

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1244

(09/2008)

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

Seguridad en el ciberespacio – Lucha contra el correo
basura

**Características generales de la lucha contra el
correo basura (spam) en aplicaciones
multimedios basadas en IP**

Recomendación UIT-T X.1244

UIT-T



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
GESTIÓN DE INTERCONEXIÓN 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	X.1140–X.1149
Protocolos de seguridad	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	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339

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

Recomendación UIT-T X.1244

Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP

Resumen

La Recomendación X.1244 especifica los conceptos y características básicos de los correos basura (spam) y las cuestiones técnicas relacionadas con la lucha contra los mismos en aplicaciones multimedios IP, como la telefonía IP, la mensajería instantánea, etc. Se establece una clasificación de los tipos de spam que pueden darse en las distintas aplicaciones multimedios IP y cada tipo se describe según sus características. En esta Recomendación se exponen diferentes amenazas de seguridad que puede conllevar spam en las citadas aplicaciones IP. Se han desarrollado varias técnicas para controlar el spam de correo electrónico, que se ha convertido en un problema social. Algunas de estas técnicas pueden emplearse para luchar contra el spam en las aplicaciones multimedios IP. En esta Recomendación se analizan los mecanismos de lucha contra el spam convencional y se argumenta su aplicabilidad al spam en aplicaciones multimedios IP. Por último, se tratan diversos factores que habrán de tenerse en cuenta en la lucha contra el spam en dichas aplicaciones.

Orígenes

La Recomendación UIT-T X.1244 fue aprobada el 19 de septiembre de 2008 por la Comisión de Estudio 17 (2005-2008) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

Palabras clave

Spam en mensajería instantánea, spam en aplicaciones multimedios IP, spam, spam en voz sobre IP.

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 propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección <http://www.itu.int/ITU-T/ipr/>.

© UIT 2009

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

	Página
1 Alcance	1
2 Referencias	1
3 Definiciones.....	1
3.1 Términos definidos en otros documentos.....	1
3.2 Términos definidos en esta Recomendación	2
4 Abreviaturas y acrónimos	3
5 Convenios	4
6 Concepto y tipos habituales de spam multimedios IP	4
6.1 Spam en VoIP.....	5
6.2 Spam multimedios IP	5
6.3 Spam en mensajería instantánea.....	5
6.4 Spam en charla	6
6.5 Spam multimodal.....	6
6.6 Spam en el servicio de compartición de ficheros P2P.....	6
6.7 Spam en direcciones web	7
7 Clasificación del spam multimedios IP	7
7.1 Spam de voz en tiempo real.....	8
7.2 Spam de texto en tiempo real	8
7.3 Spam de vídeo en tiempo real	9
7.4 Spam de voz en tiempo no real.....	9
7.5 Spam de texto en tiempo no real	9
7.6 Spam de vídeo en tiempo no real	10
8 Consideraciones técnicas de la lucha contra el spam multimedios IP.....	10
8.1 Creación y entrega de spam.....	10
8.2 Detección y filtrado de spam.....	12
8.3 Medidas aplicables al spam recibido	12
9 Amenazas de seguridad relacionadas con el spam	13
9.1 Amenazas de seguridad relacionadas con el spam	13
9.2 Clasificación de las amenazas de seguridad de spam.....	15
9.3 Contramedidas.....	16
10 Aplicabilidad de mecanismos bien conocidos en la lucha contra el spam a las aplicaciones multimedios IP.....	17
10.1 Filtrado de identificación.....	17
10.2 Enmascaramiento de dirección.....	19
10.3 Prueba interactiva humana	20
10.4 Filtrado de contenido.....	20
10.5 Autenticación por intercambio de claves	21
10.6 Filtrado de spam en red	22

	Página
10.7 Sello en línea	23
10.8 Filtrado de spam por autorización	23
10.9 Medidas jurídicas y reglamentos	24
11 Consideraciones para la lucha contra el spam en aplicaciones multimedios IP	24
11.1 Usuario del servicio (abonado al servicio)	25
11.2 Proveedor de servicios.....	25
11.3 Operador de red	26
11.4 Organización pública.....	27
11.5 Otras consideraciones	27

Introducción

Los correos basura (spam) han supuesto un problema social en los sistemas de correo electrónico de red. Se han desarrollado varias soluciones, que se han aplicado a fin de resolver el problema, pero ninguna de ellas lo ha conseguido realmente. Las aplicaciones multimedios IP están compuestas por diversos tipos de servicios, como la telefonía IP, la mensajería instantánea, etc. Estos servicios multimedios IP están convirtiéndose en el objetivo de los emisores spam, pues es técnicamente más sencillo y más económico enviar los mensajes a estos servicios. Es necesario abordar el problema del spam en las aplicaciones multimedios IP antes de que se convierta en un problema de orden público.

En esta Recomendación se describen los conceptos y características de los diversos tipos de spam que pueden recibir las aplicaciones multimedios IP. Algunas de las cuestiones se tratan desde el punto de vista técnico y de seguridad para luchar contra el spam en las aplicaciones multimedios IP, por lo que se exponen algunos aspectos que han de tener en cuenta los diversos participantes en estos servicios, como los proveedores de servicio, los usuarios del servicio, etc. a la hora de luchar contra el spam en dichas aplicaciones.

Recomendación UIT-T X.1244

Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP

1 Alcance

Esta Recomendación proporciona una visión general de los correos basura (spam) multimedios IP, centrándose en los siguientes temas:

- Concepto y las características del spam multimedios IP.
- Cuestiones técnicas relacionadas con el spam multimedios IP.
- Amenazas de seguridad que representa el spam.
- Métodos habituales de lucha contra el spam y basadas en su aplicabilidad al spam multimedios IP.
- Diversos aspectos que han de tenerse en cuenta en la lucha contra el spam en aplicaciones multimedios IP.

NOTA – El término "identidad" en esta Recomendación no ha de entenderse con su significado absoluto. En concreto, no constituye una validación positiva.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

Esta Recomendación utiliza los siguientes términos definidos en otros documentos:

3.1.1 lista de control de acceso (ACL, *access control list*) [b-UIT-T X.741]: El atributo lista de control de acceso se utiliza para contener identidades de iniciadores a los que se permite o se les niega específicamente el acceso a la información de gestión.

3.1.2 autoridad de certificación (CA, *certification authority*) [b-UIT-T X.509]: Autoridad a la cual uno o más usuarios han confiado la creación y asignación de certificados de clave pública. Facultativamente, la autoridad de certificación puede crear las claves de los usuarios.

3.1.3 conferencia [b-UIT-T T.124]: Serie de nodos unidos entre sí y que son capaces de intercambiar información audiógráfica y audiovisual a través de redes de comunicación diversas.

3.1.4 correo identificado por claves de dominio (DKIM, *DomainKeys identified mail*) [b-IETF RFC 4871]: Mecanismo mediante el cual los mensajes de correo electrónico pueden firmarse criptográficamente, permitiendo así a un dominio de firma reclamar la responsabilidad de introducción del mensaje en el flujo de correo. Los receptores del mensaje pueden verificar la firma solicitando directamente al dominio del firmante la extracción de la correspondiente clave pública, lo que confirma que el mensaje procede de una parte que posee la clave privada del dominio de firma.

3.1.5 mensajería instantánea (IM, *instant messaging*) [b-IETF RFC 3428]: Intercambio de contenido entre un grupo de usuarios en tiempo casi real. Por norma general, el contenido son mensajes de texto breves, aunque no necesariamente.

3.1.6 relación par a par (P2P, *peer-to-peer relation ship*) [b-UIT-T T.180]: En una relación par a par, los usuarios pueden negociar las características de su interacción y, posteriormente,

comunicar ateniéndose a las reglas que han negociado; ambos usuarios (una entidad y su entidad par) tienen potencialmente los mismos derechos. [b-IETF RFC 4981] indica que las redes P2P son las que tienen características de árbol: autoorganización, comunicación simétrica y control distribuido.

3.1.7 privacidad bastante buena (PGP, *pretty good privacy*) [b-IETF RFC 1991]: PGP utiliza una combinación de clave pública y encriptación convencional para prestar servicios de seguridad a los mensajes de correo electrónico y los ficheros de datos. Estos servicios comprenden la confidencialidad y la firma digital. PGP fue creada por Philip Zimmermann, y su primera versión, Versión 1.0, se lanzó en 1991. Las siguientes versiones, por ejemplo, open PGP, (PGP abierta) se describen en [b-IETF RFC 4880] y han sido diseñadas y aplicadas por una serie de voluntarios dirigidos por Philip Zimmermann. *PGP y Pretty Good Privacy son marcas registradas por Philip Zimmermann.*

3.1.8 infraestructura de clave pública (PKI, *public key infrastructure*) [b-UIT-T X.509]: Infraestructura capaz de soportar la gestión de claves públicas para los servicios de autenticación, criptación, integridad, o no repudio.

3.1.9 seguridad de la capa de transporte (TLS, *transport layer security*) [b-UIT-T Q.814]: El protocolo TLS proporciona opcionalmente privacidad en las comunicaciones. El protocolo permite aplicaciones de cliente/servidor para comunicar de manera concebida para evitar escucha indiscreta, maniobras fraudulentas e intrusión. El protocolo TLS también proporciona autenticación de pares rigurosa e integridad del flujo de datos.

3.2 Términos definidos en esta Recomendación

Esta Recomendación define los siguientes términos:

3.2.1 spam cebo: Su nombre se deriva de la analogía de la pesca ("fishing" y "phishing" (véase la cláusula 3.2.10)); el spam cebo es una variedad de mensaje basura que incluye un elemento (por ejemplo, un correo electrónico con un enlace incluido) para engañar a los usuarios. El usuario engañado se ve atacado por el spam cebo.

3.2.2 blog (bitácora): Contracción de "web log"; un blog en una lista en línea, posiblemente multimedios, con los intereses personales de su propietario y disponible al público en general para su lectura y, a veces, participación.

3.2.3 bot: Bot es una contracción de "robot", que es un programa que funciona ante el usuario u otro programa como un agente para simular una actividad humana.

3.2.4 envenenamiento de la cache DNS: El envenenamiento de la cache DNS es una técnica que hace creer al servidor de nombres de dominio (servidor DNS) que la dirección DNS de un determinado servidor se ha modificado, cuando en realidad no es cierto. Una vez envenenado el servidor DNS, la información permanece en la memoria cache durante un cierto tiempo, expandiéndose así el efecto del ataque a los usuarios del servidor.

3.2.5 mensaje multimedios IP: Mensaje de texto, voz o vídeo que se entrega y almacena en un terminal multimedios IP o un servidor para que el receptor lo consulte más adelante. Se asemeja al correo vocal del servicio de telefonía, pero se realiza a través de un servicio multimedios IP.

3.2.6 spam multimedios IP: Mensajes o llamadas no solicitadas que se reciben a través de aplicaciones multimedios IP. Para diferenciarlo del spam en correo electrónico tradicional, el spam multimedios IP se envía por nuevos métodos de telecomunicación que utilizan IP, como la mensajería instantánea (IM), presencia o voz sobre IP (VoIP).

3.2.7 modalidad: De manera general, este término se refiere a las formas, protocolos o condiciones que rodean las comunicaciones formales. En el contexto de esta Recomendación, hace referencia a la(s) codificación(es) de información que contienen información perceptible para el ser humano. Ejemplos: la modalidad comprende datos de texto, gráficos, de audio, de vídeo u hápticos

que se utilizan en las interfaces hombre-ordenador. La información multimodal puede proceder o dirigirse a dispositivos multimodales. Como ejemplos de interfaces hombre-ordenador pueden citarse los micrófonos para la voz (entrada de sonido), bolígrafos para las entradas hápticas, teclado para las entradas textuales, ratón para las entradas de movimiento, altavoces para la salida de voz sintetizada, pantallas para la salida de gráficos/texto, dispositivos vibradores para respuesta háptica y dispositivos Braille para los invidentes.

3.2.8 mensaje multimodal: Mensaje multimedios que contiene información con diversas codificaciones para la interacción a través de múltiples modalidades. Por ejemplo, un MMS (servicio de mensajería multimedios) puede transportar modalidades de texto, gráficos y audio. Una página web también puede tener contenido modal multimedios, como texto y vídeo. De forma similar, un correo electrónico puede tener un anexo gráfico además del texto. La multimodalidad permite al usuario seleccionar la modalidad que prefiera en función del entorno, la conveniencia o el contenido.

