(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 560 214**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **10.02.2011 E 11001061 (8)**

(97) Fecha y número de publicación de la concesión europea: **21.10.2015 EP 2487857**

(54) Título: **Procedimiento para ofrecer un acceso seguro a Internet**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2016

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

BENNER, ALEXANDER

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Procedimiento para ofrecer un acceso seguro a Internet

La solicitud concierne a un procedimiento para ofrecer un acceso seguro a Internet a través de un portal de red, especialmente a través de un portal de Internet, que comprende los pasos de actuación siguientes:

- habilitación de una interfaz para registrarse en el portal de red a través de un terminal,

- comprobación de la autorización de un usuario que accede al portal de red a través del terminal, y

- habilitación de un entorno de tiempo de ejecución para un usuario reconocido como autorizado.

Asimismo, la invención concierne a un portal de red para habilitar un acceso seguro a Internet.

La utilización de Internet se ha convertido hoy en día en algo francamente natural. Cada vez más terminales disponen de una conectividad de red que posibilita un acceso a informaciones facilitadas en Internet. Debido al sencillo acceso y a la continua disponibilidad es ya hoy en día algo natural que el usuario de Internet reclame funciones y servicios allí ofrecidos. Esto afecta en medida creciente también a procesos relevantes para la seguridad, tal como, por ejemplo, la banca en línea.

A pesar de la difundida utilización de cortafuegos y escáneres de virus se producen aquí cada vez con mayor frecuencia intentos de fraude que se desarrollan con éxito. Por este motivo, al usuario de funciones relevantes para la seguridad en Internet le queda cada vez con más frecuencia una incómoda sensación de si todo ha transcurrido también correctamente.

Además, la tendencia se orienta cada vez más a desplazar funciones enteras de software a Internet. Conceptos como computación en la nube y software como servicio marcan cada vez más nuestra vida cotidiana. Cuanto mayor número de estas funciones se almacenen en Internet, tanto mayor será la necesidad de mecanismos de seguridad actuales que protejan fiablemente al usuario. Una posibilidad de protección es la habilitación de las funciones se software en la red dentro de un entorno de tiempo de ejecución. Este entorno de tiempo de ejecución es en principio una máquina virtual a la que solamente tiene acceso el usuario autorizado.

El documento US 2007/180449 A1 muestra un portal de red que, después de una comprobación de autorización positiva, facilita a un usuario acceso a una máquina virtual a través de la cual puede acceder a Internet.

El problema de la invención consiste, pues, en proponer un procedimiento para ofrecer un acceso seguro a Internet que le facilite al usuario el acceso a Internet con un alto nivel de seguridad. Asimismo, es problema de la invención proponer un portal de red de esta misma clase para habilitar un acceso seguro a la red.

Estos problemas se resuelven con un procedimiento según la reivindicación 1 y un portal de red según la reivindicación 9, respectivamente. En las reivindicaciones subordinadas se citan formas de realización especialmente ventajosas. Una idea básica esencial de la invención es la de asociar al entorno de tiempo de ejecución una interfaz a través de la cual el usuario autorizado obtenga, especialmente de forma anónima, acceso a un información recuperable en Internet. Se le proporciona de esta manera al usuario un entorno seguro apantallado hacia el exterior, desde el cual se puede acceder sin gran riesgo a Internet. En este caso, el entorno de tiempo de ejecución proporcionado al usuario autorizado puede facilitarse en una red local. Es especialmente ventajosa la de su disposición en la propia Internet, ya que así se pueden facilitar centralmente todas las funciones.

