Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1231

(04/2008)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Estrategias técnicas de lucha contra el correo basura

Recomendación UIT-T X.1231

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	
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.1231

Estrategias técnicas de lucha contra el correo basura

Resumen

En esta Recomendación UIT-T X.1231 se insiste en las estrategias técnicas para la lucha contra el correo basura (spam) y se incluyen las características generales del spam, así como los principales objetivos de la lucha contra el mismo. Además, asumiendo que no hay una única solución válida para resolver el problema del spam, esta Recomendación también ofrece una lista de verificación para evaluar las posibles herramientas de lucha contra el correo basura.

Orígenes

La Recomendación UIT-T X.1231 fue aprobada el 18 de abril 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

Correo basura, estrategias técnicas, lucha contra el correo basura.

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 la evolución de la industria de la información, la generalización del correo basura plantea hoy un problema que ocasiona pérdidas de beneficios a los operadores de telecomunicación, a los proveedores de servicio y a las empresas, y que tiene efectos negativos en los usuarios en general. El correo basura, al principio una simple molestia, constituye ahora una verdadera plaga mundial.

Por lo tanto, es necesario hallar medios aptos y eficaces para combatir el correo basura. Esta lucha puede llevarse a cabo en distintos frentes, es decir, a nivel de la legislación, la capacitación, la cooperación internacional y otros. La presente Recomendación se refiere principalmente a los medios técnicos para poner freno a estos mensajes no solicitados.

Recomendación UIT-T X.1231

Estrategias técnicas de lucha contra el correo basura

1 Alcance

En la presente Recomendación se insiste en las estrategias técnicas de lucha contra el correo basura y además se describen características generales del correo basura y los principales objetivos de la lucha contra el mismo. Además, reconociendo que hay más de una solución a este problema, en esta Recomendación se presenta una lista de verificaciones para evaluar instrumentos prometedores destinados a combatirlo.

Esta Recomendación describe estrategias técnicas en general sin identificar las particulares para cada tipo de spam. Por otra parte, esta Recomendación ofrece un modelo jerárquico de categorías generales que puede contribuir a establecer una infraestructura apta y eficaz de lucha contra el correo basura. Ese modelo consta de las siguientes partes:

- estrategias de equipo;
- estrategias de red;
- estrategias de servicio;
- estrategias de filtrado;
- estrategias de intercambio de información.

En la práctica, la presente Recomendación define estrategias técnicas de lucha contra los diversos tipos de correo basura que una administración considera inapropiados, en armonía con su legislación y sus políticas nacionales.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otras Recomendaciones

La presente Recomendación utiliza los siguientes términos definidos en otras Recomendaciones:

3.1.1 autentificación [b-UIT-T X.811]: Confirmación de la identidad declarada de una entidad.

3.1.2 teléfono IP [b-UIT-T Q-Sup.49]: Terminal (por ejemplo, un terminal de voz especializado o una computadora personal polivalente) conectado directamente (por ejemplo, a través de una interfaz Ethernet o una línea xDSL) a una red IP.

3.1.3 entidad de mensajes cortos (SME, *short message entity*) [b-UIT-T Q.1742.3]: Entidad que compone y descompone mensajes cortos. Puede estar situada o no dentro de un registro de posiciones propio (HLR), un centro de mensajes (MC, *message centre*), un registro de posición de visitantes (VLR, *visitor location register*), una estación móvil (MS, *mobile station*) o un centro de conmutación de servicios móviles (MSC, *mobile switching centre*), y no ser distinguible de éstos.

3.2 Términos definidos en esta Recomendación

La presente Recomendación define los siguientes términos:

3.2.1 mensajería instantánea (IM, *instant messaging*): Transferencia de mensajes entre usuarios en tiempo casi real. Estos mensajes suelen ser breves, aunque no han de serlo obligatoriamente. La IM a menudo se emplea en modo conversación, es decir, que la transferencia de mensajes en ambos sentidos es lo suficientemente rápida para que los participantes mantengan una conversación interactiva.

3.2.2 correo basura por multimedios IP: Llamadas o mensajes no solicitados por aplicaciones de multimedios IP en tiempo real. A diferencia del correo basura tradicional recibido por correo electrónico, este término se aplica a los nuevos métodos de comunicaciones por IP como, por ejemplo, mensajería instantánea, servicio de presencia, voz por IP (VoIP) y otros. El spam por telefonía Internet (SPIT), el spam vocal o spam VoIP (VAM) y el spam por mensajería instantánea (SPIM) son las siglas habituales utilizadas para diferentes tipos de correo basura por multimedios IP.

3.2.3 modalidad: Codificación de una información cuyos datos son perceptibles para los seres humanos. Este tipo de información, por ejemplo, textos, gráficos, audio, vídeo o sensaciones táctiles utilizadas en interfaces hombre-computadora, puede provenir de ciertos dispositivos multimodo, o estar destinada a ellos. Dichos dispositivos son, por ejemplo, micrófonos para la recepción de datos vocales/sonoros, estiletes para introducir datos táctiles, teclados de texto, ratones para dispositivos vídeo o de animación, altavoces que transmiten señales de voz sintetizadas, pantallas para visualizar textos y gráficos, aparatos vibradores para una interacción táctil o sistemas de escritura con alfabeto Braille para personas ciegas.

