(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 378 298**

(51) Int. Cl.:
G06F 21/20 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04798821 .7**
(96) Fecha de presentación : **10.11.2004**
(97) Número de publicación de la solicitud: **1716468**
(97) Fecha de publicación de la solicitud: **02.11.2006**

(54) Título: **Sistema y método para impedir el robo de identidad mediante el uso de un dispositivo informático asegurado.**

(30) Prioridad: **13.11.2003 US 520022 P**
31.12.2003 US 750430

(45) Fecha de publicación de la mención BOPI:
10.04.2012

(45) Fecha de la publicación del folleto de la patente:
10.04.2012

(73) Titular/es: **GEMALTO S.A.**
6, rue de La Verrerie
92190 Meudon, FR

(72) Inventor/es: **Ali, Asad Mahboob y**
Lu, Hongqian Karen

(74) Agente/Representante:
Isern Cuyas, María Luisa

DESCRIPCIÓN

Sistema y método para impedir el robo de identidad mediante el uso de un dispositivo informático asegurado.

Esta invención se refiere en general al campo de las redes informáticas y en particular a un sistema y un método para impedir el robo de identidad durante la interacción a través de una red informática.

El comercio a través de redes informáticas se ha vuelto muy popular. Tal comercio adopta muchas formas, desde comprar libros y mercancías a vendedores en línea, por ejemplo libros a amazon.com y equipo de hockey a epuck.com, hasta realizar operaciones bancarias y de negociación de valores en línea. Lo común a todas estas transacciones es la necesidad de comunicar información privada segura. Normalmente, las transacciones se realizan a través de conexiones codificadas seguras. Sin embargo, aún existen para los taimados oportunidades de urdir planes para capturar información privada utilizada durante transacciones en línea, por ejemplo obtener contraseñas, números de identificación personal (PIN), números de la seguridad social, números de permiso de conducir y números de cuenta. La obtención ilegal de tal información y el uso fraudulento de la misma se denomina comúnmente "robo de identidad". Según la Comisión Federal de Comercio, sólo en el año 2002 hubo 9,9 millones de víctimas de robo de identidad. Los robos costaron a las empresas 47.600 millones de dólares y 5.000 millones en gastos varios para individuos en 2002 (Comisión Federal de Comercio, "Federal Trade Commission Identity Theft Survey Report", septiembre de 2003, http://www.ftc.gov/os/2003/09/synovatereport.pdf).

El documento EP 1 152 318 A1 da a conocer un sistema que comprende un servidor conectado a una red, un ordenador conectado a una red informática y un dispositivo informático seguro portátil.

En la presente memoria se utilizarán a modo de ejemplo transacciones a través de Internet. Aunque Internet es con mucho la red informática más grande y generalizada, los problemas y soluciones aquí tratados pueden también darse en y aplicarse a otras redes. Por ejemplo, el robo de identidad puede producirse enteramente dentro de los límites de una red corporativa o de una red universitaria, en las que un individuo deshonesto utilice una transacción a través del sistema para robar números PIN que le den acceso a registros de empleados o estudiantes. Aunque resulta conveniente tratar el problema del robo de identidad en el contexto de Internet, esto no debería interpretarse como limitativo del alcance de la invención.

Una forma de realizar el robo de identidad en línea es utilizar registradores de pulsaciones para registrar pulsaciones individuales y extraer información, como una contraseña y un número de tarjeta de crédito, de los registros. Dos casos conocidos son el caso Kinko en Nueva York y el caso Boston College (Jesdanun, A., "Thief captures every keystroke to access accounts", Seattle Post, julio, 2003, http://seattlepi.nwsource.com/national/131961 snoop23.html; Poulsen, K., "Guilty Plea in Kinko's Keystroke Caper", SecurityFocus, 18 de julio de 2003 http://www.securityfocus.com/printable/news/6447). En ambos casos, los ladrones instalaron software registrador de pulsaciones en ordenadores públicos conectados a Internet, en tiendas Kinko o en el campus. Capturaron identificaciones, nombres de usuario y contraseñas, utilizándolos para acceder a o incluso abrir cuentas bancarias en línea, efectuar compras y entrar ilegalmente en edificios.

El registrador de pulsaciones es bien software que se instala en un ordenador o bien un elemento de hardware que se conecta entre el cable del teclado y el ordenador, o un hardware incorporado al teclado. Los ladrones de identidades en línea utilizan normalmente registradores de pulsaciones por software porque resultan invisibles para el usuario.

En una transacción en línea típica, en la que se cree una nueva cuenta o se acceda a una cuenta ya existente, un usuario realiza la transacción en línea por medio de una interfaz gráfica de usuario en la pantalla del ordenador y utilizando un teclado para introducir la información solicitada por la interfaz de usuario. Esta interfaz gráfica de usuario representa típicamente una aplicación cliente de Internet de un banco o un comerciante al por menor en línea. El usuario introduce información personal confidencial, como un nombre, una contraseña, un número de la seguridad social, un número de tarjeta de crédito, etc., escribiéndola con el teclado. Esta información confidencial fluye en forma de texto claro del teclado al ordenador. La aplicación cliente de Internet puede utilizar el ordenador o la tarjeta inteligente conectada al ordenador para codificar la información antes de enviarla al servidor remoto. Pero el registrador de pulsaciones o capturador de pantalla podría capturar la información personal confidencial antes de que ésta sea codificada. Muchos de los actuales mecanismos de seguridad suponen que el ordenador y su teclado u otros dispositivos de entrada son seguros, lo que podría no ser verdad.

La figura 1 ilustra el problema de robo de identidad al que se puede llegar utilizando un registrador de teclado o un programa o hardware similar. La figura 1(a) es un esquema de la información normal de un teclado 101. La información puede visualizarse en una pantalla 103 conectada a un ordenador 105 utilizado por un cliente de un servicio en línea, por ejemplo un sitio de comercio bancario electrónico. Un procesador criptográfico 107, que se halla bien en el ordenador 105 o bien en una tarjeta inteligente (no mostrada), puede también codificar la información antes de que sea enviada a Internet 110. Este procesador criptográfico 107 puede ser un dispositivo de hardware o bien estar enteramente implementado en un software que se ejecute en el ordenador 105. La figura 1(b) ilustra el flujo de información cuando está instalado en el ordenador 105 un software registrador de pulsaciones 109. El registrador de pulsaciones 109 captura la información tecleada por el usuario en el teclado 101 antes de que la información vaya a ningún otro sitio y, por lo tanto, antes de que se aplique el mecanismo de seguridad existente, por ejemplo antes de que el procesador criptográfico 107 tenga siquiera oportunidad de codificar la información. La figura 1 (c) ilustra

la configuración y el flujo de información cuando está instalado un registrador de pulsaciones por hardware 111. El registrador de pulsaciones por hardware 111 se halla entre el teclado 101 y el ordenador 105. Como alternativa, el registrador de pulsaciones por hardware 111 puede estar incorporado al teclado 101. En ambos casos, la información se captura antes de entrar en el ordenador 105.

Un problema relacionado con los registradores de teclado lo presentan diversas formas de software malicioso (malware) o códigos no deseados, que el software antivirus es incapaz de combatir. Estos códigos no deseados, tales como un registrador de teclado, un spyware, un snoopware, un troyano, etc., son invisibles e irreproducibles. Este tipo de software puede estar instalado localmente o distribuirse a distancia. Algunos registradores de pulsaciones, por ejemplo, no sólo registran las pulsaciones en silencio, sino que también transmiten los registros de pulsaciones a un nodo remoto de Internet en silencio. Existen diversos programas anti malware no vírico, tales como programas contra los registradores de pulsaciones, que luchan contra estos códigos no deseados. La mayoría de estos productos detecta y lucha contra programas maliciosos ya conocidos. Por otra parte, los programas maliciosos diseñados ingeniosamente pueden tener mecanismos antidetección para defenderse. La aparición de nuevo software malicioso requiere el desarrollo de nuevo software antimalicioso. La batalla es similar a la lucha entre bacterias y antibióticos en medicina.

En el estado actual de la técnica existen varios planteamientos para ofrecer un comercio seguro por Internet y otras transacciones en línea seguras. Un método es asegurar que todos los mensajes entre dos nodos implicados en una transacción estén codificados. Si uno de los nodos de Internet está comprometido por un software malicioso que capture el mensaje antes de que sea codificado, el mecanismo de comunicación segura no sirve porque es demasiado tarde. Por ejemplo, la codificación no resuelve el problema del robo de identidad perpetrado mediante registradores de teclado, capturas de pantalla y otras técnicas para capturar la información introducida por un usuario de un ordenador, porque, como ya se ha mencionado más arriba, la codificación se realiza demasiado tarde, o sea después de que ya se haya capturado la información.

Otra forma de proteger la seguridad del comercio en línea es la autenticación de un individuo implicado en una transacción, por ejemplo a través de una federación de identidad o federación de autenticación tales como Kerberos ("Kerberos: The Network Authentication Protocol", http://web.mit.edu/kerberos/www/) y Microsoft Passport (Microsoft.Net Passport, Microsoft Cooperation, http://www.passport.net/). Sin embargo, estos mecanismos tampoco protegen contra registradores de teclado y ardides similares.

En un intento de detener el crecimiento del fraude en las tarjetas de crédito y aumentar la confianza de los consumidores durante las transacciones en línea, algunas empresas de tarjetas de crédito (por ejemplo Citibank) están facilitando números de tarjeta de crédito virtuales. Estos números de tarjeta de crédito son para un solo uso y ayudan a proteger el número real de la tarjeta de crédito del usuario durante una transacción en línea. En lugar de utilizar el número real, el usuario introduce el número virtual al efectuar compras en línea. Aunque se robe el número virtual, sirve de poco, ya que no puede volver a utilizarse tras la primera transacción.

Aunque este planteamiento ayuda a proteger al usuario contra el uso malicioso del número real de su tarjeta de crédito, presenta dos desventajas con respecto a un marco de prevención del robo de identidad más amplio. En primer lugar, el planteamiento está limitado a los números de tarjeta de crédito y no puede extenderse a otra información confidencial. En segundo lugar, para obtener un número de tarjeta de crédito de un solo uso, el usuario aún debe autenticarse en el banco. Este proceso de autenticación en línea puede ser un eslabón débil en sí, porque está sujeto a ataques de registradores de teclado. Los usuarios maliciosos pueden hacerse pasar por el usuario y obtener números de tarjeta de crédito virtuales en su nombre. En este escenario, el número real de la tarjeta de crédito del usuario es seguro, pero su identidad no.

