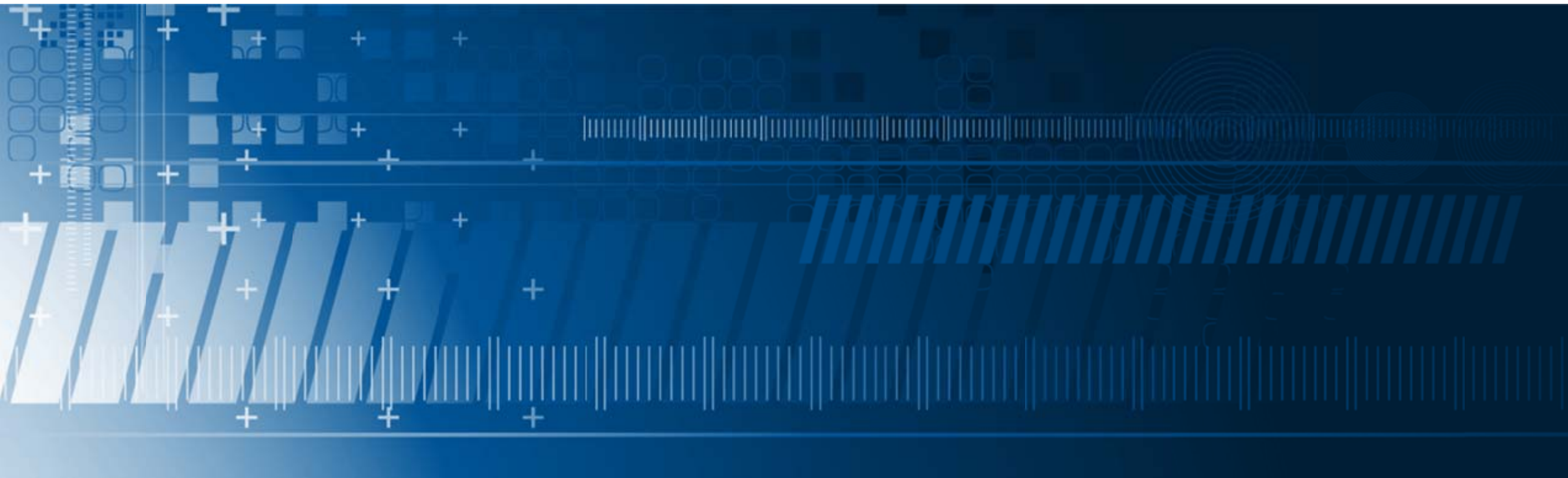
Calling Party Spoofing Mechanisms and Mitigation Techniques

Alliance for Telecommunications Industry Solutions
April 2016

ATIS-I-0000051



Abstract

The impact of illegitimate uses of Caller ID spoofing and robocalling presents unique challenges for the industry in addressing consumer concerns with unwanted and fraudulent calls. This paper outlines practical mitigation techniques being developed, and emphasizes Caller ID spoofing is not a static problem that can be solved with a single solution. Rather, a flexible, layered approach (similar to addressing cybersecurity risks) is needed to respond to these evolving threats.

Foreword

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.

Published by

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

Contents

Executive Summary

Goal

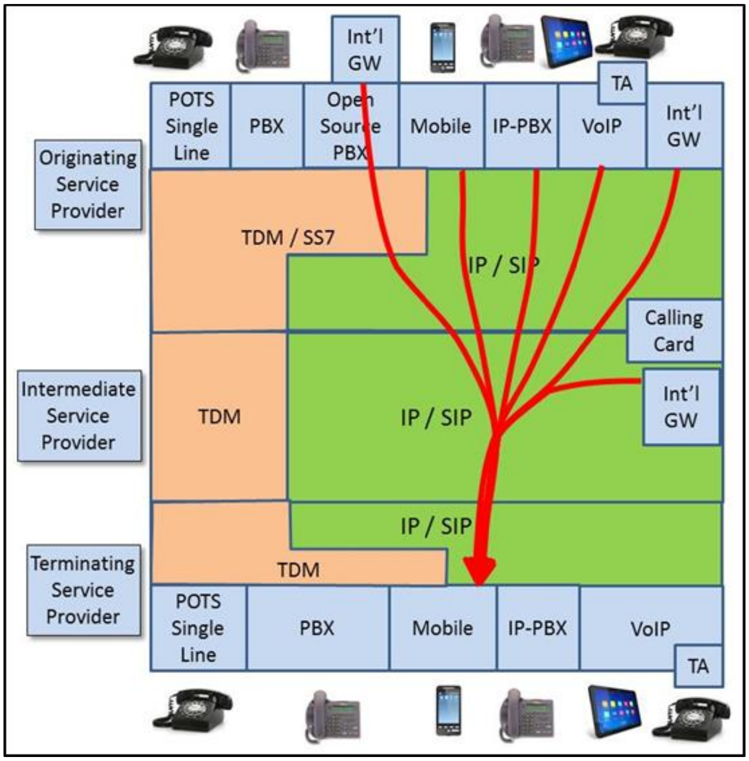
The intent of this paper is to educate and inform the reader regarding the current landscape of Caller ID spoofing and the related issue of robocalling. This document highlights practical mitigation techniques the industry is taking to provide the consumer with meaningful and useful tools.

Context

The focus of this paper is Caller ID spoofing and its impact on robocalling. Not all robocalls are spoofed, and not all spoofed calls are robocalls. There are also legitimate uses for both robocalls and Caller ID spoofing, so an outright ban would not be appropriate. However, illegitimate uses of Caller ID spoofing increase the impact of fraudulent robocalling and undermine techniques to prevent unwanted robocalls. The end goal is to give consumers the tools to reduce unwanted and fraudulent calls. Mitigating illegitimate Caller ID spoofing will not by itself fully achieve this goal but it will clearly help consumers.

Calling Scenarios

Voice calls originate and terminate from many different sources and can be transported over two technologies: TDM/SS7 (i.e., “circuit switched”), IP/SIP, or a combination thereof. This creates many possible calling scenarios involving a myriad of technology combinations, so proposing a “solution” for one specific scenario is not realistic. It is more accurate to use the Cybersecurity language of “threat vectors”. Mitigation techniques must consider all technology combinations rather than simply focus on the hot problem of the day. Vigilance and flexibility are also needed considering that technology and threat vectors continually evolve. This diagram is complex, but in reality it only provides a very simplified, current picture of the real network complexity that must be considered for every call scenario, 24/7/365.