3.2.4 mensaje multimodo: Tipo de mensaje multimedios que contiene diferentes informaciones codificadas que permiten interacciones según diversas modalidades.

3.2.5 servicio de mensajería multimedios (MMS, *multimedia messaging service*): Tipo de servicio de mensajería posterior al servicio de mensajes breves (SMS) mediante el cual se pueden transferir diversos mensajes multimedios que contienen texto, gráficos, audio, vídeo, etc., a través de redes móviles, inalámbricas o fijas.

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

3.2.7 emisor de correo basura (Spammer): Entidad o persona que crea y envía spam.

4 Abreviaturas y acrónimos

Esta Recomendación utiliza los acrónimos y abreviaturas siguientes:

Correo-e Correo electrónico (*email*)

DDoS Denegación de servicio distribuida (*distributed denial of service*)

DoS Denegación de servicio (*denial of service*)

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

IM Mensajería instantánea (*instant messaging*)

IP Protocolo Internet (*Internet protocol*)

MC Centro de mensajes (*message centre*)

MMS Servicio de mensajería multimedios (*multimedia messaging service*)

MS Estación móvil (*mobile station*)

MSC Centro de conmutación de servicios móviles (*mobile switching centre*)

RTPC Red telefónica pública conmutada

SME Entidad de mensajes breves (*short message entity*)

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

SMTP Protocolo de transferencia de correo simple (*simple mail transfer protocol*)

SPIM Correo basura por mensajería instantánea (*spam over instant messaging*)

SPIT Correo basura por telefonía Internet (*spam over Internet telephony*)

VAM Correo vocal basura o correo basura por VoIP (*voice spam or VoIP spam*)

VLR Registro de posición de visitantes (*visitor location register*)

VoIP Voz por IP o protocolo de transmisión de la voz por Internet (*voice over IP*)

5 Convenios

Ninguno.

6 Aspectos generales

Se entiende por correo basura la difusión de informaciones electrónicas por un emisor a ciertos destinatarios a través de terminales tales como computadoras, teléfonos móviles, teléfonos fijos, etc., y que, en general, no se han solicitado, no se desea recibir y resultan perjudiciales para quienes la reciben. Esas informaciones se pueden enviar por correo electrónico, mensajería móvil, multimedios IP y por otras formas electrónicas. De hecho, la definición de "correo basura" varía según la percepción de los países, las organizaciones o los individuos. Su definición evoluciona y se aplica a nuevos ámbitos debido al desarrollo de las tecnologías de la información y la comunicación que ofrecen nuevas posibilidades para el envío de estos mensajes. En términos generales, el correo basura tiene las siguientes características comunes:

Electrónico: Se trata de informaciones electrónicas que se transmiten generalmente por una red de telecomunicaciones abierta, en especial Internet, y que son muy distintas de la enviada por métodos tradicionales como el correo postal, la publicidad impresa o la comercialización directa. El correo basura es barato, práctico y puede adoptar diversas formas.

No solicitado: El correo basura suele contener anuncios publicitarios, informaciones fraudulentas o virus, etc.

Además, el correo basura presenta habitualmente todas las características que se describen a continuación, o algunas de ellas:

Masivo y repetitivo: Por lo general, los mensajes y correos no solicitados son enviados masiva e indiscriminadamente, mientras que las comunicaciones no solicitadas en tiempo real se reciben siempre en forma repetitiva. Sin embargo, los emisores de spam sólo conocen la dirección de comunicación del destinatario (por ejemplo, su dirección de correo electrónico, su número de teléfono).

Utilización de direcciones sin el consentimiento de su titular: Los emisores de correo basura suelen utilizar las direcciones de comunicación que se recopilan sin la autorización explícita del titular para enviar el spam. En realidad, algunos programas informáticos pueden obtener las direcciones de comunicación por la web o crearlas automáticamente.

Origen oculto o falso del mensaje: Este tipo de mensaje a menudo encubre a su emisor ya que se envía utilizando un encabezamiento falso o simplemente ocultando el nombre del emisor. Por regla general, quienes envían estos mensajes utilizan servidores no autorizados de proveedores de servicios ajenos, que no validan la información del emisor.

Interrupción difícil: No es nada fácil detectar este tipo de correo debido al gran volumen de mensajes enviados. Los intentos para impedir su entrada pueden ser difíciles y, a veces, darán lugar a evaluaciones positivas o negativas falsas del correo recibido.

