International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1246

(09/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Countering spam

Technologies involved in countering voice spam in telecommunication organizations

Recommendation ITU-T X.1246

International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	**X.1230–X.1249**
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1246

Technologies involved in countering voice spam in telecommunication organizations

Summary

Voice communication is a fundamental service provided by telecommunication networks. With the development of voice communication, voice spam has also been increasing with numerous negative effects on end users and network operators. In general, voice spam has content ranging from commercial advertisement to offensive pornographic material, which has various kinds of negative effects on end users and network operators. Voice spam may allure, annoy, bully or even intimidate users as well as having negative effects on network resources. To avoid these negative influences and to protect users' rights and maintain network stability, network operators may wish to increase their efforts to counter voice spam.

The objective of Recommendation ITU-T X.1246 is to review technical solutions to counter voice spam without consideration of the risk to the authenticity of the spammer identity. This Recommendation gives an overview of voice spam and summarizes the existing anti-spam technologies which are used by users and telecommunication networks alike as well as the collaboration mechanisms between them. Additional proposed technical solutions are also recommended based on these anti-spam technologies and collaboration mechanisms.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1246	2015-09-17	17	11.1002/1000/12448

Keywords

Spam, voice spam.

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1246

Technologies involved in countering voice spam in telecommunication organizations

1 Scope

This Recommendation gives an overview of voice spam and reviews existing technologies used to assist countering voice spam, including network-side and user-side technologies and the collaboration mechanism between them. In addition, this Recommendation also proposes additional practical anti-spam solutions, such as signalling records, interactive verification, controlling measures, etc.

This Recommendation focuses only on countering voice spam that has originated from the circuited-switched area in telecommunication networks with specified consideration of the characteristics of the network infrastructure. The technologies for countering voice spam originating from the IP-based area should be referred to [ITU-T X.1244], [b-ITU-T X.1245] and [b-IETF RFC 5039]. The technologies that prevent the impersonation of caller identities are outside of the scope of this Recommendation.

Compliance with all relevant laws and regulations should be considered before adopting the anti-spam methods described in this Recommendation.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1240] Recommendation ITU-T X.1240 (2008), *Technologies involved in countering e-mail spam.*

[ITU-T X.1244] Recommendation ITU-T X.1244 (2008), *Overall aspects of countering spam in IP-based multimedia applications*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 circuit-switched network [b-ITU-T M.60]: A network which provides connections for the exclusive use of the users for the duration of a call or service by interconnecting transmission channels or telecommunication circuits.

3.1.2 IP-based network [b-ITU-T E.370]: A network in which the Internet Protocol is used as the ISO layer 3 protocol (OSI Reference Model).

3.1.3 operator [b-ITU-T M.1400]: An organization responsible for identification and management of telecommunication resources. An operator must be legally recognized by the telecommunication administration of the country, or delegation thereof. An operator may or may not correspond to a trading partner.

3.1.4 spammer [b-ITU-T X.1231]: Spammer refers to the entity or the person creating and sending spam.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 voice spam: Unsolicited, automatically dialled, pre-recorded phone calls, usually with the objective of marketing commercial products or services. The content of voice spam ranges from advertisement of goods to offensive pornographic materials. Voice spam may have various kinds of harmful effects on users and operators.

3.2.2 honeypot: A software program (may be in a terminal) that emulates a terminal or a group of terminals so as to detect suspicious voice spammers and even assist in verifying them. The output of these systems can be used in evidence gathering.

3.2.3 management entity: An entity which may have one or more responsibilities for governing, auditing or guiding the work of countering voice spam.

3.2.4 third-party organization: An entity which can consult, assist or coordinate the work of countering voice spam.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CAMEL	Customized Applications for Mobile Enhanced Logic
CCLTP	Call Clear Time Point
CCOTP	Call Continued Time Point
CDMA	Code Division Multiple Access
COSN	Call Originated Subscriber Number
COTP	Call Originating Time Point
CRBT	Customized Ring Back Tone
CS	Circuit-Switched
CTSN	Call Terminated Subscriber Number
DMP	Device Management Platform
GMSC	Gateway Mobile Switching Centre
GSM	Global System for Mobile communications
HLR	Home Location Register
ID	Identification
ISIS	Information Sharing System
IMS	IP Multimedia Subsystem
IN	Intelligent Network
INAP	Intelligent Network Application Protocol

IP	Internet Protocol
IVR	Interactive Voice Response
MSC	Mobile Switching Centre
OTAP	Over-the-Air Platform
PSTN	Public-Switched Telephone Network
SCP	Service Control Point
SIM	Subscriber Identity Module
SLETP	Signalling Link Establishment Time Point
SLRTP	Signalling Link Release Time Point
SS7	Signalling System No. 7
STP	Signalling Transfer Point
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register
VMS	Voice Mail Server
VoIP	Voice over Internet Protocol

5 Conventions

None.

