ATIS STANDARD

ATIS-1000072

Analysis of Mitigation Techniques for Calling Party Spoofing

TECHNICAL REPORT

As a leading technology and solutions development organization, the Alliance for Telecommunications Industry Solutions (ATIS) brings together the top global ICT companies to advance the industry's most pressing business priorities. ATIS' nearly 200 member companies are currently working to address the All-IP transition, 5G, network functions virtualization, big data analytics, cloud services, device solutions, emergency services, M2M, cyber security, network evolution, quality of service, billing support, operations, and much more. These priorities follow a fast-track development lifecycle — from design and innovation through standards, specifications, requirements, business use cases, software toolkits, open source solutions, and interoperability testing.

ATIS is accredited by the American National Standards Institute (ANSI). The organization is the North American Organizational Partner for the 3rd Generation Partnership Project (3GPP), a founding Partner of the oneM2M global initiative, a member of and major U.S. contributor to the International Telecommunication Union (ITU), as well as a member of the Inter-American Telecommunication Commission (CITEL). For more information, visit www.atis.org.

Notice of Disclaimer & Limitation of Liability

The information provided in this document is directed solely to professionals who have the appropriate degree of experience to understand and interpret its contents in accordance with generally accepted engineering or other professional standards and applicable regulations. No recommendation as to products or vendors is made or should be implied.

NO REPRESENTATION OR WARRANTY IS MADE THAT THE INFORMATION IS TECHNICALLY ACCURATE OR SUFFICIENT OR CONFORMS TO ANY STATUTE, GOVERNMENTAL RULE OR REGULATION, AND FURTHER, NO REPRESENTATION OR WARRANTY IS MADE OFMERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR AGAINST INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. ATIS SHALL NOT BE LIABLE, BEYOND THE AMOUNT OF ANY SUM RECEIVED IN PAYMENT BY ATIS FOR THIS DOCUMENT, AND IN NO EVENT SHALL ATIS BE LIABLE FOR LOST PROFITS OR OTHER INCIDENTAL OR CONSEQUENTIAL DAMAGES. ATIS EXPRESSLY ADVISES THAT ANY AND ALL USE OF OR RELIANCE UPON THE INFORMATION PROVIDED IN THIS DOCUMENT IS AT THE RISK OF THE USER.

NOTE - The user's attention is called to the possibility that compliance with this standard may require use of an invention covered by patent rights. By publication of this standard, no position is taken with respect to whether use of an invention covered by patent rights will be required, and if any such use is required no position is taken regarding the validity of this claim or any patent rights in connection therewith. Please refer to [http://www.atis.org/legal/patentinfo.asp] to determine if any statement has been filed by a patent holder indicating a willingness to grant a license either without compensation or on reasonable and non-discriminatory terms and conditions to applicants desiring to obtain a license.

ATIS-1000072, Analysis of Mitigation Techniques for Calling Party Spoofing

Is an ATIS Standard developed by the **ATIS Packet Technologies and Systems Committee (PTSC).**

Published by

Alliance for Telecommunications Industry Solutions
1200 G Street, NW, Suite 500
Washington, DC 20005

ATIS-1000072

ATIS Technical Report on

Analysis of Mitigation Techniques for Calling Party Spoofing

Alliance for Telecommunications Industry Solutions

Approved August 24, 2016

Abstract

This document provides a Technical Report on Originating Party Spoofing in Internet Protocol (IP) Communication Networks. It describes problems associated with originating party spoofing in IP communication networks, identifies potential mitigation options, and analyzes pros and cons of mitigation options.

Foreword

The Alliance for Telecommunication Industry Solutions (ATIS) serves the public through improved understanding between providers, customers, and manufacturers. The Packet Technologies and Systems Committee (PTSC) develops and recommends standards and technical reports related to services, architectures, and signaling, in addition to related subjects under consideration in other North American and international standards bodies. PTSC coordinates and develops standards and technical reports relevant to telecommunications networks in the U.S., reviews and prepares contributions on such matters for submission to U.S. ITU-T and U.S. ITU-R Study Groups or other standards organizations, and reviews for acceptability or per contra the positions of other countries in related standards development and takes or recommends appropriate actions.

The mandatory requirements are designated by the word *shall* and recommendations by the word *should*. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages. The word *may* denotes an optional capability that could augment the standard. The standard is fully functional without the incorporation of this optional capability.

Suggestions for improvement of this document are welcome. They should be sent to the Alliance for Telecommunications Industry Solutions, PTSC, 1200 G Street NW, Suite 500, Washington, DC 20005.

At the time of consensus on this document, PTSC, which was responsible for its development, had the following leadership:

M. Dolly, PTSC Chair (AT&T)

V. Shaikh, PTSC Vice-Chair (Applied Communications Sciences)

Table of Contents

1 Scope, Purpose, & Application 1

1.1 Scope 1
1.2 Purpose 1
1.3 Application 1

2 Normative References 1

3 Definitions, Acronyms, & Abbreviations 2

3.1 Definitions 2
3.2 Acronyms & Abbreviations 2

4 Call Scenarios 4

5 Problem Descriptions 10

5.1 Valid Caller Identity Scenarios 10
5.1.1 Introduction 10
5.1.2 Simple Call Scenario 10
5.1.3 Privacy Restriction Call Scenario 11
5.1.4 Roaming Local Breakout Call Scenario 11
5.1.5 Doctor Call Scenario 11
5.1.6 Call Center Attested to by Controlling Operator 11
5.1.7 Call Center Attested to by the Borrowing Operator 11
5.1.8 IP-PBX Call Scenario 11
5.1.9 Call Originating from a Non-IMS SIP-based Network 12
5.2 Illegitimate Caller Identity Scenarios (Spoofed Calls) 12
5.2.1 Introduction 12
5.2.2 Spoofed Calls 12
5.2.3 Comparative Call Types Where Spoofing May Occur 13

6 Mitigation Techniques 14

6.1 3GPP PAI Trust Model 14
6.1.1 Description 14
6.1.2 Pros 15
6.1.3 Cons 15
6.2 Number Signing & Validation Techniques 15
6.2.1 Description 15
6.2.2 Caveats 16
6.3 Certificate Granularity (Service Provider vs. TN) 16
6.3.1 Description 16
6.3.2 Pros 17
6.3.3 Cons 17
6.4 Blacklists (Local & Global) 17
6.4.1 Description 17
6.4.2 Pros 18
6.4.3 Cons 18
6.5 Whitelists (Local & Global) 18
6.5.1 Description 18
6.5.2 Pros 18
6.5.3 Cons 18
6.6 Honeypots 19
6.6.1 Description 19
6.6.2 Pros 19
6.6.3 Cons 19

6.7 Post Call Notification (e.g., Dial a “*” Code After Hanging Up) 19
6.7.1 Description 19
6.7.2 Pros.... 19
6.7.3 Cons.... 19
6.8 Network Verification of SIP PAI/FROM for IP PBX Call Originations 19
6.8.1 Description 19
6.8.2 Pros.... 19
6.8.3 Cons.... 19
6.9 Do Not Originate 20
6.9.1 Pros.... 20
6.9.2 Cons.... 20
6.10 Call Detail Recording (CDR) Trace 20
6.10.1 Pros.... 20
6.10.2 Cons.... 20

7 Deployment Scenarios.... 21

7.1 End User Applied....21
7.1.1 Smartphone Apps 21
7.1.2 Consumer Equipment 21
7.2 Network/Service Provider Applied 21
7.2.1 Originating Service Provider.... 21
7.2.2 Intermediate Service Provider 21
7.2.3 Terminating Service Provider 21

8 Analysis of Mitigation Techniques 22

Table of Figures

Figure 4.1 – Range of Possible Calling Scenarios.... 4
Figure 4.2 – Terminating Service Provider View of an Incoming Call 5
Figure 4.3 – Terminating Service Provider View of an Incoming Call with Possible Sources 6
Figure 4.4 – International Gateway Problem 7
Figure 4.5 – Call Scenario: International Gateway Directed to a PBX 8
Figure 4.6 – Calling Party Spoofing Example 9
Figure 4.7 – End-to-End TDM Call 10

