Leave this box blank

Security Model for Blocking Spam Calls in VoIP Systems

Dr Athirah Mohd Ramly[1], Robbin Ooi Zhen Heng[2], Yahya Khamayseh[3], Tse-Kian Neo[4], Angela Amphawan[5]

[1] *University of East London, United Kingdom (Great Britain)*
E-mail: athirahr@sunway.edu.my

[2,3] *Department of Computing and Information Systems, Sunway University, 5, Bandar Sunway, Petaling Jaya, 47500, Malaysia*
E-mail: 20036505@imail.sunway.edu.my
E-mail: khamayseh.yahya@gmail.com

[4]*Faculty of Creative Multimedia, Multimedia University, 63100 Cyberjaya, Selangor, Malaysia.*
E-mail: tkneo@mmu.edu.my (Corresponding Author)

[5]*Smart Photonics Research Laboratory, School of Engineering and Technology, Sunway University, Petaling Jaya,47500, Malaysia*
Email: angelaa@sunway.edu.my

***Abstract*— In the ever-evolving landscape of digital communication, the security of VoIP systems has become a primary concern to both individuals and organizations. The escalating prevalence of threats and attacks targeting the confidentiality, integrity, and availability of VoIP systems poses a major issue in the digital age. To address this issue, this project presents a comprehensive evaluation on the cyber threats and attacks present in VoIP and its potential risks to certain systems. These security threats and attacks were simulated in a controlled environment to study their methods and impacts on VoIP infrastructure. This project also aimsto proactively mitigate one of the most prevalent threats in VoIP, spam calls, by proposing and implementing an effective security model utilizing different modules. Through rigorous testing and analysis, the simulation successfully provided valuable insights into the mechanisms of certain attacks. The security model was also capable of identifying and blocking automated spam calls and blacklisted manual spam calls before reaching a client, significantly mitigating disturbance caused by spam calls.**

***Keywords*— VoIP Security; Cyber Threats; Spam Call Mitigation; Attack Simulation; Security Model**

I. INTRODUCTION

A. Motivation

The motivation behind this project stems from the recognition that, as VoIP serves as the foundation for crucial communication services, spanning from business conference calls to personal conversations, it has introduced a complex and ever-evolving set of security challenges in telecommunications and computer networking. Thus, it is evident that the security of VoIP systems is of paramount importance to both individuals and organizations. This research contributes to the ongoing efforts to study the security of VoIP and proposes a simple method to make VoIP communication a more secure and reliable means of modern communication.

The paper is organized into 5 main sections to facilitate a comprehensive understanding of our work. Section I provides an overview of the research objectives and contextualizes the significance of our study. Section II delves into the existing body of knowledge surrounding our topic, offering a critical analysis of previous studies and establishing the foundation for our research. Section III details the approach and techniques employed in our investigation to ensure rigor and reliability. Section IV presents the empirical findings derived from our study, accompanied by analysis and interpretation. Finally, Section V concludes the paper, summarizing key insights, discussing implications, and suggesting avenues for future research.

B. Background of Study

Voice over Internet Protocol (VoIP), also known as Internet telephony, is a revolutionary technology that has transformed the way humans communicate with one another. Traditionally, voice calls relied on the Public Switched Telephone Network (PSTN), which utilizes circuit- switched networks to transmit calls over telephone lines. However, PSTN had several limitations such as limited flexibility and scalability, restraints of having advanced features, and cost inefficiency over long network distances [1]. Due to these limitations, researchers developed the VoIP technology to make and receive calls anywhere in the world using different devices including landlines, smartphones and even computers [2]. Thus, VoIP is progressively being used for both personal and commercial purposes and is expected to become the dominant technology for online communication with fifth generation (5G) networks [3], [4]. Additionally, [5] predicts that there will be at least 29 billion devices connected to IP networks by 2023, showing a steady growth of Internet devices.

VoIP takes advantage of the Internet Protocol (IP) where it converts human voice into digital signals, compresses it into data packets with its routing information, and transmits them to their intended destination over the Internet [6]. Figure 1 shows an example of a VoIP packet. At the receiving end, the transmitted packets are then reassembled to recreate the original voice for the receiver [7]. Hence, this transmission process enables real-time voice communication to be transmitted wirelessly, making VoIP an efficient communication method today for both local and international users. Figure 2 shows the overall VoIPtransmission process. However, with its numerous advantages it provides for individuals and business organizations, it still has certain limitations that may affect user experience.

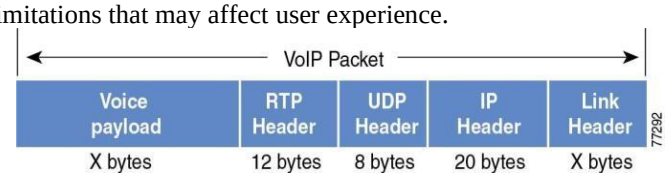

Figure 1 VoIP packet [6]

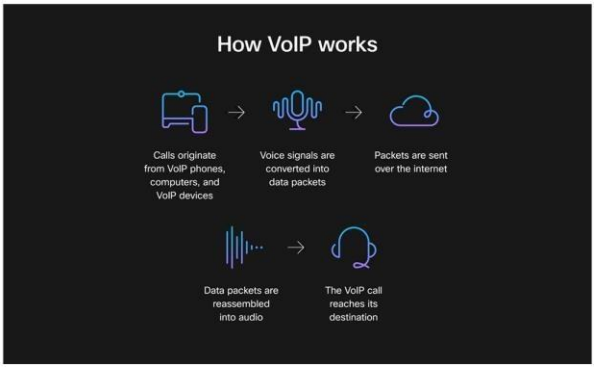

Figure 2 VoIP transmission process [7]

1) Advantages of VoIP: One key advantage of VoIP is its cost-effectiveness. Unlike traditional phone systems that rely on dedicated lines, VoIP utilizes Internet connections which eliminates the need for separate infrastructure and cables [8]. Thus, reducing implementation cost, particularly for long-distance and international networks.

Another notable benefit of VoIP is its high flexibility and scalability. It proves particularly advantageous for remote, hybrid, or highly mobile users, allowing them to make calls from anywhere at any time when connected to the Internet [6]. VoIP systems can also easily accommodate businessgrowth or fluctuations in call volume by adding or removing extension lines as needed, making it an ideal choice for any business organizations or even home networks [8].

Other than voice calls, VoIP offers a wide range of advanced features and functionalities that enhance communication efficiency including call forwarding, voicemail, video conferencing, instant messaging, and others [8].

2) Disadvantages of VoIP: One significant limitation with VoIP is its dependency on a stable and reliable Internet connection for optimal performance with no disruptions. If the Internet connection is weak, it can lead to quality of service (QoS) issues such as dropped calls, audio delay and jitters. Additionally, power outages can disrupt VoIP services unless backup power solutions are in place [9].

Next, VoIP services may not always provide the same level of reliability and location accuracy for emergency callssince the 911 emergency system was originally built fortraditional telephony systems [6]. Users relying on VoIPshould be aware of potential limitations in emergency situations and consider alternative means for ensuring communication reliability during critical times.

Lastly, since VoIP calls are connected to the public Internet, it makes calls susceptible to certain threats and attacks that aim to disrupt or intercept it [9]. This major disadvantage is why most researchers nowadays have developed security mechanisms to protect VoIP systems from risks and vulnerabilities.

