(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 102479302 A
(43)申请公布日 2012.05.30

(21)申请号 201010557454.0

(22)申请日 2010.11.24

(71)申请人 鸿富锦精密工业(深圳)有限公司
地址 518109 广东省深圳市宝安区龙华镇油松第十工业区东环二路 2 号
申请人 鸿海精密工业股份有限公司

(72)发明人 彭爽

(51)Int.Cl.
G06F 21/20(2006.01)

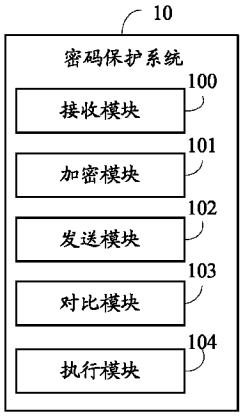
权利要求书 1 页 说明书 3 页 附图 3 页

(54)发明名称

密码保护系统及方法

(57)摘要

一种密码保护系统，包括：接收模块，用于接收用户设置的第一密码及用户输入的第二密码；加密模块，用于对该第一密码生成第一密文，对第二密码生成第二密文；发送模块，用于发送命令给基板管理控制器，通知基板管理控制器读取第一密文；对比模块，用于查看所述第二密文是否与第一密文相同；及执行模块，用于当第二密文与第一密文相同时，启动所述服务器，当第二密文与第一密文不相同且当用户输入第二密码的次数没有超过用户设置的次数时，提示用户重新输入第二密码。本发明还提供了一种密码保护方法，利用本发明，可以对用户设置的密码进行有效地保护。



CN 102479302 A

1. 一种密码保护系统，运行于服务器中，该服务器包括基板管理控制器，其特征在于，所述密码保护系统包括：

接收模块，用于接收用户设置的第一密码及用户输入的第二密码；

加密模块，用于对该第一密码生成第一密文，对第二密码生成第二密文；

发送模块，用于发送命令给基板管理控制器，通知基板管理控制器读取第一密文；

对比模块，用于查看所述第二密文是否与第一密文相同；及

执行模块，用于当第二密文与第一密文相同时，启动所述服务器，当第二密文与第一密文不相同且当用户输入第二密码的次数没有超过用户设置的次数时，提示用户重新输入第二密码。

2. 如权利要求 1 所述的密码保护系统，其特征在于，所述服务器提供一个设置界面，用于接收用户设置所述第一密码。

3. 如权利要求 1 所述的密码保护系统，其特征在于，所述发送模块还用于发送存储命令给基板管理控制器，通知基板管理控制器存储所述第一密文至基板管理控制器的现场可更换部件中。