Las estrategias a seguir deberían ser neutrales desde el punto de vista de la tecnología y permitir aún así evaluar los medios de comunicación utilizados abusivamente o que causan problemas en la circunscripción considerada, los medios de comunicación que ofrecen grandes posibilidades de ser utilizados abusivamente en el futuro y los medios de comunicación poco probable de ser utilizados abusivamente. Las opciones habituales son las siguientes:

Correo electrónico

Actualmente, de los diversos tipos de mensajes no solicitados, los enviados por correo electrónico representan la amenaza más importante debido a la vulnerabilidad del protocolo aplicado y a la inseguridad de la infraestructura básica, es decir Internet, por la cual se transmite el correo electrónico. El protocolo de transferencia de correo simple (SMTP), el protocolo más difundido en la retransmisión de correos electrónicos, define un sobre y un encabezamiento para cada correo. El sobre contiene la dirección del destinatario, que éste no puede ver, y que se utiliza como dirección de destino para la transferencia del mensaje del emisor al destinatario. Normalmente, durante la transmisión, la dirección de destino que figura en el sobre puede copiarse en el encabezamiento de correo electrónico que es visible para el destinatario. Los emisores de correo basura aprovechan dos tipos de vulnerabilidad en el proceso de autenticación del SMTP:

- la no exigencia de autenticación, gracias a lo cual los usuarios pueden ocultar o falsificar su dirección;
- la posibilidad de falsificar la mayor parte de los datos que figuran en el sobre y encabezamiento de un correo electrónico.

Por otra parte, el costo que representa el envío de mensajes basura por correo electrónico es muy bajo en tanto que sus efectos negativos son siempre muy elevados.

Servicio de mensajería móvil

Las comunicaciones móviles tienen la gran ventaja de ser prácticas, eficaces, económicas y de fácil utilización. Pero al mismo tiempo que sacan provecho de estas ventajas, los usuarios tienen que hacer frente al correo basura que reciben en su servicio de mensajería móvil, es decir, los mensajes no solicitados enviados por SMS o MMS. En la actualidad, los principales tipos de correo basura por el servicio de mensajes breves son los siguientes:

- mensajes fraudulentos incitando a los usuarios a abonarse a un servicio;
- anuncios publicitarios;
- mensajes tramposos ilícitos;
- mensajes de contenido pornográfico.

Estos tipos de mensajes, por lo general, inducen a error o son fraudulentos, y se conocen también como mensajes trampa o *scam* (intento de fraude por correo electrónico).

Es importante señalar que, con la llegada de los servicios de correo electrónico móvil, que los spammers pueden utilizar más fácilmente, resulta hoy habitual recibir mensajes electrónicos en teléfonos móviles.

Servicios multimedios IP

Con la evolución de los servicios multimedios IP, el concepto de correo basura ha comenzado a aplicarse de manera general a los servicios multimedios IP de mensajería instantánea, de telefonía por Internet, de presencia, de creación de blogs, de grupos de noticias de la red de usuarios (Usenet), de mensajería de juegos en línea, etc. En ciertos casos, se utiliza una terminología apropiada a cada tipo de correo según el medio por el que se envía, por ejemplo, correo basura o spam por mensajería instantánea (SPIM), correo basura o spam por telefonía Internet (SPIT), etc. Además, este tipo de mensajes afecta también las interacciones multimodo, como los nuevos tipos de multimedios, ya que un correo basura multimedios adopta numerosos aspectos en una interfaz de usuario. Por ejemplo, un correo basura de tipo mensaje de red puede dar lugar a la reproducción no solicitada de una audiosecuencia, la visualización de una videosecuencia y la presentación de un mensaje de texto en la pantalla. Todos estos mensajes pueden tener el mismo contenido o un contenido diferente. No obstante, las interacciones multimodo están más expuestas a recibir mensajes no solicitados y, por este motivo, a medida que se generalice la difusión de dichas interacciones, el problema planteado por esos mensajes aumentará.

Correo basura o spam por mensajería instantánea (SPIM): la mensajería instantánea es un método de comunicación por Internet en tiempo real práctico y económico que ha alcanzado una rápida evolución. Si bien es utilizada principalmente en las comunicaciones privadas, las aplicaciones de este servicio empiezan a utilizarse cada vez más en las empresas. Pero, lamentablemente, está aumentando el envío de informaciones ilícitas (virus, códigos maliciosos, etc.) por mensajería instantánea, también conocida como SPIM. Aunque estos mensajes representan un pequeño porcentaje del volumen total de correo basura, su incidencia aumenta rápidamente.

Correo basura o spam por telefonía Internet (SPIT): entre los problemas identificados hasta ahora figuran los vinculados generalmente a las redes IP, además de otras amenazas más elaboradas, tales como la representación falsa, la escucha furtiva, los ataques por denegación de servicio en VoIP, la inyección de paquetes y los mensajes no deseados (mensajes basura por IP o correo basura por telefonía Internet). Esta última amenaza se debe principalmente a la posibilidad que ofrece el VoIP de enviar mensajes de voz a muy bajo costo, lo cual puede dar lugar a una situación similar a la ya planteada con respecto a los mensajes no solicitados que se reciben por correo electrónico: en pocos segundos se pueden enviar a todo el mundo enormes cantidades de mensajes de correo vocal no deseados.

