Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1249

(01/2019)

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

Seguridad en el ciberespacio – Lucha contra el correo basura

Marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles

Recomendación UIT-T X.1249

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
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699

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

Recomendación UIT-T X.1249

Marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles

Resumen

En la Recomendación UIT-T X.1249 se describe un marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles. Por *spam* publicitario en aplicaciones móviles se entiende el envío de anuncios no solicitados que se muestran dentro de una aplicación de teléfono móvil. Esta publicidad no solicitada aparece en la pantalla del dispositivo en un cartel situado en la parte superior o inferior de la pantalla, en pantalla completa o superpuestos. Con el crecimiento acelerado del desarrollo de aplicaciones móviles se ha producido un aumento radical de la publicidad en aplicaciones móviles, y el filtrado de anuncios maliciosos puede mejorar la experiencia del usuario e incluso la seguridad. Por consiguiente, sería beneficioso definir un marco práctico para contrarrestar el *spam* publicitario en aplicaciones móviles, que pueda integrar muchas de las ventajas de todas las medidas.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T X.1249	30-01-2019	17	11.1002/1000/13605

Palabras clave

Publicidad en aplicaciones móviles, *spam*.

* 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

Recomendación UIT-T X.1249

Marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles

1 Cometido

En la presente Recomendación se describe un marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles. Se especifican los componentes funcionales, las reglas de filtrado y los flujos de trabajo. En la presente Recomendación se describe un marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles.

Está destinada a los proveedores de aplicaciones y a los proveedores del servicio Internet móvil.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones, y demás referencias, son objeto de revisión, por lo que se alienta a los usuarios de esta Recomendación a que utilicen la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no le confiere carácter de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 teléfono móvil [b-UIT-T X-Sup.19]: dispositivo electrónico utilizado para realizar llamadas telefónicas y enviar mensajes de texto por una amplia zona geográfica mediante acceso radioeléctrico a redes móviles públicas, que permite ser móvil al usuario.

3.1.2 teléfono inteligente [b-UIT-T X-Sup.19]: teléfono móvil con gran capacidad de cálculo, conectividad heterogénea y sistema operativo avanzado que constituye una plataforma para aplicaciones de terceros.

3.1.3 *spam* [b-UIT-T X.1242]: información electrónica que circula desde el remitente hasta el destinatario mediante terminales tales como computadores, teléfonos móviles, teléfonos, etc., que, por regla general, no se ha solicitado, ni se deseaba recibir y que perjudica a los destinatarios.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 filtrado asíncrono: técnica de procesamiento de ficheros para identificar *spam* publicitario y que permite procesar varias identificaciones simultáneamente.

3.2.2 aplicación móvil: aplicación *software* diseñada para ejecutarse en dispositivos móviles, como teléfonos inteligentes y tabletas.

3.2.3 publicidad en aplicaciones móviles: publicidad que se muestra dentro de la aplicación móvil. Aparecen en la pantalla del dispositivo en un cartel situado en la parte superior o inferior de la pantalla, en pantalla completa, superpuesta, etc.

3.2.4 ***spam*** **publicitario en aplicaciones móviles**: publicidad en aplicaciones móviles que, por regla general, no se ha solicitado, ni se deseaba recibir y que perjudica a los destinatarios.

NOTA 1 – En la presente, "no solicitado" significa que "el usuario no lo ha pedido" y "no deseado" significa que los usuarios han hecho algo para expresar claramente su rechazo, como por ejemplo desactivar la opción de recibir algún tipo de publicidad.

NOTA 2 – El *spam* publicitario en aplicaciones móviles suele enviarse de manera indiscriminada, en masa y de manera repetitiva. Entre los ejemplos de perjuicios reales y tangibles figuran el fraude o la transmisión de códigos maliciosos.

3.2.5 filtrado síncrono: técnica de procesamiento de ficheros para identificar anuncios de *spam*, que espera hasta terminar de procesar uno antes de procesar el siguiente.

4 Siglas y acrónimos

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

AD Anuncio (*advertisement*)

API Interfaz para la programación de aplicaciones (*application program interface*)

ID Identidad

IP Protocolo Internet (*Internet protocol*)

URL Localizador uniforme de recursos (*uniform resource locator*)

5 Convenios

Ninguno.

