(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 361 074**

(51) Int. Cl.:
G06F 21/04 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04010225 .3**
(96) Fecha de presentación : **29.04.2004**
(97) Número de publicación de la solicitud: **1473615**
(97) Fecha de publicación de la solicitud: **03.11.2004**

(54) Título: **Comunicación segura con un teclado.**

(30) Prioridad: **02.05.2003 US 428675**

(45) Fecha de publicación de la mención BOPI:
13.06.2011

(45) Fecha de la publicación del folleto de la patente:
13.06.2011

(73) Titular/es: **MICROSOFT CORPORATION**
One Microsoft Way
Redmond, Washington 98052, US

(72) Inventor/es: **Peinado, Marcus y**
Benaloh, Josh

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Comunicación segura con un teclado.

Campo de la invención

La presente invención está relacionada en general con el campo de la seguridad informática. Más en particular, la invención versa acerca del uso seguro de un teclado en un canal que comunicaciones que puede estar sometido a la interceptación o a otros tipos de manipulación.

Antecedentes de la invención

Un teclado comunica datos introducidos por un usuario a un dispositivo electrónico, como un ordenador. Cuando un usuario pulsa una tecla del teclado, el teclado genera datos representativos de la tecla particular que se pulsó (por ejemplo, el código ASCII para la letra “e”), y estos datos son recibidos por un componente del ordenador, tal como un controlador de dispositivo. Acto seguido, el controlador de dispositivo presenta los datos a cualquier programa que esté ejecutándose en el ordenador que reciba la entrada en ese momento (por ejemplo, poniendo los datos en la memoria intermedia de entrada para cualquier programa de aplicación que esté activo).

Un programa que surge en el uso de un teclado para recibir datos es cuando los datos son sensibles o sea preciso por otros motivos mantenerlos secretos. Por ejemplo, una aplicación segura (o un servicio seguro de un sistema operativo) puede pedir al usuario que introduzca una contraseña, que generalmente no debería ser divulgada al público general. Sin embargo, la ruta que conduce desde el teclado hasta el componente lógico que recibirá los datos no es segura, dado que hay varias oportunidades para interceptar los datos. Por ejemplo, los datos se desplazarán a menudo por un bus que está sometido a rastreos, y serán gestionados por un controlador de dispositivo que puede estar sujeto a manipulaciones (o a que el sistema operativo permita que sea sustituido con un controlador no seguro de dispositivo que almacene y divulgue la información que gestiona el controlador). En otras palabras, hay varias oportunidades de observar o manipular datos secretos en ruta desde el teclado a su destino definitivo.

En general, es posible cifrar los datos para la transmisión entre dos componentes que están conectados por medio de un canal no seguro. Sin embargo, muchas técnicas de cifrado no pueden aplicarse fácilmente en el contexto de un teclado, debido a diversos factores, como las cuestiones de la gestión de claves, la posibilidad de ataques de reinyección y el hecho de que el abanico relativamente pequeño de datos que puede ser generado por un teclado haría que un cifrado ordinario en las comunicaciones del teclado fuera relativamente fácil de romper si puede interceptarse una muestra de tamaño moderado de la cifra.

En vista de lo anterior, existe la necesidad de una técnica que facilite la comunicación segura con un teclado.

El documento EP-A-1 286 242 da a conocer un dispositivo de cifrado interconectado entre un dispositivo de entrada y un decodificador del dispositivo de entrada. Los dispositivos cifradores pueden ser controlados para que operen en un modo normal, en el que los datos pasan inalterados, y un modo seguro, en el que los datos son cifrados. Un caso útil dado a conocer por el documento se relaciona con la introducción de un número de identificación personal (PIN).

G. Treat: “Keyboard encryption”, IEEE Potentials, vol. 21, nº 3, agosto de 2002 – septiembre de 2002, páginas 40 a 42, se relaciona con el cifrado de datos de teclado, ya sea usando un dispositivo intercambiable entre el teclado y el ordenador, o usando un microcontrolador modificado en el teclado y componentes lógicos de decodificación cargados en un chip de BIOS existente del ordenador.

Resumen de la invención

El objeto de la presente invención es evitar los ataques de inyección en un canal de comunicaciones cifradas entre un teclado y un componente lógico de un ordenador.

Este objeto se resuelve con la materia de las reivindicaciones independientes.

Las realizaciones preferentes están definidas por las reivindicaciones dependientes.

La presente invención proporciona una técnica para una comunicación segura entre dos componentes por medio de un canal no seguro de comunicaciones. La técnica usa un modelo de cifrado que está particularmente bien adaptado para un teclado, y que aborda problemas que existirían en la aplicación de un modelo de cifrado estándar a un teclado.

Un teclado según la invención almacena una clave y un valor constante que se usa para la inicialización del modelo de cifrado. Un componente (por ejemplo, una aplicación que se ejecuta en un ordenador) almacena la misma clave y el mismo valor constante que se almacenan en el teclado. Para iniciar una sesión segura entre el componente y el teclado, cada uno genera un valor de uso único, y después intercambian el valor de uso único entre sí, de modo que el teclado y el componente estén en posesión de ambos valores de uso único. El teclado y el componente calculan

entonces dos valores iniciales, cada uno de los cuales se basa en los dos valores de uso único, la clave y el valor constante. Por ejemplo, puede crearse el primer valor inicial usando el algoritmo CBC-3DESMAC, en el que el algoritmo CBC-3DESMAC usa el valor constante almacenado como su valor inicial de encadenamiento y aplica la clave a un mensaje creado en base a los dos valores de uso único. (CBC-3DESMAC se refiere a la aplicación de un cifrado triple según el algoritmo Estándar de Cifrado de Datos (DES) con encadenamiento de bloques de cifrado y al uso del bloque final de la cifra para crear un Código de Autenticación de Mensajes (MAC)). Preferentemente, el segundo valor inicial se crea invirtiendo los bits del primer valor inicial (es decir, llevando a cabo una operación de "o exclusivo" entre el primer valor inicial y el número 0xffffffffffffffff). Dado que el teclado y el componente calculan los valores iniciales primero y segundo de la misma manera, ambos están en posesión de los mismos dos valores iniciales.

En una realización preferente alternativa, el teclado y el componente están equipados con dos valores constantes, y los valores iniciales primero y segundo pueden ser creados aplicando el algoritmo CBC-3DESMAC al mensaje que se basa en ambos valores de uso único, usando la primera constante para crear el primer valor inicial, y la segunda constante para crear el segundo valor inicial.

Una vez que han sido creados los valores iniciales primero y segundo, el teclado está listo para comunicar datos cifrados, y el componente que recibirá los datos está lista para descifrar y verificar los datos. Cuando se introducen datos en el teclado, el teclado cifra los datos en base al primer valor inicial y a la clave. Preferentemente, el teclado cifra los datos con la clave anteriormente mencionada usando CBC-3DES (triple DES con encadenamiento de bloques de cifrado), usándose el primer valor inicial para cebar la cadena de bloques de cifrado. El teclado crea también, preferentemente, un MAC para cada unidad de datos usando el algoritmo CBC-3DESMAC, en el que el algoritmo CBC-3DESMAC aplica la clave anteriormente mencionada y usa el segundo valor inicial para cebar la cadena de bloques de cifrado. Preferentemente, se cifra cada pulsación de tecla en un bloque de cifrado separado, y toda la corriente de datos generados en el teclado durante una sesión constituye una cadena de bloques de cifrado, dado que esta técnica permite que la misma pulsación de tecla (por ejemplo, la letra "e") aparezca como una cifra diferente, dependiendo de la pulsación de tecla que la precedió.

Una vez que los datos cifrados y el o los MAC han sido recibidos en el componente receptor, el componente receptor usa la clave anteriormente mencionada y los valores iniciales primero y segundo para descifrar y verificar los datos recibidos.

Más abajo se describen otras características de la invención.

