International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

M.3362

(06/2020)

SERIES M: TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Telecommunications management network

Requirements for telecommunication anti-fraud management in the telecommunication management network

Recommendation ITU-T M.3362

ITU-T

ITU International Telecommunication Union

ITU-T M-SERIES RECOMMENDATIONS

TELECOMMUNICATION MANAGEMENT, INCLUDING TMN AND NETWORK MAINTENANCE

Introduction and general principles of maintenance and maintenance organization	M.10–M.299
International transmission systems	M.300–M.559
International telephone circuits	M.560–M.759
Common channel signalling systems	M.760–M.799
International telegraph systems and phototelegraph transmission	M.800–M.899
International leased group and supergroup links	M.900–M.999
International leased circuits	M.1000–M.1099
Mobile telecommunication systems and services	M.1100–M.1199
International public telephone network	M.1200–M.1299
International data transmission systems	M.1300–M.1399
Designations and information exchange	M.1400–M.1999
International transport network	M.2000–M.2999
Telecommunications management network	**M.3000–M.3599**
Integrated services digital networks	M.3600–M.3999
Common channel signalling systems	M.4000–M.4999

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

Recommendation ITU-T M.3362

Requirements for telecommunication anti-fraud management in the telecommunication management network

Summary

Recommendation ITU-T M.3362 describes the requirements for telecommunication anti-fraud management in the telecommunication management network (TMN), the functional framework for combating telecommunication fraud management and the functional description. The requirements for telecommunication anti-fraud management include fraud detection management, fraud monitoring management, fraud mitigation management and fraud information sharing management. This Recommendation also describes telecommunication fraud scenarios including nuisance calls and spoofing calls.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T M.3362	2020-06-05	2	11.1002/1000/14197

Keywords

Telecommunication anti-fraud management, TMN.

* 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 M.3362

Requirements for telecommunication anti-fraud management in the telecommunication management network

1 Scope

This Recommendation describes the requirements for telecommunication anti-fraud management in the telecommunication management network (TMN), the functional framework for combating telecommunication fraud management and the functional description.

NOTE – This Recommendation shall be governed, construed, subject to, and enforced in accordance with the national laws and regulations of the individual Member States of the ITU-T. The obligations, rights, disputes, and remedies of the individual Member States regarding the Recommendation shall be determined in accordance exclusively within their respective national jurisdictions.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 fraud [b-ITU-T Y.140.1]: The act of acquiring pecuniary advantage by misrepresentation or unauthorized action.

NOTE – Fraud is use of numbers in the manner for which they were prescribed, but in a manner intended to generate revenue. It is the use of a number in the manner for which it was allocated but for the purpose of generating cash at the expense of the customer and/or operators. While fraud, in general, relates to Member States' application of legal and policy principles which are within their sovereign rights, in this context the term fraud is associated only with fraudulent activities related to misappropriation and misuse of international numbering resources, which are described in [b-ITU-T E.156 Sup.1].

3.1.2 telecommunication fraud [b-ITU-T Y.140.1]: Fraud which is committed directly against the telecommunication network or its subscribers.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 blacklist: A list of fraudulent numbers which need to be monitored and mitigated.

3.2.2 greylist: A list of suspicious fraudulent numbers which need to be monitored.

3.2.3 nuisance call: Any type of unsolicited or annoying telephone call. May be originated from a telemarketer, robot-caller, prankster or otherwise.

3.2.4 spoofing call: A call with a counterfeit calling party number (CPN) or calling line identity (CLI). May be originated from a rogue web dialler, SS7 hacking or otherwise.

3.2.5 telecommunication anti-fraud management: A whole range of management activities to detect, monitor and mitigate telecommunication fraud.

