Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1246

Enmienda 1

(05/2022)

SERIE X: REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Lucha contra el spam

Tecnologías implicadas en la lucha contra el spam de voz en las organizaciones de telecomunicaciones

Enmienda 1

Recomendación UIT-T X.1246 (2015) – Enmienda 1

RECOMENDACIONES UIT-T DE LA SERIE X

REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTION DE INTERCONEXION DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web (1)	X.1140–X.1149
Seguridad de aplicación (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	**X.1230–X.1249**
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319
Seguridad de las redes eléctricas	X.1330–X.1339
Correo certificado	X.1340–X.1349
Seguridad en la Internet de las Cosas	X.1350–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1399
Seguridad de tecnología de libro mayor distribuido (DTL)	X.1400–X.1429
Seguridad de aplicaciones (2)	X.1450–X.1459
Seguridad de web	X.1470–X.1489
INTERCAMBIO DE INFORMACION DE CIBERSEGURIDAD	
Aspectos generales de la Ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
Ciberdefensa	X.1590–X.1599
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminología	X.1700–X.1701
Generador de número aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE DATOS	
Seguridad de los macrodatos	X.1750–X.1759
Protección de datos	X.1770–X.1789
SEGURIDAD IMT-2020	X.1800–X.1819

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T X.1246

Tecnologías implicadas en la lucha contra el spam de voz en las organizaciones de telecomunicaciones

Enmienda 1

Resumen

La comunicación de voz es un servicio fundamental que prestan las redes de telecomunicaciones. Con el desarrollo de la comunicación de voz también se ha incrementado el spam de voz, con numerosos efectos negativos para los usuarios finales y los operadores de red. En general, el spam de voz tiene contenidos que van desde los anuncios comerciales hasta el material pornográfico ofensivo, lo cual tiene diversos tipos de efectos negativos para los usuarios finales y los operadores de red. El spam de voz puede atraer, irritar, acosar o incluso intimidar a los usuarios y tener efectos negativos en los recursos de red. Para evitar estas influencias negativas, y para proteger los derechos de los usuarios y mantener la estabilidad de la red, los operadores de red tal vez deseen incrementar sus esfuerzos para combatir el spam de voz.

El objetivo de la Recomendación UIT-T X.1246 es examinar las soluciones técnicas para combatir el spam de voz sin considerar el riesgo de la autenticidad de la identidad de quien envía el spam. En ella se ofrece una visión general del spam de voz, y se resumen las tecnologías antispam existentes que aplican tanto los usuarios como los operadores de red, y el mecanismo de colaboración entre ellos. También se recomiendan propuestas de soluciones técnicas adicionales sobre la base de las tecnologías antispam y [...] del citado mecanismo de colaboración.

En la Enmienda 1 se introduce el mecanismo de notificación por parte del cliente que recibe una posible llamada de spam (vía voz, servicio de mensajes cortos (SMS) o servicio de mensajería multimedios (MMS)) a su operador. En ella se ofrecen requisitos técnicos para que los sistemas de gestión de telecomunicaciones y/o los sistemas de soporte a clientes puedan recibir notificaciones de llamadas entrantes de spam, de voz o mensajes (SMS/MMS). Se describen escenarios de interacción activa de los clientes con los operadores/proveedores de servicio de las redes de comunicaciones telefónicas sobre las llamadas entrantes de spam y las medidas técnicas necesarias para mantener dicha interacción. La interacción se basa en la realización de una llamada al número contra el spam, proporcionado anteriormente por el operador de telecomunicaciones, inmediatamente después de que finalice la llamada de spam.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1246	2015-09-17	17	11.1002/1000/12448
1.1	ITU-T X.1246 (2015) Enm. 1	2022-05-20	17	11.1002/1000/14988

Palabras clave

Spam, spam de voz.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de la existencia de propiedad intelectual, protegida por patente o derecho de autor, que puede ser necesaria para implementar esta Recomendación. Sin embargo, debe señalarse a los implementadores que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar las correspondientes bases de datos del UIT T disponibles en el sitio web del UIT T en http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1246

Tecnologías implicadas en la lucha contra el spam de voz en las organizaciones de telecomunicaciones

Enmienda 1

Nota editorial: la presente es una publicación de texto completo. Las modificaciones introducidas por la enmienda se muestran con marcas de revisión sobre el texto de la Recomendación UIT-T X.1246 (2015).

1 Alcance

En esta Recomendación se presenta en términos generales el spam de voz y se examinan las tecnologías que actualmente se utilizan para luchar contra el spam de voz, incluidas las tecnologías del lado red y del lado usuario, así como el mecanismo de colaboración entre ellas. Además, en esta Recomendación se proponen además otras soluciones antispam prácticas, como los registros de señalización, la verificación interactiva, las medidas de control, etc.

Esta Recomendación se centra únicamente en la lucha contra el spam de voz cuyo origen se encuentra en las redes de telecomunicaciones con conmutación de circuitos, prestando especial atención a las características de la infraestructura de red. Las tecnologías para luchar contra el spam de voz con origen en las redes IP se abordan en [ITU-T X.1244], [b-ITU-T X.1245], además de en [b-IETF RFC 5039]. Quedan fuera del alcance de esta Recomendación las tecnologías que impiden la usurpación de la identidad del llamante.

Antes de adoptar los métodos de lucha contra el correo basura descritos en esta Recomendación debe considerarse la observancia de todas las leyes y reglamentaciones correspondientes.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no le otorga el rango de una Recomendación.

[ITU-T X.1240] Recomendación UIT-T X.1240 (2008), *Tecnologías utilizadas contra el correo basura.*

[ITU-T X.1244] Recomendación UIT-T X.1244 (2008), *Aspectos globales para contrarrestar el correo basura en las aplicaciones multimedios en las redes IP*.

[ITU-T X.1247] Recomendación UIT-T X.1247 (2016), *Marco técnico para luchar contra el correo basura en la mensajería móvil.*

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 red con conmutación de circuitos [b-ITU-T M.60]: Red que proporciona conexiones para la utilización exclusiva de los usuarios durante una llamada o servicio mediante la interconexión de canales de transmisión o circuitos de telecomunicación.

3.1.2 red IP [b-ITU-T E.370]: Red en que se emplea el protocolo Internet como el protocolo de capa 3 del modelo de referencia de interconexión de sistemas abierto (OSI Reference Model).

3.1.3 operador [b-ITU-T M.1400]: Organización responsable de la identificación y gestión de los recursos de la red. Un operador debe estar reconocido jurídicamente por la administración de telecomunicaciones del país o por su delegación. Un operador puede o no corresponder a un asociado comercial.

~~**3.1.4 spammer** [b-ITU-T X.1231]: Entidad o persona que crea y envía spam.~~

3.1.4 servicio de notificación [UIT-T X.1247]: Servicio que permite recopilar y agregar el informe del abonado sobre el spam recibido con arreglo al permiso, la reglamentación y la legislación nacional del usuario.

3.1.5 servicio de mensajes breves (SMS, *short message service*) [b-ITU-T X.1231]: Tipo de servicio de mensajería que permite a los teléfonos móviles, los teléfonos y otras entidades de mensajes breves (SME) transferir y recibir mensajes de texto a través de un dispositivo llamado centro de servicio que ejecuta funciones tales como "salvar" y "enviar".

3.1.6 spam en SMS [b-UIT-T X.1242]: Spam enviado por SMS.

3.1.7 spam [UIT-T X.1240]: El significado de "spam" varía según la percepción que se tiene en cada país de la privacidad y de lo que constituye spam, visto desde una óptica tecnológica, económica, social y práctica. De hecho, su significado evoluciona y se amplía a medida que evolucionan las tecnologías, ofreciendo nuevas posibilidades de utilización indebida de las comunicaciones electrónicas. Si bien no existe una definición universalmente aceptada del spam, este término se utiliza comúnmente para describir aquellas comunicaciones electrónicas masivas y no solicitadas, transmitidas a través del correo electrónico o la mensajería móvil, destinadas a promocionar la venta de productos o servicios comerciales.

