Universidad Cenfotec

Maestría en Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 1

Tema:

Análisis de factibilidad para la aplicación de mejores prácticas, por parte de los proveedores de servicio, para evitar la suplantación de números telefónicos institucionales en Costa Rica.

Elaborado por:

Rubén Amado Morales Vargas.

Fecha: Enero, 2024

Declaratoria de derechos de autor

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Rubén Morales Vargas**

Digitally signed by MIGUEL PEREZ MONTERO (FIRMA)
Date: 2024.10.18 10:45:13 -06'00'

M.Sc. Miguel Pérez Montero
Tutor

Firmado digitalmente por Rebeca Esquivel Flores

M.Sc. Rebeca Esquivel Flores
Lector 1

YAHAIRA ROCIO SOSA ARIAS (FIRMA)

Firmado digitalmente por YAHAIRA ROCIO SOSA ARIAS (FIRMA)
Fecha: 2024.10.22 12:57:44 -06'00'

MSeg. Yahaira Sosa Arias
Lector 2

San José, Costa Rica, 17 de octubre 2024

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Índice de Contenido

Índice de tablas

Índice de figuras

Abstract

El enmascaramiento del identificador de llamadas ("spoofing") es un problema creciente que afecta la seguridad y la confiabilidad de las comunicaciones telefónicas, dando lugar a diferentes tipos de estafas cada vez más frecuentes. Este estudio investiga las mejores prácticas tecnológicas y las normativas a nivel nacional para minimizar este problema, evaluando la factibilidad de su implementación en proveedores de servicios telefónicos en Costa Rica. Se realizaron pruebas de concepto en un entorno controlado y se analizaron las limitaciones actuales para aplicar estas soluciones. Los resultados muestran que la implementación de filtros en rutas internacionales y la aplicación de la normativa E.164 son métodos efectivos para combatir el enmascaramiento de llamadas, y con ello reducir los ataques de ingeniería social a las personas.

PALABRAS CLAVE: Spoofing Caller ID, Identificador de llamadas, Regulación telefónica, Telefonía IP, Suplantación de identidad.

Capítulo 1. Introducción

1.1 Generalidades

Esta investigación se centra en buscar las mejores prácticas a nivel mundial para el control y la prevención de la suplantación de números telefónicos institucionales, por parte de delincuentes, para cometer fraudes. Una vez determinadas estas mejores prácticas se procura revisar la factibilidad de ponerlas en práctica en Costa Rica para proteger a la población de este tipo de ataques.

Por la sensibilidad del tema analizado en esta investigación, se intenta, en lo posible, no mostrar datos sensibles de los proveedores de servicio, direcciones IP, privadas y públicas, de los diferentes equipos involucrados, y datos personales de los colaboradores con las pruebas e información relevante para la investigación.

Además, con el propósito de realizar pruebas para comprender el funcionamiento de la suplantación de identidad de números telefónicos. Se utilizan proveedores que lo permiten, con una verificación previa, sin embargo, se aclara que se utilizan solo números propios para realizar las simulaciones.

1.2 Antecedentes del Problema

Los avances de las telecomunicaciones traen beneficios y un impacto positivo en la interconectividad y la automatización de procesos relacionados con las comunicaciones para beneficio de compañías y personas, pero también tienen vulnerabilidades que pueden ser utilizadas por actores mal intencionados. Tal es el caso de la telefonía, más específico con el protocolo VoIP (Voz sobre IP), que con algunos ajustes permite mostrar el número telefónico que el llamante desee, en lo que se denomina como "*Spoofing Caller ID*", lo que es aprovechado de manera mundial para intentos de estafas, valiéndose de la confianza que se tenía en el *"Caller ID".*

1.3 Definición y Descripción del Problema

El "*Spoofing Caller ID*", que es una técnica permitida normalmente en el protocolo SIP, donde los proveedores de servicio permiten que el usuario final pueda configurar el número que requiera en el identificador de llamadas, si bien, esto es permitido en muchas legislaciones, donde se hace énfasis que es legal, siempre y cuando no se utilice con fines fraudulentos, pero en realidad es utilizado comúnmente para esos fines. En el caso de Costa Rica, este *spoofing* es utilizado para intentar generar confianza en los intentos de estafa vía telefónica, donde los delincuentes se hacen pasar por funcionarios de alguna institución y, aplicando diferentes estrategias de ingeniería social, logran generar que el usuario crea que en realidad lo llaman de un banco, por ejemplo.

La falta de regulaciones robustas y soluciones técnicas específicas contribuye a que el "*Spoofing Caller ID*" persista como un desafío en las comunicaciones telefónicas, requiriendo una atención continua para proteger la integridad de las llamadas y preservar la confianza de los usuarios en este medio de comunicación.

1.4 Justificación

Este tema deriva de la necesidad de disminuir la eficacia de los ataques de ingeniería social, que se llevan a cabo vía telefónica, dirigidos a los ciudadanos de Costa Rica, quienes son clientes o usuarios de diferentes instituciones, ya sean públicas o privadas en el país. El ataque, objeto de esta investigación, consiste en que, cuando el usuario recibe llamadas, estas aparentemente provienen de los números de teléfono oficiales de las entidades, de esta manera, sienten más confianza en que quien los está llamando, realmente, es un funcionario de esa institución, resultando en que brinden información personal e incluso confidencial, que puede ser usada para fines que afecten a la población, como en el caso de estafas.

1.5 Viabilidad

1.5.1. Punto de Vista Técnico.

Esta investigación es viable, desde el punto de vista técnico, ya que se tienen los conocimientos básicos y el acceso a herramientas para realizar las pruebas que correspondan en el área de Telefonía IP, adicionalmente se cuenta con la capacidad de investigar sobre el tema específico.

1.5.2. Punto de Vista Operativo.

Debido a que no se está planteando realizar cambios inmediatos a nivel de los proveedores, si no que se brindan posibles soluciones, además de generar el conocimiento de que existe una vulnerabilidad que es explotada por personas mal intencionadas. Se encuentra que es factible desde el punto operativo.

1.5.3 Punto de Vista Económico.

En la tabla 1 se detallan los costos asociados a la investigación.

Tabla 1

Costos investigación

Cantidad	Descripción	Monto	Total
416	Horas Consultor	$ 50.00	$ 20,800.00
2	Capacitación metodológica	$ 1,200.00	$ 2,400.00

1	Materiales	$ 180.00	$ 180.00
		Total	$ 23,380.00

Nota. Los costos serán asumidos por el investigador, lo que hace la investigación viable desde el punto de vista económico.

1.6 Objetivos

Para elaborar los objetivos se utiliza la taxonomía de Bloom, debido a que presenta, de forma clara, como plantear los objetivos de manera ordenada y de acuerdo con un estándar.

1.6.1 Objetivo General. Evaluar la factibilidad de la aplicación de mejores prácticas, por parte de los proveedores de servicios telefónicos, para evitar la suplantación de números telefónicos institucionales en Costa Rica.

1.6.2 Objetivos Específicos

- Investigar las mejores prácticas aplicables a nivel nacional que minimicen los medios que permiten la suplantación de números telefónicos.
- Conocer las limitaciones actuales por las cuales no se han aplicado acciones que ayuden a disminuir la suplantación de números telefónicos institucionales.
- Realizar pruebas que ayuden a identificar cómo los delincuentes se aprovechan de la vulnerabilidad que permite intentos de estafa.
- Analizar las posibilidades de la aplicación de mejores prácticas que limiten los medios que permiten la suplantación de números telefónicos en el País.

1.7 Alcances y Limitaciones

1.7.1 Alcances.

Se confecciona un documento escrito con los hallazgos encontrados a nivel país para la posibilidad de mitigar la suplantación de números telefónicos institucionales.

La investigación se realiza con datos obtenidos de diferentes entidades involucradas que regulan y brindan servicios de telecomunicaciones en Costa Rica.

1.7.2 Limitaciones.

La propuesta de esta investigación es generalizada, para sugerir mejores prácticas a nivel de proveedores de telecomunicaciones. No incluye cómo deben ser aplicadas en específico en los diferentes proveedores o equipos.

La investigación podría verse afectada por la cantidad de datos que se logren obtener de las diferentes instituciones involucradas para realizar recomendaciones específicas, por lo

que se enfoca en dar a conocer la problemática generada por el “Spoofing Caller ID” y, como se menciona anteriormente, se realiza un análisis de forma generalizada.

1.8 Estado de la Cuestión

El "Spoofing Caller ID” se debe considerar una vulnerabilidad en la tecnología de telefonía, ya que permite cambiar el número telefónico que se muestra al receptor de la llamada, o eludir sistemas de autenticación que dependen del identificador de llamadas.

Debido a esa vulnerabilidad se identifica una problemática creciente relacionada al identificador de llamadas (caller ID) debido a que es utilizada por actores mal intencionados que se aprovechan del “Spoofing Caller ID”. Esta vulnerabilidad puede ser explotada con fines maliciosos, como fraude y obtención de información sensible.

Aunque se ha sido consciente de esta vulnerabilidad, desde las primeras implementaciones de VoIP, el estado actual de las soluciones es limitado. Algunas soluciones son consideradas complejas y recae la responsabilidad en el usuario final, mientras que otras, como el protocolo "STIR/SHAKEN", requieren la implementación a nivel de los proveedores de servicios y la validación a través de terceros de confianza.

A nivel país, recientemente, la institución encargada de regular a los proveedores de servicio emitió una resolución para que las diferentes compañías, que brindan servicios de telefonía, apliquen configuraciones que minimicen las llamadas exitosas, que tengan el número enmascarado, sin embargo, a la fecha no se ha logrado realizar una implementación generalizada de la posible solución. La solución propuesta se basa en aplicar la recomendación internacional E.164 que indica cómo deben ser los formatos internacionales.

1.8.1. Planificación de la revisión

Para sustentar esta investigación, se realiza una búsqueda de publicaciones, artículos, patentes, noticias y otros trabajos de importancia, que proponen posibles soluciones. Además, se buscaron las regulaciones existentes nacionales e internacionales para validar el avance a nivel de instituciones encargadas. Por otro lado, para la búsqueda de documentación se establecen palabras clave que se consideran relevantes y asociadas al tema. Se detallan algunas de las palabras claves en el siguiente cuadro:

Tabla 2

Palabras clave.

Spoofing Caller ID

Identificador de llamadas
Telefonía IP
VoIP
Llamadas fraudulentas
Suplantación de identidad
Fraude telefónico
Consecuencias del Caller ID falso
Regulación telefónica
STIR/SHAKEN
Tecnologías anti-spoofing telefónico

1.8.2. Literatura evaluada

Se detalla la literatura y las fuentes analizadas.

Tabla 3

Extracción fuente 1.

Titulo	A Mechanism to Authenticate Caller ID
Publicación	Springer
Palabras	Caller ID · Spoofing · Fake · Authentication · Trusted
Autores	Li, J., Faria, F., Chen, J., & Liang, D
Referencia	Li, J., Faria, F., Chen, J., & Liang, D. (2017). A Mechanism to Authenticate Caller ID. En Advances in intelligent systems and computing (pp. 745-753). https://doi.org/10.1007/978-3-319-56538-5_75

Resumen	El identificador de llamadas que se muestra en el teléfono se supone que proporciona información precisa sobre el llamante. Sin embargo, con la ayuda de computadoras y Voz sobre Protocolo de Internet (VoIP), es fácil falsificar un identificador de llamadas. Los usuarios que utilizan la suplantación de identificador de llamadas pueden ser la oficina de un distrito escolar, un hospital, las fuerzas del orden, telemercadeo, entre otros. Aunque la suplantación de identificador de llamadas tiene usos legítimos, representa amenazas reales para el receptor de la llamada cuando se abusa de ella. En el mundo actual, es importante restaurar la credibilidad del identificador de llamadas entrante. En este trabajo, proponemos un mecanismo que puede autenticar identificadores de llamadas certificados, ya sean auténticos o legítimamente falsificados. El esquema propuesto implica al llamante, al receptor de la llamada y a un tercero para intercambiar información breve. Depende del llamante y del receptor adoptar este esquema. El esquema propuesto no cambia el protocolo de conmutación ni de señalización. Se puede integrar de manera natural en el sistema actual. Se desarrolló una aplicación basada en Android para probar la idea.

Nota. Elaboración propia.

Tabla 4

Extracción fuente 2.

Titulo	Spoofing Against Spoofing: Towards Caller ID Verification In Heterogeneous Telecommunication Systems
Publicación	ACM Journals
Palabras	Security and privacy, Authentication
Autores	SHEN WANG, MAHSHID DELAVAR, MUHAMMAD AJMAL AZAD, FARSHAD NABIZADEH,STEVE SMITH, FENG HAO,

Referencia	Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S. M., & Hao, F. (2023). Spoofing against spoofing: towards caller ID verification in heterogeneous telecommunication systems. ACM Transactions On Privacy And Security, 27(1), 1-25. https://doi.org/10.1145/3625546
Resumen	El spoofing Caller ID es un problema global de la industria y a menudo actúa como un facilitador crítico para el fraude telefónico. Para abordar este problema, la Comisión Federal de Comunicaciones (FCC) ha ordenado a los proveedores de servicios de telecomunicaciones en los Estados Unidos implementar STIR/SHAKEN, una solución impulsada por la industria basada en firmas digitales. STIR/SHAKEN depende de una infraestructura de clave pública (PKI) para gestionar certificados digitales, pero escalar esta PKI para la industria global de telecomunicaciones es extremadamente difícil, si no imposible. Además, solo funciona con sistemas basados en IP (por ejemplo, SIP), dejando desprotegidos los sistemas tradicionales no basados en IP (por ejemplo, SS7).

