(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 367 588**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07113638 .6**
(96) Fecha de presentación : **01.08.2007**
(97) Número de publicación de la solicitud: **2018015**
(97) Fecha de publicación de la solicitud: **21.01.2009**

(54) Título: **Procedimiento y dispositivo para una comunicación de datos y de voz móvil codificada anónima.**

(30) Prioridad: **17.07.2007 DE 10 2007 033 667**

(45) Fecha de publicación de la mención BOPI:
04.11.2011

(45) Fecha de la publicación del folleto de la patente:
04.11.2011

(73) Titular/es: **GSMK Gesellschaft für Sichere Mobile Kommunikation mbH**
Marienstrasse 11
10117 Berlin, DE

(72) Inventor/es: **Rieger, Frank y**
Gonggrijp, Robbert

(74) Agente: **De Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Procedimiento y dispositivo para una comunicación de datos y de voz móvil codificada anónima

La invención se refiere a un procedimiento que posibilita a los usuarios intercambiar mensajes codificados anónimos móviles y realizar conversaciones telefónicas. El procedimiento consiste en una combinación de codificación fuerte para la protección de los contenidos de la conversación y un mecanismo de anonimato para la protección de los datos de la comunicación de los usuarios.

Campo de la invención

Se conocer terminales móviles con codificación fuerte, que están en condiciones de codificar el contenido de conversaciones telefónicas y de mensajes cortos (por medio del Servicio de Mensajes Cortos SMS). La técnica relevante para el procedimiento previsto se basa en una memoria segura (“almacenamiento seguro”) como lugar de conservación de claves autentificadas. La memoria segura debe ser liberada por el usuario para la utilización por medio de una palabra de paso. El procedimiento soporta varios tipos de transmisión de mensajes (“tipos de transporte”), como por ejemplo SMS, CSD, GPRS, etc. así como varios tipos de mensajes, que caen entre los dos tipos principales “Texto y “Medios”. En general, existe una posibilidad de aproximación independiente del tipo de transporte de un tipo determinado de mensajes, aunque, por razones técnicas, no todos los tipos de mensajes armonizan con todos los tipos de transporte (como ejemplo se menciona la transmisión extremadamente antieconómica de mensajes de voz a través del servicio de mensajes cortos SMS).

Una codificación posible se realiza, por ejemplo, con los criptoalgoritmos AES y Twofish (ambos con 256 bits de largo de la clave) en el modo CFB con un registro de corredera de 256 bits; el intercambio de claves se realiza con un mecanismo Diffie-Helmman de 4096 bits con protección basada en cálculo de claves contra ataque “man in the middle”. Pero el procedimiento está abierto también para otros algoritmos.

La publicación “Tor: The Second-Generation Onion Router “Proceedings of the 13th Usenix security symposium”, publica la TOR – Tecnología Router para la transmisión de datos, para no posibilitar su seguimiento.

Sin embargo, en este principio es un inconveniente que se puede verificar, además, el establecimiento de la comunicación. Así, por ejemplo, se puede determinar quién ha hablado por teléfono con quien y cuándo.

Resumen de la invención

El problema de la presente invención es un anonimato de la comunicación, de manera que no se pueda determinar la identidad de los interlocutores implicados.

Este problema se soluciona por medio de un procedimiento y un dispositivo con las características de las reivindicaciones independientes.

Esencialmente, el procedimiento a patenten añade al componente de codificación existente un componente de anonimato, que no sólo posibilita ya como hasta ahora codificar la propia conversación, sino también enmascarar quién se ha comunicado con quién (y si se ha comunicado o no). Este protección se dirige en primer término contra análisis de datos de tráfico (“traffic análysis”) sobre la base de la memorización de datos de reserva (“call data record” CRD).

A tal fin, el procedimiento de acuerdo con la invención se sirve de una red de anonimato llamada “Tor”. Tor se basa en el principio del “Onion Routing”: las comunicaciones sobre el aparato del usuario se realizan a través de un llamado “Onion Proxy”, que selecciona para cada comunicación una ruta seleccionada de forma aleatoria a través del rúter existente en la red Tor. El último servidor aparece en este caso, por decirlo así, como “exit node” (nodo de salida) y emite los datos después de abandonar la nube Tor al receptor final. En este instante, no se puede determinar ya, tampoco por un observador constante del “nodo de salida”, quién era el emisor del mensaje. Este principio y sus componente se conocen a partir del proyecto “Tor”, http://tor.eff.org.

