(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 205942705 U
(45)授权公告日 2017.02.08

(21)申请号 201620686324.X

(22)申请日 2016.07.01

(73)专利权人 中国人民解放军海军航空工程学院
地址 264001 山东省烟台市芝罘区二马路188号科研部

(72)发明人 崔嘉 洪贝 齐玉东 宋伟健 阮传峰

(74)专利代理机构 中国人民解放军海军专利服务中心 11044
代理人 刘书岩 王丽婷

(51)Int.Cl.
G06F 21/78(2013.01)
G06F 21/85(2013.01)

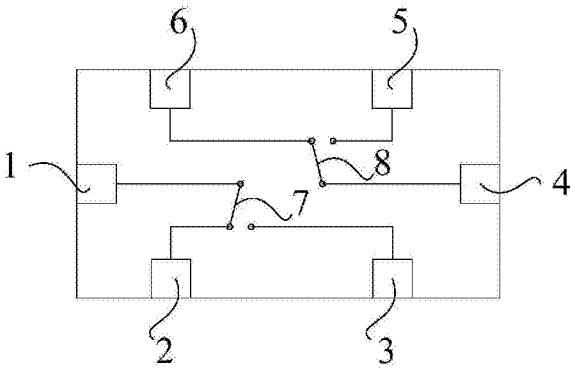
权利要求书1页 说明书4页 附图1页

(54)实用新型名称

一种计算机网络信息安全装置

(57)摘要

本实用新型公开了一种计算机网络信息安全装置，包括计算机网络接口、局域网接口、互联网接口、计算机主板硬盘接口、普通硬盘接口、内部硬盘接口、网络转换开关和硬盘转换开关；其中局域网接口和互联网接口通过网络转换开关与计算机网络接口电性连接；普通硬盘接口和内部硬盘接口通过硬盘转换开关与计算机主板硬盘接口电性连接。该装置具有结构简单，仅需在原有计算机结构的基础上，多采购一块硬盘及本装置，采购成本低等优点，但可有效避免企业内部信息在接入互联网时泄露问题的出现，并同时避免计算机硬盘在接入互联网时感染的病毒或木马等入侵局域网问题的出现，易于推广普及。



CN 205942705 U

1.一种计算机网络信息安全装置，其特征在于：该装置上设置计算机网络接口(1)、局域网接口(2)、互联网接口(3)、计算机主板硬盘接口(4)、普通硬盘接口(5)、内部硬盘接口(6)、网络转换开关(7)和硬盘转换开关(8)；

其中局域网接口(2)和互联网接口(3)通过网络转换开关(7)与计算机网络接口(1)电性连接；

普通硬盘接口(5)和内部硬盘接口(6)通过硬盘转换开关(8)与计算机主板硬盘接口(4)电性连接。

2.如权利要求1所述的一种计算机网络信息安全装置，其特征在于：网络转换开关(7)与硬盘转换开关(8)为联动开关。

3.如权利要求1或2所述的一种计算机网络信息安全装置，其特征在于：局域网接口(2)和内部硬盘接口(6)周围设置同一种标识色，互联网接口(3)和普通硬盘接口(5)周围设置成另外一种标识色。

4.如权利要求3所述的一种计算机网络信息安全装置，其特征在于：局域网接口(2)和内部硬盘接口(6)周围设置为绿色，互联网接口(3)和普通硬盘接口(5)周围设置成红色。

5.如权利要求4所述的一种计算机网络信息安全装置，其特征在于：在计算机网络接口(1)、局域网接口(2)、互联网接口(3)、计算机主板硬盘接口(4)、普通硬盘接口(5)、内部硬盘接口(6)周围均设有相应接口的文字标识。

6.如权利要求1或2所述的一种计算机网络信息安全装置，其特征在于：在网络转换开关(7)和互联网接口(3)之间还设置有互联网接入检测装置(9)，互联网接入检测装置(9)从内部硬盘接口(6)和硬盘转换开关(8)之间取工作用电。

