the vulnerabilities brought by the operating systems run by the computers used for the deployment, and the underlying network security. Keromytis [10] gave a comprehensive survey of VoIP security academic research, using a set of 245 publications. He classified these publications and provided a roadmap for researchers seeking to understand existing capabilities and to identify gaps in addressing the numerous threats and vulnerabilities present in VoIP systems. In [11], Androulidakis also made a very general introduction to IP PBX security issues.

Some other works are more oriented to the customization of the operating systems. For instance, the authors of [12] presented some recommendations and basic settings focused toward hardening the VoIP security of an IP PBX that runs on top of the CentOS operating system. These recommendations and settings were taken from books, tutorials, and the personal experiences of the authors, which help to keep a better safety in the server.

Security of the SIP [1]-[3] protocol represents an essential aspect when setting up and tearing down a VoIP session. The authors of [13] listed some of the existing vulnerabilities of SIP and provided a brief description of those, followed by a critical analysis of the security mechanisms that can be employed to mitigate the risks. The research in [14] also aims at improving security of the SIP protocol in VoIP solutions.

As stated previously, all the prior works are generic and cover a wide range of VoIP implementations. There are so general that all specific issues of a particular implementation are not covered. Up to now, just a few papers have been

DOI: 10.7763/IJCTE.2018.V10.1197

published targeted to specific IP PBX and signaling protocol. For example, [15], [16] were published by PaloSanto Solutions, the Ecuadorian company that develops Elastix as a fork of Asterisk, and is emphasized toward Elastix. In our research, we focus on Elastix as an IP PBX and SIP as a signaling protocol.

III. Basic Test Scenarios

In this section, we present three test scenarios with different characteristics, representing basic and widely used network architectures for VoIP. More complex VoIP solutions can be built in terms of these test scenarios.

A. Scenario 1: Basic VoIP Scenario Integrated with the Public Switched Telephone Network

Our first test scenario consists of a LAN network with VoIP support, connected to the Internet and the PSTN (Public Switched Telephone Network), as shown in Fig. 1. The connection to the latter is done by means of analog/digital boards. In the LAN, users access the telephone service through IP phones and softphones. It is also worth to point out that most of the modern IP phones have a small integrated Ethernet switch, allowing the connection of a PC to the LAN through the IP phones as depicted in Fig. 1.

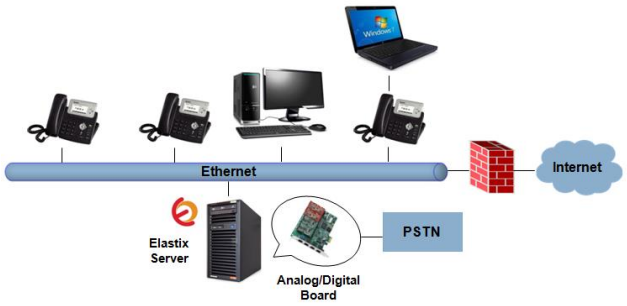

Fig. 1. VoIP network integrated with the PSTN.

B. Scenario 2: Basic VoIP Scenario with a ITSP Connection

For our second test scenario, we choose a LAN network with VoIP support, connected to an ITSP (Internet Telephony Service Provider) through a WAN link to the Internet, as shown in Fig. 2. Similarly to the first test scenario, users access the telephone service through IP phones and softphones.

Fig. 2. VoIP network connected to an ITSP.

C. Scenario 3: Basic VoIP Scenario with Remote Users

In our third test scenario, we propose a LAN network with VoIP support, connected to the Internet through a WAN link, and allowing remote users with IP phones and softphones to use the local VoIP service, as shown in Fig. 3.

Fig. 3. VoIP network with remote users.

For the three aforementioned test scenarios, we use a unified communications server (Elastix 2.4.0), connected to the LAN, for the IP PBX. Attacks against those basic architectures are generally done by hackers with a Linux distribution able to carry out VoIP penetration tests. In this work, we use Kali Linux [17]-[19], a popular Debian-based Linux distribution designed for digital forensics and penetration testing. A basic installation of Kali Linux has over 300 penetration-testing tools, where many of them are targeted for VoIP networks. It is a practical solution, which can be executed natively when installed on a computer's hard disk, or can be booted from a live CD or live USB, or can be run as a VMware or VirtualBox virtual machine.