El procedimiento de acuerdo con la invención utiliza el llamado “Tor Hidden Service” para indicar a los interlocutores de la comunicación a través de un mecanismo desarrollado la disponibilidad de un usuario. Un usuario, que está en línea, anuncia con la ayuda de otro procedimiento descrito más adelante un servicio oculto “hidden service”, que es conocido por el otro interlocutor. De esta manera tiene lugar una comunicación, que consta de dos líneas virtuales de servicio oculto “hidden service” – una para cada dirección. Todos los paquetes de datos (que contienen texto, voz, etc.), que son emitidos a través de estas líneas virtuales de servicio oculto “hidden service”, son codificados en primer lugar independientemente de la otra codificación de cana existente en la vía de transporte. De esta manera, se asegura que se mantenga la confidencialidad del mensaje, incluso si un atacante consiguiese eludir el anonimato.

Después de la codificación, todos los mensajes son emitidos desde el usuario A al usuario B en “hidden circuit” o bien un “circuito oculto”, que transporta los mensajes a través de la nube Tor y de esta manera enmascara la relación de comunicación entre A y B. A tal fin, cada usuario debería conocer la “ID del servicio oculto” de la otra

parte. A través de una distinción de IDs de servicio “público” y “privado” se impiden ataques a través de una correlación cruzada o a través de interferencia “spoofing” de los “c/o-hosts” interconectados. Las IDs de servicio para cada interlocutor de la comunicación de un usuario son memorizadas con un Alias local en la memoria segura del aparato.

La sección siguiente presenta una descripción técnica detallada del procedimiento para la utilización de la red Tor para la comunicación anónima codificada con aparatos móviles.

Los circuitos se utilizan de manera que se pueden emitir mensajes desde A hacia B en el circuito, en el que el usuario B y el usuario A están conectados como servidor de “servicio oculto”. B emite mensajes al circuito que ha establecido A, hacia su servidor de “servicio oculto”. Esto es necesario, en el caso de un usuario, que ha irrumpido o que ha eludido esquemas de autentificación o, lo que es todavía más probable, que ha robado la clave Tor de un usuario, para anunciarse entonces con las IDs de otro usuario, para acceder a sus mensajes. De esta manera se utilizan dos canales para una comunicación bidireccional, como es el caso en la comunicación de voz.

De esta manera se puede impedir que una interferencia “Spoofing” con éxito a la ID del “servicio oculto” conduzca a una pérdida de mensajes y a una pérdida de sincronización de las cadenas “key hash”. Puesto que se utiliza una codificación propia dentro de los circuitos Tor, no se publica un contenido de mensajes, de la misma manera en el caso de que fallen la codificación Tor y/o las tecnologías anti-interferencia (Anti-Spoofing).

Tan pronto como un usuario se ha conectado con el sistema Tor, se registran los servicios ocultos, a través de los cuales es accesible, en la nuble Tor. En el caso de que un cliente esté configurado en esta forma, el cliente trata entonces de contactar con un servicio oculto del usuario en su Lists Buddy o bien lista de contacto y se actualiza el estado en línea de la lista Buddy, en el caso de que se pueda alcanzar. Los circuitos de servicios ocultos se pueden mantener entonces activos para mensajes de entrada y salida y para actualizaciones de estado en línea o se pueden desconectar después de una transmisión de mensajes (en función de la configuración del usuario, ver los perfiles de conexión).