Nota. Elaboración propia.

Tabla 5

Extracción fuente 3.

Titulo	End-to-End Detection of Caller ID Spoofing Attacks
Publicación	Institute of Electrical and Electronics Engineers (IEEE)
Palabras	End-user security, caller ID spoofing.
Autores	Mustafa, Hossen; Xu, Wenyuan; Sadeghi, Ahmad-Reza and Schulz, Steffen

Referencia	Mustafa, H. A., Xu, W., Sadeghi, A., & Schulz, S. (2018). 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
Resumen	El Identificador de Llamadas (caller identification) es un servicio proporcionado por operadores de telefonía donde el número de teléfono y/o el nombre del llamante se transmiten para informar al destinatario quién está llamando. Hoy en día, la mayoría de las personas confían en la información del identificador de llamadas, e incluso algunos bancos utilizan el identificador de llamadas para autenticar a los clientes. Sin embargo, con la proliferación de teléfonos inteligentes y la telefonía por protocolo de internet (VoIP), es fácil falsificar la información del identificador de llamadas instalando una aplicación específica en el teléfono inteligente o utilizando proveedores de servicios que ofrecen la suplantación de identificador de llamadas. Dado que la red telefónica está fragmentada entre países y empresas, y las actualizaciones de hardware antiguo son costosas, no existe hoy en día un mecanismo que permita a los usuarios finales detectar fácilmente los ataques de suplantación de identificador de llamadas. En este artículo, proponemos un nuevo enfoque que utiliza esquemas de verificación de identificador de llamadas de extremo a extremo que aprovechan las características de la infraestructura existente de la red telefónica (CallerDec). Diseñamos una versión basada en SMS y otra basada en sincronización de CallerDec que funciona con combinaciones existentes de líneas fijas, redes celulares y VoIP, y que puede implementarse a voluntad de los usuarios. Implementamos ambas versiones de CallerDec como una aplicación para teléfonos basados en Android y validamos su eficacia en la detección de ataques de

	suplantación en diversos escenarios.

Nota. Elaboración propia.

Tabla 6

Extracción fuente 4.

Titulo	Increasing the efficiency of One-time key Issuing for The First Verification Caller ID Spoofing Attacks.
Publicación	Institute of Electrical and Electronics Engineers (IEEE)
Palabras	Caller ID spoofing, encryption, recommended system.
Autores	Narongsak sukma, Roongroj Chokngamwong.
Referencia	*Increasing the efficiency of One-time key Issuing for The First Verification Caller ID Spoofing Attack*s. (2018, 1 julio). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/8457341.
Resumen	En la actualidad, verificar al propietario de cada número de teléfono sigue siendo posible solo mostrando el número en la pantalla. Las redes telefónicas hoy en día no cuentan con un proceso adecuado de validación. Esta es una vulnerabilidad crítica que los atacantes pueden aprovechar para falsificar un número de teléfono, haciéndose pasar por alguien más, como una agencia gubernamental, y engañar a las personas para que crean y, eventualmente, transfieran dinero. Basándonos en este problema, nuestro equipo de investigación ha encontrado que muchos estudios han intentado resolver el problema utilizando mensajes cortos (SMS), el tiempo dedicado a la respuesta del usuario, el uso de hardware y la verificación de firmas digitales.

Nota. Elaboración propia.

Tabla 7

Extracción fuente 5.

Titulo	One time key Issuing for Verification and Detecting Caller ID Spoofing Attacks.
Publicación	Institute of Electrical and Electronics Engineers (IEEE)
Palabras	caller ID spoofing, encryption, decryption,
Autores	Narongsak sukma, Roongroj Chokngamwong.
Referencia	*One time key Issuing for Verification and Detecting Caller ID Spoofing Attacks. (2017, 1 julio). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/abstract/document/8025898.*
Resumen	El Identificador de Llamadas se ha utilizado para informar al destinatario quién está llamando antes de responder la llamada. De hecho, en la actualidad, utilizar únicamente el Identificador de Llamadas no es suficiente para comprobar la identidad real del llamante, ya que existen varias formas de manipular la identidad del llamante. Hay varias soluciones para comprobar la identidad del llamante, como el uso de bases de tiempo, bases de SMS o hardware. Incluso el uso de DSA y CA puede provocar fugas de datos o procesos de verificación inconsistentes. Las prácticas de contraseñas de un solo uso pueden mitigar el riesgo de ataques de intermediarios porque SSL tiene una evaluación de vulnerabilidades que puede llevar a un ataque de intermediario o "man-in-the-middle" (MITM). El atacante puede interceptar el proceso de verificación SSL entre el servidor y el cliente para espiar y luego realizar suplantación de identidad. Sería mejor encontrar una solución que no dependa de CA, terceros y/o hardware externo.

Nota. Elaboración propia.

Tabla 8

Extracción fuente 6

Titulo	RESEARCH OF CALLER ID SPOOFING LAUNCH, DETECTION, AND DEFENSE
Publicación	arxiv.org
Palabras	caller ID, spoofing, CIVE, callee inference, callee verification, callee, caller, SIP.
Autores	Buriachok, V., Sokolov, V., & TajDini, M.
Referencia	*Buriachok, V., Sokolov, V., & TajDini, M. (2020). RESEARCH OF CALLER ID SPOOFING LAUNCH, DETECTION, AND DEFENSE. Kìberbezpeka. Osvìta, Nauka, Tehnìka, 3(7), 6-16. https://doi.org/10.28925/2663-4023.2020.7.616.*
Resumen	El enmascaramiento del identificador de llamadas produce la apariencia de llamada válido, haciendo que parezca provenir de otro usuario. Esta estrategia de ataque aparentemente simple se ha utilizado cada vez más en el ámbito de las estafas de comunicación y llamadas engañosas, lo que resulta en pérdidas financieras significativas. Lamentablemente, el enmascaramiento del identificador de llamadas es fácil de implementar, pero aun así es difícil protegerse contra él. Además, en la actualidad no hay soluciones efectivas y defensivas disponibles. En esta investigación, se propone el CIVE (Inferencia y Verificación del Receptor), una defensa eficaz y viable contra el enmascaramiento del identificador de llamadas. De esta manera, se describe cómo es posible lanzar el enmascaramiento de llamadas y, entre líneas, cómo el método del enfoque CIVE puede ayudar a prevenir de alguna manera este tipo de ataques.

Nota. Elaboración propia.

Tabla 9

Extracción fuente 7

Titulo	Securing Confidentiality and Integrity of SIP Based VoIP System in Reduced Call Setup Time.
Publicación	ResearchGate.
Palabras	Voip.
Autores	Tesema, S. N., & Shiferaw, Y. N.
Referencia	Tesema, S. N., & Shiferaw, Y. N. (2014). Securing Confidentiality and Integrity of SIP Based VoIP System in Reduced Call Setup Time. *ResearchGate*. https://www.researchgate.net/publication/355406821.
Resumen	La Voz sobre Protocolo de Internet (VoIP) es uno de los servicios de Internet de más rápido crecimiento con una prometedora demanda en aumento. Sin embargo, esta demanda se enfrenta a desafíos debido a los problemas de seguridad actuales en Internet y a la falta de perfección en los propios protocolos de VoIP. Específicamente, dado que cualquier servicio de telecomunicaciones requiere protección de la privacidad, confidencialidad, integridad y disponibilidad, VoIP debe asegurar a sus clientes estos principios de seguridad de la información con una calidad de servicio tolerable, preocupaciones que no se plantean con frecuencia en las redes telefónicas públicas conmutadas (PSTN) y otras redes telefónicas tradicionales.

Nota. Elaboración propia.

Tabla 10

Extracción fuente 7

Titulo	You Can Call But You Can't Hide.
Publicación	Institute of Electrical and Electronics Engineers (IEEE).

Palabras	End-user Security; Caller ID Spoofing.
Autores	Mustafa Hossen, Xu Wenyuan, Sadeghi and Schulz Steffen.
Referencia	You Can Call but You Can't Hide: Detecting Caller ID Spoofing Attacks. (2014, 1 junio). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/6903577.
Resumen	El Identificador de Llamadas (identificación del llamante) es un servicio proporcionado por las compañías telefónicas para transmitir el número de teléfono y/o el nombre de un llamante a un destinatario. Hoy en día, la mayoría de las personas confían en la información del identificador de llamadas, y se utiliza cada vez más para autenticar a los clientes (por ejemplo, por bancos o compañías de tarjetas de crédito). Sin embargo, con la proliferación de teléfonos inteligentes y VoIP, es fácil falsificar el identificador de llamadas instalando aplicaciones correspondientes en los teléfonos inteligentes o utilizando proveedores de identificación falsa.

Nota. Elaboración propia.

Capítulo 2. Marco Teórico

Para facilitar la elaboración del marco teórico, se realiza una nube de palabras y un mapa conceptual, basados en los trabajos analizados en el estado de la cuestión y los objetivos específicos de la presente investigación, para de esta manera obtener conceptos claves a definir, que ayuden a un entendimiento básico.

2.1 Nube de palabras

Se elabora la siguiente nube de palabras para obtener conceptos claves e importantes.

Figura 1

Nube de conceptos básicos.

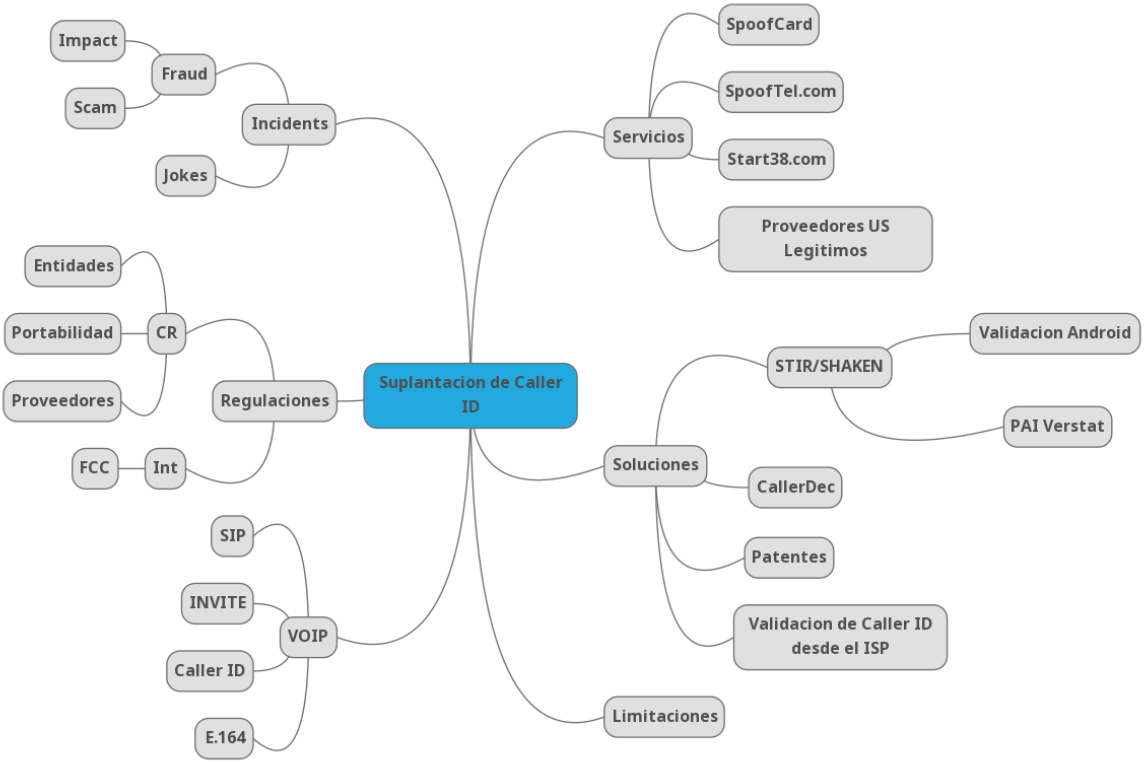
Nota. Elaboración Propia, en base del estado de la cuestion y lo objetivos de la investigación.

2.2.Mapa Conceptual

Se presentan los conceptos base y sus relaciones en el siguiente mapa conceptual, así como algunos servicios que han influenciado en la problemática actual para comprender de una mejor manera cómo el enmascaramiento del identificador de llamadas ha estado presente durante años y su afectación.

Figura 2

Mapa de conceptos relacionados al “spoofing”



Nota. Elaboración Propia, en base del estado de la cuestion.

La **suplantación del identificador de llamadas** o en inglés "*Spoofing Caller ID*", es la técnica de configurar un identificador de llamadas alterado para que se muestre un número telefónico específico a la persona que se llama. Esta práctica puede tener fines legítimos, por lo cual aún es permitida, pero en general, es utilizada para otros fines, como intentos de fraude y eludir autenticación basada en el identificador de llamadas.

