International Telecommunication Union

ITU-T Technical Report

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(06/2021)

TR.spoofing
Countering spoofing

Technical Report ITU-T TR.spoofing

Countering spoofing

Summary

The purpose of this Technical Report is not on the development of anti-fraud and identity verification platforms, but on providing information that could assist in implementing measures to counter spoofing.

Calling party number authentication mechanisms are not a global solution against fraud or spoofing, and their development is covered in the specifications of other technical standardization bodies.

Note

This is an informative ITU-T publication. Mandatory provisions, such as those found in ITU-T Recommendations, are outside the scope of this publication. This publication should only be referenced bibliographically in ITU-T Recommendations.

Keywords

.Technical Report,,Technical Report

Table of Contents

Technical Report ITU-T TR.spoofing

Countering spoofing

1 Scope

The purpose of this document is not on the development of anti-fraud and identity verification platforms, but on providing information that could assist in implementing measures to counter spoofing.

Calling party number authentication mechanisms are not a global solution against fraud or spoofing, and their development is covered under the specifications of other technical standardization bodies.

2 Background

Spoofing is the origination of calls on the public switched telephone network (PSTN), or by using the Internet/session initiation protocol (SIP), with false calling party number (CPN) or calling line identification (CLI). This makes the call appear as though it is being made by someone else and it has become a common form of misuse and misappropriation of the numbering resources. It is especially pernicious for operators because they have no way of preventing these illegal calls with their numbers and they only ever learn of them from other operators or the recipients.

In the current network environment, there appears to be more and more fraudulent devices, including the private automatic branch exchange (PABX), call centre and, voice over Internet protocol (VoIP) access system, that interconnect to the PSTN or the public land mobile network (PLMN). As a result, a huge number of phone numbers are leased to anonymous call providers who help fuel phone spam. Noticeably, caller identification (ID) spoofing is particularly effective at defeating static call blockers, thus leading to a variety of scams by avoiding identification. Current mechanisms aimed at avoiding voice scams and ping calls are insufficient from a user's standpoint.

It appears that a small number of bad actors are responsible for the majority of robocalling.

Further, illegal bypass of international calls using over-the-top (OTT) telecommunication applications, including innovative techniques to disguise these practices, has caused significant loss to national revenues and national operators' revenues as well as inconveniences to the consumers.

In contrast to the well-known subscriber identity module (SIM) box practices, the recipient cannot identify whether the call is through legacy networks or through an OTT based route. The user is thus unable to reject the call or complain if the ID has displayed a local number that has been identified as the intentional caller, such as in the case of a SIM box.

The expected scenario is as follows:

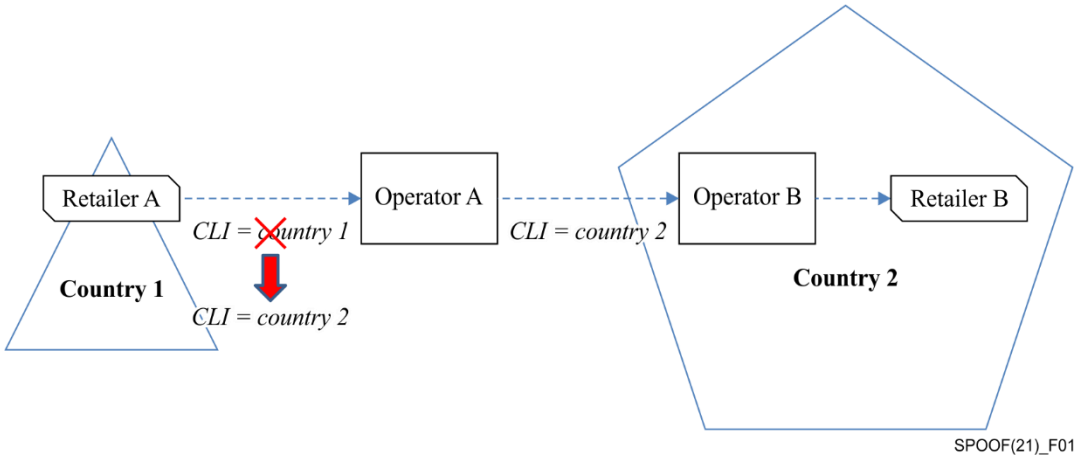
– In a normal call, the caller in country A initiates an international call to a callee in country B using a PSTN or PLMN (i.e., not using any Internet protocol (IP) based telecommunication application).
– Normally, the operator of country A will direct the call to an international operator who should in turn route the call to the international gateway of the recipient's country.
– If the international operator (e.g., a fraudulent operator) has an agreement with one or more OTT telecommunication providers, the operator will first check if the callee is a subscriber to an OTT service(s), if true, then the call is terminated automatically to the OTT application of the callee instead of being terminated to the international gateway of the recipient country B, noting that this is done without awareness, desire or consent of the originator and/or the recipient parties.

