[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610072785.9

[45] 授权公告日 2008 年 1 月 30 日

[11] 授权公告号 CN 100365641C

[22] 申请日 2006.4.11
[21] 申请号 200610072785.9
[73] 专利权人 北京飞天诚信科技有限公司
地址 100083 北京市海淀区学院路 40 号研 7 楼 5 层
[72] 发明人 陆 舟 于华章
[56] 参考文献
CN1527529A 2004.9.8
US5592553A 1997.1.7
US5732137A 1998.3.24
CN1599314A 2005.3.23
审查员 王学睿

[74] 专利代理机构 北京三高永信知识产权代理有限责任公司
代理人 何文彬

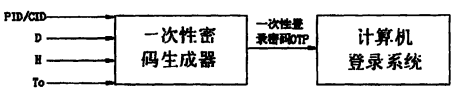
权利要求书 2 页 说明书 6 页 附图 3 页

[54] 发明名称

利用一次性密码保护计算机登录的方法

[57] 摘要

本发明提供一种保护登录计算机操作系统的方法，具体的说是利用一次性密码保护计算机登录的方法。 本发明的利用一次性密码保护计算机登录的方法采用一次性密码生成器产生一次性密码，通过计算机上的登录系统进行解码验证，从而实现登录计算机的目的。 本发明的利用一次性密码保护计算机登录的方法使得计算机使用更加安全可靠，有效的防范了非法登录的情况，且使用成本低。 因而具有很好的推广使用价值。



1、一种利用一次性密码保护计算机登录的方法，其特征在于，所述方法包括:

用户使用一次性密码登录计算机,所述一次性密码根据用户申请及输入的用户标识、随机数、有效起始时间点和有效使用时间，由密码生成器压缩、加密生成;

所述计算机解压缩、解密所述登录一次性密码，验证所述一次性密码是否有效，验证通过后，记录有效起始时间和有效使用时间，允许用户进入操作系统，并实时监控所述用户的使用时间是否超过所述有效使用时间，如果不是，保持登录状态；如果是，则提示时间到并锁定操作系统。

2、根据权利要求1所述的利用一次性密码保护计算机登录的方法，其特征在于，所述用户标识为用户号或机器号。

3、根据权利要求2所述的利用一次性密码保护计算机登录的方法，其特征在于，所述用户标识为用户号时，所述验证所述一次性密码是否有效的步骤具体为:

验证所述用户号是否与注册时的用户号一致，如果不一致，则提示登录失败；如果一致，判断当前时间是否在所述有效起始时间点之后，如果在所述有效起始时间点之后，所述一次性密码有效，否则，所述一次性密码无效。

4、根据权利要求2所述的利用一次性密码保护计算机登录的方法，其特征在于，所述用户标识为机器号时，所述验证所述一次性密码是否有效的步骤具体为:

验证所述一次性密码是否使用过，如果使用过，提示登录失败；否则，验证所述机器号是否与注册时的机器号一致，如果不一致，则提示登录失败；如果一致，判断当前时间是否在所述有效起始时间点

之后，如果在所述有效起始时间点之后，所述一次性密码有效；否则，所述一次性密码无效。

利用一次性密码保护计算机登录的方法

技术领域

本发明提供一种保护计算机登录安全的方法，具体的说是一种利用一次性密码保护计算机登录的方法。

背景技术

随着信息时代的快速发展，计算机成为人们日常生活、办公和学习必不可少的设备。计算机使用的日益广泛性，带来了计算机信息安全的问题。防止计算机在未被允许的情况下被非法登录成了计算机信息安全的一个重要课题。

以传统密码保护系统登录就是针对上述问题而设置的，但是用户设置的登录密码很容易泄露给他人，并且用户设置的密码往往比较简单，很容易被破解。一旦恶意分子知道了登录密码，密码的保护能力将完全丧失。