IV. Common Attacks Against VoIP Solutions

A. Internal Attacks

Internal attacks are the most common and dangerous. These are started by someone with authorized access or who has gained authorized access to the local network, that is, they are originated within the organization itself. The three scenarios proposed are prone to internal attacks and vulnerabilities.

Possible internal attacks and vulnerabilities regarding the LAN network are explained below:

- Social Engineering: If an attacker is part of an organization, his contact with the other members of that organization will facilitate the gathering of important information to complete his attack. In this particular case, the attacker could obtain IP addresses and extensions belonging to the IP phones of other users or sensitive information with regard to the Elastix server to find a way to make his attack easier inside the network.
- Port Scanning: The attacker can run a network scanner such as Nmap [20], [21] (Network Mapper). It is a security scanner useful to scan hosts, ports, and services in a computer network. If Nmap is executed using the IP address of the Elastix server, then it is possible to gather information such as the operating system, the running services, and the TCP/UDP [22] open ports and their status.
- Man-in-the-Middle: In order to carry out this attack, internal network traffic must be intercepted and forwarded. This can be done with Ettercap, a tool that allows the interception of VoIP packages between the Elastix server and any extension belonging to the internal network. Since the communication between the

Elastix sever and the attacked extension is still alive via the attacker device, the two legitimate parties believe they are directly communicating with each other.

- Eavesdropping: To carry out this attack, a sniffer tool such as Wireshark [23], [24] can be used in order to capture the VoIP packages (signaling requests and responses, voice traffic, among others) between the Elastix server and the attacked extension. Before carrying out eavesdropping with a capture tool, it is necessary to first complete a "Man-in-the-Middle" attack, to redirect the traffic to the attacker's device where it will be processed and/or recorded for real-time or future reproduction, before being forwarding.
- DoS Attack: The idea of the DoS (Denial-of-Service) attack is to attempt to make a device or network resource unavailable to its intended users due to the exhaustion of resources. In Kali Linux, a tool called *inviteflood* can be used to this end. With this tool, the attacker can flood the Elastix server with a number of INVITE requests. Moreover, another tool known as *rtpflood* is also available in Kali Linux and permits to send RTP [25] packages to an IP address with an opened UDP port, during a VoIP call.
- Brute Force Attack: SIPDump and SIPcrack, available in Kali Linux, are tools that are usually employed together. SIPDump allows the capture of the authentication packets that a SIP IP phone exchanges with the Elastix server during the registration process. Then, SIPcrack is executed in order to make a brute force attack to try to find the password. SIPcrack requires the capture file generated by SIPDump and a list of words (or dictionary). It is worth to mention that similarly to the Eavesdropping, a Man-in-the-Middle attack is required to redirect the traffic to the attacker's device where it will be captured.

B. External Attacks Common to the Three Proposed Scenarios

External attacks are carried out by individuals or groups from outside the organization. The attacker does not have authorized access neither to the systems, nor to the network of the organization. Some external attacks are common to the three proposed test scenarios. The common attacks include, but are not limited to:

- Social Engineering: As the attacker is located outside the LAN network, it is possible that he uses different kinds of social engineering techniques, such as phishing, in order to jeopardize the security of the firewall. Once the hacker has bypassed the protection of the firewall, he has access to the LAN resources such as the Elastix sever.
- Port Scanning: As stated previously, a port scanner (such as Nmap [20], [21]) can be used to scan the open ports of the firewall. Once the hacker has obtained the list of open TCP and UDP ports, he can make a search in specialized databases and find the corresponding vulnerabilities, before trying to compromise the security of the firewall.
- DDoS Attack: Typically, tens of thousands of active connections can be stores in the connection table of a firewall, which is sufficient for normal network activity. However, in a DDoS (Distributed Denial of Service) attack, thousands of packets per second can be generated against the victim network. As the first device in the organizational network to handle the traffic, the firewall will open a new connection in its connection table for each malicious request, resulting in the quick exhaustion of the connection table. Once the connection table had reached its maximum capacity, it will not allow additional connections to be opened, ultimately blocking legitimate users from establishing new connections.
- Brute Force Attack against the Firewall: the goal of this attack is to get administrative privileges in the firewall, using a brute force attack to guest the credentials of the administrator, through a SSH or a HTTP connection according to the technology used for the administration of the firewall.
- Brute Force Attack against the Elastix Server: If secure connections (SSH) are allowed to the Elastix server from the outside world, the attacker should try to connect to the Elastix server through the Internet, using SSH. The Medusa tool available in Kali Linux could be used to carry out brute force attacks using the username "root", TCP port 22, and a password dictionary.

