SILENCING THE VOICE IMPOSTERS

Tackling CLI Spoofing in an Interconnected World

Whitepaper

September 2024

GLOBAL CYBERSECURITY FORUM | stc

Foreword

Yasser Alswailem
stc;
Chairman of the Knowledge Community: Safeguarding Future Networks and Emerging Technologies

As our lives become increasingly punctuated by networks, ensuring their integrity becomes increasingly vital for society. Challenges are neither simple to solve, nor is there a quick fix that applies to all cases. In this whitepaper, our Knowledge Community, dedicated to informing best practices for networking and emerging technology, has chosen to isolate and provide solutions to the issue of CLI caller spoofing. We hope our technical solution provides a guide to network professionals globally.

I want to thank all of our contributors for their expert and impassioned contributions to this work. It is only by grouping diverse experience that we can guarantee our interconnected world remains defined by trust and openness.

Contributors

- **Mohammed Yousuf Uddin,** stc
- **Mahesh Sonavane,** stc
- **Islam Swelam,** stc
- **Zaki Alowini,** stc
- **Abdulrazzak Shaikh,** stc
- **Ali A. Alshehri,** stc Academy
- **Ian Keller,** Ericsson
- **Mohamed Darweesh,** ENEA
- **Peter Morgan,** Cellusys

Knowledge Community: Safeguarding Future Networks and Emerging Technologies

In an increasingly interconnected world, the evolution of next generation ICT technologies such as 6G wireless technology has emerged as a powerful catalyst. The profound implications and transformative power of this next wave of ICT technologies demand immediate attention – both to navigate its complexities, safeguard its deployment, and to harness its capabilities for the benefit of society. The knowledge community "Safeguarding the Future Networks & Emerging Technologies" is committed to promoting and safeguarding the current and future day's ICT networks, bringing together a diverse array of expertise from multiple stakeholder groups.

The community welcomes ICT providers, telecom companies, telecom industry players, cybersecurity research organizations, infrastructure operators, reputable think tanks, academia, and all stakeholders with a vested interest in the security of the ICT networks.

Terminology and Abbreviations

List of terms used in the document and their explanation

Abbreviations	Definition
CLI	Caller Line Identification
OB	Outbound Roamer
CAMEL	Customized Applications for Mobile networks Enhanced Logic
IDP	Initial Detection Point
IRSF	International Revenue Share Fraud
PBX	Private Branch Exchange
SIM	Subscriber Identity Module
SS7	Signaling System No. 7
IN	Intelligent Network
CAP	CAMEL Application Part
SCP	Service Control Point
O-CSI	Originating CAMEL Subscription Information
HLR	Home Location Register
HSS	Home Subscriber Server
MSC	Mobile Switching Center
VPMN	Visited Public Mobile Network
REST	Representational State Transfer
API	Application Programming Interface
STIR	Secure Telephone Identity Revisited
SHAKEN	Signature-based Handling of Asserted information using toKENs
CGPN	Calling Party Number
CDPN	Called Party Number
ISTP	International Signaling Transfer Point
TSC	Transit Switching Center
MNP	Mobile Number Portability
FNP	Fixed Number Portability
IAM	Initial Address Message
REL	Release Message
KPI	Key Performance Indicator
STP	Signal Transfer Point
SIGTRAN	Signaling Transport
SIP	Session Initiation Protocol
ISUP	ISDN User Part
VoIP	Voice over Internet Protocol

Contents

1. Executive Summary

A significant challenge in today's telecommunications landscape is the threat posed by outbound roamer Caller Line Identification (CLI) spoofing. This fraudulent practice, where a caller manipulates their caller identification information, undermines network security and leads to various malicious activities.

The growing prevalence of CLI spoofing necessitates the development of sophisticated defense mechanisms to protect telecommunications infrastructures globally.

Outbound roamer CLI spoofing presents a complex problem that affects voice calls. Fraudsters impersonate trusted entities such as banks or government agencies, allowing recipients to divulge sensitive information or engage in fraudulent transactions. This deception can compromise network integrity and cause financial losses and reputational damage. The proliferation of VoIP-based spoofing tools and the lack of standardized authentication mechanisms further complicate detection and mitigation efforts.

