International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Leveraging Blockchain Technology in NASCENT Framework to Mitigate Caller ID Spoofing Challenges

Rajnish Kumar Gupta[1], Pradeep Chouksey, Parveen Sadotra and Mayank Chopra

[1]Department of Computer Science & Informatics, Central University of Himachal Pradesh, Shahpur, Himachal Pradesh, India
rajnishkumargupta331@gmail.com

ABSTRACT

The factors that identify threats and vulnerabilities in terms of security incidents associated with the caller ID spoofing in Voice over Internet Protocol and Private Branch Exchange cloning systems are examined in this literature survey. This study explores novel verification techniques to prove the identities of callers while minimizing the need for major infrastructures changes. Innovations such as CallerDec, NASCENT, and iVisher offer potential methods of caller ID verification. These systems are able to detect the vast majority of spoofed calls via callback sessions. It implements low-latency consensus and ANI verification on a blockchain that is resistant to the use of VPNs, roaming, and advanced spoofing. The research identifies critical gaps in telecommunications security, from the limited ability to integrate Android Voice over Internet Protocol and codec vulnerabilities to weaknesses in network configuration. Introducing the global landscape of caller ID spoofing challenges dynamic due to limited regulatory frameworks.

Keywords: *Authentication, Blockchain, Caller ID, SIP, Spoofing & VolP.*

1. Introduction

1.1. Background of the Study

One such phenomenon, which has become one of the major concerns in today's world of telecommunication, is the caller ID spoofing, which undermines the very premise of calling over identification and threatens to be dangerous for every one and every organization. The technique where the attackers spoof the caller ID and hide their identity is mostly used in fraud such as phishing, scams and impersonation attacks. The utility of target-specific vulnerabilities facing different products is further amplified by rooted Session Initiation Protocol (SIP)-based telephony systems which are increasingly used both in private and enterprise environments to provide attackers with opportunities to exploit weaknesses in telecommunication protocols [1].

Since VolP is a common method of communication in both personal and corporate settings and the systems converge on mobile platforms and apps, the further exploitation of the risk multiplies as VolP exploits and vulnerabilities are exploited further. Even the simplest of spoofing techniques have broken existing measures, like basic caller ID authentication mechanisms. Existing communication technologies have made significant progress, but no commonly established means of verifying caller ID has been broadly deployed and thus little has been done to address the problem [2].

1.2. Problem Statement

Caller ID spoofing is becoming a bigger problem than ever in making secure, trustworthy communications in telephony. Existing detection and prevention systems have limited efficacy due to the following:

Technological Vulnerabilities: Having not put in place comprehensive verification protocols for telecommunication systems to distinguish use of caller ID manipulation for legitimate versus fraudulent purposes, the systems we use today transmit Caller ID anyway [2].

SIP vulnerabilities: VolP application SIP header manipulation and other attacks take place on both the SIP and media streams of the application, which is typically used by such different users (both human and evil) as well as widely adopted in enterprises and ITSPs, until it's torn apart to switch to different solutions [3].

Dynamic Threat Landscape: And as traditional solutions prevent them, as they are supposed to virtually, attack keep on creating new spoofing methods such as low-rate flooding, protocol abuse, etc. [4].

Inconsistency of Implementation and Enforcement of Regulations: Actual regulation is not always enforced uniformly in many regions of the world, leaving these loops for this exploitation to take place [5].

The vulnerabilities lead to fraud, leak of confidential data and user mistrust in telecommunication systems. To address these important problems, we study novel detection and prevention methods in this study [6].

1.3. Research Questions

In VolP and traditional telephony systems what are the limitations of current caller ID spoofing detection and prevention mechanisms [7]?

What can new technologies like machine learning and blockchain add to the accuracy and reliability of caller ID verification [5]?

Which technical and regulatory barriers stand in the way of universally applying a solution to caller ID spoofing [7]?

1.4. Objectives

The primary objectives of this research are:

The NASCENT framework has been proposed as one for the prevention and detection of caller ID spoofing, and as an approach for enhancing the accuracy and security of identity verification in telecommunications through the integration of blockchain technology.

I wanted to design and implement a blockchain based system capable of recording, and verifying, and authenticating caller ID information in real time so as to ensure tamper proof verification of calls while shielding the system from fraud risks related to spoofing.

The effectiveness of the proposed blockchain solution in checking the veracity of the caller ID authentication and blocking the phone spoofing attack in communication networks is examined to evaluate.

In order to analyze the scalability of the blockchain based system on large scale telecommunication infrastructure and to determine the ability of the system to respond to the changing security challenges in the industry.

The objective of promotion of blockchain based caller ID verification as a standard for fraud prevention in global communication networks, as a tool to assess the potential impact of such an approach on telecommunications policies and practices.

