International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 33

(09/2018)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1231 – Supplement on technical framework for countering telephone service scams

ITU-T X-series Recommendations – Supplement 33

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 (1)	
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 (1)	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 (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
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.

Supplement 33 to ITU-T X-series Recommendations

ITU-T X.1231 – Supplement on technical framework for countering telephone service scams

Summary

This Supplement provides a technical framework and related best practices for countering telephone service scams. In the framework, entity functions and processing procedures are specified. The best practices cover those found to be the most effective in stopping known telephone service scam methods. In addition, this Supplement specifies the characteristics and sources of telephone service scams and categorizes their main methods and relevant technical requirements according to the key technologies of telephone service scam discovery, judgement and disposition.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 33	2018-09-07	17	11.1002/1000/13731

Keywords

Countering telephone service scam, security framework.

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

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. 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

Supplement 33 to Recommendation ITU-T X.1231

ITU-T X.1231 – Supplement on technical framework for countering telephone service scams

1 Scope

This Supplement provides a technical framework and related best practices for countering telephone service scams. In the framework, entity functions and processing procedures are specified. The best practices cover those found to be the most effective in stopping known telephone service scam methods. In addition, this Supplement specifies the characteristics and sources of telephone service scams and categorizes their main methods and relevant technical requirements according to the key technologies of telephone service scam discovery, judgement and disposition.

2 References

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

[ITU-T X-Sup.28] ITU-T X-series Recommendations – Supplement 28 (2016), *ITU-T X.1245 – Technical measures and mechanisms on countering spoofed calls in the terminating network of voice over long term evolution.*

[3GPP TR 33.832] 3GPP TR 33.832 (2015), *Study on IMS Enhanced Spoofed Call Prevention and Detection.*

[IETF RFC 3325] IETF RFC 3325 (2002), *Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks.*

[IETF RFC 7340] IETF RFC 7340 (2014), *Secure Telephone Identity Problem Statement and Requirements.*

[IETF RFC 7375] IETF RFC 7375 (2014), *Secure Telephone Identity Threat Model*.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 scammer: This is a person that makes use of a telephone service network to implement fraud while concealing themselves.

3.2.2 telephone service scam: This is a type of fraud that makes use of the telephone service network which is owned and operated by a telephone service operator.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

BICC Bearer-Independent Call Control protocol

ISDN Integrated Services Digital Network

ISUP ISDN User Part

SIP Session Initiation Protocol

5 Conventions

None.

6 Overview of telephone service scam

The development and application of network technologies are not only bringing convenience to users, but also requiring users to submit their identification information. For example: when using online shopping, users are typically required to provide personal information such as their name, address, contact information, etc.; when using online banking services, users need to provide their personal identification, bank account and other information; while using mobile applications, personal identification, location and other information might be required. If any of this information is disclosed, scammers may take advantage of it to commit deceptive acts.

Scammers may also use loopholes within network technologies, such as faking a caller's phone number in order to pretend to be, for example, customer services of a bank or an airline company, to gain the user's trust.

Through telephone calls, scammers mask themselves using various false identities in an attempt to deceive users for the purpose of stealing their money. For example, scammers may collect users' personal information through Internet searches or other methods, and then, while pretending to be a tax officer or bank clerk, convey a deceptive story to the user in an attempt to steal their money.

These types of telephone service scams cause disturbances to customers' daily lives and produce many negative side effects.

6.1 Categories of telephone service scam characteristics

As compared with traditional scamming methods, telephone scam methods provide certain significant advantages to the scammers. Examples include:

– by calling random phone numbers or number lists of target victims, the cost of perpetrating telephone scams is decreased and their time efficiency is greatly improved;

– as a result of victims not being able to meet scammers in person, it is much easier for scammers to disguise their true identity; they do not require proper or relevant uniforms, ID cards, or other relevant props in order to be convincing;

– by making use of the management loopholes of telephone service providers, scammers may be able to conceal themselves from investigation;

– by making use of bank account and transfer services, scammers can coerce victims into transferring money to a specified account, enabling the scammers to extract the stolen cash remotely from any automatic teller machine (ATM).