7.如权利要求6所述的一种计算机网络信息安全装置，其特征在于：互联网接入检测装置(9)上还电性连接有声音报警装置(10)。

8.如权利要求7所述的一种计算机网络信息安全装置，其特征在于：声音报警装置(10)为蜂鸣器或扬声器。

9.如权利要求6所述的一种计算机网络信息安全装置，其特征在于：互联网接入检测装置(9)采用Ping命令判断互联网的接入。

一种计算机网络信息安全装置

技术领域

[0001] 本实用新型涉及一种信息安全装置，具体涉及一种计算机网络信息安全装置，属于计算机安全技术领域。

背景技术

[0002] 随着计算机技术的发展，计算机网络技术已得到广泛地应用，网络间的信息交换量也在逐步增大，因而网络间信息交换过程中的信息安全问题已成为人们关注的焦点。虽然人们对此也采取了一些相应的方法，如采用防火墙技术及在网络机上加装防病毒卡等，但都不是十分理想。目前，部分企业采用局域网与互联网物理隔绝的方式，采用单独的上网计算机连接互联网，该方法可有效解决上述问题；但是该种方法需要采购专门用于上网的计算机，增加了企业成本，尤其是在企业所有员工都有上网需求的时候，企业在计算机采购方面的成本将成倍增加，而且给企业办公场地提出了更高的要求。为了避免出现企业采购成本提高的问题，部分企业将同一台计算机既用于局域网的办公，又用于连接互联网，但为了局域网的信息安全，要求不允许同时连入局域网和互联网。但是在木马和病毒盛行的当下，一旦某台计算机在连接互联网时被植入木马或感染病毒，当其再次连入局域网时，木马或病毒将开始工作，或是侦听并搜集局域网中的信息包，等待该机再次连接互联网时将重要数据文件发送出去；或是对局域网中的服务器或其他计算机的中的数据文件或系统文件进行破坏，严重时甚至造成局域网的瘫痪。

实用新型内容

[0003] 为了解决企业员工采用双计算机办公带来的企业采购成本高企等问题，同时避免出现单计算机办公给企业带来的信息安全风险。

[0004] 本实用新型提供了如下的技术方案：一种计算机网络信息安全装置，该装置上设置计算机网络接口、局域网接口、互联网接口、计算机主板硬盘接口、普通硬盘接口、内部硬盘接口、网络转换开关和硬盘转换开关；其中局域网接口和互联网接口通过网络转换开关与计算机网络接口电性连接，连通时只能连通局域网接口和计算机网络接口，或者连通互联网接口和计算机网络接口，但不能连通局域网接口和互联网接口；普通硬盘接口和内部硬盘接口通过硬盘转换开关与计算机主板硬盘接口电性连接，连通时只能普通硬盘接口和计算机主板硬盘接口，或者连通内部硬盘接口和计算机主板硬盘接口，但不能连通普通硬盘接口和内部硬盘接口。计算机网络接口可通过网线与计算机的网口进行连接；局域网接口用于连接企业局域网的网线；互联网接口用于连接互联网网线；计算机主板硬盘接口用于通过SATA数据线(或IDE数据线)及电源线分别连接主板的SATA接口(或IDE接口)及计算机主机的电源；普通硬盘接口用于通过SATA数据线(或IDE数据线)及电源线连接用于连接互联网时使用的普通硬盘，普通硬盘中应不存放任何涉及企业核心信息的数据，普通硬盘仅用于连接互联网时提供操作系统及存储网络数据；内部硬盘接口用于通过SATA数据线(或IDE数据线)及电源线连接用于连接局域网时使用的内部硬盘，内部硬盘中可存放涉及

企业核心信息的数据，内部硬盘可用于连接局域网时提供操作系统及存储数据。

[0005] 优选的，网络转换开关与硬盘转换开关为联动开关。当网络转换开关连通局域网接口和计算机网络接口时，硬盘转换开关对应连通内部硬盘接口和计算机主板硬盘接口；当网络转换开关连通互联网接口和计算机网络接口时，硬盘转换开关对应连通普通硬盘接口和计算机主板硬盘接口。选用联动开关的目的在于，避免出现应开关操作错误，而带来的将内部硬盘接口和互联网接口同时接入的现象，或者是将普通硬盘接口和局域网接口同时接入的现象。从而实现两套系统的物理隔绝，避免内部硬盘中的企业内部信息泄露，同时避免普通硬盘中在接入互联网时感染的病毒或木马等入侵局域网。

[0006] 优选的，局域网接口和内部硬盘接口周围设置同一种标识色，互联网接口和普通硬盘接口周围设置成另外一种标识色。通过设置不同的标识色，可有效避免连线错误带来的信息泄露的风险。

[0007] 优选的，局域网接口和内部硬盘接口周围设置为绿色，互联网接口和普通硬盘接口周围设置成红色。通过设置两种醒目的标识色，可进一步避免连线错误带来的信息泄露的风险。

[0008] 优选的，在计算机网络接口、局域网接口、互联网接口、计算机主板硬盘接口、普通硬盘接口、内部硬盘接口周围均设有相应接口的文字标识。通过在接口周围设置文字标识，可进一步降低连线错误的可能性，避免由此带来的信息泄露的风险。