C. Problem Statement

As VoIP continues to gain popularity, it has introduced a range of security challenges that need to be addressed immediately to minimize potential risk and damage to both individuals and organizations. This technology has become prime targets for malicious actors due to various factors including their reliance on Internet connectivity, adherence to open standards, and inadequate security configurations. Additionally, VoIP faces security risks due to existing vulnerabilities within its protocols, presenting opportunities for malicious exploitation. Hence, it is important to study and analyze the various threats and attacks relevant in the field of VoIP through simulations. Such analysis would shedlight on the evolving landscape of VoIP security, enabling a comprehensive knowledge base that can serve as a foundation for future works in the fields of telephony and cybersecurity. Furthermore, as highlighted in [5], the rapid growth of devices connected to IP networks has significantly increased the susceptibility and exposure to spam calls. This endeavor seeks to address the escalating threat posed byspam calls within the dynamic landscape of IP-connected devices. Thus, an efficient security model was required to address a common issue in VoIP, spam calls.

D. Objectives

The objectives are as listed: -

- To understand the basics of VoIP technology and its protocols.
- To analyze the threats and attacks in VoIP and examine their impacts through simulations.
- To propose and implement a security model that mitigates automated spam calls

E. Project Scope

The scope of this project centers around a comprehensive evaluation of the architecture and functionalities of VoIP and its protocols. The project will explore the different threats and attacks within the VoIP landscape such as call eavesdropping, Denial of Service attack, Spam over Internet Telephony, and others, aiming to simulate them for an in- depth analysis. Furthermore, this project will delve into an extensive review of countermeasures proposed by other researchers, offering insights into various methods for mitigating VoIP-specific threats. These insights will also serve as a crucial foundation for the development of theproposed security model. However, it is essential to clarify that the primary goal of the security model was to onlymitigate spam calls, hence the focus will not be on anyauthentication or encryption mechanisms.

II. Literature Review

A. VoIP Architecture

Figure 3 illustrates the VoIP architecture that encompasses the structure and primary components involvedin enabling voice communication over the Internet [2]. These components work together to allow VoIP systems to interact with remote and local IP phones over the Internet.

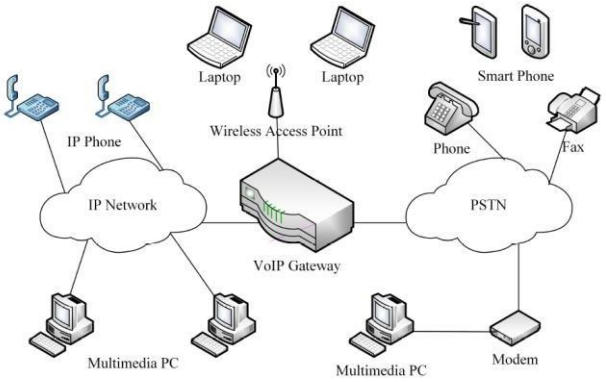

Figure 3 VoIP architecture [2]

The primary components of a VoIP system can be categorized into several key elements. This includes end- user equipment, network components, call processors, gateways, and protocols [2]. End-user equipment represents the devices used for VoIP communication between users within the network. This includes softphones, IP phones, andcomputers. Next, network components including cables, routers, switches, and other network hardware play a pivotal role in ensuring seamless connectivity and reliable data transmission between components in the network.

Another integral aspect of VoIP systems is the presence of call processors which are operating system software responsible for executing various functions such as call setup, call monitoring, and user authorization. The gateways act as intermediaries between VoIP and PSTN networks to handle analog to digital conversion and manage calls origination and detection. Gateways can include media gateways for handling media streams, media gateway controllers responsible for call control, and signaling gateways that interface with external networks [10]. Lastly, the foundation of communication in VoIP systems is laid by protocols. Protocols serve as sets of rules and standards governing the communication between different components within the VoIP system. The main categories of protocols in VoIP include signaling protocols and transport protocols.

B. Protocols

Unlike PSTN, VoIP integrates both peer-to-peer and client-server models where every user and server must be connected to the Internet. The client-server model involves communication through a server that facilitates call setup, routing, and other control functions, while peer-to-peer model enables direct communication between users [11].However, IP networks were established for regular data exchange and were not designed to be suitable for real-time transmission. This is because voice is different from regular data where data is not delay sensitive while voice requires maximum QoS with little to no delay between users in transmission [1]. Hence, certain protocols are implementedin VoIP systems to ensure full voice transmission support across a wide range of devices and networks. Generally, two primary protocols are present in VoIP, this includes a signaling and transport protocol. Signaling protocols are used to establish a session between users while transport protocols are used to transmit data in real-time by carrying the voice payload across the established session [12].

1) Session Initiation Protocol (SIP): Signaling protocols play a crucial role in VoIP to establish and handle a call session. The widely adopted signaling protocol, SIP, was originally developed by the Internet Engineering Task Force (IETF) in 1996 and published as RFC 3261 [3], [13]. It has become the primary signaling protocol and the successor to the ITU recommendation H.323. Despite both protocols providing similar functions, SIP was considered the dominant signaling protocol because of its simplicity, easy implementation, and lightweight operation [2]. Hence, SIP has garnered widespread industry support, with leading manufacturers such as Cisco, Avaya, Yealink, and software vendors like Asterisk and Freeswitch to build products and platforms that support VoIP [14].

SIP is an application layer, text-based protocol that is designed to initiate, modify, and terminate sessions between two or more parties [13]. By being text-based, SIP encompasses several elements of the Hypertext Transfer Protocol (HTTP) and the Simple Mail Transfer Protocol (SMTP) which relies on a request-response model to exchange data between clients using a server [15]. However, SIP is incapable of working alone and is commonly integrated with other protocols to support the transmission of voice packets over the Internet [16]. These protocols include the Session Description Protocol (SDP) to describe the session characteristics and media formats, Transport Layer Security (TLS) protocol to encrypt SIP messages, and even transport protocols like Real- Time Transport Protocol (RTP) and Real-Time Control Protocol (RTCP) for the transmission of voice and multimedia data in real-time.

2) Real-time Transport Protocol (RTP): As mentioned earlier, the signaling protocol is often paired with other protocols to establish a complete call. Among these protocols, transport protocols play a vital role in enabling seamless, real-time audio and video transmission during calls. RTP is the main transport protocol used for end-to-end media transmission in real-time over an established session [19]. Additionally, the Real-time Control Protocol (RTCP) is commonly used in conjunction with RTP where both protocols cooperate to ensure maximum QoS for the delivery of voice packets.

RTP works by segmenting data into small packets, which are then encapsulated in either User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) segments for transmission over IP networks. However, RTP typically utilized UDP due to its low overhead and low latency, which are crucial for maintaining real-time communication in comparison to TCP which favors data integrity and reliability rather than transmission speed [18]. Although using UDP causes some packets to be lost during transmission, this limitation is generally overlooked since a steady flow of data during calls is more important than waiting for delayed packets. Hence, RTP utilizes sequence numbers and timestamps within its packet headers to fixcertain limitations. The sequence numbers ensure that packets are reassembled in the correct order and identify anymissing or out-of-order packets, thus ensuring no packets aredropped or lost. The timestamp determines the inter-arrival packet time, thus minimizing jitter issues. Additionally, RTP

provides other features such as payload identification, source and frame identification, and delivery monitoring [15].

RTP packets are created at the application layer and handed to the transport layer for delivery. RTP data begins with a packet header which contains fields required to properly interpret and process the RTP packet, ensuring proper synchronization, sequencing, and decoding of data. An example of the RTP packet header is shown in Figure 4.