Table of Tables

Table 5.1 – Uses of Caller ID for Spoofing/Fraud 12
Table 5.2 – Types of Calls Where Caller ID Spoofing May Occur 14

ATIS Technical Report on –

An Analysis of Mitigation Techniques for Calling Party Spoofing

1 Scope, Purpose, & Application

1.1 Scope

This technical report provides analysis of calling party spoofing mitigation techniques in the converged Internet Protocol (IP) communication network environment. The scope includes the following:

- Summary description of the problems associated with originating party spoofing in IP communication networks.
- Provide an analysis of the following mitigation techniques:
    - 3GPP P-Asserted Identity (PAI) trust model;
        - Number Signaling and Validation Techniques (Secure Telephone Identity Revisited/Secure Handling of Asserted Identities Using Tokens [STIR/SHAKEN] Framework), including that of the Calling Party and International Gateway;Certificate Granularity (Service Provider versus "per TN");
    - Blacklists (local and global);
    - Whitelists (local and global);
    - Honeypots;
    - Post call notification (e.g., dial a "*" code after hanging up);
        - Network verification of Session Initiation Protocol (SIP) PAI/FROM for IP Private Branch Exchange (PBX) call originations;
    - Do Not Originate;
    - Call Detail Records (CDR) Trace.

The mitigation techniques provided in this analysis also apply to illegitimate robocalls.

1.2 Purpose

The purpose of this document is to provide an analysis of the available and proposed mitigation techniques, and guidance on standard approaches for addressing originating party spoofing.

1.3 Application

ATIS member companies may rely on this paper to conduct meetings with policymakers at all levels of government who are dealing with constituents' concerns about caller identification services (caller ID) spoofing and robocalling. Those meetings may educate government officials about these practices and may involve advocacy against premature regulation and legislation that could cement solutions or create regulatory barriers to the flexibility industry needs to mitigate caller ID spoofing and robocalling.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

- ATIS-0300114, *Next Generation Network (NGN) Reference Document Caller ID and Caller ID Spoofing.*[1]
- Draft 3GPP TR 33.8de V0.4.0, *Security study on spoofed call detection and prevention*.

3 Definitions, Acronyms, & Abbreviations

For a list of common communications terms and definitions, please visit the *ATIS Telecom Glossary*, which is located at < http://www.atis.org/glossary >.

3.1 Definitions

Attestation: This is the declaration made by a network operator that the party placing a particular call is authorized to represent themselves by a particular caller identity. The party placing the call may not be the identity owner, rather is authorized by the identity owner to represent the identity owner.

Borrowed E.164 number: This is the E.164 number that a borrowing user has obtained permission from the identity owner to use as caller identity when making calls on behalf of the identity owner.

Borrowing operator: This is an operator who is not able to assign a specific E.164 number since it is controlled by a different operator (see controlling operator). A borrowing user subscribed to a borrowing operator is authorized to use a borrowed E.164 number as caller identity in calls made on behalf of the identity owner.

Borrowing user: This is the user subscribed to a borrowing operator and is authorized by the identity owner to use the caller identity for calls made on behalf of the identity owner.

Caller identity: The originating phone number included in call signaling used to identify the caller for call screening purposes. In some cases this may be the Calling Line Identification (CLI) or Public User Identity. For the purposes of this study, the caller identity may be set to an identity other than the caller's CLI or Public User Identity.

Controlling operator: This is the network operator who controls the assignment of a specific E.164 phone number to a subscribed user for call routing and caller identity use.

Identity owner: This is the user, subscribed to the controlling operator, who is currently assigned a specific E.164 phone number for call routing purposes. This E.164 number may be presented to a called party as the user's calling party identity. The identity owner can authorize other users or subscribers of controlling or non-controlling operators to also use the E.164 number as caller identity in phone calls made on the identity owner's behalf.

Spoofed call: A call where caller identity creation, modification, or removal in call signaling results in an unauthorized or illegal use of this identity in the call., This typically occurs where the caller intends to defraud the called party or otherwise illegally obscure the real caller identity.

3.2 Acronyms & Abbreviations

ATIS	Alliance for Telecommunications Industry Solutions
B2BUA	Back2Back User Agent
Caller ID	Caller Identification Services
CDR	Call Detail Records
CLI	Calling Line Identity/Identification

[1] Available from the Alliance for Telecommunications Industry Solutions (ATIS), 1200 G Street NW, Suite 500, Washington, DC 20005, at: < https://www.atis.org/docstore/product.aspx?id=28262 >.

CNAM	Calling Name
CPE	Customer Premise Equipment
CPN	Calling Party Number
CPNI	Customer Proprietary Network Information
DECT	Digital Enhanced Cordless Telecommunications
DNO	Do Not Originate
FCC	Federal Communications Commission
FTC	Federal Trade Commission
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MITM	Man In The Middle computer security attack
NANP	North American Numbering Plan
NANPA	North American Numbering Plan Administration
NGN	Next Generation Network
PAI	P-Asserted Identity
PBX	Private Branch Exchange
PLMN	Public Land Mobile Network
POTS	Plain Old Telephone Service
PSAP	Public Safety Answering Point
PSTN	Public Switched Telephone Network
PTSC	ATIS Packet Technologies and Systems Committee
RFC	Request for Comments, an IETF publication
SHAKEN	IETF Secure Handling of Asserted Identities Using Tokens
SIP	Session Initiation Protocol
SP	Service Provider
SS7	Signaling System 7
STIR	IETF Secure Telephone Identity Revisited Working Group
TA	Terminal Adapter
TDM	Time Division Multiplexing
TN	Telephone Number

UE	User Equipment
VoIP	Voice Over Internet Protocol

4 Call Scenarios

The range of possible calling scenarios can be illustrated with the following diagram. Reality is actually far more complex than this diagram suggests, with many suppliers providing the equipment within each category shown below, and a range of software releases, with different functionality, for each supplier's equipment. In many cases the equipment has been manufacturer-discontinued, or the supplier is no longer in business. In addition, each service provider typically selects a specific set of features to enable and test in their network. There are also additional sources that can originate calls (e.g., over-the-top Voice Over Internet Protocol [VoIP] services) and additional targets for incoming calls (e.g., call centers). As a result, the following should be viewed as a highly simplified version of the reality in today's network.

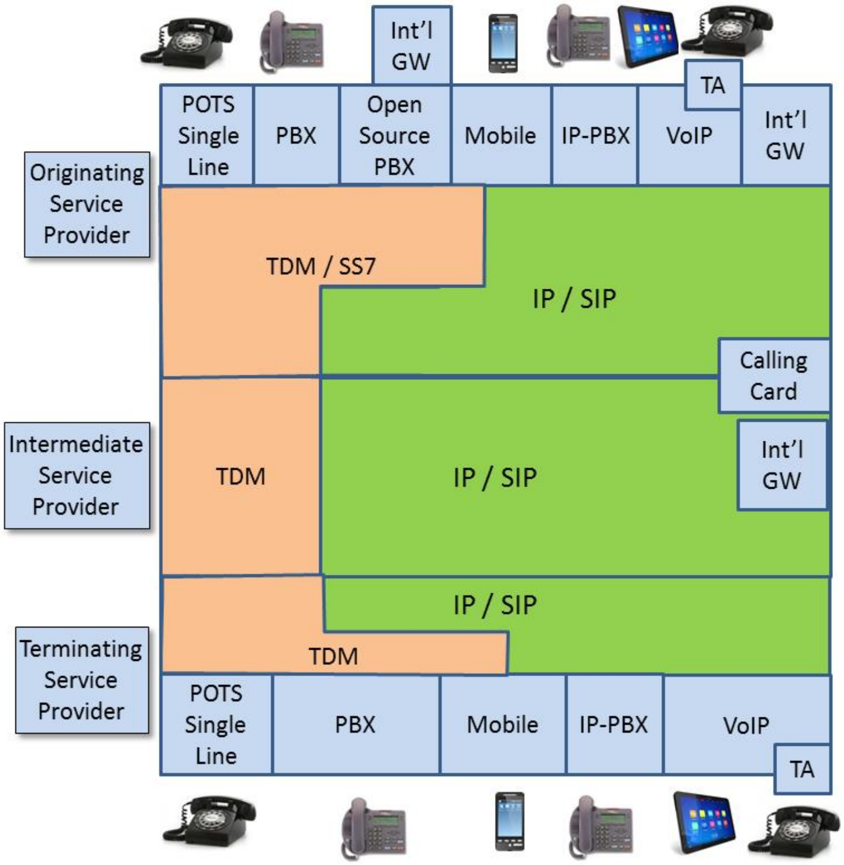

Figure 4.1 – Range of Possible Calling Scenarios

Although this diagram is a simplified picture of calling scenarios in today's network, it is adequate to illustrate the limitations of simplistic approaches that focus on only one of the many calling scenarios and then claim to "solve" the problem of caller ID spoofing for all call scenarios.