利用硬件（如智能密码锁、智能卡等）的双因子验证来登录计算机，提高了安全性。当用户想要登录时，必须拥有在这台计算机注册过的用于保护的硬件设备（如智能密码锁、智能卡等），并且知道启用此硬件设备的用户名和密码，才能登录计算机，否则不能登录。这种计算机保护系统由于利用了硬件的双因子验证，很好地防止非法用户（可能窃取了合法用户的用户名和密码）登录计算机，具有很高的安全性。但是这种方法中使用的硬件在 Windows 安全模式下无法使用，所以不能够保护 Windows 安全模式登录。并且这种硬件很容易丢失，一旦丢失硬件用户将无法登录计算机，给用户造成了麻烦，而且相对于软件，这种方法中使用的硬件的成本较高。

上述两种保护登录的方法都是针对系统正常登录的，而对于 Windows 安全模式的登录，要么就不能进行安全模式的登录（硬件方法中使用的硬件在安全模式下因找不到驱动而无法使用），要么根本就不进行保护。如果不进行保护非法用户很容易利用这个漏洞登录 Windows 计算机系统窃取信息。

发明内容

本发明针对现有保护方法中存在的问题提出利用一次性密码来保护计算机登录，使用户使用计算机更加安全可靠，有效的防范了非法登录的情况。

本发明的利用一次性密码保护计算机登录的方法，其采取的技术方案如下：

用户使用一次性密码登录计算机，所述一次性密码根据用户申请及输入的用户标识、随机数、有效起始时间点和有效使用时间，由密码生成器压缩、加密生成；

所述计算机解压缩、解密所述登录一次性密码，验证所述一次性密码是否有效，验证通过后，记录有效起始时间和有效使用时间，允许用户进入操作系统，并实时监控所述用户的使用时间是否超过所述有效使用时间，如果不是，保持登录状态；如果是，则提示时间到并锁定操作系统。

所述用户标识为用户号或机器号。

所述用户标识为用户号时，所述验证所述一次性密码是否有效的步骤具体为：

验证所述用户号是否与注册时的用户号一致，如果不一致，则提示登录失败；如果一致，判断当前时间是否在所述有效起始时间点之后，如果在所述有效起始时间点之后，所述一次性密码有效；否则，所述一次性密码无效。

所述用户标识为机器号时，所述验证所述一次性密码是否有效的步骤具体为：

验证所述一次性密码是否使用过，如果使用过，提示登录失败；否则，验证所述机器号是否与注册时的机器号一致，如果不一致，则提示登录失败；如果一致，判断当前时间是否在所述有效起始时间点之后，如果在所述有效起始时间点之后，所述一次性密码有效；否则，所述一次性密码无效。

本发明的利用一次性密码保护计算机登录的方法，其一次性密码具有有效期和次数限制，即使恶意分子知道了一次性密码，也无法登录计算机。并且一次性密码没有遗失硬件带来的麻烦，成本也较低。这样的计算机保

护系统补充了原有保护系统不能保护Windows安全模式登录的不足，使计算机使用更加安全。

附图说明

下面结合附图和实施例对本发明进一步说明。

附图1为本发明的功能实现流程框图；

附图2为本发明的一次性密码生成器的工作原理图；

附图3为本发明以时间为限制条件登录计算机操作系统的工作流程图；

附图4为本发明以次数为限制条件登录计算机操作系统的工作流程图。

具体实施方式

参照说明书附图对本发明的利用一次性密码保护计算机登录的方法给出最佳的实施例。

实施例1:

以时间为限制条件，保护计算机登录，实现本发明所述登录保护的方法。

用户想要登录计算机时，必须使用一次性密码生成器生成的一次性密码。一次性密码生成器安装在由管理人员专门管理的机器上，用户需要向管理这台机器的管理员提供用户信息，管理员根据用户提供的信息使用一次性密码生成器生成一次性密码，一次性密码生成器工作原理如图 2 所示，一次性密码生成器提示输入以下信息:

1、唯一的用户号 PID，用户号 PID 可以由软件销售商分配给用户，也可以由公司局域网的管理员分配给每个员工。

2、有效起始日期 D，这个日期默认为当前日期，也可以自定义，其代表一次性登录密码 OTP 的有效起始日期。

3、有效起始时间 H，这个时间默认为当前时间，也可以自定义，其代表一次性登录密码 OTP 的有效起始时间。

4、有效使用时间 T_0，是一个数字，单位为小时，其代表从用户使用一次性登录密码 OTP 登录开始 T_0 时间后密码失效。

一次性密码生成器每次生成一次性密码前都要由随机数生成单元 103 生成一个随机数 R，再由压缩单元 102 将用户 101 输入的用户号 PID、有效起始日期 D、有效起始时间 H 和/或有效使用时间 T_0 和随机数 R 一并压缩，压缩后的信息 M 由加密单元 104 采用某种加密算法加密生成一次性登录密码 OTP，其中加密单元 104 所采用的加密算法是公知的对称加密算法（如 DES）。由于这个一次性登录密码 OTP 是根据唯一的用户号 PID、有效起始日期 D、有效起始时间 H 和/或有效使用时间 T_0 加上随机数 R 生成的，是一个非常随机的字符串，很难被破解，具有很高的安全强度。并且一次性登录密码 OTP 是由用户号 PID 生成的，如果用户 101 使用相同的用户号 PID 在很多台计算机注册本发明所述的计算机保护系统，那么用户 101 可以在一次性登录密码 OTP 有效期内用相同用户号 PID 注册的计算机上使用该一次性登录密码 OTP，方便用户使用。

用户得到一次性登录密码 OTP 后就可以在其用户号 PID 注册过的计算机上使用该一次性登录密码 OTP 了。本发明所述的保护方法优选实施例 1 的工作流程如图 3 所示，首先进入登录界面 201，在步骤 202 中用户根据系统提示输入在一次性密码生成器中得到的一次性登录密码 OTP，步骤 203 启动解密模块将一次性登录密码 OTP 解密，解密模块的工作原理是先将一次性密码使用一次性密码生成器中相同的密钥解密，再解压缩，得到与用户在一次性密码生成器中输入的相同信息，包括用户号 PID、有效起始日期 D、有效起始时间 H 和/或有效使用时间 T_0，接下来由验证模块验证一次性登录密码 OTP 的有效性，首先步骤 204 验证用户号与注册时的用户号是否一致，如果不正确则 206 提示登录失败，如果用户号一致则步骤 205 验证当前时间是否在有效起始时间之后，如果不是 206 提示登录失败，如果是则步骤 207 记录有效起始时间 H 和/或有效使用时间 T_0，步骤 208 进入计算机操作系统，步骤 209 启动监控模块，监控模块主要控制用户使用的时间是否在有效使用时间之内，步骤 210 通过累计得出用户使用时间 T_1，步骤 211 判

断有效使用时间 T_0是否大于用户实际使用时间 T_1，如果是则 212 保持登录状态，如果超时则步骤 213 提示时间到并锁定操作系统。

实施例2:

以次数为限制条件，保护计算机登录，实现本发明所述登录保护的方法。

与实施例 1 中的思路相似，用户首先向管理人员索要一次性密码生成器生成的一次性密码。一次性密码生成器的工作原理如图 2 所示，一次性密码生成器提示输入以下信息:

1、唯一的机器号 CID，机器号 CID 与安装本发明所述计算机保护系统时输入的机器号相对应。

2、有效起始日期 D，这个日期默认为当前日期，也可以自定义，其代表一次性登录密码 OTP 的有效起始日期。

3、有效起始时间 H，这个时间默认为当前时间，也可以自定义，其代表一次性登录密码 OTP 的有效起始时间。

4、有效使用时间 T_0，是一个数字，单位为小时，其代表从用户使用一次性登录密码 OTP 登录开始 T_0时间后密码失效。

用户输入生成一次性密码所需信息后，由随机数生成单元 103 生成随机数 R，再由压缩单元 102 将用户 101 输入的机器号 CID、有效起始日期 D、有效起始时间 H 和/或有效使用时间 T_0和随机数 R 一并压缩，加密单元 104 将压缩后的信息加密成密文，这个密文就是一次性登录密码 OTP。这个一次性登录密码 OTP 由机器号 CID 生成，而严格的讲机器号是唯一的，所以一个一次性登录密码 OTP 只适用于一台机器。