1) External attacks for Scenario 1

In Scenario 1, the first objective of the intruder will be to compromise the firewall that protects the LAN from attacks started from outside the organization. That is, the VoIP system is subject to all the common attacks presented in Section IV-B. However, it is also subject to attacks to its PSTN technology, which include attacks to the TDM (Time-Division Multiplexing) voice trunk.

2) External attacks for Scenario 2

ITSPs (Internet Telephony Service Providers) offer digital telecommunication services based on VoIP through Internet. In Scenario 2, the attacker's first objective will be to compromise the firewall and/or to hijack or piggyback on the SIP trunk in order to place toll phone calls at the expense of the organization. Some of the common attacks of Scenario 2 are described below:

- Social Engineering: In this case, the attacker can use different kinds of social engineering techniques to get the credentials of the SIP trunk connection (IP address, user, and password). If he succeeds, he can establish a trunk directly with the ITSP, in order to make a DoS attack or long distance phone calls that will be billed to the organization.
- DoS or DDoS Attack: The hacker can send a bunch of petitions through the SIP trunk in order to saturate the resources. That is, a significant number of malicious packets could result in a DoS or DDoS attack.
- Brute Force Attack: the goal of this attack is to get the credentials of the SIP trunk. If the attacker succeeds in getting this private information, he can directly establish the trunk with the ITSP to carry out a DoS attack or to make long distance phone calls.

3) External attacks for Scenario 3

With remote connections, authorized users that are

physically outside the organization have access to the network resources of the LAN that include VoIP support. Hence, they can establish VoIP calls originated from a local extension as if they were located inside the organization. In Scenario 3, the attacker's first objective will be to compromise the firewall and/or to enter the LAN as a remote authorized user. Scenario 3 is prone to multiple external attacks, and we discuss some of them bellow:

- Social Engineering: In this case, an attacker can use different kinds of social engineering techniques to get the credentials of an authorized remote user. If he succeeds, he can establish a remote connection to the LAN of the organization and harm the VoIP system, by making long distance calls at the expense of the organization, for example.
- Port Scanning: A port scanner (such as Nmap [20], [21]) can be used to scan the open ports of the remote connection server. Once the hacker has obtained the list of open TCP and UDP ports, he can make a search in specialized databases and find the corresponding vulnerabilities, before trying to compromise the security of the remote connection server.
- DoS or DDoS Attack: The hacker can send a bunch of petitions to the remote connection server in order to exhaust its resources. A significant number of malicious packets could result in a DoS or DDoS attack against the remote connection server.
- Brute Force Attack: the goal of this attack is to get the credential of an authorized remote user by using a brute force attack against the remote connection server.

V. Policies and Guidelines for Mitigations

A. Services Management

When operating a Unix-like server, it is essential to have a strict control over the services that will be running. By default, many services are installed and started in the server version of most Linux distributions. For an organization, it is a good practice to evaluate periodically which services are really needed and deactivate those that are not required or are no longer in use, in the unified communication server. In Elastix, this action is carried out by running the following command:

```
chkconfig  --level  3  4  5  <service>  off
```

Hence, the specified service will be off the next time the operating system is booted. However, the previous command does not stop the service if it is already running. To do so, the following command can be entered:

```
service  <service>  stop
```

In Elastix, it is suggested to turn off some services such as: *ip6tables*, *netfs*, *nfslock*, *wanrouter*, among others.

B. SSH Configuration

SSH (Secure Shell) is useful to access devices remotely through the network (remote sessions). In Linux, the configuration of the SSH server is stored in the file located in */etc/ssh/sshd_*config. It is recommended to modify some lines of the aforementioned file in order to improve the security of the SSH protocol, i.e., disabling root access, changing the default port, and the version of this protocol, as shown below:

```
PermitRootLogin  no
Port <newPort>
Protocol 2
```

C. Fail2ban

Fail2ban [26] is a log file analyzer that blocks IP addresses when it detects a suspicious activity, for instance, failed authentication attempts. Generally Fail2ban is then used to update firewall rules (e.g., *iptables*) to reject/block the IP addresses for a specified amount of time. However, any arbitrary other action could also be configured, such as the sending of email notifications with information about the suspicious behavior. Fail2ban is an open source software distributed under the GPL license and written in Python. The standard distribution has filters for Apache, Lighttpd, SSH, vsftpd, qmail, Postfix, and Courier Mail Server. Table I shows some terms used when configuring Fail2ban. The installation in Elastix is straightforward and can be done with the following command: *yum install fail2ban*.