As terminating service providers consider mechanisms to stop unwanted calls, and in particular as they investigate caller ID spoofing mitigation techniques, their options are limited by a lack of an end-to-end view of the full path of the incoming call. They do not have reliable information on where the call originated, and do not have any information that would allow meaningful estimates of the accuracy of the calling party information in the call signaling. This can be illustrated by the following diagram showing the terminating service provider's view of an incoming call.

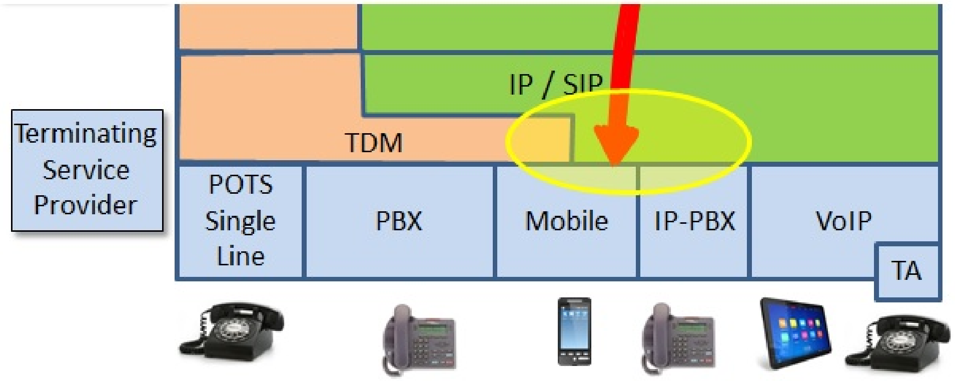

Figure 4.2 – Terminating Service Provider View of an Incoming Call

In this example, the terminating service provider only knows that the call is coming from an intermediate service provider, over an IP connection with SIP signaling. If the picture is expanded to show some of the possible sources of this incoming call, a far more complex picture emerges.

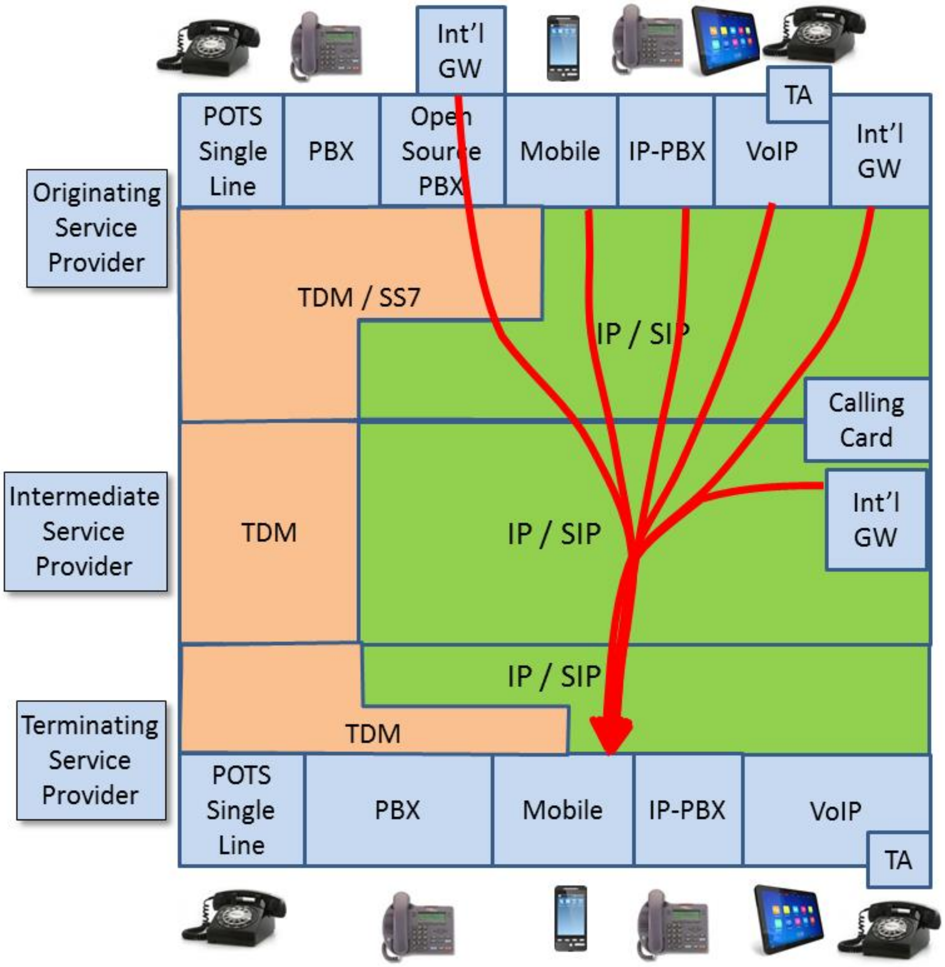

Figure 4.3 – Terminating Service Provider View of an Incoming Call with Possible Sources

The terminating service provider does not know the source of a call or the accuracy of the incoming calling party information. This undermines mitigation techniques that can be utilized with the intent to stop malicious calls.

Key insights emerge if one views this from the perspective of a “bad actor”, spoofing the caller ID to convince the called party that a call is from the IRS. One possible strategy is to identify today’s dominant weak spot (e.g., international gateways) and develop a targeted “solution” – a “silver bullet”. Unfortunately, the “international gateway problem” is not a single, well-defined problem, as illustrated by the following diagram.

