International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X
Supplement 28
(09/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1245 – Supplement on technical measures and mechanisms on countering spoofed calls in the terminating network of voice over long term evolution (VoLTE)

ITU-T X-series Recommendations – Supplement 28

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.

Supplement 28 to ITU-T X-series Recommendations

ITU-T X.1245 – Supplement on technical measures and mechanisms on countering spoofed calls in the terminating network of voice over long term evolution (VoLTE)

Summary

Since the rapid development of the fourth generation (4G) based on the Internet protocol (IP) multimedia subsystem (IMS) network generated the renovation of the network architecture and the service mode, it is possible for spoofed calls to cause security and financial threats, as well as creating new difficulties to terminal users and operators alike. The difficulties and threats can be labelled as fraud issues generated by callers who use highly impersonated telephone numbers, which are faked by certain legal or illegal measures, to allure the callee. However, in spite of the new threats and difficulties, some new opportunities have also arisen to counter spoofed calls, since particular technical measures can be implemented in the IMS network.

The objective of this Supplement to Recommendation ITU-T X.1245 is to analyse the threats and to recommend technical measures and mechanisms to counter spoofed calls in the terminating network of voice over long term evolution (VoLTE) if the identity of the incoming calls cannot be trusted securely by the terminating network. This Supplement to Recommendation ITU-T X.1245 focuses mainly on the protection of VoLTE users, to prevent them from the risk of receiving spoofed calls or to warn them in advance of suspicious spoofed calls by deploying procedures both on the network side and the user side (smartphone), after having conducted a threat analysis of spoofed calls.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 28	2016-09-07	17	11.1002/1000/13073

Keywords

IMS, spoofed call, VoLTE.

* To access the Supplement, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Supplement'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

		Page
1	Scope	1
2	References	1
3	Definitions	1
3.1	Terms defined elsewhere	1
3.2	Terms defined in this Supplement	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	Background	2
7	Threats and difficulties of the analysis	3
7.1	Participants	3
7.2	Existing threats	3
7.3	Scenario analysis	4
8	Proposed measures	5
8.1	General aspects	5
8.2	Detecting and verifying measures	6
8.3	Blocking measures	7
8.4	Alerting measures	8
8.5	Measures integration	8
Appendix I – Legal issues		9
Bibliography		10

Supplement 28 to ITU-T X-series Recommendations

ITU-T X.1245 – Supplement on technical measures and mechanisms on countering spoofed calls in the terminating network of voice over long term evolution (VoLTE)

1 Scope

This Supplement gives an overview of spoofed calls in the Internet protocol (IP) multimedia subsystem (IMS) network, analyses several aspects of existing threats and new technical difficulties, and also proposes technical measures and procedures to counter spoofed calls.

This Supplement only focuses on spoofed calls in the terminating network of voice over long term evolution (VoLTE), where there are no reliable trust mechanisms. The proposed measures and anti-spoof application servers (ASs) described are all targeted towards the IMS network.

Compliance with all relevant laws and regulations should be considered before adopting the measures discussed in this Supplement.

2 References

[ITU-T X.1246] Recommendation ITU-T X.1246 (2015), *Technologies involved in countering voice spam in telecommunication organizations*.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following term defined elsewhere:

3.1.1 vishing [b-ITU-T X.1244]: An illegal act of gaining access to private personal and financial information through the voice over IP (VoIP) service. The term vishing is a contraction of "voice phishing".

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 non-licensed ID prefix: The prefix of a terminal ID in telephone systems that has not been licensed (or enabled officially) in a living market.

3.2.2 spoofing caller: A technical device or platform that can cause a telephone network to indicate to the receiver of a call that the originator of the call is a terminal other than the true originating terminal.

3.2.3 swatting: An act which deceives an emergency service into dispatching an emergency response based on the false report of an ongoing critical incident.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

4G Fourth Generation

ARPU Average Revenue Per User

AS Application Server

BOSS Business and Operation Support System

CLI	Calling Line Identification
CS	Circuit Switched
CSCF	Call Session Control Function
DoS	Denial of Service
HSS	Home Subscriber Server
I/S-CSCF	Interrogating/Serving Call Session Control Function
ID	Identity
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol
RCS	Rich Communication Service
SCP	Service Control Point
SIM	Subscriber Identity Module
SLF	Subscriber Location Function
SS7	Signalling System No. 7
VoIP	Voice over Internet Protocol
VoLTE	Voice over Long Term Evolution

5 Conventions

None.