2. LITERATURE REVIEW

The TCI (Trusted Caller ID) mechanism trumps the problem of caller id-spoofing, a usual practice to confuse the call receiver, especially in case of VolP and PBX systems. To verify caller IDs, TCI works with an outside organization called the Phone Call Authority (PCA) which helps both identify legitimate calls as well as scam and spoofed calls – ensuring increased security for all. It provides a real-world integration into incumbent telephone networks, only requiring modest upgrades and work to implement, making it practical for step-wise deployment. But it will only work if carriers and users register IDs and embrace PCA system. Even though authentication records are valid for a small number of minutes, the temporal duration reduces the risk of continuing abuse. The system may, however, remain open to a denial-of-service attack if nefarious agents attempt to flood the service with bogus call requests. Also, international variation on the spoofing of caller ID inhibits broad enforcement [1].

In this paper we present a caller ID authentication system NASCENT for next generation network (4G/5G) that can effectively counter caller ID spoofing attacks by utilizing ubiquitous interface and authentication info in 4G/5G networks. NASCENT works in the background at call setup time to give accurate and robust spam detection with limited CI changes. We designed and tested three NASCENT prototypes, achieving low operational overhead along with high detection accuracy. On the other hand, NASCENT could mistakenly identify even legal uses of caller ID spoofing (like privacy features) as having malicious intent, and is very cumbersome to set up in NFV environments. NASCENT could be improved in future research to distinguish between benign and malicious spoofing more effectively, and extended for other voice services such as WiFi calling [2].

Abstract In recent years, caller ID spoofing has become a popular method for an attacker to mislead the call recipient by forging the identifier of the caller; as such it poses a serious threat to our communication system. CallerDec is based on existing telecommunication technology via two means, SMS-based and timing-based implementations, both of which are executed through an Android app. The authors confirmed the system's capabilities in various scenarios and found that it appears to be able to identify spoofed IDs. But some call processing delays along with a requirement for the technology to be employed widely may dilute its effectiveness. Detecting replacement call feature detection, delaying caller dec integration with different phones type in the future work would improve the CallerDec. [3].

In this paper, we describe a solution using blockchain to make caller ID verification in real time by employing a low-latency consensus algorithm as the basis of a VoIP/SIP network that is resilient against caller ID spoofing. The solution has a two-step verification process, doubles down on the integrity and accuracy of ANI making it workable even for roaming or VPN based scenarios. Through the use of a revised version of Practical Byzantine Fault Tolerance (PBFT), it allows for secure end to end validation on a decentralized ledger. Although a promising approach for solving some telecom security validation, more work must be done to prove scalability and performance when applied to complex scenarios such as call forwarding and teleconferencing. Scalability, system integration and regulatory tackling for large-scale deployment will be addressed in future work [4].

In this work, we investigate Caller ID spoofing vulnerabilities and propose a new defense mechanism called CIVE (Callee Inference & Verification) tool which we validate in experiments. One of the promising defense methods for detecting spoofed calls is CIVE, however, all the current defenses including

CIVE are still vulnerable to SS techniques and cannot work well in many situations. Detection and more resilient endpoint defenses are areas for future research that should be pursued. Method: Using Spoofing Attacks to Evaluating CIVE The authors worked in a laboratory to simulate the spoofing attacks, and then evaluate that effectiveness of CIVE under multiple mobiles phone types [5].

In this paper, we provide an overview of recent approaches to detect and prevent Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks against SIP-based VoIP networks. It classifies detection techniques into finite state machine, rules-based, statistically based, and machine learning approach and provides an extensive comparison based on their detection abilities, response time as well as performance. This analysis shows that most of the present approaches fail low-rate flooding and malformed message attacks and are usually conditioned based, meaning they cannot adapt to changing attack patterns. The authors recommend that future research explore adaptive real-time detection strategies incorporating machine learning, and in particular deep learning to improve classification rates as the network environment changes [6].

In this paper we present a caller ID authentication system NASCENT for next generation network (4G/5G) that can effectively counter caller ID spoofing attacks by utilizing ubiquitous interface and authentication info in 4G/5G networks. NASCENT works in the background at call setup time to give accurate and robust spam detection with limited CI changes. We designed and tested three NASCENT prototypes, achieving low operational overhead along with high detection accuracy. On the other hand, NASCENT could mistakenly identify even legal uses of caller ID spoofing (like privacy features) as having malicious intent, and is very cumbersome to set up in NFV environments. NASCENT could be improved in future research to distinguish between benign and malicious spoofing more effectively, and extended for other voice services such as WiFi calling [7].

