(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 104021467 A
(43)申请公布日 2014.09.03

(21)申请号 201410261588.6

(22)申请日 2014.06.12

(71)申请人 北京奇虎科技有限公司
地址 100088 北京市西城区新街口外大街28号D座112室(德胜园区)
申请人 奇智软件(北京)有限公司

(72)发明人 孟齐源 高祎玮

(74)专利代理机构 北京智汇东方知识产权代理事务所(普通合伙) 11391
代理人 康正德 范晓斌

(51)Int.Cl.
G06Q 20/08(2012.01)

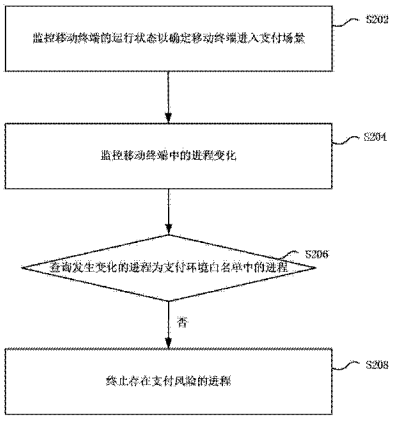
权利要求书2页 说明书10页 附图6页

(54)发明名称

保护移动终端支付安全的方法和装置以及移动终端

(57)摘要

本发明提供了一种保护移动终端支付安全的方法和装置以及移动终端。其中保护移动终端支付安全的方法包括:监控移动终端的运行状态以确定移动终端进入支付场景;监控移动终端中的进程变化;查询发生变化的进程是否为支付环境白名单中的进程,其中支付环境白名单中预先保存有允许在支付环境中运行的进程信息;若否,终止发生变化的进程。本发明的保护移动终端支付安全的方法和装置在进入支付场景后,对终端内进程的变化情况进行监控和分析,及时终止在支付场景中不允许运行的进程,因此可以保护支付场景的安全,提高移动支付的安全性。



CN 104021467 A

1. 一种保护移动终端支付安全的方法，包括：

监控移动终端的运行状态以确定所述移动终端进入支付场景；

监控所述移动终端中的进程变化；

查询发生变化的进程是否为支付环境白名单中的进程，其中所述支付环境白名单中预先保存有允许在支付环境中运行的进程信息；

若否，终止所述发生变化的进程。

2. 根据权利要求 1 所述的方法，其中，监控移动终端的运行状态包括：

获取所述移动终端中新启动的客户端的信息；

将所述客户端的信息与预置的支付类客户端信息进行比对；

在比对成功的情况下确定所述移动终端进入支付场景。

3. 根据权利要求 2 所述的方法，其中，将所述客户端信息与预置的支付类客户端信息进行比对包括：

将所述客户端信息与预置的支付客户端列表的客户端信息进行比对，如果存在比对结果一致的列表项，则比对成功，所述支付客户端列表中预先保存有多种支付类客户端的特征信息；和 / 或

提取所述客户端信息中的包名和标签名，查询所述包名和标签名中是否包含支付类客户端的特征关键字，若是则比对成功。

4. 根据权利要求 1 至 3 中任一项所述的方法，其中，

监控移动终端中的进程变化包括：监控所述移动终端有无新的窗口弹出，并确定出弹出新窗口的进程。

5. 根据权利要求 1 至 3 中任一项所述的方法，其中，

监控移动终端中的进程变化包括：监控所述移动终端有无新的进程启动；

查询发生变化的进程是否为支付环境白名单中的进程包括：将新启动的进程与所述支付环境白名单中的进程进行特征匹配，若匹配成功，确定所述新启动的进程为所述支付环境白名单中的进程。

6. 根据权利要求 5 所述的方法，其中，所述支付环境白名单中的进程包括：缓存中记录的允许开启的进程、系统进程和被云查杀服务器判定为无支付风险的进程。

7. 根据权利要求 1 至 6 中任一项所述的方法，其中，在监控移动终端中的进程变化之前还包括：

枚举所述移动终端中运行的进程；

终止不属于所述支付环境白名单的枚举出的进程。

8. 一种保护移动终端支付安全的装置，包括：

支付识别模块，配置为监控移动终端的运行状态以确定所述移动终端进入支付场景；

进程监控模块，配置为监控所述移动终端中的进程变化；

进程分析模块，配置为查询发生变化的进程是否为支付环境白名单中的进程，其中所述支付环境白名单中预先保存有允许在支付环境中运行的进程信息；

进程终止模块，配置为终止不属于所述支付环境白名单的发生变化的进程。

9. 根据权利要求 8 所述的装置，其中，所述支付识别模块还配置为：

获取所述移动终端中新启动的客户端的信息；

将所述客户端的信息与预置的支付类客户端信息进行比对；

在比对成功的情况下确定所述移动终端进入支付场景。

10. 一种移动终端，包括：

权利要求 8 或 9 中任一项所述的保护移动终端支付安全的装置。

保护移动终端支付安全的方法和装置以及移动终端

技术领域

[0001] 本发明涉及移动通信领域，特别是涉及一种保护移动终端支付安全的方法和装置以及移动终端。

背景技术

[0002] 移动支付将终端设备、互联网、应用提供商以及金融机构相融合，为用户提供货币支付、缴费等金融业务。随着移动电子商务迅速发展，第三方支付、银行等争相推出移动支付客户端，购物、理财、生活服务等交易类客户端也在不断出现，大大丰富了移动支付的市场应用环境。

[0003] 移动支付使用用户的手机号或其他标识作为关联支付账户，通过身份确认来进行支付交易活动。移动支付接入方式可以包括短信、语音、网络连接等方式。目前在远程移动支付领域，网络连接方式应用最为广泛，用户通过移动向提供某种商品或服务的商家发出交易申请，利用无线网络传输交易数据并完成交易支付。

[0004] 移动支付的安全性是影响支付业务能否发展的关键因素。移动支付的安全性涉及用户信息的保密、用户资金和支付信息的安全等问题，其面临的安全风险主要来自于两个方面：网络和系统的安全性，终端的安全性。

[0005] 在终端方面，一些木马程序和钓鱼网站会伪装成支付网站和支付客户端，骗取用户的账号密码或者直接进行金融诈骗，现有技术中，主要依靠扫描来清除木马，保证终端信息安全。然而，一些木马仅在特定的条件触发后才启动，依靠静态扫描的方式无法完全消除支付的安全隐患。

