I628558

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I628558 B**

(45)公告日： 中華民國 107 (2018) 年 07 月 01 日

(21)申請案號：103120170 (22)申請日： 中華民國 103 (2014) 年 06 月 11 日

(51)Int. Cl.： *G06F21/82 (2013.01)* *G06F21/60 (2013.01)*

(30)優先權：2013/06/25 中國大陸 201310255179.0

(71)申請人：中國銀聯股份有限公司 (中國大陸) (CN)
中國大陸

(72)發明人：柴洪峰 (CN)；魯志軍 (CN)；何朔 (CN)；郭偉 (CN)；周鈺 (CN)；陳成錢 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN 1609809A CN 101030238A

US 2008/0098229A1

審查人員：許人偉

申請專利範圍項數：10 項 圖式數：2 共 15 頁

(54)名稱

指示移動設備操作環境的方法和能夠指示操作環境的移動設備

(57)摘要

本發明公開一種指示移動設備操作環境的方法和能夠指示操作環境的移動設備。該方法包括以下步驟：生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統訪問的儲存區，當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示該個人化資訊，以向使用者指示當前運行的作業系統。

指定代表圖：

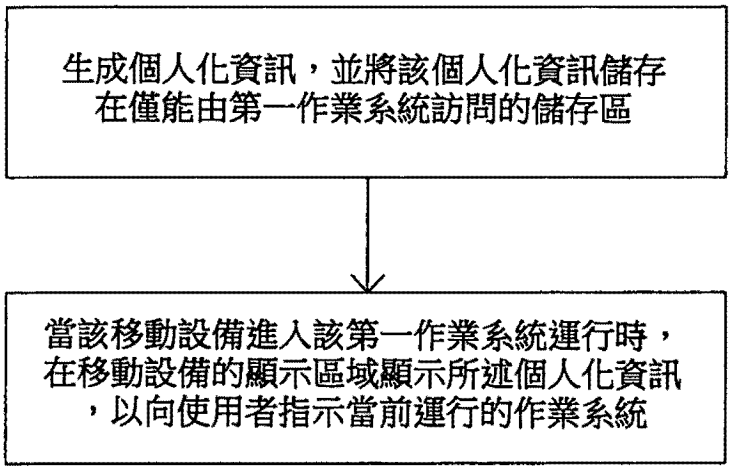

圖 1

發明專利說明書

（本說明書格式、順序，請勿任意更動）

【發明名稱】(中文/英文)

指示移動設備操作環境的方法和能夠指示操作環境的移動設備

【技術領域】

[0001] 本發明係關於移動設備安全性，並且尤其關於指示移動設備操作環境的方法和能夠指示操作環境的移動設備。

【先前技術】

[0002] 當前移動設備的作業系統由於強大的功能，複雜的程式碼和開放的平臺，會產生作業系統漏洞，這些漏洞會對作業系統的安全構成威脅。

[0003] 另一方面，用戶也可能因下載安裝惡意程式（例如，木馬、病毒）而洩漏使用者資訊。移動設備（例如，智慧手機）的人機界面（諸如螢幕、鍵盤等）是使用者與移動設備內的應用進行交互的最重要途徑。因此，使用者在使用人機界面輸入資訊時（例如，銀行卡帳戶和密碼等私密資訊），這些資訊可能被惡意程式所獲取。

[0004] 現有技術中，透過運行安全作業系統來防止惡意程式對私密資訊的竊取和篡改。安全作業系統指運行在安全模式下的一個封閉式作業系統，其為移動設備提供

可信執行環境，並且獨立於非安全模式下作業系統。安全作業系統例如可以是基於 ARM 公司的 Trust Zone 技術的 TEE 方案。TEE 是一種安全模式下的可信執行環境平臺，在該平臺上，在安全程式碼的控制之下，惡意程式無法訪問該安全模式下的資料資源或竊取資料資源，例如使用者資訊。例如，對人機界面來說，當處於移動設備安全模式時，該人機界面只被在安全系統操控，因此使用者能夠安全地透過該人機界面與應用交互。換句話說，在安全模式下，該人機界面是可信的。

[0005] 移動設備的螢幕作為一種公共介面可以被移動設備上所有程式進行訪問和使用，雖然在安全作業系統控制下可以保證該螢幕的可靠性，安全性仍然會受到挑戰。例如，惡意程式可以模擬安全作業系統下的操作環境來迷惑使用者從而竊取使用者資訊。因此，為進一步增加移動設備使用的安全性，需要一種指示操作環境的方案來提示使用者當前移動設備的操作環境，包括移動設備當前是否處於安全模式，即當前運行的作業系統是否為安全作業系統（例如，利用可靠的指示資訊來告知使用者當前正在操作的人機界面確實可信）。另外，由於存在可插拔的載體，應用動態使用也會對使用者的資訊構成潛在的威脅，因此，指示使用者當前移動設備的操作環境較佳地還可以指示移動設備當前操作的應用的安全程度。

