(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 290 167**

(51) Int. Cl.:
H04L 29/06 (2006.01)
H04L 12/28 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **01969660 .8**
(86) Fecha de presentación : **28.08.2001**
(87) Número de publicación de la solicitud: **1316188**
(87) Fecha de publicación de la solicitud: **04.06.2003**

(54) Título: **Procedimiento y nudo de acceso a Internet para la identificación de usuarios de Internet.**

(30) Prioridad: **05.09.2000 EP 00119184**

(45) Fecha de publicación de la mención BOPI:
16.02.2008

(45) Fecha de la publicación del folleto de la patente:
16.02.2008

(73) Titular/es: **SIEMENS AKTIENGESELLSCHAFT**
Wittelsbacherplatz 2
80333 München, DE

(72) Inventor/es: **Mitreuter, Ulrich;**
Unger, Stefan y
Zygan-Maus, Renate

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCIÓN

Procedimiento y nudo de acceso a Internet para la identificación de usuarios de Internet.

1. ¿Qué problema técnico debe resolverse mediante su invención?

2. ¿Cómo se resolvió este problema hasta ahora?

3. ¿De qué manera resuelve su invención el problema técnico indicado (indique Vd. ventajas)?

4. Ejemplo(s) de la invención.

Respecto al punto 1: ¿Qué problema técnico debe resolverse mediante su invención?

Los proveedores de acceso a Internet ofrecen hoy día el acceso a Internet para el mercado de masas sin la característica de servicio "identificación para toda la red del usuario de Internet". No obstante, los nuevos servicios basados en Internet precisan de una identificación del usuario de Internet frente al ofertante de servicios. Esta identificación debe estar también asegurada frente a manipulaciones y abusos por parte de otro usuario de Internet. Por ejemplo, los servicios de telefonía por Internet y los servicios de convergencia Internet - red telefónica presuponen que el usuario de estos servicios (es decir, el emisor de los paquetes IP que contienen los datos de señalización del servicio) será identificado. El ofertante de tales servicios nuevos no es necesariamente idéntico al proveedor del acceso a Internet del usuario de Internet.

Una introducción para toda la red del servicio de identificación de usuarios en Internet correspondiente a la invención incrementaría sustancialmente la confianza en mensajes IP y apoyaría mucho la difusión de aplicaciones comerciales con sus exigencias de seguridad potencialmente elevadas, así como reduciría el abuso en Internet.

Respecto al punto 2: ¿Cómo se resolvió este problema hasta ahora?

Todos los procedimientos conocidos hasta ahora para la identificación asegurada (autentificación) de un usuario de Internet utilizan el principio de la autentificación punto-a-punto. Es decir, los interlocutores de la comunicación se autentifican sobre la base de datos de identificación y autentificación que son asignados a cada interlocutor de comunicación individualmente y que se le dan a conocer al otro interlocutor de comunicación. Estos datos pueden bien

a) ser conocidos ya al otro interlocutor de comunicación antes del comienzo de la comunicación (en el interlocutor de comunicación están memorizados suficientes datos de identificación y autentificación) o bien

b) comunicarlos al otro interlocutor de comunicación al comienzo de la comunicación con la ayuda de una tercera instancia digna de confianza (los datos de identificación y autentificación están memorizados en una instancia central pública de certificación).

Los procedimientos conocidos hasta ahora para la identificación asegurada de un usuario de Internet son:

I. Identificación y autentificación a través de los hosts (servidores) de IP utilizados por los interlocutores de comunicación: IPSEC

   este procedimiento parte de la premisa de que ambos interlocutores de comunicación utilizan direcciones de IP estáticas y estas direcciones de IP están asignadas inequívocamente a ambos interlocutores de comunicación.

   IPSEC no es adecuado para el problema técnico a resolver, ya que

   1. La gran mayoría de los usuarios de Internet utiliza el acceso Dial-in y sólo reciben de su proveedor de acceso a Internet la asignación de una dirección de IP temporal;

   2. IPSEC exige como método punto-a-punto del tipo a) la memorización de los datos de identificación y autentificación de todos los interlocutores de comunicación potenciales y por lo tanto es inadecuado para el mercado de masas de nuevos servicios de Internet.