– The recipient who will receive a call on the OTT application is not able to identify whether the call was originated through the PSTN/PLMN or through the OTT application.

– The quality of service/quality of experience (QoS/QoE) of the call is usually less to significantly less than the QoS/QoE of the call through the PSTN/PLMN networks using operator grade international networks. But the user either at the originating or receiving end has no choice.

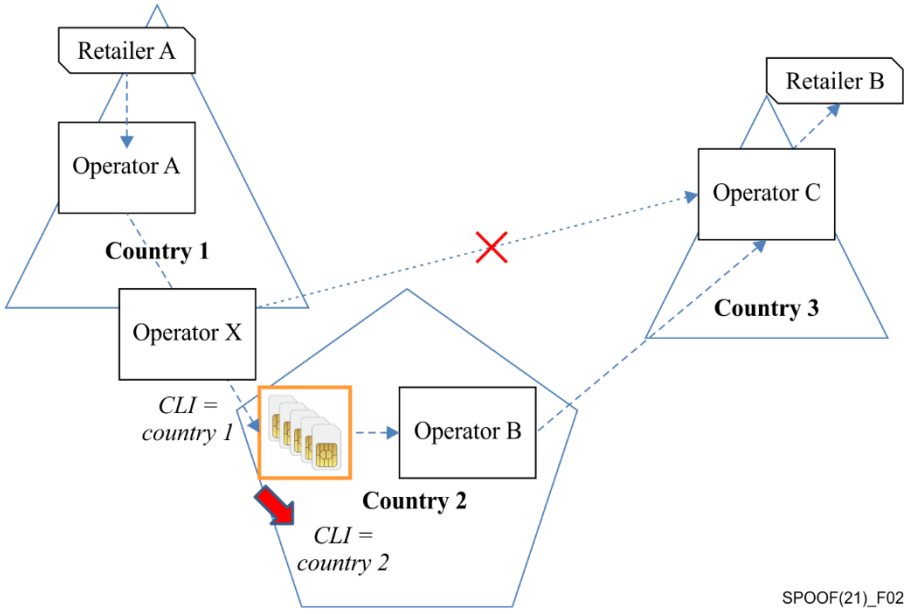
Some of the calls, in particular international calls, would partly involve Signalling System No. 7 (SS7) technology where an eventual in-band secure telephone identity revisited (STIR) mechanism (i.e., end-to-end SIP may not be applicable for the time being (see clause 3.1 below for an explanation of STIR). For the sake of the analysis, they may be assumed to be SIP-based as they may migrate to IP in the future.

a) CLI change for termination rates



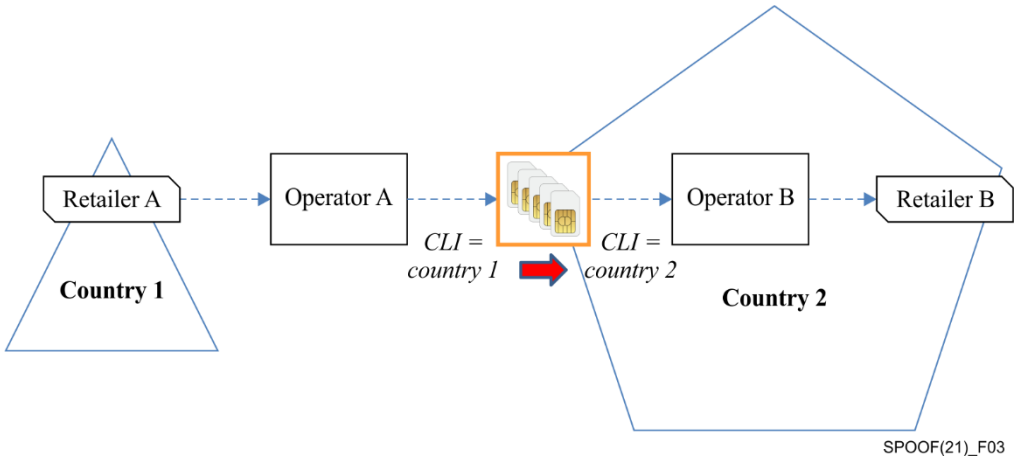
Rationale: the termination rate applied in country 2 may be partly or totally determined by the calling party number. Retailer A may spoof a number in country 2 to benefit from local/national termination rates as opposed to international rates it is normally subject to if the CLI were correct.