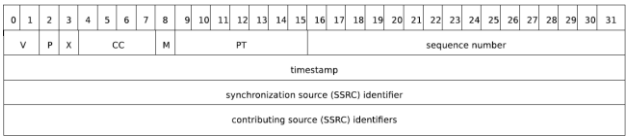

Figure 4 RTP packet header [18]

TABLE I

RTP PACKET HEADER FIELDS [18]

Fields	**Description**
V (Version)	Indicates RTP version
P (Padding)	Indicates if there is padding at the end of the payload.
X (Extension)	Indicates presence of an extension header between the header and payload data
CC (CSRC Count)	Represents the number of CSRC identifiers that follow the fixed header.
M (Marker)	Application-specific marker bit (usage depends on the application).
PT (Payload Type)	Identifies the type of data carried by the payload.
Sequence number	Provides a unique identifier for the packet's sequence within the stream.
Timestamp	Represents the timestamp of the data in the packet.
SSRC identifier	Uniquely identifies the source of a stream.
CSRC identifiers	Represents the identifiers of the contributing source for the payload contained within the given packet.

C. *Threats and Attacks in VoIP*

1) Call Eavesdropping: Call eavesdropping is one of the most common and frequent attacks in VoIP which involves an attacker passively monitoring and listening to an ongoing conversation between two parties without their knowledge or consent. Since most VoIP traffic is unencrypted, any person can easily intercept and listen in on the traffic flow between the parties to capture sensitive information [20]. Additionally, it presents a base for other VoIP attacks such as SPIT, registration hijacking and MitM attacks [10]. Tools such as Wireshark and tcpdump are commonly used by attackers to monitor network traffic and capture data packets.

2) Man-in-the-Middle (MitM) attack: MiTM attacks involve an attacker intercepting an ongoing call between two parties that are unaware of the attacker's presence. The attacker will position themselves as an intermediary between the communicating parties to both review and modify transmitted messages before forwarding it to the intended receiver [21]. Additionally, the attacker may also drop several packets from reaching its destination or alter its parameters, making the call last longer than its actual duration, hence adding higher costs than expected [1]. An example of a MitM attack is shown in Figure 5. The key difference between a MitM attack and call eavesdropping is that call eavesdropping only involves passively monitoring and sniffing traffic flow in a VoIP network, whereas a MitM attack not only intercepts and listens to the communication but also has the capability to alter the transmitted data [9].

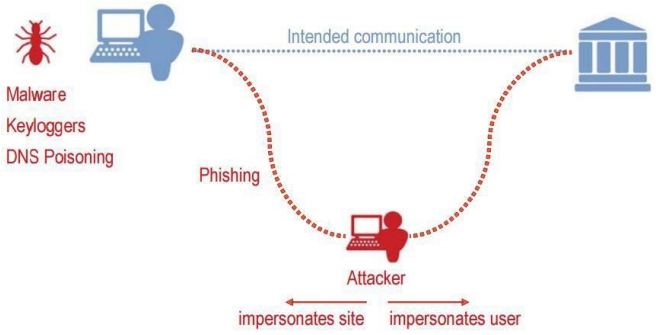

Figure 5 MiTM attack [21]

3) Denial of Service (DoS) attack: DoS attacks involve an attacker compromising and disrupting the availability of VoIP services using a single source or machine. Certainmethods are utilized to carry out DoS attacks on a VoIP network where the attacker aims to render a system from providing its services to clients or significantly degrade QoS [20], [22]. These methods often involve flooding the targeted system with either SIP messages or sending malformed messages to cause processing errors.

In message flooding attack, an attacker overwhelms a target, usually the server, with an excessive amount of generated SIP messages such that it depletes systemresources including CPU, memory, and bandwidth [20]. As aresult, the server will have insufficient memory or processing power to handle further legitimate requests, causing its services to be inaccessible for an indefinite time. Message flooding can be in multiple forms including INVITE flooding (Figure 6), REGISTER flooding, BYE flooding, ping flooding attacks and multi-attribute flooding [23].

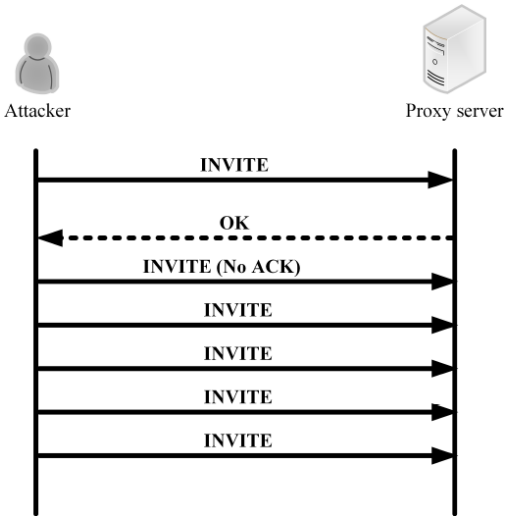

Figure 6 DoS flooding attack with INVITE [2]

In malformed message attack, tampered SIP messages are utilized to cause a partial reboot or failure of the targeted recipient when attempting to parse the message [24]. Malformed messages are messages that are incompatible with the correct SIP syntax including an invalid methodname, a disarrangement in message hierarchy, or a missing mandatory SIP header [2]. With SIP being text - based, attackers can easily alter different fields of a normal SIP message and since a parser is designed to process correctly formatted SIP messages, encountering syntactically incorrectmessages will result in numerous instances of processing failures, thus causing the terminals to malfunction or stop working entirely. Additionally, attackers can also exploit the SDP section of a message by sending SDP-crafted malformed messages and cause further DoS [17]. Figure 7 shows an example of a malformed message with an invalid method name.

```
8rafgki sip: xzmLqOZp@WD.22mSllpi.bb SIP/2.0
CSeq : 0 OPTIONS
Via: SIP/2.0/UDP pc77.atlanta.com; branch = z9hG4bK336asdhds; received = 192.0.2.5
To: sip:xzmLqOZp@WD.22mSllpi.bb; tag = U7IZWSXQ
Max-Forwards: 242
From: sip: xjlE@rCRzWf.M6ilfPsE.bs; tag = L5EgPZ1wQ
Contact: "Mr. Bill" <sip:bill@worcester.bell-telephone.com>; q = 0.7; expires = 3600
Call-ID: YeZ8Dao18g1tSj@ZtHRcJSjOXjqeL
Accept: application/sdp; level = 3, application/x-private, text/html
Content-Language: EbxqOZGc
Content-Type: application/sdp
Content-Length: 40
Date: Wed, 28 Sep 2012 23:29:00 GMT
v = 0
o = mhandley 29739 7272939 IN IP4 126.5.5.3
c = IN IP4 135.180.130.85
t = 0 0
m = audio 492170 RTP/AVP 0 12
s = 1
a = rtpmap : 31 LPC
```

Figure 7 Malformed message attack [2]

4) Distributed Denial of Service (DDoS) attack: Similar to DoS attacks, DDoS attacks also aim to compromise and disrupt the availability of VoIP services. However, instead of utilizing a single source, DDoS attacks utilize multiple sources or machines to initiate DoS methods on a target system in a coordinated and distributed manner [20], [23]. Hence, detecting DDoS attacks will be far more challenging since the attack traffic is distributed across multiple sources and compromised users are usually unaware that their machines are being controlled in a DDoS attack. This causes source blocking based on traffic limitations to be ineffective, hence more difficult to identify the attacker [24]. DDoS attacks significantly impact businesses where the huge downtime of servers will create major revenue loss and reputation damage [3]. According to [25], the result of a prolonged DDoS attack can cause significant logistic and financial consequences, including loss of customer trust and monetary damage to the business up to 35,000 euros per hour over an average duration of 15 hours.