Breve descripción de los dibujos

El resumen anterior, así como la siguiente descripción detallada de las realizaciones preferentes, se entiende mejor como se lee en conjunto con los dibujos adjuntos. Con el fin de ilustrar la invención, se muestran en los dibujos construcciones ejemplares de la invención; sin embargo, la invención no está limitada a los procedimientos e instrumentaciones dadas a conocer. En los dibujos:

la FIG. 1 es un diagrama de bloques de un entorno informático ejemplar en el que pueden implementarse aspectos de la invención;

la FIG. 2 es un diagrama de bloques de un primer entorno ejemplar en el que la comunicación entre un teclado y un componente puede tener lugar en un canal no seguro;

la FIG. 3 es un diagrama de bloques de un segundo entorno ejemplar en el que la comunicación entre un teclado y un componente puede tener lugar en un canal no seguro;

la FIG. 4 es un diagrama de bloques de un teclado y un componente que han sido configurados para una comunicación segura y que intercambian valores de uso único según aspectos de la invención;

la FIG. 5 es un diagrama de flujo de un procedimiento para entablar una sesión de comunicaciones seguras entre un teclado y un componente; y

la FIG. 6 es un diagrama de bloques de un primer entorno ejemplar en el que teclados y componentes pueden distribuirse para entablar comunicaciones seguras según aspectos de la invención.

Descripción detallada de la invención

Disposición informática ejemplar

La FIG. 1 muestra un entorno informático ejemplar en el que pueden implementarse aspectos de la invención. El entorno informático ejemplar 100 es solo un ejemplo de un entorno informático adecuado y no se pretende que sugiera ninguna limitación en cuanto al alcance del uso o la funcionalidad de la invención. Tampoco debiera interpretarse que el entorno informático 100 tenga ninguna dependencia ni requisito en cuanto un componente cualquiera o a la combinación de los componentes ilustrados en el entorno informático ejemplar 100.

La invención es operativa con numerosos entornos o configuraciones informáticos diversos de uso general o de uso especial. Ejemplos de sistemas, entornos y/o configuraciones informáticos bien conocidos que pueden ser adecuados para su uso con la invención incluyen, sin limitación, ordenadores personales, ordenadores servidores, dispositivos de bolsillo o portátiles, sistemas multiprocesador, sistemas basados en microprocesadores, convertidores de señales, aparatos electrónicos de consumo programables, ordenadores personales de red, miniordenadores, ordenadores centrales, sistemas integrados, entornos informáticos distribuidos que incluyen cualquiera de los sistemas o dispositivos anteriores, y similares.

La invención puede ser descrita en el contexto general de instrucciones ejecutables por ordenador, tales como módulos de programa que son ejecutados por un ordenador. Generalmente, los módulos de programa incluyen rutinas, programas, objetos, componentes, estructuras de datos, etc., que llevan a cabo tareas particulares o implementan tipos particulares de datos abstractos. La invención también puede ser practicada en entornos informáticos distribuidos en los que las tareas son llevadas a cabo por dispositivos remotos de proceso que están unidos mediante una red de comunicaciones u otro medio de transmisión de datos. En un entorno informático distribuido, los módulos de programa y otros datos pueden estar situados en medios de almacenamiento informático tanto locales como remotos, incluyendo los dispositivos de almacenamiento de memoria.

Con referencia a la FIG. 1, un sistema ejemplar para la implementación de la invención incluye un dispositivo informático ejemplar de uso general en forma de ordenador 110. Los componentes del ordenador 110 pueden incluir, sin limitación, una unidad 120 de proceso, una memoria 130 de sistema y un bus 121 de sistema que acopla a diversos componentes del sistema, incluyendo la memoria de sistema, a la unidad 120 de proceso. El bus 121 de sistema puede ser de cualquiera de varios tipos de estructuras de bus, incluyendo un bus de memoria o un controlador de memoria, un bus de periféricos y un bus local usando cualquiera de entre una variedad de arquitecturas de bus. A título de ejemplo, y no de limitación, tales arquitecturas incluyen el bus de Arquitectura Industrial Normalizada (ISA), el bus con arquitectura de microcanal (MCA), el bus ISA mejorado (EISA), el bus local de la Asociación de Normativa Electrónica de Vídeo (VESA) y el bus de Interconexión de Componentes Periféricos (PCI), también denominado bus de entresuelo. El bus 121 de sistema también puede implementarse como una conexión punto a punto, una matriz de conmutación o similar, entre los dispositivos de comunicaciones.

Típicamente, el ordenador 110 incluye una variedad de medios legibles por ordenador. Los medios legibles por ordenador pueden ser cualquier medio disponible al que pueda acceder el ordenador 110 e incluyen tanto los medios volátiles como los no volátiles, los medios extraíbles y los no extraíbles. A título de ejemplo, y no de limitación, los medios legibles por ordenador pueden comprender medios de almacenamiento informático y medios de comunicaciones. Los medios de almacenamiento informático incluyen medios volátiles y no volátiles, extraíbles y no extraíbles implementados en cualquier procedimiento o tecnología para el almacenamiento de información, tales como instrucciones legibles por ordenador, estructuras de datos, módulos de programas u otros datos. Los medios de almacenamiento informático incluyen, sin limitación, RAM, ROM, EEPROM, memoria flash u otra tecnología de memoria, CD-ROM, discos versátiles digitales (DVD) u otro almacenamiento de discos ópticos, casetes magnéticas, cinta magnética, almacenamiento en discos magnéticos u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y al que pueda acceder el ordenador 110. Típicamente, los medios de comunicaciones plasman instrucciones legibles por ordenador, estructuras de datos, módulos de programas u otros datos en una señal modulada de datos, como una onda portadora u otro mecanismo de transporte, e incluyen cualquier medio de suministro de la información. La expresión “señal modulada de datos” significa una señal que tiene una o más de sus características configuradas o cambiadas de tal manera que codifican la información de la señal. A título de ejemplo, y no de limitación, los medios de comunicaciones incluyen medios cableados, como una red cableada o una conexión de cableado directo, y medios inalámbricos, como medios acústicos, de RF, infrarrojos y otros medios inalámbricos. También deberían incluirse combinaciones de cualquiera de los anteriores en el abanico de los medios legibles por ordenador.

La memoria 130 de sistema incluye medios de almacenamiento del dispositivo informático en la forma de memoria volátil y/o no volátil, como la memoria de solo lectura (ROM) 131 y la memoria de acceso directo (RAM) 132. Típicamente, un sistema básico 133 de entrada salida (BIOS), que contiene rutinas básicas que contribuyen a transferir información entre elementos dentro del ordenador 110, como durante el arranque, está almacenado en la ROM 131. Típicamente, la RAM 132 contiene datos y/o módulos de programa que son inmediatamente accesibles a la unidad 120 de proceso y/o son operados por la misma en ese momento. A título de ejemplo, y no de limitación, la FIG. 1 ilustra un sistema operativo 134, programas 135 de aplicación, otros módulos 136 de programa y datos 137 de programa.

El ordenador 110 puede también incluir otros medios de almacenamiento informático extraíbles/no extraíbles, volátiles/no volátiles. A título de ejemplo únicamente, la FIG. 1 ilustra una unidad 140 de disco duro que lee o escribe en medios magnéticos no extraíbles no volátiles, una unidad 151 de disco magnético que lee o escribe a un disco magnético 152 extraíble no volátil, y una unidad 155 de disco óptico que lee o escribe en un disco óptico 156 extraíble no volátil, como un CD ROM u otros medios ópticos. Otros medios de almacenamiento informático extraíbles/no extraíbles volátiles/no volátiles que pueden usarse en el entorno operativo ejemplar incluyen, sin limitaciones, casetes de cinta magnética, tarjetas de memoria flash, discos versátiles digitales, cinta de vídeo digital, RAM de estado sólido, ROM de estado sólido y similares. Típicamente, la unidad 141 de disco duro está conectada

al bus 121 de sistema por medio de una interfaz de memoria no extraíble, como la interfaz 140, y, típicamente, una unidad 151 de disco magnético y una unidad 155 de disco óptico están conectadas al bus 121 de sistema por medio de una interfaz de memoria extraíble como la interfaz 150.