3.1.8 spammer [b-ITU-T X.1240]: Entidad o persona que crea y envía spam.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 número contra spam: ~~n~~Número de teléfono especial predefinido por el proveedor de servicio de base/proveedor de servicio propio/operador de telecomunicaciones (este número puede ser único en el país o único para cada operador) que el usuario utiliza para llamar y notificar que la llamada recibida inmediatamente antes en su número de teléfono era una llamada de spam. La notificación en sí es la llamada al número contra spam; el usuario no necesita proporcionar ninguna información.

3.2.2 cebo: Software (que puede estar en un terminal) que emula a un terminal o grupo de terminales a fin de detectar a los supuestos spammer de voz e incluso colabora en su verificación. El resultado de estos sistemas puede utilizarse como prueba en procedimientos jurídicos.

3.2.3 informe de usuario interactivo: S~~s~~e trata de una queja presentada por un abonado que ha recibido una llamada spam o con spam a su terminal telefónico. En general, un informe es una llamada (el hecho de llamar) a un número contra spam o el reenvío de una posible llamada spam con un mensaje a un número contra spam.

3.2.4 entidad de gestión: Entidad que puede tener una o más responsabilidades en lo que respecta a regir, auditor o guiar los trabajos de lucha contra el spam de voz.

3.2.5 llamada spam: L~~l~~lamada telefónica que contiene un mensaje de voz, texto o multimedios no solicitado, cuyo objetivo es, por regla general, la comercialización de productos o servicios.

3.2.6 posible llamada spam: ~~l~~Llamada telefónica indeterminada que parece ser spam.

3.2.7 organización independiente (tercero): Entidad que puede asesorar o coordinar los trabajos de lucha contra el spam de voz, o colaborar en ellos.

3.2.8~~1~~ spam de voz: Llamadas telefónicas pregrabadas, automáticamente marcadas y no solicitadas que suelen tener por objetivo la comercialización de servicios o productos. El contenido del spam de voz va desde la publicidad de bienes a material pornográfico ofensivo. El spam de voz puede tener diversos efectos perjudiciales para los usuarios y los operadores.

~~**3.2.2 cebo**: Software (que puede estar en un terminal) que emula a un terminal o grupo de terminales a fin de detectar a los supuestos spammer de voz e incluso colabora en su verificación. El resultado de estos sistemas puede utilizarse como prueba en procedimientos jurídicos.~~

~~**3.2.3 entidad de gestión**: Entidad que puede tener una o más responsabilidades en lo que respecta a regir, auditor o guiar los trabajos de lucha contra el spam de voz.~~

~~**3.2.4 organización independiente (tercero)**: Entidad que puede asesorar o coordinar los trabajos de lucha contra el spam de voz, o colaborar en ellos.~~

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

CAMEL Aplicaciones personalizadas para la lógica mejorada de red móvil (*customized applications for mobile enhanced logic*)

CCLTP Punto de tiempo finalización de llamada (*call clear time point*)

CCOTP Punto de tiempo llamada continuada (*call continued time point*)

CDMA Acceso múltiple por división de código (*code division multiple access*)

CDR Registro detallado de llamadas (*call detail record*)

CDR_n Registro detallado de llamadas iniciales (*initial call detail record*)

CDR_{n+1} Registro detallado de llamadas interactivas de vuelta del usuario a su operador (*interactive Call Detail Record back from the user to its operator*)

CLI Identificación de la línea llamante (*calling Line Identification*)

CLI_n Identificación de la línea llamante del llamante inicial al usuario (*calling Line Identification of initial caller to the user*)

CLI_{n+1} Identificación de la línea llamante del usuario cuando efectúa una llamada de notificación a un número contra spam (*calling Line Identification of the user, when it makes feedback call to an anti-spam number*)

COSN Número de abonado origen de la llamada (*call originated subscriber number*)

COTP Punto de tiempo origen de llamada (*call originating time point*)

CRBT Tono de devolución de llamada personalizado (*customized ring back tone*)

CS Conmutación de circuitos (*circuit-switched*)

CTSN Número de abonado terminación de llamada (*call terminated subscriber number*)

DMP Plataforma de gestión de dispositivo (*device management platform*)

GMSC Centro de conmutación móvil de pasarela (*gateway mobile switching centre*)

GSM Sistema mundial de comunicaciones móviles (*global system for mobile communications*)

HLR Registro de posiciones propio (*home location register)*

ID Identificación

ID de terminal llamante Identificación de terminal (*caller identification*)

ISIS Sistema de compartición de información (*information sharing system*)

IMS Subsistema multimedios IP (*IP multimedia subsystem*)

IN Red inteligente (*intelligent network*)

INAP Protocolo de aplicación de red inteligente (*intelligent network application protocol*)

IP Protocolo Internet (*Internet protocol*)

IVR Respuesta vocal interactiva (*interactive voice response*)

MMS Servicio de mensajería multimedia (*multimedia Messaging Service*)

MSC Centro de conmutación móvil (*mobile switching centre*)

OTAP Plataforma radioeléctrica (*over-the-air platform*)

QoS Calidad del servicio (*quality of Service*)

RTPC Red telefónica pública conmutada

SCP Punto de control de servicio (*service control point*)

SIM Módulo de identidad de abonado (*subscriber identity module*)

SLETP Punto de tiempo establecimiento de enlace de señalización (*signalling link establishment time point*)

SLRTP Punto de tiempo liberación de enlace de señalización (*signalling link release time point*)

SMS Servicio de mensajes cortos (*short Message Service*)

SS7 Sistema de señalización N.° 7

STP Punto de transferencia de señalización (*signalling transfer point*)

UMTS Sistema universal de telecomunicaciones móviles (*universal mobile telecommunications system*)

VLR Registro de posiciones visitadas (*visitor location register*)

VMS Servidor de correo vocal (*voice mail server*)

VoIP Voz sobre el protocolo Internet

5 Convenios

Ninguno.

6 Generalidades del spam de voz

El spam de voz son llamadas telefónicas pregrabadas, automáticamente marcadas y no solicitadas que suelen tener por objetivo la comercialización de servicios o productos. El contenido del spam de voz va desde la publicidad de bienes a material pornográfico ofensivo. El spam de voz tiene diversos efectos perjudiciales para los usuarios y los operadores.

6.1 Posibilidades de comunicación vocal

La comunicación vocal es un servicio fundamental que prestan los operadores de telecomunicaciones. En un principio, las comunicaciones de voz se realizaban a través de redes tradicionales con conmutación de circuitos (CS, *circuit-switched*). Gracias a la evolución de Internet, estas comunicaciones comprenden ahora la voz sobre el protocolo Internet (VoIP, *voice over Internet protocol*) que se realiza por redes basadas en el protocolo Internet (IP, *Internet protocol*).

A continuación, y en función de la tecnología utilizada, se muestran cuatro posibilidades de comunicación vocal:

- Caso 1: CS-CS: Comunicación vocal tradicional con conmutación de circuitos móvil/fija.
- Caso 2: CS-IP: Comunicación vocal originada por un usuario con conmutación de circuitos móvil/fijo y que termina en un usuario de telefonía IP.
- Caso 3: IP-CS: Comunicación vocal originada por un usuario de telefonía IP y que termina en un usuario con conmutación de circuitos móvil/fijo.
- Caso 4: IP-IP: Comunicación vocal entre usuarios de telefonía IP.

En la Figura 1 se muestran estos cuatro casos de comunicación y sus tecnologías asociadas.