2.2.1. Definiciones base de telefonía

***Public Switched Telephone Network* (PSTN)** es la infraestructura aún existente que permite interconexión entre diferentes proveedores nacionales, regionales e internacionales. Esta infraestructura está siendo reemplazada por la infraestructura de datos que permite migrar las telecomunicaciones a soluciones IP (*Internet Protocol*). Sin embargo, de esta infraestructura y sus funciones se her edan funciones como el *Caller ID.*

***Caller ID* o identificador de llamadas** es una función brindada por los proveedores de servicios telefónicos que ayuda a identificar quien es el llamante. Este campo, por lo general, va asociado al servicio telefónico, por lo que el proveedor de servicios es quien lo asigna, sin embargo, en servicios SIP, es posible configurarlo desde las centrales telefónicas u otros equipos que reciben el servicio de telefonía. El identificador de llamadas debe tener un formato con un estándar del plan de numeración telefónica. Internacionalmente existe el formato o plan de numeración **E.164**, que se describe en el documento *Recomendación UIT-T E.164* desarrollado por la Unión Internacional de

Telecomunicaciones y que es usado como estándar para la asignación de numeración a nivel internacional.

Voice over IP (VoIP) o telefonía IP es una tecnología que permite, en conjunto con otros protocolos, que la voz (las llamadas) puedan transmitirse por las redes de datos. Algunos de los protocolos que conforman VoIP, son:

Session Initiation Protocol **(SIP)** es un protocolo de señalización utilizado en redes de comunicaciones para iniciar, modificar y finalizar sesiones de comunicación, como llamadas de voz y video a través de las redes de datos.

SIP, es el encargado de transmitir los mensajes necesarios para establecer una llamada telefónica, entre ellos un mensaje llamado *"INVITE"* el cual contiene información necesaria para establecer las llamadas, entre estos incluye el encabezado *"FROM"* el cual por lo general es el campo encargado de indicar el "*Caller ID"* que se debería mostrar, este campo es el que, al editarlo por parte del llamante, permite generar una llamada aplicando la técnica *"Spoofing Caller ID".* Otro de los encabezados, dentro del "*INVITE*", es el PAI, que también puede ser utilizado para enviar el *"Caller ID"* o información del llamante o autenticación que pueden utilizar los proveedores. En la actualidad, el protocolo *STIR/SHAKEN* utiliza este encabezado para enviar el resultado de la verificación cuando el protocolo es utilizado por el proveedor de servicios.

Private Branch Exchange **(PBX)** en su traducción al español seria Central telefónica privada y se le domina así al equipo (virtual o físico) dentro de una compañía u organización que tiene la capacidad de administrar las comunicaciones telefónicas, la misma recibe la conexión de la PSTN de los proveedores de servicio para los números telefónicos y administra comunicación interna (entre extensiones). Actualmente, se le denominan IPPBX a las centrales telefónicas con capacidad para comunicarse por medio de las redes de datos con la tecnología y protocolos de la telefonía IP.

2.2.2. Definiciones generales relacionadas

De la vulnerabilidad denominada *"Spoofing Caller ID"* se pueden analizar algunas consecuencias o problemáticas cuando se aprovechan de la misma para generar llamadas con el fin de obtener algún beneficio o información, aprovechando la confianza que obtiene, en ocasiones, cuando se piensa que realmente el número que está llamando es de la institución o la persona que se muestra.

Es por eso por lo que, para facilitar la compresión del impacto generado por el enmascaramiento del identificador de llamadas, se definen los siguientes conceptos relacionados.

Un **ciberataque** se puede definir como un conjunto de acciones, llevadas a cabo por un individuo, o un grupo de individuos, por lo general contra sistemas informáticos, aprovechándose de vulnerabilidades u otros aspectos, normalmente se busca obtener algún beneficio, sin embargo, los ataques no solo van dirigidos a sistemas, sino también a personas. Lo anterior, por medio de la ingeniería social, que es una técnica, o conjunto de técnicas, que llevan a cabo actores mal intencionados para obtener información o datos normalmente sensibles o privados del individuo o de la empresa tales como: fechas, códigos, contraseñas, entre otros. Por lo general, primero se ganan la confianza de la víctima utilizando métodos de suplantación de identidad, ya sea sitios web falsos, correos falsos o enmascaramiento de un número telefónico, este último como resultado de aprovecharse del *"Spoofing Caller ID".* Después de un ataque de Ingeniera Social, donde en la mayoría de los casos la persona no se dio cuenta de que fue víctima de un ataque, se derivan otros temas como las estafas informáticas y fraudes con los datos facilitados por la víctima.

Otra metodología que es utilizada en conjunto con el "*Spoofing*" son las **"*Robocalls*",** que según la *Federal Communications Commission* (FCC), la cual es la comisión encargada de regular las telecomunicaciones en E.U (Estados Unidos), se definen como *"llamadas realizadas desde un marcador predictivo, o que contienen mensajes pregrabados",* son permitidas para usos como notificaciones e incluso si es para publicidad o "telemarketing", pero se deben tener documentos que autoricen ese fin. Sin embargo, al ser combinadas con el "*Spoofing Caller ID*" se utilizan para *spam*, intentos de estafa e ingeniería social.

La FFC, además de emitir regulaciones que deberían cumplir los proveedores en E.U., también propone algunas soluciones para la problemática del "*Spoofing*". Ha propuesto la autenticación del identificador de llamadas con la implementación de "***STIR/SHAKEN*",** que la FFC define como *un marco de estándares interconectados. STIR/SHAKEN son acrónimos de los estándares Secure Telephone Identity Revisited (STIR) y Signature-based Handling of Asserted Information Using toKENs (SHAKEN). Esto significa que las llamadas que viajan a través de redes telefónicas interconectadas pueden tener su identificación de llamante "firmada" como legítima por los operadores de origen y validada por otros operadores antes de llegar a los consumidores. STIR/SHAKEN valida digitalmente la transferencia de llamadas que atraviesan la compleja red de redes, permitiendo a la compañía telefónica del consumidor que recibe la llamada verificar que está realmente proviene del número mostrado en la identificación de llamante.*

STIR/SHAKEN tiene como objetivo mejorar la integridad general de la información de identificación del llamante y reducir la prevalencia de llamadas fraudulentas o no deseadas.

Capítulo 3. Marco Metodológico

3.1. Tipo de investigación

El trabajo de investigación busca evaluar la situación actual y realizar un análisis de la factibilidad para aplicar soluciones efectivas para minimizar el enmascaramiento del identificador de llamadas. Debido al impacto que tienen las técnicas de "*Spoofing Caller ID*" y su afectación a la población en general.

Con ese análisis se busca emitir un criterio que sirva de base para los entes reguladores y proveedores de servicios de aplicar técnicas que logren combatir el "*Spoofing*". Se determina que la investigación es de tipo evaluativa.

3.2. Alcance Investigativo

El alcance inicial de la investigación se define como exploratorio. Aunque existen varias soluciones propuestas para abordar la problemática, según la revisión de literatura, se encuentra que estas no son tan factibles o fáciles de aplicar. Además, la problemática persiste, y la vulnerabilidad continúa siendo explotada por actores malintencionados. Este enfoque exploratorio permitirá un análisis más detallado de las posibles soluciones y sus aplicaciones prácticas en el contexto del enmascaramiento del identificador de llamadas.

3.3. Enfoque

La investigación tiene características de un enfoque mixto, ya que incorpora elementos tanto cuantitativos como cualitativos

Cuantitativo: El análisis de la situación actual y la evaluación de la factibilidad de aplicar soluciones efectivas pueden implicar la recopilación y el análisis de datos cuantitativos. Por ejemplo, se podrían utilizar estadísticas relacionadas con incidentes de *"Spoofing Caller ID*", tasas de adopción de soluciones existentes, o encuestas cuantitativas para medir la percepción de la población sobre la problemática.

Cualitativo: La exploración de soluciones propuestas en la literatura y su aplicabilidad implica un enfoque cualitativo. La revisión de la literatura y el análisis detallado de las propuestas existentes pueden implicar la recopilación y la interpretación de información cualitativa. También se menciona la dificultad o facilidad de aplicar las soluciones, lo cual puede tener un componente cualitativo.

El enfoque de la investigación es mixto, permitiendo una aproximación a la problemática del enmascaramiento del identificador de llamadas.

3.4. Diseño

Dado que el enfoque de la investigación es mixto, el diseño de la investigación también podría ser mixto, combinando elementos tanto cuantitativos como cualitativos.

Por lo que en una primera fase el diseño es exploratorio para pasar a evaluativo en su segunda fase.

3.5. Población y muestreo

La población objetivo serían los usuarios de servicios de telefonía que se ven afectados por la problemática. También se realiza una recolección de datos con proveedores a nivel nacional para evaluar la factibilidad de la aplicación de un filtro.

3.5.1. Pruebas de Concepto: Se realizarán pruebas en un ambiente controlado para simular una red de interconexión de proveedores. Con el fin de aplicar las técnicas de "*spoofing"* y determinar la factibilidad técnica y eficiencia de un filtro de *"Caller ID"* en las rutas de un proveedor de servicios.

3.5.2. Entrevistas: Se realizarán entrevistas a personas con conocimientos técnicos en el área de telefonía, o que estén involucrados con estos procesos dentro de los proveedores de servicios.

3.5.3. Encuestas: Para valorar la percepción de la población y la afectación relacionada con el enmascaramiento de llamadas.

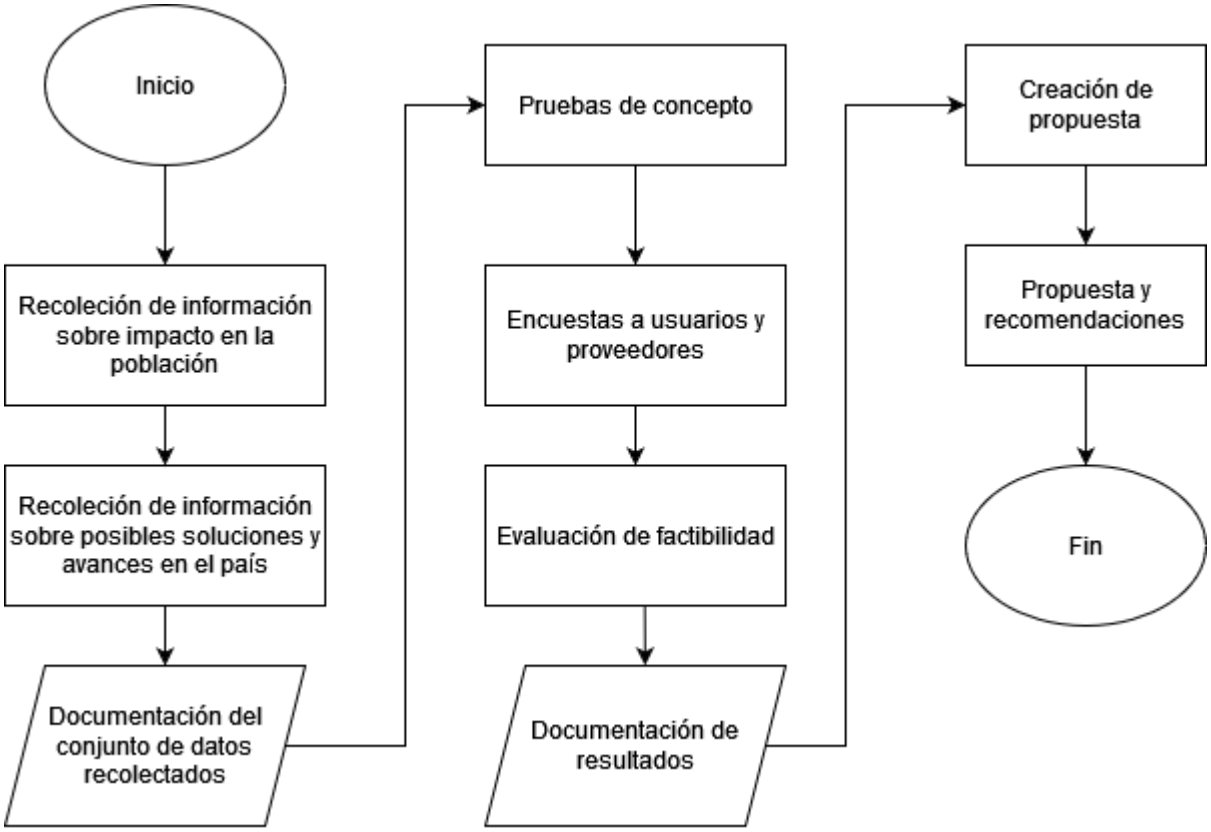
3.6. Técnicas de análisis de información

Se realiza un diagrama de flujo que muestra el proceso al realizar la recolección de datos, con las diferentes técnicas.

3.7 Diagrama de flujo

Figura 3

Diagrama de flujo de técnicas de análisis de información



Nota. Elaboración Propia.

Capítulo 4. Análisis del diagnóstico

Este capítulo se divide en tres secciones. En la primera parte se analizan los resultados de las pruebas de concepto realizadas en el ambiente de pruebas para la aplicación de las posibles soluciones. Este primer análisis tiene como objetivo revisar la factibilidad y efectividad de las soluciones para minimizar la eficacia de los ataques de *"Spoofing Caller ID"*.

