(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 109918887 A
(43)申请公布日 2019.06.21

(21)申请号 201910267302.8

(22)申请日 2019.04.03

(71)申请人 中电科技(北京)有限公司
地址 100083 北京市海淀区卧虎桥甲6号工作区(南)太极大厦13层北侧

(72)发明人 陈小春 肖志坤 张超 朱立森

(74)专利代理机构 乌鲁木齐合纵专利商标事务所 65105
代理人 程云山

(51)Int.Cl.
*G06F 21/32*(2013.01)

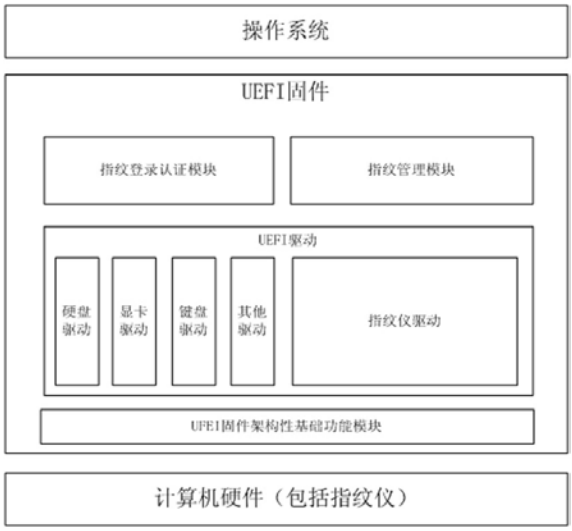
权利要求书2页 说明书5页 附图2页

(54)发明名称

基于UEFI的固件层指纹识别方法及计算机系统

(57)摘要

本发明公开了一种基于UEFI的固件层指纹识别方法、计算机系统,包括:在用户启动计算机系统后,检查计算机系统指纹仪是否存在,如果指纹仪损坏,则检测不到指纹仪,发出报警信号;如果指纹仪未损坏且硬件状态正常,则检测到指纹仪;开启指纹登陆认证功能并加载指纹仪驱动;对用户录入的指纹和指纹库中的指纹进行指纹匹配,如果指纹匹配未成功,则认定用户为非法用户,给出提示信息后强制关机;如果指纹匹配成功,则启动操作系统。还提供一种基于UEFI的固件层指纹识别方法的计算机系统。上述基于UEFI的固件层指纹识别方法和计算机系统可以独立使用,方便用户开机,具有更强的易用性,且由于指纹的唯一性,使得计算机系统具有更强的安全性。




CN 109918887 A

1.一种基于UEFI的固件层指纹识别方法,其特征在于,包括:

在用户启动计算机系统后,检查计算机系统指纹仪是否存在,如果指纹仪损坏,则检测不到指纹仪,发出报警信号;如果指纹仪未损坏且硬件状态正常,则检测到指纹仪;

开启指纹登陆认证功能并加载指纹仪驱动;

将用户录入的指纹和指纹库中的指纹进行指纹匹配,如果指纹匹配未成功,则认定用户为非法用户,给出提示信息后强制关机;如果指纹匹配成功,则启动操作系统。

2.根据权利要求1所述的基于UEFI的固件层指纹识别方法,其特征在于,在所述认定用户为非法用户后,提示用户再次录入指纹,并对新录入的再次进行指纹匹配,连续三次指纹匹配不成功后强制关机。

3.根据权利要求2所述的基于UEFI的固件层指纹识别方法,其特征在于,在所述指纹匹配成功,还包括:

对用户身份进行识别,如果用户录入的指纹和指纹库中的管理员的指纹匹配,则用户获取管理员权限;如果用户录入的指纹和指纹库中的普通用户的指纹匹配,则用户获取普通用户权限。

4.根据权利要求3所述的基于UEFI的固件层指纹识别方法,其特征在于,所述管理员权限包括选择启动操作系统或者进入指纹管理。

5.根据权利要求3所述的基于UEFI的固件层指纹识别方法,其特征在于,所述指纹管理为添加或删除管理员的指纹、添加或删除普通用户指纹、清空指纹库、开启或关闭指纹登陆认证功能。

6.一种基于UEFI的固件层指纹识别方法的计算机系统,包括硬件、UEFI固件层和操作系统,所述硬件包括指纹仪,其特征在于,所述UEFI固件层包括以下功能单元:

录入图像单元,用于探测手指并对探测到的手指指纹录入指纹原始图像;

生成特征单元,用于将录入的指纹原始图像生成为指纹的特征文件并保存到指纹库中指定编号位置;

对比指纹特征单元,用于对开机时用户录入的指纹和指纹库中所有的指纹进行对比,并返回判断结果;

指纹管理单元,用于实现对用户指纹进行管理,根据所述对比指纹特征单元的判断结果来识别用户类型,并确定是否启动操作系统,对非法用户给出提示信息后强制关机,对合法用户提供对应的权限。

7.根据权利要求6所述的基于UEFI的固件层指纹识别方法的计算机系统,其特征在于,当所述指纹管理单元确定用户类型为非法用户时,还包括提示单元,用于提示用户再次录入指纹,再通过所述对比指纹特征单元对新录入的再次进行指纹匹配,连续三次指纹匹配不成功后强制关机。

8.根据权利要求6所述的基于UEFI的固件层指纹识别方法的计算机系统,其特征在于,所述指纹管理单元还包括用户身份识别单元,如果用户录入的指纹和指纹库中的管理员的指纹匹配,则识别用户为管理员,获取管理员权限;如果用户录入的指纹和指纹库中的普通用户的指纹匹配,则识别用户为普通用户,获取普通用户权限。

9.根据权利要求8所述的基于UEFI的固件层指纹识别方法的计算机系统,其特征在于,所述管理员权限包括选择启动操作系统或者进入指纹管理。

10.根据权利要求8所述的基于UEFI的固件层指纹识别方法的计算机系统，其特征在于，所述指纹管理为添加或删除管理员的指纹、添加或删除普通用户指纹、清空指纹模块的指纹库、选择开启或关闭指纹登陆认证功能。

# 基于UEFI的固件层指纹识别方法及计算机系统

## 技术领域

[0001] 本发明涉及一种计算机应用领域，特别涉及一种基于UEFI的固件层指纹识别方法、计算机系统。

## 背景技术

[0002] 固件是计算机系统中的重要基础软件，固化存储于硬件的芯片中。计算机的主板、显卡、网卡、硬盘中都有固件，虽然作用不同，但是本质上都是使能和驱动硬件。计算机中最重要的固件称为BIOS(Basic Input/Output System，基本输入输出系统)，用于初始化硬件、管理硬件资源、屏蔽平台特性、引导操作系统，是连接计算机基础硬件和系统软件的桥梁。

[0003] 在BIOS的发展经历了两个时代，第一个时代的BIOS称之为legacy BIOS，第二个时代的BIOS称之为统一的可扩展固件接口(Unified Extensible Firmware Interface，UEFI)。Legacy BIOS诞生于1981年，IBM在研制第一台个人计算机时，将硬件初始化、操作系统引导的代码固化在32K大小的可编程只读存储器(Programmable Read-Only Memory，PROM)中，成为最早的固件。UEFI是一种计算机固件(或称为BIOS)的接口规范，也是关于固件的最主要的工业标准。UEFI规范最初是面向Intel公司的Itanium和X86处理器进行制定的，但是UEFI规范本身是与处理器架构无关的，目前已经应用于X86、Itanium、ARM等处理器平台。符合UEFI规范的计算机固件(以下简称UEFI固件)相对于传统的固件有很多优越性，目前主流的X86商用计算机系统基本上都是采用了UEFI固件。

[0004] 在UEFI固件中，对使用计算机的用户进行身份验证能够有效地保证系统安全。目前UEFI固件阶段身份认证的主要方式为密码登录，即开机过程中，UEFI固件运行阶段要求用户输入开机密码，密码输入正确后才可以引导操作系统继续启动。虽然市场中已经有一部分笔记本电脑配备了指纹检测设备，但是其指纹驱动和用户指纹管理都是在操作系统下进行的。UEFI固件可以先于操作系统启动，若在启动过程中通过旁路、木马攻击等方式，能够绕过这种指纹认证方式，无法起到安全保护的作用。因此，需要研制基于UEFI的固件层指纹识别方法。