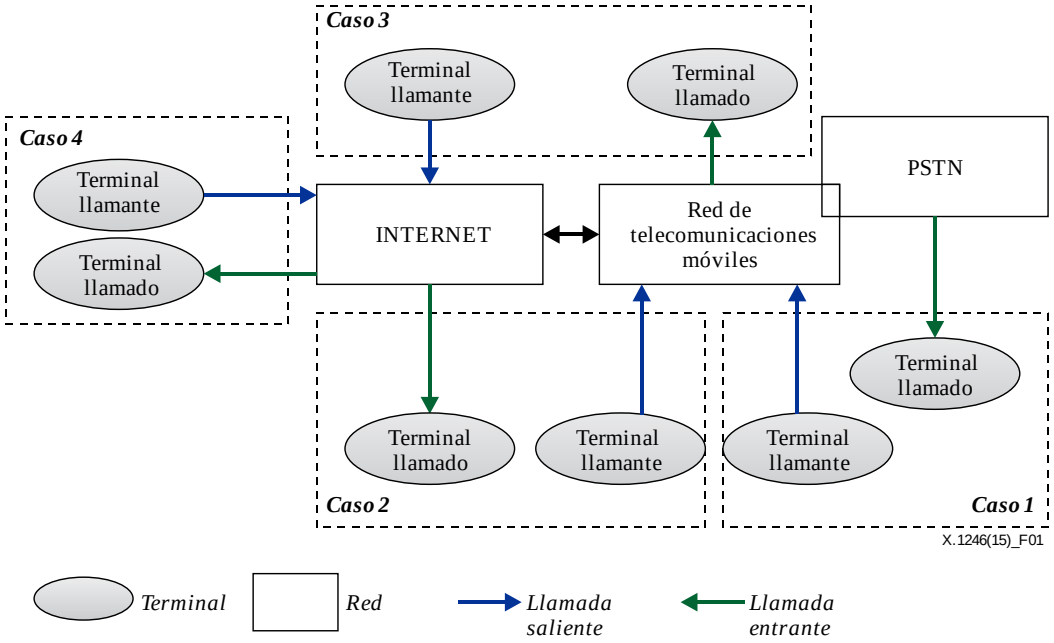

Figura 1 – Casos de comunicaciones vocales en las redes de telecomunicaciones

NOTA – En la Figura 1, el término terminal puede ser un teléfono móvil, un teléfono fijo, un ordenador portátil, una computadora personal, etc., con acceso a redes con conmutación de circuitos/IP. En términos generales, la mayoría de usuarios confía en la fuente de las telecomunicaciones vocales. Por consiguiente, los spammer de voz ven conveniente utilizar las comunicaciones vocales con conmutación de circuitos tradicionales para iniciar el spam de voz. Además, en [ITU-T X.1244] se presentan las tecnologías de lucha contra el spam de voz en los casos 3 y 4. Por consiguiente, en esta Recomendación sólo se abordará la lucha contra el spam de voz en los casos 1 (CS-CS) y 2 (CS-IP).

6.2 Características del spam de voz

El contenido del spam de voz puede ir de la publicidad comercial a material pornográfico ofensivo, que puede tener efectos negativos en los usuarios y los operadores de red:

– el contenido del spam de voz puede ser cansino, engañoso, acosador o amenazador;

– los usuarios y operadores pueden sufrir del malgasto de los recursos;

– es posible que los usuarios y operadores tengan que invertir, tiempo, dinero y esfuerzos en la lucha contra el spam de voz.

De entre todos los tipos de spam de voz, los dos más generalmente reconocidos son los siguientes:

– **Tipo uno (llamada silenciosa)**: Una llamada silenciosa es una llamada telefónica con fines de telemárketing, generada por un marcador (o marcadores) predictivo(s) sin intención de que un agente trate inmediatamente la llamada. Es posible que el marcador termine la llamada, por lo que la parte llamada recibe un silencio (aire muerto) o un todo de la compañía telefónica que indica que se ha caído la llamada. También se denomina "llamada abandonada". Con este tipo de llamada, normalmente se espera que la parte llamada efectúe una llamada al número de donde procedía la llamada abandonada.

– **Tipo dos (llamada de acoso)**: Una llamada telefónica con fines de telemárketing que, además, puede acosar, molestar, alarmar o intimidar con contenido pornográfico, amenazante, ilegal, vergonzante, etc. Normalmente, este tipo de llamada no se abandonará antes de su establecimiento.

7 Tecnologías para la lucha contra el spam de voz

7.1 Aspectos generales

Ninguna solución puede resultar plenamente satisfactoria por sí sola. A fin de paliar la influencia negativa del spam de voz, es necesario aplicar toda una gama de soluciones con sus tecnologías correspondientes, que se dividen entre tecnologías del lado red y tecnologías del lado usuario, para poner fin a los casos 1 y 2, descritos en la cláusula 6.1.

A fin de recomendar una tecnología concreta y definida, en primer lugar es necesario considerar detalladamente las características de la red con conmutación de circuitos, incluida la arquitectura de red, la topología de la red y la pila de protocolo de señalización, etc. al mismo tiempo se han de considerar los procesos del servicio vocal y las tendencias funcionales de los terminales. Las tecnologías recomendadas pueden clasificarse en tecnologías del lado red y tecnologías del lado usuario.

Las tecnologías del lado red son fundamentales para los operadores, es decir, en la red telefónica pública conmutada (RTPC), el sistema universal de telecomunicaciones móviles (UMTS), el sistema mundial de comunicaciones móviles (GSM) y las redes de acceso múltiple por división de código (CDMA). En comparación con las tecnologías del lado red, las tecnologías del lado usuario son mucho más flexibles y dependen de la iniciativa del usuario. Se necesita la información que comunican los usuarios como suplemento a las tecnologías del lado red. Por consiguiente, también ha de establecerse un mecanismo de colaboración efectiva entre ambos tipos de tecnologías.

7.2 Tecnologías del lado red

Todas las llamadas telefónicas se inician mediante señalización en la red de acceso. A fin de detectar a los presuntos spammer de voz, el método básico consiste en recopilar los datos de señalización, analizarlos y verificarlos. Este método se ha de considerar en su totalidad. En términos generales, la fase de establecimiento de llamada conlleva la conexión entre los dos extremos de la comunicación. Durante la fase de establecimiento de llamada, la única identificación de la parte llamante/llamada es la identificación del llamante (ID), lo que lleva a la siguiente observación.

1) Todas las decisiones de tratamiento de llamadas se han de tomar en tiempo real antes de que se complete el establecimiento de llamada.

El spam de voz supone un complejo reto tecnológico, por lo que las soluciones para eliminarlo han de estar sustentadas por los procedimientos adecuados, además de medidas tecnológicas. Un

procedimiento del lado red fundamental para luchar contra el spam de voz puede incluir los procesos que se muestran en la Figura 2.

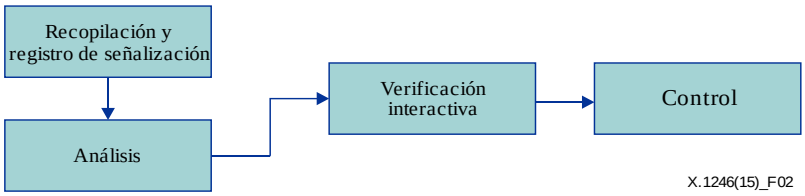

Figura 2 – Procedimiento del lado red para luchar contra el spam de voz

– **Recopilación y registro de señalización**: Para registrar y recopilar los datos de señalización originales en tiempo real.

– **Análisis**: Para identificar a los presuntos spammer de voz y establecer una lista de sus números.

– **Verificación interactiva**: Para realizar una verificación directa y detectar a los verdaderos spammer de voz en la lista de sospechosos.

– **Control**: Para restringir o desactivar a los spammer de voz confirmados por el proceso de verificación a fin de proteger a los usuarios normales.

El procedimiento del lado usuario consta prácticamente de los mismos procesos, pero con medidas más simples. En algunos casos, puede obviarse la verificación interactiva.