6 Consideraciones generales

Debido a la rápida evolución de Internet móvil y a la naturaleza abierta de los sistemas operativos móviles, la publicidad en las aplicaciones móviles también se ha desarrollado a gran velocidad. Por regla general, para enviar publicidad (anuncios) las aplicaciones móviles invocan la interfaz para la programación de aplicaciones (API) suministrada por la plataforma del servicio. Como la publicidad que hace a través de las aplicaciones móviles es gratuita o semigratuita, se han popularizado mucho los anuncios publicitarios en aplicaciones móviles. Muchos anuncios son publicidad legítima que resulta aceptable para los usuarios, mientras que otros son *spam*. Se han adoptado diversas medidas para bloquear el *spam*, como la aceptación o el rechazo explícito.

Si bien se han aplicado muchas medidas para contrarrestar el *spam* publicitario en aplicaciones móviles, sigue haciendo falta un marco técnico para luchar contra el mismo. El *spam* publicitario en aplicaciones móviles puede afectar negativamente a las aplicaciones y a los proveedores de servicio. El *spam* publicitario en aplicaciones móviles puede consumir mucho ancho de banda o generar congestión en el tráfico de datos e incluso puede ser el origen de fraude móvil. Ninguna medida concreta ha demostrado ser una solución totalmente adecuada para contrarrestar el *spam*. Se trata pues de definir un marco práctico para contrarrestar el *spam* publicitario en aplicaciones móviles, que pueda integrar muchas de las ventajas de todas las medidas empleadas a este respecto.

7 Marco técnico

Los sistemas de filtrado para contrarrestar el *spam* publicitario en aplicaciones móviles (es decir, sistemas de filtrado de *spam*) se integran principalmente en plataformas de servicio que ofrecen API para aplicaciones. Las aplicaciones pueden invocar estas API para enviar anuncios y otros mensajes. En la Figura 1 se muestra el marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles.

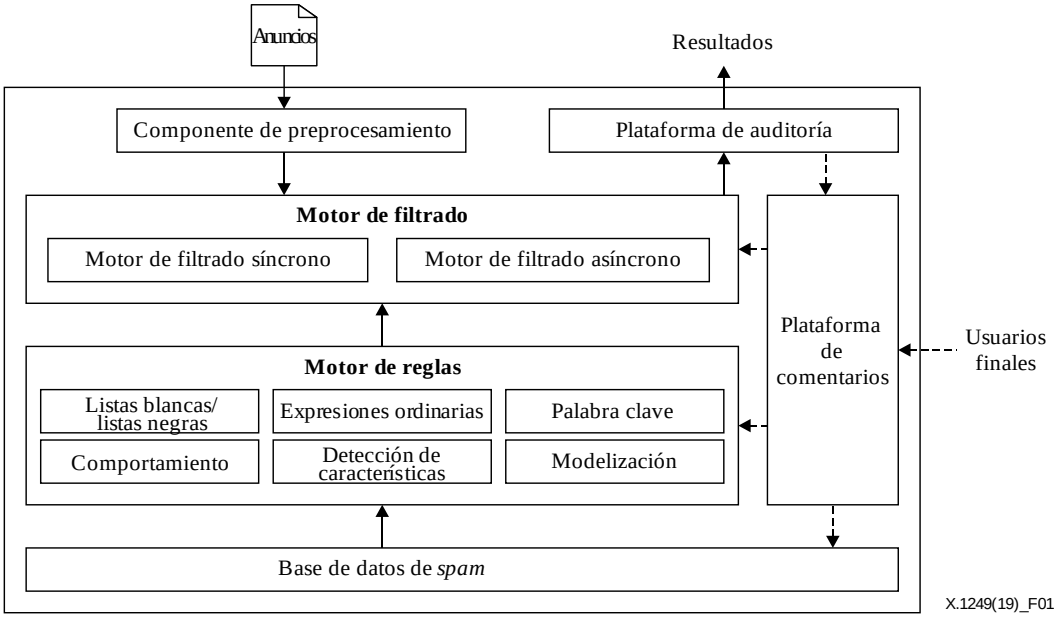

Figura 1 – Marco técnico para contrarrestar el *spam* publicitario en aplicaciones móviles

8 Componentes funcionales

8.1 Componente de preprocesamiento

El componente de preprocesamiento se utiliza para preprocesar los ficheros de anuncios originales y convertirlos al formato exigido por los motores de filtrado, como la separación del contenido de texto, las imágenes, el localizador uniforme de recursos (URL), el audio y el vídeo, etc.

