


An Approach to Mitigate DDoS Attacks on SIP Based VoIP [†]

Warda Amalou *  and Merouane Mehdi

DIC Laboratory, Department of Electronics, Faculty of Technology, University Blida 1, Soumâa Street No. 270, Blida 9068, Algeria; mmehdimerouane@gmail.com

* Correspondence: wardaamalou@gmail.com; Tel.: +213-698086200

† Presented at the 1st International Conference on Computational Engineering and Intelligent Systems, Online, 10–12 December 2021.

Abstract: Voice over Internet Protocol (VoIP) is a recent technology used to transfer video and voice over the Internet Protocol (IP). Session Initiation Protocol (SIP) is the most widely used protocol for signaling functions in VoIP networks. However, the VoIP service is vulnerable to several potential security threats. Distributed denial of service (DDoS) attack is a dangerous attack that prevents legitimate users from using VoIP services. In this paper, we propose a detection scheme based on the Deep Packet Inspection (DPI) method of analyzing packets to extract attack signatures for implementation in new VoIP DDoS attack detection rules with a low false negative rate. We have included experimental results to confirm the proposed scheme.

Keywords: DDoS; DPI; IP; SIP; VoIP



Citation: Amalou, W.; Mehdi, M. An Approach to Mitigate DDoS Attacks on SIP Based VoIP. *Eng. Proc.* **2022**, *14*, 6. <https://doi.org/10.3390/engproc2022014006>

Academic Editors:
Abdelmadjid Recioui,
Hamid Bentarzi and Fatma
Zohra Dekhandji

Published: 26 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

VoIP is an emerging voice communication technology. VoIP saw light after the appearance of the protocol of data network management. The voice is transformed into data that will then be transformed into IP packets and then transposed into the equipment of IP clients. This is how VoIP is present today on smartphones, tablets and PCs. This requires a VoIP phone, software or hardware.

Free software has caused havoc and an incursion into the world of telephony through PC-PBX solutions running under Linux or another free system and equipped with Open Source software such as Asterisk, Yate, VOCAL etc. [1].

Reliable, free and robust, Asterisk is probably the first Open Source solution of the VoIP for this we chose as solution for the realization of this work by also choosing a user-friendly and easy to use GUI named FreePBX and a multiplatform Softphone known as 3CX that allows users to make phone calls over the Internet. Like all computer systems, VoIP lines are exposed to the same attacks as your Internet connection and email. Cyber criminals develop attacks that specifically target VoIP. We have provided you with an update on the risks and best practices to know to secure your IP telephony.

2. Platform Asterisk

2.1. VoIP: Protocols and Codecs

Today's voice networks, such as the public switched telephone network (PSTN), use digital switching technology to establish a dedicated link between the caller and the recipient.

H.323 is an ITU (International Telecommunication Union) standard originally developed for real-time multimedia conferencing and additional transfer. Technically, it is a container for several network and multimedia codec standards. The connection signaling part of H.323 is managed by protocol H.225, while the negotiation function is supported by H.245.

However, SIP is defined by the Internet Engineering Task Force (IETF) under RFC 3261. It has been developed specifically for IP telephony and other Internet services. SIP is used with the session description protocol for user discovery; it provides feature negotiation and call management. SDP (Session Description Protocol) is essentially a format to describe the initialization settings for multimedia streaming during the announcement and session invitation. The SIP/SDP pair is somewhat analogous to the H.225/H.245 protocol defined in H.323. SIP uses six basic methods to express its requests [2]:

1. SIP INVITE: This request indicates that the specified SIP Uniform Resource Locator (Uniform Resource Locator) user is invited to participate in a session.
2. SIP ACK: This request allows the caller to confirm that they have received a final response to a PROMPT request.
3. SIP OPTIONS: This request is used to query a SIP server, including the UAS (User Application Server) on different information.
4. SIP BYE: This request completes a communication.
5. SIP CANCEL: This request cancels all requests that have not yet been answered to the requester.
6. SIP REGISTER: This request allows the client to save its address to the server it is linked to [3].

2.2. Presentation of Asterisk

Asterisk implements the H.323 and SIP protocols as well as a specific protocol named IAX (Inter Asterisk eXchange). It allows communication between client and server as well as between two servers.

Asterisk derives its name from the asterisk symbol "*" found on telephone keyboards, implements the features and services of a PBX, allowing telephones to make calls and interconnect to the public switched telephone network and IP telephony networks. Thanks to its software nature and the GNU General Software License without GPL public license. Users can build telephone systems, add features to existing networks, or replace existing PBXs.