3.2.6 whitelist: A list of trustworthy numbers based on contract or individual agreement.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

CLI	Calling Line Identity
CPN	Calling Party Number
FDF	Fraud Detection Function
FISF	Fraud Information Sharing Function
FMIF	Fraud Mitigation Function
FMOF	Fraud Monitoring Function
IP	Internet Protocol
OS	Operation System
PABX	Private Automatic Branch exchange
PLMN	Public Land Mobile Network
PSTN	Public Switched Telephone Network
SMS	Short Message Service
SS7	Signalling System no. 7
TAFMF	Telecommunication Anti-Fraud Management Function
TMN	Telecommunication Management Network
VoIP	Voice over IP

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this document is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "can optionally" and "may" indicate an optional requirement which is permissible, without implying any sense of being recommended. These terms are not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Telecommunication fraud scenarios

Telecommunication fraud is a national matter defined differently across jurisdictions. Activity through the means of communication (such as targeted spear-phishing SMSes, spoofing calls or nuisance calls, etc.) may constitute fraud in some jurisdictions if there is revenue generated at the

expense of customers and/or operators (subject to national laws). These fraud activities increasingly impact on telecommunication consumers or called party users.

The misuse of numbers and numbering plans might form the basis by which a fraud is perpetrated, but the misuse itself might not constitute actual fraud. Telecommunication fraud is the use of numbering resources in the manner for which they were prescribed, but in a manner intended to generate fraud revenue. Telecommunication fraud is facilitated by numbering misuse, including global numbering resources, international numbering resources, national numbering resources, local numbering resources, advertisement, short message services (SMSes) and rogue dialling see also [b-ITU-T E.156 Sup.1].

Telecommunication fraudulent calls may in some cases include, but are not limited to, the following features:

– Abandoned calls: The calls always end before they are answered by the called party user, which is commonly known as a "sound" phone, to get the consumer to call back to instigate calls with short stopping, or to confirm that the called party number is live. This kind of call occupies a large amount of network resources, which affects the communication quality of users. To induce the user to dial back, and not to wait for called party answering, they could, for example, provide peer-to-peer or broadcast advertising. Calls to the instigated numbers also incur expensive call charges and exploit settlement dates to receive payment from operators prior to the call origination costs being settled.

– Spoofing calls: Some fraudulent calls use counterfeit calling party numbers. Some of the calling party numbers are entirely or partly counterfeit of the user's real number, such as numbers of banks, operators, police, government departments, relatives, friends and other types of customer misleading numbers. Some of calling party numbers are not in conformity with international or national numbering plan, such as unassigned country code, unassigned national destination code, ultra-long or ultra-short length.

– The high frequency of the same calling number: Some calling numbers have a very high frequency rate of the same calling number. The same calling number in unit time makes a large number of outgoing calls. These numbers are suspicious and are worthy of attention excluding some call centre service numbers.

– Consecutive called party number: Calling party number initiates a call to more than 5 to 10 consecutive called party numbers. It could usually be regarded as nuisance call.

– Very short interval calls: Dialler devices may be used to misappropriate or misuse numbers. The call interval is always very short. Sometimes the calls are made through the relay. It could even generate a large number of concurrent calls.

– The high frequency of the same called number: Some phone numbers are called very frequently due to fraud calls. It influences the experience of these called party users. In these cases, the calling numbers which have received a certain amount of complaints from called party users can be judged as misappropriated or misused.

Fraud can emerge from premium rate services, telephone number misuse and mobile services, see also [b-ITU-T E.156 Sup.1].

Based on the above description, victims of telecommunication fraud include telecommunication customers, called party users, and telecommunication operators. Losses caused by telecommunication fraud are as follows:

– For called party: The loss of resources (time and money) due to advertisement listening, the expensive payment for the premium rate services, the financial loss based on fraudulent information.

– For telecommunication operator: The bills that cannot be settled, and the waste of network resources.

Additional potential telecommunication fraud scenarios are presented in Appendix I.

7 Overview of telecommunication anti-fraud management in the TMN

7.1 Telecommunication anti-fraud management function entity in telecommunication network

The telecommunication anti-fraud management function (TAFMF) entity implements the functions of mitigating fraud based on the data from the operation support system, business support system and customer complaint data, which includes signalling data, network information and user service attributes among others. The different management entities can share the fraud related information. The management entity can also share the fraud related information with anti-fraud related entities such as financial institutions, security administrations, government regulators etc. Figure 7-1 shows telecommunication anti-fraud management function entities in telecommunication networks.