II. Identificación y autentificación mediante funciones TCP (TLS, Transport Layer Security, seguridad de la capa de transporte)

   este protocolo puede ser utilizado básicamente por todos los programas de aplicación que utilizan TCP/IP. El mismo precisa de adaptaciones en los programas de aplicación, así como la puesta a disposición de datos de identificación y autentificación punto-a-punto, bien según el principio a) o b).

III. Identificación y autentificación mediante los programas de aplicación utilizados.

Los datos para la identificación del usuario, por ejemplo su "nombre", se transmiten en el protocolo de aplicación (por ejemplo HTTP, FTP, Telnet, SIP) en texto explícito. Para la comprobación de que el remitente es el portador del nombre, es decir, para la autentificación del nombre, hay varias posibilidades, por ejemplo

1. Un secreto común, por ejemplo una palabra de paso, que sólo conocen el usuario y su interlocutor de comunicación, se transmite a la vez en el protocolo de aplicación o en los datos útiles de la aplicación. Este método sólo puede utilizarse en combinación con una transmisión asegurada frente a "escuchas" (por ejemplo codificada).

2. Un secreto común se utiliza para codificar una parte del mensaje. Si el receptor puede decodificar el mensaje, entonces el emisor está autentificado como poseedor de la clave de codificación.

3. Mediante un procedimiento Challenge-Response (reto-respuesta) en el protocolo de aplicación se aporta la prueba de que el usuario está en posesión de un secreto común.

4. Un secreto común se utiliza para generar una huella dactilar digital del mensaje, que se anexa al mensaje. Si esta huella dactilar puede ser reproducida por el receptor, entonces el emisor está autentificado como poseedor del secreto común.

5. El emisor genera con ayuda de su "private key" (clave privada) de un procedimiento asimétrico de autentificación una huella dactilar digital del mensaje a enviar, que se anexa al mensaje y se añade al mensaje adicionalmente su certificado electrónico. Este certificado contiene la "public key" (clave pública) y el nombre del usuario. El receptor puede verificar con ayuda de está clave pública la huella dactilar digital. El receptor debe entonces verificar también el certificado. Esto se realiza según el procedimiento estándar para certificados. Para ello contiene el certificado una huella dactilar digital de los datos del certificado, extendida con la clave privada de una instancia de certificación. Si posee el usuario la clave pública de la instancia de certificación, puede el mismo comprobar la integridad del certificado del usuario. La posesión de la clave privada que se utilizó para generar la huella dactilar digital del mensaje autentifica al usuario.

Por el documento de patente US 5 768 391 y US 5 586 260 se conocen otros procedimientos para la identificación asegurada.

El inconveniente de todos los procedimientos conocidos es el gran coste para la instalación, administración y mantenimiento de los distintos bancos de datos que contienen los datos de la identificación y autentificación de los usuarios de Internet (bien costosos depósitos de certificado centrales o muchos bancos de datos de abonado descentralizados en diversos ofertantes de servicios), así como la gestión de la infraestructura que debe asegurar la integridad de los datos de identificación (por ejemplo listas de revocación de certificados, base de datos de política de seguridad). Este coste viene dado porque cada usuario de Internet realiza por sí mismo los protocolos de identificación y autentificación (principio de la autentificación punto-a-punto).

Respecto al punto 3: ¿De qué manera resuelve su invención el problema técnico indicado (indique Vd. ventajas)?

Este problema se resuelve con el procedimiento y el nodo de acceso a Internet según las reivindicaciones independientes 1 y 6.

El proveedor de acceso a Internet dota los mensajes IP de su cliente, según deseos, con datos que permiten la identificación de los paquetes IP del usuario de Internet. El proveedor de acceso a Internet garantiza la integridad de estos datos con medios criptográficos.

La diferencia respecto a los procedimientos antes citados reside por lo tanto en que ya no inicia el propio usuario de Internet su identificación, si no que esto lo asume el proveedor de acceso a Internet. Mediante la invención se reduce el coste para la identificación de paquetes de IP de usuarios de Internet.