Problem Statement

In today's network, terminating service providers do not have the capability to directly verify the accuracy of the calling party number. Signaling information for both SIP and TDM networks includes the calling party number, but this can be spoofed in many ways.

Mitigation Techniques Currently in Use

A variety of mitigation techniques are already available to help consumers reduce unwanted and fraudulent calls. White lists, black lists, anonymous caller rejection, smartphone apps, voicemail screening, and cloud-based applications are all offered to users by service providers, app developers, and third-party providers. Unfortunately, all of these mitigation techniques rely to some extent on the accuracy of calling party information, which is a primary motivation for the growing illegitimate use of Caller ID spoofing to undermine today's defenses.

The Way Forward – SIP

The IETF STIR Working Group is developing a mechanism to allow phone numbers to be "signed" at the origin, and "verified" at the termination. ATIS has proposed enhancements to make the approach practical by allowing service providers to perform the "validation" and "verification" on the user's behalf. Approval at the IETF is expected this year, and will set the stage for the following additional steps:

- SHAKEN: Options within protocols could lead to implementations that may not be interoperable. The ATIS/SIP Forum IP-NNI Task Force is developing a profile framework (SHAKEN) setting forth standards to allow for consistent implementation in service provider networks. Completion of this framework is planned for the end of this year.
- Display Framework: A framework is required to allow for the display of validated Caller ID information to end users in a consistent and secure format. The ATIS/SIP Forum IP-NNI Task Force is developing this framework, with the initial deliverable expected by the end of 2016.

The Way Forward – TDM

No viable mechanism has been proposed to validate and securely transmit real-time Caller ID information in TDM networks. The focus for TDM networks is shifting to forensic analysis, using Call Detail Records (CDR) to trace the call from the termination back to the network of origination to identify the source of fraudulent calls. Today, this is a time-consuming manual process, but the feasibility of automating portions of this traceback process is being evaluated.

Conclusion

Caller ID spoofing is not a problem that can be fixed with a “silver bullet”. If the dike has a leak, a flood can be stopped with a finger, but with a sieve the water simply takes another path. Mandating a single “solution” to Caller ID spoofing would be counterproductive; fraudulent callers would simply adapt to exploit other weaknesses in existing or future infrastructure. Instead a layered approach, similar to that used in cybersecurity efforts, with a range of choices of mitigation techniques, provides the flexibly to respond to an evolving threat. ATIS is playing a key role in developing industry standards for these mitigation techniques in a timely manner.

Scope & Purpose

Scope

This white paper will: define, in non-technical terms, Caller ID spoofing and its relationship to robocalling; describe the threat vectors and landscape that make Caller ID spoofing and robocalling problematic; set out use cases for legitimate Caller ID spoofing that must be allowed regardless of mitigation strategies adopted against the practice; enumerate the industry's efforts in developing those strategies; and explain the basic mitigation approaches.

While the paper's principal focus is Caller ID spoofing, it also addresses robocalling, given the close association between these two topics. We encourage the reader to keep this connection in mind, as it entails many aspects, including:

1. Not all spoofed calls are robocalls, and not all robocalls are spoofed; however, there is often a correlation between the two.
2. The ability to illegitimately spoof Caller ID information increases the impact of fraudulent robocalling, and makes techniques to block robocalling less effective.
3. There are legitimate and illegitimate uses of robocalling and spoofing, forcing industry stakeholders to struggle in the development of mitigation techniques for one or both that do not harm valid uses for either.
4. The negative consequences of robocalling span the spectrum from a nuisance to the consumer to potential fraud, as does Caller ID spoofing.
5. The mitigation techniques described in this document can impact robocalling as much as Caller ID spoofing.

Purpose

The paper educates policymakers and others about the challenges posed by Caller ID spoofing and related robocalling, provides an overview of existing mitigation techniques, and defines the clear need to allow industry to continue developing these techniques given the fast-changing and unknowable aspects of spoofing practices. The paper addresses what the industry is doing with regard to mitigation techniques to attempt to diminish the impact of illegitimate Caller ID spoofing, and may be subject to updates as ATIS learns more about the subject.

Definitions & 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 >.

For purposes of this white paper, the term "mitigation technique" will be used to describe any method(s), such as products, services, tools, applications, features, or technologies, used to lessen or reduce the frequency, magnitude, or severity of Caller ID spoofing.

Calling Party Anti-Spoofing

Caller ID is the marketing name for a Calling Number and/or Calling Number+Name service offered by service providers (SPs). While there are many terms used to refer to this service, [e.g., Calling Line Identification Presentation (CLIP) and Calling Line Identity/Identification (CLI)], Caller ID is defined in the ATIS Telecom Glossary as "a network service feature that permits the recipient of an incoming call to determine, even before answering, the number from which the incoming call is being placed". Although Caller ID can include both the calling number and the calling name, the discussion in this paper is focused principally on calling number only.

Technological changes have made it easier for callers to manipulate Caller ID (i.e., Caller ID spoofing). In combination with readily available robocalling technology, this has led to a dramatic increase in consumer fraud. It is generally illegal to transmit misleading or inaccurate caller identification information with the intent to defraud, cause harm, or wrongfully obtain anything of value, but many callers violate the *Truth in Caller ID Act* .[1,2] However, the law only applies to callers within the United States.

Examples

Some examples of Caller ID spoofing include, but are not limited to, the following:

- Reflection spoofing (i.e., spoofing the called Telephone Number (TN) in the Caller ID).
- Random number generators providing spoofed TNs.
- Calling patterns:
    - Same TN with many calls to different numbers within a short period of time.
    - Same TN sequentially calling large blocks of TNs.
- Phantom traffic (i.e., calls terminating in which the Caller ID information has been stripped or altered potentially creating billing issues).
- Local or long distance spoofed TNs resulting in call backs to the TN (i.e., individual or business) that was spoofed.
- Spoofing the TN, then hacking into the user's voice mail account and gaining access to the user's voice messages.
- Prank numbers (e.g., 911-NXX-XXXX) or other malicious activity.

These activities lead to decreased consumer confidence in their phone service, problems for law enforcement, and negative bottom-line effects on legitimate providers of voice services, among other things.

