(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 715 888**

(51) Int. CI.:

G06F 21/79 (2013.01)
G06F 21/85 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.09.2014 PCT/FR2014/052415**

(87) Fecha y número de publicación internacional: **09.04.2015 WO15049439**

(96) Fecha de presentación y número de la solicitud europea: **25.09.2014 E 14793878 (1)**

(97) Fecha y número de publicación de la concesión europea: **19.12.2018 EP 3053090**

(54) Título: **Método de protección de un conector USB**

(30) Prioridad:

02.10.2013 FR 1359568

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.06.2019

(73) Titular/es:

AVANTIX (100.0%)
655 Avenue Galilée Bâtiment Horizon BP 20140
13794 Aix-en-Provence, FR

(72) Inventor/es:

BONDOUX, CATHERINE y
LE BARTZ, JEAN-LUC

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Método de protección de un conector USB

Campo técnico de la invención

La invención se refiere a la seguridad de los dispositivos dotados con al menos un conector USB.

Antecedentes de la técnica

En la técnica anterior son conocidos los conectores USB, también llamados puertos USB, que permiten conectar un dispositivo con otro. Por ejemplo, conectar un teléfono móvil, o una tableta, a un ordenador o a un cargador.

Estos puertos funcionan de acuerdo con un estándar, llamado estándar USB, que comprende varias versiones. Este estándar describe cómo se deben conectar los periféricos, e incluye principalmente una etapa de negociación entre los aparatos conectados para que se identifiquen mutuamente y puedan cooperar eficazmente. Estamos hablando de una etapa de negociación USB. Esta etapa de negociación comprende, principalmente, una estimulación eléctrica a través de los pines D+ y D-, seguida de una enumeración de las capacidades del dispositivo. Se recuerda aquí que un conector USB tiene 4 pines:

- Alimentación
- Datos D-
- Datos D+
- Masa.

En el dominio de los aparatos seguros, los conectores USB son una de las primeras cosas que se atacan. En la técnica actual, conectar un conector USB en un aparato seguro se considera una falla de seguridad, principalmente debido a posibles errores, también llamados bug, que permanecerían en el código que lleva a cabo el estándar. Estos bugs permiten por lo tanto ataques, por ejemplo, por desbordamiento de búfer o por falsificación de paquetes.

Por lo tanto, en la técnica actual, un dispositivo seguro por tanto no se debe equipar con un conector USB.

Esto requiere, entre otras cosas, tener un conector de potencia dedicado para poder recargar la batería de un aparato móvil seguro. Esto reduce considerablemente su comodidad de uso.

El documento US 2006/0036872 titulado "Anti-burglary USB flash drive with press-button type electronic combination lock" es conocido por la técnica actual.

Descripción de la invención

La invención propone un método, un dispositivo de almacenamiento digital y un dispositivo tal como se definen en las reivindicaciones.

El objetivo de la invención es remediar todas o parte de las desventajas de la técnica actual identificadas anteriormente y, principalmente, proponer medios que permitan equipar un teléfono móvil con un conector USB.

En particular, la invención permite evitar cualquier ejecución de código de gestión de un conector USB mientras no esté garantizado que el teléfono opera en un modo seguro.

Para este propósito, un aspecto de la invención se relaciona con el método de conexión segura de un primer dispositivo a un segundo dispositivo por medio de una conexión USB, comprendiendo cada dispositivo un conector USB, caracterizado por que el método comprende las siguientes etapas, llevadas a cabo por el primer dispositivo:

- Detección de la conexión del segundo dispositivo,
- Bloqueo del primer dispositivo,
- Prohibición de la etapa de negociación USB antes de la estimulación eléctrica de acuerdo con el estándar USB.

Además de las características principales que se acaban de mencionar en el párrafo anterior, el método/dispositivo de acuerdo con la invención puede tener una o más características complementarias de entre las siguientes, consideradas individualmente o de acuerdo con las combinaciones técnicamente posibles:

- El proceso también comprende las siguientes etapas:
    - Desbloqueo del primer dispositivo,
    - Activación de la etapa de negociación USB.

- el primer dispositivo se desbloquea mediante la introducción de un identificador secreto del usuario del primer dispositivo.

- el identificador secreto es un código alfanumérico.

- el identificador secreto es un signo biométrico.

- el método también comprende la siguiente etapa:

  - ajuste del nivel de carga de una batería del primer dispositivo a un nivel predeterminado.

  - el nivel de carga predeterminado está entre 400mA y 500mA.

  - el nivel de carga predeterminado está entre 500mA y 600mA.

La invención también se relaciona con un dispositivo de almacenamiento digital que comprende un archivo que corresponde a los códigos de las instrucciones que llevan a cabo el método de acuerdo con una de las reivindicaciones anteriores.