Es una premisa para el nuevo procedimiento de identificación y autentificación correspondiente a la invención que el proveedor del acceso a Internet mantenga con el usuario de Internet una relación profesional. Con ello el mismo posee datos que puede identificar el usuario de Internet. Cuando utiliza el usuario de Internet el servicio de acceso del proveedor de acceso a Internet (por ejemplo al establecer un enlace de Internet a través de la línea telefónica) entonces el mismo debe autentificarse al comienzo frente al proveedor del acceso a Internet (usualmente con un nombre de cuenta y una palabra de paso que el proveedor del acceso a Internet ha memorizado). Tras la autentificación, el proveedor de acceso a Internet conoce así de manera asegurada la identidad del usuario de Internet. El puede ahora adjuntar una información que identifique al usuario de Internet a todos los paquetes IP del usuario de Internet. Con esta información pueden identificarse los paquetes IP del usuario de Internet de otros ofertantes de servicios de Internet sin que el propio usuario de Internet deba poner a disposición de los mismos sus datos de identificación, y precisamente según el principio a), es decir, el ofertante de servicios debe memorizar y administrar por sí mismo los datos específicos del usuario de Internet, o según el principio b), es decir, con la ayuda de una instancia central de certificación.

Una analogía de la Public Switching Telephone Network PSTN (red pública telefónica de conmutación) podría aclarar la idea. Al establecerse la llamada en la red telefónica establece la red telefónica el número de llamada del

abonado que llama. El operador de la red telefónica garantiza que este número efectivamente identifica la conexión del número que llama y el número de llamada del abonado que llama es "network provided"(proporcionado por la red) o "user provided, verified and passed" (proporcionado por el usuario, verificado y autorizado). El abonado que llama no está en condiciones de modificar el número, ya que ha sido adjudicado por la red y no por el abonado. Tampoco pueden modificar este número otros abonados de la red telefónica. Así es posible siempre identificar con seguridad las conexiones que participan en una conversación telefónica.

En la red IP esto no es posible, ya que primeramente las direcciones de IP del emisor pueden falsearse en los mensajes IP y en segundo lugar las direcciones IP sólo se ponen a disposición de los usuarios de Internet temporalmente. No obstante, en el marco de la invención puede el proveedor de acceso a Internet en una red IP dotar el mensaje IP de manera segura frente a falsificación, como instancia digna de confianza, de una información establecida por la red, para la identificación del usuario de Internet.

La invención aprovecha la identificación de usuario de Internet usual punto-a-punto para el acceso a Internet entre el usuario de Internet y su proveedor de acceso a Internet para poner a disposición en toda la red, a través de un proveedor de acceso a Internet digno de confianza (dotado de un certificado público) una identificación asegurada de un usuario de Internet.

Respecto a 4: Ejemplo(s) de ejecución de la invención

Para una solución genérica (solución que es independiente del protocolo de transporte o de aplicación utilizado) con un rendimiento lo mejor posible, se propone una realización en el nivel IP (ver figuras 1 y 2).

En el POP (Point-of-Presence, punto de presencia, nudo de acceso) del proveedor de acceso a Internet

- se investigan los paquetes IP en cuanto a si está activado un determinado indicador o Flag (aún por definir) un llamado indicador de solicitud de autentificación (Authentication-Request Flag), con lo que puede solicitarse para el usuario de Internet que se añadan datos de identificación por cada paquete de IP, y/o

- se mira en un banco de datos (que tiene una función análoga a la base de datos de política de seguridad, Security Police Database en IPSEC) respecto a si se solicita para el usuario de Internet el servicio "paquetes IP dotados de datos de identificación". Los selectores pueden ser entonces la dirección de destino de IP, el protocolo de transporte o el puerto TCP/UDP.

Caso afirmativo, añade el proveedor de acceso a Internet a la cabecera del paquete IP los datos que identifican al usuario de Internet. Es posible por ejemplo un número de teléfono del usuario de Internet, o su nombre de usuario utilizado para la suscripción de su acceso a Internet, que es conocido por el proveedor de acceso a Internet.

