(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 387 626**

(51) Int. CI.:
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07788300 .7**
(96) Fecha de presentación: **07.08.2007**
(97) Número de publicación de la solicitud: **2057778**
(97) Fecha de publicación de la solicitud: **13.05.2009**

(54) Título: **Procedimiento de autentificación**

(30) Prioridad:
22.08.2006 DE 10603932

(45) Fecha de publicación de la mención BOPI:
27.09.2012

(45) Fecha de la publicación del folleto de la patente:
27.09.2012

(73) Titular/es:
NOKIA SIEMENS NETWORKS GMBH & CO. KG
ST. MARTIN STRASSE 76
81541 MÜNCHEN, DE

(72) Inventor/es:
HÖHNE, Matthias

(74) Agente/Representante:
Zuazo Araluze, Alexander

DESCRIPCIÓN

Procedimiento de autentificación.

Problema básico de la invención

Un cliente ha de autentificarse ante un servidor, sin transmitir su palabra de paso en texto en claro. Incluso una palabra de paso codificada siempre con la misma clave puede ser capturada y utilizada por personas no autorizadas.

Solución dada hasta ahora al problema

Con el método tradicional solicita el cliente y se envía un texto de reto (signed challenge, reto firmado) codificado, aleatorio y firmado por el servidor. El cliente decodifica el mismo, forma un digest (compendio) y firma y codifica a su vez el mismo (signed digest). El servidor comprueba la coincidencia de los digests. Este procedimiento es muy costoso.

Otra posible solución al problema

Se podría intercambiar, similarmente a una lista TAN (One Time Pad, lista de un solo uso), antes de la primera autentificación por otras vías (por ejemplo papel) una lista (finita) con claves (keys), que en cada caso sólo deberían utilizarse una vez. Esta lista debería desde luego memorizarse o copiarse las claves por parte del usuario (susceptible de ataque o bien complejo y vulnerable a las faltas).

Solución del problema según la invención

A continuación se describirá la invención más en detalle con la ayuda del dibujo, que incluye una figura.

Ambas partes (cliente y servidor) acuerdan al comienzo (como parte de un seed o germen) el mismo valor inicial y el mismo algoritmo para generar claves (keys).

Mediante ello están en condiciones el cliente y el servidor de generar independientemente uno de otro la misma secuencia de claves. Una secuencia que puede generarse de esta manera se denomina también PRBS (Pseudo Random Binary Sequence, secuencia binaria pseudoaleatoria). La generación de una PRBS puede realizarse con ayuda de un LFSR (Linear Feedback Shift Register, registro de desplazamiento con retroalimentación lineal).

Los PRBS son desde luego fuertemente deterministas. Por ello puede averiguarse tras unos pocos resultados (keys) el procedimiento y un atacante conoce entonces todas las demás claves. Además, tiene lugar tras número finito de claves una repetición exacta de la secuencia de claves (periodo del LFSR).

Desde luego si se introducen a intervalos regulares interferencias en la secuencia (es decir, en la formación de las claves con ayuda del LFSR), entonces el resultado no es periódico ni determinista.

Las interferencias en la secuencia se logran como sigue (ver al respecto también la figura).

Primeramente forman el cliente y el servidor a partir del valor inicial (Start-Key) con ayuda del LFSR una primera clave, que a continuación se denomina clave épsilon ε, para una mejor diferenciación. La clave épsilon no se utiliza para la autentificación, ya que es susceptible de ataque.

Como siguiente paso, genera sólo el cliente una segunda clave, que el mismo envía al servidor. Sólo esta segunda clave se utiliza para la autentificación. Para entender la segunda clave, que es diferente de la formación con ayuda del LFSR, se realiza un pequeño excurso a la métrica.