6 Background

Spoofed calls are a type of call that exists in the telecommunication voice service. Spoofed calls are identity faked or identity modified of unwanted and unsolicited calls with the objective of fraud, vishing, identity (ID) theft, etc.

As the IMS network is developing rapidly, the VoLTE service, providing a new mode of communication, has already been deployed or is in process by some operators. Since the IMS network might not deliver complete and trusted calling information from the originating network to the terminating network, and since various new value-added services based on the VoLTE service are likely to be imported or created, security issues associated with spoofed calls are becoming more complicated compared to those in the traditional (circuit switched (CS)) network. Spoofed calls can be generated much more easily by the caller, which causes several threats to both terminal users and operators.

Both in the traditional network and in the fourth generation (4G) network, spoofed calls are generated due to protocol and management vulnerabilities. However, in the traditional network, once a spoofed call arrives at the terminated network, operators can scarcely identify whether an incoming call user identity (mostly from other networks) is spoofed or not.

IETF WG secure telephone identity revisited (STIR) and 3GPP Service & System Aspects WG3 (SA3) have approved [b-IETF RFC 7340] and [b-IETF RFC 7375], in which spoofed calls in a CS environment are emphasized, with upcoming measures in the IMS network, such as spoofed-call detection methods.

7 Threats and difficulties of the analysis

7.1 Participants

Participants involved in the analysis include the callee, the network elements and the spoofing caller.

7.1.1 Callee

In this Supplement, the callee is the entity to be protected and is the one who should have subscribed to the VoLTE service. The types of terminals that can be used by the callee are various, but with the consideration that these terminals should support the access and services of 4G networks, the de facto type of terminal can only be smart terminals in most cases.

7.1.2 Network elements

Network elements include routers, switches (call session control functions (CSCFs)), gateways, servers (home subscriber servers (HSSs) or subscriber location function (SLF)) and all the equipment provided by telecommunication operators. The terminals of the caller and the callee are connected by network elements, and the signalling is transmitted between the elements. In this Supplement, all the elements are technically allowed to modify the signalling information and abandon certain calling line identity information.

7.1.3 Spoofing caller

A spoofing caller is a technical device or platform that spreads improperly or illegally voice information through spoofed calls. To dupe the callee on a large, efficient and flexible scale, the spoofing caller may adopt some voice software platforms instead of regular terminals by abusing either the service or the network protocol vulnerabilities.

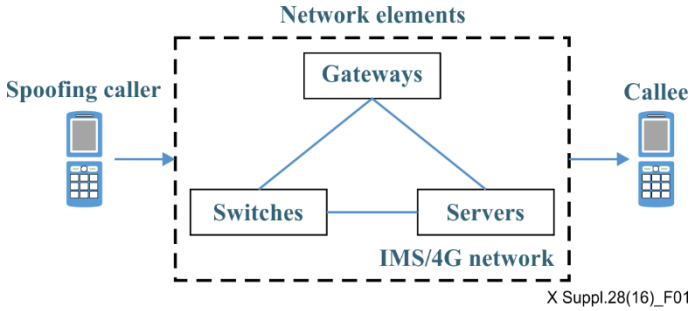

Figure 1 – Connections among participants

7.2 Existing threats

[b-3GPP TR 33.832] has analysed spoofing or malicious modification of caller information such as the calling line identification (CLI) and the caller name. CLI is analysed broadly, and it can be misused by means of spoofing, ranging from harmless to illegal issues, such as testing the responsiveness of the callee depending on the displayed caller's number or vishing by displaying the forged number of an authority organization in order to steal the user's credentials. Moreover, the widespread use of voice over Internet protocol (VoIP) via the public Internet has disclosed the unreliability and vulnerability of CLI.

Both [b-3GPP TR 33.832] and [b-IETF RFC 7375] have analysed the existing threats of spoofed calls in traditional networks as follows:

– voicemail hacking via impersonating (IETF WG STIR);

– nuisance calls, unsolicited commercial calls from impersonated numbers (3GPP SA3, IETF WG STIR);

– violations of various phone solicitation rules used as a platform for significant fraud, identity theft and social engineering (3GPP SA3);
– various malicious uses of caller information, including these categories: swatting, vishing and denial of service (DoS) (3GPP SA3).

Compared to the above threats, the spoofed calls cause more threats in the IMS network than in the traditional network.

The IMS network allows the originating network to verify the identity of a call through a certain protocol field, which may not be delivered to the terminating network; therefore, the terminating network may not be able to display the real calling identity to the callee. The characteristics of the IMS network cause new difficulties in that the spoofed calls are generated more easily by spoofing callers and are very difficult to detect by the operators in the terminating networks.