6.2 Typical scamming scenarios

The following examples are some typical scenarios that have been used by scammers. They are introduced here to demonstrate the typical crimes that have been committed, but in real life cases, the methods could be more complicated.

6.2.1 Impersonation of government or public security officer

Scammers pretend to be officers of a police department, law court, national security department, etc., claiming that the victim is involved in a criminal case. If victims panic and insist on proving their innocence, the scammers will ask them to transfer money to a specified "secure" bank account "temporarily" to make sure the "criminals" are unable to make use of the money to commit the

"crime". After the scammers have been assured that the money was received in their account, they cut off communications and refuse further contact with the victims.

6.2.2 Impersonation of bank employee

Scammers call victims pretending to be clerks of a bank, telling them that, according to the records of the bank, an "unusual transaction" has occurred using the victim's credit card. When the victim gets confused and worried about arrears fines, the scammers ask the victims to transfer money to a specified bank account to avoid interests or fines. The scammers claim that they are going to investigate the transaction, and after making sure there is no problem, the victim's money will be returned.

On some occasions, victims refuse or are unable to transfer money; in these cases scammers may alter their methods. They may then ask victims for their card number, password or other verification codes so that they can log in to their bank account through the Internet; the scammer then finishes the money transfer themselves.

6.2.3 Lottery awards

Scammers call victims pretending to be an employee of a lottery company and claiming that the victim's phone number was selected randomly as the winner of a large sum of money (or an automobile, laptop, smartphone, etc.). When victims are anxious to receive their "award", the scammers ask them to pay money ostensibly to cover taxes, fees, etc.

In cases such as these, scammers are taking advantage of people's fear, greed, ignorance or other psychologies in order to induce them into a trap. After the victims realize that they have been deceived, they typically cannot provide any useful information to investigators, other than a phone number. If telephone service providers do not have records of the scammers' personal identification, refuse to provide it to the investigators or when the scammers' phone numbers are forged, it is nearly impossible for the victims to recover their stolen money. And even in cases where it is possible to identify the scammers, it is often very difficult to collect the necessary evidence to punish these criminals.

7 Characteristics analysis

When taking advantage of communication networks scammers generally attempt to achieve two main objectives:

1) Make a high number of phone calls (number of calls per unit time) in order to reach as many users as possible. According to the research and experience of the scammers, during each phone call, the possibility that they could get the called user's trust and money is basically a fixed number. Thus, the more phone calls they can make, the more victims they can encounter.
2) Conceal their real identity as well as possible. After scammers successfully commit the scam and get the victims' money, they need to prevent the police or investigators from finding them. Therefore, the phone calls placed by scammers often are marked by specific characteristics, such as, having no registered name attached to the calling number, having no calling number displayed to the called users, using an apparent forgery in the displayed calling number, etc.

7.1 Time-related characteristics of calling

7.1.1 Calling frequency

Commonly, scammers tend to make calling frequency as high as possible, for the reasons described in clause 7 above. Thus, the phone number calling frequency of scammers would tend to be higher than that of legitimate users.

7.1.2 Called number dispersion

When researching dispersion of called phone numbers, there is another concept involved called "first call", where "first call" means one user is calling another phone number for the first time without any previous call record. Dispersion of called numbers refers to the proportion of "first call" calls among all of the user's call records.

Since most numbers called by legitimate users are to their relatives, colleagues, friends, clients, etc., with whom they have actual existing relationships, the calling records among these numbers occur repeatedly in a specified time range; thus, the occurrence of "first calls" should be low. This also leads to a low dispersion of called numbers. However, scammers need to call a large number of random phone numbers over a short time; the "first call" in these calling records should stand out as a much higher proportion than that for legitimate users; that is, for scammers, the dispersion of called numbers is much higher than the average value for legitimate users.

