



(12) 发明专利申请

(10) 申请公布号 CN 101720545 A

(43) 申请公布日 2010.06.02

(21) 申请号 200880014890.4

(74) 专利代理机构 北京市柳沈律师事务所

(22) 申请日 2008.04.06

11105

代理人 黄小临

(30) 优先权数据

60/910,708 2007.04.09 US

11/769,760 2007.06.28 US

11/769,757 2007.06.28 US

(51) Int. Cl.

H04L 29/00 (2006.01)

G06F 21/00 (2006.01)

(85) PCT申请进入国家阶段日

2009.11.05

(86) PCT申请的申请数据

PCT/IL2008/000473 2008.04.06

(87) PCT申请的公布数据

W02008/122976 EN 2008.10.16

(71) 申请人 桑迪士克以色列有限公司

地址 以色列萨巴

(72) 发明人 伊泰·戈尔德 亚历山大·佩利

利奥尼德·什马尔维科

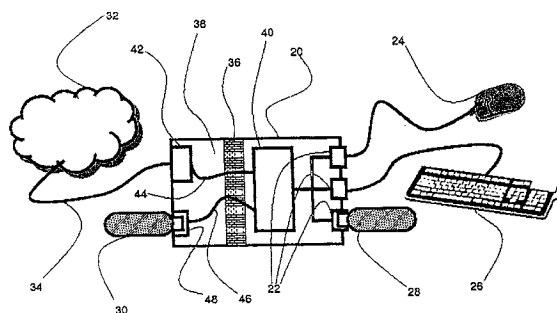
权利要求书 1 页 说明书 3 页 附图 3 页
按照条约第19条的修改 1 页

(54) 发明名称

使用对于 USB 存储设备的防火墙保护的系统和
方法

(57) 摘要

本发明公开了 USB 可移除驱动器 (URD) 和用于保护主机系统免于 URD 引起的信息安全风险的方法,该 URD 包括:具有程序代码的非易失性存储器,其中所述程序代码被配置为使能用于与主机系统通信的网络协议;以及控制器,用于控制在所述存储器上执行的操作。优选地,存储器包括闪存。一种 URD 包括:具有防火墙的主机系统;以及具有非易失性存储器的 URD,其中所述存储器包括程序代码,以及其中所述程序代码被配置为使能网络协议,所述 URD 可操作地连接到所述主机系统;其中所述防火墙被配置为提供与所述 URD 有关的安全措施。优选地,防火墙是软件防火墙或硬件防火墙。



1. 一种 URD, 包括 :
 - (a) 具有程序代码的非易失性存储器, 其中所述程序代码被配置为使能用于与主机系统通信的网络协议 ; 以及
 - (b) 控制器, 用于控制在所述存储器上执行的操作。
2. 根据权利要求 1 的 URD, 其中所述存储器包括闪存。
3. 一种系统, 包括 :
 - (a) 具有防火墙的主机系统 ; 以及
 - (b) 具有非易失性存储器的 URD, 其中所述存储器包括程序代码, 以及其中所述程序代码被配置为使能网络协议, 所述 URD 可操作地连接到所述主机系统 ;
其中所述防火墙被配置为提供与所述 URD 有关的安全措施。
4. 根据权利要求 3 的系统, 其中所述防火墙是软件防火墙。
5. 根据权利要求 3 的系统, 其中所述防火墙是硬件防火墙。
6. 一种用于保护主机系统免于 URD 引起的信息安全风险的方法, 该方法包括步骤 :
 - (a) 将 URD 可操作地连接到主机系统 ;
 - (b) 通过常驻于主机系统中的防火墙, 经由网络协议, 在 URD 和主机系统之间通信 ; 以及
 - (c) 配置所述防火墙以提供与 URD 有关的安全措施。
7. 根据权利要求 6 的方法, 其中所述防火墙是软件防火墙。
8. 根据权利要求 6 的方法, 其中所述防火墙是硬件防火墙。
9. 一种用于保护主机系统免于 URD 引起的信息安全风险的方法, 该方法包括步骤 :
 - (a) 将 URD 可操作地连接到主机系统 ;
 - (b) 通过常驻于主机系统上的防火墙, 经由网络协议在 URD 和主机系统之间通信 ; 以及
 - (c) 配置所述防火墙以限制至少一个应用对 URD 的访问。
10. 根据权利要求 9 的方法, 其中所述防火墙是软件防火墙。
11. 根据权利要求 9 的方法, 其中所述防火墙是硬件防火墙。