In this work, we present CallerDec, an end-to-end caller ID validation system for caller ID spoofing detection. CallerDec is designed to be able to deploy as an Android app without modifying system infrastructure, so that CallerDec can operate on existing phone infrastructures. It successfully performed in a number of scenarios, while other unsupported scenarios did have user experience limitations, and the system does not work on all types of network. Next steps will be to test CallerDec in PSTN and VoIP networks and drive adoption to enable the reduction of unsupported cases. CallDec uses a hidden timing channel to conduct verification, and it is evaluated by general usage on Android devices from an experimental perspective [8].

It explores security vulnerabilities in Voice over Internet Protocol (VoIP) systems, including eavesdropping on sensitive communication, unauthorized access to private networks and endpoints, identity spoofing and denial-of-service attacks. And it also highlights typical countermeasures to mitigate these threats. Nevertheless, the paper would benefit from specific empirical data or case studies to complement its theoretAbsstractual elaboration. Our work provides insight to motivate further research towards the development of higher assurance security mechanisms and in particular, real-life implementations that realize VoIP security. The study takes a qualitative approach reviewing secondary sources to discuss different vulnerabilities and mitigations for VoIP systems [9].

In this paper, we present iVisher, a system that can detect vishing calls in VoIP. iVisher authenticates the incoming caller IDs and protects against spoofed IDs that were reported in past calls with minimal call setup delay. The gateway checks the number being announced as caller ID against the actual number making a call, and if they differ, this is an indication of spoofing allowing for real-time detection of it. This will only work if companies using PBX systems do so, and end-users remain vigilant to security alerts. We will explore improving iVisher to detect other types of VoIP-related attacks (e.g., spam messages), and by combining it with existing systems, we can lower maintenance costs in `maintainers' methods. The system was then assessed via simulations that demonstrated its feasibility without having a significant impact on call setup time [10].

Security Analysis of Android’s VoIP Integration at the System Level: Exploring the Protocol Stack, Finding 4 Key Attack Surfaces We present a new methodology for vulnerability assessment that merges on-device Intent/API fuzzing, network-side packet fuzzing and targeted code auditing. Their method revealed a total of eight zero-day vulnerabilities that were verified by Google, with several serious security issues such as caller ID impersonation and remote code execution. The study only targets Android from version 7.0 to 9.0 which ignores the vulnerabilities of the newer versions and focuses on the system-level vulnerability rather than a vulnerability in third-party VoIP apps. Discussion Many of the mitigations for identified vulnerabilities need refinement and future research may take on newer Android versions and other third-party applications [11].

In this paper, we investigate the physical approaches to execution of Voice over Internet Protocol (VoIP) and variables on which call quality depends like codec selection delay as well as bandwidth efficiency. It also provides an overview of several VoIP flipping protocols such as H.323, SIP, MGCP and Megaco/H. The paper speculates about when voice and data networks will converge, but doesn't address the question here. Further, QoS approaches for public internet infrastructure could be studied and VoIP could also be combined with new technologies such as 5G and IoT in future studies to maximize performance and reliability. The paper offers an in-depth review of existing technologies and protocols, along with some technical discussions analyzing previous works and comparing performances to present engineering trade-offs evoked in the implementation of VoIP systems [12].

3. CHALLENGES AND LIMITATION

In this literature review, numerous challenges and limitations of call verification and caller ID spoofing prevention systems are explored. The ability to successfully prevent requires that both users and carriers coalesce, and adopt scalable and reliable systems. However, legacy methods like PCA systems and NASCENT are vulnerable to modern spoofing techniques and are ill suited for the installation in non-supported networks or more advanced attack types such as low-rate flooding or malformed message. Some are effective in limited situations, but new attack types evolve without addressing them as well as legitimate usage such as multiple subscriber IDs being marked as malicious [2].

Beyond this, the deployment of NASCENT in network function virtualization (NFV) environment is also quite complex as it demands excessive configuration. Proposed solutions have little empirical support, studies typically consider a subset of Android versions or traditional telephony environments, and a strong emphasis is placed on the role of big players in traditional telephony, while little is known of the free telephone market (e.g. VolP). The literature, however, lacks comprehensive discussion of regulatory or market implications, and the convergence of voice and data networks is not considered, the focus instead being on technical remedies [2].

4. FUTURE DIRECTION

In this review, we examine Trusted Caller ID (TCI) technologies that allow some improvements to security and user experience without requiring major network changes. Ceive aims to seamlessly merge with 2G, 3G, and 5G networks and provides support for multi-line and non-cellular communication, while future work improves CallerDec and NASCENT for greater network compatibility and faster, more accurate caller ID verification [1].