## 发明内容

[0005] 本发明主要解决的技术问题是提供一种安全性能较高的一种基于UEFI的固件层指纹识别方法及计算机系统。

[0006] 为解决上述技术问题，本发明采用的一个技术方案是：一种基于UEFI的固件层指纹识别方法，包括：

在用户启动计算机系统后，检查计算机系统指纹仪是否存在，如果指纹仪损坏，则检测不到指纹仪，发出报警信号；如果指纹仪未损坏且硬件状态正常，则检测到指纹仪；

开启指纹登陆认证功能并加载指纹仪驱动；

将用户录入的指纹和指纹库中的指纹进行指纹匹配，如果指纹匹配未成功，则认定用

户为非法用户,给出提示信息后强制关机;如果指纹匹配成功,则启动操作系统。

[0007] 在其中一个实施例中,在所述认定用户为非法用户后,提示用户再次录入指纹,并对新录入的再次进行指纹匹配,连续三次指纹匹配不成功后强制关机。

[0008] 在其中一个实施例中,在所述指纹匹配成功,还包括:

对用户身份进行识别,如果用户录入的指纹和指纹库中的管理员的指纹匹配,则用户获取管理员权限;如果用户录入的指纹和指纹库中的普通用户的指纹匹配,则用户获取普通用户权限。

[0009] 在其中一个实施例中,所述管理员权限包括选择启动操作系统或者进入指纹管理。

[0010] 在其中一个实施例中,所述指纹管理为添加或删除管理员的指纹、添加或删除普通用户指纹、清空指纹库、开启或关闭指纹登陆认证功能。

[0011] 还提供一种基于UEFI的固件层指纹识别方法的计算机系统,包括硬件、UEFI固件层和操作系统,所述硬件包括指纹仪,所述UEFI固件层包括以下功能单元:

录入图像单元,用于探测手指并对探测到的手指指纹录入指纹原始图像;

生成特征单元,用于将录入的指纹原始图像生成为指纹的特征文件并保存到指纹库中指定编号位置;

对比指纹特征单元,用于对开机时用户录入的指纹和指纹库中所有的指纹进行对比,并返回判断结果;

指纹管理单元,用于实现对用户指纹进行管理,根据所述对比指纹特征单元的判断结果来识别用户类型,并确定是否启动操作系统,对非法用户给出提示信息后强制关机,对合法用户提供对应的权限。

[0012] 在其中一个实施例中,所述指纹管理单元确定用户类型为非法用户时,还包括提示单元,用于提示用户再次录入指纹,再通过所述对比指纹特征单元对新录入的再次进行指纹匹配,连续三次指纹匹配不成功后强制关机。

[0013] 在其中一个实施例中,所述指纹管理单元还包括用户身份识别单元,如果用户录入的指纹和指纹库中的管理员的指纹匹配,则识别用户为管理员,获取管理员权限;如果用户录入的指纹和指纹库中的普通用户的指纹匹配,则识别用户为普通用户,获取普通用户权限。

[0014] 在其中一个实施例中,所述管理员权限包括选择启动操作系统或者进入指纹管理。

[0015] 在其中一个实施例中,所述指纹管理为添加或删除管理员的指纹、添加或删除普通用户指纹、清空指纹模块的指纹库、选择开启或关闭指纹登陆认证功能。

[0016] 本发明的有益效果是:与现有技术相比,上述基于UEFI的固件层指纹识别方法和计算机系统可以独立使用,方便用户开机,具有更强的易用性,且由于指纹的唯一性,使得计算机系统具有更强的安全性。

## 附图说明

[0017] 图1为一实施方式的基于UEFI的固件层指纹识别方法的计算机系统架构说明图。

[0018] 图2为一实施方式的基于UEFI的固件层指纹识别方法流程图。

## 具体实施方式

[0019] 本发明提供一种UEFI的固件层的指纹识别方法及计算机系统，能够对计算机用户通过指纹识别的方法进行身份认证，从而增强系统安全。在一实施方式中，请参阅图1，一种UEFI的固件层的指纹识别方法的计算机系统，整个计算机系统可以大致分为硬件、UEFI固件、和操作系统三大部分。

[0020] 计算机上电后，UEFI固件根据计算机的硬件配置，进行相关的配置，并最终从存储介质加载操作系统并完成操作系统的启动。本申请对计算机硬件平台没有特殊要求，包括通用计算机必要组成部分即可，同时需要连接指纹仪。指纹仪可以通过串口和USB接口两种方式接入到计算机系统中。

