



## (12) 发明专利申请

(10) 申请公布号 CN 104156657 A

(43) 申请公布日 2014. 11. 19

(21) 申请号 201410440696. X

(22) 申请日 2014. 09. 01

(71) 申请人 宇龙计算机通信科技(深圳)有限公司

地址 518040 广东省深圳市车公庙天安数码城创新科技广场 B 座 8 楼

(72) 发明人 岳蓬星 王振华

(74) 专利代理机构 北京友联知识产权代理事务所(普通合伙) 11343

代理人 尚志峰 汪海屏

(51) Int. Cl.

G06F 21/46 (2013. 01)

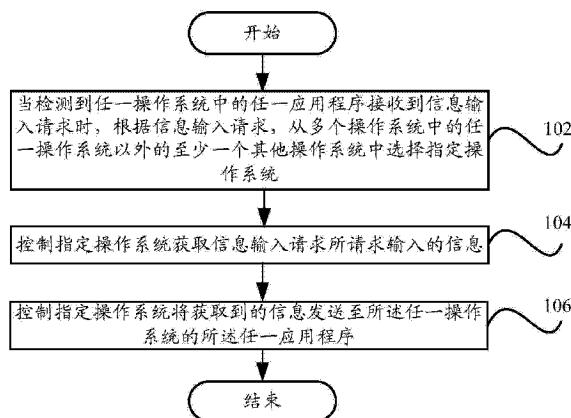
权利要求书2页 说明书9页 附图3页

### (54) 发明名称

终端的信息输入方法、终端的信息输入装置和终端

### (57) 摘要

本发明提出了一种终端的信息输入方法、一种终端的信息输入装置和一种终端，所述终端包括多个操作系统，其中，所述信息输入方法包括：当检测到任一操作系统中的任一应用程序接收到信息输入请求时，根据所述信息输入请求，从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统；控制所述指定操作系统获取所述信息输入请求所请求输入的信息；控制所述指定操作系统将获取到的所述信息发送至所述任一操作系统的所述任一应用程序。通过本发明的技术方案，避免了终端中输入的信息会被恶意软件、病毒等截取的问题，有效地保护了终端的信息安全，提升了用户的隐私安全性，增强了用户体验。



1. 一种终端的信息输入方法,所述终端包括多个操作系统,其特征在于,包括:

当检测到任一操作系统中的任一应用程序接收到信息输入请求时,根据所述信息输入请求,从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统;

控制所述指定操作系统获取所述信息输入请求所请求输入的信息;

控制所述指定操作系统将获取到的所述信息发送至所述任一操作系统的所述任一应用程序。

2. 根据权利要求 1 所述的终端的信息输入方法,其特征在于,所述根据所述信息输入请求,从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统,具体包括:

根据所述信息输入请求,确定所述至少一个其他操作系统中具有获取所述信息的权限的待选操作系统;以及

根据接收到的选择命令,从所述待选操作系统中选择所述指定操作系统,或根据所述待选操作系统的安全级别,选择具有最高所述安全级别的操作系统作为所述指定操作系统。

3. 根据权利要求 1 所述的终端的信息输入方法,其特征在于,所述根据所述信息输入请求,从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统,包括:

根据接收到的选择命令,从所述至少一个其他操作系统中选择所述指定操作系统;或

根据所述至少一个其他操作系统的安全级别,选择具有最高所述安全级别的操作系统作为所述指定操作系统。

4. 根据权利要求 2 或 3 所述的终端的信息输入方法,其特征在于,还包括:

根据所述多个操作系统中的每个操作系统的联网权限和 / 或联网类型,为所述每个操作系统设置安全级别。

5. 根据权利要求 2 或 3 所述的终端的信息输入方法,其特征在于,还包括:

根据访问所述多个操作系统中的每个操作系统时的验证方式,为所述每个操作系统设置安全级别。

6. 一种终端的信息输入装置,所述终端包括多个操作系统,其特征在于,包括:

选择单元,当检测到任一操作系统中的任一应用程序接收到信息输入请求时,根据所述信息输入请求,从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统;

控制单元,控制所述指定操作系统获取所述信息输入请求所请求输入的信息,以及控制所述指定操作系统将获取到的所述信息发送至所述任一操作系统的所述任一应用程序。

7. 根据权利要求 6 所述的终端的信息输入装置,其特征在于,所述选择单元包括:

确定单元,根据所述信息输入请求,确定所述至少一个其他操作系统中具有获取所述信息的权限的待选操作系统;

第一选择单元,根据接收到的选择命令,从所述待选操作系统中选择所述指定操作系统,或根据所述待选操作系统的安全级别,选择具有最高所述安全级别的操作系统作为所述指定操作系统;

第二选择单元，根据接收到的选择命令，从所述至少一个其他操作系统中选择所述指定操作系统；或根据所述至少一个其他操作系统的安全级别，选择具有最高所述安全级别的操作系统作为所述指定操作系统。

