T.C.

BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF EDUCATION

COMPUTER ENGINEERING HEAD OF THE DEPARTMENT

BLOCKCHAIN-BASED CALLER-ID AUTHENTICATION (BBCA): A NOVEL SOLUTION TO PREVENT SPOOFING ATTACKS IN VOIP/SIP NETWORKS WITH AN ANALYSIS OF SPOOFING ATTACK ANATOMY AND TEST RESULTS

Ph.D. THESIS

İSMAİL MELİH TAŞ

ISTANBUL 2023

T.C.

BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF EDUCATION

COMPUTER ENGINEERING HEAD OF THE DEPARTMENT

BLOCKCHAIN-BASED CALLER-ID AUTHENTICATION (BBCA): A NOVEL SOLUTION TO PREVENT SPOOFING ATTACKS IN VOIP/SIP NETWORKS WITH AN ANALYSIS OF SPOOFING ATTACK ANATOMY AND TEST RESULTS

Ph.D. THESIS

THESIS ADVISOR

Assist. Prof. Selçuk BAKTIR

ISTANBUL 2023

T.C.
BAHCESEHIR UNIVERSITY
GRADUATE SCHOOL

PhD THESIS APPROVAL FORM

Name Surname	İSMAİL MELİH TAŞ
Student Number	1406197
Program Name	COMPUTER ENGINERING (ENGLISH, PHD)
Title of Thesis	BLOCKCHAIN-BASED CALLER-ID AUTHENTICATION (BBCA): A NOVEL SOLUTION TO PREVENT SPOOFING ATTACKS IN VOIP/SIP NETWORKS WITH AN ANALYSIS OF SPOOFING ATTACK ANATOMY AND TEST RESULTS
Thesis Defense Date	

It has been approved by the Graduate School that this thesis has fulfilled the necessary conditions as a PhD thesis.

Prof. Dr. Fatma ÖZKUL

Director of Graduate School

This Thesis has been read by us, it has been deemed sufficient and accepted as a PhD thesis in terms of quality and content.

PhD Thesis Defense Jury		
Thesis Defense Jury	**Title - Name / Surname**	**Signature**
Thesis Advisor	Assist. Prof. Selçuk Baktır	
Member of Thesis Monitoring Committee	Assist. Prof. Tarkan Aydın	
Member of Thesis Monitoring Committee	Prof. Dr. Ali Gökhan Yavuz	
Member	Assist. Prof. Ece Gelal Soyak	
Member	Doç. Dr. Murat Aydos	

All the information in this thesis is obtained and presented in accordance with academic rules and ethical principles; I further declare that I have made all attributions not originating from this work as required by these rules and principles.

Name, Surname : İsmail Melih TAŞ

Signature :

ABSTRACT

BLOCKCHAIN-BASED CALLER-ID AUTHENTICATION (BBCA): A NOVEL SOLUTION TO PREVENT SPOOFING ATACKS IN VOIP/SIP NETWORKS WITH AN ANALYSIS OF SPOOFING ATTACK ANATOMY AND TEST RESULTS

TAŞ, İsmail Melih
Computer Engineering Ph.D. Program
Thessis Advisor Assist Prof. Selçuk BAKTIR

JULY 2023, 54 Pages

Voice over Internet Protocol (VoIP) networks face an increasing threat from caller-ID spoofing attacks, which jeopardize the security and privacy of telephone systems. Despite the implementation of various measures, these attacks persist, often bolstered by social engineering techniques. This research presents an analysis of caller-ID spoofing attacks conducted in a live financial call center, highlighting the associated risks and consequences. Through our experiments, we demonstrate the high feasibility of terminating calls across different networks by initiating spoofed calls supported by social engineering tactics. Our findings indicate success rates of 84% and 76% for scenarios involving telephone banking password changes and a separate test scenario, respectively, when spoofing calls to appear as though originating from valid customer or call center numbers. Remarkably, only one out of five terminating service providers effectively detected and prevented spoofing. To tackle this issue, we propose a caller-ID authentication solution based on blockchain technology. This approach utilizes a low-latency consensus algorithm to verify caller-ID information provided by ISPs and institutions, renewing ISP registration with each change in caller-ID. Consequently, it alleviates challenges associated with roaming, IP-PBX, or VPN usage. Furthermore,

we discuss the feasibility of implementing our solution, potential challenges in deployment, and future research directions. Our approach significantly enhances telecom security and offers a scalable countermeasure against caller-ID spoofing attacks.

Key Words: Caller-ID Spoofing, Session Initiation Protocol, Voice over IP, Blockchain, Authentication

ÖZET

BLOK ZİNCİRİ TABANLI ARAYAN KİMLİĞİ DOĞRULAMASI (BBCA): ARAYAN KİMLİĞİ SAHTEKARLIĞI SALDIRISI ANATOMİSİ VE TEST SONUÇLARININ ANALİZE İLE VOIP/SIP AĞLARINDA KİMLİK SAHTEKARLIĞI SALDIRILARINI ÖNLEMEK İÇİN YENİ BİR ÇÖZÜM

TAŞ, İsmail Melih
Bilgisayar Mühendisliği Doktora Programı
Tez Danışmanı Dr. Öğr. Üyesi Selçuk BAKTIR

TEMMUZ 2023, 54 Sayfa

Internet Protokolü Üzerinden Ses (VoIP) ağları, giderek artan bir şekilde arayan kimlik sahtekarlığı saldırılarına maruz kalmaktadır. Bu durum, telefon sistemlerinin güvenlik ve gizlilik açısından tehdit altında olduğunu göstermektedir. Mevcut önlemlere rağmen, bu saldırılar genellikle sosyal mühendislik teknikleriyle desteklenerek gerçekleştirilmektedir. Bu çalışma, bir finansal çağrı merkezinde gerçekleştirilen arayan kimlik sahtekarlığı saldırılarının analizini sunmaktadır ve bu saldırıların risklerini ve sonuçlarını vurgulamaktadır. Gerçekleştirdiğimiz deneyler, sosyal mühendislik taktikleri kullanılarak sahte bir çağrı başlatarak, çeşitli ağlardan çağrı sonlandırmanın oldukça uygulanabilir olduğunu göstermektedir. Elde ettiğimiz sonuçlar, sahtekarlıkla gerçekleştirilen çağrılar için telefon bankacılığı şifre değişikliği senaryoları ve diğer bir test senaryosu için sırasıyla %84 ve %76 başarı oranlarını ortaya koymaktadır. İlginç bir şekilde, beş çağrı sonlandırma hizmet sağlayıcısından sadece biri etkili bir şekilde sahtekarlığı tespit edebilmekte ve önleyebilmektedir. Bu sorunu çözmek için, blockchain tabanlı bir arayan-ID doğrulama çözümü önermekteyiz. Bu yaklaşım, arayan-ID bilgisinin ISP'ler ve kurumlar tarafından doğrulanması için düşük gecikme süresine sahip bir konsensüs algoritması kullanır ve her arayan-ID değişikliğinde ISP kaydını yeniler. Bu yaklaşım, arayan kimlik

bilgisinin İnternet Hizmet Sağlayıcıları (ISP) ve kurumlar tarafından doğrulanması için düşük gecikme süresine sahip bir konsensüs algoritması kullanır ve her arayan kimlik değişikliğinde ISP kaydını günceller. Bu yaklaşım, dolaşım, IP-PBX veya VPN kullanımı gibi sorunları hafifletir. Çözümün uygulanabilirliği, potansiyel dağıtım zorlukları ve gelecekteki araştırma yönleri de tartışılmaktadır. Bu yaklaşım, telekomünikasyon güvenliğini artırmakta ve arayan kimlik sahtekarlığı saldırılarına karşı ölçeklenebilir bir önlem sunmaktadır.

Anahtar Kelimeler: Arayan Numara Sahtekârlığı, Oturum Başlatma Protokolü, IP Üzerinden Ses İletimi, Blok Zinciri, Kimlik Doğrulama,

For my parents who always believe me and support me whatever I do.

ACKNOWLEDGEMENTS

I would like to thank my advisor Selçuk Baktır, who always motivates and encourages me to do better during my doctoral work. Selçuk Baktır gave me the freedom to do whatever I wanted while continuing to contribute valuable feedback, advice, and encouragement. In addition to our academic collaboration, I greatly value the close personal rapport that Selcuk Baktır has.

I am grateful to my brother Hüseyin Taş, for whom I always asked for support and who spent sleepless nights with me. I would like to thank my partner Neslişah Topçu, who was always with me and gave me strength and happiness in difficult times, and my mother, father, and sister, whose support I have always felt, albeit from afar.

TABLE OF CONTENTS

LIST OF TABLES

TABLES

LIST OF FIGURES

FIGURES

LISTS OF ABBREVATIONS

BBCA	Blockchain-based Caller-ID Authentication
VoIP	Voice over Internet Telephony
Caller-ID	Caller Identifier
ISP	Internet Service Provider
IP-PBX	Internet Protocol Private Branch Exchange
VPN	Virtual Private Networks
CLI	Calling Line Identity
CPN	Calling Party Number
ANI	Automatic Number Identification
DNIS	Dialed Number Identification Service
SMS	Short Message Service
TDoS	Telephony Denial of Service
FCC	Federal Communications Commission)
FTC	Federal Trade Commission
US	United States
UK	United Kingdom
ATO	Account Takeover
DTMF	Dual Tone Multiple Frequency
2FA	2 Factor Authentication
RFC	Request for Comment
PBFT	Practical Byzantine Fault Tolerance
IRSF	International Revenue Share Fraud
VoWiFi	Voice over Wi-Fi
4G	Fourth Generation
IMS	IP Multimedia Subsystem
ISDN	Integrated Services Digital Network
SS7	Signaling System No: 7
PSTN	Public Switched Telephone Network
DNO	Do Not Originate
KBA	Knowledge-Based Authentication
SIP	Session Initiation Protocol

PAI	P-Asserted-Identity
SDP	Session Description Protocol
SBC	Session Border Controller
B2BUA	Back-to-Back-User Agent
STIR	Secure Telephony Identity Revisited
SHAKEN	Signature-based Handling of Asserted Information Using Tokens
IETF	Internet Engineering Task Force
ATIS	Automatic Terminal Information Service
NPAC	Number Portability Administration Center
URI	Universal Resource Identifiers
SIP-PBX	Session Initiation Protocol-Private Branch Exchange
SIP-SIM	SIP Signaling Manipulator
LAN	Local Area Network
WAN	Wide Area Network
OTP	One Time Password
LCR	Least Cost Routing
GSM	Global System for Mobile Communication
QoS	Quality of Service
DID	Direct Inward Dialing

Chapter 1

Introduction

In an era where telecommunications have been revolutionized by technological progress, facilitating global connectivity and transcending geographical limitations, unique security challenges have emerged. One of these challenges is Caller-ID (caller-identifier) spoofing, which has become a critical concern in the telecommunications sector (Sechulzrinne, Panagia, Cox, & Balasubramaniyan, 2012). This practice involves manipulating the caller-ID information displayed on the recipient's device, enabling a range of malicious activities from fraud to identity theft (Pandit, Liu, Perdisci, & Ahamad, 2021). Despite the pressing need for robust countermeasures, caller-ID spoofing remains a substantial threat, exposing the shortcomings of current prevention and detection strategies (Communications Fraud Control Association, 2019).

The realm of caller-ID spoofing is characterized by complexity, largely due to inherent vulnerabilities within the Session Initiation Protocol (SIP) signaling, which can be exploited to execute successful attacks. These complexities and vulnerabilities are especially pronounced in real-world scenarios, such as within financial call centers, where caller-ID serves as a form of authentication. In this study, we delve into the depths of these complexities, offering a unique perspective that unearths previously overlooked aspects of caller-ID spoofing. Our aim is to emphasize the urgent need for comprehensive and effective solutions.

In an attempt to address this issue, our research also focuses on exploring the constraints of current solutions and proposing a novel approach. This involves a detailed investigation of the factors that contribute to the rise in caller-ID spoofing incidents and a thorough analysis of the difficulties associated with detecting and preventing these attacks.

The use of a low-latency blockchain-based consensus algorithm to manage and verify end-to-end caller-ID information, as proposed in this study, presents a pioneering and promising approach to addressing the issue of caller-ID spoofing. We further detail the design and implementation of our proposed solution, as well as its

evaluation against existing methods in the literature, standards, and practice in the subsequent sections.

1.1 Main Contributions of This Study

In this study, our main focus is addressing the persistent problem of caller-ID spoofing, which has been a significant headache for the telecom and banking sectors worldwide. Despite numerous efforts to tackle this problem, there is currently no universally accepted prevention mechanism. VoIP and its underlying SIP make it possible to implement caller-ID spoofing and also make it very difficult to prevent it (Tas & Kucuk, DEF CON 28 Main Stage, 2020). Existing solutions are primarily closed-loop solutions that are only applicable under the same service provider, unsuitable for real-world applications.

We make the following significant contributions in this work:

- For the first time in the literature, we introduce a blockchain-based caller-ID registration and call flow control mechanism that is deployed in the cloud. Our mechanism effectively combats caller-ID fraud attacks in real-time by managing and verifying the caller-ID information of ISPs and institutions end-to-end. Our solution verifies the caller-ID and ANI information at the initiation of a call, upon receipt, from which ISP it is coming, and during any hop changes.

- We offer a detailed technical dissection of current defensive strategies against caller-ID spoofing, juxtaposing them against our solution, thereby underlining the merits of our approach. We posit that our method could potentially enrich ongoing RFC (Request for Comments) efforts or catalyze a novel RFC on caller-ID spoofing mitigation.

- We advocate for a modified version of the Practical Byzantine Fault Tolerance (PBFT) algorithm as the cornerstone consensus algorithm within our solution (Ferrag & Maglaras, 2020) (Yang, Jia, Su, Wu, & Qin, 2022) (Wang, et al., 2019) (Cai, 2020) (Vishwakarma, Nahar, & Das, 2022) (Meshcheryakov, Melman, Evsutin, Morozov, & Koucheryavy, 2021) (Saha, et al., 2021). This modification promotes low latency and real-time performance, employing a swift two-phase commit protocol with "verifiers" selected for their reputation and past performance to ensure rapid consensus

on caller-ID validity.

- We provide a comprehensive discussion on the feasibility and potential deployment challenges of our proposed solution, including its integration into existing RFC efforts and the necessary regulations for service providers to demonstrate compliance.
- We expand the field of caller-ID spoofing through a thorough technical analysis of end-to-end caller-ID spoofing attacks, facilitated by social engineering tactics. Our study stands unique in its focus on SIP signaling vulnerabilities and the thorough examination of these vulnerabilities' exploitation in a live financial call center setting where caller-ID is used as authentication.
- Our experiments conducted in a live financial call center setting offer tangible evidence of the feasibility of caller-ID spoofing attacks. They revealed an 84% success rate in the first scenario of a call made for a telephone banking password change and a 76% success rate in the second scenario. Our findings also demonstrated that only one out of the five different terminating service providers was able to detect and prevent caller-ID spoofing effectively.
- Our findings offer new insights into the inherent risks and impacts of caller-ID spoofing, laying a firm foundation for future research. This study highlights the urgent need for effective mitigation strategies and can inform the development of more secure telecommunication systems.
- We explore potential future research directions, handling complex call scenarios such as call forwarding and teleconferencing calls. Our approach enhances telecommunication systems' security, provides an efficient and scalable solution to prevent caller-ID spoofing attacks capable of managing complex scenarios, and discusses the potential challenges and considerations for large-scale deployment and integration into existing systems and regulations.

In summary, our proposed blockchain-based caller-ID authentication (BBCA) scheme offers a groundbreaking and potent approach to addressing the caller-ID spoofing problem in the telecommunication industry.

Chapter 2

Background

2.1 Defining Caller-ID Spoofing: A Technical Overview

Caller ID, also known as Calling Line Identification (CLI), is a service that allows the call recipient to view the caller's phone number, also known as the Calling Party Number (CPN). Automatic Number Identification (ANI) is a legacy feature that functions similarly to Caller-ID but displays the billing number instead of the caller's name. Other information that can be supplied includes Dialed Number Identification Service (DNIS) (Suthar & Rughani, 2020).