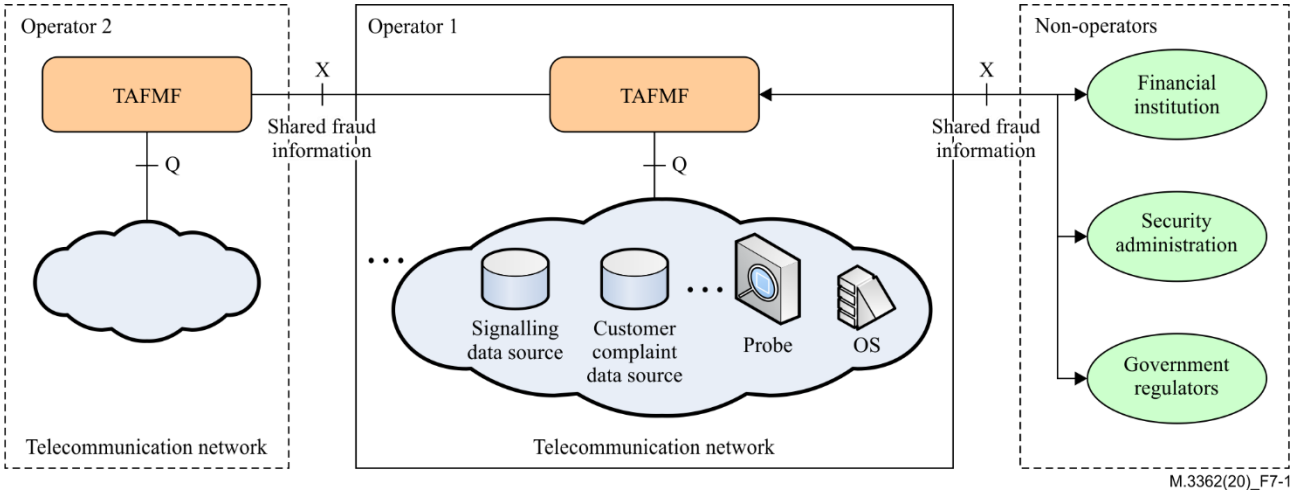

Figure 7-1 –Telecommunication anti-fraud management related entities

7.2 Telecommunication anti-fraud management function requirement

The objectives of the telecommunication anti-fraud management function are to detect different types of fraud preferably in advance, early active fraud call interception, automatic monitoring and alarm, tracing the origin of fraudulent calls, etc.

The telecommunication anti-fraud management function takes full advantage of telecommunication network data to detect the possible fraud in time and to take the appropriate measures to mitigate lost revenue due to fraud.

The telecommunication anti-fraud management functionalities include signalling detecting, data analysis, alarm monitoring, configuration management, sharing fraud information with other entities, etc.

The fraud calls could be detected based on the calling source location, the signalling analysis or the call feature analysis. It is necessary for involved entities to establish and maintain the telecommunication anti-fraud number database including whitelist, blacklist and suspicious number greylist. It needs to share the number information with the other involved entities.

The suspicious calling party number (CPN) in the telecommunication anti-fraud number database should be monitored, identified and confirmed. The numbers identified as fraud callers are added to the blacklist. The CPN in the whitelist should be confirmed. The CPN in the greylist should be continuously monitored.

The suspicious calling party numbers should be dealt with using various precautions, such as, call blocking or information sharing. The CPN in the blacklist should be blocked for some period of time. It is necessary to remind the called party users by voice and short messages about the suspicious CPN. The suspicious number database should be continuously updated.

The purpose of telecommunication anti-fraud management is to manage the number lists or the related information generated in the process of fraud detection and mitigation.