6 Overview of voice spam

Voice spam is unsolicited, automatically dialled, pre-recorded phone calls, usually with the objective of marketing commercial products or services. The content of voice spam ranges from advertisement of goods to offensive pornographic materials. Voice spam may have several harmful effects on users and operators.

6.1 Voice communication scenarios

Voice communication is a fundamental service provided by telecommunication operators. Originally, voice communication was based on the traditional circuit-switched (CS) networks. With the development of Internet, voice communication has expanded to include voice over Internet protocol (VoIP) across Internet protocol (IP)-based networks.

Four voice communication scenarios, each determined by the technologies used, are considered below:

- Scenario 1: CS-CS: Traditional mobile/fixed circuit-switched voice communications.
- Scenario 2: CS-IP: Voice communication originated from a mobile/fixed circuit-switched user and terminated at an IP telephony user.
- Scenario 3: IP-CS: Voice communication originated from an IP telephony user and terminated at a mobile/fixed circuit-switched user.
- Scenario 4: IP-IP: Voice communication between IP telephony users.

These four communication scenarios and associated technologies are shown in Figure 1.

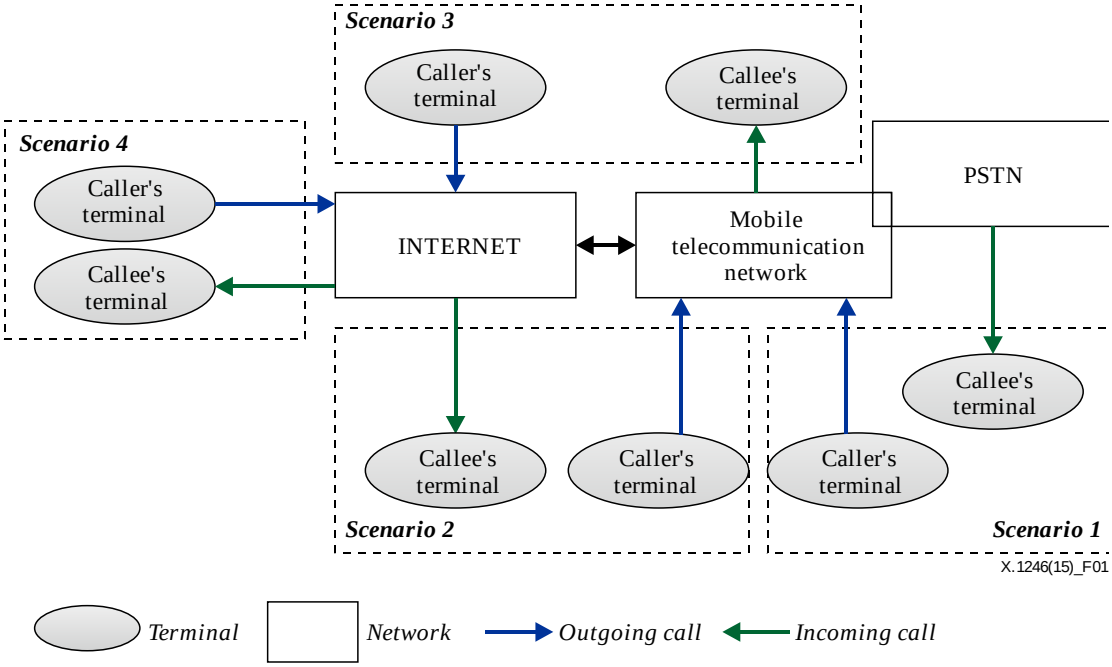

Figure 1 – Voice communication scenarios in telecommunication networks

NOTE – The term terminal as used here in Figure 1 may include mobile phones, fixed phones, laptops, personal computers and so on, which can access circuit-switched/IP-based networks. In general terms, most users do trust the source of voice telecommunication. Consequently, voice spammers are willing to use traditional circuit-switched voice communication to initiate voice spam. In addition, technologies for countering voice spam in scenario 3 and scenario 4 are recommended in [ITU-T X.1244]. Therefore, this Recommendation focuses only on countering voice spam in scenario 1 (CS-CS) and scenario 2 (CS-IP).

6.2 Characteristics of voice spam

Voice spam may spread content ranging from commercial advertisements to offensive pornographic materials, which may cause harmful effects on users and network operators:

– Voice spam may include tiresome, deceptive, bullying or threatening contents.

– Users and operators may suffer from wasting of resources.

– Users and operators may need to spend time, money and effort on countering voice spam.