Caller-ID spoofing refers to the deliberate alteration of Caller-ID information and ANI in an inbound call. This is an attack technique that allows the caller to hide or falsify their true identity by presenting a different phone number to the call recipient. The Caller-ID spoofing technique can be used to make incoming and outgoing calls, as well as SMS (Short Message Service) messages, which appear to come from any chosen phone number (Sechulzrinne, Panagia, Cox, & Balasubramaniyan, 2012).

Caller-ID spoofing poses a significant threat to telecommunications security, as it makes voice search-based assaults more difficult to detect. The majority of calls that use Caller-ID spoofing are malicious in nature, and the technique can be used for a variety of illegal activities such as fraud and identity theft. Additionally, while Caller-ID spoofing can be used for legitimate and beneficial purposes, it has contributed to an increase in robocalls and phone scam issues in recent years (Pandit, Liu, Perdisci, & Ahamad, 2021).

There are two primary forms of caller-ID spoofing: impersonation and anonymization. Impersonation is accomplished by spoofing a specific target number and can be used for tactics such as voice phishing, validation of stolen credit cards, retrieving voicemail messages, swatting (making a false emergency call to send a SWAT team to a target's location), and disconnecting utilities. Anonymization, on the other hand, is a form of spoofing that employs the use of a random number and can be used to combat robocalls, intercarrier compensation fraud, and Telephony Denial of Service (TDoS) attacks (Dantu & Kolan, 2005).

The impact of caller-ID spoofing attacks is not only limited to the immediate effects but also extends to the long-term financial and personal consequences for victims. Various studies indicate that over $450 million is lost annually due to phone scams that leverage caller-ID spoofing (Communications Fraud Control Association, 2019). In (Communications Fraud Control Association, 2019) the authors claim that the true impact of these attacks may be significantly higher, as the reported figure only accounts for individuals who have experienced incidents or financial devastation as a result of personal identity theft occurring months after the initial phone scam. This underscores the critical need for developing effective countermeasures against caller-ID spoofing attacks to mitigate their consequences on individuals and industries.

In summary, Caller-ID spoofing is a malicious technique that allows attackers to alter the Caller-ID information displayed to a call recipient in order to hide or falsify their true identity. It can be used for a variety of illegitimate activities and has become a major concern for the telecom and banking industries. To effectively combat Caller-ID spoofing, the issue must be addressed at its source and countermeasures must be developed to detect and prevent these types of attacks.

2.2 Legitimate Uses of Caller-ID Spoofing

While Caller-ID spoofing is often associated with malicious intent, it can also be used for legitimate and beneficial purposes. One example of this is when a doctor makes a call from their personal cell phone, but the caller-ID displays the office number instead. This allows the doctor to easily make calls while on the go, while still maintaining a professional appearance. Similarly, outsourced call centers for companies such as airlines can use Caller-ID spoofing to display the company's main phone number, rather than the number of the specific call center. Additionally, Caller-ID spoofing can also be used in VoIP services when an individual has multiple devices and wants to present a single call-back number to contacts. These examples highlight the potential benefits of Caller-ID spoofing, and it is important to consider both the positive and negative implications of this technology (Dantu & Kolan, 2005).

2.3 The Truth in Calling Act and Efforts to Combat Caller-ID Spoofing

The Federal Communications Commission (FCC) has enacted the “Truth in Calling Act”, which makes it illegal for any person or organization to transmit misleading or incorrect caller-ID information, whether for fraudulent and harmful

purposes or accidentally (Spoofing, 2020). Penalties for breaking this law include fines of up to \$10,000 per spoofed phone call or SMS offense. In June 2020, the FCC imposed a record $225 million in penalties for a large fraudulent robocall campaign selling health insurance (FCC Proposes Record, 2020).

Despite legal efforts, the problem of caller-ID spoofing remains prevalent. The Federal Trade Commission (FTC) aims to prevent the exploitation of caller-ID spoofing services by spammers and fraudsters. Criminals who make spoofed phone calls are aware that they are breaking the law, but the low risk of getting caught often outweighs the potential consequences (How to Stop Unwanted Calls, 2020).

To combat caller-ID spoofing, the FTC recommends utilizing call blocker software that allows for a preview of incoming calls before the phone rings. This software also blocks certain types of calls, such as those flagged as fraudulent or unwanted by other users, and calls from "unknown" or anonymous numbers. Additionally, a reverse lookup can be performed to detect fake caller-ID information in fraudulent calls (https://www.consumer.ftc.gov/blog/2017/10/apps-stop, 2021).

2.4 Background: Understanding Caller-ID Spoofing Techniques

The most common method of performing caller-ID spoofing attacks is through the use of VoIP telephony. The VoIP technology allows for voice communications to be sent over the Internet, rather than over a fixed phone line or cellular network. This convenience has led to the proliferation of VoIP providers that offer customers the ability to customize their caller-ID information via their services (Tu, Doupé, Zhao, & Ahn, SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam, 2016).

Caller-ID spoofing can also be performed using ready-made web or mobile applications. These applications typically allow users to enter the phone number they wish to call, followed by the phone number they want to display as the caller-ID. The call is then sent through a VoIP provider, which changes the outbound caller-ID information before connecting to the desired phone number.

In addition to ready-made applications, specialized services such as SpoofCard (Spoofcard, 2019) can be used to generate low-volume spoofed calls. Automated call generators, such as Mr.SIP (Mr.SIP: SIP-Based Audit and Attack Tool, 2019) or SIPp (Stanek & Kencl, 2011), can be used to generate large volumes of calls, each with individual, random, or carefully selected calling numbers. Customized scenarios can

also be produced using a VoIP provider connected to an Asterisk system (Tas, Unsalver, & Baktır, A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism, 2020) (Tas, Unsalver, & Baktır, Our Proposed SIP-Based Distributed Reflection Denial of Service (DRDoS) Attacks & Effective Defense Mechanism, 2015) (Taş & Baktır, A Novel Approach for Efficient Mitigation against the SIP-Based DRDoS Attack, 2023).

It is worth noting that the feasibility of caller-ID spoofing varies between countries and regions. In countries with strict regulations, such as the United States (US) and the United Kingdom (UK), initiating a call with a spoofed caller-ID is extremely difficult (Tu, Doupé, Zhao, & Ahn, SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam, 2016) (Pandit, Liu, Perdisci, & Ahamad, 2021). However, in countries with less regulation or oversight, such as developing countries, caller-ID spoofing is relatively simple. The ability to spoof caller-ID information and terminate calls in any country regardless of regulations highlights the need for a comprehensive solution that can effectively address this issue. In addition, the ease with which caller-ID spoofing can be performed using ready-made web or mobile applications, specialized services, and automated call generators, further emphasizes the need for a solution that can address this issue at a global scale.

2.5 Various Types of Attacks Performed Using Caller-ID Spoofing

Caller-ID spoofing is often used as a tool in various types of inbound call attacks, including telemarketing, surveys, debt collection, impersonation scams, phishing, bomb threats, swatting, voicemail attacks, telephony denial of service, account takeover, and robocalls. While its use is not inherently illegal, it is considered criminal when used with the intent to cause harm.

Caller-ID spoofing can be used in a variety of ways, such as:

- **Telemarketing, Surveys, and Debt Collection:** These types of voice SPAM use Caller-ID spoofing to trick victims into answering calls. The caller will present themselves as a legitimate representative of a company, organization, or government entity and may use pressure tactics to obtain personal information, conduct a survey, or demand payment of a debt.
- **Impersonation Scams:** These types of scams use Caller-ID spoofing to trick the victim into believing the caller is a representative of a government agency,

financial institution, or other trusted entity. The caller may then attempt to obtain sensitive information, such as Social Security numbers, credit card numbers, or login credentials. Common types of impersonation scams include tax/debt scams and technical support scams (Zhang, Wang, Yang, & Jiang, 2007).

- **Phishing:** These calls involve the use of deception and manipulation to extract sensitive information from the victim, often through the appearance of legitimacy. Fraudsters may employ various tactics, such as impersonating a representative from a trusted organization or creating a sense of urgency, to manipulate the victim into revealing personal information, login credentials, or financial details (Sahin, Francillon, Gupta, & Ahamad, 2017).
- **Bomb Threats:** Calls made to disrupt activities by targeting schools or other locations. The attacker will present themselves as a credible threat and demand that the target location be evacuated.
- **Swatting:** Calls made to emergency services to divert law enforcement resources away from illicit activities. The attacker will claim that a violent crime or hostage situation is in progress, causing a large police response.
- **Voicemail Attacks:** Unauthorized access to voicemails on systems that only verify the caller's number. The attacker will use Caller-ID spoofing to pose as the target and retrieve voicemails.
- **Telephony Denial of Service:** A call flood intended to disrupt transactions made to a public call center, which are often difficult to distinguish from legitimate calls. The attacker will use Caller-ID spoofing to present themselves as a large number of legitimate callers and overload the call center's systems.
- **Account Takeover (ATO):** A form of financial fraud in which an attacker attempts to gain control of real user accounts by calling a bank call center and withdrawing money. The attacker will use Caller-ID spoofing to present themselves as the account owner and trick the call center representative into releasing control of the account.
- **Robocalls:** Automated calls that have become increasingly prevalent, with

estimates of around 1 billion robocalls being made each month in the United States. This number has risen to 3 billion in recent months, with more than 250,000 robocall/fraud call complaints received in the United States every two weeks, and around 60,000 unique and phony numbers discovered (FCC Proposes Record, 2020) (FCC Proposes Record 225 Million Fine 1 Billion Spoofed Robocalls, 2020). Robocalls are often used to conduct scams or sell unwanted products, and Caller-ID spoofing is a common technique used to disguise the true identity of the caller.

These attacks are often carried out using social engineering techniques and DTMF (Dual Tone Multi-Frequency) solving procedures, allowing attackers to pose as customer service representatives, particularly in the banking industry. To protect against these types of attacks, it is important to be cautious of unsolicited calls, never provide personal information over the phone, and use call blocking software or perform a reverse lookup to detect fake caller-ID information.

2.6 Methods of Performing Caller-ID Spoofing

Caller-ID spoofing can be accomplished through a variety of methods, with the most prevalent method being through the use of Voice-over-Internet Protocol (VoIP) telephony. VoIP technology allows for voice communications to be transmitted over the Internet, rather than over traditional phone lines or cellular networks. Many VoIP providers also allow customers to customize their caller-ID information on their websites (Tu, Doupé, Zhao, & Ahn, SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam, 2016).

Low-volume spoofed calls can be generated using services or software such as SpoofCard (Spoofcard, 2019), Mr.SIP (Mr.SIP: SIP-Based Audit and Attack Tool, 2019), or SIPp (Stanek & Kencl, 2011). These tools can be used to generate calls automatically, with the capability to generate millions of calls, each with a unique, random, or carefully selected phone number (Tas, Ugurdogan, & Baktır, Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies, 2016) (Tas, Unsalver, & Baktır, A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism, 2020) (Tas, Unsalver, & Baktır, Our Proposed SIP-Based Distributed Reflection Denial of Service (DRDoS) Attacks & Effective Defense Mechanism, 2015). Automated call generators can also

pick numbers at random from a list and always dial the appropriate number, or employ more complex tactics such as selecting only valid and assigned numbers.

Another method for spoofing caller-ID is through the use of an Asterisk-based VoIP server and a genuine VoIP account registered with a service provider. This method is often used in conjunction with social engineering tactics to persuade the victim that the caller is someone else. To create fake outgoing calls, the attacker must use an Internet Protocol Private Branch Exchange (IP-PBX) system and find an upstream provider who will not prevent the use of caller-IDs that are not held by the company (Tu, Doupé, Zhao, & Ahn, SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam, 2016).

The black market for selling phone number lists is also a prevalent source for obtaining phone numbers for caller-ID spoofing. These lists can be obtained through various means such as harvesting address books from Outlook or public mail providers, or through old-fashioned war-dialing. Additionally, it is important to note that the ease of spoofing caller-ID varies by jurisdiction, with it being easier in countries with less regulation or strict inspection, such as developing countries in Eastern Europe. While caller-ID spoofing may be difficult to initiate in countries with strict rules, it is possible to terminate the call wherever desired, regardless of the country's regulations (Deng, Wang, & Peng, Combating Caller ID Spoofing on 4G Phones Via CEIVE, 2018) (Deng, Wang, & Peng, CEIVE: Combating Caller ID Spoofing on 4G Mobile Phones Via Callee-Only Inference and Verification, 2018) (Taş, Özbicerikli, Çağal, Taşkın, & Taş, 2014) (Acker, Plies, Massoth, Mayer, & Wiens, 2013).

2.7 Reasons for the Increase in Caller-ID Spoofing Incidents

The increase in caller-ID spoofing incidents can be attributed to the widespread adoption of VoIP telephony. VoIP technology makes caller-ID spoofing cheaper, more flexible, and more easily accessible to a global audience. Additionally, the nature of VoIP, which transfers only the audio signal and not the associated metadata, makes it significantly easier to carry out caller-ID spoofing than other forms of fraud such as email phishing.

As security measures have improved in other areas, such as email filtering, education on various forms of fraud, declining usage of insecure credit cards, and advancements in authentication technologies such as mobile authentication and two-

factor authentication (2FA), other forms of fraud have become more difficult to carry out. However, users continue to rely on the telephone system and tend to trust the caller-ID information displayed to them, making them more susceptible to caller-ID spoofing attacks (Sahin, Francillon, Gupta, & Ahamad, 2017) (Koilada, 2019).

2.8 Factors Contributing to the Rise of Caller-ID Spoofing

The rise of caller-ID spoofing is also driven by the profit motive behind these attacks. Fraudsters and scammers often use this technique to trick individuals into providing sensitive information or money, as they can make it appear as though the call is coming from a trusted source, such as a bank or government agency. This is especially prevalent in phishing scams, where the attacker tries to steal personal information or login credentials by posing as a trustworthy entity (Koilada, 2019).

The globalization of telecommunication services has also made it easier for attackers to carry out caller-ID spoofing from anywhere in the world. The complex network of carriers and solution providers makes it difficult for law enforcement agencies to track down and prosecute those engaging in illegal caller-ID spoofing.

In conclusion, the ease of use and affordability of VoIP technology, the lack of reliable caller-ID information, and the potential for financial gain, are all factors contributing to the increase in caller-ID spoofing. It is important for individuals and organizations to be aware of these attacks and to take steps to protect themselves.

2.9 Mitigating Caller-ID Spoofing Techniques and Limitations

Detection and prevention of caller-ID spoofing can be challenging, as it is difficult to determine the authenticity of an incoming call's caller-ID. Many VoIP servers now allow customers to select their own caller ID, and operators do not typically perform authentication checks to verify the caller-ID before the call is connected. The focus of service providers and operators is often on providing high-quality service, rather than ensuring reliability (Azad, Bag, Perera, Barhamgi, & Hao, 2020) (Kara, Şanlıöz, & Merzeh, 2021) (Hou, Han, & Novak, 2020).

To prevent user-level caller-ID spoofing, various mobile applications are available that allow users to verify the caller-ID information of incoming calls. However, this is not a comprehensive solution as it relies on the real caller also having the app installed (Stefanović & Ghilezan, 2020) (Li, Faria, Chen, & Liang, 2017).

Banks and other financial institutions have started to implement measures to detect and prevent caller-ID spoofing. These include using hidden inquiries, such as the mother's maiden name, and conducting further checks to verify the identity of the caller. Some institutions also rely on the assurance of service providers that caller-ID spoofing will be disallowed, while others have avoided using caller-ID as an authentication method altogether (Putra, Sadikin, & Windarta, 2017) (Mustafa, Xu, Sadeghi, & Schulz, 2018).

It can be difficult for providers and government organizations to effectively track down and prosecute those who engage in illegal caller-ID spoofing, as the telephone network is complex and involves multiple carriers and solution providers.

There are steps that individuals can take to reduce the number of unwanted phone calls they receive, such as registering for the National Do Not Call Registry, but these measures will not completely eliminate spam or phone harassment calls. Additionally, these tips are only effective in blocking approximately 30% of illegal and potentially fraudulent calls (Chen, et al., 2021) (McEachern & Burger, 2019) (Chiang & Burger, 2018).