TABLE I: Fail2ban Terminology

Terms	Fail2ban Meaning
filter	Filters are defined by Python regular expressions (regexes) and must be consistent with a pattern associated to a failed session start attempt. These filters are declared separately in files contained in the directory */etc/fail2ban/filter.d* and are invoked from the *jail.conf* file.
action	Actions are set of commands to be executed. They are declared separately in files contained in the directory */etc/fail2ban/action.d* and are invoked from the *jail.conf* file.
jail	It is a combination between a filter and multiple actions. Fail2ban is able to manage multiple jails at the same time in a file called *jail.conf* contained in the directory */etc/fail2ban*.

Before configuring Fail2ban to analyze logs files, it is necessary to verify the correct operation of *iptables*. The latter must be configured to start when the Elastix server is booting up.

For the configuration of jails, filters, and actions, the type of block that will be used by Fail2ban must be defined. File */etc/fail2ban/action.d/iptables-blocktype.conf* allows the configuration of DROP type block, which discards packets from the attacker without generating any response.

For Elastix, it is recommended to create jails associated to Apache, Asterisk, and SSH.

D. Firewall

A firewall is a hardware- or software-based security system that controls incoming and outgoing network traffic based on a set of rules. Netfilter is a software framework available in the Linux kernel for version 2.4 or higher, allowing the interception and management of network packages. *iptables*

is a user-space application built on top of Netfilter. It is a firewall tool that is not limited to packet filtering, since it also allows NAT (Network Address Translation) and log management. Its operation is based on the definition of rules added to chains, where each rule determines what to do with packets. By default, *iptables* has five predefined chains: (1) INPUT for packets entering an interface and destined to a local process, (2) OUTPUT for packets leaving an interface which was originated from a local process, (3) FORWARD for packets routed from one interface to the other, (4) PREROUTING just before deciding to use INPUT or FORWARD, and (5) POSTROUTING just after OUTPUT or FORWARD but before leaving the corresponding interface. Depending on its origin, a packet is checked against the relevant chains and a decision is made about what to do with the packet based upon the outcome of those rules, e.g. accepting (ACCEPT) or dropping (DROP) the packet.

To clean the network traffic that will be processed by the Elastix server, it is advised to setup a firewall. Rules will be needed to accept VoIP traffic in both ways (INPUT and OUTPUT) and to reject incoming traffic (INPUT) that should compromise the server (SIP vulnerabilities in ICMP messages, malformed packets, etc).

If a specific vendor firewall is used instead of *iptables*, its license must be up-to-date to avoid any disruption, periods where updating are not allowed, or security breaches due to a downgrade of functionalities.

E. PortSentry

One of the first step performed by an attacker, against a targeted system that he wants to break, is to run a port scan, with a tool such as Nmap [20], [21]. The idea of the port scan is to obtain a list of open ports (available services) on the attacked system as a starting point for break-in attempts. PortSentry, an open source tool, detects such scan attempts by monitoring the ports that are supposed to be closed. PortSentry has the ability to detect tests of connection to unused ports and to run a number of commands in response to this suspicious behavior. Common commands include the writing of a corresponding incident in system log files or the permanent blocking of the IP address of the intruder.

In the Elastix server, it is advised to use PortSentry together with Fail2ban to have time management in which the attacker IP address remains blocked for a specific amount of time and/or to send a notification email to the administrator.

F. Rootkits

A rootkit is a type of stealthy software, generally malicious and designed to hide the presence of processes or malicious programs from common detection methods. *chkrootkit* is a tool intended to help system administrators to check their systems for signs of rootkits. Some of the verifications that are done by *chkrootkit* include but are not limited to: (1) modifications of system binaries made by rootkits, (2) network interfaces in promiscuous mode, (3) deletions of entries in files related to logins made by users such as *lastlog*, *wtmp* and *utmp*, and (4) signs of LKM trojans. *chkrootkit* searches for LKM trojans by comparing a traversal of the */proc* filesystem with the output of the *ps* (process status) command to look for discrepancies.

It is recommended to install *chkrootkit* in the Elastix server to allow the detection of rootkits. Also, it is a good practice to schedule, for instance every day at 3:00 AM, the execution of *chkrootkit* to search for signs of rootkits and send a notification email to the administrators with the corresponding results. If any rootkit is found, it will be detailed in the email.