The report is an in-depth examination of outbound roamer CLI spoofing, including its underlying mechanisms, impact on telecom operators and subscribers, and challenges in detection and mitigation. It emphasizes the need for a coordinated effort to protect the telecom sector's complex and evolving ecosystem and recommends establishing minimum baseline security standards, threat monitoring strategies, regular security assessments, and fostering a practice of sharing threat intelligence among industry members.

In addition, GCF's initiatives, particularly through the 'Safeguarding the Future Networks & Emerging Technologies' knowledge community, play a pivotal role in promoting and protecting ICT networks. This community brings together diverse expertise from ICT providers, telecom companies, cybersecurity research organizations, infrastructure operators, think tanks, academia and other stakeholders.

The community conducts comprehensive assessments of the potential impacts of emerging ICT technologies, benchmarks current standards, proposes industry standards and security protocols, and defines models for network resilience.

Despite advancements in 5G security measures, a significant portion of the global market still relies on older generations of mobile networks, such as 2G and 3G, which remain vulnerable to known exploits.

Nearly 19% of mobile connections worldwide have not transitioned from legacy networks, highlighting the urgent need for robust security measures. The report underscores the importance of addressing vulnerabilities to maintain the security and integrity of telecommunications networks.

This whitepaper report is valuable for industry professionals, policymakers, and researchers because it provides clear, concise and actionable guidelines to fortify the telecom sector against evolving signaling threats. Through its comprehensive analysis and strategic recommendations, the report aims to enhance global cybersecurity, promote a secure and resilient mobile ecosystem, and ensure the continued safety and reliability of mobile communication services worldwide. By leveraging intellectual power and fostering multilateral collaboration, GCF aims to contribute to a more stable and secure cyberspace.

"Despite advancements in 5G security measures, a significant portion of the global market still relies on older generations of mobile networks, such as 2G and 3G, which remain vulnerable to known exploits."

2. Introduction

In the dynamic landscape of telecommunications, the industry faces a multifaceted challenge: telecom fraud. This illicit enterprise leverages the vast and intricate networks of telecommunications services to siphon funds or data from unwitting individuals and organizations.

The spectrum of telecom fraud is broad, embracing a variety of tactics, each varying in complexity, scale, and the technologies exploited. At its core, the primary objective of these malevolent endeavors is financial gain, although certain tricks are also devised to harvest sensitive information for other nefarious purposes.

These fraudulent activities span a spectrum of methods, each designed to exploit specific vulnerabilities within the telecom ecosystem:

1. Consumer fraud manifests through deceptive tactics such as vishing, smishing, and manipulating caller identification systems. These strategies leverage social engineering to coax personal information or financial assets directly from the targets.

2. Subscription and identity fraud is characterized by the unauthorized appropriation of personal details to access services or start new agreements. This leads to unauthorized financial transactions that often remain undetected until substantial damage has occurred.

3. International revenue share fraud (IRSF) and traffic pumping involve the generation of calls to premium-rate international numbers owned by the fraudsters themselves. This scheme is often facilitated by malware or compromised private branch exchange (PBX) systems to incur long-duration calls at the victim's expense.

4. Wangiri fraud, or the 'one ring and cut' scam, employs a simple yet effective tactic of missed calls to international numbers, prompting recipients to return the call and unwittingly subject themselves to significant charges.

5. SIM swapping and SIM box fraud present a dual threat; the former involves the unauthorized transfer of a victim's phone number to a new SIM card controlled by the attacker, and the latter utilizes a device filled with multiple SIM cards to illegally reroute international calls through local numbers, thereby evading the higher charges associated with international calling.

These underscore the evolving and pervasive nature of telecom fraud, highlighting the necessity of continuous vigilance, developing sophisticated defense mechanisms, and empowering consumers with the knowledge to protect themselves. A collective effort to combat these practices is crucial for maintaining the integrity and trustworthiness of telecommunications infrastructures worldwide.

Under the Consumer Fraud category, this whitepaper looks at the growing problem of fraud and spoofing in telecom signaling, particularly in voice calls. It will also break down issues complicating the situation and offer actionable solutions to combat it effectively.

2.1 Overview of outbound roamer CLI spoofing in voice calls

Outbound roamer CLI spoofing in voice calls has become a pressing concern for telecommunications networks worldwide.