使用对于 USB 存储设备的防火墙保护的系统和方法

技术领域

[0001] 本发明涉及用于通过经由网络协议传输通信并应用防火墙来保护主机系统免于大容量存储设备引起的信息安全风险的系统。

背景技术

[0002] USB 闪存驱动器 (UFD) 是用于提供便携式数据存储的公知设备。UFD 典型地被配置为可交换地连接到多个计算机。由于此特征, UFD 引起对主计算机的固有信息安全风险。这种风险使得安全措施的实施成为必要。

[0003] 现有技术提供了用于保护主计算机免于与便携式数据存储设备有关的风险的各种安全措施。这种安全措施的例子包括反病毒程序和 mTrust 方案 (可从以色列的 Kfar Saba 的 SanDisk 以色列公司获得)。

[0004] 现有技术解决方案承受着降低其价值的固有限制。该现有技术典型地被配置为仅处理一种类型的安全风险。反病毒工具典型地限于仅处理病毒, 而 mTrust 类型方案限于处理主要与访问控制有关的风险。

[0005] 期望具有一种信息安全系统, 用于保护主机系统免于 UFD 安全引起的大批的信息安全风险, 同时符合主机系统用户的安息安全策略。

发明内容

[0006] 本发明的目的是提供用于通过经由网络协议传输通信并通过应用防火墙来保护主机系统免于大容量存储设备引起的信息安全风险的系统。

[0007] 为了清楚, 特别定义了以下一些术语在此使用。在此使用术语“网络协议”来指代来自 OSI (开放式系统互联) 网络体系的网络层的通信协议, 更具体地, 在此是因特网协议 (IP)。在此使用术语“USB 可移除驱动器”和“URD”来指代具有非易失性存储器和控制器的可移除驱动器。UFD 是特定类型的 URD, 其中利用了闪存。

[0008] 在此使用术语“流量”来指代在给定时间段期间通信系统中的活动。在此使用术语“非武装区 (demilitarized area)”和“DMZ”来指代既不是内部网络的部分、也不直接是因特网的部分的网络的一部分。在此使用术语“防火墙”来指代根据本地访问安全策略来限制网络之间的访问的网关。

[0009] 本发明教导如下系统和用于实现这种系统的方法, 所述系统常驻于 URD 中, 并仿真用于主机系统的网络驱动器。通过改变常驻于 URD 控制器中的固件, 并通过使得 URD 能够作为 Microsoft™ Windows™ 操作系统 (OS) 上的网络设备, 来执行网络驱动器仿真。URD 被识别为网络设备, 并且可以由各种文件访问协议 (例如 HTTP、FTP 和 SMB) 访问。网络设备由驱动器名指定, 或者被指定为文件服务器 (计算机工程领域公知的, 被集成在 Windows OS 中)。

[0010] 网络驱动器是使用普通防火墙系统 (例如, 可从加利福尼亚 Sunnyvale 的 McAfee 公司获得的 McAfee 个人防火墙) 的用于保护的一般设备。一旦装有防火墙的主机系统检

测到作为网络存储设备的存储设备,主机系统就应用相关防火墙的所有相干规则,从而保护主机系统免于诸如未经授权访问之类的攻击。

[0011] 因此,根据本发明,第一次提供了包括如下的 URD:(a) 具有程序代码的非易失性存储器,其中所述程序代码被配置为使能用于与主机系统通信的网络协议;以及(b) 控制器,用于控制在所述存储器上执行的操作。