El usuario del procedimiento según la invención necesita únicamente un terminal cualquiera con capacidad de red para acceder a la interfaz a fin de registrarse en el portal de red. Después de una comprobación positiva de la autorización del usuario se le proporciona por el portal de red el entorno de tiempo de ejecución. El entorno de tiempo de ejecución habilita para el usuario, por así decirlo, un ordenador virtual en el que se ejecutan aplicaciones a las que puede acceder el usuario. El entorno de tiempo de ejecución funciona en este caso como una especie caja de arena (sandbox) para aislamiento de procesos. Éste apantalla al usuario hacia fuera. Un enlace único del entorno de tiempo de ejecución con Internet es una interfaz a través de la cual ésta le brinda al usuario autorizado acceso a una información recuperable en Internet. Los contenidos de información allí demandados se indican entonces a través de un programa que se ejecuta en el entorno de tiempo de ejecución. Por tanto, el usuario no accede directamente a Internet, sino que se inscribe en su portal de red, y, después de una autentificación satisfactoria, el usuario puede acceder a Internet a través de la caja de arena proporcionada. Mientras tanto, el software que se ejecuta en la caja de arena puede ser examinado sin un gran coste en cuanto a un desarrollo siempre ordenado de las funciones del programa.

El portal de red según la invención presenta un módulo de registro y un módulo de validación, presentando el módulo de registro una interfaz a través de la cual un usuario se registra como usuario autorizado del portal de red, proporcionando el módulo de virtualización un entorno de tiempo de ejecución para el acceso a Internet, y cooperando el módulo de registro y el módulo de validación de tal manera que un usuario reconocido como

autorizado por el módulo de registro gana acceso, a través del módulo de virtualización, a una información recuperable en la red. Por tanto, el módulo de red es de construcción modular, con lo que se pueden complementar o variar de manera sencilla algunas funciones individuales del portal.

En una forma de realización especialmente preferida el portal de Internet le proporciona al usuario autorizado un cliente o servicio de anonimización con el cual puede navegar "anónimamente" en Internet. Tales criterios técnicos, como, por ejemplo, el proyecto TOR, o las cascadas de mezcla están ya ampliamente difundidos en la actualidad y pueden integrarse de manera sencilla en el procedimiento o en el portal de red.

Preferiblemente, se evalúan las informaciones recuperables en la red, de modo que, al ganar acceso a una información contenida en Internet, se le transmita al usuario autorizado el resultado de la evaluación. La clasificación de los contenidos realizada especialmente de forma dinámica y, por tanto, siempre actualizada se puede convertir de manera sencilla en una señal que se le ofrece al usuario al recuperar la información. Tales señales se utilizan ya hoy en día con mucha frecuencia, por ejemplo como signos de cifrado en la barra del navegador. Se le indica así inmediatamente al usuario si la información recuperada por él es segura o si tiene que usar una precaución especial. En este caso, la evaluación puede ser realizada en principio también por el propio operador del portal de red. Debido a la abundancia de portales de Internet a evaluar dicho operador se sirve preferiblemente, al menos en áreas parciales, de prestadores de servicio externos especializados en ello.

Según la demanda de seguridad del usuario, se pueden instalar también barreras directas de acceso o de descarga en lugar o como complemento de un aviso, cuyas intervenciones se le señalizan entonces al usuario. Ventajosamente, el usuario puede establecer o complementar él mismo tales barreras de acceso o de descarga, de modo que puede configurar personalmente el alcance de su acceso a Internet.

En una forma de realización especialmente preferida se comprueba para la evaluación la validez de certificados que se han expedido para la información recuperable en la red. Esta función es ventajosa especialmente en operaciones bancarias en línea. Se facilita el portal de red a una plataforma de confianza que comprueba los certificados de los bancos en línea y se le pone a disposición del usuario del portal. El usuario puede estar así siempre seguro de que se comunica con un banco en línea real. El portal de red impide así fiablemente todos los intentos de robo de datos personales (phishing).