[1] U.S. Senate Committee on Commerce, Science, & Transportation, July 10, 2013 Hearing, "Stopping Fraudulent Robocall Scams: Can More Be Done?", Prepared Statement of the Federal Trade Commission, http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=aacf57ff-1b70-45c5-9ef1-837ebea0a911. Site last visited 4/19/16.

[2] See *Truth in Caller ID Act*, 47 U.S.C. § 227(e); cf. 16 C.F.R. Part 310.4(a)(8).

Comparative Call Types Where Spoofing May Occur

Table 1 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 1: Types of Calls Where Caller ID Spoofing May Occur[3]

Risk & Impacts	**Legitimate Uses**			**Potentially Illegitimate 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 [Public Safety Answer Points (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

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.

Calling Scenarios

This section defines the types of networks that can be involved in a voice call to illustrate the range of scenarios that must be considered when evaluating mitigation techniques for Caller ID spoofing.

Call Origination

Voice calls can originate from the caller's traditional Plain Old Telephone Service

[3] Table 1 is adapted from ATIS-0300114(2016), *Next Generation Interconnection Interoperability Forum (NGIIF) Next Generation Network (NGN) Reference Document Caller ID and Caller ID Spoofing.*

(POTS) phone or an Internet Protocol (IP) enabled phone, PC, tablet, or mobile phone using VoIP clients or embedded clients. Calls originating from these phones can connect to an originating network over individual lines or to a private branch exchange (PBX), which hosts multiple lines to serve a business facility. The originating network will also process and route the call as a local call or long distance call and may transfer the call on to an intermediate network for further processing and routing, or could send the call directly to the terminating network. The originating network represents the first network in the call path.

Call Termination

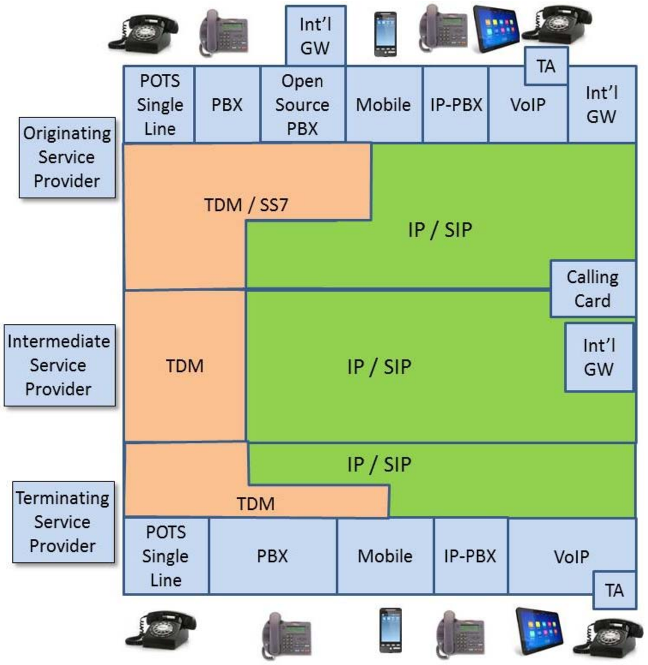
Voice calls can terminate to the called party's traditional POTS phone or an IP phone, PC, tablet, or mobile phone using VoIP clients or embedded clients. Calls terminate to these phones via a terminating network over individual lines or to a PBX, which hosts multiple lines to serve a business facility. The terminating network will alert the called party and set up the audio path when the call is answered. The terminating network represents the last network in the call path.

Intermediates

Voice calls may traverse intermediate networks in scenarios where the calling and called party are not local to each other or served by the same local service provider. Multiple intermediate networks can be involved, depending on whether the call is regional, national, or international. For the purposes of this paper, we will consider only the simplistic call scenario where there is just one intermediate network involved in the call.

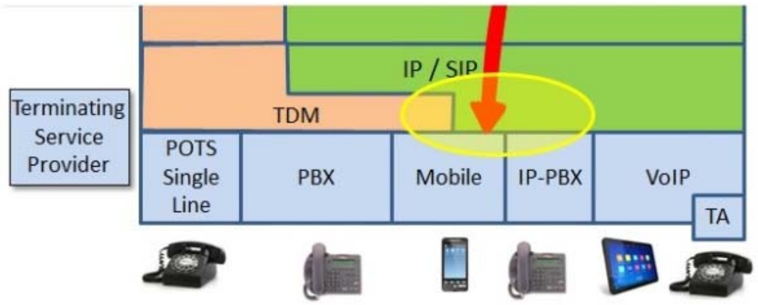
Calling Scenario Examples

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 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.

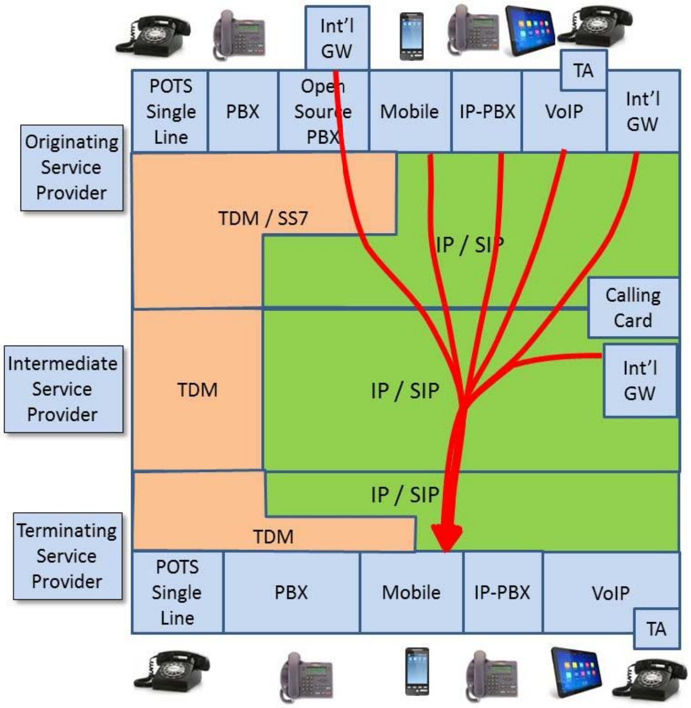


Although this diagram is a simplified picture of calling scenarios in today's network, it is adequate to illustrate the limitations of simplistic approaches that focus on only one of the many calling scenarios and then claim to "solve" the problem of Caller ID spoofing for all call scenarios.

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.

