(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295409 A
(43)申请公布日 2017.01.04

(21)申请号 201510283304.8

(22)申请日 2015.05.27

(71)申请人 天津怡凯科技发展有限公司
地址 300203 天津市武清区津京电子商务产业园综合办公楼867室

(72)发明人 陈洪运

(51)Int.Cl.
G06F 21/74(2013.01)
G06F 21/78(2013.01)

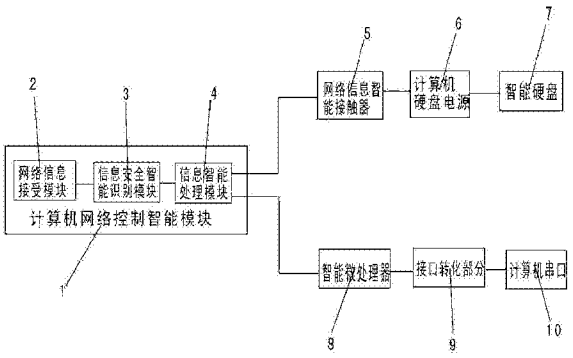
权利要求书1页 说明书2页 附图1页

(54)发明名称

一种网络信息化的安全应用装置

(57)摘要

本发明属于计算机信息安全技术领域，尤其涉及一种网络信息化的安全应用装置，其特征在于，包括：计算机网络控制智能模块，网络信息接收模块，信息安全智能识别模块，信息智能处理模块，网络信息智能接触器，计算机硬盘电源，智能硬盘，智能微处理器，接口转化部分和计算机串口。本发明可以在用户联网的情况下对计算机信息的安全起到很好的保护作用，有效地保护了用户计算机带有信息的计算机硬盘，使得网络黑客无法窃取和攻击计算机的硬盘。



CN 106295409 A

1. 一种网络信息化的安全应用装置，其特征在于，包括：计算机网络控制智能模块，网络信息接收模块，信息安全智能识别模块，信息智能处理模块，网络信息智能接触器，计算机硬盘电源，智能硬盘，智能微处理器，接口转化部分和计算机串口。

2. 根据权利要求 1 所述的网络信息化的安全应用装置，其特征在于：所述的计算机网络控制智能模块包括依次连接的网络信息接收模块，信息安全智能识别模块和信息智能处理模块。

3. 根据权利要求 1 所述的网络信息化的安全应用装置，其特征在于：所述智能微处理器输出端口一路经接口转换部分与用户计算机串口相连接，其另一路端口与计算机网络控制智能模块输出端相连接，计算机网络控制智能模块的一路与网络信息智能接触器相连接。

4. 根据权利要求 1 所述的网络信息化的安全应用装置，其特征在于：所述的网络信息智能接触器与计算机硬盘电源，智能硬盘依次连接；所述计算机硬盘电源用于控制计算机智能硬盘。

一种网络信息化的安全应用装置

[0001]

技术领域

[0002] 本发明专利属于计算机信息安全技术领域，尤其涉及一种网络信息化的安全应用装置。

背景技术

[0003] 随着计算机技术和网络的快速发展，使得计算机已经成为人们在工作、学习和生活中不可或缺的工具。同时，计算机网络的发展，在带给人们便利的同时，也带来了用户计算机信息的安全隐患，信息攻击、病毒传播、信息窃取等时时刻刻都在发生，还有来自于网络“黑客”的攻击，以及计算机网络的缺陷及计算机软件的漏洞等，给计算机用户带来很大的安全隐患，而现有的保护计算机信息安全的措施包括：以计算机软件的方式来实现计算机的信息的安全保护，这种处理方式与计算机操作系统软件有较为密切的关系，但是入侵者仍然可以通过操作系统的漏洞进入计算机，有的防护软件本人也容易被他人攻击，有的入侵者经过简单的身份认证后就可以进入系统，并可以任意的对计算机系统进行任意操作，而计算机合法用户却无法对计算机系统各个重要部分进行有效的管理和控制，无法从根本上解决信息化计算机的安全应用问题。

[0004] 发明专利内容

为了解决上述技术问题，本发明专利网络信息化的安全应用装置，目的就是解决和改善现有计算机系统存在的信息安全问题，以软硬件想结合的形式保障计算机系统的信息安全。

[0005] 本发明专利所采用的技术方案是，网络信息化的安全应用装置，其特征在于包括计算机网络控制智能模块，网络信息接收模块，信息安全智能识别模块，信息智能处理模块，网络信息智能接触器，计算机硬盘电源，智能硬盘，智能微处理器，接口转化部分和计算机串口。所述的计算机网络控制智能模块包括依次连接的网络信息接收模块，信息安全智能识别模块和信息智能处理模块；所述智能微处理器输出端口一路经接口转换部分与用户计算机串口相连接，其另一路端口与计算机网络控制智能模块输出端相连接，计算机网络控制智能模块的一路与网络信息智能接触器相连接，所述的网络信息智能接触器与计算机硬盘电源，智能硬盘依次连接；所述计算机硬盘电源用于控制计算机智能硬盘。

