Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1248

(09/2017)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Requisitos técnicos para contrarrestar el spam por mensajería instantánea

Recomendación UIT-T X.1248

Unión Internacional de Telecomunicaciones

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 (1)	
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 (1)	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	**X.1230–X.1249**
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1319

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

Recomendación UIT-T X.1248

Requisitos técnicos para contrarrestar el spam por mensajería instantánea

Resumen

En la Recomendación UIT-T X.1248 se indican las características del spam por mensajería instantánea (SPIM) y se especifican los requisitos técnicos para contrarrestarlo. A medida que aumenta la popularidad de la mensajería instantánea (IM), la proliferación de SPIM se ha convertido en un problema cada vez más grave. Las características de la IM, por ejemplo que se basa en el protocolo Internet (IP) que se utiliza de manera generalizada y gratuita, hacen que potencialmente el SPIM se propague generalizada e incontroladamente. Si no se resuelven meticulosamente los problemas de SPIM, éste tendrá consecuencias negativas sobre la utilización del servicio IM propiamente dicho.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	ITU-T X.1248	2017-09-06	17	11.1002/1000/13262

Palabras clave

Spam por mensajería instantánea, SPIM.

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

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de 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/.

ÍNDICE

Introducción

Con el rápido desarrollo de Internet e Internet móvil, la mensajería instantánea (IM) ha pasado de ser una herramienta sencilla de charla a una plataforma integrada de información que agrupa comunicación, información, ocio, búsqueda, comercio electrónico, colaboración empresarial y servicios al cliente en su conjunto. Dado su reducido precio y lo fácil que es de utilizar, cada vez son más las personas que se pasan a IM, lo que está teniendo una gran incidencia en el campo de las comunicaciones tradicionales. Hoy en día, los operadores de telecomunicaciones no dejan de aumentar la oferta de servicios de IM; en cambio, la IM se ha convertido gravemente en un medio de difusión de spam por los servicios de voz y de mensajes cortos (SMS). Los operadores de telecomunicaciones de todo el mundo son conscientes del spam por mensajería instantánea (SPIM) y sufren sus consecuencias en mayor o menor grado. El SPIM no solo malgasta recursos de red, sino que además hace perder tiempo y reduce la productividad de los usuarios. Además, el SPIM se utiliza para fines de *peska* (phishing) y difusión de virus, gusanos, software espía (spyware) y otras formas de malware, y puede incluso contener información perjudicial y ofensiva para el usuario. Por consiguiente, el SPIM reduce la satisfacción del usuario en la utilización de IM, lo que se ha convertido en un importante factor que menoscaba la utilización de este servicio.

Aunque en los sistemas IM se han desplegado mucha medidas anti-spam para contrarrestar, siguen existiendo muchos punto débiles en los sistemas IM que pueden causar SPIM, entre los que cabe citar: tasa de inscripción ilimitada, falta de confirmación cuando se reciben mensajes, mecanismos de transmisión por la red sin seguridad, carencia de controles de la tasa de envío de mensajes para los usuarios, vulnerabilidades inevitables en los sistemas IM.

En la presente Recomendación se especifican los requisitos técnicos para contrarrestar el SPIM a tenor de las funciones de los sistemas IM, a fin de detener la producción y propagación de medios de SPIM. Es importante, por ejemplo, exigir el diseño de un mecanismo de registro para impedir el registro masivo automatizado, y que el sistema IM ofrezca al usuario la posibilidad de recibir o bloquear todos los mensajes procedentes de entidades autorizadas o no autorizadas, así como limitar la tasa de envío del usuario una vez rebasado un umbral normal.

Recomendación UIT-T X.1248

Requisitos técnicos para contrarrestar el spam por mensajería instantánea

1 Alcance

En la presente Recomendación se identifican los diferentes tipos y características de spam por mensajería instantánea (SPIM). A fin de mitigar la producción y propagación de SPIM, en la presente Recomendación se especifican los requisitos técnicos para contrarrestar el SPIM, implicando tanto al cliente como al servidor de la mensajería instantánea (IM). La presente Recomendación se concentra principalmente en las medidas anti-SPIM de la capa de sistema IM y es aplicable a los operadores del servicio IM.