Although originally designed in the late 1990s for Linux, it can now be deployed on many other operating systems. What is more important is that because of its compact size code, it is possible to run it in an embedded system, while it can also boot from a flash drive, live CD or external drive [4].

2.2.1. Interface FreePBX

FreePBX is a simple-to-use GUI that controls and manages Asterisk. This interface offers pre-programmed features accessible via a user-friendly web interface to have a functional PBX without any programming [5].

2.2.2. Softphone 3CX

The 3CX phone system replaces a hardware IP phone. It supports SIP phones, VoIP providers and traditional PSTN lines. The simplicity of web-based management of the 3CX makes it easy to configure eliminating the need for costly maintenance [6].

3. Work Architecture

After presenting the Needs Identification section. This section presents the software environment by determining the different tasks performed. Figure 1 shows the working environment with the various machines installed.

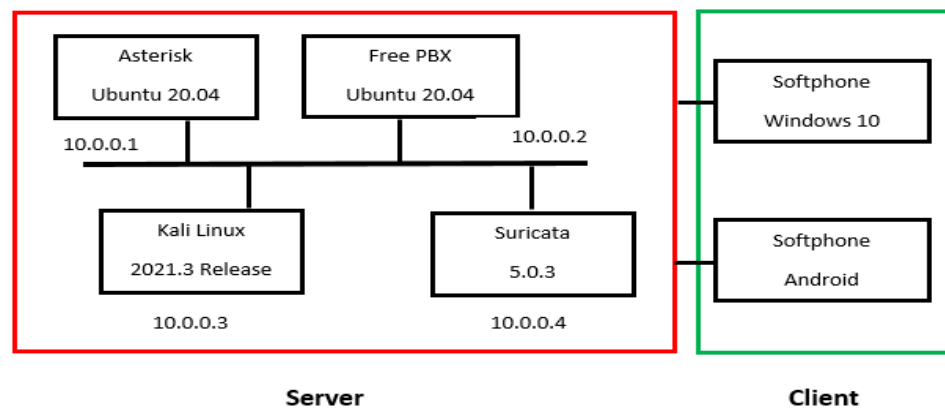


Figure 1. Overall diagram of the work carried out.

3.1. Asterisk Server Setup

Implementation of Asterisk and FreePBX

Create a new server by choosing Ubuntu 20.04 as the operating system with at least 2 GB of RAM.

FreePBX requires the Apache Web Server, MariaDB and PHP version 7.2 to be installed on your server. By default, Ubuntu 20.04 comes with PHP version 7.4, so you will need to install the Ondrej PHP repository on your server.

Thanks to the graphical interface one does not need to manage users manually with the file sip.conf of Asterisk, it is enough to access the FreePBX interface of administration after being identified. Among the FreePBX services the addition of SIP clients are shown in Figure 2.

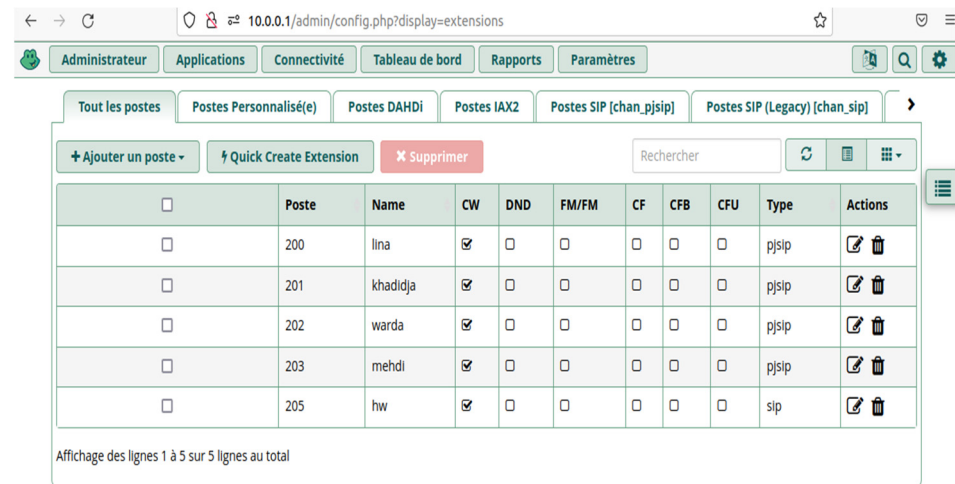


Figure 2. Adding SIP clients to FreePBX.

This interface has the role of a well-defined database that undergoes each time an update of users, we have two types of customers, pjsip clients for softphones and chansip clients for Android devices, it is a convenient and easy to handle interface.