Las unidades y sus medios de almacenamiento informático asociados expuestos más arriba e ilustrados en la FIG. 1 proporcionan almacenamiento de instrucciones legibles por ordenador, estructuras de datos, módulos de programa y otros datos para el ordenador 110. En la FIG. 1, por ejemplo, se ilustra que la unidad 141 de disco duro almacena el sistema operativo 144, programas 145 de aplicación, otros módulos 146 de programa y datos 147 de programa. Se hace notar que estos componentes pueden ser iguales o diferentes que el sistema operativo 134, los programas 135 de aplicación, otros módulos 136 de programa y datos 137 de programa. Al sistema operativo 144, a los programas 145 de aplicación, a otros módulos 146 de programa y a los datos 147 de programa se les dan números diferentes aquí para ilustrar que, como mínimo, son copias diferentes. Un usuario puede introducir órdenes e información en el ordenador 20 a través de dispositivos de entrada, como un teclado 162 y un dispositivo 161 de puntero, denominado comúnmente ratón, bola de mando del cursor o almohadilla táctil. Otros dispositivos de entrada (no mostrados) pueden incluir un micrófono, una palanca de juegos, un mando de juegos, una antena parabólica, un escáner o similares. Estos y otros dispositivos se conectan a menudo a la unidad 120 de proceso por medio de una interfaz 160 de entrada de usuario que está acoplada al bus de sistema, pero puede tener conexión por medio de otras estructuras de interfaz y de bus, como un puerto paralelo, un puerto de juegos o, en particular, un puerto USB. Un monitor 191 u otro tipo de dispositivo de visionado también está conectado al bus 121 de sistema por medio de una interfaz, como una interfaz 190 de vídeo. Además del monitor, los ordenadores también pueden incluir otros dispositivos periféricos de salida, como los altavoces 197 y la impresora 196, que pueden estar conectados por medio de una interfaz 190 de periféricos de salida.

El ordenador 110 puede operar en un entorno de red usando conexiones lógicas a uno o más ordenadores remotos, como un ordenador remoto 180. El ordenador remoto 180 puede ser un ordenador personal, un servidor, un dispositivo de encaminamiento, un PC de red, un dispositivo cooperativo u otro nodo de red común, y típicamente incluye muchos o todos los elementos descritos más arriba con respecto al ordenador 110, aunque en la FIG. 1 solo se ha ilustrado un dispositivo 181 de almacenamiento de memoria. Las conexiones lógicas representadas en la FIG. 1 incluyen una red 171 de área local (LAN) y una red 173 de área amplia (WAN), pero pueden incluir también otras redes. Tales entornos de red son comunes en oficinas, redes de ordenadores de ámbito empresarial, intranets e Internet.

Cuando se usa en un entorno de red LAN, el ordenador 110 está conectado a la LAN 171 por medio de una interfaz o un adaptador 170 de red. Cuando se usa en un entorno de red WAN, el ordenador 110 incluye típicamente un módem 172 u otros medios para establecer comunicaciones en la WAN 173, como Internet. El módem 172, que puede ser interno o externo, puede estar conectado al bus 121 de sistema por medio de la interfaz 160 de entrada de usuario u otro mecanismo apropiado. En un entorno de red, los módulos de programa representados con respecto al ordenador 110, o porciones de los mismos, pueden almacenarse en un dispositivo de almacenamiento remoto de memoria. A título de ejemplo, y no de limitación, la FIG. 1 ilustra que los programas remotos 185 de aplicación residen en el dispositivo 181 de memoria. Se apreciará que las conexiones de red mostradas son ejemplares y que pueden usarse otros medios de establecimiento de un vínculo de comunicaciones entre los ordenadores.

Seguridad de la comunicación entre un teclado y un componente

La invención aborda el problema de cómo puede usarse un teclado para comunicarse de forma segura con un componente que requiere la entrada procedente del teclado. La FIG. 2 muestra un escenario ejemplar de tal comunicación. En la FIG. 2, el teclado 162 se comunica con el componente 204. El componente 204 puede ser cualquier tipo de componente; por ejemplo, un programa que se esté ejecutando en un ordenador, un componente físico, etc. La comunicación entre el teclado 162 y el componente 202 pasa a través de un canal de comunicaciones que incluye al menos alguna porción no segura 204. Es decir, según pasan a través de algún canal los datos que representan las pulsaciones de teclas en su recorrido desde el teclado 162 hasta el componente 202, puede haber alguna oportunidad de que un tercero intercepte o manipule los datos. Esta interceptación o manipulación puede ser un problema si, por ejemplo, la información que se está mecanografiando en el teclado 162 es una contraseña secreta que no debiera ser revelada al público general.

La FIG. 3 muestra un escenario particular en el que se desea una comunicación segura entre un teclado y un componente. En la FIG. 3, el teclado 162 se usa para proporcionar una entrada al componente lógico que se está ejecutando en el ordenador 110. En el ejemplo de la FIG. 3, el teclado 162 es un teclado adaptado para su uso con un Bus Serie Universal (USB) 302. (En aras de la brevedad, se denominará a ese teclado teclado USB). El teclado 162 recibe pulsaciones de tecla, y pone los bytes representativos de esas pulsaciones de teclas en el USB 302, recogiendo los bytes el controlador 304 de USB. Acto seguido, el controlador 304 comunica esos bytes a su destino final, que, en el ejemplo de la FIG. 3, es el componente lógico 306. El componente lógico 306 es un ejemplo de componente (mostrado en la FIG. 2).

En el ejemplo de la FIG. 3, hay dos sistemas operativos 134(1) y 134(2) funcionando en el ordenador 110. El sistema operativo 134(1) es un sistema operativo típico, como MICROSOFT WINDOWS XP, Unix, Linux, Solaris, etc. El sistema operativo 134(2) es un sistema operativo de “alta seguridad” que se usa para aplicaciones en las que se tiene confianza. Por ejemplo, el sistema operativo 134(2) puede estar asociado con una memoria “de cortina” que no es accesible fuera del sistema operativo 134(2), y el sistema operativo 134(2) puede almacenar información secreta (por ejemplo, claves criptográficas, contraseñas, etc.) en esa memoria de cortina, de modo que solo ciertas aplicaciones en las que se tiene confianza a las que se les permite ejecutarse bajo el sistema operativo 134(2) sean capaces de leer esa información secreta. El sistema operativo 134(2) es de “alta seguridad” en el sentido de que el público tiene derecho a un nivel muy alto de seguridad de que llevará a cabo su función correctamente; es decir, si la protección de información secreta es una de las funciones deseadas del sistema operativo 134(2), el público tiene derecho a un nivel muy alto de seguridad de que el sistema operativo 134(2) no divulgará esa información secreta. Parte de ser capaz de proteger información secreta puede incluir ser capaz de recibir secretos mecanografiados (por ejemplo, contraseñas) sin divulgar estos secretos al mundo exterior. El sistema operativo 134(2) puede no confiar en que el controlador 304 gestione tal información secreta, ya que el controlador 304 está bajo el control del sistema operativo 134(1) (y el sistema operativo 134(1) podría permitir que un pirata informático leyera información directamente del USB 302, o que lo sustituyera con un controlador maligno que almacenase y revelase la información secreta). Así, el sistema operativo 134(2) necesita una forma de recibir información del teclado 162 a través del sistema operativo 134(1) sin preocupación de que la información secreta sea divulgada por acciones que surjan en el sistema operativo 134(1).

Debería entenderse que, aunque el ejemplo de la FIG. 3 muestra que el teclado 162 se comunica con el ordenador 110 a través de un Bus Serie Universal 302, los escenarios descritos más arriba se aplican con independencia del medio exacto mediante el cual el teclado 162 se comunique con el ordenador 110 y que, por ello, la invención no está limitada a los teclados USB.