G. TCPWrapper

It is a system Access Control Lists (ACLs) which extends the abilities of the meta-daemon called *inetd* or *xinetd*. It can be used to restrict the TCP and UDP connections to the services managed by *inetd* or *xinetd*. It is an open source software that can be installed and configured in Unix-like operating systems such as Linux or BSD.

In Elastix, TCPWrapper is installed by default. Its configuration files (*hosts.allow* and *hosts.deny*) are located in the */etc* directory. When a connection attempt is made to a service, TCPWrapper verifies the aforementioned files to determine if the client is allowed to establish the connection. If it is authorized, then access is permitted; otherwise the access is denied.

H. Shellshock

Shellshock, also known as Bashdoor, is the name of a family of security flaws (6 CVEs) that compromise the Unix Bash [27], [28] (Bourne-Again Shell), a software component that interprets commands in the system. The first one was released in September 2014. Many networking services use Bash scripts to process some requests. The buggy version of Bash affected by Shellshock allows an attacker to execute arbitrary commands and gain unauthorized access to computer systems.

Elastix is based on the CentOS operating system and therefore it is necessary to verify whether or not it is subject to the Shellshock bug. For example, it is well-known that the unified communications server Elastix 2.4.0 for Intel x86 architecture (developed on top of CentOS 5.9) is vulnerable to Shellshock. In all cases, to be out of the reach of this security vulnerability, the operating system must be updated with the following command: *yum update bash*.

I. SELinux

Security-Enhanced Linux [29], [30] (SELinux) is an advance access control mechanism available in multiple Linux distributions. It was initially developed by the NSA (National Security Agency) in the United States to protect computer systems against malicious intrusions and manipulations. Over time, SELinux was released to the public and several distributions already have it incorporated in their code. SELinux uses a number of known rules set as a policy to authorize or deny operations. Permissions management is completely different from traditional Unix systems. The permissions of a process depend on the security context.

Each context is defined by the identity of the user executing the process, the role and the domain that the user had in that moment. Permissions really depend on the domain but the roles control the transition among domains. Finally, the possible transitions among roles depend on the identity.

In the Elastix server, it is advised to consider the

installation and customization of SELinux.

J. Elastix Configurations

Once installed, it is suggested to apply adjustments to the Elastix server in order to improve its security. The default route "9_Outside" associated to outgoing routes must be removed since it allows outgoing calls.

Access Control Lists (ACLs) must be configured to register extensions, that is, SIP authentication requests should not be accepted from any IP address. Elastix ACLs are configured using fields "permit" and "deny" within the configuration of each extension.

AMI (Asterisk Manager Interface) is a client/server service over TCP to control an Asterisk PBX, make calls, monitor channels and queues, and execute Asterisk commands. The default AMI password must be changed to a secure password. Additionally, the allowed connections to the AMI service must be limited with fields "permit" and "deny".

FreePBX [31] is an open source GUI to control and manage the Asterisk PBX. It is available in Elastix. It is strongly recommended to enable it temporally at the time that administration tasks must be done in the IP PBX, and to disable it once finished.

Additionally, it is suggested to change the context "from-internal" by custom contexts. An extension belonging to this context allows the access to all outgoing routes defined in Elastix. Finally, it is also advised to create contexts for local, national, and mobile calls through the PSTN and ITSP.

K. DoS and DDoS Countermeasures

Fail2ban [26] can minimize attacks to the unified communication server when multiple requests are sent in bulk without any authentication, such as the INVITE requests generated by *inviteflood*. A firewall is able to filter incoming packets that are not authorized, adding a security level against DoS and DDoS attacks. However, Fail2ban and a firewall do not fix completely the threads caused by DoS and DDoS attacks when both are massive. As a consequence of this excessive number of requests, extensions lose their registration with the IP PBX, resulting in their incapacity to make calls. DoS and DDoS attacks can be either internal or external attacks and the Elastix server is vulnerable to them. To mitigate these threads, the usage of a firewall with an IPS (Intrusion Prevention System) module and load balancers is strongly recommended. An alternative solution, which is not always better, is the acquisition of an appliance devoted to the detection and mitigation of DoS and DDoS attacks, such as Fortinet FortiDDoS. Also, it is worth to mention that there are solutions based on cloud services to protect systems against DoS and DDoS attacks. These solutions act as a proxy that protects and cleans the traffic to the systems. In all case, it is important to avoid the exposition of the Elastix server to the Internet without any additional security device in the front line.