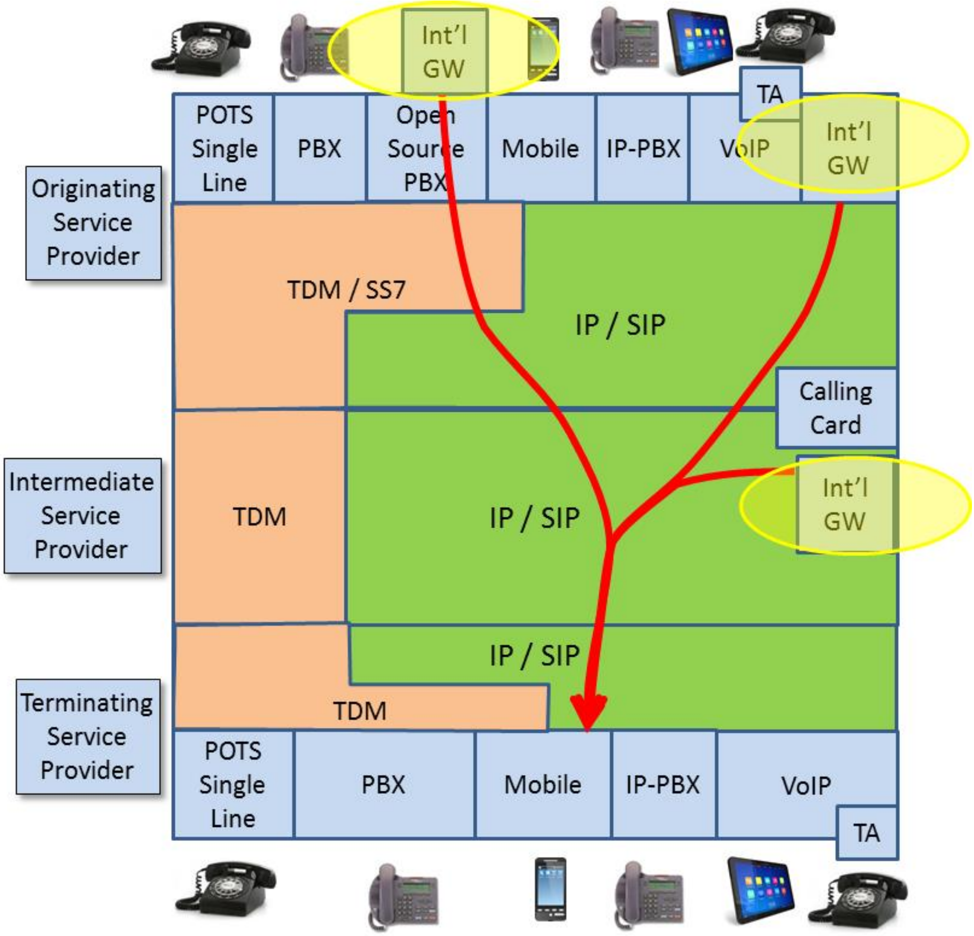

Figure 4.1 – International Gateway Problem

Mandating a targeted “solution” might block unwanted and/or illegitimate calls over one of these routes, but this could simply move the problem to other approaches, including new methods not shown here.

The “open source PBX” shown in this diagram is just one example of “re-origination” of traffic that hides the true source of a call, and can be used for many malicious reasons including arbitrage and outright fraud. The origin of a call can also be obfuscated through the use of call forwarding. In the scenario shown below, a call from an international gateway is directed to a PBX where it is then forwarded to a target number in a different network. When call forwarding is implemented as a network service, the network retains information about the original source, but if it is implemented within the PBX, it appears to the network as a new call originating at the PBX. Call forwarding is a legitimate service, yet in some cases, it can effectively re-originate the call and completely hide the true source.

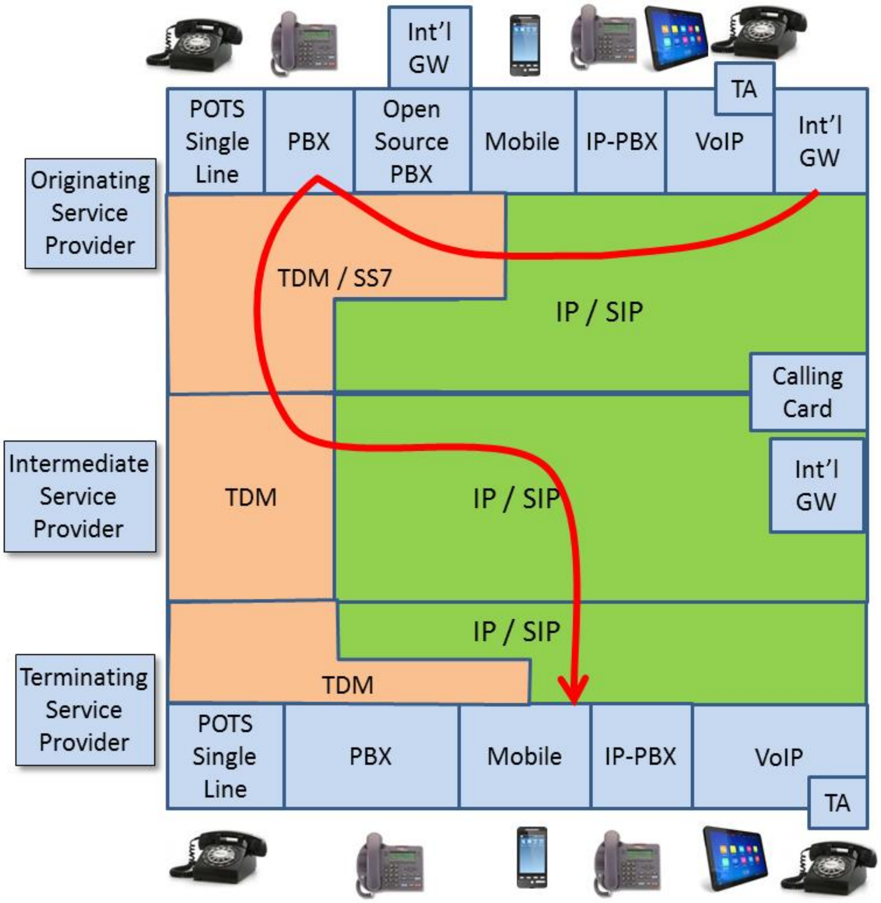

Figure 4.2 – Call Scenario: International Gateway Directed to a PBX

The following diagram highlights some of the points in the traffic flow where problems with potential spoofing occur today:

1. When traffic is passed from the intermediate service provider to the terminating service provider, although signaling information may be passed through the call path, many calls may not identify the source of calling party information and do not indicate if that information has been validated. The only information available is whether or not the service provider is “trusted”. Potential solutions are being developed for SIP signaling, but nothing exists or could be developed for validation of Time Division Multiplexing (TDM) traffic.
2. When traffic is passed from the originating service provider to the intermediate service provider, although signaling information may be passed through the call path, many calls may not identify the source of the calling party information and do not indicate if it has been validated. The only information available is whether or not the service provider is “trusted”. Potential solutions are being developed for SIP signaling, but nothing exists or could be developed for validation of TDM traffic.
3. TDM/SS7 networks do not have a mechanism to reliably validate calling party information. The end-to-end information can be limited by the SS7 network, even when most of the signaling path is via SIP.
4. Today, calling party information is inserted by the PBX and is not validated by the network. In the case of TDM equipment, it would be impossible to change this since the majority of the equipment is no longer supported by the manufacturer.
5. In this case, the ultimate source of the traffic is an “international gateway” that is “hidden” behind an enterprise PBX. With an open source PBX it could be very inexpensive to integrate international gateway functionality into the PBX and create new entry points for malicious traffic. The service provider does not have any mechanism to stop, or even to detect, this situation. The above call scenario is an example of legitimate routing in the network.