Para estar en condiciones de contactar con un usuario, debe conocerse, en general, su ID de servicio oculto (por ejemplo, 5xmm3d9vkn21kg90.onion). Hay que determinar el número máximo práctico de IDs de servicios ocultos, que se pueden mantener abiertas por aparato. En la práctica, el usuario debería poseer una ID pública de “servicio oculto” (ésta se puede publicar en tarjetas de negocios o en directorios), que se utiliza para establecer un contacto interno. El software del cliente asocia entonces a cada interlocutor de la comunicación una “ID de servicio oculto” unívoca (esto impide una relación cruzada o una interferencia en el c/o-Host, como se describe más adelante). Si se desea, un usuario puede generar de la misma manera manualmente una ID unívoca y la puede emitir manualmente a los interlocutores de la comunicación. En este caso, hay que evitar que se emitan IDs duplicadas. Este principio es posible porque las IDs de servicio son generadas por los propios terminales (algoritmos conocidos) y se evita una colisión en virtud de su longitud. Esta ID de servicio se pone a la disposición de los Rúter vecinos, que utilizan las IDs de servicio de acuerdo con un procedimiento especial para el direccionamiento.

Las IDs de los interlocutores de la comunicación son provistas con preferencia con un Alias local, que está registrado en el libro de direcciones seguro.

El tipo especial de configuración es el c/o-Host. Éste se puede presentar como una especie de contestador automático fiable para mensajes Tor. Todas las comunicaciones entre un usuario y el c/o-Host se realizan a través de un circuito de servicio oculto especial asociado con una ID secreta. El usuario transmite su ID de “servicio oculto” al c/o-Host (para ello debe depositar su llave de “servicio oculto” de Tor en el servidor). El c/-Host supervisa entonces si estas IDs están en línea a través de intento de contacto periódico. En el caso de que éstas estén fuera de línea, el c/o-Host registra las IDs en la nube Tor, conecta las IDs correspondientes de los interlocutores de la comunicación y recibe todos los mensajes de ellos con la respuesta Mensajes “registrados por c/o-Host”.

Cuando el usuario está en línea, se conecta en primer lugar con su c/o-Host, recibe los mensajes registrados e induce al c/o-Host a des-registrarse con su ID de la red. Entonces registra las IDs con su aparato y emite su mensaje de “reconocimiento recibido” para todos los mensajes, que ha recibido desde el c/o-Host. Con esta instalación se consigue la funcionalidad de un sistema e-mail actual y de un sistema de mensajes al instante (Instant Messaging), sin un Host central atacable y sin la posibilidad de lesión a través de un análisis del tráfico.

El lugar del c/o-Host no tiene que ser conocido por todos en esta configuración, salvo el operador de la máquina física (éste puede ser el propio usuario, que debería confiar un poco al menos en el servidor). El cliente total (Desktop-Client) puede contener igualmente una funcionalidad c/o, de manera que se simplifica mucho dejar funcionar un c/o-Host personal en un sistema Desktop. Lo único que debe realizar el usuario es que puede introducir la ID de “servicio oculto” de su c/o-Host, que se indica a través de software en su aparato móvil.

Puesto que el c/o-Host está conectado de la misma manea con el usuario a través del circuito Tor o bien la nube, y no registra las claves de codificación o mensajes de texto claro, una asunción del c/o-Host solamente puede provocar una pérdida de los mensajes registrados y posibilitar al atacador dejar funcionar un ataque activo contra el

anonimato del usuario, añadiendo un patrón de ciclo de tiempo durante el tráfico con el usuario. El contenido de los mensajes y los emisores originales de los mensajes registrados están asegurados, además, contra los atacantes.

Los circuitos Tor son momentáneamente comunicaciones TCP en la forma de realización preferida. Esto significa que se supone una fiabilidad relativamente alta, en el caso de que se establezca el circuito. No obstante, se contempla también emitir datos a través de redes, que son menos fiables, como puede ser, por ejemplo, una comunicación UDP. De esta manera, no está limitado a comunicaciones TCP.

Además, deberían rellenarse los mensajes, para que llenen paquetes-IP no fragmentados dentro de un circuito Tor. Los mensajes, que son más largos que un paquete se dividen en varios paquetes, con indicadores de conexión, que permiten un restablecimiento correcto. Cada paquete es tratado como mensaje separado, lo que significa que presenta un tránsito de la comunicación y se puede decodificar, aunque se pierdan otros paquetes, que pertenecen al mismo mensaje.