The most common method to carry out a DDoS attack is by building a botnet, a network of compromised machines called 'bots' or 'zombies' [21], [22]. These zombies arecontrolled by the attacker through handlers, and they are given certain commands to carry out the attacks. With the botnet, instead of flooding the target victim with just a single machine, the attacker can utilize multiple machines to flood the victim with excessive amounts of requests, thus causing severe resource consumption. Figure 8 shows a simple scenario of a botnet targeting a victim system.

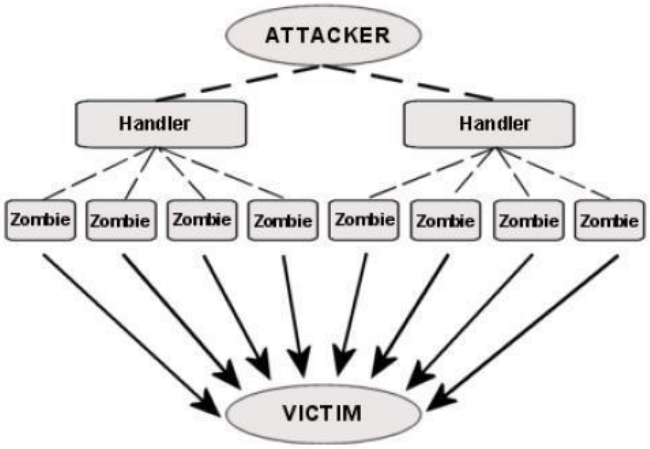

Figure 8 Botnet targeting a victim [21]

Over time, attackers have introduced a more sophisticated form of DDoS attack known as Distributed Reflection Denial of Service (DRDoS) as depicted in Figure 9. This attack extends the DDoS attack with IP spoofing mechanisms to enhance its complexity and destructiveness. In this attack, the attacker spoofs the victim's IP address to initiate requests for information from reflectors [16], [26]. These reflectors, unaware of the forged source IP address, unwittingly direct its responses to the victim's IP address, essentially flooding the victim with amplified traffic [16]. The key difference between a DRDoS and DDoS attacks is that it does not target the victim directly but instead sends packets to the victim through exploitable reflectors. DRDoS also involves spoofing the sender's IP address to imitate the target victim, effectively concealing the identity of the attacker. Consequently, existing detection and mitigation schemes for DDoS attacks will be ineffective against it [26].

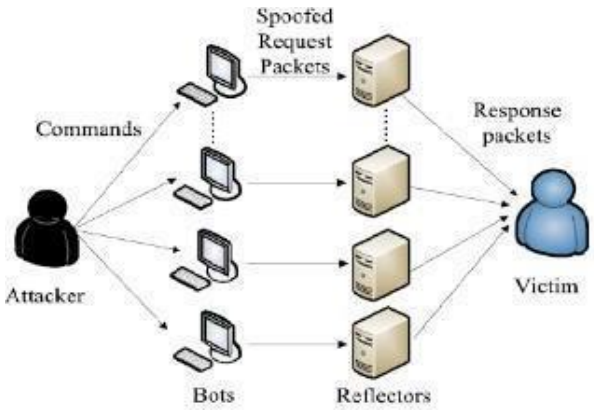

Figure 9 DRDoS attack [26]

5) Caller ID Spoofing: As shown in Figure 10, caller ID spoofing is a form of telephone fraud where attackers manipulate or forge the caller ID displayed to a party, disguising their real identity to appear as if the call is originating from a different number or a trusted entity. It is commonly used for impersonation, social engineering, swatting and other malicious acts. Nowadays, it is much simpler to spoof caller ID since many VoIP providers allow any user to claim arbitrary caller ID through VoIP client software and several fake ID providers allow users to claim any caller ID by simply dialing an unusual phone number or by utilizing readily available applications [11], [29]. With caller IDs being transmitted in plaintext, this attack will always be possible and caller identity can easily be manipulated if no proper authentication is implemented. According to [11], spoofing caller ID can be carried out in various setups, including fake ID providers, automated phone systems, or even VoIP services.

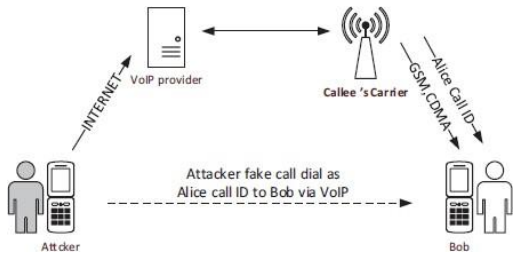

Figure 10 Caller ID spoofing attack [29]

6) Spam over Internet Telephony (SPIT): SPIT or VoIP spam, involves sending unwanted and unsolicited messages, often in the form of pre-recorded voice calls to targeted users over VoIP networks. This attack is relatively simple to propagate because attackers can create automated calls or a multi-recipient call and broadcast them to devices connected to the Internet, reaching multiple users simultaneously, hence increasing the area of the attack and bandwidth wasted[1]. SPIT is commonly used for product advertisement, user harassment, scamming, or phishing users to dial specific numbers or obtain private information. Additionally, SPIT attacks indirectly contribute to DoS since it floods a VoIP system with a high volume of unwanted calls, thus overwhelming the victim's capacity and causing network congestion [27], [28]. Spam calls can be in various formsthat aim to cause disturbance and annoyance to users. These forms include telemarketing calls, vishing (voice phishing) calls, recorded calls, and silent calls [28]. Telemarketingcalls and vishing calls are manually done by attackers while recorded calls and silent calls are generally automated using auto dialers.

Both voice and email have unwanted spam that affects user experience. However, voice spam remains more disruptive and challenging to detect compared to email spam due to several factors [1], [28]. The main factor is users are usually affected more from voice spam because it can cause immediate, real-time inconvenience to users with intrusive automated phone calls and voice messages while email spam is usually stored and processed automatically by a spam detector. The second factor is that email spam is usually easier to detect since an email contains various information for spam detection including text, images, attachments, and others. For voice spam, only caller information can be detected while the actual call content is undetectable untilthe call is accepted. In addition, because spam calls are often delivered from unknown or spoofed phone numbers, it becomes more challenging to detect [4]. Hence, these factors show that using email spam detectors to detect voice spam will be inefficient and not a suitable method to mitigate SPIT.

7) Malware: Malware, short for malicious software, refers to software developed by adversaries to infect VoIP components and cause damage. They pose great danger in VoIP as they can easily gain unauthorized access, steal sensitive information, and even disrupt or damage its services. Malware can be in different forms, including worms, trojans, viruses, spyware, and others [21].

8) Brute Force Attack: While time-consuming, brute force attacks are still considered a potential risk in VoIP. It involves a trial-and-error process where the attacker systematically attempts multiple combinations of logincredentials, mainly passwords, to gain unauthorized accessto a VoIP system [21]. Although brute forcing can takeanywhere from a few seconds to many years to succeed, depending on the password complexity, it is still a simple,yet reliable attack method done by inexperienced hackers to gain unauthorized access to VoIP systems with weak security measures and encryption.

D. Countermeasures

After reviewing various literature on security mechanisms proposed to combat certain VoIP attacks, each of them will be discussed in terms of their advantages and limitations. Since the proposed methods may be affected by factors such as hardware specification and configuration, detection time and performance will be used as the primary metrics to evaluate a method's effectiveness. Additionally, any detection time exceeding one second will be considered as a limitation because it is not suitable for VoIP systems that utilize real-time communication.

1) DoS/DDoS Countermeasures: As mentioned by [2], the methods to detect and mitigate DoS/DDoS attacks in VoIP systems can be classified into several categories including finite state machine (FSM) approach, rules-based approach, statistically-based approach, and machine learning approach. Additionally, most of the surveyed methods were tested

against flooding, specifically INVITE flooding, while others were tested against malformed messages and even DRDoS attacks.