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 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.

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

3.1.3 spam en mensajería instantánea (SPIM, *spam over instant messaging*) [b-UIT-T X.1244]: Spam cuyo objetivo son los usuarios de un servicio de mensajería instantánea.

3.1.4 spimmer [b-UIT-T X.1244]: Emisor de SPIM.

3.2 Términos definidos en la presente Recomendación

Ninguno.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

ID Identidad

IM Mensajería instantánea (*instant messaging*)

IP Protocolo Internet (*Internet protocol*)

SMS Servicio de mensajes breves (*short message service*)

SPIM Spam por mensajería instantánea

5 Convenios

Ninguno.

6 Características y casos de generación de SPIM

Por SPIM se entiende un mensaje instantáneo considerado no deseado o perturbador por el usuario que lo recibe. Las características del SPIM son las siguientes:

– El SPIM suele producirse en tiempo real. En el caso en que tanto el remitente como el destinatario están en línea, el SPIM se recibe casi al mismo tiempo que se envía. Aun cuando el destinatario no esté en línea en ese momento, recibirá el SPIM inmediatamente en cuanto entre en línea.

– El SPIM se envía a menudo a granel, transmitiéndose muchísimos mensajes con el mismo contenido simultáneamente.

– Spimmer es el término utilizado para definir al remitente no autorizado de SPIM a destinatarios IM. Ahora bien, a veces la cuenta de un amigo puede haberse pirateado para enviar mensajes SPIM debido a un código malicioso o a la revelación de información de la cuenta y la contraseña. El SPIM enviado por amigos es más engañoso, especialmente si contiene enlaces a sitios web malicioso o ficheros ejecutables, que muchos destinatarios pulsan, haciendo así que sus sistemas sean más vulnerables a la infección por código malicioso.

– El SPIM no puede rastrearse fácilmente, dado que es posible crear cuentas a discreción y, por lo general, no se corresponden con una identidad real.

La generación de SPIM está estrechamente relacionada con las funciones de los sistemas IM (véase el Apéndice I) y el SPIM se puede generar de los siguientes modos:

– Los spimmers pueden utilizar software de registro automático para registrar numerosas cuentas a fin de utilizarlas para enviar SPIM.

– Los usuarios maliciosos pueden utilizar cuentas de IM falsas para enviar SPIM.

– Si un agresor malicioso ha obtenido el control de una cuenta de usuario legítima sin la autorización de éste, podrá modificar la información de dicho usuario, como la contraseña o la información de autentificación, a fin de utilizar esa cuenta (a menudo durante un largo periodo de tiempo) para enviar SPIM.

– Si un cliente IM recibe un parámetro modificado sin autorización, el SPIM podrá recibirse sin ninguna limitación.

– Los mensajes instantáneos pueden alterarse durante la transmisión. Se puede insertar publicidad o códigos maliciosos en el IM, convirtiéndolo así en SPIM.

– Debido a la falta de mecanismos de confirmación, el spimmer puede añadir amigos y enviarles SPIM.

A fin de evitar el SPIM, es necesario considerar plenamente sus características y los casos de generación de SPIM, lo que permitirá tomar medidas preventivas exhaustivas.

7 Arquitectura funcional de IM para contrarrestar el SPIM

7.1 Generalidades

En la Figura 7-1 se ilustra la arquitectura funcional de IM para contrarrestar el SPIM.