La FIG. 4 muestra la forma en la que el teclado 162 y el componente 202 pueden ser configurados para participar en una comunicación segura a través de un canal no seguro. El teclado 162 y el componente 202 almacenan cada uno una copia de la clave criptográfica 402. Además, el teclado 162 y el componente 202 almacenan, preferentemente, un valor constante 404, que se usa como valor inicial para una técnica criptográfica particular preferente, tal como se describe en particular más abajo. En una realización adicional preferente, el teclado 162 y el componente 202 pueden almacenar (además de la clave) dos valores constantes en lugar de uno; estos dos valores constantes pueden usarse en una técnica criptográfica descrita más abajo. El teclado 162 puede contener, por ejemplo, un semiconductor no volátil incorporado que almacene la clave 402 y la constante 404, o puede tener un puerto que reciba un medio de almacenamiento extraíble en el que estén almacenadas la clave 402 y la constante 404. En el caso en el que el componente 202 es un componente lógico, la clave 402 y la constante 404 pueden estar almacenadas en el espacio de datos del componente 202. Sin embargo, se entenderá que la invención no está limitada a ninguna manera particular de almacenamiento de la clave 402 y la constante 404.

Al inicio de la comunicación segura entre el teclado 162 y el componente 202, el teclado 162 y el componente 202 pueden generar e intercambiar valores de uso único. Es decir, el teclado 162 genera el valor 412 de uso único y envía el valor 412 de uso único al componente 202. El componente 202 genera el valor 414 de uso único y envía el valor 414 de uso único al teclado 162. Según se conoce en la técnica, un valor de uso único es un dato que se usa en las aplicaciones criptográficas, a menudo para autenticar criptográficamente una entidad, o para cebar una sesión de cifrado con un elemento no fácilmente reproducible del cual puede hacerse dependiente el cifrado. Los valores 412 y 414 de uso único pueden usarse para crear valores iniciales para el cifrado y la autenticación de los datos transmitidos entre el teclado 162 y el componente 202, como se describirá más en particular más abajo.

Procedimiento del envío seguro de datos de un teclado a un componente

La FIG. 5 muestra un procedimiento mediante el cual el teclado 162 y el componente 202 pueden entablar una sesión en la que el componente 202 recibe datos con seguridad procedentes del teclado 162. El procedimiento 5 contempla tanto el cifrado (que protege contra la interceptación de los datos transmitidos) como la autenticación (que protege contra la modificación de los datos transmitidos). Sin embargo, se entenderá que pueden usarse el cifrado o la autenticación por sí solos, dependiendo de los requisitos de seguridad de la transmisión. Por ejemplo, si puede tolerarse la modificación de los datos, pero no puede tolerarse la interceptación, puede usarse únicamente el cifrado. En cambio, si puede tolerarse la interceptación de los datos, pero no puede tolerarse la modificación de los datos, puede usarse únicamente la autenticación.

Inicialmente, el teclado 162 y el componente 202 intercambian 502 los valores de uso único. Por ejemplo, tal como se ha descrito más arriba en conexión con la FIG. 4, el teclado 162 puede generar el valor 412 de uso único y enviárselo al componente 202, y el componente 202 puede generar el valor 414 de uso único y enviárselo al teclado 162. Las técnicas para la generación de valores únicos son conocidas en la técnica, y, por ello, no se describen en detalle en el presente documento. Como ejemplos, los valores 412 y 414 de uso único podrían generarse en base a un número aleatorio, al contenido de alguna zona de memoria, a la hora, la temperatura, la fase de la luna, etc., o a cualquier otro factor que sea probable que cambie a menudo y tenga un abanico suficiente que sea improbable que ni el teclado ni el componente 202 produzcan el mismo valor de uso único dos veces.

Una vez que se intercambian 502 los valores 412 y 414 de uso único, el teclado 162 y el componente 202 están cada uno en posesión de ambos valores de uso único. El teclado 162 y el componente 202 usan entonces una fórmula comúnmente acordada para calcular 504 dos valores iniciales —IV_c e IV_m— como funciones de ambos valores de uso único y de la clave 402. Es decir, si K = clave 402, N_1 = valor 412 de uso único y N_2 = valor 414 de uso único, entonces

$$IV\_c = f\left(K, N_1, N_2\right);$$

e

$$IV\_m = g\left(K, N_1, N_2\right).$$

Las funciones f y g pueden ser funciones cualesquiera. En una realización preferente,

$$f\left(K, N_1, N_2\right) = \text{CBC-3DESMAC}_{\text{K}}\left(const\_IV, N_1 \mid N_2\right);$$

y

$$g\left(K, N_1, N_2\right) = f\left(K, N_1, N_2\right) xor\ 0xffffffffffffffff,$$

en las que const_IV es igual al valor constante 404 (mostrado en la FIG. 4). En una realización adicional preferente, en la que el teclado y el componente comparten dos valores constantes (por ejemplo const_IV_1 y const_IV_2), las funciones f y g pueden calcular, alternativamente, como sigue:

$$f\left(K, N_1, N_2\right) = \text{CBC-3DESMAC}_{\text{K}}\left(const\_IV\_1, N_1 \mid N_2\right);$$

y

$$g\left(K, N_1, N_2\right) = \text{CBC-3DESMAC}_{\text{K}}\left(const\_IV\_2, N_1 \mid N_2\right),$$

(El operador "|" significa concatenación, de modo que N_1 | N_2 es el valor resultante de concatenar N_1 con N_2. "xor" es la operación "o exclusivo" bit a bit, de modo que A xor B es el valor resultado de poner a "1" cualquier bit que sea un "1" ya sea en A o en B, pero no en ambos, y poner todos los demás bits a cero). CBC-3DESMAC$_K$(const_IV, N_1| N_2) es una función criptográfica cuyo significado es conocido en la técnica y está descrito con mayor detalle más abajo.

Una vez que han sido calculados IV_c e IV_m, puede comenzar la comunicación entre el teclado 162 y el componente 202. El teclado 162 recibe una pulsación de tecla, es decir, por parte de un operador, que pulsa una de las teclas (o cierta combinación de teclas, como <MAYÚSCULA> y "A" o <CTRL" y "A") (etapa 506). A continuación, el teclado cifra 508 la pulsación de tecla; preferentemente, el cifrado se basa en la clave 402 e IV_c. En una realización preferente, las pulsaciones de tecla se cifran usando el algoritmo CBC-3DES, siendo la clave 402 la clave y siendo IV_c el valor inicial. El CBC-3DES es un algoritmo criptográfico que es conocido en la técnica y está descrito con mayor detalle más abajo. Además, el teclado 162 calcula 510 un código de autenticación de mensajes (MAC) para la pulsación de tecla, en base, preferentemente, a la tecla 402 y a IV_m. En una realización preferente, el código de autenticación de mensajes se crea usando el algoritmo CBC-3DESMAC, siendo la clave 402 la clave y siendo IV_m el valor inicial. Tal como se ha hecho notar más arriba, el algoritmo CBC-3DESMAC es conocido en la técnica y está descrito con mayor detalle más abajo.

Una vez que el teclado ha creado tanto los datos cifrados de la pulsación de tecla como el MAC, el componente 202 recibe 512 los datos cifrados de la pulsación de tecla y el MAC procedentes del teclado 162 (etapa 512). Acto seguido, el componente 202 descifra 514 los datos usando la clave 402 e IV_c, y también verifica los datos usando la clave 402 e IV_m (etapa 514). El procedimiento vuelve luego a la etapa 506 para recibir la siguiente entrada del teclado.