In the IMS network, services can be of various kinds, such as the 'one-card-multi-numbers', which is a fundamental service that can provide users with multiple calling line identities or caller names (IDs), by using only one subscriber identity module (SIM) or an equivalent card. These types of services increase significantly the difficulty of identifying the exact spoofed caller. Another service named the "multi-party call" involves multiple communication parties in one call, which increases the probability and spreading range of spoofed calls.

7.3 Scenario analysis

Generally speaking, the new difficulties could be classified into the following threat patterns:

– The spoofing caller and its originating/visiting network is not within the trusted domain; hence, the caller can fake, imitate or directly use the real calling ID to dupe the callee without hindrance.
– The spoofing caller is allowed to use a certain legal calling ID, which is highly similar or partially the same as some famous or important public service IDs.
– According to the international exchange protocol of CLI, the caller ID can be hidden and is not completely displayed on the callee's terminal, whereas the national number and the local area number are displayed, which could be quiet similar to some famous or important public service IDs.
– Video calling identity fraud: In compliance with the faked ID, a spoofed caller forges some kind of physical environment in a video call, which is faked but similar to a public service authority or financial organization; hence, callees may be deceived more easily based on what they have seen.

The origins and spread paths of spoofed calls in the terminating network of VoLTE can be classified into the following scenarios:

– IMS network to IMS network: A VoLTE service user in the IMS network fakes a calling ID and generates a call to another VoLTE service user.
– CS network to IMS network: A traditional service user in the CS network fakes a calling ID and generates a call through the signalling system No. 7 (SS7) to a callee of the VoLTE service and the call is transferred to the IMS network, where the callee is visiting.
– IMS network to CS network: A VoLTE service user in the IMS network fakes a calling ID and generates a call to a callee of the VoLTE service and the call is transferred to the CS network, where the callee is visiting because of falling back from the 4G network to the 2G/3G network.
– CS network to IMS network to CS network: A traditional service user in the CS network fakes a calling ID and generates a call through SS7 signalling to a callee of the VoLTE service and the call is transferred to the IMS network and then transferred to the CS network, where the callee is visiting because of falling back from the 4G network to the 2G/3G network.

8 Proposed measures

8.1 General aspects

There are several scenarios for spoofed calls; however, this Supplement focuses mostly on the measures to counter the following two kinds:

– complete duplicate of a real calling identity.

– mimic a real calling identity with nuance.

Based on the flexibility of the IMS network and the extensibility of the voice call procedures, a new logic entity, anti-spoof application server (AS), in or beyond the AS layer with a countering platform, can be introduced to control the suspicious incoming calls (spoofed calls). The platform network layout is as shown in Figure 2.

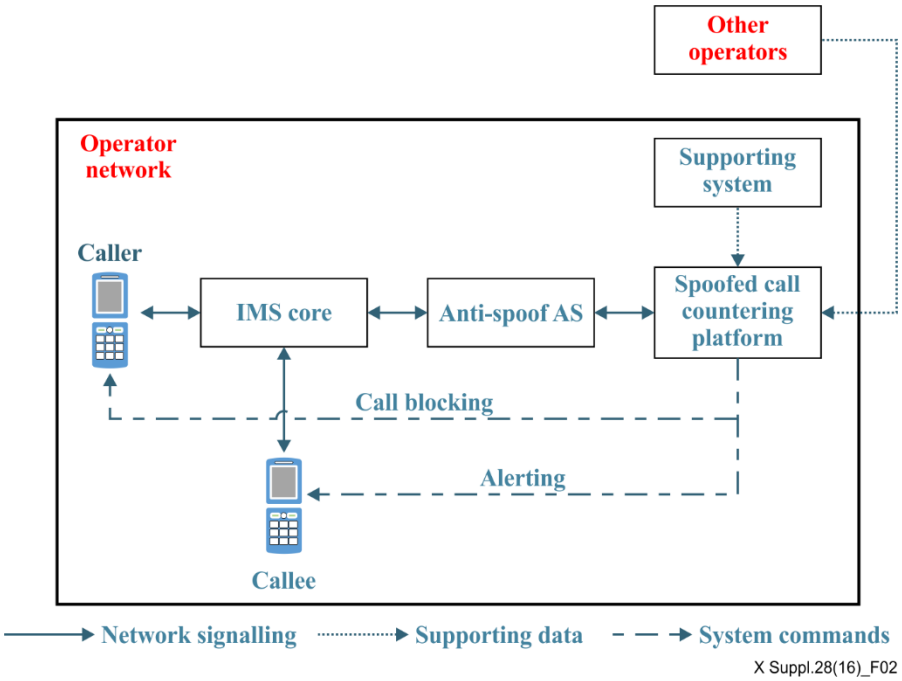

Figure 2 – Layout of the platform in the network

Based on Figure 2, the countering procedures include detecting, verifying, blocking and alerting, as shown in Figure 3.