In recent years, malicious actors have exploited vulnerabilities in network infrastructure to manipulate caller identification information, leading to fraudulent activities and compromised security. As subscribers increasingly rely on voice communication for personal and business purposes, addressing this issue has become paramount.

Understanding the implications of outbound roamer CLI spoofing is crucial for telecom operators to safeguard their networks and maintain the trust of their subscribers. CLI spoofing involves manipulating caller line identification information to mask the true origin of a call, often with malicious intent. Fraudsters may impersonate legitimate entities, such as banks or government agencies, to deceive recipients into divulging sensitive information or engaging in fraudulent transactions.

2.2 Addressing this issue to ensure network security and integrity

The impact of outbound roamer CLI spoofing extends beyond financial losses and encompasses broader concerns related to network integrity and subscriber trust. Telecom operators face significant challenges in detecting and mitigating spoofed calls, including the global nature of telecommunications networks and the evolving tactics that fraudsters employ.

2.3 Scope and objectives of this whitepaper

The scope of this whitepaper encompasses an in-depth examination of outbound roamer CLI spoofing in voice calls, including its underlying mechanisms, impact on telecom operators and subscribers, and challenges faced in detection and mitigation. The primary objectives of this whitepaper are to raise awareness about the prevalence and consequences of CLI spoofing, propose effective solutions, and provide guidelines and case studies to assist telecom operators in securing their networks against fraudulent activities.

This whitepaper focuses on research and proposes a solution for combating outbound roamer CLI spoofing, specifically targeting operators peering with CAMEL agreements. By sharing our study outcomes and recommendations, we aim to empower operators with the knowledge and tools needed to safeguard their networks and subscribers from the growing threat of outbound roamer CLI spoofing.

This white paper will delve into solutions for outbound roamer CLI spoofing across various telecom signaling domains:

- National and International SS7 interconnect
- IPX network (International Voice peering)
- IN network (Intelligent Network)
- Signaling Core Network

3. Understanding Outbound Roamer CLI Spoofing

Caller ID spoofing is a fraudulent practice in which a caller deliberately manipulates the information transmitted to a recipient's caller identification system.

This typically involves altering the caller's phone number or name displayed on the recipient's device to misrepresent the caller's identity. CLI spoofing can be used for various purposes, including impersonating trusted entities such as banks or government agencies to deceive recipients into providing sensitive information or engaging in fraudulent activities.

Outbound roamer typically refers to a mobile subscriber traveling outside their home network's coverage area or jurisdiction. When a subscriber travels to a location where their home network does not have coverage, they 'roam' onto another network that has a roaming agreement with their home network.

The subscriber is considered an outbound roamer from their home network's perspective during this period. Therefore, an "outbound roamer" is a subscriber making calls or using mobile services outside their home network's coverage area.

CAMEL (Customized Applications for Mobile Networks Enhanced Logic) is a set of protocols and standards developed for telecommunications operators to customize services and implement advanced call-processing features within mobile networks.

CAMEL enables operators to deploy value-added services and implement complex call-handling logic independently of network elements such as switches and databases. CAMEL facilitates the creation of custom services such as prepaid billing, call forwarding, call screening and more.

CAP is a protocol used for communication between network elements in an intelligent network architecture, specifically between the SCP (Service Control Point) and other network components such as switches and databases. CAP carries CAMEL service logic and instructions between these elements, enabling customized services for mobile subscribers.

InitialDP stands for Initial Detection Point. In the CAMEL protocol, InitialDP is a message sent from the switch to the SCP (Service Control Point) to initiate service logic processing for a call. It contains information about the call, such as the calling party number, the called party number, and other relevant details. The SCP evaluates the service logic associated with the call and determines the appropriate actions, such as call routing, call screening, charging and more.

'O-CSI' stands for Originating CAMEL Subscription Information and refers to the subscription information stored in a mobile subscriber's Home Location Register (HLR) or Home Subscriber Server (HSS) that is relevant to the originating leg of a call. O-CSI includes services subscribed to by the mobile user, preferences, restrictions and other information that dictates how the network should handle calls originating from the subscriber's number. This information is used by the SCP (Service Control Point) in conjunction with other network elements to execute custom service logic and provide services to subscribers tailored to their individual preferences and subscription profiles.

"CLI spoofing can be used for various purposes, including impersonating trusted entities such as banks or government agencies to deceive recipients into providing sensitive information or engaging in fraudulent activities."