8. 根据权利要求 6 或 7 所述的终端的信息输入装置，其特征在于，还包括：

第一设置单元，根据所述多个操作系统中的每个操作系统的联网权限和 / 或联网类型，为所述每个操作系统设置安全级别。

9. 根据权利要求 6 或 7 所述的终端的信息输入装置，其特征在于，还包括：

第二设置单元，根据访问所述多个操作系统中的每个操作系统时的验证方式，为所述每个操作系统设置安全级别。

10. 一种终端，其特征在于，包括：

多个操作系统；以及

如权利要求 6 至 9 中任一项所述的终端的信息输入装置。

## 终端的信息输入方法、终端的信息输入装置和终端

### 技术领域

[0001] 本发明涉及终端技术领域，具体而言，涉及一种终端的信息输入方法、一种终端的信息输入装置和一种终端。

### 背景技术

[0002] 目前，在现有的双系统终端中，用户一般直接向终端的一个操作系统的应用程序中输入密码等重要信息，由该操作系统本身接收该重要信息并进行处理，在上述操作系统接收输入的信息并进行处理的过程中，尤其在接收输入的信息的过程中，输入的重要信息很容易被恶意软件或病毒等获取，保密性差，不利于对用户的隐私进行保护。

[0003] 因此，需要一种新的信息输入方法，可以在用户向操作系统的应用程序中输入信息时利用终端中的其他系统保护终端的信息安全，成为目前亟待解决的问题。

### 发明内容

[0004] 本发明正是基于上述技术问题，提出了一种新的技术方案，可以在用户向操作系统的应用程序中输入信息时利用终端中的其他系统保护终端的信息安全，避免用户的信息泄露。

[0005] 有鉴于此，本发明的一方面提出了一种终端的信息输入方法，所述终端包括多个操作系统，包括：当检测到任一操作系统中的任一应用程序接收到信息输入请求时，根据所述信息输入请求，从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统；控制所述指定操作系统获取所述信息输入请求所请求输入的信息；控制所述指定操作系统将获取到的所述信息发送至所述任一操作系统的所述任一应用程序。

[0006] 在该技术方案中，当任一操作系统的应用程序接收到信息输入请求时，使用指定操作系统接收输入的信息，比如，当用户打开手机中操作系统A的支付宝解锁界面时，即可视为接收到解锁密码输入请求，此时，将当前操作系统A切换为指定操作系统B，由指定操作系统B接收用户输入的解锁密码，从而避免用户的密码被当前操作系统A泄漏，并由指定操作系统B将输入的信息发送至当前操作系统A的支付宝程序中，进一步地，可以设置操作系统B仅能与当前操作系统A进行通信，或者设置操作系统B在接收来自当前操作系统A的信息并将该信息向当前操作系统A的支付宝程序发送的过程中仅能与当前操作系统A进行通信，以尽可能地保护该输入信息的安全，提升了用户的隐私安全。

[0007] 在上述技术方案中，优选地，所述根据所述信息输入请求，从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统，具体包括：根据所述信息输入请求，确定所述至少一个其他操作系统中具有获取所述信息的权限的待选操作系统；以及根据接收到的选择命令，从所述待选操作系统中选择所述指定操作系统，或根据所述待选操作系统的安全级别，选择具有最高所述安全级别的操作系统作为所述指定操作系统。

[0008] 在该技术方案中,输入的信息只能由多个操作系统中的当前操作系统以外的具有接收该信息的权限的部分操作系统掌握,并由用户直接在所述部分操作系统中选定指定操作系统,或在所述部分操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案,可以根据接收到的信息输入请求,从其他操作系统中选择出合适的指定操作系统,以增强信息输入的安全性。

[0009] 在上述技术方案中,优选地,所述根据所述信息输入请求,从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统,包括:根据接收到的选择命令,从所述至少一个其他操作系统中选择所述指定操作系统;或根据所述至少一个其他操作系统的安全级别,选择具有最高所述安全级别的操作系统作为所述指定操作系统。

[0010] 在该技术方案中,可以直接在多个操作系统中的当前操作系统以外的其他操作系统中选定指定操作系统,也可以在其他操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案,可以根据用户的需求或根据安全级别选择出最合适或最安全的指定操作系统,以增强信息输入的安全性。

[0011] 在上述技术方案中,优选地,还包括:控制所述指定操作系统保存所述信息。

[0012] 在该技术方案中,可以将接收到的输入信息保存起来,以方便下次调用。

[0013] 在上述技术方案中,优选地,所述控制所述指定操作系统获取所述信息输入请求所请求输入的信息,具体包括:判断所述指定操作系统中是否保存有所述信息,其中,当判断结果为是时,获取保存的所述信息;当判断结果为否时,获取输入的所述信息。

[0014] 在该技术方案中,由于已控制指定操作系统保存输入过的信息,可以在下次接收到相同的信息输入请求时,不用再次输入该信息就可以得到相同的处理结果,在保护输入信息的安全的同时,提升了用户操作的便利性。