<u>Las funciones criptográficas CBC-3DES y CBC-3DESMAC</u>

CBC-3DES es una función criptográfica que combina en estándar de cifrado de datos (DES) con el encadenamiento de bloques de cifrado (CBC). "3DES" significa que el algoritmo DES de cifrado se aplica a un bloque dado de datos tres veces ("triple DES"). El algoritmo DES cifra los datos aplicando una clave a los datos de una manera conocida. El algoritmo DES cifra un mensaje largo dividiendo el mensaje en bloques más pequeños y cifrando los bloques individuales. (Cuando se usa el algoritmo "triple DES", se aplica el algoritmo DES tres veces a cada bloque para producir la cifra para ese bloque). El algoritmo DES (y el triple DES) puede cifrar cada bloque de datos usando solo una clave; sin embargo, cuando se usa el encadenamiento de bloques de cifrado, el cifrado de un bloque está basado no solo en la clave, sino también en la cifra que fue producida por el cifrado del último bloque. Así, el cifrado de un bloque dado se basa en dos entradas: la clave y la cifra que resultó de cifrar el bloque anterior. Dado que el primer bloque de datos que se ha de cifrar no tiene ningún bloque "anterior", el procedimiento de encadenado de bloques de cifrado debe ser cebado con un "valor inicial"; es decir, el primer bloque de datos se cifra en base a la

clave y algún valor inicial. El valor inicial no se usa en el cifrado de los bloques subsiguientes, pero puede influir indirectamente en la forma en que esos bloques son cifrados (dado que la cifra del primer bloque se basa en el valor inicial, la cifra del segundo bloque se basa en la cifra del primer bloque, y así sucesivamente).

Teniendo en cuenta la exposición anterior, la expresión "CBC-3DES$_K$(IV, mensaje)" significa cifrar "mensaje" con la clave K usando el algoritmo triple DES y el encadenamiento de bloques de cifrado, siendo IV el valor inicial para la cadena de bloques de cifrado.

CBC-3DESMAC es una manera de usar el algoritmo CBC-3DES para producir un código de autenticación de mensajes (MAC). En particular, la expresión CBC-3DESMAC$_K$(IV, mensaje) significa que "mensaje" está cifrado con una clave K usando el algoritmo triple DES y el encadenamiento de bloques de cifrado y usando IV como valor inicial para la cadena de bloques de cifrado. Sin embargo, dado que el objetivo del algoritmo CBC-3DESMAC es únicamente producir un MAC para el mensaje en vez de una cifra compleja para el mensaje, solo se guarda el último bloque de la cifra, y los bloques restantes de la cifra pueden ser descartados. Este último bloque de la cifra puede ser usado como MAC, dado que —dadas incluso una clave constante y una constante IV— es improbable que mensajes diferentes produzcan el mismo bloque final (o, más precisamente, si cada bloque puede representar 2" valores diferentes, hay solo una probabilidad de 1 en 2" de que cualesquiera dos mensajes tengan el mismo bloque final).

Debería hacerse notar que la elección particular de CBC-3DES, así como la manera en la que se usa, son particularmente ventajosas para la comunicación cifrada con el teclado. Dado que el dominio de los mensajes que han de ser cifrados es pequeño (por ejemplo, del orden de 128 caracteres ASCII diferentes), el encadenamiento de bloques de cifrado resulta particularmente útil para evitar que se rompa el cifrado. Si se usase el cifrado a secas (sin encadenamiento), entonces, dentro de una sesión dada, cada carácter se cifraría a la misma cifra cada vez que se mecanografiara; por ejemplo, mecanografiar "e" produciría siempre la misma cifra. Haciendo una conjetura con cierta base (por ejemplo, usando el hecho de que "e" es la letra que aparece más a menudo en la lengua inglesa), tal cifrado podría romperse con facilidad. Encadenar toda la entrada de la sesión hace que el cifrado sea más difícil de romper, asegurando que los mismos datos puedan aparecer como cifras diferentes dependiendo dónde aparezcan en la corriente de entrada (por ejemplo, una "e" puede no siempre producir la misma cifra). Además, cambiando el cifrado para cada sesión creando un nuevo valor en base a valores de uso único evita que los observadores detecten patrones de uso que podrían usar para poner en peligro la seguridad (por ejemplo, si el primer texto mecanografiado en cada sesión es la contraseña, un observador podría capturar la cifra de la contraseña e iniciar un ataque de inyección). Además, el tamaño de los bloques de cifrado usados por el algoritmo DES es particularmente idóneo, dado que DES opera en bloques de 8 bytes, y la mayoría de los protocolos de teclado transmiten datos en bloques que pueden encajar en este tamaño (por ejemplo, el estándar USB también maneja bloques de 8 bytes, de modo que cada bloque USB puede caber en un bloques DES sin espacio desaprovechado). Sin embargo, debería entenderse que podría usarse cualquier otro cifrado de bloques, y que podrían aplicarse conceptos de encadenamiento similares al CBC a tal cifrado de bloques.

Debería hacerse notar también que, por las mismas razones que el modelo de cifrado descrito en el presente documento resulta particularmente idóneo para un teclado, ese modelo de cifrado es también idóneo para ciertos tipos adicionales de dispositivos de entrada, como un ratón (u otro dispositivo de puntero). Estos dispositivos de entrada comparten diversas características en común con un teclado, como un vocabulario pequeño y una capacidad limitada de ejecutar un algoritmo complicado de cifrado.

Uso ejemplar de un teclado que cifra datos

La FIG. 6 muestra un entorno ejemplar en el que puede usarse un teclado que lleva a cabo el cifrado con componentes que requieren una comunicación segura. En el ejemplo de la FIG. 6 el fabricante 602 fabrica una pluralidad de teclados 162(1), 162(2), ..., 162(n), y distribuye estos teclados para un uso público. Cada uno de los teclados 162(1), 162 (2), ..., 162(n) incorpora la tecla 402 y un valor constante 404 (mostrados en la FIG. 4) (o incorpora algún medio mediante el cual se pueda acceder externamente a la clave 402 y al valor constante 404, como por medio de un puerto para una memoria extraíble de semiconductores). El fabricante 604 produce componentes 202(1), 202(2), ..., 202(m) que se benefician de una comunicación segura con un teclado. Cada uno de los componentes 202(1), 202(2), ..., 202(n) incorpora la clave 402 y el valor constante 404 (o es capaz de recibir de alguna manera la clave y el valor constate). Los componentes 202(1), 202(2), ..., 202(m) pueden entonces recibir la entrada de los teclados 162(1), 162(2), ..., 162(n) a través de las técnicas descritas más arriba.

El fabricante 602 puede tener una relación preexistente con el fabricante 604, de modo que ambos fabricantes pueden acordar una clave 402 y una constante 404 que debería incorporarse para la comunicación segura. En un ejemplo, los fabricantes 602 y 604 son la misma entidad. En otro ejemplo, el fabricante 604 es un fabricante de componentes 202(1), 202(2), ..., 202(m) al que le gustaría que esos componentes fueran capaces de recibir datos de teclados seguros, y el fabricante 602 es un fabricante de teclados a quien el fabricante 604 ha considerado lo suficientemente digno de confianza para fabricar teclados para la comunicación segura con los componentes 202(1), 202(2), ..., 202(m), y para contener la clave 402 y/o la constante 404.

Debe hacerse notar que los ejemplos anteriores han sido proporcionados meramente con fines explicativos y de ninguna manera debe interpretarse que limiten la presente invención. Aunque la invención ha sido descrita con referencia a diversas realizaciones, se entiende que las palabras que se han usado en el presente documento son palabras de descripción e ilustración, no palabras de limitación. Además, aunque la invención ha sido descrita en el presente documento con referencia a medios, materiales y realizaciones particulares, no se contempla que la invención esté limitada a los particulares dados a conocer en el presente documento; antes bien, la invención se extiende a todas las estructuras, los procedimientos y los usos funcionalmente equivalentes, tales como los que estén dentro del alcance de las reivindicaciones adjuntas. Las personas expertas en la técnica, al tener el beneficio de las enseñanzas de esta memoria, pueden efectuar numerosas modificaciones a la misma, y pueden realizarse cambios sin apartarse del alcance y el espíritu de la invención en sus aspectos.