3.1 CLI spoofing and its impact on telecommunications networks

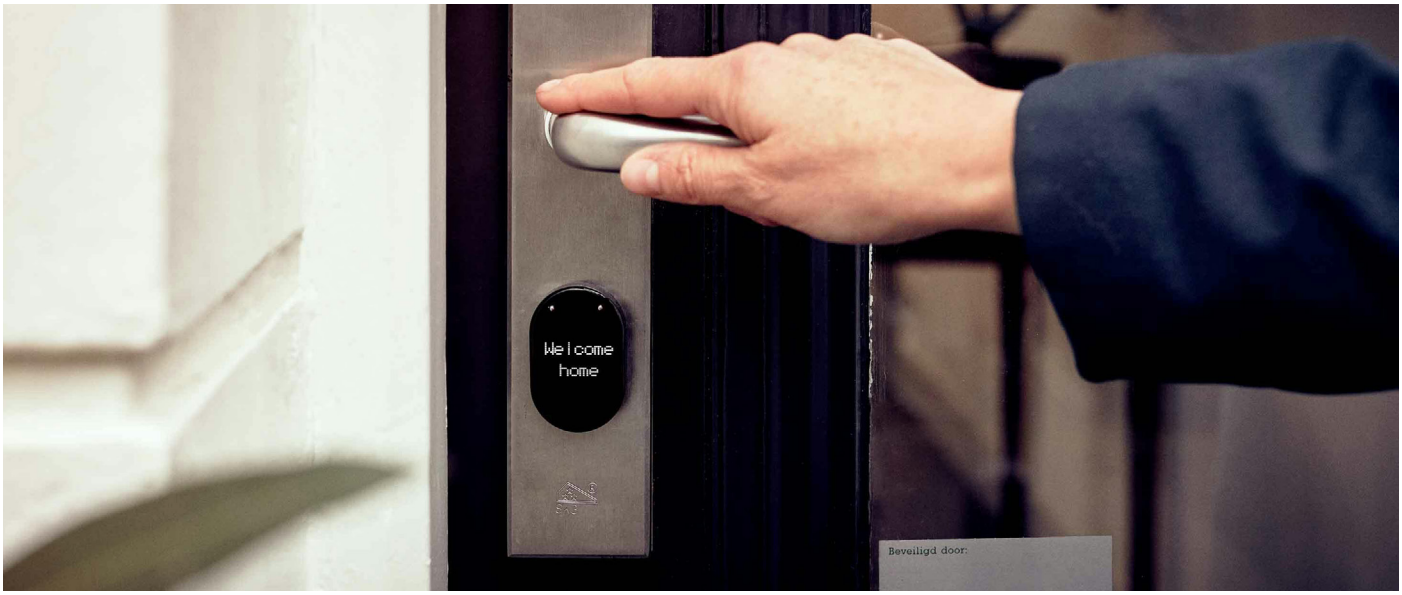
CLI spoofing involves manipulating caller identification information to disguise a call's true origin, enabling fraudsters to impersonate legitimate entities and deceive recipients. This practice undermines the integrity of telecommunications networks, leading to financial losses, reputational damage, and loss of subscriber trust. Vulnerabilities in signaling protocols and inadequate authentication mechanisms facilitate CLI spoofing, highlighting the need for proactive measures to combat this issue.

3.2 Common techniques used by fraudsters to spoof caller IDs

Fraudsters employ various techniques to spoof caller IDs, including VoIP-based spoofing, call forwarding and SIM card manipulation. These techniques exploit network infrastructure and signaling protocol weaknesses, enabling them to evade detection by traditional security measures. By leveraging advanced technologies and exploiting loopholes in regulatory frameworks, fraudsters continue to refine their tactics, posing a persistent challenge to telecom operators and law enforcement agencies.

3.3 Examples of fraudulent activities enabled by outbound roamer CLI spoofing

Examples of fraudulent activities enabled by outbound roamer CLI spoofing include phishing scams, vishing attacks and identity theft. In these scenarios, fraudsters manipulate caller IDs to impersonate trusted entities such as banks, government agencies or service providers, luring unsuspecting victims into divulging sensitive information or engaging in fraudulent transactions. These incidents underscore the urgent need for robust authentication mechanisms and proactive fraud detection systems to combat CLI spoofing effectively.