[0015] 在上述技术方案中,优选地,还包括:根据所述多个操作系统中的每个操作系统的联网权限和/或联网类型,为所述每个操作系统设置安全级别。

[0016] 在该技术方案中,可以根据每个操作系统的联网权限和/或联网类型为每个操作系统分别设置安全级别,比如,手机中具有A、B、C三个操作系统,其中,操作系统A为禁止联网的安全系统,只能与操作系统B和C通信,操作系统B为只能连接2G网络的普通系统,操作系统C为可以连接3G网络、4G网络以及可以使用蓝牙功能的多功能系统,由此可知,操作系统A的安全性最高,而操作系统C受到木马或恶意软件攻击的可能性最高,则可以设置操作系统A的安全级别为高级,操作系统B的安全级别为中级,操作系统C的安全级别为低级,当操作系统B中的支付宝程序接收到密码输入请求时,优先选择操作系统A作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统B中的支付宝程序。

[0017] 在上述技术方案中,优选地,还包括:根据访问所述多个操作系统中的每个操作系统时的验证方式,为所述每个操作系统设置安全级别。

[0018] 在该技术方案中,还可以根据用户访问每个操作系统时的验证方式分别为每个操作系统设置安全级别,比如,手机中具有A、B、C三个操作系统,其中,用户可以直接访问操作系统A而不需要任何验证,用户在访问操作系统B时需要输入密码,而用户在访问操作系统C时需要先输入密码再进行指纹验证,则可以设置操作系统A的安全级别为低级,操作系统B的安全级别为中级,操作系统C的安全级别为高级。当操作系统B中的支付宝程序接

收到密码输入请求时,优先选择操作系统 C 作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统 B 中的支付宝程序。

[0019] 本发明的另一方面提出了一种终端的信息输入装置,所述终端包括多个操作系统,包括:选择单元,当检测到任一操作系统中的任一应用程序接收到信息输入请求时,根据所述信息输入请求,从所述多个操作系统中的所述任一操作系统以外的至少一个其他操作系统中选择指定操作系统;控制单元,控制所述指定操作系统获取所述信息输入请求所请求输入的信息,以及控制所述指定操作系统将获取到的所述信息发送至所述任一操作系统的所述任一应用程序。

[0020] 在该技术方案中,当任一操作系统接收到信息输入请求时,使用指定操作系统接收输入的信息,比如,当用户打开手机中操作系统 A 的支付宝解锁界面时,即可视为接收到解锁密码输入请求,此时,将当前操作系统 A 切换为指定操作系统 B,由指定操作系统 B 接收用户输入的解锁密码,从而避免用户的密码被当前操作系统 A 泄漏,并由指定操作系统 B 将输入的信息发送至当前操作系统 A 的支付宝程序中,进一步地,可以设置操作系统 B 仅能与当前操作系统 A 进行通信,或者设置操作系统 B 在接收来自当前操作系统 A 的信息并将该信息向当前操作系统 A 的支付宝程序发送的过程中仅能与当前操作系统 A 进行通信,以尽可能地保护该输入信息的安全,提升了用户的隐私安全。

[0021] 在上述技术方案中,优选地,所述选择单元包括:确定单元,根据所述信息输入请求,确定所述至少一个其他操作系统中具有获取所述信息的权限的待选操作系统;第一选择单元,根据接收到的选择命令,从所述待选操作系统中选择所述指定操作系统,或根据所述待选操作系统的安全级别,选择具有最高所述安全级别的操作系统作为所述指定操作系统;第二选择单元,根据接收到的选择命令,从所述至少一个其他操作系统中选择所述指定操作系统;或根据所述至少一个其他操作系统的安全级别,选择具有最高所述安全级别的操作系统作为所述指定操作系统。

[0022] 在该技术方案中,可以设置输入的信息只能由多个操作系统中的当前操作系统以外的具有接收该信息的权限的部分操作系统掌握,并由用户直接在所述部分操作系统中选定指定操作系统,或在所述部分操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案,可以根据接收到的信息输入请求,从其他操作系统中选择出合适的指定操作系统,以增强信息输入的安全性。

[0023] 在该技术方案中,也可以选择直接在多个操作系统中的当前操作系统以外的其他操作系统中选定指定操作系统,或其他操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案,可以根据用户的需求或根据安全级别选择出最合适或最安全的指定操作系统,以增强信息输入的安全性。

[0024] 在上述技术方案中,优选地,所述控制单元还用于:控制所述指定操作系统保存所述信息。

[0025] 在该技术方案中,可以将接收到的输入信息保存起来,以方便下次调用。

[0026] 在上述技术方案中,优选地,还包括:判断单元,判断所述指定操作系统中是否保存有所述信息;以及所述控制单元还用于:当判断结果为是时,控制所述指定操作系统获取保存的所述信息;当判断结果为否时,控制所述指定操作系统获取输入的所述信息。

