



(12)实用新型专利

(10)授权公告号 CN 207266061 U

(45)授权公告日 2018.04.20

(21)申请号 201721387448.9

(22)申请日 2017.10.25

(73)专利权人 国家电网公司

地址 100000 北京市西城区西长安街86号

专利权人 国网湖北省电力公司信息通信公司

(72)发明人 郑蕾 袁慧 彭祥礼 邱爽 庄严
邓国如 曹波

(74)专利代理机构 北京超凡志成知识产权代理
事务所(普通合伙) 11371

代理人 王木兰

(51)Int.Cl.

H04L 29/06(2006.01)

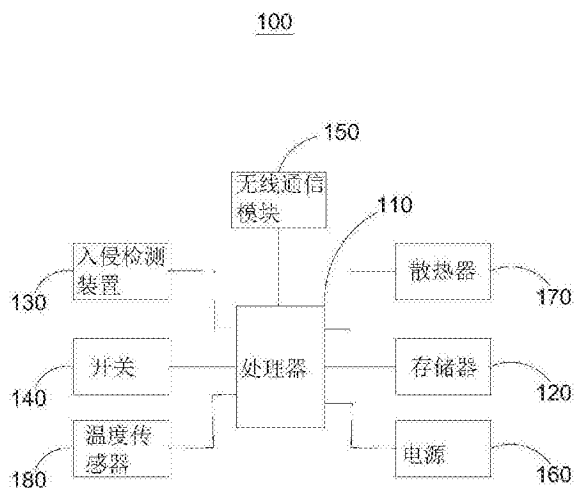
权利要求书1页 说明书5页 附图2页

(54)实用新型名称

网络安全设备与网络安全系统

(57)摘要

本实用新型提供一种网络安全设备与网络安全系统,涉及网络通信领域。网络安全设备包括处理器、存储器、开关以及入侵检测装置,入侵检测装置、开关以及存储器分别与处理器电连接,处理器通过开关接收第一智能终端的数据,并将数据传输至存储器进行存储,入侵检测装置用于检测第一智能终端的入侵信号,并将入侵信号传输至处理器,处理器用于在接收到入侵信号后控制开关断开。本实用新型提供的网络安全设备与网络安全系统具有能够保护用户的文件,避免用户遭受巨大损失的效果。



1. 一种网络安全设备,其特征在于,所述网络安全设备包括处理器、存储器、开关以及入侵检测装置,所述入侵检测装置、所述开关以及所述存储器分别与所述处理器电连接,在所述开关闭合时,所述处理器用于接收一第一智能终端的待存储数据,并将所述待存储数据传输至所述存储器进行存储,所述入侵检测装置用于检测所述第一智能终端的入侵信号,并将所述入侵信号传输至所述处理器,所述处理器用于在接收到所述入侵信号后控制所述开关断开。

2. 如权利要求1所述的网络安全设备,其特征在于,所述网络安全设备还包括无线通信模块,所述无线通信模块与所述处理器电连接,所述无线通信模块用于接收一第二智能终端发送的调用指令,并将所述调用指令传输至所述处理器,所述处理器还用于依据所述调用指令将所述存储器存储的数据通过所述无线通信模块发送至所述第二智能终端。

3. 如权利要求2所述的网络安全设备,其特征在于,所述无线通信模块包括收发模块与天线,所述收发模块包括模拟基带处理电路、数字基带处理电路以及射频电路,所述处理器、所述模拟基带处理电路、所述数字基带处理电路、所述射频电路以及所述天线依次电连接。

4. 如权利要求1所述的网络安全设备,其特征在于,所述网络安全设备还包括外壳,所述处理器与所述开关均置于所述外壳内。

5. 如权利要求4所述的网络安全设备,其特征在于,所述网络安全设备还包括散热器,所述散热器安装于所述外壳内,且所述散热器与所述处理器电连接,所述处理器还用于控制所述散热器的开启与关闭。

6. 如权利要求5所述的网络安全设备,其特征在于,所述网络安全设备还包括温度传感器,所述温度传感器安装于所述外壳内,且所述温度传感器与所述处理器电连接,所述温度传感器用于检测所述外壳内的温度信息,并将所述温度信息传输至所述处理器,所述处理器还用于判断所述温度信息是否大于预存储的温度信息,如果是,则控制所述散热器的转速增大。