2) SPIT Countermeasures: As mentioned by [34] and [35], SPIT detection and mitigation approaches can be categorized into list-based, reputation-based, pattern-based and machine learning. Most of the surveyed approaches utilized machine learning while others were either pattern-based or reputation-based to detect and mitigate SPIT attacks. However, none of the approaches utilized list-based filtering.

3) Authentication Schemes: The issue with SIP protocol being text-based is that it was not designed to be secure by default, making it vulnerable to various certain threats [38]. Hence, authentication and encryption schemes are crucial in VoIP to ensure user privacy and confidentiality by verifying the identity of callers. Thus, researchers have developed authentication schemes utilizing different methods including blockchain, VPN, verification challenges, and others.

III. Methodology

A. VoIP Network

First, a self-hosted VoIP network was required to act as a testbed for the attack simulation. This can be done using virtual machines to conserve the number of physicalmachines required for this activity. Figure 11 shows thegeneral design of the network where two end devices are connected to a VoIP server. The end devices will register themselves to the VoIP server and establish a communication channel to communicate directly with each other.

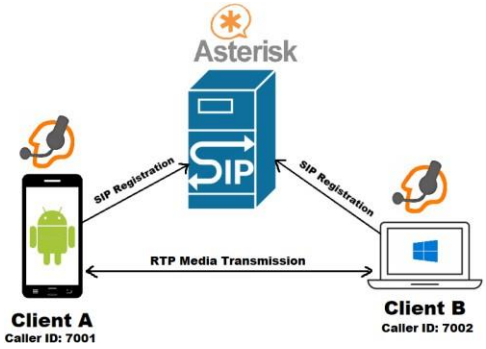

Figure 11 Self-hosted VoIP network

B. Attack Simulation

Several threats and attacks in VoIP will be simulated in a controlled environment to study their methods and impact on VoIP systems. This includes call eavesdropping, Man-in-the-Middle (MitM) attacks, Denial of Service (DoS) attacks, caller ID spoofing and Spam over Internet Telephony (SPIT). However, Distributed Denial of Service (DDoS) attacks will not be simulated because of the lack of machines and machine strength to launch a realistic DDoS attack.

1) Call Eavesdropping: Call eavesdropping is an attack where attackers passively eavesdrop on-going calls between clients, capturing SIP and RTP traffic using packet sniffing tools like Wireshark or tcpdump. Since VoIP involves the transmission of unencrypted traffic, attackers can potentially intercept the communication channel between SIP clients and steal sensitive information to perform a large variety of threats and attacks that may further damage a VoIP system. Attackers employ techniques such as placing their device in promiscuous mode, allowing it to monitor all network traffic,or utilizing port mirroring to duplicate and redirect traffic to their location. This enables the attacker to extract and obtain sensitive information including caller ID, source and destination address, RTP ports, and even the conversation. Consequently, the privacy of clients engaged in a call is therefore compromised, and confidential information may be at risk.

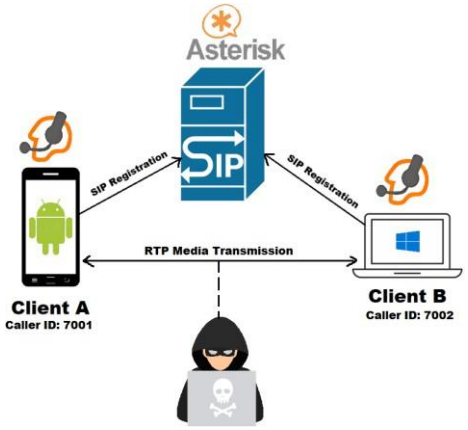

Figure 12 Call eavesdropping

2) Man-in-the-Middle (MitM) attack: Instead of passively monitoring a conversation, the attacker may attempt to intercept on-going call sessions and it is usually achieved by performing ARP poisoning with a famous attack tool, Ettercap. By performing ARP poisoning on the specified targets, the attacker will be able to eavesdrop and potentially tamper with the intercepted call flow by injecting RTP packets into it. This is because the RTP protocol is vulnerable to media tampering, especially if used without encryption and using the connectionless transport protocol UDP. Additionally, the communication session is controlled by the SSRC (Synchronization Source Identifier), sequence number, and timestamp. Exploiting these elements, the attacker can analyze the RTP packets and replicate them with the same SSRC and greater sequence number and timestamp, forcing the destination endpoint to discard legitimate packets and capture the attacker's packets, because they have a higher sequence number.

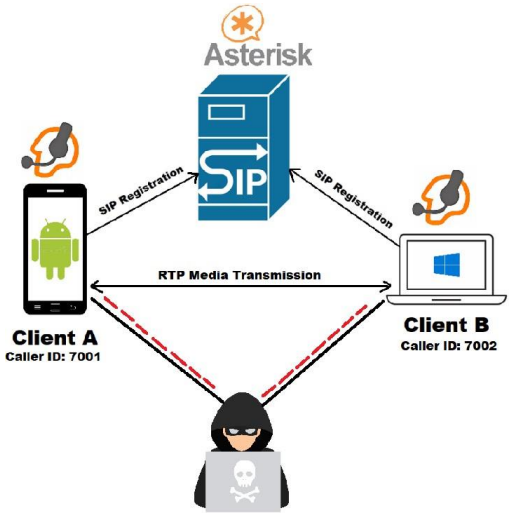

Figure 13 Man-in-the-Middle (MitM) attack

3) Denial of Service (DoS) attack: In DoS attacks, the attacker aims to overwhelm a target by sending an excessive volume of concurrent SIP call-signaling messages, surpassing the target's processing capacity. This will exhaust system resources or render it entirely nonfunctional, thereby degrading its service which causes calls to drop prematurely, and halts call processing for clients. One common technique employed in DoS attacks is the flooding attack, which involves the use of specific SIP messages to overwhelm a VoIP server. Tools such as InviteFlood or Sippts [16] are commonly used to generate and send multiple INVITE requests to Asterisk rapidly and cause DoS. Throughout the attack, the server's status is closely monitored to assess the utilization of its resources and to identify if the inundation of generated packets is affecting the server's reception.

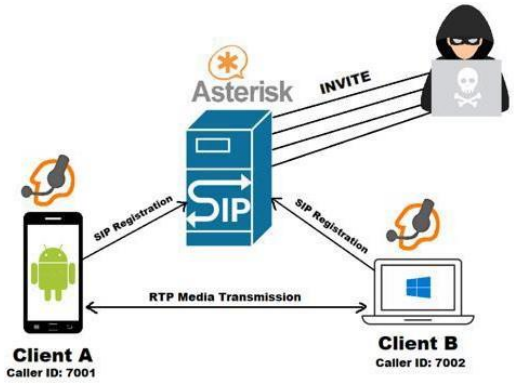

Figure 14 Denial of service (DoS) attack

4) Caller ID spoofing: Caller ID spoofing is a deceptive technique employed by attackers to manipulate their caller ID and impersonate another SIP client for potentially malicious purposes, including social engineering and fraudulent activities. This method involves altering the caller ID to impersonate and display a different phone number or name than the actual caller, often to make the call appear legitimate. This is because VoIP essentially allows callers to select their own preferred display number or name when setting up a SIP account, making it easy to mask their own identity and conduct phishing attempts. In some cases, certain providers even offer spoofing services similarly to a prepaid calling card where customers pay for a PIN code that they can use to call their service provider, allowing them to choose both the destination number and the number that will appear on the recipient's caller ID.