发明内容

[0006] 鉴于上述问题，提出了本发明以便提供一种克服上述问题或者至少部分地解决上述问题的移动终端以及保护移动终端支付安全的装置和相应的保护移动终端支付安全方法。

[0007] 本发明一个进一步的目的是要提高移动终端在支付环境下的安全性。

[0008] 依据本发明的一个方面，提供了一种保护移动终端支付安全的方法。该方法包括：监控移动终端的运行状态以确定移动终端进入支付场景；监控移动终端中的进程变化；查询发生变化的进程是否为支付环境白名单中的进程，其中支付环境白名单中预先保存有允许在支付环境中运行的进程信息；若否，终止发生变化的进程。

[0009] 可选地，监控移动终端的运行状态包括：获取移动终端中新启动的客户端的信息；将客户端的信息与预置的支付类客户端信息进行比对；在比对成功的情况下确定移动终端进入支付场景。

[0010] 可选地，将客户端信息与预置的支付类客户端信息进行比对包括：将客户端信息与预置的支付客户端列表的客户端信息进行比对，如果存在比对结果一致的列表项，则比对成功，支付客户端列表中预先保存有多种支付类客户端的特征信息；和／或提取客户端

信息中的包名和标签名，查询包名和标签名中是否包含支付类客户端的特征关键字，若是则比对成功。

[0011] 可选地，监控移动终端中的进程变化包括：监控移动终端中的进程变化包括：监控移动终端有无新的窗口弹出，并确定出弹出新窗口的进程。

[0012] 可选地，监控移动终端中的进程变化包括：监控移动终端有无新的进程启动；查询发生变化的进程是否为支付环境白名单中的进程包括：将新启动的进程与支付环境白名单中的进程进行特征匹配，若匹配成功，确定新启动的进程为支付环境白名单中的进程。

[0013] 可选地，支付环境白名单中的进程包括：缓存中记录的允许开启的进程、系统进程和被云查杀服务器判定为无支付风险的进程。

[0014] 可选地，在监控移动终端中的进程变化之前还包括：枚举移动终端中运行的进程；终止不属于支付环境白名单的枚举出的进程。

[0015] 根据本发明的另一个方面，还提供了一种保护移动终端支付安全的装置。该装置包括：支付识别模块，配置为监控移动终端的运行状态以确定移动终端进入支付场景；进程监控模块，配置为监控移动终端中的进程变化；进程分析模块，配置为查询发生变化的进程是否为支付环境白名单中的进程，其中支付环境白名单中预先保存有允许在支付环境中运行的进程信息；进程终止模块，配置为终止不属于支付环境白名单的发生变化的进程。

[0016] 可选地，支付识别模块还配置为：获取移动终端中新启动的客户端的信息；将客户端的信息与预置的支付类客户端信息进行比对；在比对成功的情况下确定移动终端进入支付场景。

[0017] 可选地，支付识别模块包括：数据比对子模块，配置为将客户端信息与预置的支付客户端列表的客户端信息进行比对，如果存在比对结果一致的列表项，则比对成功，支付客户端列表中预先保存有多种支付类客户端的特征信息；特征分析子模块，配置为提取客户端信息中的包名和标签名，查询包名和标签名中是否包含支付类客户端的特征关键字，若是则比对成功。

[0018] 可选地，进程监控模块还配置为：控移动终端有无新的窗口弹出，并确定出弹出新窗口的进程。

[0019] 可选地，进程监控模块还配置为：监控移动终端有无新的进程启动；进程分析模块还配置为：将新启动的进程与支付环境白名单中的进程进行特征匹配，若匹配成功，确定新启动的进程为支付环境白名单中的进程。

[0020] 可选地，以上保护移动终端支付安全的装置还包括：进程清场模块，配置为枚举移动终端中运行的进程，并终止不属于支付环境白名单的枚举出的进程。

[0021] 根据本发明的另一个方面，提供了一种移动终端。该移动终端包括：以上介绍的任一种保护移动终端支付安全的装置。

[0022] 本发明的保护移动终端支付安全的方法和装置在进入支付场景后，对终端内进程的变化情况进行监控和分析，及时终止不允许在支付环境中运行的进程，因此可以保护支付场景的安全，提高移动支付的安全性。

[0023] 进一步地，本发明的保护移动终端支付安全的方法，在进入支付场景时，清除与支付无关的进程，完成支付清场，为安全支付提供安全的支付环境。

[0024] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，

而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。

[0025] 根据下文结合附图对本发明具体实施例的详细描述，本领域技术人员将会更加明了本发明的上述以及其他目的、优点和特征。

附图说明

[0026] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0027] 图 1 是根据本发明一个实施例的保护移动终端支付安全的装置的示意图；

[0028] 图 2 是根据本发明一个实施例的保护移动终端支付安全的方法的示意图；

[0029] 图 3 是根据本发明实施例的基于移动终端的支付方法中确定移动终端进入支付场景的流程图；

[0030] 图 4 是根据本发明实施例的基于移动终端的支付方法中客户端扫描的界面效果图；

[0031] 图 5 是根据本发明实施例的基于移动终端的支付方法中进行版本校验的效果图；

[0032] 图 6 是根据本发明实施例的基于移动终端的支付方法中进行支付清场的流程图；以及

[0033] 图 7 是根据本发明实施例的基于移动终端的支付方法的一种可选流程图。

具体实施方式

[0034] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述，构造这类系统所要求的结构是显而易见的。此外，本发明也不针对任何特定编程语言。应当明白，可以利用各种编程语言实现在此描述的本发明的内容，并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0035] 图 1 是根据本发明一个实施例的保护移动终端支付安全的装置 100 的示意图，该保护移动终端支付安全的装置 100 一般性地可以包括：支付识别模块 110、进程监控模块 120、进程分析模块 130、进程终止模块 140、进程清场模块 150，以上模块可以根据本实施例的保护移动终端支付安全的装置的功能需求，灵活进行配置，在一些可选环境下，可以不配置以上所有模块。

[0036] 本实施例的保护移动终端支付安全的装置 100 可以安装于本实施例的移动终端或其他移动支付设备中，并在移动终端进行移动支付的过程中运行，提高移动终端的支付数据的安全性。