La segunda sección analiza el impacto en los ciudadanos, lo vulnerables que pueden ser ante estas técnicas y, además, del conocimiento general de la población encuestada, sobre técnicas como el enmascaramiento del identificador de llamadas y como esto puede impactar en la confianza del usuario al recibir una llamada telefónica.

La tercera sección determina el interés y avance por parte de los proveedores en la implementación de técnicas que ayuden a minimizar la efectividad de un ataque de *"Spoofing Caller ID"*.

Con lo anterior se puede determinar el impacto debido a la importancia del tema, así como determinar la factibilidad de minimizar, o incluso eliminar, la problemática a raíz de estos ataques.

4.1. Prueba de concepto

Para un análisis más efectivo de la factibilidad técnica de la aplicación de filtros que permitan mitigar la efectividad de llamadas con un identificador de llamadas alterado, se prepara un ambiente con tres equipos donde se realizan las conexiones necesarias para la comunicación y establecimiento de llamadas por medio del protocolo SIP.

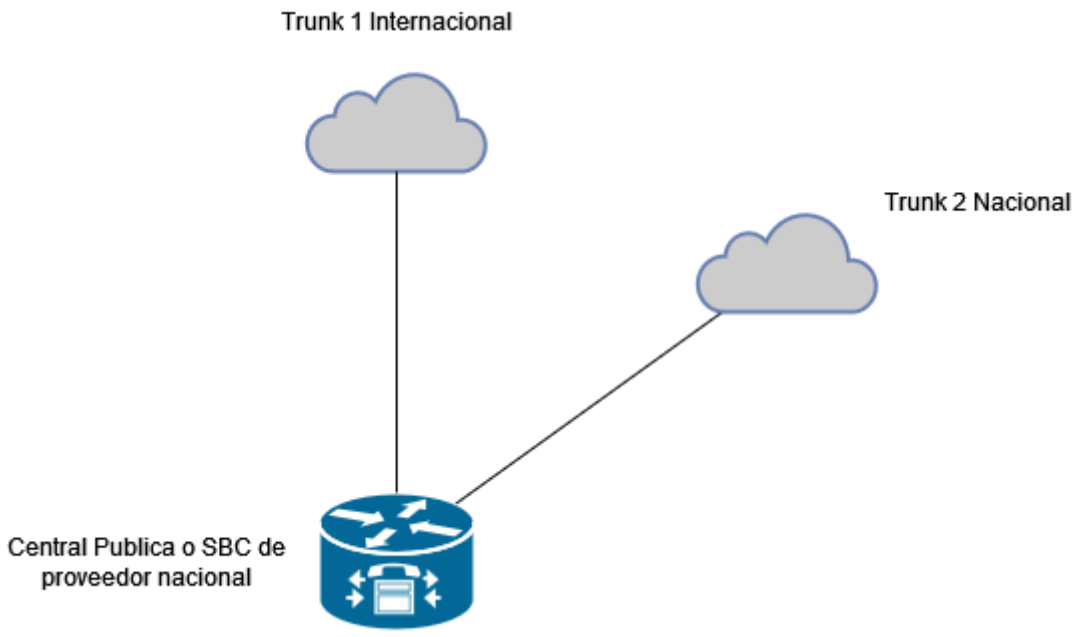
4.1.1. Escenarios

Se determinan dos escenarios posibles de las interconexiones de los proveedores, sin embargo, se va a hacer énfasis en el escenario donde los proveedores tienen conexión directa con proveedores internacionales para sus rutas de este tipo y con varios proveedores nacionales para el enrutamiento de las llamadas nacionales.

En el primer escenario planteado, el proveedor de servicios de telefonía tiene *"sip trunks"* o enlaces de SIP directos con los proveedores nacionales e internacionales, o bien para los internacionales utiliza una pasarela, pero las llamadas internacionales siempre llegan por esas rutas.

Figura 4

Escenario 1. Proveedor con comunicación directa a los proveedores.



Nota. Elaboración Propia. En este escenario el proveedor de servicios tiene sus interconexiones directas con otros proveedores.

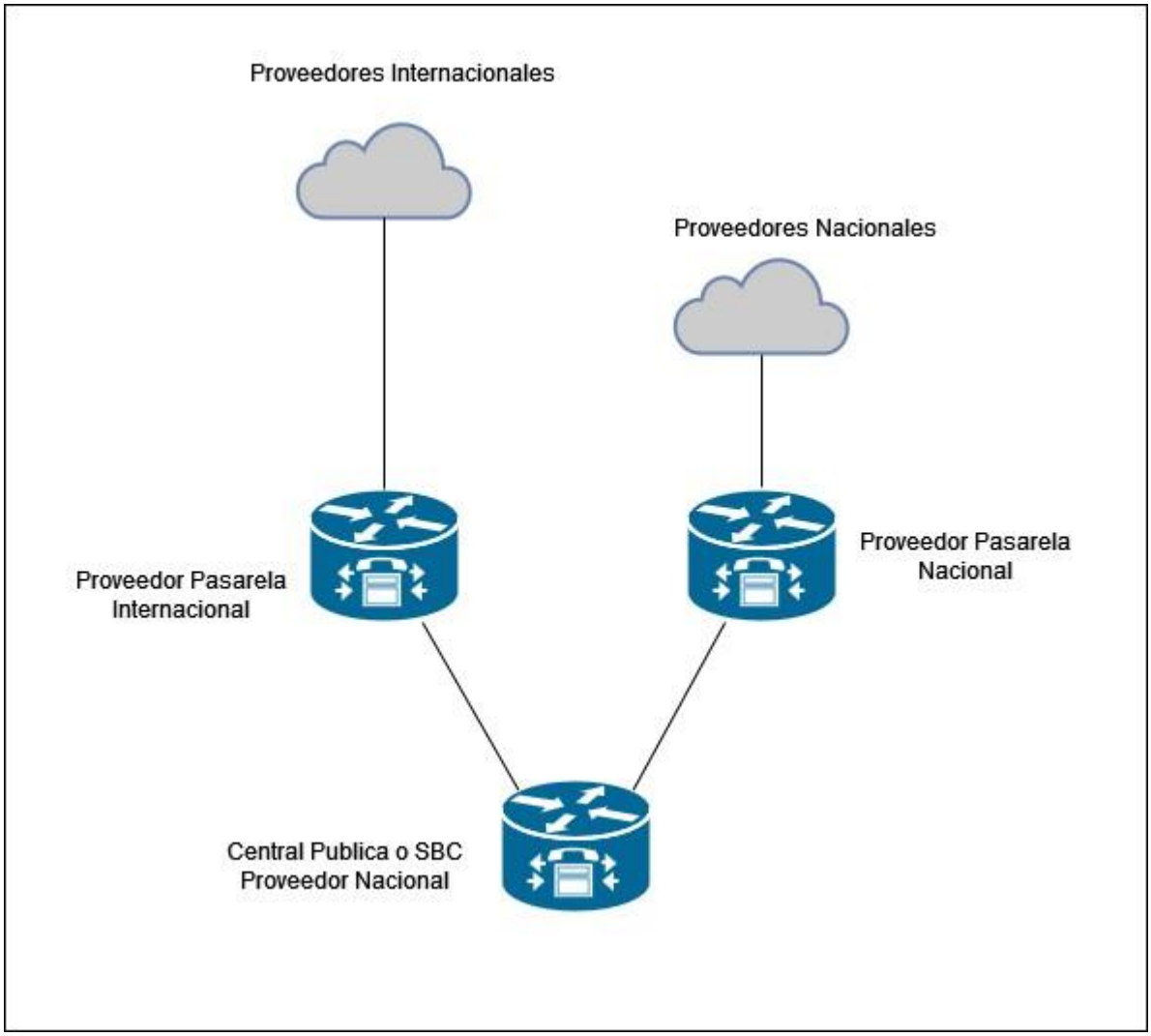
En el escenario dos, el proveedor nacional utiliza otros proveedores nacionales como pasarelas para sus intercomunicaciones, por lo que puede quedar sujeto a las

configuraciones aplicadas en los proveedores terceros para minimizar el *"Spoofing".*

Si el proveedor, en este escenario, tiene bien definido por cual pasarela puede venir el tráfico internacional y nacional, podría aplicar filtros basados en las rutas como se haría en el escenario 1, planteado anteriormente, de lo contrario, si el tráfico internacional y nacional puede proveenir de cualquier pasarela, está sujeto a las configuraciones de los otros proveedores.

Figura 5

Escenario 2. Proveedor con conexiones vía pasarelas.



Nota. Elaboración Propia. En este escenario el proveedor de servicios tiene sus interconexiones por medio de otros proveedores nacionales. Limitando las configuraciones que podria realizar.

Para ambos escenarios, los filtros se aplican a las rutas internacionales, donde no debería tener tráfico regular y válido que coincida con la numeración correspondiente a Costa Rica.

4.1.2. Equipo utilizado

Se utilizan los equipos detallados en la tabla 11 para simular un ambiente como el planteado en el escenario 1, mostrado en la figura 4.

Tabla 11

Equipos utilizados

Descripción	Equipo	Rol	IP	Host
Equipo A	IPPBX Cloud 3CX	Proveedor en ruta Internacional	x.x.23.101	saas.x.x
Equipo B	IPPBX Cloud 3CX	Proveedor en ruta Nacional	x.x.51.162	bluesky.x.x
Equipo C	IPPBX Grandstream	Proveedor Nacional – Central Pública	10.10.1.200	

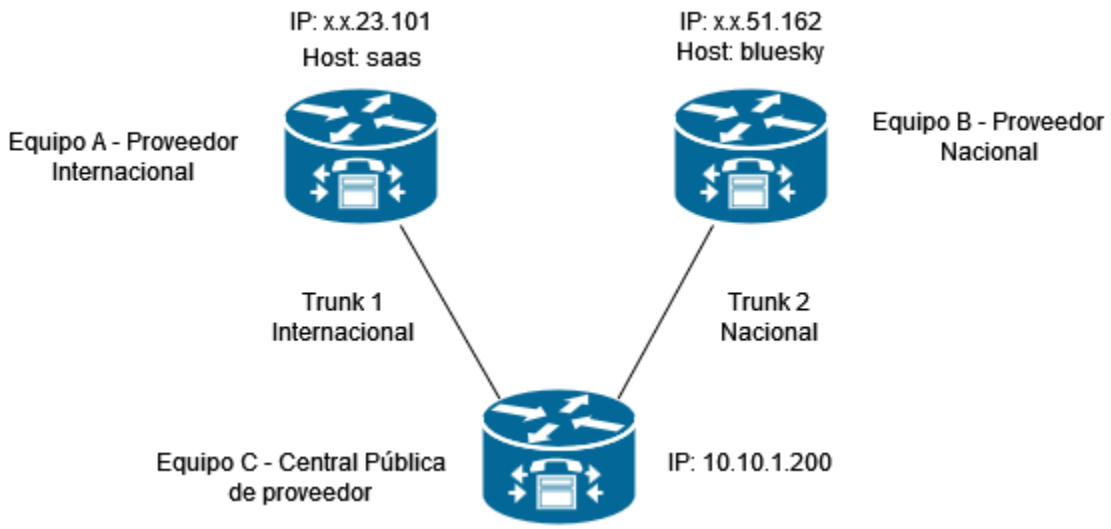
Nota. Los campos Host e IP se enmascaran para la protección de los equipos, pero se dejan los dos últimos octetos para facilitar la identificación en las capturas de red.

4.1.3. Configuraciones

Para simular el escenario 1, planteado en la figura 4, se realizan las siguientes configuraciones.

Figura 6

Enlaces entre equipos



Nota. Elaboración Propia

4.1.3.1. Equipo C con rol de Central Pública

Se crean dos enlaces "*SIP Trunk",* para realizar la comunicación con los equipos que simulan ser proveedores en el equipo C.

El enlace llamado "Trunk 1 Internacional" simula ser el enlace con un proveedor internacional y corresponde al equipo A, con la IP finalizada en "23.101".

El enlace llamado "Trunk 2 Nacional" simula ser el enlace con un proveedor nacional y corresponde al equipo B, con la IP finalizada en "51.162".

Figura 7

SIP Trunk en equipo con rol Central Pública

PROVIDER NAME	TERMINAL TYPE	TYPE	HOSTNAME/IP
Trunk 1 Internacional	SIP	peer	saas.
Trunk 2 Nacional	SIP	peer	bluesky.

Nota. Captura de la configuración en el equipo.

Se configuran las rutas entrantes que contienen las reglas que determinan donde debe ir la llamada, dependiendo de los filtros.

Rutas Entrantes

Para el enlace internacional se crean dos rutas entrantes, donde en la primera se especifica un número de prueba *+50688888888,* que simula el celular de un usuario final, y se permite cualquier identificador de llamadas para que la llamada se enrute correctamente a su destino final.

En la segunda ruta se establece el número de prueba, pero se le indica que sí contiene un "caller id" que inicia con los prefijos *+506xxxxxxxx*, *506xxxxxxxx*, *00506xxxxxxxx* o *xxxxxxxx*, donde "x" representa cualquier número del 0 al 9, lo cual correspondería a llamadas con la numeración de Costa Rica, la llamada debe ser enrutada a otro destino, para esta prueba, un destino que no existe, y de esta forma la llamada sea rechazada.