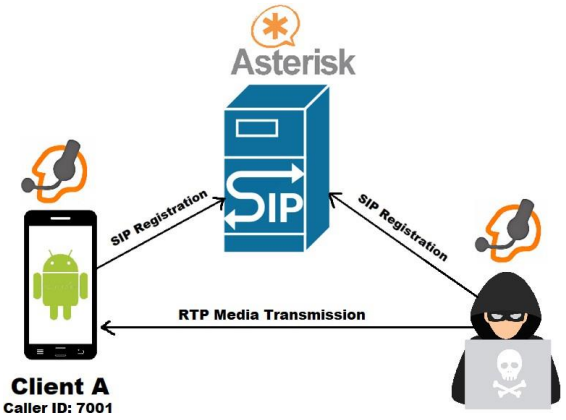

Figure 15 Caller ID spoofing

5) Spam over Internet Telephony (SPIT): SPIT involves the delivery of unsolicited and automated voice messages or silent calls, often with the intention of causing annoyance or facilitating fraudulent activities. Some may even combinethe techniques of caller ID spoofing and SPIT to send multiple calls using a spoofed caller ID to bypass certain security mechanisms and make it appear as if the call is coming from a legitimate source. This works because Asterisk by default allows guest calls which does not require any username and password to make calls. Hence, anyone can send calls to the clients within Asterisk, causing disturbance to the targeted client. Certain tools or scripts will be utilized to generate automated calls to the targeted victim continuously.

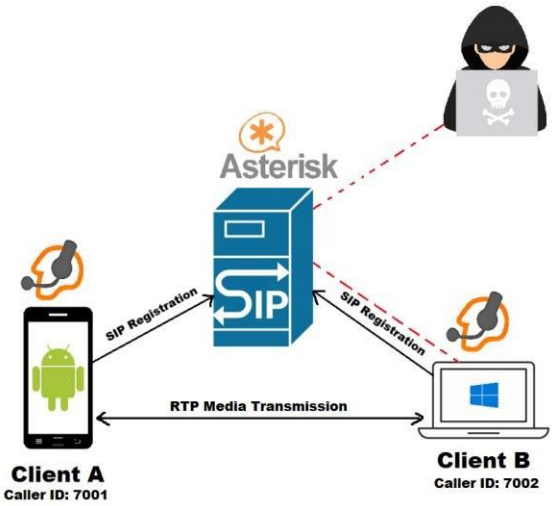

Figure 16 Spam over Internet Telephony (SPIT)

6) Expected Results

TABLE II

EXPECTED RESULTS

Attack Scenarios	Expected Results
Call eavesdropping	Able to monitor and analyze VoIP traffic in a conversation.
Man-in-the-Middle (MitM) attack	Able to eavesdrop and potentially tamper with the call flow.
Denial of Service (DoS) attack	Asterisk will have a high resource consumption and calls will not be processed.
Caller ID spoofing	Able to impersonate a targeted client and call other clients.
Spam over Internet Telephony (SPIT)	The client will receive multiple calls from an unknown caller.

7) Prerequisites: Some assumptions have been made when simulating attacks on the VoIP system:

- Assumption 1: The VoIP network is a LAN network (192.168.1.X/24).
- Assumption 2: The attacker is on the same network.
- Assumption 3: The traffic sent through the network is not encrypted due to the nature of the protocols.
- Assumption 4: The clients are password protected and registered to Asterisk.

C. Proposed Security Model

1) Design and Implementation: A security model will also be proposed and implemented within Asterisk to effectively mitigate spam callers. Essentially, the aim is to prevent robocalls and blacklisted human callers from spam calling a client. The model's design, shown in Figure 17, incorporates various methods and modules, including a blacklist in MySQL, Asterisk Gateway Interface (AGI) script, and Interactive Voice Response (IVR) system integrated within Asterisk. Additionally, the IVR system will utilize a new extension to route incoming guest calls instead of relying on a wildcard extension approach from the dialplan. External callers must now dial extension 7000 to forward a call to any of the clients instead of directly dialing the client's extension.

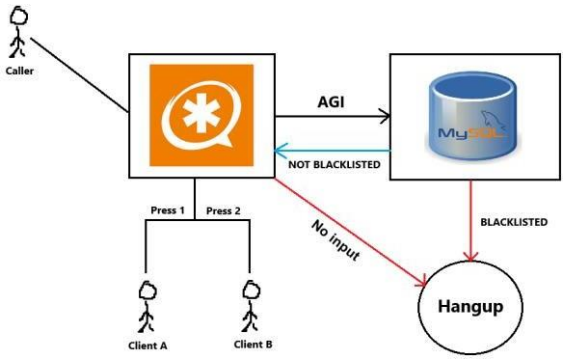

Figure 17 Security model design

As shown in the flowchart (Figure 18), the AGI script will verify if a caller is blacklisted or not by checking their caller ID in the blacklist table within a MySQL database afterdialing the extension. If present, the AGI script will label them as blacklisted, and this label will inform the dialplan to hangup their call immediately before reaching the clients. If not present in the blacklist, the caller will be passed back to the dialplan and must go through the IVR system which prompts the caller to input the last digit of the client extension they wish to call using their dialpad with an automated audio message. Example, if number 1 was pressed, a call will be forwarded to Client A (7001).

Additionally, exception handling was also implemented in the IVR system to handle invalid inputs or a timeout. If the caller enters a non-existent extension, the system will play an invalid audio message and allow them to input again. For callers who were timed out for not inputting anything in 5 seconds, an invalid audio message will be played, and the call will be hung up. Hence, even if the spam calls were spoofed numbers, the IVR system will help authenticate the caller and verify if they are actually human or not.

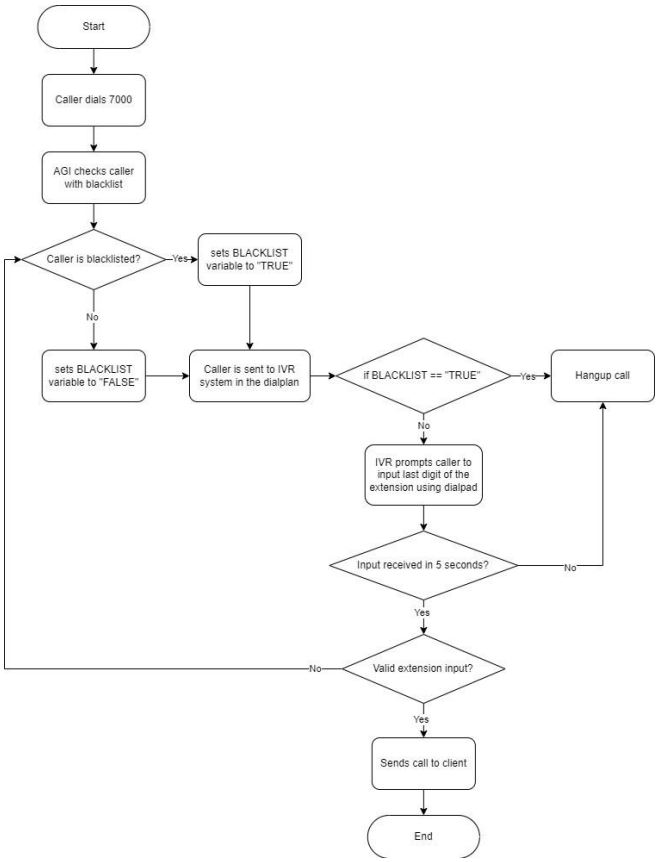

Figure 18 Security model flowchart

In summary, we identified the common attacks that were present in VoIP and planned to simulate them according to the diagrams to show readers how each of them can easily compromise the CIA triad of the victim(s). Additionally, we also drafted a simple security model within Asterisk PBX that can block spam callers according to their caller ID as an act of contribution to the field of VoIP security.

