Developing Calling Party Spoofing Mitigation Techniques: ATIS' Role

Alliance for Telecommunications Industry Solutions
August 2016

Abstract

ATIS is central to much of the coordinated industry work on solutions to prevent and reduce the impact of Caller ID spoofing and related robocalling. Illegitimate Caller ID spoofing increases the impact of fraudulent robocalls and undermines techniques to prevent unwanted calls. This report highlights the practical mitigation techniques the industry is developing to provide the consumer with useful tools to reduce unwanted robocalls, and concludes that a layered approach, similar to that used in cybersecurity efforts, provides the flexibility 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

Overview

ATIS is central to much of the coordinated industry work taking place on solutions to prevent and reduce the impact of Caller ID spoofing and related robocalling. It has previously documented the landscape on the issue, and is currently finalizing a detailed assessment of the problems associated with originating party spoofing in IP communication networks: identifying potential mitigation options: and analyzing the pros and cons of mitigation options. ATIS is also anticipating new work, led by AT&T, to analyze the feasibility of SS7 solutions associated with VoIP calls. In addition, the ATIS/SIP Forum IP-NNI Task Force is specifying a deployable mechanism for service providers to validate calling party information on SIP-based networks.

This and other related ATIS activities have been summarized in the *Calling Party Spoofing Mechanisms and Mitigation Techniques* white paper, published in April. This analysis concludes that a layered approach, similar to that used in cybersecurity efforts, provides the flexibility to respond to these evolving threats, and that mandating a single "solution" to Caller ID spoofing would be counterproductive.

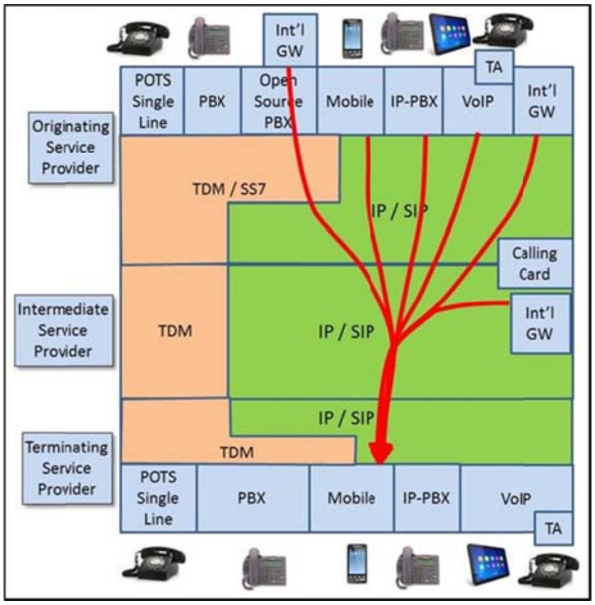
ATIS' work starts with this context. Not all robocalls are spoofed, and not all spoofed calls are robocalls. Consequently, a simple and complete ban is not a reasonable approach. There are legitimate uses for both robocalls and Caller ID spoofing. However, illegitimate Caller ID spoofing increases the impact of fraudulent robocalls and undermines techniques to prevent unwanted calls. Reducing illegitimate Caller ID spoofing will not by itself eliminate unwanted and fraudulent calls, but it will clearly help consumers.

Highlighted below are practical mitigation techniques the industry is developing to provide the consumer with useful tools to reduce unwanted robocalls, highlighting ATIS' contributions to these initiatives.

Problem Statement

In today's network, terminating service providers do not have the ability to directly verify 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. Consumers and call-blocking apps cannot distinguish between correct Caller ID information, and spoofed numbers.

Calling Scenarios



Voice calls originate and terminate from many different sources and can be transported over TDM/SS7 (i.e., "circuit switched"), IP/SIP, or a combination thereof. This creates an almost infinite number of calling scenarios involving a myriad of technology combinations.

Proposing a "solution" for one specific technology cannot address all network scenarios. Reducing unwanted robocalls will require a cybersecurity approach that addresses "threat vectors". Mitigation techniques must consider all technology combinations rather than simply focus on the hot problem of the day. Flexibility is also important, as technology and threat vectors will continue to evolve.

