

(12) 发明专利

(10) 授权公告号 CN 101924765 B

(45) 授权公告日 2013. 04. 17

(21) 申请号 201010258827. 4

CN 1687861 A, 2005. 10. 26, 全文.

(22) 申请日 2010. 08. 20

CN 1928881 A, 2007. 03. 14, 全文.

(73) 专利权人 河南省电力公司

审查员 曹晓宁

地址 450052 河南省郑州市嵩山南路 87 号
河南省电力公司科技信息部

(72) 发明人 周凤珍 杨成兴 智海燕 丁文彦
张勇 秦龙 周林峰 王宏斌
赵东

(74) 专利代理机构 郑州红元帅专利代理事务所
(普通合伙) 41117

代理人 徐皂兰

(51) Int. Cl.

H04L 29/06 (2006. 01)

(56) 对比文件

US 2003/0226015 A1, 2003. 12. 04, 全文.

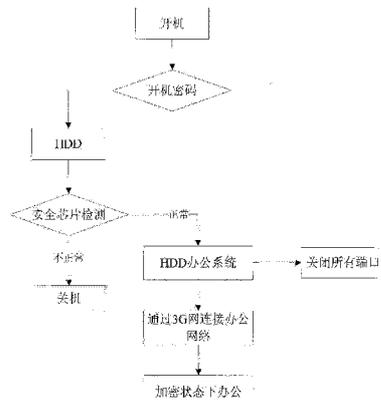
权利要求书 1 页 说明书 2 页 附图 1 页

(54) 发明名称

一种单系统单网络计算机通讯方法

(57) 摘要

本发明公开了一种单系统单网络计算机通讯方法,包括如下步骤:步骤一,主板内置 3G 通讯模块和 USB 端口,USB 端口连接内置的安全加密芯片加密;步骤二,设置 BIOS,使系统只能从指定 USB 端口的安全加密芯片启动;步骤三,系统开机,判断安全加密芯片是否正常工作,如不能正常工作,则系统自动关机;步骤四,如果安全加密芯片正常工作,则进入步骤五;步骤五,系统从硬盘启动,保留一个 VGA 接口和内置的 USB 接口,关闭其它端口;步骤六,通过 3G 网络连接内网,对硬盘进行加密设置。本发明通过内置安全加密芯片和关闭外部端口,保证了内网的信息安全,可广泛应用到内网信息安全要求高的政府机构、企业、事业单位等机构。



1. 一种单系统单网络计算机通讯方法,其特征在于:包括如下步骤:
步骤一,主板内置 3G 通讯模块和 USB 端口,USB 端口连接内置的安全加密芯片;
步骤二,设置 BIOS,使系统只能从指定 USB 端口的安全加密芯片启动;
步骤三,系统开机,判断安全加密芯片是否正常工作;
步骤四,如果安全加密芯片不能正常工作则系统自动关机,如果安全加密芯片正常工作则进入步骤五;
步骤五,系统从硬盘启动,保留一个 VGA 接口和内置的 USB 接口,关闭其它端口;
步骤六,通过 3G 网络连接内网,对硬盘进行加密设置。
2. 根据权利要求 1 所述的一种单系统单网络计算机通讯方法,其特征在于:步骤五中,端口的关闭是通过物理硬件方式进行,即通过在主板上取消该计算机的硬件连接端口,同时在整机系统的外部机构将该端口的开孔处进行物理永久封闭。
3. 根据权利要求 2 所述的一种单系统单网络计算机通讯方法,其特征在于:在 BIOS 中进行设置,屏蔽关闭端口的硬件地址和中断。

一种单系统单网络计算机通讯方法

技术领域

[0001] 本发明涉及一种计算机通讯方法,具体涉及一种单系统单网络计算机通讯方法。

背景技术

[0002] 随着计算机的普及和网络的发展,计算机在人们工作、生活中的作用也越来越大,互联网上的信息安全问题也越来越受到关注。为了保护内部的信息安全,很多单位禁止内网办公电脑连接互联网,但是一旦某台内网上的办公电脑连接了互联网或通过外部端口拷贝数据,就很容易导致信息泄露,感染病毒及木马等具有安全威胁的黑客软件,再内接办公网络(即内网),导致给办公网络带来安全威胁。