La invención también se relaciona con un dispositivo que lleva a cabo el método de acuerdo con una de las reivindicaciones anteriores.

Breve descripción de las figuras

Otras características y ventajas de la invención surgirán con la lectura de la siguiente descripción, con referencia a las figuras adjuntas, las cuales ilustran:

- Figura 1, una ilustración de los medios que permiten llevar a cabo la invención;

- Figura 2, una ilustración de las etapas del método de acuerdo con la invención.

Para mayor claridad, los elementos idénticos o similares se identifican mediante signos de referencia idénticos en el conjunto de las figuras.

La invención se comprenderá mejor con la lectura de la siguiente descripción y con el examen de las figuras que acompañan. Éstas se presentan únicamente con fines informativos y de ningún modo limitativas de la invención.

Descripción detallada de un modo de realización

En la Figura 1 se muestra el primer dispositivo 100, en el ejemplo un teléfono 100, que comprende al menos:

- Un microprocesador 110,

- Un conector 120 usb,

- Medios 130 de almacenamiento, por ejemplo, una memoria flash,

- Una pantalla 140,

- Un periférico 150 de entradas, por ejemplo, un teclado, un sensor biométrico de huellas dactilares. Se debe tener en cuenta que, en el caso de un teléfono táctil, la pantalla es capaz de desempeñar el papel de periférico de entrada en forma de teclado u otro,

- Una batería de 170.

Los elementos del teléfono 100 se interconectan por un bus 160. Los elementos del teléfono 100 interconectados por el bus 160 son:

- El microprocesador 110,

- el conector 120 USB,

- los medios 130 de almacenamiento,

- el periférico 150 de entradas,

- la batería 170.

Para la descripción del método, se asignan etapas o acciones a un dispositivo, por ejemplo, el teléfono 100. Un dispositivo de este tipo comprende al menos un microprocesador y una memoria de almacenamiento. La memoria de almacenamiento permite almacenar códigos de instrucciones cuya interpretación permite llevar a cabo las etapas o

acciones descritas. Por lo tanto, cuando se asigna una acción a un dispositivo, ésta en realidad la realiza un microprocesador del dispositivo que interpreta los códigos de instrucciones almacenados en una memoria de la máquina.

Cuando se dice que una acción es realizada por un sistema operativo, una aplicación, un proceso o una zona de código de instrucciones, esta acción corresponde a la implementación, por parte de un microprocesador, de los códigos de instrucciones correspondientes, según se describió en el párrafo anterior.

En el caso de la presente descripción, los medios de almacenamiento se consideran como una única memoria flash con la finalidad de simplificación y claridad. En la práctica, cada zona descrita se podría almacenar en un componente diferente, incluidos los componentes RAM, y estos componentes podrían ser, todos o parte de ellos, cajas fuertes digitales.

La figura 1 muestra que los medios 130 de almacenamiento comprenden:

- Una zona 131 de controlador USB que corresponde a los códigos de instrucciones ejecutados para la gestión del conector 120 USB. La zona 131 comprende los códigos de instrucciones que corresponden a la invención;

- Una zona 132 de estado del teléfono utilizada para almacenar un estado del teléfono. Los estados de interés para la invención son "bloqueado" y "desbloqueado".

La figura 2 muestra una etapa 200 inicial en la que un segundo dispositivo, no mostrado, se conecta al primer dispositivo 100 a través del conector 120 USB. En la práctica, el segundo dispositivo es, por ejemplo, un ordenador o un cargador.

En una etapa 210, después de la etapa 200, el primer dispositivo detecta la conexión del segundo dispositivo. En la práctica, una conexión se detecta mediante la medición de una potencia eléctrica al nivel de los pines de alimentación del conector 120 USB, es decir, por la aparición de una tensión en los pines de alimentación y de masa. En un caso de este tipo, el teléfono ejecuta el controlador USB.

En la invención el controlador USB se ejecuta en una etapa 220 de servicio a la conexión USB. La etapa 200 de servicio comprende la etapa 222 de verificación del estado del primer dispositivo:

- Si el estado es desbloqueado, entonces el primer dispositivo pasa a una etapa 224 de bloqueo del primer dispositivo.

- Si el estado es bloqueado, entonces el primer dispositivo pasa a una etapa 228 opcional de ajuste del nivel de carga de la batería 170.

De la etapa 224 de bloqueo, se pasa a la etapa 228 opcional de ajuste del nivel de carga. La etapa 228 de ajuste de carga es clásica y se describe por el estándar USB. La contribución de la invención es aquí que el nivel de carga se regula a un nivel predeterminado sin que se haya establecido ninguna comunicación entre los dispositivos primero y segundo. El nivel de carga se elige para que sea compatible con el menos potente de los segundos dispositivos considerados.