3.2.9 juego en línea: Juego en tiempo real que se juega a través de la red.

3.2.10 phishing (usurpación de identidad): Intento de adquirir de manera fraudulenta y delictiva información sensible, como nombres de usuario, contraseñas y datos bancarios, mediante la suplantación de una entidad fiable en las comunicaciones electrónicas.

3.2.11 pirateo de sesión: Mecanismo de robo de una sesión de usuario válida para obtener acceso no autorizado a información o servicios.

3.2.12 spam en mensajería instantánea (SPIM, *spam over instant messaging*): Spam cuyo objetivo son los usuarios de un servicio de mensajería instantánea.

3.2.13 spam en telefonía Internet (SPIT, *spam over Internet telephony*): Spam cuyo objetivo son los usuarios de un servicio de telefonía Internet.

3.2.14 spammer: Emisor de spam.

3.2.15 spammings: Cadena de actividades que realizan los spammers para enviar el spam, como elaboración de lista de objetivos, creación del spam, entrega del spam, etc.

3.2.16 spimmer: Emisor de SPIM.

3.2.17 spitter: Emisor de SPIT.

3.2.18 contenido creado por el usuario (UCC, *user created content*): Toda forma de contenido, como vídeo, blog, imágenes, audio, etc. creado por los usuarios finales (público en general) para ponerlo a disposición de todo el mundo.

3.2.19 contenido generado por el usuario (UGC, *user generated content*): Equivalente al UCC.

3.2.20 vishing (sustracción de información personal por VoIP): Método ilegal de acceder a información personal y financiera privada a través del servicio de voz sobre IP (VoIP). El término vishing es una contracción de "voz" y "phishing".

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos:

ACL	Lista de control de acceso (<i>access control list</i>)
APEC	Cooperación Económica Asia-Pacífico (<i>Asia-Pacific Economic Cooperation</i>)
ARP	Protocolo de resolución de dirección (<i>address resolution protocol</i>)
ASCII	Código de la norma americana para el intercambio de información (<i>american standard code for information interchange</i>)
CA	Autoridad de certificación (<i>certificate authority</i>)

DB	Base de datos (<i>database</i>)
DKIM	Correo identificado por claves de dominio (<i>DomainKeys identified mail</i>)
HTTP	Protocolo de transferencia de hipertexto (<i>HyperText transfer protocol</i>)
IM	Mensajería instantánea (<i>instant messaging</i>)
IP	Protocolo Internet (<i>Internet protocol</i>)
IPTV	Televisión por el protocolo Internet (<i>Internet protocol television</i>)
IPv4	Protocolo Internet version 4 (<i>Internet protocol version 4</i>)
IPv6	Protocolo Internet version 6 (<i>Internet protocol version 6</i>)
IRC	Charla interactiva Internet (<i>Internet relay chat</i>)
ISP	Proveedor de servicio Internet (<i>Internet service provider</i>)
ITSP	Proveedor de servicio de telefonía Internet (<i>Internet telephony service provider</i>)
IVR	Respuesta vocal interactiva (<i>interactive voice response</i>)
MAC	Control de acceso a medios (<i>media access control</i>)
MIPv4	IPv4 móvil (<i>mobile IPv4</i>)
MIPv6	IPv6 móvil (<i>mobile IPv6</i>)
NDP	Protocolo de descubrimiento de vecino (<i>neighbour discovery protocol</i>)
OS	Sistema operativo (<i>operating system</i>)
P2P	Par a par (<i>peer-to-peer</i>)
PGP	Privacidad bastante buena (<i>Pretty Good Privacy</i>)
PKI	Infraestructura de clave pública (<i>public key infrastructure</i>)
RTPC	Red telefónica pública conmutada
RTP	Protocolo de transporte en tiempo real (<i>real-time transport protocol</i>)
SMS	Servicio de mensajes breves (<i>short message service</i>)
SMTP	Protocolo de transferencia de correo simple (<i>simple mail transfer protocol</i>)
SQL	Lenguaje de indagación estructurado (<i>structured query language</i>)
TCP	Protocolo de control de transmisión (<i>transmission control protocol</i>)
TLS	Seguridad de la capa de transporte (<i>transport layer security</i>)
URI	Identificador uniforme de recurso (<i>uniform resource identifier</i>)
URL	Localizador uniforme de recurso (<i>uniform resource locator</i>)
VoD	Vídeo a la carta (<i>video on demand</i>)
VoIP	Voz sobre IP (<i>voice over IP</i>)

5 Convenios

Ninguno.

6 Concepto y tipos habituales de spam multimedia IP

Aunque no existe una definición acordada a nivel mundial para el spam, este término se suele utilizar para designar el flujo masivo de telecomunicaciones electrónicas no solicitadas por correo

electrónico o mensajería móvil con fines publicitarios. En la actualidad, el spam no se limita al correo electrónico o la mensajería móvil, sino que está llegando a las aplicaciones multimedios IP, como la VoIP y la mensajería instantánea. Puede definirse el spam multimedios IP como el flujo masivo de telecomunicaciones electrónicas no solicitadas por aplicaciones multimedios IP con fines publicitarios. El spam puede darse en distintas aplicaciones multimedios IP, como la VoIP y la mensajería instantánea.

En esta cláusula se presentan algunos de los tipos más habituales de spam multimedios IP que pueden sufrir las aplicaciones multimedios IP. Se presenta una descripción de sus características para cada tipo de spam.

6.1 Spam en VoIP

El spam en VoIP es el que se da en los servicios de VoIP. El spam en VoIP es un spam vocal en tiempo real, como el telemarketing, que incluye comunicaciones con la persona que lo realiza y con sistemas IVR (respuesta vocal interactiva). Como cada vez hay más servicios de telemarketing que utilizan el servicio VoIP debido al rápido desarrollo de este servicio en todo el mundo, la amenaza del spam en VoIP también está aumentando. Especialmente no resulta difícil efectuar un número ingente de llamadas. Es posible reducir el precio de la mano de obra contratando agentes en otros países con costes menores que el país objetivo, pues el precio de la llamada internacional ha disminuido de forma espectacular mediante la utilización del servicio VoIP es mucho más reducido. A los spammer les resulta más sencillo obtener información sobre los usuarios de las aplicaciones multimedios IP. Gracias a estas ventajas, el spam en VoIP puede revelarse como una amenaza para los proveedores y usuarios del servicio VoIP.

6.2 Spam multimedios IP

El mensaje multimedios IP es un mensaje de texto, voz o vídeo que se entrega a terminales multimedios IP o servidores, donde se almacena, para que el receptor lo consulte con posterioridad. Es parecido al correo vocal del servicio telefónico, pero se efectúa a través de un servicio multimedios IP. El spam multimedios IP es el que utiliza el servicio de mensajería multimedios IP. El receptor del spam consulta el mensaje y lo elimina igual que lo hace con el correo basura o el spam en mensajería móvil. Muchos terminales de aplicaciones multimedios IP, como los teléfonos VoIP, soportan funciones de mensajería multimedios convirtiéndose así en aplicaciones objetivo para el spammer que envía spam multimedios IP.

El spam multimedios puede ser spam de texto y spam de voz/vídeo. El spam de texto es un mensaje breve que incluye texto publicitario o informativo. Tiene características similares al del spam de correo electrónico o mensajería móvil breve (SMS), pues es textual. No obstante, se supone que el coste de enviar el spam textual sea muy inferior al del spam SMS. El spam de voz/vídeo es un mensaje de voz/vídeo con contenido publicitario o informativo. Se prevé que este tipo de spam aumente con la utilización de aplicaciones multimedios IP. Probablemente ocupe una gran parte del buzón de correo de voz/vídeo de los usuarios de aplicaciones IP o del almacén de los proveedores de servicio IP, pues el tamaño de los mensajes multimedios es mucho mayor que el del textual. El spam multimedios puede utilizarse para introducir software maligno, como gusanos, virus informáticos, programas espía, caballos de Troya, etc.

6.3 Spam en mensajería instantánea

El spam en mensajería instantánea (SPIM, *spam over instant messaging*) es otro amenazante spam en aplicaciones multimedios IP cuyo objetivo son los usuarios del servicio de mensajería instantánea (IM, *instant messaging*). Muchos usuarios recurren al servicio IM para comunicarse cómodamente con otros usuarios en la red. La mayoría del spam en IM son textos breves y se parecen mucho al correo basura, aunque, en este caso, se trata de un mensaje en tiempo real que puede ser más molesto. El spam multimedios también puede afectar a la IM, pues este servicio soporta muchas funciones, además de la entrega de mensajes de texto en tiempo real.

El envío de spam IM puede no ser sencillo sin realizar manipulaciones técnicas ilegales, ya que la mayoría de servicios IM crean listas de amigos autorizados y sólo los usuarios que figuran en una lista pueden enviar mensajes. Sin embargo, una debilidad de los sistemas de seguridad de los servicios IM puede permitir a los spammers robar una lista de amigos o autorizados del objetivo para enviar el spam disfrazado como un miembro de la lista.

Si bien la entrega del mensaje sólo es posible entre usuarios que se encuentren en las listas de amigos, cualquiera puede solicitar su ingreso en ellas. En muchos servicios IM, el mensaje de solicitud de ingreso puede contener un pequeño texto de presentación del solicitante para que el usuario del servicio IM sepa quién es y determine si le ha de permitir el ingreso en la lista de amigos. Un spammer que no figure en la lista de amigos puede enviar el spam gracias a esta función del servicio IM.

6.4 Spam en charla

El spam en charla puede ocurrir en diversas aplicaciones multimedios IP que contienen las funciones charla entre usuarios del servicio. La función charla y la de mensajería figuran en muchas aplicaciones multimedios IP, como los servicios de charla en línea, los servicios de juegos en línea, etc. El spam en charla suele ser un mensaje de texto breve que se envía repetidamente a todos los participantes en la charla. Por consiguiente, algunos servicios de charla y de juegos en línea limitan el número de veces que se puede enviar un mismo mensaje para evitar el spam. No obstante, la eficacia de este método es limitada y se necesitan más medidas para contrarrestar los diversos tipos de spam en charla.

El servicio de charla tiene las mismas características que el servicio IM, pero los tipos de spam que pueden afectarlos son distintos. Un usuario de los servicios IM suele comunicarse con personas de una lista de amigos, que están autorizados a comunicar con dicho usuario. Por tanto, el spammer ha de penetrar en la lista de amigos para enviar el spam. El servicio de charla se realiza en línea y los participantes suelen ser desconocidos. Cualquiera puede participar en el servicio de charla, por lo que el spammer puede ingresar en el servicio para enviar sus mensajes. El tipo de spam que puede encontrarse en los servicios de charla es el envío repetido del mismo mensaje. Por consiguiente, es mucho más sencillo generar spam en un servicio de charla que en un servicio IM.

6.5 Spam multimodal

El problema de seguridad que supone el spam llega hasta las interacciones multimodales, donde un único spam multimedios puede llegar múltiples objetivos en una interfaz de usuario con distintas modalidades. Por ejemplo, un mensaje de red spam puede resultar en la reproducción de un archivo de audio, la visualización de un archivo de vídeo y la aparición de un mensaje de texto en la pantalla, todos con el mismo contenido o con contenidos distintos. Así, la multimodalidad aumenta el riesgo de exposición al spam multimedios, por lo que se prevé que se convierta en un problema mayor a medida que se generalicen las interacciones multimodales.

6.6 Spam en el servicio de compartición de ficheros P2P

El spam en aplicaciones multimedios IP también puede tener como objetivo los usuarios de aplicaciones multimedios de los servicios P2P, como el servicio de compartición de ficheros P2P. Las personas conectadas a redes basadas en IP que utilizan software P2P pueden establecer comunicaciones entre pares para compartir entre ellas diversos ficheros informáticos. En estos servicios, los spammers pueden inducir a otros usuarios a descargar ficheros spam dándoles el nombre de una película conocida, una canción famosa, etc. Los spammers no necesitan tener un objetivo determinado, sino sólo compartir los ficheros para que otros usuarios accedan a ellos. Se supone que muchos ficheros spam descargados van ejecutarse, puesto que el receptor los descarga voluntariamente. Por ende, los daños que puede causar el spam en el servicio P2P es muy grande cuando esos mensajes contienen software maligno, como gusanos y virus, en lugar de contenidos publicitarios.