The most widely recognized forms of voice spam are classified into but not limited to two types:

– **Type one (silent call)**: A silent call is a telephone call with the intention of tele-marketing that is generated by a predictive dialler (or diallers) with no intention of an agent immediately handling the call. In this instance the call may be terminated by the dialler and the called party receives a silence ("dead air") or a tone from the telephone company which indicates the call has been dropped. The term "abandoned call" has the same meaning. Usually, this kind of call will expect a call-back.

– **Type two (harassing call)**: A telephone call with the intention of telemarketing, which may also harass, annoy, alarm, or intimidate with a content of porn, threat, illegal information, sham advertisement and so on. Usually, this kind of call will not be dropped until put through.

7 Technologies for countering voice spam

7.1 General aspects

None of the solutions can be entirely successful independently. In order to mitigate the negative influence from voice spam, it is necessary to implement a comprehensive range of solutions with

correlative technologies, which are categorized into network-side technologies and user-side technologies to cover scenario 1 and scenario 2 described in clause 6.1.

To recommend concrete and practical technologies, it is necessary to take into account an in-depth consideration of the characteristics of the circuit-switched network, including the network architecture, the network topology, the signalling protocol stack, etc. In addition, voice service processes and the functional trends of the terminals are also considered. The recommended technologies can be classified into network-side technologies and user-side technologies.

Network-side technologies are key for operators, i.e., in public-switched telephone networks (PSTNs), universal mobile telecommunications systems (UMTSs), global system for mobile communications (GSM) and code division multiple access (CDMA) networks. Compared to the network-side technologies, user-side technologies are much more flexible and dependent on user initiatives. Feedback from users is a necessary supplement to the network-side technologies. Therefore, an effective collaboration mechanism between the two technologies should also be established.

7.2 Network-side technologies

Every phone call is initiated in the access network by signalling. In order to detect the suspicious voice spammer, the basic method is to collect signalling data, analyse it and verify it. This method should be considered comprehensively. Generally speaking, a call set-up phase involves a handshake between two ends of a communication. During the call setup phase, the only identification of the caller/called party is the caller identification (ID). This leads to the following observation.

1) Any call handling decisions should be made in real time before call set-up completion.

Voice spam presents complex technological challenges, and therefore solutions to eliminate it need to be supported by appropriate procedures coupled with technological measures. A fundamental network-side procedure for countering voice spam might include the following processes shown in Figure 2:

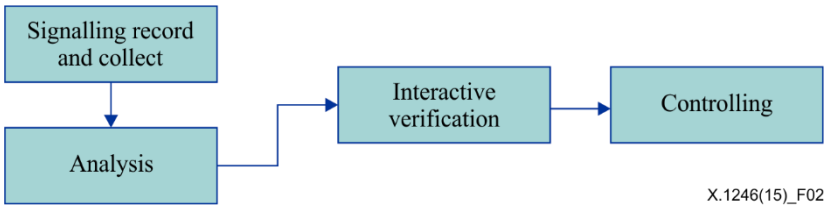

Figure 2 – Network-side procedure for countering voice spam

– **Signalling record and collect**: To record and collect the original signalling data in real-time.

– **Analysis**: To identity suspicious voice spammers and list their numbers.

– **Interactive verification**: To obtain direct verification in order to find the real voice spammers in the suspicious list.

– **Controlling**: To restrict or disable voice spammers which have been confirmed by the verification process in order to protect normal users.

The user-side procedure has almost the same processes but with simpler measures in each part. In some cases, interactive verification can be neglected.

According to the procedure, there are several technologies to deal with each part respectively. It should be noted that none of the technologies discussed in the following clauses will act as a "silver-bullet" or be the sole solution to the voice spam problems. On the contrary, all of the technologies are complementary and will be more effective when grouped together.

This Recommendation will introduce and classify technologies by their deployment positions, that is, network-side and user-side technologies and by the processes referred to in Figure 2.

7.2.1 Signalling record and collect

Signalling record and collect is to collect call detail record data in a (quasi) real-time way for analysis, which can include time-related or phone number related data, such as:

– Call originating time point (COTP): time point of a caller that generates a phone call.

– Signalling link establishment time point (SLETP): time point of signalling link establishment between a caller and a callee.

– Call continued time point (CCOTP): time point of a phone call continued and put through by callee.

– Call clear time point (CCLTP): time point of call cleared by a caller or callee.

– Signalling link release time point (SLRTP): time point of signalling link released after a call clear.

– Call originated subscriber number (COSN): normally known as the caller number, the number of a call originated by a caller.

– Call terminated subscriber number (CTSN): normally known as the callee number, the number of a call terminated by a callee.

The values of the same data, especially of time-related data, may differ slightly according to the positions of the collecting points. However, these disparities can always be ignored in practice.