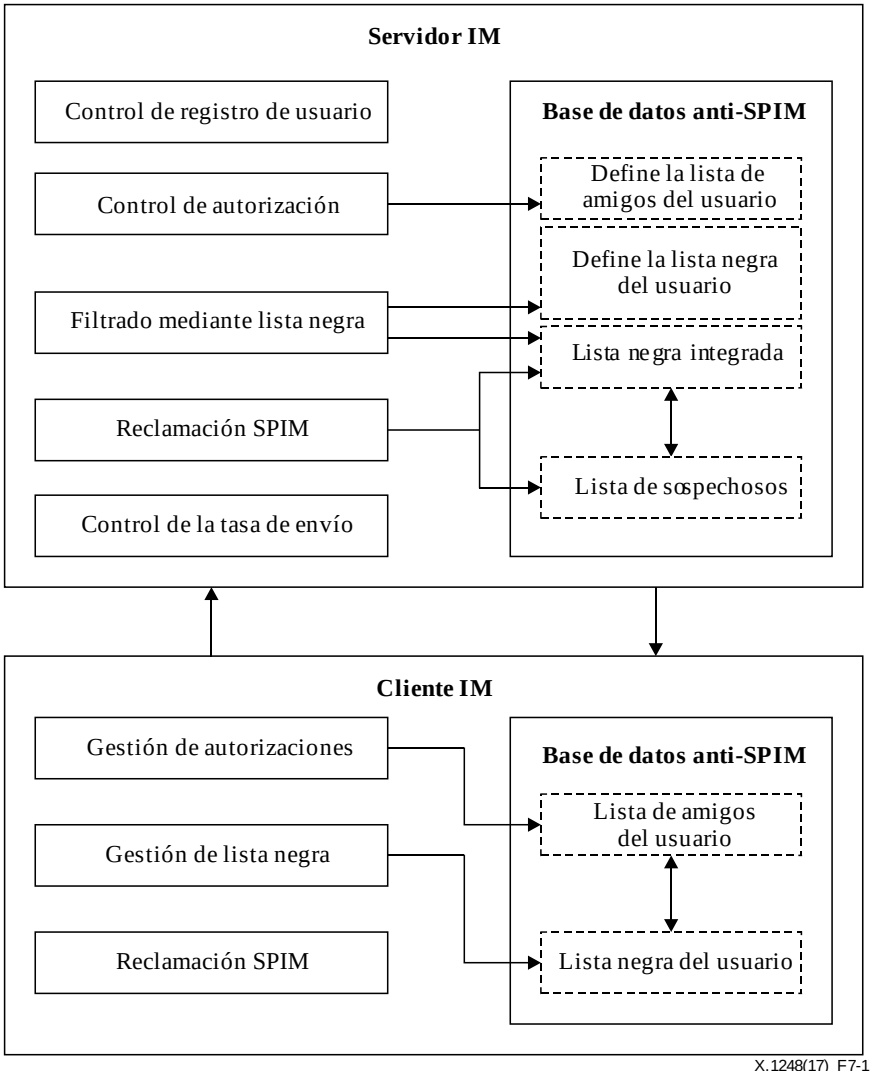

Figura 7-1 – Arquitectura funcional de IM para contrarrestar el SPIM

Esta arquitectura integra las funcionalidades para contrarrestar el SPIM, como filtrado mediante lista negra, controles de registro de usuarios y reclamaciones de SPIM. Lo que es aún más importante, la arquitectura permite el filtrado basado en la limitación de la tasa de envío de IM y el control de la autorización del remitente del IM.

En el Apéndice I se describe más detalladamente las funcionalidades del cliente y del servidor IM y las funciones del remitente IM, el receptor IM y el spimmer.

7.2 Funcionalidad de los componentes

7.2.1 Servidor IM

La funcionalidad de los componentes del servidor IM incluye los siguientes seis elementos:

1) Control del registro de usuarios

   Se aplicarán métodos de confirmación manual, como códigos de verificación, verificaciones de correo electrónico, códigos de verificación por SMS, a fin de impedir el registro automático de usuarios. De esta manera se impide enviar SPIM a los spimmers que disponen de un gran número de cuentas registradas automáticamente.

2) Control de la autorización

   Se reenviarán las solicitudes del usuario de añadir amigos y autorizar la relación de amistad con el usuario basándose en la respuesta del cliente IM.

3) Filtrado mediante listas negras

El servidor IM filtrará mensajes instantáneos basándose en una lista negra integrada y un conjunto de listas negras específicas del usuario.