Evolución del correo basura

Este tipo de correo no se limita a las opciones mencionadas *supra*. La aparición cada vez más frecuente de más tecnologías y aplicaciones de la información y la comunicación ha hecho que el spam sea ubicuo. Además, todos los tipos de tecnologías y aplicaciones de comunicaciones pueden ser vehículos de correo basura, si las soluciones propuestas para contrarrestarlo se revelan ineficaces.

7 Objetivos genéricos

La finalidad de esta cláusula es definir el principal objetivo de la lucha contra el correo basura. Se trata menos de definir las etapas de aplicación práctica que de fijar las metas previstas.

Los objetivos de la lucha contra el correo basura son los siguientes:

- Validación de las entidades, es decir, determinar si tienen los privilegios necesarios para enviar mensajes o iniciar comunicaciones tras la correspondiente autentificación y/o autorización.
- Protección de la dirección y/u otras informaciones importantes sobre los mensajes o las comunicaciones enviadas por entidades legítimas contra la ocultación o enmascaramiento.
- Protección de la privacidad durante la transmisión de la información.

- Todas las entidades asumirán la responsabilidad de sus actos con respecto a la transmisión o retransmisión de la información.
- Protección de las redes de telecomunicaciones contra el acceso o la utilización no autorizados a fin de asegurar un acceso adecuado y eficaz.
- Con objeto de asegurar el rastreo, se facilitará toda la información necesaria sobre el emisor.
- Protección de los equipos de servicio contra virus y acceso no autorizado para garantizar su disponibilidad.
- Aplicación del filtrado de correo basura y, en caso necesario, almacenamiento del mismo en ciertos equipos específicos con fines de rastreo o de análisis pormenorizado.
- Se facilitará una plataforma de denuncia o de intercambio de información que, además de fomentar la comunicación de información exacta y eficaz, promoverá la cooperación internacional, la elaboración de leyes, etc.
- Aplicación de los protocolos internacionales más conocidos para el intercambio y la difusión de la información de interés relativos a la lucha contra este tipo de mensajes.

Conviene recordar además que la realización de los objetivos citados *supra* se adaptará a cada entorno considerado.

8 Estrategias técnicas

Para combatir el correo basura debe aplicarse un enfoque polifacético que abarque los siguientes aspectos: tecnología orientada al sector privado, autodisciplina de las empresas, cooperación internacional, legislación, intercambio de información y capacitación. Entre todos estos aspectos, la tecnología es esencial para garantizar la aplicación de los demás aspectos. La presente Recomendación se refiere principalmente a las estrategias comunes de lucha contra el correo basura.

Con miras a facilitar el análisis conviene, en primer lugar, clasificar los servicios. Según el método de transmisión utilizado, los servicios pueden clasificarse en las dos categorías siguientes: almacenamiento y retransmisión o comunicación en tiempo real. La primera comprende los servicios de correo electrónico, de mensajes breves, de mensajería multimedios y otros. La segunda abarca los servicios de telefonía IP, Fax IP, mensajería instantánea y otros. Los métodos para combatir el correo basura son diferentes según los servicios. Se debe efectuar pues un análisis detallado de las estratégicas técnicas aplicadas a cada servicio.

Para una lucha eficaz contra el correo basura, se recomienda aplicar un modelo jerárquico con diferentes partes teniendo en cuenta que cuantas más partes tenga ese modelo, más eficaz será su aplicación. En la figura 1 siguiente se observa el modelo jerárquico aplicado a la lucha contra el correo basura.

<table>
<tr><td>Estrategias de filtrado</td><td>Estrategias de intercambio de información</td></tr>
<tr><td colspan="2">Estrategias de servicio</td></tr>
<tr><td>Estrategias de equipo</td><td>Estrategias de red</td></tr>
</table>

Figura 1 – Modelo jerárquico para la lucha contra el correo basura

Las cinco partes de este modelo jerárquico se dividen en tres niveles: nivel de infraestructura, nivel de servicio y nivel de aplicación. Las estrategias de equipo y de red, que pertenecen al nivel de infraestructura, constituyen los elementos básicos del modelo jerárquico. Su aplicación establece una base segura y fiable de las estrategias técnicas en las capas más altas. Del mismo modo, las

estrategias de equipo y red se influyen mutuamente. Una red segura exige equipos seguros y éstos a su vez necesitan redes razonables. Las estrategias de servicio, que pertenecen al nivel de servicio, son la más importante de las cinco partes puesto que esa capa es responsable directa de la prestación del servicio. Por último, las estrategias de filtrado e intercambio de información pertenecen al nivel de aplicación y, en el caso de la lucha contra el correo basura, son las más próximas a los usuarios. No obstante, las cinco partes interactúan entre sí. En la figura 2 se observa la relación entre las diferentes partes:

