(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 391 480**

(51) Int. CI.:
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07786426 .2**
(96) Fecha de presentación: **30.07.2007**
(97) Número de publicación de la solicitud: **2047631**
(97) Fecha de publicación de la solicitud: **15.04.2009**

(54) Título: **Procedimiento para establecer una clave secreta entre dos nodos en una red de comunicación**

(30) Prioridad:
01.08.2006 DE 102006036165

(45) Fecha de publicación de la mención BOPI:
27.11.2012

(45) Fecha de la publicación del folleto de la patente:
27.11.2012

(73) Titular/es:
NEC CORPORATION (100.0%)
7-1, Shiba 5-chome Minato-ku
Tokyo 108-8001, JP

(72) Inventor/es:
GIRAO, JOAO;
ARMKNECHT, FREDERIK;
MATOS, ALFREDO y
AGUIAR, RUI LUIS

(74) Agente/Representante:
ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Procedimiento para establecer una clave secreta entre dos nodos en una red de comunicación.

La presente invención se refiere a un procedimiento para establecer una clave secreta entre dos nodos en una red de comunicación, en particular en una red de área local inalámbrica (WLAN).

Con el fin de establecer una clave secreta entre dos nodos en una red de comunicación normalmente se usan protocolos de intercambio de claves. Los protocolos de intercambio de claves conocidos son, por ejemplo, el algoritmo de Diffie-Hellman, en particular Diffie-Hellman en curvas elípticas, o procedimientos basados en RSA. La seguridad de los procedimientos conocidos se basa en la aplicación de las llamadas funciones de un solo sentido. En este sentido, el algoritmo de Diffie-Hellman usa el hecho de que la operación de elevar a una potencia es una operación de computación muy simple, pero que en contraste la computación del logaritmo discreto de un número sólo es posible con un esfuerzo extremadamente elevado.

Tras haber realizado los procedimientos conocidos, las partes A y B involucradas en el algoritmo disponen de una clave secreta K que sólo ellas conocerán. Pero en el caso de los procedimientos conocidos el propio intercambio de claves no se mantiene en secreto lo cual puede resultar ser desventajoso en ciertos entornos. La parte iniciadora, por ejemplo, cuando se realiza el intercambio de claves de Diffie-Hellman primero tiene que transmitir dos valores por el medio inseguro. En la notación común éste es un número primo p, así como un generador g, en base a lo cual la clave compartida K_{DH} se puede computar entonces de acuerdo con $K_{DH} = (g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$. Las variables a y b denominan números al azar elegidos por las partes. Sólo debido al hecho de transmitir un mensaje con los valores g, p, así como generalmente también $A = g^a \bmod p$ por un medio inseguro, un atacante que intercepta este mensaje ya puede sacar ciertas conclusiones, por ejemplo, en el caso más simple, el hecho de que se está produciendo un acuerdo de clave y quién es la parte iniciadora.

El documento WO-00/25475-A da a conocer un procedimiento y un aparato para registrar una suscripción inalámbrica a un terminal inalámbrico, en el que un Número de Identificación Personal (PIN) corto se usa para transferir una suscripción para un servicio inalámbrico a un nuevo terminal inalámbrico, proporcionándose de ese modo una movilidad personal mejorada al suscriptor. Se hace que la transferencia sea segura por el intercambio de mensajes de intercambio de claves encriptadas de Diffie-Hellman.

El documento GB-2-390-270-A da a conocer un procedimiento para la intercepción legal de una sesión IP encriptada entre dos o más terminales, en el que la sesión usa el encriptado para asegurar el tráfico. La información requerida para reconstruir una clave de desencriptado sólo se deposita parcialmente con una autoridad.

El documento US-2003/068047-A1 da a conocer un procedimiento y aparato para una distribución broadcast de un solo sentido de claves para desencriptar contenido broadcast encriptado. Una lista de claves de actualización se genera en el sistema del proveedor de contenido en base a una tabla de claves secretas asociadas con una pluralidad de receptores de contenido.