Excurso

Métrica significa la forma como está definida la distancia (delta) entre dos puntos. Aplicada a números, que son memorizados por el ordenador en bits, esto significa en el caso más sencillo la diferencia entre dos números. La diferencia entre dos números binarios depende de la ponderación de los bits individuales de los números. Normalmente la ponderación de los bits viene fijada (métrica antigua) por su secuencia de transmisión de 0 (2^0) a 31 (2^{31}):

métrica antigua: 31……..6543210

```
  2503657302 ( 10010101001110101100011101010110 )
+  536936480 ( 00100000000000010000000000100000 )
= 3040593782 ( 10110101001110111100011101110110 )
```

nueva métrica: 1 0 2

La distancia entre los números 3040593782 y 2503657302 tiene según la métrica antigua el valor 536936480. Si ahora se define una nueva métrica otorgando o acordando nuevas ponderaciones para distintos bits, entonces tienen los números citados otra distancia. Si se otorga por ejemplo al bit 16 la nueva ponderación de bit 0 (2^0), al bit 29 la nueva ponderación de bit 1 (2^1) y al bit 5 la nueva ponderación de bit 2 (2^2), entonces tienen ambos números antes representados sólo una distancia de 7. La secuencia de los otros bits carece para ello de importancia, pero no el estado (0 ó 1) de los bits. Cuando se considera un delta de hasta 7, se encuentra según la nueva métrica el número 3040593782 en el delta de 2503657302 y el número 2503657303 está por el contrario alejado en más de 7 del 2503657302, ya que se diferencia en un bit que tiene una ponderación mayor que 2.

En la invención se realiza (como parte del seed) entre cliente y servidor un acuerdo sobre la nueva métrica tal que se acuerdan aquellos bits (los llamados bits de interferencia) que a diferencia de su secuencia de transmisión tienen otra ponderación.

Supongamos que sea el número 3040593782 la primera clave (clave épsilon) generada por cliente y servidor. Entonces forma como siguiente clave (segunda clave) el cliente una clave, cuya distancia (delta) según la nueva métrica se encuentra dentro de un valor predeterminado respecto a la clave épsilon. Esta clave se denominará en lo que sigue clave delta ð. Si genera por lo tanto el cliente como siguiente clave el número 478651654, entonces se trata de una clave delta, ya que este número se encuentra en el delta de la clave épsilon 3040593782.

Puesto que sólo el cliente y el servidor conocen la nueva métrica modificada según la posición de los bits de interferencia, puede así el servidor autentificar al cliente en base a la segunda clave recibida. Si la segunda clave enviada por el cliente se encuentra dentro del delta, entonces está autentificado el cliente. Por ambos lados se utiliza esta clave como nuevo seed (germen) y un nuevo desplazamiento en el LFSR es la nueva primera clave (nueva clave épsilon).

En el ejemplo antes representado se muestran sólo 32 bits. En la realidad los números son bastante mayores, es decir, por ejemplo 2048 ó 4096 bits con 8 ó 16 bits de interferencia. También se pueden utilizar otras operaciones como la diferencia para averiguar la distancia.

Si es n la cantidad de bits de interferencia, entonces forman el delta todas las $2^n - 1$ claves del delta, es decir, el entorno del épsilon en la métrica conocida, que a su vez conocen ambas partes por la posición de los bits de interferencia y que no puede ser detectada por el atacante.

Ventajas de la nueva función: Debe intercambiarse al principio como parte de la seed por una vez una clave de arranque con el método tradicional. A continuación, en cada nueva solicitud debe enviarse sólo una clave procedente del nuevo delta.