3.2. Implementation of 3CX Softphones

Each user has the option to download the Softphone (Android or Windows version) depending on the device used. Figure 3 shows a test of a successful call between two Softphone 3CX which are installed first on Windows XP and second on Windows 10.



Figure 3. Testing a call between two Softphones.

4. VoIP Security Risks and Methods

The VoIP is currently appearing and may be under attack. The VoIP.ms telephone service provider in Quebec implemented an aggressive denial-of-service attack that caused calls and telephone service interruptions. The incident began on or about 16 September and severely tested the VoIP provider’s systems, websites and operations [7]. A second unprecedented coordinated cyber-attack hit voice-over-IP service providers in late October 2021. This type of distributed denial-of-service attack is intended to flood a website with Internet traffic in order to take it offline or expose it. The malicious campaign recently targeted VoIP providers that provide telephone services to businesses in the UK, including emergency services. VoIP.ms serves more than 80,000 out of 125 customers, most of whom are currently experiencing call problems [8].

DDoS is a form of cyber-attack in which computers, or bots, are simultaneously hired by an attacker to send a large number of Internet server requests that exceed the capacity of the server. As a result, an Internet server, faced with a sophisticated DDoS attack, can offer degraded performance or even complete collapse.

A SYN Flood occurs when the TCP layer is saturated, preventing the completion of the three-channel TCP negotiation between the client and the server on each port. Each connection using the TCP protocol requires the three-way handshake, which is a set of messages exchanged between the client and the server as shown in Figure 4.

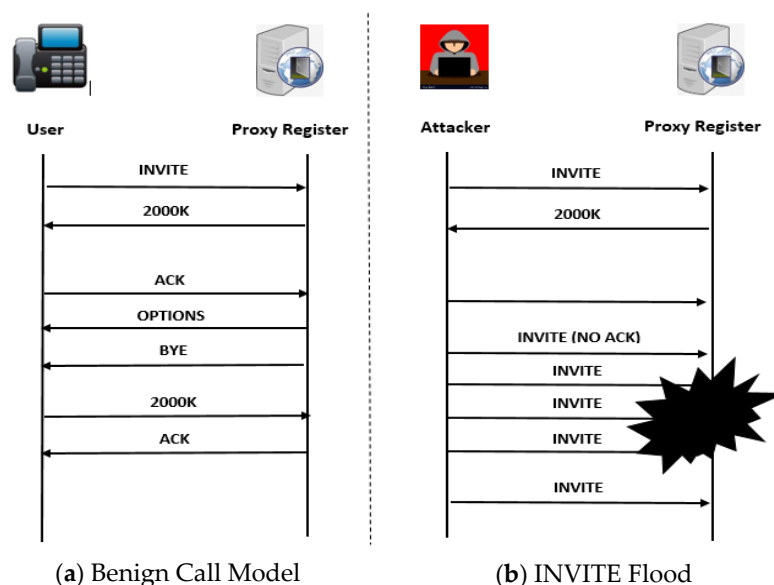


Figure 4. IP Call Models.

Different tools can be adapted to launch DoS/DDoS attacks, and others are explicitly designed for this purpose. Among these tools: (LOIC, Slowloris, Kali Linux etc...)

Kali Linux is a Debian-based GNU/Linux distribution with over 6008 pre-installed security analysis programs including Wireshark (a package analyzer), John the Ripper (a password-breaking tool) and Sipcrack (a software suite to crack the SIP protocol).

Security Solutions and Methods

In recent years, DDoS attacks against the VoIP have combined all these categories of attacks. This makes them even more dangerous and difficult. The adoption of an anti-DDoS solution is needed to strengthen the security of an IT infrastructure and applications. For this purpose, the monitoring of the health of the network is one of the essential tasks of the maintenance of infrastructures using an analysis tool such as: (tcpdump, caploader, Wireshark...). This part of work is dedicated to extracting digital fingerprints that characterize these offensives for this analysis is essential in our research before moving to detection. Wireshark captures packages and allows you to examine their contents [9].

To protect against computer attacks, firewalls are no longer enough. Intrusion detection systems are able to detect threats that the firewalls do not suspect. Like all IDS, Suricata has been developed for safety and performance as shown in Figure 5.