2.10 The Deadlock of Having No Valid Solution

The lack of a comprehensive solution for caller-ID spoofing can be attributed to several factors. Phone operators and service providers have been reluctant to offer caller-ID spoofing blocking solutions to their customers, due to a combination of opportunity cost, regulations, technical difficulties, and investment cost (Gupta, Srinivasan, Balasubramaniyan, & Ahamad, 2015).

- **Opportunity Cost:** The economics of unwanted spam calls play a role in the reluctance to address the problem. Telemarketers and spammers can make money by making phone calls at a low cost and with minimal risk. Telephone companies also profit from connecting these calls to receivers, and service providers have little motivation to prohibit these calls unless their competitors offer a superior option.
- **Regulations:** Governments heavily regulate telecommunications to promote competition and justice, but this also slows innovation and reduces the risks that service providers are willing to take, as it imposes more obligations on them (Tas, Uğurdoğan, & Taş, 2015).

- **Technical Difficulties:** The complexity of the telephone network, made up of many different operators and service providers, makes it difficult to eliminate spoofed calls without cooperation.
- **Investment Cost:** The cost of addressing the caller-ID spoofing problem is high, and phone companies are unwilling to invest in solving it since it is not a profit-generating or cost-effective position for them.

Attempts by governments, such as the US, to control telemarketing and robocall issues through new laws and regulations, and partnerships between telecom firms and third-party providers, can only improve domestic issues. However, this is a global issue, and these remedies will be insufficient for calls coming from unregulated nations or difficult-to-follow VoIP sources. It is unlikely that current methods will effectively address the problem globally. This will require governments worldwide to implement similar laws and penalties, and perform necessary oversight, as part of a coordinated effort (Sahin, Francillon, Gupta, & Ahamad, 2017) (Tu, Doupè, Zhao, & Ahn, 2019). The lack of a comprehensive solution to the caller-ID spoofing problem highlights the need for a global approach that can effectively address this issue, taking into consideration the economic, regulatory, technical, and investment challenges.

Chapter 3

Literature Review

3.1 Evaluation of Academic Literature for Caller-ID Spoofing Attack Anatomy and Test Results

Previous research in the field of caller-ID spoofing has primarily focused on identifying and predicting malicious calls, as well as proposing solutions for verifying caller-ID authenticity. However, there is a lack of in-depth analysis of the anatomy and implications of end-to-end caller-ID spoofing attacks, particularly in the context of social engineering scenarios.

Figure 1 displays the frequency distribution of the most prevalent voice search-based attacks, as reported in the State of Voice Security report. It is notable that, with the exception of International Revenue Share Fraud (IRSF), all attacks rely on caller-ID spoofing (SecureLogix, 2017).

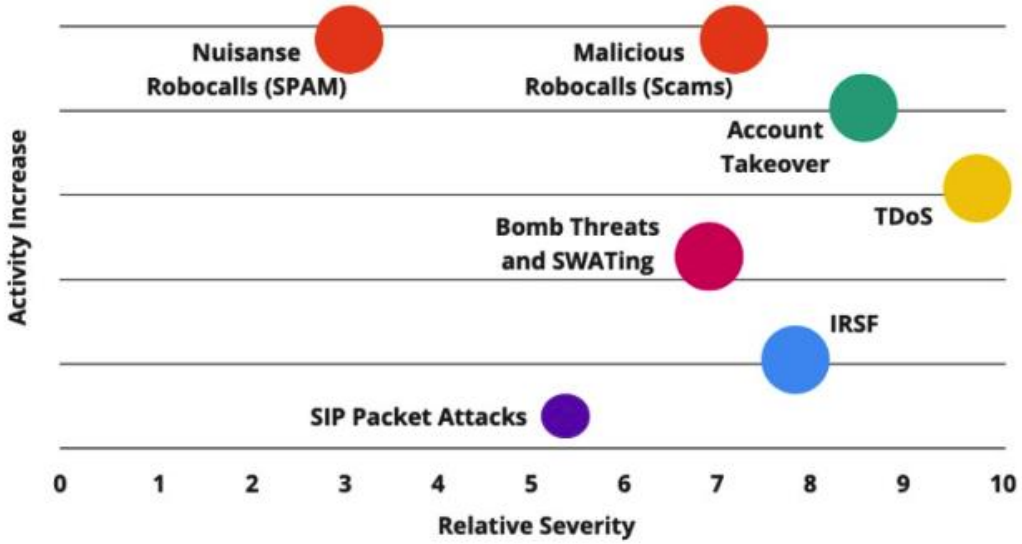

Figure 1. Overview of the most prevalent voice-related attacks.

In (Li, et al., 2018), a machine learning-based approach for predicting malicious calls was proposed. The study examined live call traffic in China but did not include tests for caller-ID spoofing. The authors created a total of 29 static and cross-referencing rule sets for machine learning but did not provide detailed information on the attack anatomy and test results.

In (Lu, et al., 2022), the authors identified the vulnerabilities of the signaling and voice sessions of VoWiFi (Voice over Wi-Fi), which can be hijacked by a malicious adversary to launch caller-ID spoofing attacks and stealthily accessible data transfer attacks. The study empirically validates these attacks in the operational 4G (fourth generation) networks of four top-tier carriers across Asia and North America with seven phone brands. The presented solutions can be used to address these vulnerabilities and improve the security of IMS (IP Multimedia Subsystem) networks. However, there is no detailed description of the caller-ID spoofing attack anatomy and test results.

In (Mustafa, Xu, Sadeghi, & Schulz, 2018), an end-to-end caller-ID verification scheme was proposed that utilizes existing phone network infrastructure and is enhanced with a SMS and timing-based version of their proposed solution. The authors examined how the caller-ID is conveyed in different call scenarios, however, there was no discussion of an end-to-end call flow or test results.

In (Sukma & Chokngamwong, One-time key Issuing for Verification and Detecting Caller-ID Spoofing Attacks, 2017) and (Sukma & Chokngamwong, Increasing the efficiency of One-time key Issuing for The First Verification Caller-ID Spoofing Attacks, 2018), the authors propose a self-controlled security and one-time key issue mechanism to avoid data leakage. They explain the mechanism of caller-ID spoofing in ISDN (Integrated Services Digital Network) networks and its potential impact on secure communication. However, there is no detailed description of the attack anatomy and test results.

In (Tu, Doupé, Zhao, & Ahn, Toward Standardization of Authenticated Caller-ID Transmission, 2017) and (Tu, Doupé, Zhao, & Ahn, Toward authenticated caller-ID transmission: The need for a standardized authentication scheme in Q.731.3 calling line identification presentation, 2016), the authors propose a standardized caller-ID authentication scheme that enables a security indicator for Signaling System No 7 (SS7) telecommunications. They provide a comprehensive explanation of how caller-ID spoofing works in PSTN (Public Switched Telephone Network) and SS7 networks and its potential impact on security. However, there is a lack of practical implementation and test results of the proposed scheme.

Table 1

Comparison of caller-ID spoofing detection and prevention techniques in recent literature.

Study	Focus	Method	Key Findings
(Li, et al., 2018)	Machine learning-based approach to predict malicious calls	Analysis of live call traffic in China	Proposed 29 rule sets for machine learning but did not examine caller-ID spoofing
(Lu, et al., 2022)	Identify vulnerabilities of VoWiFi signaling and voice sessions	Empirical validation in operational 4G networks of four top-tier carriers	Present solutions to address vulnerabilities but no detailed description of caller-ID spoofing attack anatomy and test results
Sadeghi, & Schulz, 2018)	Propose end-to-end caller-ID verification scheme	Examination of caller-ID conveyance in different call scenarios	No discussion of end-to-end call flow or test results
(Sukma & Chokngamwong, One-time key Issuing for Verification and Detecting Caller-ID Spoofing Attacks, 2017) and (Sukma & Chokngamwong, Increasing the efficiency of One-time key Issuing for The First Verification Caller-ID Spoofing Attacks, 2018)	Propose self-controlled security and one-time key issue mechanism	Explanation of caller-ID spoofing in ISDN networks and its potential impact on secure communication	No detailed description of attack anatomy and test results
(Tu, Doupé, Zhao, & Ahn, Toward Standardization of Authenticated Caller-ID Transmission, 2017) and (Tu, Doupé, Zhao, & Ahn, Toward authenticated caller-ID transmission: The need for a standardized authentication scheme in Q.731.3 calling line identification presentation, 2016)	Propose a standardized caller-ID authentication scheme	Explanation of caller-ID spoofing in PSTN and SS7 networks and its potential impact on security	Lack of practical implementation and test results of the proposed scheme
Blockchain-based Caller-ID Auth.	Anatomy and implications of end-to-end caller-ID spoofing attacks	In-depth analysis in a live financial call center environment	Provides insights into potential risks and implications of caller-ID spoofing attacks

In summary, previous studies have focused on various aspects of caller-ID spoofing such as detection and prevention methods. Still, they lack a comprehensive analysis of the anatomy and implications of end-to-end caller-ID spoofing attacks in realistic scenarios. As seen in Table 1, these studies have primarily focused on

predicting malicious calls using machine learning, proposing end-to-end caller-ID verification schemes, and implementing security mechanisms to avoid data leakage. However, none of them have provided a detailed analysis of the anatomy and implications of end-to-end caller-ID spoofing attacks supported by social engineering scenarios in a live financial call center environment. This study aims to fill this gap by providing a detailed analysis of the anatomy and implications of end-to-end caller-ID spoofing attacks supported by social engineering scenarios in a live financial call center environment.

3.2 Commonly Used Countermeasures Against Caller-ID Spoofing

There are several well-known and commonly used mechanisms that are utilized by existing prevention systems against caller-ID spoofing attacks (Tu, Doupé, Zhao, & Ahn, SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam, 2016). We classify these into three categories as follows:

- **Managed Blacklist:** The majority of telecom vendors such as Cisco Systems, Alcatel-Lucent, and Siemens use an active blacklist. This list determines whether incoming calls should be blocked or allowed, and gets updated as a result of user feedback. However, this strategy has its limitations as it is not effective for new calls coming from numbers that are not on the list or calls that use random fake dial numbers. Furthermore, managing and distributing a blacklist is difficult, risky, and susceptible to manipulation. Infrastructure entities need to be modified to support a blacklist. Additionally, the number of entries in the blacklist and whitelist would affect latency.

- **Do Not Originate (DNO):** Service providers block a call to their network that is coming from an invalid number or from a number that has never been assigned to a person. When calls are made in an irregular pattern, it is assumed that the number is invalid. These standards can be adopted more aggressively due to the impact of the caller-ID spoofing problem. However, there may be large gaps in the coverage of these techniques due to calls that traverse a legacy network. Managing and distributing a blacklist is difficult. All allocated numbers should be known by solution providers globally. This solution is prone to false positives and is simple to circumvent by using a caller-ID that has already been allocated.

- **Proprietary Authentication:** There are several methods for validating a call, such as Knowledge-Based Authentication (KBA), Voice Biometrics, Mobile Phone, and Digital Signature.
- **Knowledge-Based Authentication:** It is a typical practice in financial call centers to identify and verify a caller by asking questions that only the caller should know the answer to, but it is inconvenient for customers and requires businesses to employ costly call centers.
    - ***Voice Biometrics:*** It is a well-known method of authenticating the caller's identity using active and passive voice analysis, but it is costly and susceptible to noise, call quality, and other variables (Hou, Han, & Novak, 2020) (Kurdi, Hersi, Bahagari, Qaisar, & Subasi, 2017).
    - ***Mobile:*** The use of a mobile phone for authentication is only beneficial for specialized use cases, such as mobile or specific service providers, as it can easily be bypassed by impersonating the User-Agent information on the originating side (Kurdi, Hersi, Bahagari, Qaisar, & Subasi, 2017).
    - ***Digital Signature:*** It is a solution in which every user has a public/private cryptographic key pair associated with their phone number. This approach enables digital signature-based authentication to be used during phone calls (Sukma & Chokngamwong, Increasing the efficiency of One-time key Issuing for The First Verification Caller-ID Spoofing Attacks, 2018). However, key management and performance are significant issues with this approach. Additionally, it requires a trusted and distributed infrastructure which is costly to implement.

In summary, while these commonly known countermeasures against caller-ID spoofing have their advantages and disadvantages, none of them are fully capable of solving the problem on a global scale. It is important to note that implementing any of these solutions in isolation may not be sufficient to protect against caller-ID spoofing attacks. Additionally, these solutions are also not flexible to adapt to new technologies and changing regulations. In Section -19302071684.2 we present a comprehensive solution that will address these limitations.

Table 2

Comparison of commonly used countermeasures against caller-ID spoofing.

Countermeasure	Effectiveness	Ease of Implementation	User Impact
Managed Blacklist	Moderate	Moderate	High
Do Not Originate	Moderate	Difficult	Low
Knowledge-Based Authentication	High	Difficult	High
Voice Biometrics	High	Difficult	High
Mobile Phone	High	Difficult	Low
Digital Signature	High	Very Difficult	Low
Blockchain-based Caller-ID Auth.	High	Difficult	Low

Table 2 compares the commonly used countermeasures against caller-ID spoofing in terms of their effectiveness in preventing spoofing attacks, ease of implementation, and impact on user experience.

3.3 Evaluation of Academic Solutions for Caller-ID Spoofing

Several academic studies have proposed various approaches to address caller-ID spoofing in telephony networks.

In (Reaves, et al., 2017), the authors proposed a mechanism called AuthentiCall, which used a robust authentication method to verify caller-ID information before a call is answered. This allowed users to dismiss calls that claimed a specific caller-ID but were unable or unwilling to provide verification.

In (Reaves, Blue, & Traynor, AuthLoop: End-to- End Cryptographic Authentication for Telephony over Voice Channels, 2016), the authors proposed an authentication protocol called AuthLoop, which allowed end-to-end validation of caller-ID information for all telephony networks. The proposed protocol was based on the use of a telephony Public Key Infrastructure (PKI) and some cryptographic approaches. It was later enhanced with the RFC 8224.

In (Rebahi, 2008), the authors integrated elliptic curve cryptography (Miller, 1986) (Koblitz, 1987) into SIP and showed that the resulting performance was significantly better than the one where the Rivest-Shamir-Adleman (RSA) cryptosystem was used. They suggested that their work could be considered as a first step in standardizing the use of elliptic curves in identity management for SIP. However, the proposed method is inadequate for a spoofed call that originates via VoIP as it is not possible to check the accuracy of the data at the time the VoIP call originated

and whether the caller-ID information has been changed in the call flow. In addition, due to the computationally expensive cryptographic workload, the proposed solution is not efficient in terms of performance.

In (Li, et al., 2018), the authors proposed a machine learning-based approach to predict malicious calls. However, this approach would not work for every type of phone call and may create false positive alarms when spoofed calls originate via VoIP.

In (Azad, Bag, Perera, Barhamgi, & Hao, 2020), a self-enforcing method was proposed to perform password-based authentication in SIP (Session Initiation Protocol) without involving a trusted third party. However, this solution can only be applied by end-users at their initiative and would not be effective in preventing caller-ID spoofing attacks.

In (Mustafa, Xu, Sadeghi, & Schulz, 2018), an end-to-end caller-ID verification scheme was proposed which leverages the features of the existing phone network infrastructure. However, this solution can easily be bypassed via VoIP.

In (Sheoran, Fahmy, Peng, & Modi, 2019), a network-assisted caller-ID authentication solution was proposed to validate the caller-ID information used during call setup, but is only applicable to 4G networks and not able to prevent caller-ID spoofing initiated via VoIP.

In (Sukma & Chokngamwong, Increasing the efficiency of One-time key Issuing for The First Verification Caller-ID Spoofing Attacks, 2018) and (Sukma & Chokngamwong, One-time key Issuing for Verification and Detecting Caller-ID Spoofing Attacks, 2017), the authors proposed a self-controlled security and one-time key issue mechanism as a solution to prevent data leakage. However, this approach relies on a statistical model for the first verification unit, called the advisory system, to assist in identifying unknown calls. While this method may have some efficacy, it is not a comprehensive solution as it is dependent on the specific network infrastructure and may be easily circumvented by exploiting the flexibility of VoIP networks.

In (Tu, Doupé, Zhao, & Ahn, Toward Standardization of Authenticated Caller-ID Transmission, 2017) and (Tu, Doupé, Zhao, & Ahn, Toward authenticated caller-ID transmission: The need for a standardized authentication scheme in Q.731.3 calling line identification presentation, 2016), the authors proposed a standardized caller-ID authentication scheme for SS7 (Signaling System 7) telecommunication, but it is not useful for preventing caller-ID spoofing attacks that originate via VoIP.