b) International SIM box call termination with retail flat rate or unlimited call offers



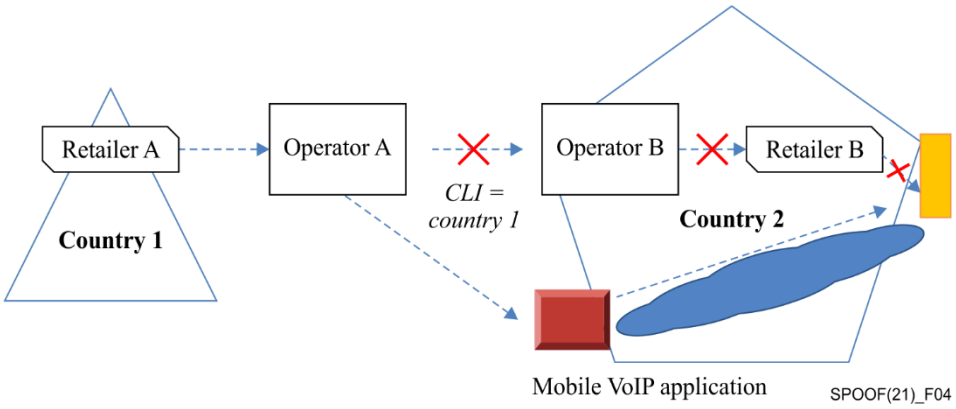
Rationale: as so-called retail "abundance offers" (national rate extensions or unlimited calls) between countries become more and more common (e.g., flat or unlimited calls between countries 2 and 3), they may be misused to obtain preferential rates for wholesale. An eventual mechanism for making the CLI unforgeable would make it possible to detect such calls more easily.

c) Local SIM box call termination for international calls



Rationale: international calls are terminated through local SIM box-initiated calls to benefit from national rates. An eventual mechanism for making the CLI unforgeable would make it possible to detect such calls more easily.

d) Local SIM box call termination for international calls



Rationale: the international call is terminated nationally through a mobile VoIP application without a CLI.

3 Possible solutions

International CPN/CLI information shall be provided in accordance with the provisions of Recommendation ITU-T E.157. However, it is recognized that various CLI and CPN spoofing activities are still ongoing globally. Different technical mechanisms are being tried or used to counter these spoofing activities, including the ones for detecting and blocking the infrastructure used for such spoofing activities and the ones for authenticating and blocking CLIs and CPNs. Such mechanisms are for further study.

Real-time solutions based on new SIP signalling information are very complex to be provided at the international level and they will impact each international network with costly modifications: it is difficult to consider a concrete viable solution at least in the short and medium-term.

The reasons for considering solutions such as STIR and/or signature-based handling of asserted information using tokens (SHAKEN) impacting, are mainly related to the impacts that these solutions would have on all existing implementations of VoIP networks based on SIP: in particular, significant costs, not sustainable, and which would require future availability of these solutions in all international networks, which is impossible to implement. To date, there is no such constraint and ITU-T SG2 cannot introduce it independently; for the European Telecommunications Standards Institute (ETSI) / 3rd Generation Partnership Project (3GPP) the STIR mechanism is only an option.

The problem of STIR/SHAKEN, and of all the solutions that mark the calls on the signalling protocol, is that, if an inconsistency of digital signatures is detected, the cause is not known (non-STIR network sections, problems on certificates, e.g., expired ones, network transmission errors, etc.) and therefore it is not possible to end calls, also because of the responsibilities towards customers. It is better to analyse offline anomalous cases to define the most appropriate actions.

Overlaid blockchain based solutions should be considered more applicable when widely defined and adopted, since, in principle, they will not impact networks and are independent of network technology (legacy and VoIP/IP).

The blockchain-based solution does not impact existing networks, is independent of technologies, and acts by overlapping an information and communications technology (ICT) platform to verify the transmitted information and carry out appropriate actions in case of inconsistencies.

Standardization and regulatory activities are needed on this matter.