REIVINDICACIONES

1. Un procedimiento de comunicación con un teclado (162) que comprende:

la recepción, en un componente, de un primer valor (412) de uso único desde el teclado;

el envío, desde el componente (202), de un segundo valor de uso único al teclado;

la creación de un primer valor inicial y de un segundo valor inicial aplicando el algoritmo triple DES y el encadenamiento de bloques de cifrado a una combinación de dicho primer valor de uso único y dicho segundo valor de uso único, usando una clave y un tercer valor inicial que es conocido tanto al teclado como al componente;

la recepción, en un componente, de una pluralidad de datos que han sido cifrados con el algoritmo triple DES y el encadenamiento de bloques de cifrado usando la clave y el primer valor inicial procedente del teclado, estando incluida cada pulsación separada de tecla procedente de dicho teclado dentro de un dato separado de dicha pluralidad de datos, estando cifrado cada dato de la pluralidad de datos usando un bloque separado de dichos algoritmo triple DES y encadenamiento de bloques de cifrado;

la decodificación de la pluralidad de datos en base a dicho valor inicial y dicha clave.

2. El procedimiento de la reivindicación 1 que, además, comprende:

la recepción, en el componente (202), de una pluralidad de códigos de autenticación de mensajes correspondientes a la pluralidad de datos procedentes del teclado (162), habiendo sido creados dichos códigos de autenticación de mensajes con el algoritmo triple DES y el encadenamiento de bloques de cifrado usando dicha clave y el segundo valor inicial diferente de dicho primer valor inicial, siendo conocido dicho segundo valor inicial tanto al componente como al teclado;

la verificación de la pluralidad de datos usando la pluralidad de los códigos de autenticación de mensajes.

3. El procedimiento de la reivindicación 2 en el que la creación de un primer valor inicial y un segundo valor inicial comprende:

la creación del primer valor inicial aplicando el algoritmo triple DES y el encadenamiento de bloques de cifrado a una combinación del primer valor de uso único y el segundo valor de uso único, usando la clave y un tercer valor inicial que es conocido tanto al teclado como al componente; y

la creación del segundo valor inicial aplicando el algoritmo triple DES y el encadenamiento de bloques de cifrado a una combinación del primer valor de uso único y el segundo valor de uso único, usando la clave y un cuarto valor inicial que es conocido tanto al teclado como al componente.

4. El procedimiento de la reivindicación 1 en el que la pluralidad de datos se recibe por medio de un canal cuya integridad conductual no goza de la confianza del componente.

5. El procedimiento de la reivindicación 4 en el que el componente (202) comprende un primer sistema operativo, que se ejecuta en un dispositivo informático junto con un segundo sistema operativo, no teniendo confianza el primer sistema operativo, al menos en algún sentido, en el comportamiento del segundo sistema operativo, comunicándose el teclado con el primer sistema operativo por medio de un controlador controlado por el segundo sistema operativo.

6. El procedimiento de la reivindicación 1 en el que el teclado comprende un teclado USB.

7. El procedimiento de la reivindicación 6 en el que dicho algoritmo triple DES y el encadenamiento de bloques de cifrado cifran los datos en bloques que tienen un tamaño predeterminado y en el que el teclado comunica datos en bloques de dicho tamaño predeterminado.

8. El procedimiento de la reivindicación 1 en el que cada dato de la pluralidad de datos se genera en base a una pulsación individual de tecla recibida en el teclado.

9. Un medio legible por ordenador cifrado con instrucciones ejecutables por ordenador para llevar a cabo un procedimiento de recepción segura de una entrada en un componente lógico (202), procedente de un teclado (162), comprendiendo el procedimiento:

la recepción, en un componente lógico, de un primer valor (412) de uso único desde el teclado;

el envío, desde el componente lógico, de un segundo valor (414) de uso único al teclado;

la creación de un primer valor inicial y de un segundo valor inicial aplicando el algoritmo triple DES y el encadenamiento de bloques de cifrado a una combinación de dicho primer valor de uso único y dicho segundo valor de uso único, usando una clave y un tercer valor inicial que es conocido tanto al teclado como al componente;

la recepción, en un componente lógico, de una pluralidad de pulsaciones cifradas del teclado, habiéndose creado en el teclado las pulsaciones cifradas cifrando las pulsaciones de teclas pulsadas recibidas en el teclado con el algoritmo triple DES y el encadenamiento de bloques de cifrado usando la clave y el primer valor inicial procedente del teclado, estando incluida cada pulsación separada de tecla procedente de dicho teclado dentro de un dato separado de dicha pluralidad de datos, estando cifrado cada dato de la pluralidad de datos usando un bloque separado de dichos algoritmo triple DES y encadenamiento de bloques de cifrado; y

en el componente lógico, la decodificación de la pluralidad de pulsaciones cifradas de tecla usando la clave y el primer valor inicial.

10. El medio legible por ordenador de la reivindicación 9 en el que el componente lógico (202) comprende un primer sistema operativo que se ejecuta en un dispositivo informático junto con un segundo sistema operativo, no teniendo confianza el primer sistema operativo, al menos en algún sentido, en el comportamiento del segundo sistema operativo, comunicándose el teclado con el primer sistema operativo por medio de un controlador controlado por el segundo sistema operativo.

11. El medio legible por ordenador de la reivindicación 9 en el que el procedimiento comprende, además:

la recepción, en el componente lógico (202), de una pluralidad de códigos de autenticación de mensajes correspondientes a la pluralidad de pulsaciones cifradas de tecla procedentes del teclado (162), habiendo sido creados dichos códigos de autenticación de mensajes con el algoritmo triple DES y el encadenamiento de bloques de cifrado usando dicha clave y el segundo valor inicial diferente de dicho primer valor inicial, siendo conocido dicho segundo valor inicial tanto al componente lógico como al teclado;

la verificación de la pluralidad de pulsaciones cifradas de tecla usando la pluralidad de los códigos de autenticación de mensajes.

12. El medio legible por ordenador de la reivindicación 11 en el que la creación de un primer valor inicial y un segundo valor inicial comprende, además:

la creación del primer valor inicial aplicando el algoritmo triple DES y el encadenamiento de bloques de cifrado a una combinación del primer valor (412) de uso único y el segundo valor (414) de uso único, usando la clave y un tercer valor inicial que es conocido tanto al teclado como al componente lógico (202); y

la creación del segundo valor inicial aplicando el algoritmo triple DES y el encadenamiento de bloques de cifrado a una combinación del primer valor de uso único y el segundo valor de uso único, usando la clave y un cuarto valor inicial que es conocido tanto al teclado como al componente lógico.

13. El medio legible por ordenador de la reivindicación 9 en el que dichos algoritmo triple DES y encadenamiento de bloques de cifrado cifran los datos en bloques que tienen un tamaño predeterminado y en el que el teclado comunica datos en bloques de dicho tamaño predeterminado.

14. Un teclado (162) que comprende:

uno o más emplazamientos de almacenamiento que almacenan un primer valor inicial y una clave;

un componente (202) de cifrado que está adaptado para recibir un primer valor (412) de uso único procedente del destinatario por medio de la interfaz de comunicaciones, para enviar un segundo valor (414) de uso único al destinatario por medio de la interfaz de comunicaciones y para crear el primer valor inicial aplicando el algoritmo triple DES y el encadenamiento de bloques de cifrado a una combinación del primer valor de uso único y el segundo valor de uso único, usando la clave y un segundo valor inicial que es conocido tanto al teclado como al componente, en el que dicho componente de cifrado cifra los datos de entrada recibidos en el teclado con el algoritmo triple DES y el encadenamiento de bloques de cifrado usando dicha clave y dicho primer valor inicial, con lo cual se crean datos cifrados en base a dichos datos de entrada, siendo representativo cada dato individual de dichos datos de entrada de una pulsación separada de tecla recibida de dicho teclado, siendo cifrado cada dato individual de dichos datos de entrada usando un bloque separado de dichos algoritmo triple DES y encadenamiento de bloques de cifrado; y

una interfaz de comunicaciones que comunica dichos datos cifrados con un dispositivo externo al teclado, estando destinados dichos datos cifrados a un destinatario que conoce dicho primer valor inicial y dicha clave.