[0037] 在以上本实施例的保护移动终端支付安全的装置 100 的各部件中，支付识别模块 110 用于监控移动终端的运行状态以确定移动终端进入支付场景。支付场景的确定可以根据移动终端的运行状态来确定，例如获取移动终端中新启动的客户端的信息；将客户端的信息与预置的支付类客户端信息进行比对；在比对成功的情况下确定移动终端进入支付场景，也就是利用移动终端启动的客户端来判断支付场景，当检测到移动终端有新的客户端

启动后，利用信息比对判断新启动的客户端是否为移动支付客户端，如果确定移动终端启动了支付客户端，则可以确定移动终端进入支付场景。判断新启动的客户端是否为移动支付客户端的过程可以通过本地的客户端列表验证以及客户端特征匹配来实现。

[0038] 支付识别模块 110 的一种具体结构可以设置：数据比对子模块和特征分析子模块。其中，数据比对子模块将客户端信息与预置的支付客户端列表的客户端信息进行比对，如果存在比对结果一致的列表项，则比对成功，支付客户端列表中预先保存有多种支付类客户端的特征信息。特征分析子模块提取客户端信息中的包名和标签名，查询包名和标签名中是否包含支付类客户端的特征关键字，若是则比对成功。数据比对子模块使用的支付客户端列表可以根据移动终端的具体使用情况进行动态调整，以记录所有已安装支付客户端的信息。

[0039] 特征分析子模块中使用的特征一般可以包括包名和标签名 (lable)，此外还可以包括签名、版本号等特征。特征分析可以在移动终端本地进行，也可以将特征信息上传至云端，由云端进行判断后，将判断结果返回给移动终端。

[0040] 进程监控模块 120 在支付场景下监控移动终端中的进程变化，进程变化的情况包括：监控移动终端有无新的进程启动，或者有无新的进程窗口弹出。

[0041] 在进程监控模块 120 检测到进程变化后，进程分析模块 130 查询发生变化的进程是否为支付环境白名单中的进程，例如查询弹出的新窗口是否为用户开启的新窗口或者白名单中允许在支付场景中后台运行的进程弹出的窗口，若否，需要由进程终止模块终止该进程。又例如，将新启动的进程与支付环境白名单中的进程进行特征匹配，若匹配成功，确定新启动的进程为支付环境白名单中的进程。

[0042] 支付环境白名单中的进程可以包括：缓存中记录的允许开启的进程、系统进程和被云查杀服务器判定为无支付风险的进程等对支付没有影响的进程，该白名单的验证执行可以采用本地验证和云验证的方式进行，例如首先在本地进行缓存验证、签名验证、系统进程验证，如果确认进程属于白名单中的进程则可以完成验证，如果本地无法验证还可以在云端进行匹配，以避免终止对支付环境没有安全威胁的进程。

[0043] 进程终止模块 140 为终止不属于支付环境白名单的发生变化的进程，从而保证支付环境下，移动终端不会产生对支付产生影响的进程，消除了移动支付中终端侧的安全隐患，另一方面还可以减少无关进程对数据传输通道的占用，提高支付效率。

[0044] 另外，进程清场模块 150 还可以在检测到移动终端进入支付场景后，枚举移动终端中运行的进程，并终止不属于支付环境白名单的枚举出的进程。也就是，进程清场模块 150 对支付环境进行了清场，可以清除与移动支付无关的进程，防止已经运行的木马或其他恶意程序盗取移动支付客户端的数据，而且还可以减少了网络通道的占用。

[0045] 本实施例的保护移动终端支付安全的装置，可以在检测到用户开启支付类客户端后，首先校验支付类客户端，并在确认支付类客户端的安全性后，进行支付清场，以终止不在支付环境白名单中的进程，并在支付过程中，实时检测移动终端的进程变化，并终止不在支付环境白名单中的进程重新启动，保护支付环境，直至移动终端退出支付场景。在移动支付的整个过程中，确保终端方面的支付安全性。

[0046] 本发明实施例还提供了一种保护移动终端支付安全的方法，该保护移动终端支付安全的方法可以由以上实施例介绍的任意一种保护移动终端支付安全的来执行，以提高本

实施例的移动终端在支付过程中的安全性。图 2 是根据本发明一个实施例的保护移动终端支付安全的方法的示意图，如图所示，该保护移动终端支付安全的方法包括以下步骤：

[0047] 步骤 S202，监控移动终端的运行状态以确定移动终端进入支付场景；

[0048] 步骤 S204，监控移动终端中的进程变化；

[0049] 步骤 S206，查询发生变化的进程是否为支付环境白名单中的进程；

[0050] 步骤 S208，若否，终止发生变化的进程。

[0051] 其中支付环境白名单中预先保存有允许在支付环境中运行的进程信息，例如缓存中记录的允许开启的进程、系统进程和被云查杀服务器判定为无支付风险的进程等可以在支付场景中运行的进程。

[0052] 若步骤 S206 判断出生变化的进程是支付环境白名单中的进程，则允许该进程运行，并可以暂停移动支付的流程。

[0053] 步骤 S202 中监控移动终端的运行状态具体可以包括：获取移动终端中新启动的客户端的信息；将客户端的信息与预置的支付类客户端信息进行比对；在比对成功的情况下确定移动终端进入支付场景。从而可以根据移动终端启动的客户端来判断进入支付场景，当检测到移动终端有新的客户端启动后，判断新启动的客户端是否为移动支付客户端，如果确定移动终端启动了支付客户端，则确定移动终端进入支付场景。判断新启动的客户端是否为移动支付客户端的过程可以通过本地的客户端列表验证以及客户端特征匹配来实现。图 3 是根据本发明实施例的基于移动终端的支付方法中确定移动终端进入支付场景的流程图，该流程包括：

[0054] 步骤 S302，监控移动终端中是否有新的客户端启动；

[0055] 步骤 S304，判断新启动的客户端是否是本地支付客户端列表中记录的客户端，若是，确定进入支付场景，若否，可以进一步执行步骤 S306 确定未进入支付场景；