[0009] 优选的，在网络转换开关和互联网接口之间还设置有互联网接入检测装置，互联网接入检测装置从内部硬盘接口和硬盘转换开关之间取工作用电。互联网接入检测装置可检测本计算机网络信息安全装置是否连入互联网，由于互联网接入检测装置是由内部硬盘接口和硬盘转换开关之间电路提供工作用电，因此该装置仅在内部硬盘接口和计算机主板硬盘接口连通时，即计算机使用内部硬盘时，才判断是否连入互联网。通过设置互联网接入检测装置，可有效避免因将互联网网线误接局域网接口而带来的企业内部信息泄露的风险。

[0010] 优选的，互联网接入检测装置上还电性连接有声音报警装置。当内部硬盘接口和互联网接口同时工作时，经互联网接入检测装置判断，将触发声音报警装置。

[0011] 优选的，声音报警装置为蜂鸣器或扬声器。通过声音报警，可及时告知使用者目前网络接线存在问题，提醒使用者及时改正，可有效降低企业内部信息泄露的风险。

[0012] 优选的，互联网接入检测装置采用Ping命令判断互联网的接入。通过该种方式判断是否接入互联网，简单高效。

[0013] 本实用新型所达到的有益效果是：本实用新型提出的一种计算机网络信息安全装置，结构简单，仅需在原有计算机结构的基础上，多采购一块硬盘及本装置，采购成本低，但可有效避免企业内部信息在接入互联网时泄露问题的出现，并同时避免计算机硬盘在接入互联网时感染的病毒或木马等入侵局域网问题的出现，易于推广普及。

附图说明

[0014] 图1是计算机网络信息安全装置结构示意图；

[0015] 图2是计算机网络信息安全装置中互联网接入检测装置安装位置示意图；

[0016] 图3是计算机网络信息安全装置中声音报警装置安装位置示意图；

[0017] 其中，1-计算机网络接口、2-局域网接口、3-互联网接口、4-计算机主板硬盘接口、5-普通硬盘接口、6-内部硬盘接口、7-网络转换开关、8-硬盘转换开关、9-互联网接入检测装置、10-声音报警装置。

具体实施方式

[0018] 下面结合附图，对本实用新型的具体实施方式进行进一步的描述。

[0019] 一种计算机网络信息安全装置，如图1所示，在装置的四周依次设置计算机网络接口1、局域网接口2、互联网接口3、计算机主板硬盘接口4、普通硬盘接口5、内部硬盘接口6，并在装置的上表面设置网络转换开关7和硬盘转换开关8；

[0020] 其中局域网接口2和互联网接口3通过网络转换开关7与计算机网络接口1电性连接，具体来说局域网接口2、互联网接口3和计算机网络接口1分别通过网线与网络转换开关7连接；

[0021] 普通硬盘接口5和内部硬盘接口6通过硬盘转换开关8与计算机主板硬盘接口4电性连接，具体来说普通硬盘接口5、内部硬盘接口6和计算机主板硬盘接口4分别通过SATA数据线和电源线与硬盘转换开关8连接。

[0022] 网络转换开关7与硬盘转换开关8为联动开关，当网络转换开关7连通局域网接口2和计算机网络接口1时，硬盘转换开关8对应连通内部硬盘接口6和计算机主板硬盘接口4；当网络转换开关7连通互联网接口3和计算机网络接口1时，硬盘转换开关8对应连通普通硬盘接口5和计算机主板硬盘接口4。

[0023] 局域网接口2和内部硬盘接口6周围设置同一种标识色，本实施例中设置为绿色，表示接入局域网，信息相对安全；互联网接口3和普通硬盘接口5周围设置成另外一种标识色，本实施例中设置为红色，表示接入互联网，信息存在泄露风险。

[0024] 在计算机网络接口1、局域网接口2、互联网接口3、计算机主板硬盘接口4、普通硬盘接口5、内部硬盘接口6周围均设有相应接口的文字标识，本实施例中具体采用的文字依次为：连接计算机网口、连接局域网、连接互联网、连接计算机主板、连接普通硬盘、连接内部硬盘。

[0025] 在网络转换开关7和互联网接口3之间还设置有互联网接入检测装置9，互联网接入检测装置9从内部硬盘接口6和硬盘转换开关8之间的电源线上取工作用电。

[0026] 互联网接入检测装置9上还电性连接有声音报警装置10，当内部硬盘供电工作时，并有接入互联网的行为时，触发声音报警装置10报警。声音报警装置10可选择蜂鸣器，可选择其它形式，诸如带有语音提示的扬声器。