Work on technical solutions is being undertaken in several forums, including 3GPP/SA1 and SA3, and the Internet Engineering Task Force (IETF)/STIR. The approaches can be categorized as follows:

1. Authentication of calling line identification, for example, the IETF, SHAKEN, and STIR frameworks for call authentication.
2. Static call blocking.
3. Dynamic call blocking, which is analogous to the solutions currently in wide use to filter e-mail spam.
4. Blocking the infrastructures used by bad actors to make unwanted calls.

3.1 Authentication

A mechanism for providing a cryptographically reliable mechanism to certify CLI could be useful to determine whether the calling number had been changed or whether the calling party "had authority" over the number.

The IETF approved the creation of a working group to define the mechanism(s) that allow verification of the calling party's authorization to use a telephone number (essentially as a calling line identity). The goal is (ultimately) to provide an instrument to prevent/circumvent calling line number "hijacking" for malicious purposes: voice mail hacking, robocalling, "vishing" (voice or VoIP phishing), or uncivil practices known as swatting (false report of an incident to emergency services).

The IETF has agreed on the STIR (see RFC 8224) and SHAKEN (see RFC 8588) frameworks for call authentication for both SIP calls and calls made on the PLMN/PSTN in the following RFCs[1]:

– RFC 8224 – Authenticated Identity Management in the Session Initiation Protocol (SIP)
– RFC 8225 – PASSporT: Personal Assertion Token
– RFC 8226 – Secure Telephone Identity Credentials: Certificates
– RFC 8588 – Personal Assertion Token (PaSSporT) Extension for Signature-based Handling of Asserted information using toKENs (SHAKEN)

[1] RFC 8224 history can be found at <https://datatracker.ietf.org/doc/rfc8224/>

These systems use public key-private key encryption for the terminating operator to validate that a call was originated by the operator associated with the CLI. Spoofed calls that cannot be validated would be blocked by the terminating operator.

To be truly effective, such authentication mechanisms should be applied at the global level, and operators should block calls from foreign entities that do not adhere to these mechanisms. This would require international agreement and corresponding national regulations. Purely national enforcement is not likely to be effective.

3.2 Static blocking

Some countries require that operators providing retail voice services implement universal call blocking at the network level for the types of calls where the caller ID (i) purports to originate from telephone numbers that do not conform to established numbering plans (i.e., national, ITU-T E.164), or (ii) matches the telephone number of the person being called.

3.3 Dynamic blocking

Some operators are offering dynamic blocking/filtering services to their customers. For example:

1. **Blacklist**: Numbers identified as nuisance callers by the operator's experts are added to an operator-maintained blacklist and calls from such numbers are sent automatically to the user's junk voicemail.
2. **Personal blacklist**: If a user gets an unwanted call, they can quickly add it to their personal blacklist. All future calls from that number will be sent to the user's junk voicemail.
3. **Individual call types**: Send calls from specific categories (such as withheld or international) straight to the user's junk voicemail.

One operator's blacklist is continuously updated to block phone numbers. The blocked numbers come from dynamic lists of known spam callers. The list includes the phone numbers of call centres that use spurious sales pitches, call at inconvenient times (before 8 a.m. or after 8 p.m. and at weekends), or do not comply with a national code of conduct. The code includes respecting directory listings marked with an asterisk to stop nuisance calls and a display of the caller's own number.

The list also contains numbers blocked personally by users. These numbers are not added to the blacklist immediately; they are anonymised and used to continuously improve call filter effectiveness. Several criteria are also checked before the relevant number is placed on the general blacklist.

In principle, the system works like an e-mail spam filter: software in the background checks the incoming call number in real-time before a connection is made. If the call is from a call centre the system decides whether it is a legitimate call from a research institute conducting a survey, a support call or an unwanted cold call. If it is blocked, the call recipient does not notice a thing. The caller hears the engaged tone. The system blocks domestic and international calls, although most unwanted calls come from abroad.

4 National actions

In general, countries and operators having inactive numbering resources like national destination codes (NDCs) should tidy up their assignments and inform the ITU accordingly to assist in the clean-up so that such resources cannot be misused and cause loss of revenue and credibility in the international telecommunications environment.

Several Member States have taken, or are planning to take, actions to reduce nuisance calls.

Member States that wish to publish the actions that they have taken may communicate them to the Director of Telecommunication Standardization Bureau (TSB), who will publish them as appropriate.