4. Challenges Faced by Telecom Operators

4.1 Identifying key challenges in detecting and mitigating CLI spoofing

Telecom operators face several challenges in detecting and mitigating CLI spoofing, including the global nature of telecommunications networks, proliferation of VoIP-based spoofing tools, and lack of standardized authentication mechanisms.

Overcoming these requires a coordinated approach that combines technological innovation, regulatory enforcement, and industry collaboration.

Challenges include:

- **Detecting the point of origin:** Spoofing can originate anywhere in the world, making it difficult to track down the source.
- **Call routing complexity:** Calls travel through various networks, making it hard to identify the exact point(s) of manipulation.
- **Verification methods:** Verifying a caller's identity in real time is not always easy.
- **Cost of implementation:** Anti-spoofing technology can be expensive for telecom operators.
- **Customer experience:** Efforts to mitigate CLI spoofing carry the possibility of an operator blocking legitimate calls.

4.2 Regulatory implications and compliance requirements related to CLI authentication

Regulatory frameworks are crucial in addressing CLI spoofing and ensuring compliance with authentication requirements.

Harmonizing regulatory frameworks and establishing clear guidelines for CLI authentication can facilitate compliance and enhance the effectiveness of fraud detection and prevention efforts.

It should be noted that numerous regulations regarding spoofing exist, and these can differ between countries, making efforts to address the phenomenon even more complex for international operators.

5. Proposed Solutions

5.1 Outbound roamer anti-CLI spoofing

Operators have a solution to combat caller ID spoofing for incoming international voice calls that prevents scammers from spoofing mobile numbers while on the home network in-country.

However, scammers have found a way to bypass this protection by spoofing the mobile numbers of subscribers who are roaming abroad (outbound roamers).

This study aims to mitigate this sophisticated threat through collaboration between the SS7 Firewall and the IPX to ensure that a CAMEL O-CSI IDP message is triggered from the visited MSC before a call is setup. This applies specifically to calls originating from operator outbound roamers while they are roaming in a CAMEL-supported network.

The legitimacy of such calls will only be confirmed if an SS7 CAMEL IDP (O-CSI) message is triggered from the visited MSC's VPMN towards the operator's home network. The IPX node is responsible for processing incoming international voice calls on the IPX (IP exchange) voice transit layer at the network border.

By blocking CLI spoofing for outbound roamers, the SS7 Firewall can cache the incoming international CAMEL IDP O-CSI messages for a configurable duration. Additionally, it functions as a REST server, accepting queries from the IPX to provide a verdict on whether the call should be allowed or blocked. It is important to note that the IPX shall initiate REST queries towards the SS7 Firewall exclusively for 'incoming international calls' that originate from 'outbound roamers while they are roaming in CAMEL-supported networks.'