[0027] 互联网接入检测装置9采用Ping命令判断互联网的接入，也可选用其它的类似方法，诸如Telnet、Tracert等命令来检测互联网的接入。

[0028] 使用前，先根据该计算机网络信息安全装置各接口处的文字标识，正确连接各种网线，以及各种数据线和电源线。使用前，应再次根据根据接口周围的标识色确认各接口连线的正确性。

[0029] 使用时，先根据需求选择计算机要接入的网络和硬盘，如果想接入互联网，则通过联动开关置于相应位置，此时普通硬盘接口和计算机主板硬盘接口连通，互联网接口将和计算机网络接口连通，然后打开计算机，连接互联网。

[0030] 如果使用互联网完毕之后，又想接入局域网，则需要先将计算机关闭，然后将联动开关置于相应位置，此时内部硬盘接口和计算机主板硬盘接口连通，局域网接口和计算机网络接口连通。然后再次打开计算机，连接内容局域网。

[0031] 最后应说明的是：以上所述仅为本实用新型的优选实施例，并不用于限制本实用新型，尽管参照前述实施例对本实用新型进行了详细的说明，对于本领域的技术人员来说，其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换。凡在本实用新型的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本实用新型的保护范围之内。

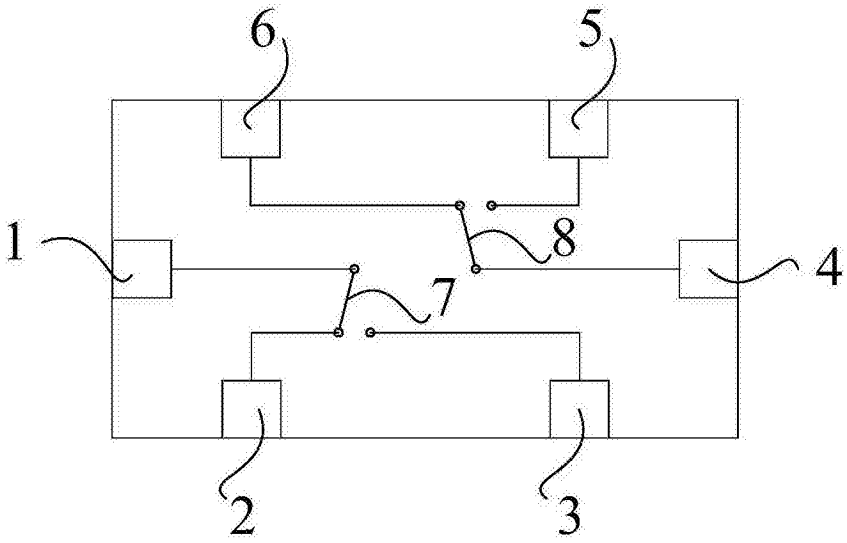


图1

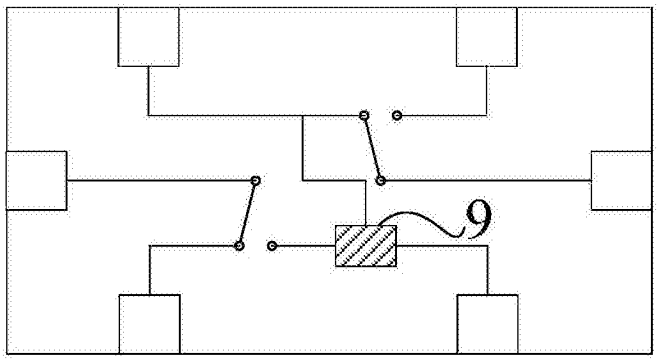


图2

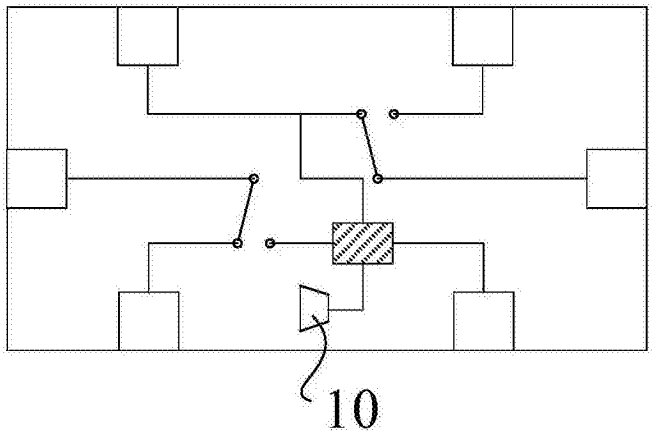


图3