[0027] 在该技术方案中,由于已控制指定操作系统保存输入过的信息,可以在下次接收

到相同的信息输入请求时,不用再次输入该信息就可以得到相同的处理结果,在保护输入信息的安全的同时,提升了用户操作的便利性。

[0028] 在上述技术方案中,优选地,还包括:第一设置单元,根据所述多个操作系统中的每个操作系统的联网权限和 / 或联网类型,为所述每个操作系统设置安全级别。

[0029] 在该技术方案中,可以根据每个操作系统的联网权限和 / 或联网类型为每个操作系统分别设置安全级别,比如,手机中具有A、B、C三个操作系统,其中,操作系统A为禁止联网的安全系统,只能与操作系统B和C通信,操作系统B为只能连接2G网络的普通系统,操作系统C为可以连接3G网络、4G网络以及可以使用蓝牙功能的多功能系统,由此可知,操作系统A的安全性最高,而操作系统C受到木马或恶意软件攻击的可能性最高,则可以设置操作系统A的安全级别为高级,操作系统B的安全级别为中级,操作系统C的安全级别为低级,当操作系统B中的支付宝程序接收到密码输入请求时,优先选择操作系统A作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统B中的支付宝程序。

[0030] 在上述技术方案中,优选地,还包括:第二设置单元,根据访问所述多个操作系统中的每个操作系统时的验证方式,为所述每个操作系统设置安全级别。

[0031] 在该技术方案中,还可以根据用户访问每个操作系统时的验证方式分别为每个操作系统设置安全级别,比如,手机中具有A、B、C三个操作系统,其中,用户可以直接访问操作系统A而不需要任何验证,用户在访问操作系统B时需要输入密码,而用户在访问操作系统C时需要先输入密码再进行指纹验证,则可以设置操作系统A的安全级别为低级,操作系统B的安全级别为中级,操作系统C的安全级别为高级。当操作系统B中的支付宝程序接收到密码输入请求时,优先选择操作系统C作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统B中的支付宝程序。

[0032] 本发明的再一方面提出了一种终端,包括有多个操作系统和上述技术方案中所述的终端的信息输入装置。因此,该终端具有上述技术方案提供的终端的信息输入装置的全部有益效果,在此不再赘述。

[0033] 通过以上技术方案,可以使输入的信息只能由指定操作系统接收,减少了信息泄漏的机会,提升了用户操作的便利性,从而避免了因接收信息输入请求的操作系统和 / 或操作系统中接收信息输入请求的应用程序不安全而造成的隐私泄露,有效地保护终端的信息安全,提升了用户的隐私安全。

## 附图说明

[0034] 图1示出了根据本发明的一个实施例的终端的信息输入方法的示意流程图;

[0035] 图2示出了根据本发明的又一实施例的终端的信息输入方法的示意流程图;

[0036] 图3示出了根据本发明的一个实施例的终端的信息输入装置的示意框图;

[0037] 图4示出了根据本发明的一个实施例的终端的示意框图;

[0038] 图5示出了根据本发明的又一实施例的终端的示意框图。

## 具体实施方式

[0039] 为了能够更清楚地理解本发明的上述目的、特征和优点,下面结合附图和具体实施方式对本发明进行进一步的详细描述。需要说明的是,在不冲突的情况下,本申请的实施

例及实施例中的特征可以相互组合。

[0040] 在下面的描述中阐述了很多具体细节以便于充分理解本发明，但是，本发明还可以采用其他不同于在此描述的其他方式来实施，因此，本发明的输入范围并不受下面公开的具体实施例的限制。

[0041] 图 1 示出了根据本发明的一个实施例的终端的信息输入方法的示意流程图。

[0042] 如图 1 所示，本发明的一个实施例的终端的信息输入方法用于具有多个操作系统的终端，包括：

[0043] 步骤 102，当检测到任一操作系统中的任一应用程序接收到信息输入请求时，根据信息输入请求，从多个操作系统中的任一操作系统以外的至少一个其他操作系统中选择指定操作系统。

[0044] 步骤 104，控制指定操作系统获取信息输入请求所请求输入的信息。

[0045] 步骤 106，控制指定操作系统将获取到的信息发送至所述任一操作系统的所述任一应用程序。

[0046] 在该技术方案中，当任一操作系统接收到信息输入请求时，使用指定操作系统接收输入的信息，比如，当用户打开手机中操作系统 A 的支付宝解锁界面时，即可视为接收到解锁密码输入请求，此时，将当前操作系统 A 切换为指定操作系统 B，由指定操作系统 B 接收用户输入的解锁密码，从而避免用户的密码被当前操作系统 A 泄漏，并由指定操作系统 B 将输入的信息发送至当前操作系统 A 的支付宝程序中，进一步地，可以设置操作系统 B 仅能与当前操作系统 A 进行通信，或者设置操作系统 B 在接收来自当前操作系统 A 的信息并将该信息向当前操作系统 A 的支付宝程序发送的过程中仅能与当前操作系统 A 进行通信，以尽可能地保护该输入信息的安全，提升了用户的隐私安全。