De acuerdo con el procedimiento, hay varias tecnologías que pueden utilizarse en cada una de las partes. Cabe señalar que ninguna de las tecnologías que se abordan a continuación será una "bala de plata", es decir, la solución única a los problemas de spam de voz. Más bien al contrario, todas las tecnologías son complementarias y serán más eficaces cuando se utilicen asociadas.

En esta Recomendación se presentan y clasifican las tecnologías en función de su lugar de aplicación, es decir, en el lado red o en el lado usuario, y por sus procesos (mencionados en la Figura 2).

7.2.1 Recopilación y registro de señalización

La recopilación y registro de señalización consiste en recopilar los registros detallados de una llamada en tiempo (casi) real para analizarlos. Entre esos datos pueden incluirse algunos relacionados con el tiempo o el número de teléfono, como los siguientes:

– punto de tiempo origen de llamada (COTP): punto en el tiempo en que el llamante genera una llamada telefónica;

– punto de tiempo establecimiento de enlace de señalización (SLETP): punto en el tiempo en que se establece el enlace de señalización entre el llamante y el llamado;

– punto de tiempo llamada continuada (CCOTP): punto en el tiempo en que se continúa la llamada telefónica y el llamado responde;

– punto de tiempo finalización de llamada (CCLTP): punto en el tiempo en que el llamante o el llamado finalizan la llamada;

– punto de tiempo liberación del enlace de señalización (SLRTP): punto en el tiempo en que se libera el enlace de señalización una vez finalizada la llamada;

– número de abonado origen de llamada (COSN): normalmente conocido como número llamante, es el número desde donde el llamante origina la llamada;

– número de abonado terminación de llamada (CTSN): normalmente conocido como número llamado, es el número donde el llamado recibe la llamada.

El valor de los datos, en particular los relacionados con el tiempo, puede diferir ligeramente en función de la posición de los puntos donde se obtengan. Sin embargo, en la práctica, casi siempre pueden ignorarse estas disparidades.

Cabe señalar que todos los datos indicados en esta cláusula se obtienen de los canales de señalización, pero no de los canales de servicio. En este proceso de registro de señalización, todos los datos que se recopilan generalmente ya figuran en el sistema de gestión de señalización para la contabilidad y el diagnóstico de rendimiento, por lo que pueden reutilizarse a fin de equilibrar los costos.

NOTA – Aunque hay otras fuentes de datos alternativas, como R2 y los sistemas de alerta de llamadas perdidas, a continuación sólo se enumeran las fuentes de datos comunes (basadas en el sistema de señalización N.° 7 (SS7), la red inteligente (IN), el subsistema multimedios IP (IMS), el tono de devolución de llamada personalizado (CRBT), el servidor de correo vocal (VMS), etc.).

7.2.1.1 Señalización SS7

La señalización SS7 puede resultar útil para controlar el spam de voz. Resulta fácil insertar un punto de recopilación de señalización para duplicar la información y los parámetros de señalización y registrarlos. El punto de recopilación de señalización se conecta en paralelo con el enlace de señalización a fin de que la señal sea efectivamente un "haz dividido", aunque el punto de recopilación sólo consumirá una pequeña parte de la potencia. En este caso el fallo del punto de señalización no tendrá consecuencias negativas para el enlace de señalización.

Para recopilar la señalización SS7 hay también otro método, que consiste en insertar un nodo de señalización oculto entre dos nodos de señalización explícitos. Esto significa que el nodo de señalización oculto "bloqueará" primero la señal para registrarla y luego la liberará sin modificarla, excepto por una ligera latencia. Sin embargo, esta tecnología conlleva un riesgo de punto de fallo único, por lo que se necesita una capacidad de reserve y fallo fiable.

La gran ventaja de utilizar los registros de señalización SS7 es que contienen los datos detallados de las llamadas, de los que pueden deducirse diversos indicadores (véase la cláusula 7.2.2). Sin embargo, si el tráfico de llamadas vocales aumenta y se amplía la red, el número de puntos de recopilación de señalización aumentará de manera sincronizada para abarcar todas las fuentes de señalización (o las fuentes principales) a fin de conservar una gama de supervisión aceptable, lo que puede aumentar los costos de la lucha contra el spam.

Se recomienda implantar los puntos de recopilación de señalización en las redes núcleo/locales. Para lograr una recopilación generalizada, estos puntos deberán abarcar todas las interfaces Mc y Nc de los conmutadores. Además, para que la recopilación sea equilibrada, estos puntos sólo deberán cubrir todas las interfaces NC. Si el objetivo son las llamadas nacionales de larga distancia o las llamadas internacionales, deberán estar cubiertos los puntos de transferencia de señalización (STP) internacionales/de larga distancia.

NOTA – El punto de recopilación de la señalización en un elemento lógico de la red, que puede estar formado por distintos tipos de elementos entidad.

7.2.1.2 Red inteligente (IN)

Un método basado en los puntos de control de servicio (SCP) consiste en recopilar la aplicación personalizada para la lógica mejorada de red móvil (CAMEL) o la señalización del protocolo de aplicación de red inteligente (INAP) para su análisis. SCP es un nodo clave de la IN y un factor determinante para decidir cómo procesar las llamadas telefónicas.

Una vez que el usuario ha contratado el servicio IN, la llamada saliente hará que el SCP solicite la información de registro de posiciones visitadas (VLR) del usuario llamado antes de establecer los enlaces de comunicación. Dado que algunos operadores conocen bien los servicios IN, resulta fácil recopilar y registrar los datos de señalización de las llamadas generadas por los usuarios que han contratado los servicios IN.

Dado que los puntos de recopilación de señalización pueden coincidir con los SCP, o encontrarse cerca de ellos, este método necesita menos puntos de recopilación de señalización que el del SS7. Estén o no utilizando los usuarios de la IN la itinerancia, con este método resulta muy fácil supervisarlos.

Este método tiene sus limitaciones. Si la penetración del servicio IN es baja, sólo se supervisará una pequeña parte del comportamiento de los usuarios. Sin embargo, esto puede solucionarse haciendo que los usuarios se abonen implícitamente a un servicio IN personalizado, que reenviará la solicitud de información incondicionalmente al SCP cada vez que se genere una llamada saliente.

Este método está limitado por el proceso común del servicio IN, por lo que sólo se pueden recopilar algunos tipos de datos, como COTP, SLETP, COSN y CTSN (véase la cláusula 7.2.1). Sin embargo, hay margen para la mejora si se introduce un proceso de servicio In más complejo, por ejemplo, si todas las señales de señalización de telefonía se cursan por un SCP.

El método del subsistema multimedios IP (IMS) se parece al expuesto anteriormente en que el IMS posee procedimientos de señalización semejantes a la IN.

7.2.1.3 Tono de devolución de llamada personalizado (CRBT)

El CRBT es un servicio al usuario específico que ofrecen algunos operadores. Cuando un usuario contrata el servicio CRBT, los demás usuarios oirán fragmentos de música predefinida en lugar del tono de llamada. Por tanto, es posible recopilar y registrar los datos de señalización a partir de los anfitriones CRBT.

Este método está limitado por el proceso de servicio, por lo que sólo se podrán recopilar en los anfitriones del servicio algunos tipos de datos, como COTP, CCOTP, CCLTP, COSN y CTSN (véase la cláusula 7.2.1) y el proceso CRBT no tiene prácticamente margen de mejora para recopilar más tipos de datos.

Sólo si un spammer de voz molesta a un usuario CRBT, podrá supervisarse al spammer, por lo que una elevada penetración del servicio es la condición necesaria para que el método resulte práctico. Si se cumple esa condición, la inversión en recopilación y registro de señalización debería ser comparativamente baja.

7.2.1.4 Servidor de correo vocal (VMS)

El VMS se hace cargo de las llamadas en caso de reenvío de llamada por no respuesta, reenvío de llamada por línea ocupada, reenvío de llamada incondicional, etc. En la mayoría de los casos, el VMS no responde a las llamadas silenciosas a menos que esté puesto a incondicional. El VMS puede grabar la voz de la parte llamante, si un llamante de spam intenta la conexión de la llamada y llegar directamente al llamado. En ese caso el servidor puede soportar el proceso de verificación interactiva gracias a las grabaciones de voz remitidas por el usuario o con su autorización (véase la cláusula 7.3.3).