7. 如权利要求1所述的网络安全设备,其特征在于,所述入侵检测装置包括IPS检测装置。

8. 如权利要求1所述的网络安全设备,其特征在于,所述网络安全设备还包括电源,所述电源与所述处理器电连接。

9. 如权利要求1所述的网络安全设备,其特征在于,所述开关为继电器。

10. 一种网络安全系统,其特征在于,所述网络安全系统包括第一智能终端与如权利要求1至9任意一项所述的网络安全设备,所述网络安全设备与所述第一智能终端通信连接,且所述网络安全设备用于接收所述智能终端传输的数据并存储。

网络安全设备与网络安全系统

技术领域

[0001] 本实用新型涉及网络通信领域,具体而言,涉及一种网络安全设备与网络安全系统。

背景技术

[0002] 目前,随着互联网的发展,给人们带来了非常多的便利,但是,与此同时,网络安全事件频发,很多黑客通过网络肆意入侵并攻击他人电脑,给很多用户带来了巨大的损失。

[0003] 当用户的电脑被黑客攻击后,重要文件也可能损坏,且这种损坏是不可逆的,即用户可能会发现存储的重要文件无法打开,且无法进行文件的修复,从而使用户遭受到巨大的损失。

[0004] 有鉴于此,如何保护用户的文件信息安全,是本领域技术人员关注的重点。

实用新型内容

[0005] 本实用新型的目的在于提供一种网络安全设备,以解决现有技术中用户电脑被黑客攻击后文件受到损坏,且无法对文件进行修复的问题。

[0006] 本实用新型的目的还在于提供一种应用上述网络安全设备的网络安全系统,以解决现有技术中用户电脑被黑客攻击后文件受到损坏,且无法对文件进行修复的问题。

[0007] 本实用新型是这样实现的:

[0008] 一方面,本实用新型实施例提供了一种网络安全设备,所述网络安全设备包括处理器、存储器、开关以及入侵检测装置,所述入侵检测装置、所述开关以及所述存储器分别与所述处理器电连接,在所述开关闭合时,所述处理器用于接收一第一智能终端的待存储数据,并将所述待存储数据传输至所述存储器进行存储,所述入侵检测装置用于检测所述第一智能终端的入侵信号,并将所述入侵信号传输至所述处理器,所述处理器用于在接收到所述入侵信号后控制所述开关断开。

[0009] 进一步地,所述网络安全设备还包括无线通信模块,所述无线通信模块与所述处理器电连接,所述无线通信模块用于接收一第二智能终端发送的调用指令,并将所述调用指令传输至所述处理器,所述处理器还用于依据所述调用指令将所述存储器存储的数据通过所述无线通信模块发送至所述第二智能终端。

[0010] 进一步地,所述无线通信模块包括收发模块与天线,所述收发模块包括模拟基带处理电路、数字基带处理电路以及射频电路,所述处理器、所述模拟基带处理电路、所述数字基带处理电路、所述射频电路以及所述天线依次电连接。

[0011] 进一步地,所述网络安全设备还包括外壳,所述处理器与所述开关均置于所述外壳内。

[0012] 进一步地,所述网络安全设备还包括散热器,所述散热器安装于所述外壳内,且所述散热器与所述处理器电连接,所述处理器还用于控制所述散热器的开启与关闭。

[0013] 进一步地,所述网络安全设备还包括温度传感器,所述温度传感器安装于所述外

壳内,且所述温度传感器与所述处理器电连接,所述温度传感器用于检测所述外壳内的温度信息,并将所述温度信息传输至所述处理器,所述处理器还用于判断所述温度信息是否大于预存储的温度信息,如果是,则控制所述散热器的转速增大。