4) Reclamaciones de SPIM

Se aceptarán las reclamaciones del usuario acerca de cuentas desde las que se envía SPIM a fin de determinar si se añade o no estas cuentas a la lista de remitentes sospechosos o a la lista negra integrada. Tendrá que interactuar con sistemas externos de gestión de reclamaciones de SPIM e importar y exportar la lista negra integrada.

5) Control de la tasa de envío

Se controlará el número de mensajes instantáneos enviados desde una misma cuenta dentro de un periodo de tiempo. Los mensajes instantáneos que rebasen un determinado umbral se eliminarán.

6) Base de datos anti-SPIM

- Conjunto de listas de amigos del usuario: incluye las listas de amigos de todos los usuarios gestionados por el servidor IM. Es necesario que la lista de amigos del usuario contenida en el servidor IM esté sincronizada con las listas de amigos de usuario en los clientes IM.
- Conjunto de listas negras del usuario: Comprende las listas negras del usuario de todos los usuarios gestionados por el servidor IM. Es necesario que la lista negra específica del usuario contenida en el servidor IM esté sincronizada con las listas negras del usuario en los clientes IM.
- Lista negra integrada: Incluye todas las cuentas contenidas en reclamaciones de los usuarios y las cuentas detectadas por el servidor IM. Por ejemplo, cuando una tasa de envío de mensajes del usuario IM rebasa un cierto umbral, el servidor IM deberá clasificar el ID del remitente y añadirlo a la lista negra. La lista negra integrada también incluye cuentas importadas de otros sistemas, como otros servidores IM.
- Lista de remitentes sospechosos: Se generará una lista de todas las cuentas sospechosas generadas por el servidor IM. La lista integrada de sospechosos puede elaborarse a partir de las reclamaciones del usuario, la importación desde otros sistemas, etc.

7.2.2 Cliente IM

La funcionalidad del componente cliente IM incluye los siguientes cuatro elementos:

1) Gestión de autorizaciones

Los dos elementos fundamentales que deben incluirse son el control de la visibilidad de la identidad (ID) IM y la gestión de solicitudes de entidades no autorizadas. En el caso del control de la visibilidad de la ID IM, es necesario que el usuario decida si su información (por ejemplo, ID IM, seudónimo, ubicación) debe ser visible para un usuario no autorizado. En el caso de la gestión de solicitudes de entidades no autorizadas, el usuario deberá ser capaz de elegir una política adecuada para gestionar dichas solicitudes. El usuario deberá poder aprobar manualmente, exigir una respuesta concreta a una pregunta personal o incluso bloquear todas las solicitudes. Asimismo, el usuario deberá poder especificar los amigos de confianza y gestionar su lista de amigos en el cliente IM.

2) Gestión de listas negras

El usuario deberá poder gestionar su lista negra y se bloquearán todos los mensajes procedentes de cuentas que figuran en la lista negra. El usuario podrá añadir, suprimir o incluso compartir su lista negra.

3) Reclamaciones de SPIM

El cliente IM dispondrá de una función para presentar reclamaciones sobre cuentas que envían SPIM. La reclamación puede referirse a la cuenta de un contacto de la lista de amigos, a un miembro de un grupo IM o incluso una cuenta no autorizada que envía solicitudes de autorización.

4) Base de datos anti-SPIM

- Lista de amigos del usuario: Necesaria para almacenar la lista de amigos aceptados por el usuario.
- Lista negra del usuario: Definida por el usuario, incluye cuentas que el usuario desea bloquear para no recibir mensajes.

La base de datos ubicada en el cliente IM debe volcarse automáticamente al servidor IM.

8 Procedimientos de trabajo

8.1 Procedimiento de trabajo del control de la tasa de envío

El umbral que define el número máximo de mensajes emitidos desde una determinada cuenta IM, dentro de un periodo de tiempo dado, se debe configurar en el servidor IM.

El umbral se debe estudiar o determinar mediante un gran número de muestras de mensajes de usuario, utilizando tecnologías tales como aprendizaje máquina, aprendizaje profundo, etc. El umbral debe configurarse para diferentes casos, como por ejemplo los siguientes:

– Número de mensajes instantáneos enviados a un grupo, del que es miembro el remitente.