In (Hou, Han, & Novak, 2020), the authors proposed an end-to-end, dual identity authentication mechanism using data transmission technology and voice-print recognition to verify the identity of the caller. However, the proposed mechanism did not explicitly address the issue of caller-ID spoofing, indicating the need for further research to develop more robust mechanisms to prevent this type of fraud.

In (Kurdi, Hersi, Bahagari, Qaisar, & Subasi, 2017), the authors presented a mobile fingerprint-based authentication system for call centers. The proposed system involved integrating a fingerprint scanner feature on smartphones and using it to verify the identities of callers before providing any services. However, the proposed approach is limited in that it does not provide network-based protection, making it susceptible to spoofing attacks and manipulation.

In (Chen, et al., 2021)., the authors proposed a blockchain-based system that authenticates the caller and receiver before establishing a call. However, the proposed system requires users to register decentralized identities and phone number credentials, making it less convenient for users. Additionally, the worst-case call establishment overhead of 2.1 seconds for the proposed system would not make it desirable for real-time communication scenarios. Furthermore, the system proposed in (Chen, et al., 2021). is limited to closed-circuit networks and may not be globally scalable. In contrast, our proposed solution in this paper, Blockchain-based Caller-ID Authentication~(BBCA), is designed to prevent spoofing attacks in VoIP/SIP networks and applies to a wide range of communication networks.

Table 3

Comparison of academic solutions for caller-ID spoofing prevention.

Study	Approach	Authentication	Validation	Anti-Spoofing	Shortcoming/Drawback
(Reaves, et al., 2017)	Phone Authentication Using Verified Protocols	High	High	Medium	Inadequate For Spoofed Calls Via Voip
(Reaves, Blue, & Traynor, AuthLoop: End-to- End Cryptographic Authentication for Telephony over Voice Channels, 2016)	Telephony Pki, Cryptographic	High	High	Medium	Inefficient İn Terms Of Performance
(Rebahi, 2008)	Elliptic Curve Cryptography	High	High	Medium	Inadequate For Spoofed Calls Via Voip, Inefficient İn Terms Of Performance
(Li, et al., 2018)	Machine Learning	Medium	Medium	Low	Inadequate For Spoofed Calls Via Voip, False Positive Alarms
(Li, Feng, Zhang, Xu, & Imran, 2021)	Password-Based Authentication	High	High	Low	Inadequate For Spoofed Calls Via Voip
(Mustafa, Xu, Sadeghi, & Schulz, 2018)	End-To-End Validation	High	High	Medium	Inadequate For Spoofed Calls Via Voip
(Sheoran, Fahmy, Peng, & Modi, 2019)	Network-Assisted	High	High	Medium	Limited To 4g Networks

Table 3 (cont.d)

(Sukma & Chokngamwong, One-Time Key Issuing For Verification And Detecting Caller-Id Spoofing Attacks, 2017) and (Sukma & Chokngamwong, Increasing the efficiency of One-time key Issuing for The First Verification Caller-ID Spoofing Attacks, 2018)	Self-Controlled Security, One-Time Key	Medium	Medium	Medium	Depends On Network Infrastructure, Inadequate For Spoofed Calls Via Voip
(Tu, Doupé, Zhao, & Ahn, Toward Standardization of Authenticated Caller-ID Transmission, 2017) and (Tu, Doupé, Zhao, & Ahn, Toward authenticated caller-ID transmission: The need for a standardized authentication scheme in Q.731.3 calling line identification presentation, 2016)	Standardized Caller-Id Authentication	High	High	Medium	Limited To Ss7 Telecommunication
(Chen, et al., 2021).	Blockchain-Based İdentity Authentication	High	High	High	Long Authentication Process, Not Suitable For Real-Time Communication
Blockchain-Based Caller-Id Auth.	Blockchain-Based Caller-Id Authentication	High	High	High	Implementation Difficulty Due To Regulatory Compliance And Integration

All in all, the existing solutions in the literature either fail to address caller-ID spoofing attacks or have limitations that make them ineffective in preventing these attacks. There is a lack of effective and efficient solutions for preventing caller-ID spoofing attacks, particularly for those that originate via VoIP. This highlights the need for further research in this area to address this important security issue.

Table 3 compares different caller-ID spoofing prevention techniques from an academic literature review perspective. It includes the academic literature and highlights the used technical approach, its level of authentication, validation, and anti-spoofing, and its shortcoming/drawback. In

Table 3, the column, titled *approach*, refers to the used technique to prevent caller-ID spoofing. The column, titled *authentication*, refers to the process of verifying the identity of the caller. The column, titled *validation*, refers to the process of verifying the authenticity of the calling party's number. The column, titled *anti-spoofing*, refers to the measures taken to prevent caller-ID spoofing attacks. Finally, the column, titled *shortcoming/drawback*, identifies the limitations and challenges of the given technique.

Table 3 also includes our new approach, named *Blockchain-based Caller-ID Authentication,* which is designed to combat caller-ID spoofing attacks in real time by managing and verifying end-to-end caller-ID information. Our approach is efficient in that it reduces the risk of hacking and data tampering while not relying on costly encryption and decryption operations for security.

3.4 Evaluation of Standards and Technical Challenges for Caller-ID Spoofing Prevention

Several standards have been proposed for the implementation of solutions against caller-ID spoofing. However, the assumptions made by these standards do not always align with the different types of infrastructures and caller-ID spoofing methods, leading to technical difficulties in their implementation (Kilinc & Yanik, 2014) (Durlanık & Soğukpınar, 2005) (Suthar & Rughani, 2020). In this section, we review six solutions against caller-ID spoofing attacks that are found in existing RFCs and standards.

- **RFC 3325 - Private Extensions to the SIP for Asserted Identity within Trusted Networks** (Jennings, Peterson, & Watson, 2002)**:** The P-Asserted-Identity (PAI) header is a SIP header used to indicate the identity of the caller in a VoIP network. It is often used to pass caller-ID information from one network element to another. In the context of caller-ID spoofing, attackers can manipulate PAI headers to impersonate legitimate callers or conceal their identities, making it difficult to trace and prevent fraudulent activities. RFC 3325 assumes that end systems that originate calls cannot change SIP headers, or that intermediary devices can be trusted to remove P-Asserted-Identity (PAI) headers. However, this approach is inadequate as both situations can easily be circumvented with the flexibility provided by VoIP, allowing attackers to manipulate the PAI header and conduct caller-ID spoofing attacks. The PAI header format is shown in *Figure 2*.

Figure 2. P-Asserted-Identity (PAI) header format in SIP.

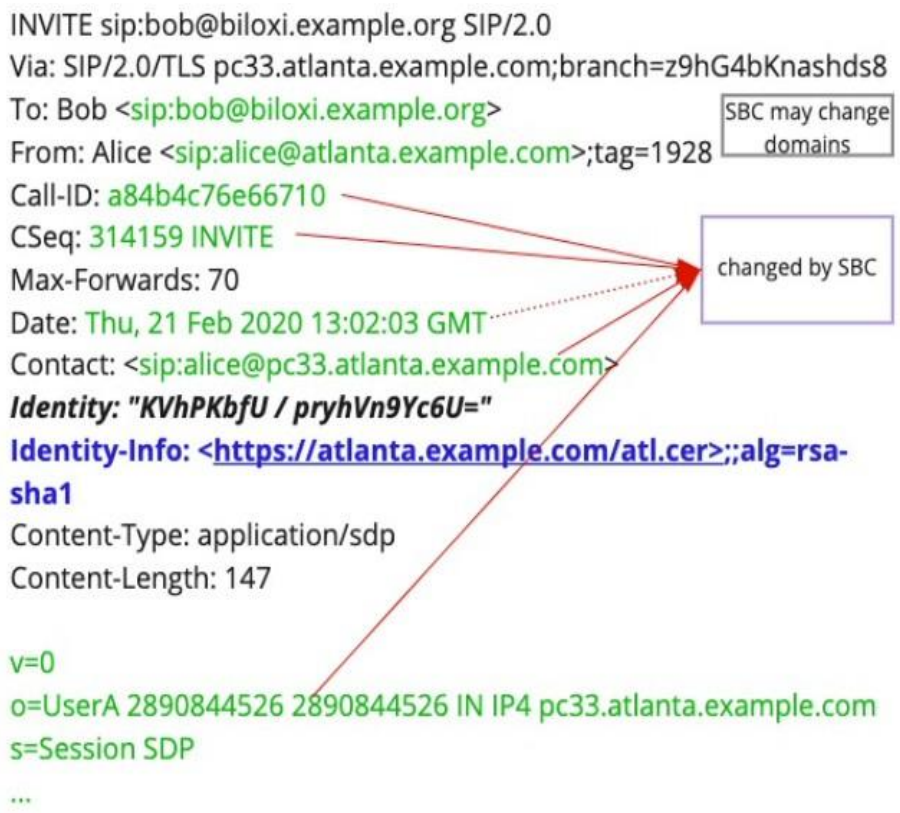

Figure 3. Example of SIP INVITE message with SDP included.

- **RFC 4474 - Enhancements for Authenticated Identity Management in the SIP** (Peterson & Jennings, RFC 4474: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), 2006)**:** RFC 4474 suggests signing all SIP INVITE messages with the Session Description Protocol (SDP). However, if there is a Session Border Controller (SBC) in the call flow, the SBC has to change the headers, as shown in *Figure 3*. This makes the proposed solution inapplicable in such scenarios. Additionally, the proposed solution relies on the RSA algorithm, which may become increasingly challenging to implement as small and simple devices proliferate and VoIP traffic increases (Peterson & Jennings, RFC 4474: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP), 2006) (Chen, Yeh, Liu, Hsiang, & Shih, 2010) (Rebahi, 2008). Moreover, the proposed caller-ID authentication mechanism cannot identify the person to whom the phone number is assigned. Intermediary devices must re-sign the request which introduces a performance overhead. Back-to-Back User Agents (B2BUA) are intermediary entities that can modify SDP messages used to establish communication sessions. In the context of caller-

ID spoofing prevention, when a B2BUA modifies an SDP message, it may change the caller number information, which can affect the accuracy of the used caller-ID authentication mechanism. Therefore, for the B2BUA scenario, the SDP must be rewritten to ensure that the caller number information remains accurate and consistent throughout the communication session.

Regulatory authorities often encourage the interconnection of VoIP networks. However, non-SIP interconnections can create challenges for implementing caller-ID authentication mechanisms that require comprehensive solutions. Changing communication infrastructures on a global scale is a challenging task, and existing infrastructures, such as SS7, which is widely used for the setup and tear-down of most telephone calls in the public switched telephone network, are expected to remain unchanged for a long time. This can create obstacles in the implementation of effective caller-ID authentication mechanisms since these mechanisms must consider the unique characteristics of the various communication infrastructures involved. Therefore, more comprehensive solutions are required to address the issue of caller-ID spoofing, which can take into account the complexities of these infrastructures and the interconnection points between them (E.164, 2016) (Fältström, 2000).

- **STIR/SHAKEN** (Wendt & Barnes, RFC 8588: Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN), 2019)**:** STIR/SHAKEN is a framework that aims to verify a caller number using a signature-based token, with the goal of minimizing the impact of robocalling (ATIS Technical Report on a Framework for Display of Verified Caller-ID, 2018). STIR (Secure Telephony Identity Revisited) RFC (Peterson, Schulzrinne, & Tschofenig, RFC 7340: Secure Telephone Identity Problem Statement and Requirements, 2014) and SHAKEN (Signature-based Handling of Asserted Information Using Tokens) (Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management (ATIS-1000080.v002), 2017) are the result of a collaboration between the Internet Engineering Task Force (IETF), Automatic Terminal Information Service (ATIS), the SIP Forum, and service providers (Signature-based Handling of

Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management (ATIS-1000080.v002), 2017). SHAKEN is a more recent definition of how to implement STIR in practice. These efforts are based on an attempt to verify the caller number presented to the target user (Peterson & Turner, RFC 8226: Secure Telephone Identity Credentials: Certificates, 2018) (Peterson, Schulzrinne, & Tschofenig, RFC 7340: Secure Telephone Identity Problem Statement and Requirements, 2014).

The STIR/SHAKEN framework allows service providers to add a digital signature to each call using public key encryption, thereby facilitating the authentication of the caller-ID information. This digital signature is included in the newly introduced SIP Identity header. When all originating service providers enable STIR/SHAKEN in their network, terminating providers will have much more control over both which calls to pass and which provider a call goes to (McEachern & Burger, 2019) (Chiang & Burger, 2018).

However, STIR/SHAKEN has some challenges in terms of interoperability. This is because it consists of works from different organizations such as IETF and ATIS, each with their own unique style of writing SIP specifications. Additionally, there are some known uncertainties in the certification model, such as determining who will sign first and who will be the first to approve. These scenarios are not clearly defined, which causes confusion regarding the applicability of this method.

- **RFC 8226 - Secure Telephone Identity Credentials: Certificates** (Peterson & Turner, RFC 8226: Secure Telephone Identity Credentials: Certificates, 2018)**:** RFC 8226 describes the use of certificates in establishing authority over telephone numbers as part of a larger architecture for handling telephone numbers as identities in protocols like the SIP. The certification model is integrated with number assignments, such as "Public key X has the authority to use number Y". Number assignments are issued by the number assignment authority, such as the Number Portability Administration Center (NPAC), possibly through a delegation chain of authorization (Mustafa, Xu, Sadeghi, & Schulz, 2018) (Peterson, RFC 7375: Secure Telephone Identity Threat Model, 2014). The certification model also offers voice verification similar to web domain verification, such as “enter the number you hear on the web

form” (Unwanted Robocalls : Challenges and Solutions, 2020) (Bhasker, 2019).

From the perspective of need, major carriers want to eliminate auto-call complaints, legitimate outgoing call centers want their messages to be delivered, and high-value users want to avoid identity theft. Carriers are concerned about inter-carrier compensation fraud and are tired of receiving complaints from customers. Newcomers look for a differentiator to make the transition and stop receiving automated calls. The certification model is proposed as a method that can meet all of these requirements. However, there are some known uncertainties in the certification model, such as who will sign first, and whether this should be done by choice or by mandate. Additionally, the applicability of this method causes confusion as the scenarios are not clearly defined.

- **RFC 8224 - Authenticated Identity Management in the SIP** (Peterson, Jennings, Rescorla, & Wendt, 2018)**:** The proposed mechanism in RFC 8224 aims to securely identify the source of SIP requests through the use of a SIP header field for transmitting a signature used for authentication, and a reference to the signer's credentials. However, as noted in previous research, the baseline security mechanisms in SIP are inadequate for cryptographically assuring the identity of end-users in an inter-domain context (OpenSIPIt ’01 – Testing the Trending SIP Security Enhancements, 2021) (Wendt & Peterson, RFC 8225: PASSporT: Personal Assertion Token, 2018). Furthermore, RFCs do not explicitly define the method or algorithm for extracting caller-ID and callee-ID information from SIP messages, leading to uncertainty in the prioritization of various SIP headers. The SIP headers used for caller-ID, such as "display name," "PAI," or "incoming," and those for callee-ID, such as "display name," "username" in the "to" header, or the "username" in the Request-URI (Universal Resource Identifier), may have different priorities depending on the implementation. This lack of clear specification poses challenges to the practical implementation of this approach. A well-defined and consistent algorithm for the extraction and prioritization of caller and callee identification information from SIP messages is needed for the proper implementation of caller-ID authentication

mechanisms.

- **RFC 8225 - A Framework for SIP Caller Authentication and Identification** (Wendt & Peterson, RFC 8225: PASSporT: Personal Assertion Token, 2018)**:** RFC 8225 presents a framework for authenticating and identifying callers in SIP-based telephony systems. The standard recommends the use of the STIR/SHAKEN framework for caller-ID validation, which utilizes digital signature-based tokens for authentication. However, the standard does not provide a comprehensive implementation guide for the proposed framework and fails to address the issue of caller-ID spoofing that originates via VoIP, highlighting the need for further research in this area.

Table 4

Comparison of standards and technical challenges for caller-ID spoofing prevention.