7.3 Functional framework for telecommunication anti-fraud management

The functional framework for telecommunication anti-fraud management that is shown in Figure 7-2 includes the following parts:

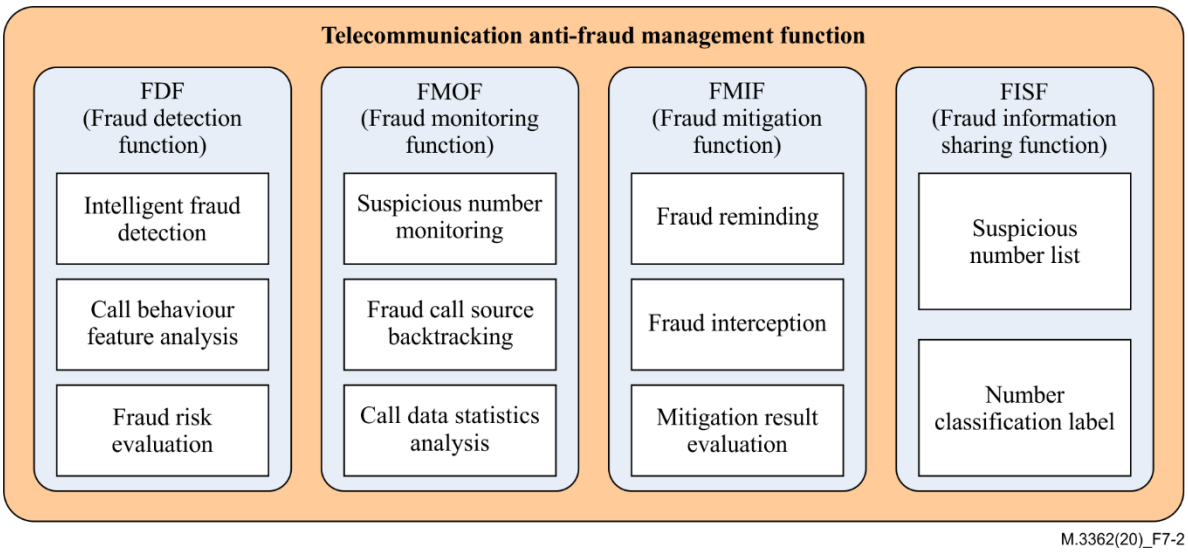

Figure 7-2 – Functional framework for telecommunication anti-fraud management

– Fraud detection function (FDF) module carries out intelligent recognition of signalling, call records, subscriber information, roaming data or routing data to analyse whether or not there are fraudulent call features. It establishes different analysis models for different fraudulent call features. It also analyses and produces statistics on the results of the detections.

– Fraud monitoring function module establishes the number source needed for early fraud detection and fraud activity monitoring. It also performs call source backtracking after the fraudulent calls are detected. It collects the network related information periodically in a way that enables immediate analysis.

– Fraud mitigation function module is responsible for querying, tagging, generating new lists, removing the repetition, and other related management activities of the fraudulent calls that need to be intercepted. It also performs interception configuration based on the list of fraudulent calls, including source interception, calling party interception, called party interception and the other configuration rules. It also analyses and produces statistics of the results of interception implementation.

– Fraud information sharing function module is responsible for sharing the fraud related information with other organizations. The information includes types of fraud as well as suspicious numbers.

This Recommendation focuses on the functional requirements of telecommunication anti-fraud management in telecommunication networks, which includes fraud detection management, fraud monitoring management, fraud mitigation management and fraud information sharing management

which are described in clauses 8 to 11. The management function entities work together to ensure the effective implementation of combating the telecommunication fraud.

8 Fraud detection management

The fraud detection capability module collects the network related information in near real time in a way that enables immediate analysis. The network related information includes signalling data, calling party roaming information, calling party user registration information, call charging detail record, call record statistical data, etc. It classifies the suspicious fraud behaviours and evaluates the level of fraud call risk.

Detection of telecommunication fraud calls provides functions to detect telecommunication fraud calls based on the call features such as the abnormal calling party number, the call with malicious behaviour, or false imitation call, among others.

The goals of fraud detection management include the need to:

– Collect the related information from the telecommunication network.

– Aggregate the multiple sources data to enable the analysis of relationships among users' attributes to detect fraud activities or misuse of ITU-T E.164 number resources.

– Define and maintain the fraud call behaviour features.

– Define the level of fraud call risk.

Fraud detection management requirements include the following function set groups:

– Intelligent fraud detection management function set.

– Fraud call behaviour feature set management function set.

– Fraud call risk evaluation management function set.