6.7 Spam en direcciones web

Los spammers pueden colgar artículos o ficheros con contenido publicitario en muchas direcciones web con diversos objetivos. El spam se cuelga en el tablón de anuncios para que muchos visitantes de la dirección web puedan verlo, por ejemplo, respuestas a artículos con contenido publicitario en portales web y blogs pueden ser spam. Además de los artículos de texto, los spammers pueden también telecargar ficheros de audio y vídeo en sitios de compartición de audio/vídeo, como contenido creado por el usuario (UCC), contenido generado por el usuario (UCG) o tabloneros de anuncios para que otros usuarios del servicio vean dichos ficheros publicitarios. El spam en direcciones web puede ser leído o visto por un gran número de usuarios de la dirección. Los spammers no han de fijarse objetivos concretos para hacer envíos masivos.

7 Clasificación del spam multimedios IP

El spam en aplicaciones multimedios IP se clasifica en dos grupos, de acuerdo con sus características. Esta clasificación puede realizarse conforme a diversos criterios, como el tipo de aplicaciones multimedios IP en que aparece el spam, el tipo de medio utilizado para el envío de los mensajes, el protocolo utilizado para la prestación del servicio, el tipo de mensaje de protocolo, etc. En esta cláusula, el spam multimedios IP se clasifica en función de las siguientes características de las aplicaciones multimedios IP, habida cuenta de que pueden utilizarse técnicas antispam adecuadas a cada una de ellas.

- spam multimedios IP en tiempo real y tiempo no real: los servicios de aplicaciones multimedios IP pueden clasificarse según sean en tiempo real o no;
- tipo de medio del spam multimedios IP: un servicio de aplicación multimedios IP puede soportar el texto, la voz, el vídeo o una combinación de ellos. El vídeo comprende la imagen fija y la imagen en movimiento.

En los servicios de aplicación multimedios IP en tiempo real, se establece la comunicación, se entrega el mensaje y el receptor lo consulta en tiempo real. Ejemplos típicos de aplicaciones multimedios IP en tiempo real son el servicio VoIP y el servicio IM. En los servicios de aplicación multimedios IP en tiempo no real, el receptor puede consultar los mensajes cuando le conviene. Ejemplos de aplicaciones multimedios IP en tiempo no real son los servicios web, los servicios P2P, los servicios de juegos en línea, etc. En el cuadro 7-1 se presenta la clasificación de spam en aplicaciones multimedios IP con ejemplos ilustrativos.

Cuadro 7-1 – Clasificación de spam en aplicaciones multimedios IP

	Texto	Voz	Vídeo
Tiempo real	<ul style="list-style-type: none">• Spam en mensajería instantánea• Spam en charla	<ul style="list-style-type: none">• Spam en VoIP• Spam en mensajería instantánea	<ul style="list-style-type: none">• Spam en mensajería instantánea
Tiempo no real	<ul style="list-style-type: none">• Spam de texto/multimedios• Spam de texto en el servicio de compartición de ficheros P2P• Spam de texto en sitio web	<ul style="list-style-type: none">• Spam de voz/multimedios• Spam de voz en el servicio de compartición de ficheros P2P• Spam de voz en sitio web	<ul style="list-style-type: none">• Spam de vídeo/multimedios• Spam de vídeo en el servicio de compartición de ficheros P2P• Spam de vídeo en el sitio web

7.1 Spam de voz en tiempo real

El spam de voz en tiempo real puede definirse como las comunicaciones vocales en tiempo real no solicitadas con fines publicitarios. Un ejemplo representativo del spam de voz en tiempo real es el spam en VoIP. Este tipo de spam puede ser menos frecuente que el que se sufre en el correo electrónico, pero los daños para un usuario del servicio se consideran mucho mayores. El spam de voz en tiempo real es muy molesto para el receptor. En el servicio de correo electrónico, los usuarios del servicio consultan su correo cuando les conviene, pueden identificar el spam en poco tiempo y eliminarlo sin grandes esfuerzos. Sin embargo, el spam de voz en tiempo real es más intrusivo, pues el receptor ha de responder inmediatamente. Además, lleva más tiempo identificar el mensaje recibido como spam. El spam de voz en tiempo real es más eficaz que el de correo electrónico o SMS móvil. Por lo general, los spammers intentan persuadir al receptor de comprar determinado producto o servicio. En el spam de voz en tiempo real, los agentes de telemarketing intentan convencer al receptor estableciendo una comunicación interactiva, que es mucho más invasiva cuando se compara con el correo electrónico o el SMS, que sólo pueden enviar mensajes o vídeos breves en formato no interactivo. A medida que aumenta la capacidad de persuasión del spam, aumentan también los daños causados. Por tanto, puede considerarse que el spam de voz en tiempo real causa unos daños relativamente elevados, habida cuenta de su volumen.

El spam de voz en tiempo real puede intentar mejorar su eficacia empleando diversos servicios IP suplementarios, además de las comunicaciones vocales básicas. En general, este tipo de spam llega a los receptores a través de terminales que soportan el servicio VoIP. Muchos terminales de este tipo pueden soportar funciones adicionales como mensajería multimedios, videofonía y visualización, además de las comunicaciones vocales, como función por defecto. Los spammers intentan ampliar el efecto del spam combinando el spam de voz en tiempo real con otros servicios de vídeo o texto.

El spam de voz en tiempo real puede ser ilegal o fraudulento cuando sus intenciones son malignas, como ya ocurre en los servicios telefónicos fijos o móviles convencionales. Además, las reducidas tarifas de la VoIP pueden propiciar que el spam en VoIP ilegal sea más activo que en los servicios telefónicos tradicionales. Por ejemplo, los spammers con malas intenciones pueden intentar acceder a información de orden financiero mediante phishing en VoIP, es decir vishing, para obtener ilegalmente información de los usuarios del servicio. También pueden enviar spam cebo para que los receptores utilicen un servicio muy oneroso sin tener intención de hacerlo. Por ejemplo, los spammers pueden utilizar una "máquina automática de un solo tono", que establece una conexión con el receptor del spam y termina la llamada tras uno o dos tonos de llamada o provoca la desconexión tras emitir una palabra corta como "hola". Muchos receptores tenderán a devolver la llamada utilizando el identificador del llamante. Entonces, el receptor se conecta automáticamente a un sistema automático de publicidad o a un servicio muy costoso. Este tipo de spam es más atractivo para el emisor, pues le resulta muy barato. Los spammers pueden utilizar el spam cebo para aprovecharse de la vulnerabilidad de seguridad del sistema VoIP. Por ejemplo, los spammers pueden recurrir a la falsificación para piratear una sesión de llamada VoIP y hacerse pasar por otra persona para conectar al usuario del servicio VoIP con su servicio cuando éste quiere comunicarse con otros usuarios del servicio. Del mismo modo, los receptores pueden recibir distintos tipos de spam cebo en las aplicaciones multimedios IP.

7.2 Spam de texto en tiempo real

El spam de texto en tiempo real puede definirse como los mensajes textuales no solicitados enviados masivamente en tiempo real, por ejemplo, con fines publicitarios. Este tipo de spam puede darse en muchas aplicaciones multimedios IP que soportan la entrega de mensajes de texto en tiempo real entre usuarios del servicio. Las características del spam de texto en tiempo real son semejantes a las del spam de correo electrónico, pues en ambos casos se trata de texto. No obstante, el spam de texto en tiempo real es más molesto que el de correo electrónico, pues interrumpe al

receptor en el momento en que lo recibe. Como ejemplos de spam de texto en tiempo real se pueden citar el spam en IM y el spam en charla.

En muchos servicios de aplicaciones multimedios IP, incluido el servicio IM, el de charla en línea y el de juegos en línea, la función de entrega de mensajes se facilita a los usuarios gratuitamente o a un precio muy reducido. Así, los spammers pueden enviar sus mensajes por muy poco dinero. A menudo los spammers pueden obtener información general o específica de los usuarios del servicio utilizando diversos métodos. Esta información puede resultar más provechosa para los spammers que la que pueden obtener con el spam de correo electrónico enviado a objetivos no específicos.

7.3 Spam de vídeo en tiempo real

El spam de vídeo en tiempo real puede definirse como una comunicación de vídeo en tiempo real no solicitada con fines publicitarios. El vídeo comprende tanto la imagen fija como en movimiento. El spam de vídeo en tiempo real puede darse en los servicios de aplicaciones multimedios IP que soportan la función de telecomunicación de vídeo en tiempo real entre usuarios del servicio.

En las primeras fases, el spam en aplicaciones multimedios IP puede ser mensajes de texto o de voz que se envían sin gran dificultad, tienen un bajo coste y no sobrecargan la red IP. El spam de voz en tiempo real en forma de telemarketing puede representar una gran porción de este tipo de spam. No obstante, con el desarrollo de las tecnologías de compartición y entrega de medios y el aumento de la capacidad de la red, también es posible que aumente la cantidad de spam de vídeo en tiempo real.

7.4 Spam de voz en tiempo no real

El spam de voz en tiempo no real puede definirse como mensajes de voz en tiempo no real no solicitados enviados masivamente con fines publicitarios. El ejemplo más representativo de este tipo de spam son los mensajes vocales grabados.

En muchos casos, el servicio VoIP puede soportar un servicio de mensajería multimedios, como el envío y la recepción de mensajes de texto, audio y vídeo, además de la función de llamada vocal en tiempo real. Los spammers pueden enviar mensajes vocales ya grabados al terminal del usuario utilizando esta función del servicio VoIP. Este tipo de spam causa grandes daños a los usuarios y proveedores del servicio VoIP al ocupar el buzón o almacén de correo vocal, pues estos mensajes vocales son de gran tamaño.

7.5 Spam de texto en tiempo no real

El spam de texto en tiempo no real puede definirse como mensajes de texto en tiempo no real no solicitados enviados masivamente, por ejemplo, con fines publicitarios. Las características de este tipo de spam son semejantes a las del spam de correo electrónico. El spam de texto en tiempo no real puede darse en diversas aplicaciones multimedios IP, pues resulta sencillo crear y entregar mensajes de texto y su coste es normalmente reducido.

El spam de texto en tiempo no real puede llegar a los terminales IP que pueden recibir largos mensajes de texto, como el correo electrónico, o a los teléfonos VoIP, que pueden recibir mensajes de texto breves, como los SMS móviles. También puede afectar a diversos servicios, como la IM y otros servicios en línea. Además de estos tipos de spam de texto que llegan a los usuarios independientemente de su voluntad, hay otros tipos de spam de texto a los que están expuestos los usuarios de servicios IP, como la publicidad en direcciones web. Las características de este tipo de spam son semejantes a las del spam de correo electrónico y para contrarrestarlo se prevé la utilización de las mismas técnicas que ya se aplican al spam de correo electrónico. Es posible que dichas técnicas sean menos efectivas cuanto más corto sea el texto empleado.

7.6 Spam de vídeo en tiempo no real

El spam de vídeo en tiempo no real puede definirse como mensajes de vídeo en tiempo no real no solicitados enviados masivamente, por ejemplo con fines publicitarios. Este tipo de spam puede tener dos formas: los usuarios del servicio IP obtienen o descargan el fichero de vídeo en cuestión o acceden al fichero en forma de vídeo a la carta (VoD, *video on demand*) a través de servicios de aplicación multimedios IP. Hay dos métodos de entrega del spam de vídeo en tiempo no real. Primero, al receptor le pueden llegar ficheros publicitarios enviados por el spammer. La segunda opción es que los usuarios descarguen los ficheros de spam a través de servicios de compartición de ficheros sin conocimiento de que se trata de spam.

Cuando el receptor descarga un fichero de vídeo, el tiempo y esfuerzo invertidos en tal operación pueden ser una pérdida de los mismos para el receptor. Una vez entregado el mensaje de vídeo independientemente de la voluntad del receptor, el spam daña a los usuarios y proveedores del servicio al ocupar el espacio del buzón o el almacén de correo, pues estos mensajes de vídeo suelen ser de gran tamaño.