[0012] 优选地,该存储器包括闪存。

[0013] 根据本发明,第一次提供了包括如下的 URD:(a) 具有防火墙的主机系统;以及(b) 具有非易失性存储器的 URD,其中,所述存储器包括程序代码,以及其中,所述程序代码被配置为使能网络协议,所述 URD 可操作地连接到所述主机系统;其中,所述防火墙被配置为提供与所述 URD 有关的安全措施。

[0014] 优选地,防火墙是软件防火墙或硬件防火墙。

[0015] 从以下详细描述和示例中,这些和进一步的实施例将变得明显。

附图说明

[0016] 在此参考附图,仅作为示例描述本发明,附图中:

[0017] 图 1 是根据本发明的优选实施例的具有针对大容量存储设备的防火墙保护的主机系统的简化方框图;

[0018] 图 2A 是根据现有技术的 URD 的简化方框图;

[0019] 图 2B 是根据本发明的优选实施例的 URD 的简化方框图;

[0020] 图 3 是根据本发明的优选实施例的具有针对大容量存储设备的防火墙保护的主机系统的操作的简化流程图。

具体实施方式

[0021] 本发明涉及用于通过经由网络协议传输通信并通过应用防火墙来保护主机系统免于大容量存储设备引起的信息安全风险的系统。参考随后的描述和附图,将更好地理解根据本发明的用于保护主机系统免于大容量存储设备引起的信息安全风险的原理和操作。

[0022] 现在参考附图,图 1 是根据本发明的优选实施例的具有针对大容量存储设备的防火墙保护的主机系统的简化方框图。图 1 中示出具有三个 USB 连接器 22 的主机系统 20。示出 USB 鼠标 24、USB 键盘 26 和 URD 28,每个可操作地连接到一个连接器 22。网络 32(例如局域网和因特网)可经由网络连接 34 来访问。

[0023] 主机系统 20 装配了防火墙 36。防火墙 36 可以是软件防火墙(例如 MacAfee 个人防火墙)或硬件防火墙(例如可从加利福尼亚,圣何塞的 Cisco 获得的 Cisco PIX 防火墙 515E)。在防火墙 36 以外的区域、典型地称作 DMZ 38,用于连接主机系统 20 与外部世界。流量从外围设备(即 USB 鼠标 24、USB 键盘 26 和 URD 28)流入 CPU 40。主机系统 20 与外部世界的连接典型地经由网卡 42 进行,可操作地连接到网络连接 34,并最终到网络 32。防火墙 36 在保护主机系统 20 免于未经授权访问方面的功能性是本领域公知的,在此不再描述。

[0024] 本发明的重要特征是本地外围设备 30、典型地是 URD 或其他大容量存储设备与主机系统 20 的 DMZ 38 的连接。这样的配置要求外围设备 30 被主机系统 20 识别为网络设备,而不是识别为大容量存储设备(比如 URD 28)。在这样的配置中,本发明的系统要求 URD 30

达到防火墙 36 的安全特征要求,该要求是强健的并被良好地维持。

[0025] 总言之,在直接连接到主机系统 20 的 URD(例如 URD 28)与连接到 DMZ 38 的 URD(例如 URD 30)之间存在两个差别:

[0026] (1) 通信协议 -URD 28 是大容量存储设备,而外围设备 30 是仿真的网络设备;以及

[0027] (2) 主机系统 20 免于与设备有关的风险的安全级别 - 主机系统 20 不具有防御 URD 28 的任何安全措施,但是具有防御外围设备 30 的全面防火墙保护。

[0028] 图 2A 是根据现有技术的 URD 的简化方框图。图 2A 中示出 URD 50 具有非易失性存储器 52、闪存控制器 54、大容量存储类协议 56 和 USB 连接器 58。数据经由 USB 连接器 58 写和读,并经由大容量存储类协议 56 编码。闪存控制器 54 编码和解码从大容量存储类协议 56 提供的数据,并将该数据写到存储器 52。