Scammers may sometimes contact the same called user multiple times. This may involve the following major possible conditions:

– Scammers are using phone numbers to make phone calls that are not directly related to the scams.

– Scammers are repeatedly calling numbers on purpose, possibly to avoid being discovered by anti-scam systems.

– Scammers call the same users more than once because they have already gained the trust of these users and have started the process of deceiving them of their money.

7.1.3 Average talk time

When receiving calls from scammers, most users would recognize the scam and actively terminate the call, while only a few people may get trapped in the scam and continue the conversations. Thus, most of the scammers' calls may be terminated in a few seconds and their average talk time should be much lower than that of legitimate users.

7.1.4 Long-distance calling rate

Most legitimate users incorporate telephone calls in their daily life or work; this implies that most calls legitimate users make are to phone numbers in the same area. Scammers, on the other hand, are searching for victims on a nationwide or global scale; this implies that they should be making more long-distance calls than most legitimate users do.

7.2 Characteristics of the calling numbers

7.2.1 Special public numbers

To gain the trust of called users, many scammers fake their calling numbers to some well-known public numbers. For example, when impersonating police officers, scammers may change the calling number to 911 or other numbers used by local police departments; when impersonating bank clerks, they use the banks' customer service numbers which are published in advertisements. However, on most occasions, these numbers are not used for contacting customers actively; they are only used to receive the customers' calls. Thus, when investigations find calls originating from these numbers, it is highly possible that the calling party is a scammer.

7.2.2 No displayed calling number

To conceal their real identity and to avoid blocking methods applied by telephone service operators, or to impeded investigators, scammers may use special technical methods to conceal their calling number. As a consequence, the called users are unable to see the calling numbers, limiting their ability to report the scam or provide relevant evidence.

7.2.3 Abnormal signalling

When scammers are making telephone calls, they may use abnormal signalling to conceal their positions; when this kind of signalling occurs, it is highly possible that the caller is engaged in illegal activity. Below are several typical examples:

– Abnormal international code: When a phone call is entering the U.S.A through the international gateway, but its country code is claimed to be "+1" and the caller's number is a landline telephone, this call would be very suspicious. Normally, these conditions mean the caller is making a domestic call and it should not reach the international gateway. When the international gateway finds an entering call holding a domestic country code, it should be determined that the caller is using unusual routing methods for abnormal reasons.

– Abnormal operator code: An inter-operator gateway (e.g., a gateway between operator A and B) is receiving a call coming from operator A requiring to enter the network of operator B, but the signalling is holding the operator code of operator B and implies it to be a landline telephone. For the similar reason of the example above, this call is very suspicious.

– Incorrect telephone number length: The length of telephone numbers in a specific area should be fixed, but when a calling number's length is different from the length defined by its local operator, according to the area code held in the signalling, it is possible that the caller is faking the calling number.

7.3 Calling mode characteristics

7.3.1 Keyboard usage during calls

On most occasions, telephones' keyboards are used when users are calling numbers used for customer services or similar purposes. On these occasions, only the calling party would use the keyboard; the called party would not. However, some scammers, in an attempt to decrease their personnel cost when calling massive number lists, play a pre-recorded sound file when the called user answers the call which requests the called user to press a specific number. Thus, if the called user recognizes the scam, they should hang up immediately without pressing the requested number (keypad button) so that the scammers do not have an opportunity to talk to them.

With the discovery of this phenomenon, the called parties' usage of keyboards could be an important characteristic to determine telephone service scams. Though there might be some legitimate scenarios that may require the called party to use the keyboard, the system could involve whitelists or other similar mechanisms to avoid false alarms.

7.3.2 Pre-recorded sound files

As mentioned above, some scammers may use pre-recorded sound files to lower their personnel cost. Thus, when a suspicious number is calling, it would be efficient to record the starting few seconds of the call and compare the sound with captured sound samples to determine if it is a scam.