Al igual que en el caso del CRBT, la penetración y utilización del servicio VMS es una condición indispensable para que el método resulte práctico.

7.2.1.5 Cebo

El método cebo se utiliza para crear una serie de números de teléfono sucesivos o aleatorios para atraer a los spammer de voz. Además de la recopilación de datos, con el método cebo también se facilita el procedimiento de análisis, además del procedimiento verificación interactiva.

Dado que el método cebo puede ser activado por cualquier llamante (llamada saliente), puede recopilar tipos concretos de datos, como COTP, CCOTP, CCLTP, COSN y CTSN (véase la cláusula 7.2.1). El método cebo calculará y transferirá los datos para efectuar ciertas medidas analíticas, como se indica en la cláusula 7.2.2.

7.2.2 Análisis

A fin de efectuar un análisis de lucha contra el spam de voz utilizando el sistema de supervisión, es necesario calcular los datos originales recopilados y transformarlos en indicadores significativos, como la tasa de conexión, el tiempo de liberación de llamada, la duración del tono de llamada, etc. a fin de diferenciar a los spammer de voz de los usuarios normales, los indicadores deben registrarse continuamente durante un periodo específico, generalmente conocido como ventana temporal (duración). Los operadores pueden ajustar la duración a un valor adecuado, en función de su experiencia con el mantenimiento.

Todos los indicadores pueden deducirse lógicamente en un indicador global denominado "la norma", que puede utilizarse en algún tipo de algoritmo para analizar el comportamiento del spammer de voz con mayor precisión. En la Figura 3 se muestra el modelo normal para analizar al spammer de voz.

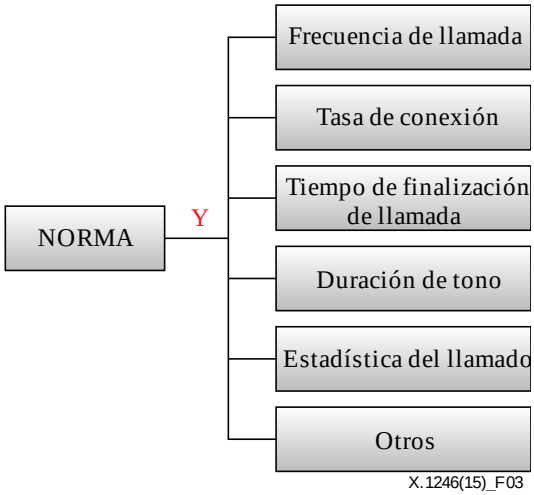

Figura 3 – Modelo normal

El modelo normal se deduce de diversos indicadores por la operación AND (Y) lógica. Dado que los datos proceden de distintas fuentes y pueden recopilarse juntos, no es posible soportar todos los indicadores al mismo tiempo. Una solución viable al problema sería fijar los indicadores no soportados a "VERDADERO" o a "1" para ignorarlos. Por ejemplo, una vez recopilados los datos y transformados éstos en indicadores, el cebo sólo necesita el indicador duración del tono para efectuar el procedimiento de análisis necesario y fijar los demás indicadores a "VERDADERO" o "1" para omitirlos.

A continuación se consignan los indicadores del modelo normal y su definición:

– frecuencia de llamada: número de llamadas en un periodo concreto;
– tasa de conexión: tasa de comunicación de llamadas o de establecimiento del enlace de señalización;
– tiempo de finalización de llamada: número de veces que el llamante o el llamado terminan la llamada por iniciativa propia;
– duración de tono: duración del tono de llamada;
– estadísticas del llamado: estadísticas sobre las características del llamado, como distribución uniforme, progresión aritmética, etc.

Los operadores ajustarán el valor de los indicadores en función de hipótesis de servicio realistas para equilibrar la precisión y el costo. Además, se han de definir normas concretas para adaptarse a los distintos tipos de spam de voz.

Por ejemplo, hay dos tipos de spam de voz ampliamente reconocidos: las llamadas silenciosas y las llamadas de acoso (véase cláusula 6.2). Una llamada silenciosa (también denominada llamada abandonada) es una llamada telefónica iniciada por un marcador que no dispone de un agente

inmediatamente disponible para tratar la llamada. En este caso, el marcado puede terminar la llamada y la parte llamante recibe un silencio ("aire muerto") o un tono de la compañía telefónica que indica que la llamada se ha abandonado. Se espera normalmente que el llamado devuelva la llamada. Una llamada de acoso es una llamada telefónica cuyo objetivo es acosar, molestar, alarmar, amenazar o intimidar con contenido pornográfico, amenazas, información ilegal, anuncios vergonzantes, etc. Generalmente, estas llamadas no se abandonarán antes de su establecimiento.

Las llamadas silenciosas y las llamadas de acoso (véase la cláusula 6.2) pueden mostrar diversas características de indicador dentro del modelo normal propuesto. Cuando el valor de frecuencia de llamada o tiempo de abandono de llamada es más alto y el valor tasa de conexión o duración de tono es más bajo, se trata de un spammer de llamada silenciosa. Por el contrario, las llamadas de acoso pueden centrarse en un llamante concreto por lo que la duración de tono suele ser mayor y, comparativamente, su tasa de conexión es más elevada.

En determinadas circunstancias, un grupo de llamantes silenciosos abrirá un servicio de "reenvío incondicional" para informar a la red del reenvío incondicional de las llamadas entrantes a un número concreto a través del cual funciona una plataforma de respuesta vocal interactiva (IVR). La plataforma IVR puede incluso devolver el spam de voz al llamante entrante mediante un tono de llamada. Resultaría útil para el análisis verificar si los llamantes sospechosos abren el servicio de "reenvío incondicional" y cuál es el número de destino.

Es evidente que existen modelos de análisis más complicados y eficaces para la lucha contra el spam de voz, como el modelo integrado en el análisis de la sociedad humana, el análisis de registros de llamantes facturables, etc. En cualquier caso, el modelo normal puede servir de base para llegar a modelos más globalizadores.

7.2.3 Verificación interactiva

Según lo exijan las entidades de gestión o el acuerdo de servicio de usuario, el número de los llamantes que figure en la lista de sospechosos se verificará antes de tomar medidas de control. En términos de exigencias, hay dos métodos distintos para realizar la verificación.

En primer lugar, las organizaciones de telecomunicaciones deberán seguir actualizando la lista de sospechosos, la someterán a las entidades de gestión y recibirán de éstas información de vuelta.

En segundo lugar, si así lo permiten el acuerdo de servicio de usuario o las entidades de gestión, el operador puede realizar una prueba de marcación en un número llamante de la lista de sospechosos a fin de efectuar una verificación directa. A partir de los resultados de la prueba de marcación, generalmente conocidos como fichero de grabación de voz, el personal de auditoría autorizado intentará determinar si la grabación es o no spam.

Sin embargo, la precisión y la calidad de la verificación interactiva afectan al procedimiento de control.

Como ya se ha indicado anteriormente, un cebo puede realizar la verificación interactiva por sí mismo, es decir, si el resultado del cálculo de los indicadores implica que una llamada saliente es una llamada silenciosa (véase la cláusula 6.2), el cebo devolverá la llamada para realizar la verificación. Por el contrario, cuando el análisis de los indicadores confirme que se trata de una llamada de acoso, el cebo establecerá la llamada y la grabará.

Además, la coordinación entre un grupo de llamantes silenciosos y una o varias plataformas IVR puede confundir a los operadores acerca de la fuente real del spam de voz. En ocasiones las plataformas IVR y los llamantes silenciosos pertenecen a distintos operadores. Una vez efectuada la grabación del spam de voz, será útil, por ejemplo, rastrear la posible conexión entre un llamante silencioso y una plataforma IVR mediante una solicitud al registro de posiciones propias (HLR).