[0056] 步骤 S306，判断新启动的客户端的特征是否与支付类客户端特征关键字匹配若是，确定进入支付场景，若否，确定未进入支付场景；

[0057] 在步骤 S304 中，移动终端在本地中可以预先保存一个支付客户端列表，用于记录移动终端安装的支付类客户端信息，具体可以将客户端信息与支付客户端列表的客户端信息进行比对，如存在比对结果一致的列表项，则比对成功，确定进入支付场景。当新启动的客户端不在列表中时，可以执行步骤 S306 利用云查询的方法进一步确定，例如提取客户端的包名、标签名、版本信息等特征信息，与查询包名和标签名中是否包含支付类客户端的特征关键字，若是则比对成功确定进入支付场景。以上支付客户端列表可以根据移动终端的使用情况进行动态调整，以记录所有已安装支付客户端的信息。

[0058] 在步骤 S202 之后，还可以首先对支付客户端进行版本校验，并进行支付清场，即关闭与支付无关的进程。

[0059] 对支付客户端进行版本校验的过程可以在首先进行病毒扫描，对客户端的权限、特征信息等特征匹配，对于不能确定的客户端可以将客户端的包名、签名、版本号等信息上传至云端进行验证，如果验证的结果确定客户端包含木马或病毒，提示用户进行卸载，对于验证结果为不包括木马或病毒的客户端，可以依次分析该客户端的以下内容：是否为正版软件、是否经过二次打包、是否存在欺诈行为，在客户端为正版无欺诈的支付类客户端时，进入支付场景的流程。如果客户端未通过验证，可以对用户进行提示，例如向用户推荐正版

软件或者提示支付风险。

[0060] 以上版本校验可以使用移动终端中预置的具有应用安全分析功能的安全软件进行，例如在安全卫士软件中预置支付安全扫描的操作选项，在用户对该操作选项进行点击或其他操作后，安全卫士按照上述的版本校验流程，扫描支付类客户端。图 4 是根据本发明实施例的基于移动终端的支付方法中客户端扫描的界面效果图，图 5 是根据本发明实施例的基于移动终端的支付方法中进行版本校验的效果图。如图在安全软件的主界面上除了快速扫描的按钮外，还可以预置支付安全的按钮，在用户操作以上按钮后，安全卫士对客户端的权限、包名、标签名、版本号依次进行扫描。

[0061] 图 6 是根据本发明实施例的基于移动终端的支付方法中进行支付清场的流程图，该流程包括以下步骤：

[0062] 在移动终端进入支付场景且支付客户端版本已经通过验证之后，枚举移动终端当前运行的所有进程，然后依次对进程进行以下判断：本地缓存查询判断、白签名判断、系统进程判断、云查杀判断、云查杀结果判断。

[0063] 其中，本地缓存查询判断是指在文件扫描过程中把文件的特征（文件路径，文件大小、文件最后修改时间、文件创建时间、通过三要素计算出全文 MD5，SHA1）存储在本地数据库，从而可以通过本地数据库获取待扫描文件的文件属性信息。例如文件大小、文件修改时间和文件路径等。系统中文件属性信息可根据文件的修改进行实时更新。根据文件路径从本地数据库获取文件信息对于同一个文件，如果应用层扫描感知到文件大小，文件最后修改时间，文件创建时间没有变化，且驱动层（qutmdrv.sys）在文件监控过程中也没有监控到文件发生过写操作，那么我们就认为两次扫描之中文件没有发生变化，就可以直接从数据库中获取该文件的特征如全文 MD5，全文 SHA1 等信息。文件监控主要是驱动来做的，主要是审计驱动检测文件是否被改动。例如，出现了写操作，或者属性进行了修改，则可以在数据库中记录该变化情况，并认为该文件已经失效，在文件扫描过程中把文件的特征（文件路径，文件大小、文件最后修改时间、文件创建时间、通过三要素计算出全文 MD5，SHA1）存储在本地数据库。如果未修改过，就可以直接从数据库中获取该文件的特征如全文 MD5，全文 SHA1 等信息。

[0064] 因为文件的最后修改时间和文件的创建时间是可以修改的，所以如果文件内容发生变化文件大小相同，且文件的最后修改时间及文件的创建时间也改为一样，就可以造成该方法会获取到一个错误的文件标识，因此引入了文件监控，当文件发生写操作或者其他的修改操作时就把本地缓存数据库的对应的记录做一个无效标志，下回扫描时，重新获取文件的特征。

[0065] 通过本地缓存查询还可以确定当前扫描的进程与之前扫描的进程进行匹配，例如该进程之前被确定为白名单进程，则可以在支付环境下保留该进程，该进程之前被确定为黑名单进程，则可以加入黑 / 灰进程列表，并清除，对于本地缓存查询无结果或者类型不明确的进程可以记为灰名单进程，进行下一步判断。

[0066] 白签名判断是指判断当前进程是否为本地记录的排序靠前的若干白签名的进程，例如使用 1000 个可以确定为白签名对进程对应的签名进行比对，如果确认进程签名属于白签名，则可以在支付环境下保留该进程，如果进程签名不在白签名中，则需要进行下一步判断。

[0067] 系统进程判断是指判断当前进程是否为系统核心进程，一般而言，系统核心进程的UID(User Identification，用户身份证明）小于1000，因此可以将UID小于1000的进程在支付环境下保留该进程，否则需要进行下一步判断。

[0068] 云查杀判断是指查询客户端的特征是否与云端的客户端特征进行匹配，若云端不存在与客户端特征匹配的特征，则可以在支付环境下保留该进程，如果在云端查询出对应特征中，则需要进行下一步判断。

[0069] 云查杀结果判断是指确定客户端云查杀的结果为白样本还是黑样本，若为白样本则可以在支付环境下保留该进程，若被确定为黑样本，则可以加入黑／灰进程列表，并清除。

[0070] 以上多个判断过程依次进行，采用非黑即白的策略，终止所有的黑／灰进程，仅允许白进程在支付环境保持运行。

[0071] 在完成支付清场后，进行进程监控、分析和处理。图7是根据本发明实施例的基于移动终端的支付方法的一种可选流程图，该可选流程可以包括：

[0072] 在完成支付清偿后，同时监控移动终端有无新的进程启动以及监控移动终端有无新的窗口弹出，在监控新窗口时，执行以下步骤：

[0073] S702，监控移动终端是否有新的进程窗口出现；

[0074] S704，查询弹出的新窗口是否为用户开启的新窗口或者允许在支付场景中后台运行的进程弹出的窗口，若否执行步骤S706，若是，执行步骤S708；

[0075] S706，在后台关闭该新窗口，并且无需给用户进行提示；

[0076] S708，允许新窗口执行，并按暂停支付客户端；

[0077] 在监控新进程时，执行以下步骤：

[0078] 步骤S710，监控移动终端有无新的进程启动；

[0079] 步骤S712，调用支付清场的缓存策略进行进程验证，与之前支付清场过程中缓存的白进程和黑／灰进程进行比对，缓存策略同样可以使用特征比对的方式进行，例如文件路径，文件大小、文件最后修改时间、文件创建时间、通过三要素计算出全文MD5或SHA1，前文已介绍，在此不做赘述；