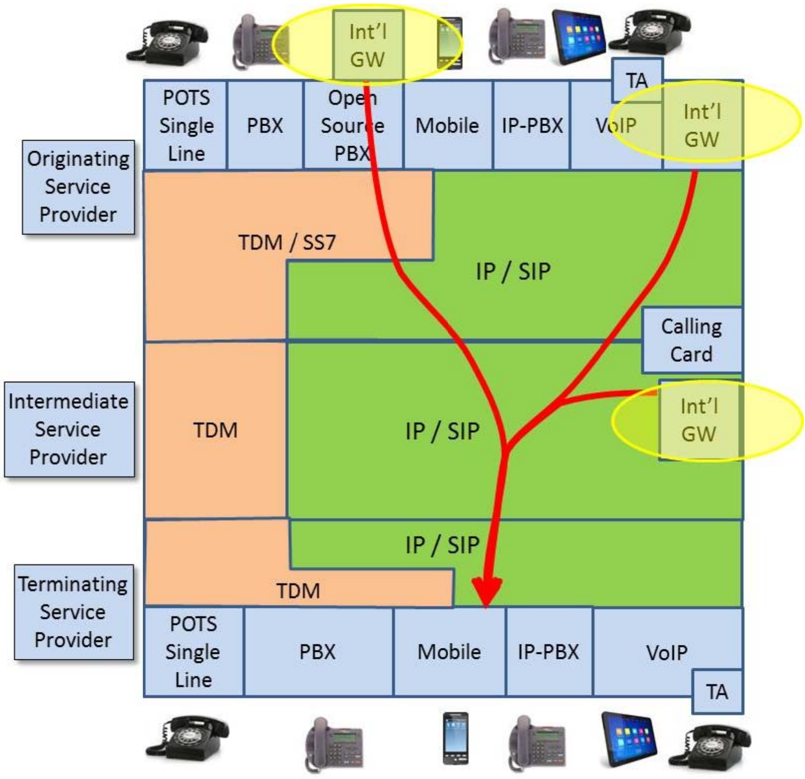


In this example, the terminating service provider only knows that the call is coming from an intermediate service provider over an IP connection with SIP signaling. If the picture is expanded to show some of the possible sources of this incoming call, a far more complex scenario emerges.



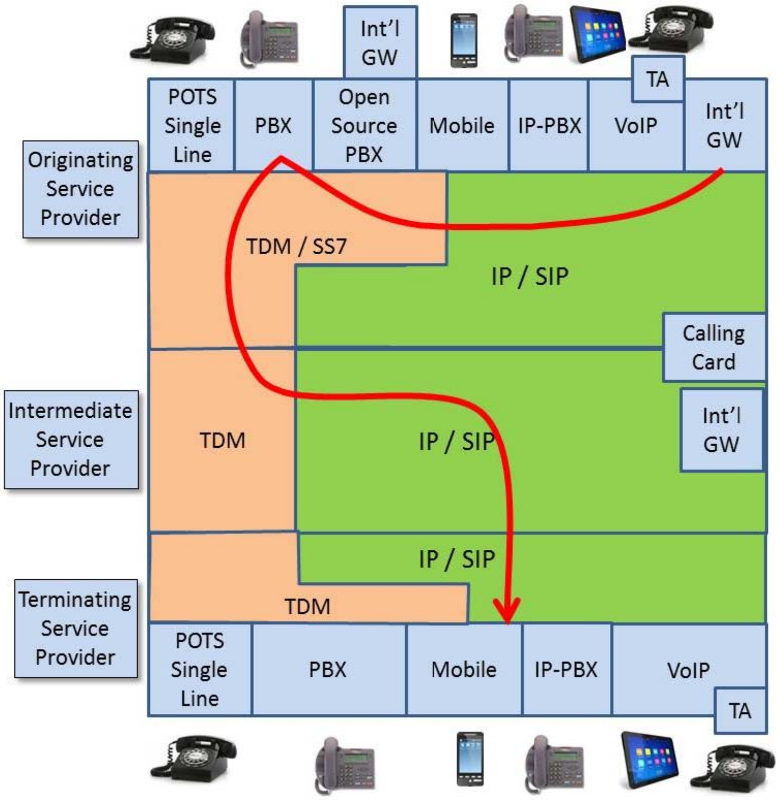
The terminating service provider does not know the source of a call or the accuracy of the incoming calling party information. This undermines mitigation techniques that can be utilized with the intent to stop malicious calls.

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.



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.

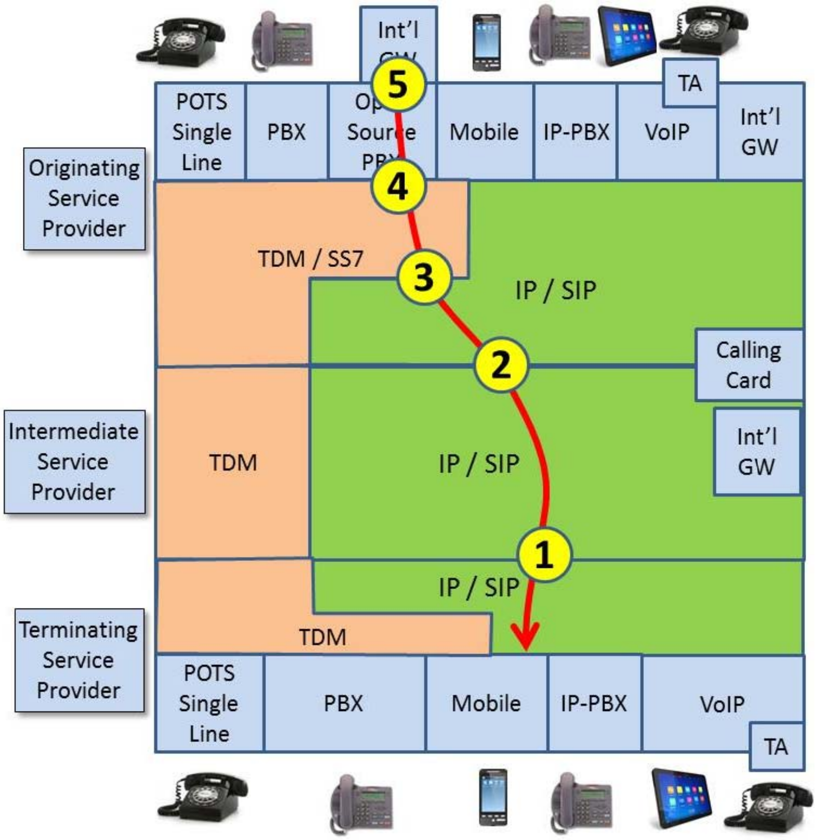
The "open source PBX" shown in this diagram is just one example of "re-origination" of traffic that hides the true source of a call, and can be used for many malicious reasons including arbitrage and outright fraud. The origin of a call can also be obfuscated through the use of call forwarding. In the 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.