7.2.4 Control

El control se utiliza para restringir o desactivar/anular a los spammer de voz confirmados mediante verificación para proteger a los usuarios normales. A continuación se presentan dos métodos de control:

7.2.4.1 Listas blancas/listas negras

Las listas blancas/listas negras, generalmente conocidas como listas de cuenta clave, llevan mucho tiempo de crear y necesitan una actualización constante. El ciclo de vida de cada elemento de la lista blanca/negra debe estar bien gestionado a fin de que la lista sea precisa y efectiva. Del mismo modo, cada elemento de la lista blanca/negra ha de estar bien mantenido de manera segura durante su ciclo de vida.

Como se indica en [ITU-T X.1240], la calidad de las listas negras varía enormemente en función del profesionalismo de su autor. Las listas negras contienen inevitablemente inexactitudes que impiden que llamadas legítimas lleguen a los receptores. Aunque su utilización plantea numerosas inquietudes, las listas negras son una solución rápida para rechazar una conexión entre fuentes de spam de voz y los receptores (usuarios telefónicos).

Las listas negras con números o segmentos de números de usuarios suelen implantarse en el centro de conmutación móvil de pasarela (GMSC), en SCP, en conmutadores y demás entidades de red. En general, las listas negras de la misma red de operador pueden implantarse en SCP, conmutadores o demás entidades de red, mientras que las listas negras de otras redes de operador pueden únicamente implantarse en un GMSC cuya capacidad de lista negra puede ser demasiado limitada para almacenar una gran lista de números. Para solucionar el problema de manera simple, se pueden utilizar tras el GMSC nodos de señalización ocultos (véase la cláusula 7.2.1.1).

Las listas blancas pueden tener que interactuar con la base de datos autorizada mantenida para los llamantes ya identificados como legítimos a fin de excluir a los llamantes verdaderos que tienen características similares a los spammer de voz. Estos llamantes pueden ser centros de llamada, servicios de notificación, servicios de recopilación de información/datos, como los recordatorios de pago, las respuestas de planes de patrocinio de las entidades de gestión, programas de información, programas de emergencia/en caso de catástrofe, etc.

7.2.4.2 Mecanismo de rastreo

Este mecanismo rastrea el emplazamiento físico real de los spammer de voz. En ocasiones puede resultar útil conocer la ubicación o dirección exacta de spammer de voz.

De acuerdo con las técnicas existentes, los operadores pueden ubicar el emplazamiento real del spammer de voz a partir de la información facilitada por el centro de conmutación móvil (MSC). Sin embargo, con esta técnica sólo se puede definir una zona aproximada. El servicio de información de ubicación del operador, como los que se sirven del servicio global de posicionamiento, puede facilitar un emplazamiento más preciso.

7.3 Tecnologías del lado usuario

Las tecnologías del lado usuario deben ser un suplemento eficaz de las tecnologías del lado red. La información proporcionada por los usuarios puede ofrecer datos detallados sobre los spammer de voz (como se indica en la cláusula 7.3.3.), que es especialmente importante para los operadores. Las tecnologías del lado usuario pueden necesitar la ayuda de ciertas características de los teléfonos inteligentes (smartphone), cuyo soporte puede variar en función del fabricante.

7.3.1 Listas blancas/listas negras

En los teléfonos, los usuarios pueden activar el control de conexión para bloquear determinados números o segmentos de números, como si fuera una lista negra, al tiempo que esta función permite

que determinados números (definidos por el usuario o sincronizados por algunas aplicaciones móviles) siempre se conecten, como si figuraran en una lista blanca.

Este método puede funcionar como una lista blanca/negra cuando la sincronización depende del lado red, mientras que el lado usuario suele estar sujeto a preferencias personales, pues los usuarios pueden definir sus propias listas.

7.3.2 Retardo de llamada

El retardo de llamada es una técnica de señalización que funciona específicamente para las llamadas silenciosas (véase la cláusula 6.2).

Una vez establecido el enlace de señalización entre un llamante y un llamado, el tono de llamada se generará periódicamente desde el enlace. Cuando se produzcan llamadas silenciosas, los usuarios recibirán un silencio ("aire muerto") o un tono de corta duración, que indica que se ha abandonado la llamada.

Con la ayuda de un teléfono inteligente, los usuarios pueden bloquear la llamada silenciosa desde el lado terminal (lado usuario). Dado que los usuarios pueden fijar un valor para la duración del tono (umbral) de todas las llamadas entrantes en la capa de señalización, es posible omitir las llamadas silenciosas, pues la duración del tono será inferior al umbral. Sin embargo, en caso de que ignore la llamada normal con "tono de llamada breve", el registro de llamadas del teléfono móvil consignará la llamada, lo que permitirá al usuario efectuar una verificación.

7.3.3 Retroinformación

Una vez recibido el spam de voz, los usuarios pueden informar a los operadores e indicarles el número del spam de voz y demás información detallada. Los canales de retroinformación incluyen los mensajes de texto, las llamadas telefónicas, los correos electrónicos o, incluso, el sitio web del departamento de atención al cliente (u otros departamentos equivalentes) de los operadores. Todos los canales deben ofrecer un procedimiento cómodo y fácil para que los usuarios faciliten tal información. Es posible crear con aplicaciones un anal de fácil utilización en los terminales o tarjetas de módulo de identidad de abonado (SIM) y en plataformas como la plataforma de gestión de dispositivos (DMP) y la plataforma radioeléctrica (OTAP) de la red.

Además, una vez recibida esa información por el departamento de atención al cliente de los operadores, un auditor autorizado debe verificar que tal información es real y efectiva, y aplicar un procedimiento similar a la verificación interactiva antes de tomar las medidas que procedan. De disponerse de una grabación vocal en el VMS, si el propietario autoriza el acceso a esa grabación, la verificación puede ser más efectiva y eficaz.

7.4 Mecanismo de colaboración

Los operadores pueden cooperar con entidades de gestión, otros operadores o usuarios para establecer algún tipo de cooperación y comunicación a fin de luchar contra el spam de voz.

Los operadores pueden crear y soportar un sistema de compartición de la información (ISS). Este sistema concreto puede abarcar los intercambios de información sobre spam de voz básico con otras organizaciones, incluidas la lista de spammer presuntos/verificados, la clasificación de cada spam de voz y las tecnologías de lucha contra el spam, etc.

Las entidades de gestión pueden considerar la posibilidad de aplicar un ISS y crear un mecanismo de intercambio de la información, o incluso organizar reuniones formales con operadores y organizaciones independientes para compartir información actualizada.

Los usuarios pueden compartir sus listas negras con el servidor en el lado red telecargando o descargando las listas negras. Sin embargo, los operadores deben disponer de un mecanismo de verificación a través del cual detectar si un elemento en una lista negra personal es realmente un spammer de voz. Los operadores deben ofrecer una interfaz para la telecarga y descarga de listas

negras. Este mecanismo puede interactuar con la información facilitada por los clientes. Entre tanto, las entidades de gestión deben auditar la información actualizada para evitar la información inapropiada.

A fin de implantar un mecanismo de compartición de la información, los operadores pueden presentar periódicamente las listas negras verificadas a las entidades de gestión y bloquear las listas negras impuestas por las entidades de gestión.

Además, las entidades de gestión pueden refundir todas las listas negras recibidas de todos los operadores y aplicar las medidas y procedimientos del caso. Por otra parte, las entidades de gestión pueden asumir más responsabilidades, como la reducción del spam de voz en la fuente, asegurándose al mismo tiempo de que los operadores cumplen con sus obligaciones.

7.5 Soluciones propuestas

Ninguna solución anteriormente mencionada puede ser enteramente satisfactoria por su cuenta. Para luchar eficazmente contra el spam de voz, se han de utilizar en cada procedimiento tecnologías del lado red y del lado usuario de manera global.