It shall be noticed that all the data referred to in this clause are from the signalling channels but not from the service channels. In this signalling record process, all the data to be collected generally already exist in the signalling management system for accounting and performance diagnosis and therefore they can be re-utilized with consideration of cost balance.

NOTE – Only common data sources (based on signalling system No. 7 (SS7), intelligent network (IN), IP multimedia subsystem (IMS), customized ring back tone (CRBT), voice mail server (VMS), etc.) will be listed hereafter, though there are other alternative data sources, such as R2 and missed call alert systems.

7.2.1.1 SS7 signalling

SS7 signalling can be a useful source to assist in the monitoring of voice spam. It is practical to insert a signalling collection point to duplicate signalling information and parameters and record them. The signalling collection point is connected in parallel with the signalling link, so the signal is effectively "beam split", though only a small part of the signal power will be consumed by the collecting point. In this situation, a failure of the signalling point shall not have any negative effects on the signalling link.

There is also another method to collect SS7 signalling by inserting a hidden signalling node between two explicit signalling nodes. This means, that the hidden signalling node will first "block" the signal in order to record it and then relay the signal without any change but with a nuance on latency. However, this technology comprises the risk of a single point of failure. Therefore, a reliable failure and backup capacity is required.

The great advantage of using SS7 signalling records is that they contain the detailed call data from which various indicators can be deduced, see clause 7.2.2. However, if the voice call traffic increases and the network expands, the number of signalling collection points shall increase synchronously to cover all/major signalling sources in order to maintain an acceptable range of monitoring, which may lead to higher costs in countering spam.

It is recommended to deploy the signalling collection points in core/local networks. To achieve an overall collection, these points shall cover all the Mc and Nc interfaces of switchers. Furthermore, to achieve a balanced collection, these points shall cover only all of the Nc interfaces. If the focus is

only on national long-distance calls or international calls, long-distance/international signalling transfer points (STPs) shall be covered.

NOTE – The signalling collection point is a logical net element, which can be formed from different kinds of entity elements.

7.2.1.2 Intelligent network (IN)

A method based on service control points (SCPs) collects the customized applications for mobile enhanced logic (CAMEL) or intelligent network application protocol (INAP) signalling for analysis. The SCP is a key node in intelligent networks (INs) and a determinant factor in deciding how to process phone calls.

Once, a user is contracted for the IN service, the outgoing call will trigger the SCP to inquire about the called user's visiting location register (VLR) information before setting up communication links. As IN services are popular with some operators, it is easy to collect and record the signalling data of the call generated from IN-contracted users.

As the signalling collection points can be at/around the SCP, the method needs less signalling collection points compared to that of SS7. Whether these IN-contracted users are roaming or not, they can be monitored easily using this method.

There is however a limitation to this method. If penetration of the IN service remains at a low level, only a small part of the users' behaviours will be monitored. However, this situation can be resolved by helping each user to subscribe implicitly to a customized IN service, which will forward the inquiry request unconditionally to the SCP when an outgoing call is generated.

This method is restricted by the common IN service process, therefore only limited types of data can be collected, such as COTP, SLETP, COSN and CTSN, see clause 7.2.1. Nevertheless there is room for improvement if a more complex IN service process is introduced, for example, if all the telephony signalling signals are relayed by SCPs.

The IP multimedia subsystem (IMS) method is similar to the above, as IMS shares similar signalling procedures with IN.

7.2.1.3 Customized ring back tone (CRBT)

CRBT is a specific user-oriented service provided by some operators. Once a user contracts the CRBT service, other users will hear pre-ordered music clips instead of the ringing tone. As a result, the signalling record and collect data can be achieved in the CRBT hosts.

This method is restricted by the service process, therefore only limited types of data can be collected in the service hosts, such as COTP, CCOTP, CCLTP, COSN and CTSN, see clause 7.2.1. There are almost no more improvements that can be made to the CRBT process to collect more types of data.

However, if a voice spammer bothers a CRBT user, the spammer could be monitored. Therefore a high service penetration is a pre-condition to make the method practical. If this situation is satisfied, the investment in the signalling record and collections should be comparatively low.

7.2.1.4 Voice mail server (VMS)

Voice mail servers (VMS) handle calls in situations of call forwarding no reply, call forwarding busy, call forwarding unconditional, etc. In most cases, the VMS is irresponsive to a silent call unless the criterion is unconditional. VMS may provide voice recordings of a calling party if the spam caller intends to get the call connected and spam a callee directly. In this case VMS may strongly support the interactive verification process via the voice recordings from user feedback or authorization, see clause 7.3.3.

Similar to CRBT, service penetration and usage of VMS is a pre-condition to make the method practical.