8 Consideraciones técnicas de la lucha contra el spam multimedios IP

Al igual que ocurre con el spam de correo electrónico o de SMS móvil, lo que sigue es una serie de procedimientos relativos a la creación, envío y lucha contra el spam en los servicios de aplicaciones multimedios IP.

- Creación y entrega del spam.
- Detección y filtrado del spam por el usuario del servicio y/o el proveedor del servicio de aplicaciones multimedios IP.
- Aplicación de medidas contra la recepción de spam.

Antes de establecer un marco técnico para la lucha contra el spam en aplicaciones multimedios IP, es necesario detectar los puntos débiles de la prevención contra el spam en cada uno de los puntos anteriores. Teniendo en cuenta las vulnerabilidades, habrán de describirse los medios técnicos aplicables en cada fase para luchar contra el spam en aplicaciones multimedios IP. A continuación se analiza qué influencia tienen en su creación y entrega. A la hora de estudiar el marco y los medios técnicos aplicables a la lucha contra este tipo de spam, puede resultar útil analizar los puntos que se exponen en esta cláusula para identificar la manera más eficaz de hacerlo.

8.1 Creación y entrega de spam

El supuesto fundamental de la expansión del spam multimedios IP es que su coste ha de ser muy inferior al beneficio que el spammer espera conseguir. En el coste no sólo se considera el gasto monetario, sino también los distintos tipos de recursos, como tiempo, esfuerzo y la dificultad técnica, que conlleva a la creación y entrega de spam multimedios IP. Los factores que intervienen en el coste de la creación y entrega del spam son los siguientes:

- Costo de recopilación de direcciones o números de teléfono de los objetivos: coste que supone la recopilación de direcciones o números de teléfono de los objetivos del spam.
- Costo de creación y entrega del spam: coste que supone para el spammer crear y entregar el spam.

8.1.1 Elaboración de la lista de objetivos

Antes de enviar el spam, en primer lugar es necesario elaborar las listas de objetivos. Los spammers pueden obtener una lista de correos electrónicos objetivo realizando un ataque de diccionario, ejecutando programas de recopilación de direcciones de correo electrónico o accediendo ilegalmente a listas de objetivos sin mucha dificultad. En el caso del spam de SMS móvil, pueden

elaborarse listas de objetivos con simples combinaciones de números, dada la limitación de números de teléfono móvil.

El tipo de identificador específico utilizado para la comunicación y el intercambio de mensajes entre usuarios del servicio de aplicación multimedios IP puede variar según el tipo de aplicación, el protocolo, la reglamentación nacional, etc. Los identificadores que se pueden utilizar en el servicio VoIP pueden ser números de teléfono semejantes a los de la RTPC, direcciones IP, cuentas de servicio IP, tales como cuentas de correo electrónico, etc. Para el servicio IM, se suele utilizar como identificador una dirección de correo electrónico, aunque también se puede utilizar otra información, como el número de teléfono móvil.

Cuando se utilizan estos identificadores en los servicios VoIP e IM, los spammers pueden acceder a ellos y a las cuentas de servicio utilizando métodos de elaboración de listas de objetivos que ya se utilizan para el spam de correo electrónico. Es posible obtener las direcciones de usuario de VoIP e IM sin gran dificultad mediante ataques de diccionario, ejecutando un programa de recopilación de identificadores mediante una búsqueda en red, etc.

Además de en VoIP e IM, los diversos tipos de spam en aplicaciones multimedios IP pueden afectar a los servicios de charla, de juegos en línea, P2P, etc. Parece que tampoco se requiere un gran esfuerzo para elaborar listas de objetivos para dichas aplicaciones. Muchas de las aplicaciones multimedios IP, como los servicios en línea, utilizan tipos de cuenta muy comunes, tales como la dirección de correo electrónico y números de teléfono como identificadores. No suele ser difícil introducirse en la lista de usuarios de los servicios de aplicación multimedios IP que sólo permiten la entrega de ficheros o mensajes de los usuarios autorizados. Habida cuenta de lo anterior, si no se cuenta con una herramienta específica para dificultar el acceso a los identificadores de usuario de los servicios de aplicación multimedios IP, los spammers pueden fácilmente, desde el punto de vista técnico o económico, elaborar listas de identificadores de usuario de los servicios IP.

8.1.2 Creación y entrega de spam

El coste que representa la creación y entrega del spam en aplicaciones multimedios IP será gran parte del coste total de la emisión del spam. El servicio VoIP o las comunicaciones vocales a través de distintas aplicaciones multimedios IP suelen ser más baratos que el servicio telefónico fijo con red de circuitos o el servicio telefónico móvil. Para los spammers tradicionales, que han estado realizando telemarketing a través de los servicios telefónicos fijos e inalámbricos tradicionales, el servicio VoIP o las comunicaciones vocales por otras aplicaciones multimedios IP son más atractivos para la entrega de spam. Además, las llamadas a larga distancia e internacionales son mucho más baratas que en los servicios telefónicos tradicionales, por lo que el telemarketing se puede realizar en otros países que utilizan el mismo idioma e, incluso, realizarse desde otros países donde los costes de personal y entrega sean más bajos.

Además del servicio VoIP, muchas aplicaciones multimedios IP, tales como los servicios IM, P2P, de charla en línea, son gratuitas o muy baratas. No parece que vaya a ser muy difícil o costoso crear y entregar spam en estas aplicaciones, pues normalmente no se invierte mucho dinero, ni tiempo, y la dificultad técnica es reducida.

8.2 Detección y filtrado de spam

La detección y el filtrado del spam en aplicaciones multimedios IP es el objetivo más importante, desde el punto de vista técnico, para contrarrestar eficazmente el spam. Es posible filtrar el spam de correo electrónico en el servidor del ISP, intranet o el terminal del receptor antes de que éste consulte el spam, pues el servicio de correo electrónico utiliza un mecanismo de comunicación de almacenamiento y reenvío. Dado que el spam de correo electrónico suele ser de texto, buena parte puede filtrarse utilizando técnicas de filtrado como el análisis del contenido. A diferencia del spam de correo electrónico, resulta difícil filtrar el spam multimedios IP a causa de las siguientes características de las aplicaciones multimedios IP:

- Comunicaciones en tiempo real.
- Dificultad del análisis de contenido de la voz y el vídeo.
- Dificultad de autenticación de spammers.

Algunas aplicaciones multimedios IP, como VoIP e IM, establecen comunicaciones en tiempo real entre los usuarios. El spam se entrega en estas aplicaciones en tiempo real sin haberse almacenado en un servidor. En algunos casos, los contenidos de VoIP e IM no pasan por servidores del proveedor de servicios sino que se entregan directamente al usuario. Por consiguiente, resulta difícil conocer información suficiente sobre la comunicación para analizar su contenido e identificar el spam antes de establecer la llamada o entregar el mensaje. Por ejemplo, cuando se ha establecido un mensaje enviado por un remitente a un receptor del spam y éste reconoce que el mensaje es spam, ya es tarde para filtrarlo, pues la conexión se ha completado. En el caso del spam en IM, es posible analizar el contenido del mensaje durante un tiempo muy breve, pues suelen ser de texto. No obstante, la brevedad del mensaje IM puede disminuir la eficacia de las técnicas de filtrado tradicionales previstas para luchar contra el spam de correo electrónico. Corresponde a los terminales de los usuarios del servicio la responsabilidad de filtrar el spam cuando el contenido de las aplicaciones multimedios IP no pasa a través del servidor del ISP. Sin embargo, añadir un filtrado de spam en los terminales de los usuarios del servicio para que ellos mismos gestionen esta función no resulta sencillo y puede no ser posible detectar y filtrar el spam en aplicaciones multimedios IP en tiempo real, como VoIP e IM, mediante el análisis de contenido.

Los mecanismos de comunicación de almacenamiento y reenvío pueden utilizarse con algunas aplicaciones multimedios IP que no son necesariamente en tiempo real, como los mensajes multimedios. La entrega de ficheros en P2P puede ser una técnica para luchar contra el spam aplicando el análisis de contenido, cuando así lo requieren los proveedores o usuarios del servicio. No obstante, sigue siendo difícil detectar y filtrar el spam con este método, pues la tecnología de reconocimiento de voz y vídeo está en sus primeras fases y su aplicación puede suponer una sobrecarga para la red.

También es posible identificar el spam a partir de la información del emisor y no la de la telecomunicación misma. Es posible identificar si el emisor es o no un spammer gracias técnicas como listas negras, listas blancas, sistemas de reputación, etc. La aplicación de estas técnicas al spam en aplicaciones multimedios IP tiene varios puntos débiles. En primer lugar, no es difícil crear cuentas de servicio o identificadores para aplicaciones multimedios IP y pueden hacerse en gran cantidad. Los spammers puede crear un nuevo identificador cuando el antiguo se clasifique como spammer. También es posible fingir que son usuarios normales aprovechando las debilidades del sistema de seguridad de las aplicaciones multimedios IP. A la luz de lo anterior, parece necesario combinar las técnicas antispam que lo identifican a partir de la información del emisor con mecanismos de autenticación efectivos.

8.3 Medidas aplicables al spam recibido

Los receptores del spam pueden tomar varias medidas una vez que lo reciben. Pueden añadir el identificador del spammer a una lista negra para impedir que se envíe más spam a él o a otros

usuarios. También pueden incorporarlo en el sistema de reputación con una baja calificación. Del mismo modo, puede denunciar el spam ilegal. Sin embargo, como ya se ha expuesto, la identificación de los spammers en muchas aplicaciones multimedios IP no es tarea sencilla y la creación de un nuevo identificador no resulta difícil. Llegados a este punto, también se necesita adoptar un mecanismo de autenticación eficaz para aumentar el efecto de las medidas adoptadas una vez recibido el spam.

9 Amenazas de seguridad relacionadas con el spam

En esta cláusula se exponen los problemas de seguridad que representa el spam multimedios IP. Algunas de las amenazas de seguridad se definen y categorizan junto con las medidas aplicables para contrarrestarlas.

9.1 Amenazas de seguridad relacionadas con el spam

En esta cláusula se exponen algunas de las amenazas de seguridad que se ciernen sobre las aplicaciones multimedios IP. Dichas amenazas se definen desde el punto de vista del envío de spam a la red. Los spammers pueden enviar sus mensajes utilizando los siguientes ataques técnicos en los entornos multimedios IP.

9.1.1 Recopilación de identificadores

Para enviar spam, un spammer reúne identificadores para encontrar sus objetivos. Por tanto, la recopilación de identificadores es la amenaza más común y el proceso preliminar básico. Un spammer procura recopilar la mayor cantidad posible de identificadores, pues representan sus objetivos. Los identificadores pueden obtenerse de distintas maneras. Pueden recopilarse motores de búsqueda, tablas abiertas, etc. Los identificadores pueden generarse con palabras comunes y nombres. En ocasiones, pueden obtenerse a través de transacciones ilegales con empresas y centros docentes, que tienen muchos clientes y poseen su información personal.

Los identificadores exclusivos, como direcciones de correo electrónico y URI, se han utilizado para distinguir a los usuarios en muchas aplicaciones multimedios IP. A diferencia del servicio telefónico, los servicios de aplicaciones multimedios IP tienen diversas ventajas, como las telecomunicaciones multicanal, precios reducidos, etc. Los spammers prefieren enviar sus mensajes en entornos multimedios IP. Así, los usuarios han de tener cuidado de proteger su identificación y no dejarla expuesta a los spammers.

9.1.2 Falsificación de identidad del emisor de spam

La falsificación es un tipo de técnica pirata. Un invasor malintencionado de la red crea una dirección web e induce a las personas a visitarla a fin de adquirir su autorización empleando un defecto de diseño del TCP/IP para robar su información personal. Además, si un spammer envía sus mensajes haciéndose pasar por una empresa reconocida, el receptor puede creer que se trata de un emisor fiable. Este spam tiene grandes probabilidades de ser aceptado. También a esto se le llama "falsificación".

El envío de spam mediante falsificación representa una amenaza, pues el spammer se hace pasar por otra persona falsificando el campo encabezamiento del mensaje o el identificador del emisor utilizado en aplicaciones multimedios IP. Esta amenaza puede anular la lista blanca y la lista negra, que son soluciones bien conocidas para el spam. Por ejemplo, los spammers sustituyen su identificador por el de un usuario válido registrado en la lista de amigos o la lista blanca del receptor, el spammer puede superar la aplicación de la lista blanca. Por otra parte, dada la naturaleza de la comunicación multimedios, resulta difícil determinar si el mensaje es o no spam antes de establecer la conexión. Por consiguiente, en este caso, no hay nada que el receptor pueda hacer para evitar el spam.