Para obtener una mayor precisión, se pueden integrar en el registro de señalización varias fuentes de datos, pero una fuente de datos global sería extremadamente onerosa.

Se han de considerar las siguientes situaciones.

En primer lugar, puede optarse únicamente por registros de señalización SS7 (véase la cláusula 7.2.1.), pues, contrariamente a otras fuentes de datos esta señalización obtiene los datos de todos los enlaces de señalización a fin de garantizar la eficacia de la lucha contra el spam de voz.

Por otra parte, un sistema de recopilación de datos basado en IN, CRBT o VMS puede ser una alternativa efectiva en cuanto a los costos, si los operadores ya ofrecen servicios IN, CRBT o VMS. Sin embargo, tal como se mencionó en la cláusula 7.2.1, de las redes CRBT o IN no se pueden obtener todos los datos, por lo que los datos obtenidos de estos servicios pueden servir de complemento.

El modelo propuesto en la cláusula 7.2.2 es fácil de utilizar y no es oneroso. Además, es el más comúnmente utilizado para luchar contra el spam de voz. Para aumentar la precisión del análisis, se pueden utilizar modelos normales y algoritmos más sofisticados. Por ejemplo, las estadísticas sobre los códigos de causa de abandono de llamada y las estadísticas sobre los códigos de llamadas rechazadas pueden reducir notablemente la lista de sospechosos.

Sin embargo, modelos normales o algoritmos globales pueden llevar a un sistema con un elevado grado de complejidad y procedimientos largos de aplicar, lo que, a su vez, aumentará el retardo del procedimiento de lucha contra el spam de voz en su conjunto y reducir la satisfacción del cliente. Habida cuenta de todo lo anterior, los operadores han de elegir cuidadosamente los modelos normales o algoritmos que aplicarán.

El procedimiento de verificación interactiva puede variar de un país a otro, por lo que las entidades de gestión podrán ayudar a los operadores a establecer el procedimiento de verificación adecuado en función de las prácticas habituales del país.

Como puede deducirse del procedimiento de control descrito en la cláusula 7.2.4., conviene que los métodos del lado usuario y del lado red estén mejor integrados para reducir el volumen del spam de voz. El departamento de atención al cliente de los operadores puede desempeñar un papel importante en el procedimiento de control y en la satisfacción de las peticiones de los clientes.

Anexo A

Medidas interactivas y técnicas contra el spam

(El presente anexo es parte integrante de la Recomendación.)

Resumen

En este anexo se presenta una visión general de los procesos destinados a luchar contra las llamadas spam y se propone una base técnica para contrarrestar dicho tipo de llamadas a partir de números (específicamente asignados por el operador de telecomunicaciones) a los que se llama inmediatamente después de haber recibido una llamada spam. En este marco se determina que el operador o los operadores tienen que tener un número o números contra spam especiales, así como funciones para diferentes niveles de procesamiento de registros detallados de llamadas para estos números. Además, en este anexo se presentan mecanismos de intercambio de información para luchar contra el spam en el marco de la interacción entre operadores.

También se presentan la base técnica para luchar contra el spam cuando un abonado notifica al operador la recepción de una llamada spam mediante una llamada breve a un número contra spam inmediatamente después de haber recibido esa llamada spam. El presente anexo se aplica al servicio de llamada de voz, el servicio de mensajes breves (SMS) y el servicio de mensajería multimedios (MMS).

Posibilidad de servicio interactivo de notificación para la interacción de un abonado con un operador de telecomunicaciones/proveedor de servicio para luchar contra el *spam* en terminales telefónicos

En [UIT-T X.1247] se introduce el concepto de mecanismos de notificación del usuario y de informes de usuario utilizados en el procesamiento de los mensajes spam.

En la Recomendación UIT-T X.1246 se presentan diversos mecanismos interactivos de verificación y procesamiento del spam.

Un mecanismo interactivo, descrito a continuación, complementa y amplía los actuales procedimientos de la parte principal de esta Recomendación (UIT-T X.1246) y [UIT-T X.1247]. La interacción propuesta del abonado/destinatario de una llamada spam con un operador/proveedor de servicio consiste en que el abonado efectúa una llamada corta a un número concreto de este operador/proveedor de servicio o reenvía a ese número el mensaje spam que ha recibido.

A.1 Caso de utilización/algoritmo/posibilidad de notificación interactiva

La posibilidad de utilizar una llamada a un número contra spam para notificar una llamada spam mediante el procesamiento automático de información de CDR/CLI consta de los siguientes pasos:

1 El destinatario/cliente/abonado recibe una llamada que identifica/define como llamada spam o posible llamada spam (spam de voz, spam en SMS o spam en MMS).

2 Se almacenan los CDR/CLI de esta llamada (así como sobre cualquier otra llamada) en el sistema de gestión de telecomunicaciones (o en otros sistemas) del operador de telecomunicaciones. En los CDRn/CLIn figura la identificación del llamante (posible fuente de la llamada spam), la identificación del receptor de la llamada (receptor de la llamada spam) y el momento de la llamada.

3 Inmediatamente, o tan pronto como sea posible, después de finalizar esta llamada, su destinatario/cliente/abonado marca un número especial contra spam definido previamente por su proveedor de servicio de base/proveedor de servicio propio/operador de telecomunicaciones (según la reglamentación nacional dicho número puede ser único en el país o único para cada operador), es decir, efectúa una llamada a un número contra spam como informe de usuario interactivo.

4 Los CDRn+1/CLIn+1 sobre esta llamada se almacenan también en el sistema de gestión de telecomunicaciones del operador.

5 El operador, al recibir dicha llamada del abonado al número contra spam, captura toda la información técnica CDRn+1 (CDR y CLI con diversos grados de detalle), localiza automáticamente la anterior llamada CDRn entrante al abonado/destinatario (posible llamada spam), y comienza a recopilar información sobre sobre su emisor (si hace falta, intercambiando esa información con otros operadores/reguladores).

6 Si la llamada al número contra spam fue una llamada única y/o errónea, puede que no sea necesario tomar más medidas.

7 Si hay varias llamadas al número contra spam procedentes de diversos destinatarios de posibles llamadas spam y, en cada caso, el sistema de procesamiento CDR determina que se trata del mismo número llamante, o de la CLIn de la última llamada entrante al abonado/usuario antes de que este llamase al número contra spam, habrá una mayor probabilidad de detectar la fuente real de las llamadas spam para encontrar al spammer.

8 Existe la opción de fijar diversos umbrales para que los sistemas de procesamiento de CDR eliminen falsas alarmas.

A.2 Requisitos técnicos

A.2.1 Para recibir llamadas de notificación del receptor, el operador de telecomunicaciones/proveedor de servicio debe tener un número especial contra spam.

A.2.2 Para procesar gran cantidad de número de llamadas de notificación, el sistema de gestión de telecomunicaciones del operador/proveedor de servicio debe tener la posibilidad de recibir y procesar estas llamadas basándose completamente en detalles CLI de nivel inferior y CDR.

A.2.3 El sistema de gestión de las telecomunicaciones debe disponer de datos estadísticos del servicio de notificación de calidad de servicio (QoS).

Apéndice I

Medidas globales de lucha contra el spam de voz

(Este apéndice no forma parte integrante de la presente Recomendación.)