[0047] 在上述技术方案中，优选地，在步骤 102 中，具体包括：根据信息输入请求，确定至少一个其他操作系统中具有获取信息的权限的待选操作系统；以及根据接收到的选择命令，从待选操作系统中选择指定操作系统，或根据待选操作系统的安全级别，选择具有最高安全级别的操作系统作为指定操作系统。

[0048] 在该技术方案中，输入的信息只能由多个操作系统中的当前操作系统以外的具有接收该信息的权限的部分操作系统掌握，并由用户直接在部分操作系统中选定指定操作系统，或在部分操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案，可以根据接收到的信息输入请求，从其他操作系统中选择出合适的指定操作系统，以增强信息输入的安全性。

[0049] 在上述技术方案中，优选地，在步骤 102 中，包括：根据接收到的选择命令，从至少一个其他操作系统中选择指定操作系统；或根据至少一个其他操作系统的安全级别，选择具有最高安全级别的操作系统作为指定操作系统。

[0050] 在该技术方案中，可以直接在多个操作系统中的当前操作系统以外的其他操作系统中选定指定操作系统，也可以在其他操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案，可以根据用户的需求或根据安全级别选择出最合适或最安全的指定操作系统，以增强信息输入的安全性。

[0051] 在上述技术方案中，优选地，还包括：控制指定操作系统保存信息。

[0052] 在该技术方案中，可以将接收到的输入信息保存起来，以方便下次调用。

[0053] 在上述技术方案中,优选地,步骤 104 具体包括:判断指定操作系统中是否保存有信息,其中,当判断结果为是时,获取保存的信息;当判断结果为否时,获取输入的信息。

[0054] 在该技术方案中,由于已控制指定操作系统保存输入过的信息,可以在下次接收到相同的信息输入请求时,不用再次输入该信息就可以得到相同的处理结果,在保护输入信息的安全的同时,提升了用户操作的便利性。

[0055] 在上述技术方案中,优选地,还包括:根据多个操作系统中的每个操作系统的联网权限和 / 或联网类型,为每个操作系统设置安全级别。

[0056] 在该技术方案中,可以根据每个操作系统的联网权限和 / 或联网类型为每个操作系统分别设置安全级别,比如,手机中具有 A、B、C 三个操作系统,其中,操作系统 A 为禁止联网的安全系统,只能与操作系统 B 和 C 通信,操作系统 B 为只能连接 2G 网络的普通系统,操作系统 C 为可以连接 3G 网络、4G 网络以及可以使用蓝牙功能的多功能系统,由此可知,操作系统 A 的安全性最高,而操作系统 C 受到木马或恶意软件攻击的可能性最高,则可以设置操作系统 A 的安全级别为高级,操作系统 B 的安全级别为中级,操作系统 C 的安全级别为低级,当操作系统 B 中的支付宝程序接收到密码输入请求时,优先选择操作系统 A 作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统 B 中的支付宝程序。

[0057] 在上述技术方案中,优选地,还包括:根据访问多个操作系统中的每个操作系统时的验证方式,为每个操作系统设置安全级别。

[0058] 在该技术方案中,还可以根据用户访问每个操作系统时的验证方式分别为每个操作系统设置安全级别,比如,手机中具有 A、B、C 三个操作系统,其中,用户可以直接访问操作系统 A 而不需要任何验证,用户在访问操作系统 B 时需要输入密码,而用户在访问操作系统 C 时需要先输入密码再进行指纹验证,则可以设置操作系统 A 的安全级别为低级,操作系统 B 的安全级别为中级,操作系统 C 的安全级别为高级。当操作系统 B 中的支付宝程序接收到密码输入请求时,优先选择操作系统 C 作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统 B 中的支付宝程序。

[0059] 图 2 示出了根据本发明的又一实施例的终端的信息输入方法的示意流程图。

[0060] 如图 2 所示,本发明的又一实施例的终端的信息输入方法用于具有系统 A 和系统 B 的终端,包括:

[0061] 步骤 202,系统 A 接收到密码采集请求。

[0062] 步骤 204,判断是否允许密码采集,当判断结果为是时,进入步骤 206,当判断结果为否时,返回步骤 202,等待下一次密码采集请求。

[0063] 步骤 206,系统 B 进行密码采集,即系统 B 接收输入的密码。通过使输入系统 A 的密码只能由系统 B 接收,减少了信息泄漏的机会,从而避免了因系统 A 不安全而造成密码在输入过程中被泄露,可以有效地保护终端的信息安全。

[0064] 步骤 208,判断是否完成密码采集,当判断结果为是时,进入步骤 210,当判断结果为否时,返回步骤 206,继续由系统 B 进行密码采集。

[0065] 步骤 210,将采集结果发送至系统 A。

[0066] 图 3 示出了根据本发明的一个实施例的终端的信息输入装置的示意框图。

[0067] 如图 3 所示,本发明的一个实施例的终端的信息输入装置 300 用于具有多个操作系统的终端,包括:选择单元 302,当检测到任一操作系统中的任一应用程序接收到信息输

