INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

SG17-C 0045

STUDY GROUP 17

Original: English

Question(s): 5/17 Geneva, 22 March 2017

CONTRIBUTION

Source:	China Unicom	
Title:	Proposal for X.ctss: add new content	
Purpose:	Proposal	
Contact:	Junjie Xia China Unicom P.R.China	Tel:+86 10-68799999-7203 Email:xiajj2@chinaunicom.cn
Contact:	Feng Gao China Unicom P.R.China	Tel: +86 10-68799999-7243 Email:gaofeng149@chinaunicom.cn
Contact:	Nan Jiang China Unicom P.R.China	Tel: +86 10-68799999-7237 Email: jiangn17@chinaunicom.cn

Keywords: Countering telephone service, technical framework

Abstract: This contribution is based on the TD 2926 Rev.1. It adds new contents and makes substantial improvements based on the discussion at the SG17 meeting in August 2016.

In this contribution, we make some revises as below.

1) add in overview of telephone service scam in clause 6;

2) propose characteristics analysis in clause 7;

3) to keep the titles consistent, change the title “telephone fraud” to “telephone service scam” of clause 6, 8, 9.

Dratf Supplement to ITU-T X.1231

X.ctss: Technical Framework for Countering Telephone Service Scam

1. Scope

This Supplement provides an overall technical framework for countering telephone service scam and related useful practices. In the framework, entity functions and processing procedures are specified. In addition, the useful practices provided in this Supplement covers most of the practices that are able to stop known telephone service scam methods. Besides, this Supplement specifies the characteristics and the source of the telephone service scam, and categorizes the main methods and relevant technical requirements according to the key technologies of the telephone service scam discovering, judgment, and disposition.

2. References

[1] ITU-T X.1231 - Technical strategies for countering spam.

[2] ITU-T X.1245 - Supplement on Technical measures and mechanism on countering the spoofed call in the terminating network of VoLTE.

[3] IETF RFC 7340: "Secure Telephone Identity Problem Statement and Requirements", September 2014.

[4] IETF RFC 7375: "Secure Telephone Identity Threat Model", October 2014.

[5] 3GPP TR 33.832: Study on IMS Enhanced Spoofed Call Prevention and Detection

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

3. Definitions

TBD

4. Abbreviations

TBD

5. Conventions

TBD

6. Overview of telephone ~~fraud~~ service scam

~~TBD~~

The development and application of network technologies are not only bringing convenience to the users, but also requiring users to submit some information about their identification. For instance, when the users are using online shopping, they need to provide their names, addresses, contact information, etc.; as they use online banking services, the users need to provide their personal identification, bank account and some other information; while they use mobile applications, personal identification, location and other information might be required. Once the information above get disclosed, the scammers may make use of it and commit deception.

Besides, the scammers may make use of the loopholes of network technology, fake the caller's phone number and pretend to be, for example, costumer services of a bank or an airline company, to get the users' trust.

Through telephone calls, the scammers mask themselves into various identifications to deceive the users for their money. For instance, they collect the users' personal information through Internet or

other methods, pretend to be tax officers or bank clerks, tell the users that they are in great trouble, and decoy the users for their money.

With the development of telecommunication network, recently, the telephone service scam is causing disturbances to customers' daily lives and has caused many negative effects.

6.1 Categories of telephone service scam characteristics

Comparing to traditional scam crime, telephone scam has some significant advantages:

- By calling random phone numbers or number lists of target victims, the costs of scams are decreased but the time efficiency is greatly improved;
- Since the victims are unable to meet the scammers in person, it is much easier for the scammers to disguise their true identification, because they don't have to prepare relevant uniforms, ID cards, standard firearms and other relevant properties to be convincing;
- By making use of the management loopholes of telephone service providers, the scammers are capable of concealing themselves from the investigation of police departments;
- By making use of bank accounts and transfer service, the scammers can ask the victims to transfer their money to a specified account and take out cash at any ATM to gain the filthy lucre remotely.