– Numero de mensajes instantáneos enviados a un grupo, del que el remitente no es miembro.

– Número de mensajes instantáneos enviados a uno o varios amigos del remitente.

– Número de mensajes instantáneos enviados a destinatarios que no son amigos del remitente.

Cuando el servidor IM recibe los mensajes enviados por una cuenta específica, deberá aplicar el control de la tasa de envío siendo el proceso el que se describe a continuación y que se ilustra en la Figura 8-1:

– Contar el número de mensajes enviados desde la cuenta dentro de un periodo de tiempo dado.

– Comparara el número de mensajes enviados (n) con el umbral mínimo para todo tipo de casos. Si el número *n* rebasa el umbral mínimo, el servidor IM determinará a continuación a qué caso corresponde y si el número *n* rebasa el umbral de dicho caso específico. De lo contrario, el servidor IM reenvía los mensajes.

– Si el número de mensajes enviados *n* rebasa el umbral del caso, el servidor IM verifica si la cuenta está en la lista de remitentes sospechosos. En caso afirmativo, el servidor IM descarta los mensajes; si no está en la lista, el servidor IM transmite el mensaje pero cuenta el número de veces que excede el umbral *m*. Si este número *m* es mayor que un determinado número α, el servidor IM añade la cuenta a la lista de sospechosos.

En la Figura 8-1 se ilustra el proceso de control de la tasa de envío.