15. El teclado (162) de la reivindicación 14 en el que el componente de cifrado crea, además, una pluralidad de códigos de autenticación de mensajes correspondientes a los datos cifrados o a los datos de entrada, habiéndose creado dichos códigos de autenticación de mensajes con el algoritmo triple DES y el encadenamiento de bloques de cifrado usando dicha clave y un valor inicial diferente de dicho primer valor inicial.

16. El teclado (162) de la reivindicación 14 en el que el teclado comprende un teclado USB.

17. El teclado (162) de la reivindicación 14 en el que la interfaz de comunicaciones comunica dichos datos cifrados a un controlador que es controlado por un primer sistema operativo que se ejecuta en dicho dispositivo, con lo que dichos datos cifrados son comunicados a dicho destinatario, siendo dicho destinatario un segundo sistema operativo que se ejecuta en dicho dispositivo, o un programa que se ejecuta bajo dicho segundo sistema operativo, no teniendo confianza el segundo sistema operativo, al menos en algún sentido, en el comportamiento del primer sistema operativo.

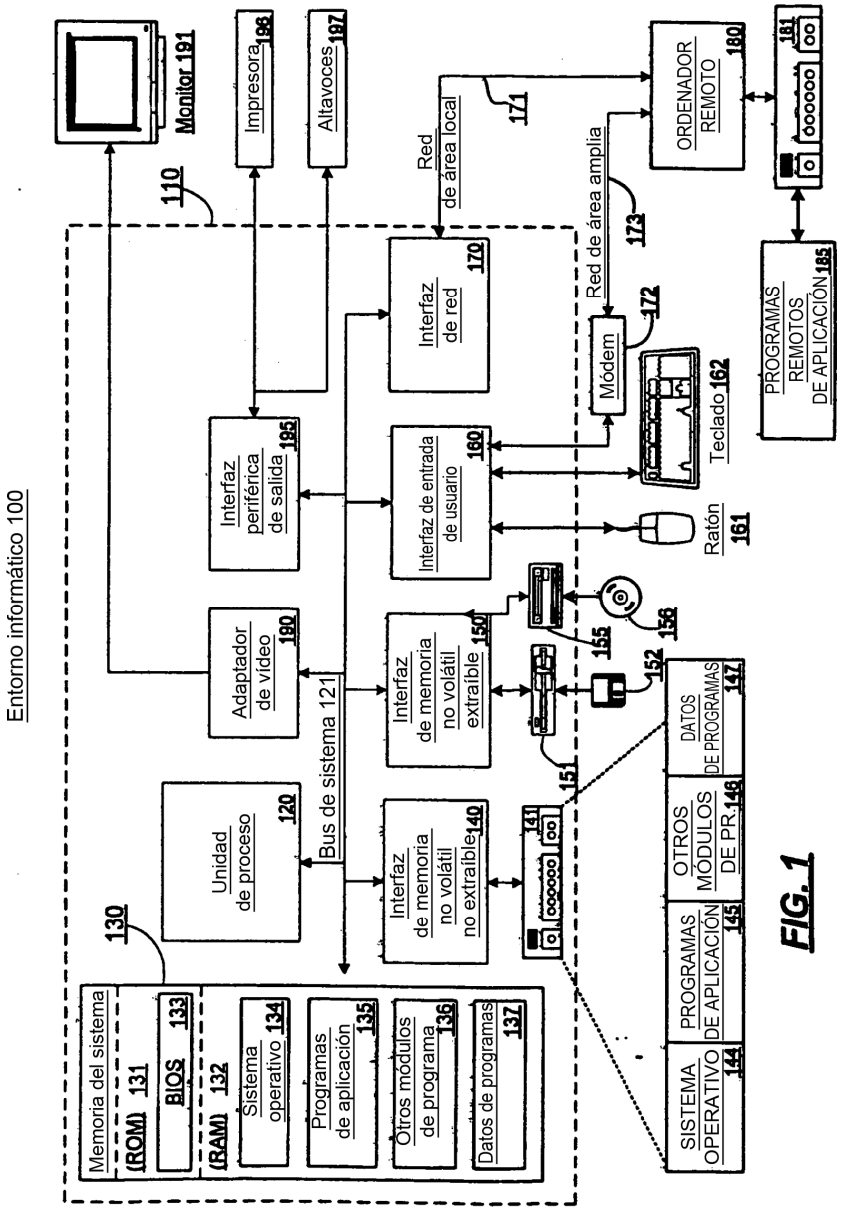
Entorno informático 100
Monitor 191
Impresora 196
Altavoces 197
110
Red de área local 171
ORDENADOR REMOTO 180
181
Red de área amplia 173
Interfaz de red 170
PROGRAMAS REMOTOS DE APLICACIÓN 185
Módem 172
Interfaz periférica de salida 195
Interfaz de entrada de usuario 160
Teclado 162
Ratón 161
Adaptador de vídeo 190
Interfaz de memoria no volátil extraíble 150
155
156
152
151
Unidad de proceso 120
Bus de sistema 121
Interfaz de memoria no volátil no extraíble 140
141
DATOS DE PROGRAMAS 147
OTROS MÓDULOS DE PR 146
PROGRAMAS DE APLICACIÓN 145
SISTEMA OPERATIVO 144
130
Memoria del sistema
(ROM) 131
BIOS 133
(RAM) 132
Sistema operativo 134
Programas de aplicación 135
Otros módulos de programa 136
Datos de programas 137