[0006] 本发明专利具有以下有益效果：

本发明专利可以在用户联网的情况下对计算机信息的安全起到很好的保护作用，有效地保护了用户计算机带有信息的计算机硬盘，使得网络黑客无法窃取和攻击计算机的硬盘。

附图说明

[0007] 图 1 本发明专利的电路结构示意图。

[0008] 图中：1- 计算机网络控制智能模块、2- 网络信息接收模块、3- 信息安全智能识别模块、4- 信息智能处理模块、5- 网络信息智能接触器、6- 计算机硬盘电源、7- 智能硬盘、8- 智能微处理器、9- 接口转化部分、10- 计算机串口。

具体实施方式

[0009] 下面结合附图，对本发明专利进一步详细说明。

实施例

[0010] 本发明专利的工作过程：

未连接网络时的状态：打开用户计算机电源，用户计算机在初始状态下，进入安全模式，此时的计算机网络控制智能模块 1 处于不工作的状态，而此时的计算机与计算机网络是断开的，计算机智能硬盘 9 处于安全状态；

连接网络时的状态：当要更换为联网模式时，用户通过操作应用程序进行控制，此时，计算机网络控制智能模块 1 开始工作，计算机网络控制智能模块 1 中的网络信息接收模块 2 接收来自网络的信息，并传送给信息安全智能识别模块 3，信息安全智能识别模块 3 对接收到的网络信息进行检测，信息智能处理模块 4 对接收到的经信息安全智能识别模块 3 检测后的信息进行处理，对于没有攻击性的网络信息，网络控制智能接触器 5 闭合，计算机硬盘电源 6 接通，计算机智能硬盘 7 接通电源，计算机智能硬盘 7 在联网的状态下可以正常工作；而信息智能处理模块 4 对接收到的经信息安全智能识别模块 3 检测后的信息进行处理，把有攻击性的网络信息应给智能微处理器 4，同时信息智能处理模块 4 发送信号给网络控制智能接触器 5，网络控制智能接触器 5 断开，计算机硬盘电源 6 断开，计算机智能硬盘 7 就与网络断开，处于安全状态。

[0011] 对于智能微处理器 8，当没有接收到攻击性的网络信息时，智能微处理器 8 不发生指令，接口转化部分 9、计算机串口 10 都处于正常工作状态，当智能微处理器 8 接收到攻击性的网络信息时，智能微处理器 8 发出指令，网络信息智能接触器 5 断开，使得计算机处于安全工作状态。

[0012] 利用本发明所述的技术方案，或本领域的技术人员在发明技术方案的启发下，设计出类似的技术方案，而达到上述技术效果的，均是落入本发明的保护范围。

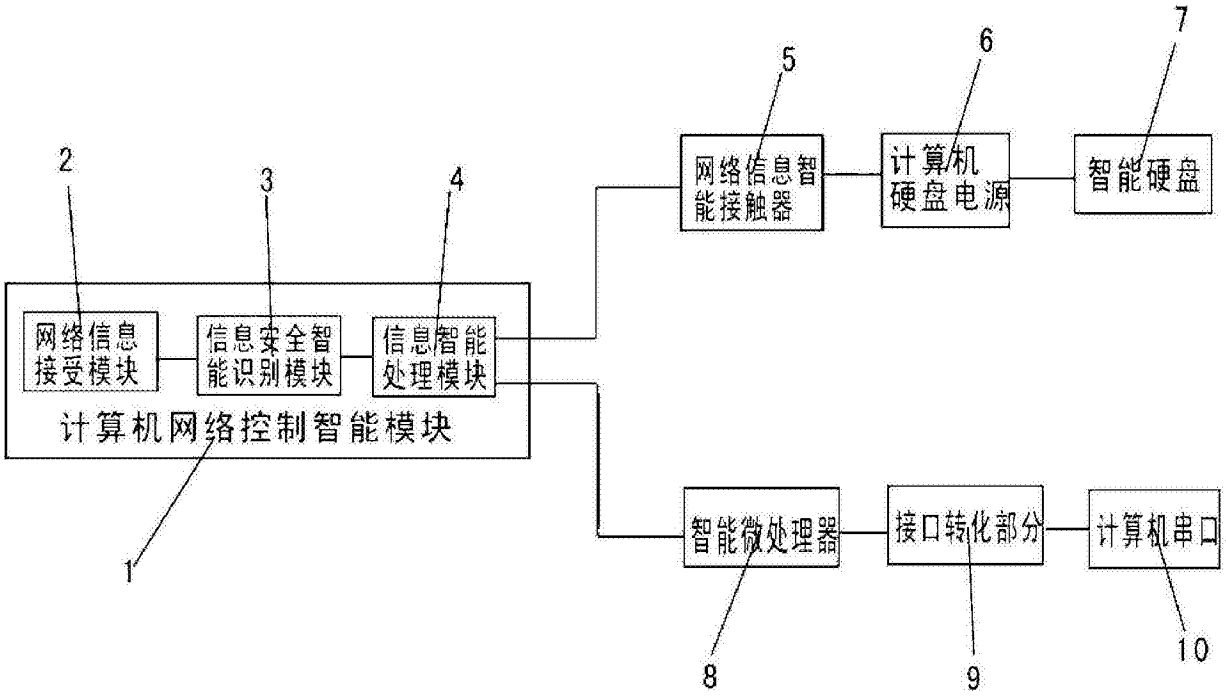

2
3
4
5
6
7
网络信息接受模块
信息安全智能识别模块
信息智能处理模块
计算机网络控制智能模块
网络信息智能接触器
计算机硬盘电源
智能硬盘
智能微处理器
接口转化部分
计算机串口
1
8
9
10

图 1