8.1 Management function set of intelligent fraud detection

Intelligent fraud detection management provides functions for the implementation and support of fraud detection as follows:

– The function set supports detection of different types of fraud call with different methods such as big data analysis, modelling, inference, etc. The fraud detection method is based on the data related to user service features including the calling party roaming location, group behaviour of the calling party, call behaviour features such as the abnormal calling party number, the continuous calling of the called party number, the very short interval calls, etc.

– The function set supports detection of the abnormal calling party number based on calling party roaming location and analysing whether the calling party number is in the correct format. If the calling party number fakes the user's real number, it should be detected that it has a different incoming source from the normal number. If the calling party number is not in conformity with the international or national numbering plan, it should be detected that the suspicious number has an unassigned country code, unassigned national destination code, and is ultra-long or ultra-short length. Services related to customer complaints about the abnormal calling party number could be supported as a major way to extend the pool of the abnormal calling party number. The pool of abnormal calling party number should be shared among the different operators.

– The function set supports detection of the high frequency of the same calling party number based on counting of the frequency of calls initiated by the calling party. If the frequency of calls initiated by the same calling party exceeds a specific value (e.g., 300 times per hour), it may be a fraudulent call.

– The function set supports detection of the consecutive called party numbers which are called by the same calling party based on counting the consecutive called parties. If the

total of consecutive called party numbers exceeds a specific value (e.g., 10 consecutive called party numbers called by the same calling party), it may be a fraudulent call.

– The function set supports detection of very short interval calls based on detecting of the interval between the calls. If the interval is very short, even the calls initiated at the same time, it may be a fraudulent call.

8.2 Management function set of fraud call behaviour features analysis

Fraud call behaviour features management provides functions to define the fraud call behaviour feature set as follows:

– The function set supports definition of the fraud call behaviour feature based on the call related information such as the calling party roaming location, call time and call duration, the frequency and call completion rate of the same calling party number, the amount and discreteness of called party number, the category and region of called party, etc.

– The function set supports to classification of the fraud call based on the fraud call behaviour feature. The fraud call includes the nuisance call, spoofing call, advertising call, etc.

8.3 Management function set of fraud call risk evaluation

Fraud call risk evaluation management function set provides functions to manage the risk classification rules as follows:

– The function set supports definition of the description of the different risk levels of fraud call. The risk levels could be defined from low level to high level. It is set based on the sphere of influence of the fraud call, the extent of harmful effect, call frequency per unit time, etc.

– The function set supports mapping of the different type of nuisance call or spoofing call, and of the different fraud call behaviour features into the different specific risk levels.

– The function set supports adjusting of the fraud call risk level of the specific calling party number based on its actual call behaviour.

9 Fraud monitoring management

In order to detect fraud calls in time, the fraud monitoring capability module needs to routinely monitor the call behaviour of the suspicious calling party numbers in the blacklist or greylist. It is responsible for backtracking the call source of the suspicious calling party numbers. It is also responsible for generating statistics and analysing the suspicious calling party numbers in the blacklist or greylist, and the calls initiated by them.

The goals of fraud monitoring management include:

– Maintaining the blacklist or greylist based on the monitored call behaviour of the suspicious calling party number.

– Generating statistics on the amount of fraud calls and analysing the distribution of suspicious calling numbers and the direction of fraud call.

Fraud monitoring management requirements include the following function set groups:

– Suspicious number monitoring management function set.

– Fraud call source backtracking management function set.

– Call data statistics analysis management function set.

9.1 Management function set of suspicious number monitoring

Suspicious number monitoring management function set provides functions to monitor the call behaviour of the suspicious calling party number as follows:

– The function set supports updating of the blacklist or greylist based on the call behaviour of the suspicious calling party number. If there is no abnormal behaviour on the call initiated by the calling party within a certain period of time, the suspicious number in the greylist should be deleted. If the call is verified as a fraud call, the suspicious number in the greylist should be moved to blacklist.
– The function set supports monitoring of the misuse of ITU-T E.164 number.
– The function set supports monitoring of the sudden increases in traffic.
– The function set supports monitoring of the subscriber call records to detect unauthorized calls.
– The function set supports detection of different hazard levels of the fraud calls. The fraud call list could be dynamically updated, queried or ranked.
– The function set supports various monitoring dimensions including the over threshold warning, fraud rising trend reminder, no more call initiated by the intercepted calling party number reminder, etc.