[0021] 其中UEFI固件架构性基础功能模块指的是从处理器上电后运行的第一行代码到准备好UEFI驱动运行环境这个阶段所执行的代码。固件架构性基础功能模块主要的作用包括对CPU运行状态进行配置，对Cache进行配置，对内存进行配置，对中断进行配置，并且按照UEFI规范提供架构性服务。最终准备好一个符合UEFI规范的设备驱动能够正常运行的环境。

[0022] 其中，在一实施方式中，UEFI驱动包括硬盘驱动、显卡驱动、键盘驱动、指纹仪驱动等。显卡和键盘驱动用于支持固件下的输入输出，硬盘驱动用于加载操作系统。指纹仪驱动是本方法的核心组成模块，是针对接入计算机系统的指纹仪硬件开发的驱动。驱动接口能实现的功能包括：

录入图像。探测手指并对探测到的手指指纹录入指纹原始图像。

[0023] 生成特征。把录入的指纹原始图像生成为特征文件并保存到指纹库指定编号位置。

[0024] 对比指纹特征。比对两个指纹库中指定编号的指纹特征是否一致。

[0025] 搜索指纹。把录入的指纹和指纹库中所有的指纹进行对比，如果存在特征值一致的指纹返回真。

[0026] 删除指纹。删除指纹库中特定编号的指纹。

[0027] 清空指纹库。清除指纹库中所有指纹。

[0028] 因此，对应地，UEFI固件层包括以下功能单元：

录入图像单元，用于探测手指并对探测到的手指指纹录入指纹原始图像；

生成特征单元，用于将录入的指纹原始图像生成为指纹的特征文件并保存到指纹库中指定编号位置；

对比指纹特征单元，用于对开机时用户录入的指纹和指纹库中所有的指纹进行对比，并返回判断结果；

指纹管理单元，用于实现对用户指纹进行管理，根据所述对比指纹特征单元的判断结果来识别用户类型，并确定是否启动操作系统，对非法用户给出提示信息后强制关机，对合法用户提供对应的权限。

[0029] 当然，在其他实施例中，指纹仪支持的功能比上述列出的接口函数要多，但是满足以上功能接口即可保证固件层下功能正常使用。以上功能函数可以通过串行总线和USB总线两种方式与CPU进行通信。

[0030] 在一实施方式中，所述指纹管理单元确定用户类型为非法用户时，还包括提示单

元，用于提示用户再次录入指纹，再通过所述对比指纹特征单元对新录入的再次进行指纹匹配，连续三次指纹匹配不成功后强制关机。

[0031] 在一实施方式中，所述指纹管理单元还包括用户身份识别单元，如果用户录入的指纹和指纹库中的管理员的指纹匹配，则识别用户为管理员，获取管理员权限；如果用户录入的指纹和指纹库中的普通用户的指纹匹配，则识别用户为普通用户，获取普通用户权限。

[0032] 在一实施方式中，所述管理员权限包括选择启动操作系统或者进入指纹管理。具体地，所述指纹管理为添加或删除管理员的指纹、添加或删除普通用户指纹、清空指纹模块的指纹库、选择开启或关闭指纹登陆认证功能。

[0033] 具体地，在其中一个实施例中，指纹管理单元是建立在指纹仪驱动上的管理模块，实现用户指纹管理功能。目前，UEFI固件通常采用一个管理员和一个普通用户的身份认证方案。以此为基础，指纹管理模块结合原有身份认证方案，给管理员用户和普通用户分别设置指纹。用户启动指纹登录认证模块后，首先要录入管理员指纹；管理员指纹设置成功后，以管理员指纹登录，即可设置普通用户指纹。管理员登录可以增加、删除管理员用户和普通用户的指纹，可以关闭指纹认证功能，可以初始化指纹仪，即清除指纹库中所有指纹。以普通用户登录无法对指纹进行增加和删除的操作。