REIVINDICACIONES

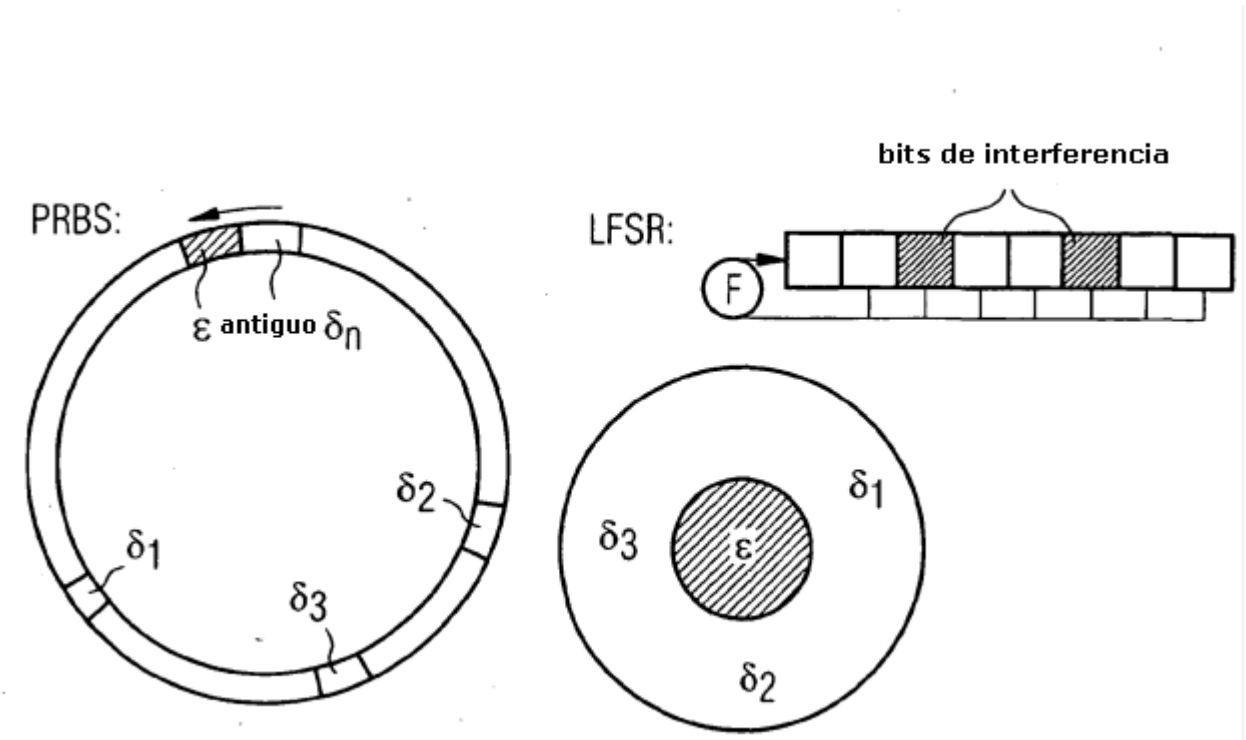
1. Procedimiento para la autentificación de un cliente respecto a un servidor, según el cual

   a) el cliente y el servidor generan según un algoritmo idéntico e independientemente entre sí una primera clave (clave épsilon), habiéndose fijado el citado algoritmo y el valor inicial del algoritmo previamente en un acuerdo secreto entre el cliente y el servidor,
   b) el cliente genera una segunda clave tal que su distancia (delta) a la primera clave se encuentra dentro de una distancia predeterminada, habiéndose fijado la distancia predeterminada y la métrica de la clave previamente en un acuerdo secreto entre cliente y servidor,
   c) la citada segunda clave se envía al servidor,
   d) el servidor autentifica con éxito al cliente cuando la distancia de la segunda clave recibida respecto a la primera clave se encuentra dentro de un delta predeterminado,
   e) la citada segunda clave se utiliza como nuevo valor inicial para la siguiente autentificación del cliente respecto al servidor, cuando el cliente ha sido autentificado con éxito por el servidor.

2. Procedimiento según la reivindicación 1,
   caracterizado porque como clave se utilizan números binarios.

3. Procedimiento según la reivindicación 2,
   caracterizado porque como distancia (delta) entre dos claves se utiliza la diferencia entre dos números binarios.

4. Procedimiento según una de las reivindicaciones 1 a 3,
   caracterizado porque el citado algoritmo se realiza con un LFSR.


PRBS:
ε antiguo δn
δ1
δ2
δ3
LFSR:
bits de interferencia
F
δ1
δ3
ε
δ2