L. ARP Spoofing and Related Attacks Countermeasures

ARP spoofing is an attack in which the attacker sends fake ARP (Address Resolution Protocol) Reply messages to ARP Request messages. This attack can only be done in the LAN where the IP address, to be resolved to a MAC address through ARP, is connected. As a result, in the requester ARP cache (the node that sent the ARP Request), the intruder's MAC address is associated with the IP address of the computer or server that should have been resolved. Once the attack is done, the intruder will begin to receive the data traffic from the requester (the node that sent the ARP Request) that is intended for the IP address that the requester tried to resolve.

With ARP spoofing, a malicious party can intercept the traffic originated by an extension toward the Elastix server. Many other attacks can be then performed, such as Man-in-the-Middle, Eavesdropping, DoS, and session hijacking. An efficient solution for ARP spoofing is to use static entries in the ARP cache of the Elastix server. This allows to invalidate ARP messages coming from any attacker because the IP addresses are statically associated with MAC addresses. This is a simple solution and it is recommended in small VoIP systems. However, it is a difficult strategy to implement if a network has a large number of extensions.

DHCP snooping [32] and DAI [32] (Dynamic ARP Inspection) are techniques used to secure a DHCP infrastructure. These techniques keep track of the MAC addresses connected to each port and immediately detect if there is an impersonation attack. Nowadays, many network vendors incorporate these solutions as a component of their instruments, such as Cisco Systems. When available in the network devices, it is a good practice to configure them.

Also, there are tools to monitor ARP traffic, such as *arpwatch*. This tool is available for CentOS and can be easily integrated in an Elastix server in order to see any suspicious change in the correspondence between IP addresses and MAC addresses.

M. OpenVPN

A VPN (Virtual Private Network) is a private network which connects remote sites and remote users located in different places of the Internet, as if they had direct links. That is, VPNs can be used to securely connect employees to a corporate intranet while located outside the office. Moreover, VPNs can also securely connect geographically separated branches of an organization, to build one cohesive network. OpenVPN [33], [34] is an open source software published under the GPL license that allows the implementation of VPNs, by establishing secure point-to-point connections and facilitating remote access. It can be used to secure all Internet traffic, including web traffic, email, instant messaging, and VoIP. Regarding VoIP, OpenVPN is used to encrypt and secure conversations passing through the Internet with remote extensions. The VPN server, OpenVPN in this particular case, is configured in the Elastix server and the VPN clients are installed on the remote extensions, such as IP phones or softphones. Thus, OpenVPN helps to add a layer of security against the "Man-in-the-Middle" attacks.

N. IDS/IPS

An IDS (Intrusion Detection System) is a device or software that detects suspicious activities in the network and system. It is responsible for monitoring events occurring in the network and system to seek attempts of intrusions and violations, before reporting them. An IPS (Intrusion

Prevention System) is a device or software that monitors the network and system activities in order to detect suspicious behaviors, log information about these events, attempt to block them, and report them. IDS are more passive, while IPS are active. That is, an IPS not only reports violations, but also is in charge to drop detected malicious packets, reset suspicious connections, and block traffic from the attacker's IP address. It is important to protect the network with an IDS/IPS and to locate it in a different computer from the Elastix server. Additionally, the packets must be intercepted by the IDS/IPS before reaching the IP PBX, so the former can make its analysis, in order to improve the protection of the unified communications server. Finally, it is vital that the IDS/IPS is kept up-to-date with the installation of updates to ensure smooth operation and prevent future attacks.

O. Good Practices and Recommendations

In this section, we present some good practices and general recommendations for VoIP infrastructures, with the aim of mitigating vulnerabilities that can be present in systems using this technology:

- Have an appropriate policy for physical access to the Elastix server.
- Keep the Elastix server up-to-date by regularly applying security patches and updates.
- Update the firmware of the IP phones as soon as the manufacturers release new versions.
- Avoid the usage of standards TCP/IP ports.
- Enforce a policy for strong passwords in SIP entities.
- Make sure that SIP usernames and their extensions are different.
- Disable international calls if they are not required.
- Deny requests to UDP port 5060 from the outside if the system has no external SIP users.
- Review the system logs periodically.
- Do not allow unauthenticated calls.
- Disable all services that are not used.
- Use VPNs (Virtual Private Networks) to allow remote users to access the corporate network services, or between remote branches of the organization.
- Verify the integrity of directories, system files, and executables in the Elastix server.
- Uninstall all the products and software that are not in use in the Elastix server.
- Use VLANs to separate the voice traffic from the data traffic.
- Disable the unused signaling protocols such as IAX2 [35], [36] (Inter-Asterisk eXchange 2), H.323 [37], MGCP [38] (Media Gateway Control Protocol), and Cisco SCCP (Skinny Call Control Protocol).
- Encrypt the traffic of the trunk between the Elastix server and the ITSP.