Otro objetivo importante de la capa de transporte Tor es el camuflaje del tráfico. Con preferencia, el tráfico de "servicio oculto" debería contemplarse como una comunicación https:// habitual. Esto se puede conseguir, por una parte, porque se pueden realizar modificaciones en el protocolo, de manera que éste se pueda retornar a la nube principal Tor y porque lo realizan los propios usuarios. En este caso, la comunicación de voz o la comunicación SMS/MMS se emiten a través de un protocolo que, en virtud de sus puertos y su direccionamiento corresponde a una comunicación https://. Puesto que el contenido de los paquetes está codificado, no se puede sacar ninguna conclusión sobre una comunicación de voz.

Esencialmente, los dos motivos principales para emplear un camuflaje del tráfico, son la prevención de problemas de los usuarios y la funcionalidad mejorada en entornos limitados de la red, como existen con frecuencia en redes IP basadas en GSM. Esto puede conducir incluso a que deba añadirse una capa exterior auténtica de http/TLS sobre la comunicación entre el cliente y el primer servidor Tor. Puesto que los certificados pueden ser depositados por el propio usuario, se pueden evitar problemas tales como Sniffen de SSL-Proxies o certificados de corriente principal.

El cliente Tor recibe momentáneamente una tabla Host grande con anchura de banda y atributos Uptime durante la conexión con la red y selecciona al menos en primer Host en la cadena, sobre la base de los atributos. Puesto que este principio se puede utilizar para reconocer que un cliente Tor está presente, exactamente como para los ataques de eliminación del anonimato y la alta necesidad de anchura de banda para un aparato basado en GRRS, el cliente debería trabajar de otra forma. Por lo tanto, con preferencia se calculan solamente subgrupos aleatorios de Hosts en una tabla o se registran las tablas en memoria Cache o se seleccionan otras vías para la actualización regular de la tabla. Idealmente se forma una pluralidad de primeros Hosts de entrada fiables o se encuentran otros medios para acondicionar puntos de entrada, para que la nube Tor no se pueda bloquear fácilmente por un operador. Así, por ejemplo, existen principios, que permiten trabajar sobre prioridades. De este modo se puede realizar una actualización para usuarios con una prioridad alta cuando se ha comunicado con ellos con frecuencia en el pasado. Puesto que los nodos de salida Tor pueden ser un objetivo para un número cada vez mayor de ataques por la puerta trasera, lo que conduce a un abuso creciente, deben estar presentes un gran número de nodos de salida, que se pueden introducir o retirar continuamente.

Los nodos, que utilizan la presente versión Tor, deberían utilizar procedimientos anti-seguimiento adicionales, como la fluctuación de tiempo aleatoria de paquetes, que se emiten. De la misma manera, se puede contemplar un indicador de protocolo fuera del tránsito de la codificación, que declara si deben liberarse paquetes de informaciones de tiempo respectivas; estos paquetes se transmiten a costa de un tiempo de latencia más elevado o se purifican de manera menos estricta y reciben de esta manera una latencia más reducida.

Breve descripción de las figuras:

Las figuras siguientes sirven para una mejor comprensión de la invención. No deben servir para la limitación del alcance de la protección. En este caso:

La figura 1 muestra el diagrama de la comunicación de dos terminales a través de la red Tor.

Descripción detallada de una forma de realización posible:

La figura 1 muestra el diagrama de la solicitud en una forma de realización preferida. Tanto el Terminal A como también el terminal B son accesibles a través de una ID pública en la red Tor. El terminal B podría establecer ahora una comunicación con el aparato A. A tal fin, se registra una ID privada (ésta se puede generar en cualquier momento de forma asíncrona. En virtud del espacio grande de direcciones se producen con muy poca probabilidad colisiones), a través de la cual hay que realizar en el futuro la comunicación. En la etapa siguiente, se emite entonces una solicitud de comunicación a la ID pública de A, que transmite la red Tor.