用户得到一次性登录密码 OTP 后就可以在相应的计算机上使用该一次性登录密码 OTP 了。本发明所述的保护方法优选实施例 2 的工作流程如图 4 所示，首先进入登录界面 301，在步骤 302 中用户根据系统提示输入在一次性密码生成器中得到的一次性登录密码 OTP，步骤 303 调用本地系统数据库，验证此一次性密码是否使用过，如果曾经使用过则提示登录失败，如果没有使用过则步骤 304 启动解密模块将一次性登录密码 OTP 解密，解密模块的工作原理是先将一次性密码使用一次性密码生成器中相同的密钥解密，

再解压缩，得到与用户在一次性密码生成器中输入的相同信息，包括机器号 CID、有效起始日期 D、有效起始时间 H 和/或有效使用时间 T_0，接下来由验证模块继续验证一次性登录密码 OTP 的有效性，步骤 305 验证解密得到的机器号 CID 与注册时的机器号是否一致，如果不一致则 307 提示登录失败，如果机器号一致则步骤 306 验证当前时间是否在有效起始时间之后，如果不是 307 提示登录失败，如果是则步骤 308 记录有效起始时间 H 和/或有效使用时间 T_0，步骤 309 进入计算机操作系统，步骤 310 将一次性密码加密后存入系统数据库中，步骤 311 启动监控模块，监控模块主要控制用户使用的时间是否在有效使用时间之内，步骤 312 通过累计得出用户实际使用时间 T_1，步骤 313 判断有效使用时间 T_0 是否大于用户实际使用时间 T_1，如果是则 314 保持登录状态，如果超时则步骤 315 提示时间到并锁定操作系统。