Ventajosamente, el enlace de red seguro entre el usuario autorizado y la información recuperable en Internet se establece con un certificado válido sobre el entorno de tiempo de ejecución. La caja de arena es entonces el intermediario (man-in-the-middle) a través del cual se establece un enlace seguro entre el terminal del usuario y la caja de arena, así como un enlace seguro entre la caja de arena y la información recuperable en Internet, como, por ejemplo, con el portal de un banco en línea. En este caso, es ventajoso hacer que la seguridad del propio portal de red sea comprobada por una parte independiente a fin de aumentar aún más el merecimiento de confianza para el cliente. La aceptación del intermediario comprobado puede aumentarse aún más mediante una especie de seguro que ofrece una compensación para casos en los que unos terceros no autorizados ganen acceso a datos de acceso o de transacción.

Cuando se reconoce como válido el certificado para el portal de banca en línea elegido, se puede establecer también un enlace directo entre el portal del banco y el terminal, a la vez que se evita el entorno de tiempo de ejecución. En una forma de realización especialmente preferida se combinan las clasificaciones en una lista negra y/o una lista blanca. Por ejemplo, los certificados de bancos en línea comprobados como positivos se depositan en una lista blanca. Los usuarios no sólo pueden ver esta lista, sino que se pueden insertar variaciones en esta lista cuando otros bancos en línea soliciten su acogida en la lista blanca. En el caso contrario, es decir, cuando, por ejemplo, se ha falseado un certificado para un banco en línea registrado o bien el banco en línea no existe, se añade este certificado a la lista negra. La naturaleza correcta de las propuestas realizadas por los usuarios para complementar las listas se comprueba de manera ventajosa antes de la inscripción de las mismas.

Preferiblemente, la ejecución del software en el portal de red se efectúa dentro de diferentes planos. Cada uno de estos planos presenta entonces un nivel de seguridad diferente de modo que, según sea necesario, se puede elevar o rebajar por elección del plano el nivel de seguridad. Este nivel de seguridad puede estar preajustado para aplicaciones diferentes, pero también puede dejarse al arbitrio del usuario. Una seguridad adicional la ofrece la habilitación de diversos escáneres de virus y otro software de seguridad que analicen la inocuidad de las informaciones recuperadas en Internet.

En una forma de realización preferida la comprobación de la autorización de un usuario se efectúa por medio de la autentificación del terminal accedente, especialmente por medio de la comprobación de la dirección MAC del terminal accedente. Tales direcciones MAC pueden ser cuidadas y depositadas de manera sencilla en una lista blanca. Cuando el terminal es conocido según esta lista blanca, éste puede acceder sin más comprobación, casi automáticamente, al portal de red.

En el caso de una dirección MAC desconocida, la autentificación se efectúa preferiblemente por medio del ingreso de una palabra de paso. El envío de esta palabra de paso puede remitirse sin gran coste a una dirección de un

terminal depositado en el portal de red, pudiendo, por ejemplo, remitirse por SMS a un número de teléfono móvil depositado. A este fin, durante la primera utilización del portal de red se tiene que depositar únicamente la dirección del terminal. Preferiblemente, la autentificación se realiza por medio de una palabra de paso de un solo uso (OTP), con lo que el usuario tiene que proveer una nueva palabra de paso propia después de su registro.

En una forma de realización especialmente preferida de la invención se pueden integrar también en el portal de red servicios de proveedores en línea que ofrecen acceso a Internet, tal como, por ejemplo, t-online.de. Estos servicios pueden ser después recuperados del portal de una manera absolutamente transparente para el usuario. Análogamente a los servicios normales de correo web, se pueden entonces también recibir y enviar aquí correos electrónicos. Para el ingreso de datos personales especialmente relevantes para la seguridad, tales, como, por ejemplo, los datos de acceso necesarios la inscripción en la cuenta de correo electrónico, se puede prever una zona especialmente securizada del portal de red, de modo que estos datos estén protegidos contra robo de la mejor manera posible.