Después de la recepción de la solicitud a través de A, A registra una ID privada A1 y establece una comunicación con B2. B acepta esta comunicación y A emite a través de B1 la información de la comunicación. B recibe la ID A1 a

través de B1 y establece ahora, además, una comunicación con A1. A acepta la comunicación con A1. De esta manera, se puede realizar una comunicación a través de IDs secretas A1 y B1, emitiendo A los datos útiles a través de la dirección B1 y B a través de la dirección A1.

Este figura sirve para una mejor comprensión de la invención. No tiene el propósito de limitar la invención. El alcance de la protección sebe determinarse a través de la interpretación más amplia de las reivindicaciones adjuntas.

REIVINDICACIONES

1.- Procedimiento para el anonimato de la comunicación de terminales móviles, que realiza una comunicación de voz, utilizando una red de anonimato, que comprende una serie de rúters, que presenta al menos un nodo de acceso, en el que cada terminal móvil establece una conexión con al menos un nodo de acceso, que comprende las etapas.

- anuncio del terminal móvil en la red a través de un nodo de acceso;

- preparación de una identidad den la red;

- comunicación a través de la red de anonimato, en la que la red selecciona para la comunicación diferentes rutas aleatorias a través de la red, de manera que es impide un seguimiento y en la que se codifica la comunicación, siendo realizada la comunicación de voz, respectivamente, a través de dos líneas virtuales, una para cada dirección, que son codificadas de manera independiente entre sí y que son direccionadas de manera diferente.

2.- Procedimiento de acuerdo con una o varias de las reivindicaciones anteriores, en el que el terminal móvil es accesible a través de una ID de servicio público y después de una toma de contacto, se transfiere la comunicación a través de una ID de servicio privado.

3.- Procedimiento de acuerdo con la reivindicación anterior, en el que se memorizan IDs de servicio para cada interlocutor de la comunicación de un usuario con un Alias local en una memoria segura del terminal móvil.

4.- Procedimiento de acuerdo con la reivindicación anterior, en el que después del anuncio se realiza una actualización del estado en línea.

5.- Procedimiento de acuerdo con la reivindicación anterior, en el que solamente se determinan subgrupos aleatorios de Hosts en una tabla, se registran las tablas en memoria Cache o se forma un número de primeros Host de entrada fiables, que registran las tablas en memoria Cache, o se lleva a cabo una actualización de usuarios según prioridad, siendo la prioridad alta cuando se ha comunicado con éstos con frecuencia en el pasado.

6.- Procedimiento de acuerdo con una o varias de las reivindicaciones anteriores, en el que se emplea un c/o-Host, que asume la función de un contestador automático para los mensajes de voz y los mensajes de texto y en el que se deposita con preferencia una ID de “servicio oculto”, verificando el c/o-Host si estas IDs están en línea, y en el caso de que estas IDs estén fuera de línea, el c/o-Host registra las IDs en la propia nube Tor y conecta las IDs correspondientes de los interlocutores de la comunicación y recibe todos los mensajes de ellos con preferencia con la respuesta Mensajes “almacenados por c/o-Host” y en el que cuando el Terminal móvil está en línea, se conecta en primer lugar con su c/o-Host, recibe los mensajes registrados y induce al c/o-Host a que se des-registre con su ID de la Red, entonces el terminal móvil registra las IDs con su aparato y emite entonces con preferencia un mensaje de “reconocimiento recibido” para todos los mensajes, que ha recibido desde el c/o-Host.

7.- Procedimiento de acuerdo con una o varias de las reivindicaciones anteriores, en el que se camufla el tráfico, viendo la comunicación como una comunicación https.// normal.

8.- Terminal móvil para el anonimato de una comunicación de voz, que comprende:

- medios, que llevan a cabo la comunicación de voz;

- medios para el anuncio del Terminal móvil en una red de anonimato a través de un nodo de acceso;

- medios para la preparación de una identidad en la red de anonimato;

- medios de comunicación para la comunicación de voz a través de la red de anonimato, seleccionando la red para la comunicación rutas aleatorias diferentes a través de la red, de manera que se impide un seguimiento y en el que se codifica la comunicación, estando presentes medios que llevan a cabo la comunicación de voz a través de dos líneas virtuales, respectivamente, una para cada dirección, que se codifican de manera independiente entre sí y que son direccionadas de forma diferente.