7.3.3 Combination with other communication methods

On many occasions, scammers do not use a telephone as their communication method. They may also involve instant messaging software, mobile communication applications, short messages, etc. Hence, if there are communications actions detected between the calling party and the called party before or after the call, the suspicion level may increase.

Countering telephone service scams is a complicated system engineering problem; it is unreasonable to determine scams with only a single characteristic. Determining by multiple characteristics could increase accuracy and decrease disturbances to legitimate users. Furthermore, combining user reports, whitelists and other mechanisms could make the entire system more efficient and reasonable. However, when applying these characteristics in practice, the determination thresholds of these characteristics should be able to be set according to local needs.

However, with the promotion of telephone service scam countering technologies, scammers may also alter their methods and techniques for committing these crimes. Thus, the characteristics used in telephone service scam recognition and technologies of blocking should also be updated over time.

8 Key technologies of the telephone service scam

8.1 Discovery

Currently, the most reliable method of telephone service scam discovery is a combination of various characteristics, especially those described above. Considering that every country or area may have unique situations or demands on this problem, the combination of characteristics selected may be significantly different. In addition, with the development of technology, scammers may also develop and apply new methods to implement these crimes. Thus, new characteristics may also need to be involved to adapt to new situations.

Considering that operators in most countries may not have permission for accessing the vocal contents of users' calls, it is difficult to assure that every judgement is absolutely correct. Thus, results may be classified into several levels, for example, "normal", "suspicious", and "confirmed" or others as may be dictated.

8.2 Judgement

After suspicious numbers are parted from definite legitimate users, it is important to make precise judgements to decrease the possibility of false alarms. Currently, the most accurate methods of making precise judgements involve manual determinations. Below are several examples that could be implemented into the judging progress.

8.2.1 Blacklist from administrative departments

Commonly, administrative departments or public security departments may have access to informational reports of scamming cases provided by deceived users. Obtaining numbers from these reports and adding them into blacklists which block them from continuing to call people could be an effective method.

8.2.2 Calling back

Telephone service operators could try to call suspicious telephone numbers and record the response to help make precise judgements. Quite often, the telephone numbers used by scammers do not accept incoming calls; when users try to call back, they may get a busy response, no answering, etc. If the suspicious number could not make normal conversations in a predetermined time interval, it could be determined as possibly being a number used by a scammer.

8.2.3 Reports made by users

Telephone service operators could cooperate with network-security-related companies to gather scamming phone numbers. These companies have developed scam reporting applications with which users can report scamming numbers conveniently and quickly. This information could be highly useful to operators.

8.3 Disposition

8.3.1 Methods of disposition

– blocking telephone calls of confirmed calling numbers;

– sending alert message to the called users;

– standardize abnormal signalling calls (e.g., constraint displaying calling number).

8.3.2 Strategies of disposition

– Apply different disposition methods according to the degree of suspicion (e.g., applying a grey list method together with a blacklist and whitelist).

– Localized blacklist and whitelist according to local situations.

– Personalize strategies configured by called users.

With the combination of multiple methods and strategies, the accuracy and flexibility could be increased greatly, and the disposition progress could be made friendlier to users.