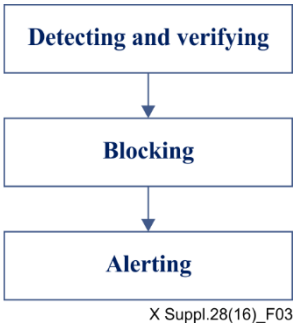

Figure 3 – Countering procedures in the platform

In this Supplement, all the countering measures should be implemented in the terminating network of the IMS, which means that the callee should be a VoLTE service user. This means that its mounting point should always be in the IMS network, no matter where the callee is visiting. In addition, it is

suggested that all countering measures be implemented in the terminating network of the IMS to enhance security integrity.

8.2 Detecting and verifying measures

Since the architecture of the IMS network is more flexible than that of the traditional network, the IMS can easily implement some (new) detecting and verifying measures to monitor the spoofed calling identity. The countering platform implements some real-time controls and historical comprehensive analysis acting in concert to detect and verify spoofed calls.

8.2.1 Caller name (ID) matching

Calling identity (number) matching is a real-time measure that can extract the caller number from the signalling and compare it with existing numbers, and support the analysis of the authenticity of the caller number.

Existing numbers are stored as a list in the database that includes the most important and sensitive numbers or particularly the protected numbers, such as:

– blacklists or numbers of high risk;
– non-licensed ID prefixes;
– service numbers;
– government or authority numbers;
– emergency contact numbers.

Based on the above list, the platform implements complete matching, partial matching and random matching methods, respectively, to perform the comparison.

8.2.2 Calling status comparison

Calling status comparison is a real-time measure which is implemented in the calling setup procedure. After a call setup, the platform forwards the query request to a network element, such as the interrogating/serving call session control function (I/S-CSCF) in the IMS network or the service control point (SCP) in the intelligent network (IN), to confirm the real status of the caller. See Figure 4.

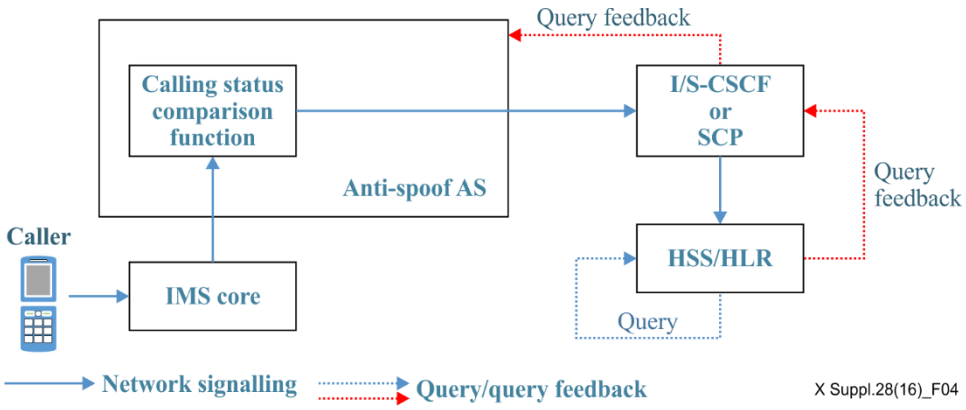

Figure 4 – Calling status comparison query

However, as mentioned above, multiple numbers (numbers associated with the main number) can be bundled into one SIM card in the 4G/IMS network, therefore it can be difficult to identify exactly which number is abused by a spoofed caller. The ID status comparison measure provides the status trace of all the ID numbers, which means the platform queries all the numbers bundled to one user and might provide one of following results.

– The current main number is online/busy and all the associated numbers are offline/idle, which is the default normal state.
– The current main number is online/busy and some associated numbers are offline/idle.
– The current main number is offline/idle and some associated numbers are online/busy.
– The current main number and all the associated numbers are offline/idle.

The platform will analyse the caller ID status based on the above results and score the caller ID.