IV. RESULTS

A. Attack Simulation

TABLE III

ATTACK SIMULATION RESULTS

Attack Scenarios	**Confidentiality**	**Integrity**	**Availability**	**Countermeasures**
Call eavesdropping	✓			1) Encryption mechanisms (SIP-TLS, SRTP) 2) VPN
Man-in-the-Middle (MitM) attack	✓	✓	✓	1) Encryption mechanisms (SIP-TLS, SRTP) 2) VPN
Denial of Service (DoS) attack			✓	1) Firewalls 2) Intrusion Prevention Systems
Caller ID spoofing		✓		1) Caller authentication
Spam over Internet Telephony (SPIT)		✓	✓	1) Blacklist and Whitelist 2) Turing tests 3) Rate limiting

B. Security Model

	Attempt 1	Attempt 2	Attempt 3	Attempt 4	Attempt 5	Attempt 6	Attempt 7	Attempt 8	Attempt 9	Attempt 10
Automated spam calls (blacklisted)	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup
Automated spam calls (non-blacklisted)	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup
Manual spam calls (blacklisted)	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup	Hangup
Manual spam calls (non-blacklisted)	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing
Legitimate calls	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing	Ringing

Figure 18 Testing the security model with different methods.

TABLE IV

SECURITY MODEL RESULTS

Scenarios	**Results**
Automated spam calls (blacklisted)	Prevented by blacklist
Automated spam calls (non-blacklisted)	Prevented by IVR
Manual spam calls (blacklisted)	Prevented by blacklist
Manual spam calls (non-blacklisted)	Allowed
Legitimate calls	Allowed

The attack simulation has demonstrated different VoIP attacks that can compromise the key concepts in cybersecurity, specifically the CIA (Confidentiality, Integrity, and Availability) triad. Following rigorous testing within a controlled environment, a range of countermeasureshas been suggested to enhance the security of VoIP systems

against these attacks. Among the threats and attacks, MiTM attacks stand out as particularly dangerous, given their potential to facilitate a range of other malicious activities such as eavesdropping and call tampering. Additionally, notice how caller ID spoofing emerges as a challenge with comparatively fewer countermeasures. This is because caller ID spoofing involves the human element in security, where attackers exploit human errors to compromise a VoIP system.Other than that, it is evident that VoIP threats and attacks demand serious attention from individuals and organizations alike. The dynamic nature of these security challenges underscores the importance of ongoing awareness, proactive measures, and the continuous enhancement of security protocols to effectively mitigate risks in the realm of VoIP technology.

Turning to the security model's performance, the results from extensive testing involving spam calls were presented. It is evident that the security model was successful in mitigating automated spam calls, both blacklisted and non-blacklisted. The results also indicate that it effectively mitigated manual spam calls that were previously blacklisted, thanks to the integration of the AGI script. However, the security model still has its caveats where it is vulnerable to manual spam calls that were not part of the blacklist. Attackers are still able to manually send spam calls to a client, albeit only if they input a valid extension for the IVR system. Similarly with legitimate calls, they both can bypass the AGI script and the IVR system due to their non- automated nature and by being non-blacklisted. Nonetheless, the primary objective of this project has been to address automated spam calls, including silent calls and telemarketers. While this approach effectively mitigates automated spam, it is important to acknowledge that manual spam calls initiated by a human attacker could still pose a challenge for the clients. Thus, the security model will be enhanced to ensure robust mitigation of even non-blacklisted spam callers and fortifying the overall security framework. Overall, the security model seems to successfully achieve the project objectives where it mitigated automated spam calls generated by malicious adversaries.

V. Conclusion

In conclusion, this project has presented a comprehensive analysis of the security concerns associated with VoIP and undertook a series of attack simulations on a self-hostedVoIP network. The simulations were instrumental in shedding light on the potential impacts that affect the core security concepts in the context of VoIP. Furthermore, the proposed security model not only mitigated automated spam calls efficiently, but also provided better call routing forlegitimate callers. In the broader context of cybersecurity, the insights and solutions presented in this paper can be invaluable for organizations and individuals looking to secure their VoIP systems against the ever-evolving realm ofcyber threats. As the world continues to rely on VoIP for communication, safeguarding these networks becomes paramount, and this research contributes to the ongoing efforts to ensure the resilience and security of VoIP in an increasingly digital age.

In the future, additional security features may be considered for implementation to further bolster the security model such as a reputation system and machine learning approaches. These additional layers of security would enhance the security model's ability to combat manual spam callers, providing a more comprehensive defense against a broader spectrum of threats in VoIP.

References

[1] A. F. Gad, “Comparison of Signaling and Media Approaches toDetect VoIP SPIT Attack,” 2018 International Conference on Innovative Trends in Computer Engineering (ITCE), 2018. doi:10.1109/itce.2018.8316600

[2] W. Nazih, W. S. Elkilani, H. Dhahri, and T. Abdelkader, “Survey of Countering DoS/DDoS Attacks on SIP Based VoIP Networks,” Electronics, vol. 9, no. 11, p. 1827, 2020. doi:10.3390/electronics9111827

[3] B. Kurt, Ç. Yıldız, T. Y. Ceritli, B. Sankur, and A. T. Cemgil, “A Bayesian change point model for detecting SIP-based DDoS attacks,” Digital Signal Processing, vol. 77, pp. 48–62, 2018. doi:10.1016/j.dsp.2017.10.009

[4] W. Nazih, K. Alnowaiser, E. Eldesouky, and O. Youssef Atallah, “Detecting SPIT Attacks in VoIP Networks Using Convolutional Autoencoders: A Deep Learning Approach,” Applied Sciences, vol. 13, no. 12, p. 6974, 2023. doi:10.3390/app13126974

[5] “Cisco annual internet Report - Cisco Annual Internet Report (2018–2023) White Paper,” Cisco, https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual- internet-report/white-paper-c11-741490.html (accessed Jul. 19, 2023).

[6] D. Suthar and P. H. Rughani, “A Comprehensive Study of VoIP Security,” 2020 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), 2020. doi:10.1109/icacccn51052.2020.9362943

[7] Webex, “What is VoIP?,” Webex, https://www.webex.com/what-is-voip.html (accessed Jul. 19, 2023).

[8] Person, “What are the advantages of VoIP?,” Vonage, https://www.vonage.com/resources/articles/what-are-advantages-of-voip/ (accessed Jul. 19, 2023).