7.2.1.5 Honeypot

The honeypot method is used for setting up a quantity of successive or random phone numbers to attract voice spammers. Besides data collecting, the honeypot method can also facilitate the analysis procedure as well as the interactive verification procedure.

Since the honeypot method can be put through by any caller (outgoing call), it can collect some particular types of data, such as COTP, CCOTP, CCLTP, COSN and CTSN, see clause 7.2.1. The honeypot method will calculate and transfer the data for some of the analytical measures which are described in clause 7.2.2.

7.2.2 Analysis

In order to make an analysis of countering voice spam by using the monitoring system, the collected original data needs to be calculated and transformed into meaningful indicators such as the connection rate, the call released time, the ringing duration, etc. In order to differentiate voice spammers from normal users, the indicators should be counted continuously for a specific period, normally known as the time window (duration). Operators may adjust the duration to an appropriate value based on the maintenance experience.

All the indicators can be deduced logically into a more comprehensive indicator called "the rule", which can be used in some algorithms to analyse the voice spammer's behaviour with a higher degree of accuracy. The rule model for analysing the voice spammer is shown in Figure 3.

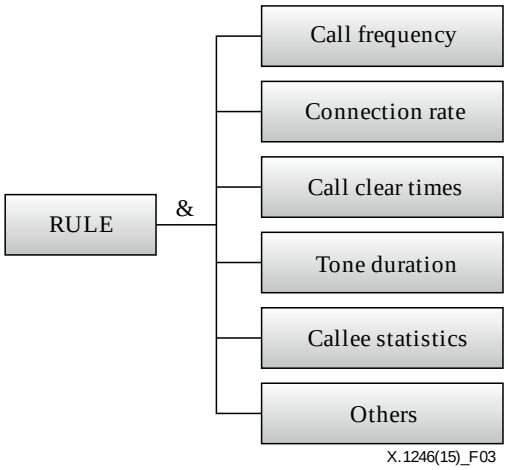

Figure 3 – Rule model

The rule model is deduced from several indicators by the logical AND operation. Since the data sources are from different sources and may be collected together, not all the indicators can be supported at the same time. A feasible solution to the problem would be to set the unsupported indicators to "TRUE" or to "1" to ignore them. For example, after collecting data and transforming them into indicators, the honeypot just needs the indicator of the tone duration to process the required analysis procedure and to set the other indicators' value to "TRUE" or to "1" to omit them.

The indicators contained in the rule model and their definitions are listed below:

– Call frequency: Number of calls in a particular period.

– Connection rate: Rate of call communications or the signalling link establishment.

– Call clear times: Number of times when the caller or callee releases the call on their own initiative.

– Tone duration: Time duration of the ringing tone.

– Callee statistics: Statistics on the callee characteristics, such as uniform distribution, arithmetic progression, etc.

The threshold value of indicators should be adjusted by the operators based on realistic service scenarios to balance the accuracy and cost. Furthermore, the concrete rules should be defined to match the different types of voice spam.

For example, there are two types of widely recognized voice spam, silent calls and harassing calls, see clause 6.2. A silent call (also called an abandoned call) is a telephone call initiated by a dialler who does not have an agent immediately available to handle the call. In this instance, the call may be terminated by the dialler and the called party receives a silence ("dead air") or a tone from the telephone company which indicates that the call has been dropped. Usually, this kind of call will expect a call-back. A harassing call is a telephone call that intends to harass, annoy, alarm, bully or intimidate with a content of porn, threats, illegal information and sham advertisement, etc. Normally, these calls will not be dropped until put through.

Silent calls and harassing calls (see clause 6.2) can show different indicator features respectively in terms of the proposed rule model. A higher value of call frequency or call clear times and a lower value of connection rate or ringing duration could indicate a silent call spammer. On the other hand, a harassing call may focus on a specified callee; it tends to keep the ringing duration longer and it obtains a higher connection rate comparatively.

In some circumstances, a group of silent callers will open the "unconditional forwarding" service to inform the network to forward the incoming calls unconditionally to a specific number, on which an interactive voice response (IVR) platform is working. The IVR platform can even send back the spam voice to the incoming caller by a ring tone. It would be helpful for the analysis to check whether the suspicious callers opened the "unconditional forwarding" service and what the destination number was.

The fact is that some more complicated and effective analysis models for countering voice spam exist, such as a model integrated with human society analysis, caller billable records analysis and so on. Nevertheless, the rule model could be a basis for evolving more comprehensive models.

7.2.3 Interactive verification

Required by the management entities or the user service agreement, the caller's number in the suspicious list shall be verified before controlling measures are taken. There are two alternative methods to operate the verification in terms of the requirement.

In the first method, the telecommunication organizations shall keep updating the suspicious list, submitting it to the management entities and accepting feedback from the management entities.