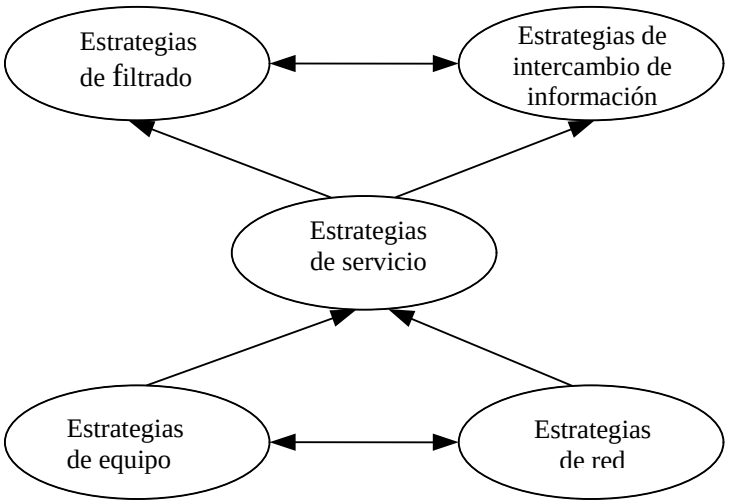

Figura 2 – Relación entre las diferentes partes

Además, se recomienda la utilización de protocolos internacionales bien conocidos a fin de aplicar estas estrategias técnicas. No obstante, de aplicarse satisfactoriamente todas las estrategias técnicas, su costo, comparado con el de los servicios protegidos, es excesivamente elevado, por lo que es muy importante adaptar las estrategias a cada situación concreta. Además, los métodos de lucha contra el spam han de permitir tal adaptación. Dadas la gran cantidad de combinaciones posibles, conviene disponer de características que se ajusten a una amplia gama de servicios. La normalización, dirigida por la industria y las organizaciones investigadoras, facilitará el reciclaje de soluciones y productos. Al mismo tiempo, resultará más fácil implantar soluciones técnicas contra el correo basura más rápidamente y a un costo inferior.

8.1 Equipo

Los equipos constituyen la base de la infraestructura de la lucha contra este tipo de mensajes y, por consiguiente, su protección es esencial.

8.1.1 Mayor seguridad en los programas informáticos de los equipos correspondientes

Quienes envían mensajes no solicitados pueden difundirlos utilizando recursos informáticos y de la red que pertenecen a operadores de servicios ajenos una vez que esos recursos hayan dado prueba de su vulnerabilidad. Los recursos afectados (dispositivos víctima) se denominan grupo de programas informáticos robot o computadoras zombi. Las personas que envían correo basura pueden controlar a distancia los dispositivos afectados para efectuar esos envíos. La instalación de un programa informático y de un sistema operativo fiables así como la actualización del programa antivirus permiten proteger eficazmente los equipos contra los virus.

8.1.2 Admisión de diferentes funciones de gestión

Dada la importancia de los sistemas de servicios, deberán facilitarse diferentes funciones de gestión que, como mínimo, serán las de gestión del usuario, gestión del sistema y gestión de auditoría. La primera función se utiliza para la gestión de las configuraciones de los administradores, operadores y auditores; la segunda, para asegurar el mantenimiento y funcionamiento de los equipos; la tercera, para comprobar los registros cronológicos de funcionamiento y los registros cronológicos del sistema. Ciertos servicios pueden también necesitar funciones de gestión particulares.

8.1.3 Creación de registros cronológicos de funcionamiento y del sistema

Para garantizar la operación lícita del sistema y mantenerlo en su estado de ejecución normal, el sistema debe establecer ficheros de registro cronológicos y de funcionamiento del sistema.

Los registros cronológicos de funcionamiento, que indican el historial de las operaciones realizadas, deben consignar todas las conexiones y operaciones establecidas. Como mínimo, incluirán los siguientes campos: el nombre del operador así como la hora, el número de orden y el resultado de la operación.

Los registros cronológicos del sistema pueden facilitar el historial del estado de funcionamiento del sistema. Incluyen principalmente informaciones relativas a la calidad de funcionamiento, a las averías, etc. Estos registros pueden variar de un sistema a otro o de un servicio a otro.

Los registros cronológicos de funcionamiento y del sistema no sólo pueden contribuir al mantenimiento del sistema sino también a que los administradores puedan aplicar los procedimientos operativos evitando todo tipo de actividades destructivas.

8.1.4 Mejora de la seguridad y flexibilidad de los terminales

Como son los equipos más importantes del usuario, los terminales son siempre las primeras víctimas de estos envíos no solicitados. Dado que las funciones son distintas según los diversos tipos de terminales, sólo pueden establecerse estrategias generales. Ofrecemos a continuación una enumeración de esas estrategias, que no es exhaustiva:

- dar soporte a la autenticación y autorización, especialmente para terminales inteligentes;
- admitir listas negras y/o listas blancas;
- instalar programas informáticos antivirus, especialmente para terminales inteligentes.