9 Structure of countering telephone service scam functions

9.1 General structure

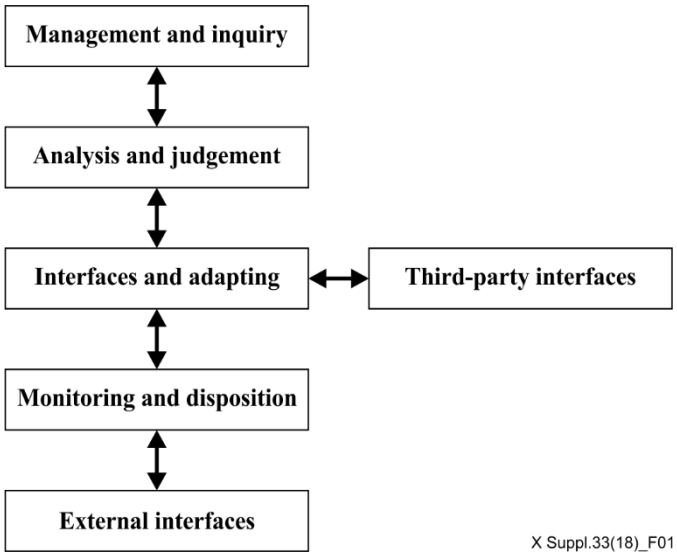

Figure 1 – General structure of countering telephone service scam functions

As the general structure of countering telephone service scam functions shown in Figure 1, there are five basic layers in the structure. These layers are sets of relevant functions and are all taking respective responsibilities to fulfil the function of the entire system.

As shown in Figure 1, in addition to the five layers, an extra layer (on the right side) enables third-party interfaces. The usage of this additional layer is optional and should be determined according to actual situations.

9.2 Functions of components

9.2.1 Management and inquiry

The management and inquiry layer is in charge of interacting with users, who, on most occasions, are the relevant personnel of the telephone service operators.

The management functions in this layer contain the configuration and management of blacklists, whitelists, local policies etc. The inquiry functions provide users with inquiry abilities like calling records of subscribers, suspicious numbers, disposition records, etc. In addition, the management and operating functions of the system itself are also contained in this layer.

9.2.2 Analysis and judgement

The analysis and judgement layer is in charge of making decisions. It contains three major modules: libraries, databases and processing. The library module consists of the libraries for action models,

telephone number characteristics, abnormal calling samples, etc. The database is the storage of subscribers' call records and other useful information as the basis for analyses. Note that call records are necessary information to the operators and are not a violation of personal privacy. The third module, processing, gains information and data from the other two modules and realizes the analysis and judging functions.

As for the method of processing, there are multiple choices available; each operator could choose the methods to use according to relevant situations. Optional technologies could also include big data analysis, artificial intelligence, etc.

9.2.3 Interfaces and adapting

The interfaces and adapting module realizes the connection between the analysis and judgement module and the monitoring and disposition module. It receives the policies designed by the disposition function or commands given by users. In addition, this layer also collects monitoring information from the monitoring and disposition layer, including calling records, usage of users' keyboards, evidence collected, etc.

9.2.4 Monitoring and disposition

The monitoring and disposition layer monitors all the calls going by the system, collects necessary information and implements required processes. The collected data and evidence are transferred to the analysis function, and the processing function implements given actions according to the commands. These could include actions such as cutting off the call, playing an alarm voice record, etc.

9.2.5 External interfaces

The external interfaces layer connects with session initiation protocol (SIP) and bearer-independent call control (BICC)/integrated services digital network user part (ISUP), and transfers the users' call signals to the system for analysis and processing.

9.2.6 Third-party interfaces

The third-party interfaces layer is an optional layer cooperating with the interfaces and adapting layer. It provides additional functions or information to the system, such as third-party marking information, blacklists given by administrative departments, small message system (SMS) gateways, calling back platforms, etc. These functions are not necessarily required but are capable of increasing system effectiveness and accuracy.