In the second method, if it is permitted by the user service agreement or the management entities, the operator could undertake a dialling test on a caller number from the suspicious list in order to obtain direct verification. Using the results of the dialling test, usually known as the voice record file, the authorized audit staff will attempt to indicate whether the record is spam or not.

However, the accuracy and quality of the interactive verification affects the controlling procedure.

As mentioned above, a honeypot can handle the interactive verification itself, i.e., if the calculation result of the indicators implies that the outgoing call is a silent call (see clause 6.2), the honeypot will call back to prove the evidence of the verification; in contrast, when the harassing call is confirmed by the indicators' analysis, the honeypot will put through the phone call and record it.

Furthermore, the coordination between a group of silent callers and an IVR platform or several IVR platforms may confuse the operators about the real source of the voice spam. Sometimes, the IVR platforms and the silent callers belong to different operators respectively. After achieving a spam voice record, it would be useful for example to trace the potential connection between a silent caller and an IVR platform by making a request to the home location registry (HLR).

7.2.4 Controlling

Controlling is used to restrict or disable/shut down voice spammers confirmed by verification in order to protect normal users. Two controlling methods are discussed below.

7.2.4.1 Whitelists/blacklists

Whitelists/blacklists, usually known as key account lists, are time consuming to create and require continued updating. The life cycle of each item in a whitelist/blacklist needs to be well-managed to keep it accurate and effective. Each item in a whitelist/blacklist also needs to be well-maintained in a secure way during its life cycle.

As described in [ITU-T X.1240], the quality of blacklists varies enormously depending on the professionalism of the compiler. Blacklists inevitably contain inaccuracies that prevent some legitimate calls from getting through to the receivers. Although their utilization raises many concerns, blacklists are a quick solution to refuse a connection between voice spam sources and receivers (phone users).

Blacklists including user numbers or number segments are usually deployed in a gateway mobile switching centre (GMSC), in SCPs, in switches and in other network entities. Generally, blacklists from the same operator network can be deployed in SCPs, switches or other network entities, while blacklists from other operator networks can only be deployed in a GMSC where the blacklist capacity may be too limited to store a large list of numbers. To solve this problem simply, hidden signalling nodes (see clause 7.2.1.1) can be used behind the GMSC.

Whitelists may need to interact with the authorized database maintained for callers already identified as legitimate to exclude unintended genuine callers that have similar characteristics to voice spammers. These callers may be call centres, notification services, feedback/data collection services such as due payment reminders, feedback of sponsored schemes from management entities, awareness programmes, emergency- or disaster-related programmes, etc.

7.2.4.2 Trace back mechanism

The trace back mechanism traces back the real physical location of voice spammers. It could be useful at certain times to point out the exact location or address of the voice spammer if necessary.

According to the existing techniques, operators can locate the voice spammer's real location based on information provided by the mobile switching centre (MSC); however, this technique can only locate the approximate area. More accurate location could be provided by the operator's location information service, such as an assisted global positioning service.

7.3 User-side technologies

User-side technologies should be an effective supplement to network-side technologies. The measure of feedback can provide detailed information on voice spammers (as discussed in clause 7.3.3), which is an especially important backup for operators. User-side technologies may need aid from some particular features of smart mobile phones, the support for which may vary according to the vendors.

7.3.1 Whitelists/blacklists

Users can utilize the connection-control feature in phones to block specific numbers or number segments as blacklists, while at the same time the connection-control feature will allow particular numbers (set by the users or synchronized by some mobile applications) to be always put through when they are treated as whitelists.

This method could work based on the whitelist/blacklist when synchronized by the network side, whereas the user side is usually subject to personal preferences because users can maintain their own lists.

7.3.2 Call-delay

Call delay is a signalling-level technique which specifically works for silent calls (see clause 6.2).

After the signalling link is established between a caller and a callee, the ring tone will be periodically generated from the link. Some silent calls will be produced and users will receive a silence ("dead air") or a short duration of the tone which indicates the call has been dropped.

With the support of a smart mobile phone, users can block the silent call at the terminal side (user side). Since users can set a value of the tone duration (threshold) for every incoming call at the signalling layer, silent calls may be omitted because the tone duration is less than the threshold. However, in the case of ignoring the "short-ring-tone" normal call, the calling record will be saved in the mobile phone's call log list to allow the user to double-check.

7.3.3 Feedback

After receiving voice spam, users can provide a feedback to the operators indicating the voice spam number and other detailed information. The feedback channels include sending text messages, phone calls and e-mails or even an official website to the customer service department (or other equivalent departments) of operators. All the channels should provide convenient and easy-to-follow procedures for users to provide a feedback. A user-friendly channel could be constructed by applications in terminals or subscriber identity module (SIM) cards and platforms such as the device management platform (DMP) or the over the air platform (OTAP) in the network.