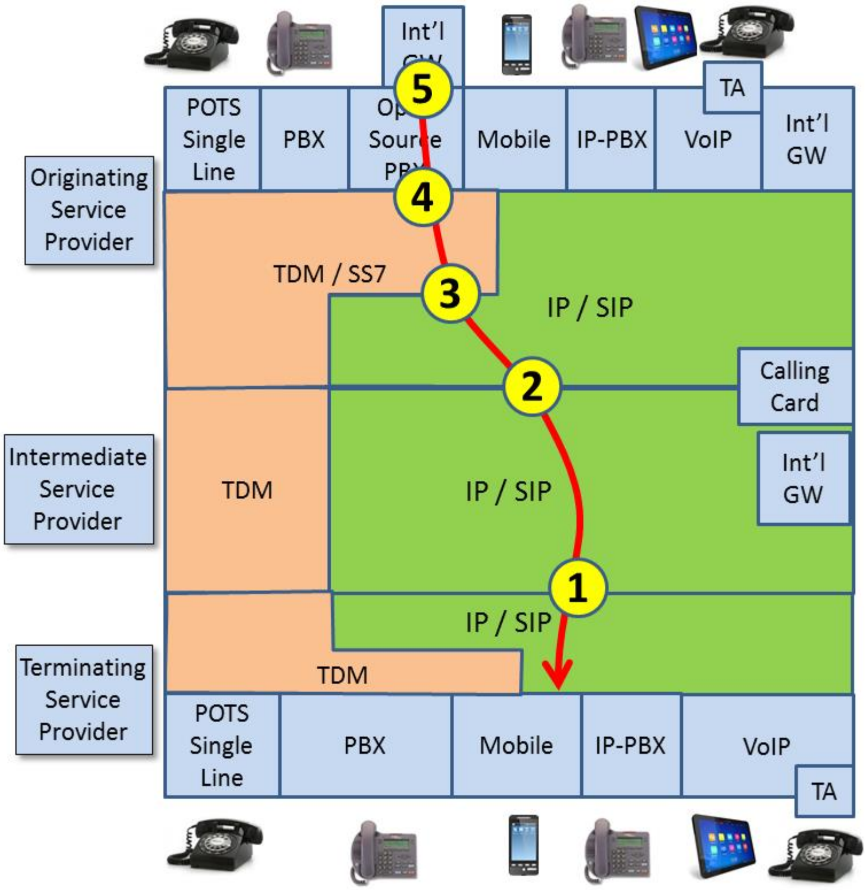

Figure 4.3 – Calling Party Spoofing Example

As this example makes clear, addressing the challenges of calling party spoofing requires an end-to-end perspective addressing a wide range of service providers, equipment types, and network functionality.

The next diagram illustrates an end-to-end TDM call. In this case, each time the TDM call passes from one service provider to another, information about the upstream source of the call may not be passed forward. Identifying the source of a malicious call would require coordination of information across the service provider boundaries shown in 2 and 3, as well as the service provider to enterprise boundary shown in 3. This is only technically feasible using CDR, to identify the source of specific problem calls. This is a complex manual process requiring correlation of CDR records to trace the call back to the origin. This process might be applied in a forensic analysis of trouble reports, but not provide real-time information that might allow the user to validate the source of a given call before answering.

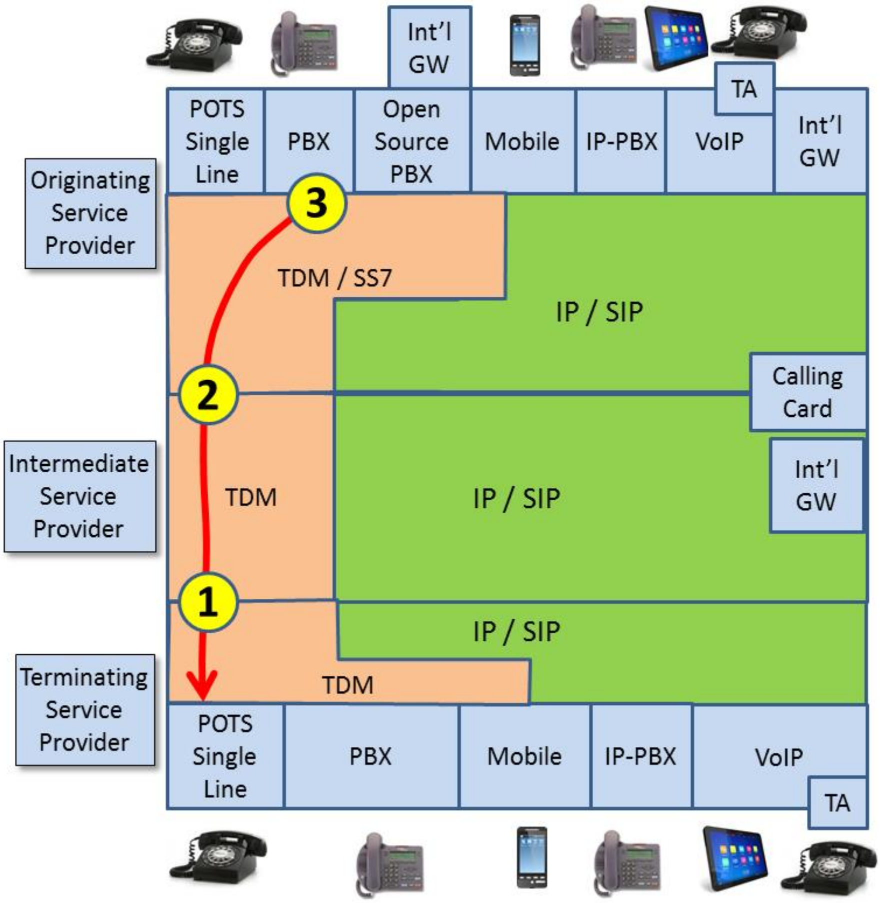

Figure 4.4 – End-to-End TDM Call

Calling party spoofing is not a single, well-defined problem that can be addressed with a “silver-bullet” solution. It’s instructive to use the analogy of a flood to better understand the situation. If the problem is a dyke with a single leak, one small finger will stem the flow. But if the problem is more like a sieve, a different approach is required. A realistic strategy must address specific threats where practical, but also requires a layered approach that adds secondary defenses to minimize the risk when even the best defense is inevitably bypassed. The strategy must also recognize that the threat is not static. As one threat vector is blocked, attacks will shift to other weak points, and discover new approaches. Effective mechanisms to mitigate calling party spoofing must recognize this reality, be dynamic and flexible, and be structured accordingly.

5 Problem Descriptions

5.1 Valid Caller Identity Scenarios

5.1.1 Introduction

This section describes representative call scenarios where the caller identity presented to the called user is allowed and valid. Some of the scenarios describe situations where the caller identity presented is different from the caller's identity. These scenarios assume the presence of a call spoofing detection capability in the terminating network.

5.1.2 Simple Call Scenario

A caller places a call and that caller's caller identity is presented to the called user. The terminating network is able to verify the attestation by the controlling operator's originating network of the caller's identity.

5.1.3 Privacy Restriction Call Scenario

A caller places a call and as part of the call, the caller identity of the caller and a privacy indication is sent to the terminating network. The terminating network is able to verify the attestation by the controlling operator's originating network of the caller identity, but does not present the caller identity to the called user.

5.1.4 Roaming Local Breakout Call Scenario

A caller places a call while roaming and the caller's caller identity is presented to the called user. The terminating network is able to verify the attestation by the home Public Land Mobile Network (PLMN) of the caller identity.

5.1.5 Doctor Call Scenario

A doctor is subscribed to different operators for his mobile service and office phone service. The doctor is performing hospital rounds and calls a patient from his UE. The doctor does not want the patient to have his UE's E.164 number, and the patient would not recognize the number. Rather the doctor's UE replaces the caller identity in the call with the E.164 number of his office. This office number is presented to the patient (called user).

5.1.6 Call Center Attested to by Controlling Operator

A call center is engaged in an outbound advertising campaign for several months on behalf of ABC Company. The call center and ABC Company each subscribe to different network operators. ABC Company as the identity owner has given permission for the call center as the borrowing user to use ABC Company's E.164 number as the caller identity in calls placed as part of the campaign.

In this scenario, the operator that ABC Company has subscribed to as the controlling operator wants to provide the attestation that the call center is authorized by ABC Company to use the ABC Company E.164 number for caller identity in the outbound calls from the call center.

The terminating network uses the caller identity credentials provided by the controlling operator to verify that the caller identity is a valid use.

5.1.7 Call Center Attested to by the Borrowing Operator

A call center is engaged in a fundraising campaign for a non-profit organization XYZ. The call center and XYZ each subscribe to different network operators. XYZ as the identity owner has given permission for the call center as the borrowing user to use XYZ's E.164 number as the call identity in calls placed as part of the campaign.

In this scenario the operator that the call center has subscribed to as the borrowing operator wants to provide the attestation that the call center is authorized by XYZ to use the XYZ E.164 number for caller identity in the outbound fundraising calls from the call center.

The terminating network uses the caller identity credentials provided by the borrowing operator to verify that the caller identity is a valid use.