Our research priorities include speeding up detections, scaling up, and interfacing TCls with existing Session Initiation Protocol (SIP) systems. It is also recommended to enhance accuracy against spoofing by means of dynamic detection strategies, real time monitoring, as well as approaches based on machine learning and especially deep learning. It is suggested that NASCENT be extended to new services such as VolP, internet telephony and WiFi calling and that such distinction is made between legitimate and malicious caller ID use [2].

Future work also includes enhancing VolP security, generalizing CallerDec to other networks and incorporating advanced QoS algorithms for improved public internet infrastructure performance. In future research, we should explore the risks associated with recent Android versions as well as recent third-party VolP apps and what we should do to mitigate these emerging vulnerabilities [4].

5. CONCLUSION

In this literature review, the authors examine the security risks involved in caller ID spoofing and analogous vulnerabilities in VolP and PBX systems. Without making big infrastructure changes such as the ones required for Trusted Caller ID (TCI) systems and other similar "caller ID verification" tools like CEIVE, NASCENT, CallerDec and iVisher, callers can be verified.

Through methods such as callback sessions and third-party verification, these systems verify authentic caller IDs and can high accuracy spot spoofed calls. But caller ID spoofs are subject to limited regulation around the world [2] [3] [10].

Research focuses on the countermeasures that address security threats, especially Distributed Denial of Service (DDoS) against VolP systems deployed based on the protocol such as SIP. In particular, CallerDec and NASCENT were built to increase caller ID verification on Android devices, and within 4G and 5G networks, while iVisher detects in real time spoofing by comparing the caller ID to actual identity [2] [3] [10].

Low latency consensus and Automatic Number Identification (ANI) verification promised by a blockchain based caller ID verification system add to the security emerging technologies. They also want to make these systems more resilient to the use of VPNs, roaming and spoofing. Future work is suggested to continue to improve the accuracy and scalability of detection through more sophisticated machine learning and adaptive security approaches, to counter growing spoofing methods and the issues of VolP security. Furthermore, Android VolP integration, codec selection, and network configurations vulnerabilities indicate that we still have some work to do to get secure, reliable telecommunications [7].

References

[1] H. Mustafa, W. Xu, A .- R. Sadeghi and S. Schulz, "End-to-end detection of caller ID spoofing attacks," IEEE Transactions on Dependable and Secure Computing, vol. 15, p. 423-436, 2016.

[2] A. U. Mentsiev and A. I. Dzhangarov, "VolP security threats," Инженерный вестник Дона, p. 75, 2019.

[3] B. Goode,"Voice over internet protocol (VoIP)," Proceedings of the IEEE, vol. 90, p. 1495-1517,2002.

[4] W. Nazih, W. S. Elkilani, H. Dhahri and T. Abdelkader, "Survey of countering DoS/DDoS attacks on SIP based VolP networks," Electronics, vol. 9, p. 1827, 2020.

[5] I. M. Tas and S. Baktir, "Blockchain-Based Caller-ID Authentication (BBCA): A Novel Solution to Prevent Spoofing Attacks in VolP/SIP Networks," IEEE Access, 2024.

[6] E. He,D. Wu and R. H. Deng, "Understanding Android VolP Security: A System-Level Vulnerability Assessment," in Detection of Intrusions and Malware, and Vulnerability Assessment: 17th International Conference, DIMVA 2020, Lisbon, Portugal, June 24-26, 2020, Proceedings 17, 2020.

[7] J. Li, F. Faria, J. Chen and D. Liang, "A mechanism to authenticate caller ID," in Recent Advances in Information Systems and Technologies: Volume 2 5, 2017.

[8] J. Song, H. Kim and A. Gkelias, "iVisher: Real-time detection of caller ID spoofing," ETRI Journal, vol. 36, p. 865-875, 2014.

[9] A. Sheoran, S. Fahmy, C. Peng and N. Modi, "NASCENT: Tackling caller-ID spoofing in 4G networks via efficient network-assisted validation," in IEEE INFOCOM 2019-IEEE Conference on Computer Communications, 2019.

[10] V. Buriachok, V. Sokolov and M. T. Dini, "ДОСЛІДЖЕННЯ СПУФІНГУ ІДЕНТИФІКАТОРА АБОНЕНТА ПРИ РЕЄСТРАЦІЇ: ВИЯВЛЕННЯ ТА ПРОТИДІЯ," Електронне фахове наукове видання \guillemotleftKi6ep6esneka: oceima, Hayka, mexHika\guillemotright, vol. 3, p. 6-16, 2020.

[11] H. Deng and C. Peng, "Combating caller ID spoofing on 4G phones via CEIVE," in Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, 2018.

[12] H. Mustafa, W. Xu, A. R. Sadeghi and S. Schulz, "You can call but you can't hide: detecting caller id spoofing attacks," in 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2014.