(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 202495949 U
(45)授权公告日 2012.10.17

(21)申请号 201220098978.2

(22)申请日 2012.03.16

(73)专利权人 杭州商易信息技术有限公司
地址 310013 浙江省杭州市西湖区塘苗路18号华星现代产业园B7层

(72)发明人 葛世安

(74)专利代理机构 北京青松知识产权代理事务所（特殊普通合伙） 11384
代理人 郑青松

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

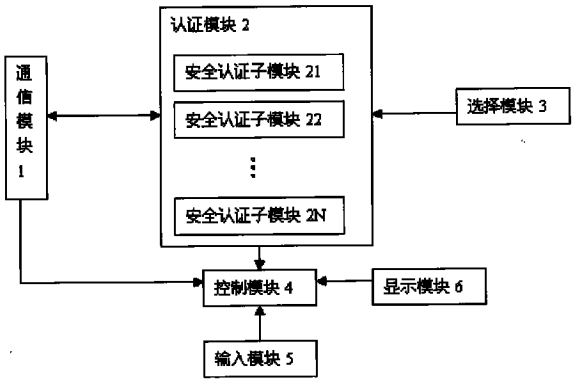
权利要求书 1 页 说明书 4 页 附图 1 页

(54)实用新型名称

一种安全性增强的信息安全设备

(57)摘要

本实用新型公开了一种安全性增强的信息安全设备，包括通信模块、认证模块、选择模块、控制模块、输入模块和显示模块，所述信息安全设备通过其内部的通信模块与计算机相连接，以通过计算机实现与网络侧的交互，其中，所述认证模块与通信模块和选择模块相连，其包括至少两个不同功能的安全认证子模块，所述选择模块依据物理方式的输入，触发所述认证模块中的一个安全认证子模块；显示模块与控制模块相连，用来显示交易金额、交易账户或者交易状态信息。相比传统的UsbKey，本实用新型能够在用户由于客户端被例如木马等病毒侵入而被欺骗的情况下，避免中间人的攻击，从而能够提高信息安全的可靠性，并且具有操作更方便的优点。



CN 202495949 U

1. 一种安全性增强的信息安全设备，包括通信模块、认证模块、选择模块、控制模块、输入模块和显示模块，所述信息安全设备通过其内部的通信模块与计算机相连接，以通过计算机实现与网络侧的交互，其特征在于：

所述认证模块与通信模块和选择模块相连，并包括至少两个不同功能的安全认证子模块；所述选择模块依据物理方式的输入，触发所述认证模块中的一个安全认证子模块；

所述显示模块与控制模块相连，从而显示交易金额、交易账户或者交易状态信息。

2. 如权利要求 1 所述的安全性增强的信息安全设备，其特征在于，所述输入模块与控制模块相连，其包括 0-9 十个数字按键以及一确认键和一取消键。

3. 如权利要求 2 所述的安全性增强的信息安全设备，其特征在于，所述选择模块为下述之一或任意组合：开关组、多向按键、拨盘、滚动按键、选择按键、触摸屏、触摸感应开关、光电感应开关。

4. 如权利要求 1 或 2 所述的安全性增强的信息安全设备，其特征在于，所述通信模块与计算机的连接方式为通过 USB 接口、无线 USB 接口、1394 接口或蓝牙接口连接。

5. 如权利要求 4 所述的安全性增强的信息安全设备，其特征在于，所述显示模块是液晶显示屏。

一种安全性增强的信息安全设备

技术领域

[0001] 本实用新型涉及信息安全技术领域，具体涉及到一种安全性增强的信息安全设备。

背景技术

[0002] 在信息科技日益发达的今天，数据信息的安全性和保密性日益受到人们的重视。同时，近年来，随着互联网技术与电子商务的快速发展，越来越多的商务活动转移到网络上开展，例如网上政府办公、网上数字银行、网上购物等等，与此同时，越来越多涉及个人隐私和商业秘密的信息需要通过网络传递。然而病毒、黑客、网络交易以及网页仿冒诈骗等恶意威胁，给用户造成了精神损害和经济上的损失。

[0003] 在现有技术中，用于身份认证一般为USBKey等信息安全设备。UsbKey是一种带有处理器和存储器的小型硬件设备，它通过计算机的数据通讯接口与计算机连接。它具有密钥生成、安全存储密钥、预置加密算法等功能。UsbKey与密钥相关的运算完全在设备内部运行，且UsbKey具有抗攻击的特性，安全性极高。UsbKey一般通过USB接口与计算机相连。