Es un objeto de la presente invención mejorar y desarrollar aún más un procedimiento del tipo descrito inicialmente para establecer una clave secreta entre dos nodos en una red de comunicación de tal modo que se oculte el hecho de que se esté produciendo un intercambio de claves.

De acuerdo con la invención, el objeto antes mencionado se consigue mediante un procedimiento que comprende las características de la reivindicación 1. De acuerdo con esta reivindicación un procedimiento del tipo descrito inicialmente está caracterizado porque

uno de los nodos - primer nodo - emite uno o más paquetes que pueden ser recibidos por el otro nodo - segundo nodo -, en el que cada uno de los paquetes contiene una primera clave y en el que cada uno de los paquetes se encripta con una segunda clave antes de ser enviado,

el segundo nodo elige al azar un paquete de los paquetes recibidos y descifra el encriptado del paquete elegido con el fin de obtener la primera clave, y

el segundo nodo inicia un protocolo de intercambio de claves, en el que el segundo nodo encripta el mensaje que se va a enviar para iniciar el protocolo de intercambio de claves con la clave revelada.

De acuerdo con la invención, se ha reconocido en primer lugar que una ocultación del intercambio de claves se puede conseguir en general realizando un protocolo en el que se combinen entre sí elementos criptográficos (encriptado de datos) y elementos esteganográficos (que hacen los datos invisibles). El elemento esteganográfico consiste concretamente en el hecho de que uno de los nodos emite un paquete o una multitud de paquetes, en el que cada uno de los paquetes contiene una primera clave y en el que cada uno de los paquetes se encripta con una segunda clave antes de ser emitido. Los paquetes pueden ser recibidos por un segundo nodo que elige al azar un paquete de los paquetes recibidos. Al ejecutar un ataque de fuerza bruta, el segundo nodo descifra el encriptado del paquete elegido y obtiene de esa manera la primera clave que se ha transportado con el paquete. En una etapa siguiente la clave revelada es usada por el segundo nodo para iniciar un protocolo de intercambio de claves. En concreto, el segundo nodo encripta el mensaje, el cual se debe enviar con el fin de iniciar el protocolo de intercambio de claves, con la clave revelada.

En el caso del procedimiento de acuerdo con la invención sólo se emiten mensajes encriptados por un medio público, por ejemplo un enlace broadcast público, por lo que un atacante no tiene ninguna posibilidad de averiguar que los mensajes son parte de un protocolo de intercambio de claves o sirven para iniciar un protocolo de intercambio de claves. Incluso si el atacante es capaz de desencriptar un paquete, se considera que la propia información obtenida de ese modo, es decir sin ella el atacante tiene que invertir mayores esfuerzos (considerables), no tiene valor, puesto que el atacante no sabe qué paquete elegirá al azar el otro nodo de la multitud de paquetes.

Con el fin de aumentar aún más la seguridad, se puede estipular que el elemento esteganográfico sea reforzado insertando un tiempo de espera de duración pre-definible entre el envío del (los) paquete(s) que contiene(n) las primeras claves por el primer nodo, y el descifrado del encriptado o la iniciación del intercambio de claves por el segundo nodo. Durante este tiempo, el resto de los nodos de la red intercambian mensajes encriptados en el contexto de su comunicación normal y hacen que sea incluso más difícil para un atacante averiguar algo acerca de un intercambio de claves que se esté produciendo.

En el contexto de una forma de realización ventajosa se estipula que el primer nodo almacene una lista con las primeras claves enviadas. Cuando el primer nodo recibe el mensaje que inicia el protocolo de intercambio de claves enviado por el segundo nodo, el primer nodo puede revisar la lista intentando desencriptar el mensaje recibido con una de las claves almacenadas. Cuando el primer nodo ha averiguado la clave con la que fue encriptado el mensaje que inicia el protocolo de intercambio de claves, se puede estipular en una etapa siguiente que el primer nodo emplee la clave encontrada para encriptar su mensaje del protocolo de intercambio de claves desde su lado. En una forma de realización alternativa, se puede estipular adjuntar un identificador al mensaje que pueda ser recuperado por la otra parte pero no por un atacante. Para este propósito, por ejemplo, se podría emplear un número al azar que identificara la clave usada respectiva.