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

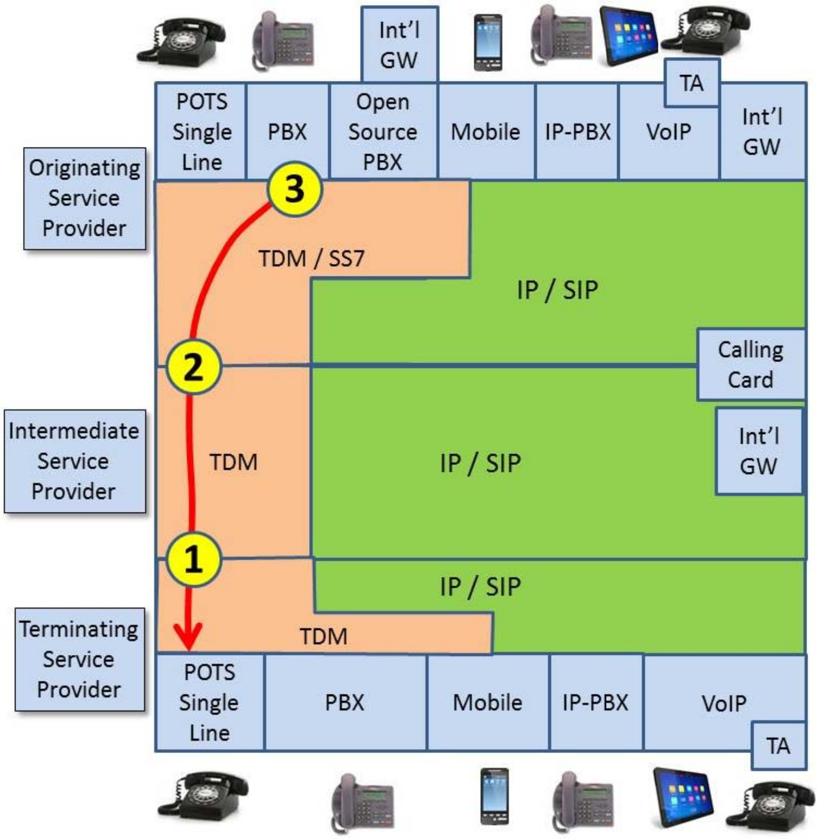
1. When traffic is passed from the intermediate service provider to the terminating service provider, although signaling information may be passed through the call path, many calls may not identify the source of calling party information and do not indicate if that information has been validated. The 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 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.



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 Call Detail Records (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.



Calling party spoofing is not a single, well-defined problem that can be addressed with a "silver-bullet" solution. It is instructive to use the analogy of a flood to better understand the situation. If the problem is a dike with a single leak, one small finger will stem the flow. 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, attackers 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.

Calling Party Spoofing Mitigation Techniques

This section provides an overview of mitigation techniques that are in use today to help consumers deal with nuisance phone calls.

Enabling Features and Technologies

This section describes a number of features that help the called party to manage incoming calls, either passively or actively. Where available, these features in general may not directly deal with Caller ID spoofing, and in many cases implicitly depend on the accuracy of Caller ID information.

Call Display / Caller ID

Call Display is a telephony feature that provides the name and telephone number of the calling party on a compatible display device. Name and number are delivered immediately following the first full ring.

Voicemail

Voicemail is a telephony service that allows callers to leave a recorded message for subscribers and stores them for later playback. It is different from traditional answering machines in that the messages are usually stored within the carrier's network.

Selective Distinctive Ringing

Selective Distinctive Ringing is a telephony feature which allows incoming calls from a list of customer-defined numbers to be identified by a special ring.

Simultaneous Ring

Simultaneous ring is a telephony feature applied to a specific number whereby any call to that number will result in other, user-defined telephone numbers ringing at the same time. For example, a subscriber may choose to have any call to their home phone number also ring their cell phone and business phone number. As soon as the call is answered by any handset, the ringing stops. Simultaneous ring is a variation on call forwarding and is implemented at the network level; however, not all switching platforms are capable of providing the feature and will have different restrictions in terms of the number of end-points that can be called.

Malicious Call Trace

Malicious Call Trace is a telephony service intended to protect customers from receiving threatening and/or malicious phone calls. After receiving such a call, the caller generally enters a star code (i.e., *57) which records details about the source, date, and time of the calls. This information can then be used by Security teams within the Carrier as well as local law enforcement to help identify the offender. The information generated may also be used as evidence for any court proceedings. This feature can only be accessed after a call has ended.

Techniques

This section describes a number of techniques that help the called party realize some degree of management of problematic incoming calls, either passively or actively. Where available, these techniques may also allow service providers, third parties, etc. to learn more about Robocalling events and/or Caller ID spoofing scenarios to potentially help mitigate future events. These techniques may not in general directly deal with Caller ID spoofing, and in many cases implicitly depend on the accuracy of Caller ID information.

Black Lists

A black list is a way to identify unwanted calls and disallow calls from undesired sources based on Caller ID. Preferences for how the call is to be treated can vary depending on the feature or application, ranging from fast busy treatment to redirection to voice mail. Caller IDs that do not appear in the black list will be allowed to ring through to the called party.

Local

Locally defined black lists would be personally managed by the end user on an ongoing basis to identify calls that the individual user does not want to receive.

Global

Globally defined black lists identify numbers associated with telemarketing or scams, and are potentially applicable to all users. Individual users can opt to use the global black list to block the call prior to reaching the called party.

White Lists

A white list allows calls from desired sources based on calling line ID. Calling line IDs not identified in the white list will be blocked or routed to treatment. This list is generally managed by the end user as a way to positively identify incoming calls to their phone.

Anonymous Call Reject

Anonymous Call Reject (ACR) is a telephony feature whereby subscribers can select not to accept calls that are not providing Calling Line ID information. Anonymous callers are typically routed to a recorded announcement, (e.g., "The party you dialed does not accept anonymous calls. Please hang up and call back with your caller identification unblocked."). ACR is a network-based feature that may not be available on all switch types. In mobile networks, ACR may also be implemented on the handset as an app.