4. 如权利要求 1 所述的密码保护系统，其特征在于，所述执行模块还用于当第二密文与第一密文不相同且用户输入第二密码的次数超过用户设置的次数时，锁住所述服务器。

5. 一种密码保护方法，应用于服务器，该服务器包括基板管理控制器，其特征在于，该方法包括如下步骤：

(a) 接收用户设置的第一密码，对该第一密码生成第一密文；

(b) 接收用户输入的第二密码，对该第二密码生成第二密文；

(c) 发送命令给基板管理控制器，通知基板管理控制器读取第一密文；

(d) 查看所述第二密文是否与第一密文相同；

(e) 当第二密文与第一密文相同时，启动所述服务器，结束流程；及

(f) 当第二密文与第一密文不相同且用户输入第二密码的次数没有超过用户设置的次数时，提示用户重新输入第二密码，并返回步骤 (b)。

6. 如权利要求 5 所述的密码保护方法，其特征在于，该方法于步骤 (a) 之前还包括：

提供一个设置界面，接收用户于该设置界面上所设置的第一密码。

7. 如权利要求 5 所述的密码保护方法，其特征在于，于步骤 (a) 之后还包括：

发送存储命令给基板管理控制器，通知基板管理控制器存储所述第一密文至基板管理控制器的现场可更换部件中。

8. 如权利要求 5 所述的密码保护方法，其特征在于，所述步骤 (f) 包括：

若用户输入的密码次数超过用户设置的次数，则锁住服务器。

密码保护系统及方法

技术领域

[0001] 本发明涉及一种密码设置系统及方法，尤其涉及一种密码保护系统及方法。

背景技术

[0002] 为了防止计算机系统被别人登录，用户往往以设置密码的方式来实现计算机锁定。传统的密码保护是基本输入输出系统 (Basic InputOutput System) 用互补金属氧化物半导体 (Complementary Metal OxideSemiconductor，CMOS) 来存储系统开机的密码。一旦计算机系统掉电，CMOS 就会被清除，这些密码就会丢失，他人便会轻易地变更 CMOS 设置，并登录到该计算机系统，导致用户私密文件的丢失。

发明内容

[0003] 鉴于以上内容，有必要提供一种密码保护系统，能够安全有效地对用户设置的密码进行保护。

[0004] 还有必要提供一种密码保护方法，能够安全有效地对用户设置的密码进行保护。

[0005] 一种密码保护系统，运行于服务器中，该服务器包括基板管理控制器，所述密码保护系统包括：接收模块，用于接收用户设置的第一密码及用户输入的第二密码；加密模块，用于对该第一密码生成第一密文，对第二密码生成第二密文；发送模块，用于发送命令给基板管理控制器，通知基板管理控制器读取第一密文；对比模块，用于查看所述第二密文是否与第一密文相同；及执行模块，用于当第二密文与第一密文相同时，启动所述服务器，当第二密文与第一密文不相同且当用户输入第二密码的次数没有超过用户设置的次数时，提示用户重新输入第二密码。

[0006] 一种密码保护方法，应用于服务器，该服务器包括基板管理控制器，该方法包括如下步骤：(a) 接收用户设置的第一密码，对该第一密码生成第一密文；(b) 接收用户输入的第二密码，对该第二密码生成第二密文；(c) 发送命令给基板管理控制器，通知基板管理控制器读取第一密文；(d) 查看所述第二密文是否与第一密文相同；(e) 当第二密文与第一密文相同时，启动所述服务器，结束流程；及 (f) 当第二密文与第一密文不相同且用户输入第二密码的次数没有超过用户设置的次数时，提示用户重新输入第二密码，并返回步骤 (b)。

[0007] 相较于现有技术，所述密码保护系统及方法，利用基板管理控制器的安全功能，不会因为系统掉电造成用户设置的密码丢失，有效地加强了密码的稳定性，用户计算机系统内的数据从而得到了有效的保护。

附图说明

[0008] 图 1 是本发明密码保护系统较佳实施例的运行环境图。

[0009] 图 2 是图 1 中密码保护系统 10 的功能模块图。

[0010] 图 3 是本发明密码保护方法较佳实施例的作业流程图。

[0011] 主要元件符号说明

[0012]

服务器	1
密码保护系统	10
基本输入输出系统	11
基板管理控制器	12
现场可更换部件	120
接收模块	100
加密模块	101
发送模块	102
对比模块	103
执行模块	104

[0013]

具体实施方式

[0014] 如图 1 所示，是本发明密码保护系统较佳实施例的运行环境图。该密码保护系统 10 运行于服务器 1 的基本输入输出系统 (Basic InputOutput System,BIOS)11 中，该服务器 1 包括基板管理控制器 (Baseboard Management Controller,BMC)12。该 BIOS 11 提供了一个设置界面，该设置界面提供了设置密码的功能。所述 BMC 12 包括现场可更换部件 (field-replaceable unit,FRU)120，用于存储用户设置的密码对应的密文。

[0015] 如图 2 所示，是图 1 中密码保护系统 10 的功能模块图。所述密码保护系统 10 包括：接收模块 100、加密模块 101、发送模块 102、对比模块 103 及执行模块 104。所述模块是具有特定功能的软件程序段，该软件存储于计算机可读存储介质或其它存储设备，可被计算机或其它包含处理器的计算装置执行，从而完成本发明中的密码保护的作业流程。