[0034] 具体地，在其中一个实施例中，指纹管理单元中还包括指纹认证模块，指纹认证模块是建立在指纹管理模块上负责校验开机用户身份的模块。在指纹管理模块中，如果录入了指纹并且开启指纹识别功能，那么每次开机过程中都会在固件阶段通过显示器探索提示信息，要求用户录入指纹。在开机用户成功录入指纹后，指纹认证模块会把当前录入的指纹和指纹库中的指纹进行对比。如果开机用户录入的指纹和管理员指纹匹配，那么用户将会获取管理员权限，可以选择启动操作系统或者调用指纹管理模块对指纹进行管理。如果开机用户录入的指纹和普通用户的指纹匹配，那么开机用户获取普通用户权限，可以启动操作系统，但是不能对指纹进行管理。如果开机用户录入的指纹没有和任何指纹库中的指纹成功匹配，那么开机用户还有两次录入指纹的机会，如果连续三次录入的指纹都没有和指纹库中的指纹完成匹配，那么指纹管理模块会提示用户计算机即将关机，然后执行关机操作。

[0035] 本申请的技术方案对操作系统没有任何要求。通过指纹登录认证模块的用户可以继续开机，启动操作系统。

[0036] 在一实施方式中，一种基于UEFI的固件层指纹识别方法包括：

S110、在用户启动计算机系统后，检查计算机系统指纹仪是否存在，如果指纹仪损坏，则检测不到指纹仪，发出报警信号；如果指纹仪未损坏且硬件状态正常，则检测到指纹仪；

S120、开启指纹登陆认证功能并加载指纹仪驱动；

S130、对用户录入的指纹和指纹库中的指纹进行指纹匹配，如果指纹匹配未成功，则认定用户为非法用户，给出提示信息后强制关机；如果指纹匹配成功，则启动操作系统。

[0037] 在一实施方式中，在所述认定用户为非法用户后，提示用户再次录入指纹，并对新录入的再次进行指纹匹配，连续三次指纹匹配不成功后强制关机。

[0038] 在一实施方式中，在所述指纹匹配成功，还包括：

对用户身份进行识别，如果用户录入的指纹和指纹库中的管理员的指纹匹配，则用户获取管理员权限；如果用户录入的指纹和指纹库中的普通用户的指纹匹配，则用户获取普

通用户权限。

[0039] 在一实施方式中，所述管理员权限包括选择启动操作系统或者进入指纹管理。

[0040] 在一实施方式中，所述指纹管理为添加或删除管理员的指纹、添加或删除普通用户指纹、清空指纹库、开启或关闭指纹登陆认证功能。

[0041] 具体地，在其中一个实施例中，如图2所示，如固件层指纹识别方法流程说明图所示，固件层指纹识别方法主要步骤如下：

步骤一、检查是否存在指纹仪。扫描指纹仪是否存在，如果硬件状态正常，那么就会检测到指纹仪。如果指纹仪损坏，就会检测不到指纹仪。

[0042] 步骤二、检测到指纹仪且开启指纹登陆认证功能，将会进入步骤三。检测到指纹仪且未开启指纹登陆认证功能，将会直接进入操作系统。未检测到指纹仪且指纹登陆认证功能开启的情况下，会提示指纹仪硬件异常并关机。未检测到指纹仪且指纹登陆认证功能关闭的情况下，可以直接进入操作系统。

[0043] 步骤三、加载指纹仪驱动。此时UEFI的固件层已经完成了驱动执行环境的准备工作，加载各个硬件驱动的同时，也加载指纹仪驱动。确保指纹仪的各项功能接口函数可以在指纹登陆认证模块和指纹管理模块正常使用。

[0044] 步骤四、要求用户录入指纹，并对用户录入的指纹和指纹库中的指纹进行比对。录入的指纹和指纹库中的指纹比对后，如果没有匹配成功，那么开机用户为非法用户。如果录入的指纹和管理员的指纹匹配，用户将获取管理员权限。如果录入的指纹和普通用户的指纹匹配，用户将获取普通用户权限。

[0045] 步骤五、如果开机用户为非法用户，会要求用户再次录入指纹并对新录入的指纹进行步骤四的处理。连续三次录入的指纹都无法和指纹库中的指纹匹配成功，会给出提示信息后强制关机。

[0046] 步骤六、如果开机用户为普通用户，那么直接启动操作系统。

[0047] 步骤七、如果开机用户为管理员，可以选择启动操作系统或者进入指纹管理模块。

[0048] 步骤八、管理员用户进入指纹管理模块后，可以添加或删除管理员的指纹，可以添加或删除普通用户指纹，可以清空指纹模块的指纹库，可以选择开启或关闭指纹登陆认证功能。