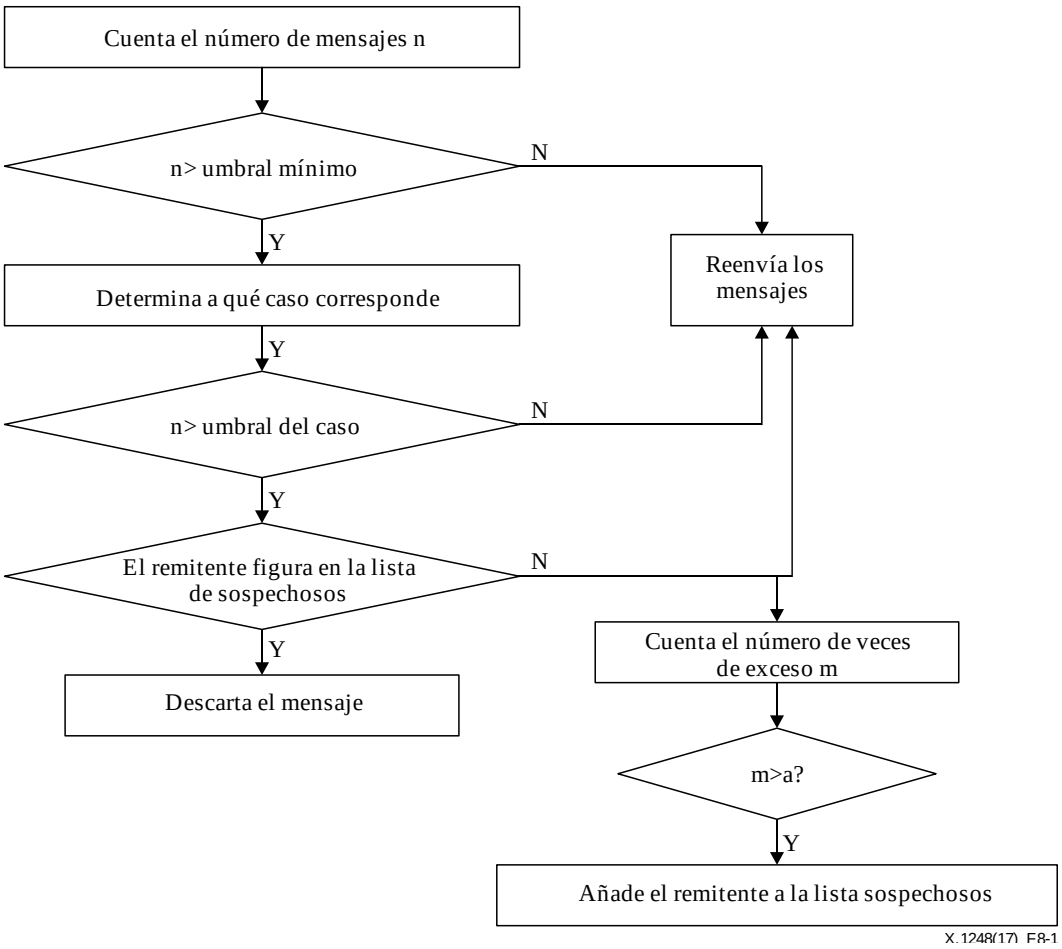

Figura 8-1 – Proceso de control de la tasa de envío

8.2 Procedimiento de trabajo de listas negras

Los sistemas IM son comparativamente independientes, por lo que los proveedores de servicios IM están obligados a crear sus propias listas negras integradas para sus servidores IM. Además, por el bien del usuario, es indispensable que las listas negras del usuario se comuniquen a los clientes IM.

A continuación se describe el proceso de interacción de todos los tipos de listas negras de un sistema IM:

– El usuario edita su lista negra en el cliente IM. El servidor IM supervisa la lista negra del usuario en tiempo real y actualiza el conjunto de listas negras del usuario cada vez que éste modifica su lista.

– El servidor IM rastrea el número de veces que se ha añadido la misma cuenta en las listas negras de usuario. Si el número rebasa un determinado umbral, el servidor IM añade la cuenta a la lista negra integrada.

– El servidor IM añade la cuenta objeto de una reclamación de cliente a la lista negra de remitentes sospechosos, si dicha cuenta no figura en dicha lista ni en la lista negra integrada. El servidor IM cuenta el número de reclamaciones registrada para esa cuenta; si el número rebasa un determinado umbral, el servidor IM añade esta cuenta a la lista negra integrada.

A continuación se describe el proceso de filtrado de mensajes basado en la lista negra:

– Cuando el servidor IM recibe un mensaje, verifica si la cuenta del remitente figura en la lista negra integrada; en tal caso, el servidor IM descarta el mensaje.

– Si la cuenta del remitente no está en la lista negra integrada, el servidor IM verifica además si la cuenta del remitente está en la lista negra del usuario receptor y, en tal caso, el servidor IM descarta el mensaje. De lo contrario, el servidor IM transmite el mensaje.

8.3 Procedimientos de gestión de autorizaciones

Se recomienda que el cliente IM pueda permitir al usuario definir qué tipo de mensajes puede recibir y que servidor IM debe poder filtrar los mensajes no deseados por el usuario, a fin de impedir que remitentes no autorizados (por ejemplo, los que no son amigos, los miembros de un grupo que no son amigos, amigos de otros sistemas IM, contactos del teléfono) le envíen mensajes que no desea recibir. Se distinguen, entre otros, los siguientes cinco casos de autorización de remitentes:

1) Se configura el cliente IM para "sólo recibir mensajes de amigos". Cuando el servidor IM recibe un mensaje del usuario B al usuario A, verificará primero si el usuario B figura en la lista del usuario A. De lo contrario, el servidor descarga el mensaje.

2) Se configura el cliente IM para "recibir mensajes de un grupo al que el cliente se ha unido explícitamente". Cuando el servidor IM recibe un mensaje del grupo B hacia el usuario A, verificará si el usuario A es miembro del grupo B. De lo contrario, el servidor descarta el mensaje. Además, cuando el servidor IM recibe una invitación de un miembro del grupo B al usuario A, éste debe aceptar la invitación antes de que el servidor IM añada el usuario A al grupo B.

3) Se configura el cliente IM para "recibir mensajes de miembros de un grupo que son amigos del cliente". Cuando el servidor IM recibe un mensaje enviado por el usuario B del grupo A al usuario A, el servidor verifica si el usuario B está en la lista de amigos de A. De lo contrario, el servidor descarta el mensaje.