8.2 Estrategias de red

Como ocurre con los requisitos en materia de equipos, la seguridad de la red constituye también un elemento esencial en la lucha contra el correo basura. La reducción de estos mensajes puede ser considerable gracias a un diseño apropiado de la topología de la red y a la instalación de diversos equipos de seguridad tales como cortafuegos, encaminadores fiables, pasarelas seguras, etc.

8.2.1 Protección de las redes de servicios contra las amenazas de Internet

Internet representa una amenaza para diversas redes de servicios ya que la mayoría de éstos utilizan una tecnología IP de normas abiertas.

Son necesarias las siguientes funciones:

- Proteger las redes de servicios contra los ataques por Internet, por ejemplo, los ataques por denegación de servicio (DoS) y por denegación de servicio distribuido (DDoS). Las redes de servicios son muy importantes y suelen estar controladas a distancia por administradores. Dado el libre acceso a Internet, estas redes deben estar en condiciones de resistir la explotación de las vulnerabilidades de Internet. Para proteger las redes de servicios contra estas vulnerabilidades, suelen utilizarse cortafuegos y otros dispositivos de seguridad.

- Proteger las señales de protocolo en el plano de control para impedir intrusiones ilícitas. Esta protección es especialmente importante para el protocolo VoIP. En tanto que la RTPC es segura y fiable, Internet es todo lo contrario. Las pasarelas VoIP deberán pues impedir la entrada de señales de protocolo ilícitas para lograr el mismo nivel de seguridad alcanzado en la RTPC.

8.2.2 Creación de mecanismos de redundancia y de reserva para mantener la estabilidad de las redes de servicios

Los equipos y redes de servicios son tan importantes que convendría prever equipos redundantes e itinerarios de reserva. Además, los mecanismos de redundancia y de reserva deben ser prácticos, eficaces y económicos.

8.3 Estrategias de servicio

Las estrategias de servicio son la parte más importante del modelo jerárquico porque son los servicios los que directamente satisfacen los requisitos de los usuarios. No obstante, son tan diversos los tipos de servicios con diferentes funciones y puntos débiles, que las estrategias de servicio para luchar contra el spam son totalmente diferentes dependiendo del servicio de que se trate. Sin embargo, hay algunas estrategias de servicio generales para luchar contra el correo basura y son las que se indican a continuación:

8.3.1 Soporte de la autentificación

Cuando las entidades (usuario o equipo) acceden a un servicio, los sistemas de servicio han de soportar un mecanismo de autentificación estricto. Por una parte, la autentificación estricta puede impedir que una entidad no válida acceda a los servicios y, por otra, los registros de autentificación pueden utilizarse para el rastreo.

Hoy en día, algunos países han hecho grandes progresos en las redes móviles gracias a la aplicación de mecanismos de autentificación y nombre real.

8.3.2 Soporte de direcciones de retransmisión configurables

Los equipos de servicio deberían prescindir de los retransmisores abiertos y optar por la retransmisión limitada. El equipo de servicio ha de poder soportar listas de direcciones de retransmisión configurables y sólo retransmitir mensajes de las direcciones permitidas al tiempo que se bloquean los mensajes de otras direcciones.

8.3.3 Soporte del formato estricto de mensajes

Se debe definir de manera rigurosa el formato de determinados mensajes, especialmente los mensajes comerciales. De este modo, los sistemas de servicio pueden obtener la información necesaria para el tratamiento de los mensajes.

8.3.4 Compatibilidad con normas internacionales

Para reforzar la capacidad de interconexión y compatibilidad, los protocolos de comunicación de los servicios deben ser compatibles con las normas internacionales.

8.3.5 Mayor eficacia en el rastreo del correo basura

En primer lugar, los sistemas de servicio deben identificar y autentificar a las entidades (usuarios o equipos) en el momento en que acceden a los sistemas de servicio, y obtener la información de origen precisa de las entidades para luego registrarla en la base de datos. En segundo lugar, deben facilitar funciones de auditoría para efectuar un rastreo a partir de los registros de la base de datos.

8.3.6 Soporte del control de flujo

Los administradores de sistema pueden limitar la anchura de banda de la comunicación o el número de mensajes transmitidos durante determinados intervalos de tiempo.

8.3.7 Funciones estadísticas

La información estadística revela claramente a los administradores la situación actual del sistema, por ejemplo, el volumen de tráfico y algunos datos sobre los usuarios y sitios consultados.

8.4 Estrategias de filtrado

El filtrado es la tecnología más común en la lucha contra el correo basura. Su principal ventaja es la simplicidad y la flexibilidad de su aplicación.

8.4.1 Soporte del filtrado de correo basura

Generalmente, hay dos tipos de filtrado: el filtrado por dirección y el filtrado por contenido (incluye el filtrado por contraseña).