[0049] 步骤九、管理员退出指纹管理模块后，直接启动操作系统。

[0050] 与现有技术相比，与现有技术相比，上述基于UEFI的固件层指纹识别方法和计算机系统即可以独立使用，方便用户开机，具有更强的易用性，且由于指纹的唯一性，使得计算机系统具有更强的安全性。

[0051] 以上所述仅为本发明的实施方式，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

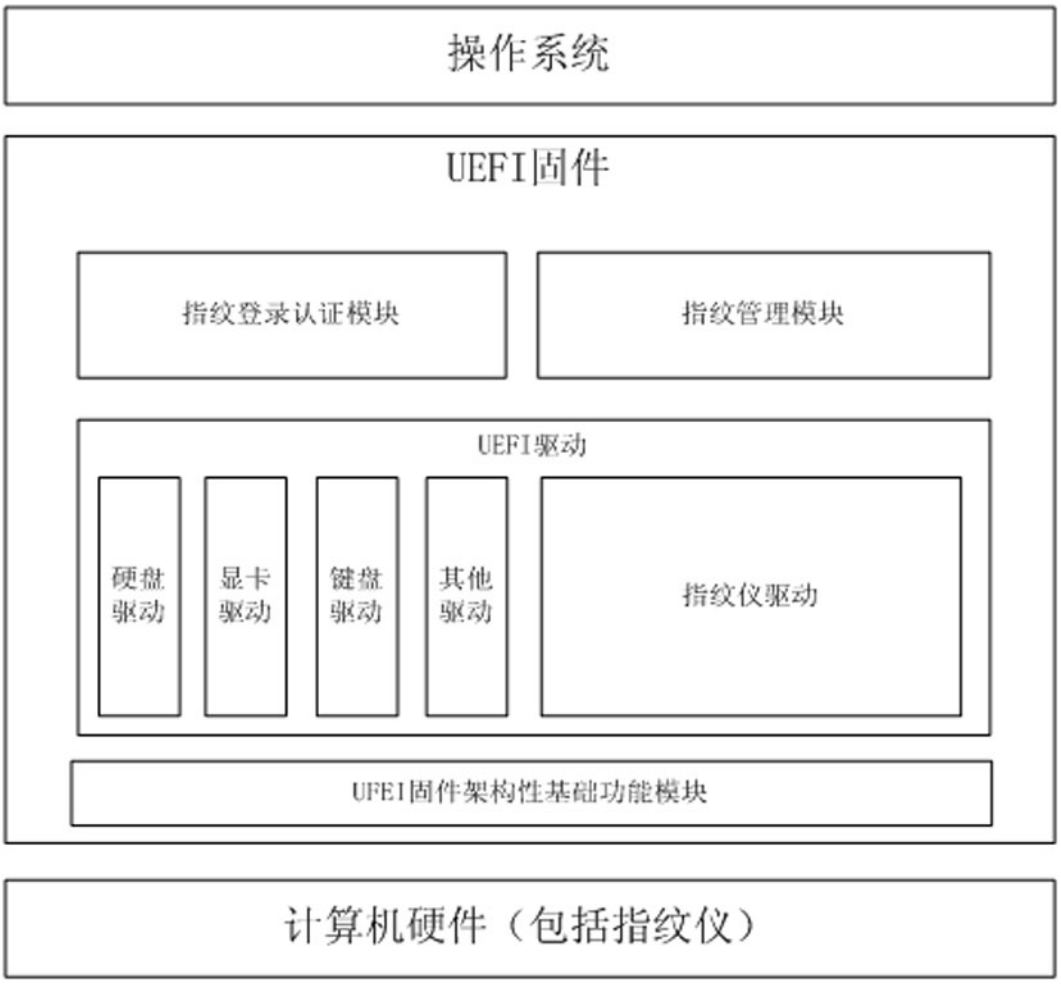

操作系统
UEFI固件
指纹登录认证模块
指纹管理模块
UEFI驱动
硬盘驱动
显卡驱动
键盘驱动
其他驱动
指纹仪驱动
UFEI固件架构性基础功能模块
计算机硬件（包括指纹仪）