8.2 Motores de filtrado

Los motores de filtrado son los componentes más importantes de los sistemas de filtrado de *spam* publicitario en aplicaciones móviles. El principal objetivo de los motores de filtrado es identificar el *spam* publicitario en aplicaciones móviles reales o la posibilidad de dicho *spam*. Con arreglo a las distintas maneras de identificar el *spam* publicitario en aplicaciones móviles, los motores de filtrado se pueden clasificar en síncronos o asíncronos. En términos de eficiencia temporal, un motor de filtrado asíncrono es mejor que un motor de filtrado síncrono.

8.2.1 Motor de filtrado síncrono

El filtrado síncrono es el que espera a terminar una regla de filtrado antes de aplicar la siguiente. El filtrado síncrono se denomina filtrado en línea debido a su menor complejidad y a que los resultados del filtrado se obtienen en muy poco tiempo. Por lo general, los resultados del filtrado síncrono se conocen inmediatamente, lo que significa que las decisiones pueden tomarse en cuanto termina éste. Si los resultados de la regla de filtrado afectan a la ejecución de las subsiguientes reglas de filtrado, se sugiere utilizar el filtrado asíncrono. El filtrado síncrono puede incluir el filtrado basado en listas blancas o negras, expresiones ordinarias, modelos de comportamiento, detección de características, etc.

8.2.2 Motor de filtrado asíncrono

El filtrado asíncrono permite ejecutar diversos procesos de trabajo al mismo tiempo, es decir, cada flujo de trabajo no depende del resultado de los demás. El filtrado asíncrono se denomina también filtrado fuera de línea debido a la mayor complejidad del filtrado del *spam* publicitario en aplicaciones móviles y a que los resultados del filtrado tardan mucho tiempo en obtenerse. El filtrado asíncrono suele incluir reconocimiento de audio y de vídeo, la concordancia de palabras clave, modelización profunda, etc.

8.3 Motores de reglas

Los motores de reglas proporcionan reglas de filtrado, incluidas todas las que pueden utilizarse en los motores de filtrado. Las reglas de filtrado tienen varias fuentes: configuraciones del operador, bases de datos de *spam* y compartición de reglas de terceros. El motor de reglas proporciona reglas destinadas a tomar decisiones para identificar *spam* publicitario en aplicaciones móviles. Algunas de estas reglas se basan en la suma de valores ponderados de las diferentes pruebas de *spam*, si los resultados del filtrado no son determinantes. El motor de reglas proporciona un valor umbral (es decir, fijo). Si la suma es superior al valor umbral, el motor de filtrado decidirá que el anuncio es *spam*. Además, el motor de reglas puede integrar distintos factores de detección procedentes del motor de filtrado para determinar si el anuncio es o no *spam* publicitario en aplicaciones móviles.

8.4 Plataforma de auditoría

No todo el *spam* publicitario en aplicaciones móviles puede detectarse con motores de filtrado. Por consiguiente, deben utilizarse métodos manuales para evaluar el *spam*, por lo que se recurre a una plataforma de auditoría. A través de esta plataforma, el auditor puede detectar *spam* publicitario en aplicaciones móviles desconocidas que los motores de filtrado no pudieron reconocer. La exactitud de la plataforma de auditoría suele ser mayor que la de los motores de filtrado. Por consiguiente, los resultados de la plataforma de auditoría pueden registrarse en una base de datos de *spam* publicitario en aplicaciones móviles para su utilización ulterior.

8.5 Base de datos de *spam* publicitario en aplicaciones móviles

Esta base de datos se utiliza para almacenar características de *spam* publicitario en aplicaciones móviles. Se trata de una base de datos lógica que puede ser mantenida por cada proveedor de servicio o compartirse entre varios proveedores de servicio. Las características del *spam* publicitario en aplicaciones móviles de la base de datos pueden utilizarse con fines comparativos y de filtrado. Enriquecer la base de datos de *spam* publicitario en aplicaciones móviles puede ayudar a mejorar el rendimiento de los motores de reglas. La base de datos de *spam* publicitario en aplicaciones móviles puede enriquecerse si la plataforma de información extrae las características del *spam* publicitario en aplicaciones móviles nuevamente.