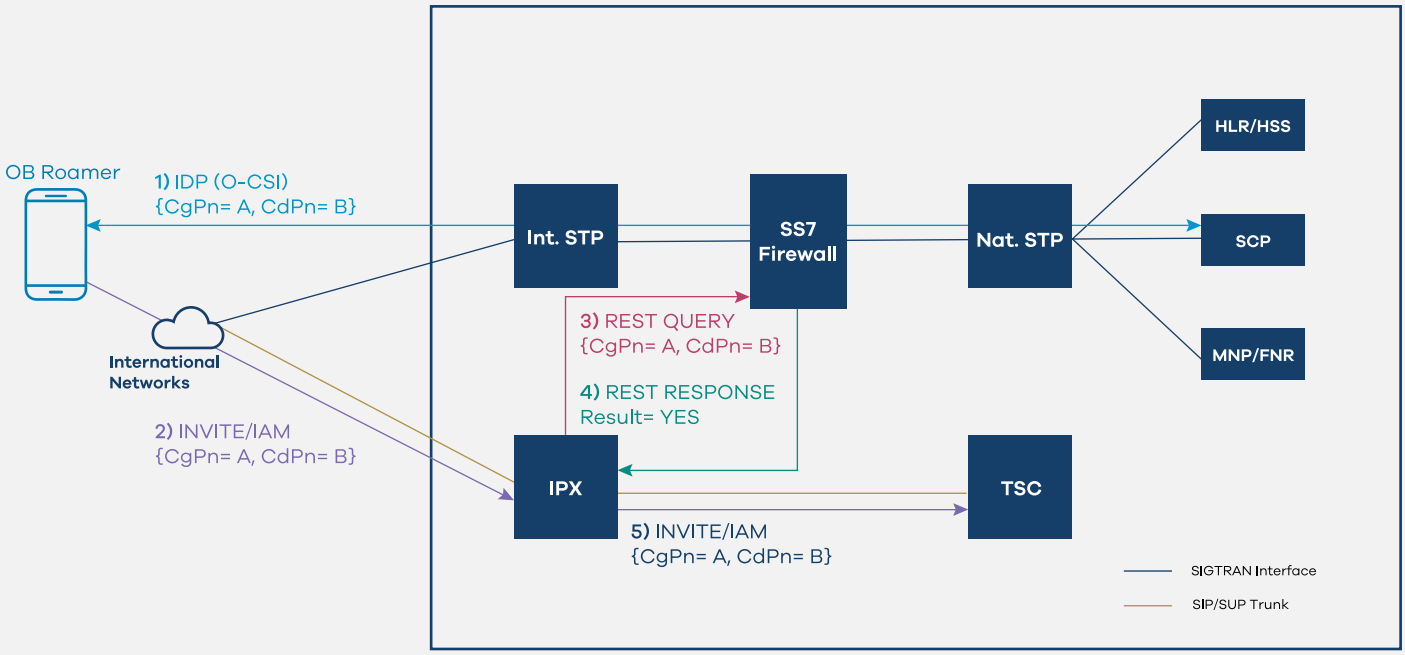


Figure-1 Outbound Roaming CLI Spoofing – Firewall Caches IDPs – Rest Integration

5.2 Advantages of anti-spoofing

Enhanced security: Anti-spoofing solutions help prevent fraudulent activities, strengthening the overall security of voice networks and protecting against malicious spoofing attempts.

Customer trust and confidence: When subscribers feel their calls are secure from spoofing attacks, they are more likely to trust the network, increasing customer satisfaction and loyalty.

Reduced fraud and scams: Spoofing is often used in fraudulent activities, such as phishing, scam calls, and financial fraud. Anti-spoofing solutions can significantly reduce these incidents, protecting the operator and its customers from financial losses and reputational damage.

Regulatory compliance: By adhering to telecommunications regulations and industry standards related to caller identification, the anti-CLI spoofing solution helps telecommunications providers maintain compliance, avoiding potential fines and penalties associated with non-compliance.

Implementing anti-spoofing solutions for voice calls strengthens security and regulatory compliance, enhances customer trust, reduces fraud, and provides numerous other benefits.