El filtrado por dirección puede aplicarse en los servicios de almacenamiento y retransmisión y en los servicios en tiempo real. En el primer caso, el filtrado por dirección, que se emplea para filtrar mensajes y correos electrónicos en función de la dirección de su emisor, es un método eficaz para impedir que los sistemas de servicio envíen o retransmitan mensajes y correos basura. En el segundo caso, este filtrado se utiliza para bloquear llamadas en función del número de teléfono o la dirección de la persona que llama. En términos generales, el filtrado por dirección es muy eficaz y práctico en la lucha contra el correo basura.

El filtrado por contenido también puede utilizarse en los servicios de almacenamiento y retransmisión y en los servicios en tiempo real. En el primer caso, se filtran los mensajes y correos electrónicos según los contenidos o las contraseñas. En el segundo, se corta la comunicación en función de su contenido. Teóricamente es más razonable el filtrado por dirección que el filtrado por contenido. No obstante, el filtrado por contenido siempre consume numerosos recursos y su precisión está estrechamente vinculada a los algoritmos de análisis.

Dado que ninguno de estos métodos de filtrado puede ser eficaz para eliminar todos los correos basura, conviene utilizarlos simultáneamente. Por otra parte, convendría que los equipos de servicio admitieran métodos que también pudieran filtrar virus.

8.4.2 Mecanismo de salvaguardia y registro para el filtrado de correo basura

En lo que respecta a los servicios de almacenamiento y reenvío, convendría que los equipos de servicio salvaguardaran automáticamente los mensajes basura. En el caso de los servicios en tiempo real, los equipos de servicio deberían registrar automáticamente los perfiles del spam. En ambos casos, conviene realizar un almacenamiento para una consulta ulterior.

8.4.3 Calidad requerida en el filtrado de correo basura

La calidad del filtrado de correo basura es muy importante y para evaluarla los índices de evaluación positiva y negativa falsas son los factores más importantes. Por evaluación positiva falsa se entienden los casos negativos detectados en ausencia de casos negativos y por evaluación negativa falsa, la ausencia de casos negativos detectados en presencia de casos negativos. Por lo tanto, el índice de evaluación positiva falsa es la proporción de casos negativos señalados erróneamente como casos positivos, y el índice de evaluación negativa falsa, la proporción de casos positivos señalados erróneamente como casos negativos. En el Cuadro 1 se observa el resultado del filtrado de correo basura.

Cuadro 1 – Resultado del filtrado de correo basura

		Situación actual	
		Casos positivos	**Casos negativos**
Resultado de la prueba	Casos positivos detectados	A	B
	Casos negativos detectados	C	D
NOTA – Los casos positivos son correo basura, los casos negativos no son correo basura.			

El número total de casos puestos a prueba es T.

T = A + B + C + D

El número de evaluaciones positivas falsas es B.

El número de evaluaciones negativas falsas es C.

Índice de evaluación positiva falsa = B / (B + D).

Índice de evaluación negativa falsa = C / (A + C).

Los índices de evaluación positiva falsa y de evaluación negativa falsa guardan una estrecha correlación. Por lo general, cuanto mayor es el índice de evaluación positiva falsa, menor es el índice de evaluación negativa falsa. Sin embargo, La importancia de uno u otro de estos índices dependerá de circunstancias concretas. En el ámbito comercial, es preferible que el índice de evaluación negativa falsa sea mayor al índice de evaluación positiva falsa.

8.4.4 Configuración de filtrado fácil y flexible

Dado el gran número de mensajes basura y su variedad, convendría establecer una configuración de filtrado fácil y flexible, por ejemplo, interfaces de fácil utilización, métodos de configuración optativos y otras posibilidades. Además, las normas generales de filtrado pueden clasificarse en diferentes categorías, que se incorporarán en bases de datos o depósitos. En caso necesario, esas categorías de filtrado se podrán seleccionar y utilizar con facilidad.

8.4.5 Máxima reducción posible de los costos de filtrado

Conviene proceder cuanto antes al filtrado del correo basura y no esperar a que ocupe una gran cantidad de recursos. Conviene pues efectuarlo al inicio de la transmisión y no en los equipos de servicio.

8.4.6 Soporte de listas negras y listas blancas

Hay dos tipos de filtrado por dirección: listas blancas de emisores de correo aceptables y listas negras de emisores de correo sospechosos.

Las listas negras que contienen la enumeración de los originadores de mensajes basura, pueden incluir nombres de dispositivos, direcciones IP, direcciones MAC u otro tipo de direcciones electrónicas. El sistema de filtrado se ocupará de filtrar los mensajes o comunicaciones en bloque teniendo en cuenta las listas negras.

Las listas blancas contienen la enumeración de los originadores aceptables. Su mecanismo de funcionamiento es similar al utilizado para las listas negras con la diferencia de que en las listas blancas se enumeran las direcciones aceptables.

De hecho, el criterio fundado en el establecimiento de listas blancas/listas negras suele ser demasiado burdo para que reciba la aceptación de la mayoría de los usuarios. Con todo, este enfoque es muy simple y no exige una cantidad de recursos considerable. Para lograr una mayor eficacia del filtrado, conviene que los filtros admitan listas blancas y listas negras, especialmente las listas negras creadas para combatir el correo basura.