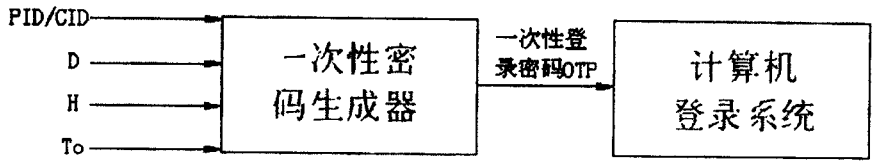

PID/CID
D
H
To
一次性密码生成器
一次性登录密码OTP
计算机登录系统

图1

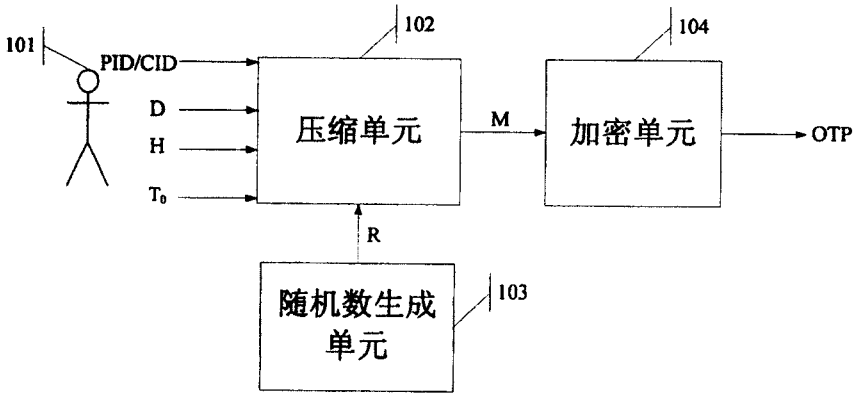

101
PID/CID
D
H
T0
102
压缩单元
M
104
加密单元
OTP
R
随机数生成单元
103

图 2

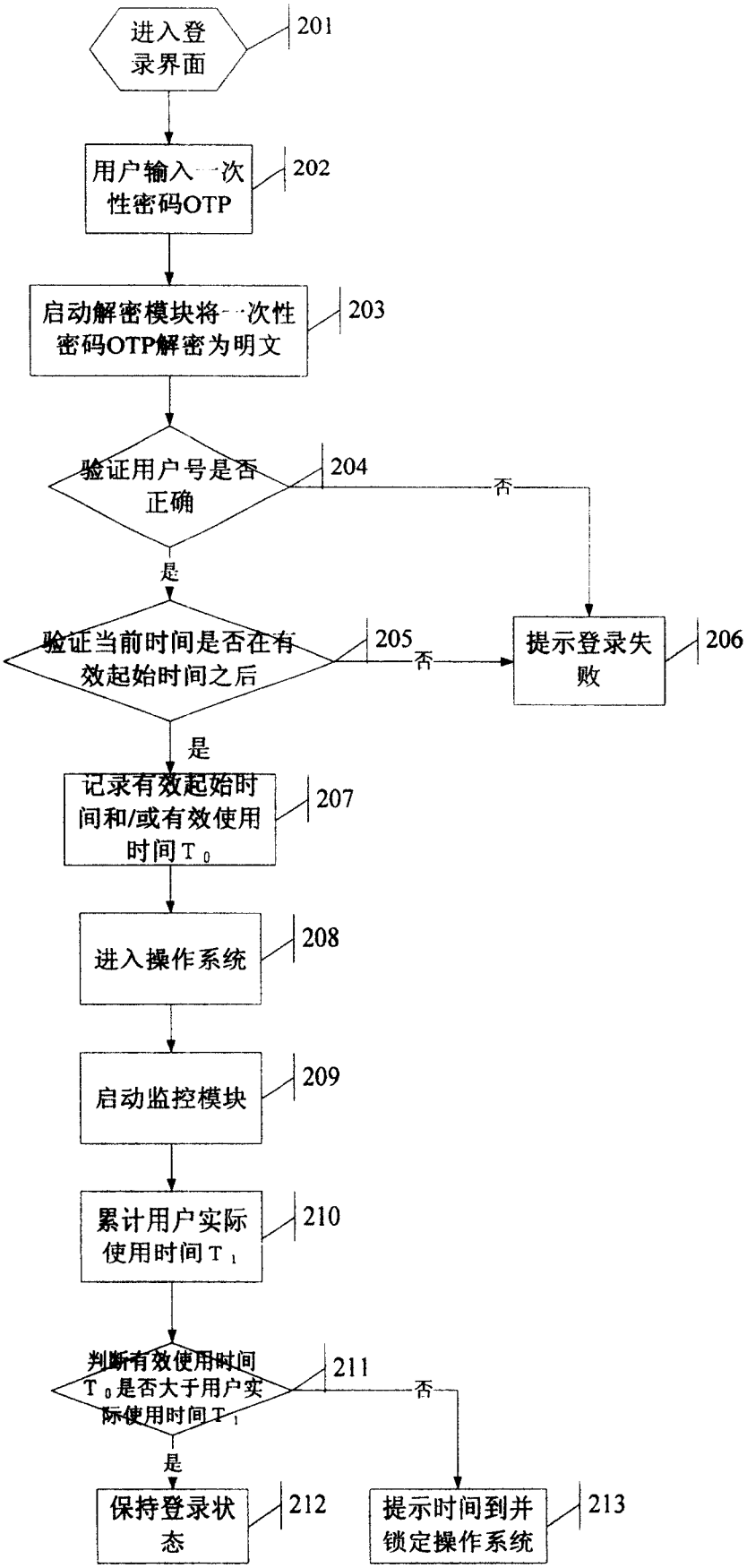

进入登录界面
201
用户输入一次性密码OTP
202
启动解密模块将一次性密码OTP解密为明文
203
验证用户号是否正确
204
否
是
验证当前时间是否在有效起始时间之后
205
否
提示登录失败
206
是
记录有效起始时间和/或有效使用时间T0
207
进入操作系统
208
启动监控模块
209
累计用户实际使用时间T1
210
判断有效使用时间T0是否大于用户实际使用时间T1
211
否
是
保持登录状态
212
提示时间到并锁定操作系统
213