8.2.3 Calling line identification analysis

CLI analysis is a real-time measure that is implemented during the calling setup procedure. Since a spoofing caller is the origin of spoofed calls, operators can manage the scores of the caller ID under legislation (if applicable) to reduce the risk of spoofed calls. Several factors, such as user reliability, average revenue per user (ARPU) and ID, can be scaled and managed by scores. It is convenient for the platform to evaluate the caller ID and scale it. This measure needs support from certain systems, such as an HSS, business and operation support system (BOSS) or any system that stores customer ID information.

8.2.4 Calling characteristics analysis

The calling characteristics analysis is a historic comprehensive measure, since signalling can provide a lot of data to analyse the calling characteristics, including call frequency, connection rate, call clear times, tone duration and callee statistics. The platform analyses the user with the main number and all the associated numbers in the long term.

The calling characteristics analysis can be found in [ITU-T X.1246].

8.2.5 Systematic evaluation

The anti-spoof application server (AS) or equivalent system comprehensively analyses the calling identity, calling status, calling party identity and calling characteristics, and scores an incoming call or a caller ID.

If the score of a call or caller is lower than the particular pre-set threshold that is determined by the operating practice, the call or caller is further processed by the platform. Details will be discussed in clause 8.3.

8.3 Blocking measures

After the detecting and verifying procedure in Figure 3, a call might be put through. If not, the call is processed further, and particular measures taken to block certain calls or certain callers (or calling parties).

8.3.1 Call real-time blocking

Call real-time blocking is aimed at the current calling procedure so that the platform can handle calls immediately. The platform can instruct a voice application server (AS) to either forward the call or to block it.

8.3.2 Caller (or calling party) blocking

Caller blocking is aimed at the caller. The platform can provide diversified forms, which include blacklist mechanisms and number cancellation, to handle spoofed callers.

Since one spoofing caller may hold several calling numbers based on flexible 4G services, the platform might need in practice to block batches of calling numbers of a caller.

8.3.3 Customization of blocking lists

The platform enables the customization blocking function, whereby the user can upload blocking lists into the network side and block calls from certain numbers. In addition, the user can customize their own lists and specify them by more accurate rules, such as a certain number can only get through during working hours.

8.4 Alerting measures

As the IMS network can invoke certain elements to counter spoofed calls collaboratively, alerting measures can also be implemented on both the network side and the terminal side.

8.4.1 Rich communication services-based alerting

Due to rich communication services (RCSs) or other kinds of messaging service, operators can maintain communications with the callee more easily and in real time. As a result, operators can: warn the callee of those calls that are spoofed suspiciously and of those callers that are suspected spoofed callers; or alert the callee that the call last put through may be of high risk or suspiciously spoofed.

8.4.2 Smartphone-based alerting

Nowadays, various smartphone functions can provide validation functions in collaboration with an anti-spoof AS or a platform to alert terminal users about whether an incoming call is suspiciously spoofed. The alert information that is generated from the platform is directly pushed to the terminals and displayed on the screen before or while the call is connected.

8.5 Measures integration

None of these measures can be entirely successful independently. In order to counter spoofed calls effectively, network-side and user-side technologies should be deployed comprehensively in each procedure.

For high accuracy, measures in the detecting and verifying procedure should be implemented in turn.

The measure proposed in clause 8.2.4 is easy-to-use and not costly. To increase the accuracy of the analysis, more sophisticated rule models and algorithms can be introduced, see clause 7.5 of [ITU-T X.1246].

As can be seen from the blocking and alerting measures, the user-side and network-side measures should be better integrated to mitigate spoofed calls. The customer service departments of operators could play a significant role in getting feedback from customers.

Appendix I

Legal issues

In consideration of the sensitivity of countering spoofed calls, all measures in this Supplement should be deployed in accordance with legislation or obtain approval from relevant authorities or organizations.

Due to the blocking measures, such as call real-time blocking or calling party blocking, operators should inform existing and future potential customers that there are possibilities that their incoming calls may be blocked before they get through or that certain calling parties cannot be connected to the network. Whether alerting measures are enabled, operators should get full agreement and permission from the customer.

However, operators will be exposed to more risks when the proposed measures are implemented improperly. Hence, operators should adjust measures in daily operation to meet actual needs.

Bibliography

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

[b-3GPP TR 33.832] 3GPP TR 33.832 (2015), *Study on IMS enhanced spoofed call prevention and detection*.

[b-IETF RFC 7340] IETF RFC 7340 (2014), *Secure telephone identity problem statement and requirements*.

[b-IETF RFC 7375] IETF RFC 7375 (2014), *Secure telephone identity threat model*.

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, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2019