Para mejorar la seguridad en línea, también pueden utilizarse tarjetas inteligentes. Una tarjeta inteligente es una tarjeta con microprocesador resistente a la falsificación, segura y portátil. Se ha utilizado con fines de seguridad en diversas aplicaciones (Jurgensen, T.M. and Guthery, S.B. Smart Cards, Pearson Education, Inc., 2002). La tarjeta inteligente es un token de seguridad para el acceso a ordenadores y a la red y para comunicaciones seguras. Para utilizar la tarjeta inteligente, ésta se conecta a un ordenador anfitrión. Empleando la infraestructura de clave pública (PKI) para asegurar la comunicación, la tarjeta guarda la clave privada de su propietario. Para enviar un mensaje de un usuario a otro usuario a través de Internet, el ordenador del remitente genera una clave compartida aleatoria, codifica el mensaje empleando la clave compartida y codifica la clave compartida empleando la clave pública del destinatario. Tanto el mensaje codificado como la clave codificada se envían al destinatario. El ordenador del destinatario utiliza la clave privada del destinatario almacenada en la tarjeta inteligente del mismo para decodificar la clave compartida codificada. A continuación, utiliza la clave compartida para decodificar el mensaje. De este modo, sólo puede leer el mensaje el destinatario deseado. Sin embargo, si el ordenador del usuario estuviese comprometido por un registrador de pulsaciones, el registrador capturaría la información antes de que se aplicase el mecanismo de la tarjeta inteligente.

Otro método existente es almacenar la información confidencial del usuario en la tarjeta inteligente. Para las transacciones en línea, el middleware ejecutado en el ordenador obtiene la información de la tarjeta inteligente y rellena los campos apropiados de un formulario web. Este planteamiento requiere un software especial en el ordenador. No proporciona más seguridad que la introducción manual en el formulario web, porque la información confidencial se halla en una forma no codificada en el navegador. En este sentido, es una característica de comodidad en lugar de una característica de seguridad.

Así pues, existe una necesidad de sistemas y métodos adicionales para combatir el robo de identidad que puede lograrse empleando un registrador de teclado en una estación de trabajo pública y capturando así información privada de un usuario que haya utilizado ésta para realizar transacciones seguras a través de Internet.

En una realización preferida, la invención proporciona un mecanismo para permitir a un usuario de un servicio en línea la transmisión de información personal confidencial necesaria para llevar a cabo negocios con dicho servicio en línea, sin tener que introducir dicha información personal confidencial de un modo que esté sujeto a una captura por parte de un registrador de teclado o un software o dispositivo de hardware similar. En la realización preferida, la información privada confidencial se almacena en una tarjeta inteligente para Internet bajo el control físico del usuario. El usuario dirige la tarjeta inteligente para transmitir la información privada confidencial al servidor del servicio en línea a través de una conexión segura. La información privada confidencial no existe nunca en una forma no codificada en el ordenador empleado por el usuario para realizar la transacción.

Un sistema y un método para efectuar transacciones seguras a través de una red informática de una manera diseñada para frustrar el robo de identidad perpetrado desde un ordenador no fiable. Una conexión de un ordenador cliente a la red en la que el ordenador cliente proporciona una interfaz de usuario para un usuario, una conexión de un ordenador servidor a la red y una conexión de un dispositivo informático seguro portátil a la red permiten una transmisión segura de información confidencial privada de un usuario del usuario a un servidor. La información privada se transmite directamente del dispositivo informático seguro al servidor a través de la conexión segura, sin posibilidad de que sea capturada en el ordenador con el que el usuario está interaccionando. El objeto de la invención se logra mediante el contenido de las reivindicaciones adjuntas.

Breve descripción de los dibujos

Las figuras 1(a), 1(b) y 1(c) son ilustraciones de cómo puede lograrse el robo de identidad empleando un registrador de teclado o un programa o hardware similar.

Las figuras 2(a) y (b) son ilustraciones de dos configuraciones físicas alternativas empleadas en una realización preferida de la invención.

La figura 3 es una ilustración gráfica de las conexiones lógicas a través de Internet con el empleo de una tarjeta inteligente para Internet según la invención.

La figura 4 es una ilustración gráfica de las conexiones lógicas seguras entre un servidor y múltiples clientes y tarjetas inteligentes según la invención.

La figura 5 es un diagrama de tiempo y flujo de datos que ilustra el modelo push para transmitir información privada confidencial de una tarjeta inteligente para Internet a un servidor remoto según la invención.

La figura 6 es un diagrama de tiempo y flujo de datos que ilustra el modelo pull para la recuperación de información privada confidencial de una tarjeta inteligente para Internet por parte de un servidor remoto según la invención.

La presente invención impide el robo de identidad perpetrado empleando registradores de teclado, capturas de pantalla o vigilancia a distancia, e incluso por personas que miren por encima del hombro del usuario, proporcionando un mecanismo para evitar que un usuario de una estación de trabajo tenga siquiera que introducir información confidencial, tal como contraseñas, números de la seguridad social, números de cuentas bancarias o números de tarjetas de crédito, al realizar transacciones seguras a través de Internet.

El robo de identidad en línea con mecanismos de registro es posible porque en el ordenador existe durante cierto tiempo, aunque sea poco, información confidencial no codificada. Un usuario malicioso puede lograr acceder a la información confidencial antes de que se aplique cualquier mecanismo de seguridad. Sin embargo, el mecanismo de registro no funcionará si la información confidencial, por ejemplo una contraseña, un número de la seguridad social, números de tarjetas de crédito, etc., no aparece nunca en texto claro en el ordenador o en línea. La noción de proporcionar un mecanismo que permita a un usuario evitar incluso introducir tal información confidencial es la idea base que subyace tras la presente invención. Un componente de una realización preferida de la invención es una tarjeta inteligente para Internet destinada a almacenar información personal confidencial. Cuando el propietario de la tarjeta lo necesite y autorice, la información fluye de manera segura de la tarjeta al cliente o servidor remoto de Internet sin ser siquiera visualizada o tecleada en la estación de trabajo del usuario. La tarjeta codifica y decodifica la información de forma enteramente interna. Aunque la información se transmite a través del ordenador que el usuario está utilizando para la transacción en línea, la información se codifica antes de que entre en dicho ordenador y, por lo tanto, sigue siendo segura. Desde el punto de vista del paso de información, el ordenador del usuario es sólo un encaminador más de la red.

Las tarjetas inteligentes para Internet pueden combatir el problema del registro de pulsaciones (y los problemas relacionados) porque una tarjeta inteligente para Internet es un nodo de red seguro portátil. Para usar la tarjeta, hay que poseerla físicamente, tener su número PIN y/o poseer la biometría almacenada en la misma. Existen varios niveles de seguridad: qué sé, qué tengo, quién soy. Así, proporcionando un mecanismo que utiliza tanto el conocimiento de un PIN como la posesión de una tarjeta, o incluso la identidad demostrada a través de un identificador biométrico, se

aumenta la seguridad. Y se aumenta aun más gracias a que la información asociada no se proporciona nunca en una manera que no sea totalmente codificada, de extremo a extremo, ni siquiera al ordenador que esté siendo empleando por un usuario para realizar alguna forma de comercio en línea.

Para cualquier transacción de cuentas en línea, por ejemplo la solicitud de una nueva cuenta o el acceso a una cuenta existente, en lugar de teclear información personal confidencial que pueda ser espiada a través de un registrador de teclado, una captura de pantalla o incluso por alguien que esté mirando por encima del hombro, según la invención un usuario establece una conexión segura de Internet entre la tarjeta inteligente del usuario y un servidor remoto seguro de un proveedor de servicios, por ejemplo el servidor de un banco o comerciante en línea. A través de la interfaz de la aplicación cliente de Internet, por ejemplo un navegador, el usuario decide qué información debe introducir directamente y qué información puede obtener el servidor de la tarjeta inteligente (o qué información puede enviar automáticamente la tarjeta inteligente al servidor). Por ejemplo para un número de la seguridad social o un número de tarjeta de crédito, un usuario puede elegir enviar esta información desde la tarjeta inteligente directamente al servidor. Esta información personal altamente confidencial se codifica en primer lugar en la tarjeta inteligente. Durante la transacción, el ordenador local no ve nunca la información personal confidencial almacenada en la tarjeta en su forma original, como tampoco lo hacen las personas que miren por encima del hombro del usuario ni el ladrón que captura cada pulsación, cada captura de pantalla u otras partes del ordenador.

Para acceder a la tarjeta inteligente para Internet, el usuario ha de introducir el código PIN o sus identificadores biométricos. Aunque el ordenador anfitrión esté comprometido y se capture el código PIN, el ladrón difícilmente podrá hacer algo con el PIN porque no tiene la tarjeta. Además, la mayor parte de la información capturada se analiza fuera de línea. Es sumamente difícil, si no imposible, descifrar qué PIN es para qué tarjeta inteligente.

Las figuras 2(a) y (b) son ilustraciones de dos configuraciones físicas alternativas empleadas en una realización preferida de la invención. Un servidor remoto se ejecuta en un ordenador remoto 201 ó 201'. El cliente local se ejecuta en un ordenador local 203 ó 203' que está utilizando un usuario 205 ó 205'. En ambos casos, los dos ordenadores 201 y 203 están conectados a Internet 209. Una tarjeta inteligente para Internet 207 ó 207' se conecta a Internet 209 bien conectándola directamente al ordenador local 203, que sirve de encaminador, o bien conectándola a otro dispositivo (no mostrado). La conexión a Internet 209 puede ser por cable o inalámbrica.

Más abajo en la presente memoria, nos referiremos al ordenador remoto, al ordenador local, a la tarjeta inteligente para Internet y al usuario utilizando los números de referencia sin virgulilla. Sin embargo, tales referencias se refieren a los dos escenarios presentados en las figuras 2(a) y 2(b), así como a cualesquiera otros equivalentes.

La figura 3 es una ilustración gráfica de las conexiones lógicas a través de Internet con el empleo de una tarjeta inteligente para Internet según la invención. El usuario utiliza un navegador 305, que se ejecuta en un ordenador local 301, para conectarse a la tarjeta inteligente para Internet 207 del usuario. El usuario puede pedir a su tarjeta inteligente 207 que establezca una conexión segura con el servidor remoto seguro 303, puede autorizar transacciones y puede vigilar estas últimas. La tarjeta inteligente para Internet 207 se conecta al servidor remoto seguro 303 según lo solicitado por el usuario, es decir su propietario. Todas las transacciones de datos se transmiten a través de una conexión segura. Los datos personales confidenciales del usuario se codifican y decodifican en la tarjeta inteligente 207 y en el servidor remoto seguro 303. El ordenador local 301 es uno de los nodos de Internet 209. El usuario utiliza otro navegador 307 para conectarse al servidor remoto 303, que ejecuta una aplicación de servidor 309.