图 3

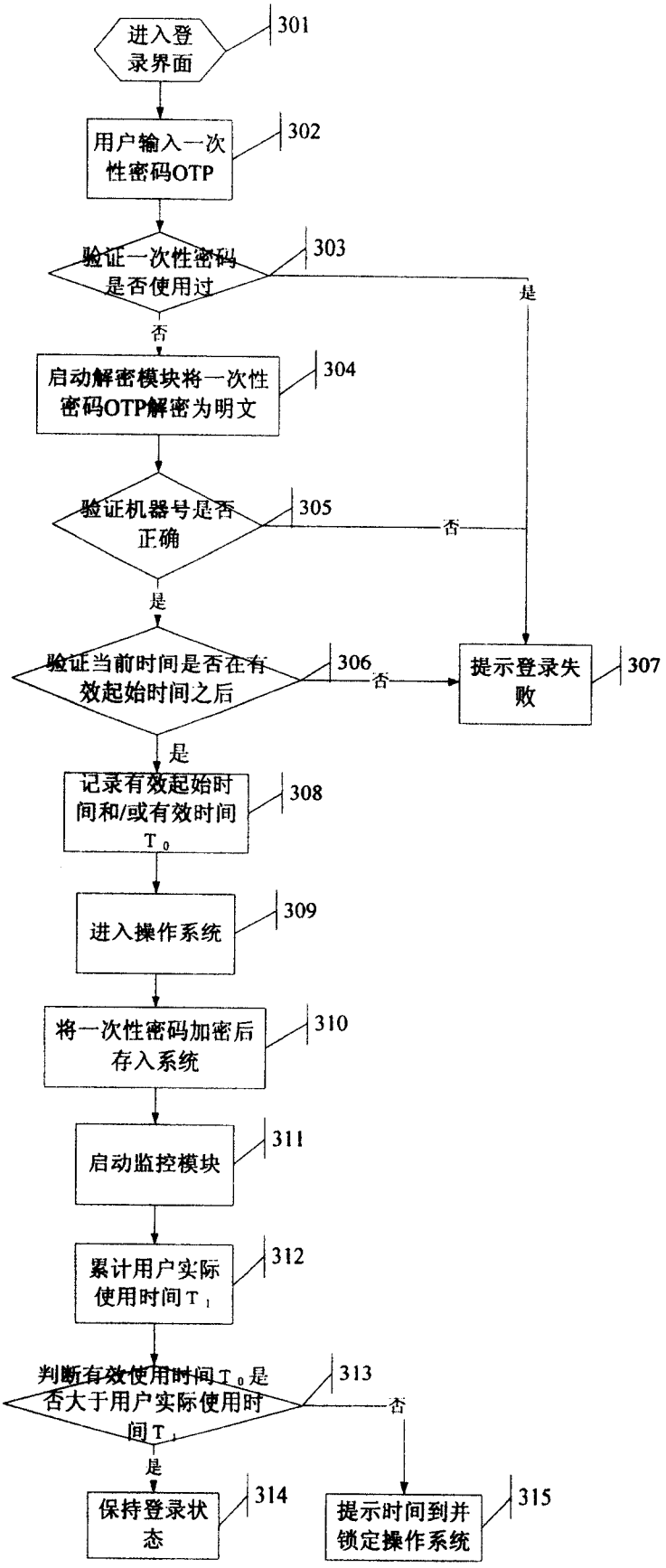

进入登录界面
301
用户输入一次性密码OTP
302
验证一次性密码是否使用过
303
是
否
启动解密模块将一次性密码OTP解密为明文
304
验证机器号是否正确
305
否
是
验证当前时间是否在有效起始时间之后
306
否
提示登录失败
307
是
记录有效起始时间和/或有效时间 T_0
308
进入操作系统
309
将一次性密码加密后存入系统
310
启动监控模块
311
累计用户实际使用时间 T_1
312
判断有效使用时间 T_0 是否大于用户实际使用时间 T_1
313
否
是
保持登录状态
314
提示时间到并锁定操作系统
315

图 4