Se consideran de este modo niveles de carga comprendidos entre 400mA y 500mA, o entre 500mA y 600mA. Esto permite que el primer dispositivo se cargue en todos los casos, sin el desbloqueo del primer dispositivo y sin el agotamiento de una batería del segundo dispositivo.

En la práctica, estos valores corresponden a potencias que se pueden suministrar por segundos dispositivos. Si se consideran los casos de utilización en los que esta potencia que puede ser suministrada es superior o inferior a los valores citados, entonces la enseñanza de la invención sigue siendo válida. Basta con ajustar el nivel predeterminado a las condiciones de utilización previstas.

El hecho de que la etapa 228 de ajuste del nivel de carga sea opcional significa que existe una variante de la invención en la que no se lleva a cabo. En un caso de este tipo, las etapas que se han descrito como que conducen a la etapa 228 de ajuste del nivel de carga conducen entonces a la etapa 230 de prohibición de la etapa de negociación USB.

La etapa 224 de bloqueo es clásica en el sentido de que a la salida de la etapa de bloqueo el primer dispositivo reacciona a cualquier solicitación de petición de desbloqueo hasta que se consigue un desbloqueo. La etapa de bloqueo pasa el estado del primer dispositivo a "bloqueado". La etapa de bloqueo se puede ejecutar en un contexto distinto al de la gestión de una conexión USB, por ejemplo, en una petición expresa de bloqueo por parte de un usuario. Tiene, sea cual sea el contexto, los mismos efectos que los descritos anteriormente.

Desde la etapa 228 de ajuste del nivel de carga se pasa a una etapa 230 de prohibición de la etapa de negociación USB.

La etapa 230 es, por ejemplo, un bucle mientras que comprueba el estado del primer dispositivo. El bucle sólo se cierra si el estado del primer dispositivo es "desbloqueado". La única forma de salir del bucle es desbloquear el primer dispositivo o desconectar el segundo dispositivo.

Por lo tanto, el código de gestión del conector USB sólo se ejecuta si el primer dispositivo ha pasado de un estado "bloqueado" a un estado "desbloqueado" después de la conexión del segundo dispositivo. Si se produce un desbloqueo durante la etapa 230, el primer dispositivo pasa a una etapa 240 de gestión clásica de una conexión USB. Aquí, la utilización de un estado del primer dispositivo es equivalente a la gestión de un estado del conector 120 USB. En el caso del estado del conector se procedería de la siguiente manera:

- En la etapa 224 el estado del conector se pasa a "en espera".

- En el bucle mientras que se comprueba el estado del conector y sólo se sale si se vuelve "activo".

- En la etapa 300 de desbloqueo se pasa el estado del conector a "activo".

En la práctica, si se considera la conexión de un dispositivo de acuerdo con la invención a un ordenador, el ordenador sólo detectará la conexión una vez que el dispositivo de acuerdo con la invención se haya desbloqueado.

Se tendrá que entender que estamos en un contexto de multitareas y que por lo tanto el bucle "mientras que" se utiliza a título de ejemplo no es limitador desde el punto de vista del primer dispositivo. Esto es como poner un proceso, aquí la gestión de una conexión USB, en espera hasta que no se cumpla una condición.

La precisión, antes de la estimulación eléctrica, quiere decir que el código de gestión de la conexión USB se prohíbe antes de que se pueda ejecutar una acción que señale la conexión al segundo dispositivo.

Con la invención podemos decir por lo tanto que la gestión de las conexiones USB está fuera del estándar. A pesar de ello, aquella redujo sobre todo la superficie de exposición a ataques de un dispositivo que lleve a cabo el método de acuerdo con la invención.

La figura 2 muestra una etapa 300 de desbloqueo que interviene durante la prohibición 230 de la etapa de negociación USB. Este desbloqueo permite al primer dispositivo pasar a la etapa 240 de gestión clásica de la conexión USB, es decir, de identificarse al segundo dispositivo y de proceder a la enumeración de las capacidades USB del primer dispositivo. Una capacidad es, por ejemplo, la capacidad de asumir la responsabilidad del protocolo MTP en la conexión USB.

En la medida de que el primer dispositivo debe estar asegurado, la etapa 300 de desbloqueo es:

- Una entrada de una secuencia válida de códigos alfanuméricos, esta entrada se realiza, por ejemplo, a través de la pantalla que en tal caso es una pantalla táctil,

- Una entrada de una huella dactilar reconocida, esta entrada se realiza en tal caso a través del periférico 150 de entradas.

La ejecución de la etapa de desbloqueo pasa el estado del primer dispositivo a "desbloqueado".

Con la invención es imposible hacer una conexión USB sin que el usuario haya efectuado un desbloqueo del primer dispositivo. Eso hace que los ataques a través del puerto USB sean imposibles sin el consentimiento del usuario.