Furthermore, once the service department of the operator has received the feedback, an authorized auditor should check whether the feedback information is real and effective and apply a similar procedure of interactive verification before taking proper further action. If there is a voice recording as proof from the VMS and if the access to the recording is authorized by the owner, the verification could be more effective and more efficient.

7.4 Collaboration mechanism

Operators may co-operate with management entities, other operators or users to establish a corresponding co-operation and communication mode, in order to counter voice spam.

Operators may establish or support an information sharing system (ISS). This particular system could cover the basic voice spam information exchanges with other organizations, including the suspicious/verified spam caller list, classification of each voice spam, the countering technologies, etc.

Management entities may consider the implementation of an ISS and the establishment of an information exchange mechanism or even the organization of formal meetings for operators and third-party organizations to share up-to-date information.

Users could share their blacklists with the server at the network side by uploading or downloading the blacklists. However, operators should have a verification mechanism through which they could detect whether an item in a personal blacklist is a real voice spammer or not. Operators should provide an interface for uploading and downloading blacklists. This mechanism could interact with customer feedback. At the same time, management entities should audit the updated information to avoid inappropriate information.

In order to implement the information sharing mechanism, operators may submit the verified blacklists, on a recurring basis to the management entities and block the established blacklists enforced by the management entities.

Management entities may also consolidate all the received blacklists from all the operators and apply appropriate actions and procedures. In addition, management entities may take on more responsibilities, such as restraining voice spam at source, while ensuring that operators implement their duties.

7.5 Proposed solutions

None of the solutions mentioned above can be entirely successful independently. In order to counter voice spam effectively, network-side and user-side technologies should be deployed comprehensively in each procedure.

In order to obtain a high degree of accuracy, it is possible for the signalling record procedure to integrate various data sources together. However, a comprehensive data-source would be an extremely expensive implementation.

The following situations should be considered:

The SS7 signalling records (see clause 7.2.1) alone could be an option because, compared to other data sources, SS7 signalling covers all the signalling links to obtain the most useful data to guarantee the effective countering of voice spam.

On the other hand, a data collecting system based on IN, CRBT or VMS may be a cost-effective alternative, if operators have already launched IN, CRBT or VMS services. However, as discussed in clause 7.2.1, data sources from CRBT or IN networks may not cover all the specific data. Hence, a data source from these services could be complementary.

The model proposed in clause 7.2.2 is easy-to-use and is not costly; it is also commonly deployed in countering voice spam. To increase the accuracy of the analysis, more sophisticated rule models and algorithms can be used. For example, statistics on the codes of calling release causes and statistics on the codes of rejected calls could significantly narrow down the suspicious list.

However, comprehensive rule models or algorithms may lead to a high degree of system complexity and long time-consuming procedures, which in turn, increase the delay of the whole procedure of countering voice spam, which may ultimately decrease customer satisfaction. Given all that, a wise choice of proper rule-models or algorithms is a quite significant factor for operators.

The interactive verification procedure may be different from nation to nation. Hence, management entities may assist operators to establish a proper verification procedure based on their national practice.

As can be seen from the controlling procedure described in clause 7.2.4, the user-side and network-side methods should be better integrated to mitigate the volume of voice spam. The customer service departments of the operators could play a significant role in the controlling procedure and in meeting customer demands.

Appendix I

Comprehensive measures on countering voice spam

(This appendix does not form an integral part of this Recommendation.)

Figure I.1 shows technical and non-technical approaches for countering voice spam. Since countering voice spam is not a simple technical problem, various approaches should be applied together:

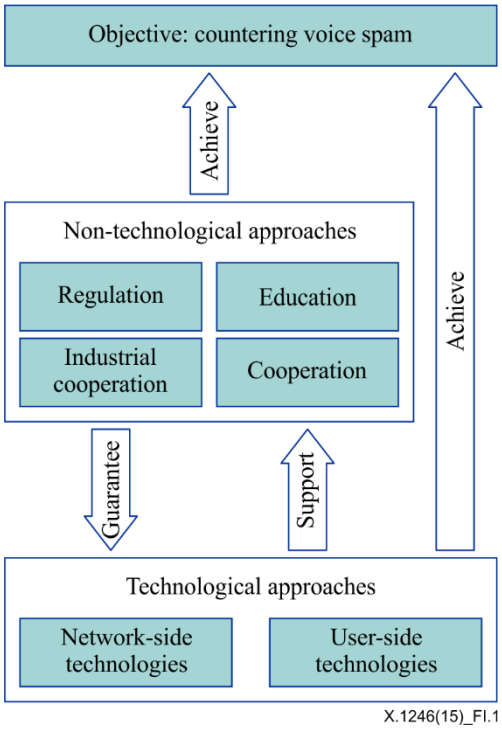

Figure I.1 – Structure for countering voice spam

– Regulations can help protect users and operators from voice spam.