Este mecanismo es aplicable a todos los tipos de transacciones electrónicas que utilicen Internet, por ejemplo la creación de una nueva cuenta y el acceso a una cuenta ya existente. El propietario de la tarjeta determina qué tipo de información personal se guarda dentro de la tarjeta 207. Por ejemplo, la tarjeta 207 puede contener contraseñas, números de la seguridad social y números de tarjeta de crédito. Dado que la información se codifica/decodifica dentro de la tarjeta inteligente 207 o dentro del servidor remoto seguro 303, la información queda oculta al ordenador local 203 que utiliza el usuario. El registro de pulsaciones, u otro mecanismo de registro, no puede obtener la información personal confidencial necesaria para completar las transacciones.

Una característica de una realización de la invención es establecer una conexión de Internet segura entre una tarjeta inteligente 207 y un servidor remoto 303 de un proveedor de servicios y enviar información codificada entre la tarjeta inteligente 207 y el servidor 303 directamente a través de la conexión segura. Dos realizaciones alternativas incluyen: (1) la tarjeta 207 envía los datos personales confidenciales al servidor remoto 303 y (2) el servidor remoto 303 recupera los datos de la tarjeta 207.

Aunque las realizaciones preferidas se describen empleando tarjetas inteligentes para Internet, los sistemas y métodos de la invención son aplicables también a otros token seguros.

Tarjeta inteligente para Internet 207

En la solicitud de patente 60/506,992, titulada SECURE NETWORKING USING A RESOURCE-CONSTRAINED DEVICE, también pendiente de concesión, se describe con mayor detalle una tarjeta inteligente para Internet 207. Una tarjeta inteligente es una tarjeta con microprocesador resistente a la falsificación, segura y portátil. La tarjeta inteligente para Internet 207 es, además, un nodo de Internet seguro según lo descrito en la solicitud de

patente 60/506,992. Por consiguiente, es posible establecer conexiones de Internet seguras entre la tarjeta inteligente para Internet 207 y otros nodos de Internet. El límite de seguridad está dentro de la tarjeta inteligente para Internet 207. Por ejemplo, la tarjeta Inteligente para Internet tiene implementación de SSL o bien TLS. Así pues, puede establecerse una conexión segura SSL/TLS entre la tarjeta 207 y otro nodo de Internet, por ejemplo el servidor remoto 303. Ésta es de hecho una RPV SSL de la tarjeta 207 a una aplicación remota, por ejemplo la aplicación de servidor 309.

En una realización de la invención, la información del usuario se almacena en la tarjeta inteligente 207 durante el proceso de personalización de la tarjeta. Una personalización posterior podría también almacenar información personal adicional en la tarjeta 207 después de haber sido emitida ésta o modificar información en la tarjeta 207 de una manera segura. El usuario también puede personalizar la tarjeta inteligente utilizando un ordenador seguro, por ejemplo cambiando el PIN. La tarjeta inteligente sólo proporciona información a clientes o servidores de confianza si lo autoriza el usuario.

En una realización preferida, la tarjeta inteligente para Internet puede hacer lo siguiente:

1. Establecer conexiones seguras con un cliente de Internet y un servidor de Internet simultáneamente. La tarjeta es un servidor con respecto al cliente de Internet. Puede ser un cliente o un servidor con respecto al servidor remoto.

2. Comunicarse de manera segura con el cliente de Internet.

3. Comunicarse de manera segura directamente con el servidor de Internet. La tarjeta inteligente codifica los datos dentro de la tarjeta, envía los datos codificados al otro nodo de Internet y decodifica los datos dentro de la tarjeta.

4. Notificar al usuario, a través de la aplicación cliente, cuándo trata el servidor remoto de obtener información. Sólo proporciona información si el usuario lo autoriza.

Es importante que se realice una autenticación mutua cuando la tarjeta inteligente para Internet 207 esté conectada. Con SSL, la autenticación de cliente es opcional. Sin embargo, con la tarjeta inteligente para Internet 207 como servidor, la autenticación de cliente es obligatoria. De lo contrario, si sólo se realizase la autenticación de servidor, el cliente estaría protegido, pero no así la tarjeta inteligente 207.

Aplicación cliente de Internet

Los navegadores 305 y 307 son aplicaciones cliente de Internet. Son clientes locales que se ejecutan en el ordenador local 301. El usuario 205 utiliza un navegador para acceder a los servicios prestados por un proveedor de servicios de Internet. La técnica presentada en este documento no requiere cambio alguno en los navegadores estándar, tales como Internet Explorer, Netscape, Safari o Mozilla. El único requisito para el navegador es que soporte conexiones HTTPS. El usuario 205 utiliza una instancia 307 del navegador para conectarse a un servidor remoto 303 de un proveedor de servicios y utiliza otra instancia 305 del navegador para conectarse a su tarjeta inteligente para Internet 207.

Interacciones del usuario

La técnica de impedir el robo de identidad según una realización de la invención prevé una interacción particular del usuario al interaccionar el usuario 205 con el servidor remoto seguro 303 a través de la aplicación cliente de Internet, por ejemplo un navegador. Para la información personal confidencial, en lugar de teclearla, el usuario 205 puede elegir enviar la información desde su tarjeta inteligente para Internet 207 directamente a un servidor de confianza, por ejemplo el servidor remoto 303. El usuario 205 puede dar, por ejemplo, los siguientes pasos para realizar una transacción en línea según la invención, por ejemplo para crear una nueva cuenta o acceder a una cuenta ya existente en un banco:

1. Establecer una conexión segura de un navegador (B1) 305 a la tarjeta inteligente para Internet 207 del usuario. Para identificar al usuario 205 ante la tarjeta inteligente 207 se utiliza el número PIN o información biométrica.

2. Pedir, a través del navegador (B1) 305, a la tarjeta inteligente 207 que establezca una conexión segura con el servidor remoto seguro 303.

3. Arrancar otro navegador (B2) 307 y establecer una conexión segura de B2 307 al servidor remoto 303. Si se pide, el usuario 205 introduce un valor secreto compartido.

4. Rellenar en B2 307 un formulario solicitado, por ejemplo un formulario para crear una nueva cuenta o un formulario para acceder a una cuenta ya existente. Para la información personal confidencial, por ejemplo el número de la seguridad social o un número de tarjeta de crédito, el usuario 205 elige enviar los datos de la tarjeta inteligente 207 al servidor remoto 307 directamente y de manera segura.

5. Desde el navegador B1 305, seleccionar la información almacenada en la tarjeta inteligente 207, que a su vez envía la información al servidor remoto 303.

6. Una vez concluido el proceso, el usuario 205 cierra la sesión en ambas instancias de navegador, B1 305 y B2 307.

La sección de más abajo relativa a la secuencia de trabajo contiene una descripción más detallada de las interacciones entre el usuario 205 y las instancias de navegador 305 y 307. En la etapa de la conexión a la tarjeta inteligente (paso 1, más arriba), aunque el ordenador anfitrión 203 (en el que se ejecuta la aplicación cliente local, el navegador B1 305) esté comprometido y se capture el código PIN, por ejemplo a través de un registrador de teclado, el ladrón difícilmente podrá hacer nada con el PIN porque no posee la tarjeta 207. Además, la mayor parte de la información capturada se analiza fuera de línea. Para quienquiera que hubiese capturado el PIN, sería sumamente difícil, si no imposible, determinar a qué tarjeta inteligente corresponde el mismo.

Relación entre la tarjeta inteligente 207 y el usuario 205 desde el punto de vista del servidor remoto 303

Por regla general, el servidor remoto 303 de un proveedor de servicios puede atender múltiples aplicaciones cliente de distintos nodos de Internet simultáneamente. Por lo tanto, el servidor remoto 303 puede conectarse a múltiples tarjetas inteligentes para Internet 207 a la vez. Con el fin de hacer seguras las transacciones entre la aplicación cliente 307, la tarjeta inteligente 207 y el servidor remoto 303, la realización preferida de la invención proporciona un mecanismo para abordar las siguientes cuestiones:

1. ¿Cómo consigue un usuario 205 que el servidor remoto 303 asocie su aplicación cliente 307 a su tarjeta inteligente 207 para una sesión concreta, sí la aplicación cliente 307 reside en un nodo de Internet 203 diferente a su tarjeta inteligente 207?.

2. ¿Cómo impedir que un usuario 205, a través de su aplicación cliente 307, se asocie a la tarjeta inteligente de otro usuario?.

La figura 4 es una ilustración gráfica de las conexiones lógicas seguras entre un servidor y múltiples clientes y tarjetas inteligentes según la invención. Los nodos del gráfico 400 representan el servidor 303, un cliente 301 o una tarjeta inteligente 207 (utilizándose las designaciones de letras (k, m, n) para indicar diferentes instancias de dispositivos similares).

Todas las conexiones son seguras y cada una de ellas tiene asociado un secreto compartido único. Una arista 401 (nodo i, nodo j) está, por lo tanto, especificada por un canal, que es un cuadruplete {(dirección IP y número de puerto de nodo i), (dirección IP y número de puerto de nodo j)}, y el secreto compartido entre el nodo i y el nodo j. Cada nodo conoce y sólo conoce las aristas que están conectadas al nodo. Las cuestiones anteriores pueden volver a plantearse de la siguiente manera:

1. ¿Cómo asocia el servidor remoto seguro 303 el cliente n (301 n) a la tarjeta n 207n?.

2. ¿Cómo impedir que el nodo cliente k 301 k pida al nodo servidor 303 que lo asocie a la tarjeta 207n?.

Como se ha mencionado más arriba, el usuario 205 pide a su tarjeta inteligente para Internet 207 (tarjeta n) que inicie una conexión entre la tarjeta 207 y el servidor remoto 303. La tarjeta 207 envía al servidor remoto 303 la credencial de inicio de sesión del usuario, la dirección IP del nodo cliente (cliente n) y un PIN secreto (sPin). El servidor remoto 303 utiliza la información para establecer una asociación entre el usuario 205, el nodo cliente 301 y la tarjeta inteligente 207. Cuando el usuario 205 accede al servidor remoto 303 mediante el navegador 307 (cliente n 307n), introduce el PIN secreto. A partir de la dirección IP del nodo cliente 301 y el PIN secreto, el servidor remoto 303 mapea la tarjeta inteligente 207n del usuario 205 (tarjeta n). Un usuario malicioso, el cliente k 301 k, puede pretender conectarse al servidor 303 mediante la dirección IP del cliente n, pero no tiene el PIN secreto y no puede establecer la asociación.