La lógica utilizada para crear los filtros se basa en el formato sugerido por la norma E.164, que establece que una llamada internacional se debe formar con los prefijos "+" o "00", luego código de país y por último el número, por lo que se determina que una llamada regular y válida no debería mostrar el *"caller id"* solo el prefijo *506* más 8 dígitos o solo 8 dígitos.

Figura 8

Rutas entrantes en equipo central pública para *SIP Trunk* 1 Internacional

INBOUND ROUTE NAME	PATTERN	CALLERID PATTERN	INBOUND MODE	INBOUND MODE SUFFIX	TIME CONDITION	TIME	TYPE	DESTINATION
	_+50688888888	No Limit	Default Mode		--	Default	--	Default Mode IVR -- test
	_+50688888888	_+506xxxxxxxx _506xxxxxxxx _00506xxxxxxxx ... More (1)	Default Mode		--	Default	--	Default Mode By DID -- Strip 0

Nota. Captura de la configuración en el equipo.

En el enlace nacional se configura una sola ruta entrante, para validar que el filtro de la internacional no afecte las rutas nacionales.

Se establece el mismo número de prueba que simula un número de un usuario final.

Figura 9

Rutas entrantes en equipo central pública para *SIP Trunk* 2 Nacional

INBOUND ROUTE NAME	PATTERN	CALLERID PATTERN	INBOUND MODE	INBOUND MODE SUFFIX	TIME CONDITION	TIME	TYPE	DESTINATION
	_+50688888888	No Limit	Default Mode		--	Default	--	Default Mode IVR -- test

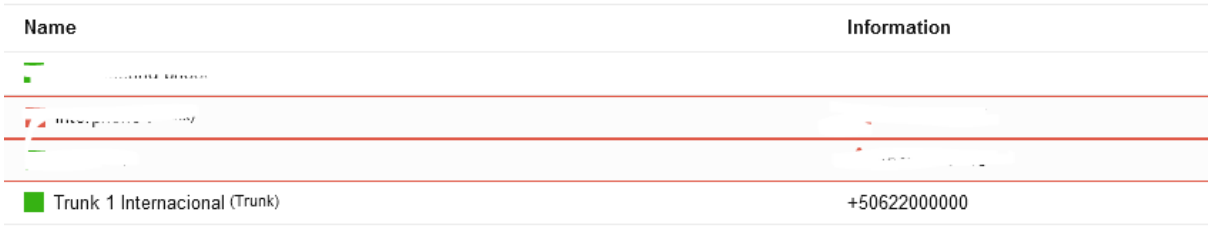
Nota. Captura de la configuración en el equipo.

4.1.3.2. Equipo A con rol de Proveedor Internacional

En el equipo A, asignado para simular el rol de proveedor internacional, se crea el enlace con el equipo C y la ruta saliente. Se le configura, de prueba, el número *+50622000000* para simular el número de una institución que el equipo C no debería recibir por esa ruta.

Figura 10

Enlace troncal en equipo A



Nota. Captura de la configuración en el equipo.

Figura 11

Ruta saliente hacia equipo C desde equipo A

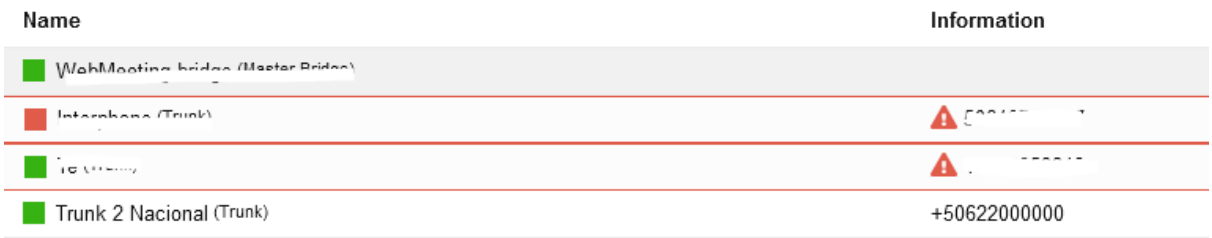
Nota. Captura de la configuración en el equipo.

4.1.3.3. Equipo B con rol de Proveedor Nacional

En el equipo B, asignado para simular el rol de proveedor internacional, se crea el enlace con el equipo C y la ruta saliente. Se le configura, de prueba, el número *+50622000000* para simular el número de una institución correspondiente a ese proveedor por lo que la llamada es válida.

Figura 12

Enlace troncal en equipo B



Nota. Captura de la configuración en el equipo.

Figura 13

Ruta saliente hacia equipo C desde equipo B

Outbound Rule Name	Prefix	Call from Ext.	Length	Department	Route 1
[redacted]		ALL			[redacted]
[redacted]		ALL			[redacted]
Equipo C		ALL	8		Trunk 2 Nacional

Nota. Captura de la configuración en el equipo.

4.1.4. Pruebas

En el ambiente de pruebas de concepto, se llevaron a cabo una serie de llamadas con el objetivo de evaluar la efectividad de las reglas aplicadas para la detección y prevención del *"Spoofing Caller ID".*

En el siguiente cuadro se muestran las pruebas realizadas y los resultados esperados y los obtenidos, así como los números de origen y destino establecidos para las pruebas.

Tabla 12

Tabla de resultados de las pruebas

Ruta	**NO**	**ND**	**Spoofed**	**RE**	**RO**
Internacional	+50622000000	+50688888888	Sí	Rejected	Rejected
Internacional	50622000000	+50688888888	Sí	Rejected	Rejected
Internacional	0050622000000	+50688888888	Sí	Rejected	Rejected
Internacional	22000000	+50688888888	Sí	Rejected	Rejected
Nacional	+50622000000	+50688888888	No	Completed	Completed
Nacional	50622000000	+50688888888	No	Completed	Completed
Nacional	22000000	+50688888888	No	Completed	Completed

Nota. Elaboración propia. NO= Número origen, ND= Número destino, RE= Respuesta esperada, RO= Respuesta Obtenida

Figura 14

Muestra de resultados de las llamadas.

Start Tim	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
0.000000	5.488424	[redacted]51.162	<sip:+50622000000@[redacted]51.162:5060>	<sip:+50688888888@10.10.1.200:5060>	SIP	00:00:05	6	COMPLETED	INVITE 200
29.252951	34.749457	[redacted]51.162	<sip:50622000000@[redacted]51.162:5060>	<sip:+50688888888@10.10.1.200:5060>	SIP	00:00:05	6	COMPLETED	INVITE 200
55.410032	60.888476	[redacted]51.162	<sip:22000000@[redacted]51.162:5060>	<sip:+50688888888@10.10.1.200:5060>	SIP	00:00:05	6	COMPLETED	INVITE 200
97.190388	97.512412	[redacted]23.101	<sip:+50622000000@[redacted]23.101:5060>	<sip:+50688888888@10.10.1.200:5060>	SIP	00:00:00	4	REJECTED	INVITE 404
108.388895	108.727551	[redacted]23.101	<sip:50622000000@[redacted]23.101:5060>	<sip:+50688888888@10.10.1.200:5060>	SIP	00:00:00	4	REJECTED	INVITE 404
120.379476	120.716662	[redacted]23.101	<sip:22000000@[redacted]23.101:5060>	<sip:+50688888888@10.10.1.200:5060>	SIP	00:00:00	4	REJECTED	INVITE 404
135.897700	136.229041	[redacted]23.101	<sip:0050622000000@[redacted]23.101:5060>	<sip:+50688888888@10.10.1.200:5060>	SIP	00:00:00	4	REJECTED	INVITE 404

Pruebas desde ruta internacional

Prueba 1. Se realiza una llamada desde el equipo A hacia el equipo C, utilizando la ruta internacional para simular una llamada con el identificador de llamadas enmascarado que aparenta ser de una institución o empresa con el número *+50622000000* hacia el número telefónico celular establecido de prueba para un usuario final *+50688888888*.

En la figura 15 se puede observar que el campo *"From",* el cual es el campo que se determina el identificador de llamadas, muestra el número +50622000000.

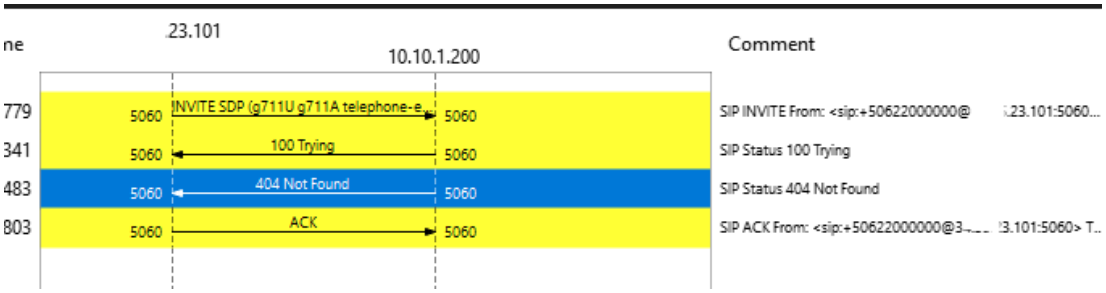
Figura 15

Paquete "*Invite"* de la llamada realizada en Prueba 1

En la figura 16 se observa el flujo de la llamada, donde el equipo A envia la llamada al equipo C y este último termina por rechazar la llamada.

Figura 16

Flujo de la llamada en prueba 1

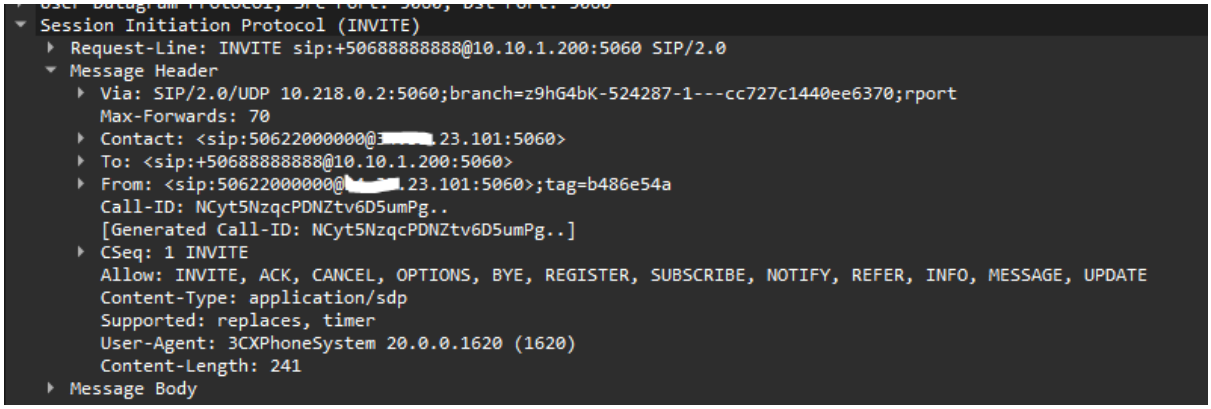


Prueba 2. Se realiza una llamada desde el equipo A hacia el equipo C, utilizando la ruta internacional para simular una llamada con el identificador de llamadas enmascarado que aparenta ser de una institución o empresa con el número *50622000000* hacia el número telefónico celular establecido de prueba para un usuario final *+50688888888*.

En la figura 17 se puede observar que el campo *"From"* muestra el número 50622000000.

Figura 17

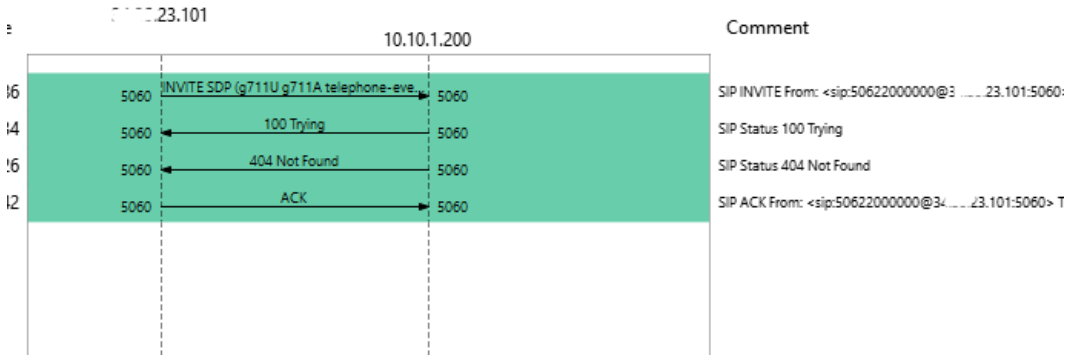
Paquete “*Invite”* de la llamada realizada en Prueba 2



En la figura 18 se observa el flujo de la llamada, donde el equipo A envia la llamada al equipo C y este último termina por rechazar la llamada.

Figura 18

Flujo de la llamada en prueba 2



Prueba 3. Se realiza una llamada desde el equipo A hacia el equipo C, utilizando la ruta internacional para simular una llamada con el identificador de llamadas enmascarado que aparenta ser de una institución o empresa con el número 00506*22000000* hacia el número telefónico celular establecido de prueba para un usuario final *+50688888888*.