[0016] 接收模块 100 用于当用户需要对服务器 1 设置密码时，接收用户设置的第一密码。本实施例中，用户于所述 BIOS 11 提供的设置界面上输入需要设置的第一密码，该输入的第一密码为明文。所述用户需要对服务器 1 设置密码包括用户需要对该服务器 1 修改密码的情形。

[0017] 加密模块 101 用于对用户设置的第一密码生成对应的第一密文。

[0018] 发送模块 102 用于发送存储命令给 BMC 12，通知 BMC 12 存储该第一密文至所述 FRU 120 中。

[0019] 所述接收模块 100 还用于在 BIOS 11 进行初始化操作后，接收用户输入的第二密码。

[0020] 所述加密模块 101 还用于对用户输入的第二密码生成第二密文。

[0021] 所述发送模块 102 还用于发送命令给 BMC 12，通知 BMC 12 读取 FRU 120 中的第一密文。

[0022] 对比模块 103 用于查看所述第二密文与所读取的第一密文是否相同。当第二密文与第一密文不相同时，该对比模块 103 还用于查看用户输入第二密码的次数是否超过用户设置的次数。本实施例中，该用户设置的次数为 3 次。当用户输入第二密码的次数超过用户设置的次数时，执行模块 104 用于锁住该服务器 1，该服务器 1 处于当机状态。当用户输入第二密码的次数没有超过用户设置的次数时，执行模块 104 提示用户重新输入第二密码，所述接收模块 100 接收用户重新输入的第二密码。

[0023] 若所述第二密文与第一密文相同，则所述执行模块 104 还用于启动所述服务器 1。

[0024] 如图 3 所示，是本发明密码保护方法较佳实施例的作业流程图。

[0025] 步骤 S30，当用户需要对服务器 1 设置密码时，接收模块 100 接收用户设置的第一密码。本实施例中，用户于所述 BIOS 11 提供的设置界面上输入需要设置的第一密码，该输入的第一密码为明文。所述用户需要对服务器 1 设置密码包括用户需要对该服务器 1 修改密码的情形。

[0026] 步骤 S31，加密模块 101 对用户设置的第一密码生成对应的第一密文。

[0027] 步骤 S32，发送模块 102 发送存储命令给 BMC 12，通知 BMC 12 存储该第一密文至所述 FRU 120 中。

[0028] 步骤 S33，所述接收模块 100 接收用户输入的第二密码。本实施例中，在用户设置完密码后，需要重新启动服务器 1 该密码的设置才能够生效，在服务器 1 重启时，BIOS 11 进行初始化。

[0029] 步骤 S34，所述加密模块 101 对用户输入的第二密码生成第二密文。

[0030] 步骤 S35，发送模块 102 发送命令给 BMC 12，通知 BMC 12 读取 FRU 120 中的第一密文。

[0031] 步骤 S36，对比模块 103 查看所述第二密文是否与第一密文相同。若相同，则执行步骤 S37。若不相同，则执行步骤 S38。

[0032] 步骤 S37，执行模块 104 启动所述服务器 1，用户进入该服务器 1 进行相应操作，所述密码保护流程结束。

[0033] 步骤 S38，对比模块 103 查看用户输入第二密码的次数是否超过用户设置的次数。本实施例中，该用户设置的次数为 3 次，该次数可由用户设置。当用户输入第二密码的次数超过用户设置的次数时，执行步骤 S40。若用户输入第二密码的次数没有超过用户设置的次数时，于步骤 S39，执行模块 104 提示用户重新输入第二密码，并返回至步骤 S33，接收模块 100 接收用户重新输入的第二密码。

[0034] 步骤 S40，执行模块 104 锁住服务器 1，该服务器 1 处于当机状态。

[0035] 最后所应说明的是，以上实施例仅用以说明本发明的技术方案而非限制，尽管参照较佳实施例对本发明进行了详细说明，本领域的普通技术人员应当理解，可以对本发明的技术方案进行修改或等同替换，而不脱离本发明技术方案的精神和范围。