9.2 Management function set of fraud call source backtracking

Fraud call source backtracking management function set provides functions to backtrack the fraud call source as follows:

– The function set supports backtracking of the fraud call source including fraud call initiated location, the distribution and call direction information including the international gateway switch of international calls, the interconnection gateway switch of calls between networks, the trunk gateway switch of local calls, etc.
– The function set supports storage of the call records of the suspicious calling party number in the greylist for a period of time. These call records are the reference information for fraud mitigation. If there are no more calls initiated by this calling party number for some time, it could be deleted from the greylist.

9.3 Management function set of call data statistics analysis

Call data statistics analysis management function set provides functions to generate statistics on the fraud calls as follows:

– The function set supports generation of statistics on the amount of different types of fraud calls, detection timeliness rate, etc.
– The function set supports analysis of the regional distribution area of the suspicious fraud calls that are initiated.
– The function set supports analysis of the direction of fraud calls and the regional distribution area of the victims.

10 Fraud mitigation management

Fraud mitigation module mitigates the possible fraud calls. The mitigation methods include intercepting the fraud calls, reminding the called party user of the potential problems to prevent the fraud behaviour, etc.

The goals of fraud mitigation management include:

– Maintaining the blacklist or greylist based on the mitigation result after the fraud calls are intercepted and the called party users are reminded.

– Managing the fraudulent call lists that need to be intercepted, including querying, tagging, generating new lists, removing the repetition, etc. It should be able to tag the unprocessed numbers, the numbers in monitoring, the numbers not in monitoring, the numbers in the interception, the numbers not in the interception, whitelist, etc. It should be able to query the numbers of different areas and states.
– Evaluating the effect of fraud mitigation.

Fraud mitigation management requirements include the following function set groups:

– Fraud reminding management function set
– Fraud interception management function set
– Mitigation result evaluation management function set

10.1 Management function set of fraud reminding

Fraud reminding management function set provides functions to remind the victim of fraud calls as follows:

– The function set supports notifying of the victim of fraud calls in various ways, such as short messages, flash SMS, telephone call, etc. The purpose of the reminder is to alert and to prevent loss to victims in terms of time and resources.

10.2 Management function set of fraud interception

Fraud interception management function set provides functions to intercept the fraud calls as follows:

– The function set supports gaining access to information about the suspicious fraud calls that need to be mitigated and to obtain information to maintain the fraud mitigation list. The fraud mitigation list with the mitigation processing state could be queried, updated, removed and tagged. The fraud mitigation list could be queried by areas, call sources, etc.
– The function set supports configuring of the equipment in the network to intercept the suspicious fraud call based on the call features. It should configure the capacity of equipment to intercept the call source, calling party, called party, etc. It should be able to implement the regionalized interception and global interception.
– The function set supports storing of the fraud calling party number in the blacklist for a period of time. If there are no more calls initiated by this calling party number for some time, it could be deleted from the blacklist. It could release the network resource for fraud interception.
– The function set supports reallocating of the number in the blacklist after a period of time.
– The function set supports moving of the calling party numbers from the greylist to blacklist when the calls initiated by suspicious calling party numbers are intercepted.

10.3 Management function set of mitigation result evaluation

Mitigation result evaluation management function set provides functions to evaluate the mitigation result as follows:

– The function set supports generating of statistics on call interception timeliness rate, success rate of interception, the distribution of intercepting implementation, etc.
– The function set supports accessing of the evaluation summary of the fraud mitigation result. It includes the evaluation of effect after fraud mitigation (i.e., interception success rate, etc.).

11 Fraud information sharing management

In order to effectively implement fraud call mitigation, the fraud related information needs to be shared among the different operators or with other organizations, including financial institutions, security administrations, government regulators, etc.

The goals of fraud information sharing management include:

– Management of the shared fraud related information including suspicious number list, number classification labels, etc.

Fraud information sharing management requirements include the following function set groups:

– Suspicious number list management function set

– Number classification label management function set

11.1 Management function set of suspicious number list

Suspicious number list management function set provides functions to share the suspicious number list as follows:

– The function set supports sharing of the numbers in the whitelist, greylist or blacklist among the different systems of the network operator.