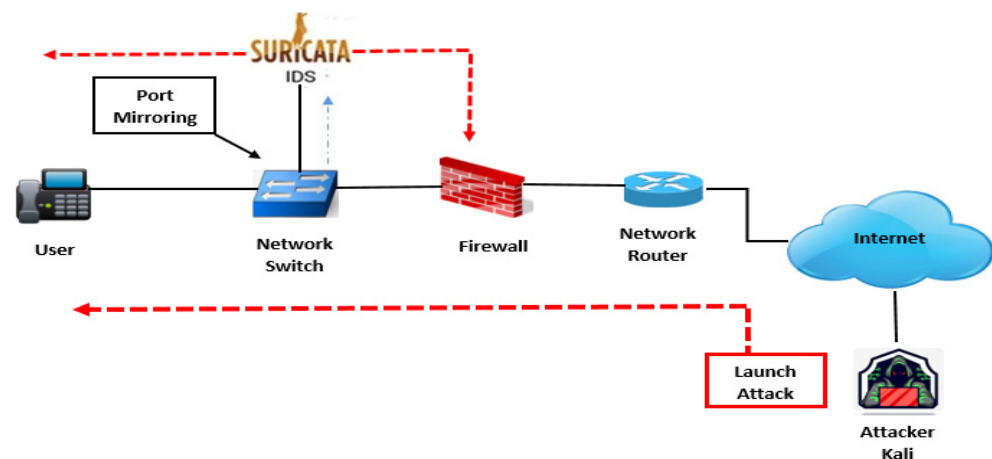


Figure 5. Network Intrusion Detection System Suricata Engine.

In terms of safety, good practices apply: dangerous functions are prohibited, defensive programming is the rule, a few thousand tests have been carried out.

Suricata can be configured to operate in four modes:

- Sniffer mode: in this mode, Suricata reads packets circulating on the network and displays them continuously on the screen;
- The “packet logger” mode: in this mode Suricata logs network traffic in directories on the disk.
- Network Intrusion Detection (NIDS) mode: in this mode, Suricata analyzes the network traffic, compares that traffic to rules already defined by the user and establishes actions to be performed.

5. Conclusions

VoIP is in danger. While voice communications (VoIP) have become more vulnerable to the same type of attacks that data has undergone over the past two decades, Organizations are constantly trying to ensure that precautions are taken to ensure the confidentiality and security of their communications. An IDS is an essential element for SIP user agents, but more SIP-based VoIP endpoints provide it. VoIP network administrators should consider implementing this technology within their SIP-based networks to benefit from the

additional level of security that fire can provide. Using an IDS helps to keep the network safe from the real user and prevents DDoS, redirections and disconnections.

Author Contributions: Conceptualization, W.A. and M.M.; methodology, W.A. and M.M.; software, W.A. and M.M.; validation, W.A. and M.M.; investigation, W.A. and M.M.; resources, W.A. and M.M.; data curation, W.A. and M.M.; writing—original draft preparation, W.A. and M.M.; writing—review and editing, W.A. and M.M.; visualization, M.M.; supervision, M.M.; project administration, W.A. and M.M.; funding acquisition, W.A. and M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Kasse, B. Study and Implementation of a VoIP Communication System: Applied to an Open-Source IP PABX. Master's Thesis, University Cheikh Anta Diop de Dakar, Dakar, Senegal, 2011.
2. How VoIP Works: Protocols, Codecs and More. Available online: <https://www.eetimes.com/how-voip-works-protocols-codecs-and-more/> (accessed on 21 September 2021).
3. What Is Session Initiation Protocol (SIP) & How Does It Work? Available online: <https://www.nextiva.com/blog/sip-protocol.html> (accessed on 5 September 2021).
4. Andreoulakis, I.I.; Pedini Ioannina, B. *VoIP and PBX Security and Forensics, a Practical Approach*, 2nd ed.; Springer Nature: Cham, Switzerland, 2016; pp. 154–196.
5. ALEX Robar, *FreePBX 2,5 Powerful Telephony Solution*; Packet Publishing: Birmingham, UK, August 2009; ISBN 9781847194725.
6. DON Ayupo, *Break Free from Outdated Phone*; 3cx Innovating Communications: Nicosia, Cyprus, 15 May 2020; pp. 1–8.
7. Canadian VoIP Provider Hit by DDoS Attack, Phone Calls Dropped. Available online: <https://www.oxtero.com/2021/09/22/un-fournisseur-de-voip-canadien-touche-par-une-attaque-ddos-les-appels-telephoniques-interrompus/> (accessed on 29 October 2021).
8. DDoS Attack against VoIP Service Providers, the New Form Of Ransomware, November 2021 by Patrick LEBRETON. Available online: <https://www.globalsecuritymag.fr/Attaque-DDoS-contre-des,20211104,117891.html> (accessed on 9 November 2021).
9. Strengthen IT Security against DDoS Attacks. Available online: <https://www.clarinet.fr/expertises/cyber-securite/renforcer-la-securite-informatique-contre-les-attaques-ddos> (accessed on 7 September 2021).