– Industry cooperation is necessary so that various kinds of technologies are appropriate to be developed and installed by industry participants.

– Cooperation can help operators and management entities to share information about effective adoption of the regulations and technology development.

– Education is important for users to minimize economic loss incurred by voice spam.

Appendix II

A suggested solution for interactive verification

(This appendix does not form an integral part of this Recommendation.)

Generally speaking, every interactive verification implies the dialling of a suspicious caller number, the recording of the ring-back tone before being connected and of the voice after the connection and finally the auditing of the content to check whether it is voice spam or not. If all these steps are done manually, this could be tremendously exhausting of the human resources of the operators. Therefore, an optimized approach shall be considered to balance the costs.

The interactive verification can be operated in a centralized way to dial records and audit semi-automatically the voice proofs of the suspicious voice spammers, who may be distributed sparsely and perhaps in every corner of the network.

The centralized approach executes the dialling and the recording job automatically with high concurrency and would allow the auditors to only audit the successful voice proofs without white noise and other useless ring-back tones.

Appendix III

Policy considerations in countering voice spam

(This appendix does not form an integral part of this Recommendation.)

Voice spam is a dangerous tool used to advertise, to commit fraud and to harass, etc., which may occur in daily communications. In order to counter voice spam effectively, different approaches in various aspects of the participating groups should be considered and various types of technologies are introduced in this Recommendation. The participating groups are users (or subscribers), operators, management entities and third-party organizations. This appendix describes several aspects of the participating groups which should be considered in countering voice spam.

III.1 Users

Users are the final victims in the voice spam communication chain and so they have a high level of motivation to block spam. Consequently, users should implement some approaches applied in the whole process of countering spam. Suggested approaches which may vary based on the situation include:

– Users should install anti-spam applications on their own devices, such as on smart mobile phones, if possible. For better effectiveness, the anti-spam application must be up to date.

– Users should send feedback to the telecommunication operators or third-party organizations of all the detailed information of the voice spammer as soon as they receive voice spam.

– Users should be much more conscious in their daily communications and protect personal information from being exposed to spammers.

III.2 Operators

Operators are significant players in the whole procedure of countering voice spam. Since voice spam may severely reduce user satisfaction rates and cause a lot of waste in network resources, operators should be aware of voice spam and implement approaches to protect their networks and provide better services. Such approaches may include:

– Operators should monitor the whole communication network to detect potential voice spam, which may incur abnormal signalling transmissions or traffic patterns.

– Operators should pre-install the latest version of anti-spam applications in all the devices that could be the targets of voice spam through their own distribution or sales channels. For third-party distribution channels, operators should guarantee that all the devices are fully protected by up-to-date applications.

– Operators should provide awareness and training campaigns and encourage users to submit feedback about voice spammers by providing detailed information to third-party organizations; such feedback can be operated through incentive programs.

– Operators should be involved in building alliances with management entities and third-party organizations to consolidate their efforts in countering voice spam.

III.3 Management entities and third-party organizations

Management entities and third-party organizations may supervise or guide operators directly and even provide necessary backup:

– Management entities and third-party organizations may train or provide training and awareness campaigns to users and operators to counter voice spam.

– Management entities and third-party organizations should conduct more research on voice spam trends and should endeavour to find more effective countering approaches or technologies on the latest patterns in voice spam.

– Management entities and third-party organizations should unclog advertisement or promotion channels to normalize the current voice communication environment, or regulate chartered advertisement dialling systems for the promotion entity.

– Management entities and third-party organizations should share the latest blacklists with operators and even with users; this blacklist should be maintained with the support of operators and users.

– Management entities should provide the resources to reinforce the strength for countering voice spam under the protection offered as part of the users' commercial offer benefits.

Bibliography

[b-ITU-T E.370] Recommendation ITU-T E.370 (2001), *Service principles when public circuit-switched international telecommunication networks interwork with IP-based networks*.

[b-ITU-T M.60] Recommendation ITU-T M.60 (1993), *Maintenance terminology and definitions*.

[b-ITU-T M.1400] Recommendation ITU-T M.1400 (2015), *Designations for interconnections among operators' networks*.

[b-ITU-T X.1231] Recommendation ITU-T X.1231 (2008), *Technical strategies for countering spam.*

[b-ITU-T X.1245] Recommendation ITU-T X.1245 (2010), *Framework for countering spam in IP-based multimedia applications*.

[b-ITU-T Y.1001] Recommendation ITU-T Y.1001 (2000), *IP framework – A framework for convergence of telecommunications network and IP network technologies*.

[b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2015