National Do Not Call Registry

The National Do Not Call Registry is the result of the Do Not Call Implementation Act of 2003 as initiated in 2004 by the Federal Trade Commission (FTC). Citizens have the opportunity to place their assigned TNs in the Federal registry. This can currently be done via the FTC web site: www.donotcall.gov. Telemarketers then have 31 days from the time that a TN is put on the registry to stop calling that TN (with some exceptions such as political calling, not for profits, surveys, etc. as called out in the Act). It should be noted that the Federal regulations currently prohibit telemarketers from calling wireless TNs.

Citizen complaints regarding inappropriate telemarketing calls can be made to the FTC or the FCC via their web sites:

- FTC site is www.donotcall.gov
- FCC site is www.FCC.gov/consumers/guides/unwanted-telephone-marketing-calls

The National Do Not Call Registry is intended to reduce instances of unwanted telemarketing calls, whether these calls are originated by robocalling or by other means. Similarly, the National Do Not Call Registry applies whether or not caller-id spoofing is involved. However, since caller-id spoofing can significantly increase the impact of unwanted calls, it is appropriate to consider the registry in the context of a full range of mitigation techniques.

Federal Communications Commission

End users may file a complaint with the FCC (https://consumercomplaints.fcc.gov/hc/en-us), whereupon each individual complaint will be given a tracking number and a response due date. Customers are advised of the complaint procedure at https://consumercomplaints.fcc.gov/hc/en-us/articles/202752940-How-the-FCC-Handles-Your-Complaint, and the FCC provides its own consumer information page regarding Caller ID Spoofing: https://www.fcc.gov/consumers/guides/spoofing-and-caller-id.

End users whose own telephone numbers have been used in a spoofing scenario may also alert their service provider. In these cases, although there is still limited recourse, it is possible that the local service provider may offer to provide the end user with a new telephone number.

State Do Not Call Lists

Currently, all 50 states in the U.S. operate state Do Not Call programs, many of which are linked to the National Do Not Call Registry. A number of states continue to maintain their own, separate Do Not Call lists. An aggregated list of the various programs for all states can be found on the Direct Marketing Association website: http://www.the-dma.org/government/donotcalllists.shtml. Called parties who have registered with their state program may wish to lodge a complaint with the state in addition to the FTC.

CRTC

Canada has federal Do Not Call rules that are substantially similar to those in the U.S. Under the Canadian *Telecommunications Act* there is a National Do Not Call Administrator that enables consumers to place their telephone numbers on a National Do Not Call List at https://www.lnnte-dncl.gc.ca/index-eng. Companies engaged in telemarketing or their agents must register with this administrator and subscribe to the lists. Failure to add a consumer to the list within the prescribed timelines, or telemarketing a consumer who is on the National Do Not Call List, subject to certain exceptions, can result in Administrative Monetary Penalties. In addition, the rules require entities engaged in telemarketing to maintain up-to-date Internal Do Not Call Lists comprised of both businesses and consumers. Telephone numbers placed on Internal Do Not Call Lists are effectively embargoed from telemarketing for a significant period of time. Failure to add a telephone number to one’s internal list or telemarketing to a telephone number on the Internal Do Not Call List is also subject to Administrative Monetary Penalties.

Do Not Originate

Do Not Originate is a proposed list-based filtering technique designed to block calls at the point(s) where the domestic VoIP network connects to the international network. These interconnection points (called VoIP international gateways) do not currently check the originating number; however, it has been proposed that they could be programmed to reject specific originating phone numbers. Any calls from numbers on the do-not-originate list—a reverse Do Not Call list—would be rejected by the gateway and either blocked from entering the phone system or marked with a fraud indicator, such as a made-up area code. Call filtering technologies can then reject those calls. The do-not-originate approach may not require changes in telephony protocols to implement at the international gateway, but it would require development of a "fraud indicator" for the terminating service provider.[4,5,6]

Initiate Legal Complaint

Called parties may lodge complaints via the Federal Trade Commission's website, www.donotcall.gov. The website advises, however, that a called party's number must be on the Do Not Call list for 31 days in order for a complaint to be validly filed. Additionally, the FTC's Consumer Information website (http://www.consumer.ftc.gov/blog/your-top-5-questions-about-unwanted-calls-and-national-do-not-call-registry) advises that a complainant's individual filing may not receive a direct response; however, the complaints are used by both the FTC in conjunction with law enforcement to spot trends and to take legal action against calling parties that have been identified. On its consumer site, the FTC also cautions that in all likelihood, originating numbers provided by a complainant have been falsified, and as such, are challenging to trace.

In many cases it is also possible to file a complaint about malicious calls directly with the service provider.

Honeypots

For the purposes of tracking call spoofing behavior, a voice honeypot is simply a collection of valid telephone numbers that should not typically be receiving inbound calls. Some of these numbers may be 'clean' (not having been previously assigned to an end-user) or 'dirty' (numbers that were assigned and sometimes abandoned possibly due a high rate of voice spam). Details of any inbound call attempt can be collected and analyzed with calls attributable to simple misdials identified and omitted. The remaining calls can be further evaluated to collect information related to possible unsolicited/spoofed calling patterns to help quantify the problem in greater detail (i.e., patterns and frequency). Although honeypots do not directly stop unwanted

[4] http://www.aging.senate.gov/imo/media/doc/Schulzrinne_6_10_15.pdf

[5] www.nanc-chair.org/docs/mtg_docs/Jun15_Numbering_Update.pptx

[6] http://www.cs.columbia.edu/2015/Schulzrinne-senate-testimony-robocalls/

calls, they can provide useful information to reduce the overall incidence of unwanted calls (e.g., support legal investigation, identify global black list numbers).

Location Where Mitigation Technique is Applied

This section describes the locations where mitigation techniques can be applied or controlled.

End User Applied

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 and 2) those available with downloadable apps. Each allow for setting up and maintaining black lists or white lists 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.

Consumer Equipment

Call blocking devices exist that can be installed by a user between their phone and the network. Users can set white lists or black lists through the unit's user interface and can also view call logs, including blocked calls. Similar call blocking functionality is also built into some phones through a similar user interface.

Direct User Action

The end user can manually decide whether to answer a call, ignore a call, or send it to voice mail based on the information in the Caller ID.