[0080] 步骤S714，判断是否为清场过程中终止的进程，若是，执行步骤S718，若否，执行步骤S716；

[0081] 步骤S716，对该进程按照支付清场的逻辑进一步进行检测，检测同样可以采用本地缓存查询判断、白签名判断、系统进程判断、云查杀判断、云查杀结果判断等步骤进行，对支付清场中未出现的新进程进行扫描；

[0082] 步骤S718，终止新进程。

[0083] 在步骤S708和S718之后，可以分别判断当前支付场景是否已退出，即判断用户是否已关闭支付客户端，若否分别返回执行步骤S702和步骤S708，若是，结束支付环境保护，返回支付场景之前的移动终端状态。

[0084] 本实施例的保护移动终端支付安全的方法在进入支付场景后，对终端内进程的变化情况进行监控和分析，及时终止存在支付风险的进程，因此可以保护支付场景的安全，提高移动支付的安全性。并且在进入支付场景时，清除与支付无关的进程，完成支付清场，为安全支付提供安全的支付环境。从而消除了移动支付过程中由于移动终端进程导致的安全

隐患。

[0085] 在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

[0086] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0087] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和／或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0088] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0089] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的客户端模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的保护移动终端支付安全的装置和移动终端中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0090] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0091] 至此，本领域技术人员应认识到，虽然本文已详尽示出和描述了本发明的多个示例性实施例，但是，在不脱离本发明精神和范围的情况下，仍可根据本发明公开的内容直接确定或推导出符合本发明原理的许多其他变型或修改。因此，本发明的范围应被理解和认定为覆盖了所有这些其他变型或修改。

[0092] 本发明实施例还提供了 A1. 一种保护移动终端支付安全的方法，包括：

[0093] 监控移动终端的运行状态以确定所述移动终端进入支付场景；

[0094] 监控所述移动终端中的进程变化；

[0095] 查询发生变化的进程是否为支付环境白名单中的进程，其中所述支付环境白名单中预先保存有允许在支付环境中运行的进程信息；

[0096] 若否，终止所述发生变化的进程。

[0097] A2. 根据 A1 所述的方法，其中，监控移动终端的运行状态包括：

[0098] 获取所述移动终端中新启动的客户端的信息；

[0099] 将所述客户端的信息与预置的支付类客户端信息进行比对；

[0100] 在比对成功的情况下确定所述移动终端进入支付场景。

[0101] A3. 根据 A2 所述的方法，其中，将所述客户端信息与预置的支付类客户端信息进行比对包括：

[0102] 将所述客户端信息与预置的支付客户端列表的客户端信息进行比对，如果存在比对结果一致的列表项，则比对成功，所述支付客户端列表中预先保存有多种支付类客户端的特征信息；和 / 或

[0103] 提取所述客户端信息中的包名和标签名，查询所述包名和标签名中是否包含支付类客户端的特征关键字，若是则比对成功。

[0104] A4. 根据 A1 至 A3 中任一项所述的方法，其中，

[0105] 监控移动终端中的进程变化包括：监控所述移动终端有无新的窗口弹出，并确定出弹出新窗口的进程。

[0106] A5. 根据 A1 至 A3 中任一项所述的方法，其中，

[0107] 监控移动终端中的进程变化包括：监控所述移动终端有无新的进程启动；

[0108] 查询发生变化的进程是否为支付环境白名单中的进程包括：将新启动的进程与所述支付环境白名单中的进程进行特征匹配，若匹配成功，确定所述新启动的进程为所述支付环境白名单中的进程。

[0109] A6. 根据 A5 所述的方法，其中，所述支付环境白名单中的进程包括：缓存中记录的允许开启的进程、系统进程和被云查杀服务器判定为无支付风险的进程。

[0110] A7. 根据 A1 至 A6 中任一项所述的方法，其中，在监控移动终端中的进程变化之前还包括：

[0111] 枚举所述移动终端中运行的进程；

[0112] 终止不属于所述支付环境白名单的枚举出的进程。

[0113] 本发明实施例还提供了 B8. 一种保护移动终端支付安全的装置，包括：

[0114] 支付识别模块，配置为监控移动终端的运行状态以确定所述移动终端进入支付场景；

[0115] 进程监控模块，配置为监控所述移动终端中的进程变化；

[0116] 进程分析模块，配置为查询发生变化的进程是否为支付环境白名单中的进程，其中所述支付环境白名单中预先保存有允许在支付环境中运行的进程信息；

[0117] 进程终止模块，配置为终止不属于所述支付环境白名单的发生变化的进程。

[0118] B9. 根据 B8 所述的装置，其中，所述支付识别模块还配置为：

[0119] 获取所述移动终端中新启动的客户端的信息；

[0120] 将所述客户端的信息与预置的支付类客户端信息进行比对；

[0121] 在比对成功的情况下确定所述移动终端进入支付场景。

[0122] B10. 根据 B9 所述的装置，其中，所述支付识别模块包括：

[0123] 数据比对子模块，配置为将所述客户端信息与预置的支付客户端列表的客户端信息进行比对，如果存在比对结果一致的列表项，则比对成功，所述支付客户端列表中预先保存有多种支付类客户端的特征信息；