En la figura 19 se puede observar que el campo *“From”* muestra el número 0050622000000.

Figura 19

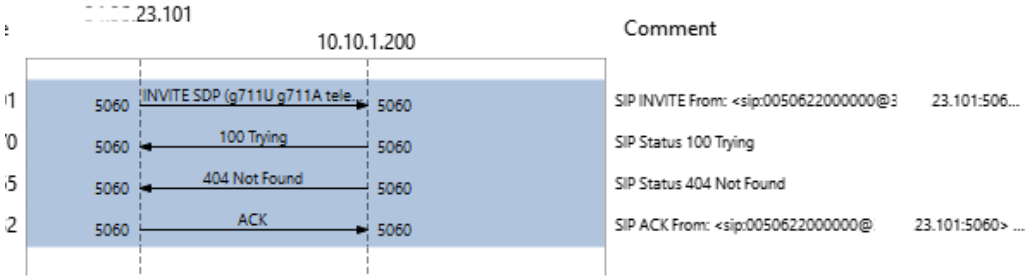
Paquete “*Invite”* de la llamada realizada en Prueba 3

```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:+50688888888@10.10.1.200:5060 SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 10.218.0.2:5060;branch=z9hG4bK-524287-1---5d02cb2c442ec95a;rport
    Max-Forwards: 70
    Contact: <sip:0050622000000@3[redacted]23.101:5060>
    To: <sip:+50688888888@10.10.1.200:5060>
    From: <sip:0050622000000@3[redacted]23.101:5060>;tag=59c27759
    Call-ID: BGIYrv0bh40H6LU11-Q8SQ..
    [Generated Call-ID: BGIYrv0bh40H6LU11-Q8SQ..]
    CSeq: 1 INVITE
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE, UPDATE
    Content-Type: application/sdp
    Supported: replaces, timer
    User-Agent: 3CXPhoneSystem 20.0.0.1620 (1620)
    Content-Length: 241
  Message Body
```

En la figura 20 se observa el flujo de la llamada, donde el equipo A envia la llamada al equipo C y este último termina por rechazar la llamada.

Figura 20

Flujo de la llamada en prueba 3



Prueba 4. Se realiza una llamada desde el equipo A hacia el equipo C, utilizando la ruta internacional para simular una llamada con el identificador de llamadas enmascarado que aparenta ser de una institución o empresa con el número *22000000* hacia el número telefónico celular establecido de prueba para un usuario final *+50688888888*.

En la figura 21 se puede observar que el campo *"From"* muestra el número 22000000.

Figura 21

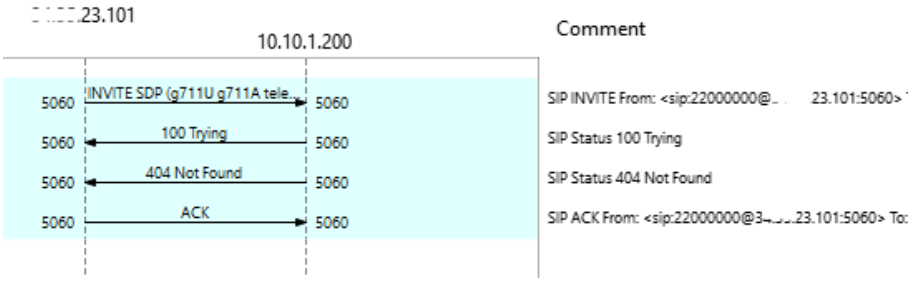
Paquete "*Invite"* de la llamada realizada en Prueba 4

```
Session Initiation Protocol (INVITE)
  Request-Line: INVITE sip:+50688888888@10.10.1.200:5060 SIP/2.0
  Message Header
    Via: SIP/2.0/UDP 10.218.0.2:5060;branch=z9hG4bK-524287-1---7fc6b94a773f925a;rport
    Max-Forwards: 70
    Contact: <sip:22000000@3[redacted]23.101:5060>
    To: <sip:+50688888888@10.10.1.200:5060>
    From: <sip:22000000@3[redacted].23.101:5060>;tag=64d84e03
    Call-ID: WUnuCqCQvOmbl2ieYQWvvA..
    [Generated Call-ID: WUnuCqCQvOmbl2ieYQWvvA..]
    CSeq: 1 INVITE
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REGISTER, SUBSCRIBE, NOTIFY, REFER, INFO, MESSAGE, UPDATE
    Content-Type: application/sdp
    Supported: replaces, timer
    User-Agent: 3CXPhoneSystem 20.0.0.1620 (1620)
    Content-Length: 240
```

En la figura 22 se observa el flujo de la llamada, donde el equipo A envia la llamada al equipo C y este último termina por rechazar la llamada.

Figura 22

Flujo de la llamada en prueba 4



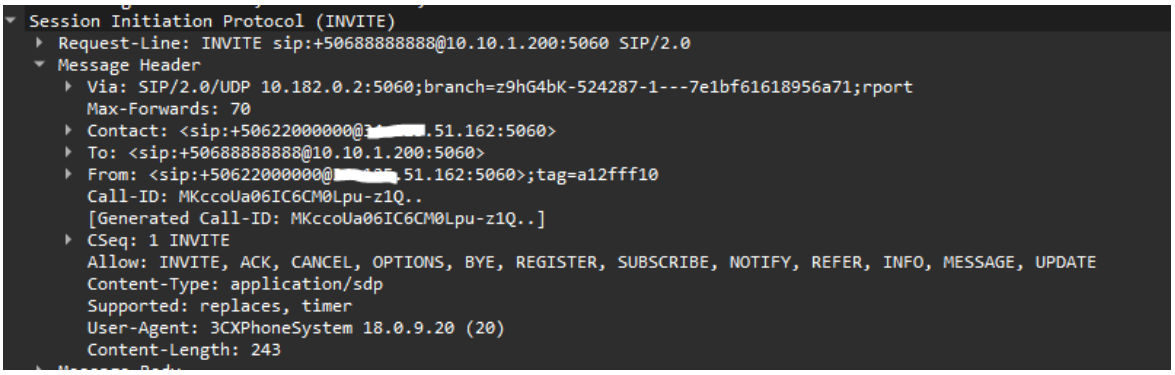
Pruebas desde ruta nacional

Prueba 5. Se realiza una llamada desde el equipo B hacia el equipo C, utilizando la ruta nacional para simular una llamada desde una institución o empresa con el número *+50622000000* hacia el número telefónico celular establecido de prueba para un usuario final *+50688888888*.

En la figura 23 se puede observar que el campo *"From"* muestra el número +50622000000.

Figura 23

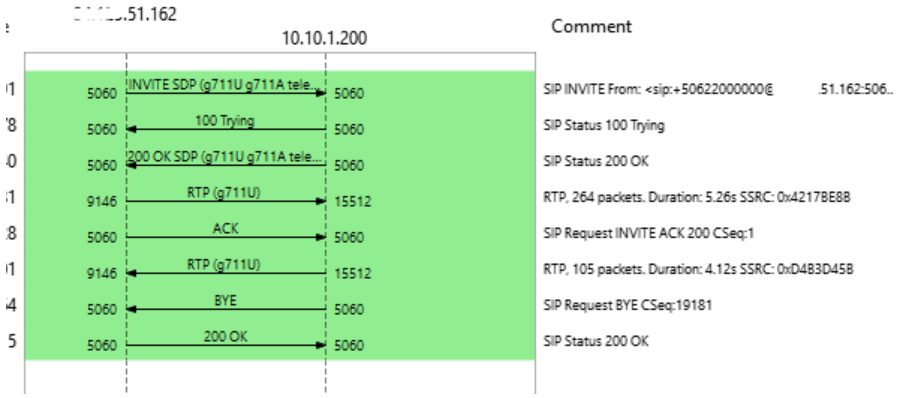
Paquete "*Invite"* de la llamada realizada en Prueba 5



En la figura 24 se observa el flujo de la llamada, donde el equipo B envia la llamada al equipo C, la cual se enruta y se establece de manera correcta.

Figura 24

Flujo de la llamada en prueba 5

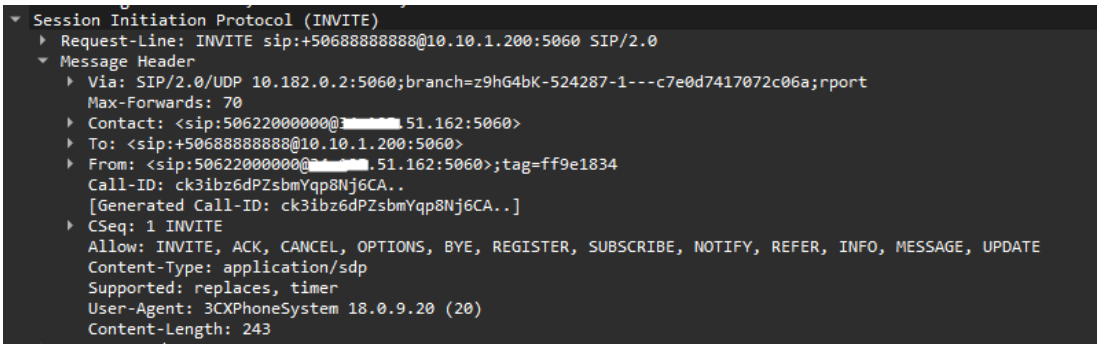


Prueba 6. Se realiza una llamada desde el equipo B hacia el equipo C, utilizando la ruta nacional para simular una llamada desde una institución o empresa con el número *50622000000* hacia el número telefónico celular establecido de prueba para un usuario final *+50688888888*.

En la figura 25 se puede observar que el campo *"From"* muestra el número 50622000000.

Figura 25

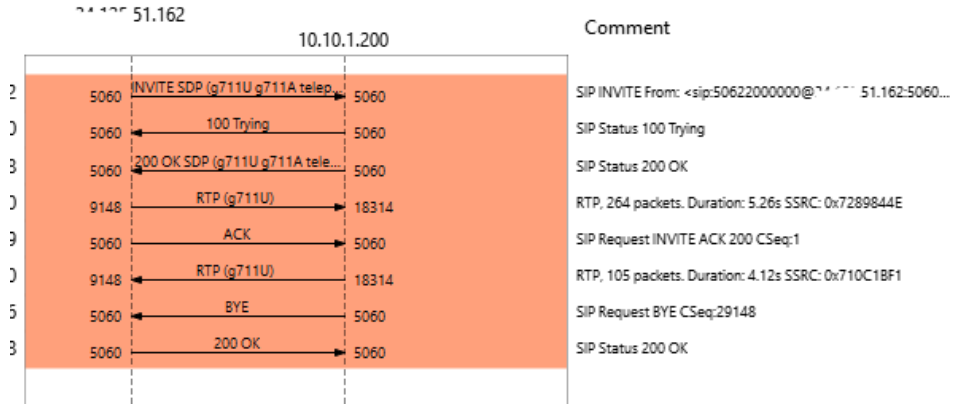
Paquete "*Invite"* de la llamada realizada en Prueba 6



En la figura 26 se observa el flujo de la llamada, donde el equipo B envia la llamada al equipo C, la cual se enruta y se establece de manera correcta.

Figura 26

Flujo de la llamada en prueba 6.

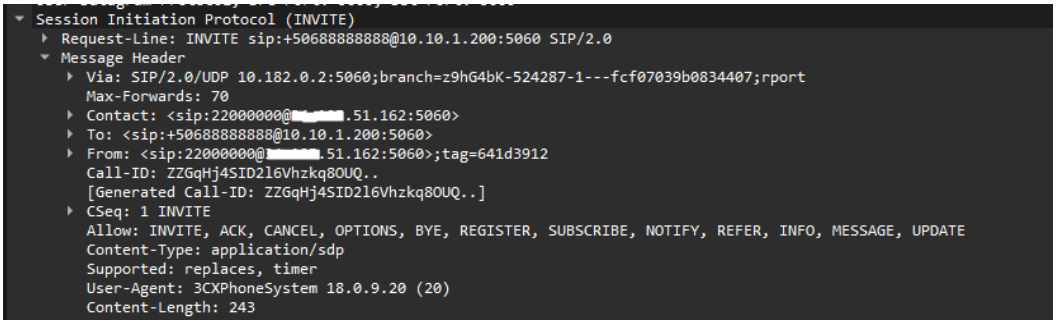


Prueba 7. Se realiza una llamada desde el equipo B hacia el equipo C, utilizando la ruta nacional para simular una llamada desde una institución o empresa con el número *22000000* hacia el número telefónico celular establecido de prueba para un usuario final *+50688888888*.

En la figura 27 se puede observar que el campo *"From"* muestra el número 22000000.

Figura 27

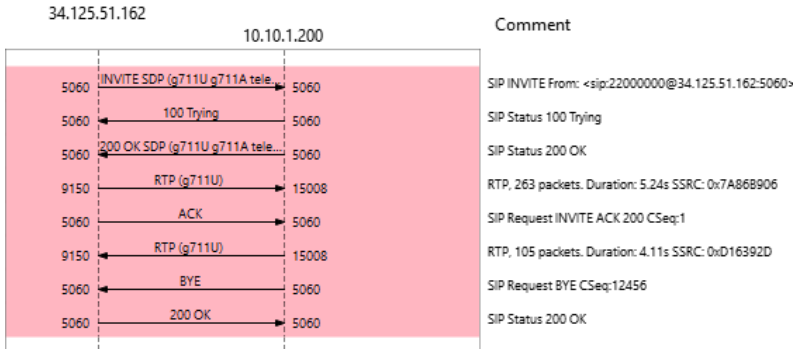
Paquete "*Invite"* de la llamada realizada en Prueba 7.