REIVINDICACIONES

1. Método de conexión segura de un primer dispositivo de tipo teléfono a un segundo dispositivo a través de una conexión USB, comprendiendo cada dispositivo un conector USB, caracterizado por que el método comprende las siguientes etapas, llevadas a cabo por el primer dispositivo en este orden:

- Detección (200) de la conexión del segundo dispositivo a través del conector USB mediante la medida de una potencia eléctrica,

- Bloqueo (224) del primer dispositivo,

- Inhibición (230) de la etapa de negociación USB antes de la estimulación eléctrica de acuerdo con el estándar USB:

  - Si el primer dispositivo se desbloquea por un usuario (300):

    - Activación (240) de la etapa de negociación USB.

2. Método de conexión segura de acuerdo con la reivindicación 1, caracterizado por que el primer dispositivo se desbloquea mediante la introducción de un identificador secreto del usuario del primer dispositivo.

3. Método de conexión segura de acuerdo con la reivindicación 2, caracterizado por que el identificador secreto es un código alfanumérico.

4. Método de conexión segura de acuerdo con la reivindicación 2, caracterizado por que el identificador secreto es un signo biométrico.

5. Método de acuerdo con una de las reivindicaciones anteriores, caracterizado por que comprende la siguiente etapa:

- Ajuste (228) del nivel de carga de una batería del primer dispositivo a un nivel predeterminado.

6. Método de acuerdo con la reivindicación 5 caracterizado por que el nivel de carga predeterminado está entre 400mA y 500mA.

7. Método de acuerdo con la reivindicación 5 caracterizado en que el nivel de carga predeterminado está entre 500mA y 600mA.

8. Dispositivo (130) de almacenamiento digital que comprende un fichero que corresponde a los códigos de instrucciones que llevan a cabo el método de acuerdo con una de las reivindicaciones anteriores.

9. Dispositivo (100) que lleva a cabo el método de acuerdo a una de las reivindicaciones anteriores.

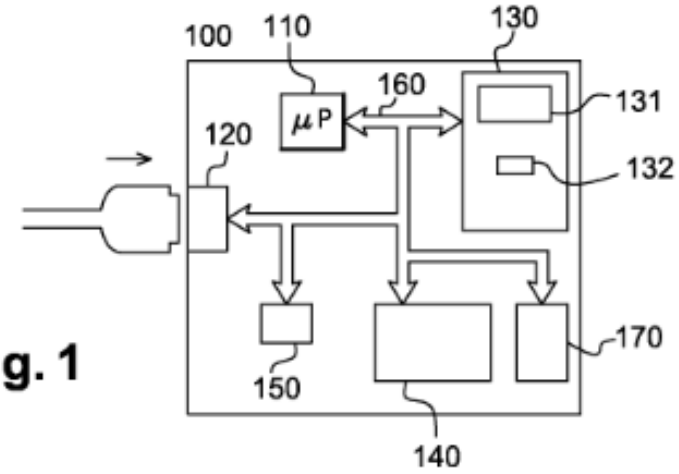
100
110
130
160
131
120
132
170
150
140

Fig. 1

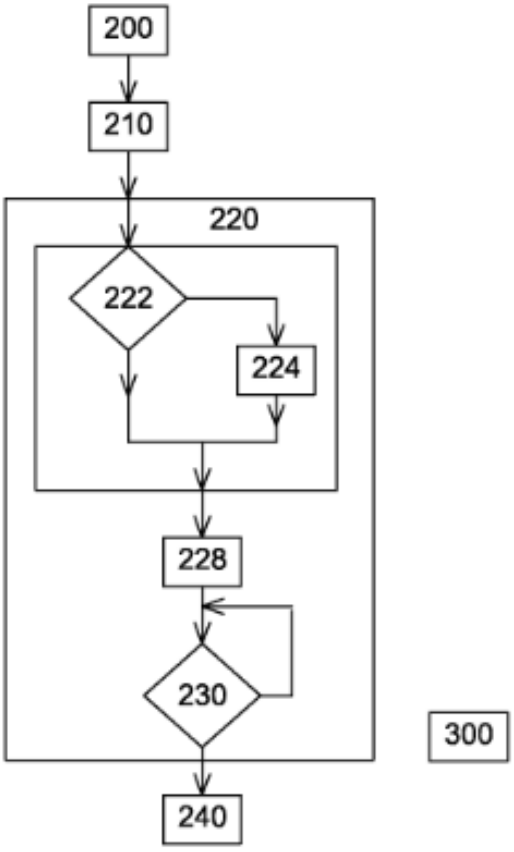
200
210
220
222
224
228
230
300
240

Fig. 2