[0014] 进一步地,所述入侵检测装置包括IPS检测装置。

[0015] 进一步地,所述网络安全设备还包括电源,所述电源与所述处理器电连接。

[0016] 进一步地,所述开关为继电器。

[0017] 另一方面,本实用新型实施例还提供了一种网络安全系统,所述网络安全系统包括第一智能终端与网络安全设备,所述网络安全设备包括处理器、存储器、开关以及入侵检测装置,所述入侵检测装置、所述开关以及所述存储器分别与所述处理器电连接,在所述开关闭合时,所述处理器用于接收所述第一智能终端的待存储数据,并将所述待存储数据传输至所述存储器进行存储,所述入侵检测装置用于检测所述第一智能终端的入侵信号,并将所述入侵信号传输至所述处理器,所述处理器用于在接收到所述入侵信号后控制所述开关断开。

[0018] 相对现有技术,本实用新型具有以下有益效果:

[0019] 本实用新型提供的一种网络安全设备与网络安全系统,该网络安全装置包括处理器、存储器、开关以及入侵检测装置,入侵检测装置、开关以及存储器分别与处理器电连接,处理器可以通过开关与用户的电脑通信连接,实时接收电脑传输的数据,并将该数据传输至存储器中进行存储。即当用户在智能终端中存储有重要文件时,该文件也会同时被传输至网络安全设备中进行存储备份。当有黑客攻击该电脑时,入侵检测装置能够检测到电脑正在被黑客攻击,此时,入侵检测装置会将检测到的入侵信号传输至处理器,处理器接收到入侵信号后,会断开开关,使得网络安全设备与电脑之间的通信连接断开。由于网络安全设备与电脑为两个独立的装置,所以即使当黑客攻击电脑,使电脑内存储的文件损坏,也无法损坏到网络安全设备中存储的文件数据,用户在需要使用该文件时,调用该网络安全设备中存储的文件数据即可,从而有效的保护了用户的文件,避免用户遭受巨大损失。

[0020] 为使本实用新型的上述目的、特征和优点能更明显易懂,下文特举较佳实施例,并配合所附附图,作详细说明如下。

附图说明

[0021] 为使本实用新型实施例的目的、技术方案和优点更加清楚,下面将结合本实用新型实施例中的附图,对本实用新型实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例是本实用新型一部分实施例,而不是全部的实施例。通常在此处附图中描述和示出的本实用新型实施例的组件可以以各种不同的配置来布置和设计。因此,以下对在附图中提供的本实用新型的实施例的详细描述并非旨在限制要求保护的本实用新型的范围,而是仅仅表示本实用新型的选定实施例。基于本实用新型中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本实用新型保护的范围。

[0022] 图1示出了本实用新型第一实施例所提供的网络安全设备的电路连接框图。

[0023] 图2示出了本实用新型第一实施例所提供的网络安全设备与第二智能终端的交互示意图。

[0024] 图3示出了本实用新型第一实施例所提供的无线通信模块与处理器的电路连接框图。

[0025] 图4示出了本实用新型第二实施例所提供的网络安全系统的交互示意图。

[0026] 图标:100-网络安全设备;110-处理器;120-存储器;130-入侵检测装置;140-开关;150-无线通信模块;151-收发模块;1511-模拟基带处理电路;1512-数字基带处理电路;1513-射频电路;152-天线;160-电源;170-散热器;180-温度传感器;201-第二智能终端;202-网络;300-网络安全系统;310-第一智能终端。

具体实施方式

[0027] 下面将结合本实用新型实施例中附图,对本实用新型实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本实用新型一部分实施例,而不是全部的实施例。通常在此处附图中描述和示出的本实用新型实施例的组件可以以各种不同的配置来布置和设计。因此,以下对在附图中提供的本实用新型的实施例的详细描述并非旨在限制要求保护的本实用新型的范围,而是仅仅表示本实用新型的选定实施例。基于本实用新型的实施例,本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例,都属于本实用新型保护的范围。

[0028] 在本实用新型的描述中,还需要说明的是,除非另有明确的规定和限定,术语“设置”、“安装”、“相连”、“连接”应做广义理解,例如,可以是固定连接,也可以是可拆卸连接,或一体地连接;可以是机械连接,也可以是电连接;可以是直接相连,也可以通过中间媒介间接相连,可以是两个元件内部的连通。对于本领域的普通技术人员而言,可以根据具体情况理解上述术语在本实用新型中的具体含义。