En la figura 28 se observa el flujo de la llamada, donde el equipo B envia la llamada al equipo C, la cual se enruta y se establece de manera correcta.

Figura 28

Flujo de la llamada en prueba 7



4.1.5. Análisis de los resultados

Después de la implementación de los filtros en la ruta internacional, se determina que el equipo C, simulando una central pública o un SBC de un proveedor nacional, logró con éxito enrutar la llamada con el número enmascarado hacia un destino para su rechazo. Como se visualiza en la tabla 12, donde los resultados fueron conforme a lo esperado al rechazar las llamadas clasificadas como irregulares, ya que coincidían con el formato del identificador de llamadas para Costa Rica, el cual no debería estar recibiendo llamadas por la troncal internacional.

Además, los filtros fueron efectivos para otros intentos de enmascaramiento que no cumplen con la normativa E.164 pero que intentan coincidir con numeración nacional, siendo por lo tanto también consideradas irregulares. Esto se debe a que una llamada proveniente de una ruta internacional debería mostrar en el identificador el prefijo "+" o "00", seguido del código de país correspondiente.

Estos resultados confirman la efectividad de los filtros implementados para detectar y rechazar llamadas irregulares que intentan enmascarar su identificador de llamadas de manera fraudulenta.

Se determina que técnicamente el equipo es capaz, con la correcta configuración, de minimizar el establecimiento de llamadas enmascaradas provenientes de proveedores internacionales.

4.2. Prueba con proveedores

Con el fin de validar que la vulnerabilidad del "*spoofing caller id*" en el país, se realizan pruebas con servicios de *VoIP* brindados por un proveedor nacional y otro internacional, de esta manera confirmar que sin los filtros y aplicación de buenas prácticas es posible realizar llamadas correctas con un identificador de llamadas alterado.

4.2.1 Proveedor Internacional

Se utiliza un servicio prepago de un proveedor de Canadá donde se realizan llamadas a número de proveedores en Costa Rica. Los números utilizados para realizar las pruebas de enmascaramiento del identificador de llamadas son propios, hacia números propios.

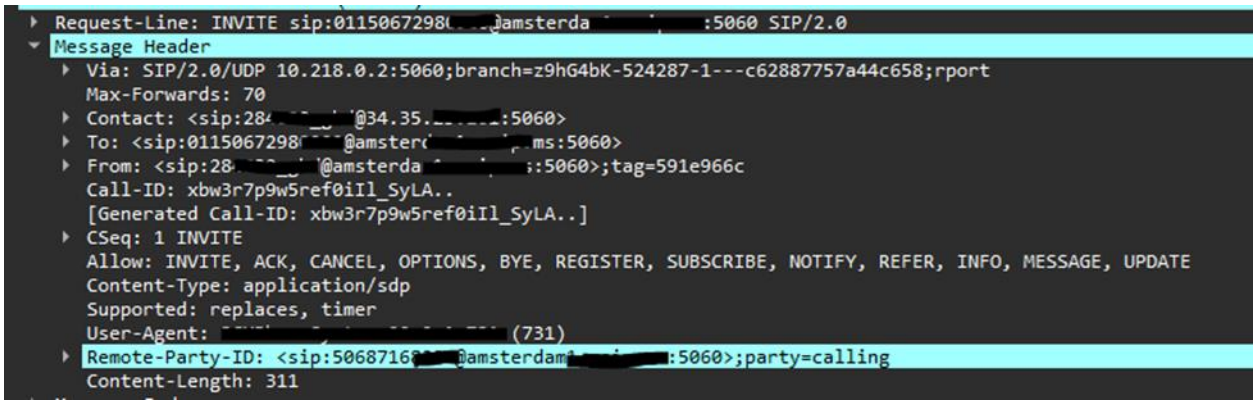
Figura 29

PO	NO	PD	ND	RE	RO
PI1	+5068716xxxx	PN1	+5068716xxxx	Rejected	Completed
PI1	+5068716xxxx	PN2	+5067298xxxx	Rejected	Incompleted

Nota. Elaboración propia. PO=Proveedor de origen, PD=Proveedor destino, NO= Número origen, ND= Número destino, RE= Respuesta esperada, RO= Respuesta Obtenida.

En la figura 30 se observa que se utiliza el número 5068716xxxx en el campo "*Remote-Party-ID"* que en este ejemplo configura el "*Caller Id",* el mismo corresponde a un número telefónico registrado en Costa Rica y luego se llama hacia Costa Rica donde se marca 011 para tomar ruta internacional y 5067298xxxx correspondiente a un número de Costa Rica.

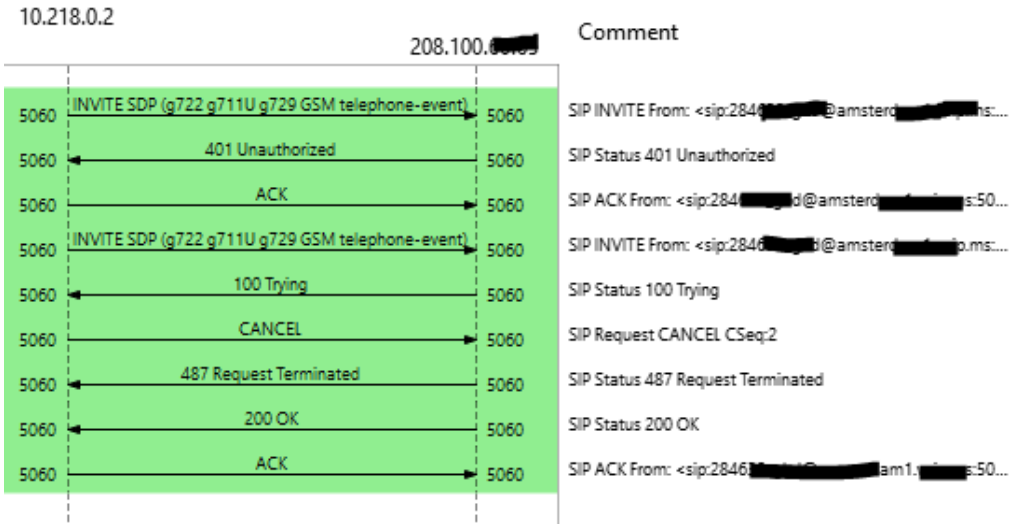
Figura 30



En la figura 31 se puede observar que la llamada no se establece desde PI1 hacia PN2.

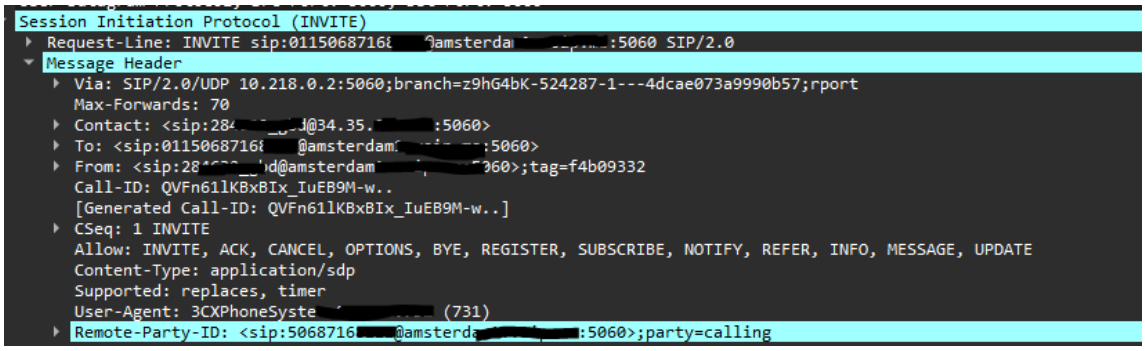
Lo cual indica que el proveedor podría estar filtrando estas llamadas o no logrando enrutarlas correctamente.

Figura 31



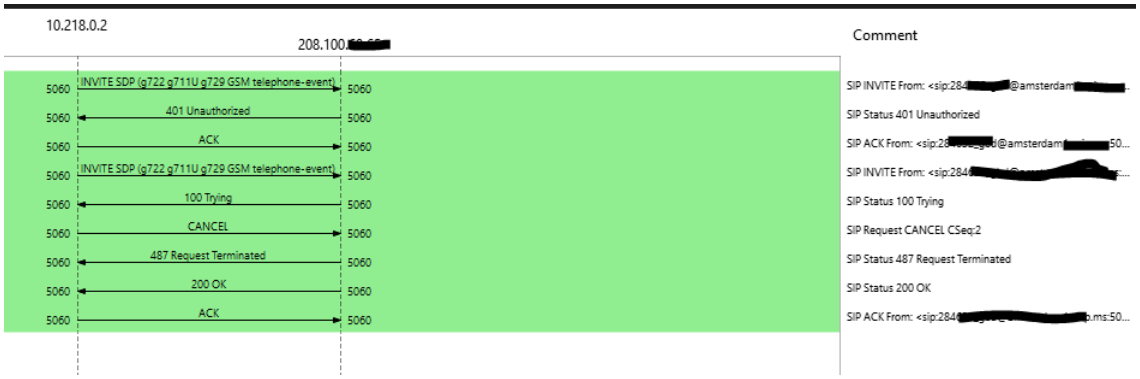
En la figura 32 se observa que se utiliza el número 5068716xxxx en el campo "*Remote-Party-ID"* que en este ejemplo configura el "*Caller Id",* el mismo corresponde a un número telefónico registrado en Costa Rica y luego se llama hacia Costa Rica donde se marca 011 para tomar ruta internacional y 5068716xxxx correspondiente a un número de Costa Rica.

Figura 32



En la figura 33 se puede observar que la llamada se establecio correctamente desde PI1 hacia PN1.

Figura 33



4.2.2 Proveedor Nacional

Se utiliza un servicio prepago de un proveedor de Costa Rica regulada por Sugef donde se realizan llamadas a otros proveedores en Costa Rica. Los números utilizados para realizar las pruebas de enmascaramiento del identificador de llamadas son propios, hacia números propios.

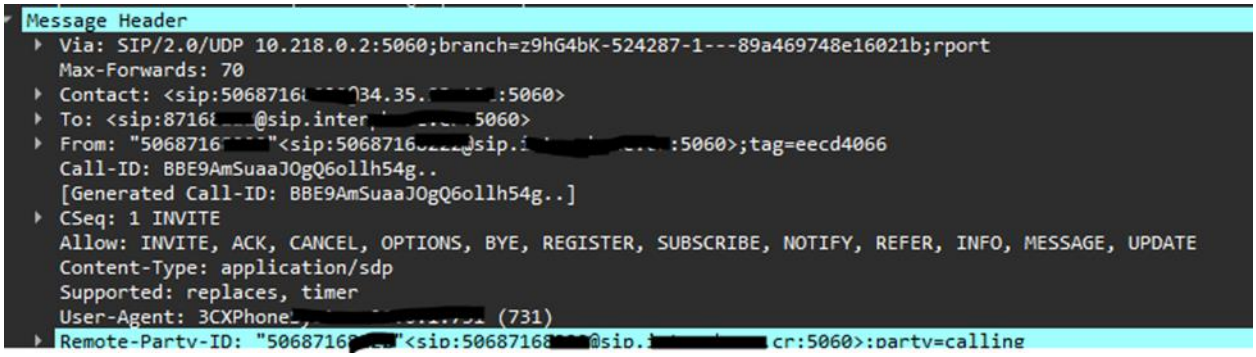
Figura 34

PN3	+5068716xxxx	PN1	8716xxxx	Rejected	Completed
PN3	+5068716xxxx	PN2	7298xxxx	Rejected	Completed

Nota. Elaboración propia. PO=Proveedor de origen, PD=Proveedor destino, NO= Número origen, ND= Número destino, RE= Respuesta esperada, RO= Respuesta Obtenida.

En la figura 35 se observa que se utiliza el número 5068716xxxx en el campo "*From"* que en este ejemplo configura el "*Caller Id",* el mismo corresponde a un número telefonico registrado en Costa Rica y luego se llama hacia el número 8716xxxx correspondiente a un número de Costa Rica.