El proveedor de acceso a Internet forma a continuación mediante el paquete IP modificado, inclusive los datos útiles no modificados enviados por el usuario, una firma digital, para asegurar los datos de identificación y los datos útiles enviados por el usuario frente a falsificación (integridad de datos). Para ello se calcula una suma de comprobación mediante el paquete de IP modificado y ésta se codifica con la clave secreta del ISP (Integrity Check Value, valor de comprobación de integridad). Finalmente añade el proveedor de acceso a Internet a la cabecera del paquete de IP su certificado electrónico (ISP X.509 Certificate), que contiene la clave pública del ISP para decodificar la suma de comprobación. De esta manera puede comprobar todo receptor del mensaje IP si la firma digital es correcta, decodificando la suma de comprobación y comparándola con la suma de comprobación que ha calculado el receptor. Además, el receptor tiene la posibilidad de acceder a través del poseedor del certificado citado en el certificado (el proveedor de acceso a Internet) a otros datos del usuario de Internet (nombre, dirección). (Esto podría utilizarse para la identificación de quienes llaman con malicia (Malicious Caller Identification).

La realización propuesta posee similitudes con IPSEC. No obstante, la diferencia esencial es que, contrariamente a IPSEC, no puede realizarse ninguna autentificación punto-a-punto, sino una autentificación punto-a-multipunto, ya que todos los datos relevantes para la autentificación (el "nombre" del usuario de Internet, el nombre del proveedor de acceso Internet (ISPs) y su certificado) están contenidos en el paquete IP. Además, no existe una autentificación punto-a-punto ni una autentificación servidor-a-servidor, sino una autentificación ISP-a-servidor.

La realización de la identificación del usuario de Internet al nivel IP exige una nueva función opcional de la pila de IP (IP-Stack). En el caso de que esta función no esté disponible en el Host (servidor) del receptor, ha de ignorarse toda la información AOD nueva (ver figura 2) de un mensaje IP. Esta función, para opciones IP desconocidas, viene apoyada ya hoy día por pilas IP (IP-Stacks) estándar.

Puesto que la longitud de un mensaje IP se modifica mediante la inserción de la información AOD, deben calcularse de nuevo tanto el campo de la longitud total (TotalLength) como también la suma de comprobación de cabecera (HeaderChecksum) en la cabecera (Header) IP. La firma digital del proveedor de acceso a Internet rige hasta que se modifican los datos en el IP Payload (carga útil).

Es posible que los datos en el IP Payload (carga útil) puedan ser modificados en la trayectoria del mensaje IP hacía el interlocutor de comunicación propiamente dicho, por ejemplo mediante Proxies (servidores intermediarios)

autorizados (por ejemplo el campo VIA en SIP, direcciones de IP en NAT). El Proxy calcula entonces el campo TotalLength (longitud total), así como HeaderChecksum (suma de comprobación de cabecera) en la cabecera IP.

En un caso así, puede el Proxy opcionalmente ser ya End-Host (servidor terminal) de la transmisión asegurada según la invención. Este es el caso por ejemplo cuando el Proxy realiza la autentificación del usuario de Internet para comprobar si el mismo por ejemplo es ya un cliente del receptor de mensajes. El Proxy comprueba el AOD y retransmite el mensaje IP sin el AOD.

Otra opción es que el Proxy realice una adaptación de la información AOD y firme estas modificaciones mediante la firma digital. Para ello calcula el Proxy el Integrity Check Value (valor de comprobación de identidad) y sobrescribe el que había hasta ahora. Adicionalmente, el Proxy sustituye el certificado ISP por su certificado y amplía los Origin Identification Data (datos de identificación de origen) en informaciones que identifican el ISP.

La ventaja de la realización en el nivel IP frente a una realización en el nivel de transporte o de aplicación es que el proveedor de acceso a Internet en el POP puede ver muy rápidamente si deben insertarse datos de identificación o no, ya que para ello sólo tiene que analizarse la cabecera IP o consultarse el banco de datos Policy (política) (ventaja de Performance o rendimiento). Los datos de los niveles de protocolos más elevados que se intercambian punto-a-punto, no se modifican. Las aplicaciones sobre los Hosts (servidores) de Internet que utilizan esta nueva opción IP, necesitan una interfaz de red IP ampliada (IP socket - Interface, interfaz de conexión IP) para al salir activar dado el caso el identificador de autentificación para un paquete de IP o transferir los datos de identificación del emisor a la interfaz de red de IP y al llegar leer los datos de identificación del emisor recibidos. EL ISP, que ofrece la nueva característica de acceso a Internet “Identificación de usuarios de Internet”, necesita un banco de datos Policy (política) que debe ser administrado. Adicionalmente necesita el ISP para sí mismo un certificado de una instancia pública de certificación, que también debe ser gestionado y mantenido (actualización de las listas de revocación de certificados, etc).