【發明內容】

[0025] 在一個實施例中，在所述移動設備第一次被啟動時生成所述個人化資訊。在移動設備第一次啟動時，由於移動設備尚未被使用，因此是可信的、安全的，這能夠保證輸入的個人化資訊的安全性。

[0026] 在一個實施例中，所述顯示區域可以是在移動設備螢幕上設置的特定區域。

[0027] 在一個實施例中，當該移動設備運行在安全作業系統時，在移動設備的顯示區域進一步顯示當前操作的應用的最終可信等級，以向使用者指示當前操作的應用的安全性。例如，可以在顯示區域的左邊顯示個人化資訊，在顯示區域的右邊顯示應用的最終可信等級。應用的最終可信等級表示該應用防篡改、防洩密、防仿冒、防攻擊的能力。這樣，用戶就知道當前操作的應用的安全性，讓使用者在面對低可信等級的應用時，提高警惕，並進一步確認要操作的應用是否是自己所要的應用。

[0028] 應用的最終可信等級基於應用可信等級和應用的載體可信等級生成。

[0029] 應用可信等級基於應用是否經過所述安全作業系統的認證和/或應用的載體，其中，所述載體是物理安全載體或者虛擬安全載體。舉例來說，對於同一個應用，如果該應用處於物理安全載體，那麼就比處於虛擬安全載體的該應用具有更高的可信等級。這是因為物理安全載體還包括了獨立的硬體，而這樣的獨立的硬體是具有高安全性，可防禦物理攻擊的。應用可信等級的具體分級方

式可根據實際情況的不同而有不同的劃分，作為示例，可以對應用的可信等級劃分為低、中、高三種等級，其中位於安全載體（SIM 卡、智慧卡等）上的被安全作業系統認證過的應用為高可信等級，對於虛擬安全載體（VSE，virtual secure element）上的通過安全作業系統認證的應用為中可信等級，對於那些未與安全作業系統進行認證的應用為低可信等級。

[0030] 所述應用的載體的可信等級基於該載體是否經過所述安全作業系統的認證。

[0031] 由此，本發明可以結合應用可信等級（應用本身可信程度）和應用的載體可信等級（應用實際所運行環境的可信程度）來確定應用的實際可信等級，即應用的最終可信等級。例如，一個高可信等級的應用在低可信等級的環境中運行時，該應用的實際可信等級可以被確定為中可信等級。

[0032] 在一個實施例中，可以將所述應用可信等級、所述應用的載體可信等級、應用標識儲存在可信等級清單中，當一個應用被選擇啟動作為當前應用時，根據該可信等級清單來獲得當前應用的最終可信等級。作為示例，當前應用的最終可信等級顯示的形式可以採用文字（如可在顯示區域顯示文字“高”代表高可信等級、“中”代表中可信等級、“低”代表低可信等級）、圖像顯示等，也可透過顏色來表示等級。

[0033] 圖 2 是根據本發明實施例的能夠指示操作環

境的移動設備的示意圖。如圖 2 所示，該移動設備包括個人化資訊模組和指示器模組。其中，個人化資訊模組，用於生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統中的指示器模組訪問的儲存區。指示器模組，用於當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示所述個人化資訊，以向使用者指示當前運行的作業系統。

[0034] 應當理解的是，所描述的各態樣和/或實施例僅僅是實例，並且可採用其它態樣和/或實施例，且在不背離本公開的範圍的情況下可做出結構的和功能的修改。另外，儘管可以僅關於若干實施方式中的一個已公開實施例的特定特徵或態樣，但可針對任何給定的或特定的應用所期望和有利地，這種特徵或態樣可與其它實施方式的一種或多個其它特徵或態樣相組合。

公告本

發明摘要

※申請案號：103120170

※申請日：103 年 06 月 11 日　　**※IPC 分類：** *G06F 21/82* (2013.01)
G06F 21/60 (2013.01)

【發明名稱】(中文/英文)

指示移動設備操作環境的方法和能夠指示操作環境的移動設備

【中文】

本發明公開一種指示移動設備操作環境的方法和能夠指示操作環境的移動設備。該方法包括以下步驟：生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統訪問的儲存區，當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示該個人化資訊，以向使用者指示當前運行的作業系統。