[0004] UsbKey采用PIN（个人身份识别）码或生物特征（如指纹或虹膜等）验证用户身份的合法性，在进行身份认证时将UsbKey与计算机相连，用户在计算机上输入PIN码或生物特征，UsbKey会自动校验该PIN码或生物特征的正确性，只有当用户输入的PIN码或生物特征正确时，才允许用户使用UsbKey。UsbKey具有物理抗攻击的特性，安全性极高。

[0005] 利用UsbKey可以实现多种信息安全操作，主要包括：数据交互（在UsbKey内对写入的数据进行加密或对读取的数据进行解密）；身份认证信息处理、存储/验证密码信息、存储/验证签名、存储/验证证书、权限管理；以及预置代码进行数据运算等等；其中预置代码包括预置用户软件部分片断（用户软件部分片断不能被读出UsbKey，并在UsbKey内部运行进行数据运算），和预置软件保护应用接口函数（软件保护应用接口函数为UsbKey和软件开发商应用之间的接口级函数）等等。

[0006] 现有技术中的UsbKey能够实现用户登录网上银行后进行安全的交易，由于网上银行的特殊性，交易的频次相对较低，因此上述方法对于防范虚假交易有较高的价值。但是，对于更多的网络应用，例如网络游戏中的虚拟物品交易，交易是高度频繁的操作，在实际应用中根本不可能对每次交易都在USBkey的显示屏上确认后进行，这样会使得游戏过程无法进行。因此，对于这一类的网络应用通常采用的是高可靠性的安全登录技术，确保黑客不能顺利仿冒用户进行登录。上述参考技术并不能防止客户端被例如木马等病毒侵入后，中间人仿冒用户的身份登录网上银行，因为在整个登录过程中显示屏上显示的都将是服务器提供的真实的信息，只不过通信的过程被黑客所接管和利用。仅仅在USB Key上增加简单的确认按钮只能解决木马病毒在后台执行的静默攻击，木马病毒还完全能够在后台执行某一网络操作、并利用虚假信息欺骗用户当前正在执行另一网络操作，则用户会再次通过物理方式进行确认，从而使得中间人能够在用户被欺骗的情况下实现攻击，因此现有UsbKey的信息安全可靠性不高。

[0007] 另外，UsbKey 的作用仅仅是建立一个 UsbKey 本身和银行账户卡之间的对应关系，也就说其他人如果得到这个 UsbKey，同样可以进行操作。而交易账户的密码都是通过电脑在应用系统（如网银）的页面上输入的，很容易受到木马、病毒和键盘截取等攻击，这是现有 UsbKey 的薄弱环节。

[0008] 综上所述，现有技术的信息安全设备主要存在的问题就是存在安全隐患，或容易被攻击窃取密码，或容易被盗用的问题。

实用新型内容

[0009] 本实用新型的目的就是为了解决上述问题，提供一种一种安全性增强的信息安全设备。

[0010] 为实现上述目的，本实用新型采用如下技术方案：

[0011] 一种安全性增强的信息安全设备，包括通信模块、认证模块、选择模块、控制模块、输入模块和显示模块，所述信息安全设备通过其内部的通信模块与计算机相连接，以通过计算机实现与网络侧的交互，其特征在于：

[0012] 所述认证模块与通信模块和选择模块相连，其包括至少两个不同功能的安全认证子模块，所述选择模块依据物理方式的输入，触发所述认证模块中的一个安全认证子模块；

[0013] 显示模块与控制模块相连，用来显示交易金额、交易账户或者交易状态信息。

[0014] 根据本实用新型一优选实施例，所述输入模块与控制模块相连，其包括 0-9 十个数字按键以及一确认键和一取消键。

[0015] 根据本实用新型一优选实施例，所述选择模块为下述之一或任意组合：开关组、多向按键、拨盘、滚动按键、选择按键、触摸屏、触摸感应开关、光电感应开关。

[0016] 根据本实用新型一优选实施例，所述通信模块与计算机的连接方式为通过 USB 接口、无线 USB 接口、1394 接口或蓝牙接口连接。

[0017] 根据本实用新型一优选实施例，所述显示模块是液晶显示屏。

[0018] 本实用新型提供的信息安全设备，如果用户受到虚假信息的欺骗，以物理方式的输入触发另一网络操作需要的安全认证模块，也会使得中间人在后台真正执行的该某一网络操作无法成功。另外，本实用新型提供的信息安全设备，可以将用户的交易信息，例如交易金额等直接在此终端显示，可直接通过此终端确认和取消交易。由此可知，相比传统的 UsbKey，本实用新型能够在用户由于客户端被例如木马等病毒侵入而被欺骗的情况下，避免中间人的攻击，从而能够提高信息安全的可靠性，并且具有操作更方便的优点。