El propietario de cada tarjeta inteligente para Internet 207 controla el PIN secreto de la tarjeta en cuestión. El servidor remoto 303 guarda un registro del PIN secreto sólo para una sesión. La asociación usuario-cliente-tarjeta que incluye el PIN secreto se elimina una vez finalizada la sesión. Por motivos de seguridad, este PIN secreto debería ser diferente del PIN de la tarjeta inteligente utilizado por el usuario para entrar en el sistema de la misma.

Este PIN secreto funciona como secreto compartido entre el usuario 205 y el servidor remoto 303 durante la sesión. El usuario conoce este secreto porque procede de su tarjeta inteligente para Internet. Tiene control sobre los PIN para cada uno de los proveedores de servicios de confianza almacenados en la tarjeta. El servidor remoto 303, por otra parte, conoce este secreto porque la tarjeta inteligente 207 se lo ha pasado de forma segura.

Si el usuario 205 se halla en un PC público que esté comprometido, toda pulsación que realice puede ser capturada y almacenada sin su conocimiento. Con el mecanismo convencional de inicio de sesión por nombre de usuario/contraseña, una persona maliciosa puede utilizar el nombre de usuario y la contraseña capturados para entrar en la cuenta del usuario en el servidor remoto. El nombre de usuario y la contraseña persisten en el servidor remoto. Por otra parte, desde el punto de vista del servidor remoto, el PIN secreto es un PIN de un solo uso. Por lo tanto, aunque que se capture el PIN secreto, no podrá utilizarse para iniciar de nuevo sesión sin la tarjeta inteligente para Internet 207.

Si no se utiliza un PIN secreto, un código malicioso podría potencialmente enviar una petición de inicio de sesión al servidor remoto 303 fingiendo que procede de la misma dirección IP que el PC local. Este código malicioso puede conseguir acceder al servidor remoto 303 y obtener información confidencial de la tarjeta inteligente para Internet 207 del usuario. El uso del PIN secreto cierra este resquicio potencial.

Secuencia de trabajo

Como se ha mencionado más arriba, existen dos realizaciones alternativas de la invención en cuanto a si la información confidencial es extraída por el método pull por el servidor remoto 303 (el modelo pull) o enviada por el método push al servidor remoto 303 (el modelo push). En ambos casos, la información fluye de la tarjeta inteligente para Internet 207 al servidor remoto 303. El modelo push puede utilizarse en la mayoría de las configuraciones de red en las que una tarjeta inteligente para Internet 207 tenga una dirección IP y esté conectada a Internet 209. Sin embargo, el modelo pull puede utilizarse sólo si la tarjeta inteligente para Internet 207 es globalmente accesible desde fuera de la LAN a la que está conectada.

La figura 5 es un diagrama de tiempo y flujo de datos que ilustra el modelo push, en el que la tarjeta inteligente 207 envía por el método push datos personales confidenciales al servidor remoto 303, e ilustra la interacción de tres elementos clave en este modelo, o sea el PC local 203, la tarjeta inteligente para Internet 207 y el servidor remoto 303 de un proveedor de servicios. En el modelo push, la dirección IP de la tarjeta inteligente para Internet 207 puede estar o no estar accesible desde fuera de la LAN a la que la tarjeta inteligente 207 está conectada. Todas las flechas que indican interacciones entre elementos representan conexiones HTTPS que emplean el protocolo SSL/TLS.

1. El usuario 205 arranca un navegador B1 305 en el PC local 203. El navegador B1 305 funciona como aplicación cliente de Internet.

2. Desde B1 305, el usuario se conecta a la tarjeta inteligente para Internet 207 y se autentica empleando su PIN a través de una conexión HTTPS segura, paso 502.

3. Una vez autenticado, se ofrece al usuario 205 una lista de proveedores de servicios de confianza 503. El usuario selecciona un proveedor de servicios y pide a la tarjeta inteligente para Internet que establezca una conexión segura con este proveedor de servicios, paso 505.

4. La tarjeta inteligente para Internet 207 conoce la dirección IP del servidor remoto 303 que corresponde al proveedor de servicios seleccionado. La tarjeta 207 establece una conexión segura con el servidor remoto 303 empleando el protocolo SSL/TLS, paso 507, y envía al servidor remoto 303 los datos 509 almacenados en la tarjeta inteligente siguientes:

    a. IP de cliente (clientIP): dirección IP del PC local 203.

    b. IP de tarjeta (cardIP): dirección IP de la tarjeta inteligente para Internet 207.

    c. Credenciales de inicio de sesión (login credentials): estas credenciales permiten al usuario 205 autenticarse en el servidor remoto 303. Ejemplos de estas credenciales pueden ser un nombre de usuario y una contraseña.

    d. PIN secreto (sPin): un PIN secreto compartido, que proporciona un nivel adicional de autenticación cuando el usuario inicia realmente una sesión en el servidor remoto 303.

5. Una vez recibidos los datos 509 que le han sido enviados en el paso 4, el servidor remoto 303 crea un mapa interno que vincula el IP de cliente con otros tres atributos: IP de tarjeta, credenciales de inicio de sesión y PIN secreto, paso 511.

6. El usuario 205 hace ahora clic en un vínculo en B1 305 para iniciar (paso 513) otra instancia, B2 307, del navegador con el URL puesto en la página de autenticación del servidor remoto 303.

7. La segunda instancia de navegador B2 307 se conecta al servidor remoto 303 para solicitar una nueva sesión, paso 515.

8. Una vez recibida la petición de nueva sesión del PC local 203, el servidor remoto 303 puede determinar si la petición procede de la misma dirección IP de cliente que la que le fue transmitida en el paso 4 en el mensaje 509. El servidor remoto 303 marca el mapeado de este IP de cliente como "conectado" pero hasta el momento no "autorizado", paso 517. "Conectado" significa que el usuario se ha conectado desde la dirección IP correspondiente y, dado que sólo está permitida una conexión, no se atenderá ninguna petición de conexión subsiguiente.

9. Para autorizar la sesión actual, el servidor remoto 303 envía un mensaje 519 al usuario 205 pidiéndole que introduzca el PIN secreto correspondiente a esta conexión.

10. A continuación, el servidor remoto 303 determina si el usuario 205 puede ser autenticado y autorizado a continuar la transacción, paso 521. Si el PIN secreto introducido por el usuario 205 coincide con el que aparece en el mapa para el IP de cliente, el usuario 205 inicia sesión utilizando las credenciales apropiadas, que también están almacenadas en el mismo mapa. La secuencia de trabajo puede continuar ahora con el paso 12 (ilustrado en la figura 5 como elemento 523).

11. Sin embargo, si el PIN secreto introducido por el usuario 205 no coincide con el que aparece en el mapa, el servidor remoto 303 termina la conexión con el usuario 205. No se permite el acceso. Además se destruye el mapa que vincula el IP de cliente a una cuenta de usuario específica y la tarjeta inteligente para Internet, paso 521'. Los pasos subsiguientes que se indican a continuación se vuelven irrelevantes.

12. Una vez concedido el acceso, el usuario 205 puede ahora interaccionar 523 con los servicios web prestados por el servidor remoto 303 a través del navegador B2 307. Un paso en esta interacción puede ser pedir que se recupere cierta información confidencial (por ejemplo el número y la fecha de caducidad de la tarjeta de crédito del usuario) de la tarjeta inteligente para Internet en lugar de teclearla manualmente. El usuario 205 indica al servidor remoto 303 que la tarjeta inteligente para Internet 207 va a enviar esta información.

13. El servidor remoto 303 espera ahora 525 a que llegue la información confidencial de la tarjeta inteligente para Internet 207. La transacción en el servidor remoto 303 y la interfaz de usuario en el navegador B2 307 estarán en el modo de espera.

14. El usuario 205 cambia ahora al navegador B1 305 que está conectado al servidor web en la tarjeta inteligente para Internet. El usuario 205 selecciona, paso 527, la información confidencial que debe enviarse al servidor remoto 303 e interacciona, mensaje 529, con la tarjeta 207 para ordenar a ésta que envíe la información confidencial que ha de enviarse al servidor remoto 303. Ésta es la misma información que está esperando el servidor remoto 303.

15. La tarjeta inteligente 207 envía la información seleccionada al servidor remoto, paso 531, y lee la repuesta, mensaje 533, del servidor remoto 303. La respuesta puede incluir el estado de la transacción y cualquier información adicional que el servidor remoto 303 desee enviar de vuelta.

16. El servidor remoto utiliza la información confidencial recibida en el mensaje 531 para completar la transacción, paso 535, que había sido puesta en estado de espera en el paso 13.

17. El servidor remoto 303 envía un mensaje de actualización 537 al navegador B2 307 para hacer que éste actualice la interfaz de usuario en el navegador B2 307 con el fin de indicar que la transacción solicitada se ha completado.

18. El usuario 205 cierra la sesión en el servidor remoto 303, mensaje 539.

19. Después de recibir la petición de cierre de sesión 539 del usuario, el servidor remoto borra el mapeado del IP de cliente, paso 541. Esto impide que se envíen transacciones subsiguientes a la tarjeta inteligente 207.

20. El usuario 205 cierra la sesión, mensaje 543, en su tarjeta inteligente para Internet 207 y puede retirar la tarjeta inteligente 207 del lector.

El modelo pull

En el modelo pull, la tarjeta inteligente para Internet 207 está conectada a una red 209 de tal modo que es accesible desde fuera de la LAN a la que está conectada. Esto permite a clientes externos conectarse al servidor web en la tarjeta inteligente para Internet 207 y extraer por el método pull información confidencial. La figura 6 es un diagrama de tiempo y flujo de datos que ilustra el modelo pull, en el que el servidor remoto 303 extrae por el método pull datos personales confidenciales de la tarjeta inteligente para Internet 207, e ilustra la interacción de tres elementos clave en este modelo, o sea el PC local 203, la tarjeta inteligente para Internet 207 y el servidor remoto 303 de un proveedor de servicios. Como en la figura 5, todas las flechas que indican interacciones entre elementos representan conexiones HTTPS que emplean el protocolo SSL/TLS.