9.3 Reference model

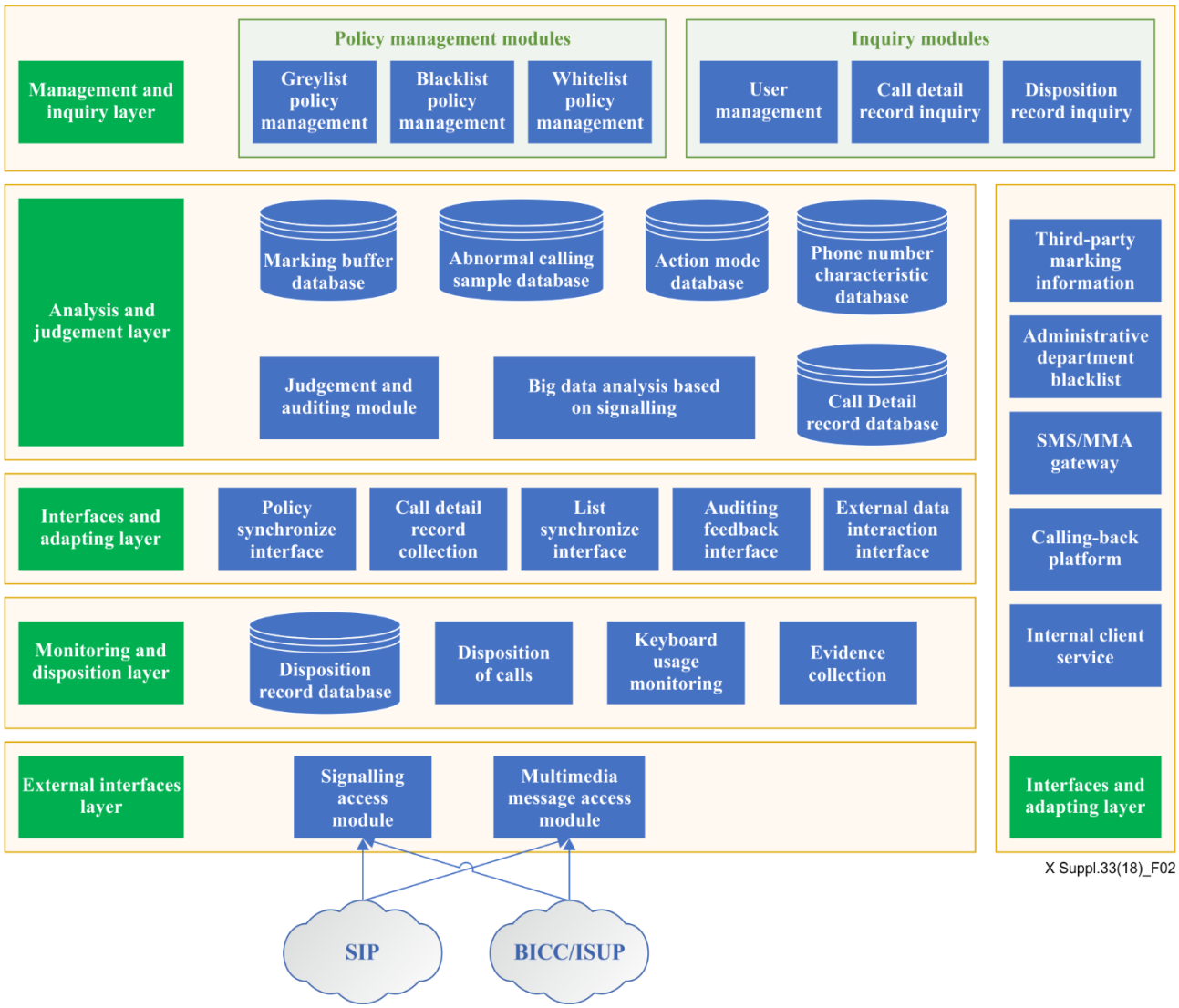

Figure 2 – System function structure diagram of a reference model

Figure 2 shows the system function structure diagram of a reference model, in which, each layer has been demonstrated with more details. Note that, in this reference model, the analysis and judgement layer is making use of big data analysis technology, but it is optional to use other technologies or the combination of multiple technologies.

10 Countering processing

It is significant to determine if a calling number is being used by the scammers as accurately as possible. Figure 3 illustrates the basic progress of judgement processing.