5.1.8 IP-PBX Call Scenario

An employee of a company using an IP-PBX places a call to another party outside of the IP-PBX. The controlling operator that the IP-PBX is connected to verifies that the caller identity provided is assigned to the IP-PBX and attests to the caller identity validity. It is assumed that any restriction by specific IP-PBX users to use specific assigned IP-PBX numbers for caller identity, if present, is performed by the IP-PBX.

The terminating network uses the caller identity credentials provided by the controlling operator of the IP-PBX to verify that the caller identity is a valid use.

5.1.9 Call Originating from a Non-IMS SIP-based Network

A subscriber of a network that is SIP based but has not deployed IP Multimedia Subsystem (IMS) capabilities calls a user who is subscribed to a terminating network that is IMS based. The terminating network is able to verify the attestation by the controlling operator's originating network of the caller identity even though 3GPP defined IMS SIP extensions are not present in the call signaling.

5.2 Illegitimate Caller Identity Scenarios (Spoofed Calls)

5.2.1 Introduction

This clause describes representative call scenarios where the caller identity presented to the called user is not allowed or invalid. These scenarios assume the presence of a call spoofing detection capability in the terminating network.

A caller intending to commit fraud places a call and sets the caller identity to an invalid or unauthorized number (it may or may not be a valid E.164 number) which is presented to the called user. The terminating network is able to verify that the caller is not authorized to use the provided caller identity.

Examples of spoofed caller identities include:

- Unassigned E.164 numbers.
- Invalid E.164 numbers.
- E.164 numbers local to the called user.
- The called user's own E.164 number (called number).
- E.164 numbers billed at international rates.

5.2.2 Spoofed Calls

The *Truth in Caller ID Act* prohibits spoofing, or deliberately falsifying the telephone number (TN) and/or name relayed as the caller ID information to disguise the identity of the caller ***for harmful or fraudulent purposes***. However, the law only applies to callers within the United States.

- Reflection spoofing (i.e., spoofing the called TN in the caller ID).
- Random number generators providing spoofed TN.
- Calling patterns:
  - Same phone number with many calls to different numbers within a short period of time.
  - Same phone number sequentially calling large blocks of phone numbers.
- Phantom traffic (i.e., calls terminating in which the caller ID information has been stripped).
- Call back to the number (i.e., individual or business) that was spoofed.
- Local spoofed TNs resulting in call backs to the number.
- Next Generation Network (NGN) number may be an exception being in the IP environment.

The following table describes uses of Caller ID and how the spoofing/fraud works.

Table 5.1 – Uses of Caller ID for Spoofing/Fraud

Use Case	Scam uses of Caller ID	How the spoofing/fraud works
1	Robocaller hangs up before consumer answers, leaving behind a Caller ID that the consumer calls back out of curiosity or concern.	Caller ID is in another country and is expensive for the (unwitting) consumer to call. Robocaller gets a share of revenue from his telco.

Use Case	Scam uses of Caller ID	How the spoofing/fraud works
2	Robocaller leaves voice-mail telling consumer they need to call back this number regarding problems with their account at IRS or bank.	Consumer gets engaged in conversation that extracts personal details and results in identity theft or tax/credit fraud.
3	Calling number shows a “name” (CNAM) such as “Card Services” or “FBI” selected by the caller to lend credibility to the call.	Robocaller just “rents” a number in a non-authoritative, most likely disreputable database that is willing to attach *any* name to the given number *for a fee*. The robocaller is able to extract personal details that could result in identity theft or fraud. In addition, the robocaller tenant may earn revenue shares each time the bogus name is retrieved from the illicit database.
4	Calling number really belongs to somebody else and is chosen for the CNAM it presents, or just to confuse.	Consumer answers call because the CNAM looks familiar. Attempts to trace the call lead to contacting the authorized user of the calling number but not the party that placed the spoofed call, which leads to frustration for the innocent number holder.
5	Calling number is chosen arbitrarily or at random to obfuscate who is actually making the call.	Call origin cannot be traced or determined based on Caller ID.

5.2.3 Comparative Call Types Where Spoofing May Occur

Table 5.2 below illustrates examples and potential impacts of caller ID spoofing. This table is for illustrative purposes and should not be considered an all-inclusive list.

Table 5.2 – Types of Calls Where Caller ID Spoofing May Occur[2]

Risk & Impacts	Legitimate Uses			Potentially Illegal Activities
	Domestic Violence Shelters, Hospitals, Doctor's Offices, Telemarketers, Answering Services, School Announcements, Newspaper Reporters, Certain Businesses, and Government Announcements	**Political Solicitation, Solicitation for Charities, Informational Surveys**	**Public Emergency Notifications (from PSAPs)**	**Phishing for Active Subscribers, Changed/Deleted/Augmented Caller ID, Phantom Traffic (i.e., non-billable traffic), International Revenue Sharing Fraud, Focused Nuisance Attack, For Harmful or Fraudulent Purposes**
Network Congestion	Low	Medium	High	High
Blocking E911 Calls	Low	Medium	High	High
Consumer Impact	Low	Medium	Medium	High

Table 5.2 Legend:

- High: Has high potential of experiencing the risk or impact.
- Medium: Has medium potential of experiencing the risk or impact.
- Low: Has low potential of experiencing the risk or impact.

6 Mitigation Techniques

The following mitigation techniques are examined:

- 3GPP PAI trust model;
- ATIS Verified Token;
- Secure Telephone Identity Revisited (STIR): signing parts of SIP messages based on RFC 4474bis;
- Blacklists (local and global);
- Whitelists (local and global);
- Honeypots;
- Post call notification (e.g., dial a "*" code after hanging up);
- Network Verification of SIP PAI/FROM for IP PBX call originations;
- Do Not Originate.

The pros and cons analysis will address coverage (e.g., IP, circuit switched, wireless), availability, and deployment complexity.

6.1 3GPP PAI Trust Model

6.1.1 Description

P-Asserted-Identity and Privacy headers are defined in RFC 3325. The P-Asserted-Identity contains the caller ID information for the call on the INVITE SIP packet. The Privacy header contains information on which parts of the

[2] Table 5.2 is adapted from ATIS-0300105, *Next Generation Interconnection Interoperability Forum (NGIIF) Auto Dialers Reference Document*, Table 8.1, Robocall Matrix.

caller ID are private. In “trusted” networks, the identity of the Calling Party Number (CPN) is validated and placed in the SIP PAI header.

6.1.2 Pros

- Useful in “trusted” network deployments for IP to IP calls, assuming a “trusted” chain of trust between all service providers in the call path.

6.1.3 Cons

- Does not address CS originated calls.
- Can be modified by Man In The Middle (MITM) computer security attacks.
- IP PBX’s send PAI to the originating SP, who is likely not authenticating use of the number.
- Not all networks are trusted thereby PAI is now tainted.
- Operational impact determining how to indicate trusted networks.
- Though the original intent of PAI was that only the contents of the PAI would be presented to the Called Party, carriers have been presenting the untrusted information contained in the SIP FROM header to the Called Party if there is no PAI present.

6.2 Number Signing & Validation Techniques

6.2.1 Description

STIR provides a protocol framework for the signing and validation of the telephone number or caller ID of the originating caller. It uses two specifications nearing completion draft-ietf-stir-rfc4474bis and draft-ietf-stir-passport. Persona Assertion Token, or PASSporT, defines a token framework for defining a method of signing the identity of a user and associated information with a call that can be passed over potentially untrusted networks. The signature at the terminating side of the call can validate this token and check the credentials to see if the caller identity has not been altered or spoofed. 4474bis defines the protocol framework to use PASSporT inside the SIP INVITE as part of a new header “identity”.

As defined in 4474bis, the “Authentication service” performs the role of authenticating the originator of the SIP request, and then signing the request with the private key of the credential corresponding to the domain or a telephone number used by the originator. Commonly, this role will be instantiated by a proxy server, since these entities are likely to have a static hostname, hold corresponding credentials, and have access to SIP registrar capabilities that allow them to authenticate users.

The “Verification service” or “verifier” performs the role of inspecting the signature and verifying the identity of the sender of the message. This role is typically instantiated by a proxy server at the target domain.