9.1.3 Rastreo de información de registro

El rastreo se da cuando un spammer observa las conexiones en curso que mantienen otros usuarios. La herramienta utilizada se denomina rastreador.

En el entorno multimedios IP, un spammer puede enviar sus mensajes ilegalmente utilizando esta técnica. En primer lugar, el spammer observa la información de registro válida del usuario para una determinada aplicación utilizando un rastreador y genera una información de registro falsa con la información adquirida. Luego, el spammer inserta una dirección IP atacante en lugar de la dirección IP válida del usuario en el mensaje de registro. A continuación, el spammer puede enviar sus mensajes gracias al registro falso.

9.1.4 Pirateo de sesión

El pirateo de sesión es una técnica en la que una persona piratea una sesión de comunicación entre otros usuarios. Puede utilizarse para enviar spam en entornos multimedios IP. Los spammers pueden forzar la desconexión entre dos usuarios en medio de una sesión. En este caso, los usuarios tienden a restablecer la sesión que estaban manteniendo. Los spammers pueden entonces piratear la sesión e insertar una transmisión de medios RTP con spam en medio de la sesión restablecida.

9.1.5 Inyección SQL

La inyección SQL es una técnica de pirateo que provoca un resultado anormal insertando sintaxis de indagación que el receptor no pretende. En un entorno de aplicaciones multimedios IP, la inyección SQL puede utilizarse cuando se emplea un mecanismo de compendio HTTP para la autenticación. El spammer modifica el encabezamiento de autenticación e inserta la indagación SQL falsificada. Entonces, el spammer falsifica un encabezamiento de autenticación del mensaje en el servidor intermediario (proxy) que utiliza el mecanismo de compendio HTTP para la autenticación e inserta una indagación SQL falsa. Si este ataque tiene éxito, el spammer puede hacerse pasar por un usuario autenticado y enviar spam con autorización válida al falsificar la información de registro válida del usuario.

9.1.6 Bot de spam

Un bot de spam es un bot maligno que adopta la forma de un programa o código que puede controlarse y utilizarse a partir de una ubicación distante, pero que no puede activarse por sí solo. Por norma general, está controlado a través de una conexión que utiliza el protocolo IRC. Una red formada por bots se denomina botnet. Un spammer puede controlar muchos sistemas infectados con una sola instrucción, porque la botnet está vinculada. Por tanto, un spammer puede fácilmente enviar una gran cantidad de mensajes con esta técnica en el entorno de aplicaciones multimedios IP.

9.1.7 Envenenamiento de cache

El envenenamiento de cache es un ataque que sustituye las direcciones de dominios por otras direcciones falsas. El envenenamiento de cache puede utilizarse para ARP y NDP en las aplicaciones multimedios IP. ARP se emplea para hacer coincidir las direcciones IP y MAC en las redes IPv4 y NDP para descubrir vecinos en las redes IPv6. Los paquetes ARP y NDP se reenvían a todos los dispositivos conectados a un único enlace. Los spammers pueden recurrir a este método para modificar contenidos en la cache ARP o la cache NDP mediante la interceptación de paquetes.

Por ejemplo, un spammer puede hacerse pasar por una pasarela gracias al envenenamiento de la cache ARP para interceptar todos los paquetes en el mismo enlace. Por tanto, si el usuario inicia una conexión, el spammer puede insertar un spam RTP preparado en la sesión en curso. Los spammers pueden modificar el identificador del objetivo. De hacerlo, el usuario puede intentar establecer otra conexión con un tercero, cuyo identificador direcciona el spammer, y que no es el tercero original. Con este ataque, los spammers pueden enviar mensajes al usuario que solicita la conexión.

9.1.8 Control de encaminamiento

Suponiendo que hay una comunicación de aplicaciones multimedios IP en curso entre encaminadores y usuarios, un spammer puede hacer de encaminador en la comunicación dentro de una red pirateándola. Si el usuario intenta establecer una conexión con otros usuarios de una red específica, el spammer responde a la petición haciéndose pasar por un usuario válido y envía spam al usuario que solicitó la conexión.

9.1.9 Sistema de gestión vulnerable

Puede haber otras amenazas que se sirven de las debilidades del sistema de gestión del servicio. En este caso, los spammers pueden modificar la información de registro válida del usuario y enviar spam haciéndose pasar por un usuario válido.

9.2 Clasificación de las amenazas de seguridad de spam

Las amenazas de seguridad de spam expuestas pueden clasificarse según la técnica de ataque. Esta clasificación se muestra en el cuadro 9-1.

Cuadro 9-1 – Amenazas de seguridad de spam clasificadas por técnica de ataque

Técnica de ataque	Amenaza de seguridad de spam
Código maligno/control remoto	Bot de spam
Piratería de sesión	Piratería de sesión
Inyección SQL	Inyección SQL
Rastreo	Rastreo de información de registro
Falsificación de identidad	Falsificación de emisor, envenenamiento de cache, control de encaminamiento
Otras	Recopilación de identificadores, sistema de gestión vulnerable

El código maligno/control remoto es una técnica con la que se puede enviar fácilmente una gran cantidad de spam. Los spammers pueden introducir de diversas maneras códigos malignos y controlar los dispositivos infectados para enviar spam, como, por ejemplo, bots de spam.

El pirateo de sesión es una técnica con la que se roba la sesión de otra persona. Por lo general, puede efectuarse simplemente adivinando el ID de sesión y utilizando la cookie de ID de sesión. Los spammers pueden observar la conexión entre un servidor y un usuario sin someterse a procedimientos de autenticación o con la autoridad del servidor.

Con la inyección SQL se explota una vulnerabilidad de la base de datos. Así, se puede modificar la indagación SQL normal y efectuar ilegalmente el proceso de autenticación. Este método suele utilizarse para piratear direcciones web y robar la información de usuario.

El rastreo es una técnica en la que el pirata observa los paquetes intercambiados entre dos o más usuarios.

La falsificación de identidad es la técnica según la cual una persona se hace pasar por otra. Así, se puede hacer creer a la máquina de la otra persona que el spammer es una fuente fiable.

9.3 Contramedidas

Hay tres maneras de solucionar los problemas de spam expuestos: autenticación, autorización y gestión de seguridad. Por gestión de seguridad se entienden las contramedidas que pueden aplicarse a una configuración de seguridad adecuada instalando un parche de seguridad en los sistemas para mantener, reparar y mejorar los conocimientos sobre seguridad del usuario. Hay diversas medidas de este tipo, como el flujo de control, la encriptación, etc., que pueden utilizarse. En esta cláusula se tratan las tres principales contramedidas.

La relación entre las contramedidas y las amenazas de seguridad de spam se resume en el cuadro 9-2.

Cuadro 9-2 – Relación entre contramedidas y amenazas de seguridad de spam en comunicaciones multimedia

Constramedidas Amenazas	Autenticación	Autorización	Gestión de seguridad
Recopilación de identificadores			X
Falsificación de emisor	X		
Rastreo de información de registro	X		
Piratero de sesión	X		
Inyección SQL		X	X
Bot de spam			X
Envenenamiento de cache	X		
Control de encaminamiento	X		
Sistema de gestión vulnerable		X	X

La autenticación puede solucionar muchos de los problemas de seguridad que representa el spam al resolver los problemas de la falsificación de identidad. Esta falsificación se utiliza en diversos ataques, como la falsificación del emisor, el rastreo de la información de registro, el pirateo de sesión, el envenenamiento de cache y el control de encaminamiento. En el caso de la falsificación del emisor, cada emisor se autentifica siguiendo el correspondiente proceso una vez recibido el mensaje. En cuanto al ataque de rastreo de información de registro, se prohíbe a un usuario no autenticado que modifique la información de registro con un proceso de autenticación. En los ataques de pirateo de sesión y envenenamiento de cache, sólo los usuarios autenticados pueden ingresar en la conexión. Y en el control de encaminamiento, sólo los usuarios autenticados pueden controlar el encaminador.

No obstante, la autenticación no puede solucionar los problemas de seguridad que representa el spam en la inyección SQL. Por tanto, es necesario establecer una política de autorización para casos así. También puede incluirse en esta categoría los sistemas de gestión vulnerables. El gestor de un sistema debe otorgar diferentes autorizaciones de acceso a los usuarios en función de sus cuentas.

Por ultimo, algunas amenazas de seguridad necesitan una cuidadosa gestión de seguridad. La recopilación de identificadores, la inyección SQL, el bot de spam y los sistemas de gestión vulnerables entran en esta categoría. Los spammers pueden recopilar el identificador del usuario de diversas maneras y enviar el spam, por lo que han de gestionarse cuidadosamente los identificadores. Los diseñadores del sistema han de tener esto en cuenta al desarrollarlo, porque las inyecciones SQL en ocasiones se deben a fallos en el código. Los bot de spam están causados por infecciones malignas. Por consiguiente, los usuarios han de tener cuidado a la hora de descargar

ficheros o acceder a sitios web y deben proteger su sistema operativo. Para evitar el sistema de gestión vulnerable, los gestores del sistema han de gestionar cuidadosamente sus sistemas.

10 Aplicabilidad de mecanismos bien conocidos en la lucha contra el spam a las aplicaciones multimedios IP

Se han realizado numerosos estudios sobre los distintos mecanismos para luchar contra el spam de correo electrónico convencional. Algunas de las soluciones utilizadas para ello también pueden aplicarse al spam en aplicaciones multimedios IP. Antes de tratar la manera en que se aplican al spam multimedios IP, es necesario analizar los mecanismos convencionales de lucha contra el spam y argumentar su aplicabilidad a las aplicaciones multimedios IP. Así, en esta cláusula se exponen algunos de los mecanismos más conocidos y se considera su aplicabilidad al spam multimedios IP.

10.1 Filtrado de identificación

10.1.1 Lista negra

Una lista negra es una lista de identificación (por ejemplo, de direcciones de correo electrónico, en ese caso) de posibles spammers o de los ya identificados. El mecanismo de una lista negra consiste en filtrar mensajes o llamadas procedentes de emisores que figuren en la lista. La lista puede ser de direcciones IP, nombres de dominio, identificadores o direcciones de llamantes, contenido de cabecera o cuerpo de mensaje, o una combinación de cualquiera de los anteriores, útil para identificar el spam.

Es posible que no baste con una lista negra para luchar contra el spam de manera eficaz en aplicaciones IP. El spammer puede utilizar la identificación de personas ajenas a su actividad y engañar al receptor. Este problema puede resolverse aplicando un mecanismo de autenticación basado en la dirección de origen. Otro problema de este método es que el usuario puede crear nuevas identificaciones con mucha facilidad. Diversas aplicaciones multimedios IP están diseñadas para telecomunicaciones utilizan direcciones de correo electrónico, que se pueden crear fácilmente en diversos portales conocidos. La mayoría de abonados normales utilizan estas direcciones de portales conocidos, por lo que no se puede incluir el nombre de dominio en la lista negra. Para solucionar este problema, los proveedores de servicio del portal han de hacer que la creación de nuevas direcciones sea algo más compleja. Si crear una nueva dirección necesita un considerable tiempo y esfuerzo, el spammer terminará utilizando cualquier otro método para crear nuevas direcciones. Habrá más posibilidades de poder filtrar estas nuevas direcciones gracias a una lista negra de dominios. Por consiguiente, el método de lista negra es efectivo si se utiliza además de otros métodos.

El método de lista negra se aplica sólo una vez al inicio de la comunicación, cuando aparece por primera vez la identificación del origen. Así, es posible utilizar este método en cualquier aplicación multimedios IP que utilice identificaciones tales como la dirección de origen. También puede utilizarse para las direcciones web, pues es posible aplicar el método de la lista negra concediendo derechos de contribución sólo a los usuarios normales, es decir, los que no están en la lista negra. Por consiguiente, puede utilizarse la lista negra para bloquear cualquier tipo de spam multimedios IP que emplee algún tipo de identificación en las aplicaciones en tiempo real y tiempo no real.