6.2 Typical scamming scenes

The following examples are some typical scenes that have been used by scammers.

6.2.1 Camouflage as government or public security officer

The scammers pretend to be officers of police department, law court, national security departments, etc., claiming that the victims are involved in some criminal cases. If the victims panic and urge to prove their innocence, they will be asked to transfer their money to a specified "secure" bank account "temporarily" to make sure the "criminals" won't be able to make use of the money to commit the "crime". After the scammers receive the money in their account, they will cut of the communication method and refuse to contact to the victim.

6.2.2 Credit card arrears

The scammers call the victims pretending to be clerks of a bank. They tell the victims that, according to the record of the bank, there is an unusual transaction occurred using the victims' credit card. When the victims get confused and worried about arrear fines, they would ask the victims to transfer their money to a specified bank account to avoid interests or fines. The scammers claim that they are going to investigate the transaction, and after they make sure the problem, the victims' money would be returned.

On some occasions, the victims may refuse or unable to transfer their money, so the scammers may alter the methods. They may ask the victims for their card number, password or other verification codes, so they can login the bank account through Internet and finish the transfer progress by themselves.

6.2.3 Lottery awards

The scammers call the victims claiming to be an employee of some lottery company and the victims' phone number was selected randomly to win a lot of money (or an automobile, a laptop, a smartphone, etc.). When the victims are urging to get the "award", the scammers would ask them to pay some money in the name of tax, some fees, etc.

On most occasions, the scammers make use of people's fear, greed, ignorance and other psychologies to induce them into the trap. After the victims realize that they have been deceived, they cannot provide any useful information to the police other than a phone number. If the telephone service providers don't have any records about the users' personal identification, refuse to

provide it to the police or the scammers' numbers are forged, it is almost impossible for the victims to get their money back. Even though it is possible to find the scammers, it would be very difficult to collect necessary evidence to punish the criminal.

7. Characteristics analysis

~~TBD~~

When taking advantages of communication network, generally, the scammers want to achieve two main purposes:

- Make phone calls at a very high frequency to reach as many users as possible in unit time. 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. Thusly, the more phone calls they make, the more victims they could encounter.
- Conceal their real identification as well as possible. After the scammers successfully commit the scam and get the victims' money, they need to prevent the police or public security departments from finding them. Therefore, the phone calls may maintain some specific characteristics, such as, unable to find registered name attached to the calling number, no calling number displayed to the called users, apparent forgery of the displayed calling number, etc.

According to the results of researches on the crimes, there are three major characteristic categories of the telephone service scam.

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 reason explained above. Thusly, their phone numbers' calling frequency would be apparently higher than legit users.

7.1.2 Dispersion of called numbers

When researching dispersion of called numbers, there is another concepted involved called "first call". "First call" means one user is calling another phone number for the first time without previous call records. Dispersion of called numbers refers to the proportion of the "first call" in all the user's call records.

Since most numbers called by legit users are their relatives, colleagues, friends, clients, etc., these actual existing relationships make the calling records among these numbers occur repeatedly in some specified time range, thus the occurrence of "first calls" should be relatively low. And this leads to a low dispersion of called numbers. However, the scammers need to call a lot of random phone numbers in a short time, the "first calls" in their calling records should stand for a much higher proportion than legit users, that is, their dispersion of called numbers are much higher than the average value of legit users.

Sometimes, the scammers may contact the same called user for multiple times. Thismay involve three major possible conditions:

- The scammers are using the phone numbers to make phone calls that are not directly related to the scams.
- The scammers are calling repeated numbers on purpose, to avoid being discovered by anti-scam systems.
- The scammers call the same users for more than once because they have already got these users' trust and started to deceive them for their money.
- If the third condition occurs, the relative departments could contact the victim-to-be to alert them.

7.1.3 Average talk time

When receiving calls from scammers, most users could recognize the scam and terminate the call actively, while only few people may get trapped in the scam and keep the conversations continuing. Thusly, scammers' average talk times may get terminated in very few seconds which is much lower than legit users.