发明内容

[0003] 本发明的目的在于提供一种单系统单网络计算机通讯方法,通过内置安全加密芯片和关闭外部端口,保证了内网的信息安全。

[0004] 本发明采用以下技术方案:

[0005] 一种单系统单网络计算机通讯方法,包括如下步骤:

[0006] 步骤一,主板内置 3G 通讯模块和 USB 端口,USB 端口连接内置的安全加密芯片加密;

[0007] 步骤二,设置 BIOS,使系统只能从指定 USB 端口的安全加密芯片启动;

[0008] 步骤三,系统开机,判断安全加密芯片是否正常工作,如不能正常工作,则系统自动关机;

[0009] 步骤四,如果安全加密芯片正常工作,则进入步骤五;

[0010] 步骤五,系统从硬盘启动,保留一个 VGA 接口和内置的 USB 接口,关闭其它端口;

[0011] 步骤六,通过 3G 网络连接内网,对硬盘进行加密设置。

[0012] 作为本发明的一种优选方式,步骤五中,端口的关闭是通过物理硬件方式进行,即通过在主板上取消该设备的硬件连接端口,同时在整机系统的外部机构将该端口的开孔处进行物理永久封闭。

[0013] 作为本发明的另一优选方式,在 BIOS 中进行设置,屏蔽关闭端口的硬件地址和中断。

[0014] 本发明的有益效果是:

[0015] 本发明设置了安全加密芯片,通过该加密芯片对系统进行加密管理,分别实现系统通讯数据加密,系统网络连接加密。有效防止了办公电脑外接互联网而导致信息泄露,感染病毒及木马等具有安全威胁的黑客软件,再内接办公网络,导致给办公网络带来安全威胁。同时为了保证用户硬件系统信息的保密安全,本发明还取消相应的外部硬件设备通讯及连接端口,以保证用户硬盘的信息数据不泄漏。

[0016] 本发明通过在软件层级 Bios 里对系统外接硬件设备的端口禁用及中断控制和在物理层级对系统的外接硬件设备端口实行裁减,外部端口部分永久封闭,实现了办公环境

下的信息安全,信息无法被非法获得、截取。并且通过 Bios 特殊设置,计算机只能从指定 USB 端口的安全加密芯片启动,无法从其他 USB 端口的 USB 启动设备启动。本发明基于 3G 网络连接,通过加密芯片进行数据通讯加密;仅可接入用户的办公网络,如电力行业的办公内网,无法连接外部的 Internet 网络。

本发明可在电力系统内部使用,也可广泛应用到内网信息安全要求较高的政府机构、企业、事业单位等机构。

[0017] 本发明的其他优点、目标和特征在某种程度上将在随后的说明书中进行阐述,并且在某种程度上,基于对下文的考察研究对本领域技术人员而言将是显而易见的,或者可以从本发明的实践中得到教导。本发明的目标和其他优点可以通过下面的说明书或者附图中所特别指出的结构来实现和获得。

附图说明

[0018] 图 1 是本发明的系统启动原理图。

具体实施方式

[0019] 下面结合附图和实施例对本发明作进一步描述:

[0020] 主板内置 3G 通讯模块 (EVDO/WCDMA/TD-SCDMA),确保所有对外通信只能通过上述无线通信模块。采用内置 USB 端口,连接内置的安全加密芯片进行加密管理。

[0021] 如图 1 所示,本发明包括如下步骤:

[0022] 步骤一,主板内置 3G 通讯模块和 USB 端口,USB 端口连接内置的安全加密芯片加密;

[0023] 步骤二,设置 BIOS,使系统只能从指定 USB 端口的安全加密芯片启动;

[0024] 步骤三,系统开机,判断安全加密芯片是否正常工作,如不能正常工作,则系统自动关机;

[0025] 步骤四,如果安全加密芯片正常工作,则进入步骤五;