[0124] 特征分析子模块，配置为提取所述客户端信息中的包名和标签名，查询所述包名和标签名中是否包含支付类客户端的特征关键字，若是则比对成功。

[0125] B11. 根据 B8 至 B10 中任一项所述的装置，其中，

[0126] 所述进程监控模块还配置为：控所述移动终端有无新的窗口弹出，并确定出弹出新窗口的进程。

[0127] B12. 根据 B8 至 B10 中任一项所述的装置，其中，

[0128] 所述进程监控模块还配置为：监控所述移动终端有无新的进程启动；

[0129] 所述进程分析模块还配置为：将新启动的进程与所述支付环境白名单中的进程进行特征匹配，若匹配成功，确定所述新启动的进程为所述支付环境白名单中的进程。

[0130] B13. 根据 B8 至 B12 中任一项所述的装置，还包括：

[0131] 进程清场模块，配置为枚举所述移动终端中运行的进程，并终止不属于所述支付环境白名单的枚举出的进程。

[0132] 本发明实施例还提供了 C14. 一种移动终端，包括：B8 至 B13 中任一项所述的保护移动终端支付安全的装置。

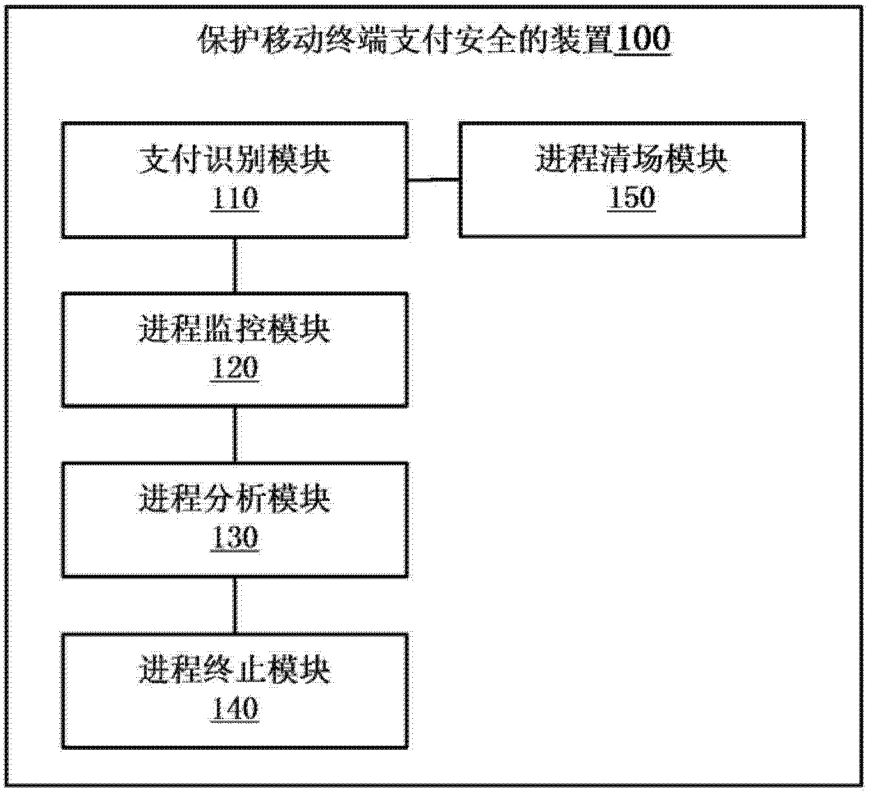

保护移动终端支付安全的装置100
支付识别模块
110
进程清场模块
150
进程监控模块
120
进程分析模块
130
进程终止模块
140

图 1

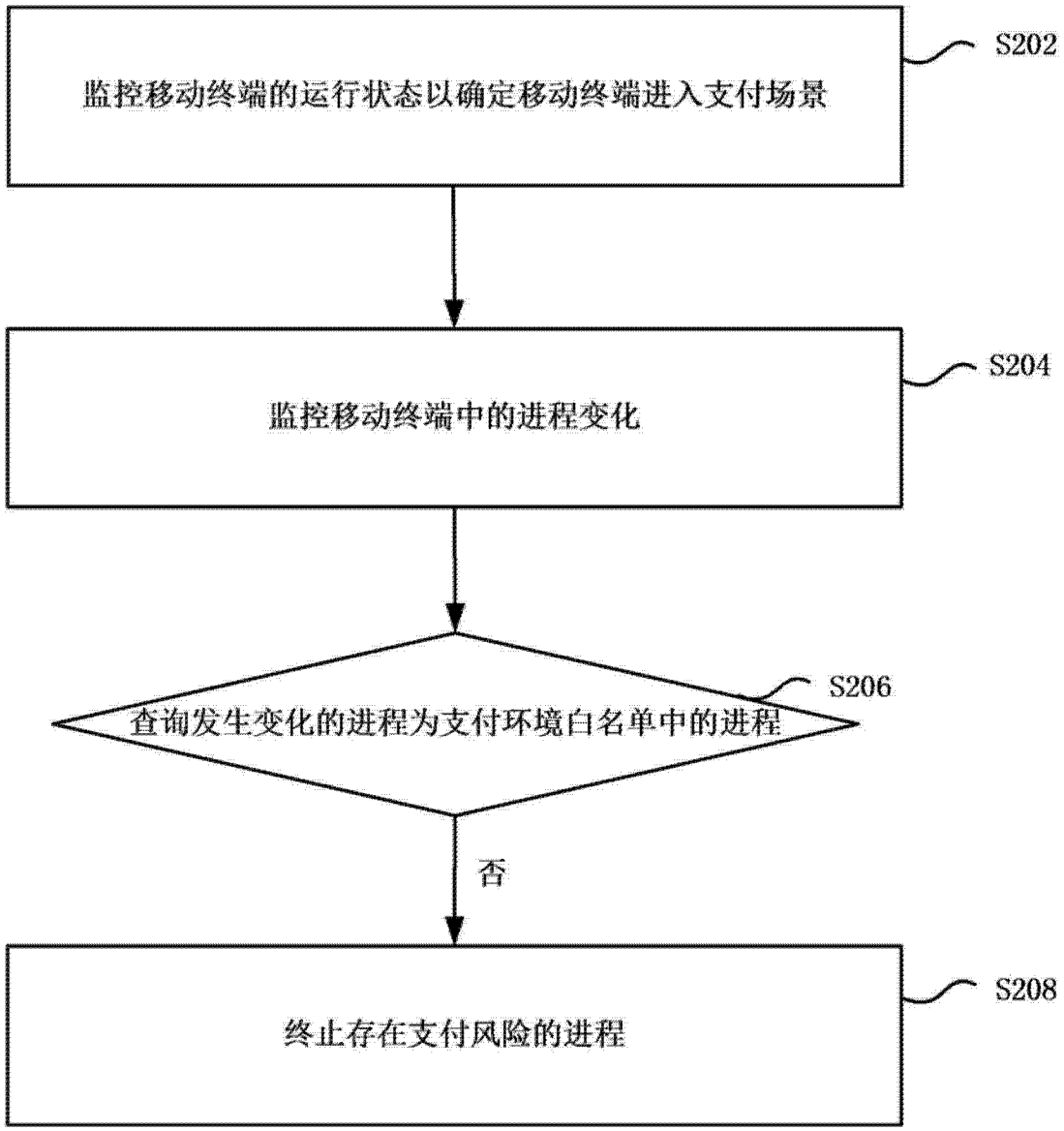

监控移动终端的运行状态以确定移动终端进入支付场景
S202
监控移动终端中的进程变化
S204
查询发生变化的进程为支付环境白名单中的进程
S206
否
终止存在支付风险的进程
S208