Figura 35

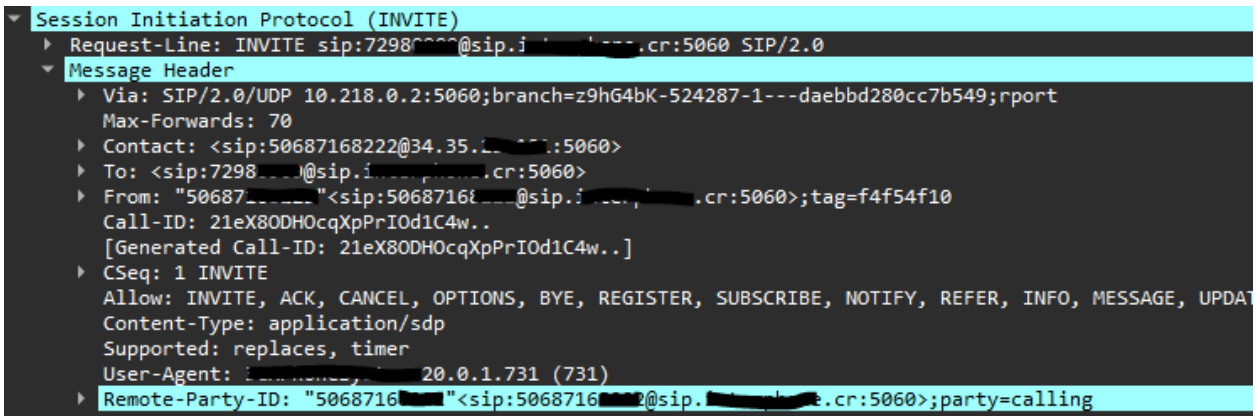


En la figura 36 se puede observar que la llamada se establecio correctamente desde PN3 hacia PN1 con un identificador que no corresponde al contratado, lo que deja la posibilidad de utilizar cualquier identificador de llamadas debido a la falta de la aplicación de las normativas y estándares. .

Figura 36

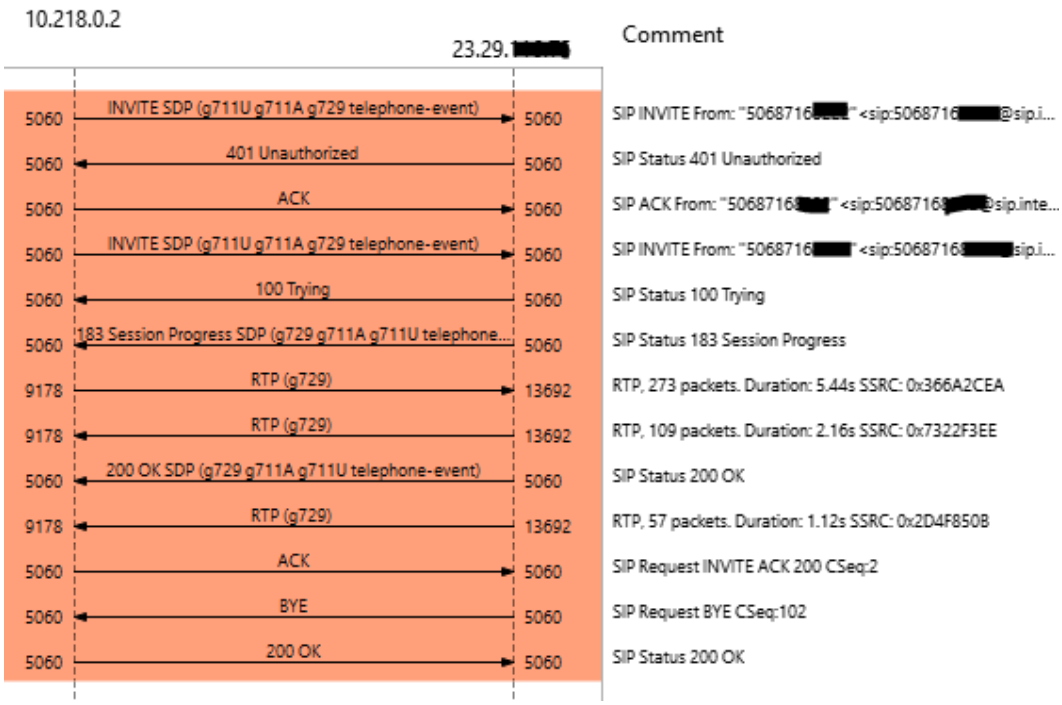
En la figura 37 se observa que se utiliza el número 5068716xxxx en el campo "*From"* que en este ejemplo configura el "*Caller Id",* el mismo corresponde a un número telefonico registrado en Costa Rica y luego se llama hacia el número 7298xxxx correspondiente a un número de Costa Rica.

Figura 37



En la figura 38 se puede observar que la llamada se establecio correctamente desde PN3 hacia PN2 que con la primera prueba no logro establecer, esto debido a que es posible que encuentre que el número tiene un origen a una ruta nacional. .

Figura 38



Capítulo 6. Conclusiones y recomendaciones

A continuación, se presentan las conclusiones que corresponden a cada objetivo planteado en la presente investigación.

6.1. Conclusiones

6.1.1. Conclusiones del primer objetivo.

Investigar las mejores prácticas aplicables a nivel nacional que minimicen los medios que permiten la suplantación de números telefónicos.

El objetivo se cumple y se concluye que:

- Después del análisis de las diferentes técnicas propuestas en distintos artículos, patentes y nuevos protocolos sobre métodos existentes o nuevas formas de minimizar la efectividad de la suplantación se encuentra que el más factible para la aplicación a nivel nacional son:

- **Aplicación de Filtros en Rutas Internacionales**: La implementación de filtros en las rutas internacionales ha demostrado ser una medida efectiva para detectar y rechazar llamadas fraudulentas que intentan enmascarar su identificador de llamadas. Esto ayuda a bloquear el acceso de llamadas con identificadores irregulares o sospechosos que provienen de fuera del país, reduciendo así la vulnerabilidad ante el *Spoofing Caller ID*.

- **Cumplimiento de la Normativa E.164**: El cumplimiento de la normativa E.164, que establece estándares para el formato de los números telefónicos a nivel internacional, es fundamental para asegurar la autenticidad y legitimidad de las llamadas. Garantizar que los identificadores de llamadas cumplan con este estándar ayuda a prevenir la suplantación de números telefónicos y a mantener la integridad de las comunicaciones.

6.1.2. Conclusiones del segundo objetivo.

Conocer las limitaciones actuales por las cuales no se han aplicado acciones que ayuden a disminuir la suplantación de números telefónicos institucionales.

El objetivo se cumple y se concluye que:

- La Superintendencia de Telecomunicaciones (SUTEL) como ente encargado de regular las telecomunicaciones a pesar de que emitió una resolución para la aplicación de filtros en la que se estuvo trabajando desde finales de 2021 hasta finales de 2023, la misma no ha sido aún implementada por los proveedores debido a que algunos emitieron un recurso. Adicionalmente, la SUTEL indica que no supervisa, ni emite guías o estándares a nivel nacional obligatorios para todos los proveedores, por lo que cada proveedor establece sus propias configuraciones las cuales no siempre cumplen con las normas sugeridas internacionalmente y lo que permite que por errores de configuración se pueda realizar un enmascaramiento utilizando un servicio de un proveedor local.
- Por su parte el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MITCITT) en una sesión virtual dada en el 2021, indica que ellos a pesar de ser conscientes del impacto de la problemática generada por el enmascaramiento, no tiene injerencia en el tema y por eso no toman acciones para minimizarlo.
- Lo anterior genera que los proveedores que, si buscan solventar la situación o tienen la capacidad y el conocimiento para aplicarlo, no hayan logrado algún avance, debido a la poca coordinación entre proveedores y las entidades regulatorias.

6.1.3. Conclusiones del tercer objetivo.

Realizar pruebas que ayuden a identificar cómo los delincuentes se aprovechan de la vulnerabilidad que permite intentos de estafa.

El objetivo se cumple y se concluye que:

- A pesar de ser una problemática mundial y que en países como EUA (Estados Unidos de América) causa un impacto considerable en la población y han implementado entre sus proveedores protocolos como el "STIR/SHAKEN" la misma solo es obligatoria para los proveedores mayores, adicionalmente el "*Spoofing Caller ID*" no es considerado ilegal del todo por las leyes de ese país, siempre y cuando se utilice para fines legítimos, lo que deja un portillo a que se puedan utilizar proveedores de ese país y otros, para realizar llamadas exitosas que utilicen la técnica el enmascaramiento.
- La existencia de aplicaciones como "*SpoofCard*" y otras que se venden para protección de la privacidad, permiten de una manera sencilla a una persona enmascarar el número, si bien las tiendas de aplicaciones limitaron estas aplicaciones, las mismas ahora han restringido a ciertos países su uso, sin embargo, esto no limita que personas mal intencionadas en el país logren tener una cuenta y utilizarlas para intentos de fraude.

6.1.4. Conclusiones del cuarto objetivo.

Analizar las posibilidades de la aplicación de mejores prácticas que limiten los medios que permiten la suplantación de números telefónicos en el País.

El objetivo se cumple y se concluye que:

- A nivel técnico es factible para los proveedores aplicar reglas o filtros a nivel de sus interconexiones con otros proveedores. Para facilitar las configuraciones específicamente en conexiones con rutas internacionales de esta manera restringir que las llamadas con el identificador enmascarado se logren establecer correctamente. Lo anterior se probó en un ambiente de pruebas simulando un escenario común para los proveedores. Aún no se ha probado directamente en equipos en producción en la red de un proveedor.
- Los proveedores nacionales pueden utilizar la norma E.164 para las interconexiones incluso nacionales y de esta forma todos seguir un estándar.
- Los proveedores nacionales pueden restringir que un cliente envíe un número que no corresponde al servicio contratado, evitando que sus servicios sean utilizados para hacer una llamada con la técnica del "*spoofing"*.

6.2. Recomendaciones

A continuación, se mencionan recomendaciones basadas en la investigación y la experiencia en el tema, considerando procesos, y factibilidades técnicas.

- **Implementación de filtros en interconexiones entre proveedores:** Para los proveedores, debido al costo y dificulta de la implementación de protocolos como "*STIR/SHAKEN*", se pueden implementar filtros a nivel de rutas para detectar llamadas irregulares, sin embargo, a pesar de que estos filtros se pueden aplicar a nivel de todas las conexiones entre proveedores, ya que no hay portabilidad numérica en números fijos, los números telefónicos están bien identificados a cual proveedor pertenecen, por lo que se puede definir por la ruta que debería ser permitido, aunque lo anterior sea posible se recomienda aplicarlo a nivel de rutas internacionales para facilitar su implementación.

- **Establecer guías y homologaciones:** Las entidades regulatorias, como la Superintendencia de Telecomunicaciones (SUTEL), junto con los proveedores de servicios telefónicos, deben trabajar en conjunto para desarrollar guías y políticas internas claras y detalladas. Estas guías deben abordar aspectos técnicos, de seguridad y operativos relacionados con la implementación de servicios telefónicos, incluyendo medidas para prevenir el *"spoofing*" del identificador de llamadas.

  La homologación implica establecer estándares y prácticas comunes que todos los proveedores de servicios telefónicos regulados por la SUTEL deben seguir. Esto incluye la adopción de protocolos de seguridad, la configuración adecuada de redes y sistemas, y la implementación de medidas de prevención de fraudes telefónicos. La homologación garantiza coherencia y consistencia en las operaciones de todos los actores del sector.

- **Colaboración entre entidades:** Para proveedores, fortalecer la comunicación y colaboración entre proveedores por medio de comités técnicos integrados por expertos de diferentes proveedores para analizar a fondo los desafíos técnicos asociados con el *"spoofing*" del identificador de llamadas. Estos comités pueden desarrollar estrategias y soluciones técnicas que puedan ser implementadas de manera coordinada por todos los participantes minimizando las dificultades de implementación de cada proveedor.

- **Capacitaciones en los proveedores:** Los proveedores de servicios telefónicos deben organizar sesiones de capacitación interna para todo su personal, incluyendo técnicos, administradores de sistemas y personal de atención al cliente. Estas

sesiones deben enfocarse en las guías y políticas establecidas para prevenir el "spoofing", explicando detalladamente las medidas de seguridad y las mejores prácticas a seguir.

Capitulo 7. Bibliografía

Buriachok, V., Sokolov, V., & TajDini, M. (2020). Research of caller ID spoofing launch, detection, and defense. Kìberbezpeka. Osvìta, Nauka, Tehnìka, 3(7), 6–16. https://doi.org/10.28925/2663-4023.2020.7.616

IEEE Xplore. (2014). You can call but you can't hide: Detecting caller ID spoofing attacks. IEEE Conference Publication. https://ieeexplore.ieee.org/document/6903577

IEEE Xplore. (2017). One-time key issuing for verification and detecting caller ID spoofing attacks. IEEE Conference Publication. https://ieeexplore.ieee.org/abstract/document/8025898

IEEE Xplore. (2018). Increasing the efficiency of one-time key issuing for the first verification caller ID spoofing attacks. IEEE Conference Publication. https://ieeexplore.ieee.org/document/8457341

Li, J., Faria, F., Chen, J., & Liang, D. (2017). A mechanism to authenticate caller ID. En Advances in Intelligent Systems and Computing (pp. 745–753). https://doi.org/10.1007/978-3-319-56538-5_75

Mustafa, H. A., Xu, W., Sadeghi, A., & Schulz, S. (2018). 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

Tesema, S. N., & Shiferaw, Y. N. (2014). Securing confidentiality and integrity of SIP based VoIP system in reduced call setup time. ResearchGate. https://www.researchgate.net/publication/355406821

Wang, S., Delavar, M., Azad, M. A., Nabizadeh, F., Smith, S. M., & Hao, F. (2023). Spoofing against spoofing: Towards caller ID verification in heterogeneous telecommunication systems. ACM Transactions on Privacy and Security, 27(1), 1-25. https://doi.org/10.1145/3625546