FIG. 1

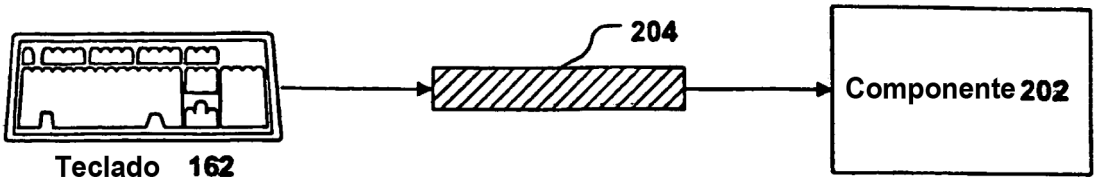

FIG. 2

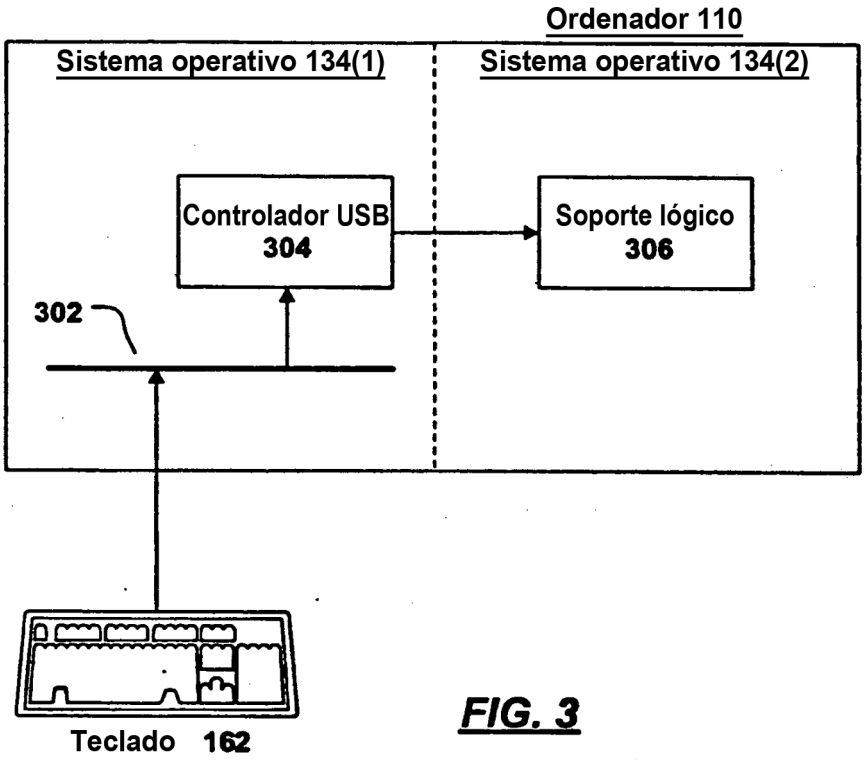

FIG. 3

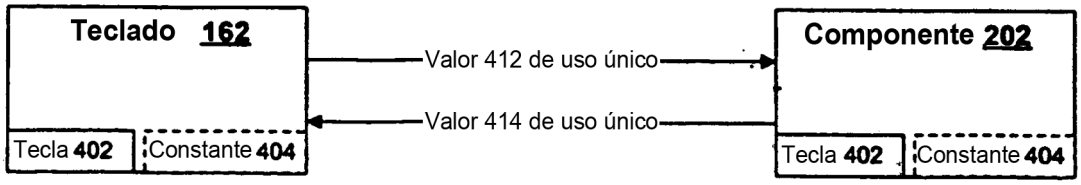

FIG. 4

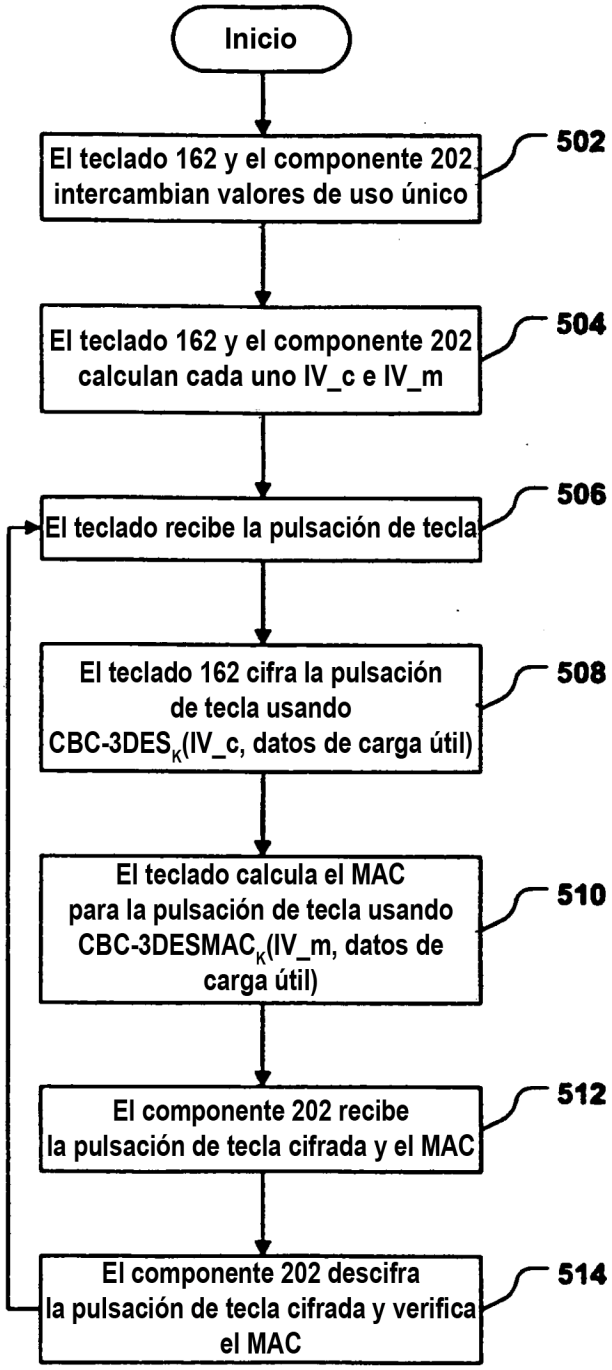
Inicio
El teclado 162 y el componente 202 intercambian valores de uso único
502
El teclado 162 y el componente 202 calculan cada uno IV_c e IV_m
504
El teclado recibe la pulsación de tecla
506
El teclado 162 cifra la pulsación de tecla usando CBC-3DES$_K$(IV_c, datos de carga útil)
508
El teclado calcula el MAC para la pulsación de tecla usando CBC-3DESMAC$_K$(IV_m, datos de carga útil)
510
El componente 202 recibe la pulsación de tecla cifrada y el MAC
512
El componente 202 descifra la pulsación de tecla cifrada y verifica el MAC
514

FIG. 5

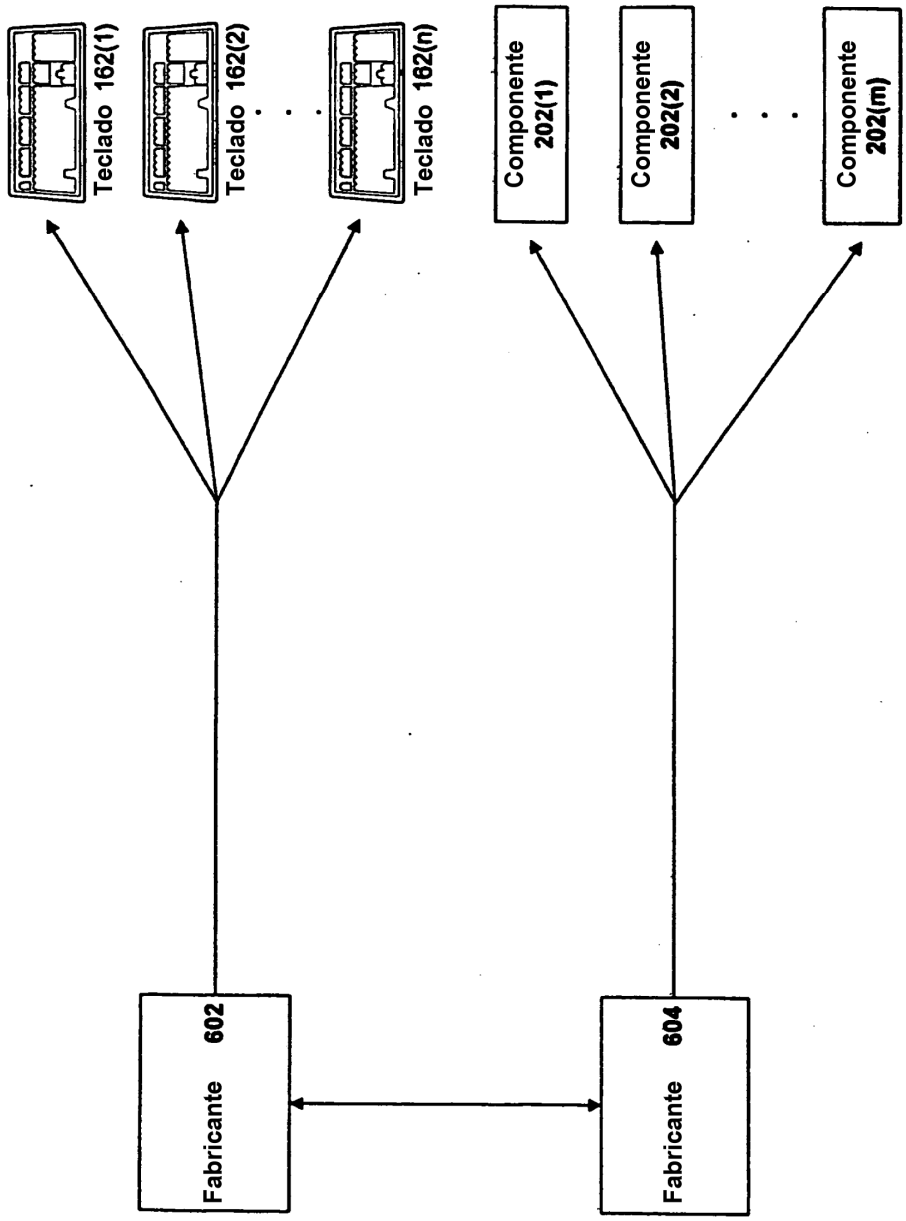
Teclado 162(1)
Teclado 162(2)
Teclado 162(n)
Componente 202(1)
Componente 202(2)
Componente 202(m)
Fabricante 602
Fabricante 604

FIG. 6