Las segundas claves con las que el primer nodo ha encriptado los paquetes enviados están diseñadas de un modo ventajoso como encriptados que son fáciles de descifrar. El hecho de que un atacante pueda descifrar fácilmente un encriptado ligero cuando los paquetes son transmitidos por un canal público no es relevante en el sentido de que no obtiene ninguna información a pesar del desencriptado, puesto que no sabe qué paquete elegirá el segundo nodo de la multitud de los paquetes enviados.

Con respecto a una aplicación flexible del procedimiento, se puede estipular que la longitud de las claves con las que el primer nodo encripta los paquetes se defina de acuerdo con los requisitos de seguridad respectivos. En un ejemplo concreto, se podría elegir un encriptado RC5, en el que se asume que un encriptado RC5 con una longitud de clave entre 16 y 64 bits es apropiado en una multitud de posibles aplicaciones.

Con respecto a una simplificación, se puede estipular que la primera clave K_i que se transporte en cada caso con un paquete, y la segunda clave k_i usada para encriptar el paquete correspondiente se elijan para ser idénticas.

En el contexto de un escenario de aplicación concreto uno de los nodos puede, por ejemplo, ser un punto de acceso de una red. El otro nodo puede ser un nodo asociado con o un nodo que se asocia con el punto de acceso, en el que el procedimiento descrito puede ejecutarse entre el punto de acceso y el nodo en el contexto del registro del nodo en el punto de acceso.

Con respecto a un aumento adicional de la seguridad, se puede estipular que los paquetes sean emitidos periódicamente. Esto de nuevo refuerza el elemento esteganográfico, puesto que el procedimiento se lleva a cabo independientemente del hecho de si un nodo nuevo se registra en la red. Es por tanto imposible para un atacante averiguar cuándo comienza un intercambio de claves, puesto que el proceso de enviar paquetes se desvincula

completamente de cualquier procedimiento de asociación de nodos en la red. Con el fin de evitar un tráfico de datos innecesario, en particular cuando se aplica a una WLAN, se puede estipular que los paquetes que vayan a ser enviados por el primer nodo sean balizas que se envíen de todos modos a intervalos de tiempo regulares de habitualmente 100 milisegundos. En otras palabras, la primera clave K_i que vaya a ser transportada por el paquete está integrada en un campo de la baliza no utilizado.

De forma alternativa, es posible anexar las primeras claves K_i a todos los paquetes que se envíen dentro de la red.

También en el contexto de un escenario de aplicación concreto se puede estipular que el intercambio de claves iniciado sea un intercambio de claves de Diffie-Hellman. Otros procedimientos, como por ejemplo RSA, también se pueden prever.

Hay diversos modos de cómo diseñar y desarrollar aún más la enseñanza de la presente invención de un modo ventajoso. Con este fin, se debe aludir a las reivindicaciones de patente subordinadas a la reivindicación de patente 1 por un lado y a la siguiente explicación de formas de realización preferidas de la invención a modo de ejemplo, ilustrada mediante la figura por otro lado. En conexión con la explicación de la forma de realización preferida de la invención mediante la ayuda de la figura, se explicarán en líneas generales formas de realización preferidas y desarrollos adicionales de la enseñanza. En el dibujo,

la única figura muestra esquemáticamente un ejemplo de una forma de realización del procedimiento de acuerdo con la invención para establecer una clave secreta entre un punto de acceso y un nodo asociado.

La única figura muestra - esquemáticamente - un ejemplo de una forma de realización de un procedimiento de acuerdo con la invención en base a un punto de acceso AP de una red local inalámbrica y un nodo asociado A.