8.6 Plataforma de comentarios

Los usuarios finales son los destinatarios, las víctimas y los receptores del *spam* publicitario en aplicaciones móviles. Además de los resultados de la plataforma de auditoría, la participación de los usuarios finales sirve de ayuda para contrarrestar eficaz y eficazmente el *spam* publicitario en aplicaciones móviles. Por consiguiente, la plataforma de comentarios debe tomar en consideración las respuestas de los usuarios. Hay que establecer mecanismos para cumplir este objetivo, por ejemplo, mecanismos de formulación de comentarios sobre la base de datos de anuncios *spam*. Los procedimientos para gestionar esos comentarios deben ser transparentes, eficientes y eficaces. Además, estas plataformas deben registrar los comentarios en un formato normalizado, a fin de que diferentes operadores y entidades puedan compartirlos. La compartición de comentarios permite obtener las principales direcciones de los remitentes de *spam*, las cuales pueden añadirse y utilizarse en las listas negras.

9 Reglas de filtrado

9.1 Palabras clave

Se utilizan palabras clave para determinar si el contenido (es decir, las palabras) de un anuncio concuerda con las muestras registradas en la base de datos de *spam* publicitario en aplicaciones móviles. Las palabras clave se obtienen de las fuentes siguientes: configuración del operador, canales externos, plataforma de comentarios y aprendizaje automático a partir de las bases de datos de *spam*.

Las palabras clave pueden servir para identificar con exactitud anuncios maliciosos de elevado riesgo, de manera rápida y económica; por ese motivo se suelen utilizar en el filtrado síncrono. Para mejorar el efecto de las palabras clave, es necesario considerar la posibilidad de procesar previamente el texto original para filtrar caracteres mal escritos deliberadamente y otros tipos de codificación de palabras clave, especialmente al filtrar direcciones URL.

9.2 Listas negras/blancas

Las listas negras se basan en el principio de mantener direcciones o dominios del protocolo Internet (IP) que son sospechosos de enviar *spam* publicitario en aplicaciones móviles. Estas listas pueden también incluir la identidad del dispositivo (ID), los URL o las cuentas remitentes en la plataforma del servicio. Pueden confeccionarlas una entidad para su uso compartido o puede ser la plataforma del servicio la que las cree y mantenga con arreglo a sus necesidades. Las listas blancas se basan en el principio de enumerar las fuentes y entidades de anuncios aprobados o reconocidos. Estas listas pueden también incluir la ID del dispositivo o las cuentas remitentes en las plataformas de servicio. Al igual que las palabras clave, aunque las listas negras y blancas contienen inevitablemente errores y las listas negras pueden posiblemente evitar que algunos anuncios legítimos se pasen por los motores de filtrado, ambos tipos de listas son una solución eficaz para filtrar *spam* publicitario en aplicaciones móviles.

9.3 Expresiones ordinarias

Las expresiones ordinarias se utilizan generalmente para determinar la concordancia exacta y filtrar anuncios maliciosos en formato de texto con arreglo a determinados patrones. Son flexibles, lógicas y funcionales, por lo que suelen dar lugar a un resultado final que no requiere un examen adicional o modificaciones. A diferencia de las palabras clave o las listas negras/blancas, las expresiones ordinarias pueden utilizarse para determinar la concordancia de una serie de anuncios que difieren en contenido, pero tienen un formato concreto. También se utilizan ampliamente en el filtrado síncrono con el fin de aumentar la eficiencia. Las expresiones ordinarias también se utilizan ampliamente en el filtrado síncrono, dado que cuando están bien concebidas aumentan la exactitud. A fin de evitar un consumo imprevisible de recursos, antes de su utilización se deben efectuar pruebas completas de las expresiones ordinarias, incluidas pruebas de rendimiento y exactitud.