[0029] 应注意到:相似的标号和字母在下面的附图中表示类似项,因此,一旦某一项在一个附图中被定义,则在随后的附图中不需要对其进行进一步定义和解释。

[0030] 下面结合附图,对本实用新型的一些实施方式做详细说明。在不冲突的情况下,下述的实施例及实施例中的特征可以相互组合。

[0031] 第一实施例

[0032] 请参阅图1,本实用新型实施例提供了一种网络安全设备100,该网络安全设备100包括处理器110、存储器120、开关140以及入侵检测装置130,入侵检测装置130、开关140以及存储器120分别与处理器110电连接。

[0033] 具体地,在本实施例中,为了实现该网络安全设备100与第一智能终端(如电脑)之间的数据传输,处理器110通过开关140与该第一智能终端建立通信连接,当用户在电脑上存储重要的文件时,电脑会同时将该文件传输至处理器110,并通过处理器110将文件传输至存储器120重进行存储,从而实现了文件的同步存储。

[0034] 需要说明的是,由于本实施例中提供的网络安全设备100的存储器120的存储空间有限,有鉴于此,在建立网络安全设备100与电脑的通信连接之前,可预先设定相应的存储协议,例如,用户存储在D盘中的文件为重要文件,即建立的存储协议为网络安全设备100与电脑的D盘同步,当用户在D盘中存储文件时,电脑自动将文件传输至网络安全设备100中,从而实现了文件的同步存储。

[0035] 在本实施例中,入侵检测装置130为IPS检测装置,即该入侵检测装置130包括有

IPS(入侵防御系统),当然地,在其它的一些实施例中,入侵检测装置130也可以为其它装置,本实施例对此并不做任何限定。入侵检测装置130能够检测出该第一智能终端是否被何可入侵,一旦检测到第一智能终端被何可入侵,入侵检测装置130可向处理器110传输入侵信号,当处理器110接收到入侵信息时,会控制开关140断开,从而使本实施例提供的网络安全设备100与第一智能终端之间的通信连接断开。由于本实施例提供的网络安全设备100相对于第一智能终端而言为独立的设备,所以即使当第一智能终端被黑客入侵,导致存储的文件损坏,黑客也无法入侵到网络安全设备100,保证了网络安全设备100中存储的文件的安全性。

[0036] 需要说明的是,在本实施例中,为了达到控制器能够控制开关140开启与闭合的效果,开关140选用继电器,继电器为一种可用于自动化控制的开关140,当然地,在其它的一些实施例中,开关140也选用其它装置,本实施例对此并不做任何限定。

[0037] 请参阅图2,在本实施例中,为了方便用户利用其它智能终端读取网络安全设备100中的数据,网络安全设备100还包括无线通信模块150,无线通信模块150与处理器110电连接,用户可将第二智能终端201通过网络202与无线通信模块150建立通信连接,从而使第二智能终端201可以向无线通信模块150发送调用指令,无线通信模块150在接收到调用指令后,可将该调用指令传输至处理器110,并由处理器110依据该调用指令将存储器120中存储的数据通过无线通信模块150发送至第二智能终端201,从而实现了网络安全设备100与第二智能终端201之间的数据传输。

[0038] 并且,通过设置无线通信模块150,还可使得用户通过手机等移动智能终端读取电脑等固定智能终端的数据信息。通过将电脑等智能终端中的文件数据传输至本实施例提供的网络安全设备100,然后通过手机等移动智能终端读取网络安全设备100中的文件数据的方式,即可实现文件数据的交互,使用户更加方便。

[0039] 具体的,请参阅图3,在本实施例中,无线通信模块150包括收发模块151与天线152,收发模块151包括模拟基带处理电路1511、数字基带处理电路1512以及射频电路1513,处理器110、模拟基带处理电路1511、数字基带处理电路1512、射频电路1513以及天线152依次电连接,从而实现了网络安全设备100与第二智能终端201之间的数据交互。

[0040] 需要说明的是,在本实施例中,第二智能终端201与网络安全设备100之间采用无线的方式进行数据传输,但在其它的一些实施例中,第二智能终端201与网络安全设备100之间也可采用有线的方式进行数据传输,本实施例对此并不做任何限定。

[0041] 当然地,为了为整个网络安全设备100供电,网络安全设备100还包括电源160,电源160与处理器110电连接。

[0042] 为了使网络安全设备100整体更加美观,在本实施例总,网络安全设备100还包括外壳,处理器110、开关140、电源160以及无线通信模块150均置于外壳内。