附图说明

[0019] 图 1 为根据本实用新型实施例的信息安全设备的结构示意图。

具体实施方式

[0020] 下面参照附图对本实用新型进行更全面的描述，其中说明本实用新型的示例性实施例。

[0021] 图 1 为根据本实用新型实施例的信息安全设备的结构示意图。如图 1 所示，本实用

新型提供的安全性增强的信息安全设备包括：通信模块 1、认证模块 2、选择模块 3、控制模块 4、输入模块 5 和显示模块 6。信息安全设备通过其内部的通信模块 1 与计算机相连接，以通过计算机实现与网络侧的交互。连接方式与现有技术相同，例如可通过 USB 接口、无线 USB 接口、1394 接口或蓝牙接口实现通信模块 1 与计算机的连接。

[0022] 认证模块 2 与通信模块 1、选择模块 3 和控制模块 4 相连接，其包括至少两个不同功能的安全认证子模块。其中，本文所述的“不同功能”，较佳地是指网络侧的不同网络操作所需的不同功能。也就是说，不同功能、或不全相同的功能组合可以分别对应网络侧的不同网络操作。

[0023] 实际应用中，安全认证子模块可以为具有下述功能之一或任意功能组合的安全认证子模块：密码学加密算法、密码学解密算法、数字签名、数据存储、随机数生成、哈希算法、消息鉴别码算法。

[0024] 选择模块 3 与认证模块 2 和控制模块 4 相连接，选择模块 3 可依据物理方式的输入，触发认证模块 2 中任一或一组安全认证子模块，等效于触发了网络操作所需要的功能所对应的安全认证子模块。

[0025] 具体来说，选择模块 3 可以包括与至少两种功能分别一一对应的至少两路输出，且选择模块 3 还包括能够以物理方式导通任一路或一组输出的开关，此处所述的开关，其闭合与断开只依据其物理结构受到外力后的接触状态变化，而并不直接受任何电信号的控制，相应地，本文所述的物理方式主要也是指不直接受任何电信号控制的方式。由此，通过闭合任意类型的开关将与任一或一组功能所对应的一路输出导通，即可以依据物理方式的输入，触发所述信息安全多功能模块中与网络操作所需要的功能所对应的安全认证子模块。

[0026] 实际应用中，选择模块 3 可以是下述之一或任意组合：开关组、多向按键、滚动按键、选择按键、多重选择功能的拨盘、触摸屏、触摸感应开关、光电感应开关。

[0027] 基于上述信息安全设备，当用户获知当前正在执行某一网络操作时，可以通过对选择模块 3 施加外力，以通过选择模块 3 的物理方式输入，触发认证模块 2 中与该用户所获知的某一网络操作需要的功能所对应的安全认证子模块。这样，如果用户获知当前正在执行某一网络操作的信息，是网络侧提供的真实信息，则基于被触发的该网络操作需要的功能所对应的安全认证子模块实现该网络操作的认证；如果用户获知当前正在执行某一网络操作的信息，是由于该用户使用的客户端被木马病毒侵入而产生的虚假信息，即用户获知的当前正在执行某一网络操作并不是当前所执行的真实网络操作，则由于被触发的用户获知的某一网络操作需要的功能所对应的安全认证子模块，不同于真实网络操作所需要的功能所对应的安全认证子模块，因而真实网络操作的认证不会在用户被欺骗的情况下通过。

[0028] 在本实用新型的实施例中，用户通过物理方式的输入操作选择模块 3 并选择 N 个网络操作所分别需要的安全认证子模块 1、安全认证子模块 2... 安全认证子模块 N，以此来触发与 N 个网络操作所分别需要的 N 个功能所一一对应的 N 个安全认证子模块。

[0029] 可见，本实施例的信息安全设备中设置了至少两个不同功能的安全认证子模块，不同功能、或不全相同的功能组合可以分别对应网络侧的不同网络操作，这样，在任一个网络操作之前，该信息安全设备均可依据物理方式的输入来触发该网络操作所需要的功能所对应的安全认证子模块。这样，即便客户端被例如木马等病毒侵入，以至于中间人能够在后

台执行某一网络操作，却利用虚假信息欺骗用户当前正在执行另一网络操作，但由于不同网络操作需要不同功能的安全认证子模块，因此，如果用户受到虚假信息的欺骗，以物理方式的输入触发另一网络操作需要的功能所对应的安全认证子模块，也会使得中间人在后台真正执行的该某一网络操作无法成功。也就是说，上述信息安全设备能够在用户由于客户端被例如木马等病毒侵入而被欺骗的情况下，避免中间人的攻击，从而能够提高信息安全认证的可靠性。