7.1.4 Long distance calling rate

Most legit users are using their telephones for daily life or work, and this implies that most of calls they make should be contacting phone numbers in the same area. While the scammers are searching for victims in a nationwide scale, that means they make more long distance calls than most users.

7.2 Characteristics of the calling numbers

7.2.1 Special public numbers

To get the called users' trust, a lot of the scammers fake their calling numbers into some well-known public numbers. For example, when they are pretending to be police officers, they may change the calling number into 911 or other numbers used by local police departments; when they are pretending to be clerks of banks, they use the banks' costumer service numbers which are published in advertisements. However, on most occasions, these numbers are not used for contacting costumers actively; they are only used to answer the costumers' calls. Thusly, when the operators or relative departments find out a call using these numbers as calling numbers, the calling party is highly possible to be a scammer.

7.2.2 No displayed calling number

To conceal their real identification and to avoid the blocking applied by operators or the investigations of the police, the scammers may use special technical methods to conceal their calling number. As a consequence, the called users are unable to see the calling numbers so they cannot report the scam or provide relative evidences.

7.2.3 Abnormal signaling

When the scammers are making telephone calls, they may make use of abnormal signaling to conceal their positions, and when these kinds of signaling occurs, it is highly possible that the caller is performing illegal behaviors. Below are several typical examples:

- Abnormal international code: when a phone call is entering U.S.A through international gateway, but it's country code is claimed to be "+1" and the caller's number is a landline telephone, this call could be very suspicious. Normally, these conditions mean the caller is making a domestic call and it shouldn't reach the international gateway, so when the international gateway finds out an entering call holding 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 (for instance, gateway between operator A and B) is receiving a call coming from operator A and requiring to enter the network of operator B, but the signaling is holding the operator code of operator B and implies to be a landline telephone. For the similar reason of the example above, this call is very suspicious.
- Wrong telephone number length: the length of telephone numbers in 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 signaling, 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, the telephones' keyboards are used when the users are calling numbers used for customer service or similar purposes. On these occasions, only the calling party would use keyboard while the called party don't. However, some scammers intent to decrease their personnel cost when calling massive numbers so they intent to play a pre-recorded sound file when the called parties answer the call and ask them to press a specific number. Thusly, if the called user recognizes the scam, they may hang up immediately without pressing the button required so the scammers don't have to talk to them, repeating the same lies time after time.

With the discovery of this phenomenon, the called parties' usage of keyboard could be an important characteristic to determine telephone service scam. Though there might be some legit scenes that may require the called party to use the keyboard, the system could involve whitelist or other similar mechanisms to avoid false alarm.

7.3.2 By pre-recorded sound files

As mentioned above, some scammers may use pre-recorded sound files to lower the personnel cost, so 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 sample to determine if it is a scam.

7.3.3 Combination with other communication methods

On a lot of occasions, the scammers do not use telephone as the only communication method. They may also involve instant messaging software, mobile communication applications, short message, etc. Hence, if there is communication actions detected between the calling party and the called party before or after the call, the suspicion may increase.

Countering telephone service scam is a complicated system engineering problem, so it is unreasonable to determine scam crime with one single characteristic. Determining by multiple characteristics could incredibly increase the accuracy and decrease disturbance to legit users. Furthermore, combining user report, whitelist and other mechanisms could make the entire system more efficient and reasonable. However, when applying these characteristics to practice, the determination thresholds of these characteristics should be set up according to local reality.

Besides, with the promotion of countering telephone service scam technologies, the scammers may also alter their applying methods of crime commitment. Thusly, the characteristics used in telephone service scam recognition and technologies of blocking should also be updated time to time.

8. Key technologies of the telephone ~~fraud~~ service scam

8.1 Discovering

TBD

8.2 Judgment

TBD

8.3 Disposition

TBD

9. Structure of countering telephone service scam ~~fraud~~ functions

9.1 General structure

TBD

9.2 Reference model

TBD

9.3 Functions of components

TBD

10. Countering processing

TBD

_____