9.4 Detección de características

La detección de características es una aplicación común de la visión artificial basada normalmente en el reconocimiento de patrones y el aprendizaje automático. La aplicación más representativa de la detección de características es el reconocimiento de anuncios maliciosos a partir de miles de imágenes. Para realizar la detección de características se necesita calcular, extraer y almacenar en una base de datos las características del *spam* publicitario en aplicaciones móviles conocidas. Cuando se recibe una imagen sospechosa, la detección de características extrae información de la imagen y toma una decisión para determinar si contiene anuncios maliciosos. Los algoritmos de extracción de características y los correspondientes algoritmos de determinación de concordancias determinan si se pueden encontrar rápidamente y con exactitud imágenes publicitarias maliciosas. Por lo general suele llegar a una conclusión parcial, por lo que se ha de combinar con otros procesos de adopción de decisiones para determinar el resultado final. Debido a la complejidad de los cálculos y la necesidad de comparar el fichero íntegro, la detección de características se utiliza sobre todo en el filtrado asíncrono.

9.5 Comportamiento

El *spam* publicitario en aplicaciones móviles se suele enviar de manera masiva, indiscriminada o repetitiva, y presenta además otras particularidades. Los motores de filtrado pueden registrar el comportamiento de los anuncios móviles y calcular las relaciones entre ellos. Cuando el comportamiento de los anuncios recibidos se corresponde con las características ya almacenadas en

la base de datos de *spam*, es posible determinar que el fichero sea probablemente un anuncio *spam*. Dado que el comportamiento de los anuncios es independiente del tiempo, la detección del comportamiento puede utilizarse para identificar anuncios maliciosos desconocidos, por lo que es más adecuado para el filtrado asíncrono.

9.6 Verificación mediante modelos

La verificación mediante modelos es un método importante que ha surgido para verificar requisitos. Por ejemplo, el modelo de similitudes y el modelo de árbol de decisiones son eficaces a la hora de detectar *spam* publicitario en aplicaciones móviles. A veces un determinado modelo no puede determinar si un anuncio es malicioso, por lo que para obtener una detección más exhaustiva puede recurrirse a la combinación de varios modelos, como el apilamiento de modelos. La verificación mediante modelos puede utilizarse tanto en el filtrado síncrono como en el asíncrono.

10 Diagrama de flujo

El filtrado de *spam* publicitario en aplicaciones móviles suele seguir el proceso en serie mostrado en la Figura 2. En algunos casos, los motores de filtrado síncrono y de filtrado asíncrono pueden funcionar en paralelo.

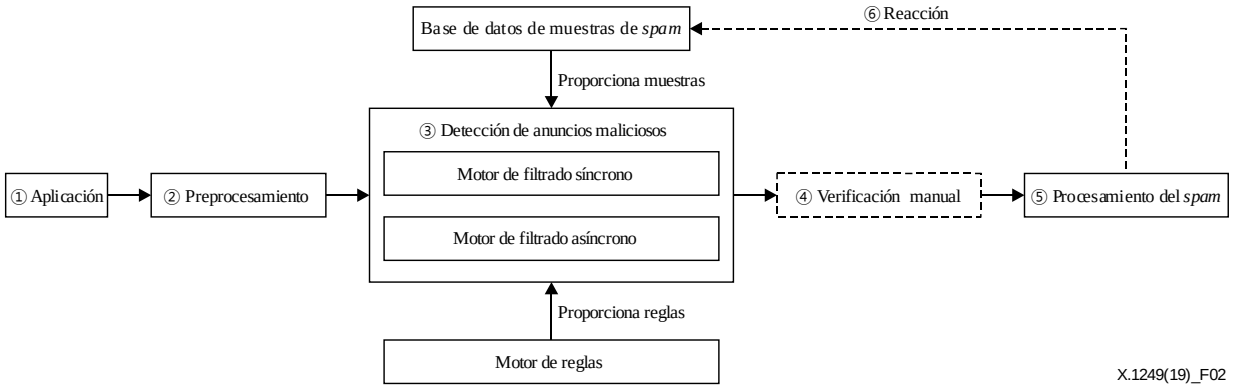

Figura 2 – Diagrama de flujo del filtrado de anuncios de *spam*

En general, los pasos son los siguientes:

1) Se suministran y envían anuncios a las aplicaciones del teléfono móvil.
2) En primer lugar, se efectúa un preprocesamiento. Por ejemplo, se separan los diversos tipos de medios publicitarios en URL, texto, audio, vídeo, etc.
3) Dependiendo de las amenazas y de la complejidad del filtrado, el contenido se suministra al motor de filtrado síncrono o al asíncrono, que están preconfigurados pero que pueden ajustarse en función de las necesidades. Para una detección exhaustiva, a veces es necesario cargar el mismo contenido en los dos motores de filtrado, el síncrono y el asíncrono. Combinados junto con las reglas y las muestras proporcionadas por el motor de reglas y la base de datos de muestras de *spam* publicitario en aplicaciones móviles, se examinan los anuncios para determinar si es necesario proceder al filtrado.
    a) El motor de filtrado síncrono detecta el *spam* publicitario en aplicaciones móviles en los anuncios en el paso 2, basándose en las reglas de filtrado del motor de reglas. Si el módulo de filtrado síncrono encuentra *spam* publicitario en aplicaciones móviles, el filtrado termina y el anuncio se bloquea inmediatamente; se procede al paso 6. Si los URL o las cuentas en las aplicaciones figuran en la lista blanca del motor de filtrado síncrono, el anuncio se retransmite directamente. Si no se puede determinar, se procede al paso 4.

b) El motor de filtrado asíncrono detecta *spam* en los anuncios en el paso 2, basándose en las reglas de filtrado del motor de reglas. Si el módulo de filtrado asíncrono encuentra *spam*, el filtrado termina y el anuncio se bloquea inmediatamente; se procede al paso 6. Si no se puede determinar, se procede al paso 4.

4) A veces es preciso verificar y evaluar los anuncios manualmente. Si se detecta y confirma la existencia de *spam*, se procede al paso 5.

5) El *spam* se tramita dependiendo de la preconfiguración, por ejemplo, se registra, se sustituye, etc.

6) El *spam* publicitario en aplicaciones móviles se almacena en la base de datos de *spam* publicitario en aplicaciones móviles. Además, el *spam* publicitario en aplicaciones móviles contenido en la base de datos de *spam* puede extraerse como nuevas reglas y cargar en el motor de reglas, o se puede utilizar para optimizar el motor de reglas.

11 Requisitos de rendimiento

La exactitud de la detección de *spam* publicitario en aplicaciones móviles debe cuantificarse mediante la combinación del índice de falsos positivos y el de falsos negativos, que deben considerarse equilibrados.

11.1 Requisitos de exactitud

El índice de falsos positivos se calcula como la relación entre el número de anuncios válidos que se confunden con *spam* o maliciosos y el número total de anuncios válidos. Si el índice de falsos positivos es elevado, significa que se han bloqueado publicidades válidas para las aplicaciones móviles. Por consiguiente, se debe tratar de reducir lo más posible el índice de falsos positivos.

El índice de falsos negativos se calcula como la relación entre el número de anuncios de *spam* publicitario en aplicaciones móviles que se confunden con anuncios válidos y el número total de anuncios de *spam* publicitario en aplicaciones móviles. Si el índice de falsos negativos es elevado, significa que los usuarios recibirán más *spam* publicitario en aplicaciones móviles. Por consiguiente, se debe tratar de reducir lo más posible el índice de falsos negativos.

11.2 Requisitos de eficiencia

La eficiencia del algoritmo de filtrado de *spam* publicitario en aplicaciones móviles puede medirse por su complejidad temporal y espacial en el motor de filtrado. Por complejidad temporal se entiende el tiempo necesario para filtrar un anuncio, mientras que la complejidad espacial es el espacio necesario para ello (memoria). Estos dos indicadores afectan sobremanera al tipo de aplicación de la regla de filtrado. En el filtrado síncrono se pueden aplicar reglas de filtrado de menor complejidad temporal y espacial, mientras que las de mayor complejidad se aplicarán en los motores de filtrado asíncrono.

Bibliografía

[b-UIT-T X.509] Recomendación UIT-T X.509 (2016), *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

[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.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.*

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

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

[b-UIT-T X.1254] Recomendación UIT-T X.1254 (2012), *Marco de garantía de autenticación de entidad.*

[b-UIT-T X-Sup.19] Recomendaciones UIT-T de la serie X – Suplemento 19 (2013), *Supplement on security aspects of smartphones.*

[b-UIT-T X-Sup.24] Recomendaciones UIT-T de la serie X – Suplemento 24 (2014), *Suplemento sobre marcos seguros de distribución de aplicaciones para dispositivos de comunicación.*

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 telegráficos
Serie T	Terminales para servicios telemáticos
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 los sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2019