Varios de los pasos (números 1 a 11) del modelo pull son idénticos a los del modelo push, pero se repiten aquí para guardar la integridad. Los elementos y acciones semejantes llevan en las figuras 5 y 6 los mismos números de referencia.

1. El usuario 205 arranca un navegador B1 305 en el PC local 203. El navegador B1 305 funciona como aplicación cliente de Internet.

2. Desde B1 305, el usuario se conecta a la tarjeta inteligente para Internet 207 y se autentica empleando su PIN a través de una conexión HTTPS segura, paso 502.

3. Una vez autenticado, se ofrece al usuario 205 una lista de proveedores de servicios de confianza 503. El usuario selecciona un proveedor de servicios y pide a la tarjeta inteligente para Internet que establezca una conexión segura con este proveedor de servicios, paso 505.

4. La tarjeta inteligente para Internet 207 conoce la dirección IP del servidor remoto 303 que corresponde al proveedor de servicios seleccionado. La tarjeta 207 establece una conexión segura con el servidor remoto 303 empleando el protocolo SSL/TLS, paso 507, y envía al servidor remoto 303 los datos 509 almacenados en la tarjeta inteligente siguientes:

   a. IP de cliente (clientIP): dirección IP del PC local 203.

   b. IP de tarjeta (cardIP): dirección IP de la tarjeta inteligente para Internet 207.

   c. Credenciales de inicio de sesión (login credentials): estas credenciales permiten al usuario 205 autenticarse en el servidor remoto 303. Ejemplos de estas credenciales pueden ser un nombre de usuario y una contraseña.

   d. PIN secreto (sPin): un PIN secreto compartido, que proporciona un nivel adicional de autenticación cuando el usuario inicia realmente una sesión en el servidor remoto 303.

5. Una vez recibidos los datos 509 que le han sido enviados en el paso 4, el servidor remoto 303 crea un mapa interno que vincula el IP de cliente con otros tres atributos: IP de tarjeta, credenciales de inicio de sesión y PIN secreto, paso 511.

6. El usuario 205 hace ahora clic en un vínculo en B1 305 para iniciar (paso 513) otra instancia, B2 307, del navegador con el URL puesto en la página de autenticación del servidor remoto 303.

7. La segunda instancia de navegador B2 307 se conecta al servidor remoto 303 para solicitar una nueva sesión, paso 515.

8. Una vez recibida la petición de nueva sesión del PC local 203, el servidor remoto 303 puede determinar que la petición procede de la misma dirección IP de cliente que la que le fue transmitida en el paso 4 en el mensaje 509. El servidor remoto 303 marca el mapeado de este IP de cliente como “conectado” pero hasta el momento no “autorizado”, paso 517. “Conectado” significa que el usuario se ha conectado desde la dirección IP correspondiente y, dado que sólo está permitida una conexión, no se atenderá ninguna petición de conexión subsiguiente.

9. Para autorizar la sesión actual, el servidor remoto 303 envía un mensaje 519 al usuario 205 pidiéndole que introduzca el PIN secreto correspondiente a esta conexión.

10. A continuación, el servidor remoto 303 determina si el usuario 205 puede ser autenticado y autorizado a continuar la transacción, paso 521. Si el PIN secreto introducido por el usuario 205 coincide con el que aparece en el mapa para el IP de cliente, el usuario 205 inicia sesión utilizando las credenciales apropiadas, que también están almacenadas en el mismo mapa. La secuencia de trabajo puede continuar ahora con el paso 12 (ilustrado en la figura 6 como elemento 623).

11. Sin embargo, si el PIN secreto introducido por el usuario 205 no coincide con el que aparece en el mapa, el servidor remoto 303 termina la conexión con el usuario 205. No se permite el acceso. Además se destruye el mapa que vincula el IP de cliente a una cuenta de usuario específica y la tarjeta inteligente para Internet, paso 521’. Los pasos subsiguientes que se indican a continuación se vuelven irrelevantes.

12. Una vez concedido el acceso, el usuario 205 puede ahora interaccionar con los servicios web prestados por el servidor remoto 303 a través de B2 307, paso 623. Un aspecto de esta interacción puede ser pedir que el servidor remoto 303 recupere cierta información confidencial (por ejemplo el número y la fecha de caducidad de la tarjeta de crédito del usuario) de la tarjeta inteligente para Internet 207 en lugar de teclearla manualmente.

13. El servidor remoto 303 remite esta petición a la tarjeta inteligente para Internet 207, mensaje 625. Dado que es el servidor remoto 303 quien inicia la petición de información confidencial, es un modelo pull. El servidor remoto 303 extrae por el método pull la información de la tarjeta inteligente para Internet 207.

14. La tarjeta inteligente para Internet 207 no envía inmediatamente la información confidencial solicitada. En lugar de ello, notifica al usuario 205 que el servidor remoto 303 está solicitando esta información, mensaje 627. Esta notificación se envía al usuario 205 a través del navegador B1 305 que está conectado a la tarjeta inteligente para Internet 207.

15. El usuario responde bien con una aprobación o bien con una denegación, mensaje 629.

16. A continuación, la tarjeta inteligente para Internet 207 responde al servidor remoto 303 sobre la base de la respuesta recibida del usuario 205, mensaje 631. Si el usuario 205 lo aprueba, la información confidencial se envía al servidor remoto 303. Si no, se envía un mensaje de denegación.

17. Si la tarjeta inteligente 207 envía la información confidencial, el servidor remoto 303 completa la transacción, paso 633. Si se recibe un mensaje de denegación, el servidor remoto 303 abandona la transacción (no mostrado). Una vez completa la transacción, el servidor remoto envía el estado y cualquier información adicional a la tarjeta inteligente para Internet, mensaje 635.

18. El usuario cierra la sesión en el servidor remoto, mensaje 637.

19. Después de recibir la petición de cierre de sesión del usuario, el servidor remoto borra el mapeado del IP de cliente, paso 639. Esto impide que se envíen transacciones subsiguientes a la tarjeta inteligente.

20. El usuario cierra la sesión en su tarjeta inteligente para Internet, mensaje 641.

Comparación de los modelos push y pull

Como se ha mencionado más arriba, el modelo push puede utilizarse en la mayoría de las configuraciones de red, siempre que la tarjeta inteligente para Internet 207 tenga una dirección IP. Esta dirección IP puede ser o no ser globalmente accesible o única. Además puede haber un firewall que impida el acceso directo desde el exterior al servidor web ejecutado en la tarjeta inteligente para Internet 207. Dado que la tarjeta inteligente para Internet 207 puede iniciar una conexión TCP/IP y conectarse a servidores web fuera de la LAN, el modelo push puede soportar transacciones en línea seguras.

En cambio, el modelo pull sólo puede utilizarse si la tarjeta inteligente para Internet 207 está conectada a una red de tal modo que sea visible y accesible desde fuera de la LAN. En este modelo, una entidad exterior, por ejemplo un servidor remoto 303, se conecta al servidor web ejecutado en la tarjeta inteligente para Internet 207.

Escenario de uso

En un escenario de uso típico, el usuario 205 lleva consigo la tarjeta inteligente para Internet 207. La tarjeta 207 puede conectarse a la red 209 a través de cualquier PC 203. El PC 203 puede hallarse en un lugar público y puede no ser seguro, pero aún puede utilizarse para conectar la tarjeta inteligente para Internet 207 a Internet 209 con el fin de realizar transacciones en línea seguras. Este escenario proporciona la seguridad añadida del paradigma de “lo que tienes”. La tarjeta inteligente para Internet 207 puede quitarse de la red y devolverse al bolsillo del usuario una vez completada una transacción. Cuando se halla en el bolsillo del usuario, ningún código malicioso puede organizar un ataque a la tarjeta inteligente para Internet 207. Aunque existen defensas contra tales ataques, la no presencia de la tarjeta 207 en la red excluye incluso la posibilidad remota de dichos ataques.

Prevención del robo de identidad basado en la captura de pantalla

Además de los registradores de pulsaciones, existen otros mecanismos espía que pueden observar qué están haciendo las personas en un ordenador y enviar los registros por Internet. Por ejemplo, algunos productos capturan la pantalla del ordenador; otros productos capturan tanto la pantalla como las pulsaciones. La información capturada se transmite a través de Internet o bien se recupera posteriormente para realizar un análisis destinado al extraer información confidencial, por ejemplo contraseñas.

El método para impedir el robo de identidad según la invención puede impedir también el robo de identidad en línea basado en la captura de pantalla. La información confidencial se codifica y se envía entre la tarjeta inteligente para Internet 207 y el servidor remoto seguro 303 directamente. El ordenador local 203 que está empleando el usuario 205 no ve tal información en texto claro y, por lo tanto, no puede visualizarla en la pantalla. Por consiguiente, el capturador de pantalla no puede conseguir la información.

Los únicos dos elementos de información confidencial introducidos manualmente por el usuario 205 son su PIN para autenticarse ante la tarjeta inteligente y el PIN secreto para autenticarse ante el servidor remoto 303. Ninguno de éstos compromete la sesión actual en modo alguno. Aunque se capturen, el PIN y el PIN secreto son inútiles sin el acceso físico a la tarjeta inteligente para Internet 207. Además, estos dos valores pueden cambiarse fácilmente una vez que el usuario vuelva a un entorno de PC seguro, por ejemplo en su casa o despacho.

Conclusión

La presente invención presenta un nuevo sistema y método para utilizar tarjetas inteligentes para Internet con el fin de impedir el robo de identidad en línea y hacer seguras las transacciones en línea. Con este nuevo método se establece una conexión de Internet segura entre la tarjeta inteligente 207 y el servidor remoto seguro 303 del proveedor de servicios, por ejemplo un banco. La información personal, por ejemplo contraseñas, números de la seguridad social y números de tarjeta de crédito, está almacenada en la tarjeta inteligente 207. La información se codifica en la tarjeta inteligente 207 y se envía de forma segura y directamente de la tarjeta al servidor 303 con la autorización del usuario. Así pues, a través del ordenador local 203 e Internet 209 no pasa ninguna información personal confidencial en formato claro (no codificado). Este mecanismo combate el mecanismo del robo de identidad que captura la información en el ordenador antes de que sea codificada. Este método no está limitado a la forma de las tarjetas inteligentes para Internet seguras. Es aplicable a otros token seguros que sean nodos de Internet y tengan también un límite de seguridad dentro de los token.