5.3 Call flow

5.3.1 Legitimate case call flow

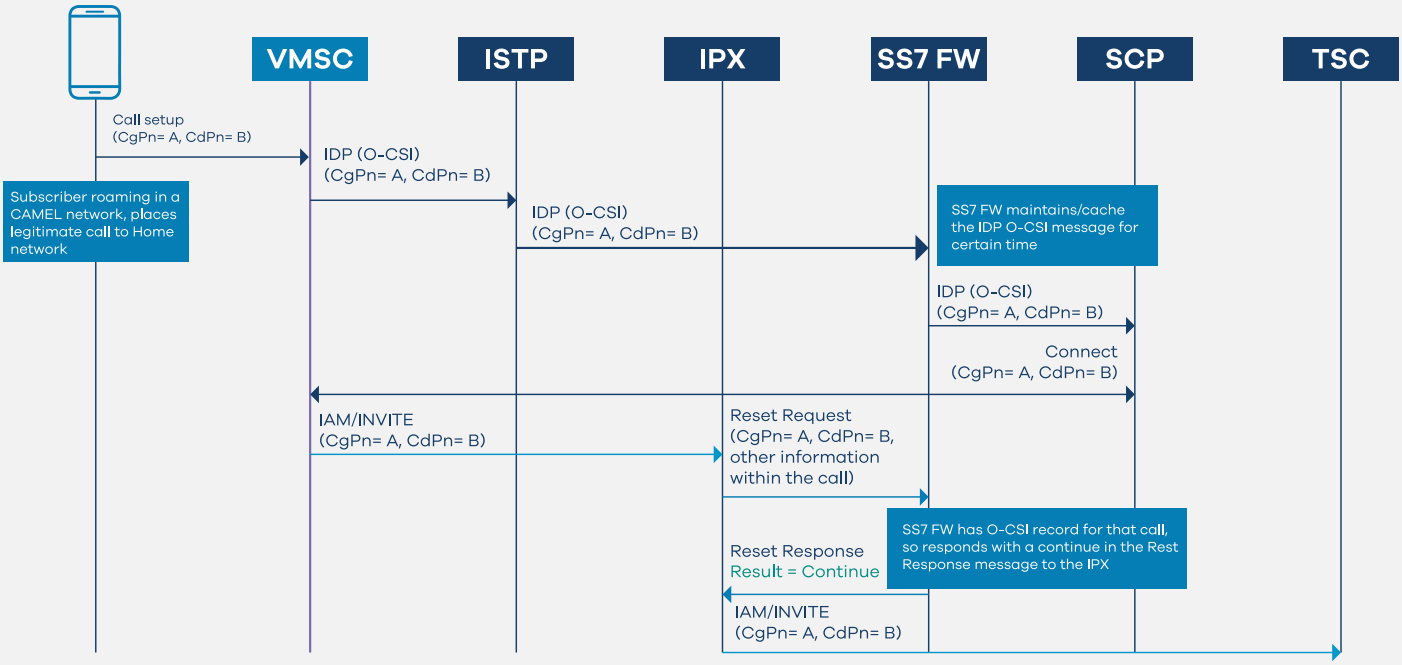


Figure-2 Legitimate International Call – OB Roamer in a Camel Network

5.3.2 Spoofing case call flow

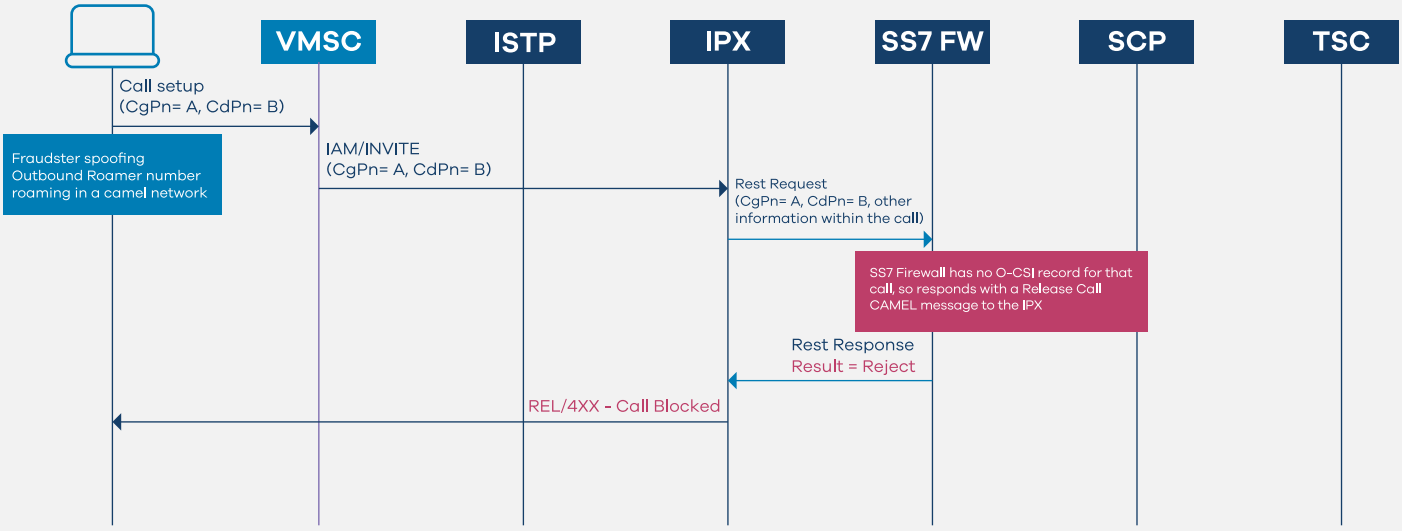


Figure-3 Spoofed International Call – OB Roamer in a Camel Network

5.4 Other controls to resolve outbound roamer CLI spoofing

5.4.1 Implementation of call-trust solution using STIR/SHAKEN

To combat outbound roamer CLI spoofing effectively, telecom operators should implement robust signaling security mechanisms. These include: STIR/SHAKEN (Secure Telephone Identity Revisited/Signature-based Handling of Asserted information using toKENs). These protocols enable the verification of caller identities and the detection of spoofed calls, enhancing the overall security posture of telecommunications networks.

