(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 382 361**

(51) Int. CI.:
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05250157 .4**
(96) Fecha de presentación: **14.01.2005**
(97) Número de publicación de la solicitud: **1681825**
(97) Fecha de publicación de la solicitud: **19.07.2006**

(54) Título: **Sistema de seguridad basado en red**

(45) Fecha de publicación de la mención BOPI:
07.06.2012

(45) Fecha de la publicación del folleto de la patente:
07.06.2012

(73) Titular/es:
BAE SYSTEMS PLC
6 Carlton Garden, London
SW1 5AD, GB

(72) Inventor/es:
Curnyn, Jon

(74) Agente/Representante:
González Palmero, Fe

DESCRIPCIÓN

Sistema de seguridad basado en red

Antecedentes de la invención

La suplantación de identidad (*phishing*) es un problema en aumento en el que personas u organizaciones criminales o malintencionadas engañan a personas u organizaciones desprevenidas para que revelen información corporativa o personal, permitiendo el robo de identidad de las víctimas. La suplantación de identidad se compone habitualmente de dos partes:

(1) Entregar mensajes de suplantación de identidad; y,

(2) Efectuar el ataque de suplantación de identidad.

La entrega de un mensaje de suplantación de identidad puede producirse a través de cualquier aplicación de Internet tal como correo electrónico, navegador web, medios de comunicación, mensajería instantánea (IM), y el suplantador de identidad (*phisher*) envía información en estos mensajes esperando engañar al usuario desprevenido para que proporcione sin darse cuenta información al suplantador de identidad. Los mensajes usan ingeniería social y otras técnicas usadas por creadores de virus para facilitar el ataque de suplantación de identidad.

El ataque de suplantación de identidad puede ser uno en el que el usuario ejecuta sin percatarse el ataque, o mediante medios automatizados empleados normalmente por los creadores de virus. Por ejemplo, el usuario puede estar instruido para ir a un sitio web, que él/ella cree que es su banco, e introducir su nombre y contraseña de banca en línea, pero el sitio está operado en realidad por el suplantador de identidad. De manera similar, el ataque puede implicar la descarga de *malware* que captura automáticamente información (por ejemplo, los registradores de pulsaciones de teclas (*keylogger*)) o aprovecha las vulnerabilidades en la máquina del usuario lo que provocará que la información se envíe al suplantador de identidad, cuando el usuario cree que se está enviando a un sitio legítimo.

La intercepción de la entrega de mensajes de suplantación de identidad puede lograrse por la existencia de herramientas de seguridad de contenido tales como filtros *antispam* y bloqueadores de contenido de página web (que bloquean tipos genéricos de contenido tales como *scripts* o controles *ActiveX*).

Estas defensas pueden proporcionar buena protección de ataques de suplantación de identidad, pero algunos mensajes siempre pasarán, y entonces pueden provocar que se produzca un ataque de suplantación de identidad sobre la víctima.

También se conoce inspeccionar sitios web periódicamente en cuanto al uso de logotipos y mensajes no autorizados, y si éstos están pensados entonces para usarse en ataques de suplantación de identidad, los sitios web se añaden a listas de bloqueo usadas por productos de filtrado de webs convencionales.

Las soluciones actuales en lugar de impedir la ejecución de un ataque de suplantación de identidad son soluciones tanto lentas como incompletas. Los sistemas en la actualidad que preparan filtros de *spam* y bloqueadores de filtrado web están de manera eficaz fuera de línea, y con frecuencia llevados a cabo por la gente, de manera que la detección de nuevos mensajes de suplantación de identidad o sitios web puede llevar días antes de que esta información alcance el sistema de defensa.

De manera similar, los suplantadores de identidad cambian constantemente sus sitios de ataque, de manera que nunca pueden observarse mediante métodos de detección fuera de línea. Normalmente, los sitios de suplantación de identidad existen durante alrededor de 48 horas. Por tanto, cualquier información tal como firmas cargadas en los sistemas de defensa siempre estará incompleta.

Sumario de la invención

Según un primer aspecto de la presente invención, se proporciona un método alojado en red para proporcionar un servicio de seguridad de contenido de protección de suplantación de identidad, que comprende:

(i) almacenar una pluralidad de direcciones de red legítimas con datos asociados;

(ii) analizar el tráfico soportado por la red para los datos que aparecen relacionados con los datos asociados;

(iii) impedir en el caso de que los datos de tráfico soportado por la red analizados en la etapa (ii) estén relacionados con los datos asociados, el acceso de usuario a cualquier dirección de red que sea el origen o el destinatario previsto de dichos datos de tráfico soportado por la red en el que dicha dirección de red no es una dirección de red legítima almacenada; y,

(iv) añadir direcciones de red a las que se impide el acceso de usuario a una lista de direcciones de red prohibidas.

Según un segundo aspecto de la invención se proporciona un producto de programa informático que comprende

instrucciones ejecutables por ordenador para realizar el método de la presente invención.

Según un tercer aspecto de la presente invención se proporciona un sistema alojado en red para proporcionar un servicio de seguridad de contenido de protección de suplantación de identidad, que comprende:

un medio de almacenamiento para almacenar una pluralidad de direcciones de red legítimas con datos asociados;

medios para analizar el tráfico de red para los datos que aparecen relacionados con los datos asociados; y,

medios para impedir el acceso de usuario a cualquier dirección de red que sea el origen o el destinatario previsto de dichos datos de tráfico de red en el caso de que se descubra que dichos datos de tráfico de red están relacionados con los datos asociados y que dicha dirección de red no es una dirección de red legítima almacenada y añadir direcciones de red a los que se niega el acceso de usuario a una lista de direcciones de red prohibidas.

La presente invención se implementa preferiblemente en Internet como un servicio de protección de suplantación de identidad. En particular; puede proteger contra ataques en la *world wide web* o el correo electrónico. Sin embargo, puede implementarse en otros tipos de redes, por ejemplo para proteger contra ataques de suplantación de identidad de servicio de mensajes cortos (SMS), y también puede usarse para proteger contra otros fallos de seguridad, por ejemplo podría usarse para impedir la infracción del derecho de autor o marca registrada.

Cuando se usa para proporcionar un servicio de protección de suplantación de identidad, la presente invención analiza automáticamente el contenido tal como se transfiere entre un usuario y un sitio remoto, y comprueba si este contenido se conoce que va a usarse por los suplantadores de identidad, o puede originarse por los suplantadores de identidad. Si se descubre que el contenido que es del tipo usado por los suplantadores de identidad entonces la dirección del sitio remoto se contrasta con una lista de sitios legítimos, y si el sitio remoto no está en la lista entonces se niega el acceso a este. Preferiblemente, esto se produce en tiempo real a medida que el usuario descarga el contenido y no depende de la actualización de cualquier información basada en firma que se determina fuera de línea. Esto es una ventaja significativa sobre con la técnica anterior puesto que es imposible para los suplantadores de identidad superar la protección al cambiar la dirección web del sitio de suplantación de identidad.