– The function set supports sharing of the suspicious number in the blacklist or greylist and number classification with financial institutions, security administrations, government regulators, etc.

11.2 Management function set of number classification label

Number classification label management function set provides functions to share number classification label as follows:

– The function set supports sharing of the number classification label among the different systems of the network operator. The number classification labels identify blacklist numbers or greylist numbers, nuisance calls or spoofing call type, call update time, etc.

Appendix I

Potential telecommunication fraud scenarios

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

The advancement of technological tools such as computers, the Internet, and cellular phones has made life easier and more convenient for most people in our society. However, some individuals and groups have subverted these telecommunication devices into tools to defraud numerous unsuspecting victims. It is not uncommon for a scam to originate in a city, country, state, or even a country different from that in which the victim resides.

Telecommunication fraud calls include, but are not limited to, the following scenarios.

I.1 Nuisance calls

Nuisance calls and messages come in a variety of different shapes and sizes and can be inconvenient and annoying to the users. The following are scenarios of nuisance calls:

– Abandoned calls: The calls always end before they are answered by the called party.

– Consecutive called party number: Calling party number initiates call to more than 5 to 10 consecutive called party numbers.

– Unsolicited telesales calls

– Recorded marketing message calls: A recorded marketing message being played when the users answered the phone.

– Unsolicited marketing faxes: A marketing fax sent to users personal/business fax machine.

– Unsolicited marketing texts: Users received a text marketing a particular product or service.

– Abusive and threatening calls: Malicious, abusive or threatening calls, whether from people who you know or from strangers, which are a criminal offence.

The nuisance calls always have malicious purposes, such as voice mail hacking, robot calling, phishing or uncivil practices known as false report of an incident to emergency services.

The communications providers should be able to stop nuisance calls getting through to consumers in the first place. The communications providers block problem calls at source based on evidence of fraud. It also enables the telephone number of the person making the call to be displayed to the person receiving the call. This helps the call recipient to make a more informed decision about whether to accept the call or not, and to report problem calls to regulators and law enforcement agencies more effectively.

I.2 Spoofing calls

Many phone handsets can now display the calling party number before the called party user answers. This feature – known as 'caller ID' or 'calling line identity' (CLI) – is a handy way of screening the calls that the individual wants to answer from the ones that they do not want to answer. Nuisance callers and criminals deliberately changing the caller ID, are a practice known as 'spoofing calls'.

Sometimes there is a good reason for a caller to modify the caller ID to leave an 0800 number for called party users to call back if they want.

However, with spoofing callers deliberately change the telephone number and/or name relayed as the caller ID information. They do this to either hide their identity or to try to mimic the number of a real company or person who has nothing to do with the real caller. For example, identity thieves

who want to steal sensitive information such as users' bank account or login details, sometimes use spoofing to pretend that they are calling from the users' bank or credit card company.

Calls with spoofed numbers come from all over the world and account for a significant and growing proportion of nuisance calls. Voice over IP (VoIP) technology - the type of technology used to make Internet calls - is often used in spoofing. 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 numbering resources. It is especially malicious for operators because they have no way of preventing these spoofing calls with their numbers and they only ever learn of them from other operators or the recipients.

In the current network environment, more and more untrustworthy devices are present (including the private automatic branch exchange (PABX), call centre and VoIP access system) that interconnect to a public land mobile network/public switched telephone network (PLMN/PSTN). As a result, a large number of phone numbers are leased to anonymous call providers who help fuel phone spam. Noticeably, caller 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 scam and spoofing calls are insufficient from a user's standpoint. It is difficult to validate the spoofing calls.

Bibliography

[b-ITU-T E.156 Sup.1] Recommendation ITU-T E.156 – Supplement 1 (2007), *Guidelines for ITU-T action on reported misuse of E.164 number resources. Supplement 1: Best practice guide on countering misuse of E.164 number resources.*

[b-ITU-T E.164] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

[b-ITU-T Y.140.1] Recommendation ITU-T Y.140.1 (2004), *Guideline for attributes and requirements for interconnection between public telecommunication network operators and service providers involved in provision of telecommunication services.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020