10.1.2 Lista blanca

Una lista blanca es lo contrario de una lista negra. En esta lista se consigna la información de los usuarios fiables. Los correos electrónicos procedentes de emisores que figuren en la lista blanca siempre serán aceptados. A diferencia de una lista negra, la creación masiva de direcciones de correo electrónico para cambiar de identidad no será de gran ayuda para vencer a la lista blanca, pero se sigue estando expuesto a la falsificación de dirección. El spam con direcciones falsificadas puede filtrarse fácilmente con métodos de autenticación fuertes.

Aunque el método de lista blanca puede filtrar casi todo el spam, una persona normal habrá de comunicarse con personas que no figuren en ella. Si un emisor, que no esté en lista blanca, ha de comunicarse con el usuario, es necesario contar con algún método de autorización para introducirse en la lista blanca del usuario. Los usuarios habrán de validar al emisor gracias a su identificación o a comentarios introductorios. El usuario puede aceptar o denegar la petición de comunicación. Todo usuario aceptado puede ingresar en la lista blanca del usuario. Si los usuarios han de aceptar o denegar todas las nuevas peticiones, le resultará molesto, pues casi todas las nuevas peticiones son spam. Otro problema de este método es que el usuario ha de configurar la lista blanca cada vez que se modifique su entorno, lo que supone una pérdida de tiempo y energía.

El concepto de listas blancas ya está incluido en el sistema IM, donde se conoce como lista de amigos. Muchos sistemas IM sólo permiten la comunicación con los usuarios de la lista de amigos y el usuario ha de dar su consentimiento para que otra persona ingrese en su lista de amigos. Por tanto, sumado a fuertes mecanismos de autenticación, puede resultar un método muy útil para luchar contra el spam en IM. Sin embargo, la VoIP tiene características distintas a las de los sistemas IM. Al igual que ocurre en los sistemas de correo electrónico, las listas blancas pueden ser un adecuado método suplementario, con la utilización de otros métodos pues los usuarios tienden a aceptar llamadas de origen desconocido.

El método de lista blanca se utiliza únicamente al inicio de la comunicación, por lo que se adapta a aplicaciones en tiempo real y tiempo no real. Este método puede utilizarse también en las direcciones web, pues se puede aplicar otorgando derechos de contribución sólo a los usuarios que figuran en la lista blanca.

10.1.3 Sistema de reputación

Un sistema de reputación se usa junto con una lista negra o blanca. Si un emisor, que no figura ni en la lista blanca ni en la lista negra del receptor, desea entrar en comunicación con este último, aparece en el terminal del receptor su valoración de reputación. Esta valoración ayuda al receptor a decidir si ha de aceptar o rechazar la llamada. Si el usuario acepta la solicitud de comunicación y descubre que el emisor es un spammer, puede incluirlo en el sistema de reputación y no se incluirá la identificación del spammer en la lista blanca. Todas las aportaciones se acumulan en el servidor de reputación, donde se establece la valoración.

El problema de este método es que un spammer con una mala valoración de reputación puede cambiar su identificación e iniciar el spamming con una nueva identificación. La nueva identificación no tendrá una valoración negativa y llevará algún tiempo antes de que vuelva a considerarse como spammer al acumular valoraciones negativas. Otro problema es que es posible amenazar a víctimas inocentes con asignarles malas valoraciones de reputación. Al haber acumulado dichas valoraciones negativas, la víctima tendrá dificultades para seguir llevando a cabo sus actividades en las redes IP.

Existe otro tipo de sistema de reputación, el sistema de reputación positiva. El receptor recibe buenas valoraciones si no es un spammer. Resultaría más difícil enviar spam con una nueva identificación basada en este método, pues cualquier nueva identificación tendría una valoración bastante baja. El problema que presenta este método es que varios spammers pueden asociarse para otorgarse valoraciones positivas entre ellos. No obstante, tendrían que formar algún tipo de consorcio para ello, pues resultaría extremadamente oneroso. Por consiguiente, un sistema de reputación positiva es más eficaz que el sistema de reputación negativa.

Para que un sistema de reputación pueda funcionar, se necesita un sistema de telecomunicaciones centralizado y con un sólido control. Este método puede funcionar bien con aplicaciones de tipo IM, que normalmente dependen de un proveedor de servicios. Sin embargo en las aplicaciones VoIP se supone que la comunicación se lleva a cabo entre distintos proveedores de servicios. La valoración de la reputación puede diferir de un proveedor a otro al no existir una definición normalizada. Así,

este método no es adecuado para aplicaciones como la VoIP sin un sistema de descripción normalizado.

También puede utilizarse el sistema de reputación en aplicaciones que emplean algún tipo de identificación de los emisores, pues la valoración puede asignarse a la identificación. Si el emisor supera el sistema de reputación, quedará incluido en la lista blanca del receptor. Por tanto, este método puede utilizarse en cualquier aplicación en tiempo real y en tiempo no real.

Este método puede utilizarse en las aplicaciones web al otorgarse derechos de contribución únicamente también a usuarios que superan una determinada valoración de reputación. La dirección web puede mantener una lista clasificatoria de cada miembro con las valoraciones obtenidas con anterioridad.

10.1.4 Círculos de confianza

En el método de círculos de confianza, grupos de personas fiables o dominios fiables se reúnen y comparten sus listas blancas. Este método se basa en que las personas confían en los amigos de sus amigos. En el grupo se forma una relación de confianza y los miembros podrían ponerse de acuerdo en la aplicación de sanciones si se descubre a alguno de ellos enviando spam.

Una variante de los círculos de confianza es la lista negra distribuida, en la que un grupo de personas o grupos fiables comparten sus listas negras. Este método es muy eficaz para filtrar el spam abusivo. Hay muchos servidores que reúnen listas negras utilizando este método y las ponen a disposición del público.

Este método funciona bien en grupos pequeños de proveedores que pueden compartir la información y aplicar una misma política. El crecimiento del círculo fiable imposibilita que se llegue a un consenso sobre el nivel de penalización adecuado aplicable al envío de spam.

10.2 Enmascaramiento de dirección

Diversas aplicaciones multimedios IP necesitan direcciones para utilizar sus servicios, por lo que es importante no exponer la dirección propia al público. Sin embargo, al utilizar servicios web, es necesario que los nuevos clientes faciliten su dirección para entrar en contacto con el prestatario. Los spammers utilizan esta falla para establecer una lista de direcciones objetivo. Los spammers pueden analizar varias páginas web y anotar las direcciones que contengan los caracteres "@" y ".". Dichas direcciones se utilizan para enviar spam y también se comunican a otros spammers, pues suelen compartir objetivos.

El enmascaramiento de dirección es un método de ocultar la dirección propia de manera que el spammer no la puede obtener automáticamente. La manera más sencilla de hacerlo es sustituir "@" por ARROBA y "." por PUNTO. De este modo la dirección aparecerá como texto normal y no será detectada por los sistemas de análisis de los spammers.

El enmascaramiento de dirección no es un método de lucha contra el spam, sino de prevención. Se evita exponer la dirección propia a los programas de extracción automática de direcciones que se utilizan para establecer las direcciones de los spammers. Por tanto, este método conviene para la prevención del spam en las aplicaciones multimedios IP que utilizan la misma dirección con un servicio web.

A continuación se describen otras técnicas que pueden utilizarse para enmascarar la dirección.

10.2.1 JavaScript

En el entorno JavaScript, es fácil añadir una dirección del tipo "abc@xyz.com" utilizando funciones Java. La página web la mostrará como "abc@xyz.com", pero cuando se utilice la función document.write() de JavaScript, resultará muy sencillo ocultar la dirección de correo electrónico, como se muestra en el siguiente ejemplo.

```
<SCRIPT TYPE="text/javascript">
  document.write('abc@' + 'xyz.com')
</SCRIPT>
```

Es posible utilizar otras funciones o métodos de JavaScript para ocultar las direcciones de correo electrónico, pero de lo que se trata aquí es de indicar que es posible ocultar direcciones en el entorno JavaScript. Por tanto, utilizando JavaScript para ocultar las direcciones, al spammer le resultará difícil obtener la dirección de correo electrónico con métodos automáticos, aunque en la página web aparezca como una dirección de correo electrónico normal.

Este método sólo puede utilizarse en entornos JavaScript, pero, si el usuario quiere indicar su ID de mensajería o dirección de contacto VoIP en una página web utilizando JavaScript, este método contribuirá a hacer de él un objetivo para los spammers.

10.2.2 Código ASCII

Con el método de código ASCII se pretende ocultar información importante en forma de código ASCII, "&#number". La información importante puede ser una dirección de correo electrónico o un número de teléfono, que son los objetivos de los spammers. En la página web no aparecerá como un texto normal, sino como una imagen. Así, cuando se descargue la página web, sólo se verá un código ASCII. Si el spammer dispone de la función de conversión de código ASCII en su herramienta de búsqueda, podrá romper el código con facilidad.

10.3 Prueba interactiva humana

Cada una de las partes de la comunicación recibe un rompecabezas o adivinanza previstos para que solo un humano, y no una máquina, pueda resolver. Se trata de una imagen o sonido de una palabra o número, que sólo una persona pueda entender y no una máquina. Puede tratarse de una imagen oculta detrás de varios colores o de un sonido oculto por ruidos, difícilmente reconocibles por una máquina. Hoy en día, cada vez es más difícil encontrar pruebas de este tipo que no puedan entender las máquinas, dados los avances realizados en el procesamiento automático de imágenes y sonidos y de la inteligencia artificial.

El método de prueba interactiva humana se utiliza en las aplicaciones web en la fase de inscripción a servicios de red, por lo que es muy adecuado para luchar contra el spam en web. Este método también puede utilizarse para filtrar el spam de llamadas con un método de autorización por sonidos. Cuando un llamante, que no figure en la lista blanca o la lista negra, inicia una llamada vocal, el receptor activa automáticamente el sistema de respuesta vocal interactiva (IVR, *interactive voice response*) que solicita al llamante que introduzca una serie de números con el teclado del teléfono. Si el llamante introduce la serie correctamente, su número de teléfono se incorpora a la lista blanca del receptor. Un usuario del servicio charla también puede utilizar este método para ingresar en una conversación.

10.4 Filtrado de contenido

El filtrado de contenido de la línea "asunto" es el método más común y utilizado en la lucha contra el spam en correo electrónico. Se analiza la línea "asunto" para determinar si contiene palabras sospechosas que a menudo se utilizan en el spam.

En la mensajería instantánea las comunicaciones se hacen con breves mensajes de texto, por lo que este mecanismo también se puede aplicar aquí. El contenido del cuerpo de cada mensaje IM puede analizarse por la misma tecnología con la que se analiza la línea "asunto" del correo electrónico.

No obstante, por ahora este método no se adapta a la VoIP u otras telecomunicaciones multimedios IP de audio y/o vídeo. Los medios se envían una vez establecida la llamada, por lo que no se obtiene beneficio alguno del prefiltrado del contenido. Por otra parte, aunque el spam se entregue en

forma de correo de voz o vídeo almacenado en un servidor, la tecnología actual de análisis de palabras no es suficientemente buena para luchar contra el spam.

10.5 Autenticación por intercambio de claves

La autenticación tiene la capacidad de identificar de manera segura al emisor de un mensaje multimedios IP, lo que contribuye a bloquear muchos ataques de spam de tipo falsificación.

10.5.1 Infraestructura de clave pública (PKI, *public key infrastructure*) y (PGP, *Pretty Good Privacy*)

Es posible autenticar a los emisores para bloquear las peticiones de conexión de los spammers que se hacen pasar por otra persona, especialmente si dicha persona figura en la lista blanca. La infraestructura de clave pública (PKI) y la *Pretty Good Privacy* (PGP (privacidad bastante buena)) son métodos de autenticación bien conocidos que utilizan el mecanismo de clave pública. Con PKI se emplea un mecanismo de clave pública en el que el emisor puede ser autenticado mediante una clave pública certificada por una autoridad de certificación (CA, *certificate authority*). PGP utiliza un programa informático que contiene una función de firma para la autenticación. En los sistemas de correo electrónico, estos mecanismos se utilizan para criptar un mensaje y añadirle firmas digitales. Se trata de mecanismos sólidos para prevenir el spam.