图 2

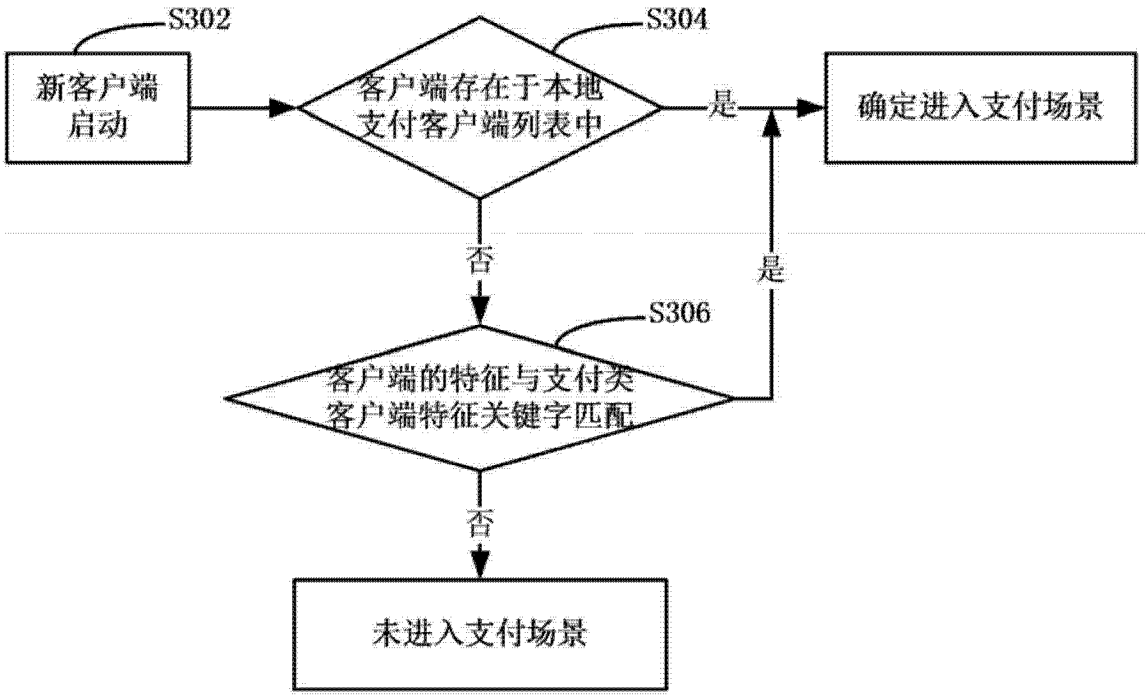

S302
新客户端
启动
S304
客户端存在于本地
支付客户端列表中
是
确定进入支付场景
否
是
S306
客户端的特征与支付类
客户端特征关键字匹配
否
未进入支付场景

图 3


快速扫描
防隐私泄露
防广告骚扰
防通知打扰
清理优化
支付安全
骚扰拦截

图 4


12%
取消
正在扫描：/storage/sdca...ndroid.fileexplorer/cache
.../data/com.android.fileexplorer/cache
...ndroid/data/com.android.fileexplorer
...n.gallery/cache/local-image-thumbs
...sson.gallery/cache/local-skip-cache
...son.gallery/cache/local-meta-cache