图1

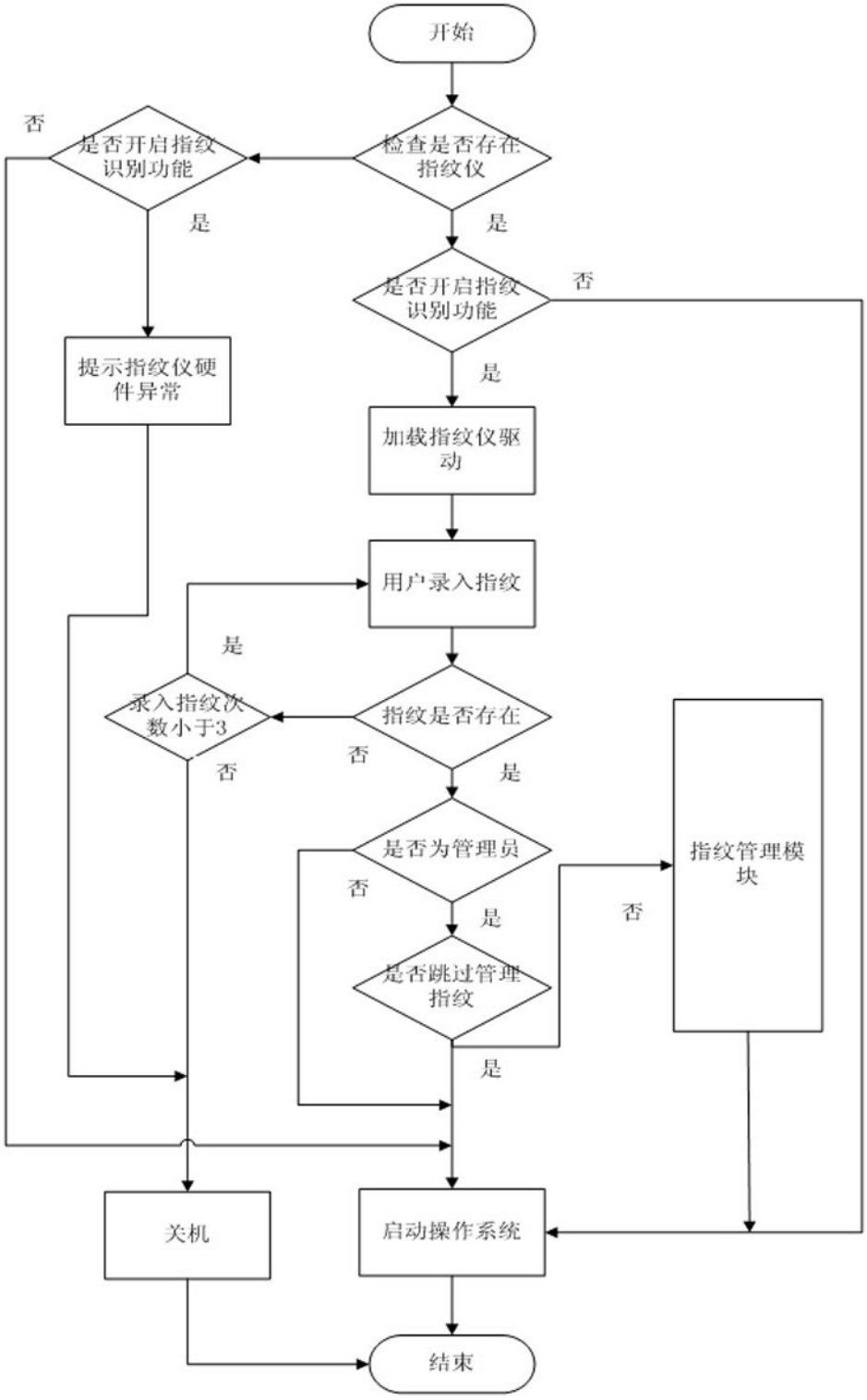

开始
检查是否存在指纹仪
是否开启指纹识别功能
否
是
是否开启指纹识别功能
否
是
提示指纹仪硬件异常
加载指纹仪驱动
用户录入指纹
是
录入指纹次数小于3
指纹是否存在
否
否
是
是否为管理员
否
是
指纹管理模块
否
是否跳过管理指纹
是
关机
启动操作系统
结束

图2