入请求时,根据信息输入请求,从多个操作系统中的任一操作系统以外的至少一个其他操作系统中选择指定操作系统;控制单元 304,控制指定操作系统获取信息输入请求所请求输入的信息,以及控制指定操作系统将获取到的信息发送至所述任一操作系统的所述任一应用程序。

[0068] 在该技术方案中,当任一操作系统接收到信息输入请求时,使用指定操作系统接收输入的信息,比如,当用户打开手机中操作系统 A 的支付宝解锁界面时,即可视为接收到解锁密码输入请求,此时,将当前操作系统 A 切换为指定操作系统 B,由指定操作系统 B 接收用户输入的解锁密码,从而避免用户的密码被当前操作系统 A 泄漏,并由指定操作系统 B 将输入的信息发送至当前操作系统 A 的支付宝程序中,进一步地,可以设置操作系统 B 仅能与当前操作系统 A 进行通信,或者设置操作系统 B 在接收来自当前操作系统 A 的信息并将该信息向当前操作系统 A 的支付宝程序发送的过程中仅能与当前操作系统 A 进行通信,以尽可能地保护该输入信息的安全,提升了用户的隐私安全。

[0069] 在上述技术方案中,优选地,选择单元 302 包括:确定单元 3022,根据信息输入请求,确定至少一个其他操作系统中具有获取信息的权限的待选操作系统;第一选择单元 3024,根据接收到的选择命令,从待选操作系统中选择指定操作系统,或根据待选操作系统的安全级别,选择具有最高安全级别的操作系统作为指定操作系统;第二选择单元 3026,根据接收到的选择命令,从至少一个其他操作系统中选择指定操作系统;或根据至少一个其他操作系统的安全级别,选择具有最高安全级别的操作系统作为指定操作系统。

[0070] 在该技术方案中,可以设置输入的信息只能由多个操作系统中的当前操作系统以外的具有接收该信息的权限的部分操作系统掌握,并由用户直接在部分操作系统中选定指定操作系统,或在部分操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案,可以根据接收到的信息输入请求,从其他操作系统中选择出合适的指定操作系统,以增强信息输入的安全性。

[0071] 在该技术方案中,也可以选择直接在多个操作系统中的当前操作系统以外的其他操作系统中选定指定操作系统,或其他操作系统中选择安全级别最高的系统作为指定操作系统。通过上述技术方案,可以根据用户的需求或根据安全级别选择出最合适或最安全的指定操作系统,以增强信息输入的安全性。

[0072] 在上述技术方案中,优选地,控制单元 304 还用于:控制指定操作系统保存信息。

[0073] 在该技术方案中,可以将接收到的输入信息保存起来,以方便下次调用。

[0074] 在上述技术方案中,优选地,还包括:判断单元 306,判断指定操作系统中是否保存有信息;以及控制单元 304 还用于:当判断结果为是时,控制指定操作系统获取保存的信息;当判断结果为否时,控制指定操作系统获取输入的信息。

[0075] 在该技术方案中,由于已控制指定操作系统保存输入过的信息,可以在下次接收到相同的信息输入请求时,不用再次输入该信息就可以得到相同的处理结果,在保护输入信息的安全的同时,提升了用户操作的便利性。

[0076] 在上述技术方案中,优选地,还包括:第一设置单元 308,根据多个操作系统中的每个操作系统的联网权限和 / 或联网类型,为每个操作系统设置安全级别。

[0077] 在该技术方案中,可以根据每个操作系统的联网权限和 / 或联网类型为每个操作系统分别设置安全级别,比如,手机中具有 A、B、C 三个操作系统,其中,操作系统 A 为禁止联

网的安全系统,只能与操作系统B和C通信,操作系统B为只能连接2G网络的普通系统,操作系统C为可以连接3G网络、4G网络以及可以使用蓝牙功能的多功能系统,由此可知,操作系统A的安全性最高,而操作系统C受到木马或恶意软件攻击的可能性最高,则可以设置操作系统A的安全级别为高级,操作系统B的安全级别为中级,操作系统C的安全级别为低级,当操作系统B中的支付宝程序接收到密码输入请求时,优先选择操作系统A作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统B中的支付宝程序。

[0078] 在上述技术方案中,优选地,还包括:第二设置单元310,根据访问多个操作系统中的每个操作系统时的验证方式,为每个操作系统设置安全级别。

[0079] 在该技术方案中,还可以根据用户访问每个操作系统时的验证方式分别为每个操作系统设置安全级别,比如,手机中具有A、B、C三个操作系统,其中,用户可以直接访问操作系统A而不需要任何验证,用户在访问操作系统B时需要输入密码,而用户在访问操作系统C时需要先输入密码再进行指纹验证,则可以设置操作系统A的安全级别为低级,操作系统B的安全级别为中级,操作系统C的安全级别为高级。当操作系统B中的支付宝程序接收到密码输入请求时,优先选择操作系统C作为指定操作系统来接收输入的密码,并将接收到的密码发送至操作系统B中的支付宝程序。