[0043] 由于在工作环境下,处理器110对温度有一定的要求,所以在本实施例中,网络安全设备100还包括散热器170,散热器170安装于外壳内,且散热器170与处理器110电连接,处理器110还用于控制散热器170的开启与关闭。

[0044] 需要说明的是,本实施例提供的散热器170包括但不限于风扇。

[0045] 不仅如此,为了达到节能的效果,散热器170以低速运行,保证空气流通即可,但有时可能出现外壳内温度过高的情况的出现。有鉴于此,在本实施例中,网络安全设备100还

包括温度传感器180,温度传感器180安装于外壳内,且温度传感器180与处理器110电连接,温度传感器180能够检测外壳内的温度信息,并将温度信息传输至所处理器110,处理器110还能够判断温度信息是否大于预存储的温度信息,如果是,则控制散热器170的转速增大,从而使空气流通的速度增强,达到有效散热的效果。

[0046] 需要说明的是,通过设置温度传感器180,使得散热器170在正常工作时可以低速运转,当温度较高时,处理器110能够通过控制输出功率的方式控制散热器170的转速增大,使本实施例提供的网络安全设备100不仅节能,且始终处于正常运行状态。

[0047] 第二实施例

[0048] 请参阅图4,本实用新型实施例提供了一种网络安全系统300,该网络安全系统300包括第一智能终端310与第一实施例所述的网络安全设备100,网络安全设备100与第一智能终端310通信连接,且网络安全设备100用于接收智能终端传输的数据并存储。需要说明的是,由于本实施例提供的网络安全设备100与第一实施例提供的网络安全设备100的结构与功能均相同,所以在本实施中不再对网络安全设备100的机构与功能进行赘述。

[0049] 综上所述,本实用新型提供的一种网络安全设备与网络安全系统,该网络安全装置包括处理器、存储器、开关以及入侵检测装置,入侵检测装置、开关以及存储器分别与处理器电连接,处理器可以通过开关与用户的电脑通信连接,实时接收电脑传输的数据,并将该数据传输至存储器中进行存储。即当用户在智能终端中存储有重要文件时,该文件也会同时被传输至网络安全设备中进行存储备份。当有黑客攻击该电脑时,入侵检测装置能够检测到电脑正在被黑客攻击,此时,入侵检测装置会将检测到的入侵信号传输至处理器,处理器接收到入侵信号后,会断开开关,使得网络安全设备与电脑之间的通信连接断开。由于网络安全设备与电脑为两个独立的装置,所以即使当黑客攻击电脑,使电脑内存储的文件损坏,也无法损坏到网络安全设备中存储的文件数据,用户在需要使用该文件时,调用该网络安全设备中存储的文件数据即可,从而有效的保护了用户的文件,避免用户遭受巨大损失。

[0050] 在本实用新型的描述中,需要说明的是,术语“第一”、“第二”等仅用于区分描述,而不能理解为指示或暗示相对重要性。以上所述仅为本实用新型的优选实施例而已,并不用于限制本实用新型,对于本领域的技术人员来说,本实用新型可以有各种更改和变化。凡在本实用新型的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本实用新型的保护范围之内。