【英文】

圖 式

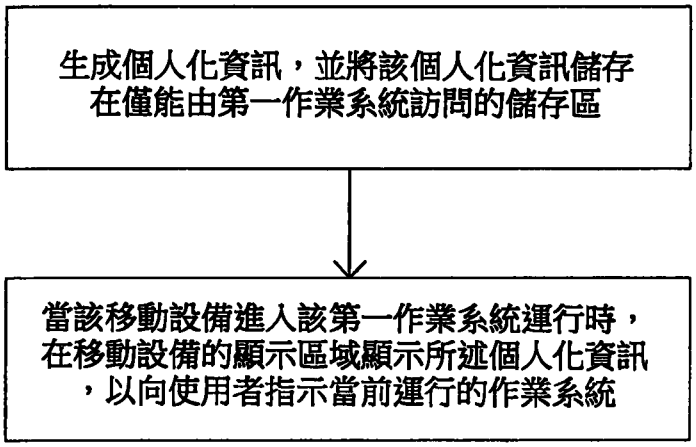
生成個人化資訊，並將該個人化資訊儲存在僅能由第一作業系統訪問的儲存區
當該移動設備進入該第一作業系統運行時，在移動設備的顯示區域顯示所述個人化資訊，以向使用者指示當前運行的作業系統

圖 1

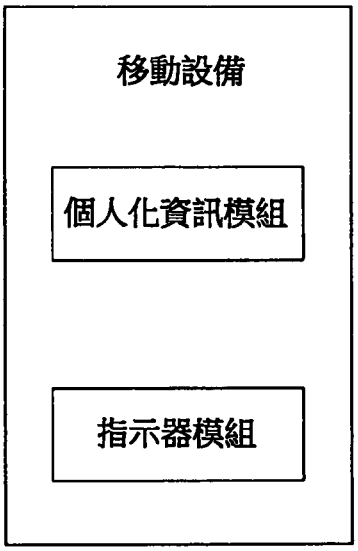
移動設備
個人化資訊模組
指示器模組

圖 2

【代表圖】

【本案指定代表圖】：第(1)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

[0006] 根據本發明的一個目的，公開一種指示移動設備操作環境的方法，包括以下步驟：

生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統訪問的儲存區，

當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示所述個人化資訊，以向使用者指示當前運行的作業系統。

[0007] 該方法還包括以下步驟：

基於使用者的輸入來生成所述個人化資訊，所述個人化資訊包括文字、圖像或者文字和圖像的組合。

[0008] 該方法還包括以下步驟：

在所述移動設備第一次被啟動時生成所述個人化資訊。

[0009] 該方法還包括以下步驟：

當該移動設備運行在安全作業系統時，在移動設備的顯示區域進一步顯示當前操作的應用的最終可信等級，以向使用者指示當前操作的應用的安全性。

[0010] 應用的最終可信等級基於應用可信等級和應用的載體可信等級生成，其中，所述應用可信等級基於應用是否經過所述安全作業系統的認證和/或應用的載體，其中，所述載體是物理安全載體或者虛擬安全載體，所述應用的載體可信等級基於該載體是否經過所述安全作業系統的認證。

[0011] 該方法還包括以下步驟：

將所述應用可信等級、所述應用的載體可信等級、應用標識儲存在可信等級清單中，

當一個應用被選擇啟動作為當前應用時，根據該可信等級清單來獲得當前應用的最終可信等級。

[0012] 根據本發明的另一個目的，公開一種能夠指示操作環境的移動設備，該移動設備包括：

個人化資訊模組，用於生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統中的指示器模組訪問的儲存區，

指示器模組，用於當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示所述個人化資訊，以向使用者指示當前運行的作業系統。

[0013] 所述個人化資訊模組基於使用者的輸入來生成所述個人化資訊，所述個人化資訊包括文字、圖像或者文字和圖像的組合。

[0014] 所述個人化資訊模組在所述移動設備第一次被啟動時生成所述個人化資訊。

[0015] 當該移動設備運行在安全作業系統時，該指示器模組在移動設備的顯示區域進一步顯示當前操作的應用的最終可信等級，以向使用者指示當前操作的應用的安全性。

[0016] 應用的最終可信等級基於應用可信等級和應用的載體可信等級生成，其中，

所述應用可信等級基於應用是否經過所述安全作業系

統的認證和/或應用的載體，其中，所述載體是物理安全載體或者虛擬安全載體，

所述應用的載體可信等級基於該載體是否經過所述安全作業系統的認證。

[0017] 該指示器模組還用於將所述應用可信等級、所述應用的載體可信等級、應用標識儲存在可信等級清單中，

當一個應用被選擇啟動作為當前應用時，該指示器模組被配置成根據該可信等級清單來獲得當前應用的最終可信等級。

【圖式簡單說明】

[0018] 在參照附圖閱讀了本發明的具體實施方式以後，本領域技術人員將會更清楚地瞭解本發明的各個態樣。本領域技術人員應當理解的是，這些附圖僅僅用於配合具體實施方式說明本發明的技術方案，而並非意在對本發明的保護範圍構成限制。其中，