Study	Approach	Authentication	Validation	Anti-Spoofing	Shortcoming/Drawback
RFC 3325	Uses the P-Asserted-Identity header in SIP to assert the identity of the caller	Medium	Low	Low	Inadequate for VoIP calls, easily circumvented and vulnerable to spoofing attack
RFC 4474	Uses digital signatures to ensure the authenticity of the SIP INVITE message	High	High	Medium	Complexity of legacy infrastructure, not applicable in scenarios w/ SBCs, requires a public key infrastructure
STIR/SHAKEN	Uses a signature-based token to verify the caller's number, aiming to reduce the impact of robocalling	High	High	Medium	Complexity of legacy infrastructure, centralized database required
RFC 8226	Uses X.509 certificates to authenticate the identity of the caller	High	High	Medium	Requires a trusted certificate authority
RFC 8224	Uses a header field in SIP to carry a signature of the caller's identity. Requires a centralized database	Medium	Medium	Low	Complexity of extracting caller-ID information, requirement for a centralized database
RFC 8225	A framework for verifying caller ID using digital certificates. Only applicable to VoIP calls that traverse the IP network and not to calls that are made via SS7	Medium	Medium	Medium	Lack of detailed implementation solution, inadequate for VoIP calls
Blockchain-based Caller-ID Auth.	Uses blockchain technology to create a decentralized ledger that stores caller-ID information and allows for real-time validation of caller-ID information, thus preventing spoofing attacks	High	High	High	Implementation difficulty due to regulatory compliance and integration

Similar to

Table 3, which compares the solutions against caller-ID spoofing in the academic literature, Table 4 compares different standards and technical challenges for caller-ID spoofing prevention. Each standard has its own set of strengths and weaknesses, as described in the table. For instance, RFC 3325 assumes that end systems that originate the call will not change the SIP headers or intermediary devices can be trusted to remove PAI headers. This approach is inadequate as both situations can easily be circumvented with the flexibility provided by VoIP. On the other hand, STIR/SHAKEN is a framework to verify a caller number using a signature-based token aiming to minimize the impact of robocalling, but it is only applicable to VoIP calls that traverse the IP network and not to calls that are made via SS7. Additionally, it still suffers from challenges such as the need for a centralized database and the need to handle the complexity of the legacy infrastructure. Overall, it can be concluded that while existing standards have the potential to address the caller-ID spoofing problem, they also have limitations and challenges that need to be overcome.

In Table 4, we also include our novel blockchain-based caller-ID authentication solution which will be explained in detail in Section -19302071684.2. Our solution has the advantage of allowing for real-time validation of caller-ID information by using a decentralized ledger that stores caller-ID information.

Chapter 4

Methodology

4.1 Anatomy of End-To-End Caller-ID Spoofing Attacks in Live Financial Call Centers and Results

4.1.1 Experimental testing environment. In order to provide a thorough examination of the implications of end-to-end caller-ID spoofing attacks in a realistic scenario, we conducted our studies in a live testing environment. Specifically, we used a VoIP-based SIP-PBX (Session Initiation Protocol-Private Branch Exchange) system, configured with the Asterisk-based FreePBX on a VMware virtualization platform, to simulate a financial call center environment. We utilized the SIP trunk service provided by a US-based VoIP service provider, Origin-ISP, which allowed us to generate customized SIP messages with spoofed caller-ID information during our tests (Tas, Ugurdogan, & Baktır, Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies, 2016) (Tas & Kucuk, DEF CON 28 Main Stage, 2020) (Mr.SIP: SIP-Based Audit and Attack Tool, 2019) (https://wiki.asterisk.org/, 2020).

We employed the SIP-SIM (SIP Signaling Manipulator) module of our VoIP security research tool, Mr.SIP, to capture and modify call traffic between the SIP client and SIP-PBX. SIP-SIM operates as an intercepting SIP proxy and can perform both LAN (Local Area Network)-based and WAN (Wide Area Network)-based caller-ID spoofing attacks. In this study, we conducted WAN-based spoofing attacks in our live test environment.

We obtained written and authorized consent from a financial call center in Turkey to conduct our tests in their live environment. The call center in question accepts caller-ID information as a method of authentication and assumes that the identity of the caller has been verified by the mobile phone number registered in their system. In cases where additional verification is required, an SMS verification message (OTP (One Time Password)) is sent to the customer's mobile phone. We simulated both scenarios of a financial customer calling the call center and making

sensitive transactions and a customer representative calling a financial customer from the call center and requesting information.

In order to gather sufficient data of significance for analysis, we conducted numerous test calls to confirm that the phone number obtained or the caller ID impersonated corresponded to three GSM operators, one land-line operator, and one VoIP ISP in Turkey and that the operator that terminated the call at the call center traversed each of the aforementioned three GSM operators, one land-line operator, and one VoIP ISP. This enabled us to amass adequate data of substance for analysis.

4.1.2 Methodologies and implementation. The aim of this study was to evaluate the feasibility and implications of end-to-end caller-ID spoofing attacks in a live financial call center environment. The study was designed to examine the anatomy and impact of caller-ID spoofing attacks that utilize both technical and social engineering aspects. To achieve this objective, the following research design and data collection methods were employed.

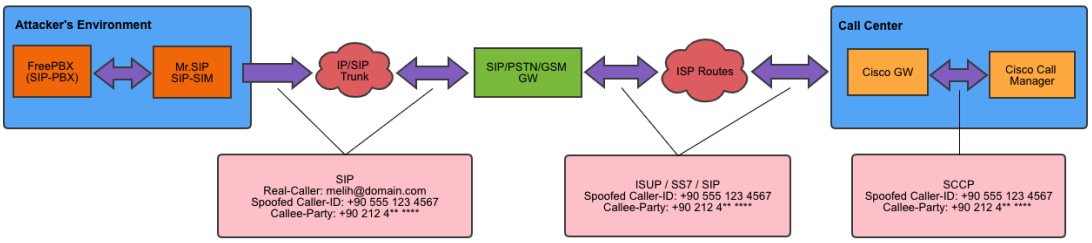

Figure 4. Representation of the caller-ID spoofing attack flow in the studied live environment.

4.1.2.1 Research design.

1. The study was conducted in a controlled environment with the permission of the financial call center.
2. The call center's VoIP infrastructure was subjected to security tests with attacks made over the internet at mutually agreed upon times.
3. The objective of the study was to verify that the caller-ID information could be manipulated to simulate a call from a customer or a customer representative using the spoofing method, and in doing so, unauthorized transactions could be made in both directions.

4.1.2.2 Data collection methods.

1. Examination of the network connection and infrastructure of the call center.

2. Tests were conducted using the SIP-SIM module of Mr.SIP to simulate a client software (soft-client) registered to FreePBX using SIP trunk service over Origin-ISP.
3. The spoofed calls were transferred to the IP network and then routed through the service providers contracted by Origin-ISP over the wide area network, passing over the SIP/PSTN Gateway to the PSTN, and finally reaching the call center via Cisco Call Manager.

4.1.2.3 Implementation.

1. The call center employed Cisco Call Manager as the call server, which was connected to the internal IP network.
2. Incoming calls from PSTN were managed by the Cisco Voice Gateway and were transferred to a process step or forwarded to a customer representative using the IVR (Interactive Voice Recording) application.
3. If the voice command could not be matched with any label defined in the background, it would be transferred to the selected menu with DTMF tones.
4. The SIP-SIM module of Mr.SIP was used to simulate a client software (soft-client) registered to FreePBX using SIP trunk service over Origin-ISP.
5. The spoofed calls were transferred to the IP network, where they reached the dialed number (bank call center) by being routed through the service providers contracted by Origin-ISP over the wide area network.
6. The calls were then passed over the SIP/PSTN Gateway to the PSTN and finally reached the call center via Cisco Call Manager, exposing the call center to a caller-ID spoofing attack from an IP network.

The methodology and implementation of this study are depicted in *Figure 4,* which provides a flowchart representation of the process and components involved in the caller-ID spoofing attack and tests performed.

4.1.2.4 Analysis.

1. The results of the study were analyzed to determine the feasibility and implications of end-to-end caller-ID spoofing attacks in a live financial call center environment.
2. The results were compared with the methods and approaches used in previous

studies and in practice to demonstrate the effectiveness of the caller-ID spoofing attack.

3. The results of the study were used to provide insights into the anatomy and implications of caller-ID spoofing attacks and to demonstrate the need for effective countermeasures to prevent these attacks (Tas & Kucuk, DEF CON 28 Main Stage, 2020).

Overall, the methodology and implementation of this study were designed to provide a comprehensive examination of the anatomy and implications of end-to-end caller-ID spoofing attacks in a live financial call center environment.

4.1.2.5 Ethical consideration and safeguards. This study was conducted in strict adherence to ethical principles and with the utmost regard for safety. We obtained explicit approval from the financial company involved, and no harmful actions were taken during the experiment. The purpose of the test was to evaluate the possibility of using caller-ID information as part of the authentication process. All experiments were performed in a controlled environment and monitored carefully to avoid potential risks. No real customers were involved in the testing phase, and no actual customer data was used. Post-study, we collaborated with the company to share our findings and recommend preventive measures against such attacks, ensuring the practical value and responsible conduct of our research.

4.1.3 Evaluation of implementation results. In this study, it was demonstrated that caller-ID spoofing can be used to bypass SMS verification (OTP) in a live financial call center environment, allowing unauthorized transactions, such as telephone banking and internet branch password changes, to be made during conversations with customer representatives. Additionally, it was verified that customers can be targeted by spoofing bank phone numbers, potentially leading to the disclosure of sensitive customer information.

The results of the caller-ID spoofing tests conducted in this study were inconsistent, with varying success rates depending on the date of the test. This is likely due to the regulatory requirements and technical capabilities of different service providers in detecting and blocking spoofed calls on domestic or international routes. The phone numbers used in the tests were selected from both real registered phone numbers of fixed/mobile operators and completely random numbers.

The success rate of call termination, or the successful completion of a call to the intended recipient, was found to be 7 out of 10 for the scenario of spoofing a call as if it were coming from a valid personal phone number. However, the SIP trunk service may not always be able to successfully terminate the call. In the second test scenario, where attempts were made to call customers by imitating the number of the financial call center, 4 out of 10 spoofed phone calls were not terminated successfully at the service provider level.

Intermediary operators in the call route can differ for each call and may have the ability to block or alter the caller-ID information of spoofed calls due to legal obligations. The reasons for the inconsistencies in test results may include unsuccessful call termination, call blocking before reaching the destination, alteration or deletion of caller-ID information by an intermediary service provider, or temporary routing issues. Further analysis of these factors is discussed in the rest of this section.

In the following, we give the detailed call flow for a sample test, including information and observations on the success and failure of the results, as well as evaluations on potential points of blocking. In order to maintain confidentiality, we have refrained from disclosing the names of the service providers from which the test calls were terminated in Turkey. We refer to the service providers that took part in our tests as GSM-Operator-1, GSM-Operator-2, GSM-Operator-3, Land-Line-ISP, and VoIP-ISP throughout this paper. The results of the test scenarios conducted in this study provide insight into the effectiveness of caller-ID spoofing prevention measures in different stages of the call routing process. The consistency of the results was found to be influenced by various factors, including regulatory compliance and the technical capabilities of intermediary service providers to detect and block spoofed calls. A detailed analysis of these factors is presented in the following steps.

4.1.3.1 Sample test call flow.

Step 1: Asterisk-based FreePBX > Origin-ISP: The call was initiated with a custom SIP INVITE message containing the spoofed caller number information via the SIP trunk service of a US-based ISP named Origin-ISP, which was linked to the Asterisk-based FreePBX system installed on our virtual machine, targeting a Turkish phone number.

Step 2: Origin-ISP > Intermediary Service Providers Contracted: As the call was routed through different operators each time, the spoofed call was directed through various ISPs on the internet until it reached its destination. At this stage, if the call

passes through an ISP in a country where it is legally required to block spoofed calls, the successful termination of the call is hindered by the spoofed caller-ID information, or the spoofed caller-ID information is manipulated (typically deleted or truncated). However, if the call does not pass through an ISP with strict regulations, it was able to successfully terminate in Turkey. It is worth noting that this does not necessarily imply that a regulated ISP can intercept the spoofed call or manipulate the caller-ID information, but rather depends on the ISP's ability to detect the spoofed call and monitor its origin.

Step 3: Intermediary Service Providers Contracted > Border ISP in Turkey: Upon reaching the terminating service provider in Turkey, the spoofed test call was successfully terminated to its target. However, at this point, the spoofed call can also be detected and blocked by the terminating service provider, or the caller-ID information can be manipulated.

Step 4: Border ISP in Turkey > Terminating ISP in Turkey (in our case the Land-Line-ISP): The ISP at the first point reached by the spoofed call in Turkey varied each time according to the routing algorithms typically used such as LCR (Least Cost Routing). Although the number dialed belongs to the Land-Line-ISP, the call was not routed directly through the Land-Line-ISP each time upon entering Turkey. It sometimes came via GSM (Global System for Mobile Communication)-Operator-1, GSM-Operator-2 or GSM-Operator3 and was forwarded to the Land-Line-ISP from there. This is one of the reasons for the inconsistency in the successful termination of the spoofed call each time. For example; If the spoofed call comes from GSM-Operator-2 upon entry into Turkey and is forwarded to the Land-Line-ISP from there, the test call may fail to terminate if GSM-Operator-2 detects and blocks the spoofed caller-ID information. If the call goes directly through the Land-Line-ISP upon entering Turkey, the call can be successfully terminated.

Step 5: The Land-Line-ISP > PBX of the Financial Call Center (in our case Cisco Call Manager): If the spoofed call was blocked at the ISP level, it could not reach the call center's PBX anyway. Occasionally, and inconsistently, the caller-ID information has been truncated, and the call was successfully terminated. Instead of blocking, one of the ISPs truncated the caller's credentials and successfully ended the call.

In *Figure 5*, we give the call dump from Cisco Gateway in the scenario where the call center is called by spoofing the customer phone number. We can see here that the caller-ID information is transmitted as it is in its original form.

```
1.Test Call:
Mar 6 10:36:48.214: ISDN Se7/2:15 Q931: RX <- SETUP pd = 8 callref = 0x017E
Bearer Capability i = 0x8090A3
Standard = CCITT
Transfer Capability = Speech
Transfer Mode = Circuit
Transfer Rate = 64 kbit/s
Channel ID i = 0xA98382
Exclusive, Channel 2
Calling Party Number i = 0x1183, '009055548*****'
Plan:ISDN, Type:International
Called Party Number i = 0xC1, '4132500'
Plan:ISDN, Type:Subscriber(local)
Sending Complete
```

Figure 5. Cisco Gateway call dump in the first test call of caller-ID spoofing on a live financial call center.

```
2. Test Call:
8214021: Mar 6 10:58:04.604: ISDN Se7/4:15 Q931: RX <- SETUP pd = 8 callref = 0x1572
Sending Complete
Bearer Capability i = 0x8090A3
Standard = CCITT
Transfer Capability = Speech
Transfer Mode = Circuit
Transfer Rate = 64 kbit/s
Channel ID i = 0xA1839C
Preferred, Channel 28
Progress Ind i = 0x8281 - Call not end-to-end ISDN, may have in-band info
Calling Party Number i = 0x1181, '0055548*****'
Plan:ISDN, Type:International
Called Party Number i = 0xA1, '21247*****'
Plan:ISDN, Type:National
```

Figure 6. Cisco Gateway call dump in the second test call of caller-ID spoofing on a live financial call center.

In *Figure 6*, we give the call dump from Cisco Gateway in the scenario where the call center is called by spoofing the customer's phone number. We can observe here that the spoofed caller-ID was transmitted, instead of the original caller-ID, and the attack was successful.

In order to gain a deeper understanding of the results obtained from our study, the signal flow of our test calls was thoroughly tracked and analyzed at the operator level terminating at the call center's PBX. This enabled us to determine whether the test calls had successfully reached their destination, and if so, with what caller-ID information.

In order to provide a concrete example, we present an excerpt from a sample test call trace taken from the PBX where the call was terminated, which includes the caller-ID information. During a normal call, the caller-ID information is transmitted as is, as given in *Figure 5*,. In the scenario of the attack that we simulated, the financial call center was called, pretending to be the customer's registered mobile phone number, allowing the telephone banking password to be changed without the need for an SMS verification by relying on the caller number information. Upon examining the call trace of this scenario, we observed that the spoofed caller-ID was transmitted as is, and we found that the attack was successful, as given in *Figure 6*.