图 5

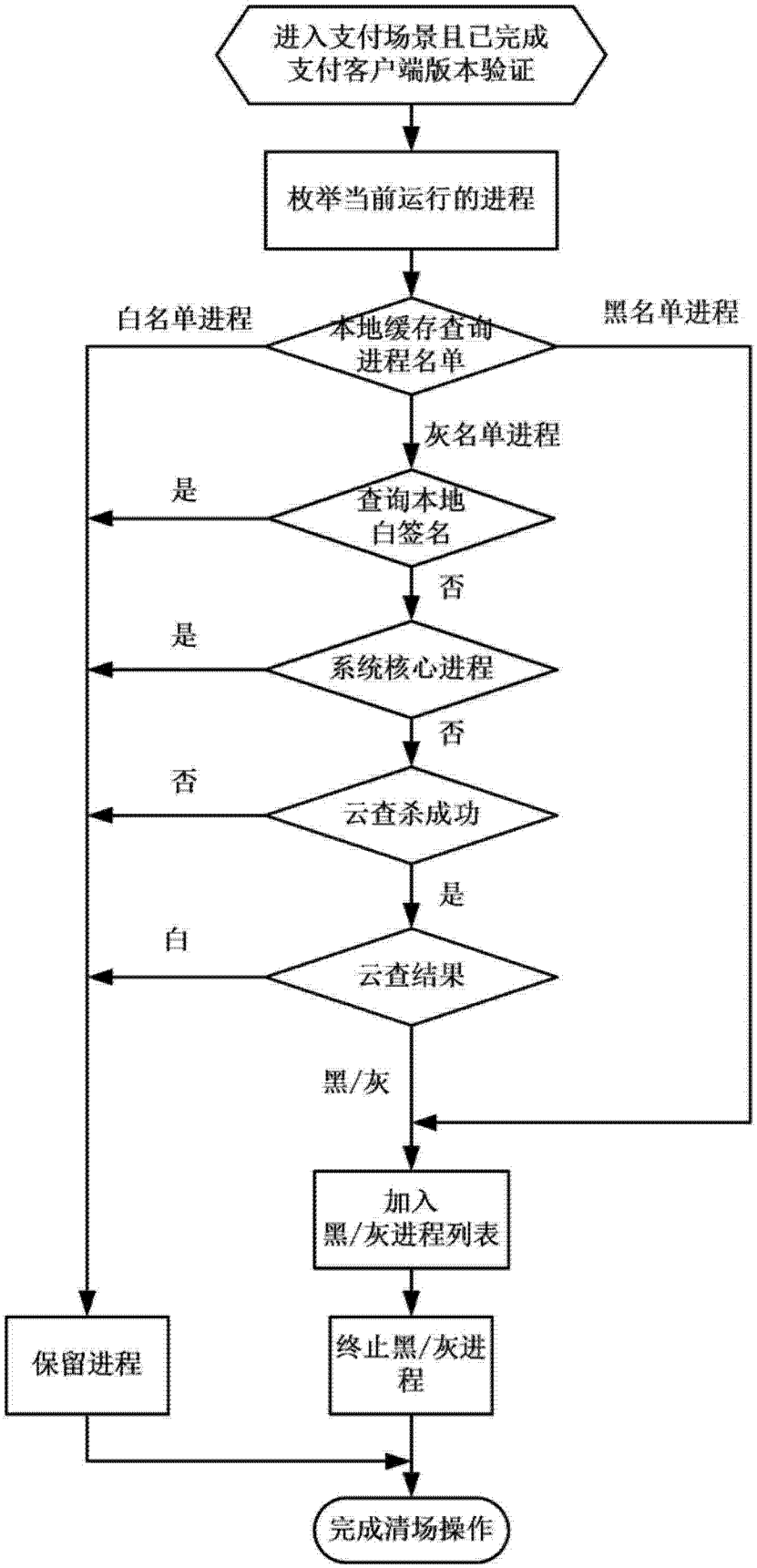

进入支付场景且已完成
支付客户端版本验证
枚举当前运行的进程
白名单进程
本地缓存查询
进程名单
黑名单进程
灰名单进程
是
查询本地
白签名
否
是
系统核心进程
否
否
云查杀成功
是
白
云查结果
黑/灰
加入
黑/灰进程列表
保留进程
终止黑/灰进
程
完成清场操作

图 6

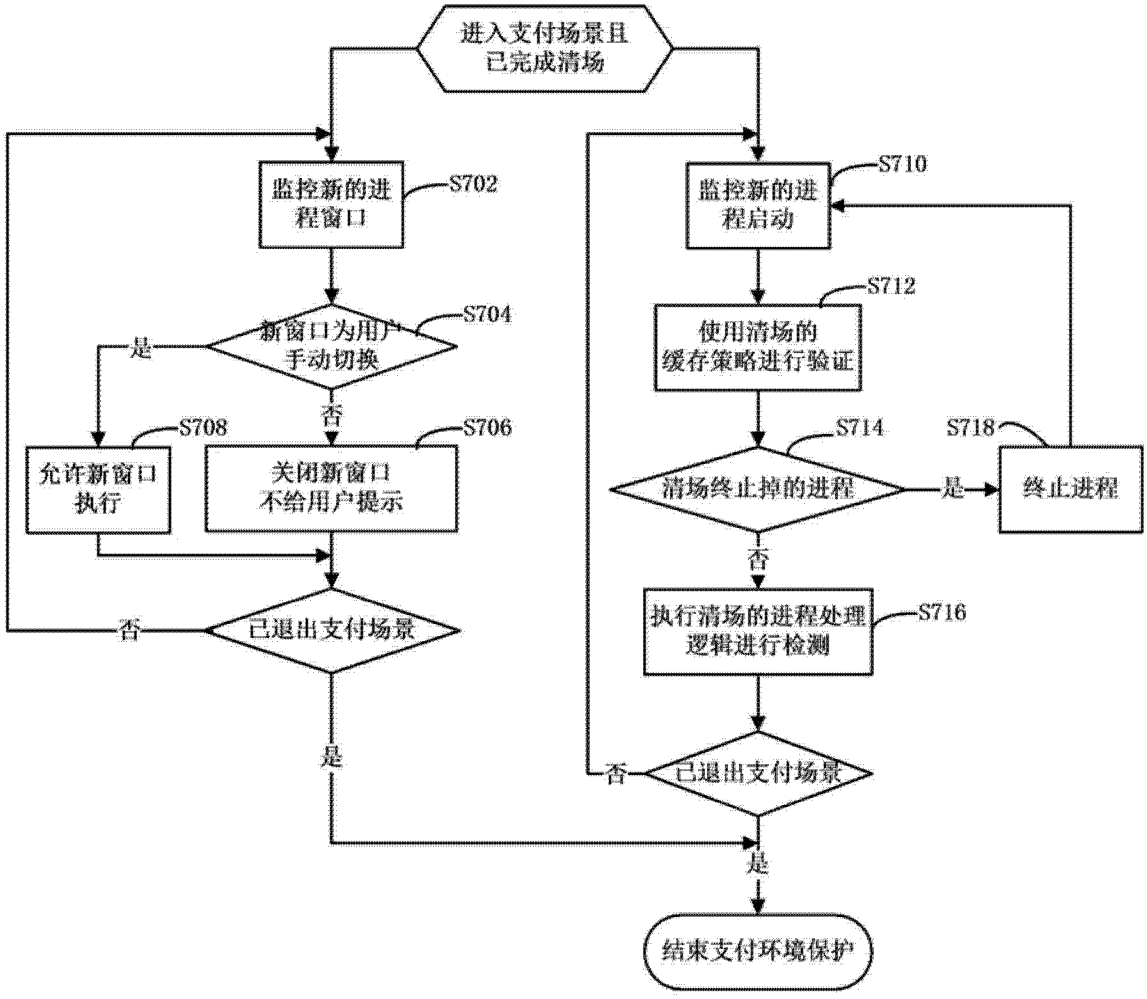

进入支付场景且
已完成清场
监控新的进
程窗口
S702
新窗口为用户
手动切换
S704
是
否
S708
允许新窗口
执行
S706
关闭新窗口
不给用户提示
否
已退出支付场景
是
S710
监控新的进
程启动
S712
使用清场的
缓存策略进行验证
S714
清场终止掉的进程
是
S718
终止进程
否
执行清场的进程处理
逻辑进行检测
S716
否
已退出支付场景
是
结束支付环境保护

图 7