En una primera etapa el punto de acceso AP genera una multitud de paquetes P_i. Cada uno de los paquetes P_i contiene una primera clave K_i. El punto de acceso AP encripta cada uno de los paquetes Pi con una segunda clave k_i y envía los paquetes P_i encriptados de ese modo por el enlace inalámbrico, de modo que los paquetes P_i puedan ser recibidos por el nodo A. En la forma de realización mostrada en concreto los paquetes P_i se encriptan con el cifrado por bloques RC5.

En una etapa siguiente el nodo A elige de la multitud de paquetes P_i recibidos un paquete P_m al azar. Al ejecutar un ataque de fuerza bruta el nodo A descifra el encriptado del paquete P_m elegido para obtener de ese modo la clave K_m. El ataque de fuerza bruta se puede realizar con esfuerzos razonables puesto que los paquetes P_i han sido encriptados por el punto de acceso AP con un encriptado relativamente débil.

En una tercera etapa el nodo A usa la clave K_m encontrada para iniciar un protocolo de intercambio de claves con el punto de acceso AP. En la forma de realización representada, el protocolo de intercambio de claves sigue el algoritmo de Diffie-Hellman conocido. Específicamente, el nodo A genera de un modo conocido por sí mismo el número primo p, así como un generador g con $2 \leq g \leq p - 2$. El nodo A envía un mensaje que contiene los valores g, p y A, en el que el valor A se computará como sigue: $A = g^a \bmod p$. a es un número al azar elegido por el nodo A que no se hace público. El mensaje con los valores g, p, A se transmite de una manera encriptada, en el que el nodo A emplea la clave K_m encontrada para encriptar el mensaje.

El punto de acceso AP desencripta el mensaje recibido por el nodo A, en el que en la forma de realización mostrada, el punto de acceso AP ha almacenado una tabla que contiene todas las primeras claves K_i enviadas con los paquetes P_i. El punto de acceso AP accede a la tabla y prueba una clave tras otra hasta que llega a la clave K_m con la que el desencriptado tiene éxito. Acto seguido el punto de acceso AP en su parte genera un número al azar b y computa $B = g^b \bmod p$ y envía el valor B encriptado con la clave K_m encontrada al nodo A.

Finalmente, se computa la nueva clave K_{DH}, en la parte del nodo A de acuerdo con $B^a \bmod p$ y en la parte del punto de acceso AP de acuerdo con $A^b \bmod p$, en el que la nueva clave K_{DH} sirve entonces para encriptar el futuro intercambio de datos entre el nodo A y el punto de acceso AP.

Muchas modificaciones y otras formas de realización de la invención expuestas en este documento le vendrán a la mente al experto en la materia a la cual pertenece la invención teniendo el beneficio de las enseñanzas presentadas en la descripción precedente y los dibujos asociados. Por lo tanto, se debe entender que la invención no se debe limitar a las formas de realización específicas dadas a conocer y que las modificaciones y otras formas de realización están destinadas a incluirse dentro del ámbito de las reivindicaciones anexas. Aunque se emplean

términos específicos en este documento, se usan sólo en un sentido genérico y descriptivo y no a efectos de limitación.

REIVINDICACIONES

1. Procedimiento para establecer una clave secreta entre dos nodos en una red de comunicación,

en el que

uno de los nodos - primer nodo - emite uno o más paquetes que pueden ser recibidos por el otro nodo - segundo nodo -, en el que

el segundo nodo inicia un protocolo de intercambio de claves, en el que el segundo nodo encripta un mensaje que se va a enviar para iniciar el protocolo de intercambio de claves con una clave obtenida (K_m)

caracterizado porque

cada paquete contiene una primera clave respectiva y se encripta con una segunda clave respectiva antes de ser enviado, y porque

el segundo nodo elige al azar un paquete de los paquetes recibidos y descifra el encriptado del paquete elegido con el fin de obtener, como la clave obtenida, la primera clave respectiva del paquete elegido.

2. Procedimiento de acuerdo con la reivindicación 1, caracterizado porque entre el envío de los paquetes P_i por el primer nodo y el descifrado del encriptado o la iniciación del intercambio de claves por el segundo nodo se permite una duración pre-configurable.