[0030] 另外，本实用新型提供的信息安全设备还具有与控制模块 4 连接的输入模块 5 和显示模块 6。所述显示模块 6 可用于显示交易信息。输入模块 5 可以是键盘，设置有 12 个按键，具体包括 0-9 十个数字按键 2 以及一个确认按键 5 和一个取消按键 4。

[0031] 在交易过程中，用户必须通过信息安全设备的键盘输入 6-8 位数字密码后，控制模块 4 即捕获相应的数字信息。当此安全终端应用在网络交易过程，网络应用服务器是银行服务器，所述输入模块能够输入交易金额，并通过所述显示模块上显示，通过所述键盘确认或取消交易。

[0032] 实际应用中，显示模块可以是液晶显示屏。

[0033] 本实用新型提供的信息安全设备，如果用户受到虚假信息的欺骗，以物理方式的输入触发另一网络操作需要的安全认证模块，也会使得中间人在后台真正执行的该某一网络操作无法成功。另外，本实用新型提供的信息安全设备，可以将用户的交易信息，例如交易金额等直接在此终端显示，可直接通过此终端确认和取消交易。由此可知，相比传统的 UsbKey，本实用新型能够在用户由于客户端被例如木马等病毒侵入而被欺骗的情况下，避免中间人的攻击，从而能够提高信息安全的可靠性，并且具有操作更方便的优点。

[0034] 以上对本实用新型所提供的一种网络安全终端进行了详细介绍。本文中应用了具体个例对本实用新型的原理及实施方式进行了阐述。以上实施例的说明只是用于帮助理解本实用新型的方法及其实现思想；同时，对于本领域的一般技术人员，依据本实用新型的思想，在具体实施方式及应用范围上均会有改变之处。综上所述，本说明书内容不应理解为对本实用新型的限制。

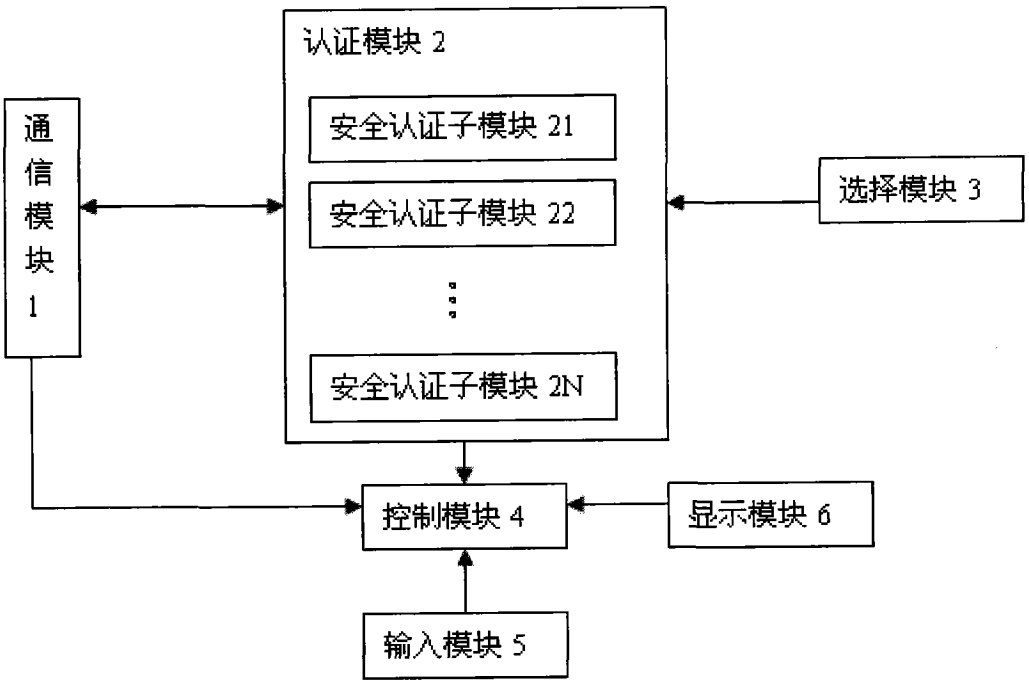

认证模块 2
安全认证子模块 21
安全认证子模块 22
安全认证子模块 2N
通信模块 1
选择模块 3
控制模块 4
显示模块 6
输入模块 5

图 1