4) Se configura el cliente IM para "recibir mensajes de cuentas de otros sistemas IM o contactos del teléfono sólo cuando estas cuentas o contactos se haya añadido explícitamente como amigos". Cuando el servidor IM recibe un mensaje desde una cuenta B asociada hacia el usuario A, el servidor verificará si la cuenta B está en la lista de amigos de A. En caso negativo, el servidor descarta el mensaje. Por otra parte, cuando el servidor IM recibe una solicitud de añadir un amigo de la cuenta B a la lista de amigos del usuario A, éste debe aceptar la invitación antes de que el servidor añada la cuenta B a la lista de amigos de A.

5) Se configura el cliente IM para "limitar el establecimiento de una conexión punto a punto sólo a los amigos". Cuando el servidor IM recibe una solicitud del usuario B para establecer una conexión punto a punto con el usuario A, éste verifica si el usuario B figura en la lista de amigos de usuario A. En tal caso, el servidor IM reenvía la solicitud del usuario B al usuario A, y ayuda al usuario A y al usuario B a establecer la conexión punto a punto. De lo contrario, el servidor IM descartará la solicitud del usuario B.

En la Figura 8-2 se ilustra la relación entre el usuario A, el usuario B, el grupo A, el grupo B y la cuenta B.

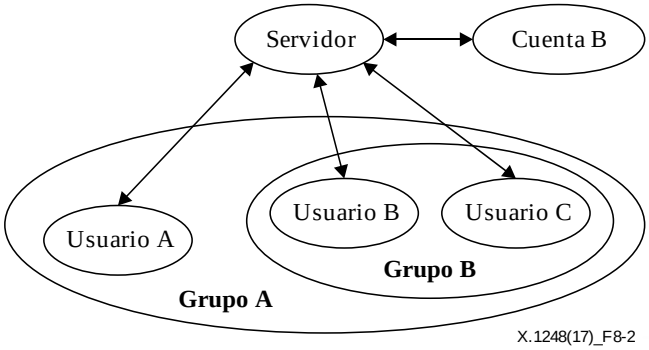

Figura 8-2 – Relación entre usuarios y grupos

8.4 Procedimientos de gestión de registro de usuario

A fin de impedir el registro automático de cuentas, los sistemas IM deben aplicar una o varias medidas de confirmación manual, como el código de verificación, la verificación por correo electrónico, el código de verificación SMS.

Cuando un usuario envía información para registrarse (por ejemplo, nombre de usuario, contraseña, número de móvil, dirección de correo electrónico) en el cliente IM o en la página web de registro de usuarios IM, el servidor IM envía de vuelta al cliente una confirmación de registro, como un código de verificación por SMS o por correo electrónico.

Una vez los usuarios envían la confirmación de registro de vuelta al servidor IM, éste verifica la confirmación enviada por el usuario. Si la verificación es positiva, el servidor IM envía de vuelta al usuario un mensaje de registro exitoso, y guarda la información de registro del usuario en la base de datos. En caso negativo, envía un mensaje de fallo de registro.

El sistema IM debe actuar de interfaz con la pasarela SMS o implantar un servidor de correo electrónico, para poder enviar al usuario un código de verificación por SMS o un correo electrónico de confirmación del registro.

8.5 Procedimientos para reclamaciones de SPIM

Se debe dar soporte a dos procedimientos de notificación de reclamaciones SPIM:

1) Reclamación a través del cliente IM. A continuación se describe el proceso de gestión de reclamaciones para este método:

   Tras recibir SPIM, el usuario IM indica la cuenta de la que procede el SPIM en el cliente IM; la reclamación se envía al servidor IM. El servidor IM debe disponer de un umbral de reclamaciones predefinido. Tras recibir la reclamación del usuario, el servidor IM verifica en primer lugar si la cuenta ya figura en la lista integrada de sospechosos o en la lista negra integrada. De lo contrario, el servidor IM añade la cuenta a la lista de sospechosos y cuenta el número de veces que dicha cuenta ha sido objeto de reclamación. Si este número rebasa el umbral predefinido, el servidor IM añade la cuenta a la lista negra integrada. Si la cuenta ya figura en la lista de sospechosos, el servidor IM suma el número de reclamaciones presentadas para dicha cuenta. Si el valor rebasa el umbral predefinido dentro de un determinado periodo de tiempo, el servidor IM añade esta cuenta a la lista negra integrada. Si la cuenta ya figura en la lista negra integrada, el servidor IM no hace nada y descartará luego los mensajes enviados por esa cuenta.