Network / Service Provider Applied

Mitigation techniques can be applied in the network by service providers. 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.

Originating Service Provider

An originating service provider may be able to authenticate a phone number assigned by the North American Numbering Plan (NANP); however, no mechanism is currently available that would allow the originating service provider to inform the terminating service provider and intermediate service provider(s) that specific phone numbers have been authenticated and others have not been authenticated. To address this, the IETF, with input from ATIS and the ATIS/SIP Forum IP-NNI Task Force, is defining a protocol (STIR) and an implementation guideline (SHAKEN) that will allow the originating service provider to authenticate Caller ID information and the terminating service provider to verify this information. This approach may be useful for SIP calls, but is not applicable for TDM calls.

Intermediate Service Provider

In the call path, the originating carrier provides the call signaling. 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]

Terminating Service Provider

A terminating service provider can apply mitigation techniques at the request of the end user. This could be done using a technique, such as invoking a Caller ID check against a black list, 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 black list and on the accuracy of the calling party information in the call signaling. STIR, which is being developed in IETF with input from the ATIS/SIP Forum IP-NNI Task Force, is working to provide a mechanism to attempt to enhance the accuracy of Caller ID information for SIP calls; however, this mechanism is not applicable for TDM calls.

Other Considerations

Calling Party Identification, Authentication, and Authorization at the User-to-Network Interface

Mechanisms to mitigate calling party identity spoofing depend on procedures in the originating network to identify and authenticate the end user, and to validate that the user is authorized to use an identity at the user-to-network interface (UNI). The procedure for verification in the originating network over the UNI is left to the originating service provider. This section summarizes key aspects of this process as it might occur within the originating network.

Identity

The caller identity used in call processing is a telephone number (TN). In its simplest form, this may be a geographic TN assigned directly by the service provider to a particular subscriber or a TN previously assigned by another service provider to the subscriber and ported into the originating service provider’s network. Through administrative procedures, these numbers may be tied to other identities representing the originating subscriber entity, such as a subscriber account ID, an individual or business name, a user login account, or an equipment identifier (such as an International Mobile Equipment Identity [IMEI]). These other identities are typically not

[7] 47 C.F.R. § 64.1601(a)(2)

significant to call processing, are not standardized across the telecommunications network, and are mostly not signaled with the call. In some cases a calling name may be signaled from the originating network, but it is more typical in current PSTN usage to use the presented calling TN at the terminating network to independently retrieve the Calling Name (CNAM) from a database. In more complex forms, there may not be a one-to-one correspondence between the calling TN and a subscriber, user entity, or device. Some of the situations where this can occur include the following:

- A call is marked with a calling number indicating a main business phone number or call center number, independent of the subscriber account or service provider used to originate the call.
- A call is marked with one of a pool of TNs assigned to a service reseller entity (e.g., an interconnected VoIP provider that utilizes TNs and facilities of another service provider) where the underlying service provider whose facilities actually carry the service is unaware of the specific user or subscriber account.
- A call originating on a personal device (such as a mobile phone) is re-marked with the TN of a business entity, such as in a physician call center system for selected calls.

Some Threats to Identity

Spoofing: An endpoint may mark a call with a TN other than its own. Note that there are valid scenarios for doing this, but when it is illegitimate, it is the primary threat that anti-spoofing mitigation mechanisms are intended to address.

Hijacking: An endpoint with an authorized TN identity may be hijacked, for instance via malware, and used by an attacker.

Re-origination: An endpoint may be used, with or without consent of the authorized entity, to re-originate traffic from other parties, and therefore is marked with the identity of the re-origination entity, rather than the original source of the traffic.

Identity ambiguity: An identity shared by multiple users does not indicate origination by any particular user. A TN assigned to a reseller may be assigned to a specific user entity in the reseller's service but that entity may not be known to the underlying service provider. Likewise, an identity not directly authorized to originate traffic (such as a toll-free TN) may be difficult to trace back to an originating service provider and/or subscriber entity.

Authentication

Authentication in the context of the UNI is the process of the originating service provider determining that an entity (user or device) is a valid entity entitled to use the telecommunications service. The purpose of UNI authentication is tying the user or device to a subscriber account for commercial purposes and, where applicable, registering it to the network for call processing purposes. An authentication process may or may not result in the user or device being tied directly to a specific TN. For instance, an authenticated device might be a mobile handset associated with one specific number, or a corporate PBX serving a fixed number of extensions, or network equipment within an interconnected VoIP reseller network serving a variable number of identities.

The legacy PSTN model for authenticating an originator was through the association of a physical analog loop with a TN, or possibly a physical digital loop, such as Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI), with one or more TNs. Mobile network authentication has typically used device-based authentication using credentials stored in the device firmware and/or Subscriber Identity Module (SIM). IP-based UNIs may utilize various methods of authentication including the following:

IP address access control lists: Devices at known fixed IP addresses are allowed to use the service.

Private/managed network connections or VPNs: Users or devices reached through private or managed access facilities or with access protected at the IP layer (VPNs) are allowed to use the service.

Device-based authentication: As with mobile network authentication, devices contain credentials in firmware used to authenticate the specific device to the originating service provider's network.

User authentication: A human or machine user logs into an account associated with its service, such as through username/password and/or two-factor authentication using credentials provided in real-time or credentials stored or cached on a device.

Some Threats to Authentication

Account hijacking: An account may be broken into and used by the attacker to originate calls.

Device/credentials cloning: A device's credentials may be cloned, and the attacker's device presenting the authorized credentials may originate calls appearing to be the authorized user.

IP address spoofing: A device authorized by IP address alone may have its address spoofed by another device such as via direct access to the device LAN or IP subnet hijacking.

Authorization

Subscriber entities are allowed to use a service provider's services based on an authorization process that results in accounts being provisioned and/or enabled in the network. As part of this process, there will typically be some form of TN authorization that associates one or more TNs with the account. In its simplest form, an individual TN is assigned by the service provider or ported from another provider and associated with a specific mobile or broadband endpoint or subscriber line. In more complex arrangements, a service provider may assign a block of TNs to an enterprise or reseller for use over a trunking connection. Where some TNs are not directly assigned by the service provider, authorization may be explicitly arranged with the subscriber or reseller and the third-party service provider that sourced the TNs, or it may be implicit in service agreements (a subscriber or reseller commits to only present calling TNs they are authorized to use by the originating service provider or another party). The service provider may potentially require a letter of authorization from another service provider or toll-free Responsible Organization (RespOrg, a company that maintains registrations for individual toll-free TNs) to accept TNs they did not either allocate directly or port in from another provider.

