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.

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

Table of Figures

Table of Tables

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.