REIVINDICACIONES

1. Método para realizar transacciones seguras a través de una red informática, que comprende:

conexión de un ordenador cliente a la red, proporcionando el ordenador cliente una interfaz de usuario para interaccionar con un usuario;

conexión de un ordenador servidor a la red;

conexión de un dispositivo informático seguro portátil a la red;

utilización del dispositivo informático seguro para comunicar una lista de servicios disponibles al ordenador cliente;

capacidad de respuesta para recibir la lista de servicios disponibles utilizando la interfaz de usuario para mostrar la lista de servicios disponibles a un usuario;

capacidad de respuesta a una selección de un servicio disponible por parte del usuario, estableciendo una conexión segura del dispositivo informático seguro al servidor;

comunicación segura de información privada del dispositivo informático seguro al servidor a través de la conexión segura, comprendiendo la información privada credenciales de inicio de sesión y un secreto compartido;

envío de un mensaje del servidor al usuario en el que se pide al usuario que introduzca el secreto compartido;

determinación en el servidor de si el secreto compartido recibido del usuario coincide con el secreto compartido recibido del dispositivo informático seguro;

impidiendo así el robo de identidad durante la interacción a través de la red informática.

2. Método según la reivindicación 1, que además comprende:

autenticación de un usuario sobre la base de la información privada y,

en respuesta a una autenticación del usuario efectuada con éxito, realización de una transacción entre el ordenador cliente y el ordenador servidor.

3. Método según la reivindicación 1, que además comprende:

transmisión, del dispositivo informático seguro al ordenador servidor, de información identificativa del usuario.

4. Método según la reivindicación 3, en el que la información identificativa del usuario incluye un número de identificación personal secreto (sPIN).

5. Método según la reivindicación 4, que además comprende:

capacidad de respuesta a la recepción de la información identificativa del usuario, utilizando el ordenador servidor para establecer una asociación entre el usuario, el cliente y el dispositivo informático seguro.

6. Método según la reivindicación 4, en el que el dispositivo informático seguro tiene un número de identificación personal (PIN), no estando relacionados el PIN secreto (sPIN) y el PIN.

7. Método según la reivindicación 4, en el que el ordenador servidor utiliza el PIN secreto para una sola sesión.

8. Método según la reivindicación 1, en el que el dispositivo informático seguro portátil es una tarjeta inteligente.

9. Método para realizar transacciones seguras a través de una red informática, que comprende:

conexión de un ordenador cliente a la red, proporcionando el ordenador cliente una interfaz de usuario para interaccionar con un usuario;

conexión de un ordenador servidor a la red;

conexión de un dispositivo informático seguro a la red;

establecimiento de una conexión segura del dispositivo informático seguro al servidor;

comunicación segura de información privada del dispositivo informático seguro al servidor a través de la conexión segura, comprendiendo la información privada credenciales de inicio de sesión y un secreto compartido;

envío de un mensaje del servidor al usuario en el que se pide al usuario que introduzca el secreto compartido;

determinación en el servidor de si el secreto compartido recibido del usuario coincide con el secreto compartido recibido del dispositivo informático seguro;

autenticación de un usuario utilizando las credenciales de inicio de sesión de la información privada y,

en respuesta a una autenticación del usuario efectuada con éxito, realización de una transacción entre el ordenador cliente y el servidor;

impidiendo así el robo de identidad durante la interacción a través de la red informática.

10. Método según la reivindicación 9, en el que el paso de la comunicación segura de información privada comprende enviar por el método push la información privada del dispositivo informático seguro al ordenador servidor.

11. Método según la reivindicación 10, que además comprende:

en respuesta a una autenticación de un usuario realizada con éxito, utilización del cliente para transmitir al servidor una indicación de que el dispositivo informático seguro va a enviar información necesaria para una transacción;

utilización del servidor para que espere a la información del dispositivo informático seguro,

utilización del cliente para seleccionar la información necesaria para la transacción y,

en respuesta a la selección de la información necesaria para la transacción, utilización del dispositivo informático seguro para transmitir de forma segura al servidor la información seleccionada.

12. Método según la reivindicación 9, en el que el paso de la comunicación segura de información privada comprende la utilización del ordenador servidor para extraer por el método pull la información privada del dispositivo informático seguro.

13. Método según la reivindicación 9, que además comprende:

en respuesta a una autenticación de un usuario realizada con éxito, utilización del servidor para transmitir al dispositivo informático seguro una petición para que proporcione información necesaria para completar la transacción;

en respuesta a una petición del servidor de información necesaria para completar una transacción, utilización del dispositivo informático seguro para notificar al cliente que el servidor ha hecho una petición de información necesaria para completar una transacción;

en respuesta a la notificación del dispositivo informático seguro de que el servidor está pidiendo la información necesaria para completar una transacción, utilización del cliente para obtener del usuario una aprobación o una denegación de la petición y,

en respuesta a una aprobación del usuario, transmisión de la información solicitada del dispositivo informático seguro al servidor de un modo seguro.

14. Sistema para realizar transacciones seguras a través de una red informática, que comprende:

un ordenador servidor conectado a una red informática y utilizable para prestar algún tipo de transacciones en línea;

un ordenador cliente conectado a la red informática y utilizable para que actúe de interfaz con un usuario;

un dispositivo informático seguro conectado a la red informática y capaz de establecer una conexión segura con el ordenador servidor y el ordenador cliente;

teniendo el dispositivo informático seguro una lógica utilizable para almacenar información privada de usuario, comprendiendo la información privada credenciales de inicio de sesión y un secreto compartido;

teniendo el dispositivo informático seguro una lógica que, en respuesta a la iniciación de una transacción entre un usuario que utilice el ordenador cliente y el ordenador servidor, pueda utilizarse para transmitir de forma segura la información privada de usuario al ordenador servidor de tal modo que sólo el servidor pueda interpretar la información privada de usuario

y teniendo el ordenador servidor una lógica utilizable para enviar al usuario un mensaje en el que se pida al usuario que introduzca el secreto compartido y para determinar si el secreto compartido recibido del usuario coincide con el secreto compartido recibido del dispositivo informático seguro;

impidiendo así el robo de identidad durante la interacción a través de la red informática.

15. Sistema para realizar transacciones seguras a través de una red informática según la reivindicación 14, en el que el dispositivo informático seguro tiene una lógica para transmitir al ordenador servidor un mapa, teniendo el mapa los elementos IP de cliente (clientIP), IP de tarjeta (cardIP), credenciales de inicio de sesión y número de identificación personal secreto (sPIN);

teniendo el ordenador servidor una lógica para pedir a un usuario que introduzca el PIN secreto (sPIN) y una lógica para comprobar si el PIN secreto introducido coincide con el PIN secreto que aparece en el mapa.

16. Sistema para realizar transacciones seguras a través de una red informática según la reivindicación 15,

en el que el ordenador servidor tiene una lógica para destruir el mapa si el PIN secreto introducido por el usuario no coincide con el PIN secreto que aparece en el mapa.

17. Sistema para realizar transacciones seguras a través de una red informática según la reivindicación 14,

en el que el dispositivo informático seguro portátil transmite la información privada de usuario a petición del usuario.

18. Sistema para realizar transacciones seguras a través de una red informática según la reivindicación 14,

en el que el dispositivo informático seguro portátil transmite la información privada de usuario a petición del ordenador servidor.

19. Sistema para realizar transacciones seguras a través de una red informática según la reivindicación 18,

en el que el dispositivo informático seguro portátil transmite al ordenador servidor la información privada de usuario sólo tras haber dado el usuario permiso para ello.

20. Sistema para realizar transacciones seguras a través de una red informática según la reivindicación 19,

en el que el ordenador servidor destruye el mapa en respuesta a un PIN secreto no válido, a una denegación del permiso por parte del usuario y a la conclusión de la transacción.

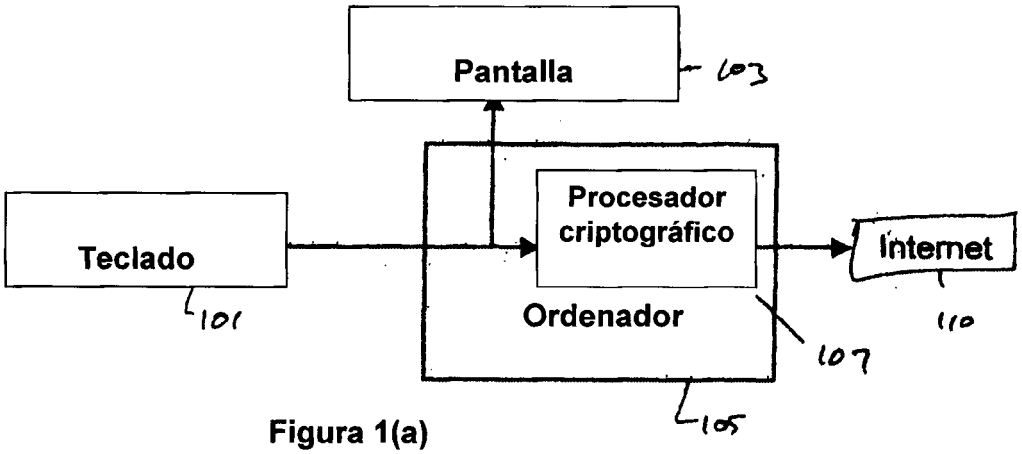

Figura 1(a)

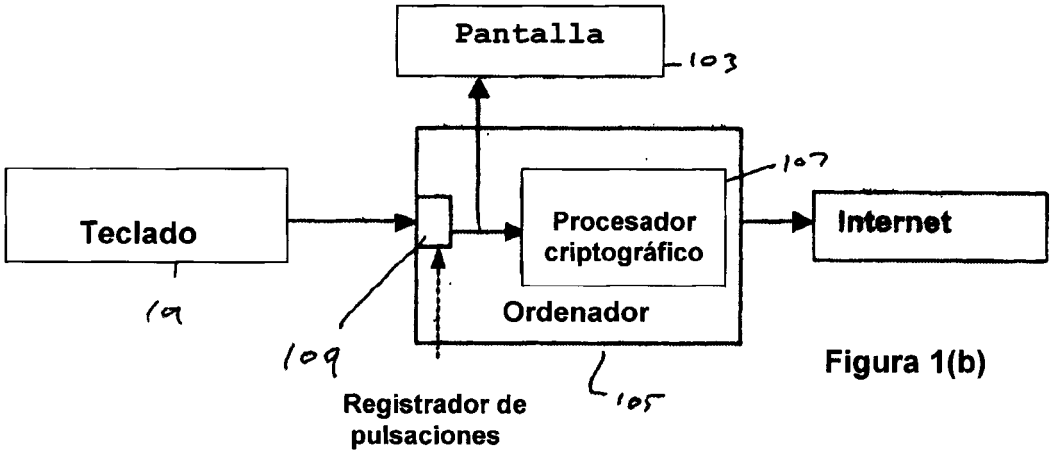

Figura 1(b)