5.4.2 Implementing advanced fraud detection systems

Integrating real-time monitoring and alerting systems can help promptly detect and respond to fraudulent signaling events. Advanced fraud detection systems powered by artificial intelligence and machine learning algorithms can analyze call patterns and identify anomalous behavior indicative of CLI spoofing. By leveraging real-time analytics and threat intelligence, telecom operators can proactively detect and mitigate spoofed calls, reducing the risk of fraudulent activities and protecting subscribers from potential harm.

5.4.3 Enhancing collaboration and information sharing

Establishing industry-wide collaborative platforms can help share threat intelligence and best practices to combat pressing issues. This can take the shape of partnerships between telecom operators, vendors and regulatory agencies to coordinate efforts and exchange insights on signaling fraud trends. By sharing threat intelligence, best practices and mitigation strategies, stakeholders can collectively identify emerging threats and implement coordinated responses.

6. Implementation Guidelines

6.1 Guidelines for telecom operators to implement the proposed solution framework

Telecom operators should follow specific guidelines to implement the proposed solution framework effectively. Guidelines for a SS7-FW Anti CLI spoofing solution include:

- Ensure a thorough understanding of the proposed solution and its integration with existing network infrastructure.
- Develop clear documentation outlining the configuration and deployment procedures for integrating the SS7 Firewall and IPX using REST-API.
- Establish communication protocols and procedures between the SS7 Firewall and IPX to facilitate seamless data exchange and decision-making.
- Implement robust security measures to safeguard REST-API endpoints and prevent unauthorized access or tampering.
- Conduct thorough testing and validation of the integrated solution in a controlled lab environment before deployment in production networks.
- Establish key performance indicators (KPIs) to measure the solution's effectiveness in detecting and mitigating outbound roamer CLI spoofing.
- Develop incident response plans and procedures to address any issues or anomalies encountered during the implementation and operation of the solution.
- Foster collaboration and knowledge-sharing among network operators and industry stakeholders to exchange best practices and lessons learned.
- Regularly monitor and evaluate the performance of the integrated solution, making necessary adjustments and optimizations to ensure continued effectiveness.
- Stay abreast of emerging threats and vulnerabilities related to outbound roamer CLI spoofing and update the solution accordingly to maintain a robust security posture.
- Maintain compliance with regulatory requirements and industry standards governing telecommunications security and privacy.
- Document and share insights, challenges, and success stories from the solution's implementation to contribute to industry knowledge and best practices.
- Continuously evaluate and refine the solution based on feedback from subscribers and other stakeholders to improve its effectiveness and relevance over time.
- Conduct comprehensive training sessions for network personnel responsible for implementing and managing the solution.

6.2 Considerations for interoperability and compatibility with existing network infrastructure

When implementing CLI authentication mechanisms and fraud detection systems, telecom operators must consider interoperability and compatibility with existing network infrastructure. This includes evaluating the scalability, performance, and integration capabilities of proposed solutions to ensure seamless deployment and operation across diverse network environments. Additionally, operators should prioritize interoperability testing to minimize disruptions and maximize the effectiveness of CLI spoofing prevention measures.

7. Conclusion

This whitepaper aims to raise awareness about the prevalence and consequences of CLI spoofing, propose effective solutions to address this issue and provide practical guidelines and case studies to assist operators in securing their networks against fraudulent activities.

Combating outbound roamer CLI spoofing requires a concerted effort from telecom operators, industry stakeholders and regulatory authorities. By implementing advanced authentication mechanisms, enhancing collaboration and information sharing, and adopting proactive fraud detection systems, operators can mitigate the risks associated with CLI spoofing and protect their networks and subscribers from malicious activities. This can enable a safer and more resilient telecommunications ecosystem that fosters trust, innovation and prosperity for all.

"Combating outbound roamer CLI spoofing requires a concerted effort from telecom operators, industry stakeholders and regulatory authorities."

GLOBAL CYBERSECURITY FORUM

stc