[0080] 图4示出了根据本发明的一个实施例的终端的示意框图。

[0081] 如图4所示,本发明的一个实施例的终端400包括:多个操作系统402和信息输入装置404(相当于图3示出的实施例中的终端的信息输入装置300)。

[0082] 其中,信息输入装置404用于在任一操作系统中的应用程序接收到信息输入请求时,控制指定操作系统接收输入的信息,并将对输入的信息的处理结果发送给所述任一操作系统中的所述应用程序。比如,当用户打开手机支付宝解锁界面时,即可视为接收到解锁密码输入请求,此时,信息输入装置404将当前的所述任一操作系统切换为指定操作系统,由指定操作系统接收用户输入的解锁密码,并将解锁密码发送给所述任一操作系统中的所述应用程序,从而避免用户的密码被当前操作系统泄漏。

[0083] 通过上述技术方案,使输入的信息只能由指定操作系统接收,减少了信息泄漏的机会,从而避免了因接收信息输入请求的操作系统和/或操作系统中接收信息输入请求的应用程序不安全而造成的隐私泄露,可以有效地保护终端的信息安全,提升了用户的隐私安全。

[0084] 图5示出了根据本发明的又一实施例的终端的示意框图。

[0085] 如图5所示,根据本发明的又一实施例的终端500由两个系统即系统A和系统B构成。其中,系统A为一般的操作系统,系统B为带有输入信息保护功能的系统,用于处理系统A接收到的密码输入请求,接收输入的密码,并可以接收到的密码发送至系统A。

[0086] 因此,密码只能在系统B中输入,而不会因系统A中误安装恶意软件而带入病毒等原因造成在输入密码过程中密码被他人截取,这样,减少了密码泄漏的机会,有效地保护了终端的信息安全。

[0087] 在本发明中,术语“第一”、“第二”仅用于描述的目的,而不能理解为指示或暗示相对重要性。对于本领域的普通技术人员而言,可以根据具体情况理解上述术语在本发明中的具体含义。

[0088] 以上结合附图详细说明了本发明的技术方案,通过本发明的技术方案,可以使输

入的信息只能由指定操作系统接收，减少了信息泄漏的机会，提升了用户操作的便利性，从而避免了因接收信息输入请求的操作系统和 / 或操作系统中接收信息输入请求的应用程序不安全而造成的隐私泄露，有效地保护终端的信息安全，提升了用户的隐私安全。