We observed that the authentication of the customer is typically checked with an SMS verification message (OTP message) based on the customer number defined in the call center, but this security step can be bypassed for incoming calls with the customer number registered in the system. Based on this result, it is possible for various transactions to be made on behalf of the customers by individuals impersonating real customers. We also noted that there was no warning in the target system during the attack, and no abnormality was detected by the system administrators of the bank where the call center was located.

Based on our observations of mobile and land-line phone calls made to customers in Turkey, we found that the five major operators (three GSM operators, one fixed-line operator, and one VoIP-ISP) were not successful in stopping caller-ID fraud. Specifically, our testing demonstrated that these operators were unable to detect spoofed caller-ID information when the attack was carried out using call center and bank numbers, as shown in Table 5. As a result, attackers were able to display fraudulent caller-ID information on the customer's side, highlighting the potential for obtaining private and confidential customer information through the use of social engineering tactics. This finding highlights the need for further research and development of effective methods for detecting and preventing caller-ID spoofing in communication systems.

In order to collect meaningful statistics, we performed two-way spoofed calls between the financial call center and the customer's mobile number, with terminating ISPs including Land-Line, GSM and VoIP. We made a total number of over 200 spoofed test calls. The originator ISP, spoofed caller-ID information, callee-party, and attack success rate of the test spoofed call associated with each terminating ISP are shown in Table 5.

Table 5

Comparative analysis of the effectiveness of different service providers in terminating spoofed calls.

Origin	Terminating ISP	Spoofed Caller-ID	Callee-Party	Attack Success
Origin-ISP (US)	Land-Line-ISP	Customer mobile no	Financial call center	100%
Origin-ISP (US)	GSM-Operator-1	Customer mobile no	Financial call center	80%
Origin-ISP (US)	GSM-Operator-2	Customer mobile no	Financial call center	70%
Origin-ISP (US)	GSM-Operator-3	Customer mobile no	Financial call center	70%
Origin-ISP (US)	VoIP ISP	Customer mobile no	Financial call center	100%
Origin-ISP (US)	Land-Line-ISP	Financial call center	Customer mobile no	80%
Origin-ISP (US)	GSM-Operator-1	Financial call center	Customer mobile no	70%
Origin-ISP (US)	GSM-Operator-2	Financial call center	Customer mobile no	60%
Origin-ISP (US)	GSM-Operator-3	Financial call center	Customer mobile no	70%
Origin-ISP (US)	VoIP ISP	Financial call center	Customer mobile no	100%

4.1.4. Detailed Experiment Analysis. In our comprehensive study, we performed over 200 two-way spoofed calls between the financial call center and the customer's mobile number, using a diverse set of terminating ISPs, which included Land-Line, GSM, and VoIP. In order to replicate real-world scenarios, we utilized 50 different spoofed numbers randomly selected from an existing pool of customer numbers.

Our experiments, conducted over a span of two months, brought forth some critical findings. We observed that customer authentication, typically carried out through an SMS verification message (OTP message) based on the customer number registered in the call center system, could be bypassed for incoming calls with the customer number. This loophole can be exploited by threat actors impersonating real customers to carry out transactions on their behalf, emphasizing the potential risk to customer security.

Interestingly, during the course of these spoofing attacks, we noticed that the target system did not trigger any warning, and no anomalies were detected by the system administrators of the bank where the call center was located. This indicates a significant gap in the current detection and prevention mechanisms for caller-ID spoofing attacks.

Moreover, our research shows that five major operators in Turkey, including three GSM operators, one fixed-line operator, and one VoIP-ISP, were unsuccessful in stopping caller-ID fraud. When the attack was carried out using call center and bank numbers, these operators were unable to detect the spoofed caller-ID information. Consequently, attackers were able to display fraudulent caller-ID information on the customer's side, thereby increasing the potential for gaining unauthorized access to private and confidential customer information through social engineering tactics.

The detailed results of these experiments, including the specific success rates associated with each terminating ISP, are outlined in Table 5. These findings underscore the urgent need for more effective caller-ID spoofing detection and prevention across all types of service providers. These insights are intended to fuel further innovation in the detection and prevention of such attacks, ultimately contributing to a more secure telecommunication environment.

4.2 Our Novel Blockchain-Based Solution Approach for Caller-ID Authentication

4.2.1 Methodology and design. We have designed a novel defense mechanism that employs a low latency blockchain consensus algorithm to effectively prevent caller-ID spoofing attacks in real time. Our blockchain-based novel registration and call flow control processes that are positioned in the cloud are able to manage and verify ISPs' and institutions' caller-ID information end-to-end. Our solution verifies when a call is initiated, from which ISP the call originated, whether there is a change in the caller-ID and ANI information, and whether there is a change in the ANI information where the call originates at each hop change.

We choose to design a blockchain-based solution for caller-ID spoofing prevention because it offers a transparent, decentralized, and distributed solution that also helps reduce the risk of hacking and data tampering. Additionally, it allows for a more efficient approach to security by eliminating the need for costly encryption and decryption operations, resulting in less computational load and lower delay (Chen, et al., 2021). Our solution is designed to meet the requirements of the real-time critical nature of voice communication and its sensitivity to Quality of Service (QoS) parameters. The consensus algorithm used in our solution is a modified version of the PBFT algorithm. The modification allows for low latency and real-time performance by implementing a two-phase commit protocol, where a small subset of nodes called "verifiers" are responsible for quickly reaching a consensus on the validity of a caller-ID. The verifiers are selected based on their reputation and past performance in the network similar to the blockchain consensus mechanisms used in (Ferrag & Maglaras, 2020) (Yang, Jia, Su, Wu, & Qin, 2022) (Cai, 2020) (Vishwakarma, Nahar, & Das, 2022) (Meshcheryakov, Melman, Evsutin, Morozov, & Koucheryavy, 2021) (Saha, et al., 2021).

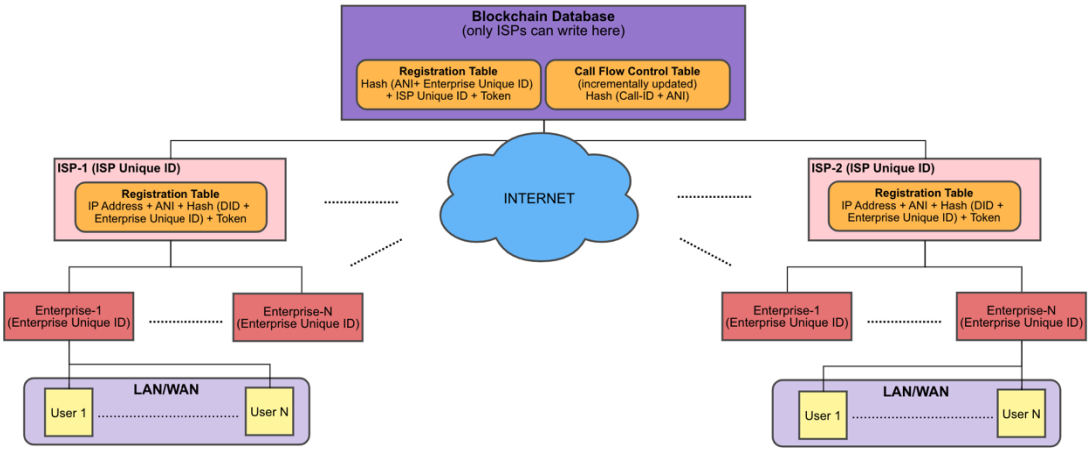

Figure 7. Visual representation of the proposed Blockchain Based Caller-ID Authentication (BBCA) mechanism.

Call Flow Control Table Structure

1	Reg ID-1 (hash)	Call Flow ID-1 (hash)	Call initiated
2	Reg-ID-1 (hash)	Call Flow ID-2 (hash)	SBC involved
3	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Call initiated
4	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Call forwarded
5	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Roaming
6	Reg ID-1 (hash)	Call Flow ID-1 (hash)	Call terminated
7	Reg-ID-2 (hash)	Call Flow ID-1 (hash)	Call terminated

Figure 8. Call flow control table structure for the proposed Blockchain Based Caller-ID Authentication (BBCA) mechanism.

Registration Table Structure

1	ISP-1	Reg ID-1 (hash)	First registration
2	ISP-1	Reg ID-2 (hash)	Update-1
3	ISP-2	Reg ID-1 (hash)	First registration
4	ISP-2	Reg ID-1 (hash)	Update-1
5	ISP-1	Reg ID-3 (hash)	Update-2

Figure 9. Registration table structure for the proposed Blockchain Based Caller-ID Authentication (BBCA) mechanism.

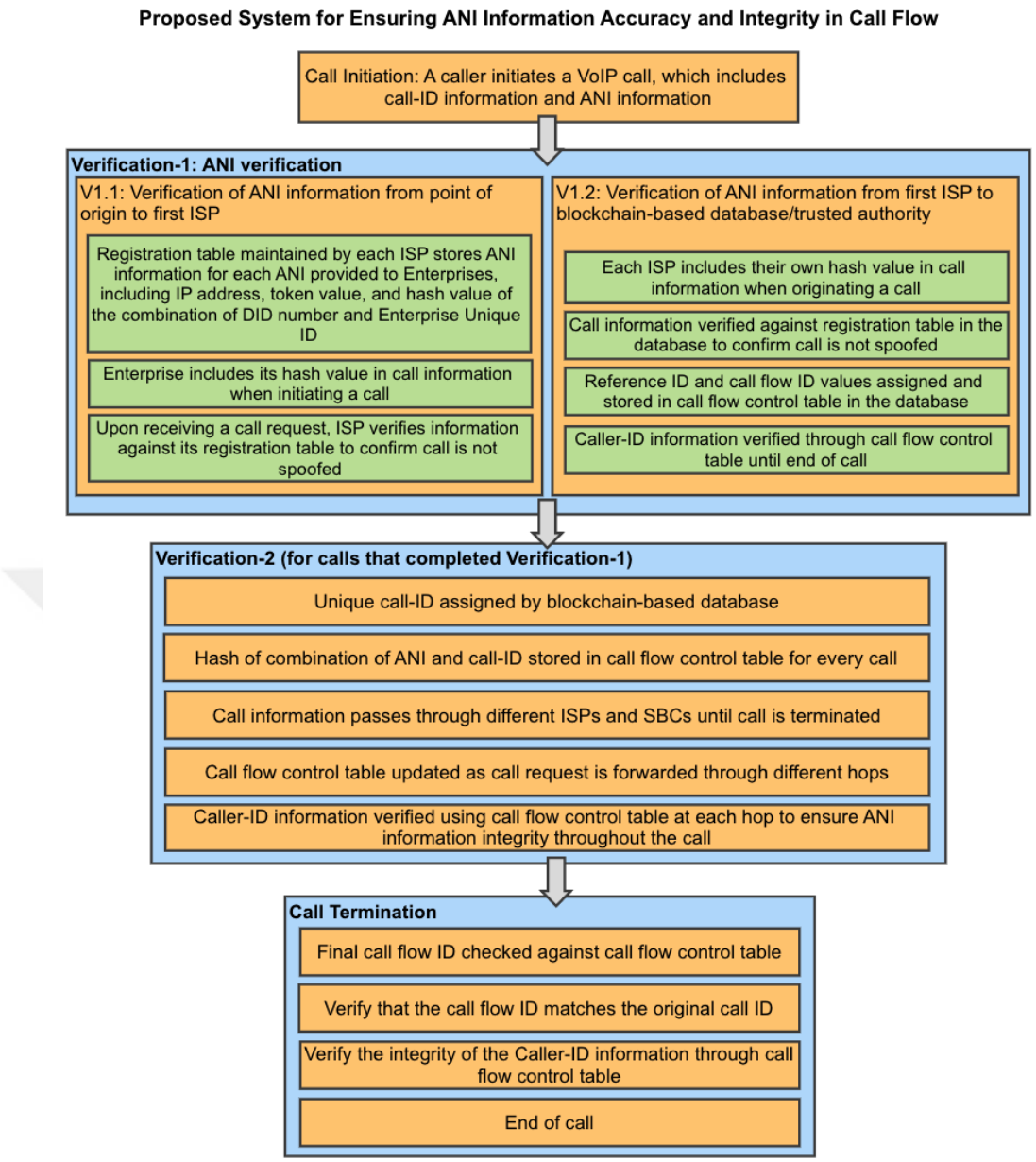

Figure 10. Flow diagram of ANI verification process for VoIP calls using a blockchain-based database and trusted authorities.

Our proposed solution for caller-ID spoofing prevention uses a modified version of the Practical Byzantine Fault Tolerance (PBFT) algorithm as the consensus algorithm. PBFT is a consensus algorithm that ensures all nodes in a distributed system agree on a common state, even in the presence of some faulty or malicious nodes. PBFT is known for its high performance, low latency, and tolerance to a large number of faulty nodes. In our modification, we implement a two-phase commit protocol where a small subset of nodes called "verifiers" are responsible for quickly reaching a consensus on the validity of a caller-ID. The selection of verifiers is based on their reputation and past performance in the network, similar to the blockchain consensus

mechanisms used in. (Ferrag & Maglaras, 2020) (Yang, Jia, Su, Wu, & Qin, 2022) (Wang, et al., 2019) (Cai, 2020) (Vishwakarma, Nahar, & Das, 2022) (Meshcheryakov, Melman, Evsutin, Morozov, & Koucheryavy, 2021) (Saha, et al., 2021). This modification allows for low latency and real-time performance, which is critical for voice communication. The use of PBFT allows for a transparent, decentralized, and distributed solution that reduces the risk of hacking and data tampering. It eliminates the need for costly encryption and decryption operations, resulting in less computational load and lower delay, and thus helps meet the constraints on the real-time nature of voice communication and its sensitivity to Quality of Service (QoS) parameters.

In our blockchain-based caller-ID authentication mechanism, described in *Figure 7*, the Registration and Call Flow Control tables are kept in the blockchain database located in the cloud. Only the ISPs that are registered to this database are allowed to write to it, but everyone can read from it. Each ISP has a unique ID value, named *ISP Unique ID*, that is assigned to it. Each organization that receives voice service from an ISP has a unique ID value, named *Enterprise Unique ID*, that is assigned to it.

Each ISP registers to the Registration Table using a Token value and its *ISP Unique ID*. ISPs renew their registrations periodically. The registration table logic is implemented similarly for sub-parties served by ISPs. Each ISP provides its enterprise clients with an ANI number or a group of ANI numbers based on the client's needs. A SIP client is registered in the Registration Table in the ISP with its registered IP address, ANI information, the hash of its Direct Inward Dialing (DID) number, and its *Enterprise Unique ID*. This information is updated whenever there is any change. When a VoIP call is initiated, the call-ID information along with this recorded information is stored in the Call Flow Control Table in the blockchain database, as shown in *Figure 7*. This information is kept in this table until the call is terminated. The ISP, enterprise or user information from which the call originated can be checked from the blockchain database at any time during the call flow. Hence, one can verify if the caller-ID is forged, hidden, or altered. Exemplary contents for the Call Flow Control and Registration tables are given with *Figure 8.* Call flow control table structure for the proposed Blockchain Based Caller-ID Authentication (BBCA) mechanism.and *Figure 9.* Registration table structure for the proposed Blockchain Based Caller-ID Authentication (BBCA) mechanism.respectively. By using a

blockchain-based consensus algorithm, our proposed solution can handle call flows under many different conditions. Additionally, the use of a reputation-based selection of verifiers allows for increased security and resilience against potential malicious actors in the network.

An example of the use of this verification method is to send a certain verification token to the receiving end of the call to show whether the call is trustworthy or not. This verification mark can be a predefined sound recording or a certain signal tone, or it can be verification information that will be displayed on the phone screen if this is used on a mobile phone.

In our proposed system, we employ a two-step verification process to ensure the accuracy and integrity of ANI information throughout the entire call flow, as described in *Figure 7*.

The first step, Verification-1, is divided into two sub-stages:

- V1.1 - Verifying the accuracy of the ANI information from the point of origin until it reaches the Internet via the first ISP.
- V1.2 - Verifying the accuracy of the ANI information from the first ISP until it reaches the blockchain-based database/trusted authority.