[0029] 图 2B 是根据本发明的优选实施例的 URD 的简化方框图。在图 2B 中示出 URD 60 具有非易失性存储器 62、闪存控制器 64、网络协议 66 和 USB 连接器 68。数据经由 USB 连接器 68 写和读,并经由网络协议 66 编码。闪存控制器 64 编码和解码从网络协议 66 提供的数据,并将该数据写到存储器 62。很清楚,根据本发明的系统使得能够将防火墙安全措施应用于 URD 60。

[0030] 图 3 是根据本发明的优选实施例的具有针对大容量存储设备的防火墙保护的主机系统的操作的简化流程图。URD 可操作地连接到主机系统(步骤 70)。URD 的网络协议指定 URD 作为主机系统上的网络设备(步骤 72)。常驻于主机系统上的防火墙检测 URD 网络设备(步骤 74)。由防火墙的安全措施中转在 URD 与主机系统之间的通信(步骤 76)。注意,防火墙还可以被配置为限制特定应用对 URD 的访问。

[0031] 尽管已经关于有限数量的实施例描述了本发明,但是将认识到,可以进行本发明的许多修改、组合和其他应用。

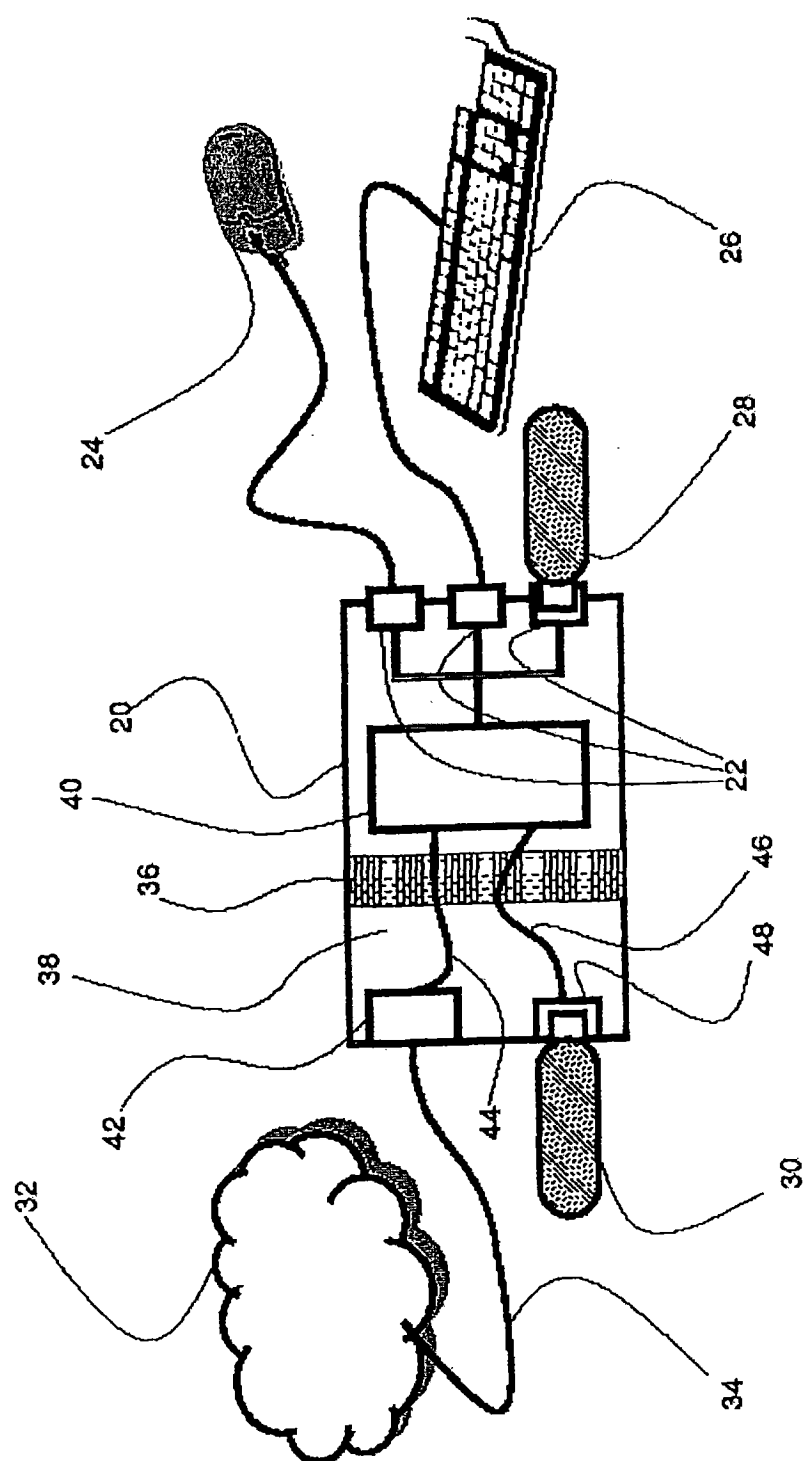


图 1

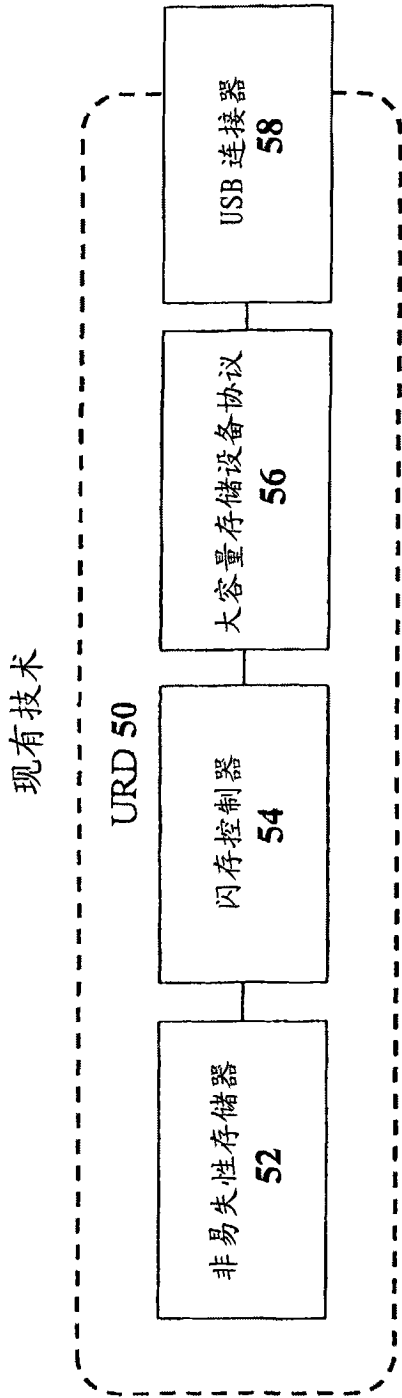


图 2A

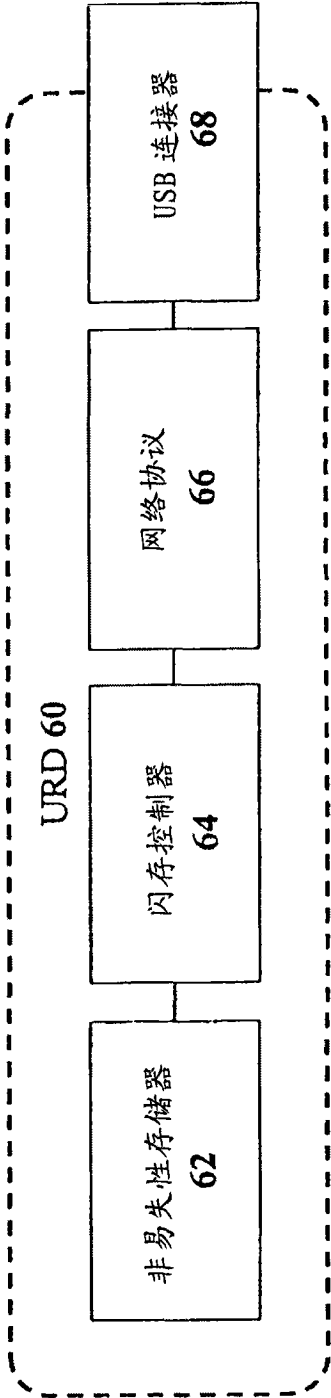


图 2B

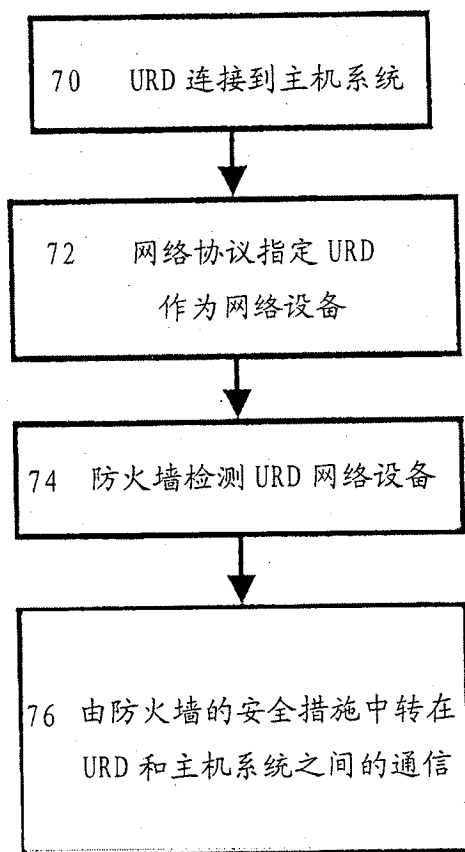


图 3

1. 一种 USB 可移除驱动器 (URD), 包括 :
 - (a) 非易失性存储器 ; 以及
 - (b) 控制器, 用于控制在所述存储器上执行的操作, 以及用于通过仿真网络驱动器来与 URD 的主机通信。
2. 根据权利要求 1 的 URD, 其中所述存储器包括闪存。
3. 根据权利要求 1 的 URD, 其中所述控制器通过使用网络协议与所述主机通信来仿真所述网络驱动器。
4. 根据权利要求 1 的 URD, 其中所述网络驱动器的所述仿真通过所述控制器的固件实现。
5. 一种系统, 包括 :
 - (a) 权利要求 1 的 URD ; 以及
 - (b) 主机系统, 具有被配置为提供与所述 URD 有关的安全措施的防火墙。
6. 根据权利要求 5 的系统, 其中所述防火墙是软件防火墙。
7. 根据权利要求 5 的系统, 其中所述防火墙是硬件防火墙。
8. 一种用于保护主机系统免于 USB 可移除驱动器 (URD) 引起的信息安全风险的方法, 该方法包括步骤 :
 - (a) 将 URD 可操作地连接到主机系统 ;
 - (b) 将 URD 作为网络驱动器呈现给主机系统 ;
 - (c) 通过常驻于主机系统中的防火墙, 经由网络协议在 URD 和主机系统之间通信 ; 以及
 - (d) 配置所述防火墙以提供与 URD 有关的安全措施。
9. 根据权利要求 8 的方法, 其中所述防火墙是软件防火墙。
10. 根据权利要求 8 的方法, 其中所述防火墙是硬件防火墙。
11. 根据权利要求 8 的方法, 其中所述安全措施包括限制至少一个应用对 URD 的访问。