REIVINDICACIONES

1. Procedimiento para la identificación de usuarios de Internet, según el cual

un usuario de Internet es identificado y autentificado en el nodo de acceso a Internet del proveedor de acceso a Internet en el marco de una comprobación de acceso cuando utiliza el servicio de acceso a Internet de un proveedor de acceso a Internet con el que el usuario de Internet mantiene una relación profesional,

caracterizado porque

una vez realizada con éxito la comprobación de acceso por el nodo de acceso a Internet y antes de su retransmisión, se añade a la cabecera IP de un mensaje IP del usuario de Internet una información que identifica al usuario de Internet, garantizándose la integridad de esta información con medios criptográficos.

2. Procedimiento según la reivindicación 1,

caracterizado porque

a la cabecera (Header) de un mensaje IP se le adjunta la información que identifica al usuario de Internet sólo cuando se da la correspondiente premisa.

3. Procedimiento según la reivindicación 2,

caracterizado porque

la citada premisa viene predeterminada por el usuario de Internet.

4. Procedimiento según la reivindicación 1 ó 2,

caracterizado porque

la existencia de la citada premisa es comprobada por el nodo de acceso, tomando el mismo informaciones del mensaje de IP y/o de un banco de datos para este fin.

5. Procedimiento según una de las reivindicaciones 1 a 4,

caracterizado porque

la integridad de la información que identifica al usuario de Internet se garantiza con una firma digital.

6. Nodo de acceso a Internet, que

identifica o autentifica a un usuario de Internet en el marco de la realización del servicio de acceso a Internet,

caracterizado porque

el mismo, tras realizarse con éxito el servicio de acceso a Internet añade a la cabecera de IP de un mensaje IP del usuario de Internet, antes de su retransmisión, una información que identifica al usuario de Internet, garantizando el mismo la integridad de esta información con medios criptográficos.

7. Nodo de acceso a Internet según la reivindicación 6,

caracterizado porque

el mismo sólo añade a la cabecera de IP de un mensaje de IP la información que identifica al usuario de Internet cuando se da la correspondiente premisa.

8. Nodo de acceso a Internet según la reivindicación 7,

caracterizado porque

el mismo comprueba la existencia de la citada premisa con ayuda de informaciones que toma del propio mensaje de IP y/o de un banco de datos.