In V1.1, as depicted in *Figure 7*, each VoIP service provider, referred to as an ISP, is assigned an *ISP Unique ID*. Each ISP customer, referred to as an Enterprise, is assigned an *Enterprise Unique ID*. Each ISP provides its enterprise clients with one or more ANI numbers based on their needs. The registration table, maintained by each ISP, stores the ANI information for each ANI provided to the Enterprises, along with the IP address, a token value and the hash value of the combination of the DID number and *Enterprise Unique ID*. Each Enterprise is aware of its own hash value and includes it in the call information when initiating a call. Upon receiving a call request to be sent over the Internet, the ISP verifies the information against its registration table to confirm that the call is not spoofed.

In V1.2, our solution employs a low-latency consensus algorithm and a blockchain-based database that all ISPs can access in near real-time. Only registered ISPs are permitted to write to this database. Each ISP is assigned an *ISP Unique ID*, and for each Enterprise, the *ISP Unique ID*, a token value, and the hash value calculated from the combination of ANI and *Enterprise Unique ID* are stored in the registration table in the blockchain-based database. Each row in the registration table

has a unique reference ID. Each ISP is aware of its own hash values in the registration table and includes the corresponding hash value in the call information when a call originates from its network. For each call request sent over the Internet, the call information is verified against the registration table to confirm that the call is not spoofed, and the reference ID and call flow ID values are assigned and stored in the call flow control table in the blockchain-based database. The verification of the caller-ID information is carried out through this table until the end of the call.

The second step, Verification-2, is used for calls that have completed Verification-1. A unique call-ID is assigned by the blockchain-based database and the hash of the combination of ANI and call-ID is stored in the call flow control table for every call, as shown in *Figure 7*. This information passes through different ISPs and SBCs until the call is terminated. The originating information of the call may change as it passes through different ISPs and SBCs. The information in the call flow control table is updated as the call request is forwarded through different hops. The caller-ID is verified using the call flow table in the blockchain-based database at each hop, ensuring the integrity of the ANI information throughout the call.

To ensure the scalability and robustness of our proposed solution, we have employed a low-latency consensus algorithm for maintaining the blockchain-based database. The consensus algorithm ensures that all registered ISPs have a copy of the same database and that any changes made to the database are validated and agreed upon by all registered ISPs. This ensures that the database remains tamper-proof and that any malicious attempts to alter the caller-ID information are immediately detected and rejected.

In order to address scenarios in which caller-ID information may need to change frequently, our proposed system includes a mechanism for initiating a renewal of ISP registration every time the caller-ID information is updated. This approach ensures that our solution is not affected by situations such as the use of an IP-PBX at the end-user level, the use of a VPN at the end-user level, or instances in which roaming causes the caller-ID information to fluctuate between ISPs. By implementing this feature, we aim to ensure that our proposed solution remains effective and robust in dealing with these unusual scenarios.

Figure 10. Flow diagram of ANI verification process for VoIP calls using a blockchain-based database and trusted authorities.shows the steps involved in verifying the authenticity of the ANI information for VoIP calls using a combination

of a blockchain-based database and trusted authorities, which are third-party organizations or entities that are trusted to verify and validate the ANI information. The verification process consists of three main phases: V1.1, V1.2, and Verification-2, which together ensure that the ANI information remains intact and untampered throughout the call. In the V1.1 phase, the ANI information is verified from the point of origin to the first ISP by checking the hash values stored in a registration table. In the V1.2 phase, the ANI information is verified from the first ISP to the blockchain-based database by checking the hash values stored in the registration table in the database. Finally, in the Verification-2 phase, the ANI information is verified throughout the call by assigning unique call IDs and storing hash values in a call flow control table in the database. At the end of the call, the final call flow ID is checked against the call flow control table to ensure it matches the original call ID, and the caller-ID information is verified to ensure it has not been tampered with during the call.

4.2.2 Security features. In addition to protecting against caller-ID spoofing attacks, the proposed system includes several other security features to protect against other types of attacks such as denial of service and man-in-the-middle attacks. The system is designed to be highly resilient to these types of attacks by incorporating a number of different security measures.

One key security feature of the proposed system is its use of a low-latency consensus algorithm. This algorithm ensures that all ISPs have access to the blockchain database in almost real-time, making it difficult for an attacker to disrupt the system by overwhelming it with a large number of requests. Additionally, the system only allows registered ISPs to write to the blockchain database, further reducing the risk of a denial-of-service attack (Chen, et al., 2021) (Ferrag & Maglaras, 2020).

The proposed system also includes a number of measures to protect against man-in-the-middle attacks. For example, the system uses a unique call ID that is assigned by the blockchain database, which is used to verify the integrity of the ANI information during the call flow. Additionally, the system uses a combination of the ANI and the unique call ID to verify the caller-ID information at each hop, further reducing the risk of a man-in-the-middle attack (Chen, et al., 2021) (Ferrag & Maglaras, 2020).

In order to ensure the integrity of the system, the proposed system also includes a number of other security features such as the use of a token value and the hash value of the combination of the ANI and Enterprise Unique ID. These features, along with the other security measures, ensure that the proposed system is highly resilient to a variety of different types of attacks (Okoye & Kim, 2022) (Fan, et al., 2019).

It should be noted that the proposed system is not completely immune to all types of attacks, and there may still be some vulnerabilities that need to be addressed in future research. However, the proposed system is designed to be highly robust and resilient to a wide range of different types of attacks, making it a highly effective defense against caller-ID spoofing attacks (Wang & Wang, 2020) (Pourvahab & Ekbatanifard, 2019) (Kfoury, Gomez, Crichigno, Bou-Harb, & Khoury, 2019).

Chapter 5

Discussions and Conclusions

5.1 Limitations and Future Work

Our proposed solution holds considerable potential for mitigating caller-ID spoofing attacks effectively in real time. Nevertheless, several areas still require further research and certain issues need resolution before a successful large-scale deployment can be realized.

Subsequent investigations are imperative to fully assess the scalability and performance of our proposed consensus algorithm within real-world settings. This includes exploring the solution's capacity to handle complex scenarios such as call forwarding and teleconference calls. It also necessitates the exploration of alternative consensus methods, as indicated in (Li, Feng, Zhang, Xu, & Imran, 2021) (Abishu, et al., 2022) (Wang, et al., 2021) (Zhang, et al., 2022). These alternatives could potentially enhance the system's overall efficiency and security.

The proposed solution's integration with existing standards and regulations, coupled with the duration required for telecom vendors to comply with new specifications, warrants evaluation. This step is crucial to ascertain the solution's feasibility and timeline for deployment. In support of this, an RFC study should be conducted to update protocol specifications crucial for implementing authentication and call-control operations. The compliance of telecom vendors to these updated RFC specifications at server, client, and network levels is critical, and therefore necessary updates should be made to their products.

Regulatory compliance remains a crucial factor in the successful deployment of our proposed solution. Therefore, service providers need to demonstrate compliance and integrate identity verification processes in their operations. This includes call centers, public services, and financial organizations. To facilitate effective system administration, these regulations should be collaboratively defined by service providers under an alliance agreement. Future research should focus on the feasibility of implementing these regulations and the time required for service providers to demonstrate compliance.

In parallel to technical solutions, the necessity for robust detection and prevention methods is evident. Future research should delve deeper into this area, emphasizing the development of effective mechanisms. Utilization of advanced technologies, such as machine learning, could significantly enhance the detection accuracy of spoofed calls. Alongside, stricter policies and regulations could deter the misuse of spoofed caller-ID information. Additionally, a comprehensive evaluation of the effectiveness of our proposed solution along with the existing Caller-ID spoofing prevention measures across various networks, call centers, and differing levels of social engineering complexity will shed more light on the practical implications of these strategies.

In summary, while our proposed solution marks a promising stride towards understanding and mitigating Caller-ID spoofing attacks, the pressing need for extensive research, particularly around robust detection and prevention methods, remains.

5.2 Conclusion

This research provides an in-depth examination of Caller-ID spoofing attacks and their implications, with a significant emphasis on the role of social engineering in these deceptive strategies. We thoroughly reviewed existing solutions to caller-ID spoofing from both academic and standard perspectives, highlighted their limitations, and proposed an innovative, blockchain-based defense mechanism. This solution leverages blockchain technology to create an immutable record for each call and its origin, providing a secure and decentralized method for managing and verifying caller-ID information.

Our study further illustrated a live financial call center scenario where the Caller-ID was used as a form of authentication, revealing the severe threat posed by spoofed customers. This novel contribution to the existing literature demonstrated the feasibility of such attacks and evaluated their associated risks, exposing a substantial vulnerability in the current telecommunications framework.

Our experimental findings underscored this significant exposure. We achieved an 84% success rate in the first scenario, where we made a call that appeared to be from a valid customer to a real financial call center and successfully changed the telephone banking password. The second scenario yielded a 76% success rate, where the call seemed to come from a valid financial call center number contacting a real customer.

The inability of five different service providers, including three GSM operators, one land-line operator, and one VoIP ISP, to effectively detect and prevent these attacks highlighted a significant deficiency in the current systems. These findings signify a glaring need for further research and development in the area of caller-ID spoofing detection and prevention.

While the failures of spoofed calls cannot always be attributed to the service providers' effective detection measures, they emphasize the complexity of the issue. Failures could occur due to stringent regulations in certain countries or technical issues like packet loss, delay, or timeouts, showcasing the multifaceted challenge of combating Caller-ID spoofing.

In conclusion, our study underlines the critical need to address these shortcomings, suggesting potential future research directions for mitigating the risks

associated with Caller-ID spoofing attacks. We aim to foster a safer and more trustworthy telecommunications environment and significantly contribute to the efforts against telecommunications fraud.

5.3 Additional Note

This Ph.D. thesis was won the first prize among 55 theses in the 2nd Cyber Security Thesis Projects Competition held by the Turkey Cyber Security Cluster, Turkish Defense Industry Presidency and Turkish Republic Presidency Digital Transformation Office in December in 2020.

REFERENCES

Abishu, H. N., Seid, A. M., Yacob, Y. H., Ayall, T., Sun, G., & Liu, G. (2022, January). Consensus Mechanism for Blockchain-Enabled Vehicle-to-Vehicle Energy Trading in the Internet of Electric Vehicles. *IEEE Transactions on Vehicular Technology, 71*(1), 946-960. https://doi.org/10.1109/TVT.2021.3129828

Acker, R., Plies, A., Massoth, M., Mayer, R. S., & Wiens, T. (2013). Mobile Call Authentication using Near Field Communication-based Smart Cards for Proof of Identity towards a Company. *International Conference on Advances in Mobile Computing & Multimedia (MoMM '13), Association for Computing Machinery* (pp. 244-248). New York: ACM.

ATIS Technical Report on a Framework for Display of Verified Caller-ID. (2018, May). Retrieved April 2019, from access.atis.org/: https://access.atis.org/apps/group_public/download.php/40779/ATIS-1000081.pdf

Azad, M., Bag, S., Perera, C., Barhamgi, M., & Hao, F. (2020, May). Authentic Caller: Self-Enforcing Authentication in a Next-Generation Network. *IEEE Transactions on Industrial Informatics, 16*(5), 3606-3615. https://doi.org/10.1109/TII.2019.2941724

Bhasker, D. (2019, Mart 4-8). *RSA Conferance 2019: STIR SHAKE'N SIP to Stop Robocalling.* Retrieved May 2020, from published-prd.lanyonevents.com: https://published-prd.lanyonevents.com/published/rsaus19/sessionsFiles/14182/STR-F01-STIR-SHAKE%E2%80%99N-SIP-to-Stop-Robocalling.pdf

Cai, Z. (2020). Usage of Deep Learning and Blockchain in Compilation and Copyright Protection of Digital Music. *IEEE Access, 8*, 164144-164154. https://doi.org/10.1109/ACCESS.2020.3021523

Chen, T.-H., Yeh, H.-L., Liu, P.-C., Hsiang, H.-C., & Shih, W.-K. (2010). A Secured Authentication Protocol for SIP Using Elliptic Curves Cryptography. *Communication and Networking*, 46-55. https://doi.org/10.1007/978-3-642-17587-9_6

Chen, Y., Wang, Y., Wang, Y., Li, M., Dong, G., & Liu, C. (2021). CallChain: Identity Authentication Based on Blockchain for Telephony Networks. *2021 IEEE 24th*

International Conference on Computer Supported Cooperative Work in Design (CSCWD) (pp. 416-421). Dalian, China: IEEE. https://doi.org/10.1109/CSCWD49262.2021.9437650

Chiang, M., & Burger, E. (2018). An affordable solution for authenticated communications for enterprise and personal use. *2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC)* (pp. 810-815). Las Vegas, NV, USA: IEEE. https://doi.org/10.1109/CCWC.2018.8301725

Communications Fraud Control Association. (2019). *CFCA Fraud Loss Survey.* Retrieved from https://cfca.org/wp-content/uploads/2021/02/CFCA-2019-Fraud-Loss-Survey.pdf

Dantu, R., & Kolan, P. (2005). Detecting Spam in VoIP Networks. *SRUTI '05: Steps to Reducing Unwanted Traffic on the Internet Workshop, USENIX Association.* Cambridge, MA, USA: USENIX.

Deng, H., Wang, W., & Peng, C. (2018). CEIVE: Combating Caller ID Spoofing on 4G Mobile Phones Via Callee-Only Inference and Verification. *24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), Association for Computing Machinery* (pp. 369–384). New York: ACM.

Deng, H., Wang, W., & Peng, C. (2018). Combating Caller ID Spoofing on 4G Phones Via CEIVE. *24th Annual International Conference on Mobile Computing and Networking (MobiCom '18), Association for Computing Machinery* (pp. 846-848). New York: ACM.

Durlanik, A., & Soğukpinar, İ. (2005). SIP Authentication Scheme using ECDH. *Engineering and Technology International Journal of Computer and Information Engineering, 8*, 350-353.

E.164. (2016, June 7). Retrieved October 2020, from en.wikipedia.org: https://en.wikipedia.org/wiki/E.164

Fältström, P. (2000, September). RFC 2916: E.164 number and DNS. *IETF*. Retrieved from https://tools.ietf.org/html/rfc2916

Fan, K., Wang, S., Ren, Y., Yan, Z., Li, H., & Yang, Y. (2019, June). Blockchain-Based Secure Time Protection Scheme in IoT. *IEEE Internet of Things Journal, 6*(3), 4971-4679. https://doi.org/10.1109/JIOT.2018.2874222

FCC Proposes Record. (2020). Retrieved May 15, 2022, from Federal Commnications Commission: https://www.fcc.gov/document/fcc-proposes-record

FCC Proposes Record 225 Million Fine 1 Billion Spoofed Robocalls. (2020). Retrieved May 29, 2022, from Federal Communication Commision: https://www.fcc.gov/document/fcc-proposes-record-225-million-fine-1-billion-spoofed-robocalls

Ferrag, M. A., & Maglaras, L. (2020, November). DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids. *IEEE Transactions on Engineering Management, 67*(4), 1285-1297. https://doi.org/10.1109/TEM.2019.2922936

Gupta, P., Srinivasan, B., Balasubramaniyan, V., & Ahamad, M. (2015). Phoneybot: Data-driven Understanding of Telephony Threats. *NDSS 2015.* San Diego, CA.