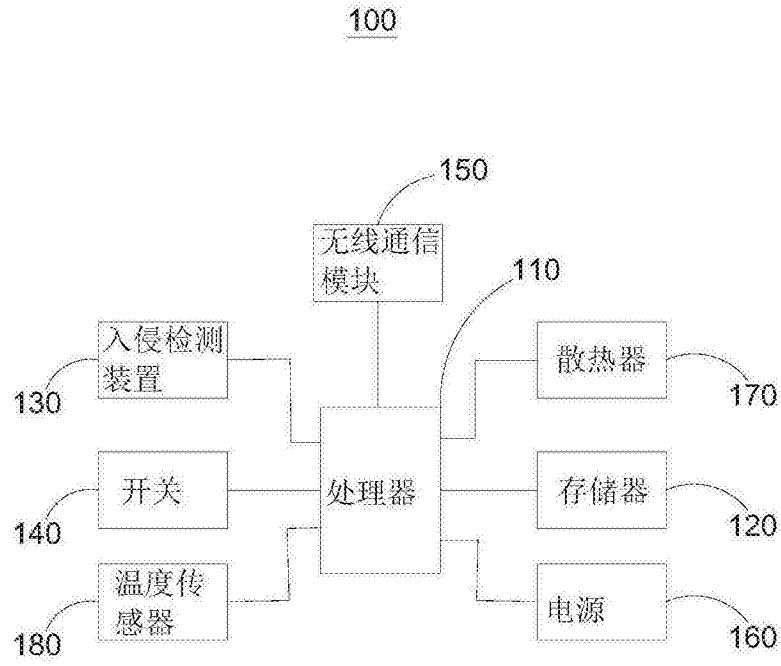


图1



图2

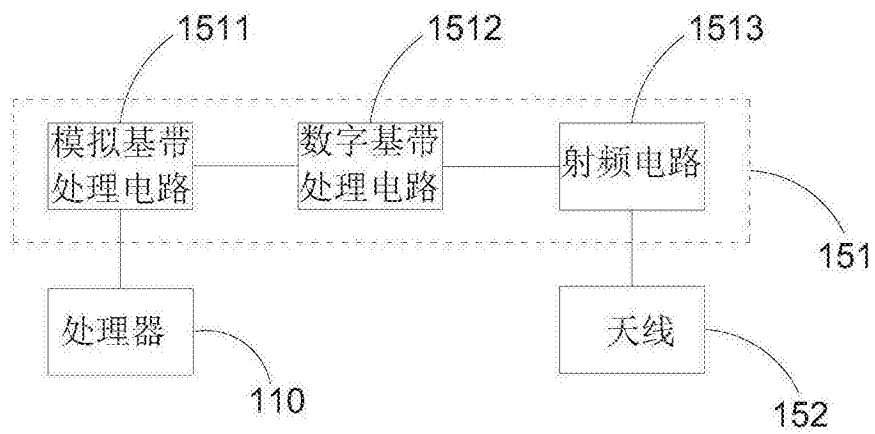


图3

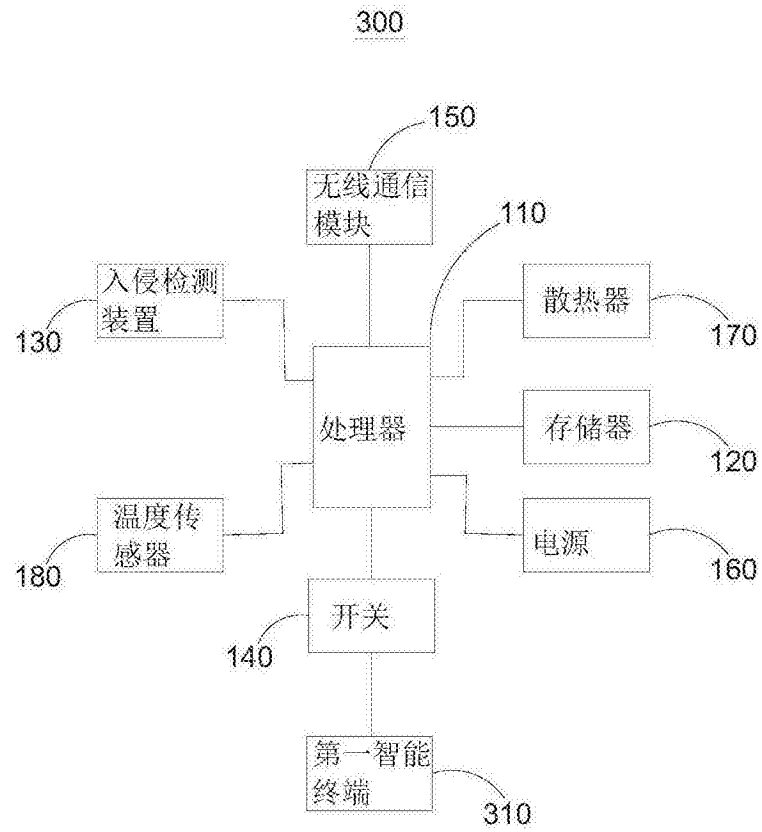


图4