9.- Terminal móvil de acuerdo con una o varias de las reivindicaciones anteriores del terminal, en el que están presentes medos, de manera que el terminal móvil es accesible a través de una ID de servicio público en la red de anonimato, y después de una toma de contacto, se transfiere la comunicación a través de una ID de servicio privado.

10.- Terminal móvil de acuerdo con la reivindicación anterior del terminal, en el que está presente una memoria segura, y las IDs de servicio para cada interlocutor de la comunicación de un usuario están registradas con un Alias local en una memoria segura.

11.- Terminal móvil de acuerdo con la reivindicación anterior del terminal, en el que después del anuncio se lleva a

cabo una actualización del estado en línea del usuario en la memoria segura.

12.- Terminal móvil de acuerdo con la reivindicación anterior del terminal, en el que solamente se determinan subgrupos aleatorios de Hosts en una tabla y se registra una base de datos con los usuarios en una memoria Cache; o se forma un número de primeros Hosts de entrada fiables, que registran las tablas en memoria Cache, y son recuperadas desde éstos, o se lleva a cabo una actualización de usuarios según prioridad, siendo la prioridad alta cuando se ha comunicado con éstos con frecuencia en el pasado.

13.- Terminal móvil de acuerdo con la reivindicación anterior del terminal, en el que la red de anonimato es la red Tor.

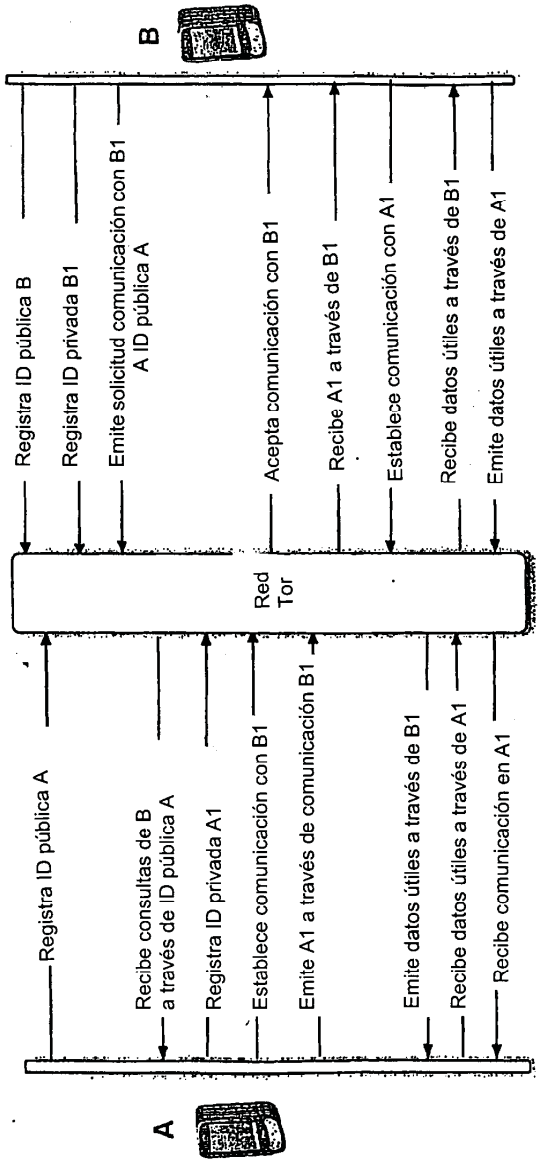
B
Registra ID pública B
Registra ID privada B1
Emite solicitud comunicación con B1 A ID pública A
Acepta comunicación con B1
Recibe A1 a través de B1
Establece comunicación con A1
Recibe datos útiles a través de B1
Emite datos útiles a través de A1
Red Tor
Registra ID pública A
Recibe consultas de B a través de ID pública A
Registra ID privada A1
Establece comunicación con B1
Emite A1 a través de comunicación B1
Emite datos útiles a través de B1
Recibe datos útiles a través de A1
Recibe comunicación en A1
A

Fig. 1