Some Threats to Authorization

Unsupported authorization claims: A subscriber or reseller entity claims authority to use TNs to which they are not entitled.

Exceeding authorization: A subscriber or reseller entity, if allowed to mark its own calls, uses a TN outside its authorization (essentially another aspect of identity spoofing).

No enforcement: An originating service provider does not specify or enforce a TN authorization policy.

Presentation to the End User

In today's environment, the calling party information presented does not convey any degree of trust to the end user. The standards groups are working to determine the most appropriate means to indicate their best effort validation of trust within the Caller ID based on certification. As the standards groups' work to define mechanisms to verify the trust for calling party information continues, it is also including work to identify a means to communicate this information to the user.

Clear indicators are needed to help users make their responsive decisions related to accepting an inbound call. The end user has choice in the selection of their CPE devices which provide the display of this information. Providers working to assess the certification of the Caller ID information then also need to determine the means to provide information that can be used in the CPE display to the end user. The information will need to show the provider's best effort reliability determination of the Caller ID information to aid the end user in making a responsive decision on whether to accept the inbound call and how to proceed if accepted.

Given the variety of capabilities of end user CPE devices, the determination of the means to provide information that can be used in the CPE display to the end user needs to be as simple and understandable as possible. Accessibility is another consideration, including diminished sight and hearing, as well as other disabilities.

Other factors outside the scope of this document such as user awareness, education, and best practices will also shape implementation.

Industry Initiatives

This paper has discussed a number of techniques in use today to reduce the incidence of unwanted or fraudulent calls in general, and robocalls in particular. These vary widely in their approach and implementation, but to a large degree, they all depend, to some degree, on the accuracy of the Caller ID information. The ability to spoof Caller ID information, without being detected, represents the Achilles Heel of all of these systems. As a result, significant effort is being expended to define mechanisms to verify Caller ID information during call setup, (primarily for SIP). Where real-time verification is not possible, the feasibility of tracing calls back to the origin, as part of a forensic analysis, is also being considered. This section provides additional information on these forward-looking industry initiatives.

SIP

The IETF STIR Working Group (draft-ietf-stir-rfc4474bis) has for some time been working on a mechanism that would allow individual phone numbers to be “signed” at the origin, and “verified” at the termination. The ATIS/SIP Forum IP-NNI Task Force has been working with the IETF to ensure this technique will also allow originating service providers to “validate” the calling number and for the terminating service provider to “verify” this information. Specifically, Persona Assertion Token, or PASSporT, defines a token framework for a method of signing the identity of a user and associated information for a call that can be transported by any network. IETF is also working on defining the protocol framework (RFC4474bis) to carry the PASSporT token inside the mechanism employed by SIP to establish a voice call over IP (SIP INVITE) as part of a new header “identity”. The additions proposed by the NNI Task Force to the work of IETF are intended to allow this technique to be applicable to service providers, which is important to ensure it is considered as deployable in service providers’ business decisions. While service providers understand the potential use of this technology in the future, consumers may find the concept of cryptographic signatures more difficult to appropriately understand. The IETF is in the final stages of defining STIR and PASSporT, and it is expecting approval this year. These are critical first steps in defining a mitigation technique for end-to-end SIP traffic. With the underlying protocol agreed, the following additional steps can proceed:

- SHAKEN (Secure Handling of Asserted information using toKENs): In practice, there are many potential ways to deploy a protocol in a network. This flexibility could lead to subtly different implementations by each service provider. If these implementations are not interoperable, it may not be possible to validate a call end-to-end with sufficient confidence. The ATIS/SIP Forum IP-NNI Task Force is developing a profile framework that will provide implementation guidelines defining how STIR can be implemented by network equipment vendors and deployed in service provider networks to support interoperability and potentially increase the level of confidence in the Caller ID displayed. This profile framework is called SHAKEN.
- Display Framework: Once SHAKEN is deployed it may be possible to begin validating the Caller ID information on individual calls, and potentially displaying this information directly to the end user using a consistent framework. Verified Caller ID information should be displayed to the user in a recognizably consistent manner, across a wide range of devices, or user confusion will result. This could actually make the situation worse by creating new opportunities for fraud, allowing spoofed Caller ID information to claim it is authentic. Network equipment providers will need to implement support for the access network interfaces.

Ultimately manufacturers of consumer equipment capable of displaying Caller ID information could implement the user interface, and a defined framework could provide consistency, avoid user confusion, and ensure interoperability with service provider implementations. The ATIS/SIP Forum IP-NNI Task Force is developing this framework.

TDM Networks

STIR will not provide a mitigation technique that can be extended to include calls over TDM networks, as STIR relies on SIP signaling versus SS7, the signaling system used for TDM voice calls. No viable mechanism has been proposed that would validate and securely transmit Caller ID information end-to-end in TDM networks in real-time. The TDM switches currently in the PSTN are largely manufacturer discontinued, making any potential change efforts moot. It is sometimes possible to use Call Detail Records (CDR) to trace the SS7 signaling information from the terminating Service Provider back to the originating Service Provider to identify the source of fraudulent calls and report this information to the appropriate authorities. Today, this CDR Traceback approach is a time consuming manual process, and while it may not require new standards, it may require new processes and most likely new systems to be developed, implemented, and operationalized. CDR Traceback could potentially complement STIR (deployed in SIP networks) and help mitigate Caller ID spoofing in TDM networks.

Summary

Caller ID spoofing is not a single well-defined problem that can be fixed with a “silver bullet”. The illegitimate uses of Caller ID spoofing increase the impact of fraudulent robocalling and undermine techniques to prevent unwanted robocalls. The end goal is to give consumers the tools to reduce unwanted and fraudulent calls. Mitigating illegitimate Caller ID spoofing will not by itself fully achieve this goal but it will clearly help consumers. Mandating a single “solution” to Caller ID spoofing would be counterproductive; fraudulent callers would simply adapt to exploit other weaknesses in the infrastructure. Instead a layered approach, similar to that used in cybersecurity efforts, with a range of choices of mitigation techniques, provides the flexibility to respond to an evolving threat. ATIS is playing a key role, working with IETF and the SIP Forum, in developing industry standards for these mitigation techniques in a timely manner.