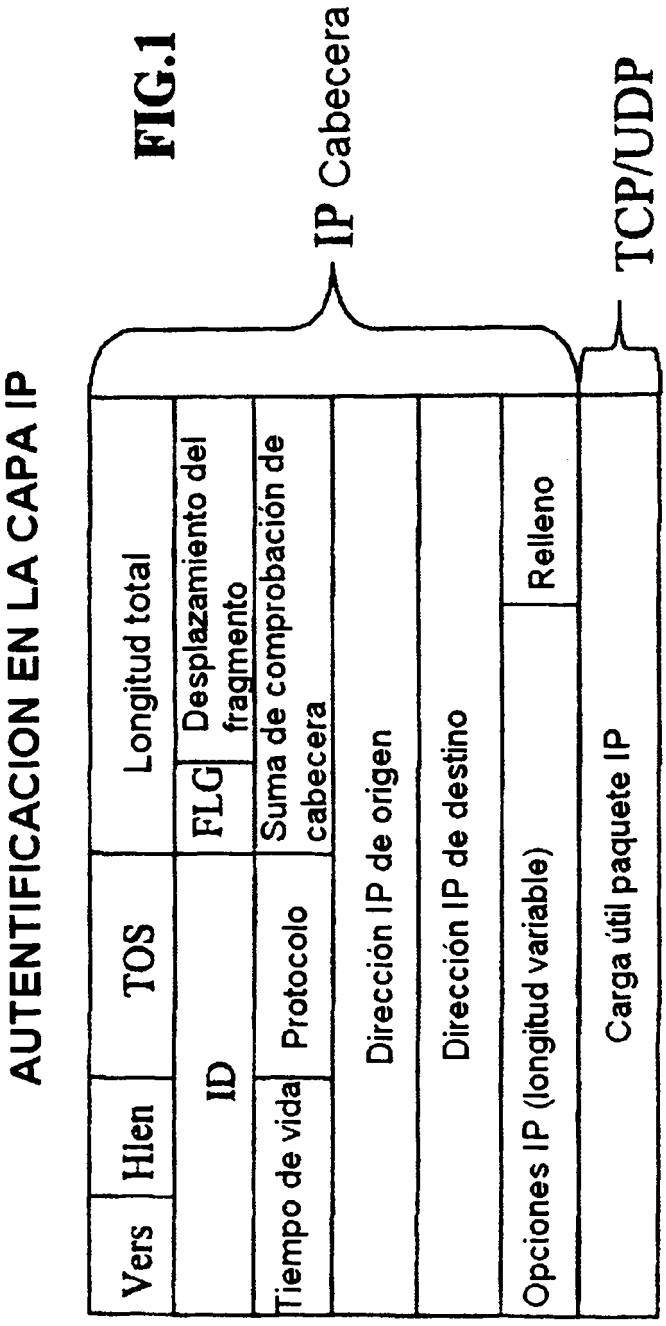
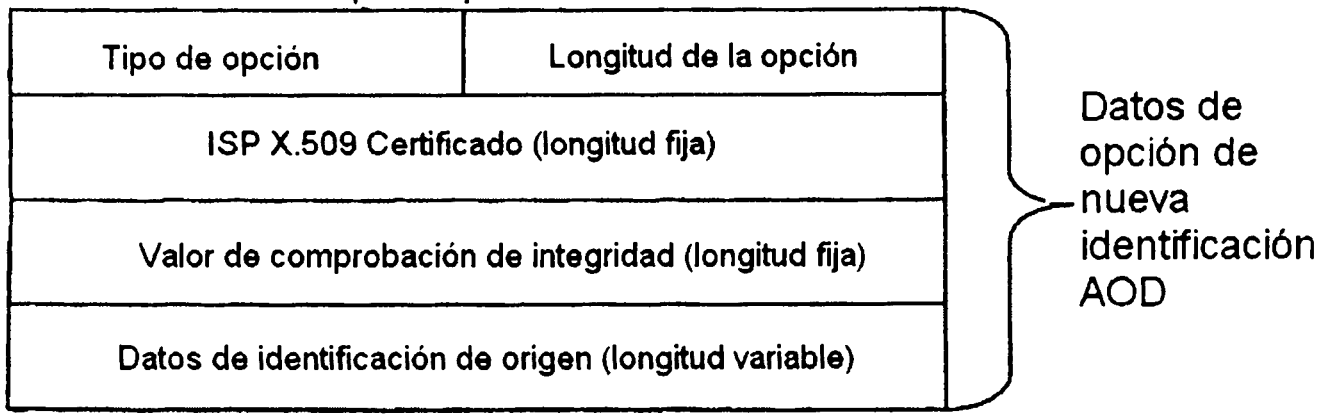


FIG.1

Los datos de identificación se inscriben en el campo "Opciones IP" (ver figura 2)

AUTENTIFICACION EN LA CAPA DE IP

Campo de opciones de IP



Campo de tipo de opción IP

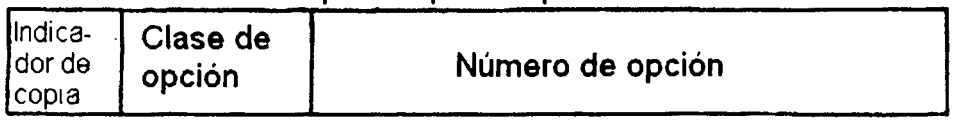


FIG.2

En el campo IP Options Type Field (campo de tipos de opción) se coloca la clase de opción en 1 ó 3 (actualmente reservado para futura utilización); debe asignarse un nuevo Option Number (número de opción).
El Integrity Check Value (valor de comprobación de integridad) se calcula sobre los datos originales de identificación y el IP Packet Payload (carga útil del paquete de IP).