At a high level the proposed mechanism works as follows:

a) The incoming SIP requests such as INVITE are processed at the originating end by the Authentication service.
   - The service first authenticates the originator (sender) and validates that sender is authorized to assert the identity that it populated in the “From” header field.
   - The service then computes a hash over some headers, including the “From” header field of the message.
   - The hash is signed with the appropriate credential (for ex., private key) and inserted in the “Identity” header of the SIP message. The authentication service, as the holder of the private key, is asserting that the originator of the SIP message has been authenticated and that the originator is authorized to claim the identity that appears in the “From” header field.
   - The service also inserts a companion header field “Identity-Info”, that tells the receiver how to acquire keying material necessary to validate its credentials.
   - The modified request is forwarded to the target domain.

b) At the receiving domain, the “Verification service” receives the request.
   - Verifies the signature provided in the “Identity” header, and validates that the authority over the identity in the “From” header field has authenticated the originator and permitted the originator to assert that “From” header field value.
   - The message is then forwarded to the receiver.

In summary, the mechanism requires:

- SIP header information.
  - Canonical TN from FROM or PAI headers.
  - Time Stamp + replay sequence or call id.
    - Prevents cut/paste attack.
  - Signed by a credential assigned to the number holder (device or service provider).
- A credential database.
  - URI to cert in the SIP header. Hypertext Transfer Protocol (HTTP) GET on the URI returns the cert from the database.
  - Database that can be queried with TN and returns valid cert(s).
- A certificate management infrastructure.

The following items have been identified but have not been addressed to date:

- Certificate framework hierarchy is not yet defined.
- Additional functional elements to provide an originating authentication service and terminating validation service are not yet defined.
- Use of the knowledge at the terminating end that the information in the signaling is or is not valid is not yet defined.
- There are policy issues surrounding actions that the terminating service provider may take in terms of call blocking based on potentially invalid information.
- Mechanisms for presenting the validity of calling party information to the end user need to be developed.

6.2.2 Caveats

- STIR has been designed in the context of VoIP services and therefore signed caller identity information cannot be conveyed in SS7 ISUP.
  - International VoIP calls can terminate on the backend of a PBX with CS access to the Public Switched Telephone Network (PSTN).
- There will be operational impacts, to develop a database to manage either tokens or certificates, initiate/manage/maintain changes to routing with those, potential equipment augments, and ongoing management and maintenance. Systems will also be impacted, so there will be added Operational work for IT teams.
- Deployment issues:
  - What will be displayed to the user?
  - What actions can be taken by the terminating service provider?
  - Will carriers in high cost areas request cost recovery?

6.3 Certificate Granularity (Service Provider vs. TN)

6.3.1 Description

With the use of STIR defined protocols, digital signatures based on X.509 certificates are mandated with the purpose of using PKI and features like a certificate chain to a trust anchor that represents a common set of trusted authorities that validate that the authentication service created signature is associated with an authorized provider of telephone services.

Building and managing this certificate management infrastructure requires the cooperation and participation of telephone service providers that incorporate STIR authentication and verification services in their networks.

The ATIS/SIP Forum NNI Task Force and ATIS PTSC are in the process of defining an industry framework for a common approach to the deployment of STIR services and the requirements for interworking between providers. This framework is called SHAKEN, Secure Handling of Asserted Identities Using Tokens.

Certificate management between providers, we believe, needs to be an evolutionary process in order to facilitate early and quick adoption of STIR services.

Initial deployments should focus on getting the STIR protocol level functionality in place with a simple set of certificate granularity corresponding to service provider level certificates. From a telephone number allocation and number portability point of view the association of service provider level certificates to telephone numbers is straight forward.

Once there is wide industry adoption of STIR protocol, and there is a need for and justification supporting more granular TN level certificates, the ability to revoke certificates ownership for porting using OSCP, and other more advanced techniques can more easily adopted across VoIP networks.

NOTE: There are proposals to have TN range certificates and other granularity as well that could be considered.

6.3.2 Pros

6.3.2.1 Service Provider Level

- Easier industry adoption with straight forward certificate management techniques.
- Service Provider Level certificates are highly cacheable, i.e., few certificates vs. total number of calls.
- Limited scale and functionality required to manage.

6.3.2.2 TN Level

- Provides more advanced capability for providing validation of individual TNs and ownership.

6.3.3 Cons

6.3.3.1 Service Provider Level

- None

6.3.3.2 TN Level

- Large scale certificate management required day one.
- Requires network dip for almost every call to get TN certificate.
- Requires additional functionality for revoking ownership.

6.4 Blacklists (Local & Global)

6.4.1 Description

Blacklists place numbers in a table that are blocked at the terminating end, either in the terminating network or a Customer Premise Equipment (CPE) device in the home. Local blacklists are unique to a single subscriber, typically with input from the subscriber. The list of numbers provided by the subscriber can contain numbers that are unwanted versus robo/spoofed calls. Global blacklists are centrally administrated, and common to all or a portion of a service provider's subscriber base.

6.4.2 Pros

- Subscribers can provide input to their local blacklists avoiding calls from numbers that they do not want to receive calls from.
- Applicable for circuit switch terminated calls.

6.4.3 Cons

- Global blacklists treat all subscribers the same, where a number in one geographic area is “good”, and not in a different geo-area.
- Numbers on blacklists can be reassigned; thereby good calls may be blocked.
- Spoofers quickly and easily move to different numbers as soon as they encounter blocking.
- Too easy for spoofers to utilize numbers from global whitelist pool.
- Administrative overhead.
- Scalability.
- There are operational management needs for the white/blacklists if they are carrier-specific, and for customer-specific lists there will be repair issues when customers have some problems or confusion.
- The lists will need to be maintained and referenced in the termination of each call, so there are routing issues and potential equipment augmentation and ongoing maintenance (even if cloud-based).
- To the extent these lists are scalable, more resources will need to be dedicated to maintain and manage the lists and ensure accuracy (e.g., a “good” number is not mistakenly included on a blacklist).

6.5 Whitelists (Local & Global)

6.5.1 Description

Whitelists place numbers in a table of numbers that would be accepted by the Called Party, with all other numbers being blocked. The whitelist table is either in the terminating network or a CPE device in the home.

6.5.2 Pros

- Local whitelists on the subscriber’s UE or on a front end “adapter” in front of the subscriber’s UE can be controlled by the subscriber.
- Though whitelists will block legitimate calls, with the “consent of the subscriber”, whitelists allowing only the following could be set up to protect the “vulnerable” population:
  - Address book entries.
  - Government agencies.
  - Medical providers.
  - Emergency alerts.

6.5.3 Cons

- Global and local whitelists will block legitimate calls. Global whitelists will block a larger amount of legitimate calls that will result in subscriber complaints.
- Too easy for spoofers to utilize numbers from global whitelist pool.
- Administrative overhead.
- Scalability.
- There are operational management needs for the white/blacklists if they are carrier-specific, and for customer-specific lists there will be repair issues when customers have some problems or confusion.
- The lists will need to be maintained and referenced in the termination of each call, so there are routing issues and potential equipment augmentation and ongoing maintenance (even if cloud-based).

- To the extent these lists are scalable, more resources will need to be dedicated to maintain and manage the lists and ensure accuracy (e.g., a “good” number is not mistakenly included on a blacklist).

6.6 Honeypots

6.6.1 Description

Place attractive (dirty or selected isolated good) numbers in a “Honeypot” to catch bad guys.

6.6.2 Pros

- Proactive approach for identifying the bad guys.

6.6.3 Cons

- Operational needs for building the honeypots, managing/maintaining them, and data review and handling.

6.7 Post Call Notification (e.g., Dial a “” Code After Hanging Up)*

6.7.1 Description

Called Party suspects a spoofed/fraud call. Upon off-hook, the Called Party dials a new vertical service code that would result in the terminating SP marking the CDR and reporting it to the Federal Trade Commission (FTC) and/or centralized clearinghouse.