Los mecanismos de intercambio de claves son útiles para casi todos los sistemas de telecomunicaciones multimedios IP. Han de aplicarse cuidadosamente a los servicios de conferencias IP, pues las claves de grupo de una conferencia corren un alto riesgo de ser robadas.

Los métodos PKI y PGP pueden utilizarse prácticamente en todos los tipos de aplicaciones multimedios IP, como VoIP e IM. También pueden utilizarse en aplicaciones web que sólo permiten a las personas certificadas telecargar ficheros o mensajes.

10.5.2 Correo identificado por claves de dominio (DKIM, *DomainKeys identified mail*) [b-IETF RFC 4871]

El correo identificado por claves de dominio (DKIM) es un método creado por el IETF (Grupo de Tareas sobre Ingeniería de Internet) que puede utilizarse para la autenticación de correo electrónico. El servidor de correo electrónico adjunta una firma criptográfica al correo para validar que el servidor ha enviado realmente dicho correo. Con DKIM una organización puede asumir la responsabilidad de un mensaje que habrá de ser validado por el receptor. DKIM define un marco de autenticación de firma digital a nivel de dominio para el correo electrónico utilizando la criptografía de clave pública y la tecnología de servidor de claves. Un correo electrónico fraudulento puede causar daños no sólo al receptor, sino también a la reputación de las grandes empresas u organizaciones. El método DKIM puede proteger a estas últimas de los daños.

DKIM puede utilizarse para evitar comunicaciones fraudulentas por VoIP o IM. El receptor puede verificar con el servidor si el emisor del mensaje o llamada es realmente quien dice ser. El proceso de autenticación puede realizarse al principio de la comunicación de manera que no se vean afectadas ni siquiera las aplicaciones en tiempo real más importantes.

10.5.3 Autenticación HTTP y conexión TLS

La utilización de la autenticación de compendio HTTP [b-IETF RFC 5090] junto con la conexión TLS (seguridad de capa de transporte) en el servidor es muy eficaz para las aplicaciones multimedios IP con una estructura cliente-servidor. El servidor del dominio valida a sus usuarios mediante la autenticación de compendio HTTP. Este método se utiliza para autenticar al usuario de la aplicación multimedios IP, normalmente mediante un nombre de usuario y una contraseña. El cliente, es decir, el usuario, mantiene una conexión TLS persistente con el servidor. El cliente verifica la identidad del servidor con esta conexión, y el servidor autentifica al cliente mediante el intercambio de compendio en la conexión TLS. Cuando un usuario autenticado envía un mensaje a otro dominio, el dominio emisor certifica al usuario insertando una firma que valida el mensaje.

Los dominios emisor y receptor deberían autenticarse mutuamente para confiar en los usuarios del otro.

Este método puede utilizarse para autenticar a los usuarios que comunican por IM o VoIP. El proceso de autenticación puede realizarse al principio de la comunicación de manera que no se vean afectadas ni siquiera las aplicaciones en tiempo real más importantes.

10.6 Filtrado de spam en red

Los mecanismos de filtrado de spam expuestos están diseñados para funcionar en el lado servidor y en el lado cliente. No obstante, es importante construir redes seguras para prevenir el spam. A continuación se exponen brevemente algunos métodos de filtrado de spam en red.

10.6.1 Rechazo de paquetes en la entidad de red

Es posible imponer alguna política, como ACL (lista de control de acceso) en un encaminador o cualquier entidad de red para descartar paquetes sospechosos de ser spam procedente de una dirección o prefijo IP concretos. El spammer puede enviar sus mensajes desde dentro o desde fuera de la red del ISP. Los ISP que quieren proteger sus redes contra el spam habrán de solucionar ambos problemas con distintos enfoques.

Si el origen del spam se encuentra dentro de la red del ISP, éste puede hacer que la entidad de red de origen anule la conectividad IP del mismo. El spammer se dará cuenta de que ha perdido la conectividad de red y habrá de admitir que actúa erróneamente. Sin embargo, es necesario contar con algunos criterios para utilizar adecuadamente esta herramienta. Una persona puede acusar en falso a una persona inocente de ser un spammer y dejarlo sin conectividad. También es posible que el spammer utilice la dirección IP de otra persona ajena a tales actividades y dejarlo sin conectividad después de haber enviado spam durante cierto tiempo.

Supongamos que la red del ISP A está conectada a la red del ISP B y el spammer utiliza esta última. Si el origen del spam está fuera de la red del ISP A, éste debe verificar si ISP B quiere controlar el spam en su red. Si el ISP B del spammer carece de política de control de spam, el ISP A debe establecer una política de este tipo en la pasarela con el ISP B para evitar que el spam inunde su red. De este modo, el ISP A no puede bloquear la conectividad de red del spammer, pero sí proteger su red del spam. Este método puede proteger y salvaguardar sus recursos de red. El problema del mismo es que puede bloquear la conexión a su red a un usuario cualquiera del ISP B.

Otro problema es que el spammer puede cambiar con frecuencia de dirección IP. Por tanto, el ISP del spammer debe controlar y autenticar la dirección IP utilizada por el spammer para que este método funcione.

El rechazo de paquetes en la entidad de red puede utilizarse para cualquier aplicación, pues es un método independiente de la aplicación multimedios IP de que se trate.

10.6.2 Lista negra distribuida

Una lista negra distribuida es una lista negra que reside en la red y está a disposición de la comunidad de red. Las listas negras distribuidas generalmente se implantan en el DNS. Los usuarios pueden añadir direcciones que hayan estado enviando spam. Muchos sitios rechazarán los mensajes de una determinada dirección IP si aparece en una lista negra distribuida. La aplicabilidad de este método a las aplicaciones multimedios IP es equivalente a la de la lista negra.

10.6.3 Cortafuegos de spam

Las redes de empresa o de ISP utilizan cortafuegos de spam para protegerse del spam. El cortafuegos de spam emplea diversos de los métodos mencionados para bloquear el spam antes de que se introduzca en la red. El usuario de una red protegida no recibe mucho spam. Este método es una combinación de lista negra y filtrado de contenido, pues aplica los dos métodos a los paquetes que atraviesan la red de empresa.

Hoy en día se utiliza el cortafuegos de spam para el correo electrónico y la IM. Es posible que el método no sea eficaz para los servicios VoIP, pues no se puede aplicar al inicio de las llamadas VoIP; pero sí sirve para filtrar el spam de web, ya que se puede examinar el contenido y filtrarlo.

10.7 Sello en línea

Con el método del sello en línea, un emisor, que no esté en la lista blanca del receptor, tendrá que comprar un sello en línea para enviar un mensaje. Si un emisor que no figura en la lista envía un mensaje sin este sello, el servidor del proveedor de servicios rechazará el mensaje. Únicamente los mensajes de direcciones que no estén en la lista que lleven el sello en línea se remitirán al terminal del receptor. Si el receptor acepta el mensaje, devolverá el sello en línea al emisor. La dirección del emisor se añadirá automáticamente a la lista blanca del receptor. Si el receptor decide que el emisor es un spammer, puede quedarse con el dinero del sello en línea. Los spammer suelen enviar un gran volumen de mensajes, por lo que este método incrementa mucho el coste del spam.

Este método también puede utilizarse para el correo electrónico, la VoIP, o los servicios IM. No es un método molesto o caro, ya que el emisor sólo ha de adquirir el sello en línea una vez. Por lo tanto, se trata de un método eficaz en la lucha contra el spam cuando se utiliza con una adecuada autenticación de la identidad del emisor.

10.8 Filtrado de spam por autorización

Un elemento muy importante del filtrado de spam es un mecanismo que indique a determinadas entidades de la red que "filtren" las peticiones de conexión entrantes en función de la política del usuario o de la red. Varias entidades, como los usuarios o administradores del sistema, pueden crear y modificar las políticas de autorización. Es necesaria una política de red que defina los flujos de comunicación entre dominios.

Tanto el usuario extremo como los elementos de red, o ambos, pueden aplicar políticas de autorización. La entidad decisoria puede ser un usuario extremo propietario de un dispositivo, un proveedor de servicio VoIP, una persona relacionada con el usuario extremo (por ejemplo, los padres de un niño que utiliza un teléfono móvil). A continuación se presentan diversos mecanismos de filtrado de spam por autorización.

10.8.1 Comunicaciones con consentimiento

Las comunicaciones con consentimiento se basan en la autorización directa del mensaje por el receptor. Este método se utiliza además de la lista blanca o negra. Si un emisor no está en la lista negra o la lista blanca e intenta comunicar con el usuario, envía su identificación y/o un mensaje de texto breve para identificarse. En principio se rechaza al emisor. Se informa al usuario de que hay un llamante intentando comunicar con él y entonces puede aceptar o rechazar la comunicación tras consultar la identificación y/o el mensaje breve enviado por el emisor.

Este tipo de filtrado ya se utiliza en varios servicios IM. Ha demostrado ser muy efectivo para gestionar la lista blanca. También puede aplicarse a la lucha contra el spam de llamadas, habiéndose de dar el consentimiento desde el principio, pero no es adecuado para el spam de web, que es un servicio unidireccional. Es posible que tampoco sea adecuado para servicios en que participan múltiples usuarios, pues habría de recibirse el consentimiento de todos los participantes en el servicio en curso.

El problema de este método es que puede molestar al usuario con demasiadas peticiones de consentimiento, por lo que deberían someterse algunas de ellas a otro sistema de filtrado.

10.8.2 Autorización basada en la política de usuario

Con el método de autorización basada en la política de usuario, un usuario multimedios IP define la política de aceptación para filtrar las peticiones de emisores desconocidos. La política se configura en el terminal del usuario o en el servidor de aplicación para aceptar o denegar las peticiones

automáticamente. Esta política puede aplicarse a la dirección de origen del spam, la identificación y/o el mensaje breve enviado por el usuario, al igual que el método de comunicación con consentimiento. La política también puede aplicarse al contenido (imágenes, sonido o texto) recibidos para filtrar automáticamente las peticiones de comunicación que no se ajusten a la política. La información de las peticiones rechazadas se registrará en un depósito, de manera que el usuario pueda volver y consultar las peticiones que no deberían haberse rechazado. El usuario puede modificar la política según sus necesidades.

El problema del método de consentimiento es que el usuario ha de responder a todas las peticiones de comunicación. En el método autorización basada en política, sin embargo la mayoría del spam se filtra automáticamente, de manera que el usuario no sufre el problema de tener demasiadas peticiones de consentimiento. La creación de la política dependerá de las características de la aplicación multimedios IP de que se trate. El filtrado basado en política del usuario ha de definirse para todas las aplicaciones que puedan sufrir spam.

Este método ha demostrado ser muy eficaz en la gestión de listas blancas. Se trata de un método basado en el usuario, por lo que puede utilizarse en cualquier tipo de servicio bidireccional, como VoIP e IM.

10.8.3 Autorización basada en la política de red

El operador de red ha de utilizar la autorización basada en la política de red al filtrar el spam para proteger la red. La política de red puede utilizarse en una sola red o entre redes vecinas. Este método es equivalente al rechazo de paquetes en la entidad de red.

Para facilitar el filtrado del spam, el operador de red puede externalizar parte de los derechos de la administración a los usuarios extremos más hábiles y permitirles que configuren la política de red en sus enlaces con el proveedor de red. Podrá realizarse la necesaria autenticación en el encaminador de servicio para validar la identidad del usuario y sus derechos de administración. Sólo los usuarios válidos estarán autorizados a configurar las políticas de red que les correspondan.

10.9 Medidas jurídicas y reglamentos

Para evitar el spam, es importante definir las leyes y reglamentos que lo prohíben, aunque no está muy clara su eficacia. Muchos países cuentan con leyes para que la víctima emprenda acciones jurídicas contra el spam molesto. En la mayoría de los casos, el anunciante ha de insertar unos contenidos especiales para que los receptores puedan reconocer que el spam es publicitario. De no hacerlo, pueden ser penalizados.

El problema es que es difícil aplicar leyes antispam locales al spam originado en otros países. Habrán de establecerse acuerdos internacionales para que este método sea realmente eficaz. Las organizaciones internacionales, incluido el UIT-T, la OCDE, la APEC, etc., se están esforzando por definir una legislación antispam eficaz que pueda aplicarse a nivel internacional gracias a la cooperación.

Este método no es técnico y no depende de las características de las aplicaciones multimedios IP.