Los datos almacenados por la presente invención preferiblemente incluyen información conocida de sitios web comerciales legítimos susceptibles de ser objeto de ataques de suplantación de identidad de sus clientes (por ejemplo logotipos, palabras clave, estilos, direcciones de IP, URL). Esto permite que los ataques de suplantación de identidad a estos sitios web se detecten por la presente invención. Los datos asociados con sitios legítimos también pueden incluir los identificadores o credenciales usados por el usuario para identificar a los mismos para ese sitio.

El tráfico de red preferiblemente comprende uno o más de los siguientes: el usuario solicita el contenido desde una dirección, el contenido se transmite al usuario desde un sitio remoto, y el contenido se transmite a un sitio remoto desde el usuario. La presente invención puede, por tanto, detectar la suplantación de identidad u otros ataques en varias fases posibles, permitiendo que se proporcione una defensa por capas. En el caso de suplantación de identidad, si la presente invención falla en impedir a un usuario acceder a un sitio de suplantación de identidad, no obstante, puede reconocer el contenido descargado desde ese sitio como relacionado con la suplantación de identidad. Si esto también falla entonces la presente invención impide al usuario transmitir detalles personales a cualquier sitio web que no se sepa que es legítimo. Esto permite que la presente invención proporcione una solución significativamente más eficaz que métodos previos, no por capas.

Preferiblemente, se usan varios algoritmos para determinar si los datos de tráfico de red están relacionados con los datos almacenados. Éstos puede incluir pero no se limitan a, análisis léxico, reconocimiento de imágenes, coincidencia de patrones exacta e inexacta y cálculo de resumen. También se concibe que en algunos casos los datos se consideren relacionados debido al protocolo adoptado.

Cuando la presente invención determina que un intento de violación de seguridad está en curso, se niega el acceso de usuario al sitio sospechoso y se envía preferiblemente una notificación al usuario en lugar de cualquier dato solicitado. Esta notificación proporciona realimentación al usuario. Por ejemplo, puede explicar que se ha negado el acceso al sitio relevante e indicar el tipo de ataque detectado por la presente invención. Cuando la presente invención se implementa a través de Internet la notificación preferiblemente adopta la forma de una página de bloqueo aunque se reconoce que puede tener una forma diferente en otros tipos de red.

Se conoce que aquellos que perpetran ataques de red con frecuencia realizan “pruebas de vulnerabilidad” para determinar las capacidades de cualquier sistema de seguridad presente. Por tanto, se concibe que, para detectar un ataque, puede realizarse una comprobación que determina si una prueba de vulnerabilidad está en curso. Por ejemplo, puede suponerse que una prueba de vulnerabilidad está en curso si N ataques similares se han producido en un tiempo T. Preferiblemente, cuando se detecta una prueba de vulnerabilidad, se impide el envío de una notificación del tipo descrito anteriormente puesto que una notificación de este tipo puede poner sobre aviso al atacante de las capacidades de la presente invención.

Preferiblemente, la presente invención informa a los propietarios del sitio legítimo de cualquier intento de violación de seguridad.

La presente invención puede usarse en combinación con productos de seguridad de contenido existentes. Por ejemplo, un filtro web convencional puede contener una gran base de datos de dominios o sitios web, y puede, por tanto, usarse para eliminar muchos sitios web legítimos que están usándose en ataques de suplantación de identidad. De manera similar, los filtros *antispam* incorporan listas negras de direcciones de red, que incluyen las usadas por los suplantadores de identidad, por tanto, pueden identificar contenido que está enviándose hasta/desde los suplantadores de identidad. Por tanto, se concibe que la presente invención pueda usar estos sistemas convencionales como una línea de seguridad inicial, y que la información deducida por la presente invención pueda usarse para actualizar tales sistemas. Por ejemplo, en el caso de filtros *antispam*, esta actualización puede comprender una adición a la lista negra o reponderación de reglas heurísticas.

La presente invención puede implementarse en varios dispositivos, por ejemplo un PC, pero para un alto rendimiento para varios usuarios, se prefiere un dispositivo de análisis de hardware dedicado que tiene capacidad de análisis en tiempo real.

Breve descripción de los dibujos

Ahora se describirá en detalle un ejemplo de la presente invención con referencia a los dibujos adjuntos, en los que:

la figura 1 muestra la posición de una puerta de enlace de seguridad de contenidos (CSG) en una red que conecta servidores remotos con un usuario;

la figura 2 muestra un diagrama conceptual de la operación de una puerta de enlace de seguridad de contenidos (CSG) según una realización de la presente invención;

la figura 3 es un diagrama de flujo que ilustra una comprobación de URL según la presente invención;

la figura 4 es un diagrama de flujo que ilustra un análisis de contenido según la presente invención; y,

la figura 5 es un diagrama de flujo que ilustra comprobación de información personal según la presente invención.

Descripción detallada

En una realización preferida, la presente invención se implementa usando una puerta de enlace de seguridad de contenidos (CSG). Una CSG es un dispositivo de propósito múltiple que puede proporcionar varios servicios de seguridad en tiempo real al usuario. Por ejemplo, puede comprender capacidades de *antispam* y de antivirus además del sistema de protección de suplantación de identidad de la presente invención. Tal como puede observarse en la figura 1, la CSG 12 intercepta todos los datos transmitidos entre servidores 10 remotos u otros dispositivos y el usuario 14 a través de Internet 11. En el ejemplo mostrado en la figura 1, el usuario está alojado en una red 13 de área local (LAN) y la CSG 12 puede monitorizar los datos transmitidos hasta/desde cualquier dispositivo en la LAN 13. Además, aunque no se muestre en la figura 1, la CSG 12 puede estar monitorizando de manera independiente los datos transmitidos a dispositivos adicionales no en la LAN 13 del usuario. Por tanto, la CSG 12 puede monitorizar los datos transmitidos a una pluralidad de destinatarios, y por tanto puede detectar ataques de suplantación de identidad o de spam masivos, identificando y anulando amenazas antes que hardware o software de seguridad alojado por (y que da servicio sólo a) el usuario 14.

En una realización preferida, la CSG 12 forma parte de un sistema del ISP, y sus capacidades son, por tanto, servicios proporcionados por el ISP al usuario. Alternativamente, la CSG 12 puede implementarse en el nivel de la LAN 13 o en cualquier otro nivel en el que la CSG 12 pueda interceptar todos los datos previstos para el usuario.

En una realización preferida, la CSG 12 se realiza como un producto de sistema integrado que incorpora hardware, software y elementos microcodificados, que cuando se combinan con otros elementos de infraestructura convencionales tales como bases de datos y servidores web, permiten a un proveedor de servicio gestionado, entregar servicios de seguridad de contenido en tiempo real.

Un diagrama conceptual de la operación de una CSG se muestra en la figura 2. Se recibe tráfico de red, luego se identifica, y entonces se manipula, antes de transmitirse. Tal como puede observarse en la figura 2, se proporcionan una pluralidad de módulos de servicio (etiquetados servicio 1 a servicio N). Habiéndose identificado, los datos se envían al módulo de servicio definido por la política. Cada módulo de servicio puede proporcionar un servicio diferente (tal como *antispam* o antivirus) o alternativamente pueden dedicarse varios módulos de servicio a cada servicio con el fin de mejorar la velocidad en la que se procesan datos. La provisión de una pluralidad de módulos de servicio permite optimizar cada módulo para la tarea que lleva a cabo.

Sin embargo, se reconoce que la presente invención puede implementarse por dispositivos distintos de las CSG. Puede usarse cualquier dispositivo con la potencia computacional requerida que esté en una posición que intercepta todas las comunicaciones entre el usuario y el sitio remoto. Por ejemplo, si el volumen de tráfico es pequeño, o bien el PC del usuario o bien el PC implantado en la puerta de enlace de red (por ejemplo, un *proxy*) pueden implementar el sistema de la presente invención.

En uso, la CSG se programa con las siguientes listas de información

ID de sitio: organización, URL, direcciones de IP,

Palabras clave de URL: por ejemplo, nombres de bancos y otras organizaciones,

Información específica de organización: tamaño de logotipo, colores, formas, compendios de páginas, atributos (por ejemplo, tamaño), palabras clave, imágenes, etc.

Credenciales de usuario: nombres de usuario, contraseñas, PIN, direcciones.

Preferiblemente, las organizaciones tales como bancos y otros servicios financieros proporcionan esta información a los administradores del sistema de protección de suplantación de identidad de manera directa. Como tal, se concibe que estas organizaciones son “asociados” en el servicio de protección de suplantación de identidad y por tanto a continuación en el presente documento se denominarán de esta manera. Sin embargo, es posible que la información se obtenga por otros medios. Por ejemplo, por detalles de “recopilación” simplemente de la *world wide web*.

Una vez que la CSG se prepara con esta información, el usuario puede protegerse entonces mediante un servicio de protección de suplantación de identidad.

El usuario puede recibir un mensaje de suplantación de identidad que lo dirige a un sitio web que están usándose por un suplantador de identidad. La invención lleva a cabo las siguientes defensas:

(i) Comprobación de URL: tal como se muestra en la figura 3, la presente invención intercepta el URL saliente en peticiones de HTTP, y opera con uno o más algoritmos en tiempo real para determinar si el URL destino puede usarse por los suplantadores de identidad. Cuando un navegador de usuario solicita un URL (etapa 301), la presente invención intercepta el flujo y decodifica el protocolo (etapa 302). Entonces extrae el URL y ejecuta diversos algoritmos tras éste (etapa 304) para determinar si el URL podría ser relevante para la suplantación de identidad. Por ejemplo, se consulta el URL para palabras clave (por ejemplo, *Natwest*, *Barclays*), y se considera relevante si una palabra clave de este tipo está presente. Si se determina que el URL no tiene relevancia para la suplantación de identidad entonces se permite la petición (etapa 313). Sin embargo, si el URL parece relevante, entonces se contrasta el URL con una lista de direcciones legítimas (etapa 305). Si el URL es relevante y no está incluido en esta lista de sitio legítimo, se bloquea el acceso del usuario al sitio web sospechoso, por ejemplo, bloqueando la petición HTTP GET (etapa 306). En este caso la presente invención puede ejecutar una “comprobación de prueba de vulnerabilidad” (etapa 307) tal como se describe en mayor detalle a continuación en el punto (v). Si esta comprobación no encontrara evidencia de que una prueba de vulnerabilidad está en curso entonces se proporciona una página de bloqueo (etapa 309) que informa al usuario del ataque intentado y el sitio también se “aprende”, y se añade a un filtro de acceso web convencional que puede estar ejecutando la invención (etapa 311). Debe entenderse que la información de sitio aprendida puede incluir el URL, la dirección de IP y el dominio. Finalmente, se informa al propietario de sitio legítimo del intento de violación de seguridad (etapa 312).

La siguiente es una lista no exhaustiva de algoritmos adecuados para la comprobación de URL:

a) Hacer coincidir palabras clave de URL proporcionadas por asociados, que son un subconjunto del URL total, detectar entonces como falso mediante la comprobación de tamaño frente al URL legítimo). Por ejemplo, el URL falso es www.natwest_com.ukvalidator.com, coinciden en natwest, rechazar por tener demasiados caracteres, o a través del compendio comparar en ambos URL, o en una comparación sencilla con el URL legítimo.

b) Comprobación sencilla de URL objetivo contra una lista negra.

c) Algoritmo de coincidencia difusa y comparar el nombre derivado con una lista de palabras clave (por ejemplo, coincidir en nat_west.com). Comparar entonces el URL derivado con una lista de URL legítimos (atributo, compendio, comparación total).

d) La comprobación con un filtro de acceso web convencional.

e) Cualquier combinación de (a) a (d) anterior.

Alternativa o adicionalmente, la presente invención puede explorar mensajes entrantes, por ejemplo correos electrónicos, para los URL e impedir el acceso de usuario a estos mensajes si se considera que los URL son sospechosos y/o el mensaje no se origina desde una dirección legítima.

También se concibe que pueda ser preferible analizar sólo el dominio en lugar del URL completo.

(ii) Análisis de contenido conocido: si el acceso de sitio web está permitido por la invención, se comprueba el contenido que está retornándose. Tal como se muestra en la figura 4, el contenido se quita de los paquetes de protocolo que lo portan (etapa 401), para conseguir el HTML, y éste se decodifica entonces (etapa 402), y se analiza posteriormente usando una serie de técnicas tales como coincidencia de patrones, cálculo de resumen y comprobación de atributo (etapa 403) frente a la información proporcionada por asociados. Si esta información no coincide, el contenido se considera no relevante para la suplantación de identidad y el contenido pasa al usuario (etapa 413). Si la información coincide, el contenido se considera relevante para la suplantación de identidad y se

identifica como específico para una organización, y el origen del contenido se valida entonces frente a direcciones de IP legítimas para esa organización (etapa 405). Si el origen es legítimo el contenido pasa al usuario (etapa 413). Si no proviene de un origen legítimo, se bloquea el contenido (etapa 406). La presente invención puede entonces ejecutar una "comprobación de prueba de vulnerabilidad" (etapa 408) tal como se describe en mayor detalle a continuación en el punto (v). Si esta comprobación no encuentra evidencia de que una prueba de vulnerabilidad está en curso entonces se proporciona una página de bloqueo (etapa 409) que informa al usuario del ataque intentado y el sitio también se "aprende", y se añade a un filtro de acceso web convencional que puede estar ejecutándose en la invención (etapa 411). Debe entenderse que la información de sitio aprendida puede incluir el URL, la dirección de IP y el dominio. Finalmente, se informa al propietario de sitio legítimo del intento de violación de seguridad (etapa 412).

La siguiente es una lista no exhaustiva de algoritmos adecuados:

a) Calcular compendios de páginas, *scripts*, imágenes y otras características. Comparar con la información de sitios legítimos.

b) Palabras clave de coincidencia de patrones. Comparar con las palabras clave de sitios legítimos.

c) Medir atributos de páginas (por ejemplo, tamaño, colores, fuentes, diseño de página), comparar con la lista de URL legítimos.

d) Cualquier combinación de (a) a (c) anterior.

(iii) Análisis de contenido desconocido: si el acceso de sitio web está permitido por la invención, se comprueba el contenido que está retornándose. Tal como se muestra también en la figura 4, el análisis de contenido desconocido se lleva a cabo de manera preferible conjuntamente con el análisis de contenido conocido. En particular, el contenido se quita de los paquetes de protocolo que lo portan (etapa 401), para conseguir el HTML, y se decodifica entonces (etapa 402) y esto se analiza entonces usando un algoritmo para determinar si el contenido puede intentar pretender darse servicio por un asociado (por ejemplo, la imagen que identifica un logotipo, la aparición de un nombre de organización, etc.) (etapa 403). Si el algoritmo consigue un resultado negativo entonces el contenido pasa al usuario (etapa 413). Si el algoritmo consigue un resultado positivo, el contenido se considera relevante para la suplantación de identidad y se identifica como específico para una organización, y el origen del contenido se valida entonces frente a direcciones de IP legítimas para esa organización (etapa 405). Si el origen es legítimo el contenido pasa al usuario (etapa 413). Si no proviene de un origen legítimo, se bloquea el contenido (etapa 406). En el caso de que se bloquee el contenido, la presente invención puede ejecutar entonces una "comprobación de prueba de vulnerabilidad" (etapa 408) tal como se describe en mayor detalle a continuación en el punto (v). Si esta comprobación no encuentra evidencia de que una prueba de vulnerabilidad está en curso entonces se proporciona una página de bloqueo (etapa 409) que informa al usuario del ataque intentado y el sitio también se "aprende", y se añade a un filtro de acceso web convencional que puede estar ejecutándose en la invención (etapa 411). Debe entenderse que la información de sitio aprendida puede incluir el URL, la dirección de IP y el dominio. Finalmente, se informa al propietario de sitio legítimo del intento de violación de seguridad (etapa 412).

La siguiente es una lista no exhaustiva de algoritmos adecuados:

a) Análisis de imágenes para determinar un compendio de formas (por ejemplo, logotipos). Comparar con compendios de sitios legítimos.

b) Análisis de imágenes: comparar colores en uso con sitios legítimos.

c) Análisis léxico: aplicar testigos al contenido, ejecutar el algoritmo heurístico que pondera palabras clave (por ejemplo, un banco).

d) Análisis de atributos: medir atributos de páginas (por ejemplo, tamaño, colores, fuentes, diseño de página), comparar con listas de atributos de URL legítimos.

e) Cualquier combinación de (a) a (d) anterior.

(iv) Comprobación de información personal: si las defensas anteriores no impiden el acceso al destino que está usándose en el ataque de suplantación de identidad, entonces, tal como se muestra en la figura 5, la invención monitoriza el acceso a destinos (por ejemplo, sitios web) y busca en el contenido saliente credenciales e identificadores de usuario. Cuando el navegador del usuario transmite tal contenido (etapa 501) la invención se pone sobre aviso inicialmente de la posibilidad de un ataque de suplantación de identidad mediante el protocolo usado (etapa 502). Por ejemplo, los HTTP POST se usan con frecuencia para portar credenciales e identificadores de usuario. Cuando se detecta un protocolo de este tipo la invención busca para ver si los detalles del usuario particular están disponibles (etapa 504) (es decir, si las credenciales e identificadores de usuario se almacenan para este usuario). Si la invención no tiene acceso a estos detalles entonces el contenido se considera relevante para la suplantación de identidad por defecto y sólo se permite pasar (etapa 511) si la dirección del URL objetivo está en una lista blanca (etapa 507). Sin embargo, si el acceso a estos detalles está disponible entonces se busca en ellos a

través de técnicas de coincidencia de patrones sencillas (con anticonfusión) (etapa 505). Si se encuentran los identificadores y credenciales del usuario, entonces el contenido se considera de nuevo relevante para la suplantación de identidad y sólo se permite pasar (etapa 511) si la dirección del URL objetivo está en una lista blanca (etapa 507). Si no se encuentran entonces se permite automáticamente al contenido pasar (etapa 511). Si el contenido es relevante para la suplantación de identidad y la dirección del URL objetivo no está en la lista blanca entonces se bloquean los datos (etapa 508), el URL y la dirección y dominio de IP asociados, se añaden a una lista de sitios de suplantación de identidad (etapa 509), y se informa al propietario de sitio (etapa 510).

(v) Comprobación de prueba de vulnerabilidad: se conoce ampliamente de escritores o distribuidores de mensajes *de malware* o *spam*, probar productos que bloquean, detectan o notifican *malware* o *spam* distribuido por aquellos escritores o distribuidores. El propósito de estas pruebas por el escritor o distribuidor es buscar debilidades (o vulnerabilidades) en las capacidades de detección y bloqueo de estos productos, usando nuevas formas de contenido, o nuevas técnicas de confusión, o nuevas combinaciones de ambas para determinar cómo hacer estos productos inútiles.

Tal como se muestra en las figuras 3 y 4, cuando se encuentra evidencia de suplantación de identidad la presente invención, por tanto, autocomprueba altos volúmenes de apariciones de URL o contenido que son similares a los URL o contenido conocidos que son de naturaleza similar uno con el otro, o de naturaleza similar a sitios conocidos (etapas 307 y 407). Si estos volúmenes traspasan un umbral programado, se supone que una “prueba de vulnerabilidad” está en curso, y esto se notifica a los asociados (etapas 312 y 412). También es posible para el URL objetivo (y dominio y direcciones de IP asociados) que van añadirse a una lista de sitios web de suplantación de identidad en este punto (etapas 310 y 410). Sin embargo, esto no es necesariamente deseable puesto que una prueba de vulnerabilidad puede incluir un gran número de peticiones de sitios que no existen y de direcciones similares (por ejemplo, mybank001, mybank002, mybank003 etc.). Por tanto, la presente invención contiene algoritmos para decidir si un URL debe añadirse a la lista o no, y si es así, si debe incluirse sólo el URL exacto o coincidencias imperfectas del URL. Cuando se detecta una prueba de vulnerabilidad no se proporciona ninguna página de bloqueo al usuario puesto que no es deseable dar ninguna indicación de que el ataque intentado se ha impedido por la presente invención. Además, los detalles de la prueba de vulnerabilidad (por ejemplo, la dirección de IP de origen y el URL objetivo) también se almacenan, permitiendo un análisis fuera de línea posterior de estos datos.

Ejemplos específicos de comprobaciones de prueba de vulnerabilidad adecuadas incluyen:

a) Comprobación de URL: si se detectan N coincidencias con una palabra clave en el tiempo T, se desencadena entonces una “prueba de vulnerabilidad en progreso” y se notifica esto al propietario de sitio. Se añaden estos sitios a las listas de filtro de URL para prohibir su uso futuro. No se proporciona una página de bloqueo, simplemente se bloquea el HTTP GET saliente.

b) Comprobación de contenido: si se detectan N coincidencias de patrones, compendios, etc. en el tiempo T, desencadenan entonces se desencadena una “prueba de vulnerabilidad en progreso” y se notifica esto al propietario de sitio. Se añaden estos sitios a las listas de filtro de URL para prohibir su uso futuro. No se proporciona una página de bloqueo, simplemente se bloquea el contenido para no entregarlo al usuario.

Se concibe que la presente invención proporcionará un sistema de defensa por capas. Es decir, cada mecanismo de defensa sucederá a su vez, y por tanto la oportunidad de detectar un ataque de suplantación de identidad se aumenta en gran medida. En resumen, para el ejemplo dado anteriormente: la primera fase es la comprobación de URL, prevista para impedir el acceso a sitios de suplantación de identidad; si esto falla, se proporciona el análisis de contenido desconocido y conocido para impedir la descarga de material de suplantación de identidad; si esto también falla, la comprobación de información personal impide al usuario proporcionar información confidencial a sitios sospechosos. El prever la comprobación de prueba de vulnerabilidad durante la comprobación de URL y las fases de análisis de contenido conocido/desconocido es preferible pero no necesario para la provisión de un sistema de protección de suplantación de identidad eficaz.

Aunque la presente invención se haya tratado en el contexto de los PC conectados a la *world wide web* ésta puede aplicarse a cualquier dispositivo de red conectado a cualquier red. Por ejemplo, los ataques de suplantación de identidad a través de la red de telefonía móvil (a través de SMS) o a través de comunicaciones de correo electrónico puede impedirse usando la presente invención.

Cuando un ataque se efectúa por correo electrónico, se envía un correo a un usuario desde un suplantador de identidad que solicita información confidencial, tal como detalles de banca. El ataque sólo está completo cuando el usuario responde a este correo electrónico con los detalles requeridos. Por tanto, como antes, se interceptan las comunicaciones hasta/desde el usuario y el protocolo en uso se decodifica (para correo electrónico, un ejemplo es SMTP) y el contenido y/o peticiones de contenido se analizan para ver si pueden relacionarse con la suplantación de identidad. Además, los identificadores que contienen los destinatarios previstos de los correos electrónicos también se interceptan y analizan. Si cualquiera del contenido, peticiones de contenido o identificadores se considera que están relacionados con la suplantación de identidad entonces se bloquea el acceso a menos que la dirección remota esté contenida en una lista de direcciones de red legítimas. Tal como será evidente para un experto en la técnica, en

este caso son direcciones de correo electrónico, más que URL, las que se comprueban con direcciones de red legítimas.

En otros contextos, el proceso equivalente implica cribar los identificadores (tales como URL o direcciones de correo electrónico) frente direcciones de red legítimas. Por ejemplo, en el caso de mensajería instantánea, el identificador de IM se extrae y posteriormente (si el mensaje parece relevante para la suplantación de identidad) se compara con direcciones de red legítimas.

Un experto en la técnica reconocerá que el dominio de términos de Internet, el URL y la dirección de IP usados anteriormente se relacionan de la siguiente manera. Una dirección de IP es el término usado para una dirección de red en Internet. Un dominio define un grupo de direcciones de IP y puede proporcionarse un nombre de la forma de, por ejemplo, “bbc.co.uk”. Un URL define una ubicación en la *world wide web*. Un URL a modo de ejemplo sería “http://www.bbc.co.uk/newsitem.html” que apunta a una página web que alberga un documento en un servidor web dentro del dominio de “bbc.co.uk”. Un experto en la técnica reconocerá, por tanto, que existen direcciones asociadas con tanto los URL como los dominios y que éstos se usan cuando se comprueba un URL o dominio con una lista de direcciones legítimas.

REIVINDICACIONES

1. Método alojado en red para proporcionar un servicio de seguridad de contenido de protección de suplantación de identidad:

(i) almacenar una pluralidad de direcciones de red legítimas con datos asociados;

(ii) analizar (302) el tráfico soportado por la red para los datos que aparecen relacionados con los datos asociados;

(iii) impedir (306), en el caso de que los datos de tráfico soportado por la red analizados en la etapa (ii) estén relacionados con los datos asociados, el acceso de usuario a cualquier dirección de red que sea el origen o el destinatario previsto de dichos datos de tráfico soportado por la red en el que dicha dirección de red no es una dirección de red legítima almacenada; y,

(iv) añadir (311) direcciones de red a las que se impide el acceso de usuario a una lista de direcciones de red prohibidas.

2. Método según la reivindicación 1, en el que la lista de direcciones de red prohibidas se utiliza por uno o más servicios de seguridad de contenido adicionales.

3. Método según la reivindicación 1 o la reivindicación 2, que comprende además la reponderación de reglas heurísticas utilizadas por uno o más servicios de seguridad de contenido en función del resultado de la etapa (iii).

4. Método según cualquier reivindicación anterior, en el que los datos de tráfico de red comprenden un identificador que indica el destinatario previsto de los datos.

5. Método según cualquier reivindicación anterior, en el que el tráfico de red analizado en la etapa (ii) comprende una petición de contenido del usuario desde una dirección.

6. Método según cualquier reivindicación anterior, en el que el tráfico de red analizado en la etapa (ii) comprende contenido transmitido al usuario desde un sitio remoto.

7. Método según cualquier reivindicación anterior, en el que el tráfico de red analizado en la etapa (ii) comprende datos transmitidos a un sitio remoto desde el usuario.

8. Método según cualquier reivindicación anterior en el que la etapa (ii) comprende las etapas de:

analizar (303) una petición de contenido del usuario desde una dirección, y, si dicha dirección no está relacionada con los datos asociados, posteriormente

analizar (403) el contenido transmitido al usuario desde dicha dirección, y, si dicho contenido no está relacionado con los datos asociados, posteriormente

analizar (503) los datos transmitidos a dicha dirección desde el usuario.

9. Método según cualquier reivindicación anterior, que comprende además la etapa de establecer, en el caso de que los datos de tráfico de red analizados en la etapa (ii) estén relacionados con los datos asociados, si una prueba de vulnerabilidad está en curso.

10. Método según la reivindicación 9, que comprende además la etapa de enviar, en el caso de que los datos de tráfico de red analizados en la etapa (ii) estén relacionados con los datos asociados y que no se haya establecido que una prueba de vulnerabilidad está en curso, la notificación al usuario en lugar de cualquier dato solicitado desde dicha dirección de red.

11. Método según cualquier reivindicación anterior, en el que la red es Internet.

12. Método según la reivindicación 11, que comprende además la etapa de añadir el dominio que contiene las direcciones de red a las que se impide el acceso de usuario a una lista de dominios prohibidos.

13. Método según cualquiera de las reivindicaciones 1 a 10, en el que la red es una red de datos de propósito general.

14. Método según cualquiera de las reivindicaciones 1 a 10, en el que la red es una red usada para telefonía móvil.

15. Producto de programa informático que comprende instrucciones que cuando se ejecutan por un ordenador provocan que el ordenador realice cada una de las etapas del método según cualquier reivindicación anterior.

16. Sistema de seguridad alojado en red para proporcionar un servicio de seguridad de contenido de protección de suplantación de identidad, que comprende:

un medio de almacenamiento para almacenar una pluralidad de direcciones de red legítimas con datos asociados;

medios para analizar el tráfico de red para los datos que aparecen relacionados con los datos asociados; y,

medios para impedir el acceso de usuario a cualquier dirección de red que sea el origen o el destinatario previsto de dichos datos de tráfico de red en el caso de que se descubra que dichos datos de tráfico de red están relacionados con los datos asociados y que dicha dirección de red no es una dirección de red legítima almacenada y añadir direcciones de red a las que se niega el acceso de usuario a una lista de direcciones de red prohibidas.

17. Sistema según la reivindicación 16, en el que la lista de direcciones de red prohibidas se utiliza por uno o más servicios de seguridad de contenido adicionales.

18. Sistema según la reivindicación 16 o la reivindicación 17, que comprende además medios para reponderar reglas heurísticas en el caso de que se niegue el acceso de usuario a una dirección de red.

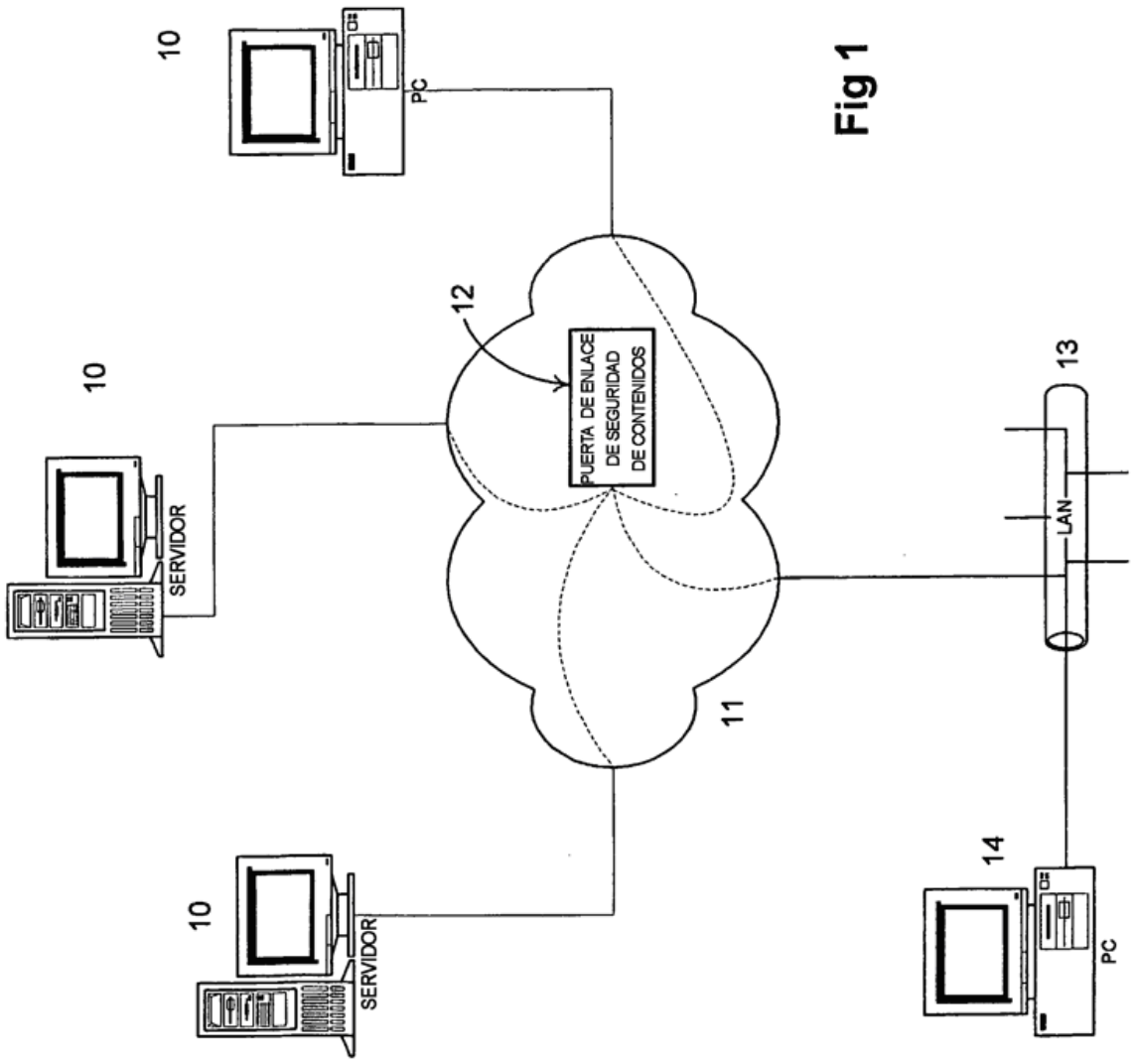

10
PC
10
SERVIDOR
12
PUERTA DE ENLACE DE SEGURIDAD DE CONTENIDOS
13
LAN
11
10
SERVIDOR
14
PC

Fig 1

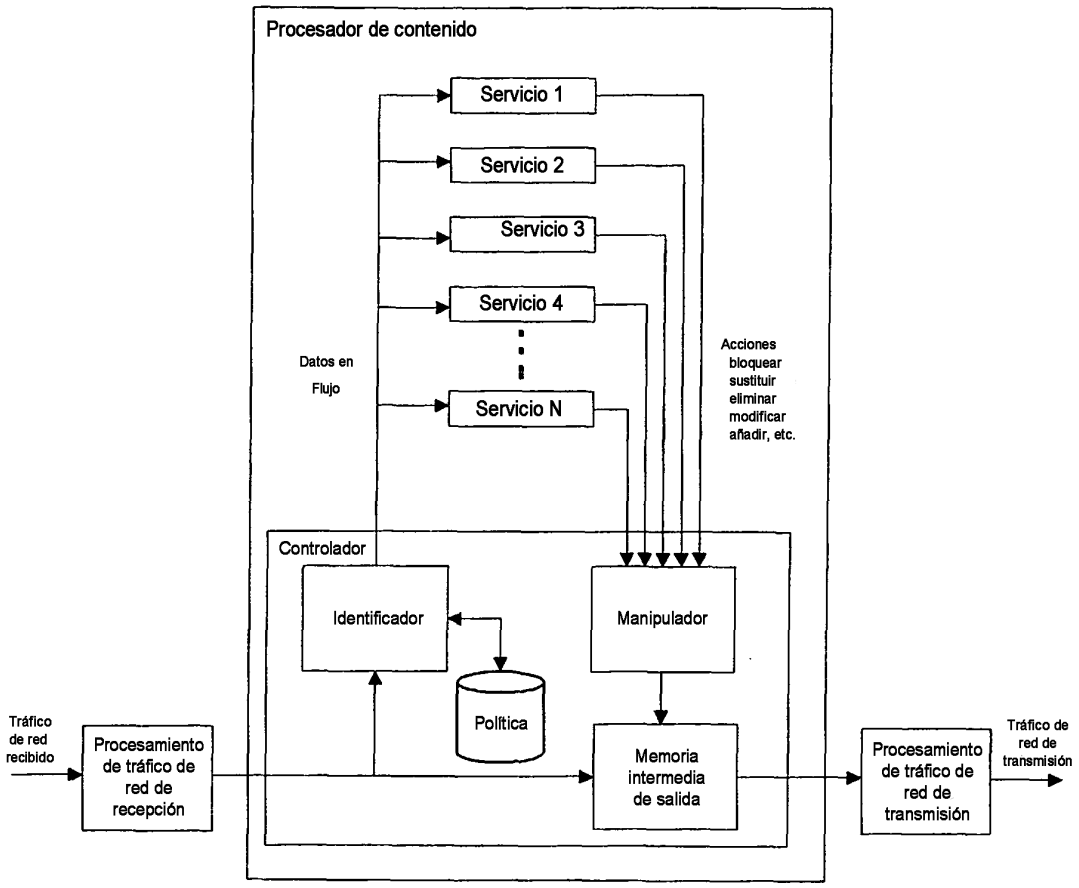

Procesador de contenido
Servicio 1
Servicio 2
Servicio 3
Servicio 4
Servicio N
Datos en Flujo
Acciones bloquear sustituir eliminar modificar añadir, etc.
Controlador
Identificador
Manipulador
Política
Tráfico de red recibido
Procesamiento de tráfico de red de recepción
Memoria intermedia de salida
Procesamiento de tráfico de red de transmisión
Tráfico de red de transmisión

Fig 2

Fig 3

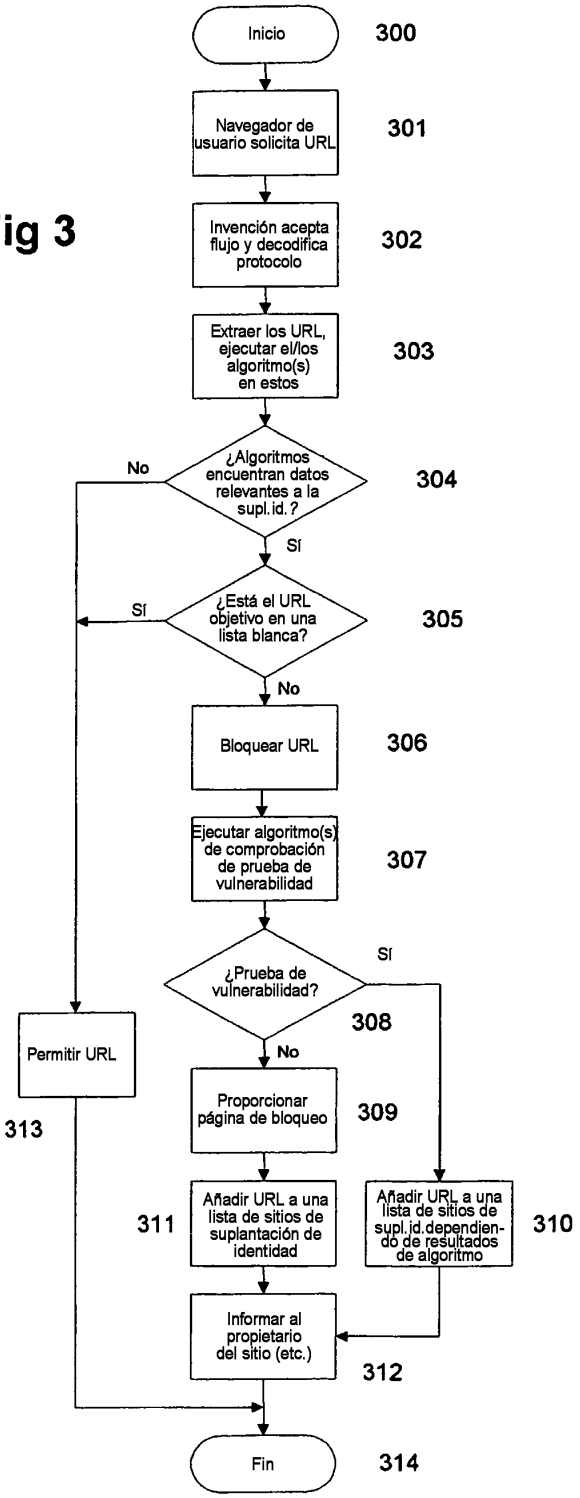

Inicio
300
Navegador de usuario solicita URL
301
Invención acepta flujo y decodifica protocolo
302
Extraer los URL, ejecutar el/los algoritmo(s) en estos
303
¿Algoritmos encuentran datos relevantes a la supl.id.?
304
No
Sí
¿Está el URL objetivo en una lista blanca?
305
Sí
No
Bloquear URL
306
Ejecutar algoritmo(s) de comprobación de prueba de vulnerabilidad
307
¿Prueba de vulnerabilidad?
308
Sí
No
Permitir URL
313
Proporcionar página de bloqueo
309
Añadir URL a una lista de sitios de suplantación de identidad
311
Añadir URL a una lista de sitios de supl.id.dependiendo de resultados de algoritmo
310
Informar al propietario del sitio (etc.)
312
Fin
314

Fig 5

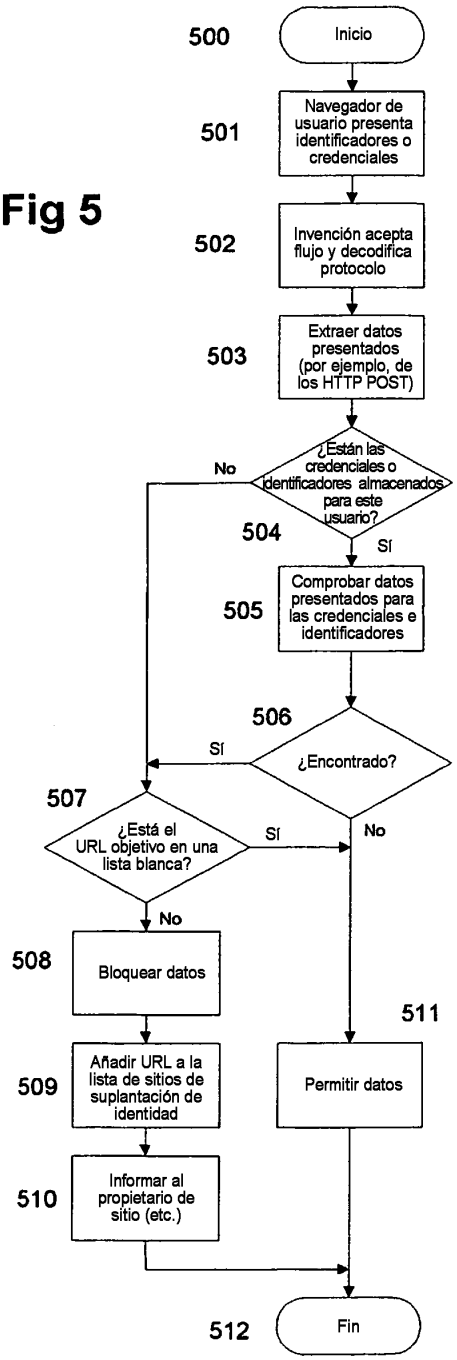
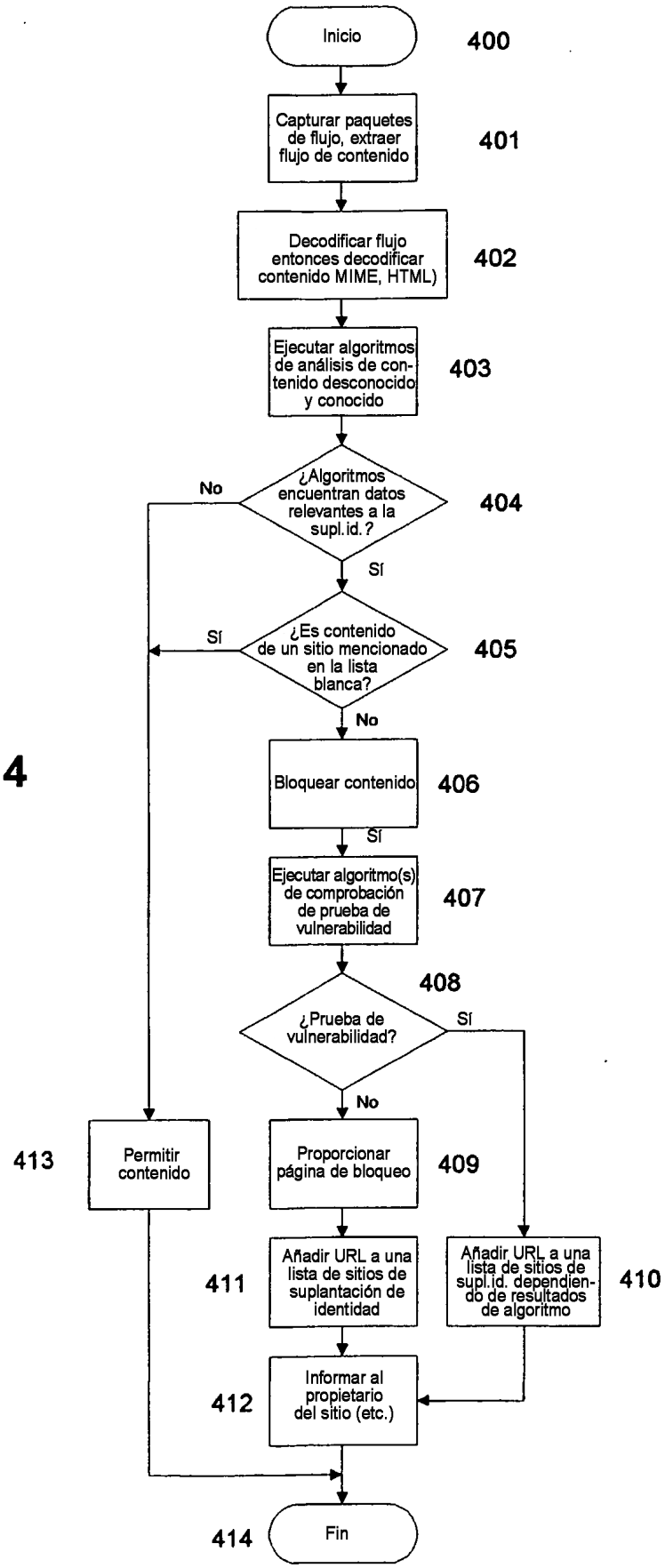

500
Inicio
501
Navegador de usuario presenta identificadores o credenciales
502
Invención acepta flujo y decodifica protocolo
503
Extraer datos presentados (por ejemplo, de los HTTP POST)
¿Están las credenciales o identificadores almacenados para este usuario?
No
504
Sí
505
Comprobar datos presentados para las credenciales e identificadores
506
¿Encontrado?
Sí
No
507
¿Está el URL objetivo en una lista blanca?
Sí
No
508
Bloquear datos
511
509
Añadir URL a la lista de sitios de suplantación de identidad
Permitir datos
510
Informar al propietario de sitio (etc.)
512
Fin

Fig 4


Inicio
400
Capturar paquetes de flujo, extraer flujo de contenido
401
Decodificar flujo entonces decodificar contenido MIME, HTML)
402
Ejecutar algoritmos de análisis de contenido desconocido y conocido
403
¿Algoritmos encuentran datos relevantes a la supl.id.?
404
No
Sí
¿Es contenido de un sitio mencionado en la lista blanca?
405
Sí
No
Bloquear contenido
406
Sí
Ejecutar algoritmo(s) de comprobación de prueba de vulnerabilidad
407
408
¿Prueba de vulnerabilidad?
Sí
No
413
Permitir contenido
Proporcionar página de bloqueo
409
Añadir URL a una lista de sitios de suplantación de identidad
411
Añadir URL a una lista de sitios de supl.id. dependiendo de resultados de algoritmo
410
Informar al propietario del sitio (etc.)
412
414
Fin