圖 1 是根據本發明實施例的指示移動設備操作環境的方法的示意圖。

[0019] 圖 2 是根據本發明實施例的能夠指示操作環境的移動設備的示意圖。

【實施方式】

[0020] 下面參照附圖，對本發明的具體實施方式作

進一步的詳細描述。在下面的描述中，為了解釋的目的，陳述許多具體細節以便提供對實施例的一個或多個態樣的透徹理解。然而，對於本領域技術人員可以顯而易見的是，可以這些具體細節的較少程度來實踐各實施例的一個或多個態樣。因此下面的描述不被視為局限性的，而是透過所附申請專利範圍來限定保護範圍。

[0021] 圖 1 是根據本發明實施例的指示移動設備操作環境的方法的示意圖。如圖 1 所示，指示移動設備操作環境的方法包括以下步驟：

第一個步驟：生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統訪問的儲存區。

[0022] 第二個步驟：當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示所述個人化資訊，以向使用者指示當前運行的作業系統。

[0023] 在一個實施例中，儲存區中的個人化資訊僅僅能由安全作業系統的指示器模組訪問，如此能夠防止惡意程式獲取個人化資訊。

[0024] 在一個實施例中，可以基於用戶的輸入來生成所述個人化資訊，所述個人化資訊包括文字、圖像或者文字和圖像的組合。個人化資訊透過使用者生成，具有特有性，因而能夠防止非安全模式下的惡意程式仿冒這些資訊來欺騙使用者。作為示例，這些個人化資訊可以是由使用者編輯的圖形、選擇的圖案、拍攝的圖像、輸入的文字（例如，使用者最愛的食物，最喜歡的動物）。

第 103120170 號 民國 105 年 3 月 23 日修正

申請專利範圍

1. 一種指示移動設備操作環境的方法，其特徵在於，包括以下步驟：

生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統訪問的儲存區；

當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示該個人化資訊，以向使用者指示當前運行的作業系統；

當該移動設備運行在安全作業系統時，在移動設備的顯示區域進一步顯示當前操作的應用的最終可信等級，以向使用者指示當前操作的應用的安全性。

2. 如申請專利範圍第 1 項所述的方法，其中，還包括以下步驟：

基於使用者的輸入來生成該個人化資訊，該個人化資訊包括文字、圖像或者文字和圖像的組合。

3. 如申請專利範圍第 2 項所述的方法，其中，還包括以下步驟：

在該移動設備第一次被啟動時生成該個人化資訊。

4. 如申請專利範圍第 1 項所述的方法，其中，

應用的最終可信等級基於應用可信等級和應用的載體可信等級生成，其中，

該應用可信等級基於應用是否經過該安全作業系統的認證和/或應用的載體，其中，該載體是物理安全載體或者虛擬安全載體，

該應用的載體可信等級基於該載體是否經過該安全作業系統的認證。

5. 如申請專利範圍第 4 項所述的方法，其中，還包括以下步驟：

將該應用可信等級、該應用的載體可信等級、應用標識儲存在可信等級清單中，

當一個應用被選擇啟動作為當前應用時，根據該可信等級清單來獲得當前應用的最終可信等級。

6. 一種能夠指示操作環境的移動設備，其特徵在於，該移動設備包括：

個人化資訊模組，用於生成個人化資訊，並將該個人化資訊儲存在僅能由安全作業系統中的指示器模組訪問的儲存區；

指示器模組，用於當該移動設備進入該安全作業系統運行時，在移動設備的顯示區域顯示該個人化資訊，以向使用者指示當前運行的作業系統；

當該移動設備運行在安全作業系統時，該指示器模組在移動設備的顯示區域進一步顯示當前操作的應用的最終可信等級，以向使用者指示當前操作的應用的安全性。

7. 如申請專利範圍第 6 項所述的移動設備，其中，

該個人化資訊模組基於使用者的輸入來生成該個人化資訊，該個人化資訊包括文字、圖像或者文字和圖像的組合。

8. 如申請專利範圍第 7 項所述的移動設備，其中，

S

該個人化資訊模組在該移動設備第一次被啟動時生成該個人化資訊。

9. 如申請專利範圍第 8 項所述的移動設備，其中，

應用的最終可信等級基於應用可信等級和應用的載體可信等級生成，其中，

該應用可信等級基於應用是否經過該安全作業系統的認證和/或應用的載體，其中，該載體是物理安全載體或者虛擬安全載體，

該應用的載體可信等級基於該載體是否經過該安全作業系統的認證。

10. 如申請專利範圍第 9 項所述的移動設備，其中，

該指示器模組還用於將該應用可信等級、該應用的載體可信等級、應用標識儲存在可信等級清單中，

當一個應用被選擇啟動作為當前應用時，該指示器模組被配置成根據該可信等級清單來獲得當前應用的最終可信等級。