3. Procedimiento de acuerdo con la reivindicación 1 ó 2, caracterizado porque el primer nodo almacena una lista de las claves enviadas (K_i).

4. Procedimiento de acuerdo con la reivindicación 3, caracterizado porque el primer nodo prueba las claves (K_i) almacenadas con el fin de desencriptar el mensaje del segundo nodo que inicia el protocolo de intercambio de claves.

5. Procedimiento de acuerdo con la reivindicación 4, caracterizado porque el primer nodo encripta un segundo mensaje del protocolo de intercambio de claves con la clave (K_m) encontrada.

6. Procedimiento de acuerdo con las reivindicaciones 1 a 5, caracterizado porque el encriptado de los paquetes P_i con las segundas claves (k_i) es un encriptado que se puede descifrar fácilmente.

7. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 6, caracterizado porque la longitud de las segundas claves (k_i) se determina de acuerdo con requisitos de seguridad respectivos.

8. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 7, caracterizado porque se emplea un encriptado RC5 para encriptar los paquetes P_i.

9. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 8, caracterizado porque la primera clave (K_i) transportada con el paquete P_i y la segunda clave (k_i) usada para encriptar el paquete P_i se eligen para ser idénticas.

10. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 9, caracterizado porque uno de los nodos es un punto de acceso (AP) de una red, y porque el otro de los nodos es un nodo (A) asociado con dicho punto de acceso (AP).

11. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 10, caracterizado porque los paquetes P_i son enviados periódicamente.

12. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 11, caracterizado porque los paquetes P_i son balizas.

13. Procedimiento de acuerdo con una cualquiera de las reivindicaciones 1 a 12, caracterizado porque el protocolo de intercambio de claves iniciado es un intercambio de claves de Diffie-Hellman.

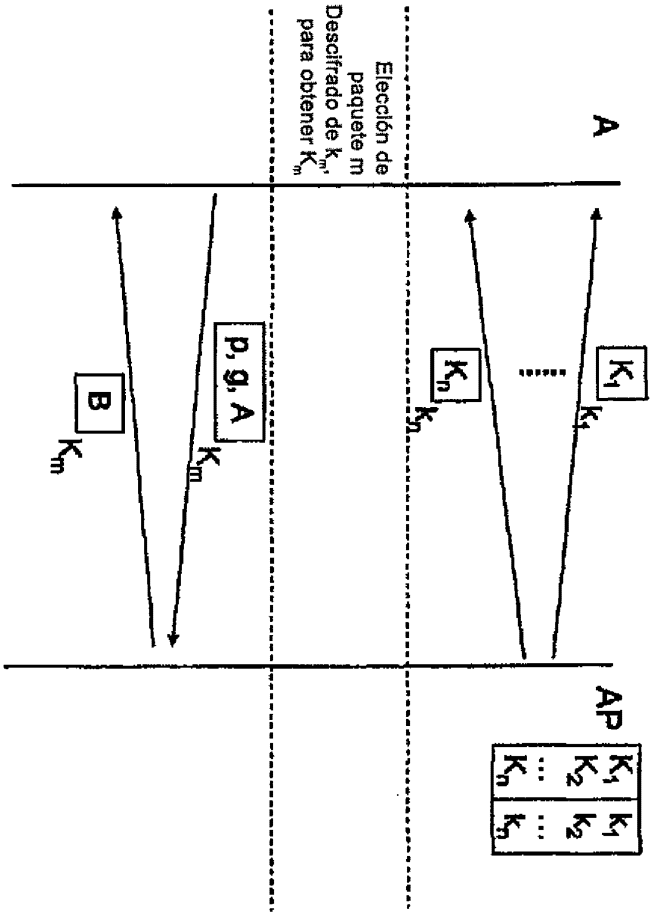
A
AP
Elección de paquete m
Descifrado de k_m, para obtener K_m
K_1
K_n
k_1
k_n
p, g, A
B
K_m
K_1 K_2 ... K_n
k_1 k_2 ... k_n

Fig.