8.4.7 Soporte de filtrado de mensajes multimodo

Con respecto a los mensajes multimodo, se deben admitir las siguientes capacidades:

- Interrupción completa de la recepción de ciertos mensajes multimodo.
- Eliminación de ciertos ficheros adjuntos al mensaje multimodo o de contenidos multimodo parciales en un mensaje multimedios.
- Filtrado de mensajes multimodo entrantes (recibido) y/o salientes (enviados).

8.5 Estrategias de intercambio de información

Los usuarios, posibles víctimas de virus y correo basura, son los destinatarios finales de este tipo de mensajes. La participación de los usuarios contribuirá en forma eficaz a combatir el correo basura. Por consiguiente, hay que tener en cuenta las soluciones propuestas por los usuarios para luchar contra este tipo de correo. No obstante, la participación de los usuarios finales en el mecanismo de intercambio de información ha de ser voluntaria.

8.5.1 Creación de una plataforma para denunciar el correo basura

Convendría ofrecer ciertos recursos a las personas afectadas por la recepción de mensajes basura perjudiciales. La legislación debe proteger los derechos de las personas físicas ya que son los destinatarios de ese tipo de mensajes. Es imprescindible por tanto poner a su disposición las vías de recursos necesarias. Hay que establecer mecanismos para cumplir este objetivo, por ejemplo crear vías que permitan denunciar a una autoridad apropiada la violación que representa la recepción de correo basura. Estos tipos de procedimientos destinados a la gestión de la información facilitada por los usuarios deben ser transparentes, aptos y eficaces. Una plataforma de denuncia puede desempeñar esa función.

8.5.2 Elaboración de formatos normalizados para el intercambio de información

A fin de registrar la información recibida, una plataforma de denuncia debe adoptar un formato normalizado. De esta manera, diferentes operadores y entidades podrán intercambiar esa información y, a partir de ella, obtener las principales direcciones de los emisores de correo basura e incorporarlas a las listas negras.

9 Evaluación del sistema

Para evaluar la eficacia de la tecnología y los sistemas en la lucha contra el correo basura, conviene tener en cuenta los siguientes aspectos:

- Índice de evaluación positiva falsa.
- Índice de evaluación negativa falsa.
- Costo: los métodos para combatir el correo basura deben ser flexibles a fin de ofrecer soluciones personalizadas. Debido al gran número de posibles combinaciones de estrategias, es conveniente contar con perfiles que abarquen una gran gama de servicios.
- Interfuncionamiento del sistema actual: la condición previa de la lucha contra el correo basura es garantizar el funcionamiento normal del sistema actual. En otras palabras, no se pueden interrumpir los sistemas actuales aplicando soluciones destinadas a combatir ese tipo de mensajes.

- Conformidad a normas internacionales: de preferencia, las soluciones técnicas deben inspirarse en normas internacionales con objeto de lograr una interconexión y difusión a escala mundial. Por otra parte, la normalización facilitará la reutilización de soluciones y componentes. Esto contribuirá a crear rápidamente y a bajo costo nuevas soluciones y técnicas destinadas a combatir el correo basura.

Los aspectos citados *supra* constituyen criterios generales para evaluar las medidas adoptadas en la materia. En la práctica, será necesario tener en cuenta otros aspectos concretos vinculados a la red de servicios.

Bibliografía

[b-UIT-T Q.1742.3] Recomendación UIT-T Q.1742.3 (2004), *Referencias en las IMT-2000 a la red núcleo desarrollada por ANS-41 con red de acceso cdma2000*, que eran aprobadas al 30 de junio de 2003.

[b-UIT-T Q-Sup.49] Serie de Recomendaciones Q del UIT-T – Suplemento 49 (2004), *Informe técnico TRQ.2840: Requisitos de señalización para el soporte de telefonía IP*.

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT*.

[b-UIT-T X.811] Recomendación UIT-T X.811 (1995) | ISO/CEI 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autenticación*.

[b-IETF RFC 2505] IETF RFC 2505 (1999), *Anti-Spam Recommendations for SMTP MTAs*. <http://www.ietf.org/rfc/rfc2505.txt>.

[b-IETF RFC 2554] IETF RFC 2554 (1999), *MTP Service Extension for Authentication.* <http://www.ietf.org/rfc/rfc2554.txt>.

[b-IETF RFC 2635] IETF RFC 2635 (1999), *DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*).* <http://www.ietf.org/rfc/rfc2635.txt>.

[b-IETF RFC 2821] IETF RFC 2821 (2001), *Simple Mail Transfer Protocol.* <http://www.ietf.org/rfc/rfc2821.txt>.

[b-IETF RFC 3685] IETF RFC 3685 (2004), *SIEVE Email Filtering: Spamtest and VirusTest Extensions*. <http://www.ietf.org/rfc/rfc3685.txt>.

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

Impreso en Suiza
Ginebra, 2009