[0026] 步骤五,系统从硬盘启动,保留一个 VGA 接口和内置的 USB 接口,关闭其它端口;

[0027] 步骤六,通过 3G 网络连接内网,对硬盘进行加密设置。

[0028] 取消的外部端口包括:网卡设备,无线网卡设备,串口,1394 接口,读卡器接口,HDMI 接口,Displayport 接口,Esata 接口,PCMCIA 接口等。保留的端口:VGA(连接外解显示器/投影设备)和内置的 USB 端口。通过 Bios 特殊设置,使电脑只能从指定 USB 端口的安全加密芯片启动,无法从其他 USB 端口的 USB 启动设备启动。

[0029] 以上所有取消的端口,是通过在主板上取消该设备的硬件连接端口,同时在整机系统的外部机构将该端口的开孔处进行物理永久封闭,以保证外部设备无法通过以上的端口连接到主机,侵入读取数据。通过主机的 BIOS 硬件管理系统,在 BIOS 中进行设置,将以上所有端口的硬件地址和中断屏蔽,在上层操作系统中该端口无法被识别并使用。本发明是分别通过物理硬件方式及软件方式将外部端口屏蔽以防止硬盘信息的泄漏。

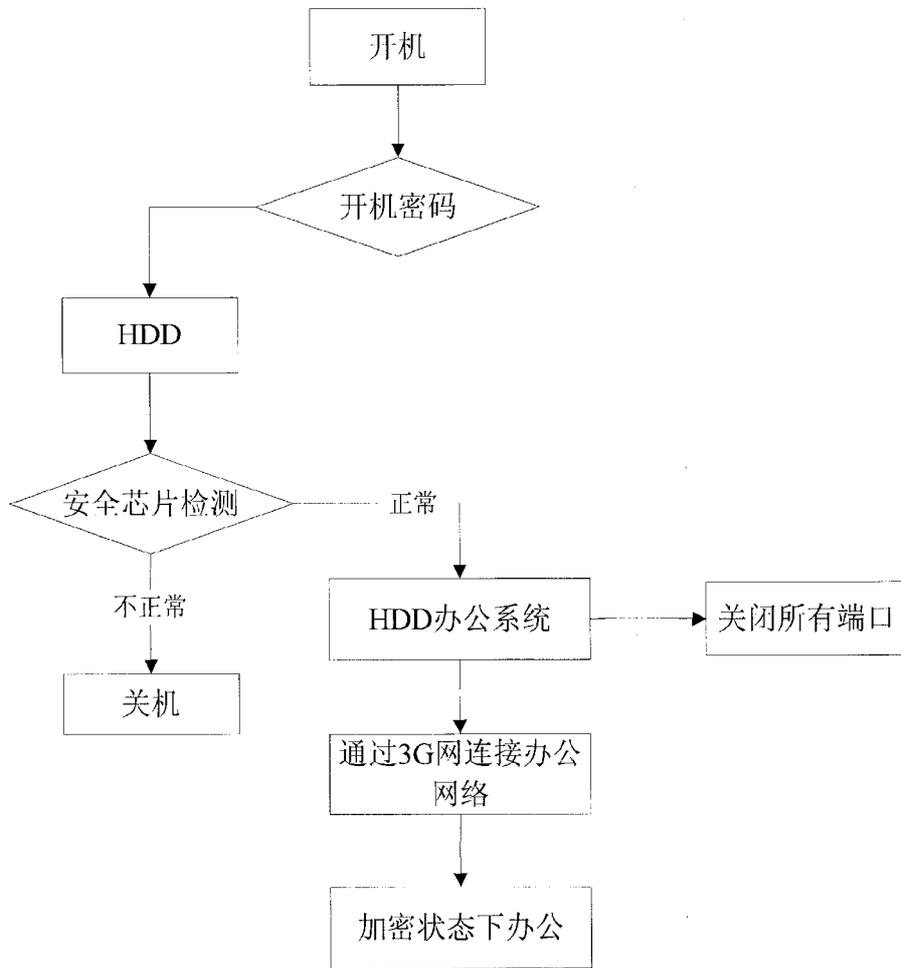


图 1