Mandating a prescriptive technology approach would not provide a stable long-term solution. This diagram illustrates the existing communications network. While the diagram is complex, it offers a very simplified view of the actual network complexity that must be addressed. ATIS' Technical Report on an Analysis of Mitigation Techniques for Calling Party Spoofing would be an excellent resource to the strike force as it considers solutions.

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 available to consumers from 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. Illegitimate Caller ID spoofing will increasingly undermine today's call-blocking services and applications.

The Way Forward – SIP

The IETF STIR WG (Secure Telephone Identity Revisited) 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 this mechanism practical in the near-term 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: A service provider profile for STIR will provide implementation guidelines and specify options within the protocol to ensure interoperability between all service providers. The ATIS/SIP Forum IP-NNI Task Force will complete this profile framework (SHAKEN) before the end of this year. Additional enhancements to the profile will be developed in 2017.
- 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.
- Root Certificate Authority: The signing and verification of calling party information is based on certificates issued by a recognized certificate authority. ATIS is working with the IP-NNI Task Force to specify the technical requirements and operational procedures for the SHAKEN Root CA.
- Testbed: ATIS has developed a detailed test plan to validate the SHAKEN protocol in real network configurations. This will verify the protocol and ensure interoperability between service providers.

The Way Forward – TDM

No viable mechanism has been proposed to cryptographically validate and securely transmit real-time Caller ID information in TDM networks. However, it is anticipated that AT&T will initiate a new study in ATIS to assess if existing ISUP capabilities can be used to provide limited validation for the TDM portion of VoIP calls. In addition, work is underway to enhance "forensic analysis" in TDM networks, 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. SHAKEN also supports traceback within SIP networks, and by combining CDR and SHAKEN it will also be possible to offer traceback for hybrid TDM/SIP calls.

Timeline

The focus of this assessment is the development and validation of standards to support enhanced validation of calling party information, as a mechanism to alleviate unwanted robocalling. The following timeline specifically addresses the underlying standards. Deployment timelines will require additional input from service providers. Key standards deliverables include:

- IETF STIR/PASSport (a.k.a. RFC4474bis): Complete 4Q2016 (content is stable now). STIR provides a framework to cryptographically sign calling party information at the origin, and to verify this information at the call termination point.
- ATIS/SIP Forum IP-NNI Task Force SHAKEN Framework Document: Complete December 2016 (content stable by the end of August 2016). SHAKEN provides an implementation profile for service provider implementation of the base protocol defined by STIR.
- STIR/SHAKEN Lab beta software: available 3Q2016 for initial testing in 4Q.
- STIR/SHAKEN Testbed: Testing dates under discussion.
- Display Framework Requirements: base requirements complete December 2016.

Conclusion

Caller ID spoofing is not a problem that can be fixed with a “silver bullet”. Mandating a single solution for Caller ID spoofing would be counterproductive. Fraudulent callers would simply exploit other weaknesses in existing or future infrastructure. A layered approach is needed, similar to that used in cybersecurity, with a range of mitigation techniques and “best practices” providing the flexibility to adapt to evolving threats. The end goal is not to “eliminate robocalls”, but instead to give consumers the tools to reduce unwanted and fraudulent calls based on their individual preferences. Mitigating illegitimate Caller ID spoofing will not by itself fully achieve this goal but it will clearly help consumers. ATIS is playing a key role, working with IETF and the SIP Forum, to develop industry standards for these mitigation techniques in a timely manner.

Supplemental Information: Details on Mitigation Techniques

SIP

The IETF STIR WG (draft-ietf-stir-rfc4474bis) has for some time been working on a mechanism to allow individual phone numbers to be “signed” at the origin, and “verified” at the termination. The ATIS/SIP Forum IP-NNI Task Force worked with the IETF to ensure this technique allows originating service providers to “validate” the calling number and terminating service providers 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.

The additions proposed by the NNI Task Force to the work of IETF are intended to allow STIR/PASSport 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 directly 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 cryptographically 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. However, it may be possible to leverage the existing “Screening Indicator” parameter in ISUP to give an indication of the calling party information. It is anticipated that AT&T will initiate a new ATIS study in August to assess the feasibility of this approach. In addition, 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 potentially new systems to be developed, implemented, and operationalized. CDR Traceback could potentially complement STIR (deployed in SIP networks to provide Caller ID verification and traceback) and help mitigate Caller ID spoofing in TDM networks and in hybrid networks.