2) Reclamación a través de un sistema externo de gestión de reclamaciones de SPIM. A continuación se describe el proceso de gestión de reclamaciones para este método:

Tras recibir SPIM, el usuario IM presenta una reclamación ante un sistema externo de gestión de reclamaciones. El sistema externo de gestión de reclamaciones SPIM se encarga de analizar la reclamación del usuario y de decidir si añadir la cuenta a la lista negra. El servidor IM interactúa con el sistema externo de gestión de reclamaciones SPIM e importa o exporta la lista negra de la interfaz. El servidor IM descartará los mensajes enviados desde cuentas que figuran en la lista negra.

8.6 Procedimiento de filtrado de SPIM

Cuando el servidor IM recibe mensajes instantáneos, realiza un filtrado SPIM basado en la lista negra integrada y en el conjunto de listas negras del usuario; este proceso se describe en la cláusula 8.2.

Si la cuenta del remitente de IM no figura en la lista negra integrada ni en el conjunto de listas negras del usuario, el servidor IM realiza un filtrado de SPIM basado en el control de autorización y analiza si el remitente dispone de autorización para enviar mensajes al destinatario (que ha configurado el propio destinatario). Si no lo está, el mensaje se descarta. El caso de autorización se describe en la cláusula 8.3.

Si sí está autorizado, el servidor IM lleva a cabo un filtrado SPIM basado en la tasa de envío límite, proceso que se describe en la cláusula 8.1.

Apéndice I

Roles y funciones del sistema IM

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

En la Figura I.1 se ilustra el modelo básico de sistema IM.

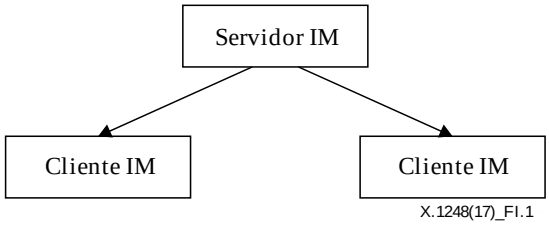

Figura I.1 – Modelo básico de IM

El modelo básico de sistema IM consta de un servidor IM y varios clientes IM homogéneos. El servidor IM se utiliza para recibir y reenviar mensajes instantáneos que envían los clientes IM. El cliente IM tiene dos roles: remitente IM y destinatario IM. El remitente IM reenvía los mensajes instantáneos al servidor IM para su transmisión, y éste trata de enviarlos a los correspondientes destinatarios IM. Si el remitente IM envía SPIM, se considerará un spimmer.

Las funciones del sistema IM deben realizarlas el servidor IM, los clientes IM y la interacción entre ellos.

Las principales funciones del servidor IM son las siguientes:

– Administración de usuarios, como el registro de usuarios, el inicio y cierre de sesión, la edición de la cuenta del usuario.
– Gestión de mensajes instantáneos, como el envío, recepción y transmisión de mensajes.
– Administración de amigos, como búsqueda de amigos, gestión de lista de amigos.
– Administración del sistema, como configuración de parámetros, actualización del sistema, inicio, reinicio y salida del sistema.

Las principales funciones del cliente IM son las siguientes:

– Administración del usuario, como registro de usuarios, inicio y cierre de sesión.
– Gestión de mensajes instantáneos, como el envío y recepción de mensajes.
– Administración de amigos, como la adición, eliminación y búsqueda de amigos.
– Administración de clientes, como la configuración de parámetros, la actualización del cliente, el inicio, reinicio y salida del cliente.

Bibliografía

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

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

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

[b-IETF RFC 2778] IETF RFC 2778 (2000), *A Model for Presence and Instant Messaging*.

[b-IETF RFC 3428] IETF RFC 3428 (2002), *Session Initiation Protocol (SIP) Extension for Instant Messaging*.

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2018