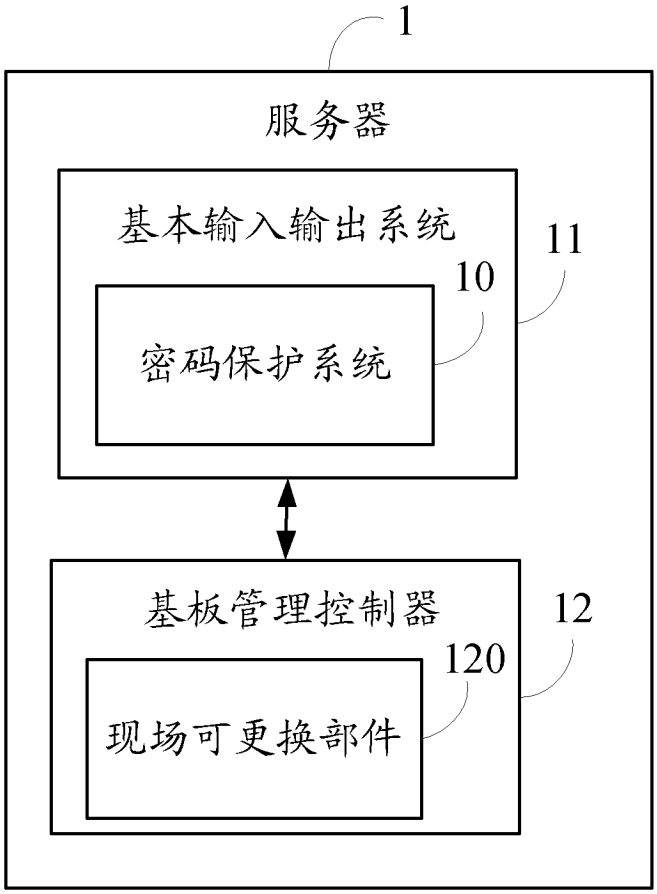


图 1

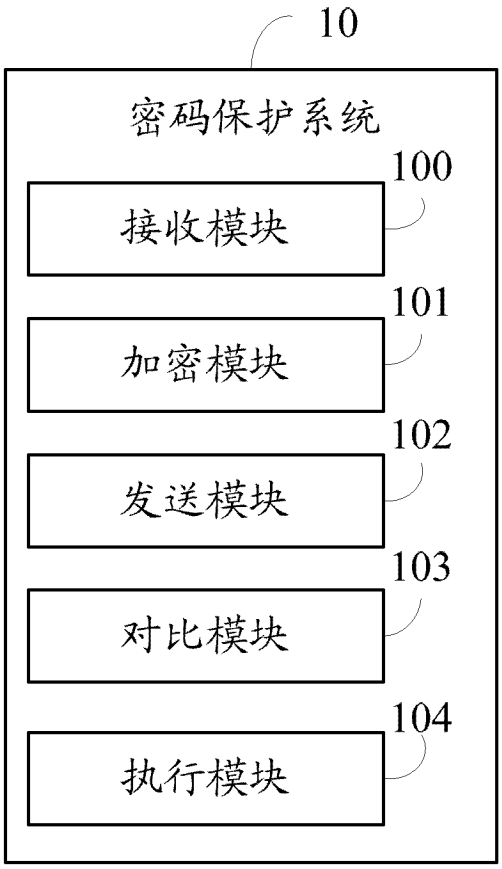


图 2

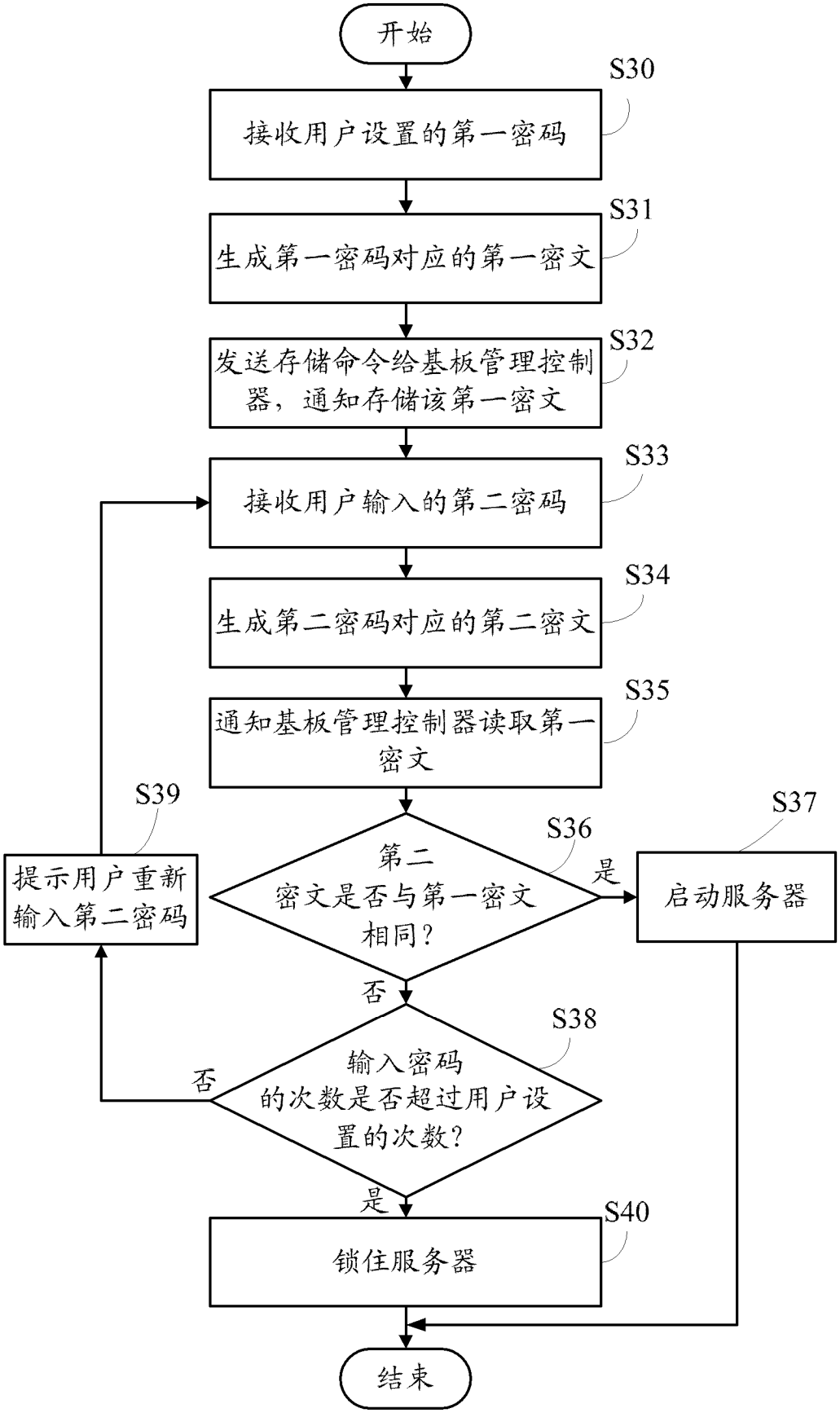

开始
S30
接收用户设置的第一密码
S31
生成第一密码对应的第一密文
S32
发送存储命令给基板管理控制器，通知存储该第一密文
S33
接收用户输入的第二密码
S34
生成第二密码对应的第二密文
S35
通知基板管理控制器读取第一密文
S36
第二密文是否与第一密文相同？
是
S37
启动服务器
否
S38
输入密码的次数是否超过用户设置的次数？
否
S39
提示用户重新输入第二密码
是
S40
锁住服务器
结束

图 3