6.7.2 Pros

- Deployable in newer equipment, allowing the subscriber to identify unwanted calls in real time.

6.7.3 Cons

- There are codes like this today, such as *57, however, any new vertical service codes would require significant network upgrades that may not even be feasible due to some switch vendors no longer being in business.
- It will require the development of processes and procedures operationally, management/maintenance, and action taken on the data.
- Currently, reporting is performed manually which is time consuming and not scalable.

6.8 Network Verification of SIP PAI/FROM for IP PBX Call Originations

6.8.1 Description

The originating SP authenticates that the enterprise IP PBX can use the CPN place by the IP PBX in the PAI header, or the FROM header if the PAI is not present,. The originating service provider’s network validates that the number in the PAI or FROM header can be used by the IP PBX. The service provider can then sign the PAI.

6.8.2 Pros

- Protects against spoofing traffic from IP PBX origination.

6.8.3 Cons

- Does not protect from calls originating from PBXs with circuit switched access to the PSTN, as modifications cannot be made to circuit switched equipment.

- While these PBXs are CPE and customers have choice for the management and maintenance of the equipment, the demark at the originating network will have operational needs, processes, and procedures, should something new and different be set as the standard to accommodate the new standard from PTSC. In addition, anti-spoofing credentials carried in SIP FROM headers are likely to be discarded by Back2Back User Agent (B2BUA) software in older VoIP implementations.

6.9 Do Not Originate

Do Not Originate (DNO) servers would be deployed at IP gateways, where the gateway blocks numbers that “should not be there”. It predicates on the premise that almost all illegal robocalls originate on VoIP. Example of numbers that “should not be there” include:

- 911 DNC list.
- Financial institutions.
- Government agencies.
- North American Numbering Plan Administration (NANPA): unassigned numbers.
- TDM carrier numbers.
- Facilities-based VoIP (with own gateways).
- OTT VoIP (except for contracted GWs).

6.9.1 Pros

- Deployment in a small number of large gateways can make a significant impact, at least initially.
- The number of numbers to be managed is manageable.

6.9.2 Cons

- Too easy for spoofers to gain access via smaller gateways.
- Does not protect against international VoIP originated calls to the back end of a PBX that accesses the PSTN via circuit switched trunks.
- Third party clearinghouse required once coverage expands beyond the large gateway providers.
- How high is the bar that defines a “large gateway” provider?
- A database in which customers enter TNs and then carriers’ IP gateways need to block the origination of calls on this list. As thus described, it will require the selection of a national database vendor, and management of the vendor, a database build and data loads for TNs that “should not be there”, and then links to each IP provider’s gateway, with management and maintenance of the links. All of which have operational aspects.

6.10 Call Detail Recording (CDR) Trace

Use of CDRs to trace back from the destination carrier to the originating carrier.

6.10.1 Pros

- Effective tool independent whether the call/session originated or terminated on CS or IP.

6.10.2 Cons

- Manual processes, though some automation can be realized.

7 Deployment Scenarios

This section describes the locations where mitigation techniques can be applied to mitigate nuisance calls.

7.1 End User Applied

7.1.1 Smartphone Apps

Many call blocking features exist that work across all smartphone operating systems (IOS, Android, and QNX). Two categories of features exist: 1) those native to the smartphone dialer and 2) those available with downloadable VoIP apps. Each allow for setting up and maintaining blacklists or whitelists directly from call logs or contact lists. Do not disturb features also exist that disable all incoming calls. Blocked calls using these features can be optionally routed to voice mail, busy signal, recorded announcement, picked up and hung up automatically, or mute the ringer. Pre-canned text messages can optionally be sent to the caller explaining why the call was not answered.

7.1.2 Consumer Equipment

Call blocking devices exist that can be installed by a user between their phone and phone line. Users can set whitelists or blacklists through the unit's user interface and can also view call logs, including blocked calls. Similar call blocking functionality is also built into Digital Enhanced Cordless Telecommunications (DECT) cordless phones through a similar user interface.

7.2 Network/Service Provider Applied

Mitigation techniques can be applied in the network by service providers. These include mitigation techniques provided by 3rd party platform/services facilitated by the serving carrier. Calls pass through different categories or types of service providers, i.e., originating, terminating, and/or intermediate service providers, so there are several areas where mitigation techniques could be applied. The information available, as well as applicable regulation, varies significantly for each category of service provider, and this can limit the utilization of mitigation techniques. The role of each category of service provider is discussed in the remainder of this section.

7.2.1 Originating Service Provider

An originating service provider may be able to authenticate a phone number assigned by the North American Numbering Plan (NANP). For groups of lines served by a PBX, the originating network has to rely on the PBX to ensure the integrity of the calling line IDs being sent. (Additional detail is provided in clause 8.1.) This may allow the originating service provider to authenticate the identity of the calling party; however, no mechanism is currently available that would allow the originating service provider to inform the terminating service provider, and intermediate service provider(s), as applicable, that specific phone numbers have been authenticated and others have not been authenticated.

7.2.2 Intermediate Service Provider

In the call path, the originating carrier provides the call signaling. It is important that the intermediate service provider(s) then reliably passes the calling information in the signaling path to the downstream providers on the terminating side, unaltered.

7.2.3 Terminating Service Provider

A terminating service provider can apply spoofing mitigation techniques at the request of the end user. This could be done using techniques such as invoking a Calling Line ID check against a blacklist, and blocking certain calls prior to reaching the called party. The ability to reliably block unwanted calls and to prevent legitimate calls from being blocked in error is contingent on the integrity of the blacklist and on the accuracy of the calling party information in the call signaling.

8 Analysis of Mitigation Techniques

Just like with cybersecurity, protection against calling party spoofing has no silver bullet and can only be realized by a layered approach of mitigation techniques. The mitigation techniques provided in this analysis also apply to illegitimate robocalls.

Even with the deployment of the STIR/SHAKEN framework, traffic from CS originations and IP Gateways (International & Wholesale) will be an issue for robocalling/spoofing, therefore deployment of other mitigation techniques in a layered approach is required.

Everyone has a role in the fight against calling party spoofing:

- FTC in prosecuting the bad actors.
- The carriers in deploying an appropriate layering of mitigation techniques to protect their customers. These include mitigation techniques provided by 3rd party platform/services facilitated by the serving carrier.
- Consumers in managing their communications. Only the consumer can choose to block a call/session on a per call/session basis, or give permission to the carrier or 3rd party on their behalf.

The layered approach of mitigation techniques needs to consider the following:

- Deployment of the STIR/SHAKEN framework.
    - The STIR/SHAKEN framework will provide a positive verification to the user that they can trust the caller ID information received. With that said, it does not address CS origination/termination.
    - In addition, the framework can be used to identify if the source of the traffic is coming from an international gateway, and the customer with this knowledge and the number can choose to receive the call or not.
    - The STIR/SHAKEN framework can be initially deployed using service provider-managed certificates as a more comprehensive and automated certificate management framework is developed and the policy around them is enhanced.
- Some form of post call reporting is a MUST, whether via a web portal, call center, or in/post-call signaling (e.g., *xx or indication in SIP BYE) to the terminating carrier or FTC, where appropriate and aligned with Customer Proprietary Network Information (CPNI) rules.
- Operationalize CDR tracing which provides a mechanism for identifying the source of the calling party spoofing in both CS, PS, and across CS-PS domains. Though parts maybe automated, it is mainly a manual process to start.
- DNO servers should be deployed at IP gateways, where the gateway blocks numbers that “should not be there” (e.g., 911 DNC List, government agencies).
- Blacklist/whitelists are useful, but require data analytics to be effective.
- Service Providers must verify numbers originating from IP PBXs. Likely performed by the service provider’s business subscriber Application Server.

Considering a layered approach will be required, and since not all Service Providers are the same with respect to the traffic mix they serve, the Federal Communications Commission (FCC) should consider “Safe Harbor” versus prescriptively regulating mitigation techniques.