Preferiblemente, se facilitan al portal de red funciones diferentes, especialmente servicios recuperables a través del portal de red, para la personalización de dicho portal de red. Caen entre éstos, por ejemplo, la selección de un navegador preferido para la navegación por Internet o el preajuste de determinadas herramientas, como, por ejemplo, el tiempo atmosférico, favoritos o registros de entrada. A través de la herramienta o la función "tiempo atmosférico" se puede indicar automáticamente, por ejemplo, el tiempo atmosférico actual y eventualmente una predicción para el lugar establecido por el usuario. En los favoritos están depositadas funciones recuperadas frecuentemente por el usuario. En la herramienta "registro de entrada" el usuario puede depositar datos de accesos con un bajo escalón de seguridad, por ejemplo para foros o grupos de noticias y también para aplicaciones de medios sociales.

El portal personalizado de esta manera asegura también que no se produzcan ataques de robo de datos personales, ya que se establece un enlace directo portal-banco en línea durante las operaciones bancarias en línea y se efectúa la autentificación del banco con ayuda del certificado, con lo que no es posible una operación de robo de datos personales. En otra forma de realización ventajosa el usuario recibe durante cada registro en el portal una información referente a cuándo él se había registrado por última vez (y eventualmente cuándo y en qué volumen) ha intentado sin éxito registrarse para el portal.

REIVINDICACIONES

1. Procedimiento para ofrecer un acceso seguro a Internet a través de un portal de red, especialmente un portal de Internet, que comprende los pasos de actuación siguientes:

habilitación de una interfaz para registrarse en el portal de red a través de un terminal,

comprobación de la autorización de un usuario que accede al portal de red a través del terminal, y

habilitación de un entorno de tiempo de ejecución para un usuario reconocido como autorizado,

asociándose al entorno de tiempo de ejecución una interfaz a través de la cual el usuario autorizado gana acceso a una información recuperable en Internet,

caracterizado por que

se evalúan las informaciones recuperables en Internet y por que, al producirse un acceso a una información en Internet, se ofrece al usuario autorizado una señal sobre la clasificación de la información recuperable en Internet.

2. Procedimiento según la reivindicación 1, **caracterizado** por que, para la evaluación, se comprueba la validez de certificados que se hayan expedido para las informaciones recuperables en la red.

3. Procedimiento según la reivindicación 2, **caracterizado** por que se establece a través del entorno de tiempo de ejecución un enlace de red seguro entre el usuario autorizado y las informaciones con certificado válido recuperables en la red.

4. Procedimiento según cualquiera de las reivindicaciones 1 a 3, **caracterizado** por que se combinan las clasificaciones en una lista negra y/o una lista blanca.

5. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que, al comprobar la autorización de un usuario, se efectúa una autentificación del terminal accedente, especialmente una comprobación de la dirección MAC del terminal accedente.

6. Procedimiento según la reivindicación 5, **caracterizado** por que, ante una información MAC desconocida, se efectúa la autentificación por medio del ingreso de una palabra de paso, especialmente el ingreso de una palabra de paso de un solo uso enviada a un terminal predeterminado.

7. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que se facilitan en el portal de red funciones diferentes, especialmente servicios recuperables a través del portal de red, para personalizar dicho portal de red.

8. Procedimiento según cualquiera de las reivindicaciones anteriores, **caracterizado** por que se facilita en el portal de red una función de anonimización por medio de la cual el usuario autorizado puede acceder anónimamente a la red.

9. Portal de red para realizar el procedimiento según cualquiera de las reivindicaciones 1 a 8, en el que el portal de red comprende un módulo de registro y un módulo de virtualización, en el que el módulo de registro presenta una interfaz a través de la cual el usuario se registra como usuario autorizado del portal de red, en el que el módulo de virtualización proporciona un entorno de tiempo de ejecución para el acceso a la red, y en el que el módulo de registro y el módulo de virtualización cooperan de tal manera que un usuario reconocido como autorizado por el módulo de registro gana acceso, a través del módulo de virtualización, a una información recuperable en Internet.