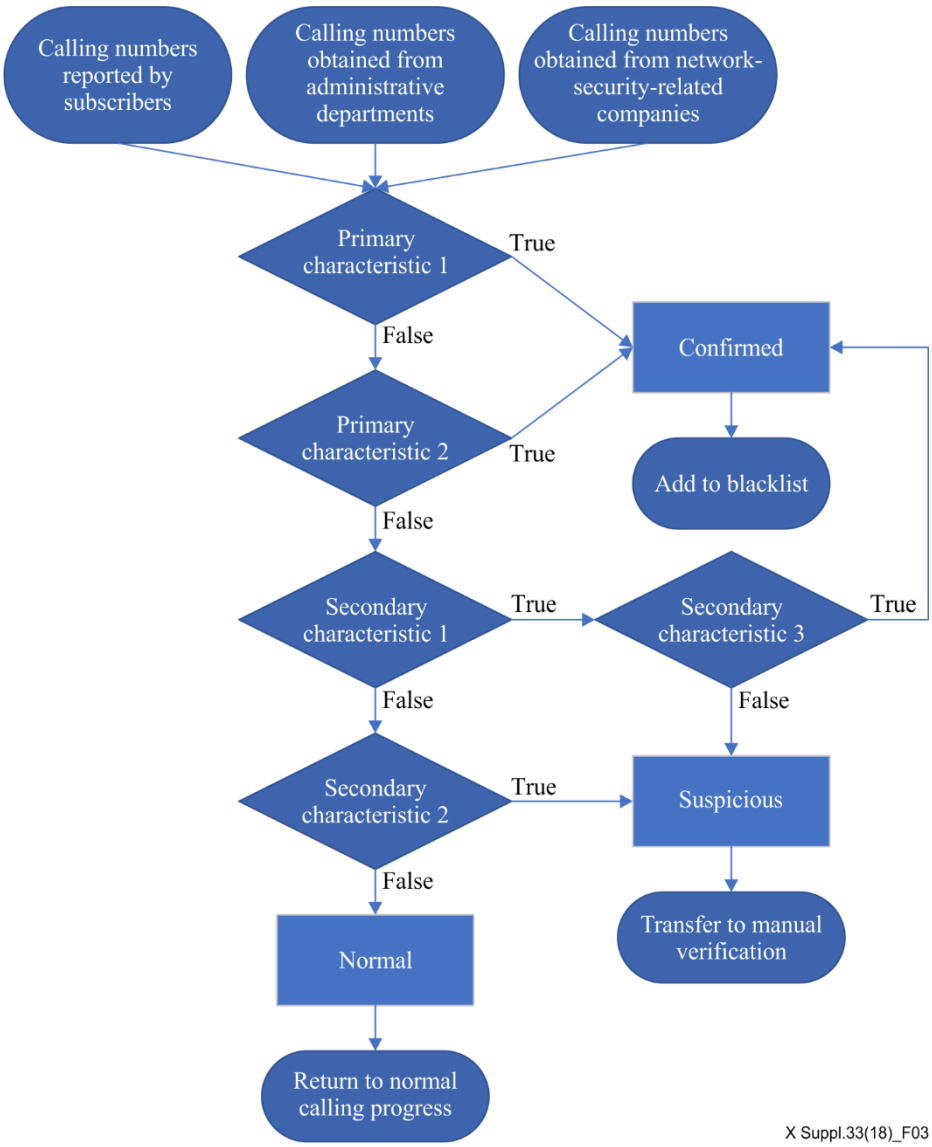

Figure 3 – Basic judgement progress of calling numbers

According to the characteristics discussed above, each operator could select a different set of characteristics for the judgement progress and decide on more complex conditions for more accurate results. In addition, except for the characteristics discussed above, the blacklist and whitelist mechanism could also be invoked to make faster decisions.

In Figure 3, there are two types of characteristics used; these are primary and secondary characteristics:

1) Primary characteristic: These are characteristics that are considered to be impossible to return "true" in normal calling occasions.

2) Secondary characteristic: These are characteristics that are possible to return "true" in normal calling occasions, but still may be caused by scamming actions. These characteristics may need to be combined with other characteristics for more accurate results.

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, 2019