Hou, D., Han, H., & Novak, E. (2020). TAES: Two-factor Authentication with End-to-End Security against VoIP Phishing. *2020 IEEE/ACM Symposium on Edge Computing (SEC)* (pp. 340-345). San Jose, CA, USA: IEEE. https://doi.org/10.1109/SEC50012.2020.00049

How to Stop Unwanted Calls. (2020). Retrieved June 16, 2022, from FTC Consumer Advice: https://www.consumer.ftc.gov/features/how-stop-unwanted-calls

https://wiki.asterisk.org/. (2020). Retrieved from Wikipedia: https://wiki.asterisk.org/wiki/display/AST/Home

https://www.consumer.ftc.gov/blog/2017/10/apps-stop. (2021, October 10). Retrieved from Federal Trade Commission Consumer Advice: https://www.consumer.ftc.gov/blog/2017/10/apps-stop

Jennings, C., Peterson, J., & Watson, M. (2002, November). RFC 3325: Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks. *IETF*. Retrieved from https://tools.ietf.org/html/rfc3325

Kara, M., Şanliöz, Ş. G., & Merzeh, H. R. (2021). Blockchain Based Mutual Authentication for VoIP Applications with Biometric Signatures. *2021 6th International Conference on Computer Science and Engineering (UBMK)* (pp. 133-138). Ankara, Turkey: IEEE. https://doi.org/10.1109/UBMK52708.2021.9558972

Kfoury, E. F., Gomez, J., Crichigno, J., Bou-Harb, E., & Khoury, D. (2019). Decentralized Distribution of PCP Mappings Over Blockchain for End-to-End Secure Direct Communications. *IEEE Access*, 110159-110173. https://doi.org/10.1109/ACCESS.2019.2934049

Kilinc, H., & Yanik, T. (2014). A survey of SIP authentication and key agreement schemes. *The IEEE Communications Surveys & Tutorials, 16*(2), 1005-1023.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation, 48*(177), 203-209.

Koilada, D. (2019, September). Strategic Spam Call Control and Fraud Management: Transforming Global Communications. *IEEE Engineering Management Review, 47*(3), 65-71. https://doi.org/10.1109/EMR.2019.2924635

Kurdi, R., Hersi, F., Bahagari, S., Qaisar, S., & Subasi, A. (2017). A mobile fingerprint authentication in Saudi Arabian call centers. *2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA)* (pp. 1-4). Ras Al Khaimah, United Arab Emirates: IEEE. https://doi.org/10.1109/ICECTA.2017.8252000

Li, H., Xu, X., Liu, C., Ren, T., Wu, K., Cao, X., . . . Song, D. (2018). A Machine Learning Approach to Prevent Malicious Calls Over Telephony Networks. *2018 IEEE Symposium on Security and Privacy.* San Francisco, CA, USA: IEEE.

Li, J., Faria, F., Chen, J., & Liang, D. (2017). A Mechanism to Authenticate Caller ID. In Á. Rocha, A. M. Correia, H. Adeli, L. P. Reis, S. Costanzo, & S. Cham (Ed.), *Recent Advances in Information Systems and Technologies* (Vol. 570). Advances in Intelligent Systems and Computing.

Li, W., Feng, C., Zhang, L., Xu, H., & Imran, M. A. (2021, May 1). A Scalable Multi-Layer PBFT Consensus for Blockchain. *IEEE Transactions on Parallel and Distributed Systems, 32*(5), 1146-1160. https://doi.org/10.1109/TPDS.2020.3042392

Lu, Y., Hsiao, H.-Y., Li, C.-Y., Hsieh, Y.-C., Chou, P.-Y., Li, Y.-Y., . . . Tu, G.-H. (2022). Insecurity of Operational IMS Call Systems: Vulnerabilities, Attacks, and Countermeasures. *IEEE/ACM Transactions on Networking*. https://doi.org/10.1109/TNET.2022.3205183

McEachern, J., & Burger, E. (2019, December). How to shut down robocallers: The STIR/SHAKEN protocol will stop scammers from exploiting a caller ID loophole. *IEEE Spectrum, 56*(12), 46-52. https://doi.org/10.1109/MSPEC.2019.8913833

Meshcheryakov, Y., Melman, A., Evsutin, O., Morozov, V., & Koucheryavy, Y. (2021). On Performance of PBFT Blockchain Consensus Algorithm for IoT-

Applications With Constrained Devices. *IEEE Access, 9,* 80559-80570. https://doi.org/10.1109/ACCESS.2021.3085405

Miller, V. S. (1986). Use of Elliptic Curves in Cryptography. *Advances in Cryptology - CRYPTO '85 Proceedings, Springer Berlin Heidelberg* (pp. 417-426). Springer.

Mr.SIP: SIP-Based Audit and Attack Tool. (2019, November). Retrieved November 2020, from github.com: https://github.com/meliht/mr.sip

Mustafa, H., Xu, W., Sadeghi, A.-R., & Schulz, S. (2018, May-June 1). End-to-End Detection of Caller-ID Spoofing Attacks. *IEEE Transactions on Dependable and Secure Computing, 15*(3), 423-436. https://doi.org/10.1109/TDSC.2016.2580509

Okoye, M. O., & Kim, H.-M. (2022). Optimized User-Friendly Transaction Time Management in the Blockchain Distributed Energy Market. *IEEE Access, 10,* 34731-34742. https://doi.org/10.1109/ACCESS.2022.3162214

OpenSIPIt '01 – Testing the Trending SIP Security Enhancements. (2021, April). Retrieved August 2021, from blog.opensips.org: https://blog.opensips.org/2021/04/20/opensipit-01-testing-the-trending-sip-security-enhancements/

Pandit, S., Liu, J., Perdisci, R., & Ahamad, M. (2021). Applying Deep Learning to Combat Mass Robocalls. *2021 IEEE Security and Privacy Workshops (SPW)* (pp. 63-70). San Francisco, CA, USA: IEEE. https://doi.org/10.1109/SPW53761.2021.00018

Peterson, J. (2014, October). RFC 7375: Secure Telephone Identity Threat Model. Retrieved from https://tools.ietf.org/html/rfc7375

Peterson, J., & Jennings, C. (2006, August). RFC 4474: Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP). *IETF*. Retrieved from https://tools.ietf.org/html/rfc4474

Peterson, J., & Turner, S. (2018, February). RFC 8226: Secure Telephone Identity Credentials: Certificates. *IETF*. Retrieved from https://tools.ietf.org/html/rfc8226

Peterson, J., Jennings, C., Rescorla, E., & Wendt, C. (2018, February). RFC 8224: Authenticated Identity Management in the Session Initiation Protocol (SIP). *IETF*. Retrieved from https://tools.ietf.org/html/rfc8224

Peterson, J., Schulzrinne, H., & Tschofenig, H. (2014, September). RFC 7340: Secure Telephone Identity Problem Statement and Requirements. *IETF*. Retrieved from https://tools.ietf.org/html/rfc7340

Pourvahab, M., & Ekbatanifard, G. (2019). An Efficient Forensics Architecture in Software-Defined Networking-IoT Using Blockchain Technology. *IEEE Access*, 99573-99588. https://doi.org/10.1109/ACCESS.2019.2930345

Putra, D., Sadikin, M., & Windarta, S. (2017). S-Mbank: Secure mobile banking authentication scheme using signcryption, pair-based text authentication, and contactless smart card. *2017 15th QiR: International Symposium on Electrical and Computer Engineering* (pp. 230-234). Nusa Dua, Bali, Indonesia: IEEE. https://doi.org/10.1109/QIR.2017.8168487

Reaves, B., Blue, L., & Traynor, P. (2016). AuthLoop: End-to- End Cryptographic Authentication for Telephony over Voice Channels. *25th USENIX Security Symposium.* Austin, TX: USENIX.

Reaves, B., Blue, L., Abdullah, H., Vargas, L., Traynor, P., & Shrimpton, T. (2017). AuthentiCall: Efficient Identity and Content Authentication for Phone Calls. *26th USENIX Security Symposium.* Vancouver, BC: USENIX.

Rebahi, Y. (2008). Performance Analysis Of Identity Management In The Session Initiation Protocol (SIP). *2008 IEEE/ACS International Conference on Computer Systems and Applications* (pp. 711-717). Doha, Qatar: IEEE.

Saha, R., Kumar, G., Geetha, G., Hoon-Kim, T., Alazab, M., Thomas, R., . . . Rodrigues, J. J. (2021, August). The Blockchain Solution for the Security of Internet of Energy and Electric Vehicle Interface. *IEEE Transactions on Vehicular Technology*, *70*(8), 7495-7508. https://doi.org/10.1109/TVT.2021.3094907

Sahin, M., Francillon, A., Gupta, P., & Ahamad, M. (2017). SoK: Fraud in Telephony Networks. *2017 IEEE European Symposium on Security and Privacy (EuroS&P)* (pp. 235-250). Paris, France: IEEE. https://doi.org/10.1109/EuroSP.2017.40

Sechulzrinne, H., Panagia, A., Cox, P., & Balasubramaniyan, V. A. (2012, October). *Caller-ID Spoofing and Call Authentication Technology*. Retrieved May 1, 2022, from Federal Trade Commission: https://www.ftc.gov

SecureLogix. (2017, May 2020). SecureLogix Annual State of Voice Report. USA. Retrieved April 15, 2022, from https://securelogix.com/wp-content/uploads/2019/06

Sheoran, A., Fahmy, S., Peng, C., & Modi, N. (2019). Nascent: Tackling Caller-ID Spoofing in 4G Networks via Efficient Network-Assisted Validation. *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications* (pp. 676-684). Paris, France: IEEE. https://doi.org/10.1109/INFOCOM.2019.8737567

Signature-based Handling of Asserted information using toKENs (SHAKEN): Governance Model and Certificate Management (ATIS-1000080.v002). (2017, July). Retrieved April 2020, from atis.org: https://www.atis.org/resources/signature-based-handling-of-asserted-information-using-tokens-shaken-governance-model-and-certificate-management-atis-1000080-v002/

Spoofcard. (2019, November). Retrieved November 17, 2021, from SpoofCard: https://www.spoofcard.com/

Spoofing. (2020). Retrieved May 2, 2022, from Federal Communications Commission: https://www.fcc.gov/consumers/guides/spoofing

Stanek, J., & Kencl, L. (2011). SIPp-DD: SIP DDoS Flood-Attack Simulation Tool. *2011 Proceedings of 20th International Conference on Computer Communications and Networks (ICCCN)* (pp. 1-7). Lahaina, HI, USA: IEEE. https://doi.org/10.1109/1-7

Stefanović, T., & Ghilezan, S. (2020). Preserving Privacy in Caller ID Applications. In M. Friedewald, S. Schiffner, S. Krenn, & C. Springer (Ed.), *Privacy and Identity Management* (Vol. 619). IFIP Advances in Information and Communication Technology.

Sukma, N., & Chokngamwong, R. (2017). One-time key Issuing for Verification and Detecting Caller-ID Spoofing Attacks. *14th International Joint Conference on Computer Science and Software Engineering (JCSSE)* (pp. 1-4). NakhonSiThammarat, Thailand: IEEE. https://doi.org/10.1109/JC-SSE.2017.8025898

Sukma, N., & Chokngamwong, R. (2018). 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) (pp. 1-6). Nakhonpathom, Thailand: IEEE. https://doi.org/10.1109/JCSSE.2018.8457341

Suthar, D., & Rughani, P. H. (2020). A Comprehensive Study of VoIP Security. *2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)* (pp. 812-817). Greater Noida, India: IEEE. https://doi.org/10.1109/ICAC- CCN51052.2020.9362943

Tas, İ. M., Uğurdoğan, B., & Taş, H. (2015). Integrating VoIP/UC Security into the Holistic Information Security Planning. (pp. 771-792). Malatya, Turkiye: Signal Processing and Communications Applications Conference SIU.

Tas, I. M., Unsalver, B. G., & Baktir, S. (2015). Our Proposed SIP-Based Distributed Reflection Denial of Service (DRDoS) Attacks & Effective Defense Mechanism. *ICR 2015.* Tallin.

Tas, I. M., Unsalver, B. G., & Baktir, S. (2020). A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism. *IEEE Access*, 112574-112584. https://doi.org/10.1109/ACCESS.2020.3001688

Tas, I., & Kucuk, K. (2020). DEF CON 28 Main Stage. *Practical VoIP-UC Hacking Using Mr.SIP-SIP-Based Audit & Attack Tool*. Las Vegas, Nevada, USA: DEF CON. Retrieved from https://media.defcon.org/DEF CON 28/

Tas, I., Ugurdogan, B., & Baktir, S. (2016). Novel session initiation protocol-based distributed denial-of-service attacks and effective defense strategies. *Computers & Security, 63*, 29-44. https://doi.org/10.1016/j.cose.2016.08.007

Taş, İ. M., & Baktir, S. (2023). A Novel Approach for Efficient Mitigation against the SIP-Based DRDoS Attack. *Applied Sciences, 13*(1684). https://doi.org/doi.org/10.3390/app13031864

Taş, İ. M., Özbicerikli, O., Çağal, U., Taşkin, E., & Taş, H. (2014). Anatomy of SIP registration removal attack and defense strategies. *2014 22nd Signal Processing and Communications Applications Conference (SIU)* (pp. 1600-1603). Trabzon, Turkiye: IEEE. https://doi.org/10.1109/SIU.2014.6830550

Tu, H., Doupé, A., Zhao, Z., & Ahn, G.-J. (2016). SoK: Everyone Hates Robocalls: A Survey of Techniques against Telephone Spam. *2016 IEEE Symposium on Security and Privacy.* San Jose, CA, USA: IEEE. https://doi.org/10.1109/SP.2016.27

Tu, H., Doupé, A., Zhao, Z., & Ahn, G.-J. (2016). Toward authenticated caller-ID transmission: The need for a standardized authentication scheme in Q.731.3 calling line identification presentation. *2016 ITU Kaleidoscope: ICTs for a Sustainable World (ITU WT)* (pp. 1-8). Bangkok, Thailand: IEEE. https://doi.org/10.1109/ITU- WT.2016.7805728

Tu, H., Doupé, A., Zhao, Z., & Ahn, G.-J. (2017, September). Toward Standardization of Authenticated Caller-ID Transmission. *IEEE Communications Standards Magazine, 1*(3), 30-36. https://doi.org/10.1109/MCOMSTD.2017.1700019

Tu, H., Doupè, A., Zhao, Z., & Ahn, G.-J. (2019). Users Really Do Answer Telephone Scams. Santa Clara: USENIX.

Unwanted Robocalls : Challenges and Solutions. (2020, February 6). Retrieved January 2021, from gsma.com: https://www.gsma.com/northamerica/wp-content/uploads/2020/02/GSMA_Robocall-White-Paper.pdf

Vishwakarma, L., Nahar, A., & Das, D. (2022, June). LBSV: Lightweight Blockchain Security Protocol for Secure Storage and Communication in SDN-Enabled IoV. *IEEE Transactions on Vehicular Technology, 71*(6), 5983-5994. https://doi.org/10.1109/TVT.2022.3163960

Wang, L.-e., Bai, Y., Jiang, Q., Leung, V. C., Cai, W., & Li, X. (2021, April-June 1). Beh-Raft-Chain: A Behavior-Based Fast Blockchain Protocol for Complex Networks. *IEEE Transactions on Network Science and Engineering , 8*(2), 1154-1166. https://doi.org/10.1109/TNSE.2020.2984490

Wang, Y., Cai, S., Lin, C., Chen, Z., Wang, T., Gao, Z., & Zhou, C. (2019). Study of Blockchains's Consensus Mechanism Based on Credit. *IEEE Access, 7*, 10224-10231. https://doi.org/10.1109/ACCESS.2019.2891065

Wang, Z., & Wang, Y. (2020). Global Synchronization of Pulse-Coupled Oscillator Networks Under Byzantine Attacks. *IEEE Transactions on Signal Processing , 68*, 3158-3168. https://doi.org/10.1109/TSP.2020.2993643

Wendt, C., & Barnes, M. (2019, May). RFC 8588: Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN). *IETF*. Retrieved from https://tools.ietf.org/html/rfc8588

Wendt, C., & Peterson, J. (2018, February). RFC 8225: PASSporT: Personal Assertion Token. *IETF*. Retrieved from https://tools.ietf.org/html/rfc8225

Yang, J., Jia, Z., Su, R., Wu, X., & Qin, J. (2022). Improved Fault-Tolerant Consensus Based on the PBFT Algorithm. *IEEE Access, 10*, 30274-32083. https://doi.org/10.1109/ACCESS.2022.3153701

Zhang, R., Wang, X., Yang, X., & Jiang, X. (2007). Billing Attacks on SIP-Based VoIP Systems. *Billing Attacks on SIP-Based VoIP Systems.* Santa Clara, CA, USA: USENIX.

Zhang, W., Sun, G., Lu, Q., Ning, H., Zhang, P., & Yang, S. (2022, June 1). A Trustworthy Safety Inspection Framework Using Performance-Security Balanced Blockchain. *IEEE Internet of Things Journal, 9*(11), 8178-8190. https://doi.org/10.1109/JIOT.2021.3121512