VI. Conclusions and Future Work

In this research work, we proposed three basic scenarios for VoIP architecture. More complex VoIP implementations can be built as a combination of those proposed basic scenarios. We also provided policies and guidelines for hardening the security of VoIP systems, including firewalls, end-devices, the operating system of the IP PBX, and some additional recommendations to comply with the five basic objectives related to security: (1) confidentiality, (2) integrity, (3) availability, (4) authentication, and (5) non-repudiation.

It is clear that in parallel with technology advances, vulnerabilities and attacks will continue to appear and evolve. Nevertheless, essential mechanisms for protection will be developed too. The challenge lies in the definition of adequate policies for organizations and a strict application of them. VoIP inherits the security issues of the protocols and systems supporting it, hence the security policies of a VoIP implementation should not be limited to this technology, but must also include the operating system of VoIP servers, the firmware of IP phones, the classical vulnerabilities related to TCP/IP, and even the transmission network itself. By proposing the implantation of the aforementioned policies and guidelines, we pretend to reach higher security levels and a better operation in telephony solutions based on VoIP technology (aka, Elastix server and SIP). Of course, this proposal is not definitive, because the attacks and solutions evolve over the years.

As future work, we plan to study vulnerabilities in other IP PBX solutions such as FreeSWITCH [39], [40], and sipXcom. Moreover, we are also interested to further investigate security threads related to IAX2 [35], [36] (Inter-Asterisk eXchange 2), since it is now published as an informational Request For Comment by the IETF.

References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, "RFC 3261: SIP: Session initiation protocol," presented at the Workshop on Contemporary Communications, June 2002.

[2] A. Johnston, *SIP: Understanding the Session Initiation Protocol*, 4th ed. Artech House Publishers, October 2015.

[3] H. Sinnreich and A. Johnston, *Internet Communications Using SIP: Delivering VoIP and Multimedia Services with Session Initiation Protocol*, 2nd ed. Wiley, July 2006.

[4] E. Land ívar, *Comunicaciones Unificadas con Elastix*, vol. 1, 2008.

[5] E. Land ívar. *Comunicaciones Unificadas con Elastix*, vol. 2, 2009.

[6] G. Barajas, *Elastix Unified Communications Server Cookbook*, Packt Publishing, March 2015.

[7] R. Kuhn, T. Walsh, and S. Fries, *Security Considerations for Voice over IP Systems*, National Institute of Standards and Technology, January 2005.

[8] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman, "The secure real-time transport protocol (SRTP). RFC 3711," March 2004.

[9] DesignDATA, "Top ten security issues with Voice over IP (VoIP)," *White Paper Series*, 2010.

[10] A. Keromytis, "A comprehensive survey of Voice over IP security research," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 514–537, April 2011.

[11] I. Androulidakis, *VoIP and PBX security and forensics – A practical approach*, 2nd ed. Springer, May 2016.

[12] PaloSanto Solutions, *Seguridad en Servidores CentOS con Elastix*, 2010.

[13] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and S. Gritzalis, in *Proc. of the Fifth International Network Conference 2005 (INC 2005)*, Samos, Greece, July 2005.

[14] R. del Valle and M. Herrera, "Seguridad del protocolo SIP en la VoIP," *Serie Cient fica*, vol. 2, no. 4, 2009.

[15] PaloSanto Solutions, *Seguridad en Implementaciones de Voz Sobre IP*, April 2014.

[16] R. Martin, *Seguridad en Servidores CentOS con Elastix + Buenas Pr cticas*, PaloSanto Solutions.