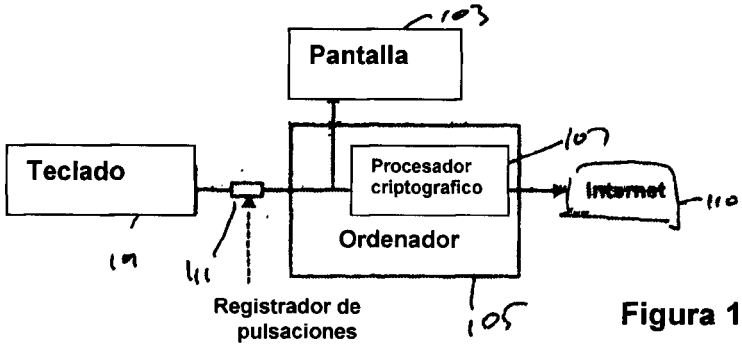

Figura 1(c)

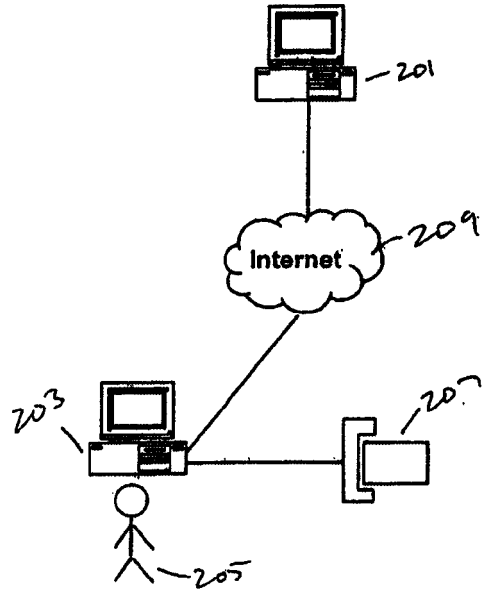

Figura 2(a)

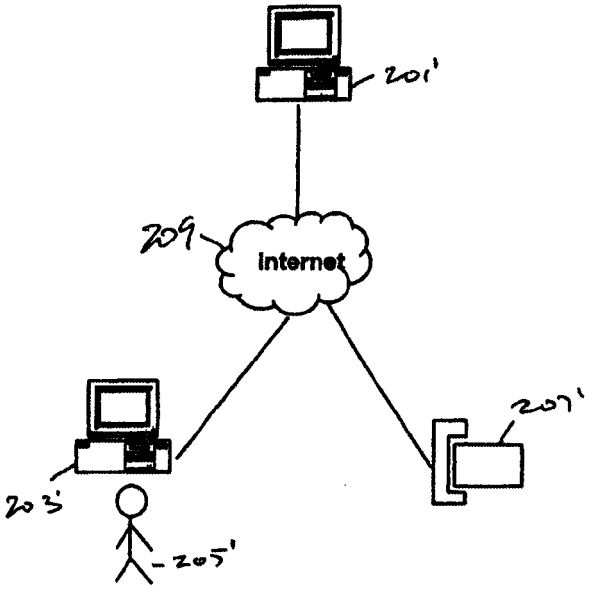

Figura 2(b)

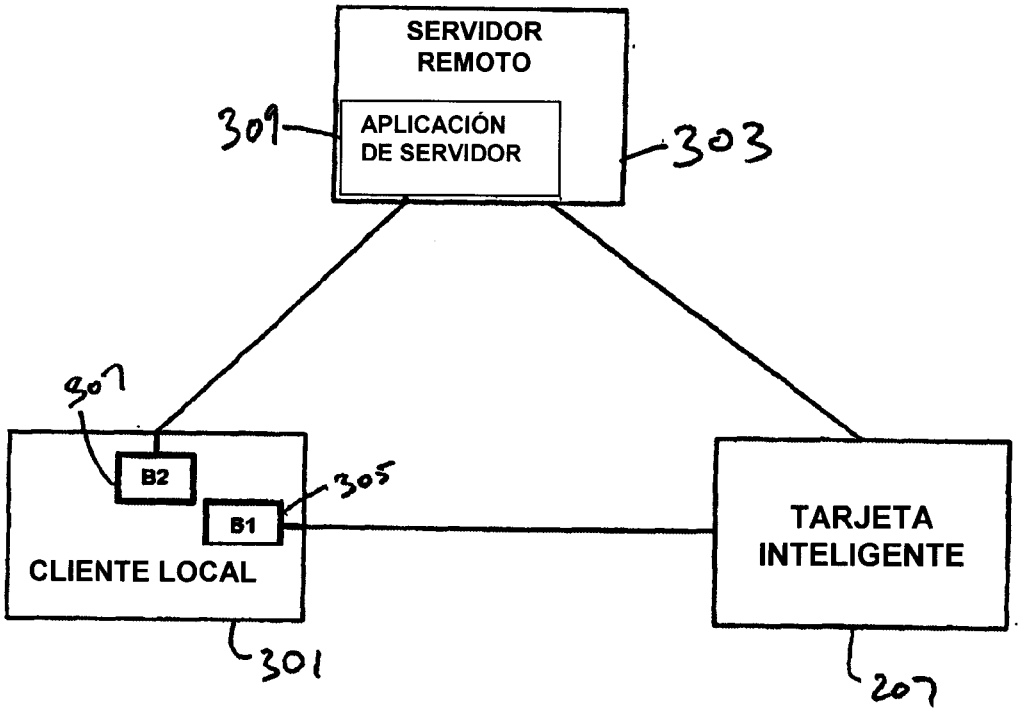
SERVIDOR
REMOTO
APLICACIÓN
DE SERVIDOR
309
303
307
B2
B1
305
CLIENTE LOCAL
301
TARJETA
INTELIGENTE
207

Figura 3

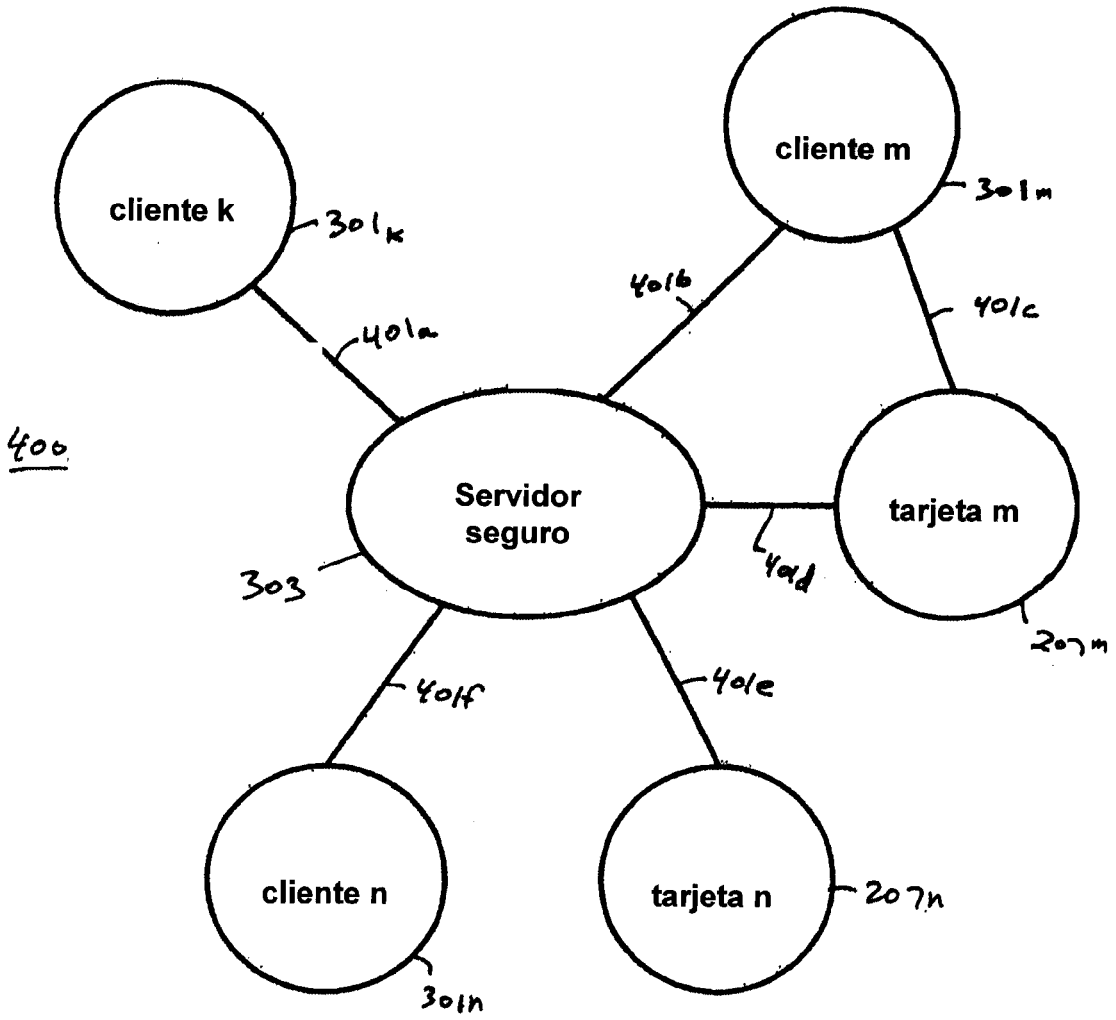
cliente k
301k
cliente m
301m
401a
401b
401c
400
Servidor seguro
303
tarjeta m
401d
207m
401f
401e
cliente n
301n
tarjeta n
207n