[9] M. Kara, H. R. J. Merzeh, M. A. Aydın, and H. H. Balık, “VoIPChain: A decentralized identity authentication in Voice over IP using Blockchain,” Computer Communications, vol. 198, pp. 247– 261, 2023. doi:10.1016/j.comcom.2022.11.019

[10] R. Safoine, S. Mounir, and A. Farchi, “Comparative study on DOS attacks Detection Techniques in SIP-based VOIP networks,” 2018 6th International Conference on Multimedia Computing and Systems (ICMCS), 2018. doi:10.1109/icmcs.2018.8525878

[11] H. Mustafa, W. Xu, A.-R. Sadeghi, and S. Schulz, “End-to-End Detection of Caller ID Spoofing Attacks,” IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 3, pp. 423–436, 2018. doi:10.1109/tdsc.2016.2580509

[12] T. Surasak and S. C.-H. Huang, “Enhancing VoIP Security and Efficiency using VPN,” 2019 International Conference onComputing, Networking and Communications (ICNC), 2019. doi:10.1109/iccnc.2019.8685553

[13] B. B. Gupta and V. Prajapati, “Secure and efficient Session Initiation Protocol authentication scheme for VoIP Communications,” 2019 International Conference on Communication and Electronics Systems (ICCES), 2019. doi:10.1109/icces45898.2019.9002125

[14] N. Mcinnes, E.J. Zaluska, and G Wills, “Analysis of threats on a VoIP Based PBX Honeypot,” 2018. doi:10.2053/ICITST.WorldCIS.WCST.WCICSS.2018.0015

[15] V. Ganesan and M. msk, “A scalable detection and prevention scheme for voice over internet protocol (VoIP) signaling attacksusing handler with Bloom filter,” International Journal of Network Management, vol. 28, no. 2, 2018. doi:10.1002/nem.1995

[16] I. M. Tas, B. G. Unsalver, and S. Baktir, “A Novel SIP Based Distributed Reflection Denial- of-Service Attack and an Effective Defense Mechanism,” IEEE Access, vol. 8, pp. 112574– 112584, 2020. doi:10.1109/access.2020.3001688

[17] Z. Tsiatsikas, G. Kambourakis, D. Geneiatakis, and H. Wang, “The Devil is in the Detail: SDP-Driven Malformed Message Attacks and Mitigation in SIP Ecosystems,” IEEE Access, vol. 7, pp. 2401–2417, 2019. doi:10.1109/access.2018.2886356

[18] L. Sjöström, “Detecting SQL Injection Attacks in VoIP using Real-time Deep Packet Inspection,” Dissertation, 2019.

[19] M. Kara, M. Ali Aydın, and H. Hüseyin Balık, “Bcvop2p: Decentralized Blockchain-Based Authentication Scheme for Secure Voice Communication,” Intelligent Automation & Soft Computing, vol. 31, no. 3, pp. 1901–1918, 2022. doi:10.32604/iasc.2022.021309

[20] M. Semerci, A. T. Cemgil, and B. Sankur, “An intelligent cyber security system against DDoS attacks in SIP networks,” Computer Networks, vol. 136, pp. 137–154, 2018. doi:10.1016/j.comnet.2018.02.025

[21] H. H. Kilinc and O. F. Acar, “Analysis of attack and attackers on VoIP Honeypot environment,” 2018 26th Signal Processing and Communications Applications Conference (SIU), 2018. doi:10.1109/siu.2018.8404331

[22] W. Nazih, Y. Hifny, W. S. Elkilani, H. Dhahri, and T. Abdelkader, “Countering DDoS Attacks in SIP Based VoIP Networks Using Recurrent Neural Networks,” Sensors, vol. 20, no. 20, p. 5875, 2020. doi:10.3390/s20205875

[23] M. Hosseinpour, M. H. Yaghmaee, S. A. Hosseini Seno, H. Khosravi Roshkhari, and M. Asadi, “Anomaly‐based DoS detection and prevention in SIP networks by modeling SIP normal traffic,” International Journal of Communication Systems, vol. 31, no. 18, 2018. doi:10.1002/dac.3825

[24] W. Nazih, Y. Hifny, W. S. Elkilani, and T. Mostafa, “Fast Detection of Distributed Denial of Service Attacks in VoIP Networks Using Convolutional Neural Networks,” International Journal of Intelligent Computing and Information Sciences, vol. 20, no. 2, pp. 125–138, 2020. doi:10.21608/ijicis.2021.51555.1046

[25] P. Biondi, S. Bognanni, and G. Bella, “VoIP Can Still Be Exploited — Badly,” 2020 Fifth International Conference on Fog and Mobile Edge Computing (FMEC), 2020. doi:10.1109/fmec49853.2020.9144875

[26] R. R. Nuiaa, S. Manickam, and A. H. Alsaeedi, “Distributed reflection denial of service attack: A critical review,” International Journal of Electrical and Computer Engineering (IJECE), vol. 11, no.6, p. 5327, 2021. doi:10.11591/ijece.v11i6.pp5327-5341

[27] M. Azrour, Y. Farhaoui, M. Ouanan, and A. Guezzaz, “SPIT Detection in Telephony over IP Using K-Means Algorithm,” Procedia Computer Science, vol. 148, pp. 542–551, 2019. doi:10.1016/j.procs.2019.01.027

[28] I. T. Javed, K. Toumi, F. Alharbi, T. Margaria, and N. Crespi, “Detecting Nuisance Calls over Internet Telephony Using Caller Reputation,” Electronics, vol. 10, no. 3, p. 353, 2021. doi:10.3390/electronics10030353

[29] N. Sukma and R. Chokngamwong, “Increasing the efficiency of One-time key Issuing for The First Verification Caller ID Spoofing Attacks,” 2018 15th International Joint Conference on Computer Science and Software Engineering (JCSSE), 2018. doi:10.1109/jcsse.2018.8457341

[30] J. Kafke and T. Viana, “Call Me Maybe: Using Dynamic Protocol Switching to Mitigate Denial-of-Service Attacks on VoIP Systems,” Network, vol. 2, no. 4, pp. 545–567, 2022. doi:10.3390/network2040032

[31] A. Febro, H. Xiao, and J. Spring, “Telephony Denial of Service Defense at Data Plane (TDoSD@DP),” NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium, 2018. doi:10.1109/noms.2018.8406281

[32] W. Nazih, Y. Hifny, W. Elkilani, T. Abdelkader, and H. Faheem, “Efficient Detection of Attacks in SIP Based VoIP Networks using Linear l1-SVM Classifier,” International Journal of Computers Communications & Control, vol. 14, no. 4, pp. 518–529, 2019. doi:10.15837/ijccc.2019.4.3563

[33] S. Armoogum and N. Mohamudally, “Closest Adjacent Neighbour: A Novel Deep Learning Intruder Detection Technique in VoIP Networks,” Proceedings of the 2nd International Conferenceon Intelligent and Innovative Computing Applications, 2020. doi:10.1145/3415088.3415129

[34] L. Behan, J. Rozhon, J. Safarik, F. Rezac, and M. Voznak, “Efficient Detection of Spam Over Internet Telephony by Machine Learning Algorithms,” IEEE Access, vol. 10, pp. 133412– 133426, 2022. doi:10.1109/access.2022.3231384

[35] M. Swarnkar and N. Hubballi, “SpamDetector: Detecting spam callers in Voice over Internet Protocol with graph anomalies,” Security and Privacy, vol. 2, no. 1, 2018. doi:10.1002/spy2.54

[36] M. A. Azad and R. Morla, “Rapid detection of spammers through collaborative information sharing across multiple service providers,” Future Generation Computer Systems, vol. 95, pp. 841–854, 2019. doi:10.1016/j.future.2017.12.026

[37] G. Vennila, M. S. K. Manikandan, and M. N. Suresh, “Dynamic voice spammers detection using Hidden Markov model for voice over internet protocol network,” Computers & Security, vol. 73, pp. 1–16, 2018. doi:10.1016/j.cose.2017.10.003

[38] M. Abubakar, Z. Jaroucheh, A. Al Dubai, and B. Buchanan, “Blockchain-Based Authentication and Registration Mechanism for SIP-Based VoIP Systems,” 2021 5th Cyber Security in Networking Conference (CSNet), 2021. doi:10.1109/csnet52717.2021.9614646

[39] D. Hou, H. Han, and E. Novak, “TAES: Two-factor Authentication with End-to-End Security against VoIP Phishing,” 2020 IEEE/ACM Symposium on Edge Computing (SEC), 2020. doi:10.1109/sec50012.2020.00049