La Figura I.1 muestra las soluciones técnicas y no técnicas para luchar contra el spam de voz. Dado que la lucha contra el spam de voz es un problema técnico complejo, pueden aplicarse al mismo tiempo varios métodos:

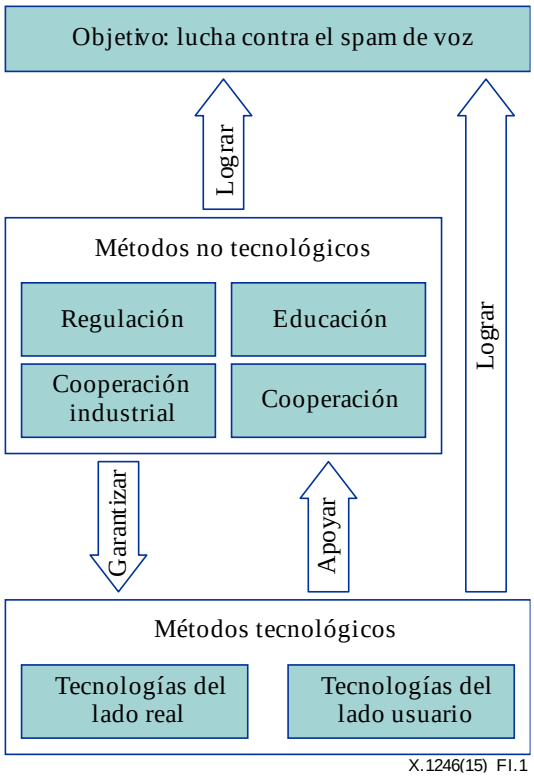

Figura I.1 – Estructura de la lucha contra el spam de voz

– La reglamentación puede contribuir a proteger a usuarios y operadores contra el spam de voz.

– La cooperación industrial es necesaria para que los participantes industriales elaboren y apliquen las distintas tecnologías adecuadas.

– La cooperación puede ayudar a operadores y entidades de gestión a compartir información sobre la adopción efectiva de la reglamentación y la evolución tecnológica.

– La educación es importante para que los usuarios minimicen las pérdidas económicas causadas por el spam de voz.

Apéndice II

Sugerencia para la verificación interactiva

(Este apéndice no forma parte integrante de la presente Recomendación.)

En términos generales, toda verificación interactiva implica la marcación del número llamante sospechoso, la grabación del tono de devolución de llamada antes de la conexión y de la voz después de la conexión. Posteriormente se audita el contenido para verificar si se trata o no de spam de voz. Si todos estos pasos se realizan manualmente, los recursos humanos de los operadores se agotarían rápidamente. Por consiguiente, se ha de considerar un método optimizado para equilibrar los gastos.

La verificación interactiva puede realizarse de manera centralizada en lo que respecta a los registros de marcación y la auditoría semiautomática de las grabaciones de voz de los presuntos spammer de voz, que pueden encontrarse repartidos por todos los rincones de la red.

El método centralizado se ocupa automáticamente de la marcación y la grabación y permite a los auditores escuchar únicamente las grabaciones de voz sin ruido blanco ni demás tonos de devolución de llamada inútiles.

Apéndice III

Consideraciones políticas de la lucha contra el spam de voz

(Este apéndice no forma parte integrante de la presente Recomendación.)

El spam de voz es una herramienta peligrosa utilizada para la publicidad, el fraude, el acoso, etc., que puede utilizarse en las comunicaciones cotidianas. Para luchar eficazmente contra el spam de voz se han de considerar distintos enfoques en función de las características de los grupos participantes, por lo que en esta Recomendación se presentan distintos tipos de tecnologías. Tales grupos pueden ser los usuarios (o abonados), los operadores, las entidades de gestión y las organizaciones independientes. En este apéndice se presentan los distintos aspectos de los grupos participantes que se habrán de tener en cuenta a la hora de luchar contra el spam de voz.

III.1 Usuarios

Los usuarios son en último término las víctimas de la cadena de comunicación de spam de voz por lo que están muy motivados por bloquear el spam. Así, los usuarios han de aplicar determinados métodos dentro del proceso de lucha contra el spam. A continuación se presentan diversas sugerencias, que deberán adaptarse a cada situación determinada:

– De ser posible, los usuarios deben instalar en sus dispositivos, como los teléfonos inteligentes, aplicaciones antispam. Para lograr una mayor eficacia, estas aplicaciones deben estar actualizadas.

– Los usuarios deben comunicar a los operadores de telecomunicaciones o a las organizaciones independientes toda la información detallada que posean sobre los spammer de voz tan pronto como reciban el spam de voz.

– Los usuarios han de ser mucho más precavidos en sus comunicaciones cotidianas y proteger su información personal contra los spammer.

III.2 Operadores

Los operadores son una parte importante del procedimiento de lucha contra el spam de voz. Dado que el spam de voz puede reducir notablemente la satisfacción de los usuarios y malgastar de manera importante los recursos de la red, los operadores han de conocer el fenómeno y aplicar soluciones para proteger sus redes y ofrecer mejores servicios. Algunas de éstas serían:

– Los operadores deben supervisor toda la red de comunicaciones para detectar posibles spam de voz, que pueden causar transmisiones de señalización o patrones de tráfico anormales.

– Los operadores deben preinstalar la versión más reciente de las aplicaciones antispam en todos los dispositivos que pueden ser objetivo de spam de voz a través sus propios canales de distribución o venta. En lo que respecta a los canales de distribución de terceros, los operadores han de garantizar que todos los dispositivos están totalmente protegidos por aplicaciones actualizadas.

– Los operadores han de realizar campañas de formación e información, e instar a los usuarios a comunicar la información detallada sobre los spammer de voz a organizaciones independientes. Esto puede lograrse con programas de incentivación.

– Los operadores debe establecer alianzas con las entidades de gestión y las organizaciones independientes para consolidar sus esfuerzos de lucha contra el spam de voz.

III.3 Entidades de gestión y organizaciones independientes

Las entidades de gestión y las organizaciones independientes pueden supervisar o guiar a los operadores directamente e, incluso, prestarles los refuerzos necesarios.

– Las entidades de gestión y las organizaciones independientes pueden formar a los usuarios y operadores para luchar contra el spam de voz, o llevar a cabo campañas de formación e información.

– Las entidades de gestión y las organizaciones independientes pueden estudiar más detalladamente las tendencias de spam de voz y procurar encontrar métodos o tecnologías de lucha más eficaces contra los últimos patrones de spam de voz.

– Las entidades de gestión y las organizaciones independientes deben desatascar los canales publicitarios y promocionales para normalizar el actual entorno de comunicaciones vocales, o regular los sistemas de marcación publicitarios de las entidades promocionales.

– Las entidades de gestión y las organizaciones independientes deben compartir las listas negras más actualizadas con los operadores e, incluso, con los usuarios. Estas listas negras se mantendrán con la colaboración de operadores y usuarios.

– Las entidades de gestión deben crear los recursos propicios para fortalecer la lucha contra el spam de voz a fin de proteger los beneficios que forman parte de la oferta comercial de los usuarios.

Bibliografía

[b-ITU-T E.370] Recomendación UIT-T E.370 (2001), *Principios de servicio aplicables al interfuncionamiento entre las redes públicas de telecomunicaciones internacionales con conmutación de circuitos y las redes basadas en el protocolo Internet.*

[b-ITU-T M.60] Recomendación UIT-T M.60 (1993), *Terminología y definiciones relativas al mantenimiento*

[b-ITU-T M.1400] Recomendación UIT-T M.1400 (2015), *Designaciones para interconexiones entre operadores de red.*

[b-ITU-T X.1231] Recomendación UIT-T X.1231 (2008), *Estrategias técnicas contra el correo basura.*

[b-ITU-T X.1242] Recomendación UIT-T X.1242 (2009), *Sistema de filtrado de correo basura en el servicio de mensajes cortos (SMS) basado en reglas especificadas por el usuarios.*

[b-ITU-T X.1245] Recomendación UIT-T X.1245 (2010), *Marco de aplicaciones multimedios IP para la lucha contra el correo basura.*

[b-ITU-T Y.1001] Recomendación UIT-T Y.1001 (2000), *Marco de protocolo Internet – Marco para la convergencia de tecnologías de redes de telecomunicaciones y de redes de protocolo Internet.*

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

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	**Redes de datos, comunicaciones de sistemas abiertos y seguridad**
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2022