[17] D. Dieterle, *Basic Security Testing with Kali Linux*, CreateSpace Independent Publishing Platform, March 2016.
[18] S. Oriyano, *Learning Kali Linux: An Introduction to Penetration Testing*, 1st ed. O'Reilly Media, September 2016.
[19] R. Beggs, *Mastering Kali Linux for Advanced Penetration Testing*, Packt Publishing, June 2014.
[20] D. Shaw, *Nmap Essentials*, Packt Publishing, May 2015.
[21] N. Marsh, *Nmap 6 Cookbook: The Fat Free Guide to Network Security Scanning*, 6th ed. CreateSpace Independent Publishing Platform, February 2015.
[22] W. Stallings, *Data and Computer Communications*, 10th ed. Pearson, September 2013.
[23] C. Mishra, *Mastering Wireshark*, Packt Publishing, March 2016.
[24] J. Bullock and J. Kadijk, *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework*, 1st ed. Wiley, September 2016.
[25] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, *RTP: A Transport Protocol for Real-Time Applications. RFC 3550*, July 2003.
[26] M. Ford, C. Mallery, F. Palmasani, M. Rabb, R. Turner, L. Soles, and D. Snider, "A process to transfer fail2ban data to an adaptive enterprise intrusion detection and prevention system," in *Proc. the 2016 IEEE Region 3 South East Conference (SoutheastCon 2016)*, Norfolk, VA, USA., April 2006.
[27] R. Blum and C. Bresnahan, *Linux Command Line and Shell Scripting Bible*, 3rd ed. Wiley, January 2015.
[28] W. Shotts, *The Linux Command Line: A Complete Introduction*, 1st ed. No Starch Press, January 2012.
[29] S. Vermeulen, *SELinux Cookbook*, Packt Publishing, September 2014.
[30] S. Vermeulen, *SELinux Policy Administration*, Packt Publishing, October 2013.
[31] A. Robar, *FreePBX 2.5 Powerful Telephony Solutions*, Packt Publishing, October 2009.
[32] G. Kaur and J. Malhotra, "An Integrated Approach to ARP Poisoning and its Mitigation using Empirical Paradigm," *International Journal of Future Generation Communication and Networking*, vol. 8, no. 5, pp. 51–60, 2015.
[33] E. Crist and J. Just Keijser, *Mastering OpenVPN*, Packt Publishing, August 2015.
[34] M. Feilner, *OpenVPN: Building and Integrating Virtual Private Networks*, 2nd ed. Packt Publishing, October 2016.
[35] M. Spencer, B. Capouch, E. Guy, F. Miller, and K. Shumard, *IAX: Inter-Asterisk eXchange Version 2. RFC 5456*, February 2010.
[36] M. Boucadair, *Inter-Asterisk Exchange (IAX): Deployment Scenarios in SIP-Enabled Networks*, 1st ed. Wiley, February 2009.
[37] V. Kumar and M. Korpi, *IP Telephony with H.323: Architectures for Unified Networks and Integrated Services*, 1st ed. Wiley, March 2001.
[38] B. Foster and C. Sivachelvan, *Media Gateway Control Protocol (MGCP) Return Code Usage. RFC 3435*, December 2003.
[39] A. Minessale, M. Collins, and G. Maruzzelli, *FreeSWITCH 1.6 Cookbook*, Packt Publishing, July 2015.
[40] A. Minessale and G. Maruzzelli, *Mastering FreeSWITCH*, Packt Publishing, August 2016.

Amelia Araneo received her B.S. degree in computer science from the Central University of Venezuela, Venezuela, in 2015. She has worked for one year at Cotronica C.A., Venezuela, as a software developer. Currently, she is working at Mijao Asesores C.A., Venezuela, as a software developer. Her research interests include voice over IP and security.

Eric Gamess received a M.S. in industrial computation from the National Institute of Applied Sciences of Toulouse (INSA de Toulouse), France, in 1989, and a Ph.D. in computer science from the Central University of Venezuela, Venezuela, in 2000. He is currently working as a professor at Jacksonville State University, Jacksonville, AL, USA. Previously, he worked as a professor at University of Puerto Rico, Puerto Rico, Central University of Venezuela, Venezuela, and "Universidad del Valle", Colombia. His research interests include vehicular adhoc networks, network performance evaluation, IPv6, and network protocol specifications. He is a member of the Venezuelan Society of Computing and has been in the organization committee and program committee of several national and international conferences.

Dedaniel Urribarri received his B.S. degree in computer science from the Central University of Venezuela, Venezuela, in 2002. He is currently pursuing a master degree in computer science in the aforementioned university and also acts as a professor. For 5 years, he worked as a project manager in Symantec Inc, for the Latin America Region. Currently, he is the CEO of CGTS Corp., a company dedicated to the installation, maintenance, and development of VoIP solutions and Full Stack Software Factory. His research interests include voice over IP, security, network administration, and social networks.