[0089] 以上所述仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的输入范围之内。

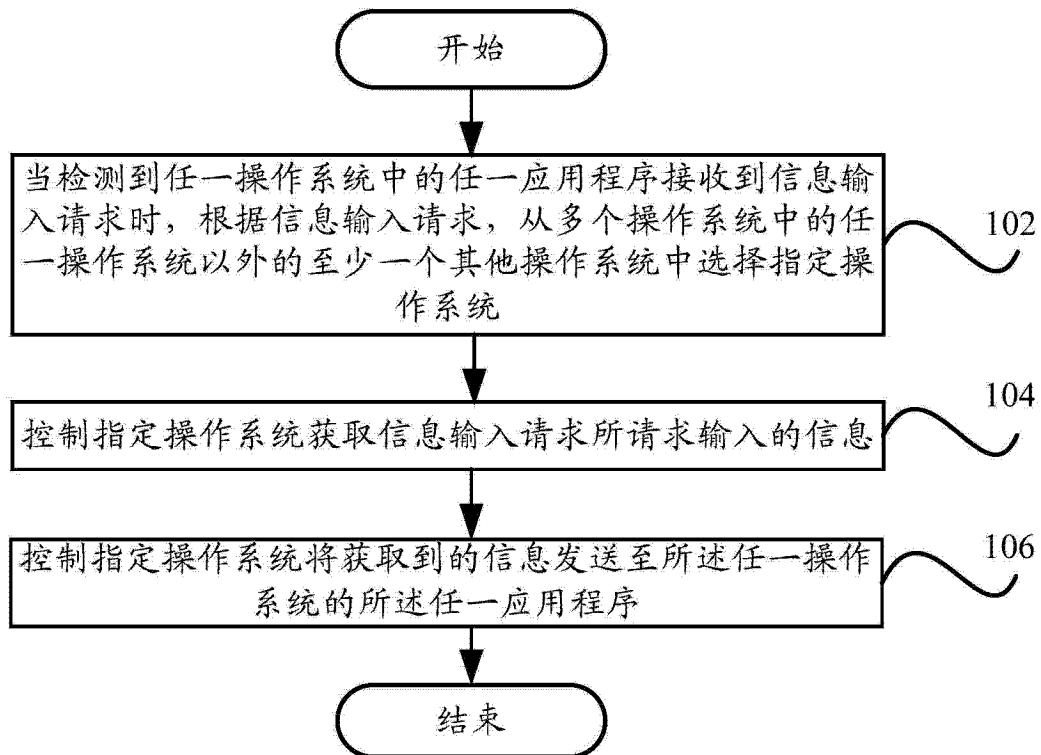


图 1

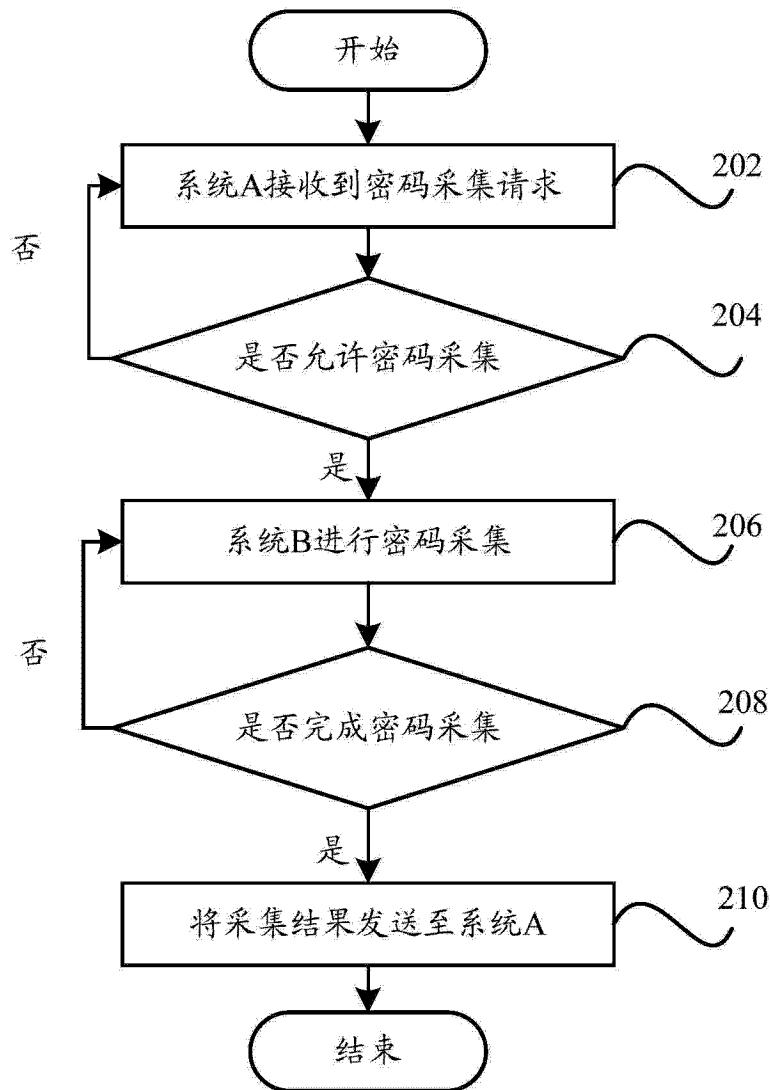


图 2

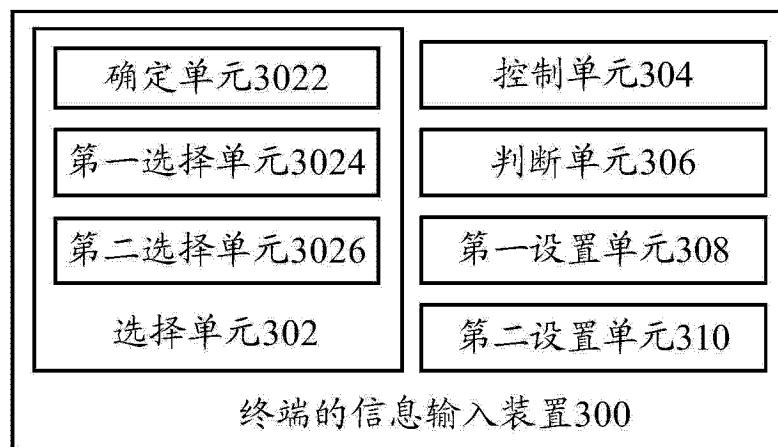


图 3

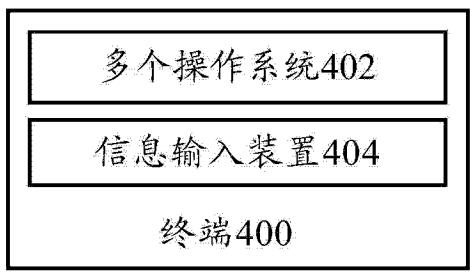


图 4

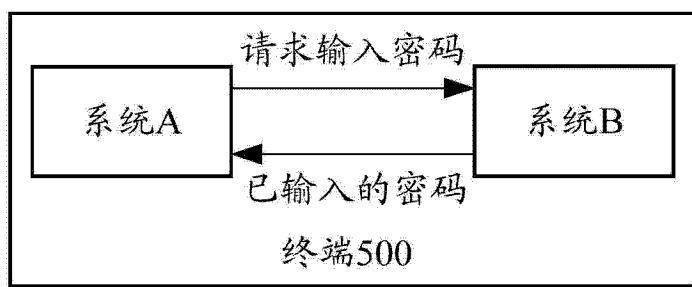


图 5