Figura 4

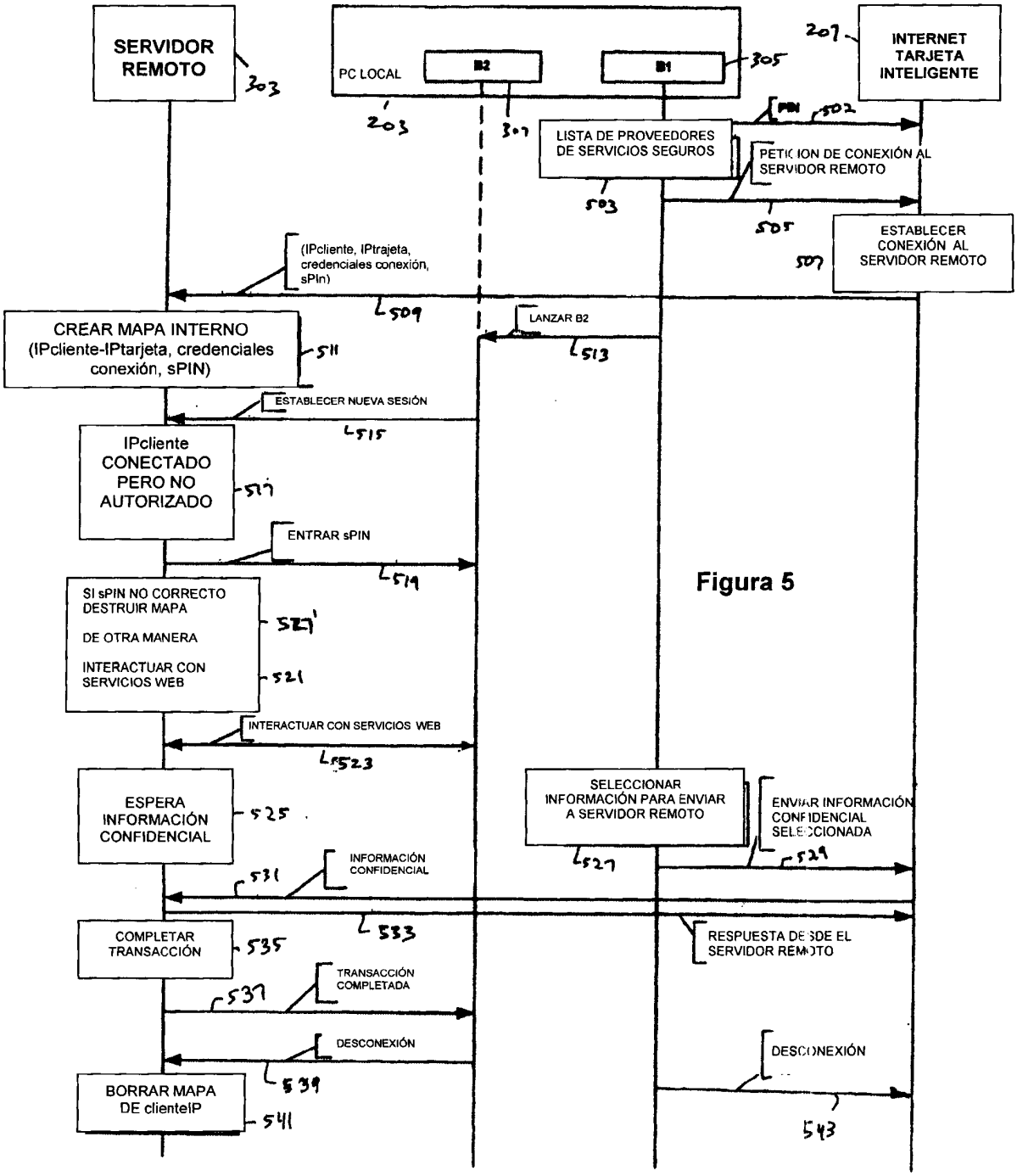
SERVIDOR REMOTO
303
PC LOCAL
B2
B1
305
203
307
INTERNET TARJETA INTELIGENTE
207
PIN
502
LISTA DE PROVEEDORES DE SERVICIOS SEGUROS
503
PETICION DE CONEXIÓN AL SERVIDOR REMOTO
505
ESTABLECER CONEXIÓN AL SERVIDOR REMOTO
507
(IPcliente, IPtrajeta, credenciales conexión, sPin)
509
CREAR MAPA INTERNO (IPcliente-IPtarjeta, credenciales conexión, sPIN)
511
LANZAR B2
513
ESTABLECER NUEVA SESIÓN
515
IPcliente CONECTADO PERO NO AUTORIZADO
517
ENTRAR sPIN
519
SI sPIN NO CORRECTO DESTRUIR MAPA
DE OTRA MANERA
INTERACTUAR CON SERVICIOS WEB
521
INTERACTUAR CON SERVICIOS WEB
523
ESPERA INFORMACIÓN CONFIDENCIAL
525
SELECCIONAR INFORMACIÓN PARA ENVIAR A SERVIDOR REMOTO
527
ENVIAR INFORMACIÓN CONFIDENCIAL SELECCIONADA
529
INFORMACIÓN CONFIDENCIAL
531
533
COMPLETAR TRANSACCIÓN
535
RESPUESTA DESDE EL SERVIDOR REMOTO
TRANSACCIÓN COMPLETADA
537
DESCONEXIÓN
539
DESCONEXIÓN
543
BORRAR MAPA DE clienteIP
541

Figura 5

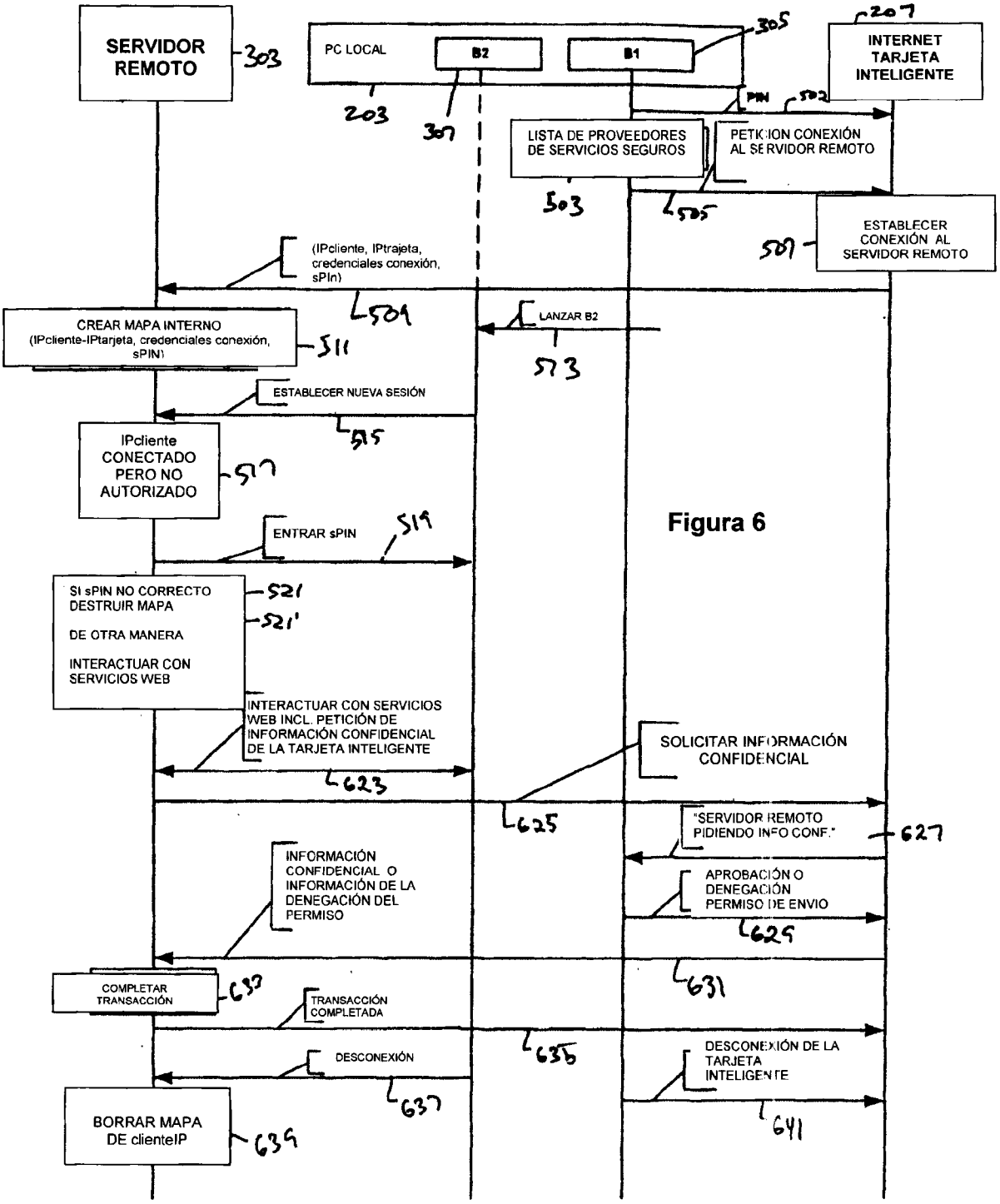
SERVIDOR REMOTO
303
PC LOCAL
B2
B1
305
INTERNET TARJETA INTELIGENTE
207
203
307
PIN
502
LISTA DE PROVEEDORES DE SERVICIOS SEGUROS
PETICION CONEXIÓN AL SERVIDOR REMOTO
503
505
ESTABLECER CONEXIÓN AL SERVIDOR REMOTO
507
(IPcliente, IPtrajeta, credenciales conexión, sPIn)
509
CREAR MAPA INTERNO (IPcliente-IPtarjeta, credenciales conexión, sPIN)
511
LANZAR B2
513
ESTABLECER NUEVA SESIÓN
515
IPcliente CONECTADO PERO NO AUTORIZADO
517
ENTRAR sPIN
519
SI sPIN NO CORRECTO DESTRUIR MAPA
521
DE OTRA MANERA
521'
INTERACTUAR CON SERVICIOS WEB
INTERACTUAR CON SERVICIOS WEB INCL. PETICIÓN DE INFORMACIÓN CONFIDENCIAL DE LA TARJETA INTELIGENTE
623
SOLICITAR INFORMACIÓN CONFIDENCIAL
625
"SERVIDOR REMOTO PIDIENDO INFO CONF."
627
INFORMACIÓN CONFIDENCIAL O INFORMACIÓN DE LA DENEGACIÓN DEL PERMISO
APROBACIÓN O DENEGACIÓN PERMISO DE ENVIO
629
631
COMPLETAR TRANSACCIÓN
633
TRANSACCIÓN COMPLETADA
635
DESCONEXIÓN
637
DESCONEXIÓN DE LA TARJETA INTELIGENTE
641
BORRAR MAPA DE clienteIP
639

Figura 6