11 Consideraciones para la lucha contra el spam en aplicaciones multimedios IP

La utilización de redes basadas en IP para publicidad no sólo es económica, sino, además, muy efectiva. El spam es el problema que se crea cuando se hace una mala utilización de la publicidad. Pueden aparecer serios problemas sociales, debido al spam tales como la publicidad masiva, fraudulenta y engañosa que acosa y causa daños a los usuarios de la red.

En esta Recomendación se han presentado varios métodos para luchar contra el spam en aplicaciones multimedios IP. Estas aplicaciones tienen diversas características, por lo que el spam también puede variar. La utilización de sólo uno o dos métodos no conseguirá eliminar todos los tipos de spam multimedios IP. Habrán de estudiarse detalladamente los distintos tipos de spam que

afectan a las diversas aplicaciones multimedios para realmente solucionar o, al menos, aliviar el problema del spam. Por consiguiente, los métodos de lucha contra el spam deben analizarse de conformidad con las características de la aplicación multimedios IP de que se trate. En esta cláusula se exponen algunos puntos que habrán de tenerse en cuenta en la lucha contra el spam en aplicaciones multimedios IP.

Para luchar eficazmente contra el spam en aplicaciones multimedios IP, habrán de considerarse diversos aspectos de los participantes en el servicio: los usuarios del servicio (y/o abonados), los proveedores de servicios, los operadores de red, las organizaciones públicas y los anunciantes. Así, en esta cláusula se presentan algunos puntos que habrán de estudiarse en cada caso para luchar contra el spam en aplicaciones multimedios IP.

11.1 Usuario del servicio (abonado al servicio)

El usuario del servicio y/o el abonado al servicio es la víctima real del spam y ha de saber lo importante que es bloquear el spam para proteger sus derechos. A la hora de luchar contra el spam, los usuarios del servicio habrán de tener en cuenta lo siguiente, aunque la aplicación de estas sugerencias puede variar según el medio de que se trate.

- El usuario puede adquirir un motor de filtrado de spam y mantenerlo actualizado para bloquear el spam no deseado. Siempre puede aparecer spam nuevo y de ahí la importancia de mantener el motor actualizado para que pueda bloquearlo.
- El usuario debe abonarse a diversos filtros de spam, como la lista negra, la lista blanca, etc., y actualizar constantemente las listas de filtrado.
- Cuando se encuentre con spam, el usuario debe eliminarlo inmediatamente y compartir la información con otras personas para evitar que sean víctimas a su vez.
- El usuario debe participar en cursos de prevención contra el spam para conocer el spam nuevo, así como las técnicas para eliminarlo. Pueden aparecer nuevos tipos de spam en los servicios convencionales y en los nuevos. Aunque no es necesario utilizar todas las técnicas de lucha contra el spam, se debe encontrar la solución que mejor controle el spam.
- El usuario debe proteger adecuadamente su información personal contra los spammers. No deben emplearse identificaciones o números fáciles de recordar y de adivinar.
- El usuario debe emplear técnicas de prevención, para bloquear peticiones de comunicación procedentes de spammers, y configurar su sistema de manera que a un spammer le resulte difícil comunicar con él.

11.2 Proveedor de servicios

Los proveedores de servicios tienen mucho que ganar de proporcionar un servicio de calidad. El spam puede causar serios daños al servicio, pues el spammer lo utiliza inadecuadamente o abusa de él. Los proveedores de servicio han de conocer bien el problema del spam para proteger su red y hacer un mejor servicio. Estos son algunos de los puntos que habrán de tener en cuenta los proveedores de servicio para luchar contra el spam.

- Antes de lanzar un nuevo servicio multimedios IP, el proveedor de servicio debería analizar las posibilidades de que el nuevo servicio o las nuevas aplicaciones sean objetivo del spam. No todos los servicios multimedios interesan a los spammers. Realizando el análisis y encontrando las soluciones para dificultar el spam, se aumentan las posibilidades de que el nuevo servicio tenga éxito. Si se crea un nuevo servicio, susceptible de recibir spam, sin efectuar el proceso descrito, resultará muy difícil controlar el spam y los usuarios dejarán de utilizar el servicio cuando sea víctima del spam.
- El proveedor de servicios debe verificar todas las entidades, como usuarios, red, componentes del servicio, etc., que constituyen el servicio o aplicación multimedios IP y analizar los diversos métodos de introducir spam en cada una de ellas para encontrar

soluciones más simples y eficaces contra el mismo. Es posible aplicar técnicas de lucha contra el spam únicamente en el servicio multimedios IP, pero existen mejores soluciones cuando las entidades de la red se consideran en su conjunto.

- El proveedor de servicios debe realizar constantes investigaciones sobre la aparición de nuevos tipos de spam en las aplicaciones tradicionales. Incluso en los servicios más antiguos pueden surgir nuevos tipos de spam. El proveedor de servicios debe observar este fenómeno e intentar encontrar soluciones para el nuevo spam, incluso en los servicios antiguos.
- Los proveedores de servicios deben utilizar varios filtros, como la lista blanca y la lista negra, para controlar a los usuarios que acceden al servicio. Lo mejor es impedir que los spammers utilicen el servicio, pues sólo lo harían para abusar de él.
- Si el servicio está sometido a un proceso de inscripción, el proveedor de servicios lo dificultará lo suficiente para que los spammers eviten inscribirse. Muchos spammers utilizan métodos automatizados o contratan mano de obra barata para realizar numerosas inscripciones, que es un método muy efectivo para enviar spam. El proceso de inscripción debería contar con un método de autenticación fuerte para verificar al abonado, además de algún tipo de límite que evite que un mismo usuario efectúe múltiples inscripciones, a fin de desalentar a los spammers.
- Si el servicio mantiene una lista de usuarios, el proveedor debería aplicar un método para evaluar la credibilidad de los usuarios del servicio y asegurarse de que no abusan del servicio o de otros usuarios. El proveedor de servicios debería contar con técnicas de protección para evitar que la información personal de los abonados quede expuesta a otros usuarios internos o externos.
- Si el servicio dispone de un depósito, el proveedor del servicio debe comprobar que el contenido de la dirección web se controla para eliminar el spam. Puede aplicarse el análisis de contenido incluso a los datos de audio y vídeo a fin de detectar los contenidos inadecuados.
- El proveedor del servicio debe disponer de un método para que el usuario del servicio pueda controlar el spam. Puede ser un motor de filtrado, una lista de filtrado, herramientas de configuración de política, manuales contra el spam o cualquier otra cosa que el usuario pueda utilizar para luchar contra el spam.

11.3 Operador de red

El spam puede malgastar los recursos de la red, sobre todo si su contenido es multimedios. El operador de red debe intentar bloquear el spam para proteger la red y dar un mejor servicio. Estos son algunos puntos que el operador de red ha de tener en cuenta a la hora de luchar contra el spam.

- El operador de red debe controlar el tráfico de la red para encontrar tráfico anormal que pueda considerarse spam. El operador debe poder analizar el tráfico anormal y tomar las medidas apropiadas. No resultará fácil localizar el spam analizando el tráfico de red, pero algunos mensajes o programas maliciosos tienen un patrón de tráfico anormal.
- El operador de red debe limitar el tráfico del spammer o aplicar cualquier otra medida que le impida enviar los mensajes.
- El operador de red puede cooperar con el proveedor de servicios compartiendo la información relativa al spam. El operador puede realmente detener el tráfico de spam, de manera que enviar los mensajes resulte inútil.
- El operador de red debe utilizar diversos cortafuegos de spam para proteger la red.
- La red sólo habrá de configurarse con otras redes fiables, de manera que únicamente los usuarios autenticados y autorizados por la red fiable puedan comunicar. Si las redes tienen esta relación de confianza, es posible que la red controle el tráfico y a los usuarios.

Posteriormente, puede protegerse toda la red contra el spam y el tráfico malicioso cuando todas las subredes puedan fiarse del tráfico procedente de las otras subredes.

11.4 Organización pública

Una organización pública puede ser un organismo gubernamental o privado consistente en grupos de interés cuya labor consiste en controlar el spam. Las organizaciones privadas pueden ser las que, con fines lucrativos o caritativos, poseen una solución eficaz para controlar el spam. Estos son algunos puntos que las organizaciones públicas habrán de tener en cuenta a la hora de luchar contra el spam.

- Las organizaciones públicas deben tener un sistema para que las víctimas informen de los daños sufridos a causa del spam. La organización puede amonestar o penalizar al spammer. Esta organización podrá ser gubernamental o privada con capacidad para amonestar efectivamente al spammer.
- Las organizaciones públicas deben poseer un programa de formación, o proporcionar algunas directrices a los usuarios de los servicios multimedios IP, a los proveedores de servicios y a los operadores de red IP en materia de lucha contra el spam. Para luchar contra el spam se requiere una gran experiencia y es posible que el proveedor de servicios o el operador de red no estén preparados.
- Las organizaciones públicas pueden proporcionar listas negras o filtros de dominio público, a los que todo el mundo pueda aportar su contribución.
- Un sistema de aprobación de publicidad no falsificable y autenticado que las agencias de publicidad puedan utilizar sin que se les considere spammers, ayudaría a dichas agencias.

11.5 Otras consideraciones

Los siguientes puntos no guardan relación con los mencionados anteriormente.

- El problema del spam probablemente no desaparezca por muchos esfuerzos que se inviertan en luchar contra él. Siempre habrá nuevos tipos de spam, que habrán de estudiarse para eliminarlos, pero, si estos estudios se realizan de antemano, es posible crear un mejor entorno de aplicación para los servicios.
- Deben utilizarse varios métodos contra el spam al mismo tiempo. Aún así, no existe una solución óptima, pues no resuelve totalmente el problema. La diversidad de métodos contribuirá a luchar contra distintos tipos de spam que pueden aparecer en diferentes servicios y con distintas técnicas.
- La mejor solución podría ser dificultar la creación de spam y que resultase caro. El principal objetivo del spammer es emplear un método barato y fácil para hacer publicidad. Quizá los spammers abandonasen su actividad si, en ultimo término, la dificultad, el coste o las posibles penalizaciones fuesen excesivos.

Bibliografía

- [b-UIT-T Q.814] Recomendación UIT-T Q.814 (2000), *Especificación de un agente interactivo de intercambio electrónico de datos.*
- [b-UIT-T T.124] Recomendación UIT-T T.124 (1998), *Control genérico de conferencia.*
- [b-UIT-T T.180] Recomendación UIT-T T.180 (1998), *Mecanismo de acceso homogéneo a servicios de comunicación.*
- [b-UIT-T X.509] Recomendación UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*
- [b-UIT-T X.741] Recomendación UIT-T X.741 (1995) | ISO/CEI 10164-9:1995, *Tecnología de la información – Interconexión de sistemas abiertos – Gestión de sistemas: Objetos y atributos para el control de acceso.*
- [b-IETF RFC 1991] IETF RFC 1991 (1996), *PGP Message Exchange Formats.*
<<http://www.ietf.org/rfc/rfc1991.txt?number=1991>>
- [b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging.* <<http://www.ietf.org/rfc/rfc3428.txt?number=3428>>
- [b-IETF RFC 4871] IETF RFC 4871 (2007), *DomainKeys Identified Mail (DKIM) Signatures.*
<<http://www.ietf.org/rfc/rfc4871.txt?number=4871>>
- [b-IETF RFC 4880] IETF RFC 4880 (2007), *OpenPGP Message Format.*
<<http://www.ietf.org/rfc/rfc4880.txt?number=4880>>
- [b-IETF RFC 4981] IETF RFC 4981 (2008), *Survey of Research towards Robust Peer-to-Peer Networks: Search Methods.* <<http://www.ietf.org/rfc/rfc4981.txt?number=4981>>
- [b-IETF RFC 5039] IETF RFC 5039 (2008), *The Session Initiation Protocol (SIP) and Spam.*
<<http://www.ietf.org/rfc/rfc5039.txt?number=5039>>
- [b-IETF RFC 5090] IETF RFC 5090 (2008), *RADIUS Extension for Digest Authentication.*
<<http://www.ietf.org/rfc/rfc5090.txt?number=5090>>

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
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	Construcción, instalación y protección de los cables y otros 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	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
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 y Redes de la próxima generación
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación