(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 430 992**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/55 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.04.2006 E 06007693 (2)**

(97) Fecha y número de publicación de la concesión europea: **17.07.2013 EP 1845468**

(54) Título: **Método, sistema de red informática y portal informático para identificar y controlar un tráfico no solicitado**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.11.2013

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
FRIEDRICH-EBERT-ALLEE 140
53113 BONN, DE

(72) Inventor/es:

KARRER, ROGER, DR. y
KÜHN, ULRICH, DR.

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método, sistema de red informática y portal informático para identificar y controlar un tráfico no solicitado.

CAMPO TÉCNICO

La presente invención se refiere a un método para identificar y controlar un tráfico no solicitado en un sistema de red informática, que comprende redes de acceso para conectar fuentes y destinos, respectivamente, a una red central, tal como Internet. La presente invención se refiere, además, a un sistema de red informática y a un portal informático adaptado para poner en práctica un método para identificar y controlar un tráfico no solicitado.

ANTECEDENTES DE LA INVENCIÓN

El diseño abierto de Internet ha sido un factor clave para su crecimiento y éxito. Sin embargo, la capacidad para enviar algo a cualquier destinatario en cualquier momento, ha demostrado tener graves inconvenientes. La falta de funciones de autenticación y de seguridad es, cada vez más, explotada para inyectar un tráfico no solicitado en la red, dando lugar a la presencia de gusanos informáticos y virus incontrolados y a ataques devastadores de los denominados Ataques Distribuidos de Denegación de Servicio (DDoS).

Virus y los denominados gusanos informáticos se ha demostrado que ocluyen partes completas de la red Internet dando lugar a un tráfico congestionado. Además, pueden transmitir códigos que modifican o destruyen sistemas finales infectados hasta una pérdida completa de datos o la captura ilegal de datos privados.

Los ataques de DDoS tienen, como objetivo, sobrecargar un recurso, de modo que a los usuarios legítimos se les deniegue el acceso al recurso. Los objetivos de los DDoS bien conocidos incluyen, sin limitación, a los servidores Web y a los Centros de Datos de Internet.

El daño operativo causado por un tráfico no solicitado ha aumentado rápidamente en los últimos años y su perjuicio es superior a miles de millones de dólares.

Existen ya métodos que tienen, como objetivo, proteger los sistemas o servicios finales contra un tráfico no solicitado tales como los Ataques de Denegación de Servicio, gusanos informáticos o virus.

La presente invención tiene como objetivo proteger los recursos de redes En particular, las redes de acceso, que tienen una capacidad notablemente más baja que la red central, deben protegerse contra un tráfico no solicitado. Dicha protección incluye la prevención de numerosos ataques con tráfico no solicitado (DDoS), de tal modo que el tráfico legítimo ya no sea capaz de alcanzar su destino debido a una capacidad de red excesiva, así como la pronta prevención de un tráfico no solicitado (malicioso o infeccioso) que se dispersa en la red central para infectar operativamente a otros sistemas.

Un método conocido está basado en métodos estadísticos tales como, a modo de ejemplo, los dados a conocer por Y. Kim et al. en el documento "Packetscore: control de sobrecarga, basado en estadísticas, contra los ataques distribuidos de denegación de servicio", Proceedings of IEEE INFOCOM'04, Hong Kong, Marzo 2004.

Los métodos estadísticos no requieren ninguna interacción del usuario que podría perturbar al usuario. Sin embargo, la sofisticación, cada vez mayor, de los ataques, tal como imitar ataques como congestiones instantáneas o ataque con modelos de tráfico específicos, lo que hace notablemente más difícil resolver el problema operativo del tráfico no solicitado por métodos estadísticos.

Otros procedimientos se dan a conocer por S. Savage et al. en el documento "Soporte de red para el seguimiento de direcciones IP", IEEE/ACM Transactions on Networking, 9(3):226-237, Junio 2001 y A. Yaar et al. "Un filtro del flujo de Internet sin estados para mitigar los ataques de invasión informática de DDoS; Proceedings of the IEEE Symposium on Security y Privacy, Oakland, CA, Mayo 2004. En estos procedimientos, la totalidad o al menos un gran número de routers a lo largo de una ruta de comunicación, dentro de una red, participan en la defensa de los sistemas finales contra los ataques de DDoS. En la práctica, dichas soluciones son lentas en su desarrollo puesto que requieren cambios por múltiples proveedores o incluso soporte desde routers en la red.

Otra solución es la dada a conocer por X. Yang et al. en el documento "Una arquitectura de red limitadora de los ataques de DoS", ACM SIGCOMM'05, Philadelphia, PA, Agosto 2005. Esta solución requiere una colaboración de múltiples entidades en el borde de una red de acceso y de una red central. De nuevo, su desarrollo es lento y difícil de conseguir, en la práctica, habida cuenta que es difícil imaginar que múltiples proveedores de Servicios de Internet (ISPs) intercambien información, en particular con respecto a cuestiones relacionadas con la seguridad.

Otro método se conoce para proteger los dispositivos finales contra los ataques de Denegación de Servicio en donde una fuente, que desea enviar datos a un destino, debe recibir primero un permiso para comunicarse antes de enviar datos. Este permiso para comunicarse se denomina también como capacidad. Véase, a modo de ejemplo, la

publicación de T. Anderson et al. "Cómo impedir la Denegación de Servicio de Internet con capacidades", Proceedings of Hot Topics in Networking (HotNetsII), Boston, Octubre 2003. Las denominadas capacidades se utilizan para la autenticación de fuentes sobre una base de extremo a extremo. Esto significa que las capacidades se emiten por un destino después de comprobar la legitimidad de una fuente y de este modo, se comprueba el tráfico para capacidades por el destino para proteger los recursos de los sistemas finales. Sin embargo, dicho sistema 'extremo a extremo' no protege a las redes de acceso y a la red central contra un tráfico no solicitado. Por lo tanto, no se resuelven los ataques de DDoS sobre una red de acceso o la dispersión del denominado *malware* (software malicioso) en la red central.

Además, el documento EP 1 284 558 B1 da a conocer un método y un aparato para limitar el efecto sobre algunos clientes que acceden a un servidor de comerciante electrónico frente a un ataque de denegación de servicio contra dicho servidor. Por lo tanto, el comerciante electrónico designa a algunos clientes como clientes VIP, en donde un paquete a ese servidor es marcado para el reenvío en una clase privilegiada de servicios, si la fuente del paquete es un cliente VIP.

En el documento US 2004/230797 se da a conocer un sistema en donde se comprueba el tráfico si se marca como no válido.

SUMARIO DE LA INVENCIÓN

Es un objetivo de la presente invención dar a conocer un método y un sistema de red informática que son capaces de impedir que un tráfico no solicitado se disperse en la red central o de impedir que un tráfico no solicitado sobrecargue la red de acceso de un destino.

Es un importante aspecto de la invención las funciones de identificar y controlar un tráfico no solicitado, en particular limitando o bloqueando, en su integridad, un tráfico no solicitado en una red de acceso o en la red central, p. e. Internet. En particular, la presente invención se refiere a un sistema de red informática y a un método que utilizan la autenticación o permisos, también bajo la denominación de capacidades, para

a) frustrar los Ataques Distribuidos de Denegación de Servicio (DDoS) contra la red de acceso de un destino en el borde operativo de una red central y su repercusión consiguiente sobre los servidores y

b) detener la dispersión de virus y gusanos informáticos antes de alcanzar la red central.

Por lo tanto, la presente invención, basada en las capacidades ubicadas en los bordes operativos protege a la red central y/o la red de acceso de un destino, mientras que los sistemas conocidos, antes citados, protegen los sistemas o los recursos de destinos.

Según un aspecto de la invención, la autoridad de autenticación utiliza las modernas técnicas de autenticación, tales como CAPTCHAS según se describe en el documento L. v. Ahn et al. en "CAPTCHA: Utilización de los Problemas de Hard AI para Seguridad"; Avances en Criptología-EUROCRYPT 2003, volumen 2656 de Lecture Notes in Computer Science, páginas 294-311, Springer Verlag y/o IP Puzzles según se describe por D. Dean et al. en el documento "Utilización de los puzzles de clientes para proteger TLS", Proceedings of the 10th USENIX Security Symposium, Washington, D.C., Agosto 2001 para transmitir información de permisos a las fuentes. Las fuentes, i.e. usuarios y/o ordenadores intentan obtener la clave de etiquetado válida a partir de la información de permiso, usada para paquetes de etiquetado a enviarse a un destino.

Otro aspecto de la invención es que el sistema de red informática puede ponerse en práctica con facilidad, p.e. por un Proveedor de Servicios de Internet (ISP) único. Los propietarios de sistemas finales conectados a la red de ISP tienen el incentivo para instalar los respectivos componentes de la presente invención para beneficiarse de la protección contra un tráfico no solicitado.

El problema técnico, antes citado, se resuelve por los métodos según las reivindicaciones 1 y 2.

El método según la reivindicación 1 ayuda a frustrar los ataques distribuidos de la Denegación de Servicio (DDoS) contra la segunda red de acceso en el borde de una red central y en consecuencia, mediante la repercusión operativa en los servidores

El método según la reivindicación 2 tiene como objetivo detener la dispersión de gusanos y virus informáticos antes de alcanzar la red central.

Formas de realización preferidas se establecen en las reivindicaciones subordinadas.

El problema antes citado se resuelve también por un sistema de red informática para identificar y controlar un tráfico no solicitado, según se define en la reivindicación 10.

Conviene señalar que la característica operativa de “unidad de tráfico mercada como siendo no válida" cubre también las unidades de tráfico que no están marcadas en absoluto.

Formas de realización preferidas se establecen en la reivindicación subordinada 11.

BREVE DESCRIPCIÓN DE LOS DIBUJOS:

La Figura 1 es un diagrama de bloques, de principio, de un sistema de comunicación que ilustra el concepto básico de la presente invención;

La Figura 2 es un diagrama de bloques de un sistema de comunicación adaptado para frustrar los denominados ataques de DoS contra la red de acceso de un destino;

La Figura 3 es un diagrama de bloques de un sistema de comunicación adaptado para detener la dispersión de virus y de gusanos informáticos antes de alcanzar la red central;

La Figura 4 es un diagrama de bloques que ilustra los módulos funcionales asociados con los respectivos componentes de los sistemas de comunicación según se describe en las figuras 2 y 3;

La Figura 5 es un diagrama de flujo que ilustra las etapas realizadas en el portal informático.

DESCRIPCIÓN DETALLADA

La Figura 1 ilustra un diagrama de bloques de un sistema de comunicación preferido basado en un sistema conectado en red distribuido que incluye un aspecto de la presente invención. El sistema de comunicación comprende los sistemas o dispositivos finales y una red. Los sistemas finales están separados en fuentes 101 y destinos 103, en donde solamente se ilustran una fuente y un destino. La red está dividida en una red central 104, p.e. Internet y redes de acceso. Con el fin de facilitar la ilustración, solamente se representa una red de acceso del lado de la fuente 105 única y una red del lado del destino 107 única. La conjunción de una red de acceso y la red central se denomina borde operativo. De este modo, distinguimos entre un borde operativo en el lado de la fuente 106 y un borde operativo en el lado del destino 108. Cada borde operativo suele comprender uno o múltiples componentes de hardware, tales como routers. Una característica común de los bordes operativos es que la capacidad de la red es notablemente diferente entre una red de acceso y la red central, esto es, la capacidad de la red es uno o varios órdenes de magnitud más pequeña en las redes de acceso 105, 108 que en la red central 104. Por lo tanto, una red de acceso es bastante más vulnerable a los ataques invasivos del tráfico que la red central 104. Por lo tanto, un tráfico no solicitado debe identificarse y controlarse, p.e. mediante una limitación o bloqueo por completo, en un borde operativo. Para esta finalidad, un elemento de red específico, denominado portal informático 109 se añade a la infraestructura de la red al menos en un borde operativo, a modo de ejemplo en el lado de la fuente y/o en el lado del destino, lo que garantiza que los recursos de la red estén disponibles para el tráfico legítimo.

La Figura 2 ilustra una primera forma de realización preferida de un sistema de comunicación, según se ilustra, en general, en la Figura 1. Este sistema de comunicación comprende un portal informático 109 en un borde operativo de una red central 104, esto es, entre una red de acceso del lado del destino 107 y la red central 104. La red de acceso del lado del destino 107 sirve para conectar destinos, p.e. servidores Web 103-1 a 103-N a la red central 104. Ha de entenderse que, esencialmente, una pluralidad de redes de acceso en el lado del destino está conectadas a la red central 104. El portal informático 109 opera para proteger la red de acceso del lado del destino 107 contra los ataques invasivos de DDoS.

En esta forma de realización, las fuentes legítimas 101-1 a 101-N, tales como clientes Web, se conectan a la red central 104 por intermedio de una red de acceso del lado de la fuente 105a, mientras que las fuentes maliciosas (*zombies*) 102-1 a 102-N están conectadas a la red central 104 a través de una red de acceso 105b separada. En la Figura 2, el tráfico operativamente solicitado, generado por las fuentes legítimas 101-1 a 101-N se designa por la referencia numérica 111, mientras que un tráfico no solicitado, generado por las fuentes maliciosas 102-1 a 102-N se designa por las referencias numéricas 112. Se describirá, más adelante, cómo los clientes se identifican y distinguen como fuentes legítimas y fuentes maliciosas, respectivamente.

El ataque o tráfico no solicitado 112 desde las fuentes maliciosas 102 a 102-N, enviado a uno o múltiples destinos 103-1 a 103-N converge en el borde operativo que une la red central 104 con la red de acceso del lado del destino 107. Sin portal informático 109, la red de acceso 107, con su más baja capacidad, puede invadirse con tráfico no solicitado 112.

En el sistema de comunicación, cuando una fuente desea comunicarse con un destino, debe recibir primero un permiso para comunicarse. Este permiso para comunicarse se denomina también capacidad en la documentación técnica. El permiso 115 se genera y reenvía a una o más fuentes por intermedio de un módulo de software específico denominado autoridad de autentificación 113. La autoridad de autenticación 113 podría ponerse en

práctica en uno o más destinos 103 a 103-N o en un dispositivo separado asociado al portal informático 109 para generar y reenviar permisos a fuentes que deseen comunicarse con destinos, las fuentes se hacen implícitamente autenticadas, esto es, fuentes legítimas, solamente si son capaces de obtener una clave de etiquetado válida a partir del permiso recibido. Este procedimiento se explicará a continuación en detalle. Dicho de otro modo, las capacidades o los permisos se utilizan para la autenticación implícita de las fuentes. Una fuente legítima usa la clave de etiquetado, incluida en el permiso, para etiquetar paquetes que han de enviarse a un destino.

Con un portal informático 109, el tráfico de ataque 112 se identifica y se puede filtrar, de modo que solamente un número controlable de paquetes legítimos 111 sean reenviados desde la red central 104 a la red de acceso 107. El tráfico no solicitado 112 filtrado por el portal informático 109 se ilustra, de forma simbólica, por un símbolo de tierra.

De forma adicional o alternativa, la cantidad del tráfico de ataque 112 que fluye a través de la red de acceso 107 se puede controlar por el portal informático 109 dependiendo de la condición de la red de acceso 107. El portal informático 109 identifica el tráfico como tráfico no solicitado si los paquetes recibidos no contienen una etiqueta válida generada sobre la base del permiso.

Además, según se describirá más adelante, el portal informático 109 utiliza un algoritmo de generación de claves para generar claves de etiquetado. Las claves de etiquetado se transportan a la autoridad de autenticación 113 que reenvía el permiso y la clave de etiquetado o parte de la clave a las fuentes. Solamente fuentes, que funcionan correctamente, son capaces de calcular la clave de etiquetado a partir del permiso, que luego se utiliza para etiquetar o marcar paquetes a enviarse a sus respectivos destinos.

La Figura 3 ilustra una segunda forma de realización de un sistema de comunicación. Este sistema de comunicación difiere del que se ilustra en la Figura 2, en que un portal informático 109 está dispuesto en un borde operativo, en el lado de la fuente, de una red central 104, esto es, entre una red de acceso del lado de la fuente 105 y la red central 104. Se supone que un software malicioso *malware*, p.e. un virus o un gusano informático ha infectado a un conjunto de fuentes 102-1 a 102-N, a modo de ejemplo, ordenadores y se auto-replica a una gran velocidad para infectar operativamente a otros ordenadores fuentes. Estos ordenadores fuentes 102-1 a 102-N no podrán obtener un permiso correcto generado por, y recibido desde, una autoridad de autenticación 115. Se supone, además, que el *malware* 112 se dispersa a través del correo electrónico. El portal informático 109 está adaptado para determinar automáticamente si un correo electrónico 111 ha sido enviado por una fuente legítima 101-1 a 101-N o por un ordenador malicioso 102-1 a 102-N. Solamente los correos electrónicos 111, enviados por una fuente legítima 101 a 101-N, han sido marcados correctamente y pasarán a través del portal informático 109. Por lo tanto, el *malware, que* no esté marcado, o que incluya una etiqueta no válida, puede identificarse como tráfico no solicitado 112 y se impide su dispersión, a través del portal informático 109, hacia Internet 104.

La operación interna del portal informático 109, según se representa en las figuras 2 y 3, se ilustra en la Figura 5. El portal informático 109 tiene la capacidad para identificar y controlar, p. e. filtrar o limitar un tráfico no solicitado. Cuando un paquete 110 llega desde las fuentes 101 o 102 al portal informático 109, el portal informático 109 comprueba primero, en la etapa 123, si el paquete contiene, o no, una etiqueta. Si el paquete contiene una etiqueta, en tal caso, el portal informático 109 recupera, en la etapa 120, una clave de etiquetado anteriormente generada para una sesión dada. Si una clave de etiquetado adecuada está disponible, el portal informático 109 usa la clave de etiquetado para determinar, en la etapa 124, si el paquete incluye, o no, una etiqueta válida. Si la etiqueta es válida, el paquete 111 puede reenviarse inmediatamente a una cola de salida del portal informático 109.

Si, sin embargo, una etiqueta no está incluida en un paquete 118 o no es válida 122 o una clave de etiquetado no está disponible 121 en el portal informático 109, el paquete se considera como un paquete malicioso o no solicitado 112 y por ello, se filtrará o controlará 125 por el portal informático 109. El término "filtrado" o "controlado" 125 se puede interpretar y poner en práctica en varias formas. Realizaciones, a modo de ejemplo, incluyen, sin limitación, a los paquetes no solicitados 112 simplemente eliminados o para reenviarles a una cola de baja prioridad 125. Una solución eficiente tal que el portal informático 109 no desacelere el tráfico en la red de acceso del lado del destino 107 o en la red central 104. Además, la solución necesita escalar operativamente a un gran número de flujos.

Como una breve descripción general, el intercambio de capacidad para legitimar fuentes para enviar un tráfico solicitado 111 implica a tres componentes independientes: fuentes que deben adquirir una capacidad, la autoridad de autenticación 113 para emitir y reenviar capacidades y el portal informático 109 para comprobar capacidades con el fin de identificar y controlar un tráfico no solicitado. El concepto general se ilustra en la Figura 4.

Para esta finalidad, el portal informático 109 usa un sistema de etiquetado para verificar paquetes y un sistema de formación de claves para generar claves de etiquetado. El sistema de formación de claves puede ponerse en práctica en medios de generación de claves 114 y el sistema de etiquetado puede localizarse en un medio de verificación de etiquetas 117, ambos situados dentro del portal informático 109.

Además, un Sistema de Transporte de Claves se utiliza por la autoridad de autenticación 113. El Sistema de Transporte de Claves puede ponerse en práctica en un medio de transporte de claves 118. En una forma de realización, la autoridad de autenticación 113, así como el Sistema de Transporte de Claves se ponen en práctica en

uno o más de los destinos 103-1 a 103-N. Además, un sistema de etiquetado se utiliza por las fuentes para generar etiquetas e incorporarlas en paquetes a enviarse. Por lo tanto, un medio de generación de etiquetas 116 puede ponerse en práctica en cada fuente para realizar el sistema de etiquetado. Una descripción detallada de estos sistemas se dará a continuación.

En una primera etapa, una clave de etiquetado se genera por el medio de generación de claves 114 del portal informático 109. Derivaciones de esta clave se transmiten a la autoridad de autenticación 113. La autoridad de autenticación 113 es una unidad lógica o módulo de software que puede mapearse en correspondencia en un dispositivo independiente, o puede co-situarse con otros dispositivos, tales como el servidor 103-1. La autoridad de autenticación 113 está adaptada para una autenticación implícita de clientes 101. Esta función se realiza generando un permiso o una capacidad, a modo de ejemplo, bajo la forma de una prueba, que incluye una clave de etiquetado, o una parte de una clave de etiquetado, que es válida para una sesión única. La prueba a superar se reenvía a las fuentes 101 y 102. Cada fuente intenta resolver la prueba recibida para obtener una etiqueta válida que se utiliza para marcar paquetes a enviarse a destinos. En el portal informático 109, los paquetes marcados con una etiqueta válida se consideran como un tráfico legítimo 111, mientras que el tráfico sin una etiqueta, o con una etiqueta no válida, se identifican como tráfico no solicitado 112 y así se filtran, respectivamente, según se ilustra en las Figuras 2, 3 y 5.

Una operación ilustrativa del sistema de red informática, según se representa en la Figura 2, se describirá con más detalle.

Este sistema de red informática está adaptado para impedir los ataques DDoS a la red de acceso 107, pero, como se indicó con anterioridad, se puede utilizar también para otros escenarios operativos.

Se supone que los destinos 103-1 a 103-N son servidores, que las fuentes 101-1 a 102-N son ordenadores clientes y que la autoridad de autenticación 113 está situada en al menos uno de los servidores 103.

En una forma de realización preferida, el Sistema de Formación de Claves, incorporado el medio de generación de claves 114, es responsable para generar una clave en el portal informático 109 y de su comunicación a uno o más de los servidores 103-1 a 103-N o, en general, a la autoridad de autenticación 113. Es importante conocer que el portal informático 109 define y gestiona claves y las intercambia con los servidores, pero no al contrario. La clave enviada al servidor 103-1 es específica del servidor. El servidor 103-1 memoriza su clave a nivel local. Una vez que el servidor 103-1 reciba una demanda desde un cliente, p.e. cliente 101-1, deriva una clave específica de la sesión como una clave de etiquetado a enviarse a las fuentes.

El Sistema de Transporte de Claves asociado a la autoridad de autenticación y puesto en práctica, a modo de ejemplo, en el servidor 103-1, es responsable para comunicar la sesión o clave de etiquetado a clientes, p.e.. en la forma de una prueba a superar, generada por la autoridad de autenticación 113. Cuando el usuario del cliente 101-1 y/o el propio cliente resuelve esta prueba, el cliente 101-1 y el propio usuario se considera como habiendo sido autenticado.

En la presente forma de realización, los clientes 101-1 a 101-N se suponen que son capaces de resolver la prueba recibida correctamente y en consecuencia, están legitimados o autenticados. Se supone que los clientes 102-1 a 102-N no son capaces de resolver la prueba recibida correctamente y por ello, se consideran como *zombies*.

El sistema de etiquetado, puesto en práctica en los clientes, permite a los clientes legítimos incorporar una etiqueta en cada paquete a enviar, después de su autenticación y después de obtener una clave de etiquetado, con la resolución correcta de la prueba a superar.

En el portal informático 109, el sistema de etiquetado define cómo el portal informático 109 verifica las etiquetas incluidas en los paquetes con información memorizada en el portal informático 109.

A continuación, describimos los tres sistemas en detalle. Para la descripción, introducimos la notación siguiente: Notación 1:Para un paquete P de IP utilizamos $IP_S(P)$, $IP_d(P)$, Ident(P), Flow(P), Len(P) para indicar los respectivos campos de cabecera, dirección fuente, dirección destino, identificación (en IPv4), etiqueta de flujo (en IPv6) y longitud de carga útil del paquete. De modo similar, utilizamos $Port_s(P)$, $Port_d(P)$, Seq(P), Ack(P) para indicar el puerto fuente, el puerto destino, la secuencia y el número de confirmación en caso de que P sea un paquete TCP.

Notación 2: Para una cadena de bits X, let [X] z indica los *r* bits más a la izquierda de X; si X tiene menos de *r* bits, se rellena con bits cero. Let $[X]_{r,s}$ con $r \leq s$ indica la subcadena de bits constituida por los bits *r,…,s,* con el relleno de ceros si fuere necesario.

1. Sistema de formación de claves

A continuación, se describen dos sistemas para generación de claves de etiquetado y la gestión para el portal informático, los servidores y los clientes. El primer sistema, que se denomina *stateless keying*, deriva todas las

claves de etiquetado a partir de una clave maestra central mantenida en el portal informático 109. En el segundo sistema, el portal informático 109 necesita mantener algún estado para cada flujo que se le encamine.

a) Formación de claves sin estados (*Stateless Keying*)

En este sistema de formación de claves, el portal informático 109 tiene una clave maestra central o clave de portal informático k_G. Como todas las demás claves se derivan a partir de esta clave se mantiene en secreto en todo momento. El sistema usa, además, dos funciones de derivación de claves KDF_1, KDF_2 para derivar claves de servidores y claves de cliente o de sesión. Las claves de sesión se denominan también claves de etiquetado. Dado un servidor S con dirección IP*(S)*, su clave es

$$k_S \leftarrow KDF_1(k_G, IP(S))$$

Además, para un cliente *C* con dirección IP*(C)*, la clave de etiquetado usada para etiquetar cualquier paquete enviado al servidor *S* es

$$k_{C,S} \leftarrow KDF_2(k_S, IP(C), IP(S))$$

La interfaz para el medio de verificación de tarjetas 117, en el portal informático 109, puede ponerse en práctica fácilmente utilizando estas funciones. Conviene señalar que el cliente solamente recibe $k_{c,s}$ por lo que no necesita conocer nada sobre KDF_1, KDF_2.

La adición de una memoria caché (no ilustrada) en el portal informático 109, para los resultados de la derivación de claves, no afecta a la propiedad de que el sistema es sin estados. Sin embargo, mejoran la eficiencia del cálculo del sistema. Usamos dos tablas de LRU (de uso menos reciente) en el portal informático 109 que mantienen entradas (IP*(S),* k_s) y (IP*(S)*, IP*(C)*, $k_{c,s}$). De ese modo, podemos atenuar la complejidad operativa de la derivación de claves de etiquetado a través de un número considerable de verificaciones de etiquetas, mientras las tablas son fáciles de mantener. La mejora conseguible en el tiempo de cálculo depende de la memoria disponible en el portal informático 109 y del número de diferentes flujos que pasan a través del portal informático en cualquier instante único.

b) Formación de claves con estado en el portal informático

En lugar de derivar todas las claves a partir de una clave maestra única 10 mantenida en el portal informático 109, el portal informático 109 podría emitir una nueva clave de etiquetado para cada conexión única que encuentre. A continuación, describimos cómo podría funcionar dicho sistema de formación continua de claves.

En este sistema, el portal informático 109 genera una clave de sesión o clave de etiquetado k cuando detecta una iniciación de conexión que implica a un cliente *C* y a un servidor *S* por donde pasa, esto es, en la forma de un paquete SYN. A continuación, memoriza *k* junto con *(C, S)* y otra información que identifica el flujo, p.e. números de puertos, para uso futuro.

A continuación, el portal informático 109 transmite la clave de etiquetado al respectivo servidor en donde se pone en práctica la autoridad de autenticación 113, de modo que el servidor pueda transportarla al cliente. Esto exige que la clave de sesión o la clave de etiquetado *k* sea encriptada con alguna clave ks compartida entre el portal informático 109 y el servidor 103-1. La comunicación entre el portal informático 109 y el servidor 103-1 se puede realizar 'en banda', esto es, añadiendo la clave encriptada al paquete SYN original del cliente 101-1 antes de transmitirla al servidor 103-1. Para agotar las claves de sesión, el portal informático 109 tiene un control de la conexión y conoce los tiempos de espera de los protocolos. Esto exige un mantenimiento del estado similar como en un denominado 'cortafuegos' de inspección de estados de carácter completo.

Selección de Algoritmos y de Parámetros

Para el sistema de formación de claves sin estados, necesita especificarse las magnitudes de las claves así como las funciones de derivación de claves. Dado que seleccionamos CBC-MAC con AES y un tamaño de clave de 128 bits para el sistema de etiquetado, es razonable usar también estos parámetros para el sistema de formación de claves. Además, las funciones de derivación de claves KDF_1, KDF_2 pueden ponerse en práctica usando CBC-MAC, dado que es una función pseudo-aleatoria adecuada. Esta función se describe, a modo de ejemplo, por M. Bellare et al. en "La seguridad del código de autenticación del mensaje de encadenamiento de bloques de cifrado.", Journal of Computer and Systems Sciences, 61(3):362-399, Diciembre 2000. Este modo sin código adicional necesita añadirse. Más concretamente,

$$KDF_1(k_G, IP(S) := CBC - MAC[AES]_{k_G}(c_1 \| IP(S)),$$
$$KDF_2(k_S, IP(C), IP(S) := CBC - MAC[AES]_{k_S}(c_2 \| IP(C) \| IP(S))$$

que utiliza dos constantes distintas C_1, C_2 para separar la entrada para la función de encriptación. Utilizamos constantes de 12 o 8 bytes cada una. El comportamiento de estas funciones es entonces como sigue: Para IPv4, las direcciones IP y las constantes dan lugar a entradas de 16 bytes para KDF_1 respectivamente. KDF_2, esto es, una operación de cifrado de bloque único. Para IPv6, las direcciones IP y las constantes dan lugar a entradas de 28 o 40 bytes, con el resultado en KDF_1 resp. KDF_2 utilizando 2 o 3 operaciones de cifrado de bloques. Además, una operación de programación de claves se necesita cuando se pone en uso la clave resultante.

2. Sistema de transporte de claves

En esta sección, proponemos métodos para transportar la clave criptográfica, generada por el portal informático 109, desde el servidor 103-1 o la autoridad de autenticación 113 al cliente 101-1 en el inicio de la respectiva conexión. El cliente usa esta clave para etiquetar cada paquete a enviarse a un servidor.

Utilizamos la idea general idea de una prueba CAPTCHA (Prueba de Turing pública y automática para diferenciar máquinas y humanos) para distinguir entre un usuario humano y una maquina o cliente. La prueba de CAPTCHA se describe, a modo de ejemplo, por L.v.Ahn et al. en "CHAPTCHA: Utilizando Hard AI Problems para Seguridad", Advances in Cryptology-EUROCRYPT 2003, vol. 2656 de Lecture Notes in Computer Science, páginas 294-311, Springer Verlag.

De este modo, nuestro sistema garantiza que los usuarios humanos puedan seguir teniendo acceso a un servidor incluso bajo ataque informático. Por el contrario, un cliente malicioso, p.e. 102-1, que sea potencialmente parte de una red de ataque de DDoS y que puede, por lo tanto, no confiar en la ayuda de un usuario humano, no es capaz de obtener una clave de etiquetado válida.

Las CAPTCHAs fueron originalmente designadas como pruebas. En esta forma de realización, usamos una sub-clase de aquellos problemas que permiten al usuario introducir alguna información derivada a partir de un problema de inteligencia artificial (AI) dado. En particular, tal problema de AI se denomina una prueba a superar. Esta prueba se genera por la autoridad de autenticación 113 utilizando una clave de etiquetado recibida por el portal informático 109. La prueba a superar, que incluye la clave de etiquetado, se transmite luego a los clientes 101 y 102.

A continuación, utilizamos esta entrada para un cálculo que proporcionará una clave criptográfica al ordenador cliente.

Un problema con el que nos enfrentamos, en este caso, es que probablemente sólo una pequeña fracción de los potenciales usuarios está predispuesta a introducir el equivalente de una clave de etiquetado de 128 bits, que es una tarea tediosa y propensa a los errores, p.e. la lectura de la clave desde una imagen distorsionada. Por lo tanto, debemos auto-restringirnos a utilizar solamente un pequeño número de bits, lo que da lugar a una entrada de baja entropía.

A continuación, proponemos dos soluciones que combinan CAPTCHA con una variante de puzles IP en un modo que el usuario ayuda a la máquina del cliente a resolver el puzzle con mayor rapidez o permita a la máquina del cliente usar la solución en todo momento. Los puzles de IP son conocidos y se describen, a modo de ejemplo, en el documento de D. Dean et al. en "Utilización de los puzzles del cliente para proteger a TLS", Proceedings of the 10th USENIX Security Symposium, Washington, D.C., Agosto 2001.

De hecho, en el primer sistema, la resolución mediante puzles resulta ayudada por el usuario humano, mientras que el segundo sistema requiere una solución correcta de CAPTHCA por el usuario.

En ambos sistemas la máquina del cliente intenta obtener la clave que se utiliza por el servidor 103-1 o la autoridad de autenticación 113 para encriptar la clave de etiquetado.

Nuestras propuestas son escalables en el sentido de que un servidor 103-1 ocupado puede seleccionar qué esfuerzo, p. e., en el cálculo de ciclos o el tiempo de espera que un ordenador cliente ha de dedicar para poder acceder al servidor.

Los sistemas hacen uso de una función de intrusión criptográfica h resistente a la pre-imagen (tal como SHA-256) con

$$h: \{0,1\}^* \rightarrow \{0,1\}^n.$$

La función de intrusión SHA-256 se describe, a modo de ejemplo, en National Institute of Standards and Technology (NIST), Computer Systems Laboratory. Secure Hash Standard. Federal Information Processing Standards Publications (FIPS PUB 180- 2), Febrero 2004.

Suponemos que *h* es compartida, en alguna manera, entre el cliente y el servidor o por el contrario, es pública.

Además, conviene señalar que, debido a la forma en la que los Sistemas de Transporte de Claves están integrados en el sistema de comunicación EC, los sistemas necesitan realizarse como una operación única, esto es, un intercambio de mensajes errático único. La idea es superponer un mensaje de cliente a servidor, si existiere, en un paquete SYN inicial, mientras que el mensaje de servidor-a-cliente se integra en el paquete SYN-ACK. Preferentemente, estamos utilizando la comunicación 'en-banda'.

Con los dos sistemas de transporte de claves, el diseñador del sistema, u operador, tiene una opción de que las máquinas del cliente fueren capaces de efectuar la conexión aun cuando ningún usuario humano permanezca esencialmente detrás de ella. Esta elección podría depender también del sistema actual y de la carga de la red.

a) Sistema asistido por la solución de CAPTCHA

En el primer sistema, estamos realizando efectivamente una carga de trabajo diferencial para un ordenador cliente esto es, un ordenador cliente y un usuario humano trabajando juntos tendrán un acceso mucho más rápido a la clave de etiquetado que la máquina por sí sola.

Nuestro puzzle IP funciona como sigue. El servidor 103-1 o la autoridad de autenticación 113 selecciona un $m<n$, esto es, el factor de trabajo y una cadena aleatoria r^* de longitud n. El propio valor r^* no se transmitirá al ordenador cliente. Además, el servidor calcula

$$k_e \leftarrow h(c_p \| IP(S) \| IP(C) \| r^*)$$

y utiliza k_e para encriptar la clave de etiquetado. Suponiendo n_p=n-m que indica que el número de bits de texto sin cifrado, m_u the número de bits a introducir por el usuario y m_c el número de bits determinado por la máquina. Requerimos que sea $m_u+m_c=m$. Se supone que $r\hat{}=[r^*]_{np}$, $r_c=[r^*]_{n-m+1,\ n-mu,}$ y $r_u=[r^*]_{n-mu+1,n}$. Entonces, $r^* = r\hat{} \,||\, r_c \,||\, r_u$.

El cliente viene dado por el tuplo

$$(r\hat{}, s^*, C)$$

con

$$s^* = h(r^* \| IP(C) \| IP(S)),$$
$$C = Enc_{k_e}(k_t),$$

en donde k_t es la clave de etiquetado que ha de transmitirse.

Para poder obtener el k_t ,de texto sin cifrado, el cliente necesita encontrar r_c y r_u para poder recuperar r^*. El cliente puede comprobar que encontró una solución *r* probando si

$$h(r \| IP(C) \| IP(S)) = s^*$$

Dado que *h* es una función de intrusión criptográfica que está proporcionando alguna resistencia de pre-imagen de entrada parcial, necesita que se realice por la fuerza bruta. Esto nos permite una predicción aproximada de la cantidad media de tiempo de cálculo que necesita dedicar el cliente. Después de encontrar el valor de r^*, el cliente puede calcular k_e y desencriptar k_t.

El algoritmo CAPTCHA entra ahora en juego operativo dando una recomendación adicional sobre r^* proporcionando r_u en la forma de un CAPTCHA, de modo que el usuario pueda teclear r_u en el ordenador cliente y de este modo, ayudar efectivamente al ordenador cliente a resolver el puzzle y recuperar la clave de etiquetado .

b) Sistema que requiere una Solución CAPTCHA

Una ligera variación del sistema anterior permite cerciorarse de que el ordenador cliente pueda hacer uso de la solución para el puzzle del cliente solamente si un usuario humano proporciona la solución correcta para CAPTCHA. El puzzle del cliente es muy similar al anteriormente dado.

Utilizando la notación r^*, $r\hat{}$, r_c, r_u antes establecida, el servidor 103-1 selecciona, en lugar de r^*, un $r\hat{}$, r_c, r_u, aleatorio, calcula $r\tilde{}_u = [h\ (c\_u\ ||\ r\_u)\ ]_{mu}$. Luego, usamos $r^*=r\hat{}\ l\ l\ r_c|\ |\ r\tilde{}_u$ y

$$k_e \leftarrow h(c_p \| IP(S) \| IP(C) \| r^*) \oplus h(c_p' \| IP(S) \| IP(C) \| h(c_u' \| r_u))$$

como clave para encriptar o desencriptar k_t. En este caso, c_u y c'_u son, de nuevo, dos constantes de conocimiento público (que difieren también de las otras constantes antes usadas). Como en el primer sistema de transporte de claves, al usuario se le dará r_u en la forma de CAPTCHA. La observación crucial aquí es que el cliente no se le proporciona un medio para comprobar la integridad de ke o kt y por lo tanto, no dispone de ningún medio para constatar directamente que se ha encontrado la clave correcta. Esto significa que esencialmente la clave correcta se obtiene solamente si, a la vez, la solución correcta al puzle de IP y CAPTCHA se conoce para el ordenador cliente.

c) Selección de Algoritmos y Parámetros

Proponemos una posible instancia operativa de nuestro primer sistema para el transporte de claves, el de realizar un factor de trabajo diferencial. Propiciamos la 2ª función de intrusión resistente a la pre-imagen *h* con SHA-256. Para la función de encriptación $Enc_k(.)$, usamos el AES de cifrado de bloques con una clave de 128 bits; obtenemos la clave k_e desde la salida de *h* truncando la salida para el tamaño requerido.

La selección de m_c y m_u (y por lo tanto, *m*) es crítica para la seguridad así como para la utilizabilidad del sistema. Suponemos que un algoritmo gráfico CAPTCHA constituido por caracteres y dígitos (y con la resolución de algunas ambigüedades tales como '0' vs. 'O', '1' vs. 'l') es aceptable. Usamos solamente los caracteres en minúsculas y convertimos las mayúsculas si fuere necesario. Esto nos proporcionará aproximadamente 5 bits por carácter tecleado por el usuario. En nuestra opinión, 4 caracteres o 20 bits en total sería aceptable. Además, en un sistema Pentium M (1.5 GHz), la puesta en práctica de SHA-256 se realiza en unas 2^{18} operaciones por segundo.

Esta elección de $m_u=20$ da lugar a un factor de trabajo diferencial de aproximadamente 2^{20}, por lo que una elección de m_c=18 y por lo tanto, *m*=38 serían suficientes en el momento actual. Resolver el puzzle con la asistencia humana necesitaría unos 0.5 segundos, como media, en la máquina dada como referencia con anterioridad. El valor de m_c necesitaría un aumento gradual en el futuro cuando máquinas mucho más rápidas sean de uso ordinario.

3. Sistema de etiquetado

En primer lugar, recordamos los requisitos que el sistema de etiquetado realizado por un cliente debe cumplir para poder trabajar de forma eficiente y segura. A continuación, describimos el sistema concreto y proporcionamos algunas cifras del rendimiento operativo.

Para explicar el sistema de etiquetado, suponemos que un ordenador cliente *C,* que desea comunicarse con un servidor *S* detrás del portal informático 109, tiene una clave criptográfica $k_{c,s}$ que es específica para el par de cliente-servidor y posiblemente dependiente del tiempo o incluso dependiente de la sesión. Además, suponemos que el portal informático 109 mismo conoce también a $k_{c,s}$, posiblemente derivándolo mediante el sistema de formación de claves a partir de otra información conocida para el portal informático 109.

a) Requisitos operativos

La finalidad del sistema de etiquetado es proporcionar una prueba para el portal informático 109 acerca de la autenticidad de un paquete enviado el ordenador cliente C al servidor S, puesto que el portal informático establece - en el caso de un ataque o sobrecarga – la prioridad con la que el paquete se reenvía a través de la red de acceso 107 al servidor.

* Seguridad. El mecanismo de etiquetado impedirá que un adversario se aprenda la clave criptográfica $k_{c,s}$ a partir de los paquetes de un flujo. Además, un adversario será incapaz de rehusar la etiqueta desde un paquete para formar una etiqueta válida para otro paquete, aun cuando el adversario falsifique la dirección del cliente como origen.

* Eficiencia de la verificación. El portal informático 109 ha de comprobar cada paquete que se etiqueta, de modo que el sistema de etiquetado no habrá de imponer una sobrecarga de cálculo excesiva con el fin de mantener pequeñas las latencias.

Conviene señalar que el servidor *S* o la autoridad de autenticación no tienen que hacer frente a la generación o verificación de etiquetas.

b) El Sistema Concreto

Para etiquetar un paquete, el medio de generación de etiquetas 116 de un cliente usas un campo de etiquetas de carácter especial en la cabecera de IP de un paquete a enviarse. El portal informático 109 buscará luego etiquetas disponibles en los paquetes recibidos, comprobará las etiquetas y a modo de ejemplo, basará una decisión sobre la prioridad del paquete a este respecto.

Habida cuenta de los requisitos antes examinados, empleamos un sistema de Código de Autenticación de Mensajes (MAC), esto es, un par de algoritmos posiblemente aleatorizados (*Mac, Ver*) para etiquetar paquetes y su verificación, haciendo uso de parámetros *k* y *t* para la clave de etiquetado y longitudes de etiquetas medidas en bits:

$$Mac : \{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^t$$
$$Ver : \{0,1\}^k \times \{0,1\}^* \times \{0,1\}^t \rightarrow \{0,1\}$$

con Ver *(k, M, Mac (k, M))*$\Rightarrow$ 1.

A continuación, describimos el sistema de etiquetado y verificación basado en estas funciones.

En primer lugar, describimos qué datos, desde un paquete *P*, se incluyen en el cálculo y verificación de tarjetas. En este caso, distinguimos entre IPv4 e IPv6: Para un paquete *P* dado, usamos los tuplos

$$M_{hdr}(P) \leftarrow \begin{cases} IP_s(P), IP_d(P), Len(P), Ident(P)) \\ IP_s(P), IP_d(P), Len(P), Flow(P) \end{cases}$$

Y para un paquete TCP

$$M_{tcp}(P) \leftarrow (Port_s(P), Port_d(P), Seq(P), Ack(P))$$

(o $M_{tcp}(P) \leftarrow ()$ para paquetes no de TCP) para establecer la entrada a las operaciones de etiquetado y verificación como

$$M(P) \leftarrow (M_{hdr}(P), M_{tcp}(P))$$

Para IPv4, el tamaño total máximo de *M(P)* es 12+12 bytes o 96+96=192 bits; para IPv6, estos números son 37+12=49 bytes respectivamente. 296+96=392 bits (en donde contamos *Flow (P*) como 3 bytes o 24 bits).

Ahora, los procedimientos para calcular una etiqueta en el cliente 101-1 y para comprobar una etiqueta en el portal informático 109 son como sigue:

* El cliente intenta recuperar desde su almacenamiento de claves internas, la clave de etiquetado para cada paquete *P* que envía al servidor:

$$k \leftarrow \texttt{client\_get\_session\_key}(IP_d(P)).$$

Si ninguna clave de etiquetado está disponible, el paquete se envía no etiquetado. De no ser así, el cliente establece M(P), calcula

$$\tau(P) \leftarrow \texttt{Mac}(k, M(P)),$$

e incluye $\tau(P)$ en *P* utilizando la opción de etiqueta.

* El portal informático 109 mantiene una etiqueta (véase la Figura 5)

$\lambda(P) \in$ (untagged, invalid, valid}

para cada paquete para nuevas decisiones de puesta en cola de espera, que se determina como sigue. Si un paquete *P* no está etiquetado $\lambda(P) \leftarrow$ Untagged.

Si un paquete *P* incluye una opción de etiqueta, el portal informático obtiene

K ← gate_get_session_key *(IP_s (P), IP_d(P))*.

Si ninguna clave de etiquetado está disponible $\lambda(P)$ ← Invalid.

De no ser así, el portal informático extrae la etiqueta alegada $\tau'(P)$, obtiene *M(P) a partir de la* otra información de paquete según se describió anteriormente y calcula

$$b \leftarrow Ver(k, M(P), \tau'(P)),$$

Entonces

$$\lambda(P) \leftarrow \begin{cases} Valid & b = 1 \\ Invalid & b = 0 \end{cases}$$

En función de la etiqueta, el portal informático 109 decide qué hacer más con el paquete, p.e. reenviarlo con alta o baja prioridad o eliminarlo completamente. Conviene señalar, sin embargo, que la eliminación de paquetes SYN no es una buena idea, puesto que, esencialmente, impediría que el servidor sea alcanzable.

d) Selección de Algoritmos y de Parámetros

Para poner en práctica el sistema de MAC, se dispone de varias opciones directas, tales como CBC-MAC con varios cifrados de bloques o la construcción de HMAC, p.e. HMAC-SHA1. Esta elección afecta directamente al tamaño de clave natural y a la longitud máxima de la etiqueta de nuestro sistema. Para IPv4 *M(P)*, se adapta en dos bloques AES, por lo que el uso de CBC-MAC, con AES, requeriría solamente dos operaciones de encriptación, mientras que para IPv6 se necesitarían cuatro operaciones de encriptación. En ambos casos, se necesitaría HMAC-SHA1, dependiendo de la puesta en práctica, 2 o 4 operaciones de la función de compresión, por lo que elegimos CBC-MAC con AES y una clave de 128 bits.

Acortamos la salida de 128 bits a los primeros 80 bits de datos de etiquetas, de modo que la opción para IPv4, incluyendo el tipo y la longitud de la opción, tiene una longitud total de 96 bits o 12 bytes. Esto ofrece todavía un nivel de seguridad contra un adversario que sea adecuado para nuestro propósito.

REIVINDICACIONES

1. Un método para identificar y controlar un tráfico no solicitado en un sistema de red informática (10), que comprende al menos una primera red de acceso (105, 105a, 105b) que conecta al menos una fuente (101-1 a 101-N; 102-1 a 102-N) a una red central (104) y al menos una segunda red de acceso (107) que conecta al menos un destino (103-1 a 103-N) a dicha red central(104),en donde dicho método comprende las etapas:

- dirigir unidades de tráfico direccionadas a al menos un destino (103-1) a partir de la al menos una fuente (101-1) hacia el portal informático (109) que está interconectado entre la red central (104) y la segunda red de acceso (107);

- verificar cada unidad de tráfico en el portal informático (109) para determinar si la unidad de tráfico ha sido marcada como siendo válida o no;

- identificar cada unidad de tráfico (112) como estando no solicitada si ha sido marcada como no válida o si no ha sido marcada en absoluto;

- controlar el flujo de cada unidad de tráfico (112) que ha sido identificado como no solicitado en respuesta al por lo menos un parámetro del sistema predeterminado, caracterizado por cuanto que

- un mensaje de permiso se genera y transmite a la por lo menos una fuente (101-1);

- las unidades de tráfico, que han de enviarse, son marcadas en la fuente utilizando información procedente del mensaje de permiso e

- información que se relaciona con el mensaje de permiso se memoriza en el portal informático (104) para permitir al portal informático verificar unidades de tráfico, en donde

el mensaje de permiso incluye una clave de etiquetado utilizada para marcar unidades de tráfico que han de enviarse en la fuente y en donde el mensaje de permiso se transmite bajo la forma de una prueba que ha de resolverse por la por lo menos una fuente para obtener la clave de etiquetado, en donde solamente se resuelve la prueba en la fuente con una interacción de un usuario humano.

2. Un método para identificar y controlar un tráfico no solicitado en un sistema de red informática, que comprende al menos una primera red de acceso (105) que conecta al menos una fuente (101-1 a 101-N; 102-1 a 102-N) a una red central (104) y al menos una segunda red de acceso (107) que conecta al menos un destino (103-1 a 103-N) a dicha red central (104), en donde dicho método comprende las etapas:

- dirigir unidades de tráfico direccionadas a al menos un destino (103-1) a partir de la al menos una fuente (103-1) hacia el portal informático (109) que está interconectado entre la red central (104) y la primera red de acceso (105);

- verificar cada unidad de tráfico en el portal informático (109) para determinar si la unidad de tráfico ha sido marcada como válida o no;

- identificar cada unidad de tráfico (112) como no solicitada si ha sido marcada como no válida o si no ha sido marcada en absoluto;

- controlar el flujo de cada unidad de tráfico que ha sido identificada como no solicitada en respuesta a por lo menos un parámetro del sistema predeterminado, caracterizado por cuanto que

- un mensaje de permiso se genera y transmite a por lo menos una fuente (101-1);

- las unidades de tráfico, que han de enviarse, son marcadas en la fuente utilizando información procedente del mensaje de permiso e

- información que se relaciona con el mensaje de permiso se memoriza en el portal informático (104) para permitir al portal informático verificar las unidades de tráfico, en donde

el mensaje de permiso incluye una clave de etiquetado utilizada para marcar unidades de tráfico a enviarse en la fuente y en donde el mensaje de permiso se transmite bajo la forma de una prueba que al menos una fuente ha de resolver para obtener la clave de etiquetado, en donde la prueba se resuelve en la fuente solamente con una interacción de un usuario humano.

3. El método según la reivindicación 1 o 2, en donde

las unidades de tráfico son paquetes IP o paquetes TCP y en donde la red central (104) es la red de Internet.

4. El método según cualquiera de las reivindicaciones 1 a 3, en donde la etapa de control comprende las etapas siguientes:

bloquear, retardar y/o limitar el flujo de cada unidad de tráfico que haya sido identificado como no solicitado a un destino (103-1 a 103-N) en función del estado de congestión de la red central (104) y/o de la segunda red de acceso (107).

5. El método según cualquiera de las reivindicaciones precedentes, en donde un algoritmo CAPTCHA y/o un algoritmo de puzzles de direcciones IP se utilizan para generar una prueba para transmitir el mensaje de permiso a la al menos una fuente.

6. El método según cualquiera de las reivindicaciones precedentes, en donde la clave de etiquetado se utiliza en un código de autenticación de mensaje (MAC) para calcular una etiqueta para marcar unidades de tráfico, en donde la clave de etiquetado o la información destinada a derivar la clave de etiquetado se memoriza en el portal informático.

7. El método según la reivindicación 6, en donde la clave de etiquetado es una clave criptográfica que se utiliza por la fuente para generar etiquetas para marcar unidades de tráfico y que se utiliza por el portal informático para verificar etiquetas incluidas en las unidades de tráfico.

8. El método según cualquiera de las reivindicaciones 1 a 7, en donde el mensaje de permiso se genera por el portal informático (104) y se reenvía a un medio de autenticación (113) que, a su vez, transmite el mensaje de permiso a la al menos una fuente.

9. El método según cualquiera de las reivindicaciones 1 a 7, en donde el mensaje de permiso se genera por un medio de autenticación (113) que transmite el mensaje de permiso a la al menos una fuente y al portal informático.

10. Un sistema de red informática para identificar y controlar un tráfico no solicitado, que comprende

una red central (104),

al menos una primera red de acceso (105; 105a, 105b),

al menos una fuente (101-1 a 101-N; 102-1 a 102-N) conectada a dicha primera red de acceso (105; 105a, 105b),

al menos una segunda red de acceso (107),

al menos un destino (103-1 a 103-N) conectado a dicha segunda red de acceso (107),

al menos un portal informático (109) situado entre la primera red de acceso (105; 105a, 105b) y la red central 104) y/o entre la segunda red de acceso (107) y la red central (104),

un medio (113; 114) para generar y transmitir un mensaje de permiso a la al menos una fuente (101-1 a 101-N; 102-1 a 102-N), en donde

la al menos una fuente (101-1 a 101-N; 102-1 a 102-N) comprende un medio (116) para obtener una clave de etiquetado a partir de un mensaje de permiso utilizada para marcar unidades de tráfico direccionadas a un destino,

el portal informático (109) comprende:

- un medio de memorización para almacenar información relacionada con un mensaje de permiso,
- un medio (117) para verificar las unidades de tráfico recibidas sobre la base de la información memorizada para determinar si las unidades de tráfico están marcadas como siendo válidas o no,
- un medio (117) para identificar como no solicitada a cada unidad de tráfico marcada como no siendo válida y
- un medio (117) para controlar el flujo de cada unidad de tráfico que está marcada como siendo no válida en respuesta a por lo menos un parámetro de sistema predeterminado, caracterizado por cuanto que el medio para generar y transmitir un mensaje de permiso a la al menos una fuente se pone en práctica en una unidad de autenticación (113) que está situada en un dispositivo conectado al portal informático (104) o en al menos un destino, en donde la unidad de autenticación (113) está adaptada para generar un mensaje de permiso bajo la forma de una prueba que ha de resolverse por la al menos una fuente, en donde solamente las fuentes (101-1 a 101-N), que hayan resuelto la prueba, son capaces de marcar unidades de tráfico como siendo válidas, en donde solamente con una interacción de un usuario humano se puede resolver la prueba en la fuente.

11. El sistema de red informática según la reivindicación 10, en donde cada fuente (101-1 a 101-N; 102-1 a 102-N) comprende un ordenador cliente, cada destino (103-1 a 103-N) comprende un servidor y en donde la red central (104) es la red Internet.

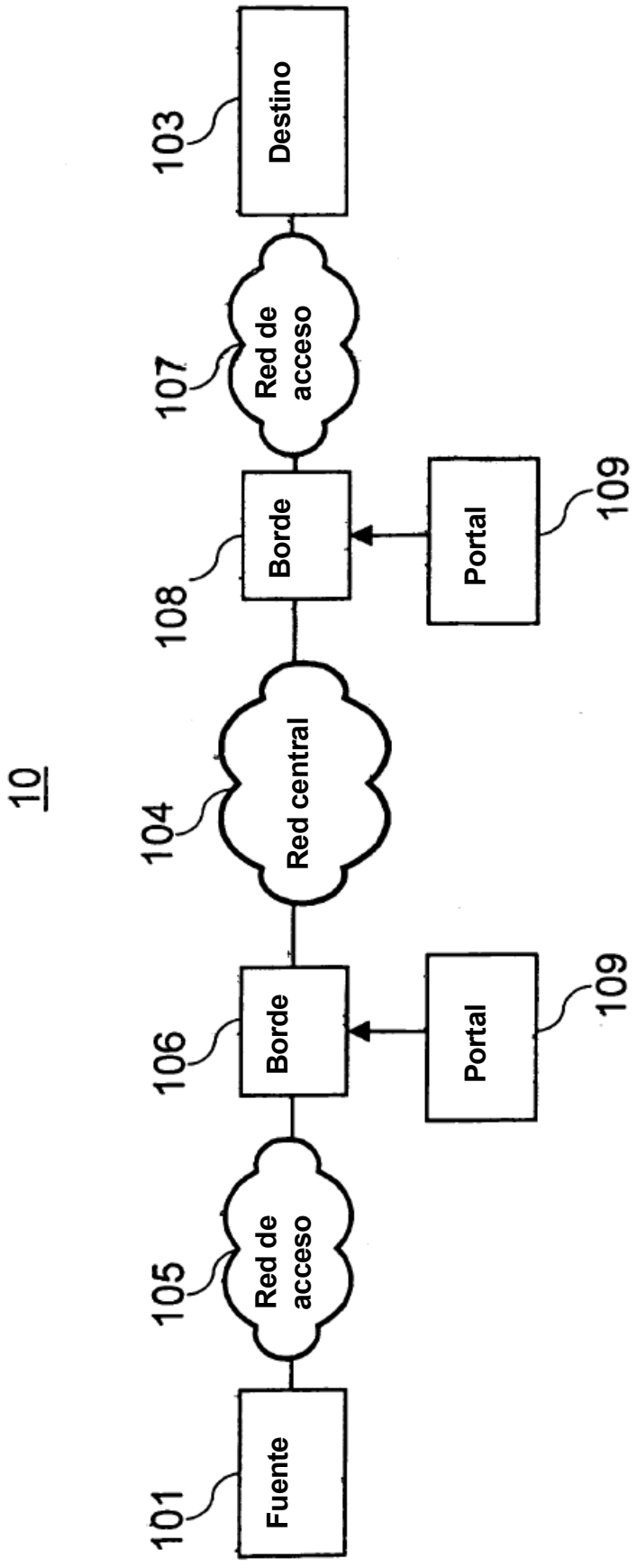
10
101
Fuente
105
Red de acceso
106
Borde
109
Portal
104
Red central
108
Borde
109
Portal
107
Red de acceso
103
Destino

Fig. 1

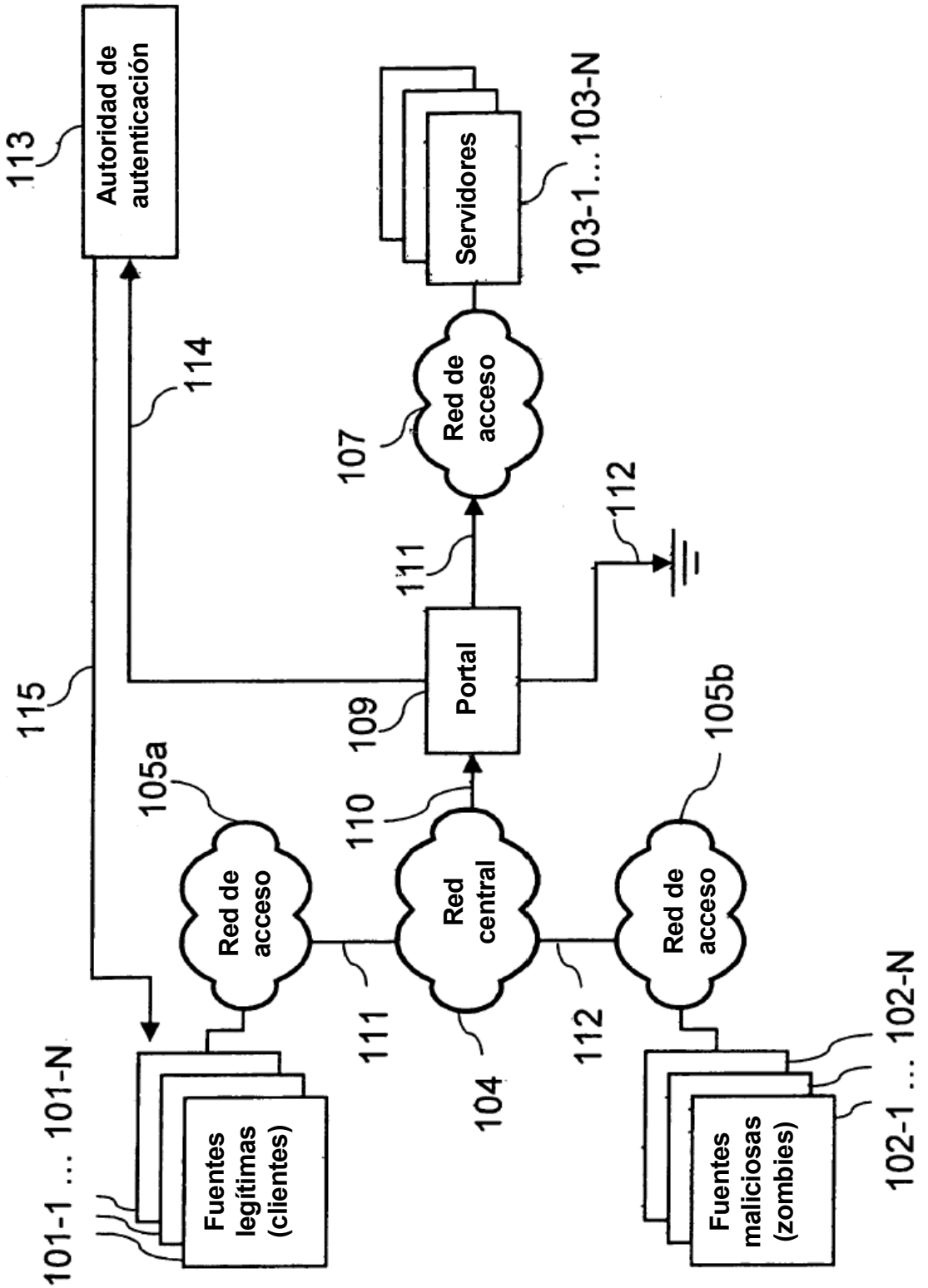
Autoridad de autenticación
113
114
115
Servidores
103-1...103-N
Red de acceso
107
Portal
109
111
112
105a
Red de acceso
110
Red central
104
105b
Red de acceso
Fuentes legítimas (clientes)
101-1 ... 101-N
Fuentes maliciosas (zombies)
102-1 ... 102-N

Fig. 2

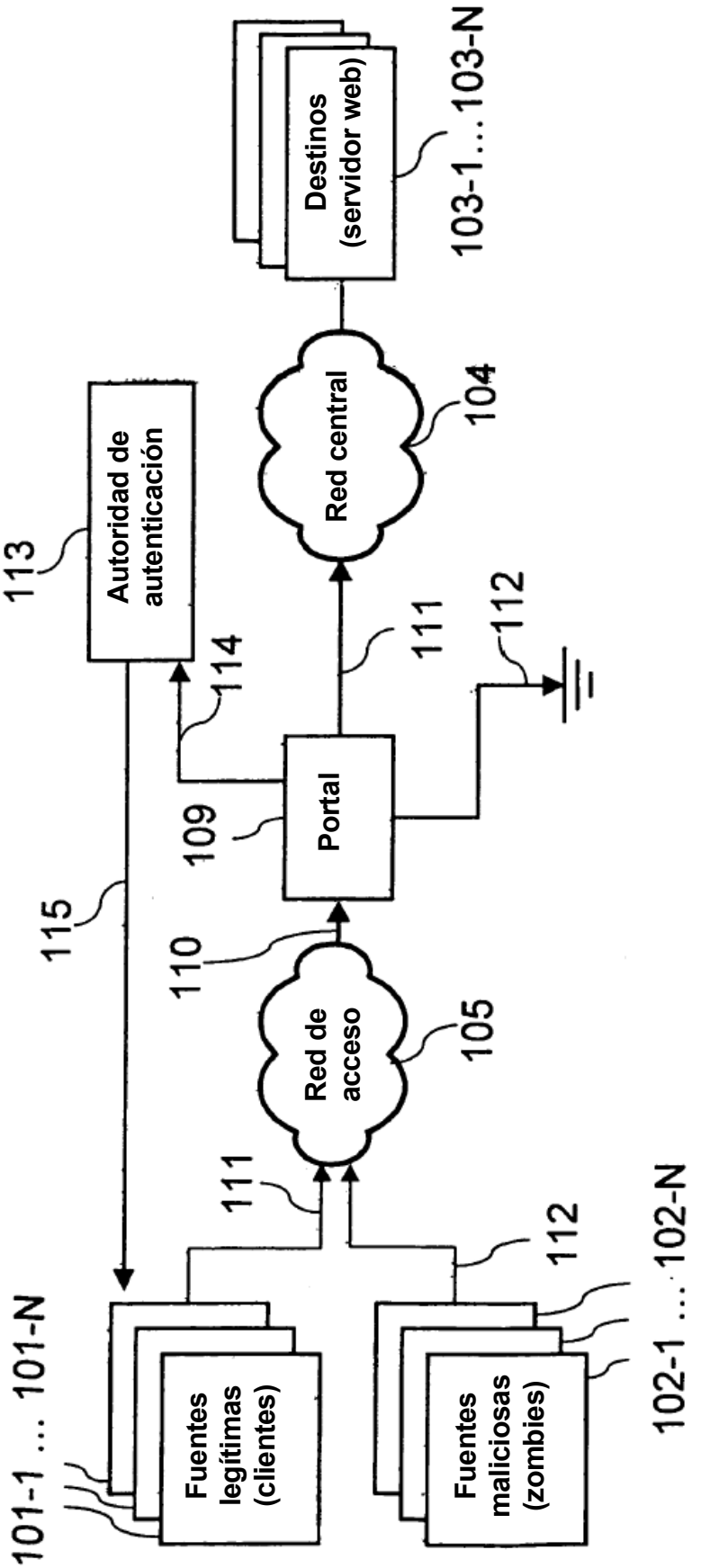
Destinos (servidor web)
103-1....103-N
Red central
104
Autoridad de autenticación
113
114
111
112
109
Portal
115
110
Red de acceso
105
111
112
101-1 ... 101-N
Fuentes legítimas (clientes)
Fuentes maliciosas (zombies)
102-1 ... 102-N

Fig. 3

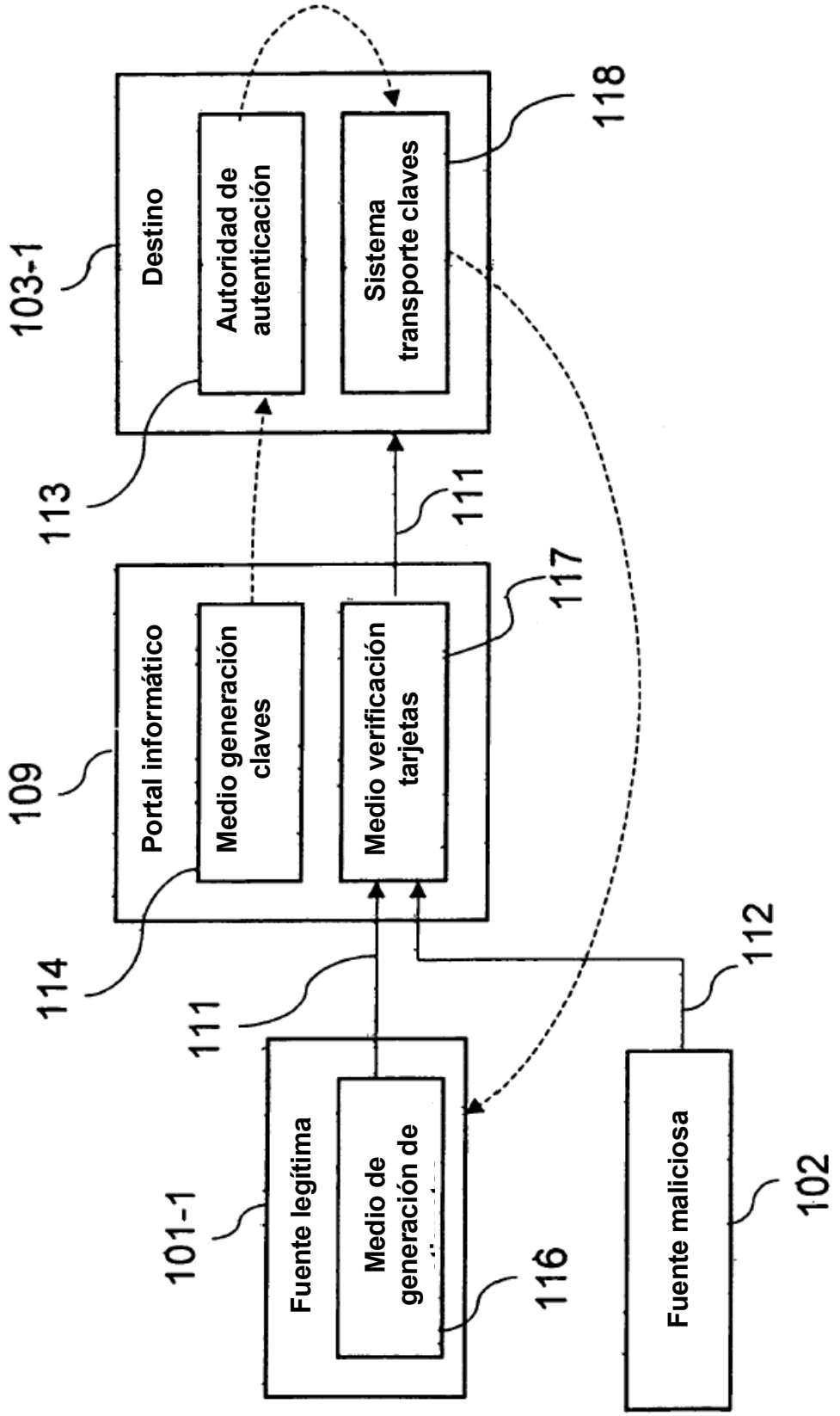
Destino
Autoridad de autenticación
Sistema transporte claves
Portal informático
Medio generación claves
Medio verificación tarjetas
Fuente legítima
Medio de generación de
Fuente maliciosa
103-1
113
111
118
109
114
117
111
112
101-1
116
102

Fig. 4

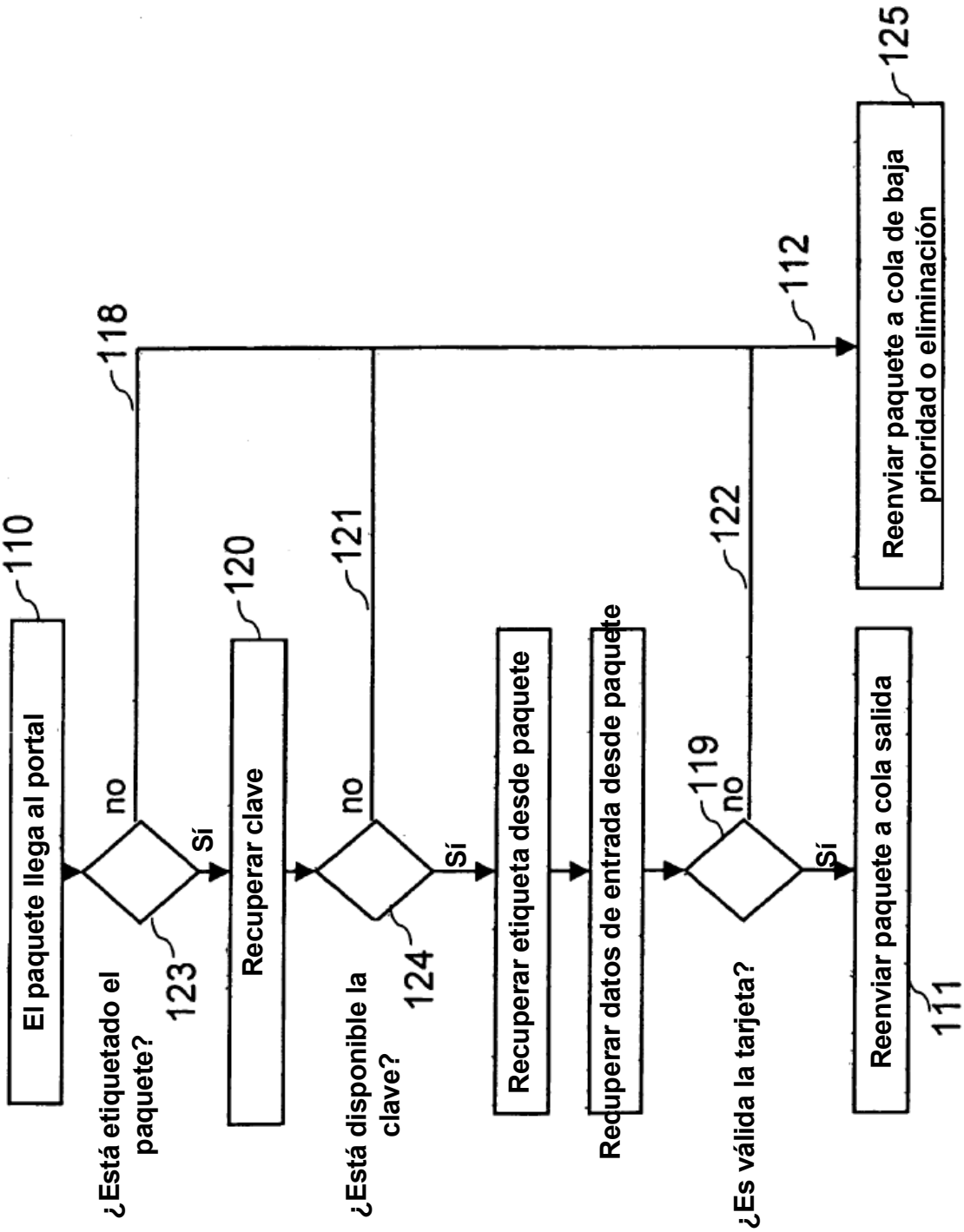
El paquete llega al portal
110
¿Está etiquetado el paquete?
123
no
Sí
118
Recuperar clave
120
¿Está disponible la clave?
124
no
Sí
121
Recuperar etiqueta desde paquete
Recuperar datos de entrada desde paquete
¿Es válida la tarjeta?
119
no
Sí
122
Reenviar paquete a cola salida
111
112
Reenviar paquete a cola de baja prioridad o eliminación
125

Fig. 5